Check for updates

NIST Special Publication
NIST SP 800-63B-4

Digital Identity Guidelines

Authentication and Authenticator Management

David Temoshok
James L. Fenton
Yee-Yin Choong
Naomi Lefkovitz
Andrew Regenscheid
Ryan Galluzzo
Justin P. Richer

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63B-4

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Check for updates

NIST 特别出版物
NIST SP 800-63B-4

数字身份指南

认证与认证器管理

大卫·特莫肖克詹
姆斯·L.芬顿·余-
尹·钟娜奥米·莱
夫科维茨
安德鲁·雷根沙伊德
瑞安·加卢佐 贾斯汀·P·
里彻

本出版物可从以下网址免费获取：
https://doi.org/10.6028/NIST.SP.800-63B-4

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

本译本由机器翻译生成，供快速理解条文与内部培训使用；
涉及合规判断或法律适用时，请咨询专业顾问，并以官方英文文本为准。
翻译您自己的文件，请选择桐鸾译馆 · https://www.ivyivy.com.cn
扫码关注服务号

NIST Special Publication
NIST SP 800-63B-4

Digital Identity Guidelines

Authentication and Authenticator Management

David Temoshok
Naomi Lefkovitz *
Ryan Galluzzo
Applied Cybersecurity Division
Information Technology Laboratory

Yee-Yin Choong
Information Access Division
Information Technology Laboratory

Andrew Regenscheid
Computer Security Division
Information Technology Laboratory

James L. Fenton
Altmode Networks

Justin P. Richer
Bespoke Engineering

* *Former NIST employee; all work for this publication was done while at NIST.*

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63B-4

July 2025

U.S. Department of Commerce
Howard Lutnick, Secretary

National Institute of Standards and Technology
Craig Burkhardt, Acting Under Secretary for Standards and Technology and Acting NIST Director

NIST 特别出版物
NIST SP 800-63B-4

数字身份指南

认证与认证器管理

大卫·特莫肖克
娜奥米·莱夫科维茨 *

瑞安·加卢佐
应用网络安全部
信息技术实验室

容仪
信息访问部
信息技术实验室

安德鲁·雷根沙伊德
计算机安全部
信息技术实验室

James L.Fenton
阿尔特模式网络

Justin P.Richer
定制工程

* 前*NIST*员工；本出版物的所有工作均在*NIST*任职期间完成。

本出版物可从以下网址免费获取：
https://doi.org/10.6028/NIST.SP.800-63B-4

2025年7月

美国商务部
霍华德·卢特尼克，部长

美国国家标准与技术研究院
Craig Burkhardt，标准与技术代理副部长兼*NIST*代理主任

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

NIST Technical Series Policies

Copyright, Fair Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

本文中标识了某些商业或非商业设备、仪器、软件或材料，以便充分说明实验程序。此类标识并不意味着NIST对任何产品或服务的推荐或认可，也不意味着所标识的材料或设备必然是用于该目的的最佳可用选择。

本出版物可能引用NIST根据其法定职责正在制定的其他出版物。本出版物中的信息，包括概念和方法，联邦机构甚至可以在这些配套出版物完成之前使用。因此，在每份出版物完成之前，现有的要求、指南和程序(如存在)仍然有效。出于规划和过渡目的，联邦机构可能希望密切关注NIST这些新出版物的制定进展。

鼓励各组织在公开评论期内审阅所有草案出版物并向NIST提供反馈。除上述出版物外，许多NIST网络安全出版物可在https://csrc.nist.gov/publications.获取

权限

本出版物由NIST根据2014年《联邦信息安全管理现代化法案》(FISMA),44 U.S.C.3551 et seq.，公法(P.L.)113-283赋予的法定职责制定。NIST负责制定信息安全标准和指南，包括联邦信息系统的最低要求，但此类标准和指南不得适用于国家安全系统，除非对此类系统行使政策权力的适当联邦官员明确批准。本指南与管理和预算办公室(OMB)A-130号通告的要求一致。

本出版物中的任何内容均不得被视为与商务部长根据法定权力对联邦机构强制实施并具有约束力的标准和指南相矛盾。这些指南也不应被解释为改变或取代商务部长、OMB主任或任何其他联邦官员的现有权力。本出版物可由非政府组织自愿使用，在美国不受版权限制。但NIST希望在使用时予以注明出处。

NIST 技术系列政策

版权、合理使用和许可声明 NIST技术系列出版物标识符语法

Publication History

Approved by the NIST Editorial Review Board on 2025-05-30.
Supersedes NIST SP 800-63B (June 2017; updated March 2, 2020) https://doi.org/10.6028/NIST.SP.800-63b

How to Cite this NIST Technical Series Publication

Temoshok D, Fenton JL, Choong YY, Lefkovitz N, Regenscheid A, Galluzzo R, Richer JP (2025) Digital Identity Guidelines: Authentication and Authenticator Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-63B-4. https://doi.org/10.6028/NIST.SP.800-63B-4

Author ORCID iDs

David Temoshok: 0000-0001-6195-0331
James L. Fenton: 0000-0002-2344-4291
Yee-Yin Choong: 0000-0002-3889-6047
Naomi Lefkovitz: 0000-0003-3777-3106
Andrew Regenscheid: 0000-0002-3930-527X
Ryan Galluzzo: 0000-0003-0304-4239
Justin P. Richer: 0000-0003-2130-5180

Contact Information

mailto:dig-comments@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

Additional Information

Additional information about this publication is available at https://csrc.nist.gov/pubs/sp/800/63/B/4/final, including related content, potential updates, and document history.

All comments are subject to release under the Freedom of Information Act (FOIA).

出版历史

2025-05-30 经 NIST 编辑审查委员会批准。
取代NIST SP 800-63B(2017年6月；2020年3月2日更新)https://doi.org/10. 6028/NIST.SP.800-63b

如何引用本 NIST 技术系列出版物

Temoshok D, Fenton JL, Choong YY, Lefkovitz N, Regenscheid A, Galluzzo R, Richer JP(2025) 数字身份指南：身份验证与认证器管理。(美国国家标准与技术研究院，马里兰州盖瑟斯堡),NIST特别出版物(SP)NIST SP 800-63B-4。https://doi.org/10.6028/NIST.SP.800-63B-4

作者 ORCID iD

David Temoshok：0000-0001-6195-0331
James L. Fenton：0000-0002-2344-4291
Yee-Yin Choong：0000-0002-3889-6047
Naomi Lefkovitz：0000-0003-3777-3106
安德鲁·雷根沙伊德：0000-0002-3930-527X
Ryan Galluzzo：0000-0003-0304-4239
Justin P. Richer：0000-0003-2130-5180

联系信息

mailto:dig-comments@nist.gov

美国国家标准与技术研究院
收件人：应用网络安全部，信息技术实验室 100 Bureau Drive(Mail Stop 2000)Gaithersburg, MD 20899-2000

附加信息

有关本出版物的更多信息，请访问https://csrc.nist.gov/pubs/ sp/800/63/B/4/final，包括相关内容、可能的更新和文档历史。

所有评论均须根据《信息自由法》(FOIA)予以公开。

Abstract

This guideline focuses on the authentication of subjects who interact with government information systems over networks to establish that a given claimant is a subscriber who has been previously authenticated. The result of the authentication process may be used locally by the system performing the authentication or asserted elsewhere in a federated identity system. This document defines technical requirements for each of the three authentication assurance levels. The guidelines are not intended to constrain the development or use of standards outside of this purpose. This publication supersedes NIST Special Publication (SP) 800-63B.

Keywords

authentication; authentication assurance; credential service provider; digital authentication; passwords.

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

摘要

本指南侧重于对通过网络与政府信息系统交互的主体进行身份验证，以确定某个声称者是此前已经过身份验证的订阅者。身份验证过程的结果可由执行身份验证的系统在本地使用，也可在联合身份系统的其他地方进行断言。本文档定义了三个身份验证保证等级各自的技术要求。本指南无意限制此目的之外标准的制定或使用。本出版物取代NIST特别出版物(SP)800-63B。

关键词

身份验证；身份验证保证；凭证服务提供商；数字身份验证；密码。

计算机系统技术报告

美国国家标准与技术研究院(NIST)的信息技术实验室(ITL)通过为国家测量和标准基础设施提供技术领导，促进美国经济和公共福利。ITL开发测试、测试方法、参考数据、概念验证实现和技术分析，以推进信息技术的发展和高效使用。ITL的职责包括为联邦信息系统中非国家安全相关信息的经济高效安全性和隐私性制定管理、行政、技术和物理标准及指南。特别出版物800系列报告了ITL在信息系统安全方面的研究、指南和外展工作，以及与行业、政府和学术组织的合作活动。

Patent Disclosure Notice

NOTICE: ITL has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

专利披露声明

通知：ITL已要求，其使用可能为遵守本出版物的指南或要求所必需的专利权利要求持有人向ITL披露此类专利权利要求。但是，专利持有人没有义务回应ITL的专利征集，ITL也未进行专利检索以确定是否有任何专利可能适用于本出版物。

截至出版之日，在发出征集以识别其使用可能为遵守本出版物的指南或要求所必需的专利权利要求之后，ITL未收到任何此类专利权利要求的标识。

ITL未作出或暗示任何陈述，表明在使用本出版物时无需许可即可避免专利侵权。

Table of Contents

1. Introduction . . . 1
1.1. Notations . . . 2
1.2. Document Structure . . . 3
2. Authentication Assurance Levels . . . 4
2.1. Authentication Assurance Level 1 . . . 4
2.1.1. Permitted Authenticator Types . . . 5
2.1.2. Authenticator and Verifier Requirements . . . 5
2.1.3. Reauthentication . . . 5
2.2. Authentication Assurance Level 2 . . . 6
2.2.1. Permitted Authenticator Types . . . 6
2.2.2. Authenticator and Verifier Requirements . . . 7
2.2.3. Reauthentication . . . 7
2.3. Authentication Assurance Level 3 . . . 8
2.3.1. Permitted Authenticator Types . . . 8
2.3.2. Authenticator and Verifier Requirements . . . 8
2.3.3. Reauthentication . . . 9
2.4. General Requirements . . . 9
2.4.1. Security Controls . . . 9
2.4.2. Records Retention Policy . . . 9
2.4.3. Privacy Requirements . . . 9
2.4.4. Redress Requirements . . . 10
2.5. Summary of Requirements . . . 11
3. Authenticator and Verifier Requirements . . . 12
3.1. Requirements by Authenticator Type . . . 13
3.1.1. Passwords . . . 13
3.1.2. Look-Up Secrets . . . 17
3.1.3. Out-of-Band Devices . . . 18
3.1.4. Single-Factor OTP . . . 23
3.1.5. Multi-Factor OTPs . . . 25

目录

1. **引言** 1
1.1. 符号说明 2
1.2. 文档结构 3
2. **认证保证等级** 4
2.1. 认证保证等级 1 4
2.1.1. 允许的认证器类型 5
2.1.2. 认证器与验证器要求 5
2.1.3. 重新身份验证 5
2.2. 认证保证等级 2 6
2.2.1. 允许的认证器类型 6
2.2.2. 认证器与验证器要求 7
2.2.3. 重新身份验证 7
2.3. 认证保证等级3 8
2.3.1. 允许的认证器类型 8
2.3.2. 认证器与验证器要求 8
2.3.3. 重新身份验证 9
2.4. 一般要求 9
2.4.1. 安全控制 9
2.4.2. 记录保留政策 9
2.4.3. 隐私要求 9
2.4.4. 补救要求 10
2.5. 要求摘要 11
3. **认证器与验证器要求** 12
3.1. 按认证器类型划分的要求 13
3.1.1. 密码 13
3.1.2. 查找型密钥 17
3.1.3. 带外设备 18
3.1.4. 单因素 OTP 23
3.1.5. 多因素OTP 25

3.1.6. Single-Factor Cryptographic Authentication 26
3.1.7. Multi-Factor Cryptographic Authentication 27
3.2. General Authenticator Requirements 30
3.2.1. Physical Authenticators 30
3.2.2. Rate Limiting (Throttling) 30
3.2.3. Use of Biometrics 31
3.2.4. Attestation 34
3.2.5. Phishing Resistance 35
3.2.6. Verifier-CSP or IdP Communications 36
3.2.7. Replay Resistance 36
3.2.8. Authentication Intent 37
3.2.9. Restricted Authenticators 37
3.2.10. Activation Secrets 38
3.2.11. Connected Authenticators 39
3.2.12. Random Values 41
3.2.13. Exportability 41
4. Authenticator Event Management 43
4.1. Authenticator Binding 43
4.1.1. Binding at Enrollment 44
4.1.2. Post-Enrollment Binding 44
4.1.3. Binding to a Subscriber-Provided Authenticator 46
4.1.4. Renewal 46
4.2. Account Recovery 47
4.2.1. Account Recovery Methods 47
4.2.2. Recovery Requirements by IAL/AAL 49
4.2.3. Account Recovery Notification 50
4.3. Loss, Theft, Damage, and Compromise 50
4.4. Expiration 51
4.5. Invalidation 51
4.6. Account Notifications 51

3.1.6. 单因素加密认证 26
3.1.7. 多因素加密认证 27
3.2. 通用认证器要求 30
3.2.1. 物理认证器 30
3.2.2. 速率限制(节流) 30
3.2.3. 生物特征的使用 31
3.2.4. 证明 34
3.2.5. 抗钓鱼 35
3.2.6. 验证方-CSP 或 IdP 通信 36
3.2.7. 重放抵抗 36
3.2.8. 认证意图 37
3.2.9. 受限认证器 37
3.2.10. 激活密钥 38
3.2.11. 已连接认证器 39
3.2.12. 随机值 41
3.2.13. 可导出性 41
4. 认证器事件管理 43
4.1. 认证器绑定 43
4.1.1. 注册时的绑定 44
4.1.2. 注册后绑定 44
4.1.3. 绑定到用户提供的认证器 46
4.1.4. 续期 46
4.2. 账户恢复 47
4.2.1. 账户恢复方法 47
4.2.2. 按 IAL/AAL 划分的恢复要求 49
4.2.3. 账户恢复通知 50
4.3. 丢失、被盗、损坏和泄露 50
4.4. 到期 51
4.5. 失效 51
4.6. 账户通知 51

5. Session Management . . . 53
5.1. Session Bindings . . . 53
5.1.1. Browser Cookies . . . 55
5.1.2. Access Tokens . . . 55
5.2. Reauthentication . . . 56
5.3. Session Monitoring . . . 57
6. Threats and Security Considerations . . . 58
6.1. Authenticator Threats . . . 58
6.2. Threat Mitigation Strategies . . . 62
6.3. Authenticator Recovery . . . 65
6.4. Session Attacks . . . 65
7. Privacy Considerations . . . 66
7.1. Privacy Risk Assessment . . . 66
7.2. Privacy Controls . . . 66
7.3. Use Limitation . . . 66
7.4. Agency-Specific Privacy Compliance . . . 67
8. Customer Experience Considerations . . . 68
8.1. Usability . . . 68
8.1.1. Common Usability Considerations for Authenticators . . . 69
8.1.2. Usability Considerations by Authenticator Type . . . 71
8.1.3. Summary of Usability Considerations . . . 76
8.1.4. Usability Considerations for Biometrics . . . 76
8.2. Customer Success Considerations . . . 79
References . . . 81
Appendix A. Strength of Passwords . . . 87
A.1. Introduction . . . 87
A.2. Length . . . 87
A.3. Complexity . . . 88
A.4. Central vs. Local Verification . . . 89
A.5. Summary . . . 90

5. **会话管理** 53
5.1. 会话绑定 53
5.1.1. 浏览器 Cookie 55
5.1.2. 访问令牌 55
5.2. 重新身份验证 56
5.3. 会话监控 57
6. **威胁与安全考量** 58
6.1. 认证器威胁 58
6.2. 威胁缓解策略 62
6.3. 认证器恢复 65
6.4. 会话攻击 65
7. **隐私考量** 66
7.1. 隐私风险评估 66
7.2. 隐私控制 66
7.3. 使用限制 66
7.4. 机构特定隐私合规 67
8. **客户体验考量** 68
8.1. 可用性 68
8.1.1. 认证器的常见可用性考虑因素 69
8.1.2. 按认证器类型划分的可用性考量 71
8.1.3. 可用性考量摘要 76
8.1.4. 生物识别的可用性考量 76
8.2. 客户成功考量 79
参考文献 81
附录 A.密码强度 87
A.1. 引言 87
A.2. 长度 87
A.3. 复杂性 88
A.4. 集中式验证与本地验证 89
A.5. 摘要 90

Appendix B. Syncable Authenticators 91
B.1. Introduction 91
B.2. Cloning Authentication Keys 91
B.3. Implementation Requirements 92
B.4. Sharing 94
B.5. Example 95
B.6. Security Considerations 96
Appendix C. List of Symbols, Abbreviations, and Acronyms 99
Appendix D. Glossary 102
Appendix E. Change Log 117

List of Tables

Table 1. Summary of requirements by AAL 11
Table 2. Summary of secrets (non-normative) 12
Table 3. Authenticator threats 58
Table 4. Mitigating authenticator threats 62
Table 5. Syncable authenticator threats, challenges, and mitigations 96

List of Figures

Fig. 1. Transfer of secret to primary device 19
Fig. 2. Transfer of secret to out-of-band device 19
Fig. 3. Usability considerations by authenticator type 77

附录 B.可同步认证器 91
B.1. 引言 91
B.2. 克隆认证密钥 91
B.3. 实施要求 92
B.4. 共享 94
B.5. 示例 95
B.6. 安全考虑 96
附录 C.符号、缩写和首字母缩略语列表 99
附录 D.术语表 102
附录 E.变更日志 117

表目录

表1. 按AAL划分的要求摘要 11
表2. 秘密摘要(非规范性) 12
表3. 认证器威胁 58
表4. 缓解认证器威胁 62
表5. 可同步认证器的威胁、挑战与缓解措施 96

图目录

图 1. 将密钥传输至主设备 19
图 2. 将密钥传输至带外设备 19
图 3. 按认证器类型划分的可用性考量 77

Preface

This publication and its companion volumes — [SP800-63], [SP800-63A], and [SP800-63C] — provide technical guidelines for organizations to implement digital identity services.

This document, SP 800-63B, provides requirements to credential service providers (CSPs) for remote user authentication at each of three authentication assurance levels (AALs).

Acknowledgments

The authors would like to thank their fellow collaborators — Christine Abruzzi, Sarbari Gupta, Connie LaSalle, Diana Proud-Madruga, and Maria Vachino — on the current revision of this special publication, as well as Kerrianne Buchanan, Greg Fiumara, and Evelyn Petrella for their contributions and review. The authors would like to also acknowledge the past contributions of Donna F. Dodson, W. Timothy Polk, Emad A. Nabbus, Paul A. Grassi, Elaine M. Newton, Ray Perlner, William E. Burr, Kristen K. Greene, Mary F. Theofanos, Kaitlin Boeckl, Kat Megas, Ellen Nadeau, Ben Piccarreta, and Danna Gabel O'Rourke.

前言

本出版物及其配套卷--[SP800-63]、[SP800-63A]和[SP800-63C]--为组织实施数字身份服务提供了技术指南。

本文件SP 800-63B规定了凭证服务提供商(CSP)在三个身份验证保证等级(AAL)中任一等级下进行远程用户身份验证的要求。

致谢

作者感谢当前版本特别出版物的合作者--Christine Abruzzi、Sarbari Gupta、Connie LaSalle、Diana Proud-Madruga 和 Maria Vachino，以及 Kerrianne Buchanan、Greg Fiumara 和 Evelyn Petrella 的贡献和审阅。作者还要感谢 Donna F.Dodson、W.Timothy Polk、Emad A.Nabbus、Paul A.Grassi、Elaine M.Newton、Ray Perlner、William E.Burr、Kristen K.Greene、Mary F.Theofanos、Kaitlin Boeckl、Kat Megas、Ellen Nadeau、Ben Piccarreta 和 Danna Gabel O'Rourke 过去的贡献。

1. Introduction

This section is informative.

Authentication is the process of determining the validity of one or more authenticators used to claim a digital identity by establishing that a subject attempting to access a digital service is in control of the secrets used to authenticate. If return visits are applicable to a service, successful authentication provides reasonable risk-based assurance that the subject accessing the service today is the same as the one who previously accessed the service. One-time services (i.e., the *subscriber* will only ever access the service once) do not necessarily require persistent digital authentication nor the issuance of authenticators.

The authentication of *claimants* is central to the process of associating a subscriber with their online activity as recorded in their *subscriber account*, which is maintained by a *credential service provider* (CSP). Authentication is performed by verifying that the claimant controls one or more *authenticators* (called *tokens* in some earlier editions of SP 800-63) associated with a given subscriber account. The authentication process is conducted by a *verifier*, which is a role of the CSP or — in federated authentication — of an *identity provider* (IdP). Upon successful authentication, the verifier asserts the *identifier* for the subscriber to the *relying party* (RP). Optionally, the verifier may assert additional *attributes* to the RP.

This guideline provides recommendations on types of authentication processes, including choices of authenticators, that may be used at various *authentication assurance levels* (AALs). It also provides recommendations on events that may occur during the lifetime of authenticators, including initial issuance, maintenance, and invalidation in the event of loss or theft of the authenticator.

This guideline applies to the digital authentication of subjects to systems over a network. It also requires that verifiers and RPs participating in authentication protocols be authenticated to claimants to assure the identity of the services with which they are authenticating. It does not address the authentication of a person for physical access (e.g., to a building).

This guideline recognizes that subscribers are responsible for protecting their authentication secrets and not disclosing them to others (e.g., credential sharing). The protections at the various AALs are intended to protect against credential theft and are not intended to protect against willful disclosure of credential secrets by a subscriber. In most cases, there are very few technical controls that can detect and prevent such willful collusion and sharing.

AALs categorize the strength of an authentication transaction. Stronger authentication (i.e., a higher AAL) requires malicious actors to have better capabilities and to expend greater resources to successfully subvert the authentication process. Authentication

1. 引言

本节为说明性内容。

身份验证是确定用于声称数字身份的一个或多个认证器有效性的过程，其方式是确立试图访问数字服务的主体控制着用于身份验证的密钥。如果服务适用回访，则成功的身份验证可提供基于风险的合理保证，即今天访问服务的主体与先前访问服务的主体相同。一次性服务(即订阅者仅会访问该服务一次)不一定需要持久性数字身份验证，也不一定需要签发认证器。

对声称者的身份验证是将订阅者与其订阅者账户中记录的在线活动相关联这一过程的核心，该账户由凭证服务提供商(CSP)维护。身份验证通过验证声称者控制与给定订阅者账户关联的一个或多个认证器(在 SP 800-63 的某些早期版本中称为令牌)来执行。身份验证过程由验证器执行，验证器是 CSP 的角色，或者在联邦身份验证中是身份提供方(IdP)的角色。身份验证成功后，验证器向依赖方(RP)断言订阅者的标识符。验证器还可以选择向 RP 断言附加属性。

本指南就身份验证流程的类型(包括认证器的选择)提供建议，这些流程可用于各种身份验证保证等级(AAL)。本指南还就认证器生命周期内可能发生的事件提供建议，包括初始签发、维护以及在认证器丢失或被盗时的失效处理。

本指南适用于主体通过网络对系统进行数字身份验证的情形。它还要求参与身份验证协议的验证器与RP向声称者进行身份验证，以确保其所验证的服务的身份。本指南不涉及人员物理访问(例如进入建筑物)的身份验证。

本指南认识到，订阅者有责任保护其身份验证机密不向他人泄露(例如凭证共享)。各AAL下的保护措施旨在防范凭证被盗，而非防范订阅者故意泄露凭证机密。在大多数情况下，能够检测和防止此类故意串通与共享的技术控制手段非常有限。

AAL对身份验证交易强度进行分类。更强的身份验证(即更高的AAL)要求恶意行为者具备更强的能力并投入更多资源才能成功破坏身份验证流程。身份验证

at higher AALs can effectively reduce the risk of attacks. A high-level summary of the technical requirements for each of the AALs is provided below; see Sec. 2 and Sec. 3 of this document for specific normative requirements.

Authentication Assurance Level 1: AAL1 provides basic confidence that the claimant controls an authenticator bound to the subscriber account being authenticated. AAL1 requires only single-factor authentication using a wide range of available authentication technologies. However, it is recommended that applications assessed at AAL1 offer multi-factor authentication options. Successful authentication requires the claimant to prove *possession and control of the authenticator*.

Authentication Assurance Level 2: AAL2 provides high confidence that the claimant controls one or more authenticators bound to the subscriber account being authenticated. Proof of the possession and control of two distinct *authentication factors* is required. Applications assessed at AAL2 must offer a *phishing-resistant* authentication (see Sec. 3.2.5) option.

Authentication Assurance Level 3: AAL3 provides very high confidence that the claimant controls one or more authenticators bound to the subscriber account being authenticated. Authentication at AAL3 is based on the proof of possession of a key through the use of a public-key cryptographic protocol. AAL3 authentication requires a phishing-resistant authenticator (see Sec. 3.2.5) with a non-exportable authentication key (see Sec. 3.2.13). To authenticate at AAL3, claimants are required to prove possession and control of two distinct authentication factors.

When a *session* has been authenticated at a given AAL and a higher AAL is required, an authentication process may also provide step-up authentication to raise the session's AAL.

1.1. Notations

This guideline uses the following typographical conventions in text:

- Specific terms in `CAPITALS` represent normative requirements. When these same terms are not in `CAPITALS`, the term does not represent a normative requirement.
  - The terms "`SHALL`" and "`SHALL NOT`" indicate requirements to be followed strictly in order to conform to the publication and from which no deviation is permitted.
  - The terms "`SHOULD`" and "`SHOULD NOT`" indicate that among several possibilities, one is recommended as particularly suitable without mentioning or excluding others, that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited.

在更高AAL下可有效降低攻击风险。以下提供各AAL技术要求的概要说明；具体规范性要求见本文件第2节和第3节。

身份验证保证等级1:AAL1提供基本信心，即声称者控制着与正在被验证的订阅者账户绑定的认证器。AAL1仅要求使用广泛的可用身份验证技术进行单因素身份验证。然而，建议在AAL1级别评估的应用程序提供多因素身份验证选项。成功的身份验证要求声称者证明对认证器的拥有和控制。

身份验证保证等级2:AAL2提供高置信度，确保声称者控制绑定到所验证订阅者账户的一个或多个认证器。要求证明拥有并控制两个不同的身份验证因素。按AAL2评估的应用必须提供抗钓鱼的身份验证(见第3.2.5节)选项。

身份验证保证等级3:AAL3 提供非常高的置信度，确保声称者控制一个或多个绑定到正在被验证的订阅者账户的认证器。AAL3 的身份验证基于通过使用公钥密码协议来证明对密钥的持有。AAL3 身份验证要求使用抗钓鱼的认证器(见第 3.2.5 节)，并具有不可导出的身份验证密钥(见第 3.2.13 节)。要在 AAL3 进行身份验证，声称者必须证明持有并控制两个不同的身份验证因素。

当会话已在给定AAL下完成身份验证且需要更高AAL时，身份验证流程还可提供逐步提升身份验证以提高该会话的AAL。

1.1. 符号说明

本指南在文本中使用以下排版约定：

- **大写**的特定术语表示规范性要求。当这些相同术语不以**大写**形式出现时，该术语不表示规范性要求。

  -术语"**SHALL**"和"**SHALL NOT**"表示
  为符合本出版物而必须严格遵循的要求，不允许任何偏离。

  -术语"**SHOULD**"和"**SHOULD NOT**"表示在若干
  可能性中，推荐某一种为特别合适，但不提及或排除其他可能性；表示某种做法是首选但并非必需；或(在否定形式中)表示不鼓励某种可能性或做法但并非禁止。

- The terms “ **MAY** ” and “ **NEED NOT** ” indicate a course of action permissible within the limits of the publication.
- The terms “ **CAN** ” and “ **CANNOT** ” indicate a possibility and capability — whether material, physical, or causal — or, in the negative, the absence of that possibility or capability.

1.2. Document Structure

This document is organized as follows. Each section is labeled as either normative (i.e., mandatory for compliance) or informative (i.e., not mandatory).

- Section 1 introduces the document. This section is *informative*.
- Section 2 describes requirements for AALs. This section is *normative*.
- Section 3 describes authenticator and verifier requirements. This section is *normative*.
- Section 4 describes requirements for authenticator event management. This section is *normative*.
- Section 5 describes requirements for session management. This section is *normative*.
- Section 6 provides security considerations. This section is *informative*.
- Section 7 provides privacy considerations. This section is *informative*.
- Section 8 provides customer experience considerations. This section is *informative*.
- The References section lists publications that are cited in this document. This section is *informative*.
- Appendix A discusses the strength of passwords. This appendix is *informative*.
- Appendix B discusses syncable authenticators. This appendix is *normative*.
- Appendix C contains a selected list of abbreviations used in this document. This appendix is *informative*.
- Appendix D contains a glossary of selected terms used in this document. This appendix is *informative*.
- Appendix E contains a summarized list of changes in this document’s history. This appendix is *informative*.

-术语“**MAY**”和“**NEED NOT**”表示允许的做法
在出版范围内。

-术语“**CAN**”和“**CANNOT**”表示一种可能性与能力--
无论是物质的、物理的还是因果的--或在否定形式中，表示该可能性或能力的缺失。

1.2. 文档结构

本文件组织如下。每一节均标注为规范性(即为合规所必需)或资料性(即非必需)。

- 第1节介绍本文件。本节为资料性内容。
- 第2节描述AAL的要求。本节为规范性。
- 第3节描述认证器与验证器的要求。本节为规范性。
- 第4节描述了认证器事件管理的要求。本节为规范性内容。
- 第5节描述了会话管理的要求。本节为规范性内容。
- 第6节提供了安全考虑。本节为信息性内容。
- 第7节提供了隐私考虑。本节为信息性内容。
- 第8节提供了客户体验考虑。本节为信息性内容。
- 参考文献部分列出了本文档中引用的出版物。本节为信息性内容。
- 附录A讨论了密码强度。本附录为信息性内容。
- 附录B讨论了可同步认证器。本附录为规范性内容。
- 附录C包含本文档中使用的缩写的精选列表。本附录为信息性内容。
- 附录D包含本文档中使用的选定术语的词汇表。本附录为信息性内容。
- 附录E包含本文档历史变更的汇总列表。本附录为信息性内容。

2. Authentication Assurance Levels

This section is normative.

To satisfy the requirements of a given AAL and be recognized as a subscriber, a claimant **SHALL** authenticate to an RP (or IdP, as described in [SP800-63C]) with a process whose strength is equal to or greater than the requirements at that level. The authentication process results in an identifier that uniquely identifies the subscriber each time they authenticate to that RP. The identifier **MAY** be pseudonymous. Other attributes that identify the subscriber as a unique subject **MAY** also be provided. Detailed normative requirements for authenticators and verifiers at each AAL are provided in Sec. 3. See [SP800-63] Sec. 3 for details on how to choose the most appropriate AAL.

Personal information collected during and after identity proofing (see [SP800-63A]) **MAY** be made available to the subscriber by the digital identity service through the subscriber account. The release or online availability of any personal information by federal agencies requires multi-factor authentication in accordance with [EO13681]. Therefore, federal agencies **SHALL** select a minimum of AAL2 when personal information is made available online.

At all AALs, indicators of potential fraud, including applicable indicators described in Sec. 5.3, **MAY** be used to lower the risk of misauthentication. For example, authentication from an unexpected geolocation or IP address block (e.g., a cloud service) might prompt the use of additional risk-based controls. CSPs or verifiers **SHALL** assess their use of indicators of potential fraud for efficacy and to identify and mitigate potential negative impacts on their user populations. CSPs or verifiers **SHALL** include fraud indicators in the authentication privacy risk assessment. The use of potential fraud indicators prior to or during the authentication process does not impact or change the AAL of a transaction or substitute for an authentication factor.

Throughout this document, [FIPS140] requirements are satisfied by security technologies, products, and services that utilize implementations of cryptography validated by the Cryptography Module Validation Program [CMVP]. FIPS 140 requirements at a given AAL are often different for authenticators and verifiers, with more stringent requirements generally applying to verifiers. This is in recognition of the practical limitations on the certification of authenticators as well as the broader scope that is often associated with a security breach at a verifier.

2.1. Authentication Assurance Level 1

AAL1 provides basic confidence that the claimant controls an authenticator that is bound to the subscriber account. AAL1 requires either single-factor or multi-factor authentication using a wide range of available authentication technologies. Verifiers **SHOULD** make multi-factor authentication options available at AAL1 and encourage their use. Successful authentication requires that the claimant prove possession and control of the authenticator through a secure authentication protocol.

2. 认证保证等级

本节为规范性内容。

为满足给定AAL的要求并被识别为订阅者，声称者**SHALL**通过其强度等于或大于该级别要求的过程向RP(或IdP，如[SP800-63C]所述)进行身份验证。身份验证过程产生一个标识符，该标识符在订阅者每次向该RP进行身份验证时唯一标识该订阅者。该标识符**MAY**为假名。其他将订阅者标识为唯一主体的属性**MAY**也被提供。各AAL下认证器和验证器的详细规范性要求见Sec.3。关于如何选择最合适的AAL的详细信息，参见[SP800-63] Sec.

在身份核验期间及之后收集的个人信息(参见[SP800-63A])**可以**由数字身份服务通过订阅者账户提供给订阅者。联邦机构发布或在线提供任何个人信息须按照[EO13681]进行多因素身份验证。因此，当个人信息在线提供时，联邦机构**应**至少选择AAL2。

在所有AAL下，潜在欺诈指标(包括Sec.5.3中所述的可适用指标)**MAY**被用于降低错误身份验证的风险。例如，来自意外地理位置或IP地址块(例如云服务)的身份验证可能会促使采用额外的基于风险的控制措施。CSP或验证器**SHALL**评估其对潜在欺诈指标的使用是否有效，并识别和缓解对其用户群体的潜在负面影响。CSP或验证器**SHALL**将欺诈指标纳入身份验证隐私风险评估。在身份验证过程之前或期间使用潜在欺诈指标不影响或改变交易的AAL，也不替代认证因素。

在本文档全文中，[FIPS140]要求由使用经密码模块验证计划[CMVP]验证的密码学实现的安全技术、产品和服务来满足。给定AAL下的FIPS 140要求对认证器和验证器通常不同，更严格的要求一般适用于验证器。这是考虑到认证器认证的实际限制以及验证器安全泄露通常涉及的更广泛范围。

2.1. 认证保证等级 1

AAL1提供基本信心，即声称者控制着绑定到订阅者账户的认证器。AAL1要求使用广泛的可用身份验证技术进行单因素或多因素身份验证。验证器**宜**在AAL1提供多因素身份验证选项并鼓励使用。成功的身份验证要求声称者通过安全的身份验证协议证明对认证器的拥有和控制。

2.1.1. Permitted Authenticator Types

AAL1 authentication **SHALL** use any of the following authentication types, which are further defined in Sec. 3:

- Password (Sec. 3.1.1): A memorizable secret typically chosen by the subscriber
- Look-up secret (Sec. 3.1.2): A secret determined by the claimant by looking up a prompted value in a list held by the subscriber
- Out-of-band device (Sec. 3.1.3): A secret sent or received through a separate communication channel with the subscriber
- Single-factor one-time password (OTP) (Sec. 3.1.4): A one-time secret obtained from a device or application held by the subscriber
- Multi-factor OTP (Sec. 3.1.5): A one-time secret obtained from a device or application held by the subscriber that requires activation by a second authentication factor
- Single-factor cryptographic authentication (Sec. 3.1.6): Proof of possession and control via an authentication protocol of a cryptographic key held by the subscriber
- Multi-factor cryptographic authentication (Sec. 3.1.7): Proof of possession and control via an authentication protocol of a cryptographic key held by the subscriber that requires activation by a second authentication factor

2.1.2. Authenticator and Verifier Requirements

Authenticators used at AAL1 **SHALL** use *approved cryptography*. In other words, they must use approved algorithms, but the implementation need not be validated under [FIPS140].

Communication between the claimant and verifier **SHALL** occur via one or more *authenticated protected channels*.

Cryptography used by verifiers operated by or on behalf of federal agencies at AAL1 **SHALL** be validated to meet the requirements of [FIPS140] Level 1.

2.1.3. Reauthentication

These guidelines provide for two types of timeouts, which are further described in Sec. 5.2:

1. An overall timeout limits the duration of an authenticated session to a specified period following authentication or a previous reauthentication.
2. An inactivity timeout terminates a session that has not had activity from the subscriber for a specified period.

2.1.1. 允许的认证器类型

AAL1身份验证**应**使用以下任一身份验证类型，这些类型在第3节中进一步定义：

- 密码(第3.1.1节)：通常由订阅者选择的记忆型密钥
- 查询性秘密(第3.1.2节)：声称者通过在订阅者持有的列表中查找提示值而确定的秘密
- 带外设备(第3.1.3节)：通过与订阅者的独立信道发送或接收的秘密
- 单因素一次性密码(OTP)(第3.1.4节)：从订阅者持有的设备或应用程序获得的一次性秘密
- 多因素OTP(第3.1.5节)：从订阅者持有的设备或应用程序获得的一次性秘密，需要第二身份验证因素激活
- 单因素加密身份验证(第3.1.6节)：通过身份验证协议证明对订阅者持有的加密密钥的拥有和控制
- 多因素加密身份验证(第3.1.7节)：通过身份验证协议证明对订阅者持有的加密密钥的拥有和控制，需要第二身份验证因素激活

2.1.2. 认证器与验证器要求

在AAL1使用的认证器**应**使用经批准的加密技术。换言之，它们必须使用经批准的算法，但实现无需在[FIPS140]下验证。

声称者与验证器之间的通信**应**通过一个或多个经身份验证的受保护信道进行。

由联邦机构或代表联邦机构运营的验证器在AAL1使用的加密技术**应**经验证符合[FIPS140]第1级的要求。

2.1.3. 重新身份验证

本指南规定了两种类型的超时，在第5.2节中进一步描述：

1. 总体超时将会话的身份验证持续时间限制为身份验证或先前重新身份验证后的指定时间段。
2. 不活动超时终止订阅者在指定时间段内没有活动的会话。

Periodic reauthentication of subscriber sessions **SHALL** be performed, as described in Sec. 5.2. A definite reauthentication overall timeout **SHALL** be established, which **SHOULD** be no more than 30 days at AAL1. An inactivity timeout **MAY** be applied but is not required at AAL1.

2.2. Authentication Assurance Level 2

AAL2 provides high confidence that the claimant controls one or more authenticators that are bound to the subscriber account. Proof of possession and control of two distinct authentication factors through the use of secure authentication protocols is required. Approved cryptographic techniques are required.

2.2.1. Permitted Authenticator Types

At AAL2, authentication **SHALL** use either a multi-factor authenticator or a combination of two separate authentication factors. A multi-factor authenticator requires two factors to execute a single authentication event, such as a cryptographically secure device with an integrated biometric sensor that is required to activate the device. Authenticator requirements are specified in Sec. 3.

When a multi-factor authenticator is used, any of the following **MAY** be used:

- Multi-factor out-of-band authenticator (Sec. 3.1.3.4)
- Multi-factor OTP (Sec. 3.1.5)
- Multi-factor cryptographic authentication (Sec. 3.1.7)

When a combination of two single-factor authenticators is used, the combination **SHALL** include one *physical authenticator* (i.e., “something you have”) from the following list in conjunction with either a password (Sec. 3.1.1) or a biometric comparison:

- Look-up secret (Sec. 3.1.2)
- Out-of-band device (Sec. 3.1.3)
- Single-factor OTP (Sec. 3.1.4)
- Single-factor cryptographic authentication (Sec. 3.1.6)

订阅者会话的定期重新身份验证**SHALL**按照Sec.5.2所述执行。必须建立明确的重新身份验证总体超时**SHALL**，在AAL1下**SHOULD**不超过30 days。不活动超时**MAY**可以应用，但在AAL1下不是必需的。

2.2. 认证保证等级 2

AAL2提供高置信度，确保声称者控制一个或多个绑定到订阅者账户的认证器。需要通过使用安全身份验证协议来证明对两个不同身份验证因素的拥有和控制。需要使用经批准的密码技术。

2.2.1. 允许的认证器类型

在AAL2下，身份验证**SHALL**使用多因素认证器或两个单独身份验证因素的组合。多因素认证器需要两个因素来执行单个身份验证事件，例如带有集成生物特征传感器的加密安全设备，该传感器是激活设备所必需的。认证器要求在Sec.3中规定。

当使用多因素认证器时，可以使用以下任一**MAY**:

- 多因素带外认证器(Sec.3.1.3.4)
- 多因素 OTP(第 3.1.5 节)
- 多因素加密认证(第 3.1.7 节)

当使用两个单因素认证器的组合时，该组合**SHALL**必须包括以下列表中的一个物理认证器(即“你拥有的东西”)与密码(Sec.3.1.1)或生物特征比对结合使用：

- 查找型密钥(Sec.3.1.2)
- 带外设备(第 3.1.3 节)
- 单因素 OTP(Sec.3.1.4)
- 单因素加密认证(第 3.1.6 节)

> A biometric characteristic is not recognized as an authenticator by itself. Section 3.2.3 requires a physical authenticator to be authenticated along with a biometric comparison. The physical authenticator then serves as "something you have," while the biometric match serves as "something you are." When a biometric comparison is used as an activation factor for a multi-factor authenticator, the authenticator itself serves as the physical authenticator. As noted in that section, local verification of biometric factors (i.e., the use of a multi-factor authenticator with a biometric comparison as an activation factor) is preferred over central biometric factor comparison.

2.2.2. Authenticator and Verifier Requirements

Authenticators used at AAL2 **SHALL** use approved cryptography. Cryptographic authenticators procured by federal agencies **SHALL** be validated to meet the requirements of [FIPS140] Level 1. At least one authenticator used at AAL2 **SHALL** be replay-resistant, as described in Sec. 3.2.7. Authentication at AAL2 **SHOULD** demonstrate authentication intent from at least one authenticator, as discussed in Sec. 3.2.8.

Communication between the claimant and verifier **SHALL** occur via one or more authenticated protected channels.

Cryptography used by verifiers operated by or on behalf of federal agencies at AAL2 **SHALL** be validated to meet the requirements of [FIPS140] Level 1 unless otherwise specified.

Verifiers **SHALL** offer at least one phishing-resistant authentication option at AAL2, as described in Sec. 3.2.5. Federal agencies **SHALL** require their staff, contractors, and partners to use phishing-resistant authentication to access federal information systems. In all cases, verifiers **SHOULD** encourage the use of phishing-resistant authentication at AAL2 whenever practical since phishing is a significant threat vector [IC3].

2.2.3. Reauthentication

Periodic reauthentication of subscriber sessions **SHALL** be performed, as described in Sec. 5.2. A definite reauthentication overall timeout **SHALL** be established, which **SHOULD** be no more than 24 hours at AAL2. The inactivity timeout **SHOULD** be no more than 1 hour. When the inactivity timeout has occurred but the overall timeout has not yet occurred, the verifier **MAY** allow the subscriber to reauthenticate using only a successful password or biometric comparison in conjunction with the *session secret*, as described in Sec. 5.1.

> 生物特征本身不被视为认证器。第3.2.3节要求物理认证器与生物特征比对一同进行身份验证。此时物理认证器充当"你拥有的东西"，而生物特征匹配充当"你是什么"。当生物特征比对用作多因素认证器的激活因素时，认证器本身即充当物理认证器。如该节所述，生物特征因素的本地验证(即使用以生物特征比对作为激活因素的多因素认证器)优于集中式生物特征因素比对。

2.2.2. 认证器与验证器要求

在AAL2下使用的认证器**SHALL**使用经批准的密码技术。联邦机构采购的密码认证器**SHALL**经过验证以满足[FIPS140] Level 1的要求。在AAL2下使用的至少一个认证器**SHALL**具有抗重放能力，如Sec.3.2.7所述。AAL2下的身份验证**SHOULD**展示至少一个认证器的身份验证意图，如Sec.3.2.8所讨论。

声称者与验证器之间的通信**SHALL**通过一个或多个经过身份验证的受保护信道进行。

由联邦机构运营或代表联邦机构运营的验证器在AAL2下使用的密码技术**SHALL**经过验证以满足[FIPS140] Level 1的要求，除非另有规定。

验证器**SHALL**在AAL2下提供至少一种抗钓鱼的身份验证选项，如Sec.3.2.5所述。联邦机构**SHALL**要求其员工、承包商和合作伙伴使用抗钓鱼的身份验证来访问联邦信息系统。在所有情况下，验证器**SHOULD**在可行时鼓励在AAL2下使用抗钓鱼的身份验证，因为钓鱼是一个重要的威胁向量[IC3]。

2.2.3. 重新认证

订阅者会话的定期重新身份验证**SHALL**按照第5.2节所述执行。应建立明确的重新身份验证总超时**SHALL**，在AAL2下**SHOULD**不超过24小时。非活动超时**SHOULD**不超过1小时。当非活动超时已发生但总超时尚未发生时，验证器**MAY**允许订阅者仅使用成功的密码或生物特征比对结合会话密钥进行重新身份验证，如第5.1节所述。

2.3. Authentication Assurance Level 3

AAL3 provides very high confidence that the claimant controls authenticators that are bound to the subscriber account. Authentication at AAL3 is based on the proof of possession of a key through the use of a cryptographic protocol along with either an activation factor or a password. AAL3 authentication requires the use of a cryptographic authenticator with a non-exportable *private key* that provides phishing resistance. Approved cryptographic techniques are required.

2.3.1. Permitted Authenticator Types

AAL3 authentication **SHALL** require one of the following authenticator combinations:

- Multi-factor cryptographic authentication (Sec. 3.1.7)
- Single-factor cryptographic authentication (Sec. 3.1.6) used in conjunction with either a password (Sec. 3.1.1) or a biometric comparison

> A biometric characteristic is not recognized as an authenticator by itself. Section 3.2.3 requires a physical authenticator to be authenticated along with the biometric comparison. The physical authenticator then serves as "something you have," while the biometric match serves as "something you are." When a biometric comparison is used as an activation factor for a multi-factor authenticator, the authenticator itself serves as the physical authenticator. As noted in that section, local verification of biometric factors (i.e., the use of a multi-factor authenticator with a biometric comparison as an activation factor) is preferred over central biometric factor comparison.

2.3.2. Authenticator and Verifier Requirements

Authenticators used at AAL3 **SHALL** use approved cryptography. Communication between the claimant and verifier **SHALL** occur via one or more authenticated protected channels. The cryptographic authenticator used at AAL3 **SHALL** have a non-exportable private key and **SHALL** provide phishing resistance, as described in Sec. 3.2.5. The cryptographic authentication protocol **SHALL** be replay-resistant, as described in Sec. 3.2.7. All authentication and reauthentication processes at AAL3 **SHALL** demonstrate authentication intent from at least one authenticator, as described in Sec. 3.2.8. Cryptographic authenticators used at AAL3 **SHALL** use public-key cryptography to protect the authentication secrets from compromise of the verifier.

Single-factor and multi-factor authenticators used at AAL3 **SHALL** be validated to meet the requirements of [FIPS140] Level 1 or higher overall. As described in Sec. 3.2.12, cryptographic authenticators used at AAL3 are required to provide a hardware-protected, isolated environment to prevent authentication keys from being leaked or

2.3. 认证保证等级 3

AAL3提供非常高的置信度，确保声称者控制绑定到订阅者账户的认证器。AAL3下的身份验证基于通过使用密码协议证明对密钥的拥有，并结合激活因素或密码。AAL3身份验证需要使用具有不可导出私钥并提供抗钓鱼能力的密码认证器。需要使用经批准的密码技术。

2.3.1. 允许的认证器类型

AAL3身份验证**SHALL**需要以下认证器组合之一：

- 多因素加密认证(第 3.1.7 节)
- 单因素密码认证(Sec.3.1.6)与密码(Sec.3.1.1)或生物特征比对结合使用

> 生物特征本身不被视为认证器。第3.2.3节要求物理认证器与生物特征比对一同进行身份验证。此时物理认证器充当"你拥有的东西"，而生物特征匹配充当"你是什么"。当生物特征比对用作多因素认证器的激活因素时，认证器本身即充当物理认证器。如该节所述，生物特征因素的本地验证(即使用以生物特征比对作为激活因素的多因素认证器)优于集中式生物特征因素比对。

2.3.2. 认证器与验证器要求

在AAL3使用的认证器**SHALL**使用经批准的密码学。声称者与验证器之间的通信**SHALL**通过一个或多个经身份验证的受保护信道进行。在AAL3使用的密码学认证器**SHALL**具有不可导出的私钥，并**SHALL**提供抗钓鱼能力，如第3.2.5节所述。密码学身份验证协议**SHALL**具有抗重放能力，如第3.2.7节所述。AAL3的所有身份验证和重新身份验证过程**SHALL**展示来自至少一个认证器的身份验证意图，如第3.2.8节所述。在AAL3使用的密码学认证器**SHALL**使用公钥密码学以保护身份验证密钥免受验证器被攻破的影响。在AAL3使用的单因素和多因素认证器**SHALL**经验证满足[FIPS140]总体1级或更高要求。如第3.2.12节所述，在AAL3使用的密码学认证器须提供硬件保护的隔离环境，以防止身份验证密钥被泄露或

extracted. Since *syncable authenticators* (described in Appendix B) require the private key to be exportable, syncable authenticators **SHALL NOT** be used at AAL3.

Cryptography used by verifiers at AAL3 **SHALL** be validated at [FIPS140] Level 1 or higher.

Hardware-based authenticators and verifiers at AAL3 **SHOULD** resist relevant side-channel (e.g., timing and power-consumption analysis) attacks.

2.3.3. Reauthentication

Periodic reauthentication of subscriber sessions **SHALL** be performed, as described in Sec. 5.2. At AAL3, the overall timeout for reauthentication **SHALL** be no more than 12 hours. The inactivity timeout **SHOULD** be no more than 15 minutes. Unlike AAL2, AAL3 reauthentication requirements are the same as for initial authentication at AAL3.

2.4. General Requirements

The following requirements apply to authentication at all AALs.

2.4.1. Security Controls

The verifier **SHALL** employ appropriately tailored security controls from the moderate baseline security controls defined in [SP800-53] or an equivalent federal (e.g., [FEDRAMP]) or industry standard that the organization has chosen for the information systems, applications, and online services that these guidelines are used to protect.

2.4.2. Records Retention Policy

The verifier **SHALL** comply with its respective records retention policies in accordance with applicable laws, regulations, and policies, including any National Archives and Records Administration (NARA) records retention schedules that may apply. If the verifier opts to retain records in the absence of mandatory requirements, the verifier or the CSP or IdP of which it is a part **SHALL** conduct a *risk management* process [NISTRMF], including assessments of privacy and security risks, to determine how long records should be retained and **SHALL** inform the subscriber of that retention policy.

2.4.3. Privacy Requirements

The verifier **SHALL** employ appropriately tailored privacy controls defined in [SP800-53] or an equivalent industry standard.

If CSPs or IdPs process attributes for purposes other than identity services (i.e., identity proofing, authentication, or attribute *assertions*), related fraud mitigation, or compliance with laws or legal processes, they **SHALL** implement measures to maintain predictability and manageability commensurate with the privacy risks that arise from the additional processing. Examples of such measures include providing clear notice, obtaining

提取。由于可同步认证器(在Appendix B中描述)要求私钥可导出，可同步认证器**SHALL NOT**在AAL3下使用。

验证器在AAL3下使用的密码技术**SHALL**在[FIPS140] Level 1或更高级别经过验证。AAL3下的基于硬件的认证器和验证器**SHOULD**抵抗相关的侧信道(例如，时序和功耗分析)攻击。

2.3.3. 重新认证

订阅者会话的定期重新身份验证**SHALL**按照Sec.5.2所述执行。在AAL3下，重新身份验证的总体超时**SHALL**不超过12 hours。不活动超时**SHOULD**不超过15 minutes。与AAL2不同，AAL3重新身份验证要求与AAL3初始身份验证相同。

2.4. 通用要求

以下要求适用于所有 AAL 的认证。

2.4.1. 安全控制

验证器**SHALL**采用[SP800-53]中定义的适度基线安全控制或等效的联邦(例如，[FEDRAMP]) 或组织为这些指南所保护的信息系统、应用程序和在线服务选择的行业标准。

2.4.2 记录保留政策

验证器**SHALL**依照适用法律、法规和政策遵守其各自的记录保留政策，包括可能适用的任何国家档案与记录管理局(NARA)记录保留计划。如果验证器选择在没有强制性要求的情况下保留记录，验证器或其所属的CSP或IdP**SHALL**执行风险管理流程[NISTRMF]，包括对隐私和安全风险的评估，以确定记录应保留多长时间，并**SHALL**将该保留政策告知订阅者。

2.4.3. 隐私要求

验证器**SHALL**采用[SP800-53]或等效行业标准中定义的适当定制的隐私控制。

如果CSP或IdP处理属性的目的不是身份服务(即身份核验、身份验证或属性断言)、相关欺诈缓解或遵守法律或法律程序，则它们**SHALL**实施措施，以保持与额外处理产生的隐私风险相称的可预测性和可管理性。此类措施的示例包括提供明确通知、获取

subscriber consent, and enabling the selective use or disclosure of attributes. When CSPs or IdPs use consent measures, they **SHALL NOT** make consent for the additional processing a condition of the identity service.

Regardless of whether the CSP or IdP is an agency or private-sector provider, the following requirements apply to federal agencies that offer or use the authentication service:

1. The agency **SHALL** consult with their *Senior Agency Official for Privacy* (SAOP) and conduct an analysis to determine whether the collection of personal information to issue or maintain authenticators triggers the requirements of the *Privacy Act of 1974* [PrivacyAct] (see Sec. 7.4).
2. The agency **SHALL** publish a *System of Records Notice* (SORN) to cover such collections, as applicable.
3. The agency **SHALL** consult with its SAOP and conduct an analysis to determine whether the collection of personal information to issue or maintain authenticators triggers the requirements of the *E-Government Act of 2002* [E-Gov].
4. The agency **SHALL** publish a *Privacy Impact Assessment* (PIA) to cover such collection, as applicable.

2.4.4. Redress Requirements

The verifier and associated CSP or IdP **SHALL** provide mechanisms for the redress of subscriber complaints and problems that arise from subscriber authentication processes, as described in Sec. 5.6 of [SP800-63]. These mechanisms **SHALL** be easy for subscribers to find and use. The CSP or IdP **SHALL** assess the mechanisms for efficacy in resolving complaints or problems.

订阅者同意，以及启用属性的选择性使用或披露。当CSP或IdP使用同意措施时，它们**SHALL NOT**将额外处理的同意作为身份服务的条件。

无论CSP或IdP是机构还是私营部门提供商，以下要求适用于提供或使用身份验证服务的联邦机构：

1. 机构**SHALL**咨询其*Senior Agency Official for Privacy*(SAOP)并进行分析，以确定为签发或维护认证器而收集个人信息是否触发*Privacy Act of 1974*[Privacy Act]的要求(见Sec.7.4)。
2. 机构**SHALL**发布*System of Records Notice*(SORN)以涵盖此类收集(如适用)。
3. 机构**SHALL**咨询其SAOP并进行分析，以确定为签发或维护认证器而收集个人信息是否触发*E-Government Act of 2002*[E-Gov]的要求。
4. 机构**SHALL**发布*Privacy Impact Assessment*(PIA)以涵盖此类收集(如适用)。

2.4.4. 补救要求

验证器和相关CSP或IdP**SHALL**提供机制，用于纠正订阅者投诉和因订阅者身份验证过程产生的问题，如[SP800-63]的Sec.5.6所述。这些机制**SHALL**便于订阅者找到和使用。CSP或IdP**SHALL**评估这些机制在解决投诉或问题方面的有效性。

2.5. Summary of Requirements

Table 1 provides a non-normative summary of the requirements for each of the AALs.

Table 1. Summary of requirements by AAL

Requirement	AAL1	AAL2	AAL3
Permitted Authenticator Types	* *Any AAL2 or AAL3 authenticator type* * Password * Look-up secret * Out-of-band * SF OTP * SF cryptographic	* MF cryptographic * MF out-of-band * MF OTP * Password or biometric comparison plus: –SF cryptographic –Look-up secret –Out-of-band –SF OTP	* MF cryptographic * SF cryptographic plus: –Password –Biometric comparison
FIPS 140 Validation (Government Verifiers and Authenticators)	**Verifiers** –Level 1	**Verifiers** –Level 1 **Authenticators** –Level 1 overall	**Verifiers** –Level 1 **Authenticators** –Level 1 overall
Reauthentication (recommended)	30 days overall	24 hours overall 1 hour inactivity Single factor required	12 hours overall 15 minutes inactivity
Phishing Resistance	Not required	Recommended; Must be available	Required
Replay Resistance	Not required	Required	Required
Authentication Intent	Not required	Recommended	Required
Key Exportability	Permitted	Permitted	Prohibited

2.5. 要求摘要

Table 1提供了每个AAL要求的非规范性摘要。

表 1.按 AAL 划分的要求摘要

要求	AAL1	AAL2	AAL3
允许认证器类型	任何 AAL2 或 AAL3 认证器类型 * 密码 * 查询性秘密 * 带外 * 旧金山一次性密码 * SF 密码学	* MF 加密 * MF 带外 * MF 一次性密码 * 密码或生物特征比对 加上： - SF 加密 - 查找型密钥 - 带外 - SF OTP	* MF 加密 * SF密码学 加上： –密码 –生物特征比对
FIPS 140 验证（政府验证器和认证器）	**验证器** –级别 1	**验证器** –级别 1 **认证器** –级别 1 总体	**验证器** –级别 1 **认证器** –级别 1 总体
重新身份验证（推荐）	共30天	总共24小时 1 小时不活动 需要单一因素	共12小时 15分钟不活跃
抗钓鱼	不需要	推荐； 必须可用	必需
重放抵抗	不需要	必需	必需
身份验证意图	不需要	推荐	必需
密钥可导出性	允许	允许	禁止

3. Authenticator and Verifier Requirements

This section is normative.

This section provides detailed requirements that are specific to each type of authenticator. With the exception of the reauthentication requirements specified in Sec. 2 and the requirement for phishing resistance at AAL3 described in Sec. 3.2.5, the technical requirements for each authenticator type are the same, regardless of the AAL at which the authenticator is used.

In federated applications described in [SP800-63C], the authentication functions of an IdP correspond closely with that of a CSP or verifier. In the discussion below, the requirements associated with a CSP also apply to an IdP.

In many circumstances, subscribers need to share devices that are used in authentication processes, such as a family phone that receives OTPs. In public-facing applications, CSPs **SHOULD NOT** prevent a device from being registered as an authenticator by multiple subscribers. However, they **MAY** establish restrictions to prevent large-scale fraud or misuse (e.g., limiting the total number of subscriber accounts a single device can be registered with).

Authentication, *authenticator binding* (discussed in Sec. 4.1), and session management (discussed in Sec. 5) are based on proof of possession of one or more types of secrets, as shown in Table 2.

Table 2. Summary of secrets (non-normative)

Type of Secret	Purpose	Reference Section
Password	A subscriber-chosen secret used as an authentication factor	3.1.1
Look-up secret	A secret issued by a verifier and used only once to prove possession of the secret	3.1.2
Out-of-band secret	A short-lived secret generated by a verifier and independently sent to a subscriber's device to verify its possession	3.1.3

Continued on next page

3. 认证器与验证器要求

本节为规范性内容。

本节提供了针对每种认证器类型的详细要求。除第2节中规定的重新身份验证要求以及第3.2.5节中描述的AAL3抗钓鱼要求外，每种认证器类型的技术要求相同，无论认证器用于何种AAL。

在[SP800-63C]描述的联邦应用中，IdP的身份验证功能与CSP或验证器的功能密切相关。在下文的讨论中，与CSP相关的要求同样适用于IdP。

在许多情况下，订阅者需要共享用于身份验证过程的设备，例如接收OTP的家庭电话。在面向公众的应用中，CSP**不应**阻止设备被多个订阅者注册为认证器。但是，它们**可以**建立限制以防止大规模欺诈或滥用(例如，限制单个设备可注册的订阅者账户总数)。

身份验证、认证器绑定(在第4.1节中讨论)以及会话管理(在第5节中讨论)基于对一种或多种类型秘密的持有证明，如表2所示。

表 2.密钥摘要(非规范性)

密钥类型用途		参考章节
密码	用户选择的记忆型密钥 用作认证 因素	3.1.1
查询性秘密	由验证者签发的密钥 并且仅使用一次以证明拥有该密钥	3.1.2
带外 秘密	一个短时效秘密 由验证器生成并独立发送至订阅者设备以验证其持有	3.1.3

下页续

Continued from previous page

Type of Secret	Purpose	Reference Section
One-time passcodes (OTP)	A secret generated by an authenticator and used only once to prove possession of the authenticator	3.1.4, 3.1.5
Activation secret	A password that is used locally as an activation factor for a multi-factor authenticator	3.2.10
Long-term authenticator secret	A secret embedded in a physical authenticator to allow it to function for authentication	4.1
Recovery code	A secret issued to the subscriber to allow them to recover an account at which they are no longer able to authenticate	4.2
Session secret	A secret issued by the verifier at authentication and used to establish the continuity of authenticated sessions	5.1

3.1. Requirements by Authenticator Type

The following requirements apply to specific authenticator types.

3.1.1. Passwords

A password (sometimes referred to as a *passphrase* or, if numeric, a *personal identification number [PIN]*) is a secret value intended to be chosen and either memorized or recorded by the subscriber. Passwords must be of sufficient effective strength and secrecy that it would be impractical for an attacker to guess or otherwise discover the correct secret value. A password is “something you know.”

The requirements in this section apply to centrally verified passwords that are used as independent authentication factors and sent over an authenticated protected channel to the verifier. Passwords used locally as an activation factor for a multi-factor authenticator (e.g., an unlock PIN) are referred to as *activation secrets* and discussed in Sec. 3.2.10. In contrast to centrally verified passwords, activation secrets (similar to the

续上页

密钥类型	用途	参考章节
一次性密码（OTP）	由以下生成的秘密认证器，且仅使用一次以证明对该认证器的持有	3.1.4 , 3.1.5
激活秘密	在本地用作多因素认证器激活因素的密码	3.2.10
长期认证器秘密	嵌入物理认证器中的秘密，使其能够用于身份验证	4.1
恢复代码	签发给以下对象的秘密订阅者以使其能够恢复其已无法访问的账户进行身份验证	4.2
会话秘密	由验证器在身份验证时签发并用于建立已认证会话连续性的秘密	5.1

3.1. 按认证器类型划分的要求

以下要求适用于特定的认证器类型。

3.1.1. 密码

密码(有时称为口令短语，若为数字则称为个人识别码 *[PIN]*)是供订阅者选择并记忆或记录的秘密值。密码必须具有足够的有效强度和保密性，使攻击者猜测或以其他方式发现正确秘密值不可行。密码是“你知道的东西”。

本节的要求适用于作为独立身份验证因素使用并通过经过身份验证的保护信道发送至验证器的集中验证密码。在本地用作多因素认证器激活因素的密码(例如解锁PIN)称为激活秘密，在第3.2.10节中讨论。与集中验证密码不同，激活秘密(类似于许多设备上的

unlock passwords or PINs on many devices) are not sent to the verifier and instead used locally to gain access to the authentication secret.

Passwords are not phishing-resistant.

3.1.1.1. Password Authenticators

Passwords **SHALL** either be chosen by the subscriber or assigned randomly by the CSP.

If the CSP disallows a chosen password because it is on a blocklist of commonly used, expected, or compromised values (see Sec. 3.1.1.2), the subscriber **SHALL** be required to choose a different password. Other composition requirements for passwords **SHALL NOT** be imposed. A rationale for this is presented in Appendix A, *Strength of Passwords*.

3.1.1.2. Password Verifiers

The following requirements apply to passwords.

1. Verifiers and CSPs **SHALL** require passwords that are used as a single-factor authentication mechanism to be a minimum of 15 characters in length. Verifiers and CSPs **MAY** allow passwords that are only used as part of multi-factor authentication processes to be shorter but **SHALL** require them to be a minimum of eight characters in length.
2. Verifiers and CSPs **SHOULD** permit a maximum password length of at least 64 characters.
3. Verifiers and CSPs **SHOULD** accept all printing ASCII [RFC20] characters and the space character in passwords.
4. Verifiers and CSPs **SHOULD** accept Unicode [ISO/ISC 10646] characters in passwords. Each Unicode code point **SHALL** be counted as a single character when evaluating password length.
5. Verifiers and CSPs **SHALL NOT** impose other composition rules (e.g., requiring mixtures of different character types) for passwords.
6. Verifiers and CSPs **SHALL NOT** require subscribers to change passwords periodically. However, verifiers **SHALL** force a change if there is evidence that the authenticator has been compromised.
7. Verifiers and CSPs **SHALL NOT** permit the subscriber to store a hint (e.g., a reminder of how the password was created) that is accessible to an unauthenticated claimant.
8. Verifiers and CSPs **SHALL NOT** prompt subscribers to use knowledge-based authentication (KBA) (e.g., “What was the name of your first pet?”) or security questions when choosing passwords.

解锁密码或PIN)不发送至验证器，而是在本地用于获取身份验证秘密。

密码不能抵御网络钓鱼。

3.1.1.1. 密码认证器

密码**应**由订阅者选择或由CSP随机分配。

如果CSP因所选密码在常用、预期或已泄露值的阻止列表中(见第3.1.1.2节)而拒绝该密码，则**应**要求订阅者选择不同的密码。**不应**施加其他密码组成要求。其理由见附录A,密码强度。

3.1.1.2. 密码验证器

以下要求适用于密码。

1. 验证器和CSP**应**要求用作单因素身份验证机制的密码长度至少为15个字符。验证器和CSP**可以**允许仅用作多因素身份验证过程一部分的密码更短，但**应**要求其长度至少为八个字符。
2. 验证器和CSP**宜**允许密码最大长度至少为64个字符。
3. 验证器和CSP**宜**接受所有可打印ASCII[RFC20]字符以及密码中的空格字符。
4. 验证器和CSP**宜**接受密码中的Unicode[ISO/ISC 10646]字符。在评估密码长度时，每个Unicode码点**应**计为单个字符。
5. 验证器和CSP**不应**对密码施加其他组成规则(例如，要求混合不同字符类型)。
6. 验证器和CSP**不应**要求订阅者定期更改密码。但是，如果有证据表明认证器已被泄露，验证器应强制更改。
7. 验证器和CSP**不应**允许订阅者存储未经身份验证的声称者可访问的提示(例如，关于密码如何创建的提醒)。
8. 验证器和CSP**不应**在订阅者选择密码时提示其使用基于知识的身份验证(KBA)(例如，“你第一只宠物的名字是什么?”)或安全问题。

9. Verifiers **SHALL** request the password to be provided in full (not a subset of it) and **SHALL** verify the entire submitted password (e.g., not truncate it).

If Unicode characters are accepted in passwords, the verifier **SHOULD** apply the normalization process for stabilized strings using the Normalization Form Canonical Composition (NFC) normalization defined in Sec. 12.1 of *Unicode Normalization Forms* [UAX15]. This process is applied before hashing the byte string that represents the password. Subscribers choosing passwords that contain Unicode characters **SHOULD** be advised that some endpoints may represent some characters differently, which would affect their ability to authenticate successfully.

When processing a request to establish or change a password, verifiers **SHALL** compare the prospective secret against a blocklist that contains known commonly used, expected, or compromised passwords. The entire password **SHALL** be subject to comparison, not substrings or words that might be contained therein. For example, the list may include:

- Passwords obtained from previous breach corpuses
- Dictionary words
- Context-specific words, such as the name of the service, the username, and derivatives thereof

If the chosen password is found on the blocklist, the CSP **SHALL** require the subscriber to select a different secret and **SHALL** provide the reason for rejection. Since the blocklist is used to defend against brute-force attacks and unsuccessful attempts are rate-limited, the blocklist **SHOULD** be of sufficient size to prevent subscribers from choosing passwords that attackers are likely to guess before reaching the attempt limit.

> Excessively large blocklists are of little incremental security benefit because the blocklist is used to defend against online attacks, which are already limited by the throttling requirements described in Sec. 3.2.2.

Verifiers **SHALL** offer guidance to the subscriber to help the subscriber choose a strong password. This is particularly important following the rejection of a password on the blocklist as it discourages trivial modifications of listed weak passwords [Blocklists].

Verifiers **SHALL** implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber account, as described in Sec. 3.2.2.

Verifiers **SHALL** allow the use of password managers and autofill functionality. Verifiers **SHOULD** permit claimants to use the “paste” function when entering a password to facilitate password manager use when password autofill APIs are unavailable. Password managers have been shown to increase the likelihood that subscribers will choose

9. 验证器**SHALL**要求用户完整提供密码(而非其子集)，并且**SHALL**验证所提交的完整密码(例如，不得截断)。

如果密码中接受 Unicode 字符，验证器**应**对稳定化字符串应用规范化处理，使用*Unicode* 规范化形式[UAX15]第 12.1 节中定义的规范化形式规范组合(NFC)规范化。此处理在对表示密码的字节串进行哈希之前应用。选择包含 Unicode 字符的密码的订阅者**应**被告知，某些端点可能以不同方式表示某些字符，这将影响其成功认证的能力。

在处理建立或更改密码的请求时，验证器**应**将预期秘密与包含已知常用、预期或已泄露密码的阻止列表进行比较。**应**对整个密码进行比较，而非其中可能包含的子串或单词。例如，该列表可包括：

- 从以往泄露数据集中获取的密码
- 字典词汇
- 上下文相关的词语，例如服务名称、用户名及其派生词

如果所选密码出现在阻止列表中，CSP **SHALL**要求订阅者选择不同的秘密，并**SHALL**提供拒绝原因。由于阻止列表用于防御暴力攻击且不成功尝试受到速率限制，阻止列表**SHOULD**具有足够的大小，以防止订阅者选择攻击者在达到尝试限制之前可能猜到的密码。

> 过大的阻止列表带来的增量安全收益很小，因为阻止列表用于防御在线攻击，而在线攻击已经受到Sec.3.2.2中描述的节流要求的限制。

验证器**SHALL**向订阅者提供指导，帮助订阅者选择强密码。这在密码因出现在阻止列表中而被拒绝后尤为重要，因为它阻止对所列弱密码的简单修改[Blocklists]。

验证器**SHALL**实施速率限制机制，有效限制可在订阅者账户上进行的失败身份验证尝试次数，如Sec.3.2.2所述。

验证器**SHALL**允许使用密码管理器和自动填充功能。验证器**SHOULD**允许声称者在输入密码时使用“粘贴”功能，以便在密码自动填充 API 不可用时促进密码管理器的使用。密码管理器已被证明可以提高订阅者选择

stronger passwords, particularly if the password managers include password generators [Managers].

To help the claimant successfully enter a password, the verifier **SHOULD** offer an option to display the password — rather than a series of dots or asterisks — while it is entered and until it is submitted to the verifier. This allows the claimant to confirm their entry if they are in a location where their screen is unlikely to be observed. The verifier **MAY** also permit the claimant's device to display individual entered characters for a short time after each character is typed to verify the correct entry. This is common on mobile devices.

Verifiers **MAY** make limited allowances for mistyping (e.g., removing leading and trailing whitespace characters before verification, allowing the verification of passwords with differing cases for the leading character) if the password remains at least the required minimum length after such processing and the complexity of the resulting password is not significantly reduced.

Verifiers and CSPs **SHALL** use approved encryption and an authenticated protected channel when requesting passwords.

Verifiers **SHALL** store passwords in a form that is resistant to offline attacks. Passwords **SHALL** be *salted* and hashed using a suitable password hashing scheme. Password hashing schemes take a password, a salt, and a cost factor as inputs and generate a password hash. Their purpose is to make each password guess more expensive for an attacker who has obtained a hashed password file, thereby making the cost of a guessing attack high or prohibitive. The chosen cost factor **SHOULD** be as high as practical without negatively impacting verifier performance. It **SHOULD** be increased over time to account for increases in computing performance. An approved password hashing scheme published in the latest revision of [SP800-132] or updated NIST guidelines on password hashing schemes **SHOULD** be used. The chosen output length of the password verifier, excluding the salt and versioning information, **SHOULD** be the same as the length of the underlying password hashing scheme output.

The salt **SHALL** be at least 32 bits in length and chosen to minimize salt value collisions among stored hashes (i.e., to prevent multiple subscriber accounts from having the same hashed password). Both the salt value and the resulting hash **SHALL** be stored for each password. A reference to the password hashing scheme used, including the cost factor, **SHOULD** be stored for each password to allow migration to new algorithms and work factors.

In addition, verifiers **SHOULD** perform an additional iteration of a keyed hashing or encryption operation using a secret key known only to the verifier. If used, this key value **SHALL** be generated by an approved random bit generator, as described in Sec. 3.2.12. The secret key value **SHALL** be stored separately from the hashed passwords. It **SHOULD** be stored and used within a hardware-protected area, such as a hardware security

更强密码的可能性，特别是如果密码管理器包含密码生成器[Managers]。

为帮助声称者成功输入密码，验证器**应**提供在输入密码时显示密码的选项--而非显示一系列圆点或星号--直至密码提交给验证器。这允许声称者在屏幕不太可能被观察到的位置确认其输入。验证器**可**还允许声称者的设备在每输入一个字符后短暂显示单个已输入字符，以验证输入正确。这在移动设备上很常见。

验证器**MAY**对输入错误做出有限容忍(例如，在验证前删除前导和尾随空白字符，允许验证首字符大小写不同的密码)，前提是经过此类处理后密码仍至少达到所需的最小长度，且所得密码的复杂性没有显著降低。

验证器和 CSP 在请求密码时**SHALL**使用经批准的加密和经过身份验证的受保护信道。

验证器**应**以能够抵抗离线攻击的形式存储密码。密码**应**经过加盐并使用合适的密码哈希方案进行哈希。密码哈希方案以密码、盐和成本因子作为输入，生成密码哈希。其目的是使已获得哈希密码文件的攻击者每次猜测密码的成本更高，从而使猜测攻击的成本高昂或不可行。所选成本因子**应**在不对验证器性能产生负面影响的前提下尽可能高。它**应**随时间增加，以考虑计算性能的提升。应使用[SP800-132]最新修订版或更新的 NIST 密码哈希方案指南**中发布的经批准的密码哈希方案**。所选密码验证器输出长度(不包括盐和版本信息)**应**与底层密码哈希方案的输出长度相同。

盐值**SHALL**至少为 32 位长度，并选择以最小化存储哈希之间的盐值冲突(即防止多个订阅者账户具有相同的哈希密码)。盐值和所得哈希**SHALL**均须为每个密码存储。所使用的密码哈希方案的引用(包括成本因子)**SHOULD**为每个密码存储，以允许迁移到新算法和工作因子。

此外，验证器**SHOULD**使用仅验证器知道的秘密密钥执行一次额外的带密钥哈希或加密操作迭代。如果使用，此密钥值**SHALL**由经批准的随机位生成器生成，如Sec.3.2.12所述。秘密密钥值**SHALL**与哈希密码分开存储。它**SHOULD**在硬件保护区域内存储和使用，例如硬件安全

module or trusted execution environment (TEE), such as a trusted platform module (TPM). With this additional iteration, brute-force attacks on the hashed passwords are impractical as long as the secret key value remains secret.

3.1.2. Look-Up Secrets

A look-up secret authenticator is a physical or electronic record that stores a set of secrets shared between the claimant and the CSP. The claimant uses the authenticator to look up the appropriate secrets needed to respond to a prompt from the verifier. For example, the verifier could ask a claimant to provide a specific subset of the numeric or character strings printed on a card in table format. A typical application of look-up secrets is for one-time saved recovery codes (see Sec. 4.2.1.1) that the subscriber stores for use if another authenticator is lost or malfunctions. A look-up secret is "something you have."

Look-up secrets are not phishing-resistant.

3.1.2.1. Look-Up Secret Authenticators

CSPs that create look-up secret authenticators **SHALL** use an approved random bit generator, as described in Sec. 3.2.12, to generate the list of secrets and **SHALL** deliver the authenticator list securely to the subscriber (e.g., in an in-person session, via an online session, through the postal mail to a contact address). If delivered via an online session, the session **SHALL** be authenticated by the subscriber at AAL2 or higher and **SHALL** deliver the secrets through an authenticated protected channel and in accordance with the post-enrollment binding requirements in Sec. 4.1.2. Look-up secrets **SHALL** be at least six decimal digits (or equivalent) in length. Additional requirements described in Sec. 3.1.2.2 may also apply, depending on their length.

3.1.2.2. Look-Up Secret Verifiers

Verifiers of look-up secrets **SHALL** prompt the claimant for a secret from their authenticator. A secret from a look-up secret authenticator **SHALL** be used successfully only once. If the look-up secret is derived from a grid card, each grid cell **SHOULD** be used only once, which limits the number of authentications that can be accomplished using look-up secrets. A very long list of secrets is potentially required.

Verifiers **SHALL** store look-up secrets in a form that is resistant to offline attacks. All look-up secrets **SHALL** be stored in a hashed form using an approved hashing function.

Look-up secrets **SHALL** be at least six decimal digits (or equivalent) in length, as specified in Sec. 3.1.2.1. Look-up secrets that are shorter than specified lengths have additional verification requirements as follows:

- Look-up secrets that are shorter than the minimum security strength specified in the latest revision of [SP800-131A] (i.e., 112 bits as of the date of this publication)

模块或可信执行环境(TEE)，例如可信平台模块(TPM)。通过此额外迭代，只要秘密密钥值保持机密，对哈希密码的暴力攻击就不可行。

3.1.2. 查询型密钥

查询性秘密认证器是一种物理或电子记录，存储声称者与 CSP 之间共享的一组秘密。声称者使用认证器查找响应验证器提示所需的相应秘密。例如，验证器可以要求声称者提供以表格格式印在卡片上的数字或字符串的特定子集。查询性秘密的典型应用是一次性保存的恢复代码(见第 4.2.1.1 节)，订阅者存储这些代码以备另一个认证器丢失或故障时使用。查询性秘密是"你拥有的东西"。

查找型密钥不能抵御网络钓鱼。

3.1.2.1. 查询式密钥认证器

创建查询性秘密认证器的 CSP**应**使用经批准的随机位生成器(如第 3.2.12 节所述)生成秘密列表，并**应**将认证器列表安全地交付给订阅者(例如，通过面对面会话、在线会话、邮寄至联系地址)。如果通过在线会话交付，该会话**应**由订阅者以 AAL2 或更高等级进行认证，并**应**通过经认证的保护信道并按照第 4.1.2 节中的注册后绑定要求交付秘密。查询性秘密**应**至少为六位十进制数字(或等效长度)。根据其长度，第 3.1.2.2 节中描述的附加要求也可能适用。

3.1.2.2. 查询密钥验证器

查询性秘密的验证器**SHALL**提示声称者从其认证器提供秘密。来自查询性秘密认证器的秘密**SHALL**只能成功使用一次。如果查询性秘密源自网格卡，每个网格单元**SHOULD**仅使用一次，这限制了使用查询性秘密可完成的身份验证次数。可能需要非常长的秘密列表。

验证器**SHALL**以抵抗离线攻击的形式存储查询性秘密。所有查询性秘密**SHALL**使用经批准的哈希函数以哈希形式存储。

查询性秘密**SHALL**至少为六位十进制数字(或等效值)长度，如Sec.3.1.2.1所规定。短于规定长度的查询性秘密具有如下附加验证要求：

- 短于[SP800-131A]最新修订版中规定的最小安全强度(即截至本出版物日期为 112 位)的查询性秘密

SHALL be stored in a salted and hashed form using a suitable password hashing scheme, as described in Sec. 3.1.1.2. The salt value **SHALL** be at least 32 bits in length and arbitrarily chosen to minimize salt value collisions among stored hashes. Both the salt value and the resulting hash **SHALL** be stored for each look-up secret.

- The verifier **SHALL** implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber account, as described in Sec. 3.2.2.

The verifier **SHALL** use approved encryption and an authenticated protected channel when requesting look-up secrets.

3.1.3. Out-of-Band Devices

An out-of-band authenticator is a physical device that is uniquely addressable and can communicate securely with the verifier over an independent communications channel, which is referred to as the secondary channel. The device is possessed and controlled by the claimant and supports private communication over this separate secondary channel, which is separate from the primary channel for authentication. An out-of-band authenticator is "something you have." Examples of out-of-band devices include smartphones equipped with applications that allow the verifier to independently communicate with the subscriber or the use of text messaging or audio calls to communicate with the subscriber.

Out-of-band authentication uses a short-term secret generated by the verifier. The secret securely binds the authentication operation on the primary and secondary channels and establishes the claimant's control of the out-of-band device.

Out-of-band authentication is not phishing-resistant.

The out-of-band authenticator can operate in one of the following ways:

- The claimant transfers a secret received by the out-of-band device via the secondary channel to the verifier using the primary channel. For example, the claimant may receive the secret (typically a 6-digit code) on their mobile device and type it into their authentication session. This method is shown in Fig. 1.
- The claimant transfers a secret received via the primary channel to the out-of-band device for transmission to the verifier via the secondary channel. For example, the claimant may view the secret on their authentication session and either type it into an application on their mobile device or use a technology such as a barcode or QR code to effect the transfer. This method is shown in Fig. 2.

SHALL使用合适的密码哈希方案以加盐和哈希形式存储，如Sec.3.1.1.2所述。盐值**SHALL**至少为 32 位长度，并任意选择以最小化存储哈希之间的盐值冲突。盐值和所得哈希**SHALL**均须为每个查询性秘密存储。

- 验证器**SHALL**实施速率限制机制，有效限制可在订阅者账户上进行的失败身份验证尝试次数，如Sec.3.2.2所述。

验证器在请求查询性秘密时**SHALL**使用经批准的加密和经过身份验证的受保护信道。

3.1.3. 带外设备

带外认证器是一种物理设备，具有唯一可寻址性，并可通过独立通信信道与验证器安全通信，该信道称为辅助信道。该设备由声称者拥有和控制，并支持通过这一独立的辅助信道进行私密通信，该辅助信道与用于身份验证的主信道分离。带外认证器是"你拥有的东西"。带外设备的示例包括配备有允许验证器与订阅者独立通信的应用程序的智能手机，或使用文本消息或音频呼叫与订阅者通信。

带外身份验证使用由验证器生成的短期秘密。该秘密安全地将主信道和辅助信道上的身份验证操作绑定，并确立声称者对带外设备的控制。

带外认证不能抵御网络钓鱼。

带外认证器可通过以下方式之一运行：

- 声称者将通过辅助信道由带外设备接收的秘密转移到验证器，使用主信道。例如，声称者可以在其移动设备上接收秘密(通常为 6 位代码)并将其输入到其身份验证会话中。此方法如Fig.1所示。
- 声称者将通过主信道接收的秘密转移到带外设备，以通过辅助信道传输给验证器。例如，声称者可以在其身份验证会话中查看秘密，并将其输入到其移动设备上的应用程序中，或使用条形码或 QR 码等技术来实现转移。此方法如Fig.2所示。

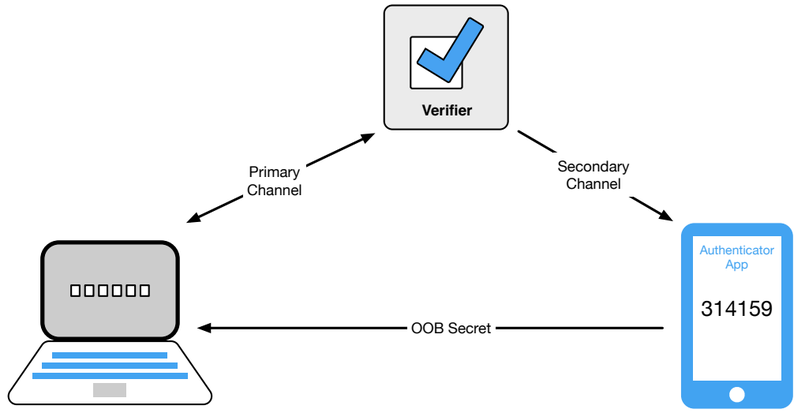


Fig. 1. Transfer of secret to primary device

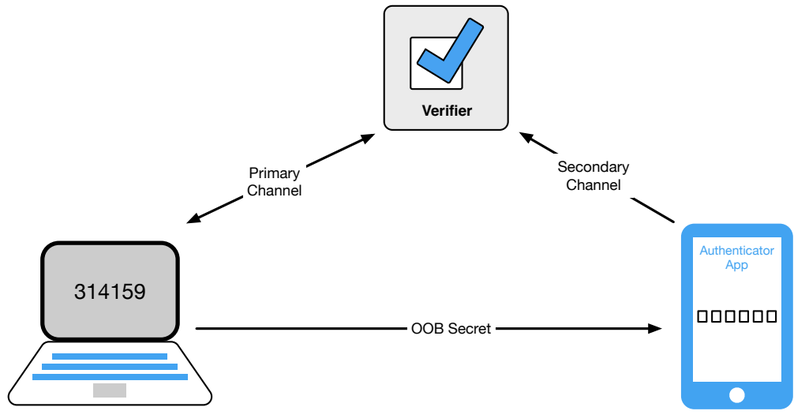


Fig. 2. Transfer of secret to out-of-band device

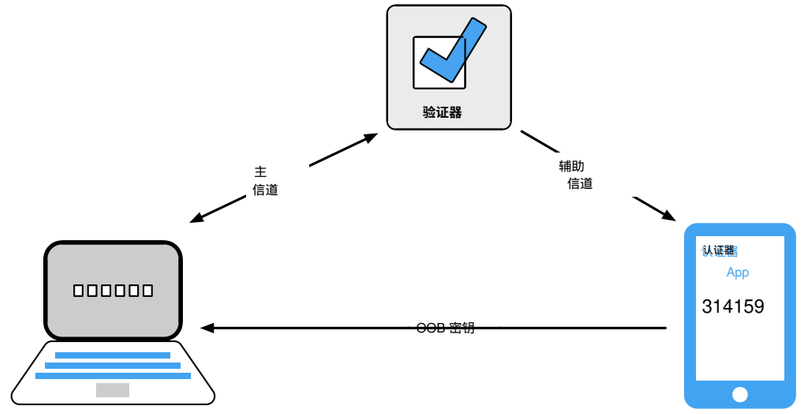


图 1. 将密钥传输至主设备

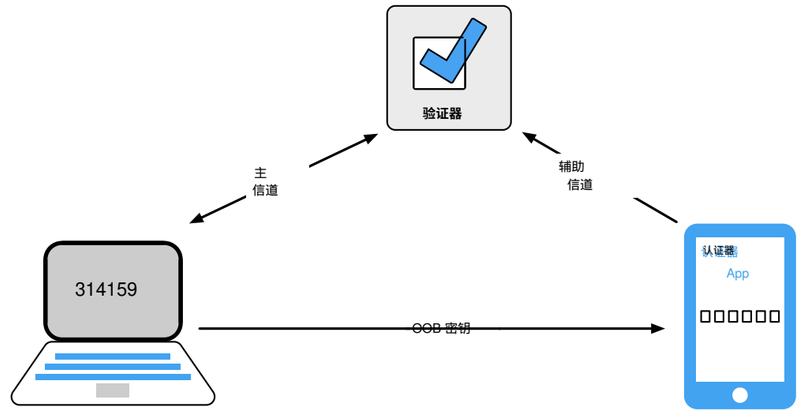


图 2. 将密钥传输到带外设备

> **Note:** A third method of out-of-band authentication compares the secrets received from the primary and secondary channels and requests approval on the secondary channel. This method is no longer considered acceptable because it increases the likelihood that the subscriber would approve an authentication request without actually comparing the secrets as required. This has been observed with "authentication fatigue" attacks in which an attacker generates many out-of-band authentication requests to the subscriber, who might approve one to eliminate the annoyance. For this reason, these guidelines require the transfer of the secret between the out-of-band device and the primary channel to increase assurance that the subject is actively participating in the session with the verifier. Presenting the claimant with a list of secrets to compare is not sufficient to meet this requirement, as the claimant may reasonably guess the secret due to the limited size of the list that can be presented.

3.1.3.1. Out-of-Band Authenticators

The out-of-band authenticator **SHALL** establish a separate channel with the verifier to retrieve the out-of-band secret or authentication request. This channel is considered to be out-of-band with respect to the primary communication channel (even if it terminates on the same device), provided that the device does not leak information from one channel to the other without the claimant's participation.

The out-of-band device **SHOULD** be uniquely addressable by the verifier. Communication over the secondary channel **SHALL** use approved encryption unless sent via the public switched telephone network (PSTN). For additional authenticator requirements that are specific to using the PSTN for out-of-band authentication, see Sec. 3.1.3.3.

Email **SHALL NOT** be used for out-of-band authentication because it may be vulnerable to:

- Access using only a password
- Interception in transit or at intermediate mail servers
- Rerouting attacks, such as those caused by Domain Name System (DNS) spoofing

> Confirmation codes that are sent to validate email addresses or are issued as recovery codes (see Sec. 4.2.1.2) are not authentication processes and not affected by the above prohibition.

The out-of-band authenticator **SHALL** uniquely authenticate itself in one of the following ways when communicating with the verifier:

> **注：**带外身份验证的第三种方法比较从主信道和辅助信道接收的密钥，并在辅助信道上请求批准。该方法不再被认为可接受，因为它增加了订阅者在实际未按要求比较密钥的情况下批准身份验证请求的可能性。这已在"身份验证疲劳"攻击中被观察到，其中攻击者向订阅者生成许多带外身份验证请求，订阅者可能批准其中一个以消除烦扰。因此，这些指南要求带外设备与主信道之间传输密钥，以增加保证主体正在积极参与与验证器的会话。向声称者呈现要比较的密钥列表不足以满足此要求，因为由于可呈现的列表大小有限，声称者可能合理地猜测密钥。

3.1.3.1. 带外认证器

带外认证器**SHALL**与验证器建立单独的信道以检索带外秘密或身份验证请求。该信道相对于主通信信道被视为带外(即使它终止于同一设备)，前提是该设备在未经声称者参与的情况下不会从一个信道泄露信息到另一个信道。

带外设备**SHOULD**可由验证器唯一寻址。通过辅助信道的通信**SHALL**使用经批准的加密，除非通过公共交换电话网络(PSTN)发送。有关使用 PSTN 进行带外身份验证的附加认证器要求，请参见Sec.3.1.3.3。

电子邮件**SHALL NOT**用于带外身份验证，因为它可能容易受到

- 仅使用密码访问
- 在传输途中或中间邮件服务器上截获
- 重路由攻击，例如由域名系统(DNS)欺骗引起的攻击

> 用于验证电子邮件地址或作为恢复代码发放的确认码(见第4.2.1.2节)不属于身份验证过程，不受上述禁令的影响。

带外认证器**SHALL**在与验证器通信时，通过以下方式之一唯一地认证自身：

- Using approved cryptography, establish a mutually authenticated protected channel (e.g., client-authenticated *transport layer security* (TLS) [RFC8446]) with the verifier. Communication between the out-of-band authenticator and the verifier **MAY** use a trusted intermediary service to which each authenticates. The key used to establish the channel **SHALL** be provisioned in a mutually authenticated session during authenticator binding, as described in Sec. 4.1.
- Authenticate to a public mobile telephone network using a SIM card or equivalent secret that uniquely identifies the subscriber. This method **SHALL** only be used if a secret is sent from the verifier to the out-of-band device via the PSTN (i.e., SMS or voice) or an encrypted instant messaging service.
- Use a wired connection to the PSTN that the verifier can call and dictate the out-of-band secret. For the purposes of this definition, "wired connection" includes services such as cable providers that offer PSTN services through other wired media and fiber via analog telephone adapters.

For single-factor out-of-band authenticators, if a secret is sent by the verifier to the out-of-band device, the device **SHOULD NOT** display the authentication secret while it is locked by the owner. Rather, the device **SHOULD** require the presentation and verification of a PIN, passcode, or biometric characteristic to view the secret. However, authenticators **SHOULD** indicate the receipt of an authentication secret on a locked device.

If the out-of-band authenticator requests approval over the secondary communication channel rather than by presenting a secret that the claimant transfers to the primary communication channel, it **SHALL** accept a transfer of the secret from the primary channel and send it to the verifier over the secondary channel to associate the approval with the authentication transaction. The claimant **MAY** perform the transfer manually or with the assistance of a representation, such as a barcode or quick response (QR) code.

3.1.3.2. Out-of-Band Verifiers

The verifier waits for an authenticated protected channel to be established with the out-of-band authenticator and verifies its identifying key. The verifier **SHALL NOT** store the identifying key itself but **SHALL** use a verification method (e.g., an approved hash function or proof of possession of the identifying key) to uniquely identify the authenticator. Once authenticated, the verifier transmits the authentication secret to the authenticator. The connection with the out-of-band authenticator **MAY** be either manually initiated or prompted by a mechanism, such as a push notification.

Depending on the type of out-of-band authenticator, one of the following **SHALL** take place:

- **Transfer of the secret from the secondary to the primary channel**. As shown in Fig. 1, the verifier **MAY** signal the device that contains the subscriber's

- 使用经批准的密码学，与验证器建立相互身份验证的保护信道(例如，客户端身份验证的传输层安全(TLS)[RFC8446])。带外认证器与验证器之间的通信**可以**使用受信任的中间服务，双方各自向其进行身份验证。用于建立信道的密钥**应**在认证器绑定期间的相互身份验证会话中配置，如第4.1节所述。
- 使用唯一标识订阅者的SIM卡或等效秘密向公共移动电话网络进行认证。仅当秘密由验证器通过PSTN(即SMS或语音)或加密即时消息服务发送到带外设备时，**SHALL**才使用此方法。
- 使用验证器可以呼叫并口述带外秘密的PSTN有线连接。就本定义而言，"有线连接"包括通过其他有线介质提供PSTN服务的电缆提供商等服务，以及通过模拟电话适配器提供的光纤服务。

对于单因素带外认证器，如果验证器向带外设备发送秘密，则该设备在被所有者锁定时**SHOULD NOT**显示身份验证秘密。相反，设备**SHOULD**要求出示并验证PIN、密码或生物特征以查看该秘密。然而，认证器SHOULD在锁定设备上指示已收到身份验证秘密。

如果带外认证器在辅助通信信道上请求批准，而不是通过呈现声称者传输到主通信信道的密钥来请求批准，则它**应**接受来自主信道的密钥传输，并通过辅助信道将其发送给验证器，以将批准与身份验证事务关联。声称者**可以**手动执行传输，或在表示的协助下执行传输，例如条形码或快速响应(QR)码。

3.1.3.2. 带外验证器

验证器等待与带外认证器建立经身份验证的保护信道，并验证其标识密钥。验证器**不得**存储标识密钥本身，但应使用验证方法(例如，经批准的哈希函数或标识密钥的拥有证明)来唯一标识认证器。一旦通过身份验证，验证器将身份验证密钥传输给认证器。与带外认证器的连接**可以**手动发起，或由机制(例如推送通知)提示发起。

根据带外认证器的类型，**SHALL**发生以下情况之一：

- **将秘密从辅助信道传输到主信道**。如图1所示，验证器**MAY**向包含订阅者

authenticator to indicate a readiness to authenticate. It **SHALL** then transmit a random secret to the out-of-band authenticator and wait for the secret to be returned via the primary communication channel.

- **Transfer of the secret from the primary to the secondary channel**. As shown in Fig. 2, the verifier **SHALL** transmit a random authentication secret to the claimant via the primary channel. It **SHALL** then wait for the secret to be returned via the secondary channel from the claimant's out-of-band authenticator. The verifier **MAY** additionally display an address, such as a phone number or VoIP address, for the claimant to use in addressing its response to the verifier.

In all cases, the authentication **SHALL** be considered invalid unless completed within 10 minutes. Verifiers **SHALL** accept a given authentication secret as valid only once during the validity period to provide *replay resistance*, as described in Sec. 3.2.7.

The verifier **SHALL** generate random authentication secrets that are at least six decimal digits (or equivalent) in length using an approved random bit generator as described in Sec. 3.2.12. If the authentication secret is less than 64 bits long, the verifier **SHALL** implement a rate-limiting mechanism that effectively limits the total number of consecutive failed authentication attempts that can be made on the subscriber account as described in Sec. 3.2.2. Generating a new authentication secret **SHALL NOT** reset the failed authentication count.

Out-of-band verifiers that send a push notification to a subscriber device **SHOULD** implement a reasonable limit on the rate or total number of push notifications that will be sent since the last successful authentication.

For additional verification requirements that are specific to the PSTN, see Sec. 3.1.3.3.

3.1.3.3. Authentication Using the Public Switched Telephone Network

Use of the PSTN for out-of-band verification is *restricted* as described in this section and **SHALL** satisfy the requirements of Sec. 3.2.9. Setting or changing the pre-registered telephone number is considered to be the binding of a new authenticator and **SHALL** only occur as described in Sec. 4.1.2.

Some subscribers may be unable to use PSTN to deliver out-of-band authentication secrets in areas with limited telephone coverage, particularly without mobile phone service. Accordingly, verifiers **SHALL** ensure that alternative authenticator types are available to all subscribers and **SHOULD** remind subscribers of this limitation of PSTN out-of-band authenticators before binding one or more devices controlled by the subscriber.

Verifiers **SHOULD** consider risk indicators (e.g., device swap, SIM change, number porting, other abnormal behavior) before using the PSTN to deliver an out-of-band authentication secret.

认证器以表明准备进行身份验证。然后，它**SHALL**向带外认证器发送一个随机秘密，并等待该秘密通过主通信信道返回。

- **秘密从主信道转移到辅助信道**。如图2所示，验证器**SHALL**通过主信道向声称者发送一个随机身份验证秘密。然后，它**SHALL**等待该秘密通过辅助信道从声称者的带外认证器返回。验证器**MAY**额外显示一个地址，例如电话号码或VoIP地址，供声称者在其对验证器的响应中使用。

在所有情况下，除非在10分钟内完成，否则身份验证**SHALL**被视为无效。验证器**SHALL**在有效期内仅接受给定的身份验证秘密一次为有效，以提供抗重放，如第3.2.7节所述。

验证器**应**使用经批准的随机位生成器(如第3.2.12节所述)生成至少六位十进制数字(或等效长度)的随机身份验证密钥。如果身份验证密钥长度小于64位，验证器**应**实施速率限制机制，有效限制订阅者账户上可进行的连续失败身份验证尝试总数，如第3.2.2节所述。生成新的身份验证密钥**不得**重置失败身份验证计数。

向订阅者设备发送推送通知的带外验证器**SHOULD**对自上次成功身份验证以来将发送的推送通知的速率或总数实施合理限制。

有关PSTN特有的额外验证要求，请参见第3.1.3.3节。

3.1.3.3. 使用公共交换电话网的认证

使用PSTN进行带外验证受到本节所述的限制，并且**SHALL**满足第3.2.9节的要求。设置或更改预注册电话号码被视为新认证器的绑定，并且**SHALL**仅在第4.1.2节所述的情况下发生。

在电话覆盖有限的地区，特别是没有移动电话服务的地区，一些订阅者可能无法使用PSTN来传递带外身份验证秘密。因此，验证器**SHALL**确保所有订阅者都可以使用替代认证器类型，并且**SHOULD**在绑定由订阅者控制的一个或多个设备之前，提醒订阅者PSTN带外认证器的这一限制。

验证器**SHOULD**在使用PSTN传递带外身份验证秘密之前考虑风险指标(例如，设备更换、SIM卡更换、号码移植、其他异常行为)。

> Consistent with the discussion of *restricted authenticators* in Sec. 3.2.9, NIST may adjust the restricted status of out-of-band authentication using the PSTN based on the evolution of the threat landscape and the technical operation of the PSTN.

3.1.3.4. Multi-Factor Out-of-Band Authenticators

Multi-factor out-of-band authenticators operate similarly to single-factor out-of-band authenticators (see Sec. 3.1.3.1). However, they require the presentation and verification of an activation factor (i.e., a password or a biometric characteristic) before allowing the claimant to complete the authentication transaction (i.e., before accessing or entering the authentication secret as appropriate for the authentication flow being used). Each use of the authenticator **SHALL** require the presentation of the activation factor.

Authenticator activation secrets **SHALL** meet the requirements of Sec. 3.2.10. A biometric activation factor **SHALL** meet the requirements of Sec. 3.2.3, including limits on the number of consecutive authentication failures. The password or biometric sample used for activation and any biometric data derived from the biometric sample (e.g., a fingerprint image and feature locations produced by a fingerprint feature extractor) **SHALL** be erased immediately after an authentication operation.

3.1.4. Single-Factor OTP

A single-factor OTP generates one-time passwords (OTPs). This category includes hardware devices and software-based OTP generators that are installed on devices such as mobile phones. These authenticators have an embedded secret that is used as the seed for generating OTPs and do not require activation through a second factor. The OTP is displayed on the authenticator and manually input for transmission to the verifier, thereby proving possession and control of the authenticator. A single-factor OTP authenticator is “something you have.”

Single-factor OTPs are similar to look-up secret authenticators except that the secrets are cryptographically and independently generated by the authenticator and the verifier and compared by the verifier. The secret is computed based on a nonce that may be time-based or from a counter on the authenticator and verifier.

OTP authentication is not phishing-resistant. [FIPS140] validation of OTP authenticators and verifiers is not required.

3.1.4.1. Single-Factor OTP Authenticators

Single-factor OTP authenticators and verifiers contain two persistent values: 1) a symmetric key that persists for the authenticator’s lifetime and 2) a nonce that is either changed each time the authenticator is used or is based on a real-time clock.

> 与第3.2.9节中关于受限认证器的讨论一致，NIST可以根据威胁态势的演变和PSTN的技术运行情况，调整使用PSTN进行带外身份验证的受限状态。

3.1.3.4. 多因素带外认证器

多因素带外认证器的操作方式与单因素带外认证器类似(参见第3.1.3.1节)。但是，它们要求在允许声称者完成身份验证事务之前(即，在根据所使用的身份验证流程访问或输入身份验证密钥之前)，出示并验证激活因子(即密码或生物特征)。每次使用认证器**应**要求出示激活因子。

认证器激活密钥**应**满足第3.2.10节的要求。生物特征激活因子**应**满足第3.2.3节的要求，包括对连续身份验证失败次数的限制。用于激活的密码或生物特征样本以及从生物特征样本衍生的任何生物特征数据(例如，指纹特征提取器生成的指纹图像和特征位置)**应**在身份验证操作后立即擦除。

3.1.4. 单因素 OTP

单因素OTP生成一次性密码(OTP)。此类别包括硬件设备和安装在移动电话等设备上的基于软件的OTP生成器。这些认证器具有嵌入式密钥，用作生成OTP的种子，并且不需要通过第二因素激活。OTP显示在认证器上，并手动输入以传输给验证器，从而证明对认证器的拥有和控制。单因素OTP认证器是“你拥有的东西”。

单因素OTP与查询性秘密认证器类似，不同之处在于秘密由认证器和验证器以密码学方式独立生成，并由验证器进行比较。秘密基于随机数计算，该随机数可以是基于时间的，或来自认证器和验证器上的计数器。

OTP身份验证不抗钓鱼。[FIPS140]不要求对OTP认证器和验证器进行验证。

3.1.4.1. 单因素 OTP 认证器

单因素OTP认证器和验证器包含两个持久值：1)在认证器生命周期内持久的对称密钥，以及2)每次使用认证器时更改或基于实时时钟的随机数。

The secret key and its algorithm **SHALL** provide at least the minimum security strength specified in the latest revision of [SP800-131A] (i.e., 112 bits as of the date of this publication). The nonce **SHALL** be of sufficient length to ensure that it is unique for each operation of the authenticator over its lifetime. If a subscriber needs to change the device on which a software-based OTP authenticator resides, they **SHOULD** bind the authenticator application on the new device to their subscriber account, as described in Sec. 4.1.2, and invalidate the authenticator application that will no longer be used. Alternatively, the subscriber **MAY** export the secret key and store it in a *sync fabric* that meets the requirements in Appendix B.2 and then retrieve the key with their new device.

The authenticator output is obtained using an approved block cipher or hash function to securely combine the key and nonce. In coordination with the verifier, the authenticator **MAY** truncate its output to as few as six decimal digits (or an equivalent representation).

If the nonce used to generate the authenticator output is based on a real-time clock, the nonce **SHALL** be changed at least once every two minutes.

3.1.4.2. Single-Factor OTP Verifiers

Single-factor OTP verifiers effectively duplicate the process of generating the OTP used by the authenticator. As such, the symmetric keys used by authenticators are also present in the verifier and **SHALL** be strongly protected against unauthorized disclosure by access controls that limit access to the keys to only those software components that require access.

When binding a single-factor OTP authenticator to a subscriber account, the verifier or associated CSP **SHALL** use approved cryptography for key establishment to generate and exchange keys or to obtain the secrets required to duplicate the authenticator output.

The verifier **SHALL** use approved encryption and an authenticated protected channel when collecting the OTP. Verifiers **SHALL** accept a given OTP only once while it is valid to provide replay resistance, as described in Sec. 3.2.7. If a claimant's authentication is denied due to the duplicate use of an OTP, verifiers **MAY** warn the claimant if an attacker has been able to authenticate in advance. Verifiers **MAY** also warn a subscriber in an existing session of the attempted duplicate use of an OTP.

Time-based OTPs [TOTP] **SHALL** have a defined lifetime that is determined by the expected clock drift in either direction of the authenticator over its lifetime plus an allowance for network delay and claimant entry of the OTP.

The verifier **SHOULD** implement or, if the authenticator output is less than 64 bits in length, **SHALL** implement a rate-limiting mechanism that effectively limits the number of failed authentication attempts that can be made on the subscriber account, as described in Sec. 3.2.2.

密钥及其算法**应**至少提供[SP800-131A]最新修订版中规定的最低安全强度(即，截至本出版物发布之日为112位)。随机数**应**具有足够的长度，以确保其在认证器生命周期内的每次操作中都是唯一的。如果订阅者需要更改基于软件的OTP认证器所在的设备，他们**宜**按照第4.1.2节所述，将新设备上的认证器应用程序绑定到其订阅者账户，并使不再使用的认证器应用程序失效。或者，订阅者**可**导出密钥并将其存储在满足附录B.2要求的同步结构中，然后使用其新设备检索该密钥。

认证器输出通过使用经批准的块密码或哈希函数安全地组合密钥和随机数来获得。在与验证器协调的情况下，认证器**MAY**将其输出截断为少至六位十进制数字(或等效表示)。

如果用于生成认证器输出的随机数基于实时时钟，则该随机数**SHALL**至少每两分钟更改一次。

3.1.4.2. 单因素 OTP 验证器

单因素OTP验证器有效地复制了认证器生成OTP的过程。因此，认证器使用的对称密钥也存在于验证器中，并且**SHALL**通过访问控制受到强力保护，防止未经授权的泄露，该访问控制仅允许需要访问的软件组件访问密钥。

将单因素OTP认证器绑定到订阅者账户时，验证器或相关CSP**SHALL**使用经批准的密码学进行密钥建立，以生成和交换密钥，或获取复制认证器输出所需的秘密。

验证器**应**在收集OTP时使用经批准的加密和经过身份验证的保护信道。验证器**应**在其有效期内仅接受给定的OTP一次，以提供抗重放能力，如第3.2.7节所述。如果声称者的身份验证因OTP的重复使用而被拒绝，验证器**可以**在攻击者已能够提前通过身份验证的情况下警告声称者。验证器**还可以**在现有会话中警告订阅者OTP被尝试重复使用。

基于时间的OTP[TOTP]**SHALL**具有定义的生存期，该生存期由认证器在其生存期内任一方向的预期时钟漂移加上网络延迟和声称者输入OTP的余量确定。

验证器**SHOULD**实施，或者如果认证器输出长度小于64位，则**SHALL**实施一种速率限制机制，有效限制可对订阅者账户进行的失败身份验证尝试次数，如第3.2.2节所述。

3.1.5. Multi-Factor OTPs

A multi-factor OTP generates one-time passwords for authentication following the input of an activation factor. This includes hardware devices and software-based OTP generators that are installed on mobile phones and similar devices. The second authentication factor may be provided through an integral entry pad, an integral biometric (e.g., fingerprint) reader, or a direct computer interface (e.g., universal serial bus [USB] port). The OTP is displayed on the authenticator and manually input for transmission to the verifier. The multi-factor OTP authenticator is "something you have" activated by either "something you know" or "something you are."

OTP authentication is not phishing-resistant. [FIPS140] validation of OTP authenticators and verifiers is not required.

3.1.5.1. Multi-Factor OTP Authenticators

Multi-factor OTP authenticators operate similarly to single-factor OTP authenticators (see Sec. 3.1.4.1), except they require the presentation and verification of an activation factor (i.e., a password or a biometric characteristic) to obtain the OTP from the authenticator. Each use of the authenticator **SHALL** require the input of the activation factor.

In addition to activation information, multi-factor OTP authenticators and verifiers contain two persistent values: 1) a symmetric key that persists for the authenticator's lifetime and 2) a nonce that is either changed each time the authenticator is used or based on a real-time clock.

The secret key and its algorithm **SHALL** provide at least the minimum security strength specified in the latest revision of [SP800-131A] (i.e., 112 bits as of the date of this publication). The nonce **SHALL** be of sufficient length to ensure that it is unique for each operation of the authenticator over its lifetime. If a subscriber needs to change the device on which a software-based OTP authenticator resides, they **SHOULD** bind the authenticator application on the new device to their subscriber account, as described in Sec. 4.1.2, and invalidate the authenticator application that will no longer be used. Alternatively, the subscriber **MAY** export the secret key and store it in a sync fabric that meets the requirements in Appendix B.2 and retrieve the key with their new device.

The authenticator output is obtained using an approved cryptography block cipher or hash function to securely combine the key and nonce. In coordination with the verifier, the authenticator **MAY** truncate its output to as few as six decimal digits or equivalent.

If the nonce used to generate the authenticator output is based on a real-time clock, the nonce **SHALL** be changed at least once every two minutes.

Authenticator activation secrets **SHALL** meet the requirements of Sec. 3.2.10. A biometric activation factor **SHALL** meet the requirements of Sec. 3.2.3, including limits on the number of consecutive authentication failures. The unencrypted key and

3.1.5. 多因素 OTP

多因素OTP在输入激活因素后生成用于身份验证的一次性密码。这包括安装在移动电话及类似设备上的硬件设备和基于软件的OTP生成器。第二身份验证因素可以通过集成输入板、集成生物特征(例如指纹)读取器或直接计算机接口(例如通用串行总线[USB]端口)提供。OTP显示在认证器上，并手动输入以传输给验证器。多因素OTP认证器是"你拥有的东西"，由"你知道的东西"或"你是什么"激活。

OTP身份验证不抗钓鱼。[FIPS140]不要求对OTP认证器和验证器进行验证。

3.1.5.1. 多因素 OTP 认证器

多因素OTP认证器的操作与单因素OTP认证器类似(参见第3.1.4.1节)，不同之处在于它们需要呈现和验证激活因子(即密码或生物特征)才能从认证器获取OTP。每次使用认证器**SHALL**需要输入激活因子。

除激活信息外，多因素OTP认证器和验证器还包含两个持久值：1)在认证器生命周期内持久的对称密钥，以及2)每次使用认证器时更改或基于实时时钟的随机数。

密钥及其算法**应**至少提供[SP800-131A]最新修订版中规定的最低安全强度(即截至本出版物发布之日为112位)。随机数**应**具有足够的长度，以确保其在认证器的整个生命周期内对每次操作都是唯一的。如果订阅者需要更换基于软件的OTP认证器所在的设备，他们**宜**按照第4.1.2节所述，将新设备上的认证器应用程序绑定到其订阅者账户，并使不再使用的认证器应用程序失效。或者，订阅者**可以**导出密钥并将其存储在满足附录B.2要求的同步结构中，并使用其新设备检索该密钥。

认证器输出通过使用经批准的密码学块密码或哈希函数安全地组合密钥和随机数来获得。在与验证器协调的情况下，认证器**MAY**将其输出截断为少至六位十进制数字或等效值。

如果用于生成认证器输出的随机数基于实时时钟，则该随机数**SHALL**至少每两分钟更改一次。

认证器激活秘密**SHALL**满足第3.2.10节的要求。生物特征激活因子**SHALL**满足第3.2.3节的要求，包括对连续身份验证失败次数的限制。未加密的密钥和

activation secret or biometric sample and any biometric data derived from the biometric sample (e.g., a fingerprint image and feature locations produced by a fingerprint feature extractor) **SHALL** be erased immediately after an OTP has been generated.

3.1.5.2. Multi-Factor OTP Verifiers

Multi-factor OTP verifiers effectively duplicate the process of generating the OTP used by the authenticator without requiring a second authentication factor. As such, the symmetric keys used by authenticators **SHALL** be strongly protected against unauthorized disclosure by access controls that limit access to the keys to only those software components that require access.

When binding a multi-factor OTP authenticator to a subscriber account, the verifier or associated CSP **SHALL** use approved cryptography for key establishment to generate and exchange keys or to obtain the secrets required to duplicate the authenticator output.

The verifier **SHALL** use approved encryption and an authenticated protected channel when collecting the OTP. Verifiers **SHALL** accept a given OTP only once while it is valid to provide replay resistance, as described in Sec. 3.2.7. If a claimant's authentication is denied due to the duplicate use of an OTP, verifiers **MAY** warn the claimant if an attacker has been able to authenticate in advance. Verifiers **MAY** also warn a subscriber in an existing session of the attempted duplicate use of an OTP.

Time-based OTPs [TOTP] **SHALL** have a defined lifetime that is determined by the expected clock drift in either direction of the authenticator over its lifetime plus an allowance for network delay and claimant entry of the OTP.

The verifier **SHALL** implement a rate-limiting mechanism that effectively limits the number of consecutive failed authentication attempts that can be made on the subscriber account, as required by Sec. 3.2.10.

3.1.6. Single-Factor Cryptographic Authentication

Single-factor cryptographic authentication is accomplished by proving the possession and control of a cryptographic key via an authentication protocol. Depending on the strength of authentication required, the authentication key may be stored in a manner that is accessible to the endpoint associated with the authenticator or in a separate, directly connected processor or device. The authenticator output is highly dependent on the specific cryptographic protocol used but is generally some type of signed message. A single-factor cryptographic authenticator is "something you have." Single-factor cryptographic authenticators used at AAL3 **SHALL** use public-key cryptography to protect the authentication secrets from compromise of the verifier.

Cryptographic authentication is phishing-resistant if it meets the additional requirements in Sec. 3.2.5.

激活秘密或生物特征样本以及从生物特征样本导出的任何生物特征数据(例如，指纹图像和指纹特征提取器产生的特征位置)**SHALL**在生成OTP后立即擦除。

3.1.5.2. 多因素 OTP 验证器

多因素OTP验证器有效地复制了认证器生成OTP的过程，而无需第二身份验证因素。因此，认证器使用的对称密钥**SHALL**通过访问控制受到强力保护，防止未经授权的泄露，该访问控制仅允许需要访问的软件组件访问密钥。

将多因素OTP认证器绑定到订阅者账户时，验证器或相关CSP**SHALL**使用经批准的密码学进行密钥建立，以生成和交换密钥，或获取复制认证器输出所需的秘密。

验证器**应**在收集OTP时使用经批准的加密和经过身份验证的保护信道。验证器**应**在其有效期内仅接受给定的OTP一次，以提供抗重放能力，如第3.2.7节所述。如果声称者的身份验证因OTP的重复使用而被拒绝，验证器**可以**在攻击者已能够提前通过身份验证的情况下警告声称者。验证器**还可以**在现有会话中警告订阅者OTP被尝试重复使用。

基于时间的OTP[TOTP]**SHALL**具有定义的生存期，该生存期由认证器在其生存期内任一方向的预期时钟漂移加上网络延迟和声称者输入OTP的余量确定。

验证器**SHALL**实施一种速率限制机制，有效限制可对订阅者账户进行的连续失败身份验证尝试次数，如第3.2.10节所要求。

3.1.6. 单因素加密认证

单因素加密身份验证通过身份验证协议证明对加密密钥的拥有和控制来实现。根据所需身份验证的强度，身份验证密钥可以以与认证器相关联的端点可访问的方式存储，或存储在单独的、直接连接的处理器或设备中。认证器输出高度依赖于所使用的特定加密协议，但通常是某种类型的签名消息。单因素加密认证器是"你拥有的东西"。在AAL3下使用的单因素加密认证器**应**使用公钥加密来保护身份验证机密免受验证器泄露的影响。

如果密码学身份验证满足第3.2.5节中的额外要求，则它是抗钓鱼的。

3.1.6.1. Single-Factor Cryptographic Authenticators

Single-factor cryptographic authenticators encapsulate one or more authentication keys. Authentication keys are described as either exportable (see Sec. 3.2.13) or non-exportable. Exportable authentication keys (usable at AAL2 or below) **SHOULD** be stored in appropriate storage that is available to the authenticator (e.g., keychain storage). If they are accessible to the endpoint being authenticated, exportable authentication keys **SHALL** be strongly protected against unauthorized disclosure with access controls that limit access to the key to only those software components that require access. Non-exportable authentication keys (usable at AAL3 or below) **SHALL** be stored in an isolated execution environment that is protected by hardware or in a separate processor with a controlled interface to the central processing unit of the user endpoint.

Some cryptographic authenticators, referred to as syncable authenticators, can manage their authentication keys using a sync fabric (e.g., a cloud provider). Additional requirements for using syncable authenticators are in Appendix B.

External (i.e., non-embedded) cryptographic authenticators **SHALL** meet the requirements for connected authenticators in Sec. 3.2.11.

As required by Sec. 2.3.2, single-factor cryptographic authenticators that are being used at AAL3 must meet the authentication intent requirements of Sec. 3.2.8.

3.1.6.2. Single-Factor Cryptographic Verifiers

Single-factor cryptographic verifiers generate a challenge nonce, send it to the corresponding authenticator, and use the authenticator output to verify possession of the authenticator. The authenticator output is highly dependent on the specific cryptographic authenticator and protocol used but is generally some type of signed message.

The verifier has a public cryptographic key that corresponds to each authenticator. While both types of keys **SHALL** be protected against modification, symmetric keys **SHALL** additionally be protected against unauthorized disclosure by access controls that limit access to the key to only those software components that require access.

The authentication key and its algorithm **SHALL** provide at least the minimum security strength specified in the latest revision of [SP800-131A] (i.e., 112 bits as of the date of this publication). The challenge nonce **SHALL** be at least 64 bits in length and **SHALL** either be unique over the authenticator's lifetime or statistically unique (i.e., generated using an approved random bit generator, as described in Sec. 3.2.12). The verification operation **SHALL** use approved cryptography.

3.1.7. Multi-Factor Cryptographic Authentication

Multi-factor cryptographic authentication uses an authentication protocol to prove possession and control of an authentication key that requires activation through a

3.1.6.1. 单因素加密认证器

单因素加密认证器封装一个或多个身份验证密钥。身份验证密钥被描述为可导出(见第3.2.13节)或不可导出。可导出的身份验证密钥(可在AAL2或以下使用)**宜**存储在认证器可用的适当存储中(例如钥匙串存储)。如果可导出的身份验证密钥可被正在通过身份验证的端点访问，则**应**通过访问控制对其进行强保护，防止未经授权的泄露，访问控制将密钥的访问限制为仅需要访问的那些软件组件。不可导出的身份验证密钥(可在AAL3或以下使用)**应**存储在受硬件保护的隔离执行环境中，或存储在具有与用户端点中央处理单元受控接口的单独处理器中。

一些密码学认证器，称为可同步认证器，可以使用同步结构(例如，云提供商)管理其身份验证密钥。使用可同步认证器的额外要求见附录B。

外部(即非嵌入式)密码学认证器**SHALL**满足第3.2.11节中连接认证器的要求。

按照第2.3.2节的要求，在AAL3级别使用的单因素加密认证器必须满足第3.2.8节的身份验证意图要求。

3.1.6.2. 单因素加密验证器

单因素加密验证器生成一个挑战随机数，将其发送给相应的认证器，并使用认证器输出来验证对认证器的持有。认证器输出高度依赖于具体的加密认证器和所使用的协议，但通常是某种类型的签名消息。

验证器拥有与每个认证器相对应的公共加密密钥。虽然两种类型的密钥**SHALL**受到防修改保护，但对称密钥**SHALL**额外受到访问控制的保护以防止未经授权的泄露，该访问控制将密钥的访问限制为仅限那些需要访问的软件组件。

认证密钥及其算法**应**至少提供[SP800-131A]最新修订版中规定的最低安全强度(即截至本出版物发布之日为112位)。挑战随机数**应**至少为64位长度，并且**应**在认证器的生命周期内唯一或统计唯一(即使用经批准的随机位生成器生成，如第3.2.12节所述)。验证操作**应**使用经批准的密码学。

3.1.7. 多因素加密认证

多因素加密身份验证使用身份验证协议来证明对身份验证密钥的持有和控制，该密钥需要通过以下方式激活：

second authentication factor. Depending on the strength of authentication needed, the authentication key may be stored in a manner that is accessible to the endpoint being authenticated or in a separate, directly connected processor or device. The authenticator output is highly dependent on the specific cryptographic protocol used but is generally some type of signed message. A multi-factor cryptographic authenticator is “something you have” and is activated by an activation factor that represents either “something you know” or “something you are.” Multi-factor cryptographic authenticators used at AAL3 **SHALL** use public-key cryptography to protect the authentication secrets from compromise of the verifier.

Cryptographic authentication is phishing-resistant if it meets the additional requirements in Sec. 3.2.5.

3.1.7.1. Multi-Factor Cryptographic Authenticators

Multi-factor cryptographic authenticators encapsulate one or more authentication keys that **SHALL** only be accessible through the presentation and verification of an activation factor (i.e., a password or a biometric characteristic). Non-exportable authentication keys, suitable for use at AAL3, **SHALL** be stored in an isolated execution environment that is protected by hardware or in a separate processor with a controlled interface to the central processing unit of the user endpoint. Exportable authentication keys (usable at AAL2 or below) **SHOULD** be stored in appropriate storage that is available to the authenticator (e.g., keychain storage). If accessible to the endpoint being authenticated, authentication keys **SHALL** be strongly protected against unauthorized disclosure by using access controls that limit access to the authentication keys to only those software components that require access.

External (non-embedded) cryptographic authenticators **SHALL** meet the requirements for connected authenticators in Sec. 3.2.11. Each authentication event **SHALL** require input and verification of the local activation factor. Authenticator activation secrets **SHALL** meet the requirements of Sec. 3.2.10. A biometric activation factor **SHALL** meet the requirements of Sec. 3.2.3, including limits on the number of consecutive authentication failures. The activation secret or biometric sample and any biometric data derived from the biometric sample (e.g., a fingerprint image and feature locations produced by a fingerprint feature extractor) **SHALL** be erased after an authentication transaction.

3.1.7.2. Multi-Factor Cryptographic Verifiers

The requirements for a multi-factor cryptographic verifier are identical to those for a single-factor cryptographic verifier, as described in Sec. 3.1.6.2. Some multi-factor authenticators include flags to indicate whether an activation factor was used. If such a flag is present and indicates that an activation factor was not used, the authentication

第二认证因素。根据所需身份验证的强度，认证密钥的存储方式可以是可被所验证的端点访问的，也可以是存储在单独的、直接连接的处理器或设备中。认证器输出高度依赖于所使用的特定密码协议，但通常是某种类型的签名消息。多因素密码认证器是“你拥有的东西”，并由代表“你知道的东西”或“你是什么”的激活因素激活。在AAL3中使用的多因素密码认证器**应**使用公钥密码学来保护认证秘密免受验证器泄露的影响。

如果密码学身份验证满足第3.2.5节中的额外要求，则它是抗钓鱼的。

3.1.7.1. 多因素加密认证器

多因素密码认证器封装一个或多个认证密钥，这些密钥**应**仅通过激活因素(即密码或生物特征)的呈现和验证才能访问。适用于AAL3的不可导出认证密钥**应**存储在受硬件保护的隔离执行环境中，或存储在具有受控接口的单独处理器中，该接口连接到用户端点的中央处理单元。可导出认证密钥(可用于AAL2或以下)**宜**存储在认证器可用的适当存储中(例如钥匙串存储)。如果可被所验证的端点访问，则认证密钥**应**通过使用访问控制来强力防止未经授权的泄露，这些访问控制将认证密钥的访问限制为仅需要访问的软件组件。

外部(非嵌入式)密码认证器**应**满足第3.2.11节中连接认证器的要求。每次身份验证事件**应**要求输入并验证本地激活因素。认证器激活秘密**应**满足第3.2.10节的要求。生物特征激活因素**应**满足第3.2.3节的要求，包括对连续身份验证失败次数的限制。激活秘密或生物特征样本以及从生物特征样本导出的任何生物特征数据(例如指纹图像和指纹特征提取器产生的特征位置)**应**在身份验证事务后擦除。

3.1.7.2. 多因素加密验证器

多因素加密验证器的要求与第3.1.6.2节中描述的单因素加密验证器的要求相同。一些多因素认证器包含标志以指示是否使用了激活因素。如果存在此类标志并指示未使用激活因素，则身份验证

SHALL be treated as single-factor. Otherwise, verification of the output from a multi-factor cryptographic authenticator indicates that the activation factor was used.

3.1.7.3. Usage With Subscriber-Controlled Wallets

A specific form of multi-factor cryptographic authentication is a subscriber-controlled wallet on the subscriber's device, as described in Sec. 5 of [SP800-63C]. After the claimant first unlocks the wallet using an activation factor, the authentication process uses a federation protocol, as detailed in [SP800-63C]. The assertion contents and presentation requirements of the federation protocol provide the security characteristics required of cryptographic authenticators. As such, subscriber-controlled wallets on the subscriber's device can be considered multi-factor authenticators through the activation factor and the presentation and validation of an assertion generated by the wallet.

> Cloud-hosted wallets are not considered cryptographic multi-factor authenticators because access is maintained through authentication over the internet rather than locally. All authentication information from hosted wallets is treated as an assertion, as addressed in Sec. 5 of [SP800-63C].

Access to the private key **SHALL** require an activation factor. Authenticator activation secrets **SHALL** meet the requirements of Sec. 3.2.10. Biometric activation factors **SHALL** meet the requirements of Sec. 3.2.3, including limits on the number of consecutive authentication failures. The password or biometric sample used for activation and any biometric data derived from the biometric sample **SHALL** be erased immediately after an authentication transaction.

Authentication processes using subscriber-controlled wallets **SHALL** be used with a federation process as detailed in Sec. 5 of [SP800-63C]. Signed audience-restricted assertions that are generated by subscriber-controlled wallets are considered phishing-resistant because they prevent an assertion presented to an impostor RP from being used by the legitimate one. Assertions that lack a valid signature from the wallet or an audience restriction **SHALL NOT** be considered phishing-resistant. Assertions **SHALL** also include sufficient information to determine the nature of the activation method used to activate the wallet.

3.1.7.4. Syncable Authenticators

Some cryptographic authenticators allow the subscriber to copy (i.e., clone) the authentication secret to additional devices, usually via a sync fabric. This eases the burden for subscribers who want to use additional devices to authenticate. Specific requirements for syncable authenticators and the sync fabric are given in Appendix B.

SHALL被视为单因素。否则，对多因素加密认证器输出的验证表明使用了激活因素。

3.1.7.3. 与用户控制钱包的使用

多因素密码认证的一种特定形式是订阅者设备上由订阅者控制的钱包，如[SP800-63C]第5节所述。在声称者首次使用激活因素解锁钱包后，身份验证过程使用联合身份协议，详见[SP800-63C]。联合身份协议的断言内容和呈现要求提供了密码认证器所需的安全特性。因此，订阅者设备上由订阅者控制的钱包可以通过激活因素以及钱包生成的断言的呈现和验证被视为多因素认证器。

> 云托管钱包不被视为加密多因素认证器，因为访问是通过互联网上的身份验证而非本地方式维护的。来自托管钱包的所有身份验证信息均被视为断言，如[SP800-63C]第5节所述。

访问私钥**应**要求激活因子。认证器激活密钥**应**满足第3.2.10节的要求。生物特征激活因子**应**满足第3.2.3节的要求，包括对连续身份验证失败次数的限制。用于激活的密码或生物特征样本以及从生物特征样本衍生的任何生物特征数据**应**在身份验证事务后立即擦除。

使用订阅者控制钱包的身份验证过程**应**与[SP800-63C]第5节中详述的联合身份过程一起使用。由订阅者控制钱包生成的签名受众限制断言被认为是抗钓鱼的，因为它们防止呈现给冒充RP的断言被合法RP使用。缺少钱包有效签名或受众限制的断言**应**不被视为抗钓鱼的。断言还应包括足够的信息以确定用于激活钱包的激活方法的性质。

3.1.7.4. 可同步认证器

一些加密认证器允许订阅者将身份验证秘密复制(即克隆)到其他设备，通常通过同步结构进行。这减轻了希望使用其他设备进行身份验证的订阅者的负担。可同步认证器和同步结构的具体要求见附录B。

3.2. General Authenticator Requirements

The following requirements apply to all types of authentication.

3.2.1. Physical Authenticators

CSPs **SHALL** provide subscriber instructions for appropriately protecting the authenticator against theft or loss. The CSP **SHALL** provide a mechanism to invalidate[1] the authenticator immediately upon notification from a subscriber that the authenticator's loss, theft, or compromise is suspected.

Possession and control of a physical authenticator are based on proof of possession of a secret associated with the authenticator. When an embedded secret (typically a certificate and associated private key) is in the endpoint, its "device identity" can be considered a physical authenticator. However, this requires a secure authentication protocol that is appropriate for the AAL being authenticated. Browser cookies do not satisfy this requirement except as short-term secrets for session maintenance (not authentication), as described in Sec. 5.1.1.

3.2.2. Rate Limiting (Throttling)

When required by the authenticator type descriptions in Sec. 3.1, the verifier **SHALL** implement controls to protect against *online guessing attacks*. Unless otherwise specified in the description of a given authenticator, the verifier **SHALL** limit consecutive failed authentication attempts using a specific authenticator on a single subscriber account to no more than 100 by disabling that authenticator. If more than one authenticator is involved with an excessive number of authentication attempts (e.g., single-factor cryptographic authenticator and centrally verified password), both authenticators **SHALL** be disabled. Authenticators that have been disabled **SHALL** be required to rebind to the subscriber account, as described in Sec. 4.1, to be usable in the future.

> The limit of 100 attempts is an upper bound, and agencies **MAY** impose lower limits. The limit of 100 was chosen to balance the likelihood of a correct guess (e.g., 100 attempts against a six-digit decimal OTP authenticator output) versus the potential need for account recovery when the limit is exceeded.

Additional techniques **MAY** be used to reduce the likelihood that an attacker will lock the legitimate claimant out due to rate limiting. These include:

- Requiring the claimant to complete a bot detection and mitigation challenge before attempting authentication

[1] Invalidation can take several forms, including the revocation of a *public-key infrastructure (PKI)*-based authenticator and removal from the subscriber account.

3.2. 通用认证器要求

以下要求适用于所有类型的认证。

3.2.1. 物理认证器

CSP**SHALL**向订阅者提供适当保护认证器免遭盗窃或丢失的说明。CSP**SHALL**提供一种机制，在收到订阅者怀疑认证器丢失、被盗或泄露的通知后立即使[1]认证器失效。

物理认证器的拥有和控制基于对与认证器关联的密钥的拥有证明。当嵌入式密钥(通常是证书和关联的私钥)位于端点中时，其"设备身份"可以被视为物理认证器。然而，这需要适用于所验证AAL的安全身份验证协议。浏览器cookie不满足此要求，除非作为会话维护(非身份验证)的短期密钥，如第5.1.1节所述。

3.2.2. 速率限制(节流)

当第3.1节中的认证器类型描述要求时，验证器**应**实施控制措施以防止在线猜测攻击。除非给定认证器的描述中另有规定，验证器**应**通过禁用该认证器，将单个订阅者账户上使用特定认证器的连续失败身份验证尝试限制为不超过100次。如果涉及多个认证器且身份验证尝试次数过多(例如，单因素加密认证器和集中验证密码)，两个认证器**应**被禁用。已禁用的认证器**应**要求重新绑定到订阅者账户，如第4.1节所述，以便将来使用。

> 100次尝试的限制是一个上限，机构**MAY**施加更低的限制。选择100这一限制是为了在正确猜测的可能性(例如，针对六位十进制OTP认证器输出的100次尝试)与超过限制时账户恢复的潜在需求之间取得平衡。

可以使用额外技术**MAY**来降低攻击者因速率限制而锁定合法声称者的可能性。这些包括：

- 要求声称者在尝试身份验证之前完成机器人检测和缓解挑战

1 失效可以采取多种形式，包括撤销基于公钥基础设施*(PKI)*的认证器并将其从订阅者账户中移除。

- Requiring the claimant to wait after a failed attempt for a period of time that increases as the subscriber account approaches its maximum allowance for consecutive failed attempts (e.g., 30 seconds up to an hour)
- Leveraging other risk-based or adaptive authentication techniques to identify claimant behaviors that fall within or outside of typical norms (e.g., the use of the claimant's IP address, geolocation, timing of request patterns, or browser metadata)

When the subscriber successfully authenticates, the verifier **SHOULD** disregard any previous failed attempts for the authenticators used in the successful authentication.

Following successful authentication at a given AAL, the verifier **SHOULD** reset the retry count of the authenticators that were used. If this is provided, the maximum AAL of the authenticator being reset **SHALL** not exceed the AAL of the session from which it is being reset. If the subscriber cannot authenticate at the required AAL, the account recovery procedures in Sec. 4.2 **SHALL** be used.

3.2.3. Use of Biometrics

Biometrics is the automated recognition of individuals based on their biological and behavioral characteristics, such as fingerprints, voice patterns, facial features, keystroke patterns, angle of holding a smart phone, screen pressure, typing speed, mouse movements, or gait. Such characteristics have multiple modalities that may differ in the extent to which they establish authentication intent, as described in Sec. 3.2.8.

Biometric comparisons are based on a measurement from the biometric sensor (e.g., camera, fingerprint reader). This measurement is subject to noise and presentation variations that require setting an acceptance threshold based on the differences between the measured biometric and the reference against which it is being compared. Due to these factors, there is some probability that a comparison will not result in a match, which is referred to as a false non-match rate (FNMR). Similarly, there is a probability that an impostor comparison will result in a match, referred to as a false match rate (FMR). A high-quality biometric system has both a very low FMR and FNMR. The chosen threshold usually emphasizes a low FMR to maximize security since false non-matches can often be mitigated by repeating the measurement or using an alternative authentication method.

For a variety of reasons, this document supports only a limited use of biometrics for authentication. These reasons include:

- The biometric FMR does not provide sufficient confidence in the subscriber's authentication by itself because it does not account for active impersonation attacks.
- Biometric comparison is probabilistic, whereas the other authentication factors are deterministic.

- 要求声称者在失败尝试后等待一段时间，该时间随着订阅者账户接近其连续失败尝试的最大允许次数而增加(例如，从30秒到一小时)
- 利用其他基于风险或自适应身份验证技术来识别声称者行为是否处于典型规范之内或之外(例如，使用声称者的IP地址、地理位置、请求模式的时间或浏览器元数据)

当订阅者成功通过身份验证时，验证器**SHOULD**忽略成功身份验证中所使用认证器的任何先前失败尝试。

在给定AAL级别成功通过身份验证后，验证器**SHOULD**重置所使用认证器的重试计数。如果提供了此功能，被重置的认证器的最大AAL**SHALL**不得超过执行重置的会话的AAL。如果订阅者无法在所需AAL级别通过身份验证，SHALL使用第4.2节**中的账户恢复程序**。

3.2.3. 生物特征的使用

生物特征是基于个体的生物学和行为特征(如指纹、声音模式、面部特征、击键模式、握持智能手机的角度、屏幕压力、打字速度、鼠标移动或步态)对个体进行的自动识别。此类特征具有多种模态，其在建立身份验证意图的程度方面可能有所不同，如第3.2.8节所述。

生物特征比对基于生物特征传感器(例如摄像头、指纹读取器)的测量值。该测量值会受到噪声和呈现变化的影响，需要根据所测量的生物特征与用于比对的参考值之间的差异来设定接受阈值。由于这些因素，比对存在一定概率不会产生匹配，这被称为错误未匹配率(FNMR)。同样，冒名者比对存在一定概率会产生匹配，这被称为错误匹配率(FMR)。高质量的生物特征系统具有非常低的 FMR 和 FNMR。所选择的阈值通常强调较低的 FMR 以最大化安全性，因为错误未匹配通常可以通过重复测量或使用替代身份验证方法来缓解。

出于多种原因，本文档仅支持有限度地将生物特征用于身份验证。这些原因包括：

- 生物特征FMR本身不能为订阅者的身份验证提供足够的置信度，因为它没有考虑主动冒充攻击。
- 生物特征比较是概率性的，而其他身份验证因素是确定性的。

- Biometric template protection schemes provide a method for revoking biometric characteristics that are comparable to other authentication factors (e.g., PKI certificates, passwords). However, the availability of such solutions is limited.
- Biometric characteristics do not constitute secrets. They can often be obtained online or otherwise without consent. A facial image can be obtained by taking a picture; latent fingerprints can be obtained from objects someone touches; and iris patterns can be captured with high-resolution cameras. While presentation attack detection (PAD) technologies can mitigate the risks of these types of attacks, additional trust in the sensor or biometric processing is required to ensure that PAD is operating in accordance with the needs of the CSP and the subscriber.
- The use of biometric characteristics, especially when stored for central verification, introduces new privacy concerns, which are discussed further in Sec. 7.

Therefore, the limited use of biometrics for authentication is supported with specific requirements and guidelines.

Biometrics **SHALL** only be used as part of multi-factor authentication with a physical authenticator (i.e., "something you have"). The biometric characteristic **SHALL** be presented and compared for each authentication operation. An alternative non-biometric authentication option **SHALL** always be provided to the subscriber. Biometric data **SHALL** be treated and secured as sensitive personal information.

3.2.3.1. Biometric Accuracy

The biometric system **SHALL** operate with an FMR [ISO/IEC2382-37] of one in 10000 or better for all demographic groups. Demographic categories to be considered **SHALL** include sex and skin tone when these factors affect biometric performance. This FMR **SHALL** be achieved under the conditions of a conformant attack (i.e., zero-effort impostor attempt), as defined in [ISO/IEC30107-1]. The biometric system **SHOULD** demonstrate a false non-match rate (FNMR) of less than 5 %. Biometric performance **SHALL** be tested in accordance with [ISO/IEC19795-1]. The biometric system **SHALL** be configured with a fixed threshold; it is not feasible to change the threshold for each demographic.

3.2.3.2. Presentation Attack Detection

The biometric system **SHOULD** implement PAD for iris and fingerprint modalities and **SHALL** implement PAD for facial recognition. Biometric comparison based on voice **SHALL NOT** be used. Testing the biometric system for deployment **SHOULD** demonstrate an impostor attack presentation accept rate (IAPAR) of less than 0.07. Presentation attack resistance **SHOULD** be tested in accordance with Clause 13 of [ISO/IEC30107-3] following security evaluation methodologies in [ISO/IEC19792] or [ISO/IEC19989-1] and [ISO/IEC19989-3]. The PAD decision **MAY** be made either locally on the claimant's device or by a central verifier.

- 生物特征模板保护方案提供了一种撤销生物特征的方法，可与其他身份验证因素(例如，PKI证书、密码)相媲美。然而，此类解决方案的可用性有限。
- 生物特征不构成秘密。它们通常可以在线或以其他方式未经同意获取。面部图像可以通过拍照获取；潜在指纹可以从某人接触过的物体上获取；虹膜图案可以用高分辨率相机捕获。虽然呈现攻击检测(PAD)技术可以缓解这些类型攻击的风险，但需要对传感器或生物特征处理有额外的信任，以确保PAD按照CSP和订阅者的需求运行。
- 生物特征的使用，特别是在存储用于集中验证时，引入了新的隐私问题，这些问题在第7节中进一步讨论。

因此，生物特征在身份验证中的有限使用受到具体要求和指南的支持。

生物特征**SHALL**仅作为使用物理认证器(即"你拥有的东西")的多因素身份验证的一部分使用。生物特征**SHALL**在每次身份验证操作中呈现并进行比较。**SHALL**始终向订阅者提供替代的非生物特征身份验证选项。生物特征数据**SHALL**作为敏感个人信息进行处理和保护。

3.2.3.1. 生物特征准确性

生物特征系统**应**在所有人口群体中以万分之一或更好的FMR[ISO/IEC2382-37]运行。当性别和肤色影响生物特征性能时，应考虑的人口统计类别**应**包括这些因素。该FMR**应**在符合性攻击(即零努力冒充尝试)的条件下实现，如[ISO/IEC30107-1]所定义。生物特征系统**宜**表现出低于5%的假不匹配率(FNMR)。生物特征性能**应**按照[ISO/IEC19795-1]进行测试。生物特征系统**应**配置固定阈值；为每个人口群体更改阈值是不可行的。

3.2.3.2. 呈现攻击检测

生物特征系统**宜**为虹膜和指纹模态实施PAD，并且**应**为人脸识别实施PAD。基于语音的生物特征比较**不得**使用。部署时测试生物特征系统**宜**证明冒充攻击呈现接受率(IAPAR)低于0.07。呈现攻击抵抗力**宜**按照[ISO/IEC30107-3]第13条进行测试，遵循[ISO/IEC19792]或[ISO/IEC19989-1]和[ISO/IEC19989-3]中的安全评估方法。PAD决策**可**在声称者设备上本地做出，或由中央验证器做出。

3.2.3.3. Injection Attack Detection

The biometric system **SHALL** allow no more than five consecutive failed authentication attempts or 10 consecutive failed attempts if PAD is implemented and meets the above requirements. Once that limit has been reached, the biometric authenticator **SHALL** impose a delay of at least 30 seconds before each subsequent attempt with an overall limit of no more than 50 consecutive failed authentication attempts or 100 if PAD is implemented due to the mitigation of presentation attacks. Once the overall limit is reached, the biometric system **SHALL** disable biometric authentication and offer another factor (e.g., a different biometric modality or an activation secret if it is not a required factor) if such an alternative method is already available. These limits are upper bounds, and agencies **MAY** make risk-based decisions to impose lower limits.

The verifier **SHOULD** determine the performance and integrity of the sensor and its associated endpoint. This increases the likelihood of detecting injection attacks due to compromised endpoints, sensor emulators, and similar threats. Acceptable methods for making this determination include:

- Use of a known sensor, as determined by sensor authentication
- First- or third-party testing against biometric performance standards
- Runtime interrogation of signed metadata (e.g., attestation), as described in Sec. 3.2.4

Biometric comparison can be performed locally on a device being used by the claimant or at a central verifier. Since the potential for attacks on a larger scale is greater at central verifiers, comparison **SHOULD** be performed locally.

The presentation of a biometric factor for authenticator activation **SHALL** be a separate operation from unlocking the host device (e.g., smartphone). However, the same activation factor used to unlock the host device **MAY** be used in the authentication operation. Agencies **MAY** lower this requirement for authenticators that are managed by or on behalf of the CSP (e.g., via mobile device management) and constrained to have short agency-determined inactivity timeouts and biometric systems that meet the above requirements.

If the comparison is performed centrally:

- The sensor or endpoint **SHALL** be authenticated before capturing the biometric sample from the claimant. The verifier **MAY** limit the use of the centrally stored biometric template to particular sensors or sensor classes (e.g., sensor manufacturers or models).
- Appropriate controls (e.g., encryption and access controls) for sensitive personal information **SHALL** be implemented.

3.2.3.3. 注入攻击检测

生物特征系统**应**允许不超过五次连续失败的身份验证尝试，或者如果实施了PAD并满足上述要求，则允许不超过10次连续失败尝试。一旦达到该限制，生物特征认证器**应**在每次后续尝试前施加至少30秒的延迟，总体限制为不超过50次连续失败的身份验证尝试，或者如果实施了PAD，由于缓解了呈现攻击，则为100次。一旦达到总体限制，生物特征系统**应**禁用生物特征身份验证并提供另一种因素(例如，不同的生物特征模态或激活秘密，如果它不是必需因素)，如果这种替代方法已经可用。这些限制是上限，机构**可**做出基于风险的决定以施加更低限制。

验证器**SHOULD**确定传感器及其相关端点的性能和完整性。这增加了检测因端点被入侵、传感器模拟器和类似威胁而导致的注入攻击的可能性。进行此确定的可接受方法包括：

- 使用已知传感器，由传感器认证确定
- 依据生物特征性能标准进行的第一方或第三方测试
- 对签名元数据(例如，认证声明)的运行时询问，如所述于Sec.3.2.4

生物特征比较可以在声称者使用的设备上本地执行，也可以在中央验证器处执行。由于中央验证器处大规模攻击的可能性更大，比较**SHOULD**在本地执行。

用于认证器激活的生物特征因素的呈现**应**与解锁主机设备(例如，智能手机)是分开的操作。然而，用于解锁主机设备的相同激活因素**可**用于身份验证操作。机构**可**对由CSP管理或代表CSP管理的认证器(例如，通过移动设备管理)降低此要求，并限制为具有机构确定的短不活动超时和满足上述要求的生物特征系统。

如果比较是集中进行的：

- 传感器或端点**SHALL**在从声称者采集生物特征样本之前进行身份验证。验证器**MAY**将中央存储的生物特征模板的使用限制为特定传感器或传感器类别(例如，传感器制造商或型号)。
- 敏感个人信息**SHALL**实施适当的控制(例如，加密和访问控制)。

- An authenticated protected channel between the sensor (or an endpoint containing a sensor that resists sensor replacement) and the verifier **SHALL** be established. All transmission of biometric information **SHALL** be conducted over that authenticated protected channel.

3.2.3.4. Use of Biometric Samples

Biometric samples collected in the authentication process **MAY** be used locally within the authenticator or verifier performing the biometric comparison to update the templates for the purpose of compensating for changes in subscriber characteristics or — with explicit subscriber consent — other research purposes. The biometric samples and any other biometric data derived from them **SHALL** be erased immediately after any adaptation or research data has been derived. A limit on the allowable time for adaptation **SHALL** be established and enforced by the authenticator or the CSP.

3.2.4. Attestation

The CSP needs to have a reliable basis for evaluating the characteristics of the authenticator, such as the inclusion of a signed attestation. An attestation is information conveyed to the CSP, generally when an authenticator is bound, regarding that connected authenticator or the endpoint involved in an authentication operation. Information conveyed by attestation **MAY** include but is not limited to:

- The provenance (e.g., manufacturer or supplier certification), health, and integrity of the authenticator and endpoint
- Security features of the authenticator
- Security and performance characteristics of biometric sensors
- Sensor modality
- Properties of the authentication key

Attestations **SHALL** be signed using a digital signature that provides at least the minimum security strength specified in the latest revision of [SP800-131A] (i.e., 112 bits as of the date of this publication).

Verifiers in federal enterprise systems[2] **SHOULD** use attestation features to verify the capabilities and sources of authenticators. In other applications, attestation information **MAY** be used as part of a verifier's risk-based authentication decisions.

[2] Federal enterprise systems include those considered in scope for PIV guidance, such as government contractors, government employees, and mission partners. It does not include government-to-consumer or public-facing use cases.

- 传感器(或包含抗传感器更换传感器的端点)与验证器之间**SHALL**建立经过身份验证的受保护信道。生物特征信息的所有传输**SHALL**通过该经过身份验证的受保护信道进行。

3.2.3.4. 生物特征样本的使用

在身份验证过程中收集的生物特征样本**可以**在本地由执行生物特征比对的认证器或验证器使用，以更新模板，目的是补偿订阅者特征的变化，或在订阅者明确同意的情况下用于其他研究目的。生物特征样本以及由此衍生的任何其他生物特征数据**应**在得出任何适配或研究数据后立即擦除。认证器或CSP**应**建立并执行允许适配时间的限制。

3.2.4. 证明

CSP 需要具备可靠依据来评估认证器的特性，例如包含签名断言。断言是在认证器绑定时通常向 CSP 传达的关于该连接的认证器或身份验证操作中所涉及端点的信息。断言传达的信息**可能**包括但不限于：

- 认证器和端点的来源(例如，制造商或供应商认证)、健康状况和完整性
- 认证器的安全特性
- 生物识别传感器的安全与性能特征
- 传感器模态
- 认证密钥的属性

断言**应**使用数字签名进行签名，该签名至少提供[SP800-131A]最新修订版中规定的最低安全强度(即截至本出版物发布之日为 112 位)。

联邦企业系统中的验证器[2]**宜**使用断言功能来验证认证器的能力和来源。在其他应用中，断言信息**可能**作为验证器基于风险的身份验证决策的一部分使用。

2 联邦企业系统包括被视为 PIV 指南范围内的系统，例如政府承包商、政府雇员和任务合作伙伴。不包括政府对消费者或面向公众的用例。

3.2.5. Phishing Resistance

Phishing attacks, previously referred to in SP 800-63B as “verifier impersonation,” are attempts by fraudulent verifiers and RPs to fool an unwary claimant into presenting an authenticator to an impostor. In some prior versions of SP 800-63, protocols that are resistant to phishing attacks were also referred to as “strongly MitM-resistant.”

In this document, phishing resistance is the ability of the authentication protocol to prevent the disclosure of authentication secrets and valid authenticator outputs to an impostor verifier (i.e., an attacker fraudulently posing as the verifier) without relying on the vigilance of the claimant. How the claimant is directed to the impostor verifier is not relevant. For example, regardless of whether the claimant was directed there via search engine optimization or prompted by email, it is considered to be a phishing attack.

Approved cryptographic algorithms **SHALL** be used to establish phishing resistance where required. Keys used for this purpose **SHALL** provide at least the minimum security strength specified in the latest revision of [SP800-131A] (i.e., 112 bits as of the date of this publication).

Phishing resistance requires single- or multi-factor cryptographic authentication. Authenticators that involve the manual entry of an authenticator output (e.g., out-of-band and OTP authenticators) **SHALL NOT** be considered phishing-resistant because the manual entry does not bind the authenticator output to the specific session being authenticated. For example, an impostor verifier could relay an authenticator output to the verifier and successfully authenticate.

Two methods of phishing resistance are recognized: channel binding and verifier name binding. Channel binding is considered more secure than verifier name binding because it is not vulnerable to the misissuance or misappropriation of verifier certificates, but both methods satisfy the requirements for phishing resistance.

3.2.5.1. Channel Binding

An authentication protocol with channel binding **SHALL** establish an authenticated protected channel with the verifier. The protocol **SHALL** then strongly and irreversibly bind a channel identifier negotiated in establishing the authenticated protected channel to the authenticator output (e.g., by signing the two values together using a private key controlled by the claimant for which the public key is known to the verifier). The verifier **SHALL** validate the signature or other information used to prove phishing resistance. This prevents an impostor verifier — even one that has obtained a certificate that represents the actual verifier — from successfully relaying that authentication on a different authenticated protected channel.

An example of a phishing-resistant authentication protocol that uses channel binding is client-authenticated TLS [RFC8446] in which the client signs the authenticator output along with earlier messages from the protocol that are unique to the particular TLS

3.2.5. 抗钓鱼

钓鱼攻击在 SP 800-63B 中以前称为“验证器冒充”，是欺诈性验证器和 RP 试图欺骗不慎的声称者将认证器出示给冒充者的行为。在 SP 800-63 的某些先前版本中，抗钓鱼攻击的协议也称为“强抗 MitM”。

在本文件中，抗钓鱼是指身份验证协议在不依赖声称者警惕性的情况下，防止身份验证秘密和有效认证器输出泄露给冒名验证器(即欺诈性地冒充验证器的攻击者)的能力。声称者如何被引导至冒名验证器并不相关。例如，无论声称者是通过搜索引擎优化被引导到那里，还是通过电子邮件被提示，都被视为钓鱼攻击。

在需要抗钓鱼时，**应**使用经批准的密码算法。用于此目的的密钥**应**至少提供[SP800-131A]最新修订版中规定的最低安全强度(即截至本出版物发布之日为 112 位)。

抗钓鱼需要单因素或多因素密码身份验证。涉及手动输入认证器输出的认证器(例如，带外和 OTP 认证器)**不得**被视为抗钓鱼的，因为手动输入不会将认证器输出绑定到正在身份验证的特定会话。例如，冒充者验证器可以将认证器输出中继给验证器并成功通过身份验证。

认可两种抗钓鱼方法：信道绑定和验证器名称绑定。信道绑定被认为比验证器名称绑定更安全，因为它不易受到验证器证书的错误签发或盗用，但两种方法都满足抗钓鱼的要求。

3.2.5.1. 通道绑定

具有信道绑定的身份验证协议**应**与验证器建立经过身份验证的受保护信道。然后，该协议**应**将建立经过身份验证的受保护信道时协商的信道标识符强有力地且不可逆地绑定到认证器输出(例如，通过使用由声称者控制、且验证器已知其公钥的私钥将这两个值一起签名)。验证器**应**验证用于证明抗钓鱼的签名或其他信息。这可以防止冒名验证器--即使是已获得代表实际验证器的证书的冒名验证器--在不同的经过身份验证的受保护信道上成功转发该身份验证。

使用信道绑定的抗钓鱼身份验证协议的一个示例是客户端认证 TLS [RFC8446]，其中客户端对认证器输出以及协议中早先的、特定于正在协商的特定 TLS

connection being negotiated. Personal identity verification (PIV) and common access card (CAC) cards, which use client-authenticated TLS, provide phishing resistance through channel binding.

3.2.5.2. Verifier Name Binding

An authentication protocol with verifier name binding **SHALL** establish an authenticated protected channel with the verifier. The protocol **SHALL** then generate an authenticator output that is cryptographically bound to a verifier identifier that is authenticated as part of the protocol. In the case of DNS identifiers, the verifier identifier **SHALL** be either the authenticated hostname of the verifier or a parent domain that is at least one level below the public suffix [PSL] associated with that hostname. The binding **MAY** be established by choosing an associated authenticator secret, deriving an authenticator secret using the verifier identifier, cryptographically signing the authenticator output with the verifier identifier, or using similar cryptographically secure means.

WebAuthn [WebAuthn], which is used by authenticators that implement the Fast Identity Online 2 (FIDO2) specifications [FIDO2], is an example of a standard that provides phishing resistance through verifier name binding by choosing an authenticator secret based on the authenticated domain name of the verifier.

3.2.6. Verifier-CSP or IdP Communications

If the verifier and CSP or IdP are separate entities (as shown by the dotted line in Fig. 3 of [SP800-63]), communications between the verifier and CSP or IdP **SHALL** occur through a mutually authenticated protected channel (e.g., a client-authenticated TLS connection) using approved cryptography.

3.2.7. Replay Resistance

An authentication process resists *replay attacks* if it is impractical to achieve a successful authentication by recording and replaying a previous authentication message. Replay resistance is in addition to the replay-resistant nature of authenticated protected channel protocols since the output could be stolen before entry into the protected channel. Protocols that use nonces or challenges to prove the “freshness” of the transaction are resistant to replay attacks since the verifier will easily detect when old protocol messages are replayed because they will not contain the appropriate nonces or timeliness data. Examples of replay-resistant authenticators include OTP authenticators, cryptographic authenticators, and look-up secrets.

In contrast, passwords are not considered replay-resistant because the same authenticator output (i.e., the password itself) is provided for each authentication.

连接的消息进行签名。使用客户端认证 TLS 的个人身份验证(PIV)和通用访问卡(CAC)卡通过信道绑定提供抗钓鱼。

3.2.5.2. 验证方名称绑定

具有验证器名称绑定的身份验证协议**应**与验证器建立经过身份验证的受保护信道。然后，该协议**应**生成认证器输出，并以密码学方式将其绑定到作为协议一部分经过身份验证的验证器标识符。对于DNS标识符，验证器标识符**应**是验证器经过身份验证的主机名，或是与该主机名相关联的公共后缀[PSL]之下至少一级的父域。绑定**可以**通过选择关联的认证器秘密、使用验证器标识符派生认证器秘密、使用验证器标识符对认证器输出进行密码学签名，或使用类似的密码学安全手段来建立。

WebAuthn [WebAuthn]由实现快速身份在线 2(FIDO2)规范[FIDO2]的认证器使用，是通过基于验证器的已认证域名选择认证器秘密来提供验证器名称绑定抗钓鱼的标准示例。

3.2.6. 验证方与CSP或IdP之间的通信

如果验证器和 CSP 或 IdP 是独立实体(如[SP800-63]的图 3 中虚线所示)，验证器与 CSP 或 IdP 之间的通信**应**通过使用经批准密码学的相互认证保护信道(例如，客户端认证 TLS 连接)进行。

3.2.7. 重放抵抗

如果通过记录并重放先前的身份验证消息来成功实现身份验证是不可行的，则身份验证过程可抵御重放攻击。重放抵御是在经过身份验证的受保护信道协议本身具有抗重放性质之外的额外要求，因为输出可能在进入受保护信道之前被窃取。使用随机数或挑战来证明事务“新鲜性”的协议可抵御重放攻击，因为验证器很容易检测到旧协议消息何时被重放，因为这些消息不会包含适当的随机数或时效数据。抗重放认证器的示例包括OTP认证器、密码学认证器和查询性秘密。

相比之下，密码不被视为抗重放的，因为每次身份验证都提供相同的认证器输出(即密码本身)。

3.2.8. Authentication Intent

An authentication process demonstrates intent if it requires the claimant to respond explicitly to each authentication or reauthentication request. The goal of authentication intent is to make it more difficult for authenticators (e.g., multi-factor cryptographic authenticators) to be used without the claimant's knowledge, such as by malware on the endpoint. The authenticator itself **SHALL** establish authentication intent. Multi-factor authenticators **MAY** establish intent by reentry of the activation factor for the authenticator.

Authentication intent **MAY** be established in several ways. Authentication processes that require the claimant's intervention can be used to prove intent (e.g., a claimant entering an authenticator output from an OTP authenticator). Cryptographic authenticators that require claimant action for each authentication or reauthentication operation can also be used to establish intent (e.g., by pushing a button or reinsertion).

The presentation of biometric characteristics does not always establish authentication intent. For example, using a front-facing camera on a mobile phone to capture a face biometric does not necessarily constitute intent, as it can be reasonably expected to capture a face image while the device is used for other non-authentication purposes. In these scenarios, an explicit mechanism (e.g., tapping a software or physical button) **SHALL** be provided to establish authentication intent.

3.2.9. Restricted Authenticators

As threats evolve, authenticators' ability to resist attacks typically degrades. Conversely, the performance of some authenticators may improve, such as when changes to their underlying standards increase their ability to resist particular attacks.

To account for these changes in authenticator performance, NIST places additional restrictions on authenticator types or specific classes or instantiations of an authenticator type. Although they represent a less secure approach to multi-factor authentication, *restricted authenticators* remain necessary for some government-to-public applications. At the time of publication of these guidelines, there is one restricted authenticator: the use of the PSTN for out-of-band authentication, as described in Sec. 3.1.3.3.

The acceptance of a restricted authenticator requires the implementing organization to assess, understand, and accept the risks associated with that authenticator and acknowledge that risks will likely increase over time. It is the RP's responsibility to determine the level of acceptable risk for their systems and associated data, define any methods for mitigating excessive risks, and communicate those determinations to the verifier. If the RP determines that the risk to any party is unacceptable, the restricted authenticator **SHALL NOT** be used, and an alternative authenticator type **SHALL** be used.

3.2.8. 认证意图

如果身份验证过程要求声称者明确响应每个身份验证或重新身份验证请求，则该过程体现了意图。身份验证意图的目标是使认证器(例如，多因素加密认证器)更难以在声称者不知情的情况下被使用，例如通过端点上的恶意软件。认证器本身**SHALL**建立身份验证意图。多因素认证器**MAY**通过重新输入认证器的激活因素来建立意图。

身份验证意图**可能**通过多种方式建立。需要声称者干预的身份验证过程可用于证明意图(例如，声称者从 OTP 认证器输入认证器输出)。需要声称者对每次身份验证或重新身份验证操作采取行动的密码认证器也可用于建立意图(例如，通过按下按钮或重新插入)。

生物特征的呈现并不总是建立身份验证意图。例如，使用手机上的前置摄像头捕获面部生物特征不一定构成意图，因为在设备用于其他非身份验证目的时，可以合理预期会捕获面部图像。在这些场景中，**应**提供显式机制(例如，点击软件或物理按钮)来建立身份验证意图。

3.2.9 受限认证器

随着威胁的演变，认证器抵御攻击的能力通常会下降。相反，某些认证器的性能可能会提高，例如当其底层标准的变化增加了其抵御特定攻击的能力时。

为了应对认证器性能的这些变化，NIST对认证器类型或认证器类型的特定类别或实例施加了额外限制。尽管受限认证器代表了一种安全性较低的多因素身份验证方法，但受限认证器对于某些政府对公众的应用仍然是必要的。在本指南发布时，有一种受限认证器：使用PSTN进行带外身份验证，如第3.1.3.3节所述。

接受受限认证器要求实施组织评估、理解并接受与该认证器相关的风险，并承认风险可能会随着时间的推移而增加。RP有责任确定其系统及相关数据的可接受风险水平，定义缓解过度风险的任何方法，并将这些决定传达给验证器。如果RP确定对任何一方的风险不可接受，则**SHALL NOT**使用受限认证器，并且SHALL使用替代认证器类型。

Furthermore, the risk of an authentication error is typically borne by multiple parties, including the implementing organization, organizations that rely on the authentication decision, and the subscriber. Because the subscriber may be exposed to additional risks when an organization accepts a restricted authenticator and the subscriber may have a limited understanding of and ability to control those risks, the CSP **SHALL** do all of the following:

1. Offer subscribers at least one alternative authenticator that is not restricted and can be used to authenticate at the required AAL
2. Provide subscribers with meaningful notice regarding the restricted authenticator's security risks and the availability of unrestricted alternatives
3. Address any additional risks to subscribers and RPs in its risk assessment
4. Develop a migration plan for the possibility that the restricted authenticator will not be acceptable in the future and include this migration plan in its Digital Identity Acceptance Statement (see Sec. 3.4.4 of [SP800-63])

3.2.10. Activation Secrets

A password used locally as an activation factor for a multi-factor authenticator is referred to as an *activation secret*. An activation secret is used to obtain access to a stored authentication key. In all cases, the activation secret **SHALL** remain within the authenticator and its associated user endpoint.

Authenticators that use activation secrets **SHALL** require the secrets to be at least four characters in length and **SHOULD** require the secrets to be at least six characters in length. Activation secrets **MAY** be entirely numeric (i.e., a PIN). Otherwise, all printing ASCII [RFC20] characters, the space character, and Unicode [ISO/ISC 10646] characters **SHOULD** be permitted in activation secrets. The authenticator or its management tools **SHOULD** implement a blocklist to discourage subscribers from selecting commonly used activation secrets (e.g., 123456).

The authenticator or verifier **SHALL** implement a retry-limiting mechanism that limits the number of consecutive failed activation attempts using the authenticator to no more than 10. If an incorrect activation secret entry causes the authenticator to provide an invalid output to the central verifier, the verifier **MAY** implement this retry-limiting mechanism. Otherwise, retry limiting **SHALL** be implemented in the authenticator. Once the limit of attempts is reached, the authenticator **SHALL** be disabled, and a different authenticator **SHALL** be required for authentication.

For authenticators that are usable at AAL3, verification of activation secrets **SHALL** be performed in a hardware-protected environment (e.g., a secure element, TPM, or TEE). At AAL2, if a hardware-protected environment is not used, the authenticator **SHALL** use the activation secret to derive a key used to decrypt the authentication key.

此外，身份验证错误的风险通常由多方承担，包括实施组织、依赖身份验证决策的组织以及订阅者。由于当组织接受受限认证器时，订阅者可能面临额外风险，且订阅者对这些风险的理解和控制能力可能有限，因此CSP **SHALL**执行以下所有操作：

1. 向订阅者提供至少一个不受限的替代认证器，可用于在所需AAL级别进行身份验证
2. 向订阅者提供关于受限认证器安全风险及不受限替代方案可用性的有意义通知
3. 在其风险评估中处理用户和 RP 面临的任何额外风险
4. 制定迁移计划以应对受限认证器未来可能不被接受的情况，并将该迁移计划纳入其数字身份接受声明(参见[SP800-63]第3.4.4节)

3.2.10. 激活密钥

在本地用作多因素认证器激活因素的密码称为激活密钥。激活密钥用于获取对存储的认证密钥的访问权限。在所有情况下，激活密钥**SHALL**保留在认证器及其关联的用户终端内。

使用激活密钥的认证器**SHALL**要求密钥长度至少为四个字符，且**SHOULD**要求密钥长度至少为六个字符。激活密钥**MAY**完全为数字(即PIN)。否则，所有可打印ASCII[RFC20]字符、空格字符以及Unicode[ISO/ISC 10646]字符**SHOULD**允许用于激活密钥。认证器或其管理工具**SHOULD**实施阻止列表，以阻止订阅者选择常用的激活密钥(例如123456)。

认证器或验证器**SHALL**实施重试限制机制，将使用该认证器的连续失败激活尝试次数限制在不超过10次。如果不正确的激活密钥输入导致认证器向中央验证器提供无效输出，验证器**MAY**实施此重试限制机制。否则，重试限制**SHALL**在认证器中实施。一旦达到尝试次数限制，认证器**SHALL**被禁用，并且**SHALL**需要不同的认证器进行身份验证。

对于可在AAL3级别使用的认证器，激活密钥的验证**SHALL**在硬件保护环境中执行(例如，安全元件、TPM或TEE)。在AAL2级别，如果未使用硬件保护环境，认证器**SHALL**使用激活密钥派生用于解密认证密钥的密钥。

Submitting the activation factor **SHALL** be a separate operation from unlocking the host device (e.g., smartphone). However, the same activation factor used to unlock the host device **MAY** be used in the authentication operation. Agencies **MAY** relax this requirement for authenticators that are managed by or on behalf of the CSP (e.g., via mobile device management), are constrained to have short agency-determined inactivity timeouts, and use device activation factors that meet the corresponding requirements in this section.

3.2.11. Connected Authenticators

Cryptographic authenticators require a trustworthy connection between the authenticator and the endpoint being authenticated that provides resistance to eavesdropping, injection, and relay attacks. This connection **SHALL** be made using a wired connection (e.g., USB or direct connection with a smartcard), a wireless technology, or a hybrid of those technologies, including network connections.

Approved cryptography **SHALL** be used for all cases in which cryptographic operations are required. All communication of authentication data between authenticators and endpoints **SHALL** occur directly between those devices or through an authenticated protected channel between the authenticator and endpoint.

3.2.11.1. Wired Connections

Wired connections, including those with embedded authenticators, **MAY** be assumed to be trustworthy because their attack surface is minimal. Claimants **SHOULD** be advised to use trusted hardware (e.g., cables, adapters) to ensure that they have not been compromised.

3.2.11.2. Wireless Connections

Wireless authenticator connections are potentially vulnerable to threats, including eavesdropping, injection, and relay attacks. Wireless connections include technologies that function in the absence of a physical connection, such as radio frequency (e.g., Bluetooth and NFC), optical, and acoustic technologies.

The potential for such attacks on wireless connections depends on the technology's effective range. To minimize the attack surface for threats to the authenticator-endpoint connection, the authentication process **SHALL** require physical proximity between the authenticator and endpoint by establishing a wireless connection with a range of no more than 240 meters.[3]

Wireless connections **SHALL** establish a key for encrypted communication between the authenticator and endpoint in one of the following ways:

[3]The limit of 240 meters was chosen based on the maximum expected range of a Bluetooth connection.

提交激活因子**SHALL**是与解锁主机设备(例如智能手机)分开的操作。但是，用于解锁主机设备的相同激活因子**MAY**可用于身份验证操作。机构**MAY**对由CSP管理或代表CSP管理的认证器(例如通过移动设备管理)、被限制为具有机构确定的短不活动超时、并使用符合本节相应要求的设备激活因子的认证器放宽此要求。

3.2.11. 连接的认证器

加密认证器要求认证器与被认证端点之间建立可信连接，以提供对窃听、注入和中继攻击的抵抗能力。该连接**SHALL**通过有线连接(例如，USB或与智能卡的直接连接)、无线技术或这些技术的混合方式(包括网络连接)建立。

在所有需要加密操作的情况下，**SHALL**使用经批准的密码学技术。认证器与端点之间所有身份验证数据的通信**SHALL**直接在这些设备之间进行，或通过认证器与端点之间的经认证的保护信道进行。

3.2.11.1. 有线连接

有线连接(包括具有嵌入式认证器的连接)**MAY**可被假定为可信的，因为其攻击面极小。应建议声称者**SHOULD**使用可信硬件(例如，线缆、适配器)以确保其未被攻破。

3.2.11.2. 无线连接

无线认证器连接可能容易受到威胁，包括窃听、注入和中继攻击。无线连接包括在无物理连接情况下工作的技术，如射频(例如，蓝牙和NFC)、光学和声学技术。

对无线连接进行此类攻击的可能性取决于该技术的有效范围。为最小化认证器-端点连接威胁的攻击面，身份验证过程**SHALL**要求认证器与端点之间通过建立范围不超过240米的无线连接来实现物理接近。[3]

无线连接**SHALL**通过以下方式之一建立用于认证器与端点之间加密通信的密钥：

3 240米的限制是基于蓝牙连接的最大预期范围选定的。

1. Through a temporary wired connection between the devices.
2. Through an association process that is similar to a pairing process but does not require a persistent relationship between devices to establish a key for encrypted communication between the authenticator and endpoint. The association process **SHALL** employ a pairing code[4] or other shared secret between the devices. Either the authenticator or endpoint **SHALL** have a pairing code that **MAY** be printed on the device. The pairing code **SHALL** be at least six decimal digits (or equivalent) in length. It **SHALL** be conveyed between the devices by manual entry or using a QR code or similar representation that is optically communicated.

When using a wireless technology with an effective range of less than 1 meter (e.g., NFC), any activation secret transmitted from the endpoint to the authenticator **SHALL** be encrypted using a key that is established between the devices. An authenticated connection **SHOULD** be used. A pairing code **SHALL** be used if the authenticator is configured to require authenticated pairing.

> Encrypting only the activation secret and not the entire authentication transaction may expose sensitive information (e.g., the identity of the RP), although this would require the attacker to be very close to the subscriber. Special care should be taken with authenticators that contain personal information but do not require authenticated pairing. Encryption **SHOULD** be used to protect that information against eavesdropping attacks.

Network connections and wireless technologies with an effective range of 1 meter or more (e.g., Bluetooth Low Energy [BLE]) **SHALL** use an authenticated protected channel between the authenticator and endpoint. The entire authentication transaction **SHALL** be encrypted.

The key established by the association process may be either temporary (i.e., valid for a limited number of transactions or time-limited) or persistent. A mechanism for endpoints to remove persistent keys **SHALL** be provided.

An example of a wireless connection with an authenticator is the virtual contact interface specified in [SP800-73pt2].

3.2.11.3. Hybrid Connections

Hybrid connections use a combination of technologies to establish a secure connection between the authenticator and endpoint via a network tunnel service. A visual representation (e.g., QR code) is used to support key establishment between the

[4] As used in this section, the term *pairing code* does not imply that a persistent pairing process (e.g., Bluetooth) is necessarily used.

1. 通过设备之间的临时有线连接。
2. 通过类似于配对过程但不需要设备之间持久关系的关联过程，为认证器与端点之间的加密通信建立密钥。关联过程**SHALL**采用配对码[4]或设备之间的其他共享密钥。认证器或端点**SHALL**具有配对码，该配对码**MAY**印在设备上。配对码**SHALL**长度至少为六位十进制数字(或等效值)。它**SHALL**通过手动输入或使用QR码或类似的光学通信表示在设备之间传递。

当使用有效范围小于1米的无线技术(例如，NFC)时，从端点传输到认证器的任何激活密钥**SHALL**使用设备之间建立的密钥进行加密。**SHOULD**使用经认证的连接。如果认证器配置为要求经认证的配对，则**SHALL**使用配对码。

> 仅加密激活密钥而不加密整个身份验证事务可能会暴露敏感信息(例如，RP的身份)，尽管这需要攻击者非常接近订阅者。对于包含个人信息但不要求经认证配对的认证器，应特别小心。**SHOULD**使用加密来保护该信息免受窃听攻击。

有效范围为1米或以上的网络连接和无线技术(例如，低功耗蓝牙[BLE])**SHALL**在认证器与端点之间使用经认证的保护信道。整个身份验证事务**SHALL**被加密。

关联过程建立的密钥可以是临时的(即，在有限的事务次数或时间内有效)或持久的。**SHALL**提供端点移除持久密钥的机制。

与认证器的无线连接的一个示例是[SP800-73pt2]中规定的虚拟接触接口。

3.2.11.3. 混合连接

混合连接使用多种技术的组合，通过网络隧道服务在认证器与端点之间建立安全连接。使用视觉表示(例如，二维码)来支持

4 如本节所用，术语配对码并不意味着必然使用持久配对过程(例如，蓝牙)。

authenticator and endpoint, which is supplemented by a wireless technology (e.g., Bluetooth LE) to require physical proximity between the parties when the association is made. The requirement for physical proximity of the authenticator reduces the potential for phishing attacks that might otherwise associate the authenticator with an attacker endpoint.

Hybrid connections (e.g., hybrid transports specified by the CTAP2.2 protocol [FIDO2]) **SHALL** be established between authenticators and endpoints in one of the following ways:

1. By communicating initial keying information and the identity of the tunnel service to be used via a displayed QR code or similar visual representation coupled with the receipt by the endpoint of wireless data containing the additional information required to establish the tunnel connection. The wireless data **SHALL** be conveyed over a technology with a maximum effective range of no more than 240 meters.
2. Through cached keying and tunnel information retained by the authenticator and endpoint from a previous authentication transaction.

A mechanism for endpoints to remove cached associations with authenticators **SHALL** be provided.

3.2.12. Random Values

Random values are extensively used in authentication processes in a variety of roles (e.g., nonces, authentication secrets). Unless otherwise specified, random values that reference this section **SHALL** be generated by an approved random bit generator [RBG][5] that provides at least the minimum security strength specified in the latest revision of [SP800-131A] (i.e., 112 bits as of the date of this publication).

3.2.13. Exportability

Exportability is the ability of an authenticator to replicate, share, or store its authentication keys outside of the protected boundary of the authenticator (e.g., copying it to another authenticator, backing up a key to a separate storage location). Generally, authentication keys are considered exportable unless the authenticator generates, stores, and uses the keys in a protected hardware environment that prevents software from accessing the keys, such as in a security coprocessor (e.g., TPM) or a dedicated device (e.g., a security key). This is intended to prevent software on the endpoint from copying or leaking the authentication secret. Non-exportable authentication keys are considered more secure, and accordingly, non-exportable cryptographic keys are required at AAL3. The authentication keys on syncable authenticators are inherently exportable (see Appendix B).

[5] Detailed information on generating random values may be found in [SP800-90A], [SP800-90B], and [SP800-90C].

认证器与端点之间的密钥建立，辅以无线技术(例如，蓝牙LE)以在关联时要求各方之间的物理接近。对认证器物理接近的要求降低了网络钓鱼攻击的可能性，否则这些攻击可能将认证器与攻击者端点关联。

混合连接(例如，CTAP2.2协议[FIDO2]规定的混合传输)**SHALL**通过以下方式之一在认证器与端点之间建立：

1. 通过显示的二维码或类似视觉表示传达初始密钥信息和要使用的隧道服务身份，并结合端点接收包含建立隧道连接所需附加信息的无线数据。无线数据**SHALL**通过最大有效范围不超过240米的技术传输。
2. 通过认证器和端点从先前身份验证事务中保留的缓存密钥和隧道信息。

SHALL提供端点移除与认证器的缓存关联的机制。

3.2.12. 随机值

随机值在身份验证过程中广泛用于各种角色(例如，随机数、身份验证密钥)。除非另有规定，引用本节的随机值**SHALL**由经批准的随机位生成器[RBG][5]生成，该生成器提供至少为[SP800-131A]最新修订版中规定的最低安全强度(即，截至本出版物发布之日为112位)。

3.2.13. 可导出性

可导出性是指认证器在其受保护边界之外复制、共享或存储其身份验证密钥的能力(例如，将其复制到另一个认证器，将密钥备份到单独的存储位置)。通常，身份验证密钥被视为可导出的，除非认证器在防止软件访问密钥的受保护硬件环境中生成、存储和使用密钥，例如在安全协处理器(例如TPM)或专用设备(例如安全密钥)中。这旨在防止端点上的软件复制或泄露身份验证密钥。不可导出的身份验证密钥被认为更安全，因此，AAL3要求使用不可导出的加密密钥。可同步认证器上的身份验证密钥本质上是可导出的(参见附录B)。

5 有关生成随机值的详细信息，可参见[SP800-90A]、[SP800-90B]和[SP800-90C]。

To be considered non-exportable, an authenticator **SHALL** either be a separate piece of hardware or an embedded processor or execution environment (e.g., secure element, TEE, TPM). These hardware authenticators and embedded processors are separate from a host processor, such as the CPU on a laptop or mobile device. A non-exportable authenticator **SHALL** be designed to prohibit the export of the authentication secret to the host processor and **SHALL NOT** be capable of being reprogrammed by the host processor to allow the secret to be extracted. The authenticator is subject to applicable [FIPS140] requirements. Organizations **SHOULD** employ authenticators that have undergone independent security testing, such as authenticators validated to [FIPS140] security level 2 overall with level 3 physical security[6] or evaluated against relevant Common Criteria Protection Profiles.

[6] In this case, the FIPS 140 evaluation would satisfy the minimum [FIPS140] security level 1 validation requirement for authenticators procured by federal agencies.

要被视为不可导出，认证器**SHALL**要么是独立的硬件，要么是嵌入式处理器或执行环境(例如安全元件、TEE、TPM)。这些硬件认证器和嵌入式处理器与主机处理器(例如笔记本电脑或移动设备上的CPU)分离。不可导出的认证器**SHALL**被设计为禁止将认证密钥导出到主机处理器，并且**SHALL NOT**能够被主机处理器重新编程以允许提取密钥。认证器须符合适用的[FIPS140]要求。组织**SHOULD**采用经过独立安全测试的认证器，例如通过[FIPS140]整体安全等级2及物理安全等级3[6]验证的认证器，或依据相关Common Criteria保护配置文件进行评估的认证器。

6 在这种情况下，FIPS 140评估将满足联邦机构采购的认证器的最低[FIPS140]安全等级1验证要求。

4. Authenticator Event Management

This section is normative.

Events can occur over the lifetime of a subscriber's authenticator and affect its use. These events include binding, maintenance, loss, theft, compromise, unauthorized duplication, expiration, and revocation. This section describes the actions to be taken in response to those events.

4.1. Authenticator Binding

Authenticator binding refers to establishing an association between a specific authenticator and a subscriber account to enable the authenticator to authenticate for that subscriber account, possibly in conjunction with other authenticators.

Authenticators **SHALL** be bound to subscriber accounts by either:

- Being issued by the CSP as part of enrollment or
- Using a subscriber-provided authenticator that is acceptable to the CSP.

The SP 800-63 suite of guidelines refers to the *binding* rather than the issuance of authenticators to accommodate both options.

Throughout the lifetime of a digital identity, CSPs **SHALL** maintain a record of all authenticators that are bound to each subscriber account. The CSP **SHALL** determine the characteristics of the authenticator being bound (e.g., single-factor versus multi-factor, phishing-resistant or not) so that verifiers can assess compliance with the requirements at each AAL. This determination **MAY** be based on strong evidence (e.g., authenticator attestation), direct information from having issued the authenticator, or typical characteristics of authenticator implementations (e.g., whether a user verification bit is set by [WebAuthn]).

The CSP **SHALL** also maintain other state information that is required to meet the authenticator verification requirements. For example, the throttling of authentication attempts described in Sec. 3.2.2 requires the CSP or verifier to maintain state information on recent failed authentication attempts, except for activation factors verified at the authenticator.

The record created by the CSP **SHALL** contain the date and time of significant authenticator life cycle events (e.g., binding to the subscriber account, renewal, update, expiration). The record **SHOULD** include information about the source of the binding (e.g., IP address, device identifier) of any device associated with the event.

As part of the binding process, the CSP **MAY** require additional information about the new authenticator or its associated endpoint to determine whether it is suitable for the requested AAL.

4. 认证器事件管理

本节为规范性内容。

事件可在订阅者认证器的生命周期内发生并影响其使用。这些事件包括绑定、维护、丢失、被盗、攻破、未经授权的复制、过期和撤销。本节描述了应对这些事件应采取的措施。

4.1. 认证器绑定

认证器绑定是指建立特定认证器与订阅者账户之间的关联，使该认证器能够为该订阅者账户进行身份验证，可能与其他认证器结合使用。

认证器**SHALL**通过以下任一方式绑定到用户账户：

- 由CSP在注册或
- 使用订阅者提供且CSP可接受的认证器。SP 800-63系列指南指的是绑定，而不是发放认证器，以兼顾这两种选项。

在数字身份的整个生命周期内，CSP**SHALL**维护绑定到每个订阅者账户的所有认证器的记录。CSP**SHALL**确定所绑定认证器的特性(例如单因素还是多因素、是否抗钓鱼)，以便验证器能够评估各AAL要求的合规性。该确定**MAY**基于强有力的证据(例如认证器证明)、来自签发认证器的直接信息，或认证器实现的典型特性(例如是否由[WebAuthn]设置用户验证位)。

CSP **SHALL**还维护满足认证器验证要求所需的其他状态信息。例如，第3.2.2节中描述的认证尝试节流要求CSP或验证器维护有关近期失败认证尝试的状态信息，但在认证器处验证的激活因素除外。

CSP创建的记录**SHALL**包含重要认证器生命周期事件(例如，绑定到订阅者账户、续期、更新、过期)的日期和时间。该记录**SHOULD**包含有关与该事件相关联的任何设备的绑定来源(例如，IP地址、设备标识符)的信息。

作为绑定过程的一部分，CSP **MAY**要求提供有关新认证器或其关联端点的附加信息，以确定其是否适合所请求的AAL。

4.1.1. Binding at Enrollment

Binding at the time of enrollment is considered to be part of the enrollment process and is discussed in [SP800-63A].

4.1.2. Post-Enrollment Binding

4.1.2.1. Binding an Additional Authenticator

To minimize the need for account recovery, CSPs and verifiers **SHOULD** encourage subscribers to maintain at least two separate means of authentication. For example, a subscriber who usually uses an OTP authenticator as a physical authenticator **MAY** also be issued look-up secret authenticators or register a device for out-of-band authentication to be used if the physical authenticator is lost, stolen, or damaged. See Sec. 4.2 for more information on replacing passwords.

Accordingly, CSPs **SHALL** permit the binding of multiple authenticators to a subscriber account. When any new authenticator is bound to a subscriber account, the CSP **SHALL** ensure that the process requires authentication at either the maximum AAL currently available in the subscriber account or the maximum AAL at which the new authenticator will be used, whichever is lower. For example, binding an authenticator that is suitable for use at AAL2 requires authentication at AAL2 unless the subscriber account currently has only AAL1 authentication capabilities. When an authenticator is added, the CSP **SHALL** notify the subscriber via a mechanism independent of the transaction binding the new authenticator, as described in Sec. 4.6.

4.1.2.2. Binding Across Endpoints

It may be necessary for a subscriber to bind an authenticator to a subscriber account using a device that is different from the authenticated endpoint (i.e., the endpoint for the session being authenticated). This process is typically used when adding authenticators that are embedded in a new endpoint or when connectivity limitations prevent the newly bound authenticator from being connected to an authenticated endpoint.

The binding process **SHALL** proceed in one of the following ways:

- An endpoint that has authenticated to the CSP requests a binding code from the CSP. The binding code is input into the endpoint associated with the new authenticator and sent to the CSP.
- The endpoint associated with the new authenticator obtains a binding code from the CSP. The binding code is input to an authenticated endpoint and sent to the CSP.

4.1.1. 注册时的绑定

在注册登记时进行绑定被视为注册登记过程的一部分，并在[SP800-63A]中讨论。

4.1.2. 注册后绑定

4.1.2.1. 绑定附加认证器

为尽量减少账户恢复的需求，CSP和验证器**SHOULD**鼓励订阅者维护至少两种独立的身份验证方式。例如，通常使用OTP认证器作为物理认证器的订阅者**MAY**同时被签发查询性秘密认证器或注册一个用于带外身份验证的设备，以便在物理认证器丢失、被盗或损坏时使用。有关替换密码的更多信息，参见Sec.4.2。

因此，CSP**SHALL**允许将多个认证器绑定到订阅者账户。当任何新认证器绑定到订阅者账户时，CSP**SHALL**确保该过程要求在订阅者账户当前可用的最高AAL或新认证器将被使用的最高AAL(以较低者为准)进行身份验证。例如，绑定适合在AAL2使用的认证器要求在AAL2进行身份验证，除非订阅者账户当前仅具有AAL1身份验证能力。当添加认证器时，CSP**SHALL**通过独立于绑定新认证器的事务的机制通知订阅者，如Sec.4.6所述。

4.1.2.2. 跨端点绑定

订阅者可能需要使用与已认证端点(即正在认证的会话的端点)不同的设备将认证器绑定到订阅者账户。此过程通常用于添加嵌入在新端点中的认证器，或当连接限制导致新绑定的认证器无法连接到已认证端点时。

绑定过程**SHALL**按以下方式之一进行：

- 已向CSP认证的端点向CSP请求绑定代码。该绑定代码被输入到与新认证器关联的端点并发送给CSP。
- 与新认证器关联的端点从CSP获取绑定代码。该绑定代码被输入到已认证端点并发送给CSP。

In addition to the requirements in Sec. 4.1.2.1 and Sec. 4.2, the following requirements **SHALL** apply when binding an external authenticator:

- An authenticated protected channel **SHALL** be established by the endpoint associated with the new authenticator and the CSP.
- The subscriber **MAY** be prompted to enter an identifier by which the CSP knows them on the endpoint associated with the new authenticator.
- The CSP **SHALL** generate a *binding code* using an approved random bit generator, as described in Sec. 3.2.12 and send it to either the new authenticator endpoint or the authenticated endpoint approving the binding. The binding code **SHALL** be at least 40 bits in length if it is used with an identifier that was entered in the previous step. Otherwise, a binding code of at least 112 bits in length **SHALL** be required.
- The subscriber **SHALL** transfer the binding code to the other endpoint. This transfer **SHALL** either be manual or via a local out-of-band method (e.g., QR code). The binding code **SHALL NOT** be communicated over any insecure channel (e.g., email).
- The binding code **SHALL** be usable only once and **SHALL** be valid for a maximum of 10 minutes.
- Following the binding of the new authenticator (or issuance of a certificate, in the case of PKI-based authenticators), the CSP **SHOULD** encourage the subscriber to authenticate with the new authenticator to confirm that the process has been completed successfully.
- The CSP **SHALL** provide clear instructions on what the subscriber should do in the event of an authenticator binding mishap (e.g., making a button available to be pressed or a contact address to be used to allow a misbound authenticator to be quickly invalidated), as appropriate. This **MAY** be provided in the authenticated session in addition to the binding notification described in Sec. 4.6.

The binding of an external authenticator may introduce risks due to the potential for the subscriber to be tricked into using a binding code by an attacker or supplying a binding code to an attacker. In some cases, representations (e.g., QR codes) obtained from a trusted source (e.g., an authenticated session, especially when that authentication is phishing-resistant) are considered to be more robust against such attacks because they typically contain the URL of the CSP in addition to the binding code. As a result, there is less potential for the subscriber to be fooled into entering a binding code at a phishing site.

除第4.1.2.1节和第4.2节中的要求外，绑定外部认证器时**SHALL**适用以下要求：

- 与新认证器关联的端点和CSP **SHALL**建立已认证保护信道。
- 订阅者**MAY**被提示在与新认证器关联的端点上输入CSP用于识别其身份的标识符。
- CSP **SHALL**使用经批准的随机位生成器生成绑定代码，如第3.2.12节所述，并将其发送到新认证器端点或批准绑定的已认证端点。如果绑定代码与上一步中输入的标识符一起使用，则其长度**SHALL**至少为40位。否则，**SHALL**要求绑定代码长度至少为112位。
- 订阅者**SHALL**将绑定代码传输到另一端点。此传输**SHALL**为手动方式或通过本地带外方法(例如，QR码)。绑定代码**SHALL NOT**通过任何不安全信道(例如，电子邮件)传送。
- 绑定代码**SHALL**仅可使用一次，且**SHALL**有效期最长为 10 分钟。
- 在新认证器绑定(或对于基于PKI的认证器，颁发证书)之后，CSP **SHOULD**鼓励订阅者使用新认证器进行认证，以确认该过程已成功完成。
- CSP **SHALL**就订阅者在认证器绑定发生意外时应采取的措施(例如，提供可按下按钮或可使用的联系地址，以便快速使错误绑定的认证器失效)提供明确说明(视情况而定)。除第4.6节中描述的绑定通知外，此说明**MAY**在已认证会话中提供。

外部认证器的绑定可能引入风险，因为订阅者可能被攻击者诱骗使用绑定码，或向攻击者提供绑定码。在某些情况下，从可信来源(例如经过身份验证的会话，尤其是当该身份验证为抗钓鱼时)获得的表示(例如QR码)被认为对此类攻击更具鲁棒性，因为它们通常除绑定码外还包含CSP的URL。因此，订阅者被诱骗在钓鱼网站输入绑定码的可能性较小。

4.1.3. Binding to a Subscriber-Provided Authenticator

A subscriber may already possess authenticators that are suitable for authentication at a particular AAL. For example, the subscriber may have their own multi-factor authenticator and would like to use that authenticator at a verifier that requires AAL2.

CSPs **SHOULD**, where practical, accommodate subscriber-provided authenticators to relieve the burden on the subscriber of managing many authenticators. The binding of these authenticators **SHALL** be done as described in Sec. 4.1.2.

As part of this process, CSPs will need to establish the capabilities and characteristics of the subscriber-provided authenticator that they wish to accept to determine its suitability for the use case and the intended AAL. The level of assurance that the CSP requires in the fidelity of these authenticator attributes **MAY** vary depending on the use case and threat environment. Some authenticators, such as those based on the WebAuthn standard [WebAuthn], provide metadata about the authenticator during the binding or authentication process that can be used by the CSP to inform its decisions. This metadata, for example, could indicate whether an authenticator uses an activation factor to function as a multi-factor authenticator. Similarly, some subscriber-controlled wallets will also offer metadata about its functions, including information about the mechanisms used to unlock the wallet. CSPs **SHOULD** consider this metadata when choosing how to support a subscriber-provided authenticator. In many cases, such information will not be available, and CSPs **SHOULD** evaluate the characteristics of commercially available authenticators that are likely to be used by their subscribers and make determinations about what authenticators they will accept. The types of authenticators accepted by the CSP **SHALL** be documented in the CSP practice statement.

In some high assurance use cases, CSPs may desire additional confidence in the attributes of the authenticators registered by their subscribers. Some authenticators support attestation features that can be used to determine the capabilities and manufacturers of specific authenticators. However, such attestation features are not widely available in authenticators that are likely to be used by public users. The lack of support for attestations **SHOULD NOT** block the use of authenticators for broad public-facing applications.

4.1.4. Renewal

The subscriber **SHOULD** bind a new or updated authenticator before an existing authenticator's expiration. The process for this **SHOULD** conform closely to the binding process for an additional authenticator, as described in Sec. 4.1.2. The CSP **MAY** periodically take other actions (e.g., confirming contact addresses) as a part of the renewal process or separately. Following the successful use of the replacement authenticator, the CSP **SHOULD** invalidate the expiring authenticator.

4.1.3. 绑定到用户提供的认证器

订阅者可能已经拥有适合在特定AAL进行认证的认证器。例如，订阅者可能拥有自己的多因素认证器，并希望要求在AAL2的验证器上使用该认证器。

CSP **SHOULD**在可行的情况下容纳订阅者提供的认证器，以减轻订阅者管理众多认证器的负担。这些认证器的绑定**SHALL**按第4.1.2节所述进行。

作为此过程的一部分，CSP需要确定其希望接受的订阅者提供的认证器的能力和特性，以判断其对于用例和预期AAL的适用性。CSP对这些认证器属性保真度所要求的保证等级**MAY**因用例和威胁环境而异。某些认证器，例如基于WebAuthn标准[WebAuthn]的认证器，在绑定或身份验证过程中提供关于认证器的元数据，CSP可利用这些元数据为其决策提供依据。例如，该元数据可指示认证器是否使用激活因子来充当多因素认证器。类似地，某些订阅者控制的钱包也会提供关于其功能的元数据，包括用于解锁钱包的机制信息。CSP在选择如何支持订阅者提供的认证器时**SHOULD**考虑此元数据。在许多情况下，此类信息不可用，CSP**SHOULD**评估其订阅者可能使用的商用认证器的特性，并确定将接受哪些认证器。CSP接受的认证器类型**SHALL**记录在CSP实践声明中。

在某些高保证用例中，CSP可能希望对其订阅者注册的认证器属性有额外的信心。某些认证器支持可用于确定特定认证器能力和制造商的证明功能。然而，此类证明功能在公众用户可能使用的认证器中并不广泛可用。缺乏对证明的支持**SHOULD NOT**阻碍认证器用于广泛的面向公众的应用。

4.1.4. 续期

订阅者**SHOULD**在现有认证器过期之前绑定新的或更新的认证器。此过程**SHOULD**与Sec.4.1.2中所述的附加认证器绑定过程密切一致。CSP**MAY**作为续期过程的一部分或单独定期采取其他措施(例如，确认联系地址)。在成功使用替换认证器后，CSP**SHOULD**使即将过期的认证器失效。

4.2. Account Recovery

Account recovery is when a subscriber recovers from losing control of the authenticators that are needed to authenticate at a desired AAL. This may be accomplished by repeating portions of the identity proofing process, using a prearranged recovery contact, or presenting one or more recovery codes, perhaps in conjunction with using an authenticator that is still available to the subscriber bound to their subscriber account. Once this is completed, the subscriber can bind one or more new authenticators to their subscriber account. An account recovery event always causes one or more notifications to be sent to the subscriber to help detect the fraudulent use of account recovery.

Account recovery differs from authentication in several ways. Since account recovery is expected to be invoked infrequently, it is generally less convenient than authentication and — depending on the situation and recovery methods offered by the CSP — may involve extended waiting times.

> Replacement of a forgotten password where the subscriber can authenticate with one or more other authenticators is considered to be the binding of a new authenticator (see Sec. 4.1.2.1) rather than account recovery.

4.2.1. Account Recovery Methods

Four general classes of account recovery methods are recognized:

- Saved recovery codes
- Issued recovery codes
- Use of recovery contacts
- Repeated identity proofing

CSPs **SHALL** support one or more of these and **MAY** support an application-specific method (e.g., interaction with a CSP agent) to recover a subscriber account. The use of alternative methods **SHALL** be based on a risk analysis and documented by the CSP.

4.2.1.1. Saved Recovery Codes

At enrollment, a CSP that supports this recovery option **SHOULD** issue a recovery code to the subscriber. The recovery code **SHALL** include at least 64 bits from an approved random bit generator. The saved recovery code may be presented as numeric or a printable ASCII representation (e.g., Base64) for manual entry or as a machine-readable optical label (e.g., QR code) that contains the recovery code. At any point following enrollment, the subscriber **MAY** request a replacement recovery code. The issuance of a replacement recovery code **SHALL** result in an account recovery notification, as described in Sec. 4.6.

4.2. 账户恢复

账户恢复是指订阅者在失去对以所需AAL进行身份验证所需的认证器的控制后恢复的过程。这可以通过重复身份核验过程的部分步骤、使用预先安排的恢复联系人，或提供一个或多个恢复代码(可能结合使用订阅者仍可用的、已绑定到其订阅者账户的认证器)来实现。一旦完成，订阅者可以将一个或多个新认证器绑定到其订阅者账户。账户恢复事件总是会导致向订阅者发送一个或多个通知，以帮助检测账户恢复的欺诈使用。

账户恢复在多个方面与身份验证不同。由于账户恢复预计不常被调用，它通常比身份验证更不方便，并且--取决于情况和CSP提供的恢复方法--可能涉及较长的等待时间。

> 在订阅者可以使用一个或多个其他认证器进行认证的情况下，替换遗忘的密码被视为新认证器的绑定(参见第4.1.2.1节)，而不是账户恢复。

4.2.1. 账户恢复方法

认可四类通用的账户恢复方法：

- 已保存的恢复代码
- 已发放的恢复代码
- 使用恢复联系人
- 重复身份验证

CSP **SHALL**支持其中一种或多种方法，并且**MAY**支持特定于应用的方法(例如，与CSP代理交互)来恢复订阅者账户。替代方法的使用**SHALL**基于风险分析并由CSP记录。

4.2.1.1. 已保存的恢复代码

在注册登记时，支持此恢复选项的CSP**SHOULD**向订阅者发放恢复代码。恢复代码**SHALL**包含来自经批准的随机位生成器的至少64位。保存的恢复代码可以呈现为数字或可打印ASCII表示(例如，Base64)以供手动输入，或呈现为包含恢复代码的机器可读光学标签(例如，QR码)。在注册登记后的任何时间点，订阅者**MAY**请求替换恢复代码。替换恢复代码的发放**SHALL**导致账户恢复通知，如Sec.4.6所述。

Saved recovery codes are intended to be maintained offline (e.g., printed or written down) and stored securely by the subscriber for future use. The verification of saved recovery codes **SHALL** be subject to the throttling requirements in Sec. 3.2.2. Saved recovery codes **SHALL** be stored in the subscriber account in hashed form using an approved one-way function, as described in Sec. 3.1.1.2. Following the use of a saved recovery code, the CSP **SHALL** invalidate that recovery code and **SHALL** issue a new saved recovery code to the subscriber.

4.2.1.2. Issued Recovery Codes

CSPs that support this option allow the subscriber to maintain one or more recovery addresses (e.g., postal, email, text message, voice). When recovery is required, a recovery code will be sent to a claimant-chosen address. The issued recovery code **SHALL** include at least six decimal digits (or equivalent) from an approved random bit generator, as described in Sec. 3.2.12. The issued recovery code may be presented as a numeric or a printable ASCII representation (e.g., Base64) for manual entry, a secure (e.g., https) link with a representation of the recovery code, or a machine-readable optical label (e.g., QR code) that contains the recovery code.

Issued recovery codes **SHALL** be valid for at most:

- 21 days when sent to a postal address within the contiguous United States
- 30 days when sent to a postal address outside of the contiguous United States
- 10 minutes when sent via text message or voice
- 24 hours when sent to an email address

The verification of issued recovery codes **SHALL** be subject to the throttling requirements in Sec. 3.2.2.

When establishing recovery addresses other than those validated or verified as part of the identity proofing process, the address **SHALL** be verified. To verify an address, the CSP **SHALL** send a confirmation code with the same characteristics as a recovery code to the newly established recovery address. A recovery address **SHALL** be established only after the subscriber provides the correct confirmation code to the CSP. CSPs **SHALL** allow the subscriber to establish at least two recovery addresses.

4.2.1.3. Recovery Contacts

CSPs that support the use of recovery contacts **SHALL** allow the subscriber to specify one or more addresses of trusted associates to receive issued recovery codes. The requirements for recovery contacts are very similar to those for issued recovery codes with the following exceptions:

保存的恢复代码旨在离线维护(例如打印或写下)，并由订阅者安全存储以备将来使用。保存的恢复代码的验证**SHALL**受Sec.3.2.2中的节流要求约束。保存的恢复代码**SHALL**以哈希形式存储在订阅者账户中，使用经批准的单向函数，如Sec.3.1.1.2所述。使用保存的恢复代码后，CSP**SHALL**使该恢复代码失效，并**SHALL**向订阅者发放新的保存的恢复代码。

4.2.1.2. 发放的恢复代码

支持此选项的CSP允许订阅者维护一个或多个恢复地址(例如邮政、电子邮件、短信、语音)。当需要恢复时，恢复代码将发送到声称者选择的地址。发放的恢复代码**SHALL**包含来自经批准的随机位生成器的至少六位十进制数字(或等效物)，如Sec.3.2.12所述。发放的恢复代码可以呈现为用于手动输入的数字或可打印ASCII表示(例如Base64)、带有恢复代码表示的安全(例如https)链接，或包含恢复代码的机器可读光学标签(例如QR码)。

已发放的恢复代码**SHALL**有效期最长为：

- 当发送至美国本土的邮寄地址时，为 21 days
- 当发送至美国本土以外邮寄地址时，为30天
- 通过短信或语音发送时，为 10 分钟
- 发送至电子邮件地址时，为 24 小时

对已发放恢复代码的验证**SHALL**遵守第3.2.2节中的节流要求。

当建立除身份核验过程中验证或核实的地址之外的恢复地址时，该地址**SHALL**被验证。为验证地址，CSP**SHALL**向新建立的恢复地址发送具有与恢复代码相同特征的确认码。只有在订阅者向CSP提供正确的确认码后，恢复地址**SHALL**被建立。CSP**SHALL**允许订阅者建立至少两个恢复地址。

4.2.1.3. 恢复联系人

支持使用恢复联系人的CSP **SHALL**允许订阅者指定一个或多个可信联系人的地址以接收已发放的恢复代码。对恢复联系人的要求与对已发放恢复代码的要求非常相似，但有以下例外：

- The validity time for recovery codes sent to recovery contacts **MAY** be extended by 24 hours (e.g., valid for no more than 24 hours and 10 minutes if sent via text messaging) to provide additional time for the recovery contact to communicate the recovery code to the subscriber.
- Confirmation of the recovery code address **MAY** also be extended by 24 hours to allow the recovery contact to send the confirmation code to the subscriber for entry.

If the CSP supports the use of recovery contacts, the CSP **SHALL** provide methods for subscribers to view and manage recovery contacts. CSPs **SHOULD** send a reminder annually to subscribers to review their list of recovery contacts.

4.2.1.4. Repeated Identity Proofing

When the subscriber account has been identity-proofed at a minimum of *identity assurance level 1 (IAL1)*, CSPs **SHOULD** support account recovery by repeating a portion of the identity proofing process. The CSP **SHALL** repeat the necessary steps of identity proofing consistent with the level of initial identity proofing and **SHALL** confirm that the claimant's identity is consistent with the previously established account. If the CSP has retained a biometric sample from the user or a copy of the evidence used during the initial proofing that is of sufficient quality and resolution, the CSP **MAY** repeat only the verification portion of the identity proofing process, as described in [SP800-63A].

4.2.2. Recovery Requirements by IAL/AAL

Different recovery methods apply, depending on the IAL and the maximum AAL associated with the subscriber account.

4.2.2.1. Recovery Without Identity Proofing

When subscribers have not been identity-proofed, a reproofing option is not available to support account recovery. The recovery of such subscriber accounts **SHALL** require the successful use of a saved recovery code, issued recovery code, or recovery contact.

Since identity proofing requires issuing authenticators that are sufficient for multi-factor authentication to allow the subscriber to access personal information about themselves, subscriber accounts that can authenticate at a maximum of AAL1 are without identity proofing.

4.2.2.2. Recovery at AAL2

To recover an account that can authenticate at a maximum of AAL2, the CSP **SHALL** require the subscriber to complete one of the following:

- Two recovery codes obtained using different methods from the set (i.e., saved, issued, and recovery contacts)

- 发送给恢复联系人的恢复代码的有效期**MAY**延长24小时(例如，如果通过短信发送，有效期不超过24小时10分钟)，以便为恢复联系人向订阅者传达恢复代码提供额外时间。
- 恢复代码地址的确认**MAY**也延长24小时，以允许恢复联系人将确认代码发送给订阅者以供输入。

如果CSP支持使用恢复联系人，则CSP **SHALL**为订阅者提供查看和管理恢复联系人的方法。CSP **SHOULD**每年向订阅者发送提醒，以审查其恢复联系人列表。

4.2.1.4. 重复身份证明

当订阅者账户已至少在身份保证等级*1(IAL1)*进行身份核验时，CSP**SHOULD**通过重复身份核验过程的一部分来支持账户恢复。CSP**SHALL**重复与初始身份核验级别一致的必要身份核验步骤，并**SHALL**确认声称者的身份与先前建立的账户一致。如果CSP保留了用户的生物特征样本或初始核验期间使用的证据副本，且其质量和分辨率足够，则CSP**MAY**仅重复身份核验过程的验证部分，如[SP800-63A]所述。

4.2.2. 按 IAL/AAL 划分的恢复要求

根据IAL和与订阅者账户关联的最大AAL，适用不同的恢复方法。

4.2.2.1. 无身份证明的恢复

当订阅者尚未经过身份核验时，无法使用重新核验选项来支持账户恢复。此类订阅者账户的恢复**SHALL**要求成功使用已保存的恢复代码、已发放的恢复代码或恢复联系人。

由于身份核验要求发放足以进行多因素身份验证的认证器，以允许订阅者访问其个人信息，因此最多可在AAL1进行认证的订阅者账户无需身份核验。

4.2.2.2. AAL2 下的恢复

要恢复最多可在AAL2进行认证的账户，CSP **SHALL**要求订阅者完成以下之一：

- 使用不同方法从集合(即已保存、已签发和恢复联系人)中获取的两个恢复代码

- One recovery code from the set (i.e., saved, issued, and recovery contacts) plus authentication with a single-factor authenticator that is bound to the subscriber account
- Repeated identity proofing (provided that the subscriber account has been identity-proofed)

4.2.2.3. Recovery at AAL3

If an account that can authenticate at AAL3 has been identity-proofed at IAL1 or IAL2, the requirements are the same as those for recovery at AAL2.

If an account that can authenticate at AAL3 has been identity-proofed at IAL3, the CSP **SHALL** successfully perform a successful biometric comparison against the biometric characteristic collected during an initial on-site attended identity proofing session, as described in [SP800-63A]. The CSP **MAY** also require the presentation of the evidence used in the initial identity proofing process.

4.2.3. Account Recovery Notification

In all cases, account recovery **SHALL** cause a notification to be sent to the subscriber or their designee, as described in Sec. 4.6.

4.3. Loss, Theft, Damage, and Compromise

Compromised authenticators include those that have been lost, stolen, or subject to unauthorized duplication or that have activation factors that are no longer in the subscriber's control. Generally, one must assume that a lost authenticator has been stolen or compromised by someone other than the legitimate holder of the authenticator. Damaged or malfunctioning authenticators are also considered compromised to guard against any possibility of the extraction of the authenticator's secret.

The CSP **SHALL** suspend, invalidate, or destroy compromised authenticators from the subscriber's account promptly following compromise detection. Organizations **SHOULD** establish time limits for this process.

To facilitate the secure reporting of an authenticator's loss, theft, damage, or compromise, the CSP **SHOULD** provide the subscriber with a method of authenticating using a backup or alternate authenticator. This backup authenticator **SHALL** be a password or a physical authenticator. Either could be used, but only one authentication factor is required to make this report. Alternatively, the subscriber **MAY** establish an authenticated protected channel for the CSP to verify the information collected during identity proofing. The CSP **MAY** choose to verify a contact address (i.e., the email address, telephone number, or postal address) and suspend or invalidate authenticators that are reported to have been compromised.

- 从集合(即已保存、已签发和恢复联系人)中获取的一个恢复代码，加上使用绑定到订阅者账户的单因素认证器进行身份验证
- 重复身份核验(前提是订阅者账户已完成身份核验)

4.2.2.3. AAL3 下的恢复

若可在AAL3认证的账户已在IAL1或IAL2完成身份验证，要求与AAL2恢复相同。

如果能够在 AAL3 进行身份验证的账户已在 IAL3 完成身份核验，CSP **SHALL**成功执行与初始现场有人值守身份核验会话期间采集的生物特征进行成功的生物特征比对，如[SP800-63A]所述。CSP **MAY**还要求出示初始身份核验过程中使用的证据。

4.2.3. 账户恢复通知

在所有情况下，账户恢复**SHALL**导致向订阅者或其指定人发送通知，如Sec.4.6所述。

4.3. 丢失、被盗、损坏和泄露

受损害的认证器包括已丢失、被盗或遭受未经授权复制，或激活因素不再受订阅者控制的认证器。通常，必须假定丢失的认证器已被盗或被认证器合法持有人以外的人损害。损坏或发生故障的认证器也被视为受损害，以防止认证器密钥被提取的任何可能性。

CSP **SHALL**在检测到损害后及时从订阅者账户中暂停、使失效或销毁受损害的认证器。组织**SHOULD**为此过程设定时间限制。

为便于安全报告认证器的丢失、被盗、损坏或泄露，CSP**SHOULD**向订阅者提供使用备份或备用认证器进行身份验证的方法。此备份认证器**SHALL**是密码或物理认证器。两者均可使用，但进行此报告仅需要一个身份验证因素。或者，订阅者**MAY**建立经认证的保护信道，以便CSP验证身份核验期间收集的信息。CSP**MAY**选择验证联系地址(即电子邮件地址、电话号码或邮政地址)，并暂停或撤销被报告已泄露的认证器。

CSPs **MAY** support the temporary suspension of authenticators that are suspected of possible compromise. If suspension is supported, it **SHOULD** be reversed after the subscriber successfully authenticates to the CSP using a valid (i.e., not suspended) authenticator and requests reactivation of the suspended authenticator. The CSP **MAY** set a time limit after which a suspended authenticator can no longer be reactivated.

4.4. Expiration

CSPs **MAY** bind authenticators that expire to subscriber accounts. When an authenticator expires, it **SHALL NOT** be usable for authentication. When an authentication is attempted using an expired authenticator, the CSP **SHOULD** indicate to the subscriber that the authentication failure is due to expiration rather than some other cause.

The CSP **SHOULD** retrieve any authenticator that contains personal information or provide for its erasure or destruction promptly following expiration.

The replacement of expired authenticators **SHALL** conform to the binding process for an additional authenticator, as described in Sec. 4.1.2.

4.5. Invalidation

The invalidation of an authenticator (sometimes referred to as revocation or termination) is the removal of the binding between the authenticator and a subscriber account.

CSPs **SHALL** promptly invalidate authenticators when a subscriber account ceases to exist (e.g., subscriber's death, the discovery of a fraudulent subscriber), when requested by the subscriber, when the authenticator is compromised, or when the CSP determines that the subscriber no longer meets its eligibility requirements. The CSP **SHALL** make a risk-based determination of the authenticity of invalidation requests from the subscriber. The consequences of not invalidating a compromised authenticator are usually more significant than the denial-of-service potential of invalidating one in error.

The CSP **SHOULD** retrieve any authenticator that contains personal information or provide for its erasure or destruction promptly following invalidation. The CSP **SHOULD** notify the subscriber when an authenticator is invalidated, as described in Sec. 4.6.

Further requirements on the invalidation of PIV authenticators are found in [FIPS201].

4.6. Account Notifications

Certain subscriber account events (e.g., the binding of an authenticator, account recovery) require the subscriber or someone designated by them to be independently notified. These notifications help the subscriber detect possible fraud associated with their subscriber account.

CSP **MAY**支持对疑似可能受损害的认证器进行临时暂停。如果支持暂停，则在订阅者使用有效(即未暂停)的认证器成功向 CSP 进行身份验证并请求重新激活被暂停的认证器后，**SHOULD**撤销暂停。CSP **MAY**设定时间限制，超过该限制后被暂停的认证器不能再被重新激活。

4.4. 有效期

CSP **MAY**将过期的认证器绑定到订阅者账户。当认证器过期时，**SHALL NOT**可用于身份验证。当尝试使用过期的认证器进行身份验证时，CSP **SHOULD**向订阅者指示身份验证失败是由于过期而非其他原因。

CSP **SHOULD**在过期后及时取回任何包含个人信息的认证器，或提供其擦除或销毁。

过期认证器的更换**SHALL**符合附加认证器的绑定过程，如Sec.4.1.2所述。

4.5. 失效

认证器的失效(有时称为撤销或终止)是移除认证器与订阅者账户之间的绑定。

CSP**应**在订阅者账户不复存在时(例如订阅者死亡、发现欺诈性订阅者)、订阅者请求时、认证器被泄露时，或CSP确定订阅者不再满足其资格要求时，及时使认证器失效。CSP**应**对来自订阅者的失效请求的真实性做出基于风险的判定。未使被泄露的认证器失效的后果通常比错误地使认证器失效所带来的潜在拒绝服务更为严重。

CSP **SHOULD**在失效后及时取回任何包含个人信息的认证器，或提供其擦除或销毁。CSP **SHOULD**在认证器失效时通知订阅者，如Sec.4.6所述。

关于 PIV 认证器失效的进一步要求见[FIPS201]。

4.6. 账户通知

某些订阅者账户事件(例如，认证器的绑定、账户恢复)要求订阅者或其指定人获得独立通知。这些通知帮助订阅者检测与其订阅者账户相关的可能欺诈。

Events that require notification **SHALL** cause a notification to be sent to the notification addresses stored in the subscriber account. Notification addresses may be any means by which the subscriber can be reliably contacted, such as:

- Postal address
- Email address
- Address (e.g., telephone number) to which a text message or voice message may be sent
- Reference to the subscriber in a push notification service

CSPs **SHALL** support at least two notification addresses per subscriber account. For subscriber accounts that have undergone identity proofing, at least one address **SHALL** have been validated during the identity proofing process. The CSP **SHOULD** allow subscribers with authentication at AAL2 or higher (or at AAL1 if that is the highest AAL available for the subscriber account) to update their notification addresses. The CSP **SHOULD** encourage the subscriber to maintain multiple notification addresses to improve the likelihood of contacting them if a contact address changes.

Notifications **SHALL** be sent to all notification addresses except postal addresses. However, notifications **SHALL** be sent to postal addresses if no other form of notification address is stored in the subscriber account or if the notification is for account recovery at AAL3. Account recovery notifications **SHALL** also be sent to a postal address if the only other notification address in the subscriber account is the address to which an issued recovery code was sent.

The notification **SHALL** provide clear instructions, including contact information, in case the recipient repudiates the event associated with the notification.

需要通知的事件**SHALL**导致向存储在订阅者账户中的通知地址发送通知。通知地址可以是能够可靠联系订阅者的任何方式，例如：

- 邮寄地址
- 电子邮件地址
- 可向其发送文本消息或语音消息的地址(例如，电话号码)
- 在推送通知服务中引用用户

CSP**应**为每个订阅者账户支持至少两个通知地址。对于已经过身份核验的订阅者账户，至少一个地址**应**在身份核验过程中经过验证。CSP**宜**允许以AAL2或更高等级进行身份验证的订阅者(或者如果AAL1是该订阅者账户可用的最高AAL，则以AAL1进行身份验证的订阅者)更新其通知地址。CSP**宜**鼓励订阅者维护多个通知地址，以提高在联系地址发生变化时联系到他们的可能性。

通知**SHALL**发送到除邮政地址外的所有通知地址。
但是，如果订阅者账户中未存储其他形式的通知地址，或者通知是针对 AAL3 的账户恢复，则通知**SHALL**发送到邮政地址。如果订阅者账户中唯一的其他通知地址是已签发恢复代码发送到的地址，则账户恢复通知**SHALL**也发送到邮政地址。

通知**SHALL**提供明确的说明，包括联系信息，以备收件人否认与通知相关的事件。

5. Session Management

This section is normative.

Once an authentication event has occurred, it is often desirable to allow the subscriber to continue using the application across multiple subsequent interactions without requiring them to repeat the authentication event. This is particularly the case with federation scenarios (see [SP800-63C]) in which the authentication event necessarily involves the coordination of several components and parties across a network.

To facilitate this behavior, a *session* **MAY** be started in response to an authentication event and continue until it is terminated. The session **MAY** be terminated for any number of reasons, including an inactivity timeout or an explicit logout event. The session **MAY** be extended through a reauthentication event (see Sec. 5.2) in which the subscriber repeats some of the initial authentication process or performs a full authentication, thereby reestablishing the authenticated session.

Session management is preferable to the continual presentation of credentials, as the poor usability of continual presentation often creates incentives for workarounds (e.g., caching activation factors), thereby negating authentication intent and obscuring the freshness of the authentication event.

5.1. Session Bindings

A session occurs between the software (i.e., the session subject) that a subscriber is running (e.g., browser, application, operating system) and the RP or CSP that the subscriber is accessing (i.e., the session host). A session secret **SHALL** be shared between the subscriber's software and the accessed service. This secret binds the two ends of the session and allows the subscriber to continue using the service over time. The secret **SHALL** be directly presented by the subscriber's software, or possession of the secret **SHALL** be proven using a cryptographic mechanism.

The continuity of authenticated sessions **SHALL** be based on the possession of a session secret that is issued by the session host at the time of authentication and optionally refreshed during the session. The nature of a session depends on the application, such as:

- A web browser session with a "session" cookie
- An instance of a mobile application that retains a session secret

Session secrets that are used as bearer tokens for session management **SHOULD NOT** be persistent (i.e., retained across a restart of the associated application or a reboot of the host device) because they are tied to specific sessions that a restart or reboot would end. Cookies and similar "remember my browser" features **SHALL NOT** be used instead of authentication except as provided for reauthentication at AAL2 in Sec. 2.2.3 when the inactivity limit has been exceeded but the time limit has not.

5. 会话管理

本节为规范性内容。

一旦身份验证事件发生，通常希望允许订阅者在多个后续交互中继续使用应用程序，而无需他们重复身份验证事件。在联合身份场景(见[SP800-63C])中尤其如此，其中身份验证事件必然涉及跨网络的多个组件和参与方的协调。

为便于此行为，会话**可**响应身份验证事件而启动，并持续到其被终止。会话**可**因多种原因被终止，包括不活动超时或显式注销事件。会话**可**通过重新身份验证事件(见第5.2节)延长，在该事件中订阅者重复部分初始身份验证过程或执行完整身份验证，从而重新建立已认证的会话。

会话管理优于持续出示凭证，因为持续出示的可用性差往往会产生规避措施的动机(例如，缓存激活因素)，从而否定身份验证意图并模糊身份验证事件的新鲜度。

5.1. 会话绑定

会话发生在订阅者正在运行的软件(即会话主体)与订阅者正在访问的RP或CSP(即会话主机)之间。会话密钥**应**在订阅者的软件与被访问的服务之间共享。此密钥绑定会话的两端，并允许订阅者随时间继续使用该服务。该密钥**应**由订阅者的软件直接呈现，或者**应**使用密码学机制证明对该密钥的持有。

已认证会话的连续性**SHALL**基于对会话密钥的持有，该密钥由会话主机在身份验证时签发，并可选地在会话期间刷新。会话的性质取决于应用程序，此类

作为：

- 带有“会话”cookie 的 Web 浏览器会话
- 保留会话密钥的移动应用实例

用作会话管理持有者令牌的会话密钥**不应**是持久性的(即，在相关应用程序重启或主机设备重新启动后仍保留)，因为它们与特定会话绑定，而重启或重新启动将结束这些会话。Cookie及类似的“记住我的浏览器”功能**不得**代替身份验证使用，除非如第2.2.3节中针对AAL2的重新身份验证所规定，在已超过不活动限制但尚未超过时间限制的情况下。

Some technologies (e.g., the emerging device bound session credentials specification [DBSC]) mitigate the risk of theft of session secrets by using cryptographic protocols that prove the possession of a session secret rather than using them as bearer tokens. These technologies might additionally store and use these session secrets in protected keystores to reduce the risk of exfiltration by malware. Session secrets used with such proof of possession techniques **MAY** persist. However, RPs and CSPs **SHALL** ensure that the session lifetime limits described in Sec. 2.2.3 are enforced even when a knowledge of the session secret is demonstrated.

The secret used for session binding **SHALL** be generated by the session host in direct response to an authentication event. A session **SHOULD** inherit the AAL properties of the authentication event that triggered its creation. A session **MAY** be considered at a lower AAL than the authentication event but **SHALL NOT** be considered at a higher AAL than the authentication event.

The secrets used for session binding **SHALL** meet all of the following requirements:

1. Secrets are established during or immediately following authentication.
2. Secrets are established using input from an approved random bit generator, as described in Sec. 3.2.12, and are at least 64 bits in length.
3. Secrets are erased or invalidated by the session subject when the subscriber logs out.
4. Secrets are either transferred from the session host to the RP or CSP via an authenticated protected channel or derived from keys that are established as part of establishing a valid, mutually authenticated protected channel.
5. Secrets will time out and are not accepted after the times specified in Sec. 2.1.3, Sec. 2.2.3, and Sec. 2.3.3, as appropriate for the AAL.
6. Secrets are unavailable to intermediaries between the host and the subscriber's endpoint.

In addition, the secrets used for session binding **SHOULD** be erased on the subscriber endpoint when they log out or when the secret is deemed to have expired. They **SHOULD NOT** be placed in insecure locations (e.g., HTML5 Local Storage) due to the potential exposure of local storage to cross-site scripting (XSS) attacks.

Following authentication, authenticated sessions **SHALL NOT** fall back to an insecure transport (e.g., from https to http).

POST/PUT content **SHALL** contain a session identifier that the RP **SHALL** verify to protect against cross-site request forgery (CSRF).

Several mechanisms exist for managing a session over time. The following sections give different examples, additional requirements, and considerations for each

一些技术(例如新兴的设备绑定会话凭证规范[DBSC])通过使用密码协议来证明对会话秘密的持有，而不是将其用作持有者令牌，从而降低会话秘密被盗的风险。这些技术还可能将这些会话秘密存储和使用在受保护的密钥库中，以降低被恶意软件窃取的风险。与此类持有证明技术一起使用的会话秘密**可以**持续存在。然而，RP和CSP**应**确保即使演示了对会话秘密的知悉，也强制执行第2.2.3节中描述的会话生命周期限制。

用于会话绑定的密钥**SHALL**由会话主机直接响应身份验证事件而生成。会话**SHOULD**继承触发其创建的身份验证事件的AAL属性。会话**MAY**被视为低于身份验证事件的AAL，但**SHALL NOT**被视为高于身份验证事件的AAL。

用于会话绑定的密钥**SHALL**满足以下所有要求：

1. 密钥在认证过程中或认证后立即建立。
2. 密钥使用经批准的随机比特生成器的输入建立，如Sec.3.2.12所述，且长度至少为64比特。
3. 当订阅者注销时，密钥由会话主体擦除或失效。
4. 密钥通过经认证的受保护信道从会话主机传输到RP或CSP，或者从建立有效的、相互认证的受保护信道过程中所建立的密钥派生。
5. 密钥将超时，并在Sec.2.1.3、Sec.2.2.3和Sec.2.3.3规定的时间之后不被接受，具体视AAL而定。
6. 密钥对主机与订阅者端点之间的中间方不可用。

此外，用于会话绑定的密钥**SHOULD**在订阅者注销时或密钥被视为已过期时在订阅者端点上擦除。它们**SHOULD NOT**被放置在不安全的位置(例如HTML5 Local Storage)，因为本地存储可能暴露于跨站脚本(XSS)攻击。

身份验证之后，已认证的会话**SHALL NOT**回退到不安全的传输(例如从https回退到http)。

POST/PUT内容**SHALL**包含会话标识符，RP**SHALL**对其进行验证，以防止跨站请求伪造(CSRF)。

存在多种用于随时间管理会话的机制。以下各节给出了不同的示例、附加要求和注意事项

example technology. Additional informative guidance is available in the Open Worldwide Application Security Project (OWASP) *Session Management Cheat Sheet* [OWASP-session].

Sessions **SHOULD** provide a readily accessible mechanism for subscribers to terminate (i.e., log off) their session when their interaction is complete. Session logoff gives the subscriber additional confidence and control over the security of their session, particularly if the endpoint might be accessible to others.

5.1.1. Browser Cookies

Browser cookies are the predominant mechanism by which a session is created and tracked when a subscriber accesses a service. Cookies are not authenticators but are suitable as short-term secrets for the duration of a session.

Cookies used for session maintenance:

1. **SHALL** be tagged to be accessible only on secure (i.e., HTTPS) sessions.
2. **SHALL** be accessible to the minimum practical hostnames and paths.
3. **SHOULD** be tagged as inaccessible via JavaScript (i.e., HttpOnly).
4. **SHOULD** be tagged to expire at or soon after the session's validity period. This requirement is intended to limit the accumulation of cookies but **SHALL NOT** be relied upon to enforce session timeouts.
5. **SHOULD** have the "__Host-" prefix and set "Path=/".
6. **SHOULD** set "SameSite=Lax" or "SameSite=Strict".
7. **SHOULD** contain only an opaque string (e.g., a session identifier) and **SHALL NOT** contain cleartext personal information.

5.1.2. Access Tokens

An access token (e.g., OAuth [RFC6749]) is used to allow an application to access a set of services on a subscriber's behalf following an authentication event. The RP **SHALL NOT** interpret the presence of an access token as an indicator of the subscriber's presence in the absence of other signals. The access token and any associated refresh tokens could be valid long after the authentication session has ended and the subscriber has left the application.

示例技术。更多信息性指导见Open Worldwide Application Security Project(OWASP)*Session Management Cheat Sheet*[OWASP-session]。

会话**SHOULD**提供一种易于访问的机制，供订阅者在交互完成时终止(即注销)其会话。会话注销为订阅者提供了对其会话安全性的额外信心和控制，特别是当端点可能被他人访问时。

5.1.1. 浏览器 Cookie

浏览器cookie是订阅者访问服务时创建和跟踪会话的主要机制。Cookie不是认证器，但适合作为会话持续期间的短期密钥。

用于会话维护的Cookie:

1. **SHALL**被标记为仅在安全(即HTTPS)会话中可访问。
2. **SHALL**应可通过最少实用主机名和路径访问。
3. **应**通过JavaScript标记为不可访问(即HttpOnly)。
4. **SHOULD**被标记为在会话有效期届满时或之后不久过期。此要求旨在限制cookie的累积，但**SHALL NOT**依赖其来强制执行会话超时。
5. **应**带有"__Host-"前缀并设置"Path=/"。
6. **应**设置"SameSite=Lax"或"SameSite=Strict"。
7. **SHOULD**仅包含不透明字符串(例如会话标识符)，且**SHALL NOT**包含明文个人信息。

5.1.2. 访问令牌

访问令牌(例如OAuth [RFC6749])用于允许应用程序在身份验证事件之后代表订阅者访问一组服务。在没有其他信号的情况下，RP**SHALL NOT**将访问令牌的存在解释为订阅者存在的指示。访问令牌及任何关联的刷新令牌可能在身份验证会话已结束且订阅者已离开应用程序之后很久仍然有效。

5.2. Reauthentication

The periodic reauthentication of sessions **SHALL** be performed to confirm the subscriber's continued presence at an authenticated session (e.g., that the subscriber has not walked away without logging out).

Session management uses two types of timeouts. An *overall timeout* limits the duration of an authenticated session to a specific period following authentication or a previous reauthentication. An *inactivity timeout* terminates a session without activity from the subscriber for a specific period. For both types of timeouts, the RP **MAY** alert the subscriber that the session is about to be terminated and allow the subscriber to make the session active or reauthenticate as appropriate before the session expires. When either timeout expires, the session **SHALL** be terminated. Session activity **SHALL** reset the inactivity timeout, and successful reauthentication during a session **SHALL** reset both timeouts.

The overall and inactivity timeout expiration limits depend on several factors, including the AAL of the session, the environment in which the session is conducted (e.g., whether the subscriber is in a restricted area), the type of endpoint being used (e.g., mobile application, web-based), whether the endpoint is a managed device,[7] and the nature of the application itself. The limits **MAY** also be extended when higher security session maintenance technologies (e.g., device-bound mechanisms) are used. Agencies **SHALL** establish and document the inactivity and overall time limits being enforced in a system security plan, such as that described in [SP800-39]. Detailed requirements for each AAL are given in Sec. 2.1.3, Sec. 2.2.3, and Sec. 2.3.3.

Special considerations apply to session management and reauthentication when using a federation protocol and IdP to authenticate at the RP, as described in [SP800-63C]. The federation protocol communicates an authentication event at the IdP to the RP using an assertion, and the RP then begins an authenticated session based on the successful validation of this assertion. Since the IdP and RP manage sessions separately from each other and the federation protocol does not connect the session management between the IdP and RP, the termination of the subscriber's sessions at an IdP and RP are independent of each other. Likewise, the subscriber's sessions at multiple different RPs are established and terminated independently of each other.

Consequently, when an RP session expires and the RP requires reauthentication, it is possible that the session at the IdP has not expired and that a new assertion could be generated from this session at the IdP without explicitly reauthenticating the subscriber. The IdP can communicate the time and details of the authentication event to the RP, but the RP **SHALL** be authoritative as to whether the reauthentication requirements have

[7] Managed devices include personal computers, laptops, mobile devices, virtual machines, or infrastructure components that are equipped with a management agent that allows information technology staff to discover, maintain, and control them.

5.2. 重新认证

会话的定期重新身份验证**SHALL**被执行，以确认订阅者在已认证会话中的持续存在(例如，订阅者未在未注销的情况下离开)。

会话管理使用两种类型的超时。总体超时将已认证会话的持续时间限制为身份验证或先前重新身份验证之后的特定时间段。不活动超时在订阅者在特定时间段内无活动时终止会话。对于这两种类型的超时，RP**可以**提醒订阅者会话即将终止，并允许订阅者在会话到期之前酌情使会话处于活动状态或重新身份验证。当任一超时到期时，会话**应**被终止。会话活动**应**重置不活动超时，并且会话期间的成功重新身份验证**应**重置两个超时。

总体超时和不活动超时的到期限制取决于多个因素，包括会话的AAL、会话进行的环境(例如，订阅者是否在受限区域)、所使用的端点类型(例如，移动应用、基于Web的)、端点是否为受管理设备[7]，以及应用本身的性质。当使用更高安全性的会话维护技术(例如，设备绑定机制)时，这些限制**可以**延长。机构**应**在系统安全计划(例如[SP800-39]中描述的计划)中建立并记录所强制执行的不活动时间限制和总体时间限制。每个AAL的详细要求见第2.1.3节、第2.2.3节和第2.3.3节。

当在RP处使用联合身份协议和IdP进行身份验证时，会话管理和重新身份验证适用特殊考虑，如[SP800-63C]中所述。联合身份协议使用断言将IdP处的身份验证事件传达给RP，然后RP基于对该断言的成功验证开始已认证会话。由于IdP和RP彼此独立地管理会话，并且联合身份协议不连接IdP和RP之间的会话管理，因此订阅者在IdP和RP处的会话终止彼此独立。同样，订阅者在多个不同RP处的会话彼此独立地建立和终止。

因此，当RP会话过期且RP要求重新身份验证时，IdP处的会话可能尚未过期，并且可以在不显式重新身份验证订阅者的情况下从IdP处的该会话生成新的断言。IdP可以将身份验证事件的时间和详细信息传达给RP，但RP**SHALL**对重新身份验证要求是否

7 受管设备包括配备管理代理的个人计算机、笔记本电脑、移动设备、虚拟机或基础设施组件，该管理代理允许信息技术人员发现、维护和控制它们。

been met. Section 4.7 of [SP800-63C] provides additional details and requirements for session management within a federation context.

5.3. Session Monitoring

Session monitoring (sometimes called *continuous authentication*) is the ongoing evaluation of session characteristics to detect possible fraud during a session. Session monitoring **MAY** be performed by the RP in coordination with the CSP or IdP and associated verifier as a risk reduction measure. When potential fraud is detected during a session, the RP **SHOULD** act in conjunction with the CSP, IdP, or verifier to reauthenticate, terminate the session, or notify appropriate support personnel. Session characteristics that **MAY** be evaluated include:

- Usage patterns, velocity, and timing
- Behavioral biometric characteristics (e.g., typing cadence)
- Device and browser characteristics (e.g., accepted languages)
- Geolocation
- IP address characteristics (e.g., whether the IP address is in a block known for abuse)

Most of these characteristics have privacy implications. Collection, the storage of expected subscriber characteristics, and the processing of session characteristics **SHALL** be included in the privacy risk assessment described in Sec. 7.

Session monitoring **MAY** be facilitated by the use of shared signaling between the RP and CSP or IdP, as described in [SP800-63C].

已满足具有权威性。[SP800-63C]第4.7节提供了联合身份上下文中会话管理的更多细节和要求。

5.3. 会话监控

会话监控(有时称为持续身份验证)是对会话特征的持续评估，以检测会话期间可能的欺诈。会话监控**可以**由RP与CSP或IdP及相关验证器协调执行，作为降低风险的措施。当在会话期间检测到潜在欺诈时，RP**宜**与CSP、IdP或验证器协同行动，以重新身份验证、终止会话或通知适当的支持人员。可以**评估**的会话特征包括：

- 使用模式、速率和时序
- 行为生物特征(例如，打字节奏)
- 设备和浏览器特征(例如，接受的语言)
- 地理位置
- IP地址特征(例如，该IP地址是否位于已知用于滥用的地址块中)

这些特征大多具有隐私影响。预期订阅者特征的收集、存储以及会话特征的处理**SHALL**被纳入Sec.7所述的隐私风险评估中。

会话监控**MAY**通过RP与CSP或IdP之间使用共享信令来促进，如[SP800-63C]所述。

6. Threats and Security Considerations

This section is informative.

6.1. Authenticator Threats

An attacker who can gain control of an authenticator will often be able to masquerade as the authenticator's owner. Threats to authenticators can be categorized based on attacks on the types of authentication factors that comprise the authenticator:

- "Something you know" may be disclosed to an attacker. For example, the attacker may guess a password. If the authenticator is a shared secret, the attacker could access the CSP or verifier and obtain the secret value or perform a dictionary attack on a hash of that value. An attacker may observe the entry of a PIN or passcode, find a written record or journal entry of a PIN or passcode, or install malicious software (e.g., a keyboard logger) to capture the secret. Additionally, an attacker may determine the secret through offline attacks on a password database maintained by the verifier.
- "Something you have" may be lost, damaged, stolen from the owner, or cloned by an attacker. For example, an attacker who gains access to the owner's computer may copy a software authenticator. A hardware authenticator may be stolen, tampered with, or duplicated. Out-of-band secrets may be intercepted by an attacker and used to authenticate their own session. A subscriber may be *socially engineered* to provide access to secrets without intentional collusion.
- "Something you are" may be replicated, or a false match may occur. For example, an attacker may obtain a copy of the subscriber's fingerprint and construct a replica.

Subscribers sometimes intentionally collude with attackers, and virtually nothing can be done from an authentication perspective to prevent these attacks. With this caveat in mind, threats to the authenticators used for digital authentication are listed in Table 3 along with some examples.

Table 3. Authenticator threats

Authenticator Threat/Attack	Description	Examples
Theft	An attacker steals a physical authenticator.	A hardware cryptographic authenticator is stolen.
		An OTP authenticator is stolen.
		A look-up secret authenticator is stolen.

Continued on next page

6. 威胁与安全考量

本节为说明性内容。

6.1. 认证器威胁

能够控制认证器的攻击者通常能够冒充认证器的所有者。对认证器的威胁可以根据对构成认证器的各类身份验证因素的攻击进行分类：

- "你知道的东西"可能会被披露给攻击者。例如，攻击者可能猜出密码。如果认证器是共享密钥，攻击者可能访问 CSP 或验证器并获取该密钥值，或对该值的哈希执行字典攻击。攻击者可能观察到 PIN 或密码的输入，找到 PIN 或密码的书面记录或日志条目，或安装恶意软件(例如键盘记录器)来捕获该密钥。此外，攻击者可能通过对验证器维护的密码数据库进行离线攻击来确定该密钥。
- "你拥有的东西"可能丢失、损坏、被所有者之外的他人窃取或被攻击者克隆。例如，获得所有者计算机访问权的攻击者可能复制软件认证器。硬件认证器可能被盗、篡改或复制。带外密钥可能被攻击者截获并用于对其自己的会话进行身份验证。订阅者可能被社会工程手段诱导，在非故意串通的情况下提供对密钥的访问。
- "你是什么"可能被复制，或者可能发生错误匹配。例如，攻击者可能获取订阅者指纹的副本并构造一个
  副本。

订阅者有时会故意与攻击者串通，从身份验证的角度几乎无法阻止这些攻击。考虑到这一前提，用于数字身份验证的认证器所面临的威胁列于Table 3中，并附有一些示例。

表 3. 认证器威胁

认证器描述威胁/攻击		示例
盗窃	攻击者窃取一个物理 认证器。	硬件密码 认证器被盗。
		OTP 认证器被盗。
		一种查找型密钥认证器是 被盗。

下页续

Continued from previous page

Authenticator Threat/Attack	**Description**	**Examples**
		A cell phone is stolen.
Duplication	The subscriber's authenticator has been copied with or without their knowledge.	Passwords written on paper are disclosed.
		Passwords stored in an electronic file are copied.
		A vulnerability in an insufficiently secure password manager is exploited.
		A software PKI authenticator (i.e., private key) is copied.
		A look-up secret authenticator is copied.
		A counterfeit biometric authenticator is manufactured.
		Exportable cryptographic keys are obtained from a device or cloud-based sync fabric.
Eavesdropping	The attacker observes the authenticator secret or authenticator output as the subscriber is authenticating.	Passwords are obtained by watching keyboard entries.
		Passwords or authenticator outputs are intercepted by keystroke logging software.
		A PIN is captured from a PIN pad device.
		A hashed password is obtained and used by an attacker for another authentication.
	The attacker intercepts an out-of-band secret by compromising the communication channel.	An out-of-band secret is transmitted via unencrypted Wi-Fi and received by the attacker.
Offline Cracking	The authenticator is exposed using analytical methods outside of the authentication mechanism.	A software PKI authenticator is subjected to a dictionary attack to identify the correct password to decrypt the private key.

Continued on next page

续上页

认证器威胁/攻击	**描述**	**示例**
		一部手机被盗。
复制	订阅者的认证器已被复制，无论是否他们的知识。	写在纸上的密码被泄露。
		存储在电子文件中的密码被复制。
		一个安全性不足的密码管理器中的漏洞是被利用。
		一个软件PKI认证器(即私钥)被复制。
		一种查找型密钥认证器是被复制。
		伪造的生物特征认证器被制造出来。
		可导出的加密密钥从设备或基于云的同步结构中获得。
窃听	攻击者观察认证器秘密或认证器输出，当用户正在进行认证时。	密码通过以下方式获得监视键盘输入。
		密码或认证器输出被击键记录软件截获。
		从PIN pad捕获PIN设备。
		攻击者获取哈希后的密码并将其用于另一次身份验证。
	攻击者截获一个超出通过攻破以下内容来泄露 band secret通信信道。	带外秘密被通过未加密的Wi-Fi传输并被攻击者
离线破解	认证器暴露使用认证机制之外的分析方法。	软件PKI认证器被遭受字典攻击以识别正确的密码来解密私钥。

下页续

Continued from previous page

Authenticator Threat/Attack	**Description**	**Examples**
Side-Channel Attack	The authenticator's secret is exposed using the physical characteristics of the authenticator.	A key is extracted by differential power analysis on a hardware cryptographic authenticator.
		A cryptographic authenticator secret is extracted by analyzing the authenticator's response time over several attempts.
Phishing or Pharming	The authenticator output is captured by fooling the claimant into thinking that the attacker is a verifier or RP.	A claimant reveals a password to a website impersonating the verifier.
		A password is revealed by a bank subscriber in response to an email inquiry from a phisher pretending to represent the bank.
		A password is revealed by the claimant at a bogus verifier website reached through DNS spoofing.
Social Engineering	The attacker establishes a level of trust with a subscriber to convince them to reveal their authenticator secret or authenticator output.	A password is revealed by the subscriber to an officemate asking for the password on behalf of the subscriber's boss.
		A password is revealed by a subscriber in a telephone inquiry from an attacker masquerading as a system administrator.
		An attacker who has convinced the mobile operator to redirect the victim's mobile phone to them receives an out-of-band secret sent via SMS.
Authentication Fatigue	An attacker causes repeated authentication requests to be sent to the subscriber in an effort to get them to approve.	A subscriber approves a fraudulent push-based authentication request to stop repeated requests.

Continued on next page

续上页

认证器威胁/攻击	**描述**	**示例**
侧信道攻击	认证器的秘密被利用物理特性认证器。	密钥通过差分对硬件进行功耗分析加密认证器。
		通过分析认证器在多次尝试中的响应时间，提取出加密认证器密钥。
网络钓鱼或域欺骗	认证器输出被通过欺骗声称者捕获 认为攻击者是验证器或 RP。	声称者泄露密码到一个冒充的网站验证器。
		银行订阅者在回应冒充银行代表的钓鱼者发来的电子邮件询问时泄露了密码。
		声称者通过 DNS 到达伪造的验证器网站时泄露了密码。 欺骗。
社会工程	攻击者建立 对用户的信任级别说服他们泄露 他们的认证器密钥或认证器输出。	密码被泄露由订阅者向同事索要密码，代表 订阅者的老板。
		订阅者在冒充系统管理员的攻击者打来的电话询问中泄露了密码。
		攻击者说服移动运营商将受害者的手机重定向到其处，从而接收到通过 SMS 发送的带外密钥。
身份验证疲劳	攻击者导致重复的身份验证请求被 发送给用户，以争取其批准。	订阅者批准一个欺诈性推送式认证请求停止重复请求。

下页续

Continued from previous page

Authenticator Threat/Attack	Description	Examples
Online Guessing	The attacker connects to the verifier online and attempts to guess a valid authenticator output in the context of that verifier.	Online dictionary attacks are used to guess passwords.
		Online guessing is used to guess authenticator outputs for an OTP authenticator that is registered to a legitimate subscriber.
Endpoint Compromise	Malicious code on the endpoint proxies allows remote access to a connected authenticator without the subscriber's consent.	A cryptographic authenticator connected to the endpoint is used to authenticate remote attackers.
	Malicious code on the endpoint causes authentication to other than the intended verifier.	Authentication is performed on behalf of an attacker rather than the subscriber.
		A malicious app on the endpoint reads an out-of-band secret sent via SMS, and the attacker uses the secret to authenticate.
	Malicious code on the endpoint compromises a multi-factor software cryptographic authenticator.	Malicious code proxies authenticate or export authenticator keys from the endpoint.
Unauthorized Binding	An attacker causes an authenticator under their control to be bound to a subscriber account.	An attacker intercepts an authenticator or provisioning key en route to the subscriber.
Latent Keys	A decommissioned device retains authentication keys.	A device (e.g., laptop computer) is sold without recognition that device-based authentication keys are present and could be used by a new owner.

Continued on next page

续上页

认证器 威胁/攻击	描述	示例
在线猜测	攻击者连接到 验证器在线并尝试 在那种情境下猜测一个有效的认证器输出 验证器。	在线字典攻击被用于 猜测密码。
		使用在线猜测来猜测注册到合法订阅者的 OTP 认证器的认证器输出。
端点 泄露	端点上的恶意代码 代理允许远程访问一个 在未经用户同意的情况下连接的认证器。	加密认证器 连接到端点被用于 以认证远程攻击者。
	端点上的恶意代码导致身份验证被 导向非预期的验证器。	认证是以攻击者的名义而非用户的名义执行的。 订阅者。
		端点上的恶意应用读取通过 SMS 发送的带外密钥，攻击者利用该密钥进行身份验证。
	端点上的恶意代码 破坏多因素 软件加密 认证器。	恶意代码代理 进行身份验证或导出 认证器密钥从 端点。
未授权 绑定	攻击者导致一个 认证器在其控制下 绑定到用户 账户。	攻击者拦截一个 认证器或配置 密钥在途中发送给用户。
潜在密钥	已停用的设备保留 身份验证密钥。	设备（例如，笔记本电脑） 在未意识到存在基于设备的身份验证密钥且可能被新所有者使用的情况下被出售。

下页续

Continued from previous page

Authenticator Threat/Attack	Description	Examples
Proliferation of Keys	Transferring device-based authentication keys between devices increases the attack surface.	A subscriber copies authentication keys to many devices, possibly some that are not under their direct control, and loses track of where the keys are stored.
Key Transfer Security	Authentication keys are transferred between devices through an insufficiently secure cloud service.	Access to a cloud service that stores authentication keys requires only single-factor authentication.
		Keys are made available to others through a URL sent via email.
Untrusted Devices	Authentication keys are resident on a device that provides insufficient protection.	Keys are transferred to an insecure device via the sync fabric.
Insider Threats	A trusted insider proves to be untrustworthy.	An insider with access to the CSP (e.g., customer support representative) colludes with an attacker to give access to subscriber accounts.

6.2. Threat Mitigation Strategies

Table 4 summarizes related mechanisms that assist in mitigating the threats described in Table 3.

Table 4. Mitigating authenticator threats

Authenticator Threat/Attack	Threat Mitigation Mechanisms	Normative Reference Sections
Theft	Use multi-factor authenticators that must be activated through a password or biometric.	2.2.1, 2.3.1
	Use a combination of authenticators that includes a password or biometric.	2.2.1, 2.3.1

Continued on next page

续上页

认证器 威胁/攻击	描述	示例
扩散 密钥	转移基于设备的 身份验证密钥在 设备增加了攻击 表面。	订阅者复制 身份验证密钥到许多 设备，可能包括一些不在其直接控 制下的设备，并失去对密钥存储位 置的追踪。
密钥传输 安全	身份验证密钥是 在设备之间转移 通过不够安全的 云服务。	访问云服务， 存储身份验证密钥 仅需单因素 身份验证。
		密钥通过电子邮件发送的 URL 提供
不可信设备	身份验证密钥驻留 在提供 保护不足。	密钥被转移到 通过同步的不安全设备 架构的设备上。
内部威胁	受信任的内部人员被证明是 不可信的。	有权访问 CSP(例如客户支持代表)与攻 击者串通，授予对订阅者账户 的访问权限。

6.2. 威胁缓解策略

表 4总结了有助于缓解表 3中所述威胁的相关机制。

表 4.缓解认证器威胁

认证器 威胁/攻击	威胁缓解机制	规范性引用章节
盗窃	使用多因素认证器 必须通过密码或生物识别激活。	2.2.1 , 2.3.1
	使用以下各项的组合： 包括密码或生物特征的认证器。	2.2.1 , 2.3.1

下页续

Continued from previous page

Authenticator Threat/Attack	Threat Mitigation Mechanisms	Normative Reference Sections
Duplication	Use authenticators from which it is difficult to extract and duplicate long-term authentication secrets.	2.2.2, 2.3.2, 3.1.6.1
	Enforce AAL2 requirements for access to sync fabrics that contain exported authentication keys, and only allow them to be imported into trusted devices.	3.1.7.1
Eavesdropping	Ensure the endpoint's security before use, especially with respect to freedom from malware (e.g., key loggers).	2.2.2
	Avoid using unauthenticated and unencrypted communication channels to send out-of-band authenticator secrets.	3.1.3.1
	Authenticate over authenticated protected channels (e.g., observe the lock icon in the browser window).	2.1.2, 2.2.2, 2.3.2
	Use authentication protocols that are resistant to replay attacks (e.g., *pass-the-hash*).	3.2.7
	Use authentication endpoints that employ trusted input and display capabilities.	3.1.6.1, 3.1.7.1
Offline Cracking	Use an authenticator with a high entropy authenticator secret.	3.1.2.1, 3.1.4.1, 3.1.5.1, 3.1.6.1, 3.1.7.1
	Store centrally verified passwords in a salted, hashed form, including a keyed hash.	3.1.1.1.2
Side-Channel Attack	Use authenticator algorithms that maintain constant power consumption and timing, regardless of secret values.	2.3.2
Phishing or Pharming	Use authenticators that provide phishing resistance.	3.2.5

Continued on next page

续上页

认证器威胁/攻击	威胁缓解机制规范性参考章节	
复制	使用从中获取的认证器 很难提取和复制长期认证密钥。	2.2.2, 2.3.2, 3.1.6.1
	对以下各项强制执行 AAL2 要求： 限制对包含已导出认证密钥的同步 结构的访问，并仅允许将其导入受 信任的设备。	3.1.7.1
窃听	确保端点的安全 使用前，尤其是确保其不受恶意软 件(例如键盘记录器)影响。	2.2.2
	避免使用未认证的和 未加密的通信渠道发送带外认证器密 钥。	3.1.3.1
	通过已认证通道进行认证 受保护通道(例如，观察浏览器窗口中 的锁形图标)。	2.1.2, 2.2.2, 2.3.2
	使用认证协议，这些协议 可抵御重放攻击（如传递哈希）。	3.2.7
	使用认证端点 采用可信输入和显示功能。	3.1.6.1, 3.1.7.1
离线破解	使用具有高 熵认证器密钥。	3.1.2.1, 3.1.4.1, 3.1.5.1, 3.1.6.1, 3.1.7.1
	集中存储经过验证的密码 以加盐哈希形式，包括带密钥哈希。	3.1.1.1.2
侧信道 攻击	使用认证器算法 无论秘密值如何，均保持恒定 功耗和时序。	2.3.2
网络钓鱼或 域欺骗	使用能够提供 抗钓鱼性。	3.2.5

下页续

Continued from previous page

Authenticator Threat/Attack	Threat Mitigation Mechanisms	Normative Reference Sections
Social Engineering	Avoid using authenticators that present a social engineering risk to third parties (e.g., customer service agents).	4.1.2.1, 4.2
Authentication Fatigue	Require the transfer of an authentication secret for OOB authentication rather than approval.	3.1.3
Online Guessing	Use authenticators that generate high-entropy output.	3.1.2.1, 3.1.6.1, 3.1.7.1
	Use an authenticator that locks after repeated failed activation attempts.	3.2.2
Endpoint Compromise	Use hardware authenticators that require physical action by the claimant.	3.2.8
	Maintain software-based keys in storage with restricted access.	3.1.3.1, 3.1.6.1, 3.1.7.1, 3.2.13
Unauthorized Binding	Provision authenticators and associated keys using authenticated protected channels or in person.	4.1
Latent Keys	Ensure the secure disposal of equipment that contains device-based authentication keys.	4.4, 4.5
	In federal enterprise applications, limit the transfer of keys to organizationally managed or trusted devices.	B.2
Key Transfer Security	Encourage or require subscribers to use cloud services that have been approved for key storage and transfer.	B.2

Several other strategies may be applied to mitigate the threats described in Table 4:

- *Multiple factors* make successful attacks more difficult to accomplish. If an attacker must steal a cryptographic authenticator and guess a password, then the work to discover both factors may be too high.

续上页

认证器威胁/攻击	威胁缓解机制规范性参考章节	
社会工程	避免使用以下认证器： 对第三方(例如客服人员)构成社会工程 风险。	4.1.2.1, 4.2
身份验证 疲劳	要求转移 用于OOB认证的认证密钥，而非 批准。	3.1.3
在线猜测	使用生成型认证器 高熵输出。	3.1.2.1, 3.1.6.1, 3.1.7.1
	使用会锁定的认证器 在多次激活失败后 尝试。	3.2.2
端点 泄露	使用硬件认证器，其 要求采取物理操作，由 声称者。	3.2.8
	将基于软件的密钥保存在访问受限的 存储中。	3.1.3.1, 3.1.6.1, 3.1.7.1, 3.2.13
未授权 绑定	配置认证器 并使用经过认证的保护通道或当面 交付相关密钥。	4.1
潜在密钥	确保安全处置 包含基于设备的认证密钥的设备。	4.4, 4.5
	在联邦企业应用中， 将密钥的传输限制在组织管理 或受信任的设备上。	B.2
密钥传输 安全	鼓励或要求用户 使用已获准用于密钥存储和传输 的云服务。	B.2

可采用若干其他策略来缓解表4中描述的威胁：

- 多因素使成功攻击更难实现。如果攻击者必须窃取加密认证器并猜测密码，那么发现这两个因素的工作量可能过高。

- *Physical security mechanisms* may be employed to protect a stolen authenticator from duplication. Physical security mechanisms can provide tamper evidence, detection, and response.
- *Requiring long passwords* that do not appear in common dictionaries may force attackers to try every possible value.
- *System and network security controls* may be employed to prevent an attacker from gaining access to a system or installing malicious software.
- *Periodic training* may be performed to ensure that subscribers understand when and how to report a compromise or a suspicion of compromise and to recognize patterns of behavior that may signify that an attacker is attempting to compromise the authentication process.
- *Out-of-band techniques* may be employed to verify the proof of possession of registered devices (e.g., cell phones).

6.3. Authenticator Recovery

The weak point in many authentication mechanisms is the process followed when a subscriber loses control of one or more authenticators and needs to replace them. In many cases, the options for authenticating the subscriber are limited, and economic concerns (e.g., the cost of maintaining call centers) motivate the use of inexpensive and often less secure backup authentication methods. To the extent that authenticator recovery is human-assisted, social engineering attacks also pose risks.

To maintain the integrity of the authentication factors, it is essential that one authentication factor cannot be leveraged to obtain an authenticator of a different factor. For example, a password must not be usable to obtain a new list of look-up secrets.

6.4. Session Attacks

Hijacking attacks on the session following an authentication event can have similar security impacts. The session management guidelines in Sec. 5 are essential to maintaining session integrity against attacks (e.g., XSS). It is also important to sanitize all information to be displayed [OWASP-XSS-prevention] to ensure that it does not contain executable content. These guidelines recommend that session secrets be made inaccessible to mobile code to provide extra protection against the exfiltration of session secrets.

Another post-authentication threat is CSRF, which takes advantage of users' tendency to have multiple sessions active simultaneously. It is essential to embed and verify a session identifier for web requests to prevent a valid URL or request from being unintentionally or maliciously activated.

- 物理安全机制可用于保护被盗认证器免遭复制。物理安全机制可提供篡改证据、检测和响应。
- 要求使用长密码且不出现在常见词典中，可能迫使攻击者尝试每一个可能的值。
- 系统和网络安全控制可用于防止攻击者获得系统访问权限或安装恶意软件。
- 定期培训可确保订阅者了解何时以及如何报告泄露或疑似泄露，并识别可能表明攻击者正试图破坏身份验证过程的行为模式。
- 带外技术可用于验证对已注册设备(例如手机)的持有证明。

6.3. 认证器恢复

许多身份验证机制的薄弱环节在于订阅者失去对一个或多个认证器的控制并需要更换它们时所遵循的流程。在许多情况下，用于对订阅者进行身份验证的选项有限，而经济方面的考虑(例如维护呼叫中心的成本)促使人们采用廉价且通常安全性较低的备用身份验证方法。在认证器恢复由人工协助的范围内，社会工程攻击也构成风险。

为维护身份验证因素的完整性，至关重要的是，一个身份验证因素不能被用来获取不同因素的认证器。例如，密码不得被用来获取新的查询性秘密列表。

6.4. 会话攻击

认证事件后对会话的劫持攻击也可能产生类似的安全影响。第5节中的会话管理指南对于维护会话完整性、抵御攻击(例如XSS)至关重要。同样重要的是，对所有将要显示的信息进行净化处理[OWASP-XSS-prevention]，以确保其不包含可执行内容。这些指南建议使会话机密对移动代码不可访问，以提供额外保护，防止会话机密被窃取。

另一种身份验证后的威胁是 CSRF，它利用用户倾向于同时激活多个会话的特点。为 Web 请求嵌入并验证会话标识符至关重要，以防止有效 URL 或请求被无意或恶意激活。

7. Privacy Considerations

This section is informative.

7.1. Privacy Risk Assessment

The authentication requirements in Sec. 2 and the optional session monitoring guidelines in Sec. 5.3 require the CSP to conduct a privacy risk assessment for records retention. Such a privacy risk assessment would include evaluating:

- The likelihood that the records retention could create a privacy problem for the subscriber, such as loss of trust
- The impact if such a problem did occur

CSPs should be able to reasonably justify any response to identified privacy risks, including accepting, mitigating, and sharing the risk. Subscriber consent is a form of sharing the risk and is, therefore, only appropriate when a subscriber could reasonably be expected to have the capacity to assess and accept the shared risk.

7.2. Privacy Controls

Section 2.4.3 requires CSPs to employ appropriately tailored privacy controls. [SP800-53] provides a set of privacy controls for CSPs to consider when deploying authentication mechanisms, including notices, redress, and other important considerations for successful and trustworthy deployments.

7.3. Use Limitation

Section 2.4.3 requires CSPs to maintain the objectives of predictability (i.e., enabling reliable assumptions by individuals, owners, and operators about personal information and its processing by an information system) and manageability (providing the capability for the granular administration of personal information, including alteration, deletion, and selective disclosure) commensurate with privacy risks that can arise from processing attributes for purposes other than identity proofing, authentication, authorization, attribute assertion, or related fraud mitigation or compliance with laws or legal processes [NISTIR8062].

CSPs may have various business purposes for processing attributes, including providing non-identity services to subscribers. However, processing attributes for purposes other than those specified at collection can create privacy risks. CSPs can identify appropriate measures that are commensurate with the privacy risks that arise from additional processing. For example, absent applicable laws, regulations, or policies, obtaining consent may not be necessary when processing attributes to provide non-identity services requested by subscribers. However, notices may help subscribers maintain reliable assumptions about the processing (i.e., predictability). Other

7. 隐私考量

本节为说明性内容。

7.1. 隐私风险评估

第 2 节中的身份验证要求以及第 5.3 节中的可选会话监控指南要求 CSP 对记录保留进行隐私风险评估。此类隐私风险评估将包括评估：

- 记录保留可能给订阅者造成隐私问题(例如失去信任)的可能性
- 如果确实发生此类问题所造成的影响

CSP 应能够合理地为针对已识别隐私风险的任何应对措施提供依据，包括接受、缓解和分担风险。订阅者同意是分担风险的一种形式，因此，只有在可以合理预期订阅者具备评估和接受所分担风险的能力时，才适合采用。

7.2. 隐私控制

第 2.4.3 节要求 CSP 采用适当定制的隐私控制措施。[SP800-53]提供了一组隐私控制措施，供 CSP 在部署身份验证机制时考虑，包括通知、补救以及其他对成功且可信部署的重要考虑事项。

7.3. 使用限制

第2.4.3节要求CSP维护可预测性目标(即，使个人、所有者和运营者能够对个人信息及其由信息系统处理的情况作出可靠假设)和可管理性目标(提供对个人信息进行细粒度管理的能力，包括更改、删除和选择性披露)，并与因将属性用于身份核验、身份验证、授权、属性断言或相关欺诈缓解或遵守法律或法律程序以外的目的而产生的隐私风险相称[NISTIR8062]。

CSP处理属性可能有多种业务目的，包括向订阅者提供非身份服务。然而，将属性用于收集时指定目的以外的目的可能会带来隐私风险。CSP可以确定与额外处理所产生的隐私风险相称的适当措施。例如，在缺乏适用法律、法规或政策的情况下，当处理属性以提供订阅者请求的非身份服务时，获得同意可能并非必要。然而，通知可能有助于订阅者维持对处理情况的可靠假设(即可预测性)。其他

processing of attributes may carry different privacy risks that call for obtaining consent or allowing subscribers more control over the use or disclosure of specific attributes (i.e., manageability). Subscriber consent must be meaningful. Therefore, as stated in Sec. 2.4.3, when CSPs use consent measures, the subscriber's acceptance of additional uses shall not be a condition of providing authentication services.

Consult the SAOP if there are questions about whether the proposed processing falls outside of the scope of the permitted processing or appropriate privacy risk mitigation measures.

7.4. Agency-Specific Privacy Compliance

Section 2.4.3 describes specific compliance obligations for federal CSPs. It is critical to involve the SAOP in the earliest stages of digital authentication system development to assess and mitigate privacy risks and advise the agency on compliance requirements, such as whether or not the collection of personal information to issue or maintain authenticators triggers the *Privacy Act of 1974* [PrivacyAct] or the *E-Government Act of 2002* [E-Gov] requirement to conduct a PIA. For example, concerning the centralized maintenance of biometrics, Privacy Act requirements will likely be triggered and require coverage by a new or existing Privacy Act SORN due to the collection and maintenance of personal information and any other attributes that are necessary for authentication. The SAOP can similarly assist the agency in determining whether a PIA is required. These considerations should not be read as a requirement to develop a Privacy Act SORN or PIA for authentication alone. In many instances, a PIA and SORN can encompass the entire digital identity process or include the digital authentication process as part of a larger programmatic PIA that discusses the online services or benefits that the agency is establishing.

Due to the many components of digital authentication, the SAOP needs to be aware of and understand each component. For example, other privacy artifacts may apply to an agency that offers or uses federated CSP or RP services (e.g., Data Use Agreements, Computer Matching Agreements). The SAOP can assist the agency in determining what additional requirements apply. Moreover, a thorough understanding of the individual components of digital authentication will enable the SAOP to assess and mitigate privacy risks through compliance processes or other means.

属性的处理可能带来不同的隐私风险，需要获取同意或允许订阅者对特定属性的使用或披露拥有更多控制权(即可管理性)。订阅者同意必须是有意义的。因此，如第 2.4.3 节所述，当 CSP 使用同意措施时，订阅者对额外用途的接受不得作为提供身份验证服务的条件。

如果对拟议的处理是否超出允许处理的范围或适当的隐私风险缓解措施有疑问，请咨询SAOP。

7.4. 机构特定的隐私合规

第2.4.3节描述了联邦CSP的具体合规义务。在数字身份验证系统开发的最早阶段就让SAOP参与至关重要，以评估和缓解隐私风险，并就合规要求向机构提供建议，例如为签发或维护认证器而收集个人信息是否会触发*1974*年《隐私法》[Privacy Act]或*2002*年《电子政务法》[E-Gov]中开展PIA的要求。例如，就生物特征的集中维护而言，由于收集和维护个人信息以及身份验证所需的任何其他属性，很可能触发《隐私法》要求，并需要由新的或现有的《隐私法》SORN予以覆盖。SAOP同样可以协助机构确定是否需要PIA。这些考虑不应被解读为要求仅为身份验证制定《隐私法》SORN或PIA。在许多情况下，PIA和SORN可以涵盖整个数字身份流程，或者将数字身份验证流程作为讨论机构正在建立的在线服务或福利的更大项目性PIA的一部分纳入其中。

由于数字身份验证包含许多组成部分，SAOP需要了解并理解每个组成部分。例如，其他隐私工件可能适用于提供或使用联合CSP或RP服务的机构(例如，数据使用协议、计算机匹配协议)。SAOP可以协助机构确定适用哪些额外要求。此外，透彻理解数字身份验证的各个组成部分将使SAOP能够通过合规流程或其他方式评估和缓解隐私风险。

8. Customer Experience Considerations

This section is informative.

To align with the standard terminology of user-centered design, customer experience, and usability, the term “user” is used throughout this section to refer to the human party. In most cases, the user in question will be the subject in the role of applicant, claimant, or subscriber. Customer experience sits at the nexus of usability, accessibility, and optionality. Considering user needs allows organizations to provide responsive and secure identity solutions while minimizing unnecessary friction and frustration.

8.1. Usability

[ISO/IEC9241-11] defines usability as the “extent to which a system, product, or service can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use.” This definition focuses on users, their goals, and the contexts of use as the key elements necessary for achieving effectiveness, efficiency, satisfaction, and usability.

A user’s goal when accessing an information system is to perform an intended task. Authentication is the function that enables this goal. However, from the user’s perspective, authentication stands between them and their intended task. Effective design and implementation of the authentication process makes it easy to do the right thing, hard to do the wrong thing, and easy to recover if the wrong thing happens.

Organizations need to be cognizant of the overall implications of their stakeholders’ entire digital authentication ecosystem. Users often employ multiple authenticators, each for a different RP. They then struggle to remember passwords, recall which authenticator goes with which RP, and carry multiple physical authentication devices. Evaluating the usability of authentication is critical, as poor usability often results in coping mechanisms and unintended workarounds that can ultimately degrade the effectiveness of security controls.

Integrating usability into the development process can lead to authentication solutions that are secure and usable while still addressing users’ authentication needs and organizations’ business goals. The impacts of usability across digital systems needs to be considered as part of the risk assessment when deciding on the appropriate AAL. Authenticators with a higher AAL sometimes offer better usability and should be allowed for use with lower AAL applications.

Leveraging federation for authentication can alleviate many usability issues, though such an approach has its trade-offs, as discussed in [SP800-63C].

This section provides general usability considerations and possible implementations but does not recommend specific solutions. The implementations mentioned are examples that encourage innovative technological approaches to address specific usability

8. 客户体验考量

本节为说明性内容。

为与以用户为中心的设计、客户体验和可用性的标准术语保持一致，本节通篇使用“用户”一词来指代人的一方。在大多数情况下，所讨论的用户将是处于申请人、声称者或订阅者角色的主体。客户体验处于可用性、可访问性和可选性的交汇点。考虑用户需求使组织能够提供响应迅速且安全的身份解决方案，同时最大限度地减少不必要的摩擦和挫败感。

8.1. 可用性

[ISO/IEC9241-11]将可用性定义为“特定用户在特定使用情境中，以有效性、效率和满意度实现特定目标的程度”。该定义将用户、其目标以及使用情境作为实现有效性、效率、满意度和可用性所必需的关键要素。

用户访问信息系统时的目标是执行某项预期任务。身份验证是实现该目标的功能。然而，从用户的角度来看，身份验证横亘在他们与其预期任务之间。身份验证流程的有效设计与实施使做正确的事变得容易，使做错误的事变得困难，并且在发生错误时易于恢复。

组织需要认识到其利益相关者整个数字身份验证生态系统的整体影响。用户经常使用多个认证器，每个用于不同的 RP。然后他们难以记住密码、回忆哪个认证器对应哪个 RP，并携带多个物理身份验证设备。评估身份验证的可用性至关重要，因为糟糕的可用性往往导致应对机制和意外的变通方法，最终可能降低安全控制的有效性。

将可用性融入开发过程可以产生既安全又可用、同时仍能满足用户身份验证需求和组织业务目标的身份验证解决方案。在决定适当的 AAL 时，需要将可用性对数字系统的影响作为风险评估的一部分加以考虑。具有较高 AAL 的认证器有时提供更好的可用性，应允许其用于较低 AAL 的应用。

利用联合身份进行身份验证可以缓解许多可用性问题，不过这种方法有其权衡，如[SP800-63C]中所讨论。

本节提供一般性可用性考虑和可能的实现方式，但不推荐具体解决方案。所提及的实现方式是示例，鼓励采用创新技术方法来解决特定的可用性

needs. Furthermore, usability considerations and their implementations are sensitive to many factors that prevent a one-size-fits-all solution. For example, a font size that works in a desktop computing environment may force text to scroll off of a small OTP authenticator screen. Performing a usability evaluation on the selected authenticator is a critical component of implementation. It is important to conduct evaluations with representative users, set realistic goals and tasks, and identify appropriate contexts of use.

Guidelines and considerations are described from the users' perspective.

Section 508 of the Rehabilitation Act of 1973 [Section508] was enacted to eliminate barriers in information technology and require federal agencies to make electronic and information technology accessible to people with disabilities. While these guidelines do not directly assert requirements from Section 508, identity service providers are expected to comply with Section 508 provisions. Beyond compliance with Section 508, federal agencies and their service providers are generally expected to design services and systems with the experiences of people with disabilities in mind to ensure that accessibility is prioritized throughout identity system life cycles.

8.1.1. Common Usability Considerations for Authenticators

When selecting and implementing an authentication system, consider usability across the entire lifetime of the selected authenticators (e.g., their typical use and intermittent events) while being mindful of users, their goals, and their contexts of use.

A single authenticator type does not usually suffice for the entire user population. Therefore, whenever possible and based on AAL requirements, CSPs should support alternative authenticator types and allow users to choose the type that best meets their needs. Task immediacy, perceived cost-benefit trade-offs, and unfamiliarity with certain authenticators often impact choices. Users tend to choose options that incur the least burden or cost at that moment. For example, if a task requires immediate access to an information system, a user may prefer to create a new subscriber account and password rather than select an authenticator that requires more steps. Alternatively, users may choose a federated identity option that is approved at the appropriate IAL, AAL, and *federation assurance level* (FAL) if they already have a subscriber account with an identity provider. Users may understand some authenticators better than others and have different levels of trust based on their understanding and experience.

Positive user authentication experiences are integral to achieving desired business outcomes. Therefore, organizations should strive to consider authenticators from the users' perspective. The overarching authentication usability goal is to minimize user burden and authentication friction (e.g., the number of times a user has to authenticate, the steps involved, the amount of information they have to track). *Single sign-on* (SSO) exemplifies one such minimization strategy.

Usability considerations that are applicable to most authenticators include the following:

需求。此外，可用性考量及其实施对许多因素敏感，这些因素阻碍了一刀切的解决方案。例如，在桌面计算环境中有效的字体大小可能会迫使文本滚动到小型 OTP 认证器屏幕之外。对所选认证器进行可用性评估是实施的关键组成部分。重要的是与有代表性的用户进行评估，设定现实的目标和任务，并确定适当的使用情境。

指南和注意事项是从用户的角度进行描述的。

1973 年《康复法案》第 508 条[Section508]的颁布旨在消除信息技术中的障碍，并要求联邦机构使电子和信息技术对残疾人可访问。虽然这些指南并未直接主张第 508 条的要求，但身份服务提供商应遵守第 508 条的规定。除了遵守第 508 条之外，联邦机构及其服务提供商通常应在设计服务和系统时考虑到残疾人的体验，以确保在整个身份系统生命周期中优先考虑可访问性。

8.1.1. 认证器的通用可用性考量

在选择和实施身份验证系统时，应考虑所选认证器整个生命周期内的可用性(例如其典型使用和间歇性事件)，同时留意用户、其目标及其使用情境。

单一认证器类型通常不足以满足整个用户群体的需求。因此，在可能的情况下并基于 AAL 要求，CSP 应支持替代认证器类型，并允许用户选择最符合其需求的类型。任务紧迫性、感知的成本效益权衡以及对某些认证器的不熟悉往往会影响选择。用户倾向于选择在那一刻产生最少负担或成本的选项。例如，如果任务需要立即访问信息系统，用户可能更愿意创建新的订阅者账户和密码，而不是选择需要更多步骤的认证器。或者，如果用户已经在身份提供方处拥有订阅者账户，他们可能会选择在适当的 IAL、AAL 和联合保证等级(FAL) 下获得批准的联合身份选项。用户可能对某些认证器的理解优于其他认证器，并基于他们的理解和经验具有不同水平的信任。

积极的用户身份验证体验是实现预期业务成果不可或缺的一部分。因此，组织应努力从用户的角度考虑认证器。总体身份验证可用性目标是最小化用户负担和身份验证摩擦(例如用户必须进行身份验证的次数、涉及的步骤、必须跟踪的信息量)。单点登录(SSO)就是这种最小化策略的一个例证。

适用于大多数认证器的可用性考虑包括以下内容：

- Provide information on the use and maintenance of the authenticator (e.g., what to do if the authenticator is lost or stolen) and instructions for use, especially if there are different requirements for first-time use or initialization.
- Users will need to remember to have their authenticator readily available. Consider the need for alternative authentication options to protect against loss, damage, or other negative impacts on the original authenticator and the potential loss of battery power, if applicable.
- Alternative authentication options based on AAL requirements allow users to choose an authenticator based on their context, goals, and tasks (e.g., the frequency and immediacy of the task). Alternative authentication options also help address availability issues that may occur with a particular authenticator.
- Consider the characteristics of user-facing text:
  - Write user-facing text (e.g., instructions, prompts, notifications, error messages) in plain language for the intended audience. Avoid technical jargon, and write for the audience's expected literacy level.
  - Consider the legibility of user-facing and user-entered text, including font style, size, color, and contrast with the surrounding background. Illegible text contributes to user entry errors. To enhance legibility, consider the use of:
    * High contrast (i.e., black on white)
    * Sans serif fonts for electronic displays and serif fonts for printed materials
    * Fonts that clearly distinguish between characters that are easily confused (e.g., the capital letter "O" and the number zero "0")
    * A minimum font size of 12 points as long as the text fits for display on the device
  - Avoid using icons (e.g., padlocks or shields) that might be confused with security indicators in browsers.
- Consider user experience during authenticator entry:
  - Offer the option to display text during entry, as masked text entry is error-prone. Once a given character is displayed long enough for the user to see, it can be hidden. Consider the device when determining masking delay time, as it takes longer to enter passwords on mobile devices (e.g., tablets and smartphones) than on traditional desktop computers. Ensure that masking delay durations are consistent with user needs.
  - Ensure that the time allowed for text entry is adequate (i.e., the entry screen does not time out prematurely). Ensure that the allowed text entry times are consistent with user needs.

- 提供关于认证器使用和维护的信息(例如，认证器丢失或被盗时该怎么做)以及使用说明，特别是当首次使用或初始化有不同要求时。
- 用户需要记得将认证器放在随手可取的地方。考虑需要替代身份验证选项，以防原认证器丢失、损坏或其他负面影响，以及可能出现的电池电量耗尽(如适用)。
- 基于AAL要求的替代身份验证选项允许用户根据其情境、目标和任务(例如，任务的频率和即时性)选择认证器。替代身份验证选项还有助于解决特定认证器可能出现的可用性问题。
- 考虑面向用户的文本的特征：
  - -以目标受众易于理解的语言编写面向用户的文本(例如，说明、提示、通知、错误消息)。避免使用技术术语，并按照受众的预期识字水平编写。
  - -考虑面向用户和用户输入文本的易读性，包括字体样式、大小、颜色以及与周围背景的对比度。不可读的文本会导致用户输入错误。为增强易读性，考虑使用：
    * 高对比度(即，黑底白)
    * Sansserif字体用于电子显示屏以及serif字体用于印刷材料
    * 字体应清晰区分容易混淆的字符(例如大写字母"O"和数字零"0")
    * 最小字体大小为12点,只要文本能够适应设备显示即可在设备上
  - -避免使用可能被混淆的图标(例如，挂锁或盾牌)浏览器中的安全指示器。
- 在认证器录入过程中考虑用户体验：
  - -提供在输入期间显示文本的选项，因为掩码文本输入容易出错。一旦给定字符显示足够长时间供用户看到，就可以将其隐藏。在确定掩码延迟时间时考虑设备因素，因为在移动设备(例如，平板电脑和智能手机)上输入密码比在传统台式计算机上花费的时间更长。确保掩码延迟时长与用户需求一致。
  - -确保允许的文本输入时间充足(即，输入屏幕不会过早超时)。确保允许的文本输入时间与用户需求一致。

  - Provide clear, meaningful, and actionable feedback on entry errors to reduce user confusion and frustration. Significant usability implications arise when users have no way of knowing that they have entered text incorrectly.
  - Allow at least 10 entry attempts for authenticators that require the entry of the authenticator output by the user. The longer and more complex the entry text, the greater the likelihood of user entry errors.
  - Provide clear, meaningful feedback on the number of remaining allowed attempts. For rate limiting (i.e., throttling), inform users how long they have to wait until the next attempt.
- Minimize the impact of form-factor constraints, such as limited touch and display areas on mobile devices:
  - Larger touch areas improve usability for text entry since typing on small devices is significantly more error-prone and time-consuming than typing on a full-size keyboard due to the size of the input mechanism (e.g., a finger) relative to the size of the on-screen target.
  - Follow good user interface and information design for small displays.

Usability considerations for intermittent events (e.g., reauthentication, subscriber account lockout, expiration, revocation, damage, loss, theft, non-functional software) across authenticator types include the following:

- Prompt users to perform some activity just before (e.g., two minutes before) an inactivity timeout would otherwise occur.
- Prompt users to save their work before a fixed reauthentication timeout occurs, regardless of user activity.
- Clearly communicate how and where to acquire technical assistance (e.g., provide users with a link to an online self-service feature, chat sessions, or a phone number for help desk support). Ideally, sufficient information can be provided to enable users to recover from intermittent events on their own without outside intervention.
- Provide an accessible means for the subscriber to end their session (i.e., logoff).

Subsequent sections describe usability considerations specific to a particular authenticator.

8.1.2. Usability Considerations by Authenticator Type

The following sections describe other usability considerations that are specific to particular authenticator types.

-对输入错误提供清晰、有意义且可操作的反馈，以减少
用户困惑和挫败感。当用户无法知道自己输入了错误文本时，会产生重大的可用性影响。-对于需要用户输入认证器输出的认证器，允许至少10次输入尝试。

用户输出的认证器。输入的文本越长、越复杂，用户输入出错的可能性就越大。

-对剩余允许尝试次数提供清晰、有意义的反馈。
对于速率限制(即，节流)，告知用户需要等待多长时间才能进行下一次尝试。

• 尽量减少外形尺寸限制的影响，例如移动设备上有限的触摸和显示区域：

– 更大的触摸区域可提升文本输入的可用性，因为在小型设备上打字
由于输入机制（例如手指）相对于屏幕上目标的大小，在移动设备上输入比在全尺寸键盘上打字更容易出错且更耗时。

-为小屏幕遵循良好的用户界面和信息设计。

针对间歇性事件（例如重新身份验证、订阅者账户锁定、过期、撤销、损坏、丢失、被盗、软件无法运行）的可用性考量，跨各类认证器包括以下内容：

• 在固定重新身份验证超时发生之前提示用户保存其工作，无论用户活动如何。

• 提示用户在固定的重新身份验证超时前保存工作，无论用户活动如何。

• 清晰传达如何以及在何处获取技术支持（例如，向用户提供在线自助服务功能的链接、聊天会话或帮助台支持的电话号码）。理想情况下，应提供足够的信息，使用户能够在无需外部干预的情况下自行从间歇性事件中恢复。

• 为用户提供可访问的方式以结束其会话(即注销)。后续章节描述特定认证器的可用性考虑。

8.1.2. 按认证器类型划分的可用性考量

以下各节描述了特定认证器类型所特有的其他可用性考虑因素。

8.1.2.1. Passwords

Typical Usage

Users often manually input the password (sometimes referred to as a passphrase or PIN). Alternatively, they may use a password manager to select a secure password and maintain distinct passwords for each authenticated service. The use of distinct passwords is important to avoid "password stuffing" attacks in which an attacker uses a compromised password from one site to access the user's account on other sites. Agencies should carefully evaluate password managers before making recommendations or mandates to confirm that they meet expectations for secure implementation.

Usability considerations for typical usage without a password manager include:

- Memorability of the password
  - The likelihood of a recall failure increases if there are more items for users to remember. With fewer passwords, users can more easily recall the specific password needed for a particular RP.
  - The memory burden is greater for a less frequently used password.

Usability considerations for typical usage with a password manager include:

- Ease of entry
  - Support autofill functionality to allow for the safe retrieval of secrets from password managers.
  - Support copy and paste functionality in fields for entering passwords, including passphrases.

Intermittent Events

Usability considerations for intermittent events include:

- When users create and change passwords
  - Clearly communicate information on how to create and change passwords.
  - Clearly communicate password requirements, as specified in Sec. 3.1.1.
  - Allow at least 64 characters in length to support the use of passphrases. Encourage users to make passwords as lengthy as they want and use any characters that they like (including spaces) to aid memorization. Ensure that user interfaces support sufficient password lengths.
  - Do not impose other composition rules (e.g., mixtures of different character types) on passwords.

8.1.2.1. 密码

典型用法

用户通常手动输入密码(有时称为口令或 PIN)。或者，他们可能使用密码管理器来选择安全密码，并为每个已认证服务维护不同的密码。使用不同的密码对于避免"密码填充"攻击很重要，在这种攻击中，攻击者使用从一个站点泄露的密码来访问用户在其他站点上的账户。机构在提出建议或强制要求之前，应仔细评估密码管理器，以确认其符合安全实施的期望。

在没有密码管理器的情况下，典型使用的可用性考虑包括：

• 密码的记忆性

-如果用户需要记忆的项目越多，回忆失败的可能性就越大。
密码越少，用户就越容易回忆起特定 RP 所需的具体密码。

-对于使用频率较低的密码，记忆负担更大。

使用密码管理器进行典型使用的可用性考虑包括：

• 易于录入

-支持自动填充功能，以便从……安全检索密钥
密码管理器。

-在密码输入字段中支持复制和粘贴功能，
包括口令短语。

间歇性事件

间歇性事件的可用性考虑包括：

• 当用户创建和更改密码时

-清晰传达有关如何创建和更改密码的信息。-清晰传达密码要求，如Sec.3.1.1所规定。-允许至少 64 个字符的长度以支持使用口令短语。

鼓励用户将密码设置得尽可能长，并使用他们喜欢的任何字符(包括空格)以帮助记忆。确保用户界面支持足够的密码长度。

-不要施加其他组合规则(例如，不同字符的混合
类型)对密码的影响。

- Do not require that passwords be changed arbitrarily (e.g., periodically) unless there is a user request or evidence of authenticator compromise (see Sec. 3.1.1).

- Provide clear, meaningful, and actionable feedback when chosen passwords are rejected (e.g., when it appears on a "blocklist" of unacceptable passwords or has been used previously).

8.1.2.2. Look-Up Secrets

Typical Usage

Subscribers use a printed or electronic authenticator to look up the appropriate secrets needed to respond to a verifier's prompt. For example, a user may be asked to provide a specific subset of the numeric or character strings printed on a card in table format.

Usability considerations for typical usage include the following:

- User experience during entry of look-up secrets
  - Consider the complexity and size of the prompts. There are greater usability implications with larger subsets of secrets that a user is prompted to look up. Both the cognitive workload and physical difficulty for entry should be considered.

8.1.2.3. Out-of-Band

Typical Usage

Out-of-band authentication requires that users have access to a primary and secondary communication channel.

Usability considerations for typical usage include the following:

- Notify users of the receipt of a secret on a lockable device. If the out-of-band device is locked, authentication to the device should be required to access the secret.
- Depending on the implementation, consider form-factor constraints, which are particularly problematic when users must enter text on mobile devices. Providing larger touch areas will improve usability for entering secrets on mobile devices.
- Consider offering features that do not require text entry on mobile devices (e.g., a copy and paste feature), which are particularly helpful when the primary and secondary channels are on the same device. For example, it is difficult for users to transfer the authentication secret manually using a smartphone because they must switch back and forth — potentially multiple times — between the out-of-band application and the primary channel.

-不要要求任意更改密码(例如，定期更改)
除非用户提出请求或有证据表明认证器已被泄露(参见Sec.3.1.1)。

- 当所选密码被拒绝时(例如，当它出现在不可接受密码的"阻止列表"上或先前已被使用时)，提供清晰、有意义且可操作的反馈。

8.1.2.2. 查找型密钥

典型用法

订阅者使用印刷或电子认证器来查找响应验证器提示所需的相应密钥。例如，用户可能被要求提供以表格形式印在卡片上的数字或字符串的特定子集。

典型使用的可用性考虑包括以下内容：

- 输入查询密钥时的用户体验
  -考虑提示的复杂性和大小。当用户被提示查找的密钥子集较大时，会产生更大的可用性
  当提示用户查找更大子集的机密信息时所涉及的影响。应同时考虑认知工作量和输入的物理难度。

8.1.2.3. 带外

典型用法

带外身份验证要求用户能够访问主通信信道和辅助通信信道。

典型使用的可用性考虑包括以下内容：

- 在可锁定设备上通知用户已收到密钥。如果带外设备已锁定，则应要求对该设备进行身份验证才能访问密钥。
- 根据实现方式，考虑外形尺寸限制，当用户必须在移动设备上输入文本时，这一问题尤为突出。提供更大的触摸区域将改善在移动设备上输入密钥的可用性。
- 考虑提供不需要在移动设备上输入文本的功能(例如，复制和粘贴功能)，当主信道和辅助信道位于同一设备上时，这些功能尤其有用。例如，用户使用智能手机手动传输身份验证密钥很困难，因为他们必须在带外应用和主信道之间来回切换--可能多次切换。

- Messages and notifications to out-of-band devices should contain contextual information for the user, such as the name of the service being accessed.
- Out-of-band messages should be delivered in a consistent manner and style to help the subscriber identify potentially suspicious authentication requests.

8.1.2.4. Single-Factor OTP

Typical Usage

Users access the OTP generated by the single-factor OTP authenticator. The authenticator output is typically displayed on the authenticator, and the user enters it during the session being authenticated.

Usability considerations for typical usage include the following:

- Authenticator output allows at least one minute between changes but ideally allows users two full minutes, as specified in Sec. 3.1.4.1. Users need adequate time to enter the authenticator output, including looking back and forth between the single-factor OTP authenticator and the entry screen.

8.1.2.5. Multi-Factor OTP

Typical Usage

Users access the OTP generated by the multi-factor OTP authenticator through a second authentication factor. The OTP is typically displayed on the device, and the user manually enters it during the session being authenticated. The second authentication factor may be achieved through some kind of integral entry pad to enter a password or an integral biometric (e.g., fingerprint) reader. Usability considerations for the additional factor also apply (see Sec. 8.1.2.1 for passwords and Sec. 8.1.4 for biometrics used in multi-factor authenticators).

Usability considerations for typical usage include:

- User experience during manual entry of the authenticator output
  - For time-based OTPs, provide a grace period in addition to the time during which the OTP is displayed. Users need adequate time to enter the authenticator output, including looking back and forth between the multi-factor OTP authenticator and the entry screen.
  - Consider form-factor constraints if users must unlock the multi-factor OTP authenticator via an integral entry pad or enter the authenticator output on mobile devices. Typing on small devices is significantly more error-prone and time-consuming than typing on a traditional keyboard. Providing larger touch areas improves usability for unlocking the multi-factor OTP authenticator or entering the authenticator output on mobile devices.

- 发送到带外设备的消息和通知应包含对用户有意义的上下文信息，例如正在访问的服务的名称。
- 带外消息应以一致的方式和风格传递，以帮助订阅者识别可能可疑的身份验证请求。

8.1.2.4. 单因素 OTP

典型用法

用户访问由单因素 OTP 认证器生成的 OTP。认证器输出通常显示在认证器上，用户在正在认证的会话期间输入该输出。

典型使用的可用性考虑包括以下内容：

- 认证器输出允许至少一分钟的更改间隔，但理想情况下应为用户提供整整两分钟，如Sec.3.1.4.1所规定。用户需要充足的时间来输入认证器输出，包括在单因素 OTP 认证器和输入屏幕之间来回查看。

8.1.2.5. 多因素 OTP

典型用法

用户通过第二认证因素访问由多因素 OTP 认证器生成的 OTP。OTP 通常显示在设备上，用户在正在认证的会话期间手动输入它。第二认证因素可以通过某种集成输入板来输入密码，或通过集成生物特征(例如指纹)读取器来实现。附加因素的可使用性考虑同样适用(密码参见Sec.8.1.2.1，多因素认证器中使用的生物特征参见Sec.8.1.4)。

典型使用的可用性考虑包括：

- 手动输入认证器输出时的用户体验
  - -对于基于时间的 OTP，除 OTP 显示时间外，还应提供宽限期。用户需要充足的时间来输入认证器输出，包括在多因素 OTP 认证器和输入屏幕之间来回查看。
  - -如果用户必须通过集成输入板解锁多因素 OTP 认证器或在移动设备上输入认证器输出，则考虑外形尺寸限制。在小型设备上打字比在传统键盘上打字更容易出错且更耗时。提供更大的触摸区域可改善在移动设备上解锁多因素 OTP 认证器或输入认证器输出的可用性。

8.1.2.6. Single-Factor Cryptographic Authenticator

Typical Usage

Users authenticate by proving possession and control of the cryptographic key.

Usability considerations for typical usage include the following:

- Give cryptographic keys appropriately descriptive names that are meaningful to users so that they can recognize and recall which cryptographic key to use for which authentication task. This prevents users from having to deal with multiple similarly and ambiguously named cryptographic keys. Requiring the user to select from multiple cryptographic keys on smaller mobile devices may be particularly problematic if the names of the cryptographic keys are shortened due to reduced screen sizes.
- Requiring a physical input (e.g., pressing a button) to operate a single-factor cryptographic authenticator could pose usability difficulties. For example, some USB ports are located on the back of computers, making it difficult for users to reach the port.
- For connected authenticators, the limited availability of a direct computer interface (e.g., USB port) could pose usability difficulties. For example, laptop computers often have a limited number of USB ports, which may force users to unplug other USB peripherals to use the authenticator.

8.1.2.7. Multi-Factor Cryptographic Authenticator

Typical Usage

To authenticate, users prove possession and control of the cryptographic key and control of the activation factor. Usability considerations for the additional factor also apply (see Sec. 8.1.2.1 for passwords and Sec. 8.1.4 for biometrics used as activation factors).

Usability considerations for typical usage include the following:

- Give cryptographic keys appropriately descriptive names that are meaningful to users so that they can recognize and recall which cryptographic key to use for which authentication task. This prevents users from having to deal with multiple similarly and ambiguously named cryptographic keys. Selecting from multiple cryptographic keys on smaller mobile devices may be particularly problematic if the names of the cryptographic keys are shortened due to reduced screen sizes.
- Do not require users to keep external multi-factor cryptographic authenticators connected following authentication. Users may forget to disconnect the authenticator when they are done with it (e.g., forgetting a smartcard in the smartcard reader and walking away from the computer).

8.1.2.6. 单因素加密认证器的典型用法

用户通过证明对加密密钥的持有和控制来进行认证。

典型使用的可用性考虑包括以下内容：

- 为加密密钥赋予适当的描述性名称，使其对用户有意义，以便他们能够识别和回忆起哪个加密密钥用于哪项身份验证任务。这可以避免用户不得不处理多个名称相似且含糊不清的加密密钥。如果由于屏幕尺寸减小而缩短加密密钥的名称，则要求用户在较小的移动设备上从多个加密密钥中进行选择可能尤为困难。
- 要求物理输入(例如，按下按钮)来操作单因素加密认证器可能会带来可用性困难。例如，某些 USB 端口位于计算机背面，使用户难以触及该端口。
- 对于连接的认证器，直接计算机接口(例如，USB 端口)的可用性有限可能会带来可用性困难。例如，笔记本电脑通常只有有限数量的 USB 端口，这可能迫使用户拔下其他 USB 外设才能使用认证器。

8.1.2.7. 多因素加密认证器的典型用法

要进行身份验证，用户需证明对加密密钥的拥有和控制以及对激活因子的控制。附加因素的可用性考虑因素同样适用(密码参见Sec.8.1.2.1，用作激活因子的生物特征参见Sec.8.1.4)。

典型使用的可用性考虑包括以下内容：

- 为加密密钥赋予恰当的描述性名称，使其对用户具有意义，以便用户能够识别并回忆起哪个加密密钥用于哪项身份验证任务。这可以避免用户不得不处理多个名称相似且含义模糊的加密密钥。在较小的移动设备上从多个加密密钥中进行选择可能尤其成问题，因为屏幕尺寸减小会导致加密密钥的名称被缩短。
- 不要要求用户在身份验证后保持外部多因素加密认证器的连接。用户可能会在完成后忘记断开认证器(例如，将智能卡遗忘在智能卡读取器中并离开计算机)。

- Users need to be informed about whether the authenticator is required to stay connected or not.

- For connected authenticators, the limited availability of a direct computer interface (e.g., USB port) could pose usability difficulties. For example, laptop computers often have a limited number of USB ports, which may force users to unplug other USB peripherals to use the authenticator.

8.1.3. Summary of Usability Considerations

Figure 3 summarizes the usability considerations for typical usage and intermittent events for each authenticator type. Many of the usability considerations for typical usage apply to most of the authenticator types, as demonstrated in the rows. The table highlights common and divergent usability characteristics across the authenticator types. Each column allows readers to easily identify the usability attributes to address for each authenticator. Depending on the users' goals and context of use, certain attributes may be valued over others. Whenever possible, provide alternative authenticator types, and allow users to choose between them.

Multi-factor authenticators (e.g., multi-factor OTPs) also inherit their activation factor's usability considerations. As biometrics are only allowed as an activation factor in multi-factor authentication solutions, usability considerations for biometrics are not included in Fig. 3 and are discussed in Sec. 8.1.4.

8.1.4. Usability Considerations for Biometrics

This section provides a high-level overview of general usability considerations for biometrics. A more detailed discussion of biometric usability can be found in *Usability & Biometrics*, *Ensuring Successful Biometric Systems* [UsabilityBiometrics].

User familiarity and practice with the device improve performance for all modalities. Device affordances (i.e., properties of a device that allow a user to perform an action), feedback, and clear instructions are critical to a user's success with the biometric device. For example, provide clear instructions on the required actions for liveness detection. Ideally, users can select the modality that they are most comfortable with for their second authentication factor. Various user populations may be more comfortable, familiar with, and accepting of some biometric modalities than others. Provide meaningful feedback on the number of remaining allowed attempts. For example, for rate limiting (i.e., throttling), inform users of the time period they have to wait until their next attempt.

Typical Usage

The three biometric modalities that are most commonly used for authentication are fingerprint, facial comparison, and iris comparison.

-需要告知用户认证器是否被要求
保持连接或不连接。

• 对于连接的认证器，直接计算机接口(例如，USB 端口)的可用性有限可能会带来可用性困难。例如，笔记本电脑通常只有有限数量的 USB 端口，这可能迫使用户拔下其他 USB 外设才能使用认证器。

8.1.3. 可用性考量摘要

Figure 3总结了每种认证器类型在典型使用和间歇性事件方面的可使用性考虑。如各行所示，典型使用的许多可使用性考虑适用于大多数认证器类型。该表突出了各认证器类型之间共同和不同的可使用性特征。每一列使读者能够轻松识别每种认证器需要解决的可使用性属性。根据用户的目标和使用情境，某些属性可能比其他属性更受重视。只要可能，就提供替代认证器类型，并允许用户在它们之间进行选择。

多因素认证器(例如，多因素OTP)也继承了其激活因素的可用性考量。由于生物特征仅被允许作为多因素身份验证解决方案中的激活因素，因此生物特征的可用性考量未包含在图3中，而是在第8.1.4节中讨论。

8.1.4. 生物识别的可用性考量

本节提供生物特征一般可用性考虑的高层概述。关于生物特征可用性的更详细讨论见《可用性与生物特征：确保生物特征系统成功》[UsabilityBiometrics]。

用户对设备的熟悉程度和练习可提高所有模态的性能。设备可供性(即设备允许用户执行操作的属性)、反馈和清晰说明对于用户成功使用生物特征设备至关重要。例如，就活体检测所需的操作提供清晰说明。理想情况下，用户可以选择他们最习惯的模态作为第二认证因素。不同用户群体可能对某些生物特征模态比其他群体更习惯、更熟悉并且更接受。就剩余允许尝试次数提供有意义的反馈。例如，对于速率限制(即节流)，告知用户他们必须等待到下一次尝试的时间段。

典型用法

最常用于身份验证的三种生物特征模态是指纹、面部比对和虹膜比对。

Usability Considerations	Passwords	Look-Up Secrets	Out-of-Band Devices	Single-Factor OTP	Multi-Factor OTP	Single-Factor Cryptographic	Multi-Factor Cryptographic
Typical Usage							
Authenticator availability - authenticators readily in user's possession	•	•	•	•	•	•	•
Plain language for user-facing text (e.g., instructions, prompts, notifications, error messages)	•	•	•	•	•	•	•
Legibility of user-facing text or text entered by users	•	•	•	•	•	•	•
Unmasked text entry		•	•	•	•		
Support text entry - length of 64 characters, copy and paste	•						
Delayed masking during text entry	•						
Adequate time allowed for text entry	•	•	•	•	•		
Entry errors - Need clear and meaningful feedback	•	•	•	•	•		
Minimum of 10 attempts allowed	•	•	•	•	•		
Remaining allowed attempts - need clear and meaningful feedback	•	•	•	•	•		
Form factor constraints	•	•	•	•	•	•	•
Location and availability of a direct computer interface, such as a USB port						•	•
Physical input required (such as pressing a button)						•	
Cryptographic keys need for descriptive and meaningful names						•	•
Complexity and size of the prompts		•					
Authentication to secondary device to access the authentication secret			•				
Continuous hardware connection not required							•
Intermittent Events							
Reauthentication due to user inactivity	•	•	•	•	•	•	•
Fixed periodic reauthentication	•	•	•	•	•	•	•
Provisions for technical assistance	•	•	•	•	•	•	•
Provisions to create and change passwords	•						

Fig. 3. Usability considerations by authenticator type

可用性考量	密码	查找型密钥	带外设备	单因素 OTP	多因素OTP	单因素加密	多因素加密
典型用法							
认证器可用性--认证器随时在用户手中							
面向用户文本的简明语言(例如，说明、提示、通知、错误消息)							
面向用户的文本或用户输入的文本的可读性							
明文输入							
支持文本输入 - 长度为64个字符，复制和粘贴							
文本输入期间的延迟掩蔽							
允许有足够的时间进行文本输入							
录入错误--需要清晰且有意义的反馈							
允许至少 10 次尝试							
剩余允许尝试次数--需要清晰且有意义的反馈							
形态因素约束							
直接计算机接口(如 USB 端口)的位置和可用性							
需要物理输入(例如按下按钮)							
加密密钥需要描述性和有意义的名称							
提示词的复杂性和规模							
对辅助设备进行认证以访问认证密钥							
不需要持续硬件连接							
间歇性事件							
因用户不活动而重新认证							
固定周期性重新认证							
技术援助条款							
创建和更改密码的规定							

图 3.按认证器类型划分的可用性考量

- Fingerprint usability considerations:
  - Users have to remember which fingers they used for initial enrollment.
  - The amount of moisture on the finger affects the sensor's ability for successful capture.
  - Additional factors that influence fingerprint capture quality include age, sex, and occupation (e.g., users who handle chemicals or work extensively with their hands may have degraded friction ridges).
- Facial comparison usability considerations:
  - Users have to remember whether they wore any artifacts (e.g., glasses) during enrollment, which affects facial recognition accuracy.
  - Differences in environmental lighting conditions may affect facial recognition accuracy.
  - Facial expressions affect facial recognition accuracy (e.g., smiling versus a neutral expression).
  - Facial poses affect facial recognition accuracy (e.g., looking down or away from the camera).
- Iris comparison usability considerations:
  - Wearing colored contacts may affect iris recognition accuracy.
  - Users who have had eye surgery may need to re-enroll after surgery.
  - Differences in environmental lighting conditions may affect iris recognition accuracy, especially for certain iris colors.

Intermittent Events

Since biometrics are only permitted as a second factor for multi-factor authentication, usability considerations for intermittent events with the primary factor still apply. Intermittent events that may affect recognition accuracy using biometrics include:

- Degraded fingerprints or finger injuries
- Dirty, dry, or wet hands
- Wearing gloves or a mask
- Natural facial or weight changes over time
- Eye surgery

Across all biometric modalities, usability considerations for intermittent events include the following:

• 指纹可用性考虑因素：

-用户必须记住他们在初始注册登记时使用了哪些手指。-手指上的水分量会影响传感器的能力

成功捕获。

-影响指纹采集质量的其他因素包括年龄、性别、
和职业(例如，接触化学品或大量使用双手工作的用户可能会出现摩擦脊线退化)。

• 面部比较可用性考虑因素：

-用户必须记住他们是否佩戴了任何物品(例如，眼镜)
在注册过程中，这会影响面部识别准确性。

-环境光照条件的差异可能会影响面部识别
准确性。

-面部表情会影响面部识别准确性(例如，微笑与
(中性表情)。

-面部姿态会影响面部识别准确性(例如，向下看或看向别处
(来自摄像头)。

• 虹膜比对可用性考量：

-佩戴彩色隐形眼镜可能会影响虹膜识别的准确性。

-接受过眼部手术的用户可能需要在手术后重新注册登记。-环境光照条件的差异可能会影响虹膜识别

准确性，尤其是对某些虹膜颜色而言。

间歇性事件

由于生物特征仅被允许作为多因素身份验证的第二因素，因此针对主因素的间歇性事件的可用性考量仍然适用。可能影响使用生物特征进行识别准确性的间歇性事件包括：

• 指纹退化或手指受伤
• 脏污、干燥或潮湿的手
• 佩戴手套或口罩
• 随着时间推移自然的面部或体重变化
• 眼科手术

在所有生物特征模态中，间歇性事件的可用性考量包括以下内容：

- An alternative authentication method must be readily available and clearly communicated. Users should never be required to attempt biometric authentication and should be permitted to use a password as an alternative second factor.
- There should be provisions for technical assistance:
  - Clearly communicate information on how and where to acquire technical assistance. For example, provide users with a link to an online self-service feature or a phone number for help desk support. Ideally, provide sufficient information to enable users to recover from intermittent events on their own without outside intervention.
  - Inform users of factors that may affect the sensitivity of the biometric sensor (e.g., cleanliness of the sensor).

8.2. Customer Success Considerations

A primary aspect of customer experience is anticipating the needs of the user population and offering authenticator options that are suitable for that population. Some examples of authenticator suitability problems are:

- SMS-based out-of-band authentication may not be usable for subscribers in rural areas without mobile phone service.
- OTP authenticators may be difficult to read for subscribers with vision issues.
- Out-of-band authentication secrets sent via a voice telephone call may be difficult to understand for subscribers with hearing issues.
- Some facial matching algorithms may not perform equally well for all user populations.
- Some subscribers may have conditions that interfere with fingerprint collection, such as missing fingers, degraded fingerprints (e.g., from working with chemicals or extensively using their hands), or dexterity problems.
- The cost of hardware-based authenticators may be beyond the means of some subscribers.
- Accurate manual entry of passwords may be difficult for subscribers with mobility and dexterity-related physical disabilities.
- Certain authenticator types may be challenging for subscribers with intellectual, developmental, learning, or neurocognitive difficulties.
- Lower-income subscribers are less likely to have up-to-date devices that are required by some authentication modes.
- Subscribers with less technological skill may need help to enter OTP codes from one device to another.

- 必须随时可用替代身份验证方法并清晰传达。绝不应要求用户尝试生物特征身份验证，并且应允许用户使用密码作为替代的第二因素。

- 应提供技术援助的相关规定：
  -清晰传达关于如何以及在何处获取技术援助的信息。例如，向用户提供在线自助服务功能的链接或帮助台支持的电话号码。理想情况下，提供足够的信息以使用户能够在没有外部干预的情况下自行从间歇性事件中恢复。

  -告知用户可能影响生物特征传感器灵敏度的因素(例如，传感器的清洁度)。

8.2. 客户成功考量

客户体验的一个主要方面是预见用户群体的需求，并提供适合该群体的认证器选项。认证器适用性问题的一些示例包括：

- 基于SMS的带外身份验证对于没有移动电话服务的农村地区的订阅者可能不可用。
- OTP认证器对于有视力问题的订阅者可能难以阅读。
- 通过语音电话呼叫发送的带外身份验证密钥对于有听力问题的订阅者可能难以理解。
- 某些面部匹配算法对于所有用户群体可能表现不一致。
- 某些订阅者可能存在妨碍指纹采集的状况，例如手指缺失、指纹退化(例如，因接触化学品或大量使用双手)或灵活性障碍。
- 基于硬件的认证器的成本可能超出某些订阅者的经济能力。
- 对于有行动能力和灵活性相关身体残疾的订阅者，准确手动输入密码可能较为困难。
- 某些认证器类型对于有智力、发育、学习或神经认知困难的订阅者可能具有挑战性。
- 低收入订阅者较不可能拥有某些身份验证模式所需的、保持更新的设备。
- 技术技能较少的订阅者可能需要帮助才能将 OTP 代码从一台设备输入到另一台设备。

- The small form factor of some authenticators may pose challenges for certain users, such as senior citizens and individuals with dexterity challenges.

While CSPs are required to mitigate common and expected problems in this area, it is not feasible to anticipate all potential customer experience problems, which will vary for different applications. Accordingly, CSPs need to provide mechanisms for subscribers to report challenges with authentication requirements and advise them on potential alternative authentication strategies.

- 某些认证器的小尺寸外形可能会给特定用户带来挑战，例如老年人和有灵活性障碍的人士。

虽然要求 CSP 缓解该领域中常见和预期的问题，但预见所有潜在的客户体验问题并不可行，而且这些问题会因应用不同而异。因此，CSP 需要为订阅者提供机制，以报告身份验证要求方面的挑战，并就潜在的替代身份验证策略向其提供建议。

References

This section is informative.

[Blocklists] Habib H, Colnago J, Melicher W, Ur B, Segreti S, Bauer L, Christin N, Cranor L (2017) Password Creation in the Presence of Blacklists. *Proceedings 2017 Workshop on Usable Security* (Internet Society, San Diego, CA). https://doi.org/10.14722/usec.2017.23043

[CMVP] National Institute of Standards and Technology (2025), *Cryptographic Module Validation Program*. Available at https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program

[Composition] Komanduri S, Shay R, Kelley PG, Mazurek ML, Bauer L, Christin N, Cranor LF, Egelman S (2011) Of Passwords and People: Measuring the Effect of Password-Composition Policies. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (ACM, New York, NY), pp 2595–2604. Available at https://www.ece.cmu.edu/~lbauer/papers/2011/chi2011-passwords.pdf

[DBSC] W3C (2025) *Device Bound Session Credentials*. Available at https://github.com/w3c/webappsec-dbsc

[E-Gov] E-Government Act of 2002, P.L. 107-347, 116 Stat. 2899, 44 U.S.C. § 101 (2002). Available at https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf

[EO13681] Obama B (2014) Improving the Security of Consumer Financial Transactions. (The White House, Washington, DC), Executive Order 13681, October 17, 2014. Available at https://www.federalregister.gov/d/2014-25439

[FEDRAMP] General Services Administration (2022), *How to Become FedRAMP Authorized*. Available at https://www.fedramp.gov/

[FIDO2] Bradley J, Jones MB, Kumar A, Lindemann R, Verrept J, Waite D (2025) Client to Authenticator Protocol (CTAP). (FIDO Alliance, Beaverton, OR). Available at https://fidoalliance.org/specs/fido-v2.2-ps-20250228/fido-client-to-authenticator-protocol-v2.2-ps-20250228.html

[FIPS140] National Institute of Standards and Technology (2019) Security Requirements for Cryptographic Modules. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 140-3. https://doi.org/10.6028/NIST.FIPS.140-3

[FIPS201] National Institute of Standards and Technology (2022) Personal Identity Verification (PIV) of Federal Employees and Contractors. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 201-3. https://doi.org/10.6028/NIST.FIPS.201-3

参考文献

本节为说明性内容。

[黑名单] Habib H, Colnago J, Melicher W, Ur B, Segreti S, Bauer L, Christin N, Cranor L(2017) 黑名单存在下的密码创建。*2017* 可用安全研讨会论文集(Internet Society,San Diego,CA)。https://doi.org/10.14722/usec.2017. 23043

[CMVP] 国家标准与技术研究院（2025），密码模块验证计划。可查阅于 https://csrc.nist.gov/Projects/Cryptographic-ModuleValidation-Program

[组成] Komanduri S, Shay R, Kelley PG, Mazurek ML, Bauer L, Christin N, Cranor LF, Egelman S(2011) 密码与人：衡量密码组成策略的效果。*SIGCHI* 人机交互因素会议论文集

Computing Systems(ACM, New York, NY), pp 2595-2604. 可在以下网址获取：https://www.ece.cmu.edu/~lbauer/papers/2011/chi2011-passwords.pdf

[DBSC] W3C(2025) *Device Bound Session Credentials.*可在以下网址获取：https://github.com/ w3c/webappsec-dbsc

[E-Gov] E-Government Act of 2002, P.L. 107-347, 116 Stat. 2899, 44 U.S.C.101 (2002). Available at https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf

[EO13681] Obama B(2014) 改善消费者金融交易的安全性。(白宫，华盛顿特区)，第13681号行政命令，2014年10月17日。可访问于https://www.federalregister.gov/d/2014-25439

[FEDRAMP]美国总务管理局(2022),如何获得 *FedRAMP* 授权。可访问https://www.fedramp.gov/

[FIDO2] Bradley J, Jones MB, Kumar A, Lindemann R, Verrept J, Waite D (2025) 客户端到认证器协议（CTAP）。（FIDO联盟，俄勒冈州比弗顿）。可访问 https: //fidoalliance.org/specs/fido-v2.2-ps-20250228/fido-client-to-authenticator-protocolv2.2-ps-20250228.html

[FIPS140]美国国家标准与技术研究院(2019)《密码模块安全要求》。(美国商务部，华盛顿特区)，联邦信息处理标准出版物(FIPS)140-3。https://doi.org/10.6028/ NIST.FIPS.140-3

[FIPS201]美国国家标准与技术研究院(2022)个人身份
联邦雇员和承包商的验证(PIV)。(美国商务部，华盛顿特区)，联邦信息处理标准出版物(FIPS)201-3。https://doi.org/10.6028/NIST.FIPS.201-3

[FISMA] Federal Information Security Modernization Act of 2014, Pub. L. 113-283, 128 Stat. 3073. Available at https://www.govinfo.gov/app/details/PLAW-113publ283

[IC3] Federal Bureau of Investigation (2024) *Annual Reports - Internet Crime Complaint Center (IC3)*. Available at https://www.ic3.gov/AnnualReport/Reports/

[ISO/IEC2382-37] International Standards Organization (2022) *Information technology — Vocabulary — Part 37: Biometrics* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/73514.html

[ISO/IEC9241-11] International Standards Organization (2018) *ISO/IEC 9241-11 Ergonomics of human-system interaction – Part 11: Usability: Definitions and concepts* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/63500.html

[ISO/IEC10646] International Standards Organization (2020) *Information technology — Universal coded character set (UCS)* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/76835.html

[ISO/IEC19792] International Standards Organization (2009) *Information technology — Security techniques — Security evaluation of biometrics* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/51521.html

[ISO/IEC19795-1] International Standards Organization (2021) *Information technology - Biometric performance testing and reporting Part 1: Principles and framework* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/73515.html

[ISO/IEC19989-1] International Standards Organization (2020) *Information security — Criteria and methodology for security evaluation of biometric systems — Part 1: Framework* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/72402.html

[ISO/IEC19989-3] International Standards Organization (2020) *Information security — Criteria and methodology for security evaluation of biometric systems — Part 3: Presentation attack detection* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/73721.html

[ISO/IEC30107-1] International Standards Organization (2023) *Information technology — Biometric presentation attack detection — Part 1: Framework* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/83828.html

[ISO/IEC30107-3] International Standards Organization (2023) *Information technology — Biometric presentation attack detection — Part 3: Testing and reporting* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/79520.html

[Managers] Lyastani SG, Schilling M, Fahl S, Backes M, Bugiel S (2018) Better managed than memorized? Studying the Impact of Managers on Password Strength and Reuse. *27th USENIX Security Symposium (USENIX Security 18)* (USENIX Association, Baltimore,

[FISMA] 《2014年联邦信息安全现代化法案》，Pub.L.113-283,128 Stat.3073。可访问于https://www.govinfo.gov/app/details/PLAW-113publ283

[IC3]联邦调查局(2024) 年度报告 - 互联网犯罪投诉中心 *(IC3)*。可访问https://www.ic3.gov/Annual Report/Reports/

[ISO/IEC2382-37] 国际标准化组织（2022）信息技术——词汇——第37部分：生物特征（ISO，瑞士日内瓦）。见https://www.iso.org/standard/73514.html

[ISO/IEC9241-11]国际标准化组织(2018) *ISO/IEC 9241-11* 人机交互工效学 - 第*11*部分：可用性：定义与概念(ISO，瑞士日内瓦)。可从https://www.iso.org/standard/63500.html获取

[ISO/IEC10646]国际标准化组织(2020)信息技术 - 通用编码字符集*(UCS)*(ISO，瑞士日内瓦)。可从https: //www.iso.org/standard/76835.html获取

[ISO/IEC19792]国际标准化组织(2009)信息技术 - 安全技术 - 生物特征安全评估(ISO，瑞士日内瓦)。可从https://www.iso.org/standard/51521.html获取

[ISO/IEC19795-1]国际标准化组织(2021)信息技术 - 生物特征性能测试与报告第*1*部分：原则与框架(ISO，瑞士日内瓦)。可从https://www.iso.org/standard/73515.html获取

[ISO/IEC19989-1]国际标准化组织(2020)信息安全 - 生物特征系统安全评估的准则与方法 - 第*1*部分：框架(ISO，瑞士日内瓦)。可从https://www.iso.org/standard/ 72402.html获取

[ISO/IEC19989-3]国际标准化组织(2020)信息安全 - 生物特征系统安全评估的准则与方法 - 第*3*部分：呈现攻击检测(ISO，瑞士日内瓦)。可从https://www.iso.org/standard/73721.html获取

[ISO/IEC30107-1]国际标准化组织(2023)信息技术 - 生物特征呈现攻击检测 - 第*1*部分：框架(ISO，瑞士日内瓦)。可从https://www.iso.org/standard/83828.html获取

[ISO/IEC30107-3]国际标准化组织(2023)信息技术 - 生物特征呈现攻击检测 - 第*3*部分：测试与报告(ISO，瑞士日内瓦)。可从https://www.iso.org/standard/79520.html获取

[管理人员] Lyastani SG, Schilling M, Fahl S, Backes M, Bugiel S(2018) 管理比记忆更好吗?研究管理人员对密码强度和重复使用的影响。第*27*届 *USENIX* 安全研讨会*(USENIX Security 18)*(USENIX Association,Baltimore,

MD), pp 203–220. Available at https://www.usenix.org/conference/usenixsecurity18/presentation/lyastani

[NISTIR8062] Brooks S, Garcia M, Lefkovitz N, Lightman S, Nadeau E (2017) An Introduction to Privacy Engineering and Risk Management in Federal Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) NIST IR 8062, January 2017. https://doi.org/10.6028/NIST.IR.8062

[NISTRMF] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-37r2. https://doi.org/10.6028/NIST.SP.800-37r2

[OWASP-session] Open Web Application Security Project (2021) *Session Management Cheat Sheet*. Available at https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html

[OWASP-XSS-prevention] Open Web Application Security Project (2021) *XSS (Cross Site Scripting) Prevention Cheat Sheet*. Available at https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html

[Persistence] Herley C, Van Oorschot P (2012) A Research Agenda Acknowledging the Persistence of Passwords. *IEEE Security & Privacy Magazine*, (IEEE, Garden Grove, CA) 10(1):28–36. https://doi.org/10.1109/MSP.2011.150

[Policies] Weir M, Aggarwal S, Collins M, Stern H (2010) Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords. *Proceedings of the 17th ACM Conference on Computer and Communications Security, CCS '10*, (ACM, New York, NY, USA), pp 162–175. https://doi.org/10.1145/1866307.1866327

[PrivacyAct] Privacy Act of 1974, Pub. L. 93-579, 5 U.S.C. § 552a, 88 Stat. 1896 (1974). Available at https://www.govinfo.gov/content/pkg/USCODE-2020-title5/pdf/USCODE-2020-title5-partI-chap5-subchapII-sec552a.pdf

[PSL] Mozilla Foundation (2022) *Public Suffix List*. Available at https://publicsuffix.org/list/

[RBG] National Institute of Standards and Technology (2023) *Random Bit Generation*. Available at https://csrc.nist.gov/projects/random-bit-generation

[RFC20] Cerf V (1969) ASCII format for network interchange. (Internet Engineering Task Force (IETF)), IETF Request for Comments (RFC) 20. https://doi.org/10.17487/RFC0020

[RFC5280] Cooper D, Santesson S, Farrell S, Boeyen S, Housley R, Polk W (2008) Internet X.509 Public Key Infrastructure Certification and Certificate Revocation List (CRL) Profile. (Internet Engineering Task Force (IETF)), IETF Request for Comments (RFC) 5280. https://doi.org/10.17487/RFC5280

MD)，第 203-220 页。可访问于https://www.usenix.org/conference/usenixsecurity18/presentation/lyastani

[NISTIR8062] Brooks S, Garcia M, Lefkovitz N, Lightman S, Nadeau E (2017) 一项《联邦系统中的隐私工程与风险管理导论》(美国国家标准与技术研究院，马里兰州盖瑟斯堡),NIST 机构间或内部报告(IR)NIST IR 8062,2017 年 1 月。https://doi.org/10.6028/NIST.IR.8062

[NISTRMF] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-37r2. https://doi.org/10.6028/NIST.SP.800-37r2

[OWASP-session] Open Web Application Security Project (2021) Session Management Cheat Sheet. Available at https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html

[OWASP-XSS-prevention] Open Web Application Security Project (2021) XSS (Cross Site Scripting) Prevention Cheat Sheet. Available at https://cheatsheetseries.owasp.org/ cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html

[持久性] Herley C, Van Oorschot P(2012) 承认密码持久性的研究议程。*IEEE* 安全与隐私杂志,(IEEE， 加登格罗夫， 加利福尼亚州) 10(1): 28-36. https://doi.org/10.1109/MSP.2011.150

[策略] Weir M, Aggarwal S, Collins M, Stern H(2010) 通过攻击大量已泄露密码来测试密码创建策略的度量指标。第*17*届*ACM*计算机与通信安全会议论文集，*CCS '10*,(ACM，纽约，纽约州，美国)，第162-175页。https://doi.org/10.1145/1866307.1866327

[PrivacyAct] 1974年隐私法，Pub. L. 93-579，5 U.S.C.552a，88 Stat. 1896（1974）。可查阅于 https://www.govinfo.gov/content/pkg/USCODE-2020-title5/pdf/USCODE2020-title5-partI-chap5-subchapII-sec552a.pdf

[PSL] Mozilla Foundation (2022) Public Suffix List. Available at https://publicsuffix.org/ list/

[RBG] National Institute of Standards and Technology (2023) Random Bit Generation. Available at https://csrc.nist.gov/projects/random-bit-generation

[RFC20] Cerf V(1969) 用于网络交换的 ASCII 格式。(互联网工程任务组(IETF)),IETF 征求意见文件(RFC) 20。https://doi.org/10.17487/RFC0020

[RFC5280] Cooper D, Santesson S, Farrell S, Boeyen S, Housley R, Polk W(2008) 互联网 X.509 公钥基础设施证书和证书吊销列表(CRL) 配置文件。(互联网工程任务组(IETF)),IETF 请求注释(RFC) 5280。https: //doi.org/10.17487/RFC5280

[RFC6749] Hardt D (2012) The OAuth 2.0 Authorization Framework. (Internet Engineering Task Force (IETF)), IETF Request for Comments (RFC) 6749. https://doi.org/10.17487/RFC6749

[RFC8446] Rescorla E (2018) The Transport Layer Security (TLS) Protocol Version 1.3. (Internet Engineering Task Force (IETF)), IETF Request for Comments (RFC) 8446. https://doi.org/10.17487/RFC8446

[RFC9325] Sheffer Y, Saint-Andre P, Fossati T (2022) Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS). (Internet Engineering Task Force (IETF)), IETF Request for Comments (RFC) 9325. https://doi.org/10.17487/RFC9325

[Section508] General Services Administration (2022) *IT Accessibility Laws and Policies*. Available at https://www.section508.gov/manage/laws-and-policies/

[Shannon] Shannon CE (1948) A Mathematical Theory of Communication. *Bell System Technical Journal* 27(3):379–423. https://doi.org/10.1002/j.1538-7305.1948.tb01338.x

[SP800-39] Joint Task Force (2011) Managing Information Security Risk. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-39. https://doi.org/10.6028/NIST.SP.800-39

[SP800-52] McKay K, Cooper D (2019) Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations. (National Institute of Standards and Technology), NIST Special Publication (SP) NIST SP 800-52r2. https://doi.org/10.6028/NIST.SP.800-52r2

[SP800-53] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-53r5, Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[SP800-57Part1] Barker EB (2020) Recommendation for Key Management: Part 1 – General. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-57pt1r5. https://doi.org/10.6028/NIST.SP.800-57pt1r5

[SP800-63] Temoshok D, Galluzzo R, LaSalle C, Lefkovitz N, Regenscheid A, Choong YY, Proud-Madruga D, Gupta S (2025) Digital Identity Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-63-4. https://doi.org/10.6028/NIST.SP.800-63-4

[SP800-63A] Temoshok D, Abruzzi C, Choong YY, Fenton JL, Galluzzo R, LaSalle C, Lefkovitz N, Regenscheid A, Vachino M (2025) Digital Identity Guidelines: Identity Proofing and Enrollment. (National Institute of Standards and Technology, Gaithersburg,

[**RFC6749**] Hardt D(2012) OAuth 2.0 授权框架。(互联网工程任务组(IETF)),IETF 征求意见文件(RFC)6749。https://doi.org/ 10.17487/RFC6749

[**RFC8446**] Rescorla E(2018) 传输层安全(TLS)协议版本 1.3。(互联网工程任务组(IETF)),IETF 请求意见(RFC)8446。https: //doi.org/10.17487/RFC8446

[**RFC9325**] Sheffer Y, Saint-Andre P, Fossati T(2022) 传输层安全(TLS)与数据报传输层安全(DTLS)安全使用建议。(互联网工程任务组(IETF)),IETF 征求意见文件(RFC)9325。https://doi.org/ 10.17487/RFC9325

[Section508] General Services Administration (2022) IT Accessibility Laws and Policies. Available at https://www.section508.gov/manage/laws-and-policies/

[**Shannon**] Shannon CE(1948) 通信的数学理论.贝尔系统技术期刊 27(3): 379-423. https://doi.org/10.1002/j.1538-7305.1948.tb01338.x

[SP800-39] Joint Task Force (2011) Managing Information Security Risk. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-39. https://doi.org/10.6028/NIST.SP.800-39

[**SP800-52**] McKay K, Cooper D(2019) 传输层安全(TLS)实现的选择、配置和使用指南。(美国国家标准与技术研究院),NIST 特别出版物(SP)NIST SP 800-52r2。https://doi.org/10. 6028/NIST.SP.800-52r2

[SP800-53] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-53r5, Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[**SP800-57Part1**] Barker EB(2020) 密钥管理建议：第1部分 - 概述。(美国国家标准与技术研究院，马里兰州盖瑟斯堡),NIST 特别出版物(SP) NIST SP 800-57pt1r5。https://doi.org/10.6028/NIST.SP.800- 57pt1r5

[**SP800-63**] Temoshok D, Galluzzo R, LaSalle C, Lefkovitz N, Regenscheid A, Choong YY, Proud-Madruga D, Gupta S(2025) 数字身份指南。(美国国家标准与技术研究院，马里兰州盖瑟斯堡),NIST 特别出版物(SP) NIST SP 800-63-4。https://doi.org/10.6028/NIST.SP.800-63-4

[**SP800-63A**] Temoshok D, Abruzzi C, Choong YY, Fenton JL, Galluzzo R, LaSalle C, Lefkovitz N, Regenscheid A, Vachino M(2025) 数字身份指南：身份证明与注册登记。(美国国家标准与技术研究院，马里兰州盖瑟斯堡，

MD), NIST Special Publication (SP) NIST SP 800-63A-4. https://doi.org/10.6028/NIST.SP.800-63A-4

[SP800-63C] Temoshok D, Richer JP, Choong YY, Fenton JL, Lefkovitz N, Regenscheid A, Galluzzo R (2025) Digital Identity Guidelines: Federation and Assertions. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-63C-4. https://doi.org/10.6028/NIST.SP.800-63C-4

[SP800-73pt2] Ferraiolo H, Mehta K, Francomacaro S, Chandramouli R, Gupta S (2024) Interfaces for Personal Identity Verification: Part 2 – PIV Card Application Card Command Interface. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-73pt2-5. https://doi.org/10.6028/NIST.SP.800-73pt2-5

[SP800-90A] Barker E, Kelsey J (2015) Recommendation for Random Number Generation Using Deterministic Random Bit Generators. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-90Ar1. https://doi.org/10.6028/NIST.SP.800-90Ar1

[SP800-90B] Turan MS, Barker E, Kelsey J, McKay K, Baish M, Boyle M (2018) Recommendation for the Entropy Sources Used for Random Bit Generation. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-90B. https://doi.org/10.6028/NIST.SP.800-90B

[SP800-90C] Barker E, Kelsey J, McKay K, Roginsky A, Turan MS (2024) Recommendation for Random Bit Generator (RBG) Constructions. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Special Publication (SP) NIST SP 800-90C. https://doi.org/10.6028/NIST.SP.800-90C.4pd

[SP800-131A] Barker E, Roginsky A (2019) Transitioning the Use of Cryptographic Algorithms and Key Lengths. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-131Ar2. https://doi.org/10.6028/NIST.SP.800-131Ar2

[SP800-132] Turan M, Barker E, Burr W, Chen L (2010) Recommendation for Password-Based Key Derivation. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-132. https://doi.org/10.6028/NIST.SP.800-132

[SP800-157] Ferraiolo H, Regenscheid AR, Fenton J (2023) Guidelines for Derived Personal Identity Verification (PIV) Credentials. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-157r1 ipd (initial public draft). https://doi.org/10.6028/NIST.SP.800-157r1.ipd

[Strength] Kelley PG, Komanduri S, Mazurek ML, Shay R, Vidas T, Bauer L, Christin N, Cranor LF, Lopez J (2012) Guess again (and again and again): Measuring password

MD),NIST 特别出版物(SP) NIST SP 800-63A-4。https://doi.org/10.6028/NIST.SP.800-63A-4

[**SP800-63C**] Temoshok D, Richer JP, Choong YY, Fenton JL, Lefkovitz N, Regenscheid A, Galluzzo R(2025) 数字身份指南：联合身份与断言。(美国国家标准与技术研究院，马里兰州盖瑟斯堡),NIST 特别出版物(SP) NIST SP 800-63C-4。https://doi.org/10.6028/NIST.SP.800-63C-4

[**SP800-73pt2**] Ferraiolo H, Mehta K, Francomacaro S, Chandramouli R, Gupta S(2024) 个人身份验证接口：第2部分 - PIV 卡应用卡命令接口。(美国国家标准与技术研究院，马里兰州盖瑟斯堡),NIST 特别出版物(SP) NIST SP 800-73pt2-5。https://doi.org/10.6028/NIST.SP.800-73pt2-5

[**SP800-90A**] Barker E, Kelsey J(2015) 使用确定性随机比特生成器的随机数生成建议。(美国国家标准与
技术研究院，马里兰州盖瑟斯堡),NIST 特别出版物(SP) NIST SP 800-90Ar1。https: //doi.org/10.6028/NIST.SP.800-90Ar1

[SP800-90B] 图兰 MS， 巴克 E， 凯尔西 J， 麦凯 K， 拜什 M， 博伊尔 M (2018)
用于随机比特生成的熵源建议。(美国国家标准与技术研究院，马里兰州盖瑟斯堡),NIST 特别出版物(SP) NIST SP 800-90B。https://doi.org/10.6028/NIST.SP.800-90B

[**SP800-90C**] Barker E, Kelsey J, McKay K, Roginsky A, Turan MS(2024) 随机比特生成器(RBG)构造建议。(美国国家标准与技术研究院，马里兰州盖瑟斯堡),NIST 特别出版物(SP) 草案 NIST SP 800-90C。https://doi.org/10.6028/NIST.SP.800-90C.4pd

[**SP800-131A**] Barker E, Roginsky A(2019) 密码算法和密钥长度的过渡使用。(美国国家标准与技术研究院，
马里兰州盖瑟斯堡),NIST 特别出版物(SP) NIST SP 800-131Ar2。https://doi.org/ 10.6028/NIST.SP.800-131Ar2

[**SP800-132**] Turan M, Barker E, Burr W, Chen L(2010) 基于密码的密钥派生建议。(美国国家标准与技术研究院，马里兰州盖瑟斯堡),NIST 特别出版物(SP) NIST SP 800-132。https://doi.org/10.6028/NIST.SP.800-132

[**SP800-157**] Ferraiolo H, Regenscheid AR, Fenton J(2023) 派生个人身份验证(PIV)凭证指南。(美国国家标准与技术研究院，马里兰州盖瑟斯堡),NIST 特别出版物(SP) NIST SP 800-157r1 ipd(初始公开草案)。https://doi.org/10.6028/NIST.SP.800-157r1.ipd

[**Strength**] Kelley PG, Komanduri S, Mazurek ML, Shay R, Vidas T, Bauer L, Christin N, Cranor LF, Lopez J(2012) 再猜(再猜再猜)：测量密码

strength by simulating password-cracking algorithms. *2012 IEEE Symposium On Security and Privacy (SP)*, pp 523–537. Available at http://ieeexplore.ieee.org/iel5/6233637/6234400/06234434.pdf

[TOTP] M'Raihi D, Machani S, Pei M, Rydell J (2011) TOTP: Time-Based One-Time Password Algorithm. (Internet Engineering Task Force, Reston, VA), RFC 6238. https://doi.org/10.17487/RFC6238

[UsabilityBiometrics] National Institute of Standards and Technology (2008) Usability & Biometrics: Ensuring Successful Biometric Systems. (National Institute of Standards and Technology, Gaithersburg, MD). Available at https://www.nist.gov/system/files/usability_and_biometrics_final2.pdf

[UAX15] Whistler K (2022) Unicode Normalization Forms. (The Unicode Consortium, South San Francisco, CA), Unicode Standard Annex 15, Version 15.0.0, Rev. 53. Available at https://www.unicode.org/reports/tr15/

[WebAuthn] Hodges J, Jones JC, Jones MB, Kumar A, Lundberg E (2021) Web Authentication: An API for accessing Public Key Credentials - Level 2. (World Wide Web Consortium, Cambridge, MA). Available at https://www.w3.org/TR/2021/REC-webauthn-2-20210408/

通过模拟密码破解算法来评估强度。*2012 IEEE Symposium On Security and Privacy (SP)*, pp 523-537. 可访问于http://ieeexplore.ieee.org/iel5/6233637/ 6234400/06234434.pdf

[TOTP] M'Raihi D, Machani S, Pei M, Rydell J(2011) TOTP：基于时间的一次性密码算法。(互联网工程任务组，弗吉尼亚州雷斯顿),RFC 6238。https: //doi.org/10.17487/RFC6238

[UsabilityBiometrics] National Institute of Standards and Technology (2008) Usability & Biometrics: Ensuring Successful Biometric Systems. (National Institute of Standards and Technology, Gaithersburg, MD). Available at https://www.nist.gov/system/files/usability_and_biometrics_final2.pdf

[UAX15] Whistler K(2022) Unicode 规范化形式。(Unicode 联盟，南旧金山，加利福尼亚州),Unicode 标准附件 15，版本 15.0.0，修订版 53。可访问于https://www.unicode.org/reports/tr15/

[WebAuthn] Hodges J, Jones JC, Jones MB, Kumar A, Lundberg E (2021) Web 认证：用于访问公钥凭据的 API - 第 2 级。(万维网联盟，马萨诸塞州剑桥)。可在https://www.w3.org/TR/2021/REC-webauthn- 2-20210408/获取

Appendix A. Strength of Passwords

This appendix is informative.

This appendix uses the word “password” for ease of discussion. Where used, it should be interpreted to include passphrases and PINs.

A.1. Introduction

Passwords are a widely used form of authentication despite concerns about their use from both a usability and security standpoint [Persistence]. Humans have a limited ability to memorize complex, arbitrary secrets, so they often choose passwords that can be easily guessed. To address the resultant security concerns, online services have introduced rules that increase the effective strength of these passwords. The most notable form is composition rules, which require users to choose passwords that are constructed using a mix of character types (e.g., at least one digit, uppercase letter, and symbol). However, analyses of breached password databases reveal that the benefit of such rules is less significant than initially thought [Policies], and the impacts on usability and memorability are severe.

The effective strength of user-chosen passwords has often been characterized using the information theory concept of entropy [Shannon]. While entropy can be readily calculated for data with deterministic distribution functions, estimating entropy for user-chosen passwords is challenging. For this reason, a different and somewhat more straightforward approach based primarily on password length is presented herein. The use of passphrases (i.e., passwords with multiple words) is often an effective way to create a longer password.

Many attacks associated with passwords are not affected by password complexity and length. Keystroke logging, phishing, and social engineering attacks are equally effective on lengthy and complex passwords as they are on simple ones. These attacks are outside of the scope of this Appendix.

A.2. Length

Password length is a primary factor in characterizing password strength [Strength] [Composition]. Passwords that are too short yield to brute-force attacks and dictionary attacks. The minimum password length required depends on the threat model being addressed. Online attacks in which the attacker attempts to log in by guessing the password can be mitigated by limiting the permitted login attempt rate. To prevent an attacker (or a persistent claimant with poor typing skills) from quickly inflicting a denial-of-service attack on the subscriber by making many incorrect guesses, passwords need to be complex enough that a reasonable number of attempts can be permitted with a low probability of a successful guess, and rate limiting, as described in Sec. 3.2.2 can be applied before there is a significant chance of a successful guess.

附录 A.密码强度

本附录为资料性内容。

本附录为便于讨论使用“密码”一词。凡使用之处，应解释为包含口令短语和 PIN。

A.1. 引言

尽管从可用性和安全性的角度都存在担忧，密码仍是一种广泛使用的身份验证形式[持久性]。人类记忆复杂、任意密钥的能力有限，因此他们经常选择容易被猜到的密码。为了解决由此产生的安全问题，在线服务引入了提高这些密码有效强度的规则。最显著的形式是组合规则，它要求用户选择由混合字符类型(例如，至少一个数字、大写字母和符号)构成的密码。然而，对泄露密码数据库的分析表明，此类规则的好处不如最初想象的那么显著[策略]，并且对可用性和可记忆性的影响很严重。

用户选择的密码的有效强度通常使用信息论中的熵概念来表征[Shannon]。虽然对于具有确定性分布函数的数据，熵可以很容易地计算出来，但估计用户选择的密码的熵具有挑战性。为此，本文提出了一种主要基于密码长度的不同且更为直接的方法。使用口令短语(即包含多个单词的密码)通常是创建更长密码的有效方法。

许多与密码相关的攻击不受密码复杂度和长度的影响。击键记录、网络钓鱼和社会工程攻击对冗长复杂的密码与对简单密码同样有效。这些攻击不在本附录的范围内。

A.2. 长度

密码长度是表征密码强度的主要因素[强度][组合]。过短的密码容易受到暴力攻击和字典攻击。所需的最小密码长度取决于所应对的威胁模型。攻击者通过猜测密码尝试登录的在线攻击，可以通过限制允许的登录尝试速率来缓解。为了防止攻击者(或打字技能较差的持续声称者)通过进行多次错误猜测迅速对订阅者造成拒绝服务攻击，密码需要足够复杂，以便在成功猜测概率较低的情况下允许合理数量的尝试，并且可以在有显著成功猜测机会之前应用第3.2.2节中描述的速率限制。

Offline attacks are possible when the attacker obtains one or more hashed passwords through a database breach. The ability of the attacker to determine one or more users' passwords depends on how the password is stored. Commonly, passwords are salted with a random value and hashed, preferably using a computationally expensive algorithm. Even with such measures, the current ability of attackers to compute many billions of hashes per second in an offline environment that is not subject to rate limiting requires passwords to be orders of magnitude more complex than those expected to resist only online attacks.

Users should be encouraged to make their passwords as long as they want within reason. Since the size of a hashed password is independent of its length, there is no reason to prohibit the use of lengthy passwords (or passphrases) if the user wishes. However, extremely long passwords (perhaps megabytes long) could require excessive processing time to hash, so it is reasonable to have some limit.

A.3. Complexity

Composition rules are commonly used in an attempt to increase the difficulty of guessing user-chosen passwords. However, research has shown that users respond in very predictable ways to the requirements imposed by composition rules [Policies]. For example, a user who might have chosen "password" as their password would be relatively likely to choose "Password1" if required to include an uppercase letter and a number or "Password1!" if a symbol is also required.

Users also express frustration when online services reject their attempts to create complex passwords. Many services reject passwords with spaces and various special characters. Characters that are not accepted are sometimes the result of an effort to avoid attacks that depend on those characters (e.g., SQL injection). However, an unhashed password would not be sent intact to a database, so such precautions are unnecessary. Users should also be able to include space characters to allow the use of phrases. Repeated space characters add little to the effective strength of passwords and may introduce usability issues (e.g., the undetected use of two spaces rather than one), so removing repeated spaces in typed passwords may be beneficial if initial verification fails.

Since users' password choices are often predictable, attackers are likely to guess passwords that have previously proven successful. These include dictionary words and passwords from previous breaches, such as the "Password1!" example above. For this reason, passwords chosen by users should be compared against a blocklist of unacceptable passwords. This list should include passwords from previous breach corpuses, dictionary words used as passwords, and specific words (e.g., the name of the service itself) that users are likely to choose. Since a minimum length requirement will also govern the user's choice of passwords, this dictionary only needs to include entries that meet that requirement. As noted in Sec. 3.1.1.2, it is not beneficial for the

当攻击者通过数据库泄露获得一个或多个哈希密码时，离线攻击就成为可能。攻击者确定一个或多个用户密码的能力取决于密码的存储方式。通常，密码用随机值加盐并进行哈希处理，最好使用计算成本高昂的算法。即使采取了此类措施，攻击者当前在不受速率限制的离线环境中每秒计算数千亿次哈希的能力，要求密码比仅期望抵御在线攻击的密码复杂几个数量级。

应鼓励用户在合理范围内将密码设置得尽可能长。由于哈希后密码的大小与其长度无关，因此没有理由在用户愿意时禁止使用冗长的密码(或口令短语)。然而，极长的密码(可能是数兆字节长)可能需要过多的处理时间来进行哈希，因此设置某种限制是合理的。

A.3. 复杂性

组合规则通常被用来试图增加猜测用户所选密码的难度。然而，研究表明，用户对组合规则所施加的要求会以非常可预测的方式做出反应[Policies]。例如，原本可能选择"password"作为密码的用户，如果被要求包含大写字母和数字，则相对更可能选择"Password1"；如果还要求包含符号，则可能选择"Password1!"。

当在线服务拒绝用户创建复杂密码的尝试时，用户也会表达不满。许多服务拒绝包含空格和各种特殊字符的密码。不接受某些字符有时是为了避免依赖这些字符的攻击(例如，SQL注入)。然而，未哈希的密码不会完整地发送到数据库，因此此类预防措施是不必要的。用户还应能够包含空格字符以允许使用短语。重复的空格字符对密码的有效强度增加很少，并可能引入可用性问题(例如，未检测到使用了两个空格而不是一个)，因此如果初始验证失败，删除键入密码中的重复空格可能是有益的。

由于用户的密码选择往往可以预测，攻击者很可能猜出以前曾成功使用的密码。这些密码包括字典单词和来自以往泄露事件的密码，例如上面的"Password1!"示例。因此，用户选择的密码应与不可接受密码阻止列表进行比对。该列表应包括来自以往泄露密码集的密码、用作密码的字典单词，以及用户可能选择的具体单词(例如服务本身的名称)。由于最低长度要求也会约束用户对密码的选择，该字典只需包含满足该要求的条目。如第3.1.1.2节所述，

blocklist to be excessively large or comprehensive, since its primary purpose is to prevent the use of very common passwords that might be guessed in an online attack before throttling restrictions take effect. An excessively large blocklist will likely frustrate users who attempt to choose a memorable password.

Highly complex passwords introduce a new potential vulnerability: they are less likely to be memorable and more likely to be written down or stored electronically in an unsafe manner. While these practices are not necessarily vulnerable, some methods of recording such secrets will be. This is an additional motivation for not requiring excessively long or complex passwords.

A.4. Central vs. Local Verification

While passwords that are used as a separate authentication factor are often centrally verified by the CSP's verifier, those that are used as an activation factor for a multi-factor authenticator are either verified locally by the authenticator or used to derive the authenticator output, which will be incorrect if the wrong activation factor is used. Both of these situations are referred to as "local verification."

The attack surfaces and vulnerabilities for central and local verification are very different. Accordingly, the requirements for centrally verified passwords differ from those verified locally. Centrally verified passwords require the verifier (i.e., an online resource) to store salted and iteratively hashed verification secrets for all of the subscribers' passwords. Although the salting and hashing process increases the computational effort to determine the passwords from the hashes, the verifier is an attractive target for attackers, particularly those interested in compromising an arbitrary subscriber rather than a specific one.

Local verifiers do not have the same concerns with large-scale attacks on a central online verifier but depend on the physical security of the authenticator and the integrity of its associated endpoint. To the extent that the authenticator stores the activation factor, that factor must be protected against physical and *side-channel* (e.g., power and timing analysis) attacks on the authenticator. When the activation factor is entered through the associated endpoint, the endpoint needs to be free of malware (e.g., key-logging software). Since such threats are less dependent on the length and complexity of the password, these requirements are relaxed for local verification.

Online password-guessing attacks are a similar threat to centrally and locally verified passwords. Throttling is the primary defense against online attacks and can be particularly challenging for local verifiers because of the limited ability of some authenticators to securely store information about unsuccessful attempts. Throttling of local activation factors can be done in one of two ways. The authenticator itself could handle the throttling by keeping count of invalid activation attempts or, when activated incorrectly, the authenticator could produce an invalid authenticator output that will be rejected and throttled by the verifier.

阻止列表不应过于庞大或全面，因为其主要目的是防止使用那些在节流限制生效之前可能在线攻击中被猜到的非常常见的密码。过于庞大的阻止列表很可能会让试图选择可记忆密码的用户感到沮丧。

高度复杂的密码引入了一个新的潜在漏洞：它们不太可能被记住，更可能被写下来或以不安全的方式电子存储。虽然这些做法本身不一定存在漏洞，但记录此类密钥的某些方法会存在漏洞。这是不要求过长或过于复杂密码的另一个动机。

A.4. 集中式验证与本地验证

用作独立身份验证因素的密码通常由 CSP 的验证器集中验证，而用作多因素认证器激活因素的密码，要么由认证器本地验证，要么用于派生认证器输出；如果使用了错误的激活因素，输出将不正确。这两种情况都称为"本地验证"。

集中验证与本地验证的攻击面和漏洞非常不同。因此，集中验证密码的要求不同于本地验证密码的要求。集中验证密码要求验证器(即在线资源)为所有订阅者的密码存储加盐并迭代哈希的验证密钥。尽管加盐和哈希过程增加了从哈希值确定密码的计算工作量，但验证器仍是攻击者的有吸引力的目标，尤其是那些有意攻陷任意订阅者而非特定订阅者的攻击者。

本地验证器没有对集中在线验证器进行大规模攻击的同样担忧，但依赖于认证器的物理安全及其关联端点的完整性。如果认证器存储激活因子，则该因子必须受到保护，以防针对认证器的物理攻击和侧信道(例如功耗和时序分析)攻击。当激活因子通过关联端点输入时，该端点需要没有恶意软件(例如键盘记录软件)。由于此类威胁较少依赖于密码的长度和复杂性，因此本地验证的这些要求有所放宽。

在线密码猜测攻击对集中验证密码和本地验证密码是类似的威胁。限流是抵御在线攻击的主要防御手段，并且对本地验证器尤其具有挑战性，因为某些认证器安全存储有关不成功尝试信息的能力有限。本地激活因子的限流可以通过以下两种方式之一完成。认证器本身可以通过记录无效激活尝试次数来处理限流，或者当激活不正确时，认证器可以产生无效的认证器输出，该输出将被验证器拒绝并限流。

A.5. Summary

Length and complexity requirements beyond those recommended here significantly increase user frustration and the difficulty of using passwords. As a result, users often work around these restrictions counterproductively. Other mitigations (e.g., blocklists, secure hashed storage, machine-generated random passwords, rate limiting) are more effective at preventing modern brute-force attacks, so no additional password requirements are imposed.

A.5. 摘要

超出此处建议的长度和复杂度要求会显著增加用户的挫败感和使用密码的难度。结果，用户常常适得其反地绕过这些限制。其他缓解措施(例如，阻止列表、安全的哈希存储、机器生成的随机密码、速率限制)在防止现代暴力攻击方面更为有效，因此不施加额外的密码要求。

Appendix B. Syncable Authenticators

This appendix is normative.

B.1. Introduction

The ability to “sync” authenticators — specifically to copy (i.e., clone) their authentication secrets to the cloud and thence to additional authenticators — is a relatively new development in authentication. This appendix provides additional guidelines on the use of syncable authenticators.

B.2. Cloning Authentication Keys

In some cases, authentication keys may be stored in a sync fabric (e.g., cloud storage). This allows the keys to be backed up and transferred to other devices. The following requirements apply to keys that are managed in this manner:

- All keys **SHALL** be generated using approved cryptography.
- Authentication keys that are cloned or exported from a device to a sync fabric **SHALL** only be stored in an encrypted form using a key with the minimum security strength specified in the latest revision of [SP800-131A] (i.e., 112 bits as of the date of this publication). These keys **SHOULD** be encrypted using a method that employs a user-controlled secret.
- All authentication transactions **SHALL** perform private-key operations on the local device using cryptographic keys that are generated on-device or recovered from the sync fabric.
- Authentication keys stored in the sync fabric **SHALL** be protected by access control mechanisms such that only the authenticated user can access their authentication keys in the sync fabric.
- User access to authentication keys in the sync fabric **SHALL** be protected by AAL2-equivalent MFA to preserve the integrity of the authentication protocols using the synced keys.
- These general requirements and any other agency-specific requirements for using syncable authenticators **SHALL** be documented and communicated, including on public-facing websites and digital service policies, where applicable.
- Authenticators that enable the use of syncable authentication keys **SHOULD** provide a user interface (UI) that allows subscribers to view the services for which they have created a syncable authentication key, whether that key has been synced, and where that key has been synced. The UI **SHALL NOT** expose the authentication key itself.

附录 B.可同步认证器

本附录为规范性附录。

B.1. 引言

认证器的“同步”能力--具体而言，将其身份验证密钥复制(即克隆)到云端，再从云端复制到其他认证器--是身份验证领域相对较新的发展。本附录提供了关于使用可同步认证器的附加指南。

B.2. 克隆认证密钥

在某些情况下，身份验证密钥可能存储在同步结构(例如，云存储)中。这允许密钥被备份并传输到其他设备。以下要求适用于以这种方式管理的密钥：

- 所有密钥**SHALL**使用经批准的密码学生成。
- 从设备克隆或导出到同步架构的认证密钥 **SHALL**仅以加密形式存储，使用具有[SP800-131A]最新修订版中规定的最低安全强度的密钥(即截至本出版物发布之日为 112 位)。这些密钥**SHOULD**使用采用用户控制密钥的方法进行加密。
- 所有身份验证事务**SHALL**使用在设备上生成或从同步结构恢复的加密密钥，在本地设备上执行私钥操作。
- 存储在同步结构中的身份验证密钥**SHALL**受到访问控制机制的保护，使得只有经过身份验证的用户才能访问其在同步结构中的身份验证密钥。
- 用户对同步结构中身份验证密钥的访问**SHALL**受到等同于 AAL2 的 MFA 保护，以维护使用同步密钥的身份验证协议的完整性。
- 这些通用要求以及任何其他机构特定的使用可同步认证器的要求**SHALL**被记录并传达，包括在适用的面向公众的网站和数字服务政策上。
- 支持使用可同步身份验证密钥的认证器**SHOULD**提供用户界面(UI)，允许订阅者查看其已为其创建可同步身份验证密钥的服务、该密钥是否已同步以及该密钥已同步到何处。该 UI **SHALL NOT**暴露身份验证密钥本身。

The following additional requirements apply to federal enterprise[8] use of syncable authenticators:

- Federal enterprise authentication keys **SHALL** be stored in sync fabrics that have achieved Federal Information Security Modernization Act (FISMA) [FISMA] moderate protections or equivalent.
- Devices (e.g., mobile phones, laptops, tablets) that generate, store, and sync authenticators containing federal enterprise authentication keys **SHALL** be protected by mobile device management software or other device configuration controls that prevent the syncing or sharing of keys to unauthorized devices or sync fabrics.
- Access to the sync fabric **SHALL** be controlled by agency-managed accounts (e.g., a central identity and access management solution, platform-based managed account) to maintain federal enterprise control over the authentication key's life cycle.
- Authenticators that generate authentication keys **SHOULD** support attestation features that can be used to verify the capabilities and sources of the authenticator (e.g., enterprise attestation).

These controls specifically support syncing and should be considered additive to the existing multi-factor cryptographic authenticator requirements and AAL2 requirements, including [FIPS140] validation.

> Syncing authentication keys inherently means that the key can be exported. Authentication at AAL2 may be supported subject to the above requirements. However, syncing violates the non-exportability requirements of AAL3. Similar protocols using keys not stored in an exportable manner that meet the other requirements of AAL3 may be used.

B.3. Implementation Requirements

Many syncable authenticators are built on W3C's [WebAuthn] specification, which provides a common data structure, a challenge-response cryptographic protocol, and an API for leveraging public-key credentials. The specification is flexible and adaptive, meaning that not all deployments of WebAuthn credentials will meet the requirements of federal agencies for implementation.

The specification has a series of flags that the RP application can request from the authenticator to provide additional context for the authentication event and determine

[8] Federal enterprise systems include those considered in scope for PIV guidance, such as government contractors, government employees, and mission partners. It does not include government-to-consumer or public-facing use cases.

以下附加要求适用于联邦企业[8]对可同步认证器的使用：

- 联邦企业身份验证密钥**SHALL**存储在已获得联邦信息安全管理现代化法案(FISMA)[FISMA]中等保护或同等保护的同步结构中。
- 生成、存储和同步包含联邦企业身份验证密钥的认证器的设备(例如，移动电话、笔记本电脑、平板电脑)**SHALL**受到移动设备管理软件或其他设备配置控件的保护，以防止将密钥同步或共享到未经授权的设备或同步结构。
- 对同步结构的访问**SHALL**由机构管理的账户(例如，集中式身份和访问管理解决方案、基于平台的管理账户)控制，以维护联邦企业对身份验证密钥生命周期的控制。
- 生成身份验证密钥的认证器**SHOULD**支持可用于验证认证器能力和来源的证明功能(例如，企业证明)。

这些控制专门支持同步，应被视为对现有多因素加密认证器要求和 AAL2 要求的补充，包括[FIPS140]验证。

> 同步身份验证密钥本质上意味着密钥可以被导出。在满足上述要求的前提下，可以支持 AAL2 级别的身份验证。然而，同步违反了 AAL3 的不可导出性要求。可以使用类似协议，使用不以可导出方式存储且满足 AAL3 其他要求的密钥。

B.3. 实施要求

许多可同步认证器基于 W3C 的[WebAuthn]规范构建，该规范提供了通用数据结构、质询-响应加密协议以及利用公钥凭证的 API。该规范灵活且具有适应性，这意味着并非所有 WebAuthn 凭证的部署都能满足联邦机构的实施要求。

该规范包含一系列标志，RP 应用程序可以向认证器请求这些标志，以便为身份验证事件提供额外的上下文并确定

8 联邦企业系统包括被视为符合 PIV 指南范围的系统，例如政府承包商、政府雇员和任务合作伙伴。它不包括政府对消费者或面向公众的用例。

whether it meets the RP's access policies. This section describes certain flags in the WebAuthn specification that federal agencies acting as RPs should understand and interrogate when building their syncable authenticator implementations to align with AAL2 guidelines.

The following requirements apply to WebAuthn Level 3 flags:

User Present (UP)

The User Present flag indicates that a "presence" test confirmed that the user has interacted with the authenticator (e.g., tapping a hardware token inserted into a USB port). This supports authentication intent, as described in Sec. 3.2.8. Verifiers **SHOULD** confirm that the User Present flag has been set.

User Verified (UV)

The User Verified flag indicates that the authenticator has locally authenticated the user using one of the available "user verification" methods. Verifiers **SHALL** indicate that UV is preferred and **SHALL** inspect responses to confirm the value of the UV flag. This indicates whether the authenticator can be treated as a multi-factor cryptographic authenticator. If the user is not verified, agencies **SHALL** treat the authenticator as a single-factor cryptographic authenticator. A further extension to the WebAuthn Level 3 specification (see Sec. 10.3 of [WebAuthn]) provides additional data on verification methods if agencies seek to gain context on the local authentication event.

Backup Eligible

The Backup Eligible flag indicates whether the authenticator can be synced to a different device (i.e., whether the key can be stored elsewhere). It is important to note that just because an authenticator *can* be synced does not mean that it *has* been synced. Verifiers **MAY** use this flag to establish policies that restrict the use of syncable authenticators. This flag is necessary to distinguish authenticators that are device-bound from those that may be cloned to more than one device.

Backup State

The Backup State flag indicates whether an authenticator *has* been synced to a different device. Verifiers **MAY** use this flag to establish restrictions on authenticators that are synced to other devices. Agencies **SHOULD NOT** condition acceptance based on this flag for public-facing applications due to user experience concerns.

In addition to the flags specified above, agencies may wish to gain additional information on the origins and capabilities of the syncable authenticators that they choose to implement and accept. Within the context of WebAuthn, some authenticators support attestation features that can be used to determine the capabilities and manufacturers of

其是否满足 RP 的访问策略。本节描述了 WebAuthn 规范中的某些标志，作为 RP 的联邦机构在构建其可同步认证器实现以符合 AAL2 指南时应理解并审查这些标志。

以下要求适用于 WebAuthn Level 3 标志：

用户在场(UP)

User Present 标志表示"存在"测试确认用户已与认证器交互(例如，点击插入 USB 端口的硬件令牌)。这支持身份验证意图，如Sec.3.2.8所述。验证器**SHOULD**确认 User Present 标志已设置。

用户验证(UV)

用户验证标志表示认证器已使用可用的"用户验证"方法之一在本地对用户进行了身份验证。验证器**SHALL**表明首选UV，并且**SHALL**检查响应以确认UV标志的值。这表明认证器是否可以被视为多因素加密认证器。如果用户未经验证，机构**SHALL**将认证器视为单因素加密认证器。WebAuthn Level 3规范的进一步扩展(见[WebAuthn]第10.3节)提供了关于验证方法的附加数据，如果机构希望获得有关本地身份验证事件的上下文。

可备份

Backup Eligible 标志指示认证器是否可以同步到不同的设备(即密钥是否可以存储在别处)。需要注意的是，认证器能够被同步并不意味着它已经被同步。验证器**可以**使用此标志来制定限制使用可同步认证器的策略。此标志对于区分设备绑定的认证器与可能被克隆到多个设备的认证器是必要的。

备份状态

Backup State 标志表示认证器*has*是否已同步到其他设备。验证器**MAY**使用此标志对同步到其他设备的认证器建立限制。出于用户体验方面的考虑，机构**SHOULD NOT**对面向公众的应用程序以此标志为条件决定是否接受。

除上述标志外，机构可能希望获取有关其选择实现和接受的可同步认证器的来源和能力的额外信息。在 WebAuthn 的上下文中，某些认证器支持可用于确定特定认证器的能力和制造商的证明功能。

specific authenticators. For federal enterprise use cases, agencies **SHOULD** implement attestation capabilities based on the functionality offered by their platform providers. This would take the form of a manufacturer attestation in which the RP requests identifying information about the authenticator.

The unavailability of attestations **SHOULD NOT** block the use of syncable authenticators for broad public-facing applications. Due to the limited availability of attestations in consumer products, requiring their use is likely to divert users to less secure authentication options that are vulnerable to phishing (e.g., PSTN-based out-of-band authentication). While authentication transaction metadata (e.g., the User Verified flag indicating the use of a local activation factor) is available in WebAuthn responses, attestation can provide stronger assurance of the characteristics of the authenticator used in a transaction. RPs **SHOULD** use attestation to determine the level of confidence they have in a syncable authenticator when attestations are available.

When the RP receives flag and attestation data, the authenticator may provide information that is incomplete or inconsistent with access to a resource. Agencies **SHALL** evaluate the use cases for syncable authenticators and determine the appropriate access policy decisions that they intend to make based on the returned information.

B.4. Sharing

Cybersecurity guidelines have historically cautioned against sharing authenticators between users. Rather, different users are expected to maintain their own unique authenticators. Despite this, authenticator and password sharing occurs within some user groups and applications to allow individuals to share access to a digital account.

As indicated in Table 5, some syncable authenticator implementations have embraced this user behavior and established methods for sharing authentication keys between different users. Further, some implementations actively encourage sharing syncable authenticators as a convenient and more secure alternative to sharing passwords for common services.

For enterprise use cases, concerns over sharing keys can be effectively mitigated using device management techniques that limit the ability for keys to be moved off of approved devices or sync fabrics. However, similar mitigations are not currently available for public-facing use cases, leaving RPs dependent on the sharing models adopted by syncable authenticator providers. Owners of public-facing applications should be aware of the risks associated with shared authenticators. When interacting with the public, agencies have limited visibility into which specific authenticators are being employed by their users and should assume that all syncable authenticators may be subject to sharing. While many sharing models have substantial controls that minimize risks (e.g., requiring close proximity between devices to allow sharing), other implementations are less restrictive.

对于联邦企业用例，机构**SHOULD**基于其平台提供商提供的功能实现证明能力。这将采取制造商证明的形式，其中 RP 请求有关认证器的标识信息。

对于广泛的面向公众的应用，证明的不可用性**不应**阻止可同步认证器的使用。由于消费类产品中证明的可用性有限，要求使用证明可能会将用户转向安全性较低、易受网络钓鱼攻击的身份验证选项(例如，基于 PSTN 的带外身份验证)。虽然身份验证事务元数据(例如，指示使用了本地激活因子的 User Verified 标志)在 WebAuthn 响应中可用，但证明可以为事务中使用的认证器的特性提供更强的保证。当证明可用时，RP 应使用证明来确定他们对可同步认证器的信任程度。

当 RP 收到标志和证明数据时，认证器可能提供不完整或与资源访问不一致的信息。机构**SHALL**评估可同步认证器的用例，并确定其打算基于返回信息做出的适当访问策略决策。

B.4. 共享

网络安全指南历来告诫不要在不同用户之间共享认证器。相反，不同用户应维护各自独有的认证器。尽管如此，在某些用户群体和应用程序中仍存在认证器和密码共享的情况，以允许个人共享对数字账户的访问权限。

如Table 5所示，某些可同步认证器实现已接受这种用户行为，并建立了在不同用户之间共享身份验证密钥的方法。此外，某些实现积极鼓励共享可同步认证器，作为共享常用服务密码的一种便捷且更安全的替代方案。

对于企业用例，可以使用设备管理技术来有效缓解对密钥共享的担忧，这些技术限制密钥移出已批准设备或同步架构的能力。然而，类似的缓解措施目前尚不适用于面向公众的用例，使得 RP 依赖于可同步认证器提供商所采用的共享模型。面向公众的应用的所有者应了解与共享认证器相关的风险。在与公众交互时，机构对用户正在使用哪些特定认证器的可见性有限，应假设所有可同步认证器都可能受到共享的影响。虽然许多共享模型具有大量控制措施以最小化风险(例如，要求设备之间近距离才能允许共享)，但其他实现则限制较少。

The risk of sharing posed by this new class of authenticators is not unique. It applies to all authenticator types, some of which are weaker than syncable authenticators. Any authenticator can be shared by a user who is determined to share it. Users can actively share passwords, OTPs, out-of-band authenticators, and even push-based authentication events that allow a designee (whether formal or not) to authenticate on behalf of an end user.

Agencies determine which authenticators they will accept for their applications based on the specific risks, threats, and usability considerations they face. Syncable authenticators may be offered as a new option for applications that seek to implement up to AAL2. The trade-offs of this technology should be balanced with expected outcomes for security, privacy, and user experience.

B.5. Example

A common use of syncable authenticators is in an AAL2 authentication transaction. The following items summarize how WebAuthn syncable authenticators satisfy aspects of AAL2 requirements:

Phishing resistance (recommended, required for federal enterprise)

Achieved: Properly configured syncable authenticators create a unique public or private key pair whose use is constrained to the domain in which it was created (i.e., the key can only be used with a specific website or RP). This prevents a falsified web page from being able to capture and reuse an authenticator output.

Replay resistance (required)

Achieved: Syncable authenticators prevent replay resistance (i.e., prevention of reuse in future transactions) through a random nonce that is incorporated into each authentication transaction.

Authentication intent (required)

Achieved: Syncable authenticators require users to present an activation factor (i.e., activation secret, biometric characteristic) to initiate the cryptographic authentication protocol. This serves as authentication intent, as the event cannot proceed without the user's active participation.

Multi-factor (required)

Achieved: The User Verified flag value indicates whether a local authentication mechanism (i.e., an activation factor) was used to complete the transaction. Without user verification, the verifier prompts for an additional authentication factor as part of the transaction.

If the subscriber provides their own authenticator, the verifier may have limited visibility into the features and capabilities of the sync fabric and the devices to which the user

这类新型认证器所带来的共享风险并非独有。它适用于所有认证器类型，其中一些比可同步认证器更弱。任何认证器都可能被决心共享它的用户共享。用户可以主动共享密码、OTP、带外认证器，甚至基于推送的身份验证事件，从而允许指定人员(无论是否正式)代表最终用户进行身份验证。

机构根据其面临的具体风险、威胁和可用性考虑，确定其应用程序将接受哪些认证器。对于寻求实现至多 AAL2 的应用程序，可同步认证器可作为新选项提供。该技术的权衡应与安全性、隐私和用户体验的预期结果相平衡。

B.5. 示例

可同步认证器的一个常见用途是在 AAL2 身份验证事务中。以下各项总结了 WebAuthn 可同步认证器如何满足 AAL2 要求的各个方面：

抗网络钓鱼能力(推荐，联邦企业必需)

Achieved：正确配置的可同步认证器创建唯一的公钥或私钥对，其使用被限制在创建它的域内(即，该密钥只能与特定网站或 RP 一起使用)。这可以防止伪造的网页捕获并重用认证器输出。

重放抵抗(必需)

Achieved：可同步认证器通过纳入每个身份验证事务的随机 nonce 来防止重放(即，防止在未来事务中重用)。

认证意图(必需)

Achieved：可同步认证器要求用户提供激活因子(即，激活密钥、生物特征)以启动加密身份验证协议。这作为身份验证意图，因为没有用户的主动参与，该事件无法继续。

多因素(必需)

Achieved:User Verified 标志值表示是否使用本地身份验证机制(即，激活因子)完成事务。未经用户验证，验证器会提示提供额外的身份验证因子作为事务的一部分。

如果订阅者提供自己的认证器，验证器对同步结构以及用户可能将身份验证密钥同步到的设备的特性和能力的可见性可能有限。

may sync their authentication keys. In this scenario, the verifier **SHOULD** leverage additional risk indicators or trust signals that may be available from the transaction, device, or sync fabric to increase confidence in the authentication event.

Syncable authenticators are not unique in this respect. Any subscriber-provided authenticator is subject to the same risks as syncable authenticators, including OTP authenticators and nearly all out-of-band authenticators. It is important for CSPs and IdPs to assess each type of authenticator that they offer at each assurance level and determine which are acceptable based on their users and transaction types.

B.6. Security Considerations

Syncable authenticators present distinct threats and challenges that agencies should evaluate before implementation or deployment, as shown in Table 5.

Table 5. Syncable authenticator threats, challenges, and mitigations

Threat or Challenge	Description	Mitigations
Unauthorized key use or loss of control	Some syncable authenticator deployments support sharing authentication keys to devices that belong to other users who can then misuse the key.	Enforce enterprise device management features or managed profiles that prevent synced keys from being shared.
		Provide mechanisms for users to view keys, key statuses, and whether/where keys have been shared.
		Educate users about the risks of unauthorized key use through existing awareness and training mechanisms.
Sync fabric compromise	To support key syncing, most implementations clone keys to a sync fabric (i.e., a cloud-based service connected to multiple devices associated with an account).	Store only encrypted key material.

Continued on next page

在这种情况下，验证器**SHOULD**利用可能从事务、设备或同步结构获得的额外风险指标或信任信号，以增加对身份验证事件的信心。

可同步认证器在这方面并非独有。任何由订阅者提供的认证器都面临与可同步认证器相同的风险，包括 OTP 认证器和几乎所有带外认证器。CSP 和 IdP 必须评估其在每个保证等级提供的每种认证器类型，并根据其用户和事务类型确定哪些是可接受的。

B.6. 安全考虑

可同步认证器带来了机构在实施或部署之前应评估的独特威胁和挑战，如Table 5所示。

表 5.可同步认证器的威胁、挑战与缓解措施

威胁或挑战	描述	缓解措施
未授权密钥使用或丢失控制	某种可同步的认证器部署支持共享将身份验证密钥发送到设备属于其他用户，这些用户随后可能滥用该密钥。	强制企业设备管理功能或受管理的配置文件，以防止同步密钥以免共享。
		为用户提供查看密钥、密钥状态以及密钥是否/在何处被共享的机制。
		通过现有的意识和培训机制，教育用户了解未经授权使用密钥的风险。
同步结构泄露	为了支持密钥同步，大多数实现克隆密钥到同步结构(即，连接到与账户关联的多个设备的基于云的服务)。	仅存储加密的密钥材料。

下页续

Continued from previous page

Threat or Challenge	Description	Mitigations
		Implement sync fabric access controls that prevent anyone other than the authenticated user from accessing the authentication key.
		Evaluate cloud services for baseline security features (e.g., FISMA moderate protections or comparable).
		Leverage hardware security modules to protect encrypted keys.
Unauthorized access to sync fabric and recovery	Synced keys are accessible via cloud-based account recovery processes, which represent a potential weakness to the authenticators.	Implement authentication recovery processes that are consistent with SP 800-63B.
		Restrict recovery capabilities for federal enterprise keys through device management or managed account capabilities.
		Bind multiple authenticators at AAL2 and above to support recovery.
		Require AAL2 authentication to add any new authenticators for user access to the sync fabric.
		Only use synced keys as a derived authenticator in federal enterprise scenarios [SP800-157].
		Notify the user of any recovery activities.

Continued on next page

续上页

威胁或挑战	描述	缓解措施
		实施同步结构访问控制，防止除经过身份验证的用户之外的任何人访问身份验证密钥。
		评估云服务的基线安全功能(例如 FISMA 中等保护或同等保护)。
		利用硬件安全模块保护加密数据 密钥。
未授权同步访问织物和恢复	同步的密钥可通过基于云端的账户恢复流程，这些流程代表一个潜在的弱点认证器。	实施身份验证恢复流程访问，这些流程与 SP 800-63B 一致。
		通过设备管理或受管账户限制联邦企业密钥的恢复能力 能力。
		在AAL2及以上级别绑定多个认证 恢复。
		要求 AAL2 身份验证才能添加任何新的认证器以供用户访问同步架构的设备上。
		在联邦企业场景中仅将同步密钥用作派生认证器[SP800-157]。
		通知用户任何恢复情况活动。

下页续

Continued from previous page

Threat or Challenge	Description	Mitigations
		Leverage a user-controlled secret (i.e., something not known to the sync fabric provider) to encrypt and recover keys.
Revocation	Since syncable authenticators use RP-specific keys, the ability to centrally revoke access based on those keys is challenging. For example, with traditional PKI, CRLs can be used centrally to revoke access. A similar process is not available for syncable authenticators or any FIDO WebAuthn-based credentials.	Implement a central identity management (IDM) account for users to manage authenticators and remove them from the "home agency" account if they are compromised or expired.
		Leverage SSO and federation to limit the number of RP-specific keys that will need to be revoked in an incident.
		Establish policies and tools to request that users periodically review keys for validity and currency.

续上页

威胁或挑战	描述	缓解措施
		利用用户控制的秘密(即同步结构提供方不知道的内容)来加密和恢复密钥。
撤销	由于可同步的认证器使用特定于 RP 的密钥，基于这些密钥集中撤销访问的能力具有挑战性。例如，在传统 PKI 中，CRL 可用于集中撤销访问。对于可同步认证器或任何基于 FIDO WebAuthn 的凭证，则没有类似的流程。	实施一个中央身份管理(IDM)账户供用户管理认证器并进行移除将它们从"主机构"账户，如果它们被泄露或过期。
		利用 SSO 和联合身份来限制在事件中需要撤销的 RP 专用密钥的数量。
		制定策略和工具，要求用户定期审查密钥的有效性并货币。

Appendix C. List of Symbols, Abbreviations, and Acronyms

AAL
Authentication Assurance Level

ASCII
American Standard Code for Information Interchange

CAC
Common Access Card

CSP
Credential Service Provider

CSRF
Cross-Site Request Forgery

DNS
Domain Name System

FEDRAMP
Federal Risk and Authorization Management Program

FIPS
Federal Information Processing Standards

FMR
False Match Rate

FNMR
False Non-Match Rate

IAL
Identity Assurance Level

IdP
Identity Provider

KBA
Knowledge-Based Authentication

附录 C.符号、缩写和首字母缩略语列表 AAL

认证保证等级

ASCII
美国信息交换标准代码

CAC
通用访问卡

CSP
凭证服务提供商

CSRF
跨站请求伪造

DNS
域名系统

FEDRAMP
联邦风险与授权管理计划

FIPS
联邦信息处理标准

FMR
错误匹配率

FNMR
错误不匹配率

IAL
身份保证等级

IdP
身份提供方

KBA
基于知识的认证

MAC
Message Authentication Code

MF
Multi-Factor

MFA
Multi-Factor Authentication

NARA
National Archives and Records Administration

NFC (communications protocol)
Near-Field Communication

OTP
One-Time Password

OWASP
Open Worldwide Application Security Project

PAD
Presentation Attack Detection

PIA
Privacy Impact Assessment

PIN
Personal Identification Number

PIV
Personal Identity Verification

PKI
Public-Key Infrastructure

PSTN
Public Switched Telephone Network

QR
Quick Response

MAC
消息认证码

MF
多因素

MFA
多因素认证

NARA
国家档案与记录管理局

NFC(通信协议)近场通信

OTP
一次性密码

OWASP
开放全球应用程序安全项目

PAD
呈现攻击检测

PIA
隐私影响评估

PIN
个人识别码

PIV
个人身份验证

PKI
公钥基础设施

PSTN
公共交换电话网

QR
快速响应

RP
Relying Party

SAOP
Senior Agency Official for Privacy

SF
Single-Factor

SMS
Short Message Service

SORN
System of Records Notice

SSO
Single Sign-On

TEE
Trusted Execution Environment

TLS
Transport Layer Security

TPM
Trusted Platform Module

USB
Universal Serial Bus

VOIP
Voice-Over-IP

XSS
Cross-Site Scripting

RP
依赖方

SAOP
隐私高级机构官员

SF
单因素

SMS
短信服务

SORN
系统记录通知

SSO
单点登录

TEE
可信执行环境

TLS
传输层安全

TPM
可信平台模块

USB
通用串行总线

VOIP
IP 语音

XSS
跨站脚本

Appendix D. Glossary

This section is informative.

A wide variety of terms are used in the realm of digital identity. While many definitions are consistent with earlier versions of SP 800-63, some have changed in this revision. Many of these terms lack a single, consistent definition, warranting careful attention to how the terms are defined here.

account recovery
The ability to regain ownership of a *subscriber account* and its associated information and privileges.

activation
The process of inputting an *activation factor* into a *multi-factor authenticator* to enable its use for *authentication*.

activation factor
An additional *authentication factor* that is used to enable successful *authentication* with a *multi-factor authenticator*.

activation secret
A *password* that is used locally as an *activation factor* for a *multi-factor authenticator*.

applicant
A *subject* undergoing the processes of *identity proofing* and *enrollment*.

approved cryptography
An encryption algorithm, *hash function*, random bit generator, or similar technique that is *Federal Information Processing Standards* (FIPS)-approved or NIST-recommended. Approved algorithms and techniques are either specified or adopted in a FIPS or NIST recommendation.

assertion
A statement from an *IdP* to an *RP* that contains information about an authentication event for a *subscriber*. Assertions can also contain identity *attributes* for the subscriber in the form of attribute values, derived attribute values, and attribute bundles.

asymmetric keys
Two related *cryptographic keys* comprised of a *public key* and a *private key* that are used to perform complementary operations, such as encryption and decryption or signature verification and generation.

附录 D.术语表

本节为说明性内容。

数字身份领域使用了各种各样的术语。虽然许多定义与 SP 800-63 的早期版本一致，但本修订版中有些定义已发生变化。其中许多术语缺乏单一、一致的定义，因此需要仔细注意此处对这些术语的界定方式。

账户恢复
重新获得订阅者账户及其关联信息和权限所有权的能力。

激活
将激活因子输入多因素认证器以使其可用于身份验证的过程。

激活因子
用于实现多因素认证器成功身份验证的附加身份验证因子。

激活密钥
在本地用作多因素认证器的激活因子的密码。

申请人
正在经历身份核验和注册登记过程的主体。

批准的密码技术
经联邦信息处理标准(FIPS)批准或 NIST 推荐的加密算法、哈希函数、随机比特生成器或类似技术。经批准的算法和技术在 FIPS 或 NIST 建议中予以规定或采纳。

断言
由*IdP*向*RP*发送的、包含有关订阅者身份验证事件信息的声明。断言还可以以属性值、派生属性值和属性包的形式包含订阅者的身份属性。

非对称密钥
由公钥和私钥组成的两个相关加密密钥，用于执行互补操作，例如加密和解密或签名验证和生成。

attestation
Information conveyed to the *CSP*, generally at the time that an *authenticator* is bound, to describe the characteristics of a connected authenticator or the *endpoint* involved in an authentication operation.

attribute
A quality or characteristic ascribed to someone or something. An identity attribute is an attribute about the identity of a *subscriber* (e.g., name, date of birth, address).

attribute validation
The process or act of confirming that a set of *attributes* are accurate and associated with a real-life identity. See *validation*.

authenticate
See *authentication*.

authenticated protected channel
An encrypted communication channel that uses *approved cryptography* in which the connection initiator (client) has *authenticated* the recipient (server). Authenticated protected channels are encrypted to provide confidentiality and protection against active intermediaries and are frequently used in the user *authentication* process. *Transport Layer Security* (TLS) and Datagram Transport Layer Security (DTLS) [RFC9325] are examples of authenticated protected channels in which the certificate presented by the recipient is verified by the initiator. Unless otherwise specified, authenticated protected channels do not require the server to authenticate the client. Authentication of the server is often accomplished through a certificate chain that leads to a trusted root rather than individually with each server.

authenticated session
See *protected session*.

authentication
The process by which a *claimant* proves possession and control of one or more *authenticators* bound to a *subscriber account* to demonstrate that they are the *subscriber* associated with that account.

authentication assurance level (AAL)
A category that describes the strength of the *authentication* process.

authentication factor
The three types of authentication factors are *something you know*, *something you have*, and *something you are*. Every *authenticator* has one or more authentication factors.

证明
传达给*CSP*的信息，通常在认证器绑定之时，用于描述所连接认证器或身份验证操作中所涉端点的特征。

属性
归属于某人或某物的品质或特征。身份属性是关于订阅者身份的属性(例如姓名、出生日期、地址)。

属性验证
确认一组属性准确且与真实身份相关联的过程或行为。参见验证。

认证
见认证。

认证保护通道
一种加密通信信道，使用批准的密码学，其中连接发起方(客户端)已对接收方(服务器)进行身份验证。经过身份验证的受保护信道经过加密以提供机密性并防范主动中间人攻击，常用于用户身份验证过程。传输层安全(TLS)和数据报传输层安全(DTLS)[RFC9325]是经过身份验证的受保护信道的示例，其中接收方出示的证书由发起方验证。除非另有规定，经过身份验证的受保护信道不要求服务器对客户端进行身份验证。服务器的身份验证通常通过指向受信任根的证书链完成，而非逐个服务器单独进行。

已认证会话见受保护会话。

身份验证
声称者证明拥有并控制绑定到订阅者账户的一个或多个认证器，以表明其是与该账户关联的订阅者的过程。

认证保证等级(AAL)
描述身份验证过程强度的类别。

认证因素
三种身份验证因子类型是你知道的东西、你拥有的东西和你是什么。每个认证器都有一个或多个身份验证因子。

authentication intent
The process of confirming the *claimant's* intent to *authenticate* or reauthenticate by requiring user intervention in the authentication flow. Some *authenticators* (e.g., OTPs) establish authentication intent as part of their operation. Others require a specific step to establish intent, such as pressing a button. Authentication intent is a countermeasure against malware at the *endpoint* as a proxy for authenticating an attacker without the *subscriber*'s knowledge.

authentication key
A private or symmetric key used by an authenticator to generate the authenticator output.

authentication protocol
A defined sequence of messages between a *claimant* and a *verifier* that demonstrates that the claimant has possession and control of one or more valid *authenticators* to establish their identity and, optionally, demonstrates that the claimant is communicating with the intended verifier.

authentication secret
A generic term for any secret value that is used to verify the *subscriber* in an *authentication protocol*. These are further divided into *short-term authentication secrets*, which are only useful to an attacker for a limited period of time, and *long-term authentication secrets*, which allow an attacker to impersonate the subscriber until they are manually reset. The *authenticator* secret is the canonical example of a long-term authentication secret, while the *authenticator output* — if it is different from the authenticator secret — is usually a short-term authentication secret.

authenticator
Something that the *subscriber* possesses and controls (e.g., a *cryptographic module* or *password*) and that is used to *authenticate* a *claimant's* identity. See *authenticator type* and *multi-factor authenticator*.

authenticator binding
The establishment of an association between a specific *authenticator* and a *subscriber account* that allows the *authenticator* to authenticate the *subscriber* associated with the account, possibly in conjunction with other authenticators.

authenticator output
The output value generated by an *authenticator*. The ability to generate valid authenticator outputs on demand proves that the *claimant* possesses and controls the authenticator. Protocol messages sent to the *verifier* depend on the authenticator output, but they may or may not explicitly contain it.

认证意图
通过在身份验证流程中要求用户干预，确认声称者意图进行身份验证或重新身份验证的过程。某些认证器(例如OTP)在其操作过程中建立身份验证意图。其他认证器则需要特定步骤来建立意图，例如按下按钮。身份验证意图是针对端点恶意软件的一种对策，防止攻击者在订阅者不知情的情况下作为其代理进行身份验证。

认证密钥
认证器用于生成认证器输出的私钥或对称密钥。

认证协议
声称者与验证器之间已定义的消息序列，用于证明声称者拥有并控制一个或多个有效认证器以确立其身份，并可选地证明声称者正在与预期的验证器通信。

认证密钥
用于在身份验证协议中验证订阅者的任何秘密值的通用术语。这些秘密值进一步分为短期身份验证秘密(仅在一段有限时间内对攻击者有用)和长期身份验证秘密(允许攻击者冒充订阅者，直至被手动重置)。认证器秘密是长期身份验证秘密的典型示例，而认证器输出--如果它与认证器秘密不同--通常是短期身份验证秘密。

认证器
订阅者拥有并控制的东西(例如加密模块或密码)，用于认证声称者的身份。参见认证器类型和多因素认证器。

认证器绑定
在特定认证器与订阅者账户之间建立关联，使该认证器能够认证与该账户关联的订阅者，可能与其他认证器结合使用。

认证器输出
由认证器生成的输出值。按需生成有效认证器输出的能力证明声称者拥有并控制该认证器。发送给验证器的协议消息取决于认证器输出，但可能显式包含也可能不显式包含该输出。

authenticator type
A category of *authenticators* with common characteristics, such as the types of *authentication factors* they provide and the mechanisms by which they operate.

authenticity
The property that data originated from its purported source.

authorize
A decision to grant access, typically automated by evaluating a *subject*'s *attributes*.

biometric sample
An analog or digital representation of biometric characteristics prior to biometric feature extraction, such as a record that contains a fingerprint image.

biometrics
Automated recognition of individuals based on their biological or behavioral characteristics. Biological characteristics include but are not limited to fingerprints, palm prints, facial features, iris and retina patterns, voice prints, and vein patterns. Behavioral characteristics include keystroke cadence, the angle of holding a smartphone, screen pressure, typing speed, mouse or mobile phone movements, and gyroscope position, among others.

blocklist
A documented list of specific elements that are blocked, per policy decision. This concept has historically been known as a "blacklist."

challenge-response protocol
An *authentication protocol* in which the *verifier* sends the *claimant* a challenge (e.g., a random value or *nonce*) that the claimant combines with a secret (e.g., by hashing the challenge and a *shared secret* together or by applying a *private-key* operation to the challenge) to generate a response that is sent to the verifier. The verifier can independently verify the response generated by the claimant (e.g., by recomputing the hash of the challenge and the shared secret and comparing it to the response or performing a public-key operation on the response) and establish that the claimant possesses and controls the secret.

claimant
A *subject* whose identity is to be verified using one or more *authentication protocols*.

claimed identity
An *applicant's* declaration of unvalidated and unverified personal *attributes*.

认证器类型
具有共同特征的一类认证器，例如它们提供的身份验证因子类型及其运行机制。

真实性
数据源自其声称来源的属性。

授权
授予访问权限的决定，通常通过评估主体的属性来自动完成。

生物特征样本
在生物特征提取之前对生物特征进行的模拟或数字表示，例如包含指纹图像的记录。

生物特征识别
基于个体的生物学或行为特征对其进行自动识别。生物学特征包括但不限于指纹、掌纹、面部特征、虹膜和视网膜图案、声纹以及静脉图案。行为特征包括击键节奏、握持智能手机的角度、屏幕压力、打字速度、鼠标或手机移动以及陀螺仪位置等。

阻止列表
根据策略决定而被阻止的特定元素的书面清单。此概念在历史上被称为"黑名单"。

质询-响应协议
一种身份验证协议，其中验证器向声称者发送质询(例如随机值或随机数)，声称者将其与秘密结合(例如将质询与共享秘密一起哈希，或对质询执行私钥操作)以生成发送给验证器的响应。验证器可以独立验证声称者生成的响应(例如重新计算质询与共享秘密的哈希并与响应比较，或对响应执行公钥操作)，并确认声称者拥有并控制该秘密。

声称者
其身份将使用一个或多个身份验证协议进行验证的主体。

声称身份
申请人对未经证实和未经核验的个人属性的声明。

credential
An object or data structure that authoritatively binds an identity — via an *identifier* — and (optionally) additional *attributes* to at least one *authenticator* that is possessed and controlled by a *subscriber*. A credential is issued, stored, and maintained by the *CSP*. Copies of information from the credential can be possessed by the subscriber, typically in the form of one or more digital certificates that are often contained in an authenticator along with their associated *private keys*.

credential service provider (CSP)
A trusted entity whose functions include *identity proofing applicants* to the identity service and registering *authenticators* to *subscriber accounts*. A CSP may be an independent third party.

cross-site request forgery (CSRF)
An attack in which a *subscriber* who is currently *authenticated* to an *RP* and connected through a secure session browses an attacker's website, causing the subscriber to unknowingly invoke unwanted actions at the RP. For example, if a bank website is vulnerable to a CSRF attack, it may be possible for a subscriber to unintentionally *authorize* a large money transfer by clicking on a malicious link in an email while a connection to the bank is open in another browser window.

cross-site scripting (XSS)
A vulnerability that allows attackers to inject malicious code into an otherwise benign website. These scripts acquire the permissions of scripts that are generated by the target website to compromise the confidentiality and integrity of data transfers between the website and clients. Websites are vulnerable if they display user-supplied data from requests or forms without sanitizing the data so that it is not executable.

cryptographic authenticator
An *authenticator* that proves possession of an *authentication secret* through direct communication with a *verifier* through a cryptographic *authentication protocol*.

cryptographic key
A value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification. For the purposes of these guidelines, key requirements shall meet the minimum requirements stated in Table 2 of [SP800-57Part1]. See *asymmetric keys* or *symmetric keys*.

cryptographic module
A set of hardware, software, or firmware that implements approved security functions, including cryptographic algorithms and key generation.

凭证
一种对象或数据结构，通过标识符将身份以及(可选的)附加属性权威性地绑定到至少一个由订阅者拥有并控制的认证器。凭证由*CSP*签发、存储和维护。凭证中的信息副本可由订阅者持有，通常以一个或多个数字证书的形式存在，这些证书通常与其关联的私钥一起包含在认证器中。

凭证服务提供方(CSP)
其职能包括对身份服务的申请人进行身份核验以及将认证器注册到订阅者账户的可信实体。CSP 可以是独立的第三方。

跨站请求伪造(CSRF)
一种攻击，其中当前已向*RP*完成认证并通过安全会话连接的订阅者浏览攻击者的网站，导致订阅者在不知情的情况下在RP处调用不需要的操作。例如，如果银行网站容易受到CSRF攻击，则订阅者可能在另一个浏览器窗口中与银行的连接处于打开状态时，通过点击电子邮件中的恶意链接，无意中授权一笔大额转账。

跨站脚本(XSS)
一种允许攻击者将恶意代码注入原本无害的网站的漏洞。这些脚本获取由目标网站生成的脚本的权限，从而破坏网站与客户端之间数据传输的机密性和完整性。如果网站显示来自请求或表单的用户提供的数据而未对数据进行清理以使其不可执行，则网站易受此攻击。

加密认证器
一种认证器，通过密码学身份验证协议与验证器直接通信，以证明对身份验证秘密的持有。

加密密钥
用于控制密码学操作(如解密、加密、签名生成或签名验证)的值。就本指南而言，密钥要求应满足[SP800-57Part1]表2中规定的最低要求。参见非对称密钥或对称密钥。

密码模块
实现经批准的安全功能(包括密码学算法和密钥生成)的一组硬件、软件或固件。

digital authentication
The process of establishing confidence in user identities that are digitally presented to a system. In previous editions of SP 800-63, this was referred to as "electronic authentication."

digital identity
An *attribute* or set of attributes that uniquely describes a *subject* within a given context.

digital signature
An *asymmetric key* operation in which the *private key* is used to digitally sign data, and the *public key* is used to verify the signature. Digital signatures provide *authenticity* protection, integrity protection, and *non-repudiation* support but not confidentiality or *replay attack* protection.

digital transaction
A discrete digital event between a user and a system that supports a business or programmatic purpose.

endpoint
Any device that is used to access a *digital identity* on a *network*, such as laptops, desktops, mobile phones, tablets, servers, Internet of Things devices, and virtual environments.

enrollment
The process through which a *CSP*/*IdP* provides a successfully identity-proofed *applicant* with a *subscriber account* and binds *authenticators* to grant persistent access.

entropy
The amount of uncertainty that an attacker faces to determine the value of a secret. Entropy is usually stated in bits. A value with *n* bits of entropy has the same degree of uncertainty as a uniformly distributed *n*-bit random value.

factor
See *authentication factor*.

Federal Information Processing Standards (FIPS)
Standards for adoption and use by federal departments and agencies that are developed by NIST, a part of the U.S. Department of Commerce. FIPS address topics in information technology to achieve common levels of quality, security, and interoperability. FIPS documents are available online on the FIPS home page: https://www.nist.gov/itl/fips.cfm.

数字认证
对以数字方式呈现给系统的用户身份建立信任的过程。在 SP 800-63 的先前版本中，这被称为"电子身份验证"。

数字身份
在给定上下文中唯一描述主体的属性或属性集。

数字签名
一种非对称密钥操作，其中使用私钥对数据进行数字签名，并使用公钥验证签名。数字签名提供真实性保护、完整性保护以及不可否认性支持，但不提供机密性或重放攻击保护。

数字交易
用户与系统之间支持业务或程序目的的离散数字事件。

端点
用于在网络上访问数字身份的任何设备，例如笔记本电脑、台式机、移动电话、平板电脑、服务器、物联网设备和虚拟环境。

注册登记
CSP / *IdP*向成功通过身份核验的申请人提供订阅者账户并绑定认证器以授予持久访问权限的过程。

熵
攻击者在确定秘密值时面临的不确定性量。熵通常以比特表示。具有*n*比特熵的值与均匀分布的*n*比特随机值具有相同程度的不确定性。

因素
见认证因素。

联邦信息处理标准(FIPS)
由 NIST(美国商务部的一部分)制定、供联邦部门和机构采用和使用的标准。FIPS 涉及信息技术主题，以实现质量、安全性和互操作性的共同水平。FIPS 文档可在 FIPS 主页在线获取：https://www.nist.gov/itl/fips.cfm。

federation
A process that allows for the conveyance of identity and *authentication* information across a set of *networked* systems.

federation assurance level (FAL)
A category that describes the process used in a *federation transaction* to communicate *authentication* events and subscriber *attributes* to an *RP*.

hash function
A function that maps a bit string of arbitrary length to a fixed-length bit string. Approved hash functions satisfy the following properties:

1. One-way — It is computationally infeasible to find any input that maps to any pre-specified output.
2. Collision-resistant — It is computationally infeasible to find any two distinct inputs that map to the same output.

identifier
A data object that is associated with a single, unique entity (e.g., individual, device, or *session*) within a given context and is never assigned to any other entity within that context.

identity
See *digital identity*.

identity assurance level (IAL)
A category that conveys the degree of confidence that the *subject*'s *claimed identity* is their real identity.

identity evidence
Information or documentation that supports the real-world existence of the *claimed identity*. Identity evidence may be physical (e.g., a driver's license) or digital (e.g., a mobile driver's license or digital *assertion*). Evidence must support both *validation* (i.e., confirming *authenticity* and accuracy) and *verification* (i.e., confirming that the *applicant* is the true owner of the evidence).

identity proofing
The processes used to collect, validate, and verify information about a *subject* to establish assurance in the subject's *claimed identity*.

identity provider (IdP)
The party in a *federation transaction* that creates an *assertion* for the *subscriber* and transmits the assertion to the *RP*.

联合身份
允许在一组联网系统之间传递身份和身份验证信息的过程。

联邦保证等级(FAL)
描述在联合身份事务中用于向*RP*传达身份验证事件和订阅者属性的过程的类别。

哈希函数
一种将任意长度的位字符串映射为固定长度位字符串的函数。经批准的哈希函数满足以下特性：

1. 单向性--在计算上不可能找到任何映射到任何预先指定输出的输入。
2. 抗碰撞性--在计算上不可能找到任何两个映射到同一输出的不同输入。

标识符
在给定上下文中与单个唯一实体(例如个人、设备或会话)相关联、且在该上下文中绝不会分配给任何其他实体的数据对象。

身份
见数字身份。

身份保证等级(IAL)
一种类别，用于传达对主体所声称的身份即其真实身份的可信程度。

身份证据
支持所声称身份在现实世界中存在的信息或文件。身份证据可以是物理形式的(例如，驾驶证)或数字形式的(例如，移动驾驶证或数字断言)。证据必须同时支持验证(即确认真实性和准确性)和核验(即确认申请人是证据的真实所有者)。

身份证明
用于收集、验证和核验关于主体的信息以建立对主体所声称身份的保证的过程。

身份提供方(IdP)
联合身份事务中为订阅者创建断言并将该断言传输给*RP*的一方。

injection attack
An attack in which an attacker supplies untrusted *biometric* information or media into a program or process. For example, this could include injecting a falsified image of *identity evidence*, a forged video of a user, or a morphed image to defeat evidence validation technology or biometric and visual comparisons for user verification.

manageability
Providing the capability for the granular administration of *personal information*, including alteration, deletion, and selective disclosure. [NISTIR8062]

memorized secret
See *password*.

message authentication code (MAC)
A cryptographic checksum on data that uses a *symmetric key* to detect both accidental and intentional modifications of the data. MACs provide *authenticity* and integrity protection but not *non-repudiation* protection.

mobile code
Executable code that is normally transferred from its source to another computer system for execution. This transfer is often through the *network* (e.g., JavaScript embedded in a web page) but may transfer through physical media as well.

multi-factor authentication (MFA)
An authentication system that requires more than one distinct type of *authentication factor* for successful authentication. MFA can be performed using a *multi-factor authenticator* or by combining *single-factor* authenticators that provide different types of factors.

multi-factor authenticator
An *authenticator* that provides more than one distinct *authentication factor*, such as a cryptographic authentication device with an integrated biometric sensor that is required to activate the device.

network
An open communications medium, typically the internet, used to transport messages between the *claimant* and other parties. Unless otherwise stated, networks are assumed to be open and subject to active (e.g., impersonation, *session* hijacking) and passive (e.g., eavesdropping) attacks at any point between the parties (e.g., claimant, *verifier*, *CSP*, *RP*).

注入攻击
一种攻击，攻击者将不受信任的生物特征信息或媒体提供给程序或进程。例如，这可能包括注入伪造的身份证据图像、用户的伪造视频或变形图像，以破坏证据验证技术或用于用户核验的生物特征和视觉比对。

可管理性
提供对个人信息进行细粒度管理的能力，包括更改、删除和选择性披露。[NISTIR8062]

记忆型密钥见口
令。

消息认证码(MAC)
对数据使用对称密钥的加密校验和，用于检测数据的意外和故意修改。MAC 提供真实性和完整性保护，但不提供不可否认性保护。

移动代码
通常从其来源传输到另一计算机系统以执行的可执行代码。这种传输通常通过网络(例如嵌入网页中的JavaScript)进行，但也可能通过物理介质传输。

多因素认证(MFA)
一种需要一种以上不同类型的身份验证因素才能成功完成身份验证的身份验证系统。MFA 可以通过多因素认证器来执行，也可以通过组合提供不同类型因素的单因素认证器来执行。

多因素认证器
一种提供一种以上不同类型身份验证因素的认证器，例如带有集成生物特征传感器且需要该传感器激活设备的加密身份验证设备。

网络
一种开放的通信媒介，通常是互联网，用于在声称者与其他方之间传输消息。除非另有说明，网络被假定为开放的，并且在各方(例如声称者、验证器、*CSP*、*RP*)之间的任何位置都可能遭受主动攻击(例如冒充、会话劫持)和被动攻击(例如窃听)。

nonce
A value used in security protocols that is never repeated with the same key. For example, nonces used as challenges in *challenge-response authentication protocols* must not be repeated until *authentication keys* are changed. Otherwise, there is a possibility of a *replay attack*. Using a nonce as a challenge is a different requirement than a random challenge because a nonce is not necessarily unpredictable.

non-repudiation
The capability to protect against an individual falsely denying having performed a particular transaction.

offline attack
An attack in which the attacker obtains some data (e.g., by eavesdropping on an authentication transaction or by penetrating a system and stealing security files) that the attacker is able to analyze in a system of their own choosing.

online attack
An attack against an *authentication protocol* in which the attacker either assumes the role of a *claimant* with a genuine *verifier* or actively alters the authentication channel.

online guessing attack
An attack in which an attacker performs repeated logon trials by guessing possible values of the *authenticator* output.

passphrase
A *password* that consists of a sequence of words or other text that a *claimant* uses to *authenticate* their identity. A passphrase is similar to a password in usage but is generally longer for added security.

password
A type of *authenticator* consisting of a character string that is intended to be memorized or memorable by the *subscriber* to permit the *claimant* to demonstrate *something they know* as part of an authentication process. Passwords were referred to as *memorized secrets* in the initial release of SP 800-63B.

personal identification number (PIN)
A *password* that typically consists of only decimal digits.

personal information
Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

随机数
安全协议中使用的一种不会在同一密钥下重复的值。例如，在质询-响应身份验证协议中用作质询的随机数，在身份验证密钥被更改之前不得重复。否则，可能存在重放攻击的风险。使用随机数作为质询与使用随机质询是不同的要求，因为随机数不一定不可预测。

不可否认性
防止个人虚假否认已执行特定交易的能力。

离线攻击
一种攻击，攻击者获取一些数据(例如通过窃听身份验证事务或通过渗透系统并窃取安全文件)，攻击者能够在他们自己选择的系统中分析这些数据。

在线攻击
一种针对身份验证协议的攻击，攻击者要么冒充声称者与真正的验证器交互，要么主动篡改身份验证信道。

在线猜测攻击
一种攻击，攻击者通过猜测认证器输出的可能值来反复尝试登录。

口令短语
一种由单词序列或其他文本组成的密码,声称者使用它来验证其身份。口令短语在使用上与密码类似，但通常更长以提供额外的安全性。

密码
一种认证器，由字符串组成，旨在由订阅者记忆或便于记忆，以使声称者能够在身份验证过程中证明其所知道的内容。在 SP 800-63B 的初始版本中，密码被称为记忆性秘密。

个人识别码(PIN)
A *password*，通常仅由十进制数字组成。

个人信息
可单独使用或与其他与特定个人相关联或可关联的信息结合使用，以区分或追踪个人身份的信息。

pharming
An attack in which an attacker causes the *subscriber* to be redirected to a fraudulent website, typically a fraudulent *verifier/RP* in the context of authentication. This could cause the subscriber to reveal sensitive information (e.g., a password) to the attacker, download harmful software, or contribute to a fraudulent act. This may be accomplished by corrupting an infrastructure service (e.g., the DNS) or the subscriber's endpoint.

phishing
An attack in which the *subscriber* is lured (usually through an email) to interact with a counterfeit *verifier/RP* and tricked into revealing information that can be used to masquerade as that subscriber to the real verifier/RP.

phishing resistance
The ability of the *authentication protocol* to prevent the disclosure of *authentication secrets* and valid *authenticator* outputs to an impostor *verifier* without reliance on the vigilance of the *claimant*.

physical authenticator
An *authenticator* that the *claimant* proves possession of as part of an authentication process.

possession and control of an authenticator
The ability to activate and use the *authenticator* in an *authentication protocol*.

predictability
Enabling reliable assumptions by individuals, owners, and operators about *personal information* and its *processing* by an information system. [NISTIR8062]

presentation attack
Presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system.

presentation attack detection (PAD)
Automated determination of a *presentation attack*. A subset of presentation attack determination methods (i.e., liveness detection) involves the measurement and analysis of anatomical characteristics or voluntary or involuntary reactions to determine whether a *biometric sample* is being captured from a living *subject* that is present at the point of capture.

Privacy Impact Assessment (PIA)
A method of analyzing how *personal information* is collected, used, shared, and maintained. PIAs are used to identify and mitigate privacy risks throughout the

域欺骗
一种攻击，攻击者使订阅者被重定向到欺诈性网站，通常在身份验证上下文中是欺诈性验证器/*RP*。这可能导致订阅者向攻击者泄露敏感信息(例如密码)、下载有害软件或助长欺诈行为。这可以通过破坏基础设施服务(例如DNS)或订阅者的端点来实现。

网络钓鱼
一种攻击，其中订阅者被引诱(通常通过电子邮件)与假冒的验证器/*RP*进行交互，并被诱骗泄露可用于冒充该订阅者向真实验证器/RP进行身份验证的信息。

抗钓鱼
身份验证协议在不依赖声称者警惕性的情况下，防止身份验证秘密和有效认证器输出泄露给冒充验证器的能力。

物理认证器
声称者在身份验证过程中证明其拥有的认证器。

认证器的持有和控制
在身份验证协议中激活和使用认证器的能力。

可预测性
使个人、所有者和操作者能够对个人信息及其由信息系统进行的处理做出可靠假设。[NISTIR8062]

呈现攻击
向生物特征数据采集子系统进行的呈现，目的是干扰生物特征系统的运行。

呈现攻击检测(PAD)
对呈现攻击的自动判定。呈现攻击判定方法的一个子集(即活体检测)涉及测量和分析解剖特征或自愿或非自愿反应，以确定是否正在从采集点存在的活体主体采集生物特征样本。

隐私影响评估(PIA)
一种分析个人信息如何被收集、使用、共享和维护的方法。PIA用于在整个

development life cycle of a program or system. They also help ensure that handling information conforms to legal, regulatory, and policy requirements regarding privacy.

private key
A cryptographic key used with a public-key cryptographic algorithm that is uniquely associated with an entity and is not made public. In an asymmetric-key (public-key) cryptosystem, the private key has a corresponding *public key*. Depending on the algorithm, the private key may be used to:

1. Compute the corresponding public key,
2. Compute a digital signature that may be verified by the corresponding public key,
3. Decrypt keys that were encrypted by the corresponding public key, or
4. Compute a shared secret during a key-agreement transaction.

protected session
A *session* in which messages between two participants are encrypted and integrity is protected using a set of *shared secrets* called "session keys." A protected session is said to be *authenticated* if one participant proves possession of one or more *authenticators* in addition to the session keys and if the other party can verify the identity associated with the authenticators during the session. If both participants are authenticated, the protected session is said to be *mutually authenticated*.

pseudonym
A name other than a legal name.

pseudonymous identifier
A meaningless but unique *identifier* that does not allow the *RP* to infer anything regarding the *subscriber* but that does permit the RP to associate multiple interactions with a single subscriber.

public key
A cryptographic key used with a public-key cryptographic algorithm that is uniquely associated with an entity and that may be made public. In an asymmetric-key (public-key) cryptosystem, the public key has a corresponding *private key*. The public key may be known by anyone and, depending on the algorithm, may be used to:

1. Verify a digital signature that was generated using the corresponding private key,
2. Encrypt keys that can be decrypted using the corresponding private key, or
3. Compute a shared secret during a key-agreement transaction.

项目或系统的开发生命周期中识别和缓解隐私风险。它们还有助于确保信息处理符合有关隐私的法律、法规和政策要求。

私钥
与公钥密码算法一起使用的加密密钥，与实体唯一关联且不公开。在非对称密钥(公钥)密码系统中，私钥具有对应的公钥。根据算法的不同，私钥可用于：

1. 计算相应的公钥，
2. 计算可由相应公钥验证的数字签名，
3. 解密由对应公钥加密的密钥，或
4. 在密钥协商事务期间计算共享密钥。

受保护的会话
一种会话，其中两个参与者之间的消息使用一组称为"会话密钥"的共享密钥进行加密并保护完整性。如果一个参与者除会话密钥外还证明拥有一个或多个认证器，并且另一方能够在会话期间验证与这些认证器相关联的身份，则该受保护的会话被称为已认证。如果两个参与者都已认证，则该受保护的会话被称为双向认证。

假名
法定姓名以外的姓名。

假名标识符
一个无意义但唯一的标识符，不允许*RP*推断任何关于订阅者的信息，但允许RP将多次交互关联到单个订阅者。

公钥
与公钥密码算法一起使用的加密密钥，与实体唯一关联且可以公开。在非对称密钥(公钥)密码系统中，公钥具有对应的私钥。公钥可被任何人所知，并且根据算法的不同，可用于：

1. 验证使用相应私钥生成的数字签名，
2. 使用对应私钥可解密的加密密钥，或
3. 在密钥协商事务期间计算共享密钥。

public-key certificate
A digital document issued and digitally signed by the *private key* of a certificate authority that binds an *identifier* to a subscriber's *public key*. The certificate indicates that the *subscriber* identified in the certificate has sole control of and access to the *private key*. See also [RFC5280].

public-key infrastructure (PKI)
A set of policies, processes, server platforms, software, and workstations used to administer certificates and public-private key pairs, including the ability to issue, maintain, and revoke *public-key certificates*.

reauthentication
The process of confirming the *subscriber*'s continued presence and intent to be *authenticated* during an extended usage *session*.

relying party (RP)
An entity that relies on a *verifier*'s *assertion* of a *subscriber*'s identity, typically to process a transaction or grant access to information or a system.

remote
A process or transaction that is conducted through connected devices over a *network* rather than in person.

replay attack
An attack in which the attacker is able to replay previously captured messages between a legitimate *claimant* and a *verifier* to masquerade as that claimant to the verifier or vice versa.

replay resistance
The property of an authentication process to resist *replay attacks*, typically by the use of an *authenticator* output that is only valid for a specific authentication.

restricted authenticator
An *authenticator* type, class, or instantiation that has additional risk of false acceptance associated with its use and is therefore subject to additional requirements.

risk assessment
The process of identifying, estimating, and prioritizing risks to organizational operations (i.e., mission, functions, image, reputation), organizational assets, individuals, and other organizations that result from the operation of a system. A risk assessment is part of *risk management*, incorporates threat and vulnerability analyses, and considers mitigations provided by security *controls* that are planned or in place. It is synonymous with "risk analysis."

公钥证书
由证书颁发机构的私钥签发并进行数字签名的数字文档，将标识符绑定到订阅者的公钥。证书表明证书中标识的订阅者对私钥拥有唯一控制权和访问权。另见[RFC5280]。

公钥基础设施(PKI)
用于管理证书和公私密钥对的一组策略、流程、服务器平台、软件和工作站，包括签发、维护和撤销公钥证书的能力。

重新身份验证
在延长的使用会话期间，确认订阅者持续存在以及有意被身份验证的过程。

依赖方(RP)
依赖验证器对订阅者身份的断言的实体，通常用于处理交易或授予对信息或系统的访问权限。

远程
通过连接的设备在网络上而非亲自进行的流程或交易。

重放攻击
一种攻击，攻击者能够在合法声称者与验证器之间重放先前捕获的消息，以冒充该声称者向验证器进行身份验证，或反之。

重放抵抗
身份验证流程抵抗重放攻击的特性，通常通过使用仅对特定身份验证有效的认证器输出来实现。

受限认证器
一种认证器类型、类别或实例，其使用具有额外的错误接受风险，因此受到额外要求的约束。

风险评估
识别、评估并优先排序因系统运行而对组织运营(即使命、职能、形象、声誉)、组织资产、个人及其他组织产生的风险的过程。风险评估是风险管理的一部分，纳入威胁和脆弱性分析，并考虑计划中或已到位的安全控制措施所提供的缓解措施。它与"风险分析"同义。

risk management
The program and supporting processes that manage information security risk to organizational operations (i.e., mission, functions, image, reputation), organizational assets, individuals, and other organizations and that include (i) establishing the context for risk-related activities, (ii) assessing risk, (iii) responding to risk once determined, and (iv) monitoring risk over time.

salt
A non-secret value used in a cryptographic process, usually to ensure that the results of computations for one instance cannot be reused by an attacker.

Senior Agency Official for Privacy (SAOP)
Person responsible for ensuring that an agency complies with privacy requirements, manages privacy risks, and considers the privacy impacts of all agency actions and policies that involve *personal information*.

session
A persistent interaction between a *subscriber* and an *endpoint*, either an *RP* or a *CSP*. A session begins with an authentication event and ends with a session termination event. A session is bound by the use of a session secret that the subscriber's software (e.g., browser, application, OS) can present to the RP to prove association of the session with the authentication event.

session hijack attack
An attack in which the attacker is able to insert themselves between a *claimant* and a *verifier* after a successful authentication exchange between the latter two parties. The attacker is able to pose as a *subscriber* to the verifier or vice versa to control *session* data exchange. Sessions between the claimant and the *RP* can be similarly compromised.

shared secret
A secret used in authentication that is known to the *subscriber* and the *verifier*.

side-channel attack
An attack enabled by the leakage of information from a physical cryptosystem. Characteristics that could be exploited in a side-channel attack include timing, power consumption, electromagnetic emissions, and acoustic emissions.

single-factor
A characteristic of an authentication system or an *authenticator* that requires only one *authentication factor* (i.e., something you know, something you have, or something you are) for successful authentication.

风险管理
管理对组织运营(即使命、职能、形象、声誉)、组织资产、个人及其他组织的信息安全风险的计划及支持流程，包括(i) 建立风险相关活动的背景，(ii) 评估风险，(iii) 在确定风险后响应风险，以及(iv) 随时间监控风险。

盐值
在密码学流程中使用的非秘密值，通常用于确保某一实例的计算结果不能被攻击者重用。

隐私高级机构官员(SAOP)
负责确保机构遵守隐私要求、管理隐私风险，并考虑涉及个人信息的所有机构行动和政策的隐私影响的人员。

会话
订阅者与端点(*RP*或*CSP*)之间的持久交互。会话以身份验证事件开始，以会话终止事件结束。会话通过使用会话密钥进行绑定，订阅者的软件(例如浏览器、应用程序、操作系统)可以向 RP 出示该密钥，以证明该会话与身份验证事件的关联。

会话劫持攻击
一种攻击，攻击者在声称者与验证器之间成功完成身份验证交换后，能够将自己插入到这两方之间。攻击者能够向验证器冒充订阅者，或反之，以控制会话数据交换。声称者与*RP*之间的会话也可能以类似方式被破坏。

共享密钥
在身份验证中使用的、为订阅者和验证器所知的秘密。

侧信道攻击
一种因物理密码系统信息泄露而得以实施的攻击。
可在侧信道攻击中被利用的特征包括时序、功耗、电磁辐射和声学辐射。

单因素
身份验证系统或认证器的一种特性，仅需一个身份验证因素(即你知道的某物、你拥有的某物或你本身的某物)即可成功完成身份验证。

single sign-on (SSO)
An authentication process by which one account and its *authenticators* are used to access multiple applications in a seamless manner, generally implemented with a *federation protocol*.

social engineering
The act of deceiving an individual into revealing sensitive information, obtaining unauthorized access, or committing fraud by associating with the individual to gain confidence and trust.

subject
A person, organization, device, hardware, *network*, software, or service. In these guidelines, a subject is a *natural person*.

subscriber
An individual enrolled in the *CSP* identity service.

subscriber account
An account established by the *CSP* for each *subscriber* enrolled in its identity service that contains information about the subscriber and a record of any *authenticators* registered to the subscriber.

symmetric key
A *cryptographic key* used to perform both the cryptographic operation and its inverse (e.g., to encrypt and decrypt or to create a *message authentication code* and verify the code).

sync fabric
Any on-premises, cloud-based, or hybrid service used to store, transmit, or manage *authentication keys* generated by syncable *authenticators* that are not local to the user's device.

syncable authenticators
Software or hardware cryptographic *authenticators* that allow *authentication keys* to be cloned and exported to other storage to sync those keys to other authenticators (i.e., devices).

system of record (SOR)
A collection of records that contain information about individuals and are under the control of an agency. The records can be retrieved by the individual's name, an identifying number, a symbol, or other *identifier*.

单点登录(SSO)
一种身份验证流程，通过该流程，一个账户及其认证器以无缝方式用于访问多个应用程序，通常通过联合身份协议实现。

社会工程
通过与个人建立关系以获取信心和信任，从而欺骗个人泄露敏感信息、获取未经授权的访问或实施欺诈的行为。

主体
个人、组织、设备、硬件、网络、软件或服务。在本指南中，主体是自然人。

订阅者
已注册到*CSP*身份服务的个人。

用户账户
由*CSP*为其身份服务中登记的每个订阅者建立的账户，包含有关该订阅者的信息以及注册到该订阅者的任何认证器的记录。

对称密钥
用于执行密码学操作及其逆操作的密码密钥(例如加密和解密，或创建消息认证码并验证该码)。

同步结构
用于存储、传输或管理由可同步认证器生成的、不在用户设备本地的身份验证密钥的任何本地部署、基于云或混合服务。

可同步认证器
允许身份验证密钥被克隆并导出到其他存储，以将这些密钥同步到其他认证器(即设备)的软件或硬件密码学认证器。

记录系统(SOR)
包含有关个人的信息并受机构控制的记录集合。这些记录可通过个人的姓名、识别号码、符号或其他标识符检索。

System of Records Notice (SORN)
A notice that federal agencies publish in the Federal Register to describe their *system of record*.

token
See *authenticator*.

transaction
See *digital transaction*.

Transport Layer Security (TLS)
An authentication and security protocol that is widely implemented in browsers and web servers. TLS provides confidentiality, certificate-based authentication of the receiving (server) endpoint, and certificate-based authentication of the originating (client) endpoint. TLS is specified in [RFC8446] and [SP800-52].

usability
The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use. [ISO/IEC9241-11]

validation
The process or act of checking and confirming that the evidence and *attributes* supplied by an *applicant* are authentic, accurate, and associated with a real-life identity. See *attribute validation*.

verification
The process or act of confirming that the *applicant* undergoing *identity proofing* holds the claimed real-life identity represented by the validated identity *attributes* and associated evidence. Synonymous with *identity verification*.

verifier
An entity that confirms the *claimant's* identity by verifying the claimant's possession and control of one or more *authenticators* using an *authentication protocol*. To do this, the verifier needs to confirm the binding of the authenticators with the *subscriber account* and check that the subscriber account is active.

verifier impersonation
See *phishing*.

系统记录通知(SORN)
联邦机构在《联邦公报》上发布的、用于描述其记录系统的通知。

令牌
见认证器。

交易
见数字交易。

传输层安全(TLS)
一种在浏览器和 Web 服务器中广泛实现的身份验证和安全协议。TLS 提供机密性、接收(服务器)端点的基于证书的身份验证，以及发起(客户端)端点的基于证书的身份验证。TLS 在[RFC8446]和[SP800-52]中规定。

可用性
产品在特定使用情境下，被指定用户用于实现指定目标时所具有的有效性、效率和满意度程度。[ISO/IEC9241-11]

验证
检查并确认申请人所提供的证据和属性真实、准确且与真实身份相关联的过程或行为。参见属性验证。

核实
确认正在接受身份核验的申请人持有由已验证的身份属性及相关证据所代表的所声称真实身份的过程或行为。与身份核实同义。

验证器
通过使用身份验证协议核实声称者对一项或多项认证器的持有和控制，从而确认声称者身份的实体。为此，验证器需要确认认证器与订阅者账户的绑定，并检查该订阅者账户处于活动状态。

验证器冒充见网络钓鱼。

Appendix E. Change Log

This appendix is informative.

This appendix provides an overview of the changes made to SP 800-63B since its initial release.

- Removes Purpose, Definitions, and Abbreviations numbered sections and renumbers sections accordingly. The section numbers referenced below are the new section numbers.
- Changes the name of *memorized secrets* to *passwords*
- Section 2: Describes the use of fraud indicators rather than pre-authentication checks
- Section 2.3.2: Reduces required FIPS 140 validation level for authenticators at AAL3
- Section 2.3.2: Requires a non-exportable cryptographic authenticator rather than a hardware-based authenticator at AAL3
- Section 3.1.1.2: Increases the minimum length of passwords used as a single authentication factor
- Section 3.1.3: Disallows the comparison of secrets from primary and secondary channel for out-of-band authentication
- Section 3.1.3.1: Removes the prohibition on the use of VoIP phone numbers for out-of-band authentication
- Section 3.1.3.4: Recognizes multi-factor out-of-band authenticators that require an activation factor
- Section 3.1.4 and Sec. 3.1.5: Removes “devices” from the authenticator name to recognize OTP applications
- Section 3.1.6 and Sec. 3.1.7: Removes “software” and “device” distinction from the authenticator name and refers to them as “authenticator characteristics”
- Section 3.1.7.3: Adds requirements for authentication using subscriber-controlled wallets
- Section 3.1.7.4 and Appendix B: Adds requirements for syncable authenticators
- Section 3.2.3: Updates biometric performance requirements and metrics
- Section 3.2.3.2: Requires PAD for facial recognition and prohibits biometric comparison based on voice
- Section 3.2.5: Adds a definition and updates requirements for phishing-resistant authenticators

附录 E.变更日志

本附录为资料性内容。

本附录概述了自 SP 800-63B 首次发布以来所做的变更。

- 删除了目的、定义和缩写的编号章节，并相应重新编号各章节。下文引用的章节编号为新的章节编号。
- 将*memorized secrets*的名称更改为*passwords*
- 第 2 节：描述使用欺诈指标而非预身份验证检查
- 第 2.3.2 节：降低了 AAL3 认证器所需的 FIPS 140 验证级别
- 第 2.3.2 节：在 AAL3 要求使用不可导出的加密认证器，而非基于硬件的认证器
- 第 3.1.1.2 节：提高了用作单一身份验证因素的密码的最小长度
- 第 3.1.3 节：禁止对带外身份验证比较来自主信道和辅助信道的密钥
- 第 3.1.3.1 节：删除了禁止使用 VoIP 电话号码进行带外身份验证的规定
- 第 3.1.3.4 节：认可需要激活因素的多因素带外认证器
- 第 3.1.4 节和第 3.1.5 节：从认证器名称中删除“设备”，以认可 OTP 应用程序
- 第 3.1.6 节和第 3.1.7 节：从认证器名称中删除“软件”和“设备”的区分，并将其称为“认证器特性”
- 第 3.1.7.3 节：增加了使用订阅者控制的钱包进行身份验证的要求
- 第3.1.7.4节和附录B：增加了对可同步认证器的要求
- 第3.2.3节：更新生物特征性能要求和指标
- 第 3.2.3.2 节：要求对人脸识别使用 PAD，并禁止基于语音的生物特征比对
- 第 3.2.5 节：增加了抗钓鱼的认证器的定义并更新了要求

- Section 3.2.10: Establishes separate requirements for locally verified memorized secrets known as *activation secrets*
- Section 3.2.11: Adds requirements for authenticators that are connected via wireless technologies, such as NFC and Bluetooth
- Section 3.2.11.3: Recognizes hybrid connections as a class of connected authenticators
- Section 3.2.12: Centralizes the requirements for random values used throughout the document
- Section 3.2.13: Adds a new section on requirements for the non-exportability of authenticator secrets
- Section deleted: Removes verifier compromise resistance as a distinctly named requirement because it is generally a characteristic of the chosen authenticator type
- Section 4: Renames section to “Authenticator Event Management”
- Section 4.1.1: Moves binding at enrollment to SP 800-63A
- Section 4.1.2.1: Generalizes binding an additional authenticator to all AALs
- Section 4.1.2.2: Adds requirements for binding authenticators that are not connected to an endpoint
- Section 4.2: Revises the requirements and methods for account recovery
- Section 4.6: Revises the requirements for notifications sent to subscribers
- Section 5.1: Recognizes the use of device-bound session credentials
- Section 5.1.1: Adds requirements for browser cookies used for session maintenance
- Section 5.2: Revises reauthentication requirements to define the overall structure of reauthentication here and specify timeout values in the AAL requirements
- Section 5.3: Adds guidelines for the use of session monitoring (continuous authentication)

- 第3.2.10节：为本地验证的记忆性秘密(称为激活秘密)制定单独的要求
- 第3.2.11节：增加对通过无线技术(如NFC和蓝牙)连接的认证器的要求
- 第3.2.11.3节：将混合连接识别为一类连接式认证器
- 第3.2.12节：集中规定文档中使用的随机值要求
- 第3.2.13节：新增关于认证器秘密不可导出性要求的章节
- 删除章节：移除验证器抗泄露作为单独命名的要求，因为它通常是所选认证器类型的一个特性
- 第4节：将章节标题改为“认证器事件管理”
- 第 4.1.1 节：将注册时的绑定移至 SP 800-63A
- 第 4.1.2.1 节：将绑定附加认证器的要求推广至所有 AAL
- 第4.1.2.2节：增加对未连接到端点的认证器绑定的要求
- 第4.2节：修订了账户恢复的要求和方法
- 第4.6节：修订了向用户发送通知的要求
- 第5.1节：认可使用设备绑定的会话凭证
- 第5.1.1节：增加对用于会话维护的浏览器cookie的要求
- 第5.2节：修订重新身份验证要求，在此定义重新身份验证的整体结构，并在AAL要求中规定超时值
- 第5.3节：增加关于使用会话监控(持续身份验证)的指南

How this file was made

This is a complete Chinese translation of NIST SP 800-63B-4, Digital Identity Guidelines: Authentication and Lifecycle Management. Tables, captions, headers, footers and numbering all keep their original positions. Nothing has been cut.

If you have documents of your own

- Contracts, tenders, standards, patents, reports: original layout kept, CNY 0.15/page
- PDF to Word: free up to 100 pages, CNY 0.10/page beyond that
- Scanned or image-only PDFs: OCR to Word, free
- No sign-up, no login: upload and download

Open the address below and try it with your own file:

https://www.ivyivy.com.cn/nist-800-63b-4-zh

On-premise deployment available (subject to model and compliance review)

Machine translation, provided for reading reference only. For professional judgement and compliance citation, please refer to the original English source.

This page is a translator's note; it is not part of the original document.

这份文件是怎么做出来的

本译本是《数字身份指南：认证与生命周期管理（SP 800-63B-4）》的中文全译本，共 129 页。表格、图注、页眉页脚、编号层级都按原文位置一一还原，未做任何删节。

你手上如果也有英文文件要处理

- 合同、标书、标准、专利、报告：翻译后保留原版式，0.15 元/页
- PDF 转 Word：100 页内免费，超出 0.1 元/页
- 扫描件、图片版 PDF：先 OCR 再转 Word，免费
- 不用注册、不用登录，传上去直接下载

打开下面这个地址，把你自己的文件传上去试试：

https://www.ivyivy.com.cn/nist-800-63b-4-zh

支持私有化部署（需按贵方模型与合规要求评估）

本译本由机器翻译生成，仅供阅读参考；专业技术判断与合规引用，请以英文原文为准。

本页为译制说明，不属于原文件内容。