Thu, 26 Oct 2017 14:16:51 +0000

NIST Special Publication 800-63A

Digital Identity Guidelines (翻訳版)

Enrollment and Identity Proofing Requirements

Paul A. Grassi
James L. Fenton

Privacy Authors:
Naomi B. Lefkovitz
Jamie M. Danker

Usability Authors:
Yee-Yin Choong
Kristen K. Greene
Mary F. Theofanos

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

COMPUTER SECURITY

NIST Special Publication 800-63A

Digital Identity Guidelines

Enrollment and Identity Proofing Requirements

Paul A. Grassi
Applied Cybersecurity Division
Information Technology Laboratory

Privacy Authors:
Naomi B. Lefkovitz
Applied Cybersecurity Division
Information Technology Laboratory

Jamie M. Danker
National Protection and Programs Directorate
Department of Homeland Security

James L. Fenton
Altmode Networks
Los Altos, CA

Usability Authors:
Yee-Yin Choong
Kristen K. Greene
Information Access Division
Information Technology Laboratory

Mary F. Theofanos
Office of Data and Informatics
Material Measurement Laboratory

翻訳者:
Nov Matake
YAuth.jp LLC

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

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 information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

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

National Institute of Standards and Technology Special Publication 800-63-3
Natl. Inst. Stand. Technol. Spec. Publ. 800-63A, 45 pages (June 2017)
CODEN: NSPUE2

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

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)

Reports on Computer Systems Technology

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

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. This guideline focuses on the enrollment and verification of an identity for use in digital authentication. Central to this is a process known as *identity proofing* in which an applicant provides evidence to a credential service provider (CSP) reliably identifying themselves, thereby allowing the CSP to assert that identification at a useful identity assurance level. This document defines technical requirements for each of three identity assurance levels. This publication supersedes corresponding sections of NIST Special Publication (SP) 800-63-2.

Keywords

authentication; credential service provider; electronic authentication; digital authentication; electronic credentials; digital credentials; identity proofing; federation.

Acknowledgements

The authors would like to acknowledge the contributions and guidance of our international peers, including Adam Cooper, Alastair Treharne, and Julian White from the Cabinet Office, United Kingdom, and Tim Bouma from the Treasury Board of Canada Secretariat, Government of Canada, Kaitlin Boeckl for her artistic 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), Ben Piccarreta and Ellen Nadeau from NIST, and Danna Gabel O'Rourke from Deloitte & Touche LLP. In addition, special thanks to the Federal Privacy Council's Digital Authentication Task Force for the contributions to the development of privacy requirements and considerations.

The authors would also 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 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.

Table of Contents

1 Purpose

This section is informative.

本ドキュメントでは, 各 Identity Assurance Level (IAL) ごとに, リソースへの Access を希望する Applicant に対する, Enrollment および Identity Proofing に関する要件をまとめる. 要件は, Subscriber が自身の Identity を主張する際に提示する Identity Evidence の受け入れ可能性, 妥当性確認, 検証のそれぞれに関して詳細化されている. さらに本ドキュメントは, Enrollment レコードの作成と保守, および Authenticator (CSP が発行したものも Subscriber が提供したものも) と Enrollment レコードの紐付けに関して, Credential Service Providers (CSP) の責任を明確化する.

2 Introduction

This section is informative.

Digital Identity に関する課題の1つに, 一連のオンラインアクションを単一の特定の主体と関連付けることがある. こういった関連付けが不要であったり望ましくない (e.g., Anonymity (匿名性) や Pseudonymity (仮名性) が求められる) シチュエーションもあるが, 現実世界の Subject との関係性を確実に確立するために重要となるシチュエーションもある. ヘルスケア情報を取得したり金融取引を実行するといったシチュエーションは, その良い例である. また何らかの規制 (e.g., USA PATRIOT Act of 2001 により確立された金融業界の 'Know Your Customer' 要件) や, ハイリスクなアクション (e.g., ダムの放水率を変える) に対する説明責任の確立のために, そういった関連付けが必須となるシチュエーションもある.

Replying Party (RP) が Transaction を実行する Subscriber に関して何らかを知っているが, 現実世界の Identity については知らないという状況が望ましい場合もある. 例えば, 国勢調査や選出された公務員への嘆願のためには, Subscriber の自宅の郵便番号のみを知っている状態が望ましいかもしれない. どちらのケースでも, サービス提供のためには郵便番号がわかれば十分であり, 当該人間の見えない Identity を知ることは必要でないし望ましくもない.

下表は, 本ドキュメント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. Identity Assurance Level Requirements	Normative
5. Identity Resolution, Validation, and Verification	Normative
6. Derived Credentials	Normative
7. Threats and Security Considerations	Informative
8. Privacy Considerations	Informative
9. Usability Considerations	Informative
10. References	Informative

2.1 Expected Outcomes of Identity Proofing

Subject に対して Identity Proofing を行う際には, 以下のようなことが期待される.

- Claimed Identity を, CSP がサービスを提供するユーザー集団のコンテキストにおいて, 単一かつユニークな Identity に帰着させる.
- 提供された全てのエビデンスが正しく本物である (e.g., 偽造・悪用されていない) ことを確認する.
- Claimed Identity が現実世界に存在することを確認する.
- Claimed Identity が Identity Evidence を提示した現実世界の人間と関連づいていることを検証する.

2.2 Identity Assurance Levels

Subscriber の Identity に関する Assurance は以下の3つの IAL を利用して記述される.

IAL1: Applicant を現実世界の特定の Identity 紐づける必要はない. Subject の行動に関連して提供される Attribute は, Self-asserted であるか, Self-asserted として扱われるべきである (CSP が RP に対して Assert する Attribute を含む). Self-asserted Attribute は確認も検証もされない.

IAL2: エビデンスにより, Claimed Identity が現実世界に存在することを示す材料とし, Applicant が現実世界の当該 Identity と適切に関連づけられていることを証明する. IAL2 では Remote ないしは対面での Identity Proofing が必要となる. Attribute は RP に対して CSP によって Assert されることもあり, Pseudonymous Identity が検証済 Attribute を持つこともサポートされる. IAL2 をサポートする CSP は, ユーザーの同意があれば IAL1 の Transaction をサポートしてもよい.

IAL3: 対面での Identity Proofing が必要である. 識別に用いる Attribute は Authorized かつ訓練を受けた CSP の代理人によって検証される必要がある. IAL2 と同様, Attribute は RP に対して CSP によって Assert されることもあり, Pseudonymous Identity が検証済 Attribute を持つこともサポートされる. IAL3 をサポートする CSP は, ユーザーの同意があれば IAL1 および IAL2 の Transaction をサポートしてもよい.

IAL2 と IAL3 では, CSP から RP に送信する Attribute の数やその提示方法を制限することで, Federated 環境での Pseudonymity が実現可能である. 例えば, RP が正確な誕生日のみを必要とし, その他の個人の詳細については知らなくて良い時, RP は CSP に Subscriber の誕生日のみを要求すべきである. また可能であれば, RP は CSP に Attribute Reference を要求すべきである. 例えば, RP が Subscriber が18歳以上かどうか知る必要がある場合, RP は完全な誕生日ではなく真偽値のみを要求すべきである. 逆に言えば, より低い Assurance Level の Transaction によいて, より高い Assurance を持つ CSP を利用することは, ユーザーにとって有益たりうる. 例えば, ユーザーは IAL3 の Identity を管理し, その CSP を IAL2 や IAL1 の Transaction においても利用できるべきである.

当該個人は Enrollment 時に Identity Proofing プロセスを経るであろうから, CSP との個別のインタラクションに関する Transaction は必ずしも Pseudonymous とは限らない.

各 IAL の詳細な要件は Section 4 および Section 5 で述べる.

3 Definitions and Abbreviations

用語定義および略語については, 全て SP 800-63 (sp800-63-3.html) Appendix A を参照のこと.

4 Identity Assurance Level Requirements

This section contains both normative and informative material.

本ドキュメントは, Applicant に対する Identity Proofing および Enrollment プロセスによって, Identity Evidence と Attribute の収集が行われ, ある集団ないしはコンテキストの中でユニークかつ単一の Identity として識別可能になり, 確認および検証が行われるまでの, 共通のパターンについて記述する. 最適な IAL の選択については SP 800-63-3 (sp800-63-3.html) Section 6.1 を参照のこと. CSP はこういった Attribute を Authenticator に紐づけるかもしれない (SP 800-63B (sp800-63b.html) 参照).

Identity Proofing の唯一の目的は, あらかじめ定められた確実性でもって, Applicant が彼ら自身が主張するものであることを保証することである. このプロセスにおいては, Identity Proofing を達成するために必要最小限の Attribute の提示, 確認, 検証が行われる. 必要最小限といっても多様な組み合わせがあり得るため, CSP はプライバシーとユーザーが必要とするユーザビリティーのバランスを取りつつ, および将来 Digital Identity を利用する際に必要となるであろう Attribute を考慮した上で, 必要最小限の組み合わせを選択するべきである. 例えば, 必要最小限な Attribute の例として, 以下のような組み合わせが考えられる.

1. Full name
2. Date of birth
3. Home address

また本ドキュメントは, Identity Proofing 以外の目的で利用される追加情報を収集する際の CSP に対する要件も示している.

4.1 Process Flow

This section is normative.

Figure 4-1 は Identity Proofing および Enrollment の基本的な流れを概観したものである.

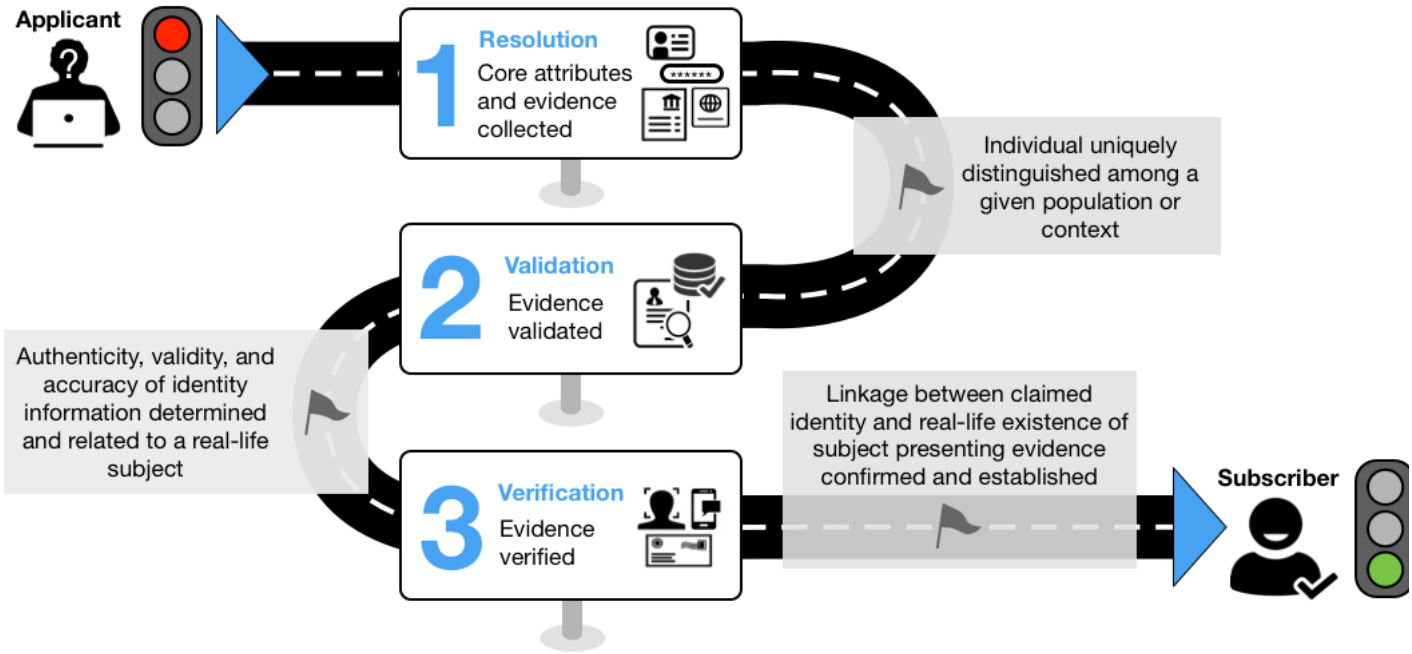

Figure 4-1 The Identity Proofing User Journey

以下では, Identity Proofing プロセス中において CSP と Applicant がどのようにインタラクションを行うかを例示する.

1. **Resolution**
   a. CSP が Applicant から名前, 住所, 誕生日, Email, 電話番号などの PII を収集する.
   b. さらに CSP は, 運転免許証とパスポートなど, 2種類の Identity Evidence を収集する. 例えば CSP は, ラップトップのカメラを使って, 両 Identity Evidence の裏表の写真をキャプチャーすることができる.
2. **Validation**
   a. CSP は Authoritative Source に照会を行い 1a で提供された情報を確認する. CSP は Applicant が提出した情報が彼らのレコードとマッチすることを確認する.
   b. CSP は免許証とパスポートの画像をチェックし, 修正などされておらず, QR コードにエンコードされているデータが平文の情報とマッチし, 識別番号が標準フォーマットに従っていることを確認する.
   c. CSP は免許証とパスポートの Issuing Source に照会をかけ, 情報がマッチすることを確認する.
3. **Verification**
   a. CSP は Applicant に免許書とパスポートにマッチする彼ら自身の写真を要求する.
   b. CSP は免許書とパスポートにある写真を Applicant の写真と比較し, 両者がマッチすることを確認する.

c. CSP は Enrollment コードを Applicant の確認済電話番号に送信し, ユーザーはその Enrollment コードを CSP に提示する. CSP は両者がマッチすることを確認し, 当該ユーザーが検証済電話番号を管理下においていることを検証する.
d. Applicant は Proofing に成功する.

> Note: Identity Proofing プロセスは複数のサービスプロバイダーによって行われうる. 単一の組織やプロセス, テクニックやテクノロジーがこのプロセスの各ステップを実行することが可能であるが, そのような想定をするものではない.

4.2 General Requirements

IAL2 ないしは IAL3 で Identity Proofing を行う CSP には, 以下の要件が課せられる.

1. Identity Proofing は, サービスまたはメリットに Access するための適格性や資格を決定するために実施してはならない (SHALL NOT).
2. PII の収集は, Claimed Identity の存在確認, および Identity Resolution, Validation, Verification のために Identity Evidence を提示している Applicant と Claimed Identity との関連づけに必要最小限な程度に制限すること (SHALL). この PII には, Identity Evidence を Authoritative Source と関連づける Attribute や, RP が Authorization の決定を行うために利用する Attribute を含みうる (MAY).
3. CSP は, 収集時に Applicaint に明示的な通知を行い, Identity Proofing に必要な Attribute の収集・記録管理の目的を知らせなければならない (SHALL). これには, Identity Proofing プロセスを完了するためにどの Attribute が任意でありどの Attribute が必須であるかや, Attribute を提供しない場合の影響といった情報を含む.
4. CSP は, Identity Proofing プロセスにおいて収集・管理することとなった Attribute を, CSP が明確な通知を行い Subscriber からの同意を得た場合を除き, Identity Proofing, Authentication, Attribute Assertion, 法律や法的プロセスに従う以外の目的で利用してはならない (SHALL NOT). CSP はこういった追加の目的をサービス提供条件としてはならない (SHALL NOT).
5. CSP は, Identity Proofing を起因とする Applicant からの苦情や問題の是正のためのメカニズムを提供しなければならない (SHALL). また CSP は, そのメカニズムによって苦情や問題の解決が有効になされているか, 評価しなければならない (SHALL).
6. Identity Proofing と Enrollmet プロセスは, 適用可能な書面によるポリシー, または Identity を検証するための特定の手続きを規定する *practice statement* に従って行うこととする (SHALL). *practice statement* は, CSP がどのように Applicant の登録失敗につながるような Proofing エラーを取り扱うかを詳説する制御情報を含むこと (SHALL). これには例えば, 許容されるリトライ回数, 代替の Proofing 方法 (e.g., Remote が失敗した場合は対面), 異常検知時の不正対策などが含まれる.
7. CSP は, 監査ログを含む Applicant の Identity を検証する際のすべての手続きの記録を管理するものとし (SHALL), Proofing プロセスにおいて提示された Identity Evidence のタイプを記録するものとする (SHALL). CSL は, プライバシーおよびセキュリティーに関する Risk Assessment を含む Risk Management プロセスを実施し, 以下の項目を定めること.
    a. ここで指定された必須要件を超えて, Applicant の Identity を検証するために必要なステップ.
    b. Biometrics, 画像, スキャン, その他 Identity Evidence のコピーを含む PII. CSP はこれらを Identity Proofing の記録として管理することになる. (Note: 特別な連邦政府要件が課せられることもある)
    c. これらの記録の保持スケジュール. (Note: CSP には, 適用可能な National Archives and Records Administration (NARA) 記録保持スケジュールを含む, 適用可能な法律, 規則, ポリシーに従って, 特定の保持ポリシーが課せられることもある)
8. Enrollmet プロセスにおいて収集されたすべての PII は, Confidentiality (機密性), Integrity (完全性), 情報源の帰属を保証するよう保護すること (SHALL).
9. 第三者が関与する Transaction を含み, Proofing Transaction 全体を Authenticated Protected Channel 上で実行すること (SHALL).
10. CSP は, 追加の対策がここで規定される必須要件に代わるものでない限り, 不正防止策 (e.g., ジオロケーションの検査, Applicant のデバイス特性の調査, 行動特性の評価, Death Master File [DMF] (sp800-63a.html#dmf) などのバイタル統計レポジトリーのチェック) を用いて Identity Proofing の信頼性を向上させるべきである (SHOULD). CSP が不正防止策を行う場合, CSP はこれらの防止策に関してプライバシー Risk Assessment を行うこと (SHALL). こういったアセスメントには, プライバシーリスク軽減策 (e.g., リスクの受容や転嫁, 制限付き保持, 使用制限, 通知), その他の技術的対策 (e.g., 暗号化), 上記 4.2(7) に記載された対策などが含まれる.
11. CSP が Identity Proogin および Enrollment プロセスを終える場合, CSP は PII は PII を含むセンシティブデータの完全な廃棄または破棄, または保持期間中の Unauthorized な Access からの保護を行う責任を持つ (SHALL).
12. CSP が政府機関か民間のプロバイダーかに関わらず, Proofing サービスを提供したり利用するには以下の要件が適用される.
    a. 機関は, Senior Agency Official for Privacy (SAOP) と協議し, Identity Proofing を実施するための PII 収集において Privacy Act 要件が適用されるかどうか判断するための分析を行うこと (SHALL).
    b. 機関は, 該当する場合は System of Records Notice (SORN) を公開し, そういった収集について記載すること.
    c. 機関は, SAOP と協議し, Identity Proofing を実施するための PII 収集において E-Government Act of 2002 要件が適用されるかどうか判断するための分析を行うこと (SHALL).
    d. 機関は, 該当する場合は Privacy Impact Assessment (PIA) を公開し, そういった収集について記載すること.
13. CSP は, Identity Resolution に必要でない限り, また Identity Resolution がその他の Attribute または Attribute の組み合わせによって実現不可能でない限り, Social Security Number (SSN) を収集すべきではない (SHOULD NOT).

4.3 Identity Assurance Level 1

This section is normative.

1. IAL1 のみをサポートする CSP は Attribute を確認したり検証してはならない (SHALL NOT).
2. CSP はサービス提供のために Applicant に0個以上の Self-asserted Attribute を要求してもよい (MAY).
3. IAL2 や IAL3 の CSP は, ユーザーの同意があれば, IAL1 を必要とする RP をサポートすべきである (SHOULD).

4.4 Identity Assurance Level 2

This section is normative.

IAL2 では **Remote** および **In-person** (対面) での Identity Proofing を許可している. IAL2 は, より多くのユーザーに選択され, フォルスネガティブ (Identity Proofing を通過できない正当な Applicant) を削減し, 悪意ある Applicant による不正な Identity の提示を可能な限り検出するため, 広範囲の受け入れ可能な Identity Proofing テクニックをサポートする.

CSP は Section 4.4.1 ないしは Section 4.4.2 の要件に従って Proofing を行わなければならない (SHALL). CSP は Section 4.4.1 に従って Identity Proofing を実装すべきである (SHOULD). CSP がサービスを提供する対象によっては, CSP は Section 4.4.2 に従って Identity Proofing を実装してもよい (MAY).

4.4.1 IAL2 Conventional Proofing Requirements

4.4.1.1 Resolution Requirements

PII の収集は, 所与のコンテキストにおいてある Identity をユニークに識別可能にするために必要最低限な範囲に限定すること (SHALL). これにはデータの照会の助けとなるような Attribute の収集を含んでも良い (MAY). 一般的な Resolution 要件は Section 5.1 を参照のこと.

4.4.1.2 Evidence Collection Requirements

CSP は以下を Applicant から収集すること (SHALL).

1. **もし** エビデンスの Issuing Source が, 発行時の Identity Proofing イベントにおいて, SUPERIOR あるいは STRONG なエビデンスを2つ以上利用して Claimed Identity の確認を行っており, **かつ** CSP が直接 Issuing Source との間でそのエビデンスを確認したのであれば, そのようなプロセスを経て発行された SUPERIOR ないしは STRONG なエビデンスを1つ. **もしくは**
2. STRONG なエビデンスを2つ. **もしくは**
3. STRONG なエビデンスを1つと FAIR なエビデンスを2つ.

受け入れ可能な Identity Evidence についての詳細は Section 5.2.1 Identity Evidence Quality Requirements を参照のこと.

4.4.1.3 Validation Requirements

CSP は Identity Evidence を以下のように確認すること (SHALL).

それぞれのエビデンスは, 提示されたエビデンスと同じ強度のプロセスによって確認すること (SHALL). 例えば2つの STRONG な Identity Evidence が提示された場合は, それぞれを STRONG な強度で確認することとなる.

Identity Evidence の確認についての詳細は Section 5.2.2 Validating Identity Evidence を参照のこと.

4.4.1.4 Verification Requirements

CSP は Identity Evidence を以下のように検証すること.

1. 最低限, Applicant と Identity Evidence の紐付けは, 強度 STRONG を達成できるプロセスによって検証しなければならない.
2. Knowledge-Based Verification (KBV) は対面 (物理的ないしは監視下における Remote) の Identity 検証のために利用してはならない (SHALL NOT).

Identity Evidence の検証についての詳細は Section 5.2.2 Validating Identity Evidence を参照のこと.

4.4.1.5 Presence Requirements

CSP は対面ないしは Remote での Identity Proofing をサポートすること (SHALL). CSP は両方を提供すべきである (SHOULD).

4.4.1.6 Address Confirmation

1. 有効な住所確認用のレコードは, Issuing Source ないしは Authoritative Source によるものでなければならない.
2. CSP は Address of Record を確認しなければならない (SHALL). CSP は, 提示された有効な Identity Evidence のいずれかに記載された住所の確認を通じて, Address of Record の確認を行うべきである (SHOULD). CSP は, Applicant が提供した, いかなる有効な Identity Evidence にも記載されていない情報の確認を通じて, Address of Record の確認を行ってもよい (MAY).
3. 記録時に未確認な Self-asserted の住所データは, 確認に用いてはならない (SHALL NOT).
4. **CSP が対面 での Proofing (物理的ないしは監視下における Remote) を行う場合は**

a. CSP は確認された Address of Record に対して Proofing の通知を送るべきである (SHOULD).
b. Subscriber と Authenticator の紐付けが後日発生する場合は, CSP は Enrollment コードを直接 Subscriber に提示してもよい (MAY).
c. Enrollment コードは最大7日間まで有効なものとする (SHALL).

5. **CSP が Remote の Proofing (非監視下) を行う場合**
   a. CSP は確認された Applicant の Address of Record に Enrollment コードを送信しなければならない (SHALL).
   b. Applicant は Identity Proofing プロセスを完了するために有効な Enrollment コードを提示しなければならない (SHALL)
   c. CSP はレコード中の確認済郵便住所に Enrollment コードを送信すべきである (SHOULD). CSP は, 確認済であれば, 携帯電話 (SMS ないしは音声), 固定電話, Email に Enrollment コードを送信してもよい (MAY).
   d. Enrollment コードが Authentication Factor としての用途も兼ねている場合は, 一度利用されたものはリセットすること (SHALL).
   e. 郵便住所に送信された Enrollment コードは最大10日間まで有効なものとする (SHALL). ただし郵送先住所が United States と地続きでない場所の場合, 例外的に30日間まで有効期間を延長してもよい (MAY). 電話で送信された Enrollment コードは最大10分間まで有効なものとする (SHALL). Email で送信された Enrollment コードは最大24時間まで有効なものとする (SHALL).
   f. CSP は, Enrollment コードと Proofing の通知を, それぞれ異なる Address of Record に送信するよう保証すること (SHALL). 例えば, もし CSP が Enrollment コードを確認済の電話番号に送ったとすれば, Proofing 通知は, 確認済の郵便住所や, 確認および検証済みの運転免許証のようなエビデンスに記載された郵便住所に送ることになろう.

> Note: 郵便住所は, Enrollment コードの通知を含む, Applicant との間のあらゆるコミュニケーションを行う手段として選好される. しかしながら, 本ガイドライン群は, 物理的であってもデジタルであっても, あらゆる確認済 Address of Record をサポートする.

4.4.1.7 Biometric Collection

CSP は Non-repudiation (否認防止) や Re-proofing を目的として Biometrics を収集してもよい (MAY). Biometrics 収集に関する詳細は SP 800-63B, Section 5.2.3 (sp800-63b.html#biometric_use) を参照のこと.

4.4.1.8 Security Controls

CSP は, SP 800-53 やそれに相当する連邦政府標準 (e.g., FEDRAMP) や業界標準に定められた, Moderate ないしは High 基準のセキュリティー制御策から, 制御強化を含み, 適切に調整されたセキュリティー制御策を採用しなければならない (SHALL). CSP は *moderate-impact* システムやそれに相当するものに対する Assurance 関連の最低限の制御策が実施されていることを保証しなければならない (SHALL).

4.4.2 IAL2 Trusted Referee Proofing Requirements

個人が Section 4.4.1 に規定された Identity Evidence 要件を満たすことができない場合, 機関は信頼できる身元保証人に Applicant の Identity Proofing を手伝わせてもよい (MAY).

4.5 Identity Assurance Level 3

This section is normative.

IAL3 では IAL2 よりさらに厳格であり, さらに強度の高いエビデンスの提供が求められると共に, なりすましや不正, その他の有害なダメージから当該 Identity および RP を保護する特定の追加プロセス (Biometrics の利用を含む) も求められることになる. Biometrics は, 不正な Enrollment や重複した Enrollment を検出するために利用され, Credential への紐付けを再確立する手段としても利用される. 加えて, IAL3 での Identity Proofing は対面 (監視下にある Remote を含む) で行われる. 詳細は Section 5.3.3 を参照のこと.

4.5.1 Resolution Requirements

PII の収集は, Identity をユニークに識別可能にするために必要最低限な範囲に限定すること (SHALL). これにはデータの照会の助けとなるような Attribute の収集を含んでも良い (MAY). 一般的な Resolution 要件は Section 5.1 を参照のこと.

4.5.2 Evidence Collection Requirements

CSP は以下を Applicant から収集すること (SHALL).

1. 2つの SUPERIOR なエビデンス. **もしくは**
2. **もし** STRONG なエビデンスの Issuing Source が, 発行時の Identity Proofing イベントにおいて, SUPERIOR あるいは STRONG なエビデンスを2つ以上利用して Claimed Identity の確認を行っており, **かつ** CSP が直接 Issuing Source との間でそのエビデンスを確認したのであれば, SUPERIOR なエビデンスとそのようなプロセスを経て発行された STRONG なエビデンスを1つずつ.
3. STRONG なエビデンスを2つと FAIR なエビデンスを1つ.

受け入れ可能な Identity Evidence についての詳細は Section 5.2.1 Identity Evidence Quality Requirements を参照のこと.

4.5.3 Validation Requirements

CSP は Identity Evidence を以下のように確認すること (SHALL).

それぞれのエビデンスは, 提示されたエビデンスと同じ強度のプロセスによって確認すること. 例えば2つの STRONG な Identity Evidence が提示された場合は, それぞれを STRONG な強度で確認することとなる.

Identity Evidence の確認についての詳細は Section 5.2.2 Validating Identity Evidence を参照のこと.

4.5.4 Verification Requirements

CSP は Identity Evidence を以下のように検証すること.

1. 最低限, Applicant と Identity Evidence の紐付けは, 強度 SUPERIOR を達成できるプロセスによって検証しなければならない.
2. KBV は対面 (物理的ないしは監視下における Remote) の Identity 検証のために利用してはならない (SHALL NOT).

Identity Evidence の検証についての詳細は Section 5.2.2 Validating Identity Evidence を参照のこと.

4.5.5 Presence Requirements

CSP は Identity Proofing の全ステップを Applicant と対面で行うこと (SHALL). 詳細は Section 5.3.3 を参照のこと.

4.5.6 Address Confirmation

1. CSP は Address of Record を確認しなければならない (SHALL). CSP は, 提示された有効な Identity Evidence のいずれかに記載された住所の確認を通じて, Address of Record の確認を行うべきである (SHOULD). CSP は, Applicant が提供した, いかなる有効な Identity Evidence にも記載されていない情報の確認を通じて, Address of Record の確認を行ってもよい (MAY).
2. Self-asserted な住所データは, 確認に用いてはならない (SHALL NOT).
3. 確認された Address of Record に Proofing の通知を送らねばならない (SHALL).
4. Subscriber と Authenticator の紐付けが後日発生する場合は, CSP は Enrollment コードを直接 Subscriber に提示してもよい (MAY). Enrollment コードは最大7日間まで有効なものとする (SHALL).

4.5.7 Biometric Collection

CSP は, Non-repudiation (否認防止) や Re-proofing を目的として, Proofing 時に Biometrics サンプルを収集・記録すること (SHALL). Biometrics 収集に関する詳細は SP 800-63B, Section 5.2.3 (sp800-63b.html#biometric_use) を参照のこと.

4.5.8 Security Controls

CSP は, SP 800-53 やそれに相当する連邦政府標準 (e.g., FEDRAMP) や業界標準に定められた, High 基準のセキュリティー制御策から, 制御強化を含み, 適切に調整されたセキュリティー制御策を採用しなければならない (SHALL). CSP は *high-impact* システムやそれに相当するものに対する Assurance 関連の最低限の制御策が実施されていることを保証しなければならない (SHALL).

4.6 Enrollment Code

This section is normative.

Enrollment コードにより, CSP は Applicant が Address of Record を管理下に置いていることを確認できるほか, Applicant と Enrollment レコードの再紐付けを行えるようにもなる. この紐付けは, もととなる Identity Proofing Transaction と同一の Session で完了する必要はない (NEET NOT).

Enrollment コードは以下の特徴を持つこと (SHALL).

1. 最低限, 6文字の英数字, またはそれ相当のエントロピーを持つもの. 例えば, 承認された乱数生成器を使って生成されたコードや, 物理ハードウェア Authenticator のシリアル番号.
2. ランダムな6文字の英数字と同じかそれ以上のエントロピーを持つデータを含んだ, QR コードなどの機械可読光学ラベル.

4.7 Summary of Requirements

This section is informative.

Table 4-1 は各 Identity Assurance Level の要件を要約したものである.

Table 4-1 IAL Requirements Summary

Requirement	IAL1	IAL2	IAL3
Presence	要件なし	対面および非監視下の Remote	対面および監視下の Remote

Requirement	IAL1	IAL2	IAL3
Resolution	要件なし	Identity Resolution に必要最低限な Attribute. KBV により信頼を高めてもよい.	IAL2 同様
Evidence	Identity Evidence は収集しない	Issuing Source が実施した Proofing および検証の強度次第で, 1つの SUPERIOR もしくは STRONG なエビデンス, もしくは 2つの STRONG なエビデンス, もしくは 1つの STRONG なエビデンスと2つの FAIR なエビデンス.	2つの SUPERIOR なエビデンス, もしくは Issuing Source が実施した Proofing および検証の強度次第で, 1つの SUPERIOR もしくは STRONG なエビデンス, もしくは 2つの STRONG なエビデンスと1つの FAIR なエビデンス.
Validation	確認なし	それぞれのエビデンスを, エビデンスと同じ強度のプロセスで確認しなければならない.	IAL2 同様
Verification	検証なし	STRONGの強度のプロセスによって検証する.	SUPERIOR の強度のプロセスによって検証される.
Address Confirmation	要件なし	必須. Enrollment コードを任意の Address of Record に送信する. 通知は Enrollment コードとは別の経路で送信する.	必須. Proofing の通知は郵便住所に対して送信する.
Biometric Collection	No	Optional	Mandatory
Security Controls	N/A	SP 800-53 Moderate 基準 (もしくはそれ相当の連邦 / 業界標準).	SP 800-53 High 基準 (もしくはそれ相当の連邦 / 業界標準).

5 Identity Resolution, Validation, and Verification

This section is normative.

本セクションでは, Identity および提示された Identity Evidence の導出, 確認, 検証に関する要件を示す. これらの要件は, Claimed Identity が CSP に Enroll しようとしている Subject の実際の Identity であり, 多数の Enroll 済の個人に影響を及ぼしうるスケーラブルな攻撃がシステムによって保護されているリソースの価値よりも大きな時間およびコストを必要とすることを, 確実にするためのものである.

5.1 Identity Resolution

Identity Resolution のゴールは, ある個人を所与の集団やコンテキスト内でユニークに区別することである. 効率的に Identity Resolution が行えれば, 最小の Attribute セットによって固有の個人を識別可能になる. これは CSP にとって Identity Proofing プロセス全体の重大な出発点であり, 潜在的な不正の初期検出を含むが, 決してそれ単体では完全かつ成功した Identity Proofing Transaction にはならない.

1. Proofing プロセスで利用される情報の完全一致によるマッチングは困難である. CSP は, 適切なマッチングアルゴリズムを用いて, 多様な Identity Evidence, Issuing Source および Authoritative Source にまたがった Personal Information やその他関連する Proofing データの差異を把握することができる (MAY). 使用するマッチングアルゴリズムとルールは公開すべきであり, 少なくとも関連する利益共同体には提示されるべきである (SHOULD). 例えば, それらは文書化されたポリシーや Section 4.2 で言及された *practice statement* に含めることができる.
2. KBV (Knowledge-Based Authentication とも呼ばれる) は, 歴史的に, 公開データベースから得られた情報に対して Applicant の知識をテストすることによって, Claimed Identity を検証するために使用されてきた. CSP は KBV を使って, ユニークな Claimed Identity を識別可能にしてもよい (MAY).

5.2 Identity Evidence Collection and Validation

Identity Validation のゴールは, Applicant からもっとも適切な Identity Evidence を収集し, その Authenticity, 正当性, 正確性を判断することである. Identity Validation は, 適切な Identity Evidence の収集, 当該エビデンスが本物かつ正当であることの確認, Identity Evidence に含まれるデータが正当, 最新, かつ現実世界の Subject に関連していることの確認, の3ステップからなる.

5.2.1 Identity Evidence Quality Requirements

本セクションでは, Identity Proofing 段階で収集される Identity Evidence の品質要件について述べる.

Table 5-1 には, 正当な Identity を確立するために収集する Identity Evidence に関しての, Unacceptable から Superior までの強度を列挙する. 特に記載がない限り, これらの強度を達成するために, 当該エビデンスは最低限ここに列挙されたすべての品質を満たす必要がある (SHALL).

Table 5-1 Strengths of Identity Evidence

Strength	Qualities of Identity Evidence
Unacceptable	- 受け入れ可能な Identity Evidence ではない.

Weak	- 当該エビデンスの Issuing Source が Identity Proofing を行なっていない.
	
	- 当該エビデンスの発行プロセスでは, 当該エビデンスが合理的に Applicant の管理下に送達されることが想定できる.
	
	- 当該エビデンスが以下を含む.
	  - 当該エビデンス自体, もしくは紐づいている人物を一意に識別できる, 少なくとも1つの参照番号.
	  OR
	  - 紐づいている人物の写真もしくは Biometrics テンプレート (様式は問わない).

Fair	- 当該エビデンスの Issuing Source が Identity Proofing プロセスを通じて Claimed Identity を確認している.
	
	- 当該エビデンスの発行プロセスでは, 当該エビデンスが合理的にそのエビデンスに紐づく人物の管理下に送達されることが想定できる.
	
	- 当該エビデンスが以下を満たす.
	  - 紐づいている人物を一意に識別できる, 少なくとも1つの参照番号.
	  OR
	  - 紐づいている人物の写真もしくは Biometrics テンプレート (様式は問わない).
	  OR
	  - KBV を通じて所有権を確認可能.
	
	- 当該エビデンスにデジタル情報が含まれる場合, その情報は暗号化やプロプラエタリーな方法, またはその両方により保護され, 情報の Integrity を確保して Claimed Issuing Source の Authenticity が確認できる.
	
	- 当該エビデンスに物理セキュリティー機能が含まれる場合, それを再現するためのプロプラエタリーな知識が必要である.
	
	- 当該エビデンスは有効期限切れしていない.

Strength	Qualities of Identity Evidence
Strong	- 当該エビデンスの Issuing Source が, 現実世界の当人の Identity についての合理的な確信を持てるように設計されている文書化された手続きを通じて, Claimed Identity を確認している. このような手続きは, 規制当局または公的に責任がある機関によって定期的に監督されることとする. そのような手続きの例としては, USA PATRIOT Act of 2001 や Fair and Accurate Credit Transaction Act of 2003 (FACT Act) Section 114 に定められた Red Flags Rule に呼応して確立された, Customer Identification Program ガイドラインなどが挙げられる. - 当該エビデンスの発行プロセスでは, 当該エビデンスがそのエビデンスに紐づく Subject の管理下に送達されることが保証される. - 当該エビデンスに紐づいている人物を一意に識別できる, 少なくとも1つの参照番号が含まれる. - 当該エビデンスに記載されたフルネームは, 当人が発行時点においてオフィシャルに認識されている名前でなければならない. 仮名, エイリアス, イニシャルなどは許容されない. - The: - 当該エビデンスは, 紐づいている人物の写真もしくは Biometrics テンプレート (様式は問わない) を含む. **OR** - Applicant が, 最低限 IAL2 の Identity に紐づいた AAL2 の Authenticator を保持していることを証明する. - 当該エビデンスにデジタル情報が含まれる場合, その情報は暗号化やプロプラエタリーな方法, またはその両方により保護され, 情報の Integrity を確保して Claimed Issuing Source の Authenticity が確認できる. - 当該エビデンスに物理セキュリティー機能が含まれる場合, それを再現するためのプロプラエタリーな知識およびテクノロジーが必要である. - 当該エビデンスは有効期限切れしていない.
Superior	- 当該エビデンスの Issuing Source が, 現実世界の Subject の Identity について確実に信頼できるように設計されている文書化された手続きを通じて, Claimed Identity を確認している. このような手続きは, 規制当局または公的に責任がある機関によって定期的に監督されることとする. - Issuing Source は Applicant を視覚的に識別し, 当人の存在確認のためのさらなるチェックを行なった. - 当該エビデンスの発行プロセスでは, 当該エビデンスがそのエビデンスに紐づく人物の管理下に送達されることが保証される. - 当該エビデンスに紐づいている人物を一意に識別できる, 少なくとも1つの参照番号が含まれる. - 当該エビデンスに記載されたフルネームは, 当人が発行時点においてオフィシャルに認識されている名前でなければならない. 仮名, エイリアス, イニシャルなどは許容されない. - 当該エビデンスは, 紐づいている人物の写真を含む. - 当該エビデンスは, 紐づいている人物の Biometrics テンプレート (様式は問わない) を含む. - 当該エビデンスはデジタル情報が含み, その情報は暗号化やプロプラエタリーな方法, またはその両方により保護され, 情報の Integrity を確保して Claimed Issuing Source の Authenticity が確認できる. - 当該エビデンスに物理セキュリティー機能を含み, それを再現するためのプロプラエタリーな知識およびテクノロジーが必要である. - 当該エビデンスは有効期限切れしていない.

5.2.2 Validating Identity Evidence

ひとたb Identity Evidence を取得すると, CSP はその正確さ, Authenticity, Integrity, および関連情報を Authoritative Source に照会し, 提示されたエビデンスに対して以下の項目を判断する.

- 偽造されていない真正なものであること.
- 正しい情報が記載されていること.
- 実在する Subject に関する情報が記載されていること.

Table 5-2 には, 当該 Proofing Session において提示されたエビデンス, およびそこに記載された情報のに対する, CSP が実施する Identity Validation に関しての, Unacceptable から Superior までの強度を列挙する.

Table 5-2 Validating Identity Evidence

Strength	Method(s) performed by the CSP

Strength	Method(s) performed by the CSP
Unacceptable	- Evidence は未確認, もしくは確認できない.
Weak	- エビデンスから得られるすべての個人に関する詳細は, Authoritative Source が保有ないしは公開している情報と比較して正当性が確認された.
Fair	- 当該エビデンスは - 詳細が Issuing Source ないしは Authoritative Source が保有ないしは公開している情報と比較して正当性が確認された. **OR** - 適切なテクノロジーによって, 物理セキュリティー機能の Integrity が確認され, 当該エビデンスが不正・改ざんされておらず, 本物であることが確認された. **OR** - 当該エビデンスが, 訓練を受けた担当者により真正であると確認された. **OR** - 暗号論的セキュリティー機能の Integrity が確認され, 当該エビデンスが真正であると確認された.
Strong	- 以下のように当該エビデンスが真正であると確認された. - 適切なテクノロジーによって, 物理セキュリティー機能の Integrity が確認され, 当該エビデンスが不正・改ざんされていないことを確認した. **OR** - 訓練を受けた担当者もしくは適切なテクノロジーによって, 物理セキュリティー機能の Integrity が確認され, 当該エビデンスが不正・改ざんされていないことを確認した. **OR** - 暗号論的セキュリティー機能の Integrity を確認した. - エビデンスから得られるすべての個人およびエビデンスに関する詳細は, Issuing Source ないしは Authoritative Source が保有ないしは公開している情報と比較して正当性が確認された.
Superior	- 訓練を受けた担当者, および物理セキュリティーと暗号論的セキュリティー機能の Integrity を含む適切なテクノロジーによって, 当該エビデンスが真正であると確認された. - エビデンスから得られるすべての個人およびエビデンスに関する詳細は, Issuing Source ないしは Authoritative Source が保有ないしは公開している情報と比較して正当性が確認された.

担当者がエビデンスを確認する際の訓練に関する要件は, CSP ないしは RP のポリシー, ガイドライン, 要件に基づくこと (SHALL).

5.3 Identity Verification

Identity Verification のゴールは, Claimed Identity とエビデンスを提示している現実世界に存在する Subject との紐付けを, 確認および確立することである.

5.3.1 Identity Verification Methods

Table 5-3 には, ある Identity Verification 強度を達成するために必要な検証手段が詳説されている. CSP は, Identity 検証に KBV を利用する際は, Section 5.3.2 の要件に従うこと (SHALL).

Table 5-3 Verifying Identity Evidence

Strength	Identity Verification Methods
Unacceptable	- エビデンスは未検証, もしくは検証できない. Applicant が Claimed Identity の所有者であることが確認できない.
Weak	- Applicant は Claimed Identity を裏付けるために提出されたエビデンスへの Access 権限を持っていることが確認された.
Fair	- Applicant が Claimed Identity の所有者であることが, 以下のように確認された. - KBV. 詳細は Section 5.3.2. を参照のこと. **OR** - Applicant と, Claimed Identity を裏付けるために提示されたものの中でもっとも強度の高い Identity Evidence との, 物理的な比較. Remote で物理比較を行なう際は, [SP 800-63B, Section 5.2.3.] (sp800-63b.html#biometric_use) に示すすべての要件に従うこと (SHALL). **OR** - Applicant と Identity Evidence の Biometric 比較. Remote で Biometric 比較を行なう際は, [SP 800-63B, Section 5.2.3.] (sp800-63b.html#biometric_use) に示すすべての要件に従うこと (SHALL).

Strength	Identity Verification Methods
Strong	- Applicant が Claimed Identity の所有者であることが, 以下のように確認された. - 適切なテクノロジーを利用した, Claimed Identity を裏付けるために提示されたものの中でもっとも強度の高い Identity Evidence に対する, 写真による物理比較. Remote で物理比較を行なう際は, [SP 800-63B, Section 5.2.3.] (sp800-63b.html#biometric_use) に示すすべての要件に従うこと (SHALL). **OR** - 適切なテクノロジーを利用した, Applicant と Claimed Identity を裏付けるために提示されたものの中でもっとも強度の高い Identity Evidence との Biometric 比較. Remote で Biometric 比較を行なう際は, [SP 800-63B, Section 5.2.3.] (sp800-63b.html#biometric_use) に示すすべての要件に従うこと (SHALL).
Superior	- Applicant が Claimed Identity の所有者であることが, Applicant と Claimed Identity を裏付けるために提示されたものの中でもっとも強度の高い Identity Evidence との, 適切なテクノロジーを利用した Biometric 比較により確認された. Remote で Biometric 比較を行なう際は, [SP 800-63B, Section 5.2.3.] (sp800-63b.html#biometric_use) に示すすべての要件に従うこと (SHALL).

5.3.2 Knowledge-Based Verification Requirements

IAL2 および IAL3 の Identity Verification では, 以下の要件が適用される. KBV を Identity Resolution に用いる場合は特に制約はない.

1. CSP は, 2つ以上の確認済 Identity Evidence に対して KBV を用いて Applicant の Identity 検証を行なってはならない (SHALL NOT).
2. CSP は, KBV プロセス開始に必要な情報を含め, Applicant と Authoritative Source のみが知っていると期待される情報のみを使用することとする (SHALL). 自由に取得可能な情報, パブリックドメインにおいて課金することで手に入る情報, ブラックマーケット経由で手に入る情報は使用しないこと (SHALL NOT).
3. CSP は, Resolution および Validation が完了した Identity に対して, Verification のために KBV 以外のプロセスを利用できるようなオプトアウト手段を提供すること (SHALL).
4. CSP は, CSP が参加していた最近の Transaction ヒストリーに関する知識を検証することで, KBV を行なうべきである (SHOULD). CSP は, Transaction 情報が最低限20ビットのエントロピーを持つよう保証すること (SHALL). 例えば, 最小のエントロピー要件に到達するには, Applicant に正規の銀行口座に対する少額デポジットのデポジット額および Transaction ナンバーを尋ねることで, 検証を行なうことができる. この例では全7桁以上の数値を聞くことになる.
5. CSP は, Applicant が Claimed Identity の所有者であることを示す質問を投げかけ, KBV を実行しても良い. しかしながらその場合は以下の要件を満たすこと.
    a. KBV は複数の Authoritative Source に基づくこと.
    b. CSP は最低限4つの質問を行い, それぞれが正解することをもって KBV ステップを成功とすること (SHALL).
    c. CSP は自由回答方式の KBV 質問を行うべきである (SHOULD). CSP は選択式質問を行っても良いが (MAY), その場合は各質問に4つ以上の選択肢を用意すること (SHALL).
    d. CSP は KBV を完了するために Applicant に2度の試行を許すべきである (SHOULD). CSP は3回以上の試行を許容してはならない (SHALL NOT).
    e. CSP は各質問ごとに2分間の無反応状態があれば KBV Session をタイムアウトさせること (SHALL). Session がタイムアウトした場合, CSP は KBV プロセス全体をリスタートし, 当該試行は失敗と扱うこと (SHALL).
    f. CSP は KBV の大部分を陽動となるような質問としてはならない (SHALL NOT). (i.e., "none of the above" が正解となるようなもの)
    g. CSP は同じ KBV 質問を連続した試行において尋ねるべきではない (SHOULD NOT).
    h. CSP は, 単一の Session ないしは失敗試行の次の Session において, 後の KBV 質問に役立つ情報を提供するような KBV 質問をしてはならない (SHALL NOT).
    i. CSP は正解が不変な KBV 質問を利用してはならない (SHALL NOT). (e.g., "What was your first car?")
    j. CSP は, いかなる KBV 質問も, Applicant がまだ提示していない PII や, KBV Session 中の他の情報と組み合わせて特定の個人の識別につながるような Personal Information を漏洩させることのないよう保証すること (SHALL).

5.3.3 In-person Proofing Requirements

対面の Proofing には, 以下の2通りの方法がある.

- オペレーターによる Applicant との物理的インタラクション.
- Section 5.3.3.2 にある特別な要件に従った, オペレーターによる Applicant との Remote インタラクション.

5.3.3.1 General Requirements

1. CSP は, 不自然な材料の存在チェックのためにオペレーターに Biometric 情報源 (e.g., 指, 顔) を確認させ, Proofing プロセスの一部としてそのような検査を行うこと (SHALL).
2. CSP は, 当該 Biometric が他の Subject ではなく当該 Applicant から収集されたことが保証される方法により Biometric を収集すること (SHALL). Biometric の実行要件については SP 800-63B, Section 5.2.3 (sp800-63b.html#biometric_use) を参照のこと.

5.3.3.2 Requirements for Supervised Remote In-person Proofing

CSP は, Remote Proofing プロセスを採用し, 対面と同等レベルの信頼性およびセキュリティーを実現することもできる. 以下の要件は, Applicant が CSP と物理的に同じ場所にいる対面での Transaction と, Applicant が Remote にいる場合の間の比較可能性を示している.

Supervised Remote (監視下にある Remote での) Identity Proofing および Enrollment Transaction においては, Section 4.6 に示した IAL3 での Validation および Verification 要件に加えて, 以下の要件に従うこと (SHALL).

1. CSP は, Applicant が Session から離れることのないよう (SHALL NOT), 全体の Identity Proofing Session を監視すること (SHALL). これには例えば, Applicant の継続的な高解像度ビデオ伝送などの手段があげられる.
2. CSP は, Identity Proofing Session 全体を通じて, Applicant から Remote でリアルタイムにオペレーターを関与させること (SHALL).
3. CSP は, Identity Proofing Session 全体を通じて, Applicant が行った全てのアクションを, Remote オペレーターにはっきりと見えるようにすること (SHALL).
4. CSP は, エビデンスに対するあらゆるデジタル検証 (e.g., チップやワイヤレス技術による) が, 統合されたスキャナーやセンサーによって実行されるようにすること (SHALL).
5. CSP は, 潜在的な不正を検出し正しく仮想の対面 Proofing Session を実行するため, オペレーターに訓練プログラムを受けさせること (SHALL).
6. CSP は, 環境に応じた適切な物理的改ざんの検出策および対抗策を施すこと (SHALL). 例えば, 制限されたエリアや信頼できる個人によって監視されているエリアにあるキオスクは, ショッピングモールのコンコースなどの半公開エリアにあるキオスクよりも, 改ざん検出の必要性は低い.
7. CSP は, 全ての通信が双方向の Authenticated Protected Channel 経由で行われるよう保証すること (SHALL).

5.3.4 Trusted Referee Requirements

1. CSP は, 交渉人や法的保護者, 医療専門家, 後見人, 法定代理人, その他の訓練を受け承認されたもの, または認定されたものなど, 適切な法律, 規則, 機関のポリシーに従って, Applicant の身元を保証したり代理人となれる信頼できる身元引き受け人 (Trusted Referee) とやり取りをしても良い (MAY). CSP は Remote, 対面どちらのプロセスでも, Trusted Referee とやり取りをしても良い (MAY).
2. CSP は, Trusted Referee がどのように決定されるか, および取り消し, 一時停止, その他いかなる制約も含め, Trusted Referee 自身のステータスのライフサイクルについて, ポリシーや手順を明文化すること (SHALL).
3. CSP は, Applicant の Proofing と同じ IAL で, Trusted Referee に対する Proofing を行うこと (SHALL). また CSP は, Trusted Referee と Applicant の関係性を測るために必要な最低限のエビデンスを決定すること (SHALL).
4. CSP は, Section 4.4.1 の要件を満たすことをゴールとして, 上記1で示された文書化されたポリシーに定義された規則的なインターバルで, Subscriber に対して Re-proofing を行うべきである (SHOULD).

Considerations for Minors

1. CSP は, Children’s Online Privacy Protection Act of 1998 およびその他の法律が適用される場合, それらに遵守すべく, Identity Proofing のエビデンス要件を満たすことができない未成年とのインタラクションに関する法的制約を特別に考慮すること (SHALL).
2. 13歳以下の未成年に関しては, CSP は COPPA およびその他の法律の遵守が求められ (SHALL), 確実に遵守するためには特別な配慮が必要となる.
3. CSP は, 本セクションですでに述べたように, 未成年の Applicant のための Trusted Referee として, 親または法定成人後見人を関与させるべきである (SHOULD).

5.4 Binding Requirements

Authenticator と Subscriber の紐付けに関しては, 800-63B (sp800-63b.html) Section 6.1 Authenticator Binding を参照のこと.

6 Derived Credentials

This section is informative.

Credential の導出は, 個人が自身の所有する1つ以上の Authenticator に紐づけられた Identity レコード (i.e., Credential) の正当な Subject であることを CSP に対して証明するプロセスに基づいている. 個人に対して既存の Identity Proofing 済のレコードや Credential に紐づいた新たな Authenticator を取得できるようにしたいと考える CSP は, このプロセスを利用可能とすることができる. Identity Proofing プロセスを繰り返す回数を最小化することは個人と CSP に対してメリットとなる. 元の Proofing 済の Digital Identity にすでに紐づいている Authenticator の保持証明と, その Authenticator 使った Authentication の成功をもって, Identity の導出は達成される.

本セクションにおける “導出 (derived)” の定義では, ある鍵から別の鍵を導出するなど, Authenticator が暗号論的に Primary Authenticator に紐づいていることは意味 しない. それよりも, すでに Proofing 済の Identity に紐づいた Authenticator を使った Authentication が成功したことにもとづき, 不必要な Identity Proofing を繰り返すことなく単に新たに Authenticator を発行することで, 導出とすることができる.

Identity 導出を行うユースケースとしては, 以下の2つがあげられる.

1. *Claimant* が, PIV スマートカードの制限と権限の範囲内で利用するためいに, 自身の Identity レコードに紐づいて導出された PIV を取得しようとする. このユースケースについては *SP 800-157, Guidelines for Derived Personal Identity Verification (PIV) Credentials* を参照のこと
2. *Applicant* が, 事前に関係性を持たない CSP との間で Credential を確立しようとする. 例えば, Applicant がある CSP から別の CSP に移行しようとしたり, 新たな CSP から独立した Authenticator を別目的 (e.g., 基本的なブラウジング vs. 金融) で得ようとしたりするといったことが考えられる. このユースケースについては*, Section 5.2* にある受け入れ可能な *Identity Evidence* に関する記述を参考のこと.

上述の通り, PIV から導出される Credential に関する要件はすべて SP 800-157 に記載されている. 上記2つめのユースケースに関しては, 本ガイドラインは物理的な Identity Evidence とデジタルな Identity Evidence の区別をつけない. 従って, Primary CSP が生成した Authenticator や Assertion が Section 5 の要件にあえば, それらを IAL2 や IAL3 の Identity Evidence としてい利用することもできる. さらに, デジタルな Identity Evidence を提示した結果として発行された Authenticator に対しては, SP 800-63B (sp800-63b.html) の要件が課される.

7 Threats and Security Considerations

This section is informative.

Enrollment プロセスにおいては, なりすまし, およびインフラストラクチャー提供者に対する不正アクセスと提供者自身の不正行為, という2つの脅威カテゴリーが一般的に存在する. インフラストラクチャーに対する脅威は従来のコンピューターセキュリティー制御策 (e.g., 侵入防止, 記録保持, 独立監査) により対応可能であるため, それらは本ドキュメントのスコープ外とし, 本セクションではなりすましの脅威に焦点を当てる. セキュリティー制御策に関する詳細は SP 800-53 *Recommended Security and Privacy Controls for Federal Information Systems and Organizations* を参照のこと.

Enrollment プロセスにおける脅威としては, なりすましに加え, Identity Proofing, Authenticator の紐付け, Credential 発行の各段階における通信メカニズムに対する脅威が挙げられる. Table 7-1 に Enrollment と Identity Proofing に関連する脅威をまとめる.

Table 7-1 Enrollment and Identity Proofing Threats

Activity	Threat/Attack	Example
Enrollment	Identity Proofing Evidence の偽造	Applicant が偽造運転免許証を利用して不正な Identity を主張する.
	他人の Identity の不正利用	Applicant が他人に紐づくパスポートを利用する.
	Enrollment 否認	Subscriber が Enrollment を拒否し, 自身は CSP に対して登録していないと主張する.

7.1 Threat Mitigation Strategies

Enrollment における脅威は, なりすましを困難にしたり, なりすましの検出率を向上させることで, 抑止することができる. 推奨案では, おもになりすましを困難にする手法について扱うが, だれがなりすましを行なったかを証明するのに役立つ手段と手順も規定する. 各レベルにおいて, Claimed Identity が存在すること, Applicant が Claimed Identity の所有者であること, Applicant が後日 Enrollment を否認できないことを確かなものにする方法が採用される. Assurance Level が上がるにつれ, カジュアル, システマチック, および内部犯によるなりすましに対する抵抗力が高まる. Table 7-2 に Enrollment および発行プロセスにおける脅威への対策に関する戦略をまとめる.

Table 7-2 Enrollment and Issuance Threat Mitigation Strategies

Activity	Threat/Attack	Mitigation Strategy	Normative Reference(s)
Enrollment	Identity Proofing Evidence の偽造	CSP が提示されたエビデンスの物理セキュリティー機能を確認する.	4.4.1.3, 4.5.3, 5.2.2
		CSP がエビデンス発行元やその他の Authoritative Source に対してエビデンスに記載された個人の詳細を確認する.	4.4.1.3, 4.5.3, 4.5.6 5.2.2
	他人の Identity の不正利用	CSP がエビデンス発行元やその他の Authoritative Source から取得した情報と照らし合わせ, Applicant の Identity Evidence と Biometrics を検証する.	4.4.1.7, 4.5.7, 5.3
		Applicant が提供した非政府発行のドキュメント (e.g., Applicant 名義で Applicant の現住所が記載された電気代の請求書や, クレジットカードの請求書) を検証し, Applicant の Identity に対する確信を高める.	4.4.1.7, 4.5.7, 5.3
	Enrollment 否認	CSP が Subscriber の Biometric を保存する.	4.4.1.7, 4.5.7

8 Privacy Considerations

This section is informative.

以下のプライバシーに関する考慮事項は, Section 4.2 の General Requirements に関する情報を提供する.

8.1 Collection and Data Minimization

Section 4.2 requirement 2 では, Identity Resolution, Validation および Verification に対する適用可能なベストプラクティスに基づいて, Claimed Identity の存在確認および Claimed Identity と Applicant の関連付けに必要な PII のみの収集を許可している. 不必要な PII を収集すると, なぜ Identity Proofing に利用されない情報が収集されているのかという混乱を生じさせる. これは侵害や不要な懸念を与え, Applicant の信頼を損ねることにつながる可能性がある. さらに, PII を保持すると, Unauthorized Access や不正利用に対して脆弱になる可能性もある. データ最小化により PII の量を減少させそのようなリスクを軽減することは, Identity Proofing プロセスにおける信頼を促進することとなろう.

8.1.1 Social Security Numbers

Section 4.2 requirement 13 では, Identity Resolution がその他の Attribute や Attribute の組み合わせによって達成不可能であり, SSN が Identity Resolution に必要でない限り, CSP が SSN を収集することを禁じている. SSN への過度な信頼は, 誤用を招き, なりすましなどにより Applicant に損害を与えかねない. しかし, こと連邦政府機関の RP にとっては, SSN により Subscriber を既存のレコードに関連づけることができ, Identity Resolution が達成されるケースもある. したがって, 本ドキュメントは SSN を識別子として捉え, その利用に関して適切な措置を行う.

> Note: 高 IAL のエビデンス要件においては, SSN や Social Security Card を Identity Evidence として受け入れることを禁止している.

Identity Proofing を目的として SSN を収集する前に, 各組織は SSN を収集する際の法的義務, 第三者のプロセスやシステムとの相互運用性のために SSN を利用する必要性, または運用要件を考慮する必要がある. 運用要件は, システムやプロセス, 形式が, コストや許容不可能なリスク要因により置き換え不可能であることにより示されるかもしれない. なお, 運用上の必要性は, 使い勝手や変更したくないという意思によって正当化されるものではない.

連邦政府機関に対する [Executive Order (EO) 9397] (#9397) の初期の要件である, 当該機関で働く個人, 取引関係にある個人, ないしは取引関係にある他組織に属する個人の識別の主要手段として SSN を利用すべしという要件は廃止された. したがって, EO 9397 はもはやそれ単体をもって SSN 収集が必要であるという権威として参照することはできない.

連邦政府機関は, Office of Management and Budget Policy に従って SSN の収集および不必要な利用を削減する義務を考慮に入れ, あらゆる SSN 収集に関する意思決定をレビューする必要がある.

8.2 Notice and Consent

Section 4.2 requirement 3 (4.2-r3) では, Identity Proofing に必要な Attribute の収集と記録管理の目的を, 当該 Attribute が Identity Proofing Transaction を完了させるために必須か否か, Attribute を提供しなかった場合の影響を含め, CSP が収集時に Applicant に明示的に通知するよう求めている.

効果的な通知を行うには, ユーザーエクスペリエンスデザイン標準と研究, および収集により発生する可能性のあるプライバシーリスクの評価を考慮することが重要であろう. Applicant が, なぜ当該 Attribute が収集されるかや, 収集された情報が他のデータソースと組み合わされるかどうかなどに関して不正確な推測を行うことなどを含め, さまざまな要素を考慮すべきである. 効果的な通知は, 決して複雑で法に固執したプライバシーポリシーや, Applicant が読んだり理解することが期待できないような全般的な利用規約への単なるポインターではない.

8.3 Use Limitation

Section 4.2 requirement 4 は, CSP が Identity Proofing において収集・管理することとなった Attribute を, CSP が明確な通知を行い Subscriber からの同意を得た場合を除き, Identity Proofing, Authentication, Authorization, Attribute Assertion, 関連する不正対策, 法律や法的プロセスに従う以外の目的で利用することを禁じている.

想定する利用目的が許容範囲内かどうかについて疑問がある場合は, SAOP に相談すること. この通知は Section 8.2 Notice and Consent と同じ原則に従うべきであり, 決して複雑で法に固執したプライバシーポリシーや全般的な利用規約に含められるべきではない. むしろ, 明示された目的の範囲外での利用を行う際は, Subscriber に追加用途とその許諾・拒否の方法が理解できるように, 意味のある通知を行うべきである. CSP は, こういった追加用途への許諾を Subscriber に対して Identity Proofing サービス提供条件としてはならない.

8.4. Redress

Section 4.2 requirement 5 は, CSP に対して, Identity Proofing によって生じた Applicant の苦情や問題に関する効果的な是正手段を提供し, その手段を Applicant が容易に発見, Access できるようにすることを求めている.

Privacy Act は, 連邦政府の CSP に対して, Applicant が Access し, 正しくない場合は記録を訂正できるよう, 訂正を可能にする手順に従った記録システムを管理することを求めている. すべての Privacy Act Statement には, 適用可能な SORN への参照を含めるべきであり, それにより Applicant が Access, 訂正するための手順書を提供すべきである. 非連邦政府の CSP は, 情報源となる第三者の連絡先を含め, 上記と同等の手順を用意すべきである.

CSP は, Applicant が自身の Identity を確立して登録プロセスをオンラインで完結できない場合に, ユーザーに当該プロセスを完了するための代替手段 (e.g., 可能であれば, カスタマーサービスセンターでの対面手続き) を提供するべきである.

> Note: Identity Proofing プロセスが失敗した場合, CSP は Applicant に問題を解決する手順を通知すべきであるが, 登録が失敗した理由そのものを Applicant に通知すべきではない (e.g., Applicant に “あなたの SSN が当方があなたのものとして保持している SSN とマッチしなかった” などと知らせてはならない). そのような情報は不正な Applicant が正しい PII に関する情報を得る手立てとなりうる.

8.5 Privacy Risk Assessment

Section 4.2 requirement 7 および 10 は, CSP に Privacy Risk Assessment の実施を求めている. Privacy Risk Assessment 実施にあたって, CSP は以下を考慮すべきである.

1. CSP が取るアクション (e.g., 追加の検証ステップや記録保持) が, 侵害や情報への Unauthorized な Access など, Applicant にとっての問題となりうる可能性.
2. 発生した問題のインパクト. CSP は, リスクの受容, 軽減, 共有など, 特定したプライバシーリスクへのあらゆるレスポンスを正当化できるようにすべきである. Applicant の同意は, リスクを共有する形態の一例とみなすべきであり, したがって Applicant が共有されたリスクを評価し受容できると合理的に期待できる場合のみ, Applicant の同意を使用すべきである.

8.6 Agency Specific Privacy Compliance

Section 4.2 requirement 12 は, 連邦政府の CSP に対する特別なコンプライアンス上の責任について述べている. 機関の SAOP を Digital Authentication システムの開発初期段階から関与させることは, プライバシーリスクを評価・軽減し, Identity Proofing のための PII 収集が, Privacy Impact Assessment のための Privacy Act of 1974 [Privacy Act] や E-Government Act of 2002 [E-Gov] の要件を引き起こすか, といったコンプライアンス要件についての助言を行う上で, 非常に重要である. 例えば, Identity Proofing に関しては, Privacy Act 要件が適用され, Identity Proofing に必要な PII やその他の Attribute の収集・保持のために, 新規または既存の Privacy Act 記録システムによるカバレッジが求められる.

SAOP は同様に PIA の必要性の決定において, 機関を支援できる. これらの考慮事項は, Identity Proofing だけのために Privacy Act SORN や PIA を開発することが要件となるという風に読むべきではない. 多くの場合, Digital Authentication プロセス全体を網羅する PIA および SORN を草稿したり, Digital Authentication プロセスを機関がオンライン Access を確立するプログラムやメリットについて議論するより広範囲で計画立った PIA の一部とすることが, もっとも理にかなっているであろう.

Digital Authentication には多くの構成要素があることから, SAOP に各個別要素を認識し理解させることが重要である. 例えば, 機関は Data Use Agreements や Computer Matching Agreements などの Proofing サービスなどの提供・利用が可能かもしれない. SAOP は機関にどのような追加要件が適用されるを判断するべく支援を行なうことができる. さらに Digital Authentication の個々の要素を完全に理解することで, SAOP はコンプライアンスプロセスやその他の手段を通じてプライバシーリスクを入念に評価し, 緩和することができる.

9 Usability Considerations

This section is informative.

本セクションでは, Enrollment と Identity Proofing に関連するユーザビリティー上の考慮事項を実装者に周知することを目的とする (典型的な Authenticator の利用と断続的イベントに関するユーザビリティー上の考慮事項については SP 800-63B, Section 10 (sp800-63b.html#sec10) を参照のこと).

ISO/IEC 9241-11 はユーザビリティーを “特定のユーザーが特定の利用コンテキストにおいて, 有効, 効率的かつ満足できる程度に特定の目的を達成するためにプロダクトを利用できる程度” と定義している. この定義は, 有効性, 効率性, 満足度を達成するために必要な主要因として, ユーザーと目標, 利用コンテキストに着目している. ユーザビリティーを達成するには, これらのキー要素を考慮した全体的アプローチが必要である.

Enrollment および Identity Proofing におけるユーザビリティーの包括的ゴールは, ユーザーの負担 (e.g., かかる時間やフラストレーション) や Enrollment における摩擦 (e.g., 完了までのステップ数とトラックされる情報量) を最小化し, スムーズでポジティブな Enrollment プロセスを促進することである. このゴールを達成するため, 組織はまずユーザーに自身をよく知ってもらう必要がある.

Enrollment および Identity Proofing プロセスでは, ユーザーは CSP および自身が Access するオンラインサービスとのインタラクションを行うことになる. ファーストインプレッションがネガティブであれば, それ以降のインタラクションに対するユーザーの印象にも影響しうるため, 組織はプロセス全体を通じてポジティブなユーザーエクスペリエンスを促進する必要がある.

ユーザビリティーは計画性なく断片的に達成できるものではない. Enrollment および Identity Proofing プロセスに対するユーザビリティー評価を行うことは, 非常に重要である. 代表的なユーザー, 現実的なゴールとタスク, 適切な利用コンテキストのもとでユーザービリティ評価を行うことが重要である. Enrollment および Identity Proofing プロセスは, ユーザーが正しいことをするのは簡単に, 間違ったことをするのは難しく, かつ間違っても簡単に回復できるように設計し実装するべきである.

ユーザー視点では, Enrollment および Identity Proofing には, Enrollment 事前準備, Enrollment および Proofing Session, Enrollment 完了後アクション, の3つの主要なステップが存在する. これらのステップは単一の Session で起こることもあれば, それぞれがかなり時間的に離れている (e.g., 数日から数週間) こともある.

全般的, および各ステップごとのユーザビリティー上の考慮事項については, 以下の各セクションで述べる.

ASSUMPTIONS

本セクションでは, “ユーザー” は “Applicant” ないし “Subscriber” を意味する.

ガイドラインおよび考慮事項はユーザー視点で記述する.

アクセシビリティーはユーザビリティーとは異なり, 本ドキュメントの扱うところではない. Section 508 は情報技術の障壁を排除するために制定され, 連邦政府機関に対して, 電子的かつ情報技術を活用し障害者が公開コンテンツにアクセス可能になるよう求めている. アクセシビリティーガイドラインについては Section 508 の法と標準を参照のこと.

9.1 General User Experience Considerations Duuring Enrollment and Identity Proofing

本サブセクションでは, Enrollment プロセスの全ステップに渡って適用可能なユーザビリティー上の考慮事項について述べる. 各ステップごとに固有のユーザビリティー上の考慮事項は Sections 9.2 から 9.4 を参照のこと.

- ユーザーのフラストレーションを回避するため, Enrollment に必要なプロセスを合理化し, 各ステップを可能な限り明確かつ容易にする.
- どこでどのように技術的支援を受けることができるかを明確に伝える. 例えば, お
- どこでどのようにして技術的な支援を得ることができるかを明確に伝える. 例えば, ユーザーにオンラインセルフサービス機能へのリンクや, ヘルプデスクサポートのためのチャットや電話番号を提供する. 理想的には, 外部からの介入なしにユーザーが自身で Enrollment 準備の疑問を解決できるよう, 十分な情報を提供するべきである.
- 誰が何の目的で彼らのデータを収集するのかを明確に説明する. また, 彼らのデータがたどるパス, 特にどこにデータが格納されるかも示す.
- 提示されたすべての情報が使用できることを保証する.
    - すべてのユーザーに提示する資料 (e.g., データ収集通知や記入式フォーム) について, 適切な情報デザインプラクティスに従う.
    - 資料, 典型的には第6学年から第8学年のリテラシーレベルの平易な言葉で記述し, 技術的な専門用語は避けること. 能動態と口語スタイルで, 主なポイントを論理的に順序立て, 混乱を避けるため同義語ではなく同一単語を一貫して使用し, 可動性向上のため可能であれば箇条書きや書式付き文書などを利用すること.
    - フォントスタイル, サイズ, 色, 周囲の背景とのコントラストなどのテキストの読みやすさを考慮する. 最もコントラスト比が高いのは, 白地に黒である. ユーザーの視力レベルは人それぞれであるため, テキストの可読性は重要である. 判読不可能なテキストは, ユーザーの誤認や入力エラーにつながる (e.g., 記入式フォームを埋める際など).
    - 電子的な資料にはサンセリフフォント, 紙の資料にはセリフフォントを使用する.
    - 可能であれば, すぐ混同しがちな文字 (文字 “O” と数字 “0” など) を明確に区別できないフォントは避ける. これは特に Enrollment コードにおいて重要である.

- テキストがディスプレイに収まる限り, 最小フォントサイズは12ポイントとする.
- 代表的なユーザーに対して各ステップのユーザビリティー評価を行う. ユーザビリティー評価においては, 現実的ゴールとタスクを定め, 適切な利用コンテキストを設定する.

9.2 Pre-Enrollment Preparation

本セクションでは, 十分な Enrollment の事前準備を促進するための効果的なアプローチについて述べる. これによりユーザーは困難でフラストレーションが溜まる Enrollment Session を避けることができる. ユーザーが Enrollment Session にできるだけ準備万端であれるよう保証することは, Enrollment および Identity Proofing の全体的な成功とユーザビリティーにとって非常に重要である.

そのような準備は, ユーザーが必要な情報 (e.g., 作成が必要な書類について) を適切な時間枠内に利用可能な形式で受け取れる場合にのみ可能となる. これにはどの Identity Evidence が必要となるかを正確にユーザーに伝えることも含まれる. ユーザーは IAL や当該 Identity Evidence が “fair”, “strong”, “superior” のどれに当てはまるかなどについては一切知る必要はない. 一方で組織は特定のシステムに Access するためにどの IAL が必要かを知っている必要がある.

ユーザーが Enrollment プロセスを進めるかどうか, およびその Session に何が必要になるかについて, 情報に基づいた判断を下せるようにするには, ユーザーに以下の項目を提供すること.

- 各ステップで何が期待されるかなど, プロセス全体についての情報.
- ユーザーがそれに応じて計画を立てられるよう, 予想される時間枠についての明確な説明.
- ユーザーに価値命題を理解させるための, Identity Proofing の必要性とメリットに関する説明.
- Enrollment 料金が発生する場合は, その額と受け入れ可能な支払い方法についての情報. より多種多様な支払い方法を許容することで, ユーザーは好みの支払い方法を選ぶことができる.
- ユーザーの Enrollment Session が対面なのか Remote チャネル越しの対面なのか, およびユーザーに選択肢があるかについての情報. 利用可能な Session の選択肢についてのみ情報を提供すること.
  - ユーザーが場所に関する選択肢を持っているかや, 対面ないし Remote チャネル越しの対面 Session に関する必要なロジスティック情報など, 場所に関する情報. 紛失や盗難への被害が増えるため, ユーザーは Identity Evidence を特定の公共空間 (e.g., 銀行 v.s. スーパーマーケット) に持っていくのを嫌がる可能性があることに注意すること.
  - Remote Session に対する技術要件 (e.g., Internet Access 要件) に関する情報.
  - 待機時間を最小限に抑えるために, 対面や Remote チャネル越しの対面での Identity Proofing Session の予約を可能にする. 予約なしでの来場が可能な場合は, 予約がない場合に待ち時間がより長くなる可能性がることをユーザーに明確に伝える.
    - Enrollment Session の予約, リマインダーの設定と, 予約の変更方法に関する明確な手順を伝えること.
    - 予約のリマインダーを提供し, ユーザーが好みのリマインダー形式 (e.g., 郵便, ボイスメール, Email, テキストメッセージ) を指定できるようにすること. ユーザーには, 日付, 時刻, 場所, 必要な Identity Evidence に関する記述などが必要である.
- 利用可能かつ必要な Identity Evidence および Attribute に関して, それぞれが任意か必須か, 完全な Identity Evidence 一式を提供しない場合の影響についての情報. ユーザーは具体的な Identity Evidence の組み合わせ, およびそれぞれの Identity Evidence に関する要件 (e.g., 出生証明書には捺印が必要) についての情報が必要である. 必要な Identity Evidence を取得することが潜在的に困難な可能性もあるため, これは特に重要である.
  - 可能であれば, 必要な Identity Evidence の取得を容易にするツールを実装する.
  - ユーザーに, 未成年や独特なニーズを持つ人々に対する特別な要件を知らせる. 例えば, 公証人, 法定後見人, その他の本人の代理権を法的に証明できる個人などの Trusted Referee を利用する場合に必要な情報 (詳細は Section 5.3.4 を参照).
  - フォームが必要であれば
    - Enrollment Session 開始前および Session 中に記入式フォームを提示すること. ユーザーにプリンターへの Access を要求しないこと.
    - ユーザーがフォームに入力しなければならない情報量を最小化すること. フォームが長くなると, ユーザーは簡単にフラストレーションを感じ, エラーを発生させがちである. 可能であれば事前にフォームを埋めておくこと.

9.3 Enrollment and Proofing Session

Enrollment Session に特化したユーザビリティー上の考慮事項としては, 以下のような項目が挙げられる.

- ユーザーに Enrollment Session 開始時に Enrollment Session の手順についてリマインドすること. ユーザーが事前準備段階でそれらを覚えてくることを期待しないように. Enrollment Session が事前準備の直後に開始されない場合, Proofing および Enrollment フェーズ完了にかかる典型的時間枠を明示的にリマインドすることが特に重要である.
  - 対面ないしは Remote チャネル越しの対面でリスケジューリングできるようにすること.
  - 可能な場合は, 利用可能かつ必要な Identity Evidence のチェックリストを提供し, Enrollment コードを含め, ユーザーが Enrollment Session を進めるのに必要な Identity Evidence を確実に持っているようにすること.
  - どの情報が破棄され, どの情報が将来のフォローアップ Session のために保管され, どの Identity Evidence が将来の Session を完了させるために必要となるかをユーザーに通知すること. 理想的には, ユーザーは Identity Proofing Session を途中で終了させるか選択でき

ることが望ましい.
    - 事前の Identity Verification の経験によりユーザーはすでに何らかの期待を持っている可能性があることから, ユーザーに Enrollment Session の結果に関する想定を伝えること (e.g., 運転免許証が対面で手渡される, パスポートが郵送で送られる).
    - ユーザーが Authenticator を Enrollment Session 成功後即時に渡されるのか否か, Authenticator を受け取るための予定を立てなければならないのか, Authenticator を郵送で受け取ればいいのか, またいつ Authenticator が受け取れると期待すれば良いかなどを明確にすること.

- Enrollment Session 中には, CSP がどのデータを記録するかなど, Identity Proofing 時にユーザーに明示的に通知を行うべきいくつかの要件が課されることになる (通知要件の詳細については Section 4.2. と Section 8. を参照). 4.2 の要件 (5) に従って, CSP がユーザーに追加の Attribute に関する同意を求めたり, Attribute を Identity Proofing, Authentication, Authorization, Attribute Assertion 以外の目的で利用することに同意を求めたりすると, そういった行為がユーザーの予期しないことであったり不快感を感じさせるかもしれない. ユーザーがそれらに対してメリットを理解できず, 余計なリスクを感じる場合, ユーザーは同意してプロセスを進めることを嫌がったりためらったりするかもしれない. 追加の要件に関して, ユーザーに明確な通知を行うこと.
- ユーザビリティー視点では KBV は非常に問題が多いため, KBV の利用は避けること. 人間の記憶力には限界があるため, KBV はエラーを引き起こしたりユーザーにフラストレーションを抱かせがちである. KBV を利用する場合は, 以下のユーザビリティー上の考慮事項に従うこと.
    - ユーザーが正しく回答できるよう, KBV の質問には関連性とコンテキストを持たせるべきである.
    - KBV の質問は明確な言い回しにすること. あいまいな表現はユーザーのエラーにつながる可能性がある. 例えば, ユーザーに社会保障残高について質問する場合, 社会保障講座の変動を考慮し期間を明確に指定すること.
    - KBV の質問をするまえに, ユーザーに以下を知らせること.
        - 許容される試行回数と残りの試行回数.
        - KBV の質問が, 次の試行において変化するであろうこと.
        - KBV Session 中, タイムアウト前にインアクティブ状態でタイムアウトが近いことを警告すること.
- Enrollment コードが発行される場合.
    - 事前に Enrollment コードが送られることを, その到着予想時期, コードの有効期間, 送付方法 (e.g., 郵送, SMS, 固定電話, Email) とともにユーザーに通知すること.
    - Enrollment コードをユーザーに送付する際は, その利用手順と有効期限を添えること. 特に Section 4.4.1.6 にあるように有効期間が短い場合, この情報は特に重要である.
    - QR コードなどの機械可読光学ラベルを発行する場合 (Section 4.6. 参照), どうすれば QR コードをスキャンできるかについての情報も添えること (e.g., 利用可能な QR コードアプリケーション).
    - Enrollment コードが期限切れしたり使用前に紛失したりすると, Enrollment プロセスを再び繰り返す必要があることをユーザーに知らせること.
    - 全てのユーザーがこのレベルの技術を使いこなせるわけではないため, 代替オプションをユーザーに提供すること. 例えば, ユーザーはこのアプローチに必要な技術を持ち合わせていないかもしれない.
- Enrollment Session 終了時には以下のようにすること.
    - Enrollment が成功した場合は, ユーザーに成功した Enrollment に関する確認と次のステップに関する情報を送ること (e.g., いつどこで Authenticator を受け取るべきかや, いつ Authenticator が郵送されるかなど).
    - Enrollment が途中で終了 (ユーザーが完全な Identity Evidence セットを持っていなかった, ユーザーがプロセス中断を選択した, Session がタイムアウトしたなど) した場合は, ユーザーに以下を伝えること.
        - どの情報が破棄されるか.
        - もしあれば, どの情報が将来のフォローアップ Session のために保持されるか.
        - どれくらいの期間その情報が保持されるか.
        - 将来の Session ではどの Identity Evidence を持ってくる必要があるか.
    - Enrollment が失敗した場合は, ユーザーに代替の Enrollment Session タイプについての明確な説明を提供すること. 例えば, Remote Proofing を完了できないユーザーに対面の Proofing を提供するなど.
- ユーザーが Enrollment Session 中に Authenticator を受け取る場合は, ユーザーに Authenticator の利用と保管に関する情報を提供すること. 例えば, 利用手順 (特に初回利用時や初期化時に特別な要件がある場合), Authenticator の有効期限, Authenticator の保護方法, Authenticator を紛失したり盗まれた場合の対応方法など.

- 対面の Proofing, および Remote の Enrollment Session 越しに行われる対面の Proofing のどちらにおいても, 追加のユーザビリティー上の考慮事項が適用される.
    - Enrollment Session 開始時に, オペレーターや係員は自身の役割をユーザーに説明すること (e.g., オペレーターないし係員は, Enrollment Session をとおしてユーザーに付き添うのか, 静かに観察し必要な時だけインタラクションを行うのか).
    - Enrollment Session 開始時に, ユーザーに Session 中に離席してはならないこと, Session をとおして彼らのアクションが可視でなければならないことを伝えること.
    - Enrollment Session 中に Biometrics が収集される場合は, その収集プロセスを完了させる手順についてユーザーに明確に説明すること. この情報はプロセス直前に提供されることが最も望ましい. その場にいるオペレーターからの修正フィードバックが可能な口頭での説

明が, 最も効果的である (e.g., Biometrics センサーがどこにあるか, いつ開始されるか, どのようにセンサーとインタラクションすべきか, いつ Biometrics の収集が完了するか).

- Remote Identity Proofing はオンラインで行われるため, 一般的な Web 上のユーザビリティー原則に従うこと. 以下に例を挙げる.
  - ユーザーが Enrollment プロセスを通過できるようにユーザーインターフェースを設計すること.
  - ユーザーが記憶しなければならないことを減らすこと.
  - インターフェースを一貫したものにすること.
  - 順序づけられたステップには明確にラベルをつけること.
  - 開始ポイントを明確にすること.
  - 多様なプラットフォームやデバイスサイズをサポートするように設計すること.
  - ナビゲーションを, 一貫性があり発見しやすく辿りやすいものにすること.

9.4 Post-Enrollment

Post-Enrollment とは, Enrollment 直後かつ Authenticator 通常利用前のステップを指す (Authenticator 通常利用と断続的イベントに関するユーザビリティー上の考慮事項については, SP800-63B (sp800-63b.html) Section 10.1-10.3 を参照). 上述のように, ユーザーは Enrollment Session 終了時に Authenticator の配送 (もしくは受け取り) 手段に関して知らされている.

Post-Enrollment に関するユーザビリティー上の考慮事項には以下のようなものがある.

- ユーザーの Authenticator 到着までの待ち時間を最小化すること. 待ち時間が短いほど, ユーザーはすぐに情報システムとサービスに Access できる.
- Authenticator を受け取るために物理的にある場所に行く必要があるかどうかを知らせること. 既出の予約とリマインダーに関するユーザビリティー上の考慮事項はここでも適用される.
- Authenticator と共に, Authenticator の利用と管理に関する情報も提供すること. これには, 利用手順 (特に初回利用時や初期化時に特別な要件がある場合), Authenticator の有効期限, Authenticator の保護方法, Authenticator を紛失したり盗まれた場合の対応方法などが含まれる.

10 References

This section is informative.

10.1 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).

[COPPA] *Children's Online Privacy Protection Act of 1998 ("COPPA")*, 15 U.S.C. 6501-6505, 16 CFR Part 312, available at: https://www.law.cornell.edu/uscode/text/15/chapter-91 (https://www.law.cornell.edu/uscode/text/15/chapter-91).

[EO 9397] Executive Order 9397, *Numbering System for Federal Accounts Relating to Individual Persons*, November 22, 1943, available at: https://www.ssa.gov/foia/html/EO9397.htm (https://www.ssa.gov/foia/html/EO9397.htm).

[DMF] National Technical Information Service, *Social Security Death Master File*, available at: https://www.ssdmf.com/Library/InfoManage/Guide.asp?FolderID=1 (https://www.ssdmf.com/Library/InfoManage/Guide.asp?FolderID=1).

[E-Gov] *E-Government Act of 2002* (includes FISMA) (P.L. 107-347), December 2002, available at: http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf (http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf).

[FBCACP] *X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA)*, Version 2.30, October 5, 2016, available at: https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/FBCA_CP.pdf (https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/FBCA_CP.pdf).

[FBCASUP] *FBCA Supplementary Antecedent, In-Person Definition*, July 16, 2009.

[FEDRAMP] General Services Administration, *Federal Risk and Authorization Management Program*, available at: https://www.fedramp.gov/ (https://www.fedramp.gov/).

[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).

[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).

[Privacy Act] *Privacy Act of 1974* (P.L. 93-579), December 1974, available at: https://www.justice.gov/opcl/privacy-act-1974 (https://www.justice.gov/opcl/privacy-act-1974).

[Red Flags Rule] 15 U.S.C. 1681m(e)(4), Pub. L. 111-319, 124 Stat. 3457, *Fair and Accurate Credit Transaction Act of 2003*, December 18, 2010, available at: https://www.ftc.gov/sites/default/files/documents/federal_register_notices/identity-theft-red-flags-and-address-discrepancies-under-fair-and-accurate-credit-transactions-act/071109redflags.pdf (https://www.ftc.gov/sites/default/files/documents/federal_register_notices/identity-theft-red-flags-and-address-discrepancies-under-fair-and-accurate-credit-transactions-act/071109redflags.pdf).

[Section 508] Section 508 Law and Related Laws and Policies (January 30, 2017), available at: https://www.section508.gov/content/learn/laws-and-policies (https://www.section508.gov/content/learn/laws-and-policies).

10.2 Standards

[Canada] Government of Canada, *Guideline on Identity Assurance*, available at: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=30678&section=HTML (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=30678&section=HTML).

[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).

10.3 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 e-authentication.

[SP 800-53] NIST Special Publication 800-53 Revision 4, *Recommended Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 (updated January 22, 2015), https://doi.org/10.6028/NIST.SP.800-53r4 (https://doi.org/10.6028/NIST.SP.800-53r4).

[SP 800-63-3] NIST Special Publication 800-63-3, *Digital Identity Guidelines*, June 2017, https://doi.org/10.6028/NIST.SP.800-63-3 (https://doi.org/10.6028/NIST.SP.800-63-3).

[SP 800-63B] NIST Special Publication 800-63B, *Digital Identity Guidelines: Authentication and Lifecycle Management*, June 2017, https://doi.org/10.6028/NIST.SP.800-63b (https://doi.org/10.6028/NIST.SP.800-63b).

[SP 800-63C] NIST Special Publication 800-63C, *Digital Identity Guidelines: Assertions and Federation*, June 2017, https://doi.org/10.6028/NIST.SP.800-63c (https://doi.org/10.6028/NIST.SP.800-63c).

[SP 800-157] NIST Special Publication 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials*, December 2014, http://dx.doi.org/10.6028/NIST.SP.800-157 (http://dx.doi.org/10.6028/NIST.SP.800-157).