1. Introduction

This document is a collection of profiles that define integration of authentication services with ISO 8583 used for financial transactions (e.g., point-of-sale (POS), automated teller machine (ATM) cash withdrawal transactions, etc.). Such services include biometric authentication (as defined by IEEE Std. 2410), PIN-based, Fast Identity Online (FIDO), and One-Time Password (OTP) and Time-based OTP (TOTP) authentication methods including risk and presentation attack defense (PAD) measures. The scope of authentication includes primary authentication, second-factor authentication (2FA), step-up authentication (SUA), and multi-factor authentication (MFA).

1.1 Requirements Notation and Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “NOT RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in IETF RFC 2119.

1.2 Terminology

This specification uses the terms “Automated Teller Machine”, “Authentication Service”, “Cryptogram”, “Vector of Trust (Vot)”, “Two-Factor Authentication” (2FA), “Multi-Factor Authentication” (MFA), “Identity Assurance”, “Identity Verification”, “Identity Proofing”, “Client”, “Payment Processor”, “Primary Authentication”, “Presentation Attack Detection” (PAD), "“,”“,”“, and”" defined by IEEE Std. 2410, the terms “Claim Name”, “Claim Value”, and “JSON Web Token (JWT)” defined by JSON Web Token (JWT) , and the terms defined by OpenID Connect Core 1.0. This document reuses terminology from VoT [RFC8485] and NIST Special Publication 800-63 [SP-800-63-3].

1.3. Conformance

The following profiles are specified in this document:

IEEE Std. 2410 (Biometric authentication)

Additional profiles may be added in future revisions of this document.

2. Profiles

A profile defines specific API calls and associated parameters in context with the IEEE P1940 trust framework defined in Section X of this document. Please refer to the transaction diagram in Section X for appropriate mappings of service requests and responses.

2.1 IEEE Std. 2410 Profile

The IEEE Std. 2410 profile maps specific API calls to IEEE P1940 transactions (see Diagram X). It specifies requirements for requests to an IEEE Std. 2410 Identity Provider service using biometric authentication.

2.1.1 AuthenticationStart/AuthenticationRequest (diagram X links 3, 11)

An AuthenticationStart typically originates with a relying party (RP) as a request that sends the userid and deviceid parameters and returns session id for an enrolled account on a specific device. The request is asynchronous resulting in a session opportunity being created. Creation of a session opportunity causes a subsequent out-of-band push notification (transaction diagram link #3) to be sent to the enrolled device for that user. OPTIONALLY, a polling sequence from the mobile device may be used instead of a push notification. OPTIONALLY, the request MAY contain a Vector of Trust Request (VTR).
2.1.2 AuthenticationResponse (diagram X links 5, 10) An AuthenticationResponse call contains the results of the mobile device execution of specified authentication mode(s) the device requested by an out-of-band push notification. The AuthenticationResponse SHOULD NOT contain the literal Vector of Trust (VOT) results, but IEEE Std. 2410 specifics of the authentication results including biometric modalities.

2.1.3 GetSessionStatus (diagram X links 5a, 10a)

The Identity Provider can be polled or notified by the Relying Party regarding an active session created by an AuthenticationStart (see 2.1.1). If the session is authenticated, a call to GetSessionStatus within its active period (i.e., not expired) will return the authentication result and MAY contain a Vector of Trust (VOT) result characterizing the context of the authentication session. ### 2.1.4 Privacy Considerations The Identity Provider and associated mobile SDK are responsible for security of the user's privately identifiable information (PII). No PII is shared to the Relying Party - only the authentication result (true or false) and MAY contain a Vector of Trust (VOT). Any additional information is outside the scope of this profile such as attribute values (i.e., name, address, DoB, etc.) obtained via other IDP APIs.

2.1.5 Security Considerations

All transactions MUST be protected in transit by TLS as described in BCP195. Authentication Servers SHOULD take into account device postures when dealing with native apps if possible. Device postures include characteristics such as a user's lock screen setting, or if the app has 'root access' (meaning the device OS may be compromised to gain additional privileges not intended by the vendor), or if there is a device attestation for the app for its validity. Specific policies or capabilities are outside the scope of this specification. All clients MUST conform to applicable recommendations found in the Security Considerations sections of [RFC6749].

2.1.6 Threat Model

IEEE Std. 2410 determines the user and device enrollment process mitigates man-in-the-middle (MiTM) attacks that may be used to intercept calls from the mobile device to the relying party and the mobile device to the identity provider. Although protected by TLS, we still recommend the association of IDP and RP within a trusted network and the IDP-RP connections MUST use client certificates (called friend certificates) as required by IEEE Std. 2410.

3. Trust Framework

IEEE P1940, in part, defines a trust framework based on Vectors of Trust (VoT) [RFC8485]. VoT prescribes an efficient method for expressing measurements of trust for use in digital identity transactions. Historically trust measurements have fallen into two main categories: either all measurements are combined into a single scalar value or trust decisions are calculated locally based on a detailed set of attribute metadata. VoT defines a method of conveying trust information that is more expressive than a single value but less complex than comprehensive attribute metadata.

3.1 Vectors of Trust

VoT [RFC8485] prescribes four vectors of trust. The trust vectors are called "components". They are:

- **Identity proofing (P)** dictates the level of scrutiny applied to the identity subject during the proofing process to establish a subject's identity.
- **Primary credential usage (C)** represents distinct categories of primary credential that MAY be used together in a single transaction.
- **Primary credential management (M)** represents distinct categories of management that MAY be considered separately or together in a single transaction.

- **Assertion presentation (A)** represents distinct categories of assertion that are RECOMMENDED to be used in a subsumptive manner but MAY be used together. Multiple distinct values from this category MAY be used in a single transaction.

Taken together, the four VoT components (P), (C), (M), and (A) allow expression of a complete lifecycle of digital identity creation and use. Each VoT component has distinct component value definitions or "categories" which convey increasing levels of assurance or strength, or different options or alternatives when multiple alternatives are available.

Naturally ordered levels are typically expressed using category values of 0, 1, 2, and so on. Alternative choices are usually indicated using lettered categories, for example, a, b, and c.

On the wire, vectors are represented as a period-separated (‘.’) list of vector components. A vector component type can occur multiple times within a single vector, but a specific value of a vector component cannot occur more than once in a single vector. That is, while “Cc.Cd” is a valid vector, “Cc.Cc” is not. Multiple values for a component are considered a logical AND of the values. Omitting a component means you are not making any claims about that component.

See the complete set of default VoT components and categories in VoT [RFC8485] Appendix A.

3.2 Trustmarks Locate Trust Frameworks

A trustmark is an HTTPS URL that references a specific set of vector values as defined by a trust framework. This URL MUST point to a human-readable document that describes what components and values are valid, how they are used together, and what practices the component values represent within the trust framework. The contents of the trustmark URL MUST be reachable by the operators or implementors of the RP. The URL MUST be stable over time for a given trust framework to allow RPs to process incoming vectors in a consistent fashion. For example, https://www.rfc-editor.org/info/rfc8485 is the trustmark that references the values defined in RFC8485 Appendix A. The trustmark for implementations of IEEE P1940 is the persistent URL of this specification: https://standards.ieee.org/standard/p1940.html. New versions of a trust framework that require different processing rules MUST use a different trustmark URL.

3.3 P1940 Trust Framework

The VoT [RFC8485] components and categories are for general purpose use across a range of digital identity systems, to use as needed and as appropriate for the system(s) involved. The components and categories in RFC8485 are referred to as a “trust framework”. For systems where using the default VoT [RFC8485] components and categories does not meet the needs of the systems involved, you can delete, modify, or add categories to define appropriate mechanisms, which results in a new trust framework.

P1940 defines a trust framework for specifying cardless identity assurance in ISO8583 card based networks. The trust framework is similar to the default trust framework defined in RFC8485 with these differences:

- The identity proofing (P) component is **outside the scope of IEEE P1940** as it occurs before a user engages in a P1940 transaction.
- The primary credential usage (C) component has additional categories to

specify authentication types provided by P1940-adherent mobile authentication applications.

- The primary credential management (M) component is **outside the scope of IEEE P1940** as P1940 transactions do not involve credential management operations.
- The assertion presentation (A) component is **outside the scope of IEEE P1940 as P1940** transactions do not involve federated (cross-domain) authentication assertions.

See Appendix X for the complete specification of the P1940 trust framework.

For now it's here:

P Identity proofing: Not Applicable

C Primary credential usage Defaults (from VoT RFC 8485) * C0 No credential is used / anonymous public service * Ca Simple session HTTP cookies (with nothing else) * Cb Known device, such as those indicated through device posture or device management systems * Cc Shared secret, such as a username and password combination * Cd Cryptographic proof of key possession using shared key * Ce Cryptographic proof of key possession using asymmetric key * Cf Sealed hardware token / keys stored in a trusted platform module

Extensions: * Cg Locally verified biometric * Ch Verified Split Biometric * Ci Authentication Freshness Not sure this can be represented practically. * Cx FIDO authentication * Cj Pad detection used * Ck UBA used * Cl Geolocation used * Cm SUA used (not sure if these last three make sense) * Cn 2FA used * Co MFA used

M Primary credential management: Not Applicable.

A Assertion presentation: Not Applicable.

4 IEEE P1940 Example

P1940 architectures involve mobile client apps communicating with backend financial servers to initiate and carry out ATM and POS transactions, using mobile app 'authenticators' to prove a user identity with an agreed-upon level of assurance suited to the transaction risk level.

End users gain access to the features through a service provider. The service provider may be a financial institution or a non-bank entity providing similar services. The service provider is called an RP (relying party). The service provider will allow users to conduct transactions using a mobile application. The service provider has a mobile application that interacts with a mobile application server. The mobile application server evaluates the risk in a proposed transaction and generates an appropriate vector of trust request (VtR) which is consumed by an IdP to issue an authentication request with the appropriate assurance level. For example, a low-risk transaction of US $10 could require just a fingerprint like Apple's proprietary TouchID on an iPhone device. A higher-risk transaction (say US $200.00) could require Touch ID with presentation attack detection and geolocation of the user.

To do this, an RP must know the types of authentication methods available and their relative assurance levels. IdP vendors use this specification to design processes that consume VtRs and generate appropriate authentication requests. The exact method for transforming VtRs into authentication requests is outside the scope of this specification.

Lastly, once an authentication has occurred, the IdP returns the result to the RP along with a vector of trust (VoT) component-value string declaring the specific methods and policies used.

The IEEE P1940 example ATM transaction involves a number of actors to handle aspects of the transaction. This architecture diagram shows the actors in an ATM network including a mobile app communicating with service provider servers to carry out a transaction.

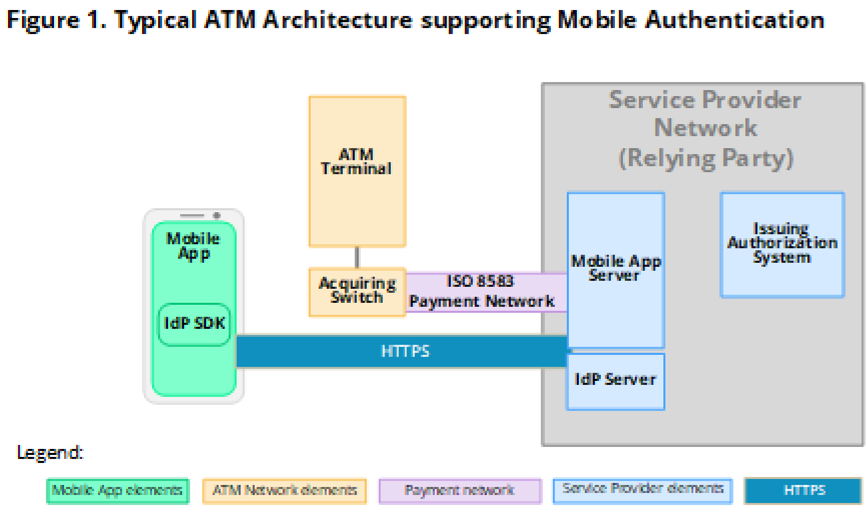


Figure 1: Image of ATM network

The architecture diagram has these elements.

- **ATM Terminal**: Standard ATM hardware terminal with software support for mobile flow.
- **Acquiring Switch**: Connects one or more ATM terminals to a payment network or issuing authorization system using the ISO 8583 protocol.
- **Mobile App**: A mobile app provided to a user by a service provider for performing mobile transactions. The app runs on a mobile device such as a smartphone. The app includes an embedded IdP SDK.

- **IdP SDK**: Handles mobile multi factor authentication operations in response to requests from the IdP server located at the service provider.
- **Mobile App Server**: Service provider server that handles user requests according to business and risk management rules.
- **Issuing authorization system**: A system that holds user parameters such as account number, card identifiers, and cryptographic keys, and responds to transaction authorization requests on behalf of a card issuer.
- **IdP Server**: An IEEE P1940-compliant service that handles multi-factor authentication in response to user authentication requests from a mobile app server.

This series of transaction diagrams shows a sample authentication scenario illustrating the use of VtRs and VoTs in an ATM transaction.

Figure 2 shows the initial transaction phase where the user stages the transaction (a cash withdrawal from the ATM). These sequences are outside the scope of IEEE P1940.

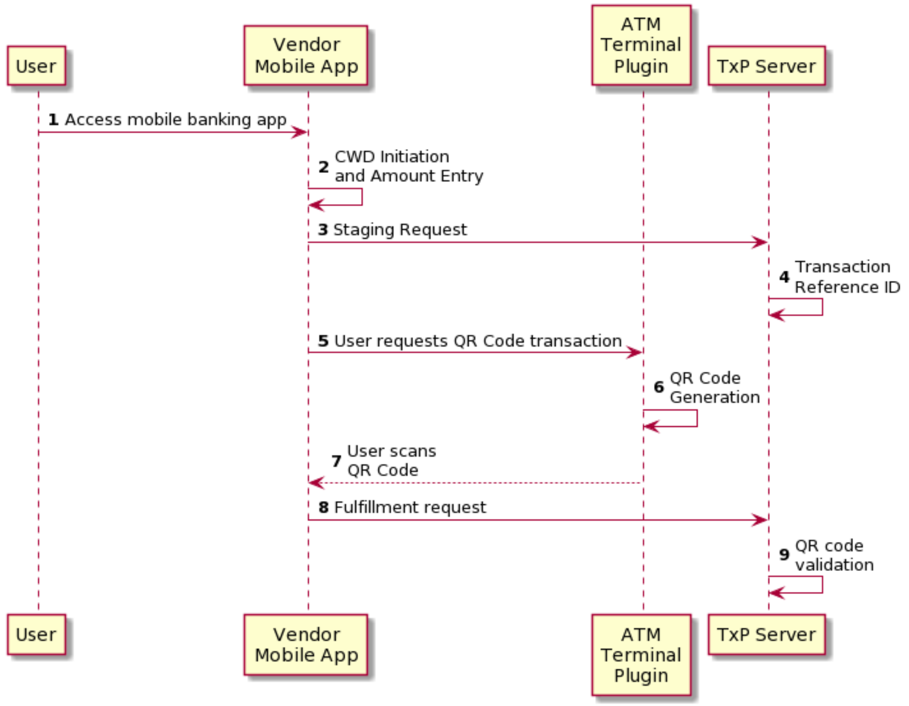


Figure 2: cached image

This diagram illustrates authentication sequences where the mobile app server knows the amount of the transaction and issues an authentication request to the

IdP. These sequences are in the scope of IEEE P1940.

The embedded IdP SDK is shown near to the IdP server to clarify these interactions.

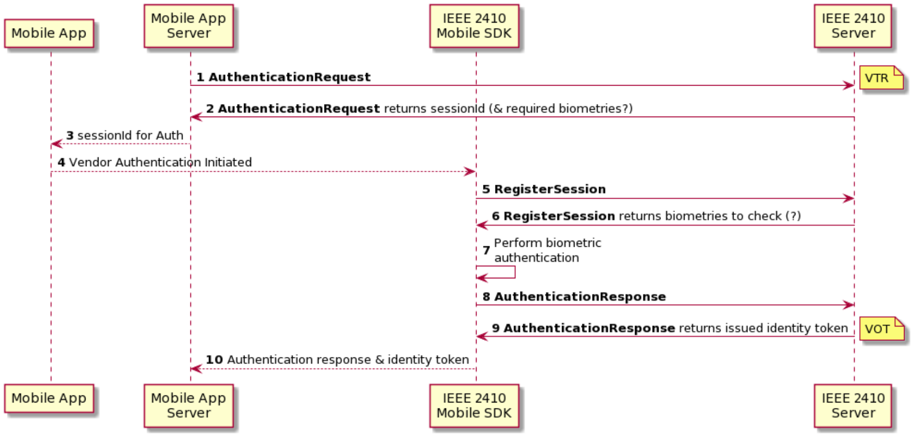

Mobile App
Mobile App Server
IEEE 2410 Mobile SDK
IEEE 2410 Server
1 AuthenticationRequest
VTR
2 AuthenticationRequest returns sessionId (& required biometries?)
3 sessionId for Auth
4 Vendor Authentication Initiated
5 RegisterSession
6 RegisterSession returns biometries to check (?)
7 Perform biometric authentication
8 AuthenticationResponse
9 AuthenticationResponse returns issued identity token
VOT
10 Authentication response & identity token
Mobile App
Mobile App Server
IEEE 2410 Mobile SDK
IEEE 2410 Server

Figure 3: cached image

This diagram shows carrying out the cash disbursement using standard ATM methods. These sequences are outside the scope of IEEE P1940.

5 Determining Risk

The relying party (RP) MUST determine the risk involved in transactions carried out using IEEE P1940 and prescribe authentication methods commensurate with the risk level.

Mobile banking apps typically have standard capabilities for which they know, by experience, the risk of financial loss or impact is low. Accordingly, mobile access to these capabilities requires a minimum level of authentication. These standard capabilities include:

- Access the mobile app
- Show account balances and account transactions
- Deposit checks
- Pay bills

IEEE P1940 adherent mobile apps MAY have one or both of these additional capabilities for which the risk of financial loss or impact is higher as the transaction results in immediate delivery of cash and merchandise which are more difficult to recover when obtained by an imposter. These additional capabilities include:

- Initiate a cardless ATM cash withdrawal

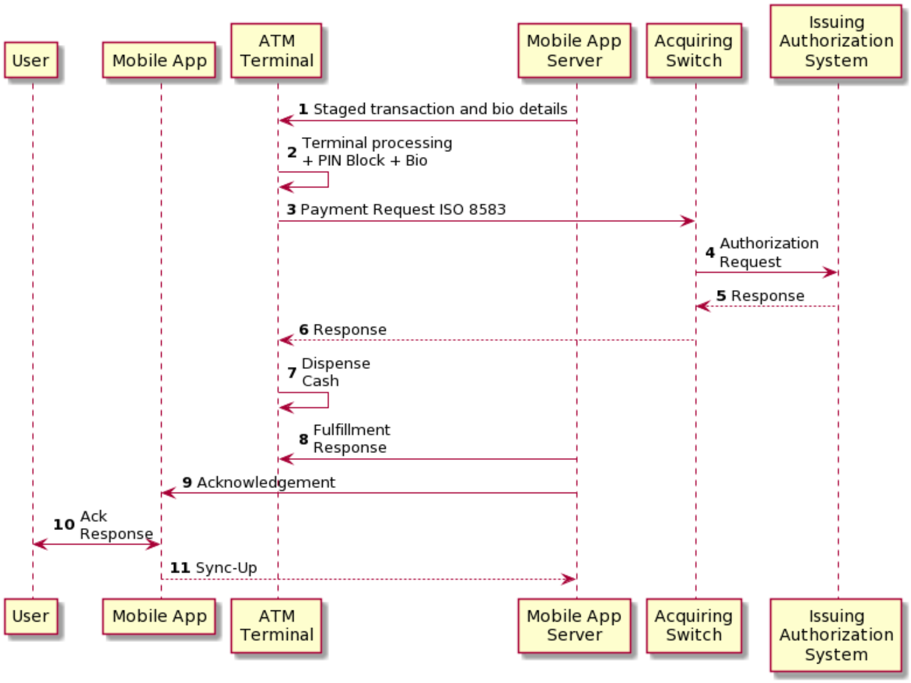


Figure 4: cached image

- Initiate a cardless point of sale transaction

Moreover, the risk increases as the amount of cash or the value of merchandise increases. Financial institutions generally have policies limiting the amounts available for withdrawal or purchase but these policies are outside the scope of IEEE P1940.

As a means to consistently measure risk inherent in various network transactions, the Vectors of Trust RFC8485 recommends using the guidelines prescribed in NIST Special Publication 800-63 Digital Identity Guidelines [SP-800-63-3].

SP-800-63-3 describes three components of identity assurance that provides agencies flexibility in choosing identity solutions.

- **IAL (Identity Assurance Level)**: The robustness of the identity proofing process to confidently determine the identity of an individual. IAL is selected to mitigate potential identity proofing errors.
- **AAL (Authenticator Assurance Level)**: The robustness of the authentication process itself, and the binding between an authenticator and a specific individual's identifier. AAL is selected to mitigate potential authentication errors (i.e., a false claimant using a credential that is not rightfully theirs).
- **FAL (Federation Assurance Level)**: The robustness of the assertion protocol the federation uses to communicate authentication and attribute information (if applicable) to an RP. FAL is optional as not all digital systems will leverage federated identity architectures. FAL is selected to mitigate potential federation errors (an identity assertion is compromised).

The above three components align closely with the components in RFC8485, and similarly some of the components are out of scope for IEEE P1940 * The IAL component is outside the scope of IEEE P1940 as identity proofing occurs before a user engages in a P1940 transaction. * The FAL component is outside the scope of IEEE P1940 as P1940 transactions do not involve federated authentication assertions.

What remains relevant to IEEE P1940 is AAL which [SP-800-63-3] breaks down into these **Strength of Authenticator Assurance Levels**. * **AAL1** provides some assurance that the claimant controls an authenticator registered to the subscriber. AAL1 requires single-factor authentication using a wide range of available authentication technologies. Successful authentication requires that the claimant prove possession and control of the authenticator(s) through a secure authentication protocol. * **AAL2** provides high confidence that the claimant controls authenticator(s) registered to the subscriber. Proof of possession and control of two different authentication factors is required through a secure authentication protocol. Approved cryptographic techniques are required at AAL2 and above. * **AAL3** provides very high confidence that the claimant controls authenticator(s) registered to the subscriber. Authentication at AAL3 is based on proof of possession of a key through a cryptographic protocol. AAL3 is like AAL2 but also requires a "hard" cryptographic authenticator that provides verifier impersonation resistance. Approved cryptographic techniques are required. To authenticate at AAL3, claimants SHALL prove possession and control of two distinct authentication factors through secure authentication protocol(s).

To determine an appropriate AAL level [SP-800-63-3] provides a decision tree where you ask questions about these potential impacts from a fraudulent or false positive authentication for each transaction type being requested by a mobile app user.

> **Important**. A transaction type (such as an ATM cash withdrawal request or POS purchase) can have different risks depending on the cash value requested.

Potential impact of inconvenience, distress, or damage to standing or reputation: * Low: at worst, limited, short-term inconvenience, distress, or embarrassment to any party. * Moderate: at worst, serious short-term or limited long-term inconvenience, distress, or damage to the standing or reputation of any party. * High: severe or serious long-term inconvenience, distress, or damage to the standing or reputation of any party. This is ordinarily reserved for situations with particularly severe effects or which potentially affect many individuals

Potential impact of financial loss: * Low: at worst, an insignificant or inconsequential financial loss to any party, or at worst, an insignificant or inconsequential institution liability. * Moderate: at worst, a serious financial loss to any party, or a serious institution liability. * High: severe or catastrophic financial loss to any party, or severe or catastrophic institution liability.

Potential impact of harm to institution programs or public interests:

- Low: at worst, a limited adverse effect on organizational operations or assets, or public interests. Examples of limited adverse effects are: (i) mission capability degradation to the extent and duration that the organization is able to perform its primary functions with noticeably reduced effectiveness, or (ii) minor damage to organizational assets or public interests.
- Moderate: at worst, a serious adverse effect on organizational operations or assets, or public interests. Examples of serious adverse effects are: (i) significant mission capability degradation to the extent and duration that the organization is able to perform its primary functions with significantly reduced effectiveness; or (ii) significant damage to organizational assets or public interests.
- High: a severe or catastrophic adverse effect on organizational operations or assets, or public interests. Examples of severe or catastrophic effects are: (i) severe mission capability degradation or loss of to the extent and duration that the organization is unable to perform one or more of its primary functions; or (ii) major damage to organizational assets or public interests.

Potential impact of unauthorized release of sensitive information:

- Low: at worst, a limited release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in a loss of confidentiality with a low impact as defined in FIPS 199.
- Moderate: at worst, a release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a moderate impact as defined in FIPS 199.
- High: a release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a high impact as defined in FIPS 199.

Potential impact to personal safety: * Low: at worst, minor injury not requiring medical treatment. * Moderate: at worst, moderate risk of minor injury or limited risk of injury requiring medical treatment. * High: a risk of serious injury or death.

The potential impact of civil or criminal violations is: * Low: at worst, a risk of civil or criminal violations of a nature that would not ordinarily be subject to enforcement efforts. * Moderate: at worst, a risk of civil or criminal violations that may be subject to enforcement efforts. * High: a risk of civil or criminal violations that are of special importance to enforcement programs.

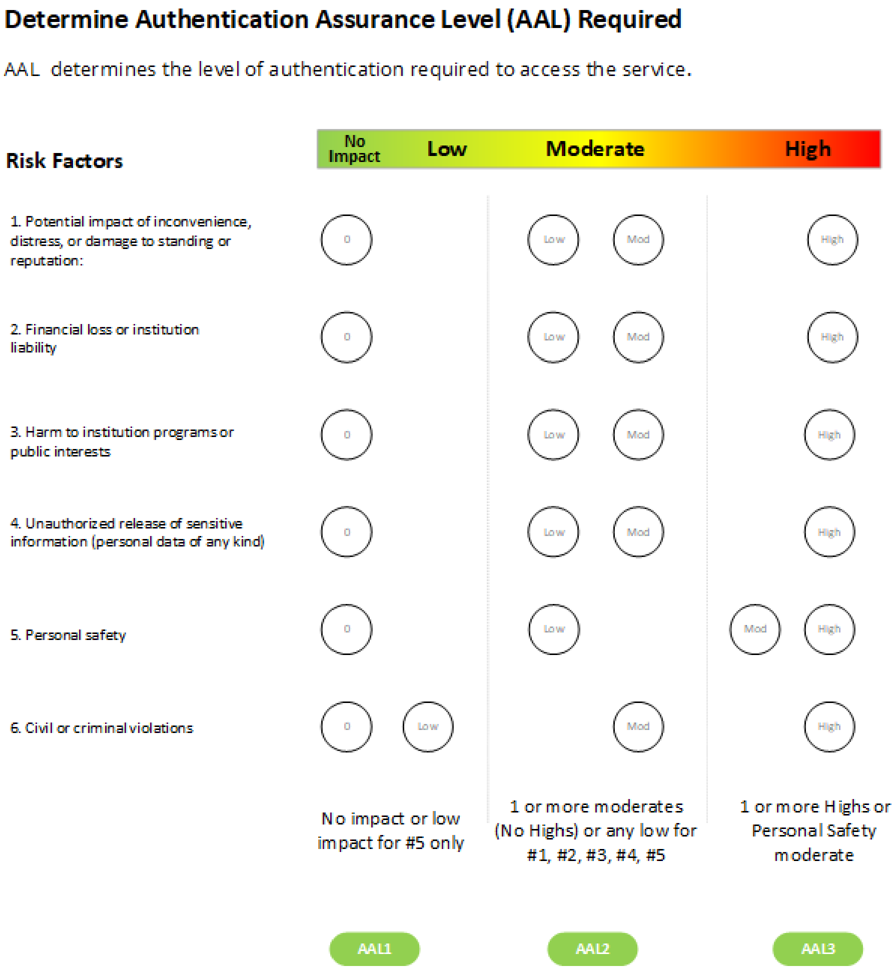
This decision matrix diagram derives from the decision tree diagram for selecting AAL in SP-800-63-3. The diagram resolves the full tree to its core decision matrix for ease of use.

SP-800-63-3 weights some questions so that a low or moderate impact response falls in the higher category. That weighting is reflected in this decision matrix for AAL.

Answering each of the above questions relative to the assets being protected leads to an appropriate AAL level.

When you have an AAL for a transaction type and value, apply the following rules to select appropriate authentication measures for that transaction type.

- For AAL1 (single-factor), use at least **one** authentication method and optionally, one or more additional security measures) as appropriate for the resource being protected.
- For AAL2 (two-factor), use at least **twov** authentication methods (and optionally, one or more additional security measures) as appropriate for the resource being protected.
- For AAL3 (multi-factor), use at least **two** authentication methods (and optionally, one or more additional security measures) as appropriate for the resource being protected.



Determine Authentication Assurance Level (AAL) Required

AAL determines the level of authentication required to access the service.

Risk Factors	No Impact	Low	Moderate	High
1. Potential impact of inconvenience, distress, or damage to standing or reputation:	0		Low Mod	High
2. Financial loss or institution liability	0		Low Mod	High
3. Harm to institution programs or public interests	0		Low Mod	High
4. Unauthorized release of sensitive information (personal data of any kind)	0		Low Mod	High
5. Personal safety	0		Low	Mod High
6. Civil or criminal violations	0	Low	Mod	High
	No impact or low impact for #5 only		1 or more moderates (No Highs) or any low for #1, #2, #3, #4, #5	1 or more Highs or Personal Safety moderate
	AAL1		AAL2	AAL3

Figure 5: AAL Decision Tree

6. Normative References

Appendix A. Acknowledgements

The IEEE Community would like to thank the following people for their contributions to this specification: John Callahan, Vince Endres, Bruce, Alan Theimann.

Appendix B. Notices

Appendix C. Document History

2019-12-31 * Initial draft completed.

Authors

John Callahan john.callahan@ieee.org