Wed, 18 Oct 2017 06:55:32 +0000

NIST Special Publication 800-63
Revision 3

Digital Identity Guidelines (翻訳版)

Paul A. Grassi
Michael E. Garcia
James L. Fenton

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63-3

COMPUTER SECURITY

NIST Special Publication 800-63-3

Digital Identity Guidelines

Paul A. Grassi Michael E. Garcia *Applied Cybersecurity Division* *Information Technology Laboratory*	James L. Fenton *Altmode Networks* *Los Altos, CA*
	翻訳者: Nov Matake *YAuth.jp LLC*

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63-3

June 2017

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Kent Rochford, Acting NIST Director and Under Secretary of Commerce for Standards and Technology

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 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.

National Institute of Standards and Technology Special Publication 800-63-3
Natl. Inst. Stand. Technol. Spec. Publ. 800-63-3, 73 pages (June 2017)
CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63-3

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment 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 http://csrc.nist.gov/publications/ (http://csrc.nist.gov/publications/).

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000
Email: dig-comments@nist.gov (mailto:dig-comments@nist.gov)

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

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 systems. The Special Publication 800-series reports on ITL’s research, guidelines, and outreach efforts in system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

These guidelines provide technical requirements for federal agencies implementing digital identity services and are not intended to constrain the development or use of standards outside of this purpose. The guidelines cover identity proofing and authentication of users (such as employees, contractors, or private individuals) interacting with government IT systems over open networks. They define technical requirements in each of the areas of identity proofing, registration, authenticators, management processes, authentication protocols, federation, and related assertions. This publication supersedes NIST Special Publication 800-63-2.

Keywords

authentication; authentication assurance; authenticator; assertions; credential service provider; digital authentication; digital credentials; identity proofing; federation; passwords; PKI.

Acknowledgements

The authors gratefully acknowledge Kaitlin Boeckl for her artistic graphics contributions to all volumes in the SP 800-63 suite and the contributions of our many reviewers, including Joni Brennan from the Digital ID & Authentication Council of Canada (DIACC), Ellen Nadeau and Ben Piccarreta from NIST, and Danna Gabel O'Rourke from Deloitte & Touche LLP.

In addition, the authors would like to acknowledge the thought leadership and innovation of the original authors: Donna F. Dodson, Elaine M. Newton, Ray A. Perlner, W. Timothy Polk, Sarbari Gupta, and Emad A. Nabbus. Without their tireless efforts, we would not have had the incredible baseline from which to evolve SP 800-63 to the document it is today.

Requirements Notation and Conventions

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, or 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.

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.

Executive Summary

This section is informative.

Digital Identity とはある Subject のオンライン上の Persona であり, その単一的な定義に関しては国際的に議論されている. Persona という語は, Subject がオンライン上で自身を多様に表現できるということを示す適した用語であろう. ある個人は, Email を利用する際の Digital Identity を持ちつつ, パーソナルファイナンス用に別の Digital Identity を持ちうる. ある個人のラップトップは, 誰かの音楽ストリーミングサーバーでありつつ, 複雑な遺伝子計算を行う分散コンピューターネットワーク内の1ワーカーボットでもありうる. コンテキストを考慮しないと, 全てを満たす単一の定義に帰着することは困難である.

法律上の Identity としての Digital Identity はさらに定義を複雑にし, Digital Identity をソーシャルやエコノミクスのユースケースにまたがって広く利用することも困難にする. Digital Identity とは難しいものである. ある人が, 自身の主張する人物であるということを - 特にリモートでデジタルサービスを通じて - 証明することは難しく, Attacker が誰かになりすます機会に満ちている. Peter Steiner in The New Yorker にも描かれている通り, “インターネットでは, 誰もあなたが犬であるとは知る由もない (On the internet, nobody knows you’re a dog.)” のである. 本ガイドラインはオンライン固有の脆弱性に対する対策を提供する. また対策の提示に際しては, 低リスクのデジタルサービスに Access する際には “being a dog” であっても問題ない一方, 高リスクのサービスでは当該 Digital Identity が実際の Subject の正当な代理であることを一定のレベルで保証できなければならない, ということを念頭に置く.

本ガイドライン群では, Digital Identity とは, オンライント上の Transaction に関与するある Subject を一意に表現するものである. Digital Identity は, 常にあるデジタルサービスのコンテキストにおいて一意となるが, すべてのコンテキストをまたいで Subject を一意に識別することは要件とはならない. 言い換えれば, デジタルサービスに Access したからといって, Subject の現実世界のアイデンティティが明らかになるとは限らない.

Identity Proofing は, ある Subject が自身で主張する主体であることを証明する行為である. Digital Authentication は, デジタルサービスに Access しようとしている Subject が, 当該 Subject の Digital Identity に紐付けられた正当な Authenticator を管理下に置いていることを証明する行為である. 繰り返し訪問されるサービスにおいて, Authentication に成功するということは, いまサービスに Access している Subject が以前に Access していた Subject と同一であることを, 適切なリスクに基づいて保証されたということである. Digital Identity は, しばしばオープンな Network を介した個人の Proofing を伴い, 政府のデジタルサービスに Access する際にはつねにオープンな Network を介した Subject の Authentication を伴うことから, 技術的課題をもたらす. Digital Identity を確立し利用するための一連のプロセスおよび技術は, なりすましやその他の Attack の機会と隣り合わせである.

本技術ガイドライン群は NIST Special Publication SP 800-63-2 に取って代わる. 各政府機関はこれらのガイドラインを自身のデジタルサービスの Risk Assessment および実装の一部として利用することとなる. 本ガイドライン群では, Identity Assurance を個別要素ごとに分割し, Authentication の誤りがもたらすネガティブインパクトへの対策を提供する. Non-federated なシステムでは, 政府機関はそれらのうち *Identity Assurance Level (IAL)* と *Authenticator Assurance Level (AAL)* という2つの要素を用いるであろう. Federated なシステムでは, それに加えて3つ目の要素となる *Federation Assurance Level (FAL)* も用いることとなろう.

本ガイドライン群は, 各実装固有の要件を追いやる単一の序数としての Level of Assurance (LOA) というコンセプトを諦め, 適切なビジネスおよびプライバシーに関する Risk Assessment のもと, 各機関が IAL, AAL, FAL を個別に選択するようにする. 多くのシステムで IAL, AAL, FAL がそれぞれ同じレベル値となるとしても, その値自体は要件ではなく, 各機関はいかなるシステムでもこの値が適切であるとみなすべきでもない.

Identity Assurance の構成要素は以下のガイドライン群に詳しい.

- **IAL** は, Identity Proofing プロセスについて述べる.
- **AAL** は, Authentication プロセスについて述べる.
- **FAL** は, Federated な環境において Authentication 情報 (および場合によっては Attribute 情報) を Relying Party (RP) に伝達する Assertion の強度について述べる.

これらのカテゴリーを分割することで, 各機関は Identity ソリューション選択の自由を獲得し, いかなる Assurance Level においても Identity システムの基本要素としてプライバシー強化手法を採用する余地を高める. 例えば, 本ガイドライン群では, 強固な多要素 Authenticator を用いる場合でも, Pseudonymous インタラクションを可能としている. また本ガイドライン群は, Federated Identity Provider (IdP) にデータ問い合わせに関する幅広い選択肢の用意を求め, 識別情報拡散の最小化を推奨している. このような選択肢の例としては, 生年月日をまるごと取得するのではなく, ある年齢より上かどうかを問い合わせられるようにするといったことがあげられる. 各機関が持つ多くのユースケースでは, 個人が完全に識別されていることが求められるであろうが, 本ガイドライン群は可能な限り政府のデジタルサービスへの Pseudonymous Access を推奨する. また完全な識別が必要な場合でも, 収集する Personal Information を最小化することが推奨される.

今日では, 組織における Identity ソリューションは単一システムや同一ベンダーが全機能を提供するといったモノリシックなものとは限らない. Identity サービスのマーケットは細分化され, 組織や機関は標準準拠かつプラガブルな Identity ソリューションを目的に合わせて採用することができるようになっている. そのようなことから, SP 800-63 は一連のドキュメントに分割されたのである. 以降この一連のドキュメント一式を “本ガイドライン群 (the guidelines)” と呼び, 個々のドキュメントは “Vol. (volumes)” と呼ぶ. RP は SP 800-63 を採用することが要求される. 残りの Vol. は, 各機関が求める要素サービスに応じて, 個別に用いても良いし一体的に用いても良い.

各 Vol. は様々な標準化団体で規範ないしは要件を示す国際的に認められた用語を用いる. 本ガイドライン群で規範的表現を用いるときには, それらは明示的に大文字表記 (CAPITALIZED) することとする. 例えば, SHALL は必須要件を示し, SHOULD は推奨されるが必須ではないということを示す. これらの用語の詳細は, 各ドキュメント冒頭の Requirements Notation and Conventions を参照のこと.

本ドキュメント群は E-Commerce などの連邦政府以外のアプリケーションにおける標準技術の開発・利用に関して言及することもあるが, 決してそれらのアプリケーションに対してなんらかの制限や制約を課すものではない.

本ガイドライン群は以下のような構成となっている.

SP 800-63 Digital Identity Guidelines (This document)

SP 800-63 では, 一般的な Identity Framework およびデジタルシステムにおける, Authenticator, Credential, Assertion の利用について概観し, リスクベースプロセスに基づく各 Assurance Level の選択方法について述べる. *SP 800-63 contains both normative and informative material.*

SP 800-63A Enrollment and Identity Proofing (sp800-63a.ja.html)

NIST SP 800-63-A では, Applicant が自身の Identity を提示し, 正当な Subscriber として Identity システムに登録されるまでの一連の流れについて記述する. この Vol. では, Remote と対面の両シナリオにおいて, Applicant が Identity を証明し登録する際のリスクレベルを3段階に分け, それぞれのレベルにおける要件をまとめる. *SP 800-63A contains both normative and informative material.*

SP 800-63A は所与の IAL を満たす要件を決める. 3つの IAL は, Attacker による不正な Identity の主張が成功してしまった場合を想定した各機関によるリスクプロファイリングと被害想定に基づいて, 各機関が選択できる選択肢を示す. 各 IAL は以下のとおりである.

IAL1: Applicant を特定の現実世界の Identity と紐づける必要はない. Authentication プロセスにおいて提供されるいかなる Attribute も Self-asserted であるものとする. (Credential Service Provider (CSP) が RP に対して Assert する Attribute も含む)

IAL2: Claimed Identity が現実世界に存在し, Applicant が現実世界の当該 Identity に適切に紐づいていることを検証し, それを証明すること. IAL2 では Remote もしくは対面での Identity Proofing が必要となる. CSP は, 検証済 Attribute を含む Pseudonymous Identity を許容しつつ, RP に対して Attribute を Assert する.

IAL3: 対面での Identity Proofing が要求される. 識別に用いられる Attribute は, 認可されトレーニングされた CSP の担当者によって検証される必要がある. IAL2 同様, CSP は, 検証済 Attribute を含む Pseudonymous Identity を許容しつつ, RP に対して Attribute を Assert する.

SP 800-63B Authentication and Lifecycle Management (sp800-63b.ja.html)

繰り返し訪問されるサービスにおいては, Authentication に成功することで, 今日当該サービスに Access している Subscriber が以前にサービスに Access してきた人物と同一であることが, 適切なリスクのもとで確かめられる. この信頼の頑健性は AAL カテゴリーによって記述される. NIST SP 800-63B では, デジタルサービスに Access する個人が CSP に対してセキュアに Authenticate されるプロセスを扱う. *SP 800-63B contains both normative and informative material.*

3つの AAL は, Attacker が Authenticator を手中に収め政府機関のシステムに Access できてしまった場合を想定した各機関によるリスクプロファイリングと被害想定に基づいて, 各機関が選択できる選択肢のサブセットを定義する. 各 AAL は以下のとおりである.

AAL1: AAL1 では, Claimant が Subscriber のアカウントに紐づく Authenticator を管理下に置いているということが, ある程度の確度で保証される. AAL1 では Single-facgtor ないしは Multi-factor Authenticator が求められるが, それらの Authenticator では幅広い種類の Authentication テクノロジーが利用可能である. Authentication を成功させるには, セキュアな Authentication Protocol によって Claimant が Authenticator を保持し管理下に置いていることを証明する必要がある.

AAL2: AAL2 では, Claimant が Subscriber のアカウントに紐づく Authenticator を管理下に置いているということが, 高い確度で保証される. セキュアな Authentication Protocol によって, 2つの異なる Authentication Factor を所有し管理下に置いていることを証明する必要がある. AAL2 以上では, Approved Cryptographic テクノロジーも必要となる.

AAL3: AAL3 では, Claimant が Subscriber のアカウントに紐づく Authenticator を管理下に置いているということが, 非常に高い確度で保証される. AAL3 の Authentication は, 暗号プロトコルによる鍵所有証明 (Proof of Possession) に基づいている. AAL3 の Authentication ではハードウェアベースの Cryptographic Authenticator および Verifier Inpersonation 耐性のある Authenticator の利用が必須となる

(SHALL). 同一デバイスがこれらの要件を同時に満たしてもよい (MAY). AAL3 で Authenticate するには, セキュアな Authentication Protocol によって, Claimant が 2つの異なる Authentication Factor を所有し管理下に置いていることを証明する必要がある (SHALL). Approved Cryptographic テクノロジーも必要となる.

SP 800-63C Federation and Assertions (sp800-63c.ja.html)

NIST SP 800-63C では, Federated Identity アーキテクチャーを採用したり, Authentication プロセスの結果と関連する Identity 情報を機関のアプリケーションに伝送する際に Assertion を利用するにあたっての要件について述べる. さらにこの Vol. では, 正当かつ Authenticated な Subject についての情報を共有する際のプライバシー強化手法や, Subject が Pseudonymous なまま強固な Multi-factor Authentication (MFA) を行う手法についても述べる. *SP 800-63C contains both normative and informative material.*

3つの FAL は, Attacker が Federated Transaction をコントロールできる状況に陥った場合を想定した各機関によるリスクプロファイリングと被害想定に基づいて, 各機関が選択できる選択肢を示す. 各 FAL は以下のとおりである.

FAL1: Subscriber は RP が Bearer Assertion を受け取ることを許容することができる. Assertion は Approved Cryptography を用いて IdP によって署名される.

FAL2: 上記に加え, Assertion は Approved Cryptography によって暗号化され, RP 以外が復号できないようになっていなければならない.

FAL3: Subscriber は Assertion Artifact に加え, Assertion が参照する Cryptographic Key の所有証明 (Proof of Possession) を提示する必要がある. Assertion は Approved Cryptography を用いて IdP によって署名され, RP に向けて暗号化されている必要がある.

本ガイドライン群は, 各機関が構築ないし調達可能な幅広い Identity サービスのアーキテクチャーについて感知しているわけではなく, 機関がどのようなアプローチをとったとしても適用できることを目的としている. しかしながら, 各機関が可能な場合には Federation を用いることを推奨し, Federated アーキテクチャーを採用する際に IAL, AAL, FAL をうまく組み合わせられるよう意図している. Federation は, 連邦政府の人々が政府のデジタルサービスに Access する際に Privacy を強化するための鍵となる.

Table of Contents

1. Purpose

2. Introduction

3. Definitions and Abbreviations

4. Digital Identity Model

5. Digital Identity Risk Management

6. Selecting Assurance Levels

7. Federation Considerations

8. References

Appendix A — Definitions and Abbreviations

1 Purpose

This section is informative.

本リコメンデーションおよび Special Publication (SP) 800-63A (sp800-63a.ja.html), SP 800-63B (sp800-63b.ja.html), SP 800-63C (sp800-63c.ja.html) は, 政府機関に対して Digital Authentication の実装に際した技術的なガイドラインを提示する.

2 Introduction

This section is informative.

Digital Identity はオンライン Transaction に関与する Subject を一意に表現するものである. Digital Identity は常にデジタルサービスのコンテキスト内でユニークであるが, 必ずしもあらゆるコンテキストをまたいで一意に Subject を識別するものである必要はない. 言い換えれば, あるデジタルサービスに Access する際に, Subject の現実世界での Identity を知る必要はないのである. Identity Proofing は, Subject が確かに自身が主張するものであるということを確立する. Digital Authentication は, Digital Identity を主張するために1つ以上の Authenticator の有効性を判断するプロセスである. Authentication により, あるデジタルサービスに Access しようとしている Subject が Authenticate のためのテクノロジーを管理下に置いていることが明らかになる. Authentication に成功すると, サービスに Access している Subject が以前に当該サービスに Access した主体と同一であることが, 適度なリスクベースの確からしさが得られる. Digital Identity に対するこういったプロセスにおいては, 個人に対してオープンな Network 越しに Proofing を行い, 典型的には個々の Subject がデジタル政府サービスにアクセスする際にオープンな Network 越しに Authentication を行うことになるため, Digital Identity には技術的なチャレンジがつきものである. そこでは, なりすましやその他の Attack など, 不正に他の Subject であると主張する機会が様々ある.

本リコメンデーションは, 各機関に対して, 政府システムにおいて Subject を Network 越しに Digital Authentication する際の技術的ガイドラインを提供する. 本リコメンデーションは Credential Service Provider (CSP), Verifier, Relying Party (RP) 向けのガイドラインも提供する.

本ガイドライン群では, 適切な Digital Identity サービスの選択に際する Risk Management プロセスや, Identity Assurance Level, Authenticator Assurance Level, Federation Assurance Level をリスクに基づいて実装する際の詳細について述べる. 本ガイドライン群が提供する Risk Assessment ガイダンスは, *NIST Risk Management Framework* [NIST RMF] およびその構成要素となる Special Publication を補完するものとなる. 本ガイドラインは各機関にさらなる Risk Management プロセスを課すものではなく, 全ての関連する RMF ライフサイクルフェーズ実行に際する Digital Identity のリスクに関しての具体的なガイダンスを提供するものである.

Digital Authentication は, 個人の情報への Unauthorized Access のリスクを軽減することによりプライバシー保護に寄与する. しかしながら同時に, Identity Proofing, Authentication, Authorization, Federation といった個々のフェーズにおいて個人の情報を扱うため, プライバシーリスクをもたらすことにもなる. したがって本ガイドライン群は, 潜在的に関連するプライバシーリスクを軽減するためのプライバシー要件や検討事項を含む.

本ガイドライン群は, Identity Assurance を個別要素ごとに分割することで, Authentication の誤りがもたらすネガティブインパクトの軽減に寄与する. Non-federated なシステムでは, 各機関はそれらのうち *Identity Assurance Level (IAL)* と *Authenticator Assurance Level (AAL)* という2つの要素を用いるであろう. Federated なシステムでは, それに加えて3つ目の要素となる *Federation Assurance Level (FAL)* も用いることとなろう. Section 5, Digital Identity Risk Management では Risk Assesment プロセスの詳細について述べる. Section 6, Selecting Assurance Levels は, Risk Assessment の結果と追加のコンテキストをふまえ, 機関によるリスクに応じた適切な IAL, AAL, FAL の選択の一助となる.

本ガイドライン群は, 実装固有の要件をもたらす単一の序数としての Level of Assurance (LOA) を構成するものではなく, ビジネス, セキュリティー, プライバシーのための適切な Risk Management をミッションニーズと組み合わせ, 各機関が個別に IAL, AAL, FAL を選択するためのものである. 特に本ドキュメントは, 各政府機関が以前利用し OMB M-04-04 でも述べられている4つの LOA モデルを認めず, 各機関が実施している各機能ごとに個別に各レベルを選択するよう求めている. 多くのシステムで IAL, AAL, FAL がそれぞれ同じレベル値となるとしても, その値自体は要件ではなく, 各機関はいかなるシステムでもこの値が適切であるとみなすべきでもない.

本ガイドライン群において詳しく扱う Identity Assurance の構成要素は以下の通りである.

- **IAL** は, Identity Proofing プロセスについて述べる.
- **AAL** は, Authentication プロセスについて述べる.
- **FAL** は, Federated な環境において Authentication 情報 (および場合によっては Attribute 情報) を Relying Party (RP) に伝達する Assertion Protocol について述べる.

SP 800-63 は以下のような一連の Vol. から構成される.

SP 800-63 *Digital Identity Guidelines*:　SP 800-63 では, Risk Assesment の方法論, デジタルシステムにおける Authenticator, Credential, Assertion を利用した一般的な Identity Framework の概観, およびリスクベースプロセスに基づく各 Assurance Level の選択方法について述べる. *SP 800-63 contains both normative and informative material.*

SP 800-63A *Enrollment and Identity Proofing*: NIST SP 800-63-A では, Applicant が自身の Identity を証明し, 正当な Subscriber として Identity システムに登録されるまでの一連の流れについて記述する. この Vol. では, Remote と対面の両シナリオにおいて, Applicant が Identity を証明し登録する際のリスクレベルを3段階に分け, それぞれのレベルにおける要件をまとめる. *SP 800-63A contains both normative and informative material.*

SP 800-63B *Authentication and Lifecycle Management*: NIST SP 800-63B では, デジタルサービスに Access する個人が CSP に対してセキュアに Authenticate されるプロセスを扱う. 本 Vol. では Authenticator を Identity に紐づけるプロセスについても記述する. *SP 800-63B contains both normative and informative material.*

SP 800-63C *Federation and Assertions*: NIST SP 800-63C では, Federated Identity アーキテクチャーを採用したり, Authentication プロセスの結果と関連する Identity 情報を機関のアプリケーションに伝送する際に Assertion を利用するにあたっての要件について述べる. さらにこの Vol. では, 正当かつ Authenticated な Subject についての情報を共有する際のプライバシー強化手法や, Subject が Pseudonymous なまま強固な Multi-factor Authentication (MFA) を行う手法についても述べる. *SP 800-63C contains both normative and informative material.*

NIST では, 本ガイドライン群中の個々の Vol. が非同期に改訂されることを想定している. いかなる場合でも, 各 Vol. のもっとも最新のリビジョンを用いること (e.g., ある時点において SP 800-63A-1 および SP 800-63B-2 がそれぞれの最新リビジョンであれば, 互いのリビジョン番号がずれていたとしてもそれらを同時に利用するべきである). 互換性エラーを最小化するため, ベースドキュメント (i.e., SP 800-63-3 ではなく SP 800-63) は常に本ドキュメントの最新バージョンを参照することとする.

下表は, 本 Vol. のどのセクションが Normative (規範) であり, どのセクションが Informative (参考) であるかを示している.

Section Name	**Normative/Informative**
1. Purpose	Informative
2. Introduction	Informative
3. Definitions and Abbreviations	Informative
4. Digital Identity Model	Informative
5. Digital Identity Risk Management	Normative
6. Selecting Assurance Levels	Normative
7. Federation Considerations	Informative
8. References	Informative

2.1 Applicability

全てのデジタルサービスが Authentication や Identity Proofing を必要とするわけではないが, 本ガイダンスはサービス対象 (e.g. 市民, ビジネスパートナー, 政府機関) によらず Digital Identity や Authentication が必要な全ての Transaction に適用される.

44 U.S.C. § 3542(b)(2) で定義される国家安全システム関連の Transaction は, 本ガイダンスでは扱わない. プライベートセクター組織や州, 地域, 部族政府は, 自身のデジタルプロセスが多様な Assurance Level を要求するものであれば, 適切な箇所で本標準を採用することを検討しても良い.

本ガイドライン群は, 市民が社会福祉サービスにアクセスしたり, プライベートセクターのパートナーが情報共有コラボレーションスペースにアクセスするなど, 主に連邦政府以外の主体と対話を行う機関サービスにフォーカスしている. しかしながら, 機関の従業員や契約業者がアクセスする内部システムにも適用される. こういったユーザーは, 主として Personal Identity Verification (PIV) カードないしはそれから派生した PIV といった, 正当な政府発行 Credential を保持しているものと期待される. したがって SP 800-63A (sp800-63a.html) および SP 800-63B (sp800-63b.html) は FIPS 201 およびその関連 Special Publication の要件および組織固有の指示に次ぐ二時的存在となる. しかしながら SP 800-63C (sp800-63c.html) およびリスクベースによる適切な FAL の選択は, 内部ユーザーの持つ Credential タイプに関係なく適用される. 各機関は FAL を選択することで, 各アプリケーションのシステムリスクに応じた PIV 採用方法について, ガイダンスと柔軟性を得ることができる.

2.2 Considerations, Other Requirements, and Flexibilities

各機関はここに指定されていない他のリスク軽減策および補完的統制を採用してもよい. ただし採用するいかなる対策および補完的統制も, 自身が選択した Assurance Level のセキュリティー・プライバシー保護レベルを低下させることがないよう保証すること. 各機関はデジタルサービスの機能を分割し, センシティブでない機能を, より低い Authentication Assurance Level および Identity Assurance Level のもとで提供することを検討してもよい.

各機関は, 自身の Risk Analysis を元に, 特定のコンテキストでは追加の措置を行うよう取り決めても良い. 特に, プライバシー要件と法的リスクにより, 追加の Authentication 措置やその他のプロセス保護が望ましいとすることもあるであろう. Digital Authentication プロセスや Digital Authentication システムを構築する際には, 各機関は *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* [M-03-22] を参照すべきである. また, 特に 1) Proofing の法的基準への準拠や, 2) 否認防止といったニーズに関連する法的リスクに関する追加情報は *Use of Electronic Signatures in Federal Organization Transactions* [ESIG] を参照のこと.

さらに, 本ガイドライン群を実装する政府機関は, Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283 [FISMA], および関連する NIST 標準およびガイドラインに基づく法定責任に準拠すべきである. FISMA は連邦政府機関に対して, 機関の業務と資産を支える情報およびシステムのセキュリティーを担保する, 機関全体にわたるプログラムを開発, 文書化, 実装するよう指示している. これには Digital Authentication を支える IT システムの Security Authorization and Accreditation (SA&A) を含む. NIST は, 本ガイドライン群を実装する非連邦政府主体に対して, デジタルシステムのセキュアな運用を確実なものにするべく, 上記と等価な標準に従うよう推奨している.

2.3 A Few Limitations

Authenticator によってはデジタル Access のみならず物理的 Access 時の Authentication の為にも利用可能なものもあるが, 本技術ガイドライン群は物理的 Access (e.g., ビル入館) に際する Subject の Authentication に関しては扱わない. さらに, 本ガイドライン群の本リビジョンでは, しばしば Machine-to-Machene (Router-to-Router など) Authentication や相互接続デバイスと呼ばれ, 一般的には Internet of Things (IoT) とも呼ばれる Device Identity については明示的には扱わない. つまり, 本ガイドライン群は可能な限り一般的 Subject について言及し, デバイスへの適用可能性を残している. また対人間の Authentication Protocol でデバイスを用いる際に, デバイスに Authenticator を発行する固有の要件についても除外されている.

2.4 How to Use this Suite of SPs

Identity サービスを提供する際のビジネスモデル, マーケットプレイス, 構成は, 最初のバージョンの SP 800-63 がリリースされて以降, 劇的に変化している. 特に CSP はコンポーネント化され, 独立して運営・保有される複数のビジネス主体により構成されるケースも出てきた. さらに Identity Proofing が必要ないケースでも強固な Authenticator を利用する大きなセキュリティー上の利点もありうる. したがって本リビジョンでは, 800-63 という呼称の元に一連の SP を置き, 上記のような新しいモデルを促進し, 全体の Digital Identity モデルの中である主体が提供可能な機能に対する特定の要件に容易にたどり着けるようにしている.

2.5 Change History

2.5.1 SP 800-63-1

NIST SP 800-63-1 は, 最新の Authenticator (“Token” と呼ばれた) 技術を反映し, 今日使われている Digital Identity アーキテクチャーモデルをよりよく理解すべく, NIST SP 800-63 を改訂したものである. 追加の (最小限の) 技術要件が, CSP, Authentication 情報伝達プロトコル, および Digital Identity モデル中で利用されていれば Assertion に対して規定された.

2.5.2 SP 800-63-2

NIST SP 800-63-2 は SP 800-63-1 の限定的アップデートであり, 実質的変更は Section 5 *Registration and Issuance Processes* のみであった. 改訂 Draft の実質的変更は, Identity Proofing プロセスにおいて専門資格の使用を促進し, Level 3 の Remote Registration における Credential 発行のため Address of Record に郵便を送る必要性を低減させることを意図したものであった. Section 5 のその他の変更は, 軽微な説明と明確化であった.

2.5.3 SP 800-63-3

NIST SP 800-63-3 は SP 800-63-2 の大幅なアップデートと再構成を伴っている. SP 800-63-3 では Digital Authentication Assurance の個々の構成要素となる AAL, IAL, FAL を導入し, Authentication の強度と個々の Claimed Identity の確実性を独立して扱いたい (e.g., 強固な Pseudonymous Authentication) という高まる要求に応えている. 本ガイドラインには, Risk Assessment 方法論とその IAL, AAL, FAL への適用が含まれる. SP 800-63-3 では, SP 800-63 がカバーする Digital Identity ガイダンス全体を, Authentication について述べる単一のドキュメントから, (上述の個々の構成要素に個別に対処するべく) SP 800-63-3 をトップレベルのドキュメントとする一連の4つのドキュメント群へと分割する.

800-63-3 でのその他の変更点は以下の通りである.

- Identity Proofing および Federation をスコープに含めていることを正しく示すべく, “Digital Identity Guidelines” に改名し, 将来のリビジョンで Device Identity や Machine-to-Machene Authentication を扱えるようスコープを拡大する余地を含めた.
- Assertion 技術における *Token* との混同を避けるため *Token* の代わりに *Authenticator* という用語を用いるなど, 用語変更を行った.
- Authentication および Assertion の要件を更新し, セキュリティー技術および脅威の進化を反映した.
- Verifier が Long-term Secret を保管する際の要件を定めた.
- Identity Proofing モデルを再構成した.
- Remote Identity Proofing に関連する要件を更新した.
- 独立したチャネルやデバイスを “something you have” として用いるということを明確化した.
- 事前登録済の Knowledge Token (Autnenticator) は, (時として非常に弱い) パスワードの特別な形態という認識のもと **削除** した.
- Authenticator の紛失や盗難時のアカウントリカバリーに関する要件を定めた.
- Out-of-band Authenticator 用の有効なチャネルとしての Email を **削除** した.
- Re-authentication や Session 管理に関するより深い議論を追加した.
- Identity Federation に関するより深い議論を追加し, Federation コンテキストにおける Assertion の再構成を行った.

3 Definitions and Abbreviations

用語定義および略語については, 全て Appendix A を参照のこと.

4 Digital Identity Model

This section is informative.

4.1 Overview

本ガイドライン群における Digital Identity モデルは, 現時点で市場で調達可能なテクノロジーやアーキテクチャーを反映したものとなっている. 多数の主体に渡って Credential 発行機能と Attribute 発行機能を分離するといったようなより複雑なモデルも, 実現可能かつある種のアプリケーションでは有用かもしれない. 本ドキュメントではよりシンプルなモデルを採用するが, これは各機関が上記の機能分割などを行うことを妨げるものではない. さらには, CSP が実行する Enrollment, Identity Proofing および発行プロセスの中には, しばしば Registration Authority (RA) や Identity Manager (IM) と呼ばれるような主体に移譲されるものもある. こういったタイプの関係性や要件は本ドキュメントの扱うところではない. また CSP といった場合には RA と IM の機能も含むものとする. また CSP が Digital Identity サービス以外のサービスを提供することもありうる. そういったシチュエーションでは, 本ガイドライン群の要件は CSP としての機能にのみ該当し, その他のサービスには影響を与えないものとする.

Digital Identity はオンライン Transaction に関与する Subject を一意に表現するものである. Subject と現実世界の Identity との紐付けを検証するプロセスは, *Identity Proofing* と呼ばれる. 本ガイドラインでは, Proof される主体を *Applicant* と呼び, Proofing プロセスを完了した Applicant のことを *Subscriber* と呼ぶ.

Identity Proofing の強度は IAL と呼ばれる序数的指標で表される. IAL1 では Identity Proofing は不要で, Applicant から提供された Attribute 情報はすべて (それが CSP / RP から提供されたものだとしても) Self-asserted であるか, 未検証の Self-asserted 相当として扱われる. IAL2 と IAL3 では Identity Proofing が必須となり, RP が CSP に対して, 検証済 Attribute Value, 検証済 Attribute Reference, ないしは Pseudonymous Identifier などといった Subscriber に関する情報を Assert するよう要求することもある. これらの情報は RP が Authorization 判定を行う際の材料となる. RP は IAL2 ないしは IAL3 を必要としつつ, 特定の Attribute のみを必須とすることもでき, そうすることで Subject に対してある一定レベルの Pseudonymity を確保することができる. このプライバシー強化アプローチは, Proofing プロセスの強度を Authentication プロセスの強度から分離したことにより可能となっている. さらに RP は Federated Identity アプローチを採用することもでき, その場合 RP は Identity Proofing, Attribute 収集および保管をすべて CSP にアウトソースすることとなる.

本ガイドライン群では Authenticate される主体を *Claimant* と呼び, 当該 Identity を検証する主体を *Verifier* と呼ぶ. Authentication Protocol を通じ, Claimant が Verifier に対して1つ以上の Authenticator を保持・管理していることを立証すると, Verifier は Claimant が正規の Subscriber であると検証できる. その後 Verifier は Subscriber に関する Assertion を RP に送る. この時 Subscriber は Pseudonymous なこともあればそうでないこともある. Assertion には識別子が含まれ, 場合によっては氏名や Enrollment プロセスにおいて収集されたその他の Attribute などの Subscriber に関する Identity 情報も含まれる. どういった情報を含むかは CSP のポリシーや RP のニーズ, Subject による Attribute 提供に関する同意内容などに依存する) Verifier 自身が RP である場合, Assertion は暗黙的なものとなる. RP は Verifier から提供された Authenticated な情報を元に, Authorization 判定を行う.

Authentication により, Claimant が Credential に紐づく Authenticator を管理下に置いていることが確かめられ, 場合によっては Subscriber の Attribute Value (e.g., Subscriber が U.S. 市民, 特定の大学の生徒であること, ある機関や組織から特定の番号やコードを割り当てられていること) についても確認できる. Authentication は Claimant の Authorization や Access 権限の決定を行うものではなく, これらは別の意思決定であり, 本ガイドライン群の扱うところではない. RP は Subscriber の Authenticated Identity および Attribute を他の要素と組み合わせ, Authorization の決定を行う. 本ドキュメントスイートは RP が Subscriber に対して Authenticate を成功させるために追加情報を要求することを妨げるものではない.

Authentication プロセスの強度は AAL と呼ばれる序数的指標で表される. AAL1 では Single-factor Authentication が求められ, 幅広い種類の Authenticator Type が利用可能である. AAL2 ではより強固なセキュリティーの為に2つの Authentication Factor が要求される. 最高レベルの Authentication である AAL3 では, さらにハードウェアベースの Authenticator と Verifier なりすまし対策が要求される.

ここで扱われる Digital Identity モデルを構成する多様な主体とインタラクションを Figure 4-1 に示す.

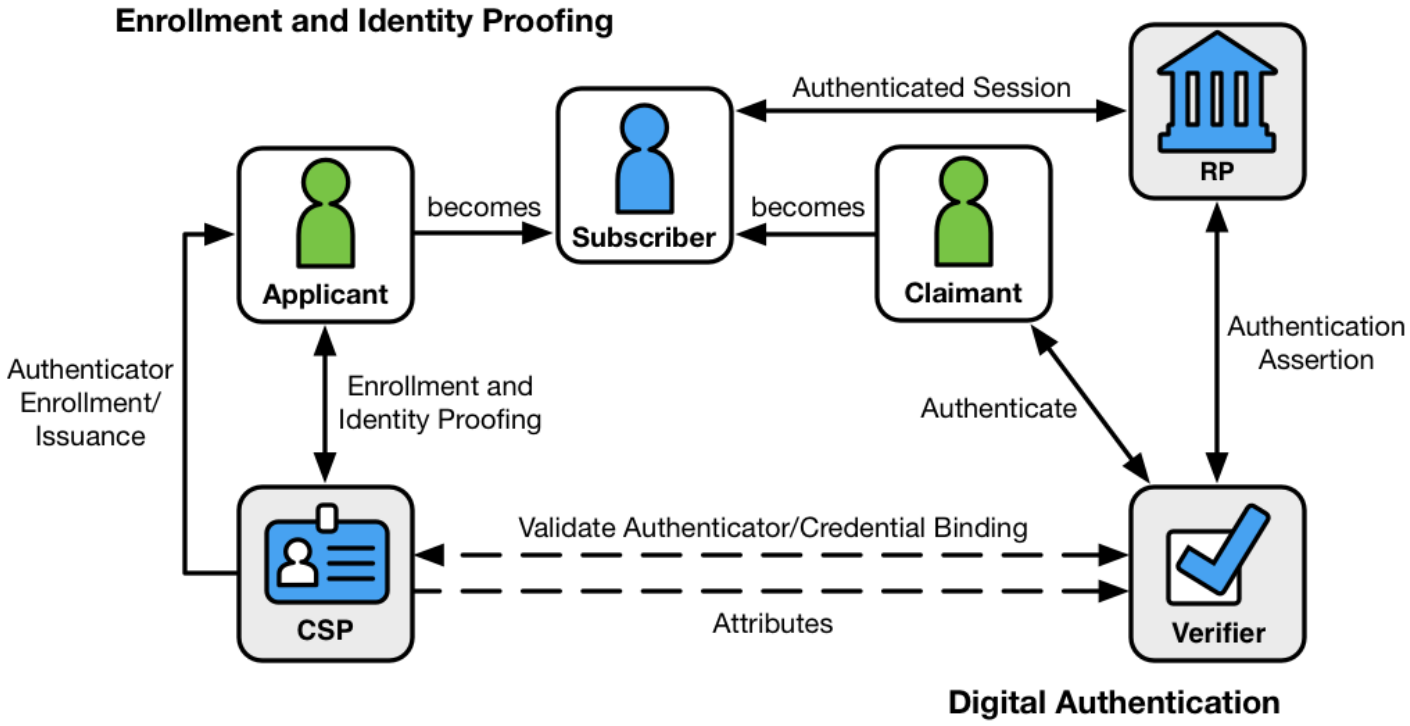


Figure 4-1 Digital Identity Model

このダイアグラム左側は Enrollment, Credential 発行, ライフサイクル管理, および Identity Proofing と Authentication プロセスにおけるさまざまなステータスを示している. 通常は以下のようなシーケンスでインタラクションが行われる.

1. Applicant が Enrollment プロセスを通じて CSP に申請を行う.
2. CSP は Applicant に対して Identity Proofing を行い, Proofing が成功すると Applicant は Subscriber になる.
3. Authenticator とそれに対応する Credential が CSP と Subscriber の間で確立される.
4. CSP は Credential とそのステータスを管理, Credential のライフタイム期間内に収集された Enrollment データを管理し, Subscriber は自身の Authenticator を管理する.

上記のシーケンスほど一般的ではなくても, 同様の機能要件を満たすその他のシーケンスもありうる.

Figure 4-1 右側は Authenticator を利用して Digital Authentication を行う主体およびインタラクションを示している. Subscriber は Verifier に対して Authenticate する必要がある時は Claimant と呼ばれる. ここでのインタラクションは以下の通りである.

1. Claimant が Authentication Protocol を通じて, Verifier に対し Authenticator を保持・管理していることを証明する.
2. Verifier は CSP とインタラクションを行い, Subscriber の Identity と Authenticator を紐づける Credential を検証し, 任意で Claimant の Attribute を取得する.
3. CSP ないし Verifier は Subscriber に関する Assertion を RP に提供する. RP は Assertion に含まれる情報を利用して Authorization の決定を行う.
4. Subscriber と RP の間で Authenticated Session が確立される.

いかなる場合でも, RP は Claimant を Authenticate する前に CSP に対して必要な Attribute を要求しべきである. さらに Claimant は Assertion の生成および送信前に Attribute 送信についての同意を求められるべきである.

場合によっては, Verifier は Authentication を完了させる為に CSP とリアルタイムでコミュニケーションする必要はない (e.g., デジタル証明書を利用する場合). したがって, Verifier と CSP の間の点線は当該2主体の論理的なリンクを示している. 実装によっては, Verifier, RP, CSP の各機能は Figure 4-1 のように分離されているが, これらの機能が同じプラットフォーム上に存在する場合, 各構成要素間のインタラクションは, 共有の信頼できない Network 越しのプロトコルではなく, 同一システム上で動作するアプリケーション間のローカルメッセージであることもある.

上述の通り, CSP は自身が発行した Credential に関するステータス情報を管理する. CSP は通常 Credential 発行時に管理期間を制限するため有限のライフタイムを設定する. ステータス変更時や Credential の期限切れに近づいた時は, Credential は更新されたり再発行されるか, 無効化され破棄される. 典型的には, Subscriber が自身の現存の期限切れしていない Authenticator および Credential を使って CSP に対して Authenticate した上で新規の Authenticator および Credential の発行を依頼する. Subscriber が有効期限切れや無効化処理が行われ

る前に Authenticator および Credential の再発行を行えなかった場合は, 再度 Enrollment プロセスを経て新規の Authenticator および Credential を取得することになるであろう. その代わりに CSP が有効期限切れ後一定期間は再発行リクエストを受け付ける, というようなことも考えられる.

4.2 Enrollment and Identity Proofing

Normative 要件は SP 800-63A (sp800-63a.html) *Enrollment and Identity Proofing* に従うこと.

前セクションでは Digital Identity 概念モデルにおける参加者を紹介した. 本セクションでは, 上記参加者の関係性と Enrollment および Identity Proofing における責任について詳説する.

このステージで *Applicant* と呼ばれている個人は, CSP に Identity Proofing を要求する. Applicant が Proofing に成功すると, 当該個人は当該 CSP の Subscriber と呼ばれることになる.

CSP は個々の Subscriber をユニークに識別する方法を確立し, Subscriber の Credential を登録し, Subscriber に発行された Authenticator をトラックする. Subscriber が Enrollment 時に Authenticator を渡されることもあれば, CSP が Subscriber のすでに所有している Authenticator に Subscriber を紐付けることもあれば, それ以降の必要となった段階で Authenticator が生成されることもある. Subscriber は Authenticator を管理し, Authenticator をアクティブに保つため CSP のポリシーにしたがう責務がある. CSP は各 Subscriber の Enrollment レコードを管理し, Authenticator の紛失・盗難時等のリカバリーに対応する責務がある.

4.3 Authentication and Lifecycle Management

Normative 要件は SP 800-63B (sp800-63b.html), *Authentication and Lifecycle Management* に従うこと.

4.3.1 Authenticators

Authentication システムの古典的パラダイムでは, 3つの要素を Authentication の要とする.

- Something you know (e.g., a password).
- Something you have (e.g., an ID badge or a cryptographic key).
- Something you are (e.g., a fingerprint or other biometric data).

MFA は上記のうち2つ以上の要素を使うことを意味する. Authentication システムの強度は, そのシステムに組み込まれた上記の要素数に大きく依存する. より多くの要素を用いれば, システムはより堅固になる. 本ガイドライン群の目的においては, Authentication システムが最高のセキュリティー要件を満たすには, 2つの要素を利用するのが適切である. Section 5.1 で述べるように, RP や Verifier は Claimed Identity に対するリスク評価のために, 位置データや Device Identity など, 上記3要素以外のタイプの情報を利用することもありうるが, それらは Authentication Factor とは見なされない.

Digital Authentication では, Claimant は CSP に登録された Authenticator を保持・管理し, 当該 Authenticator は Claimant Identity の証明に使われる. Authenticator は Claimant が正規の Subscriber であることを証明するためのシークレットを内包し, Claimant は Authenticator を保持・管理していることをネットワーク越しに証明することで, システムやアプリケーションに対して Authenticate する.

Authenticator に含まれるシークレットは, Public Key ペア (Asymmetric Keys) ないしは Shared Secret (Symmetric Key) に基づいている. Public Key と Private Key の対が Public Key ペアとなる. Private Key は Authenticator 上に保存され, Claimant が Authenticator を保持・管理していることを証明するために利用される. Verifier は何らかの Credential (典型的には Public Key Certificate) を通じて Claimant の Public Key を知っており, Authentication Protocol を通じて Claimant が対応する Private Key を含んだ Authenticator を保持・管理していることを証明することで, Claimant の Identity を検証できる.

Authenticator 上に保存される　Shared Secret は, Symmetric Key ないしは Memorized Secret (e.g., Password や PIN) となる. 上述の Asymmetric Key のケースとはことなり, Subscriber はこれらを Verifier と共有する必要がある. Symmetric Key も Password も同じようなプロトコルで利用可能だが, どのように Subscriber と関連づけられるかという点が大きく異なる. Symmetric Key は一般的に Subscriber が管理するハードウェアないしソフトウェア内に保存されるが, Password は Subscriber に記憶されることが想定される. ほとんどのユーザーは記憶および入力しやすい短い Password を選ぶため, Password は Cryptographic Key よりも短くなりがちである. さらに, 乱数を用いてシステム的に鍵を生成する場合と比べ, ユーザーはその長さのパスワードの候補空間の非常に小さなサブセットの中から記憶可能な Password を選びがちであり, その多くは似た値になりがちである. したがって, Cryptographic Key は通常 Network ベースの推測攻撃が不可能なほど十分長くなるが, ユーザーが選択した Password は, 特に何の防御策もない場合, 脆弱である可能性がある.

本 Vol. では, Authenticator は常にシークレットを含む. 古典的 Authentication Factor の中には直接 Digital Authentication に適用されないものもある. 例えば物理的な運転免許証は Something you have であり, 人間 (e.g., 警備員) に対して Authenticate する際には利用可能であるが, それ自体は Digital Authentication のための Authenticator とはならない. Something you know に分類される Authentication Factor は,

必ずしもシークレットであるとは限らない. Claimant に対して Claimant のみが知っているであろう質問に答えるよう求める Knowledge-based Authentication も, Digital Authentication で利用可能なシークレットとはならない. Biometric もシークレットとはならない. よって本ガイドライン群では Authentication のために Biometric を使うのは, それが強固に物理的 Authenticator に紐づけられている場合に限る.

Digital Authentication システムは, 以下の2つの方法のどちらかで複数の要素を内包する.

1. 複数の要素が Verifier に提示される.
2. ある要素が Verifier に提示されるシークレットを保護するために利用される.

例えば, 上記1は Memorized Secret (what you know) を Out-of-band Device (what you have) と組み合わせることで実現可能である.　両方の Authenticator Output が Verifier に提示され, Claimant の Authentication に使われる. 一方, 上記2は, Cryptographic Key を内包するハードウェア (Authenticator) があり, Cryptographic Key への Access が指紋により保護されている場合を考えるとよい. Biometric と共に利用すると, Cryptographic Key を使って Claimant を Authenticate するための Output が出力される.

上述のように, Biometrics が Authentication の1要素として用いられる場合, それ自体は Digital Authentication で利用可能なシークレットとはならないが, Digital Identity の Authentication においてはその利用箇所が存在する. Biometric 特性はユニークな個人の Attribute であり, 検証時に対面の人間の Identity を検証するためには利用可能である. 顔の特徴, 指紋, 虹彩パターン, 声紋等, 多くの Biometric 特性が存在する. SP 800-63A (sp800-63a.html) *Enrollment and Identity Proofing* では, Enrollment プロセスにおいて Biometrics を収集し, 登録した Subscriber による Enrollment の否認を防止し, 不正な Enrollment を行った人物を特定するために利用することを推奨している.

4.3.2 Credentials

前セクションで述べた通り, Credential は発行プロセスにおいて Authenticator と Subscriber を識別子を通じて紐づける. Credential は CSP によって保管・管理されるが, Claimant が保持することもある. Claimant は Authenticator を保持するが, 必ずしも Credential を保持する必要はない. 例えば, あるユーザーの Attribute を含んだデータベースエントリーは, 本ドキュメントの目的においては Credential であると見なされますが, これは Verifier が保持するものです. X.509 Public Key Certificate は Claimant が保持しうる Credential の古典的な例です.

4.3.3 Authentication Process

Authentication プロセスは, Claimant が Verifier に Authenticator の保持・管理を示すところから始まる. ここで Authenticator は Authentication Protocol を通じて Asserted Identity に紐づけられている. 一度 Authenticator の保持・管理が示されれば, Verifier は, 通常 CSP とのインタラクションを通じて, 当該 Credential が依然有効であるかどうかを確認する.

Authentication Protocol における Verifier と Claimant の間のインタラクションは, システム全体のセキュリティーにとって極めて重要である. よく設計されたプロトコルは, Authentication の最中および事後において, Claimant と Verifier の間のコミュニケーションの Integrity (完全性) および Confidentiality (機密性) を保護し, Attacker が正当な Verifier であるかのように偽装できてしまった場合の被害を限定的にする.

また, Verifier 側で Attacker による Authentication 試行レートを制限したり不正な試行を遅延させたりすることで, Password や PIN といったエントロピーの低いシークレットに対する Online Guessing Attack の影響を軽減できる. 一般的に Online Guessing Attack ではほとんどの試行が失敗するので, その対策は失敗試行数を制限するというような方式となる.

Verifier は機能的役割であるが, しばしば CSP, RP ないしはその両方と合わせて実装される. Verifier が CSP から独立した主体である場合, 一般的には Authentication プロセス中に Verifier が Subscriber の Authenticator Secret を知ることがないよう保証できることが望ましい. 少なくとも Verifier が CSP に保管されているシークレットに無制限にアクセスできるような状況ではないことが保証されるべきである.

4.4 Federation and Assertions

Normative 要件は SP 800-63C (sp800-63c.html), *Federation and Assertions* に従うこと.

全体として, SP 800-63 は Federated Identity アーキテクチャーを前提とはしていない. むしろ本ガイドライン群は市場に存在するモデルについては感知せず, 各機関は自身の要件にそった Digital Authentication スキームを導入できる. しかしながら, 単一の機関や RP が運営するサイロ化した多数の Identity システムよりも, Identity Federation の方が好ましい.

Federated アーキテクチャーには, 以下にあげたようなものをはじめとする多くの利点がある.

- ユーザーエクスペリエンスの向上. 例えば, ある個人がひとたび Identity Proofing を終えると, 発行された Credential を複数の RP に対して再利用できる.
- ユーザーと各機関双方にとってコスト低減効果がある. (ユーザーにとっては Authenticator の減少, 各機関にとっては情報テクノロジーインフラストラクチャーの縮小)

- 各機関が Personal Information を保存するにあたっての, 収集, 保管, 処理, 法令遵守活動のための活動費用が不要となり, データ最小化につながる.
- 各機関はサービス提供に必要な最小限の Attribute を要求し, それを Pseudonymous Attribute Assertion の Claim として含めるよう要求できる.
- 各機関は Identity 管理ではなく自身のミッションに集中することができる.

次のセクションでは, 各機関が Federated Identity アーキテクチャを選択する場合に登場する構成要素について説明します。

4.4.1 Assertions

Authentication プロセスが完了すると, Verifier は Authentication 結果を含んだ Assertion を生成し, それを RP に提供する. Assertion は Verifier から RP に Authentication プロセスの結果を伝えるために使われ, 時には Subscriber に関する情報を伝えることもある. Assertion は直接 RP に送信されることもあれば, Subscriber を通じて転送されることもあり, その違いはシステムデザインに大きく影響を及ぼす.

RP はその発信元, 生成日時, 生成後の有効期限, および CSP と RP のポリシーとプロセスを管理するトラストフレームワークに基づいて Assertion を信頼する. Verifier は Assertion の Integrity (完全性) を確認する手段を提供する責任を持つ.

RP は発信元 (Verifier) を Authenticate し, Assertion の Integrity (完全性) を確認する義務を負う. Verifier が Subscriber を経由して Assertion を提供する場合には, Verifier は Assertion が改ざんされないよう, その Integirity (完全性) を保護しなければならない. 一方 Verifier が直接 RP と通信を行う場合, Protected Session によって Assertion の Integrity (完全性) を確保してもよい. オープンな Network を通じて Assertion を送信する場合, Verifier は, Assertion に含まれる Subscriber に関するセンシティブな情報が, 情報の Confidentiality (機密性) を保つという点において信頼に足る RP 以外の何者の手にも渡らないことを, 確かなものとする責任がある.

Assertion の例を以下に挙げる.

- Security Assertion Markup Language (SAML) Assertion はセキュリティー Assertion を記述するためのマークアップランゲージによって規定される. SAML Assertion は Verifier が RP に対して Claimant の Identity に関するステートメントを生成するために利用される. SAML Assertion にはデジタル署名が施されることもある.
- OpenID Connect Claim は, JavaScript Object Notation (JSON) を使ってセキュリティー Claim および任意でユーザー Claim を記述するために規定される. JSON User Info Claims にはデジタル署名が施されることもある.
- Kerberos Ticket は, Ticket-granting Authority が Symmetric Key ベースのカプセル化方式を利用し, 2つの Authenticated な主体 に Session Key を発行することを可能にする.

4.4.2 Relying Parties

RP は, オンライン Transaction を行うために, Authentication Protocol の結果を頼りに Subscriber の Identity ないしは Attribute に関する確からしさを確立する. RP は, Subscriber の Authenticated Identity (Pseudonymous なこともあればそうでないこともある), IAL, AAL, FAL (FAL は Assertion Protocol の強度を示す) およびその他の要素をもとに, Authorization の決定を行う. Verifier と RP は同じ主体であることもあれば, 別の主体であることもある. 両者が別主体である場合, RP は通常 Verifier から Assertion を受け取る. RP は Assertion が信頼する Verifier から来ていることを確実なものとし, Assertion に含まれる個人の Attribute や有効期限などの追加情報を処理する. RP は Verifier によって提示された Assertion が, IAL, AAL, FAL に関係なく RP の確立されたシステム Access 基準を満たすかどうかに関する最終的な決定者となる.

5 Digital Identity Risk Management

This section is normative.

本セクションおよび対応する Risk Assessment ガイダンス は, NIST Risk Management Framework (RMF) およびその構成要素となる Special Publication を補完する. これは各機関にさらなる Risk Management プロセスを課すものではなく, 全ての関連する RMF ライフサイクルフェーズ実行に際する Digital Identity のリスクに関しての, 各機関の RP が適用しなければならない (SHALL) 具体的なガイダンスを提供するものである.

5.1 Overview

今日のデジタルサービスでは, Proofing と Authenticator と Federation の各要件をひとくくりにすると, 意図しない結果が生じ, 実装組織に不必要な実装負担をかけることがある. 単一の包括的な LOA ではなく, Digital Authentication の個々の構成要素ごとに失敗時のリスクと影響を評価することで, 機関は高確率で最も効果的に Identity Service を提供できることになるであろう. 以上のことから, 本ガイドライン群では Authentication エラーは全ての要件を満たすシングルトンではないという認識のもとに立つ.

本 Vol. では各機関が避けるべき要件をまとめる.

1. Identity Proofing エラー (i.e., 偽の Applicant が正当なふりをして Identity を主張する)
2. Authentication エラー (i.e., 本来正当でない偽の Claimant が正当なふりをして Credential を利用する)
3. Federation エラー (i.e., Identity Assertion が毀損する)

Identity Proofing の失敗という観点からは, 潜在的に以下の2種類の影響が考えられる.

1. サービスを異なる Subject に提供してしまうことによる影響. (e.g., Attacker が他人になりすませてしまう)
2. 過度の Identity Proofing による影響. (i.e., デジタルサービス提供のために, ある人物に関する必要以上に多くの情報を収集し, セキュアに保管してしまう)

そのため, 各機関は Proofing, Authentication および Federation のリスクを個別に評価し, 各トランザクションに必要な Assurance Level を決定する必要がある (SHALL).

RMF の全体的な適用を支援するため, Section 5.3 には Digital Identity 固有の影響カテゴリーを提示している.

Risk Assesment は, Identity Proofing, Authentication, Federation の各プロセスにおいて, どのようなリスクを軽減するべきかを決定するものである. こういった決定は, リスク明確化に役立つ技術への欲求を引き起こすものではなく, 適用可能な技術とリスク軽減策の選択を推進するものである. ひとたび機関が全体の Risk Assessment を終え, Identity Proofing, Authentication, (および該当する場合は) Federation それぞれに対する Assurance Level を選択し, それぞれの Assurance Level を満たすために採用すべきプロセスや技術を選定すると, 機関は SP 800-53A IA-1 a.1 に従い “Digital Identity Acceptance Statement” を策定すること (SHALL). Section 5.5 に “Digital Identity Acceptance Statement” に必要なコンテンツを詳説する.

5.2 Assurance Levels

機関の RP はリスクに基づき以下の個々の Assurance Level を選択すること (SHALL).

- IAL: 個人の Identity を確信を持って決定するための Identity Proofing プロセスの頑強性. IAL は潜在的 Identity Proofing エラーを軽減することを目的に選択される.
- AAL: Authentication プロセス自体, および Authenticator と特定個人の識別子の紐付けの頑強性. AAL は Authentication エラーを軽減することを目的に選択される. (i.e., 本来正当でない偽の Claimant が正当なふりをして Credential を利用する)
- FAL: Federation 時に Authentication および Attribute の情報をやり取りするための Assertion Protocol の頑強性. すべての Digital システムが Federated Identity アーキテクチャーを採用する訳ではないため, FAL はオプションである. FAL は Federation エラー (Identity Assertion が毀損するなど) を軽減することを目的に選択される.

Identity, Authenticator, Federation Assurance Level の概要はそれぞれ以下にまとめる.

Table 5-1 Identity Assurance Levels

Identity Assurance Level
IAL1: IAL1 では, Attribute がある場合それらは Self-asserted であるか, もしくは Self-asserted として扱われるべきである.
IAL2: IAL2 では, Remote ないしは対面での Identity Proofing が必須となる. IAL2 では, 識別に用いられる Attribute に関しては, SP 800-63A (sp800-63a.html) に従い, 対面ないしは Remote で検証する必要がある.

Identity Assurance Level
IAL3: IAL3 では, 対面での Identity Proofing が必須となる. 識別に用いられる Attribute に関しては, SP 800-63A (sp800-63a.html) に従い, Authorize された CSP の担当者によって物理ドキュメントを用いた検証がなされる必要がある.

Table 5-2 Authenticator Assurance Levels

Authenticator Assurance Level
AAL1: AAL1 では, Claimant が Subscriber に紐づく Authenticator を管理下に置いていることが, ある程度の確からしさで確認できる. AAL1 では Single-factor Authentication が必須となり, そこでは幅広い Authentication 技術が利用可能である. Authentication を成功させるには, Claimant がセキュアな Authentication Protocol を通じて Authenticator を保持・管理していることを証明する必要がある.
AAL2: AAL2 では, Claimant が Subscriber に紐づく Authenticator を管理下に置いているということが, 高い確度で保証される. セキュアな Authentication Protocol によって, 2つの異なる Authentication Factor を保持・管理していることを証明する必要がある. AAL2 以上では, Approved Cryptographic テクノロジーも必要となる.
AAL3: AAL3 では, Claimant が Subscriber のアカウントに紐づく Authenticator を管理下に置いているということが, 非常に高い確度で保証される. AAL3 の Authentication は, 暗号プロトコルによる鍵所有証明 (Proof of Possession) に基づいている. AAL3 は AAL2 と似ているが, AAL2 に加え Verifier Inpersonation 耐性のある “ハードの” Cryptographic Authenticator を要求する.

Table 5-3 Federation Assurance Levels

Federation Assurance Level
FAL1: FAL1 では, RP は Identity Provider (IdP) から Bearer Assertion を受け取ることができる. IdP は Approved Cryptography を使って Assertion に署名する必要がある.
FAL2: FAL2 では, 上記に加え, RP のみが復号可能なかたちで, Assertion に対する暗号化が必要になる. 暗号化には Approved Cryptography を用いる.
FAL3: FAL3 では, Subscriber が Assertion および Assertion Artifact から参照される Cryptographic Key を保持していることを証明する必要がある. Assertion は Approved Cryptography を使って署名され, Approved Cryptography を使って RP に対して暗号化されなければならない.

総称的ないしは一括で扱う場合, 本ガイドライン群では IAL, AAL, FAL を **_ xAL _** と呼ぶこととする.

5.3 Risk and Impacts

本セクションでは IAL, AAL, FAL を決定する際に利用される影響カテゴリーについて述べる.

潜在的影響カテゴリー: ユーザーの Asserted Identity の適切な Assurance Level を決定するため, 各機関は潜在リスクを評価し, その影響を最小限に抑える手段を特定する必要がある (SHALL).

より悪影響が予想される Authentication, Proofing, および Federation エラーには, より高い Asssurance Level が求められる. ビジネスプロセスやポリシー, 技術などがそのリスク低減に役立つ.

被害と影響のカテゴリーは次のとおりである.

1. 不便, 苦痛, または社会的地位やレピュテーションの毀損.
2. 経済的損失または機関の負債.
3. 機関のプログラムや公共の利益への損害.
4. Authorize のないセンシティブ情報の公開.
5. 個人の安全.
6. 民事または刑事上の違反.

Digital Transaction に要求される Assurance Level は, Federal Information Processing Standard (FIPS) 199 [FIPS 199] が示す潜在的影響度合いを利用し, 上記カテゴリーごとの潜在的影響評価を行うことで決定できる.

上記潜在的影響度合いには, 以下の3つの値がある.

1. 影響度 Low
2. 影響度 Moderate
3. 影響度 High

5.3.1 Business Process vs. Online Transaction

Assurance Level の決定は, Digital システムの一部をなす Transaction にのみ基づいて行われる. あるオンライン Transaction は, オフライン処理や完全にセグメント化されたシステム上でのオンライン処理を必要とする完全なビジネスプロセスとは等価でないこともありうる. 適切な Assurance Level の選択において, 当該機関は, 提供する便益やサービスに関連するビジネスプロセス全体の評価ではなく, 自身のデジタルサービスにおけるオンライン Transaction に関連するリスクの評価を行うべきである. たとえばオンラインアンケートでは Personal Information が収集されることがあるが, 当該情報が保存後に情報提供者に対してオンラインで提供されることはない. このような場合, バックエンドシステムで注意深く情報を保護することは重要だが, 情報提供者自身がシステムや関連する便益に Access するために当該ユーザーに対して Identity Proofing や Authentication を実施する必要はない. オンライン Transaction は単にデータの提出処理のみである. ビジネスプロセス全体ではかなりのデータ検証処理が必要となる可能性があるが, 正規の人物が情報を提出したかどうかを知る必要はない. このシナリオでは, Identity Proofing も Authentication も必要ではない.

機関がオンライン Transaction の要件ではなくビジネスプロセス全体を評価した場合にリスク評価が変わりうるその他の事例としては, 公開求人情報応募用の履歴書受取デジタルサービスが挙げられる. このユースケースでは, 当該デジタルサービスは個人が他人の代理で履歴書を提出することは許可する, ないしは最低でも制限はせず, その後にサイトに再訪された時にはさまざまな目的のため履歴書に Access する. 履歴書の情報は後の Session でもユーザーから利用可能であり, また Personal Information を含むため, Personal Information が Self-asserted であったとしても, 当該機関は MFA を必要とする AAL を選択する必要がある. この場合, [EO 13681] の要件が適用され, アプリケーションは AAL2 以上で提供されなければならない. しかしながら Identity Proofing 要件は依然不確定である. 履歴書を検査し最終的に雇用し新人研修を施すといったビジネスプロセス全体では, 相当の Identity Proofing が必要である. 採用決定時には, 求人情報への Applicant が実際にオンライン提出された履歴書の Subject であるという高レベルの確信が必要となる. しかしこのレベルの Proofing はオンラインでの履歴書投稿には必要ではない. Identity Proofing はデジタルな世界での Transaction を完了させるためには必要とならない. 投稿者に対して Identity Proofing を行うと, デジタル求人アプリケーションポータルによって提供される採用プロセスでの必要性を過えた Personal Information を収集することに繋がるため, 必要以上にリスクを増大させ, ユーザビリティを低下させることにつながる. 従って最も適切な IAL は1となるであろう. 当該オンライン Transaction には Identity Proofing は不要である. オンラインポータル自体に対するこの決定は, 偽の Applicant による応募を防ぐためビジネスプロセス全体で求められるであろう Identity Proofing 要件とは独立している.

5.3.2 Impacts per Category

本セクションでは各被害カテゴリーごとの潜在的影響を定義する. IAL, AAL, および (Federated Identity を受け入れないしは評価する場合は) FAL の各 Assurance Level は個別に評価すること (SHALL).

> Note: もし Identity システムのエラーがカテゴリーに測定可能な結果を及ぼさない場合, 影響はないものとする.

不便, 苦痛, または社会的地位やレピュテーションの毀損に関する潜在的影響:

- Low: 最悪でも, 任意の主体に対する, 限定的かつ短期間の不便, 苦痛, 困難.
- Moderate: 最悪でも, 任意の主体に対する, 相当かつ短期間ないしは限定的だが長期間の不便, 苦痛, 社会的地位やレピュテーションの毀損.
- High: 任意の主体に対する, 重度または重大かつ長期的な不便, 苦痛, 社会的地位やレピュテーションの毀損. これは通常, 特に重大な影響を及ぼしたり, 多くの個人に影響を及ぼす可能性のある状況を想定したレベルである.

経済的損失に関する潜在的影響:

- Low: 最悪でも, 任意の主体に対する, ささいで取るに足らない経済的損失ないしは機関の負債.
- Moderate: 最悪でも, 任意の主体に対する, 相当な経済的損失ないしは機関の負債.
- High: 任意の主体に対する, 重大または致命的な経済的損失ないしは機関の負債.

機関のプログラムや公共の利益への損害に関する潜在的影響:

- Low: 最悪でも, 組織の運用や資産, 公共の利益への限定的な悪影響. 限定的な悪影響の例としては, (i) 一定範囲および期間にわたる, 組織のミッション遂行能力の低下による組織の主たる機能の処理効率の目に見えた低下, (ii) 組織資産または公益への軽微な損害, などがある.
- Moderate: 最悪でも, 組織の運用や資産, 公共の利益への相当な悪影響. 相当な悪影響の例としては, (i) 一定範囲および期間にわたる, 組織のミッション遂行能力の著しい低下による組織の主たる機能の処理効率の著しい低下, (ii) 組織資産または公益への著しい損害, などがある.
- High: 組織の運用や資産, 公共の利益への重大または致命的な悪影響. 重大または致命的な悪影響の例としては, (i) 一定範囲および期間にわたる, 組織のミッション遂行能力の重大な低下や喪失による組織の主たる機能の処理不能, (ii) 組織資産または公益への深刻な

損害, などがある.

Authorize のないセンシティブ情報の公開に関する潜在的影響*:*

- Low: 最悪でも, FIPS 199 で定義された低インパクトの Confidentiality (機密性) 喪失をもたらす, Authorize されていない主体に対する限定的な Personal Information, U.S. 政府にとってないしは商業的にセンシティブな情報の公開.
- Moderate: 最悪でも, FIPS 199 で定義された中インパクトの Confidentiality (機密性) 喪失をもたらす, Authorize されていない主体に対する限定的な Personal Information, U.S. 政府にとってないしは商業的にセンシティブな情報の公開.
- High: FIPS 199 で定義された高インパクトの Confidentiality (機密性) 喪失をもたらす, Authorize されていない主体に対する限定的な Personal Information, U.S. 政府にとってないしは商業的にセンシティブな情報の公開.

個人の安全に関する潜在的影響*:*

- Low: 最悪でも, 治療を必要としない軽傷.
- Moderate: 最悪でも, 軽傷に関する中程度のリスク, ないしは治療を必要とする怪我に関する限定的リスク.
- High: 重大な傷害または死亡に関するリスク.

民事または刑事上の違反に関する潜在的影響*:*

- Low: 最悪でも, 通常は執行努力の対象とはならない種類の民事または刑事上の違反のリスク.
- Moderate: 最悪でも, 執行努力の対象とりうる民事または刑事上の違反のリスク.
- High: 執行プログラムにとって特に重要な民事または刑事上の違反のリスク

5.4 Risk Acceptance and Compensating Controls

SP 800-63 スイートは Assurance Level に基づき Digital Identity サービスに対する基本要件を示す. 各機関は本ガイドライン群の要件に従って Identity サービスを実装すべきであり (SHOULD), さらにシステムをセキュアにしたりプライバシーを強化するべく追加の技法や技術を検討すべきである (SHOULD).

各機関は, ミッション, リスク許容範囲, 既存のビジネスプロセス, 特定の人々への特別な考慮事項, 本スイートに記載されているものと同様の緩和策を実現するためのデータの可用性, 当該組織固有のその他の能力などに基づき, 評価された xALs に対して NIST 推奨ガイダンス代替策を講じてもよい (MAY).

適用可能な SP 800-63 要件が完全には実装されていない場合, 各機関は任意の代替策の比較可能性を示さなければならない (SHALL). 例えば, National Information Assurance Partnership (NIAP) 保護プロファイルが FIPS 要件と同等もしくはより強固である場合, 当該機関は FIPS の代わりに National Information Assurance Partnership (NIAP) 保護プロファイルを選択してもよい. 機関は機関自身の能力に基づいて評価済 xAL を変更してはならないが (SHALL NOT), SP 800-63 に明記されていない手段によりリスクを低減する能力に基づいて自身のソリューションの実装を調整することは可能である (MAY). 機関は Normative 要件から逸脱する正当な理由と, 自身が採用する代替策の詳細をドキュメント化するべく手順化しなければならない (SHALL).

本ガイダンスは Authentication と Identity Proofing エラーに関するリスクのみを扱う. NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems [SP 800-30] は, 政府システムにおいてリスクを管理する一般的方法論を推奨している.

5.5 Digital Identity Acceptance Statement

各機関は SA&A を達成するために必要な既存の成果物にこの情報を含めるべきである (SHOULD).

このステートメントには, 最低限以下の情報を含めること (SHALL).

1. 評価済 xAL.
2. 実装済 xAL.
3. 実装済 xAL が評価済 xAL と異なる場合は, その根拠.
4. 適用可能な 800-63 要件が完全には実装されていない場合, 代替策の比較可能性.
5. Federated Identity を採用していない場合は, その根拠.

5.6 Migrating Identities

本ガイドライン群は改訂され要件にも変更が起こるため, CSP はそれが自身のユーザーに与える影響を考慮しなければならない (SHALL). ユーザーに影響がない場合もあるが, ユーザーに移行手続を要求することもあるでしょう. 例えば, 改訂後の最初のログイン時に, CSP は新しい IAL 要件を遵守すべくユーザーに追加の身元確認書類を要求するかもしれません. これは CSP, 当該 CSP を利用する RP, ミッション, 対象ユーザーといったコンテキストを考慮して, リスクに基づいて決定すること (SHALL). 以下の考慮点は, 機関が要件変更の影響を考慮する場合の向けのガイドである.

1. RP で Identity 関連の詐欺が発生している場合は, 移行が有益である可能性がある. そうでなければ移行には価値がないかもしれない.
2. 新しくより強固ないしはよりユーザーフレンドリーな Authentication の選択肢が個々の AAL に追加されれば, CSP は新しい Authenticator を発行したり, ユーザーがすでに持っている Authenticator を登録させることが可能になる.
3. Federation 要件はユーザー影響があるかもしれないしないかもしれない. 例えば, 同意要件やインフラストラクチャー要件により, インフラストラクチャーやプロトコルのアップグレードが必要になることもある.
4. xAL の追加や削除は移行を必要としないかもしれないが, RP 側での変更が必要かどうかを決定すべく新規に Risk Assessment を行うことになるであろう.

本ガイダンスでは, 必ずしも移行を行う必要があるとはしておらず, 改訂版がリリースされた時点で考慮が必要であることのみを定めている. 両者のリスク許容範囲とミッションに基づいた最良のアプローチの決定は, CSP と RP の判断に委ねられる.

6 Selecting Assurance Levels

This section is normative.

Risk Assessment の結果は最適なレベル選択における第一の要素となる. 本セクションでは Risk Assessment の結果を, リスクと無関係なその他の要素と合わせて, どのように最も有益な xAL 選択を行うかについて詳説する.

第一に, Risk Assessment 影響プロファイル を, Table 6-1 にある各 Assurance Level に関連する影響プロファイルと比較する. 必要な Assurance Level を決定するには, Risk Assessment により得られた全カテゴリーにおける潜在的影響に合致ないしは超越する影響プロファイルを見つけること.

Table 6-1 Maximum Potential Impacts for Each Assurance Level

	Assurance Level		
影響カテゴリー	**1**	**2**	**3**
不便, 苦痛, または社会的地位やレピュテーションの毀損	Low	Mod	High
経済的損失または機関の負債	Low	Mod	High
機関のプログラムや公共の利益への損害	N/A	Low/Mod	High
Authorize のないセンシティブ情報の公開	N/A	Low/Mod	High
個人の安全	N/A	Low	Mod/High
民事または刑事上の違反	N/A	Low/Mod	High

リスクを分析するにあたり, 機関は, 何らかの失敗を引き起こしたり人・組織に損害を及ぼす可能性を含む, 予想される Authenticatino 失敗の直接的および間接的な結果のすべてを考慮しなければならない (SHALL). 潜在的な影響の定義には, 意味がコンテキストに依存する “相当” または “軽微” のような相対的な用語が含まれる. 機関はこういった被害の相対的重要性を決定するために, 影響を受ける人や主体のコンテキストや性質を考慮すべきである (SHOULD). 時間が経つにつれて, 機関はこれらの問題に関する実践的な経験を得ることとなり, これらの用語の意味はより明確になるであろう. 機関のプログラムや公共の利益に対する被害の分析はコンテキストに強く依存するため, 機関はこれらの問題を注意深く考慮すべきである (SHOULD).

IAL, AAL, FAL の各 Assurance Level 値はそれぞれ異なる可能性もある. 例えばある機関が, ユーザーにより Personal Health Information (PHI) といった形で Personal Information が提出される “health tracker” アプリケーションを構築したとする. EO 13681 には “デジタルアプリケーションを通じて, 市民に対して Personal Data への Access を可能にする全機関は, Multi-factor Authentication を採用する必要がある” と定められており, 当該機関は AAL2 ないしは AAL3 で MFA を実装する必要がある.

また EO 13681 は, Personal Information が公開される場合, 各機関が “必要に応じて有効な Identity Proofing プロセス” を行うことを要求している. これは (必要な AAL に合致するよう) IAL2 や IAL3 での Proofing が必要であるということを意味しない. 上記の例では, 機関のシステムはユーザーの実際の Identity を知る必要もないかもしれない. このケースでは, “有効な Proofing プロセス” というのは Proofing を一切行わないこととなり, 機関は IAL1 を選択することになるであろう. これによりHealth Tracker システムのユーザーは Pseudonymous な状態でいることができる.

ユーザーが Pseudonymous な状態である一方で, 機関 Authentication においては AAL2 や AAL3 を選択するべきである. さもないと悪意ある主体が正規ユーザーのアカウントを侵害し, 当該ユーザーの PHI に Access 可能となってしまう.

> Note: 機関は上表で求められている以上の Assurance Level を許容することもできる. 例えば Federated Transaction では, IAL2 と評価されたアプリケーションにおいて IAL3 の Identity を受け入れることも可能である. これは Authenticator に対しても同様であり, RP が必要とするより強固な Authenticator を利用することも可能である. ただし RP は, こういったことが　CSP によって適切なプライバシー保護がなされている Federated シナリオのみで発生し, RP が要求し Subscriber が Authorize した Attribute のみが RP に提供され, 過度な Personal Information が Credential や Assertion から漏れることがないよう保証する必要がある. 詳細は SP 800-63C の Privacy Considerations (sp800-63c.html#privacy) を参照のこと.

Note: 単一のアプリケーションにおいて異なる IAL, AAL, FAL を設定可能ということは, 本ドキュメントがもはや総合的な LOA という概念をサポートしていないということである. LOA 決定のための “Low Watermark” アプローチはもはや通用しない. IAL1 かつ AAL2 のアプリケーションを, IAL2 かつ AAL2 のアプリケーションよりセキュアでないとかプライバシー強度が低いとみなすべきではない. これらのアプリケーションの差異は, 必要とされる Proofing の程度のみであり, それはアプリケーションのセキュリティーやプライバシーには影響しないかもしれない. 一方でもし機関が誤った xAL 選択を行うと, セキュリティーやプライバシーに大きな影響を及ぼす可能性がある.

6.1 Selecting IAL

Figure 6-1 に示す IAL の決定木は, Risk Assessment の結果と Identity Proofing サービスに関する追加の考慮事項を組み合わせ, 各機関がデジタルサービスの提供に最適な Identity Proofing 要件を決定する際の一助となる.

IAL 選択の実施は, 当該デジタルサービス提供者が Proofing を行わなければならないということを意味するものではない. 機関が Federate できるかどうかは Section 7 に詳しく述べる.

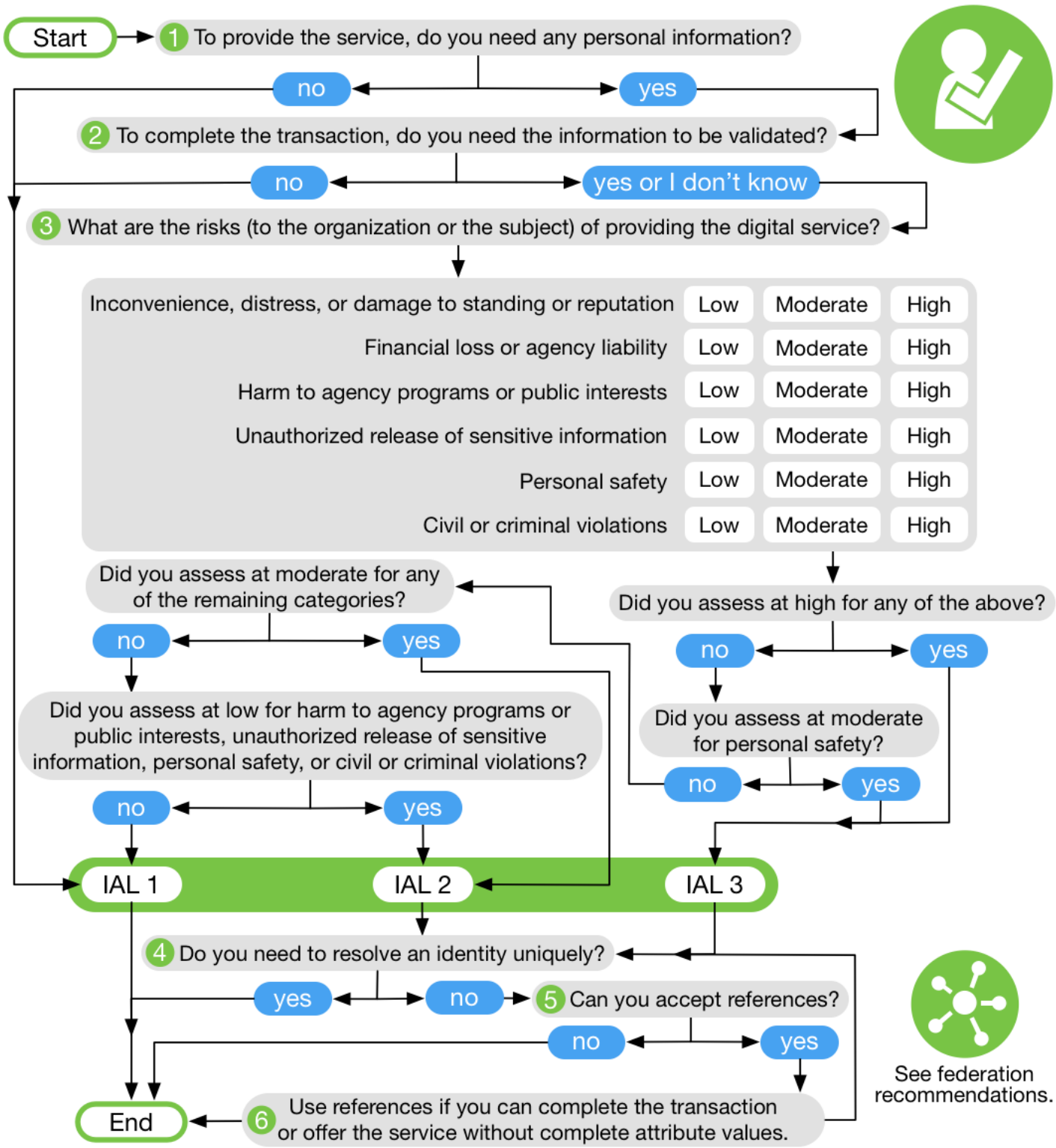


Figure 6-1 Selecting IAL

1 To provide the service, do you need any personal information?
最初にこの問いに答えることで, Risk Assessment と IAL 選択はショートカットできる. サービスがデジタル Transaction 実行に際していかなる Personal Information も必要としない場合, システムは IAL1 で運用可能である.
2 To complete the transaction, do you need the information to be validated?
RP は Personal Information が必要であれば, 確認済かつ検証済な Attribute が必要か, Self-asserted な Attribute が許容可能かを判断する必要がある. ひとつでも確認済かつ検証済な Attribute が必要な場合は, IAL2 か IAL3 の Proofing を行なった上で Attribute を受け入れる必要があるであろう. Self-asserted な Attribute のみでデジタルサービスを提供可能であれば, IAL 選択はショートカットして IAL1 に落ち着くことができる.
3 What are the risks (to the organization or the subject) of providing the digital service?
この段階では, 機関はある程度の Proofing が必要であることは理解していることになる. Step 3 は, IAL2 と IAL3 のどちらが最適な選択かを決定するために, Identity Proofing が失敗した際の潜在的影響に着目している. 機関が陥る可能性のある主な Idetity Proofing 失敗は, 偽造された Identity を真として受け入れてしまうことである. これによりサービスや利益を間違った人物や不適格な人物に提供してしまうことになる. さらに, Proofing が必要ない場合や必要以上に多くの情報を収集してしまった場合, それ自体がリスクとなりうる. 従って必要がないのに検証済 Attribute を取得することも, Identity Proofing の失敗であるとみなされる. このステップでは, サービス提供の為に Personal Information が必要であるかどうか察知し, 機関が Step 1 および 2 に誤って回答していないかどうかを検知すべきである. 片方にはネガティブな影響がない場合でも, もう一方には著しい被害が及ぶ可能性もあるため, リスクは組織およびユーザーの両方の視点で考慮すべきである. 機関の Risk Management プロセスはこのステップから開始されるべきである.
4 Do you need to resolve an identity uniquely?
Step 4 では, 機関が要求する Personal Information が最終的に Identity の特定につながるかどうかを決定する. この問いは言い換えれば, 機関がデジタルサービスに Access する Subject の完全な Identity を知る必要があり, 2-3 の Attribute が確認済かつ検証済みであったとしても Pseudonymous Access が不可能かどうかということである. 機関が Subject を特定する必要がある場合, IAL 選択プロセスは終了可能である. しかしながら機関は, Step 5 が価値あるものかどうか検討すべきである. Claim (訳注: draft 段階では "Attribute Claim" と呼ばれていた "Attribute Reference" のこと) の受け入れにより, 必要以上の Personal Information の収集や保存のリスクを軽減することができる.
5 Can you accept references?
Step 5 はデジタルサービスが完全な Attribute Value への Access なしに提供可能かどうかにフォーカスしている. これはすべての Attribute が Claim として受け渡されなければならないという意味ではなく, 機関が必要と判断する個人の各 Attribute に着目し, どれは Claim で十分であり, どれは完全な Value でないといけないかを判断するよう求めるものである. Federated な環境ではデジタルサービス提供者は Attribute 情報を最初から管理下に置いていないため, Claim 受け取りに最適である. アプリケーションがすべての必要な Identity Proofing を自身で実行するのであれば, すべての Value がすでにデジタルサービス提供者の管理下にあるため, Claim 受け渡しは意味がない可能性もある.
6 Use references if you can complete the transaction or offer the service without complete attribute values.
もし機関が Step 6 にたどり着いたとすれば, Claim を利用すべきである. このステップにたどり着いたということは, デジタルサービスの提供に完全な Attribute Value が必要でないと判断されたということであり, デジタルサービスは Federated Attribute Reference を CSP (もしくは複数の CSPs) から受け取るのに最適であると判断される.

> Note: 機関は最適な Proofing プロセスを選択する際に, 自身のサービス対象のユーザー層も考慮すべきである. IAL 選択の機能ではないものの, ある種の Proofing プロセスはある種のユーザー層に対して他のプロセスより適切である可能性がある. 対象ユーザー層により高い Proofing 成功率を高められるため, この種の分析は機関にメリットをもたらすであろう.

6.2 Selecting AAL

Figure 6-2 に示す AAL の決定木は, Risk Assessment の結果と Authentication に関する追加の考慮事項を組み合わせ, 各機関がデジタルサービスの提供に最適な Authentication 要件を決定する際の一助となる.

AAL 選択の実施は, 当該デジタルサービス提供者が自身で Authenticator を発行しなければならないということを意味するものではない. 機関が Federate できるかどうかは Section 7 に詳しく述べる.

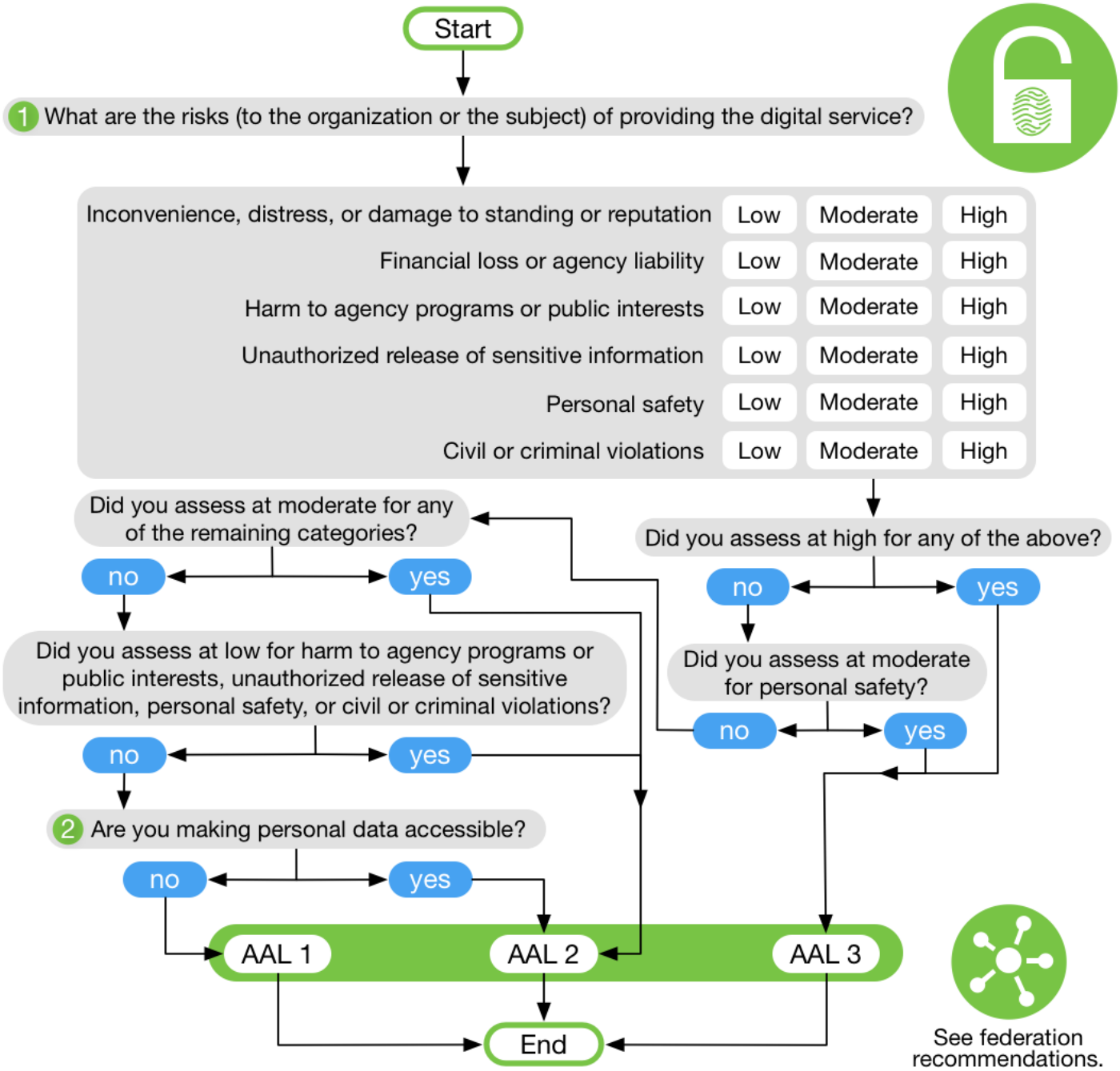


Figure 6-2 Selecting AAL

1 What are the risks (to the organization or the subject) of providing the digital service?
Step 1 では Authentication 失敗の潜在的影響に着目する. これはつまり, Authorize されていないユーザーが正規のユーザーアカウントに Access できた場合, 何が起こるかということである. 片方にはネガティブな影響がない場合でも, もう一方には著しい被害が及ぶ可能性もあるため, リスクは組織およびユーザーの両方の視点で考慮すべきである. 機関の Risk Management プロセスはこのステップから開始されるべきである.
2 Are you making personal data accessible?
Personal Information にオンラインでアクセス可能な場合は, MFA が必要となる. この決定木の他のパスではすでに MFA が必要な AAL が確定しているため, Personal Information に関して問われるのはこの段階のみとなる. Risk Assessment 実施に際しては, 全ての AAL で Personal Information の公開に関して検討すべきである. このステップで重要な点は, Personal Information をオンラインで収集しない場合, AAL2 以上を要求するために Personal Information を確認・検証する必要はないということである. Self-asserted Personal Information の公開時も MFA によるアカウント保護は必要である. Self-asserted な情報は偽造可能だが, ほとんどのユーザーはデジタルサービスの恩恵を受けるため正しい情報を提供するであろう. したがって Self-asserted データは適切に保護しなければならない.

6.3 Selecting FAL

Figure 6-3 に示す FAL の決定木は, Risk Assessment の結果と Federation に関する追加の考慮事項を組み合わせ, 各機関がデジタルサービスの提供に最適な要件を決定する際の一助となる.

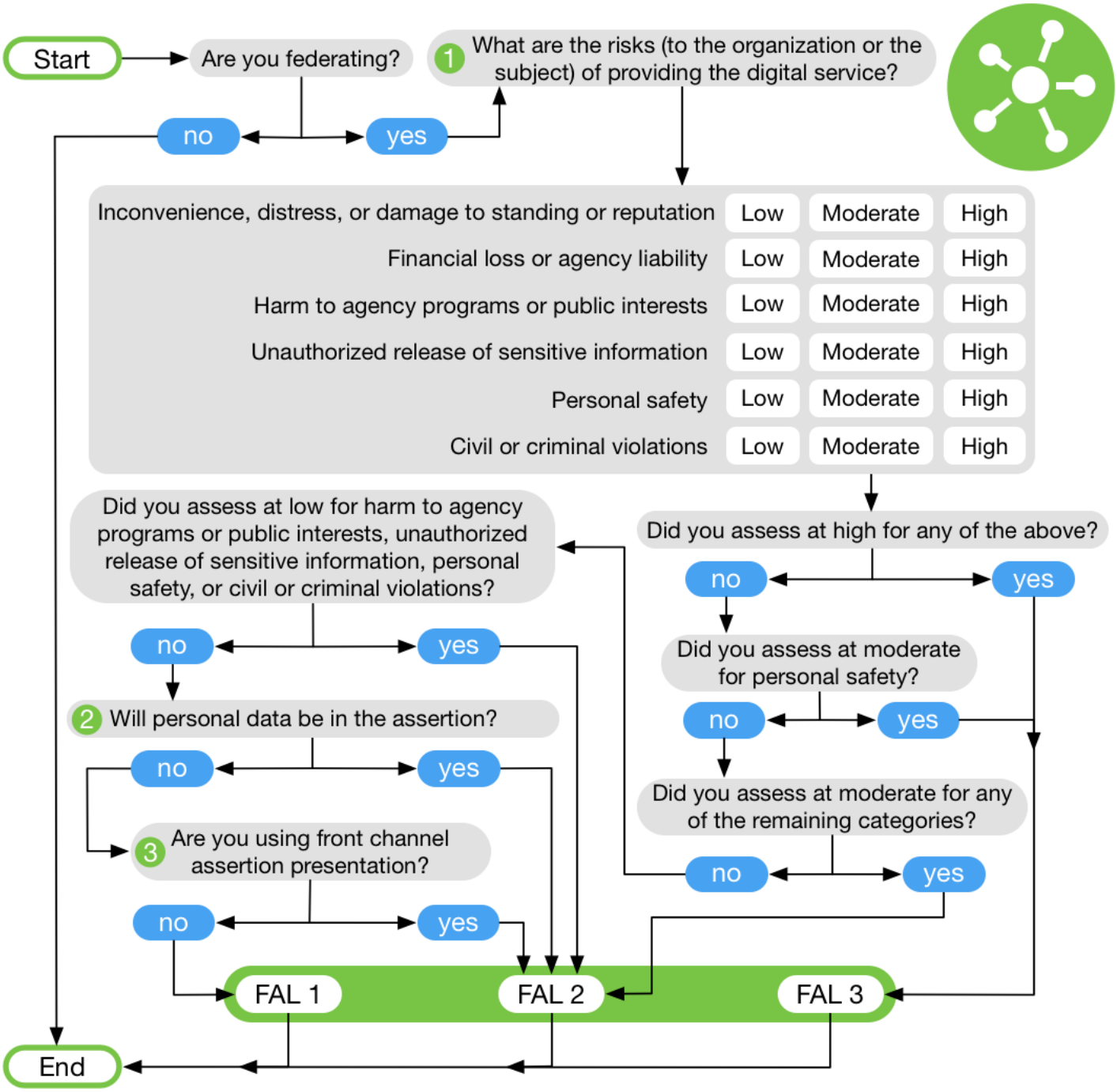


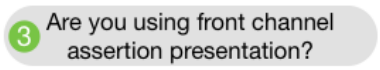
Figure 6-3 Selecting FAL

1 What are the risks (to the organization or the subject) of providing the digital service?

Step 1 では Federation 失敗の潜在的影響に着目する. これはつまり, Authorize されていないユーザーが Assertion を毀損できた場合, 何が起こるかということである. Assertion 毀損の例としては, Assertion のリプレイによるなりすまし, ブラウザを会した Assertion 情報の漏洩などが挙げられる. 片方にはネガティブな影響がない場合でも, もう一方には著しい被害が及ぶ可能性もあるため, リスクは組織およびユーザーの両方の視点で考慮すべきである. 機関の Risk Management プロセスはこのステップから開始されるべきである.

2 Will personal data be in the assertion?

Personal Information が Assertion を介してやり取りされる場合は, FAL2 が必須となる. Risk Assessment 実施にあたっては, 全ての FAL で Personal Information の公開について考慮すべきである. Assertion に Personal Information が含まれる場合は FAL2 以上が必要であり, FAL1 の Audience 要件および暗号化要件では Personal Information の保護には不十分である. Self-asserted Personal Information の公開時にも FAL2 による Assertion 保護が必要である. Self-asserted な情報は偽造可能だが, ほとんどのユーザーはデジタルサービスの恩恵を受けるため正しい情報を提供するであろう. ただし Personal Information が RP による Authorized API Call で提供される場合には, それらの情報は Assertion 自体に含める必要はない. その場合には Assertion に Personal Information が含まれないため, 暗号化は必須ではなく FAL の暗号化要件も適用されない.



RP は, より高度なプライバシーおよびセキュリティーを実現するため, 可能であれば [SP 800-63C Section 7.1](sp800-63c.html#back-channel) にある Back-channel での提示方式を用いるべきである. この方式では Subscriber は Assertion 自体ではなく Assertion Reference のみを扱うため, Subscriber のブラウザやその他のプログラムに渡った Assertion から Attribute やその他のセンシティブ情報が漏洩する可能性は低下する. RP は Assertion Reference を直接 IdP に提示するため, IdP は RP を識別し Authenticate することができる. さらに RP は Assertion を Authenticated Protected Channel 経由で IdP から直接受け取るため, Attacker が RP に対して Assertion を注入する可能性も低下する.

全ての FAL において, Assertion には, 署名, 有効期限, Audience 制約, その他 SP 800-63C (sp800-63c.html#assertions) に列挙された基本的保護策が施される. これらの対策により, Assertion は Authorize されていない主体により作成・変更されることはなくなり, RP が異なるシステム向けに作成された Assertion を受け入れることもなくなる.

6.4 Combining xALs

本ガイドラインは各 xAL を相互に一致させることなく選択可能なモデルを提示している. あるシステムに対して多様な xAL の選択肢が存在するが, 多くの場合全ての xAL に同じレベルが適用されるであろう.

多様な xAL の組み合わせが可能となったことにより, 各機関には大きな柔軟性がもたらされたが, 個人から取集するデータの性質とそのデータを保護する Authenticator の性質上, 全ての組み合わせが可能なわけではない. Table 6-2 には Personal Information が MFA で保護されることを保証可能な IAL と AAL の組み合わせをまとめる.

Table 6-2 Acceptable Combinations of IAL and AAL

	AAL1	AAL2	AAL3
IAL1: Without personal data	Allowed	Allowed	Allowed
IAL1: With personal data	**NO**	Allowed	Allowed
IAL2	**NO**	Allowed	Allowed
IAL3	**NO**	Allowed	Allowed

Note: Executive Order 13681 [EO 13681] によると, Personal Data が Self-asserted かつ未検証であっても, Personal Data 公開には MFA が必須である. Personal Data へのアクセスを生じさせない Transaction では, ユーザーにより強固な Authentication の選択肢を提供することが推奨されるものの, AAL1 での Authentication も可能である. さらに IAL1 では個人に紐づかない情報を Self-assert することもあるが, そのようなケースでは AAL1 が適用可能である.

7 Federation Considerations

This section is informative.

本ガイドラインおよび付随する Vol. は, 各機関が選択する Authentication および Identity Proofing アーキテクチャーに関しては不問である. しかしながら, 機関や個々のアプリケーションローカルで Identity サービスを構築するよりも, Identity Federation を利用した方がより効率的かつ効果的になるようなシナリオが存在する. 以下に Federation が利用可能であればそれを有望な選択肢として考慮すべきシナリオをまとめる. なおこのリストは Federation とローカルの Identity アーキテクチャーの経済的メリットデメリットを考慮したものではない.

Authenticator を Federate すべきケース:

1. 潜在的ユーザーがすでに必要な AAL 以上を満たす Authenticator を持っている.
2. 想定される全てのユーザーコミュニティーをカバーするために複数の Credential フォームファクターが必要である.
3. 機関が Authentication 管理 (e.g., アカウントリカバリー, Authenticator 発行, ヘルプデスク) のためのインフラストラクチャーを保持していない.
4. RP 実装を変更することなく, 時間経過によりプライマリーな Authenticator を追加したりアップグレードしたいという要望がある.
5. サポートすべき複数の環境がある. Federation プロトコルは Network ベースであり, 多様なプラットフォームや言語による実装が可能である.
6. 潜在的ユーザーが複数のコミュニティーに所属し, それぞれが独自に既存の Identity インフラストラクチャーを保持している.

Attribute を Federate すべきケース:

1. ステークホルダーがサービスに Access するために, Pseudonymity が必須, 必要, 実現可能ないしは重要である.
2. サービスへの Access に部分的な Attribute リストのみが必要である.
3. サービスへの Access に少なくとも1つ以上の Attribute Reference のみが必要である.
4. 当該機関は必要な Attribute の権威ある情報元や発行元ではない.
5. Attribute は (Access 判断など) 一時的な利用のためだけに必要であり, 機関は当該データをローカルに永続化する必要はない.

8 References

This section is informative.

8.1 General References

[A-130] OMB Circular A-130, *Managing Federal Information as a Strategic Resource*, July 28, 2016, available at: https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf (https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf).

[eIDAS] European Union, *REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL*, July 23, 2014, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG (http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG).

[EO 13681] Executive Order 13681, *Improving the Security of Consumer Financial Transactions*, October 17, 2014, available at: https://www.federalregister.gov/d/2014-25439 (https://www.federalregister.gov/d/2014-25439).

[ESIG] Federal CIO Council, *Use of Electronic Signatures in Federal Organization Transactions*, January 25, 2013, available at: https://cio.gov/wp-content/uploads/downloads/2014/03/Use_of_ESignatures_in_Federal_Agency_Transactions_v1-0_20130125.pdf (https://cio.gov/wp-content/uploads/downloads/2014/03/Use_of_ESignatures_in_Federal_Agency_Transactions_v1-0_20130125.pdf).

[FISMA] *Federal Information Security Modernization Act of 2014*, available at: https://www.congress.gov/bill/113th-congress/senate-bill/2521 (https://www.congress.gov/bill/113th-congress/senate-bill/2521).

[GPG 44] UK Cabinet Office, Good Practice Guide 44, *Authentication and Credentials for use with HMG Online Services*, August 8, 2016, available at: https://www.ncsc.gov.uk/guidance/authentication-and-credentials-use-hmg-online-services-gpg-44 (https://www.ncsc.gov.uk/guidance/authentication-and-credentials-use-hmg-online-services-gpg-44).

[GPG 45] UK Cabinet Office, Good Practice Guide 45, *Identity proofing and verification of an individual*, November 3, 2014, available at: https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual (https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual).

[HSPD-12] Department of Homeland Security, *Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004, available at: https://www.dhs.gov/homeland-security-presidential-directive-12 (https://www.dhs.gov/homeland-security-presidential-directive-12).

[M-03-22] OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 26, 2003, available at: https://georgewbush-whitehouse.archives.gov/omb/memoranda/m03-22.html (https://georgewbush-whitehouse.archives.gov/omb/memoranda/m03-22.html).

[M-04-04] OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, December 16, 2003, available at: https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy04/m04-04.pdf (https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy04/m04-04.pdf).

[NSTIC] *National Strategy for Trusted Identities in Cyberspace*, April 2011, available at: https://www.nist.gov/sites/default/files/documents/2016/12/08/nsticstrategy.pdf (https://www.nist.gov/sites/default/files/documents/2016/12/08/nsticstrategy.pdf).

[NIST RMF] Risk Management Framework Overview, available at http://csrc.nist.gov/groups/SMA/fisma/framework.html (http://csrc.nist.gov/groups/SMA/fisma/framework.html).

[RSDOPS] UK Cabinet Office, Good Practice Guide 43, *Requirements for Secure Delivery of Online Public Services (RSDOPS)*, November 3, 2014, available at: https://www.gov.uk/government/publications/requirements-for-secure-delivery-of-online-public-services (https://www.gov.uk/government/publications/requirements-for-secure-delivery-of-online-public-services).

[Steiner] Steiner, Peter. “On the Internet, nobody knows you’re a dog”, *The New Yorker*, July 5, 1993.

[STORK 2.0] European Union, *Secure idenTity acrOss boRders linKed 2.0*, 2014, available at: https://www.eid-stork2.eu/ (https://www.eid-stork2.eu/).

8.2 Standards

[BCP 195] Sheffer, Y., Holz, R., and P. Saint-Andre, *Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*, BCP 195, RFC 7525,DOI 10.17487/RFC7525, May 2015, https://doi.org/10.17487/RFC7525 (https://doi.org/10.17487/RFC7525).

[Canada] Government of Canada, *Standard on Identity and Credential Assurance*, February 1, 2013, available at: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26776 (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26776).

[ISO 9241-11] International Standards Organization, ISO/IEC 9241-11 *Ergonomic requirements for office work with visual display terminals (VDTs) — Part 11: Guidance on usability*, March 1998, available at: https://www.iso.org/standard/16883.html (https://www.iso.org/standard/16883.html).

[ISO 29003] International Standards Organization, ISO/IEC DTS 29003 *Information technology — Security techniques — Identity proofing*.

[ISO 29115] International Standards Organization, ISO/IEC 29115 *Information technology — Security techniques — Entity authentication assurance framework*, April 1, 2013, available at: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=45138 (http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=45138).

[OIDC] Sakimura, N., Bradley, B., Jones, M., de Medeiros, B., and C. Mortimore, *OpenID Connect Core 1.0 incorporating errata set 1*, November, 2014, available at: https://openid.net/specs/openid-connect-core-1_0.html (https://openid.net/specs/openid-connect-core-1_0.html).

8.3 NIST Special Publications

NIST 800 Series Special Publications are available at: http://csrc.nist.gov/publications/nistpubs/index.html (http://csrc.nist.gov/publications/nistpubs/index.html). The following publications may be of particular interest to those implementing systems of applications requiring digital authentication.

[SP 800-30] NIST Special Publication 800-30 Revision 1, *Guide for Conducting Risk Assessments*, September 2012, https://doi.org/10.6028/NIST.SP.800-30r1 (https://doi.org/10.6028/NIST.SP.800-30r1).

[SP 800-37] NIST Special Publication 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach*, February 2010 (updated June 5, 2014), https://doi.org/10.6028/NIST.SP.800-37r1 (https://doi.org/10.6028/NIST.SP.800-37r1).

[SP 800-52] NIST Special Publication 800-52 Revision 1, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, April 2014, http://dx.doi.org/10.6028/NIST.SP.800-52r1 (http://dx.doi.org/10.6028/NIST.SP.800-52r1).

[SP 800-53A] NIST Special Publication 800-53A Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations, Building Effective Assessment Plans*, December 2014 (updated December 18, 2014), https://doi.org/10.6028/NIST.SP.800-53Ar4 (https://doi.org/10.6028/NIST.SP.800-53Ar4).

8.4 Federal Information Processing Standards

[FIPS 199] Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, https://doi.org/10.6028/NIST.FIPS.199 (https://doi.org/10.6028/NIST.FIPS.199).

[FIPS 201] Federal Information Processing Standard Publication 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, August 2013, http://dx.doi.org/10.6028/NIST.FIPS.201-2 (http://dx.doi.org/10.6028/NIST.FIPS.201-2).

Appendix A—Definitions and Abbreviations

This section is normative.

A.1 Definitions

Authentication 分野で使われる用語は幅広く, 多くの用語は以前のバージョンの SP 800-63 と整合性を保っているものの, いくつかは本リビジョンから定義が変更になっている. 多くの用語に複数の定義がありうるため, 本ドキュメントにおける定義を明確にする必要がある.

Access

オンラインのデジタルサービスの1つ以上の個別機能に接続すること.

Active Attack

Attacker が Claimant, Credential Service Provider (CSP), Verifier, Relying Party (RP) に対してデータを送信するような Authentication Protocol における Attack のこと. Active Attack の例としては Man-in-the-Middle Attack (MitM), Impersonation, Session Hijacking などが挙げられる.

Address of Record

許可された手段によって特定個人とのコミュニケーションに利用可能な, 有効かつ検証済の (物理的またはデジタルの) 場所情報.

Applicant

Enrollment および Identity Proofing のプロセスを受けている主体.

Approved Cryptography

Federal Information Processing Standard (FIPS) の承認, もしくは NIST の推奨を受けているもの. FIPS ないしは NIST Recommendation に (1) 指定されているか, (2) 採用されているアルゴリズムおよびテクニック.

Assertion

Verifier から Relying Party (RP) に対して送られる, Subscriber の Identity 情報を含んだ Statement. Assertion は検証済属性情報を含むこともある.

Assertion Reference

Assertion と紐付けて生成されるデータオブジェクトであり, Verifier を識別するとともに, Verifier が所有する Full Assertion へのポインタとして機能する.

Asymmetric Keys

Public Key と Private Key からなる鍵ペア. 暗号化と復号, 署名生成と署名検証など, 対となるオペレーションに用いられる.

Attack

Authorize されていない主体が, Verifier や RP をだまして当該個人を Subscriber だと信じ込ませようとする行為.

Attacker

不正な意図を持ち情報システムに不正アクセスする主体. 内部犯も含む.

Attribute

人や物に関する生来の性質や特徴.

Attribute Bundle

パッケージ化された Attribute の集合で, 通常は単一の Assertion に含まれる. Attribute Bundle により, RP は関連する必要な Attribute 一式を IdP から簡単に受け取ることができる. Attribute Bundle は OpenID Connect の scope [OpenID Connect Core 1.0] と同義である.

Attribute Reference

Subscriber のプロパティーを Assert する Statement である. 必ずしも Identity 情報を含む必要はなく, フォーマットは問わない. 例えば, “birthday” という Attribute に対しては, “older than 18” や “born in December” などが Attribute Reference たりうる.

Attribute Value

Subscriber のプロパティーを Assert する完全な Statement. フォーマットは問わない. 例えば “birthday” という Attribute に対しては, “12/1/1980” や “December 1, 1980” などが Attribute Value となりうる.

Authenticate

Authentication 参照.

Authenticated Protected Channel

接続元 (Client) が 接続先 (Server) を Authenticate しており, Approved Cryptography を用いて暗号化されたコミュニケーションチャネル. Authenticated Protocol Channel は機密性および MitM 保護を提供するものであり, ユーザーの Authentication プロセスの中でよく使われるものである. Transport Layer Security (TLS) [BCP 195] がその例としてあげられ, TLS では接続先が提示した Certificate を接続元が検証することになる. 特に指定がない限り, Authenticated Protected Channel では Server が Client を Authenticate する必要はない. Server の Authentication は, 各 Server 個別の対応ではなく, しばしば Trusted Root から始まる Certificate Chain を用いて行われる.

Authentication

ユーザー, プロセス, デバイスなどの Identity を検証すること. しばしばあるシステムのリソースへの Access を許可する際の必須要件となる.

Authentication Factor

something you know, *something you have*, および *something you are* という3種類の Authentication Factor がある. 全ての Authenticator はこれら1つ以上の Authentication Factor を持つ.

Authentication Intent

ユーザーを Authentication フローに介在させるプロセスを経ることによって, Claimant が Authenticate ないしは Reauthenticate を行う意思を確認するプロセス. Authenticator によっては, Authentication Intent をオペレーションの一部に含むこともあれば (e.g., OTP デバイス), ボタンを押させるなどといった特別なステップを要求するものもある. Authentication Intent は, 当該 Endpoint を Proxy として, マルウェアが Subscriber に気づかれずに Attacker を Authenticate してしまうケースに対する対抗策となる.

Authentication Protocol

Claimant が正規の Authenticator の所有および管理権限を示すことで自身の Identity を確立するプロセスにおいて, Claimant と Verifier の間でやりとりされる一連のメッセージの定義. Claimant が意図した Verifier とコミュニケーションしていることを立証するためのプロセスを含むこともある.

Authentication Protocol Run

Claimant と Verifier との間で Authentication (または Authentication 失敗) という結果に至るまでの, 一連のメッセージ交換.

Authentication Secret

あらゆる鍵を示す一般的な呼び名. Authentication Protocol において Attacker が Subscriber になりすますために利用することもできる.

Authentication Secret は *short-term authentication secrets* と *long-term authentication secrets* に分類することができ, 前者は限定的な期間のみ利用可能なもの, 後者は手動でリセットされるまで使い続けられるものを示す. Authenticator Secret は long-term authentication secret の代表的な例であり, Authenticator の出力する鍵が Authenticator Secret と異なる場合, その出力された鍵は一般的に short-term authentication secret である.

Authenticator

Claimant が所有および管理するもので, 典型的な例としては暗号モジュールやパスワード等がある. Authenticator は Claimant の Identity を Authenticate するために用いられる. SP 800-63 の前エディションまでは *token* と呼ばれていたものと同等である.

Authenticator Assurance Level (AAL)

Authentication プロセスの強度を示すカテゴリー.

Authenticator Output

Authenticator によって生成される出力値. 必要に応じて正当な Authenticator Output を生成することで, Claimant が Authenticator を所有し管理していることを証明できる. Verifier へ送信されるプロトコルメッセージは Authenticator Output によって異なり, プロトコルメッセージが明示的に Authenticator Output を含んでいることもあればそうでないこともある.

Authenticator Secret

Authenticator に内包されるシークレット値.

Authenticator Type

共通の特徴を持つ Authenticator のカテゴリー. Authenticator Type によっては単一の Authentication Factor のみを持つものもあれば, 2つの Authentication Factor を持つものもある.

Authenticity

データが意図された情報源から得られたものであるというプロパティー.

Authoritative Source

Identity Evidence の Issuing Source がもつ正確な情報に Access できる, もしくは検証済みコピーを所有している主体. これにより Identity Proofing 実施時に CSP が Applicant の提出した Identity Evidence の有効性を確認できる. Issuing Source 自身が Authoritative Source であることもありうる. Authoritative Source は, Identity Proofing の検証フェーズの前に, 機関や CSP のポリシーによって決定されることも多い.

Authorize

access を許可するかどうかの判断. 通常は Subject の Attribute を評価することで自動的に判断される.

Back-Channel Communication

2つのシステム間で直接コネクションを貼って行われるコミュニケーション (標準プロトコルレベルでのプロキシの利用を許容する). ブラウザ等を媒介としたリダイレクトは用いない. HTTP Request & Response により実現される.

Bearer Assertion

ある主体が Identity を証明するために提示する Assertion であり, Assertion を保有していること自体が Assertion 持参人の Identity 証明として十分であるようなもの.

Binding

Subscriber の Identity と Authenticator や Subscriber Session の間の関連性.

Biometrics

個人の行動や生体情報をもとに個人を自動認識すること.

Challenge-Response Protocol

Verifier が Claimant に対してチャレンジ (通常はランダム値やノンス) を送信し, Claimant はシークレットと連結 (チャレンジと Shared Secret を一緒にハッシュしたり, チャレンジに対して Private Key による操作を実施) して応答を生成し, Verifier に返却するような Authentication Protocol. Verifier は Claimant が生成した応答を自身のみで検証 (チャレンジと Shared Secret のハッシュを再計算してレス

ポンスと比較したり, レスポンスに対して Public Key による操作を実施) し, Claimant がシークレットを所有し管理下に置いているを証明することができる.

Claimant

1つ以上の Authentication Protocol により Identity を検証される Subject.

Claimed Address

Subject により, 自分に到達可能だと Assert された物理的位置. 居住地の住所や郵便の届く住所などを含む.

例えば, 外国籍のパスポートを所持している状態で U.S. に在住する人物であれば, Identity Proofing プロセスにおいて住所を要求されることになる. そう言った場合の住所は, “address of record” ではなく “claimed address” となろう.

Claimed Identity

ある Applicant による, 個人に関する未検証かつ未証明な Attribute の申告.

Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA)

利用者が人間か自動化されたエージェントかを区別するために Web フォームに追加する対話的な機能. 典型的には, 歪んだ画像や音声に対応するテキストの入力を求める方式である.

Credential

ある Identity および (任意で) 追加の Attribute を, 識別子を通じて, Subscriber が所有ないしは管理する Authenticator に紐付ける, 信頼のおけるオブジェクトもしくはデータ構造.

一般的に Credential は Subscriber に管理されることが想定されるが, 本ガイドライン群では Subscriber の Authenticator と Identity の紐付けを確立する CSP 管理下の電子レコードを指すこともある.

Credential Service Provider (CSP)

Subscriber の Authenticator を発行もしくは登録し, Subscriber に電子的な Credential を発行する信頼された主体. CSP は独立した第三者となることもあれば, 自身で発行した Credential を用いて自らサービスを提供することもある.

Cross-site Request Forgery (CSRF)

RP に対して Authenticate されている Subscriber が, セキュアな Session をつうじて Attacker のウェブサイトに接続する場合に発生する Attack であり, 加入者が無意識のうちに望まないアクションを RP 上で実行してしまうことになる.

例えば, もし銀行のサイトが CSRF に対して脆弱である場合, 単にユーザが Web メールの本文中の悪意のあるリンクを参照するだけで, 別のブラウザウィンドウで銀行への接続が開かれ, 加入者が意図せず大きな金額の資金移動を Authorize してしまう可能性がある.

Cross-site Scripting (XSS)

Attacker が, 不正なコードを他の無害なページに対して注入することを許してしまう脆弱性. これらのスクリプトはターゲットのウェブサイトで生成されるスクリプトの権限で動作し, ウェブサイトとクライアント間でのデータ転送の Confidentiality (機密性) や Integrity (完全性) を侵害する. ウェブサイトは, ユーザが入力するデータをリクエストやフォームから受け取り, サニタイズを施して実行不可能にすることなく表示してしまう場合に脆弱である.

Cryptographic Authenticator

Cryptographic Key をシークレットとする Authenticator.

Cryptographic Key

復号, 暗号化, 署名生成, 署名検証等の暗号論的オペレーションを管理するために用いられる値. 本ガイドライン群では, NIST SP 800-57 Part 1 の Table 2 で述べられた最低限の要件を満たすものとする.

Asymmetric Keys および Symmetric Key も参照のこと.

Cryptographic Module

一式のハードウェア, ソフトウェア, およびファームウェアで, (暗号アルゴリズムや鍵生成を含む) 承認されたセキュリティ機能を実装するもの.

Data Integrity

Authorize されていないエンティティによってデータが変更されることがないというプロパティー.

Derived Credential

事前に発行済の Credential に紐づいた Authenticator を所有・管理していることを証明することで発行される Credential. このような Credential を発行することで, 再び Identity Proofing プロセスを繰り返す必要がなくなる.

Digital Authentication

情報システムに対して, 電子的に表現されたユーザーの Identity の確からしさを確立するプロセス. SP 800-63 の前エディションまでは *Electronic Authentication* と呼ばれていたもの.

Digital Signature

Private Key を用いてデータにデジタル署名を行い, Public Key を用いて署名検証を行う, Asymmetric Key を用いたオペレーション. Digital Signature は Authenticity Protection (真正性保護), Integrity Protection (完全性保護), Non-repudiation (否認防止) を提供するが, Confidentiality Protection (機密性保護) は提供しない.

Diversionary

KBV において, 多項選択式問題の全選択肢がまちがいであり, Applicant に “none of the above” といった選択肢を選択するよう要求するもの.

Eavesdropping Attack

Authentication Protocol を受動的に傾聴し, 情報を傍受する Attack. 傍受した情報は, 後続の Claimant に成りすました Active Attack で利用される.

Electronic Authentication (E-Authentication)

Digital Authentication 参照.

Enrollment

Applicant が CSP の Subscriber となるべく申し込み, CSP が Applicant の Identity を検証するプロセス.

Entropy

Attacker がシークレット値を決定することに対峙する際の不確実性の量の尺度. Entropy は通常ビットで表現される. *n* ビットの Entropy を持つ値は, *n* ビットの一様乱数と同等の不確実性を持つ.

Federal Information Processing Standard (FIPS)

Secretary of Commerce は, Information Technology Management Reform Act (Public Law 104-106) に基づいて, National Institute of Standards and Technology (NIST) により連邦政府機関のコンピュータシステムに適用するために開発された標準及びガイドラインを承認する. これらの標準及びガイドラインは NIST によって FIPS として発行されたものであり, 政府機関で横断的に使われるものである. NIST はセキュリティや相互運用性といった強制力のある連邦政府の要求事項がある場合や, 許容可能な業界標準やソリューションが存在しない場合に, FIPS を開発する. 詳細については背景を参照すること.

FIPS ドキュメントは FIPS ホームページ http://www.nist.gov/itl/fips.cfm (http://www.nist.gov/itl/fips.cfm) からオンラインアクセス可能である.

Federation

一連のネットワークシステム間で Identity および Authentication 情報の伝搬を行うためのプロセス.

Federation Assurance Level (FAL)

Federation において Authentication 情報および (場合によっては) Attribute 情報を RP に送る際に用いられる Assertion Protocol のカテゴリー.

Federation Proxy

IdP に対して論理的に RP として動作し, RP に対して論理的に IdP として動作する, 2つのシステムを Bridge するコンポーネント. “Broker” と呼ばれることもある.

Front-Channel Communication

ブラウザ等を媒介とし, 2つのシステム間でリダイレクトを用いて行われるコミュニケーション. これは通常メッセージ受信者がホストする URL に HTTP Query Parameter を付与することで実現される.

Hash Function

任意長の短いの文字列を固定長の文字列に変換する関数. 承認されている Hash Function は以下のプロパティーを満たす.

1. 一方向性 - 指定された出力結果から対応する入力を特定することが計算上困難であり
1. 衝突困難性 - 同じ出力となる任意の2つの異なる入力を特定することが計算上困難である.

Identity

特定のコンテキストにおいて, ある Subject を他と区別できるかたちで表現する, Attribute ないしは Attribute の集合.

Identity Assurance Level (IAL)

Applicant の Claimed Identity が本人の本物の Identity であることの確からしさの度合いをあらわすカテゴリー.

Identity Evidence

Applicant が Claimed Identity を裏付ける為に提出する情報ないしはドキュメント. Identity Evidence は物理的存在 (e.g. 免許証) なこともあればデジタルな存在 (e.g. CSP が Applicant を Authenticate した上で発行した Assertion) なこともある.

Identity Proofing

CSP が Credential 発行のためにある人物に関する情報を収集, 確認, および検証するプロセス.

Identity Provider (IdP)

Subscriber のプライマリーな Authentication Credentials を管理し, Assertion を発行する主体. 本ドキュメント群においては, CSP とも呼ばれる.

Issuing Source

Identity Evidence として利用可能なデータや Assertion などのデジタルなエビデンス, 物理的ドキュメント等を責任を持って生成するオーソリティー.

Kerberos

MIT で開発された, 幅広く利用されている Authentication Protocol. “classic” な Kerberos では, ユーザは秘密のパスワードを Key Distribution Center (KDC) に共有する. ユーザ Alice は他のユーザ Bob と通信するため KDC に対して Authenticate し, KDC は “ticket” を発行する. 当該チケットは Alice が Bob に対して Authenticate する為に利用する.

詳細は SP 800-63C (sp800-63c.html) Section 11.2 を参照のこと.

Knowledge-Based Verification (KBV)

当該個人の Claimed Identity と関連づけられているプライベートな情報を知っていることを根拠とした Identity 検証方法. Knowledge-Based Authentication (KBA) や Knowledge-Based Proofing (KBP) とも呼ばれる.

Man-in-the-Middle Attack (MitM)

Attacker が通信を行う2つの主体の間に介在し, 両者の間を行き交うデータを傍受したり改ざんしたりする Attack. Authentication のコンテキストでは Attacker は Claimant と Verifier の間に介在し, Enrollment のコンテキストでは Registrant と CSP の間, Authenticator 紐付けのコンテキストでは Subscriber と CSP の間に介在することとなる.

Memorized Secret

Subscriber に記憶されることを前提とした, 文字列からなる Authenticator. Subscriber が Authentication プロセスにおいて *something they know* を立証するために利用できる.

Message Authentication Code (MAC)

暗号理論に基づくデータのチェックサムであり, Synmmetric Key を用いてデータの予期していない変更及び意図的な変更との両方を検知するために用いられる. MAC は Authenticity (真正性) と Integrity (完全性) の保護を行うが, Non-repudiation (否認防止) は行わない.

Mobile Code

実行コードであり, 通常は提供元から別のコンピューターシステムに転送されたのち実行されるもの. 転送は Network を介す (e.g., Web ページに埋め込まれた JavaScript) が, 物理的なメディアを介して転送されることもある.

Multi-Factor

2つ以上の Authentication Factor を要求する Authentication システムや Authenticator の特徴. MFA には, 2つ以上の要素を提供する単一の Authenticator を用いてもよいし, 互いに異なる要素を提供する複数の Authenticator を組み合わせて用いてもよい.

Authentication Factor としては, Something You Know, Something You Have, Something You Are の3種類がある.

Multi-Factor Authentication (MFA)

2つ以上の Authentication Factor を要求する Authentication システム. Multi-Factor Authentication は単一の Multi-Factor Authenticator を用いて実現してもよいし, 互いに異なる要素を提供する複数の Authenticator を組み合わせて用いてもよい.

Authentication Factor としては, Something You Know, Something You Have, Something You Are の3種類がある.

Multi-Factor Authenticator

2つ以上の Authentication Factor を提供する Authenticator. デバイスをアクティベートする為の Biometric センサーを持った暗号論的 Authentication デバイスなど.

Network

オープンなコミュニケーションの伝達手段. Internet がその代表例である. Network は Claimant とその他の主体の間でメッセージを伝達するために用いられる. 特に明示されない限り, Network のセキュリティは前提とされず, オープンであり, 任意の主体 (e.g., Claimant, Verifier, CSP および RP) 間の任意の点において Active Attack (e.g., なりすまし, Man-in-the-Middle, Session Hijacking) や Passive Attack (e.g., 盗聴) にさらされうるものと想定される.

Nonce

セキュリティプロトコル中で利用され, 同じキーによる繰り返しを許さない値. 例えば, Nonce は Challenge-Response Authentication Protocol のチャレンジとして利用され, Authentication キーが変更されるまでの間繰り返されないものとする (SHALL NOT). さもなければ Replay Attack の可能性がある. Nonce をチャレンジとして利用することと, チャレンジをランダムにすることとは異なる要件である. Nonce は必ずしも予測不可能である必要性はない.

Offline Attack

Attacker が何らかの情報を得る (典型的には Authentication Protocol 中のやりとりを盗聴したり, システムに侵入してセキュリティファイルを盗む) ことで, 対象となるシステムを解析する Attack.

Online Attack

Authentication Protocol において, 正当な Verifier に対して Claimant のふりをしたり, または能動的に Authentication チャネルを改ざんする Attack.

Online Guessing Attack

Attacker が Authenticator Output の取りうる値を推測してログオン試行を繰り返す Attack.

Pairwise Pseudonymous Identifier

CSP が特定の RP に対して生成する, opaque で推測不可能な Subscriber の識別子. この識別子は特定の CSP-RP ペア以外には知られることはなく, 当該ペア間でのみ用いられる.

Passive Attack

Authentication Protocol に対する Attack. Claimant と Verifier との間を Network を介してやり取りされるデータを傍受するが, データは改ざんしない (例. 盗聴).

Passphrase

Passphrase は Claimant が自身の Identity を Authenticate する際に利用する, 単語列や文字列からなる Memoized Secret. Passphrase は Password と似ているが, 一般的には Password より長くセキュリティー的にも強固である.

Password

Memoized Secret 参照.

Personal Data

Personally Identifiable Information 参照.

Personal Identification Number (PIN)

通常10進数の数値のみで構成された Memoized Secret.

Personal Information

Personally Identifiable Information 参照.

Personally Identifiable Information (PII)

OMB Circular A-130 で定義されているように, Personally Identifiable Information とは個人の Identity を識別したり追跡するために用いられる情報である. 単体の情報で個人を識別・追跡可能なものもあれば, 特定の個人に紐付け済もしくは紐付け可能なその他の情報と組み合わせることで識別・追跡可能となるものもある.

Pharming

DNS (Domain Name System) のようなインフラストラクチャサービスを汚染する手法により, Subscriber を偽の Verifier/RP へ誘導し, 機微情報を入力させる, 有害なソフトウェアをダウンロードさせる, 詐欺活動に加担させるような Attack.

Phishing

Subscriber を (主に Email を通じて) 偽の Verifier/RP に誘導し, 本物の Verifier/RP に対して Subscriber になりすますための情報を騙し取る Attack.

Possession and Control of an Authenticator

Authenticator Protocol において, Authenticator をアクティベートし利用する能力.

Practice Statement

Authentication プロセスの当事者 (e.g., CSP, Verifier) が従う実践的な内容を正式に記載した文書. 通常, 当事者のポリシーと実行内容が記述されており, 法的拘束力を持つ可能性がある.

Private Credentials

Authenticator へのセキュリティー侵害につながるため, CSP によって開示されることがない Credential.

Private Key

Asymmetric Key ペアの秘密鍵. データへのデジタル署名や復号に用いられる.

Presentation Attack

Biometric システムの運用妨害を目的とした Biometric データ読み取りサブシステムへの提示.

Presentation Attack Detection (PAD)

Presentation Attack の自動検知. Presentation Attack Detection 手法のサブセットである *liveness detection* では, 解剖学的特徴または非自発的または自発的反応の測定および分析を行い, Biometric サンプルが生体の Subject から直接読み取られたものかどうかを判定する.

Protected Session

2者間でやりとりされるメッセージを, Session Key と呼ばれる Shared Secret を用いて暗号化し, Integrity を保護する Session.

当該 Session 内で, ある主体が Session Key に加えて1つ以上の Authenticator を所有していることを証明し, もう一方の主体が当該 Authenticator に紐づく Identity を検証できる場合, 当該主体は *Authenticated* であると言う. もし両主体が共に Authenticated となる場合, この Protected Session は *Mutually Authenticated* であると言える.

Protected Session

Authenticate され保護されたチャネルで確立された Session.

Pseudonym

実名 (Legal Name) 以外の名前.

Pseudonymity

Subject の識別に Pseudonym を用いること.

Pseudonymous Identifier

RP による Subscriber に関するいかなる推測をも許さず, かつ RP が複数のインタラクションに渡って Subscriber の Claimed Identity を紐づけられるような, 意味のないユニークな識別子.

Public Credentials

セキュリティー侵害を伴わず Authenticator との紐付けを表せる Credential.

Public Key

Asymmetric Key ペアの公開鍵. データへの署名検証や暗号化に用いられる.

Public Key Certificate

Certificate Authority によって発行され, Certificate Authority の秘密鍵でデジタル署名された電子文書. Public Key Certificate により Subscriber の識別子が Public Key と紐づけられる. 当該 Certificate により識別される Subscriber のみが Private Key の管理および Access を持っていることが暗示される. [RFC 5280] (sp800-63b.ja.html#RFC5280) も参照のこと.

Public Key Infrastructure (PKI)

Certificate と Public-Private Key Pair を管理する目的で利用される, 一連のポリシー, プロセス, サーバープラットフォーム, ソフトウェア, ワークステーションなど. Public Key Certificate の発行, 管理, 失効を行う能力を備える.

Reauthentication

ある Session において, Subscriber が継続してその場に存在し Authenticate する意思を持っていることを確認するプロセス.

Registration

Enrollment 参照.

Relying Party (RP)

Subscriber の Authenticator および Credential, Verifier の Claimant Identity に関する Assertion を信頼して, Transaction を処理したり情報やシステムへの Access を許可したりする主体.

Remote

(*Remote Authentication* や *Remote Transaction* といったコンテキストで) 単一組織によるセキュリティ対策のみでは End-to-End での確実な保護が期待できないような状況下での, Network 接続されたデバイス間の情報交換.

Replay Attack

Attacker が事前に記録しておいた (正当な Claimant と Verifier との間の) メッセージを, Verifier に対して Claimant になりすまして, もしくはその逆方向に, 再送する Attack.

Replay Resistance

Replay Attack 耐性のある Authentication プロセスのプロパティ. 典型的には, 特定の Authentication にのみ有効な Authenticator Output により実現される.

Restricted

誤認発生時に追加のリスクが発生するため, 追加要件を要求されるような Authenticator Type, クラス, インスタンス.

Risk Assessment

システムの運用に起因する, 組織の運営 (ミッション, 機能, イメージ, レピュテーションを含む), 組織の資産, 個人および他組織に対するリスクを, 特定, 推定, 優先順位付けするプロセス. Risk Assessment は Risk Management の一部であり, 脅威・脆弱性解析を包含し, 計画済もしくは実施中のセキュリティー管理で施される対策について考察するプロセスである. Risk Analysis と同義.

Risk Management

組織の運営 (ミッション, 機能, イメージ, レピュテーションを含む), 組織の資産, 個人および他組織に対する情報セキュリティーリスクを管理するプログラムや補助的プロセス. (i) リスクに関係するアクティビティーを見極め, (ii) リスクを評価し, (iii) ひとたびリスクが特定されればそれに対応し, (iv) 継続的にリスクをモニタリングする, という一連の行動を含む.

Salt

暗号プロセスにおいて用いられる秘密でない (non-secret) 値で, 通常ある特定の計算結果が Attacker によって再利用されないことを保証するために用いられる.

Secure Sockets Layer (SSL)

Transport Layer Security (TLS) 参照.

Session

Subscriber と RP ないしは CSP のエンドポイントの間の継続的インタラクション. Session は Authentication イベントにより開始され, Session 終了イベントで終了する. Session は Session シークレットにより紐づけられる. Session シークレットは Subscriber のソフトウェア (Browser, アプリケーション, OS) が RP や CSP に Subscriber の Authentication Credential の代わりとして提示することができる値

である.

Session Hijack Attack

Claimant と Verifier の間の Authentication のやりとりが成功したのち, Attacker が Claimant と Verifier の間に入り込む攻撃. Attacker は Verifier に対して Subscriber のふりをしたり, Subscriber に対して Verifier のふりをしたりして, Session 中のデータ交換をコントロールする. Claimant と RP の間の Session も同様に侵害されうる.

Shared Secret

Subscriber と Verifier が知っている, Authentication で使われるシークレット.

Side-Channel Attack

物理的な暗号システムからの情報漏洩によって可能となる Attack. Side-Channel Attack においては, タイミング, 消費電力, 電磁波放出, 及び音響放射といった特性が利用される.

Single-Factor

単一の Authentication Factor (something you know, something you have, or something you are) を要求する Authentication システムや Authenticator の特徴.

Social Engineering

人を欺いてセンシティブな情報を露呈させたり, Unauthorized Access を得たり, 人と付き合いながら信頼を獲得した上で詐欺を行う活動.

Special Publication (SP)

NIST が発行する出版物の一形態. 特に SP 800 シリーズは, Information Technology Laboratory による研究活動, ガイドライン, コンピューターセキュリティ分野における公共福祉のための支援活動, 民間・政府・学術組織との協調的な活動などに関するレポートとなっている.

Subject

人間, 組織, デバイス, ハードウェア, ネットワーク, ソフトウェア, サービスなど.

Subscriber

CSP から Credential や Authenticator を受け取る主体.

Symmetric Key

暗号化と復号, Message Authentication Code の生成と検証などの, 対となる暗号論的オペレーションの両方で用いられる暗号論的な鍵.

Token

Authenticator 参照.

Token Authenticator

Authenticator Output 参照.

Token Secret

Authenticator Secret 参照.

Transaction

ビジネスやプログラムの目標を支援する, ユーザーとシステムの間の個別のイベント. 政府のデジタルシステムにおいては, デジタル Identity の Risk Assessment において個別の分析が必要な, 複数のカテゴリーないしはタイプの Transaction がある.

Transport Layer Security (TLS)

ブラウザやウェブサーバに広く実装されている Authentication およびセキュリティプロトコル. TLSは [RFC 5246] で定義されている. TLS はより古い SSL プロトコルと似ており, 実質的に TLS1.0 は SSL version 3.1 といえる. [SP 800-52] (Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations) では, 政府のアプリケーションにおいてどのように TLS を用いるかを定めている.

Trust Anchor

ハードウェアやソフトウェエアに直接埋め込まれていたり, Out-of-band な手法によりセキュアに提供されたりすることで Trust される, Public Key もしくは Symmetric Key. 他の信頼できる主体の保証を受けて Trust を得るものは Trust Anchor とは呼ばない (Public Key Certificate 等). Trust Anchor はそのスコープを制限するような名称やポリシー制約を持つこともある.

Usability

ISO/IEC 9241-11 によると, 特定のユーザが特定の利用コンテキストにおいて, 効果的, 効率的かつ十分に特定の目的を果たすためにプロダクトを利用しうる度合い.

Verifier

Authentication Protocol を利用して, Claimant が1つまたは2つの Authenticator を 所有, 管理していることを検証し, Claimant の Identity を検証する主体. Verifier は上記の目的のため, Authenticator と Identity を紐付ける Credential を確認し, そのステータスをチェックする必要がある場合もある.

Verifier Impersonation

通常は正規の Verifier に対して Subscriber になりすますために使える情報を詐取することを目的とし, Authentication Protocol において Attacker が Verifier になりすますようなシナリオ. 以前の SP 800-63 では Verifier Impersonation 耐性を持つ Authentication Protocol は “strongly MitM resistant” であると記述されていた.

Virtual In-Person Proofing

Remote の Identity Proofing プロセスのうち, 物理的・技術的・手続き上の手段により Remote Session であっても物理的に対面 (In-person) の Identity Proofing プロセスと同等であると考えられるもの.

Weakly Bound Credentials

Credential を無効化することなく変更可能な方法で, Subscriber と結びつけられた Credentials.

Zeroize

データを破壊し復元できないようにするために, ゼロ値のビットだけで構成されるデータによってメモリを上書きすること. これはしばしばデータそのものを破壊するのではなく, ファイルシステム上のデータへの参照を破壊するだけの削除手法と対比される.

Zero-Knowledge Password Protocol

Claimant が Verifier に対して Authenticate を行う際, Verifier に対して Password を提示する必要がないような Password ベースの Authentication Protocol. 例としては EKE, SPEKE, SRP などが挙げられる.

A.2 Abbreviations

本ガイドライン群で選択されている略語を以下に定義する.

Abbreviation	**Term**
ABAC	Attribute Based Access Control
AAL	Authenticator Assurance Level
AS	Authentication Server
CAPTCHA	Completely Automated Public Turing test to tell Computer and Humans Apart
CSP	Credential Service Provider
CSRF	Cross-site Request Forgery

Abbreviation	Term
XSS	Cross-site Scripting
DNS	Domain Name System
EO	Executive Order
FACT Act	Fair and Accurate Credit Transaction Act of 2003
FAL	Federation Assurance Level
FEDRAMP	Federal Risk and Authorization Management Program
FMR	False Match Rate
FNMR	False Non-Match Rate
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
IAL	Identity Assurance Level
IM	Identity Manager
IdP	Identity Provider
IoT	Internet of Things
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
JOSE	JSON Object Signing and Encryption
JSON	JavaScript Object Notation
JWT	JSON Web Token
KBA	Knowledge-Based Authentication
KBV	Knowledge-Based Verification
KDC	Key Distribution Center
LOA	Level of Assurance
MAC	Message Authentication Code
MitM	Man-in-the-Middle
MitMA	Man-in-the-Middle Attack
MFA	Multi-Factor Authentication
N/A	Not Applicable
NARA	National Archives and Records Administration
OMB	Office of Management and Budget
OTP	One-Time Password
PAD	Presentation Attack Detection
PHI	Personal Health Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure

Abbreviation	Term
PL	Public Law
PSTN	Public Switched Telephone Network
RA	Registration Authority
RMF	Risk Management Framework
RP	Relying Party
SA&A	Security Authorization & Accreditation
SAML	Security Assertion Markup Language
SAOP	Senior Agency Official for Privacy
SSL	Secure Sockets Layer
SMS	Short Message Service
SP	Special Publication
SORN	System of Records Notice
TEE	Trusted Execution Environment
TGS	Ticket Granting Server
TGT	Ticket Granting Ticket
TLS	Transport Layer Security
TPM	Trusted Platform Module
VOIP	Voice-over-IP

Privacy Policy (http://www.nist.gov/public_affairs/privacy.cfm#privpolicy) | Security Notice (http://www.nist.gov/public_affairs/privacy.cfm#secnot) | Accessibility Statement (http://www.nist.gov/public_affairs/privacy.cfm#accesstate) | Send feedback (https://github.com/usnistgov/800-63-3/issues/) (/800-63-3/comment_help.html)