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

NIST Special Publication 800-63C

Digital Identity Guidelines (翻訳版)

Federation and Assertions

Paul A. Grassi
Justin P. Richer
Sarah K. Squire
James L. Fenton
Ellen M. Nadeau

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.800-63c

COMPUTER SECURITY

National Institute of Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-63C

Digital Identity Guidelines

Federation and Assertions

Paul A. Grassi Ellen M. Nadeau *Applied Cybersecurity Division* *Information Technology Laboratory*	James L. Fenton *Altmode Networks* *Los Altos, Calif.*
Justin P. Richer Sarah K. Squire *Bespoke Engineering* *Billerica, Mass.*	
Privacy Authors: Naomi B. Lefkovitz *Applied Cybersecurity Division* *Information Technology Laboratory* Jamie M. Danker *National Protection and Programs Directorate* *Department of Homeland Security*	**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.800-63c

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.

National Institute of Standards and Technology Special Publication 800-63C
Natl. Inst. Stand. Technol. Spec. Publ. 800-63C, 48 pages (June 2017)
CODEN: NSPUE2

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

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

This document and its companion documents, SP 800-63, SP 800-63A, and SP 800-63B, provide technical and procedural guidelines to agencies for the implementation of federated identity systems and for assertions used by federations. This publication supersedes corresponding sections of SP 800-63-2.

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 use of federated identity and the use of assertions to implement identity federations. Federation allows a given credential service provider to provide authentication and (optionally) subscriber attributes to a number of separately-administered relying parties. Similarly, relying parties may use more than one credential service provider.

Keywords

assertions; authentication; credential service provider; digital authentication; electronic authentication; electronic credentials; federations.

Acknowledgements

The authors gretefully acknowledge Kaitlin Boeckl for her artistic graphics contributions to all vulumed 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), Kat Megas and Ben Piccarreta from NIST, and Christine Abruzzi and Danna Gabel O'Rourke from Deloitte & Touche LLP.

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. 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.

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.

本リコメンデーションと付随ドキュメント SP 800-63 (sp800-63-3.html), SP 800-63A (sp800-63a.html), SP 800-63B (sp800-63b.html) では, Credential Service Provider (CSP) が Digital Authentication を実装する際の技術的ガイドラインを示す.

本ドキュメント SP 800-63C では, Federated Identity システムにおける Identity Provider (IdP) と Relying Party (RP) に対する要件を示す. Federation を利用すると, ある一つの IdP が, 独立して個別管理された複数の RP に対して, Assertion を通じて, Authentication と (オプションで) Subscriber の Attribute を提供することができる. 同様に RP が複数の IdP を利用することもできる.

2 Introduction

This section is informative.

Federation は Network 接続されたシステム間で Authentication および Subscriber Attribute の情報を伝達可能にするプロセスです. Federation シナリオでは Verifier ないし CSP は Identity Provider / IdP と呼ばれ, RP は IdP が提供する情報を受け取り利用する主体となる.

Federated Identity システムは, 上記タスクを完遂するために Assertion を利用する. Assertion は, IdP から RP に当てた Subscriber に関する情報を含んだステートメントである. Federation 技術は, 一般的に RP と IdP が異なる主体であり, 異なる管理下にある場合に利用される. RP は Assertion に含まれる情報を利用して Subscriber を識別し, RP が管理下に置くリソースに Subscriber が Access する際の Authorization 決定を行う. Assertion は通常 Subscriber の識別子を含み, 過去の RP とのインタラクションと Subscriber を紐づけることを可能にする. Assertion はさらに Attribute Value や Attribute Reference を含み, RP での Authorization 決定の際に Subscriber についてのより詳しい特徴を伝えることもある. より大規模な Federation プロトコルにおいては, Attribute が Assertion の外でやり取りされることもある. こういった Attribute Value や Attribute Reference は, Attribute Based Access Control (ABAC) における Access 権限の決定に使われたり, トランザクションを促進 (e.g., 配送先住所) したりする.

Federated Identity シナリオでは, Subscriber は RP に対して直接 Authenticate するわけではない. その代わり, Federation プロトコルを定義し, 通常は RP からのリクエストに応じたレスポンスとして, IdP が Subscriber に紐づいた識別子に対する Assertion を生成する手段をもうける. IdP は (SP 800-63B, Section 7 (sp800-63b.html#sec7) に述べた Session 管理を使うかもしれないが) Subscriber を責任を持って Authenticate する. このプロセスにより, Subscriber は個々の RP に対して独立した Credential を所有・管理することなく, 複数の RP からサービスを受けることができる. また *Single Sign On* も可能となり, Subscriber はひとたび IdP に対して Authenticate すれば, それ以降複数の RP からサービスを受けることもできる.

Federation には, セキュリティーとプライバシーに関する繊細な要件があり, 注意深い考慮を必要とする, 比較的複雑なマルチパーティープロトコルが必要である. 特定の Federation 構造を評価する際は, 構成要素間のインタラクションに分解すると有益かもしれない. 一般的に, Subscriber と IdP の間の Authentication は SP 800-63B で述べた Authentication 方式に基づいて行われ, IdP と RP の間のインタラクションは SP 800-63A で述べた手順により確立された Attribute およびその他の Self-asserted Attribute を伝達するものとなる. したがって, 本ドキュメントで提示される多くの要件は, これら2つのドキュメントの該当する要件と何らかの関係を有す.

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. Federation Assurance Level (FAL)	Normative
5. Federation	Normative
6. Assertion	Normative
7. Assertion Presentation	Normative
8. Security	Informative
9. Privacy Considerations	Informative
10. Usability Considerations	Informative
11. Examples	Informative
12. References	Informative

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 Federation Assurance Level (FAL)

This section is normative.

本セクションでは, 許容可能な Federation Assurance Level, FAL を定義する. FAL はある Transaction において Assertion を構成および保護するための要件について述べたものである. これらのレベルは, ある Transaction において RP が要求することもあれば, RP と IdP との間の設定で必要とされることもある.

すべての Assertion は Section 4 に述べるように Federation プロトコルと共に用いなければならない (SHALL). すべての Assertion は Section 6 に詳説する要件に従わなければならない (SHALL). すべての Assertion は Section 7 に述べるいずれかの方法で提示されなければならない (SHALL). 多様な Federation 実装パターンがありうるが, FAL はよりセキュアな構築オプションを示す明確な推奨事項を提供することを意図している. FAL の表に無いさまざまな側面がありうるが, それらは本 Vol. の扱うところではない. 最適な FAL の詳しい選択方法については SP 800-63 Section 6.3 (sp800-63-3.html#FAL_CYOA) を参考のこと.

本表は各 FAL ごとに異なる要件を示す. 一連の各レベルは, より低いレベルのすべての要件を含み, 満たしている. プロキシを介した Federation は, プロキシされる Transaction の中で最も低いレベルとなるものとする (SHALL).

Table 4-1 Federation Assertion Levels

FAL	Requirement
1	Bearer assertion, signed by IdP.
2	Bearer assertion, signed by IdP and encrypted to RP.
3	Holder of key assertion, signed by IdP and encrypted to RP.

例えば, FAL1 は特に機能追加の無い OpenID Connect Basic Client プロファイルや Security Assertion Markup Language (SAML) Web SSO Artifact Binding プロファイルに相当する. FAL2 は, それに加え Assertion (e.g., the OpenID Connect ID Token ないしは SAML Assertion) に対する RP の公開鍵による暗号化を要求する. FAL3 では, FAL2 のすべての要件に加え, Subscriber が暗号論的に Assertion に紐づく鍵の所有証明を行う (e.g., Cryptographic Authenticator を利用) 必要がある. FAL3 で新たに登場した鍵は Subscriber が IdP に対して Authenticate する際に利用する鍵と同一でなくてもいい.

RP のリクエストやプロトコルの要件に関わらず, RP は Federation プロトコルにおいて提示される Assertion の性質を観察するだけで, 容易に利用している FAL を知ることができる. したがって RP は, 特定の Authentication Transaction において受け入れる FAL を決定し, 当該 Transaction が FAL 要件を満たすことを保証する責任がある.

RP が Section 7.2 にある Front-channel 提示手法 (e.g., OpenID Connect Implicit Client プロファイルや SAML Web SSO プロファイル) を用いている場合, Assertion に含まれる情報が意図した RP をのぞく Transaction 中のブラウザやその他の主体に漏洩することを防ぐため, FAL2 以上が必要となる (SHALL).

さらに IdP は, SP 800-53 に定義されている Moderate ないしは High 基準のセキュリティー制御やそれに相当する連邦政府標準 (e.g., FEDRAMP) や業界標準から, (制御強化を含む) 適切に適合したセキュリティー制御を採用しなければならない (SHALL).

4.1 Key Management

どの FAL においても, IdP は Assertion を Approved Cryptography による署名および鍵で保護し, RP がその他の RP に対して IdP になりすますことができないよう保証しなければならない (SHALL). Assertion が Asymmetric Key を使った Digital Signature により保護されている場合, IdP は同じ Public Key と Private Key のペアを複数の RP に対する署名に利用することができる (MAY). IdP は, 自身の Public Key を, HTTPS で保護された周知の URL を通じてなど, 検証可能な形で公開することもできる (MAY). Assertion が Shared Key を用いた MAC によって保護されている場合, IdP は RP ごとに異なる Shared Key を使わねばならない (SHALL).

政府が運営する AAL2 での Authentication を行う IdP と AAL3 での Authentication を行うすべての IdP は, FIPS 140 Level 1 以上の手段で Assertion の署名および暗号化に使う鍵を保護しなければならない (SHALL).

4.2 Runtime Decisions

Federate するという事実をもって情報を提供する許可を得たと解釈してはならない (SHALL NOT). Authentication を行うかどうかや Attribute を提供するかどうかは, ホワイトリストやブラックリスト, Authorized な主体によるランタイムでの決断などによって決定されることもある.

IdP は RP のホワイトリストを作成し, そこに含まれる RP に対しては Subscriber によるランタイムでの決断なしに IdP による Authentication 結果や Attribute を受け取れるようにすることもできる (MAY). IdP のホワイトリストに含まれるすべての RP は, SP 800-63 スイートの規定と要件に従わなければならない (SHALL). IdP は, Section 9.2 にあるように, Subscriber がホワイトリストを確認可能にするものとする (SHALL). IdP は RP のブラックリストを作成し, そこに含まれる RP に対しては Subscriber からの要求があっても IdP による Authentication 結果や Attribute を受け取れないようにすることもできる (MAY). ホワイトリストにおいてもブラックリストにおいても, 利用する Federation プロトコルごとに, RP はドメインや十分にユニークな識別子を用いて識別されることとなる. ホワイトリストにもブラックリストにも含まれない RP はグレーゾーンに配置し, そういった RP に対しては Authorized な主体によるランタイムでの決断に基づいた処理を行うこととする (SHALL). ここでいう Authorized な主体とは, 通常 Subscriber を指す. IdP はある RP に対する Subscriber の Authorization の決定を記憶してもよい (MAY). ただしその場合 IdP は Subscriber が記憶済 Access を将来無効化できるようにすること (SHALL).

RP は IdP のホワイトリストを作成し, そこに含まれる IdP に関しては Subscriber によるランタイムでの決断なしに Authentication 結果や Attribute を受け入れるようにしてもよい (MAY). RP のホワイトリストに含まれるすべての IdP は, SP 800-63 スイートの規定と要件に従わなければならない (SHALL). RP は IdP のブラックリストを作成し, そこに含まれる IdP に関しては Subscriber からの要求があっても Authentication 結果や Attribute を受け入れないようにすることもできる (MAY). ホワイトリストにおいてもブラックリストにおいても, 利用する Federation プロトコルごとに, IdP はドメインや十分にユニークな識別子を用いて識別されることとなる. ホワイトリストにもブラックリストにも含まれない IdP はグレーゾーンに配置し, そういった IdP に対しては Authorized な主体によるランタイムでの決断に基づいた処理を行うこととする (SHALL). ここでいう Authorized な主体とは, 通常 Subscriber を指す. RP はある IdP に対する Subscriber の Authorization の決定を記憶してもよい (MAY). ただしその場合 IdP は Subscriber が記憶済 Access を将来無効化できるようにすること (SHALL).

たとえ相互にホワイトリストに含まれていたとしても, Section 5.2 に記載する目的以外では, Subscriber に関する情報を IdP と RP の間でやりとりしてはならない (SHALL NOT).

Authorize なしでのセンシティブ情報の漏洩リスク (e.g., ショルダーサーフィング) を軽減するため, IdP はデフォルトではセンシティブ情報をマスクして Subscriber に提示すること (SHALL). IdP は一時的にそれらのマスクを外す手段を Subscriber に提供し, Subscriber が全体の値を閲覧できるようにすること (SHALL). IdP は Subscriber の苦情や問題 (e.g., Subscriber によって Attribute Value が不正確であることが発見される) の是正のための有効な手段を提供すること (SHALL). マスキングと是正についての詳細については, Section 10 のユーザビリティーの考察を参照のこと.

Subscriber がランタイムでの決断を行う場合, Subscriber は明示的な通知を受け取り, Subscriber の Attribute が RP に送信される前に肯定的な確認を行えなければならない (SHALL). 最低限 Section 9.2 に従って, 最も効果的な通知を行える立場にあり, 確認を得ることになる主体が, 通知を行うべきである (SHOULD). もし利用するプロトコルでオプショナルな Attribute が利用可能であれば, Subscriber はそれらの Attribute を RP に提供するか否かの選択肢を与えられなければならない (SHALL). IdP はなんらかの記憶メカニズムを採用し, 同一 RP に対して同一 Attribute を再送するようにしてもよい (MAY).

5 Federation

This section is normative.

Federation プロトコルでは, Figure 5-1 に示すように Subscriber, IdP, RP の3者の関係が構築される. 各プロトコルによってどのタイムングでどの主体の間でどんな情報がやりとりされるかは異なる. Subscriber は通常ブラウザーを介して IdP と RP の両方とコミュニケーションをとる. RP と IdP の間のコミュニケーション方法は2通りある.

- *Front Channel*, Subscriber を介したリダイレクトを通じたコミュニケーション
- *Back Channel*, Subscriber を介さず RP と IdP の直接のコネクションを通じたコミュニケーション

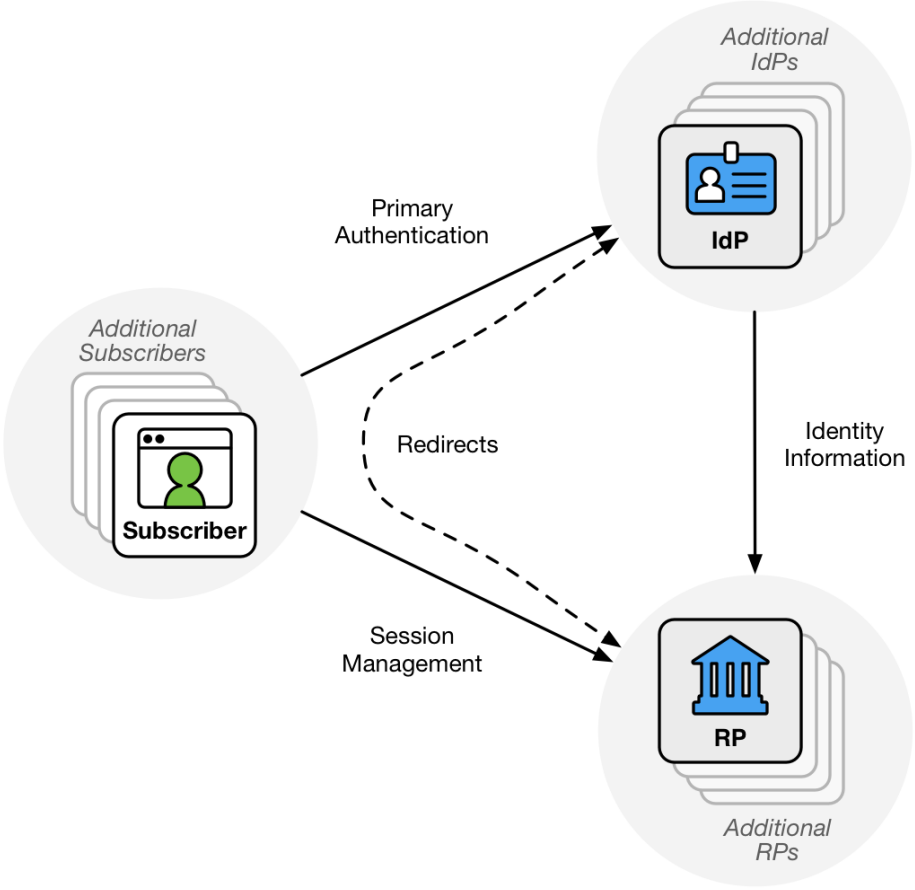

Figure 5-1 Federation

Subscriber は IdP に対して Authenticate し, Authentication イベントの結果が RP に対して Network 経由で提示される. この Transaction において, IdP は SP 800-63B (sp800-63b.html) にあるように Credential の Verifier として振る舞う. IdP はこのプロセスにおいて Subject に関する Attribute ステートメントを作成することも可能である. Attribute と Authentication イベントの情報は, Section 6 にあるように Assertion を通じて RP に伝送される. さらなる Attribute が Authorized Credential で保護されたセカンダリープロトコルを通じてやりとりされることもある (MAY).

5.1 Federation Models

Authentication サービスを提供する IdP とそれを利用する RP は Federation の参加者として知られている. IdP の視点から見れば, Federation は自身がサービス提供をする RP から構成される. RP の視点から見れば, Federation は自身が利用する IdP から構成される. 本セクションでは, 今日使われている一般的 Identity Federation モデルに対する要件を概観する. 各モデルにおいて, Federation 参加者間の関係性が確立される.

5.1.1 Manual Registration

手動の Registration モデルでは, IdP と RP が手動で相互運用する相手に関する設定情報を用意する. IdP は明示的ホワイトリストによって RP を設定し, そこに含まれる RP に関しては Authentication Transaction 中で Authentication や Attribute に関する情報を受け取れるようにしてもよい (MAY). RP がホワイトリストに含まれない場合は, IdP はユーザー情報を提供する前に Authorized な主体によるランタイムでの決断 (Section 4.2 参照) を要求とすることとする (SHALL).

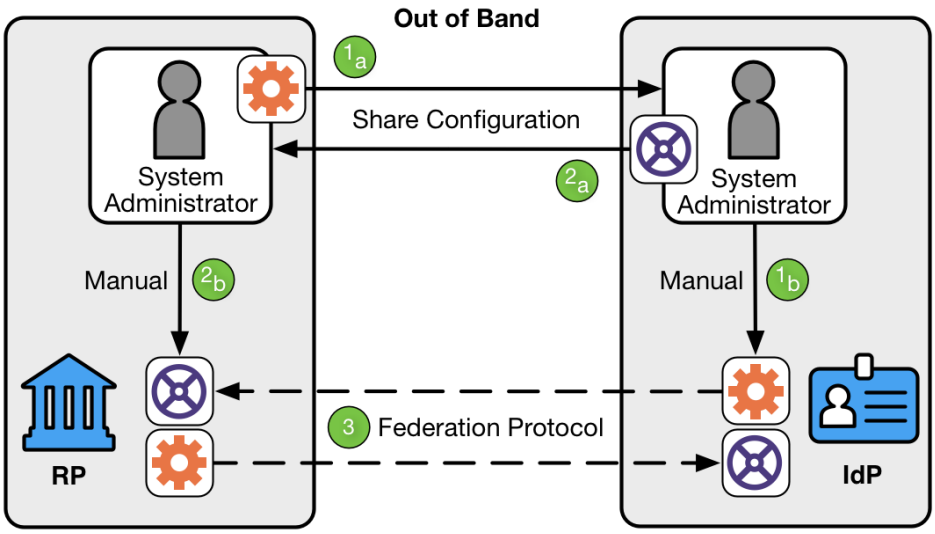

Figure 5-2 Manual Registration

Figure 5-2 に示す通り, 手動の Registration は以下の3ステップからなる.

1. RP のシステム管理者が RP の Attribute を IdP のシステム管理者に共有し, IdP のシステム管理者はその Attribute を RP に関連づける.
2. IdP のシステム管理者が IdP の Attribute を RP のシステム管理者に共有し, RP のシステム管理者はその Attribute を IdP に関連づける.
3. その後 IdP と RP は標準的 Federation プロトコルを使ってコミュニケーションする.

IdP と RP は, 自身を自身のオーソリティーとしてもよいし (MAY), Section 5.1.3 のようにオーソリティー権限を外部の主体に移譲してもよい (MAY).

鍵情報の伝送を必要とするプロトコルでは, Rigistration プロセスにおいてセキュアな方法で Federated な関係性の運用に必要な鍵情報を交換すること (SHALL). これには Shared Secret も Public Key も含まれる. この関係性を示すために利用される鍵が Symmetric Key である場合は, Federation 参加者ペア毎にユニークでなければならない (SHALL).

Federation の関係性に対して, 期待され許容される IAL および AAL についてのパラメーターを確立すること (SHALL).

5.1.2 Dynamic Registration

Federation の動的な Registration モデルでは, Transaction 実行時に Federation 参加者間でその関係性を取り決めるすることが可能である. このプロセスにおいて IdP と RP は, 手動 Registration (Section 5.1.1 参照) により手動でコネクションを確立することなく, 相互接続することができる. 動的 Registration をサポートする IdP は, 自身の設定情報 (動的 Registration のエンドポイント等) を取得可能にし, システム管理者の関与を最小化すること (SHALL).

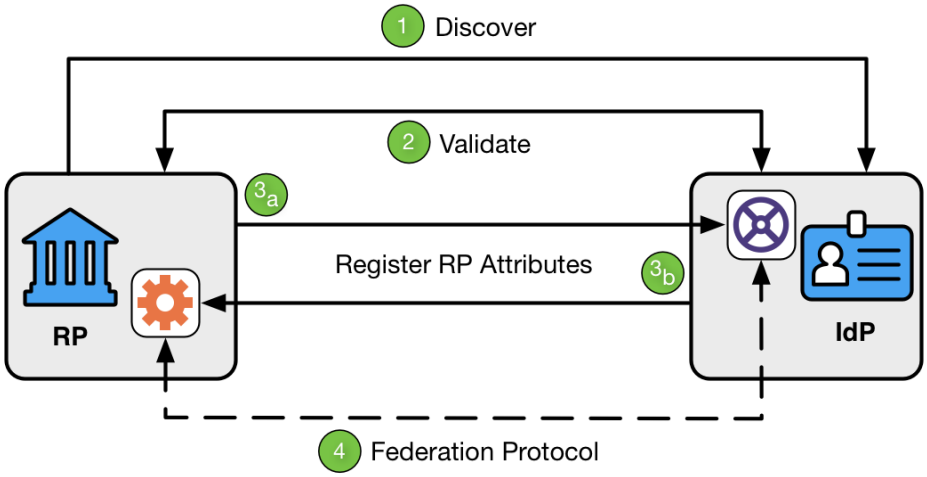

Figure 5-3 Dynamic Registration

Figure 5-3 に示す通り, 動的な Registration は以下の4ステップからなる.

1. 発見. RP は IdP の周知な場所に行き, IdP のメタデータを発見する.
2. 確認. RP と RP はお互いの正当性を確認する. これには鍵情報やメタデータ, Software Statement, その他の方法などが利用できる.
3. RP Attribute の登録. RP は自身の Attribute を IdP に送り, IdP はその Attribute を当該 RP に関連づける.
4. Federastion プロトコル. IdP と RP は標準の Federation プロトコルを使ってコミュニケーションする.

鍵情報の伝送を必要とするプロトコルでは, Rigistration プロセスにおいてセキュアな方法で Federated な関係性の運用に必要な鍵情報を交換すること (SHALL). これには Shared Secret も Public Key も含まれる. この関係性を示すために利用される鍵が Symmetric Key である場合は, Federation 参加者ペア毎にユニークでなければならない (SHALL).

IdP はユーザー情報を提供する前に Authorized な主体 (Subscriber 等) によるランタイムでの決断 (Section 4.2 参照) を要求とすることとする (SHALL). 動的 Registration を行う RP を受け入れる IdP は, そういった RP が利用できる Attribute やその他の情報のタイプを制限してもよい (MAY). 動的 Registration を利用可能な RP は, Identity 情報を受け入れる IdP を制限してもよい (MAY).

動的 Registration モデルの参加者は, しばしばお互いのことを事前に知らないことがある. 可能であれば, Federation 参加者が動的に登録した RP の Attribute のいくつかを暗号論的に検証できるよう, *Software Statement* により補強すべきである (SHOULD). Software Statement は RP ソフトウェアに関する Attribute を列挙したものであり, オーソリティー (IdP 自身, Section 5.1.3 にある Federation Authority, その他の信頼できる主体) により暗号論的に署名されている. この暗号論的に検証可能なステートメントにより, Self-asserted Attribute のみに頼る必要がなくなり, Federation 参加者間のコネクションを確立ないし向上させることができる. (RFC 7591 Section 2.3 にあるプロトコルにおける Software Statement の実装に関する詳しい情報がある)

5.1.3 Federation Authorities

一部の Federation 参加主体は, Federation の決定および主体間の関係性構築に関して, *Federation Authority* と呼ばれるオーソリティーに従う. このモデルでは, Federation Authority は Federation に参加する各主体に対して一定レベルの審査を実施し, 所定のセキュリティーおよび完全性基準を遵守しているかを検証するのが一般的である. もし審査を行う場合, 審査レベルは Federation のユースケースやモデルごとにユニークとなる. Figure 5-4 にはこの審査についての描写がある.

Federation Authority は, IdP が特定の IAL, AAL, FAL で運営することを承認する. この情報は, Figure 5-4 右にあるように, Relying Party によって利用され, どの Identity Provider が当該 RP の要件に合うかの判断材料となる.

Federation Authority は, 自身が有効化する Federated な関係性に関して, 期待され受入可能な IAL, AAL, FAL に関するパラメーターを規定すること (SHALL). Federation Authority は, Federation 参加者を個別に審査し, 期待されるセキュリティー, Identity およびプライバシー基準に準拠しているかを判断すること (SHALL).

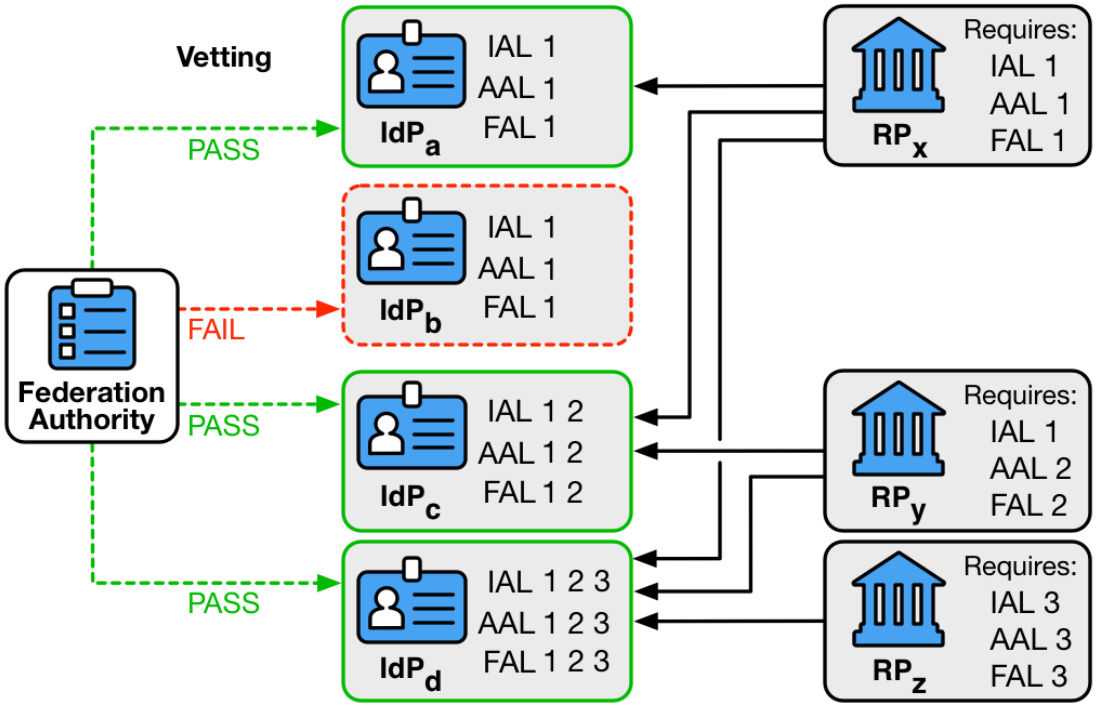

Figure 5-4 Federation Authority

IdP および RP の審査には, 最低限以下のような項目を確認すること (SHALL).

- IdP が生成した Assertion が Section 6 の要件に準拠しているか.
- RP が, Attribute データの保持, アグリゲーション, 第三者への開示などについて, IdP が求める要件に準拠しているか.
- RP と IdP の両システムが, Federation プロトコルの承認されているプロファイルを利用しているか.

Federation Authority は, IdP の設定データを公開したり RP 向けに Software Statement を発行するなど, メンバー間の技術的接続および設定プロセスを支援してもよい (MAY).

オーソリティーに管理された Federation は, ほとんどの場合シンプルなメンバーシップモデルを形成する. このモデルでは, ある主体が Federation に参加しているか否かのみを扱う. より洗練された Federation においては, 複数のメンバーシップ階層が設けられ, ある主体が他の主体に比べてより入念に審査されたかどうかを知ることができるようになっていることもある (MAY). IdP はある Subscriber の情報を一定以上の階層の RP にのみ受け渡すようにしてもよいし (MAY), RP はある情報を一定以上の階層の IdP からのみ受け入れるようにしてもよい (MAY).

5.1.4 Proxied Federation

Proxied Federation では, IdP と RP の通信は2者間の直接通信を妨げる形で仲介される. これを実現する方法は複数あるが, 共通事項として以下のような項目が挙げられる.

- 第三者が Federation Proxy (または *Broker*) として動作する.
- 通信を振り分けるノードの Network が存在する.

Proxy を利用する場合, 当該 Proxy は一方で IdP として振る舞い, もう一方では RP として振る舞う. したがって, IdP と RP に求められる全ての Normative 要件が, 当該 Proxy にも課せられる (SHALL).

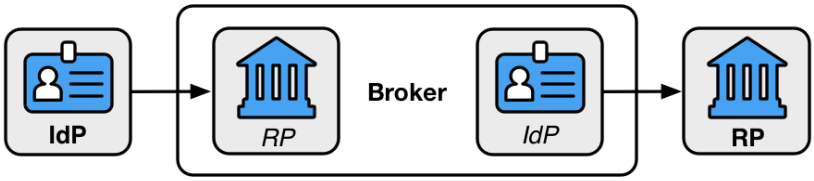

Figure 5-5 Federation Proxy

Proxied Federation モデルにはいくつかの利点がある. Federation Proxy においてインテグレーションのための共通インターフェースを提供することで, RP と IdP の技術的インテグレーションを単純化することができる. さらに, Proxy が RP と IdP を互いに効果的にブラインドことで, Subscriber のリストを相互に保護したい組織間でのビジネス上の機密性を実現することもできる. また, Proxy は Section 5.2 に述べるようにいくらかのプライバシーリスクを低減することもできる.

ブラインディング技術とその利用, 限界に関しては, Section 9.5 に詳しい.

5.2 Privacy Requirements

Federation には, それ以外では Transaction に関与しない第三者である IdP からの, 個人の Attribute の転送がつきものである. さらに Federation では, 潜在的に IdP が Subscriber の活動に関する広い視野を持つ. したがって, Federation には特別なプライバシー要件がある.

RP と IdP の間の通信は, Subscriber が Transaction を実行している IdP に明らかになりうる. 複数の RP と通信することで, IdP は Subscriber Transaction のプロファイルを作成することができる. これは Federation なしではなしえない. このアグリゲーションにより, Subscriber のトラッキングや, Subscriber のプライバシー上の利益に必ずしも一致しないプロファイル情報の利用が可能となりうる.

IdP は, ある RP における Subscriber の活動情報をいかなる主体にも開示してはならず, Federated Authentication とそれに関連する不正防止, 法律や法的手続きへの従属, ユーザーからの当該情報の送信を求める特定の要求への応答以外の目的で, Subscriber の情報を利用してはならない (SHALL NOT). IdP は, Section 6.3 に述べる Pairwise Pseudonymous Identifier やプライバシーを強化する暗号化プロトコルといった技術的手段を利用して, Unlinkability を提供したり Subscriber に対する行動トラッキングやプロファイリングを妨げるべきである (SHOULD).

IdP は, 例えば毀損した Subscriber アカウントの情報などのSubscriber の活動情報を, セキュリティー目的で Federation 範囲内の他の RP に開示してもよい (MAY).

以下の要件は, 特に政府機関に適用される.

1. 機関は, 自身の Senior Agency Official for Privacy (SAOP) と協議し, Privacy Act の要件が, IdP として機能する機関か RP として機能する機関, またはその両方を起因として満たされるかを判断すべく分析を行うこととする (SHALL).
2. 機関は, 適用可能な場合, System of Records Notice (SORN) のカバレッジを公表ないし割り出さなければならない (SHALL).
3. 機関は, 自身の SAOP と協議し, E-Government Act の要件が, IdP として機能する機関か RP として機能する機関, またはその両方を起因として満たされるかを判断すべく分析を行うこととする (SHALL).
4. 機関は, 適用可能な場合, Privacy Impact Assessment (PIA) のカバレッジを公表ないし割り出さなければならない (SHALL).

5.3 Reauthentication and Session Requirements in Federated Environments

Federated な環境では, RP は自身の Session を IdP の Session とは別に管理する. RP の Session は RP が IdP からの Federation プロトコルを処理するタイミングで開始される. Federated ログイン時に, Subscriber が IdP にすでに Session を持っていることもあり (MAY), その Session が RP に対する Authentication プロセス中で利用されることもある (MAY). IdP は IdP での最新の Authentication イベントの時刻に関する情報を伝達せねばならず (SHALL), RP は自身のアクセスポリシー決定にこの情報を利用しても良い (MAY). 利用する Federation プロトコルの性能によっては, IdP は RP が IdP による Subscriber の Re-authenticate を Federation リクエスト中で要求できるようにすべきである (SHALL).

Federated システムはその特徴として分散しているため, Subscriber は IdP と RP の Session を互いに独立して終了させることができる. RP は, Federated ログインができたからといって, Subscriber が IdP においてアクティブな Session を持っていると仮定してはならない (SHALL NOT). IdP は IdP における Subscriber Session の終了がダウンストリーム RP の任意の Subscriber Session に伝搬すると仮定してはならない (SHALL NOT).

Session Management 要件に関する詳細は SP 800-63B Section 7 (sp800-63b.html#sec7) を参照のこと.

6 Assertions

This section is normative.

Authentication 目的で利用される Assertion は, Federated Identity システム内で IdP から RP に伝搬される, Authenticated Subscriber に関するもしくは Authenticated Subscriber に紐づいた, Attribute Value や Attribute Reference のパッケージ化されたセットである. Assertion は Assertion Metadata, Subscriber に関する Attribute Value や Attribute Reference, RP が利用できるその他の情報 (制約や有効期限など) など, 多様な情報を含む. Assertion の第一の機能は RP に対してユーザーを Authenticate することであるが, Assertion 経由で伝搬される情報は RP により多様なユースケースで利用されうる. 例としては, Web サイトにおける Authorization やパーソナライゼーションなどが挙げられる. 本ガイドライン群は, 選択されたソリューションがここに含まれるすべての必須要件を満たす限り, RP のユースケースや Identity を Federate するためのプロトコルタイプやデータタイプに関しては制限しない.

Assertion は単一の Authentication イベントのみを表現することもあれば (MAY), Subscriber に関する Attribute Value や Attribute Reference を表現することもある (MAY).

すべての Assertion は, 以下にあげる Assertion Metadata を含むこととする (SHALL).

1. Subject: 当該 Assertion が指し示す主体の識別子. (i.e., Subscrier)
2. Issuer: Assertion を発行した IdP の識別子.
3. Audience: Assertion を利用することが想定される主体の識別子 (i.e., RP)
4. Issuance: Assertion が IdP に発行された日時を示すタイムスタンプ.
5. Expiration: Assertion の有効期限を示すタイムスタンプ. RP は有効期限が切れた Assertion を有効な Assertion として受け入れないこと (SHALL). (i.e., Assertion の有効期限切れであり, RP における Session の有効期限切れではない)
6. Identifier: 当該 Assertion 自身を識別するランダムでユニークな値. Attacker による以前の Assertion の再利用を防ぐために利用される.
7. Signature: IdP に紐づいた鍵の識別子や公開鍵を含んだ, Assertion 全体に対する Digital Signature もしくは Message Authentication Code (MAC).
8. Authentication Time: (可能であれば) IdP が Primary Authentication Event を通じて Subscriber を認証した日時を示すタイムスタンプ.

Assertion はさらに以下の情報を含んでもよい (MAY).

1. Key binding: Subscriber が保持する鍵の Public Key ないしは識別子であり, Section 6.1.2 にあるように当該 Assertion と Subscriber が保持する鍵 との Binding を証明するために使われる.
2. Attribute Value および Attribute Reference: Subscriber に関する情報.
3. Attribute Metadata: 一つ以上の Subscriber Attribute に関する追加の情報. NIST Internal Report 8112 [NISTIR 8112] に述べられているものなどが例として挙げられる.

Assertion は Authentication イベントが Assert された際の AAL と Identity Proofed Attribute (ないしはその Reference) が Assert された際の IAL を明記すべきである (SHOULD). もし明記がない場合, RP は当該 Assertion に対していかなる IAL, AAL も割り当ててはならない (SHALL NOT).

RP は Subject 識別子をグローバルにユニークであるものとして扱わないこと (SHALL). 代わりに, Assertion 中の Subject 識別子は, 通常 Assertion Issuer 管理下のネームスペースに所属している. これにより RP は異なる IdP から提示された Subject を誤ってまとめてしまうことなく, 複数の IdP と対話することができる.

Assertion は追加の Attribute を含むこともある (MAY). Section 7 は Assertion に Attribute を含めて提示する際のプライバシー要件を含んでいる. RP は, Assertion と一緒に発行された Authorization Credential を利用して, 別 Transaction で IdP から追加の Identity Attribute を取得してもよい (MAY). こういった追加の Attribute 取得能力は, Assertion を処理することと同等に扱ってはならない (SHALL NOT).

詳細は利用する Federation プロトコルによって様々であるが, Assertion は RP における単一のログインイベントのみを表すように利用されるべきである (SHOULD). RP が Assertion を利用したのちは, RP は Session Management (SP 800-63B Section 7 (sp800-63b.html#sec7)) 参照) を開始し, Assertion はそこに含まれる有効期限を超えて利用されてはならない (SHALL NOT). しかしながら RP における Session 有効期限は, Assertion 自体の有効期限よりも先に切れることもある (MAY). 詳細は Section 5.3 を参照のこと.

Assertion のライフタイムは発行時から有効期限までの間である. このライフタイムは, RP が Assertion を処理してから Subscriber に対してローカルのアプリケーション Session を払い出すまでに十分な長さである必要があるが, 必要以上に長くするべきではない. 長期間有効な Assertion は詐取やリプレイのリスクが高く, ライフタイムの短い Assertion の方がそういったリスクへの耐性を持つ. Assertion ライフタイムは RP 上の Session を制限するために利用してはならない (SHALL NOT). 詳細は Section 5.3 を参照のこと.

6.1 Assertion Binding

Assertion Binding は, Assertion と Subscriber の紐付けを行うのに, Assertion の Claimant が Assertion ないしは Assertion Reference 提示すれば十分か, Assertion が Subscriber に紐づいていることを示す追加の証明を RP が要求するか, という点に基づいて分類することができる.

6.1.1 Bearer Assertions

Bearer Assertion は, いかなる主体でも, Bearer の Identity の証明として提示することができる. もし Attacker が, Subscriber を示す正当な Assertion ないし Assertion Reference を詐取・偽造でき, 当該 Assertion ないし Assertion Reference を RP に提示することができれば, Attacker は RP において Subscriber になりすますことができる.

Bearer Assertion や Bearer Assertion Reference を所有しているだけでは, Subscriber になりすますには必ずしも十分ではないことに注意すること. 例えば Assertion が Back-channel Federation モデル (Section 7.1 参照) において提示される場合, Transaction 中でさらなる統制 (RP の識別や Assertion インジェクション対策など) が行われており, RP が不正なアクティビティーから保護されていることもある (MAY).

6.1.2 Holder-of-Key Assertions

Holder-of-Key Assertion は Subscriber に所持され Subscriber を表現する鍵への参照を含む. Holder-of-Key Assertion 中の鍵の参照は Subscriber を示すものであり, ブラウザー, IdP, RP など当該システム中のいかなる他の主体をも示すものではない. 鍵への参照は Assertion の Issuer によって Assert (ないしは署名) されていることに注意.

RP が Holder-of-Key Assertion を受け取ると, Subscriber は Assertion から参照された鍵を所有していることを直接 RP に証明する. Subscriber は IdP との間で鍵ベースの Authentication 方法を利用することもできるが, IdP 上の Primary Authentication と RP 上の Federated Authentication は独立したものとみなされ, 同じ鍵や関連した Session が利用されるとは想定されない.

Subscriber が RP に対して鍵所有証明を行うに際して, Claimant はさらに Assertion の正当な Subject であることをある程度の確からしさで証明することになる. Subscriber 向けに発行された Holder-of-Key Assertion に加え, そこから参照された鍵そのものを詐取する必要があるため, Attacker が詐取した Holder-of-Key Assertion を利用するのはより困難である.

Holder-of-Key Assertion には以下のすべての要件が適用される.

1. Subscriber は, Assertion 自体の提示に加えて, RP に対して鍵所有証明を行う必要がある (SHALL).
2. Subscriber が保持する鍵の参照を含み, 鍵所有証明がなされない場合, RP は当該 Assertion を Bearer Assertion とみなさなければならない (SHALL).
3. 所与の鍵への参照は, Assertion 内のその他の全ての情報と同レベルで信頼すること (SHALL).
4. Assertion には, Holder-of-Key による提示で利用する Private Key や Symmetric Key を, 暗号化せずに含めてはならない (SHALL NOT).
5. 当該鍵は Subscriber が IdP に Authentication する際に利用する鍵とは異なることもある (MAY).
6. 当該鍵は Symmetric Key でもいいし Private Key に紐づいた Public Key でもいい (MAY).
7. RP は Claimant が当該鍵を所有していることを IdP と連動して検証してもよい (MAY). これには, 暗号論的なチャレンジに対して Claimant が計算した署名や MAC を IdP に検証してもらう, などといった例が挙げられる.

6.2 Assertion Protection

Biding メカニズム (Section 6.1 参照) や Federation モデル (Section 5.1 参照) とは独立して, Assertion は, Attacker が有効な Assertion を偽造したり, 詐取した Assertion を全く異なる RP に対して再利用するといった攻撃を防ぐための一連の保護策を施さなければならない (SHALL). 必要な保護策は考慮されるユースケースの詳細に依存しているが, ここでは推奨される保護策を列挙する.

6.2.1 Assertion Identifier

Assertion は, 対象となる RP が一意に識別できる程度に, 十分ユニークでなければならない (SHALL). Assertion は Nonce, 発行日時, Assertion Identifier やそれらの組み合わせを含めたり, その他のテクニックによってこのユニーク性を達成することができる (MAY).

6.2.2 Signed Assertion

Assertion は IdP によって暗号論的に署名されること (SHALL). RP は, Issuer の鍵に基づいて各 Assertion の Digital Signature や MAC を確認すること (SHALL). 署名は, Assertion Identifier, Issuer, Audience, Subject および有効期限を含め, Assertion 全体をカバーすること (SHALL).

Assertion の署名は, Asymmetric Key を利用した Digital Signature か, RP と Issuer の間で共有される Symmetric Key を用いた MAC とすること (SHALL). 本目的のために IdP に利用される Shared Symmetric Key は, Assertion を送信する RP ごとに独立とし (SHALL), 通常は RP 登録時に確立される. Digital Signature の検証に用いる Public Key については, IdP がホストする HTTPS URL を通じてなど, セキュアな方法でランタイムに取得してもよい (MAY).

6.2.3 Encrypted Assertion

Assertion を暗号化する場合, IdP は RP の Public Key か Shared Symmetric Key を使って Assertion のコンテンツを暗号化すること (SHALL). 本目的のために IdP に利用される Shared Symmetric Key は, Assertion を送信する RP ごとに独立とし (SHALL), 通常は RP 登録時に確立される. 暗号化に用いる Public Key については, IdP がホストする HTTPS URL を通じてなど, セキュアな方法でランタイムに取得してもよい (MAY).

すべての Assertion の暗号化には Approved Cryptography を利用すること (SHALL).

Assertion がブラウザーなどの第三者を介してやりとりされる場合は, Assertion の暗号化を行うこと (SHALL). 例えば SAML Assertion は XML-Encryption により暗号化することができ, OpenID Connect ID Token は JSON Web Encryption (JWE) により暗号化することができる. IdP から直接 RP に渡される Assertion に関しては, 暗号化してもよい (MAY). 暗号化を行わない場合は Authenticated Protected Channel を介して送ること (SHALL).

> NOTE: Assertion Encryption は FAL2 と FAL3 で要求される.

6.2.4 Audience Restriction

Assertion には Audience Restriction テクニックを用い, RP が自身が Assertion 発行対象となっているか否かを判断できるようにすること (SHALL). すべての RP は, Assertion の Audience に自身の識別子が含まれているかチェックし, ある RP に対して生成された Assertion が他の RP に対してインジェクトされたりリプレイされないようにすること (SHALL).

6.3 Pairwise Pseudonymous Identifiers

状況によっては, IdP 上の Subscriber アカウントに対する共通の識別子を通じて, 複数の RP 間で当該 Subscriber が簡単にリンクされないようにすることが望ましい.

6.3.1 General Requirements

IdP が RP に対して生成する Assertion において Pairwise Pseudonymous Subject Identifier を利用する場合, IdP は Section 6.3.2 に述べるように各 RP に異なる識別子を生成すること (SHALL).

RP に対して Attribute を添えて Pairwise Pseudonymous Identifier を利用する場合は, 複数の RP が結託し, Identity Attribute をもとにシステム間で相関づけることで, Subscriber を Re-identify (再識別) することが可能かもしれない. 例えば2つの独立した RP が異なる Pairwise Pseudonymous Identifier によって識別される同一の Subscriber を観察しているとすると, 当該 RP たちは, それぞれが受け取る Assertion 中に Pairwise Pseudonymous Identifier と共に含まれる, 名前, メールアドレス, 物理アドレス, その他の識別に用いられる Attribute を比較することにより, 当該 Subscriber が同一人物であることを知るかもしれない. そういった相関づけはプライバシーポリシーによって禁じられるべきであり (SHOULD), Pairwise Pseudonymous Identifier は Attribute の相関づけに必要な管理努力を増大させることでこういったポリシーの有効性を高めることができる.

Proxied Federation モデルでは, IdP は Proxy によって Subscriber が Access しようとしている RP を知ることができない可能性があり, 最初の IdP が最後の RP に対して Pairwise Pseudonymous Identifier を生成できないこともあるので注意すること. そのような状況では, Pairwise Pseudonymous Identifier は通常 IdP と Federation Proxy の間で確立される. Proxy は IdP として機能し, ダウンストリームの RP に対して Pairwise Pseudonymous Identifier を提供することができる. プロトコルによっては, Identity プロトコルを機能させるため, Federation Proxy は Pairwise Pseudonymous Identifier をアップストリーム IdP から送られてくる関連する識別子と紐づける必要がある. そのようなケースでは, Proxy は同一の Subscriber を示す各 RP ごとの Pairwise Pseudonymous Identifier を判定し, トラックすることができる. Proxy は, Pairwise Pseudonymous Identifier とその他の識別子間のマッピングを第三者に開示したり, そのマッピング情報を Federated Authentication とそれに関連する不正防止, 法律や法的手続きへの従属, ユーザーからの当該情報の送信を求める特定の要求への応答以外の目的で利用してはならない (SHALL NOT).

6.3.2 Pairwise Pseudonymous Identifier Generation

Pairwise Pseudonymous Identifier には, Subscriber に関するいかなる識別情報も含めないようにすること (SHALL). また Subscriber を識別する情報への Access を持つ主体によって推測されないようにすること (SHALL). Pairwise Pseudonymous Identifier は, ランダムに生成し IdP が Subscriber に紐づけるようにしてもよく (MAY), Subscriber に関するその他の情報から不可逆で推測不可能な方法 (e.g., シークレット鍵を利用した鍵付きハッシュ関数を利用) により導出してもよい (MAY). 通常この識別子は, 対となるエンドポイント間 (e.g., IdP-RP) のみが知っており, 当該エンドポイント間のみで利用されることとする (SHALL). ただし IdP は以下の場合, RP の要求にしたがって, 複数の RP に同一の識別子を生成してもよい (MAY).

- 当該 RP 群が, セキュリティードメインや法的所有権を共有するなど, 運用上相関関係を持つ正当な理由があることを実証可能な関係性にある.
- 識別子を共有するすべての RP が, そのような方法で関連づけられることに同意している.

RP は, Privacy Risk Assessment を実施し, 共通の識別子を要求する場合のプライバシーリスクについて考慮すること (SHALL). プライバシー上の考慮点についての詳細は Section 9.2 を参照のこと.

IdP は意図した RP のみが相関関係にあることを保証すること (SHALL). さもないと悪意ある RP が不正に一連の相関関係にある RP になりすまし, 当該 RP 群に対して発行された Pseudonymous Identifier を知ることができてしまうかもしれない.

7 Assertion Presentation

This section is normative.

Assertion は IdP から RP に対して *Back-Channel* ないしは *Front-Channel* で提示される (MAY). それぞれのモデルにはトレードオフがあるが, どちらにおいても Assertion を正しく検証する必要がある. Section 5.1.4 にあるように, ある条件下では Federation を簡単にするため IdP と RP の間を Proxy した状態で Assertion をやりとりすることもある.

IdP は RP が明示的に要求した Attribute のみを送信することとする (SHALL). また RP は Privacy Risk Assesment を行い, どの Attribute を要求するか決定することとする (SHALL).

7.1 Back-Channel Presentation

Back-Channel モデルでは, Subscriber は Assertion Reference を渡され, 一般的には Front-Channel を通じてそれを RP に提示することになる. Assertion Reference はそれ自身では Subscriber に関する情報は持たず, Attacker による偽造や改ざんに耐えねばならない (SHALL). RP がは Assertion を取得するため Assertion Reference を IdP に提示する. その際 RP は通常 RP 自信を IdP に対して Authenticate する.

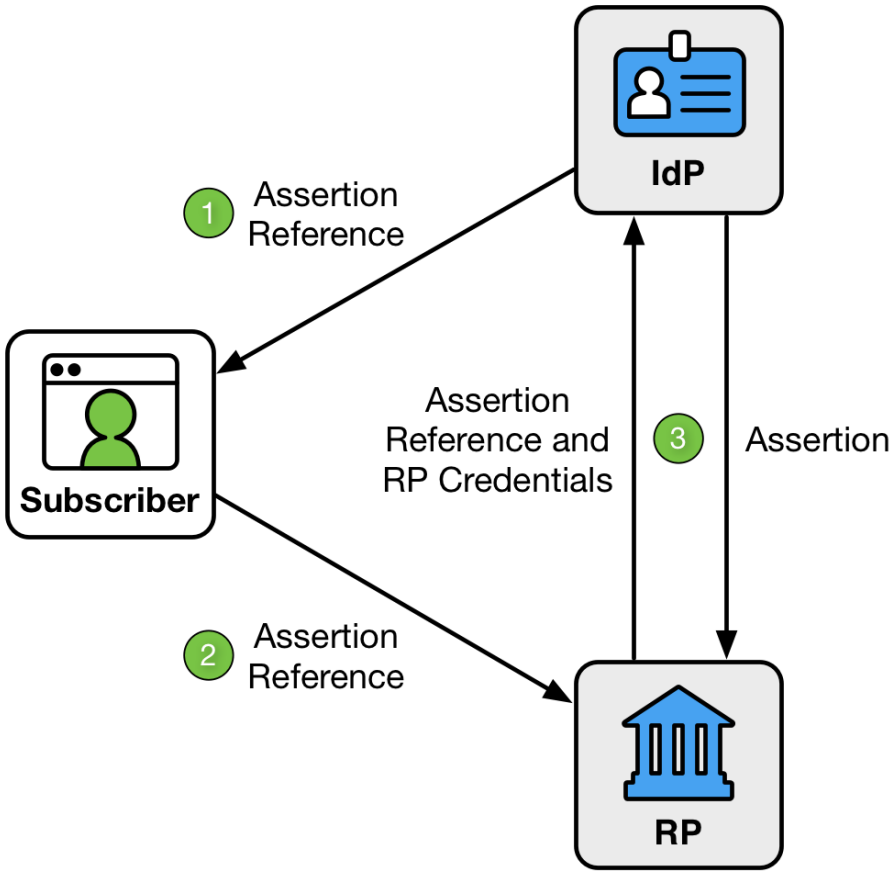

Figure 7-1 Back Channel Presentation

Figure 7-1 のとおり, Back-Channel Presentation モデルは以下の3ステップからなる.

1. IdP が Assertion Reference を Front Channel 経由で Subscriber に送信する.
2. Subscriber は Assertion Reference を Front Channel 経由で RP に送信する.
3. RP は Assertion Reference と RP 自身の Credential を Back Channel 経由で IdP に提示する. IdP は Credential を確認し, Assertion を返す.

Assertion Rference は

1. 特定 RP にのみ利用可能な制限を行うこと (SHALL)
2. ワンタイム (single-use) であること (SHALL)
3. 数秒～数分程度と有効期限が短いこと (SHOULD)
4. RP の Authentication と同時に提示されること (SHOULD)

このモデルでは, RP は第三者 (Subscriber 自身を含む) による傍受・改ざんの機会を最小化しつつ Assertion を IdP に直接要求する.

この方法では, 最初の Authentication Transaction 終了後も, ユーザーを IdP に送り返すことなく Back-Channel 通信を繰り返し行えるため, RP は IdP に Assertion 自体には含まれない追加の Subscriber に関する Attribute を問い合わせることもできる. この問い合わせは Section 6 にあるように Assertion と同時に発行された Authorization Credential を用いて行う.

Network Transaction がより多く必要となる一方, やりとりされる情報はそれを必要としている主体以外に渡されることはない. RP が IdP から直接 Assertion を受け取るため, 攻撃箇所は限定される. さらに Assertion を RP に直接インジェクトするのはより困難になる.

RP は, Cross-Site Scripting 対策やその他のテクニックを利用し, 偽造ないしキャプチャーされた Assertion Reference のインジェクションから自身を保護すること (SHALL).

RP は Assertion に含まれる要素について, 以下のような点を含めて確認すること.

- *Issuer Verification*: Assertion が RP の期待する IdP から発行されている旨を保証すること.
- *Signature Validation*: Assertion の署名が, 当該 Assertion を送信した IdP に関連する鍵と合致する旨を保証すること.
- *Time Validation*: 有効期限と発行日時が現在日時に対して許容範囲内である旨を保証すること.
- *Audience Restriction*: 当該 RP がこの Assertion の受信者として意図されている旨を保証すること.

IdP から Subscriber, Subscriber から RP へと Assertion Reference を送信する際には, Authenticated Protected Channel を利用すること (SHALL). RP から IdP に Assertion Reference を送信する際, IdP から RP に Assertion を送信する際も, Authenticated Protected Channel を利用すること (SHALL).

Assertion Reference を提示する際, IdP は Assertion Reference を提示している主体が Authentication を要求した主体と同一であることを検証すること (SHALL). IdP は, RP に対して Assertion Reference 提示時に自身を Authenticate するよう求めたり, その他の似たような方法により, これを実現することができる. (RP 識別手段となるプロトコルの一例としては RFC 7636 が参考になる)

Section 5.1.4 に述べる Federation Proxy では, IdP は Proxy に対して Assertion Reference と Assertion の Audience Restriction を行い, Proxy はダウンストリーム RP に対して新たに生成した Assertion Reference や Assertion の Audience Restriction を行うことに注意.

7.2 Front-Channel Presentation

Front-Channel モデルでは, IdP は Authentication 成功後 Assertion を生成し Subscriber に渡す. Subscriber は渡された Assertion を利用し, 大抵は Subscriber のブラウザ内のメカニズムを通じて, RP に自身を Authenticate する.

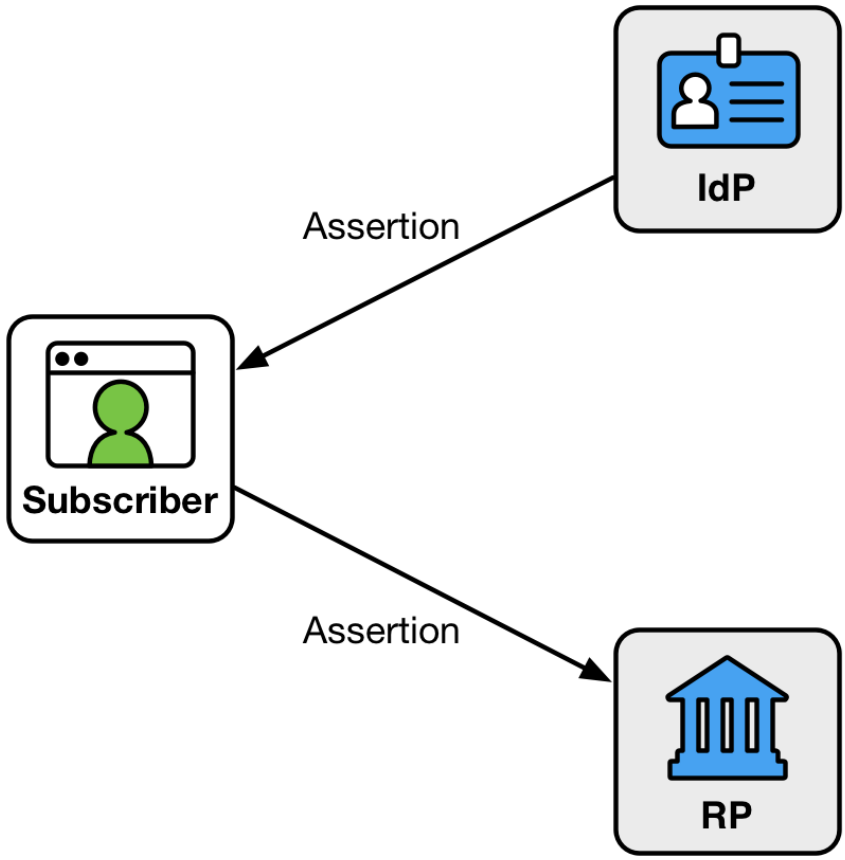

Figure 7-2 Front Channel Presentation

Front-Channel モデルでは, Assertion は Subscriber によって閲覧されうる. これは Assertion に含まれるシステム情報などの漏洩につながる可能性もある. さらにこのモデルでは, RP が IdP に Assertion 提示後に追加の Attribute を問い合わせることがより困難になる.

Assertion は Subscriber のコントロール下に置かれることから, Subscriber はブラウザをリプレイして Assertion を複数の RP に送りつけるなどの手段によって, Assertion を本来意図されない主体に送りつけることもできる. Assertion が Audience Restriction により意図しない RP に拒否されたとしても, 意図しない RP への Assertion の提示は Subscriber に関する情報や Subscriber のオンラインアクティビティの漏洩につながりうる. 意図して複数の RP に提示できるよう設計された Assertion を生成することも可能だが, そのような手法は当該 Assertion に対する Audience Restriction を緩め, 当該 RP 間における Subscriber のプライバシーおよびセキュリティー侵害につながりうる. よってそのような複数 RP に対する利用は推奨しない. RP はそれぞれ個別の Assertion を取得するよう推奨される.

RP は, Cross-Site Scripting 対策やその他のテクニックを利用し, 偽造ないしキャプチャーされた Assertion のインジェクションから自身を保護すること (SHALL).

RP は Assertion に含まれる要素について, 以下のような点を含めて確認すること.

- *Issuer Verification*: Assertion が RP の期待する IdP から発行されている旨を保証すること.
- *Signature Validation*: Assertion の署名が, 当該 Assertion を生成した IdP に関連する鍵と合致する旨を保証すること.
- *Time Validation*: 有効期限と発行日時が現在日時に対して許容範囲内である旨を保証すること.
- *Audience Restriction*: 当該 RP がこの Assertion の受信者として意図されている旨を保証すること.

IdP から Subscriber, Subscriber から RP へと Assertion を送信する際には, Authenticated Protected Channel を利用すること (SHALL).

Section 5.1.4 に述べる Federation Proxy では, IdP は Proxy に対して Assertion の Audience Restriction を行い, Proxy はダウンストリーム RP に対して新たに生成した Assertion の Audience Restriction を行うことに注意.

7.3 Protecting Information

IdP と RP の間の通信は, Authenticated Protected Channel を利用して保護すること (SHALL). Subscriber と IdP および RP それぞれとの間の通信 (通常はブラウザーを介して行われる) も Authenticated Protected Channel Channel を介して行うこと (SHALL).

IdP は, RP がセキュリティポリシーを適用する際に有用な情報に Access できる可能性もある. こういった情報としては, Device Identity, 位置情報, システムヘルスチェック情報, 設定管理情報等があげられる. IdP がこういった情報を取得できる場合, Subscriber のプライバシーを侵害しない範囲内で, そういった情報を RP に渡すことも可能であろう. 詳細は Section 9.2 を参照のこと.

ユーザーに関する追加の Attribute は, Assertion とは別に, RP から IdP への Authorized なリクエストを通じてやり取りされてもよい (MAY). こういった Attribute への Access に対する Authorization は, Assertion と一緒に発行することもできる (MAY). ユーザーに関する情報をこのように分離することで, ユーザーのプライバシー保護に役立ち, Authentication Assertion 自体に必須な情報に添える識別可能な Attribute を限定することも可能になる.

RP は, Section 9.3 にあるように, 可能な限り完全な Attribute Value ではなく Attribute Reference を要求し (SHALL), IdP は Attribute Reference をサポートすること (SHALL).

8 Security

This section is informative.

Federated Authentication プロセスには, IdP として振る舞う CSP を含め, 複数の構成要素間の連携がつきものなので, Attacker が Federated Identity Transaction を毀損するチャンスは増加する. 本セクションでは Federation に対する Attack とその対策についてまとめる.

8.1 Federation Threats

非 Federated な Authentication においては, Attacker のモチベーションは得てして RP が提供するリソースやサービスへの Access (またはより高度は Access) を取得することである. また, Attacker は Subscriber になりすまそうとすることもある. 悪意ある, もしくは侵害された IdP, RP, ユーザーエージェント (e.g., ブラウザー), 一般的に Federation Transactin の外側にいる主体が, 潜在的な Attacker となる. 攻撃を成功させるため, Attacker は Assertion や Assertion Reference を傍受したり改ざんすることも考えられる. さらに, 2者以上の主体が直接 Assertion データの Integrity (完全性) や Confidentiality (機密性) を毀損し, Federation プロトコルを台無しにしようとするかもしれない. こういったタイプの脅威を考慮すると, 自身の権限を超えた権限を取得しようとするあらゆる Authorized な主体は, Attacker とみなされる.

場合によっては, RP が認識できるように, Subscriber に秘匿情報を発行することもある. この情報を知っているかどうかで, Subscriber と Subscriber になりすまそうとする Attacker を見分けられる. Holder-of-Key Assertion のケースでは, このシークレットは Federation プロトコル開始前に IdP との間で確立されうる.

Table 8-1 Federation Threats

Federation Threats/Attacks	Description	Examples
Assertion 偽造 / 改ざん	Attacker が偽の Assertion を生成する.	侵害を受けた IdP が適切に Authenticate されていない Claimant の Identity を Assert する.

Federation Threats/Attacks	Description	Examples
	Attacker が既存の Assertion を改ざんする.	侵害を受けた Proxy が Authentication Assertion の AAL を変更する.
Assertion 漏洩	Assertion が第三者に閲覧可能になる.	Network モニタリングにより Subscriber の Address of Record が部外者に暴露される.
IdP による Assertion 否認	IdP が後になって Transaction に署名していないと主張する.	ユーザーが RP で不正なクレジットカード Transaction に関与し, IdP は彼らをログインさせていないと主張する.
Subscriber による Assertion 否認	Subscriber が Transaction を実行していないと主張する.	ユーザー同意 (e.g., 契約) の不履行.
Assertion リダイレクト	Assertion が意図しないコンテキストで利用される.	侵害を受けたユーザーエージェントが Assertino を Attacker に渡し, Attacker がどこか別の場所でそれを利用する.
Assertion 再利用	Assertion が同じ RP に複数回利用される.	傍受された Assertion が, Attacker 自身の Session を Authenticate するために利用される.
Assertion 置換	Attacker が意図されていない Subscriber の為に Assertion を利用する.	IdP と RP の間での Session Hijacking Attack.

8.2 Federation Threat Mitigation Strategies

上記の脅威を緩和するのに役立つメカニズムを Table 8-2 に示す.

Table 8-2 Mitigating Federation Threats

Federation Threat/Attack	Threat Mitigation Mechanisms	Normative Reference(s)
Assertion 偽造 / 改ざん	IdP が Assertion に暗号論的に署名を施し, RP がそれを検証する.	4.1, 6
	Assertion を Authenticated Protected Channel 経由で IdP を Authenticate した状態で送信する.	7.1, 7.2
	推測不能でランダムな識別子を Assertion に含める.	6.2.1
Assertion 漏洩	Assertion を Authenticated Protected Channel 経由で RP を Authenticate した状態で送信する.	7.1, 7.2
	Assertion を特定 RP に対して暗号化する. (双方向の Authenticated Protected Channel で実現可能)	6.2.3
IdP による Assertion 否認	IdP が否認防止 (non-repudiation) 可能な鍵で Assertion に暗号論的に署名を施し, RP がそれを検証する.	6.2.2
Subscriber による Assertion 否認	Holder-of-Key Assertion を発行する. 提示された鍵所有証明 (Proof of Posession) が Subscriber の関与を立証する.	6.1.2
Assertion リダイレクト	署名対象のコンテンツ内に, Assertion 発行先の RP (“audience”) の Identity を含める. RP は自身が意図された受信者であることを検証する.	6, 7.1, 7.2
Assertion 再利用	Assertion の有効期限を短くし, 署名対象のコンテンツ内に発行日時を含める. RP はその正当性を検証する.	6, 7.1, 7.2
	RP は任意の設定可能な時間内において消費した Assertion をトラックし, 渡された Assertion が1回以上利用されていないことを保証する.	6.2.1
Assertion 置換	Assertion に Assertion リクエストの参照や RP のリクエストに暗号論的に紐づけられたその他の nonce が含まれることを保証する.	6

Federation Threat/Attack	Threat Mitigation Mechanisms	Normative Reference(s)
	Assertion を, Back-Channel モデルなどのように, リクエストと同じ Authenticated Protected Channel で送信する.	7.1

9 Privacy Considerations

This section is informative.

9.1 Minimizing Tracking and Profiling

Federation は RP と Subscriber に多くのメリットをもたらすが, Subscriber が IdP を信頼するよう要求する. さらに Federated モデルにおいて Subscriber の信頼を確立するには, Subscriber のデータが適切に収集時の目的に制限および限定して利用されていることが重要である. 提案された用途がこれらの許可された用途の範囲内に入るかどうかについて疑問がある場合は, SAOP に相談すること. Sections 5, 5.1.4, および 6.3 は, Subscriber に対するトラッキングやプロファイリングの機会増大によるプライバシーリスクを最小化するための多くの技術的要件をカバーしている. 例えば複数の RP に対して Authenticate するために同じ IdP を利用している Subscriber がいるとすると, 当該 Subscriber は IdP に対して Federation しなかった場合には発生しなかった Subscriber Transaction のプロファイルを構築することを可能にする. このようなデータは, Subscriber の予期ないし希望しない用途に対して脆弱であり, Subscriber が Federated サービスを利用するのを妨げる可能性もある.

また Section 5.2 は Unlinkability を提供し Subscriber の行動をトラッキングしたりプロファイリングすることを抑制する技術的対策の利用を推奨している. IdP のポリシーおよび手続きは適切な利用制限や目的特定の原則の遵守徹底に重要であるが, Section 5.1.4 で述べた Proxied Federation や Section 6.3 で述べた Pairwise Pseudonymous Identifier のような技術的対策は, 運用要件を超えて Subscriber をトラックしたりプロファイリングすることを困難にし, IdP ポリシーの有効性を向上する.

9.2 Notice and Consent

Federation において Subscriber の信頼を確立するには, Subscriber が自身の情報がどのように処理されるかについて信頼できる仮定を 立てられる必要がある. 例えば, どの情報が送信されるのか, その Transaction においてどの Attribute が必須でありどれがオプションであるかを理解でき, RP にオプションの Attribute を送信するか否かの決定権があることが, Subscriber にとって有用であろう. したがって Section 7 では, Subscriber に関する Attribute が RP に送信される前に Subscriber に肯定的確認を得るよう求めている. Section 6.3.2 にように, 一連の RP 群がおなじ Pairwise Pseudonymous Identifier を共有すべきかどうかを決定する際には, IdP は Subscriber がそのような RP のグルーピングを理解できること, およびそのような理解を助ける通知を行う役目について配慮すること. 効果的な通知には, ユーザーエクスペリエンスのデザイン標準および研究, および情報処理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になろう. Subscriber が情報の処理について持つ仮定の信頼性や, Federation に関与するその他の主体の役割など, 考慮すべき要素は数多い. しかしながら, 複雑で法律に固執したプライバシーポリシーや, 相当数の Subscriber が読んだり理解したりしないような利用規約へのリンクは, 決して効果的な通知でなはい.

Section 7 はどの主体が通知を行うかは指定していない. 場合によっては Federation に関わる主体が Subscriber に通知し同意を得るための直接的な接続関係にないこともある. 通知を行うべく選択されうる主体は複数存在するが, Subscriber が通知に注意を払い情報に基づいた選択ができることを中心においた要因に基づいて決定されている限り, 事前に契約やトラストフレームワークのポリシーによりどの主体が通知と同意取得を行うかを決定しておくことは許容される.

IdP が Section 4.2 に述べたように RP のホワイトリストを利用している場合, 当該リストの RP はいずれも Authentication Transaction 中で Subscriber に提示されない. IdP はランタイムにおいて Subscriber に通知を行わないため, ホワイトリストに掲載された RP を Subscriber から確認可能にし, どの RP がどの Subscriber Attribute に Access できるか確認できるようにする. IdP は Subscriber が関与する Authentication Transaction 外では Subscriber の Authentication 情報や Attribute をホワイトリスト上の RP と共有できないため (Section 5.2 参照), RP がリスト上に存在することがそのまま Subscriber の情報が共有されることを意味するわけではない. しかしながら Subscriber が IdP を使ってホワイトリスト上の任意の RP にログインすれば, 表明された Attribute は Authentication Transaction 中で共有されることとなろう.

Subscriber のランタイムでの決定が将来の Transaction を促進するために IdP に保存されている場合は, IdP は Subscriber にランタイムの決定によりすでに許可された RP を閲覧したり許可を無効化できるようにする必要がある. このリストにはどの Attribute が許可されているかという情報を含む.

9.3 Data Minimization

Federation は RP に晒されるデータの最小化を可能にし, 結果として Subscriber のプライバシーは強化される. IdP は自身のユースケースのために RP の要求を超えて追加の Attribute を収集するかもしれないが, RP が明示的に要求した Attribute のみが IdP によって送信される. 場合によっては, RP は完全な Attribute Value を要求しないかもしれない. 例えば, RP は Subscriber が13歳以上かどうかを知る必要があるが, 完全な生年月日を知る必要はないこともある. 潜在的にセンシティブな PII の収集を最小化するため, RP は Attribute Reference (e.g., Subscriber が13歳か否かという, Y/N や Pass/Fail で答えられる質問) を要求することができる. こうすることで RP による潜在的にセンシティブかつ不要な PII の収集を最小化できる. さらに Section 7.3 は RP に可能であれば完全な Attribute Value ではなく Attribute Reference を要求するよう求めている. この RP 要件を指示するため, IdP には Attribute Reference をサポートすることが求められる.

9.4 Agency-Specific Privacy Compliance

Section 5.2 は, 機関に対して SAOP に相談してプライバシーコンプライアンス要件を決定するよう要件を定めている. プライバシーリスクの評価と対応策を施し, 機関に当該 Federation が Privacy Act of 1974 や E-Government Act of 2002 の求める PIA の実施を必要とするかといったコンプライアンス遵守に関するアドバイスを行うため, 機関の SAOP が Digital Authentication システムの開発初期段階で関わることは非常に重要である. 例えば, 当該機関が Federation における IdP を提供している場合, Credential は IdP と Federate する RP に代わって IdP に管理されることになるため, Privacy Act 要件が課せられることとなり, 新規もしくは既存の Privacy Act の記録システムによるカバレッジが必要となる. しかしながら, 機関が第三者の IdP を利用する RP の場合, RP から渡されたどのデータが RP として機関に管理されるかによっては (その場合, 機関はそのようなデータをカバーする, より広範かつプログラム的 SORN を持つことになるかもしれない), Digital Authentication には Privacy Act 要件は課されないかもしれない.

SAOP は同様に PIA が必要かどうかの決定において機関を援助できる. この考慮点は, Federated Credential の利用のためだけに, Privacy Act SORN や PIA が要件となるというふう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, ないしは 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利点に関して議論するより大きなプログラム的 PIA の一部に含む, PIA および SORN を草稿することが最も理にかなっている.

Digital Authentication の構成要素は多岐に渡るため, SAOP が個々の要素に気づいており理解していることは重要である. 例えば, Data Use Agreement, Computer Matching Agreement など, Federated IdP ないし RP サービスを提供ないし利用する機関に適用可能なその他のプライバシー上の副作用がありうる. SAOP は機関にどのような追加要件が適用されるかを決定する手助けをすることができる. さらに Digital Authentication の個々の要素を綿密に理解することにより, 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徹底的に評価し, 緩和することができる.

9.5 Blinding in Proxied Federation

典型的にはインテクレーションを単純化することを主目的する Proxy など, Proxy 構造によっては追加の Subscriber のプライバシー保護を提供しないものもあるが, Blinding 技術を用いて多様なレベルのプライバシーを Subscriber に提供するものもある. プライバシーポリシーにおいて, Subscriber Attribute と Authentication Transaction データ (e.g., 末端の IdP および RP の識別子) の IdP, RP, および Federation Proxy による適切な利用について記述してもよい. Bliding などの技術的手段はデータ取得を困難にし, そういったポリシーの有効性を高めることができる. Blindng レベルが上がるほど, 技術的および運用上の実装複雑性は上昇する. Proxy は Transaction をいずれかの側の適切な主体にマッピングし, Transaction 内のすべての関係者の鍵を管理する必要がある.

Bliding 技術を使っても, Blind された主体は, 提供された Attribute データやメタデータなどから, タイムスタンプや Attribute Bundle のサイズ, Attribute への署名者情報などを解析するなどして, 依然保護された Subscriber 情報を推測することができる. IdP は追加のプライバシー強化アプローチを検討し, Federation に参加している主体の識別可能情報の開示リスクを低減してもよい.

以下の表は Proxied Federation で利用される Bliding 実装の範囲を示したものである. なお, この表は説明を目的としたものであり, 網羅的でも技術に特化したものでもない.

Table 9-1 Federation Proxies

Proxy Type	RP knows IdP	IdP knows RP	Proxy can track subscriptions between RP and IdP	Proxy can see attributes of Subscriber
Non-Blinding Proxy with Attributes	Yes	Yes	Yes	Yes

Proxy Type	RP knows IdP	IdP knows RP	Proxy can track subscriptions between RP and IdP	Proxy can see attributes of Subscriber
Non-Blinding Proxy	Yes	Yes	Yes	N/A
Double Blind Proxy with Attributes	No	No	Yes	Yes
Double Blind Proxy	No	No	Yes	N/A
Triple Blind Proxy with or without Attributes	No	No	No	No

10 Usability Considerations

This section is informative.

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.

ユーザビリティーの観点からは, Federated Identity システムの最大の潜在的メリットの一つとして, 複数の Authentictor を管理することに関連するユーザーの疲労という問題への取り組みがあげられる. 歴史的にこれはユーザーネームとパスワードの問題であったが, ユーザーが Authenticator を管理する必要性が向上するにつれ, それが物理的なものでもデジタルなものでも, ユーザビリティーの課題が立ちはだかるようになった.

多くの他の Authentication へのアプローチが, 広範囲に研究され, かつ確立されたユーザビリティーガイドラインを持っているが, Federated Identity はより新しく, 従って研究結果の深さと決定性が不足している. 進行中のユーサビリティー研究が成熟するにつれ, Federated Identity システムに関するユーザビリティーガイドラインはより強力な支援データを持つこととなろう. 例えば, 技術的 Attribute の名前と値をユーザーフレンドリーな言語に翻訳するガイダンスを指示するには, さらなるデータが必要である.

800-63A と 800-63B のユーサビリティーセクションで述べたように, いかなる Authentication 手法においても全体のユーザーエクスペリエンスは不可欠である. Federation は多くのユーザーにとってまだ慣れないインタラクションパラダイムであるため, これは Federated Identity システムにおいては特に当てはまる. ユーザーの過去の Authentication 経験は, ユーザーの期待に影響を及ぼしうる.

Federated Identity システムにおける全体のユーザーエクスペリエンスは, 可能な限りスムーズかつ容易であるべきである. これは以下のユーザビリティー標準 (ISO 25060 シリーズの標準など) やユーザーインタラクションデザインのための確立されたベストプラクティスによって達成できる.

ASSUMPTIONS

本セクションでは, “User” とは “Claimant” ないし “Subscriber” を意味し, “Entity” とは Federated システムに関与する主体を意味する.

ガイドラインおよび考慮事項はユーザー視点で記述されている.

アクセシビリティーはユーザビリティーとは異なり, 本 Vol. 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.

10.1 General Usability Considerations

Federated Identity システムは以下を満たすべきである.

- ユーザーの負担 (e.g., フラストレーション, 学習カーブ) を最小化する.
  - 必要なユーザーアクション数を最小化する.
  - ユーザーが素早く容易に同一 IdP 上の複数のアカウントを選択できるようにする. 例えば Account Chooser (http://openid.net/wg/ac/) のようなアプローチでは, ユーザーが IdP リストから自身が利用したい IdP を選択するところから Federation プロセスを開始するのではなく, ユーザーが最近 Access したアカウントリストからアカウント選択を可能にしている.
  - ユーザーの負担の最小化とユーザーが十分に理解した上での決断を可能にする十分な情報提供の必要性のバランスを取る.
- 使い慣れていない技術用語や詳細の使用を最小限に抑える. (e.g., 基本的なコンセプトが明確に説明できれば, ユーザーは IdP や RP といった用語を知る必要はない.)
- IdP と RP で一貫性のある統合されたユーザーエクスペリエンスを目指す.
- グラフィックス, イラスト, FAQ, チュートリアル, 例などのリソースを提供し, ユーザーが Identity を理解するのを助ける. そういったリソースでは, ユーザーの情報がどのように取り扱われ, Transaction に携わる各主体 (e.g., RP, IdP, および Broker) がどのように相互関与するかを説明すべきである.

- 明確, 正直かつ有意義なユーザーとのコミュニケーションを行う. (i.e., コミュニケーションは明白で理解しやすいべきである)
- 場所やデバイスに関係なくユーザーにオンラインサービスを提供する.
- 十分に理解した上での信頼の決定を容易にするため, ユーザーに対して信頼関係を明白にする. 信頼関係はしばしばダイナミックでコンテキスト依存である. ユーザーは, 特定の Attribute を持っていたり特定の Transaction において, ある IdP および RP を他より信頼するかもしれない. 例えば, 貴重な Personal Information (金融情報や健康情報など) を含んだ Web サイトでは, ユーザーは Federated Identity システムの利用をためらうかもしれない. ユーザーが知覚する Personal Data のセンシティブさによって, ユーザーはソーシャルネットワークプロバイダーを IdP として使いたがらないこともある. これは人々がしばしばソーシャルネットワーキング実装のブロードキャスト的性質を気にするからであろう.
- ユーザーが触れるすべての情報について, SP 800-63A, Section 9 (sp800-63a.html#sec9) に示すユーザービリティー上の考慮点に従う.
- 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. Transaction に関わる主体間 (e.g., RP, IdP, および Broker) でユーザーをたらい回しにするような技術的支援は避けること.
- 適切なコンテキストで, 代表的なユーザーと現実的なタスクに対して, 統合的かつ継続的なユーザビリティー評価を行い, Federated Identity システムをユーザー視点で成功していることを保証する.

10.2 Specific Usability Considerations

本セクションでは Federated Identity システムに対する特別なユーザビリティー上の考慮点を扱う. 本セクションは, Federated Identity システムに関連する全てのユーザビリティー要素を網羅的にカバーすることを意図するものではない. ここでは, ユーザビリティーに関する文献におけるより大きくより普及したテーマである, ユーザーの Identity に対する捉え方, ユーザーの選択, 信頼, Federated Identity 空間の認識に焦点を当てる. 場合によっては実装例が提供されることもあるが, 特定のソリューションを規定することはない. 言及される実装は, 特定のユーザビリティー上のニーズに対応する革新的な技術的アプローチを推奨するための例である. さらなる例については, システム設計とコーディング, 仕様, API, 最新のベストプラクティス (OpenID や OAuth など) の標準を参照のこと. 各実装は多くの要因に対して敏感であり, ワンサイズフィットオーフなソリューションは存在しない.

10.2.1 User Perspectives on Online Identity

ユーザーが Federated Identity システムに慣れ親しんでいたとしても, (特にプライバシーと情報共有の点で) Federated Identity に対する異なるアプローチも存在し, そこではユーザーのデータ処理方法に対する信頼性の高い期待を確立する必要がある. ユーザーと実装者は異なる Identity の概念を持つ. ユーザーはログインして自身のプライベートな空間への Access を得るものとして Identity を捉えるが, 実装者は Authenticator と Assertion, Assurance Level, サービス提供に必要な一式の Identity Attribute という視点で Identity を捉える. このように, ユーザーと実装者では Identity の捉え方が異なるため, ユーザーが Federated Identity システムに適用される Identity の概念を正確に理解できるよう手助けすることが不可欠である. 優れた Identity モデルは, ユーザーが Federated システムの利点とリスクを理解し, こういったシステムを選択および信頼するよう促すための基礎となる.

Identity の特性の多くは, Federation 内, および Federation 間の両方で, ユーザーがどのように Identity を管理するかに影響を及ぼす. サイバースペースの外でコンテキストに基づいて複数の Identity を管理するのと同じように, ユーザーは自身の Identity を Federated な環境で管理するすべを学ぶ必要がある. したがって, Identity とコンテキストがどのように扱われるのかは, ユーザーに対して明確でなければならない. そのため, 以下の点が考慮されるべきである.

- 異なるユーザーの役割を区別するため, ユーザーに必要なコンテキストとスコープを提供する. 例えば, ユーザーが自身の代理として行動しているのか, 自身の雇用主など他者の代理として行動しているのかなど.
- Entity を区別するため, ユーザーにユニークで意味のある記述的な識別子を提供する.
- ユーザーにデータ所有権とデータ変更権限のある Authorized なユーザーに関する情報を提供する. Identity およびそれに関連するデータは, 複数の主体によって更新・変更可能な場合もある. 例えば, ヘルスケアデータは患者のものであるが, 一部のデータは病院や医師の診療にのってのみ更新される.
- ユーザーが簡単に Attribute を検証, 閲覧, 更新できるようにする. Identity とユーザーの役割はスタティックではなくダイナミックなものであり, 時間経過 (e.g., 年齢, 健康および金融データ) とともに変わりうる. Attribute を更新したり Attribute 提供の

決定を行う機能は, 同時に提供されることもあればそうでないこともある. ユーザーが Attribute を変更するプロセスがよく知られており, ドキュメント化され, 容易に実行できることを保証すること.

- 関連する Entity がすでに存在しない場合でも, ユーザーにデータをアップデートする手段を提供すること.
- ユーザーが, 自身の Identity を完全に消去したり, Transaction 履歴を含む自身に関するすべての情報を消去したりできるようにすること. そういったアクションを妨げる可能性のある, 適用可能な監査, 法律, ポリシー上の制約を考慮すること. 場合によっては, 消去よりも完全な無効化の方が適切なこともある.
- ユーザーに, 明確かつみつけやすい, サイト / アプリケーションのデータ保持ポリシー情報を提供すること.
- 組織のデータ Access ポリシーにしたがって, ユーザーに適切な Anonymity (匿名性) や Pseudonymity (仮名性) オプションを提供し, 要望に応じてそういった Identity オプションを切り替えられるようにすること.
- ユーザーに各 IdP および RP 間のコネクションを管理する手段を提供すること. これには, 完全な分断, 特定の RP の1つ以上の Attribute への Access 権限の削除を含む.

10.2.2 User Perspectives of Trust and Benefits

ユーザーによる Federation Identity システムの選択には, 多くの要素が影響を及ぼしうる. どのような技術においても, ユーザーはある要素を他より重視しうる. ある技術を選択する決断の前に, ユーザーはしばしば知覚されるメリットとリスクをはかりにかける. ユーザーがよく理解した上で決断できるように, IdP と RP が十分な情報を提供するのは, 非常に重要である. 信頼と信頼階層 (Tiers of Trust) というコンセプトは, Federated Identity システムの基本原理であり, ユーザーによる選択を促進する可能性がある. 最後に, ユーザーエクスペリエンスが向上すると, Federation に対するユーザーの需要が増加し, RP による Federation の選択も増加する可能性がある.

本サブセクションは, 主にユーザーの信頼とユーザーによるメリットとリスクの知覚に焦点を当てる.

ユーザーによる採用を促進するため, IdP と RP はユーザーとの信頼を確立おこび構築し, ユーザーに採用によるメリットとリスクを理解させる必要がある. 考慮点としては以下のようなものが挙げられる.

- ユーザーが自身の情報の開示をコントロールし, 適切な通知により明示的同意を行えるようにする (SP 800-63C, Section 9.2, Notice and Consent 参照). 通知の内容, サイズ, 頻度のバランスは, ユーザーが何も考えずにクリックスルーしてしまうことを避けるために必須である.
- Attribute 共有のためには以下の点を考慮すること.
    - ユーザーに共有される自身の Attribute および Attribute Value を検証する手段を提供すること. よくできたセキュリティープラクティスに従うこと (Section 7 参照).
    - オールオアナッシングアプローチではなく, ユーザーが部分的な Attribute リストに対して同意できるようにすること. ユーザーが全情報の共有に同意しない場合でも, ある程度のオンライン Access を可能にすること.
    - ユーザーが共有済 Attribute リストへの同意を更新できるようにすること.
    - ユーザーに提示される不必要な情報を最小化すること. 例えば, Authentication レスポンスの一部として共有されるとしても, システムにより生成された Attribute (Pairwise Pseudonymous Identifier など) を見せないなど.
    - ユーザーのステップおよびナビゲーションを最小化すること. 例えば, Attribute 共有の同意をプロトコルに組み込み, Federated Transaction 外の機能としないなど. OAuth や OpenID Connect といった標準にこういった例が見られる.
    - ユーザーが IdP により不正な Attribute 情報を付与された状況から回復できるよう, 効果的かつ効率的な是正手段を提供すること (Section 7 参照).
    - ユーザーに Attribute 共有の同意を要求する回数を最小化すること. 同意要求の頻度を限定することで, 何度も同じ Attribute の共有要求を受けることによるユーザーのフラストレーションを避けることができる.
- 制約内の利用目的のためにのみ情報を収集し, 情報開示を最小化すること (Section 9.3 参照). ユーザーの明示的な同意なしに不必要かつ過剰な情報の収集や開示, またはユーザーのトラッキングを行うと, ユーザーの信頼は失われる. 例えば, ユーザーに対して現在の Transaction に関連する Attribute のみを要求し, RP でユーザーが Access するかどうかわからないすべてのありうる Transaction のために Attribute を要求しないようにするなど.
- Federated Identity を利用することによる潜在的利点とリスクを, ユーザーに明確かつ正直に伝えること. ユーザーが価値を感じる利点としては, 時間節約, 使いやすさ, 管理するパスワード数の減少, 利便性向上などがある.

リスクに対するユーザーの懸念は, Federated Identity システムの選択意欲に悪影響を与えうる. ユーザーは, 信頼, プライバシー, セキュリティー, Single-point-of-failure といった点において, 懸念を抱く可能性がある. 例えば, ひとつの IdP が一時的または永続的に利用不可となった場合, ユーザーは複数のアカウントへの Access を失うおそれがある. さらに, ユーザーは新しい Authentication プロセスを学ぶことに懸念を抱いたり混乱する可能性もある. Federated Identity システムの選択を促進するには, 知覚されるメリットが知覚されるリスクを上回らねばならない.

10.2.3 User Models and Beliefs

ユーザーは何かを信じたりと知覚することによって, 特定の結果を期待し, 特定の方法で行動する傾向にある. そのように信じたり知覚したり何らかの傾向を示したりすることは, 社会科学においてメンタルモデルと呼ばれる. 例えば, ファーストフードレスランやカフェテリア, よりフォーマルなレストランなど, 人々は施設によって行動や期待を異にするような, 食事に関するメンタルモデルを持っている. したがって, それぞれの施設に精通していなくても, それぞれでどのように振る舞うのが適切かを理解することができる.

Federation におけるよくできた完全なメンタルモデルをユーザーが構築できるよう支援することで, ユーザーはある特定の実装を超えて一般化を行うことができる. Federated Identity システムがユーザー視点でデザインされていなければ, ユーザーは間違ったもしくは不完全なメンタルモデルを形成し, 彼らによるシステムの選択意思に影響を及ぼすかもしれない. 考慮点としては以下のようなものが挙げられる.

- ユーザーの誤解を避けるため, Transaction 関係者 (e.g., RP, IdP, および Broker) 間の関係性と情報の流れを明確に説明すること. 一般的用語である IdP と RP という語を使用するのではなく, 実際の Entity の名前を使用して説明すること.
    - 人目をひく視覚的合図や情報を提供し, 一見無関係な Entity が相互に関係している理由を理解できるようにすること. 例えば, ユーザーは Federated Identity システムにおける情報の流れの理解が不足しており, オンラインでの個人的な行動と政府サービスが混ぜ合わされてしまうのではないかと心配するかもしれない.
    - 人目をひく視覚的合図や情報を提供し, RP が制御を自身のサイトから IdP にリダイレクトする必要がある際に, リダイレクトに関してユーザーに知らせること. 例えば, IdP のユーザーインターフェース内に RP のブランドを表示し, 目的とする RP に Access するために当該 IdP にログインしようとしていることをユーザーに知らせるなど.
- Transaction 関係者 (e.g., RP, IdP, および Broker) の信憑性 (Authenticity) を判断するため, ユーザーに明確で利用しやすい手段 (e.g., 視覚的保証) を提供すること. これは, 特にルートドメインが変わる (e.g., .gov から .com) 場合など, あるドメインから別のドメインに移る際のユーザーの懸念を緩和するにも役立つであろう. 例えば, IdP の URL を表示して, ユーザーが悪意あるサイトにフィッシングされていないことを検証できるようにするなど.
- 暗黙的なログインと明示的なログアウトに関して, ユーザーに視覚的合図を含む明確な情報を提供すること. 実装によっては, IdP アカウントで RP にログインすると, ユーザーは IdP と RP 双方に対して Authenticate されることもある. その場合, ユーザーは RP での Session を終了したとしても, 必ずしも IdP の Session が終了されるわけではなく, IdP から明示的に “ログアウト” する必要がある, ということに気づかないかもしれない. IdP の Session を終了するために明示的なログアウトが必要な場合, ユーザーはそれを想起させる明確な情報を必要とする.

11 Examples

This section is informative.

以下では3種類の Assertion テクノロジー, SAML Assertion, Kerberos Ticket, OpenID Connect Token, について述べる. このリストには, すべてのありうる Assertion テクノロジーは含まれないが, Federated Identity システムで一般的に利用されているものを代表している.

11.1 Security Assertion Markup Language (SAML)

SAML は, Authentication および Attribute 情報を生成し, 信頼関係のある Entity 間で Internet 越しにやりとりする XML ベースのフレームワークである. 本執筆時点で最新の SAML 仕様は, 2005/03/15 発行の SAML v2.0 である.

SAML の構成要素を以下に示す.

- Assertion の構造を定義する Assertion XML Schema.
- Assertion および Artifact (Section 7.1 で述べたインダイレクトモードで使われる Assertion Reference) をリクエストする際に利用する SAML Protocol.
- 根底となる通信プロトコル (HTTP や SOAP など) を定義し, SAML Assertion の転送に利用する Binding.

上記の3要素により, “Web Browser SSO” といった特定のユースケースに対応した SAML プロファイルが定義される.

SAML Assertion は XML Schema にエンコードされ, 3つのタイプのステートメントを伝搬する.

- *Authentication Statement*: Assertion Issuer, Authenticated Subscriber, 有効期間およびその他の Authentication に関する情報を含む. 例えば, ある Authentication Assertion は Subscriber “John” が 2004/06/06 10:32pm にパスワードを使って Authenticate されたことを示すであろう.
- *Attribute Statement*: Subscriber に関する特定の追加特性を含む. 例えば, “John” という Subject に対して, “Role” という Attribute に対して “Manager” という値が付与されている, など.
- *Authorization Statement*: Subscriber が Access 権を持つリソースを示す. こういったリソースとしては, 特定のデバイス, ファイル, 特定の Web サーバー上の情報などが挙げられる. 例えば, “John” という Subject が, “Role” を拠り所として, “Webserver1002” 上で “Read” というアクションを行える, など.

Authorization Statement は本ドキュメントの扱うところではなく, ここでは議論しない.

11.2 Kerberos Tickets

Kerberos Network Authentication Service [RFC 4120] は, ローカルの共有ネットワーク上のクライアント・サーバーアプリケーションに対して, Symmetric-Key 暗号を利用した強固な Authentication を提供するべくデザインされた. Kerberos の拡張では, プロトコルの特定のステップにおいて Public Key 暗号を利用することもできる. Kerberos は Subscriber と RP の間の Session データの Confidentiality (機密性) および Integrity (完全性) 保護もサポートする. Kerberos は Assertion を利用するものの, 共有ネットワーク上での利用のためにデザインされたものなので, 真に Federation プロトコルとは言えない.

Kerberos は, 信頼できない共有ローカルネットワーク上でひとつ以上の IdP を利用した Subscriber の Authentication をサポートしている. IdP が Subscriber に対して暗号化したランダムな Session キーを復号できることを示すことによって, Subscriber は暗黙的に IdP に対して Authenticate する. (Kerboros 派生のもののなかには, Subscriber が明示的に IdP に対して Authenticate することを求めるものもあるが, 普遍的ではない) 暗号化された Session キーに加え, IdP は Kerberos Ticket と呼ばれるもうひとつの暗号化オブジェクトを生成する. この Ticket には同じ Session キー, Session キーが発行された Subscriber の Identity, Session キーの有効期限が含まれている. このチケットは, 明示的なセットアップフェーズ中に IdP と RP の間で共有される事前に確立された鍵によって, Confidentiality (機密性) および Integrity (完全性) が保護されている.

Session キーを使って Authenticate するため, Subscriber は, Subscriber が Kerberos Ticket に埋め込まれた Session キーを保有していることを証明する暗号化データとともに, Ticket を RP に送る. Session キーは, 新しい Ticket を生成したり, Subscriber と RP の間の通信を暗号化したり Authenticate するために使われる.

このプロセスを開始するため, Subscriber は Authentication Server (AS) に Authentication リクエストを送る. AS は, Subscriber の長期間有効な Credential を用いて, Subscriber に対して Session キーを暗号化する. この長期間有効な Credential は, AS と Subscriber 間の共有秘密鍵でもよいし, Kerberos 派生の PKINIT のように Public Key Certificate でもよい. Subscriber と IdP の間の共有秘密鍵

に基づいた Kerberos 派生のほとんどは, この鍵をユーザーが生成したパスワードから導出する. 従ってそれらは, Flexible Authentication Secure Tunneling (FAST) [RFC 6113] や似たようなトンネリングおよび防護メカニズムを利用していない限り, 受動的な盗聴者によるオフライン辞書 Attack に対して脆弱である.

Session キーを Subscriber に伝送するのに加えて, AS は Ticket Granting Server (TGS) と共有した鍵を使った Ticket を発行する. この Ticket は, Ticket Granting Ticket (TGT) と呼ばれる. これは Verifier が TGT 内の Session キーを利用して, 明示的に Verifier を Authenticate するかわりに Ticket を発行することに由来する. TGS は TGT 内の Session キーを利用して Subscriber に対する新規 Session キーを暗号化し, RP と共有している鍵を使って新規 Session キーに対応する Ticket を生成する. Subscriber は Session キーを復号し, Ticket と新規 Session キーを同時に使って RP に対して Authenticate する.

Keriberos Authentication がパスワードに基づいている場合, このプロトコルは最初のユーザーと KDC とのやりとりをキャプチャーする登頂者によるオフライン辞書 Attack に対して脆弱であることが知られている. 十分な長さのパスワードはえてしてユーザーにとってはわずらわしいものであるが, より長く複雑なパスワードを利用すればこの脆弱性は緩和される. ただしパスワードベースの Kerberos Authentication が FAST (または類似の) トンネル中で利用されている場合, 辞書 Attack を実行するには追加で Man-in-the-Middle Attack が必要である.

11.3 OpenID Connect

OpenID Connect [OIDC] は, OAuth 2.0 Authorizatino Framework および JSON Object Signing and Encryption (JOSE) 暗号システムに基づいた, インターネット規模の Federated Identity および Authentication プロトコルである.

OpenID Connect は OAuth 2.0 Authorizatino Framework の上に構築され, RP による Subscriber の Identity および Authentication 情報への Access を, Subscriber が Authorize することを可能にする. OpenID Connect および OAuth 2.0 における RP は Client とも呼ばれる.

OpenID Connect の Transaction が成功すると, IdP は ID Tokne という JSON Web Token (JWT) フォーマットの署名付き Assertion を発行する. Client は ID Token をパースし, Subsriber および IdP 上でのプライマリーな Authentication イベントについての情報を得る. この Token は, 最低限 Subscriber および Authentication イベントに関する以下の情報を含む.

- `iss` - Assertion を発行した IdP を識別する HTTPS URL.
- `sub` - IdP 固有の Subject 識別子であり, Subscriber を示す.
- `aud` - IdP 固有の Audience 識別子であり, IdP における当該 OAuth 2.0 Client の Client 識別子に等しい.
- `exp` - ID Token の有効期限を示すタイムスタンプ. Client はこの時刻をすぎてこの Token を受け入れてはならない (SHALL NOT).
- `iat` - ID Token の発行日時を示すタイムスタンプ. Client はこの時刻より前にこの Token を受け入れてはならない (SHALL NOT).

ID Token に加え, IdP は Client に OAuth 2.0 Access Token を発行する. この Token は IdP の UserInfo Endpoint に Access する際に利用できる. このエンドポイントは Subject の Attribute 一式を示す JSON オブジェクトを返し, そこには名前, Email アドレス, 物理アドレス, 電話番号, その他のプロフィール情報が含まれるが, それだけに限らない. ID Token 内の情報が Authentication イベントを反映したものである一方で, UserInfo Endpoint から返される情報は一般的によりステーブルかつより汎用的である. UserInfo Endpoint でのその他の Attribute に Access は, 特別に定義された OAuth 2.0 Scope である `openid`, `profile`, `email`, `phone`, および `address` により制御される. さらに `offline_access` という追加の Scope が Refresh Token の発行を制御するために使われる. Refresh Token を使うと, RP は Subscriber が不在の時にでも UserInfo Endpoint に Access することができる. したがって, UserInfo Endpoint への Access は, Subscriber がそこにいることの証明として, RP での Session を Authenticate するには不十分である.

12 References

This section is informative.

12.1 General References

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

[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).

[NISTIR 8112] NIST Internal Report 8112 (Draft), *Attribute Metadata*, available at: https://pages.nist.gov/NISTIR-8112/NISTIR-8112.html (https://pages.nist.gov/NISTIR-8112/NISTIR-8112.html).

[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).

12.2 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).

[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*, 1998, available at: https://www.iso.org/standard/16883.html (https://www.iso.org/standard/16883.html).

[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).

[RFC 4120] IETF, *The Kerberos Network Authentication Service (V5)*, RFC 4120, DOI 10.17487/RFC4120, July 2005, https://doi.org/10.17487/RFC4120 (https://doi.org/10.17487/RFC4120).

[RFC 6113] IETF, *A Generalized Framework for Kerberos Pre-Authentication*, RFC 6113, DOI 10.17487/RFC6113, April 2011, https://doi.org/10.17487/RFC6113 (https://doi.org/10.17487/RFC6113).

[RFC 7591] IETF, *OAuth 2.0 Dynamic Client Registration Protocol*, RFC 7591, DOI 10.17487/RFC7591, July 2015, https://doi.org/10.17487/RFC7591 (https://doi.org/10.17487/RFC7591).

[RFC 7636] IETF, *Proof Key For Code Exchange*, RFC 7636, DOI 10.17487/RFC7636, September 2015, https://doi.org/10.17487/RFC7636 (https://doi.org/10.17487/RFC7636).

[SAML] OASIS, *Security Assertion Markup Language (SAML) V2.0 Technical Overview*, March 2008, available at: http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html (http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html).

12.3 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 800-53] NIST Special Publication 800-53 Revision 4, *Recommended Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 (updated January 22, 2015), http://dx.doi.org/10.6028/NIST.SP.800-53r4 (http://dx.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 800-63A] NIST Special Publication 800-63A, *Digital Identity Guidelines: Enrollment and Identity Proofing Requirements*, June 2017, https://doi.org/10.6028/NIST.SP.800-63a (https://doi.org/10.6028/NIST.SP.800-63a).

[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).

12.4 Federal Information Processing Standards

[FIPS 140-2] Federal Information Processing Standard Publication 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001 (with Change Notices through December 3, 2002), https://doi.org/10.6028/NIST.FIPS.140-2 (https://doi.org/10.6028/NIST.FIPS.140-2).