COMMONWEALTH OF VIRGINIA

IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL (IMSAC)

GUIDANCE DOCUMENT 1.C
Digital Identity Assertions

In accordance with Section 2.2-436 of the *Code of Virginia*, the Secretary of Technology, after consultation with the Secretary of Transportation, approved this Guidance Document regarding digital identity assertions. This Guidance Document shall be effective as of December 1, 2017 and shall remain in force and effect unless rescinded or amended by further action pursuant to Section 2.2-436 of the *Code of Virginia*.

Table of Contents

1 Publication Version Control

The following table contains a history of revisions to this publication.

Publication Version	Date	Revision Description
1.0	10/12/2016	Initial Draft of Document
1.0	05/01/2017	Document revised by VITA staff, in consultation with the Office of the Attorney General, in preparation for review by the Identity Management Standards Advisory Council (IMSAC)
1.0	06/05/2017	Document recommended by IMSAC for adoption by the Secretary of Technology

2 Reviews

- The initial version of the document was prepared by staff from the Virginia Information Technologies Agency (VITA) at the direction of the Identity Management Standards Advisory Council (IMSAC).

- The document was revised by VITA staff, in consultation with the Office of the Attorney General, in preparation for review by IMSAC.

3 Purpose and Scope

Pursuant to §§ 2.2-436 and 2.2-437, this guidance document was developed by IMSAC, and recommended to the Secretary of Technology, to establish minimum specifications for digital identity systems so as to warrant liability protection pursuant to the Electronic Identity Management Act ("the Act"), §§ 59.1-550 to -555. This guidance document was prepared to provide information or guidance of general applicability to the public for interpreting or implementing the Act. This guidance document was not developed as a Commonwealth of Virginia Information Technology Resource Management (ITRM) Policy, Standard, and Guideline, pursuant to § 2.2-2007, and therefore the guidance document is not applicable to executive branch agencies of the Commonwealth of Virginia.

The minimum specifications in this guidance document conform with the digital identity guidelines found in the March 31, 2017, Public Review version of the National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3). IMSAC will continue to monitor modifications to NIST SP 800-63-3 and may recommend to the Secretary of Technology revisions to the minimum specifications in order to maintain consistency with the NIST guidance.

4 Statutory Authority

The following section documents the statutory authority established in the Code of Virginia for the development of minimum specifications and standards for identity assertions within a digital identity system. References to statutes below and throughout this document shall be to the Code of Virginia, unless otherwise specified.

Governing Statutes:

Secretary of Technology
§ 2.2-225. Position established; agencies for which responsible; additional powers
http://law.lis.virginia.gov/vacode/title2.2/chapter2/section2.2-225/

Identity Management Standards Advisory Council
§ 2.2-437. Identity Management Standards Advisory Council
http://law.lis.virginia.gov/vacode/title2.2/chapter4.3/section2.2-437/

Commonwealth Identity Management Standards
§ 2.2-436. Approval of electronic identity standards
http://law.lis.virginia.gov/vacode/title2.2/chapter4.3/section2.2-436/

Electronic Identity Management Act
Chapter 50. Electronic Identity Management Act
http://law.lis.virginia.gov/vacode/title59.1/chapter50/

5 Terminology and Definitions

The core terms used within the digital identity management domain may be assigned a wide range of definitions, depending on the context or community of interest. For the purpose of the IMSAC guidance document series, the terminology has been defined in the IMSAC Reference Document: Terminology and Definitions, which may be accessed at http://vita.virginia.gov/default.aspx?id=6442475952

The IMSAC terminology aligns with the definitions published in the following documents:

- National Institute of Standards and Technology Special Publication 800-63-3 March 31, 2017 Public Review version, available at https://pages.nist.gov/800-63-3/sp800-63-3.html#sec3
- Electronic Identity Management Act (§ 59.1-550), available at http://law.lis.virginia.gov/vacode/title59.1/chapter50/section59.1-550
- International Telecommunication Union, Recommendation X. 1255, available at http://www.itu.int/ITU-T/recommendations/rec.aspx?id=11951&lang=en

6 Background

In 2015, the Virginia General Assembly passed the Electronic Identity Management Act (§§ 59.1-550 to -555) to address demand in the state's digital economy for secure, privacy enhancing digital authentication and identity management. Growing numbers of communities of interest have advocated for stronger, scalable and interoperable identity solutions to increase consumer protection and reduce liability for principal actors in the identity ecosystem – identity providers, credential service providers and relying parties.

To address the demand contemplated by the Electronic Identity Management Act, the General Assembly created the Identity Management Standards Advisory Council (IMSAC) to advise the Secretary of Technology on the adoption of identity management standards and the creation of guidance documents pursuant to §2.2-436. A copy of the IMSAC Charter has been provided in **Appendix 1**.

IMSAC recommends to the Secretary of Technology guidance documents relating to (i) nationally recognized technical and data standards regarding the verification and authentication of identity in digital and online transactions; (ii) the minimum specifications and standards that should be included in an identity trust framework, as defined in § 59.1-550, so as to warrant liability protection pursuant to the Electronic Identity Management Act (§§ 59.1-550 to -555); and (iii) any other related data standards or specifications concerning reliance by third parties on identity credentials, as defined in § 59.1-550.

Purpose Statement

This guidance document was developed by IMSAC, and recommended to the Secretary of Technology, to provide information or guidance of general applicability to the public for interpreting or implementing the Electronic Identity Management Act. Specifically, this guidance document establishes minimum specifications for assertions in a digital identity system. The minimum specifications conform with NIST SP 800-63C.

This guidance document defines assertion types, core components, presentation methods, security, and privacy provisions for assertions. The document assumes that specific business, legal, and technical requirements for assertions will be established in the identity trust framework for each distinct digital identity system, and that these requirements will be designed based on the digital authentication model, Identity Assurance Level (IAL), and Authenticator Assurance Level (AAL) requirements for the system.

This guidance document focuses on digital identity assertions. Separate IMSAC guidance documents in this series define minimum specifications for other components of a digital identity system.

7 Minimum Specifications

National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3) defines an assertion in a digital identity system as a statement from a verifier to a relying party (RP) that contains identity information about a subscriber. Assertions may also contain verified attributes.[6] Systems may use the authenticated identity to determine if that user is authorized to perform an electronic transaction.

This document establishes minimum specifications for assertions within a digital identity system. The minimum specifications assume that specific business, legal, and technical requirements for a digital identity system will be documented in the identity trust framework for that system. Minimum specifications for other components of a digital identity system have been documented in separate guidance documents in the IMSAC series, pursuant to § 2.2-436 and § 2.2-437.

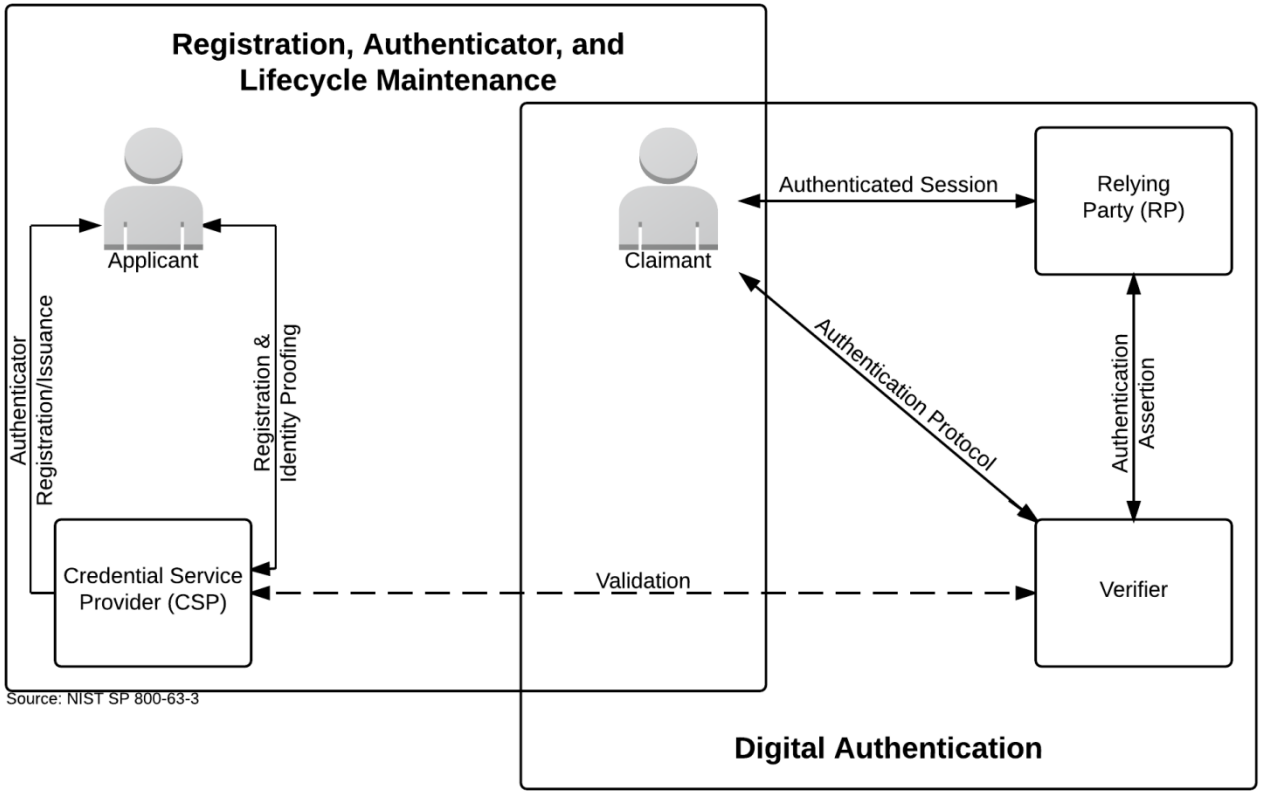
Digital Identity Model

Assertions play an integral role in digital authentication, the process of establishing confidence in individual identities presented to a digital identity system. Digital identity systems implement assertions as part of the process to authenticate a person's identity. In turn, the authenticated identity may be used to determine if that person is authorized to perform an online transaction. The minimum specifications in this document assume that the authentication and transaction take place across an open network, such as the internet.

The minimum specifications for assertions defined in this document reflect the digital authentication model used primarily by governmental entities. More complex models that separate functions among a broader range of parties are also available and may have advantages in some classes of applications. While a simpler model serves as the basis for these minimum specifications, it does not preclude members in digital identity systems from separating these functions. Minimum specifications for the digital identity model reflected in this document have been defined in *IMSAC Guidance Document 1: Digital Authentication*, and a graphic of the model has been shown in **Figure 1**.

[6] The Public Review version of National Institute of Standards and Technology Special Publication 800-63-3 (NIST SP 800-63-3) may be accessed at https://pages.nist.gov/800-63-3/sp800-63-3.html. At the time of the publication of this document, NIST SP 800-63-3 was still under development. However, this document may be updated, as recommended by IMSAC, following the final adoption and publication of NIST SP 800-63-3.

Figure 1. Digital Identity Model



Source: NIST SP 800-63-3, accessible at https://pages.nist.gov/800-63-3/sp800-63-3.html
Note: Figure 1 illustrates the model for digital authentication in a digital identity system, as documented in NIST SP 800-63-3 (Public Review), containing all components, requirements, and specifications recommended by IMSAC. However, the minimum specifications defined in this document have been developed to accommodate requirements for assertions established under other national and international standards.

Assertions

An assertion contains a set of claims or statements about an authenticated subscriber. assertions can be categorized along multiple orthogonal dimensions, including the characteristics of using the assertion or the protections on the assertion itself.

The core set of claims inside an assertion should include (but may not be limited to):

- Issuer: Identifier for the party that issued the assertion (usually the IdP)
- Subject: Identifier for the party that the assertion is about (the subscriber), usually within the namespace control of the issuer (identity provider, IdP)
- Audience: Identifier for the party intended to consume the assertion, primarily the RP
- Issuance: Timestamp indicating when the assertion was issued by the IdP
- Expiration: Timestamp indicating when the assertion expires and will no longer be accepted as valid by the relying party (RP) (Note: This is not the expiration of the session at the RP)
- Authentication Time: Timestamp indicating when the IdP last verified the presence of the subscriber at the IdP through a primary authentication event
- Identifier: Random value uniquely identifying this assertion, used to prevent attackers from manufacturing malicious assertions which would pass other validity checks

These core claims, particularly the issuance and expiration claims, apply to the assertion about the authentication event itself, and not to any additional identity attributes associated with the subscriber, even when those claims are included within the assertion. A subscriber's attributes may expire or be invalidated independently of the expiration or invalidation of the assertion.

Assertions may include other additional identity attributes. Privacy requirements for presenting attributes in assertions have been provided below in this document. The RP may fetch additional identity attributes from the IdP in a separate transaction using an authorization credential issued alongside the assertion.

Although details vary based on the exact authentication or federation protocols in use, an assertion should be used only to represent a single log-in event at the RP. After the RP consumes the assertion, session management at the RP comes into play and the assertion is no longer used directly. The expiration of the assertion must not represent the expiration of the session at the RP.

Assertion Binding

An assertion can be classified based on whether presentation by a claimant of an assertion reference or the assertion itself is sufficient for establishing the binding between the subscriber and the assertion, or if a stronger binding is required.

Holder-of-Key Assertions

A holder-of-key assertion contains a reference to a symmetric key or a public key (corresponding to a private key) possessed by and representing the subscriber. An RP may decide when to require the subscriber to prove possession of the key, depending on the policy of the RP. However, the RP must require the subscriber to prove possession of the key that is referenced in the assertion in parallel with presentation of the assertion itself in order for the assertion to be considered holder-of-key. Otherwise, an assertion containing reference to a key which the user has not proved possession of will be considered a bearer assertion.

The key referenced in a holder-of-key represents the subscriber, not any other party in the system. This key may be distinct from any key used by the subscriber to authenticate to the IdP. In proving possession of the subscriber's secret, the subscriber also proves with a certain degree of assurance that they are the rightful subject of the assertion. It is more difficult for an attacker to use a stolen holder-of-key assertion issued to a subscriber, since the attacker would need to steal the referenced key material as well.

Note that the reference to the key material in question is asserted by the issuer of the assertion as are any other claims therein, and reference to a given key must be trusted at the same level as all other claims within the assertion itself. The assertion must not include an unencrypted private or symmetric key to be used with holder-of-key presentation.

Bearer Assertions

A bearer assertion can be presented by any party as proof of the bearer's identity. If an attacker is able to capture or manufacture a valid assertion representing a subscriber, and that attacker is able to successfully present that assertion to the RP, then the attacker will be able to impersonate the subscriber at that RP.

Note that mere possession of a bearer assertion is not always enough to impersonate a subscriber. For example, if an assertion is presented in the federation model, additional controls may be placed on the transaction (such as identification of the RP and assertion injection protections) that help to further protect the RP from fraudulent activity.

Assertion Protection

Regardless of the binding mechanism used to obtain them, assertions must include an appropriate set of protections to the assertion data itself to prevent attackers from manufacturing valid assertions or re-using captured assertions at disparate RPs.

Assertion Identifier

Assertions must be sufficiently unique to permit unique identification by the target RP. Assertions may accomplish this by use of an embedded nonce, timestamp, assertion identifier, or a combination of these or other techniques.

Signed Assertion

Assertions may be cryptographically signed by the IdP, and the RP must validate the signature of each such assertion based on the IdP's key. This signature must cover all vital fields of the assertion, including its issuer, audience, subject, expiration, and any unique identifiers.

The assertion signature may be asymmetric based on the published public key of the IdP. In such cases, the RP may fetch this public key in a secure fashion at runtime (such as through an HTTPS URL hosted by the IdP), or the key may be provisioned out of band at the RP (during configuration of the RP). The signature may be symmetric based on a key shared out of band between the IdP and the RP. In such circumstances, the IdP must use a different shared key for each RP. All signatures must use approved signing methods.

Encrypted Assertion

Assertions may be encrypted in such a fashion as to allow only the intended audience to decrypt the claims therein. The IdP must encrypt the payload of the assertion using the RP's public key or a shared symmetric key. The IdP may fetch this public key in a secure fashion at runtime (such as through an HTTPS URL hosted by the RP), or the key may be provisioned out of band at the IdP (during registration of the RP). All encrypted objects must use approved cryptographic methods.

Audience Restriction

All assertions should use audience restriction techniques to allow an RP to recognize whether or not it is the intended target of an issued assertion. All RPs must check the audience of an assertion, if provided, to prevent the injection and replay of an assertion generated for one RP at another RP.

Pairwise Pseudonymous Identifiers

In some circumstances, it is desirable to prevent the subscriber's account at the IdP from being linked through one or more RPs through use of a common identifier. In these circumstances, pairwise pseudonymous identifiers must be used within the assertions generated by the IdP for the RP, and the IdP must generate a different identifier for each RP.

When unique pseudonymous identifiers are used with RPs alongside attributes, it may still be possible for multiple colluding RPs to fully identify and correlate a subscriber across digital identity systems using these attributes. For example, given that two independent RPs will each see the same subscriber identified with a different pairwise pseudonymous identifier, the RPs could still determine that the subscriber is the same person by comparing their name, email address, physical address, or other identifying attributes carried alongside the pairwise pseudonymous identifier. Privacy policies may prohibit such correlation, but pairwise pseudonymous identifiers can increase effectiveness of these policies by increasing the administrative effort in managing the attribute correlation.

Note that in a proxied federation model, the initial IdP may be unable to generate a pairwise pseudonymous identifier for the ultimate RP, since the proxy could blind the IdP from knowing which RP is being accessed by the subscriber. In such situations, the pairwise pseudonymous identifier is usually between the IdP and the federation proxy itself. The proxy, acting as an IdP, can itself provide pairwise pseudonymous identifiers to downstream RPs. Depending on the protocol, the federation proxy may need to map the pairwise pseudonymous identifiers back to the associated identifiers from upstream IdPs in order to allow the identity protocol to function. In such cases, the proxy will be able to track and determine which pairwise pseudonymous identifiers represent the same subscriber at different RPs.

Pairwise Pseudonymous Identifier Generation

Pairwise pseudonymous identifiers must be opaque and unguessable, containing no identifying information about the subscriber. Additionally, the identifiers must only be known by and used by one IdP-RP pair. An IdP may generate the same identifier for a subscriber at multiple RPs at the request of those RPs, but only if:

- Those RPs have a demonstrable relationship that justifies an operational need for the correlation, such as a shared security domain or shared legal ownership, and
- All RPs sharing an identifier consent to being correlated in such a manner.

The RPs must conduct a privacy risk assessment to consider the privacy risks associated with requesting a common identifier. The IdP must ensure that only intended RPs are correlated; otherwise, a rogue RP could learn of the Pseudonymous Identifier for a correlation by fraudulently posing as part of that correlation.

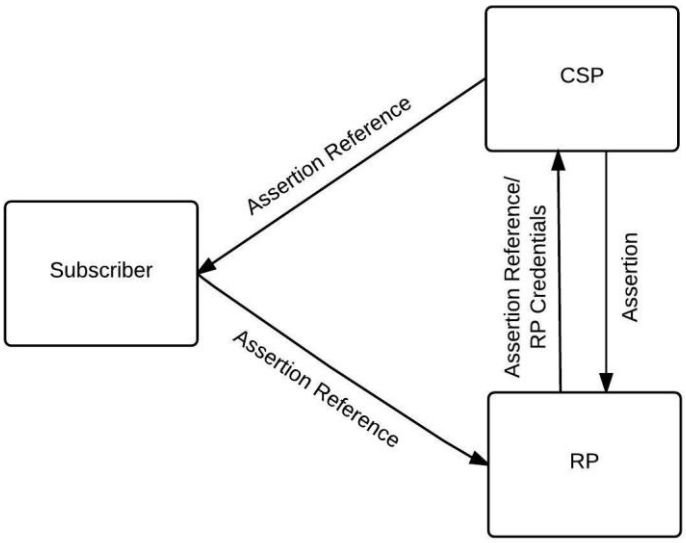
Assertion Presentation

Assertions may be presented in either a back-channel or front-channel manner from the IdP to the RP. Each model has its benefits and drawbacks, but both require the proper validation of the assertion. Assertions may also be proxied to facilitate federation between IdPs and RPs under specific circumstances. The IdP must transmit only those attributes that were explicitly requested by the RP. RPs must conduct a privacy risk assessment when determining which attributes to request.

Back-Channel Presentation

In the back-channel model, the subscriber is given an assertion reference to present to the RP, generally through the front channel. The assertion reference itself contains no information about the subscriber and must be resistant to tampering and fabrication by an attacker. The RP presents the assertion reference to the IdP, usually along with authentication of the RP itself, to fetch the assertion. **Figure 2** shows the back-channel presentation model.

Figure 2. Back-Channel Assertion Presentation



Source: NIST SP 800-63C

In the back-channel model, the assertion itself is requested directly from the IdP to the RP, minimizing chances of interception and manipulation by a third party (including the subscriber themselves). This method also allows the RP to query the credential service provider (CSP) for additional attributes about the subscriber not included in the assertion itself, since back-channel communication can continue to occur after the initial authentication transaction has completed.

The back-channel method also requires more network transactions than the front-channel model, but the information is limited to the only required parties. Since an RP is expecting to get an assertion only from the IdP directly, the attack surface is reduced since it is more difficult to inject assertions directly into the RP.

The Assertion Reference:

- Must be limited to use by a single RP
- Must be single-use
- Should be time limited with a short lifetime of seconds or minutes
- Should be presented along with authentication of the RP

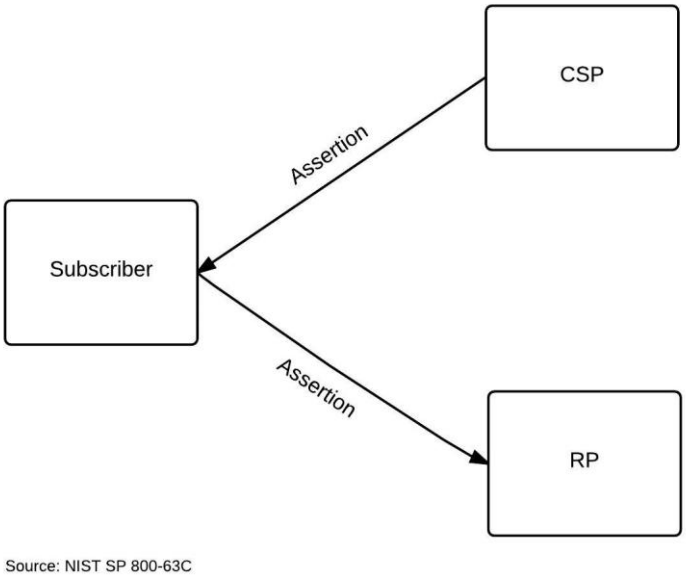
The RP must protect itself against injection of manufactured or captured assertion references by use of cross-site scripting protection or other accepted techniques. Claims within the assertion must be validated including issuer verification, signature validation, and audience restriction.

Conveyance of the assertion reference from the IdP to the subscriber as well as from the subscriber to the RP must be made over an authenticated protected channel. Conveyance of

the assertion reference from the RP to the IdP as well as the assertion from the IdP to the RP must be made over an authenticated protected channel. Presentation of the assertion reference at the IdP should require authentication of the RP before issuance of an assertion.

Front-Channel Presentation
In the front-channel model, the IdP creates an assertion and sends it to the subscriber after successful authentication. The assertion is used by the subscriber to authenticate to the RP. This is often handled by mechanisms within the subscriber's browser. **Figure 3** shows the front-channel presentation model.

Figure 3: Front-Channel Assertion Presentation



Source: NIST SP 800-63C

In the front-channel model, an assertion is visible to the subscriber, which could potentially cause leakage of system information included in the assertion. In this model, it is more difficult for the RP to query the IdP for additional attributes. Since the assertion is under the control of the subscriber, the front-channel presentation method allows the subscriber to submit a single assertion to unintended parties, perhaps by a browser replaying an assertion at multiple RPs. Even if the assertion is audience restricted and rejected by RPs, its presentation at unintended RPs could lead to leaking information about the subscriber and their online activities.

Though it is possible to intentionally create an assertion designed to be presented to multiple RPs, this method can lead to lax audience restriction of the assertion itself, which in turn could lead to privacy and security breaches for the subscriber across these RPs. Such multi-RP use is not recommended. Instead, RPs are encouraged to fetch their own individual assertions.

The RP must protect itself against injection of manufactured or captured assertions by use of cross-site scripting protection or other accepted techniques. Claims within the assertion must be validated including issuer verification, signature validation, and audience restriction.

Conveyance of the assertion from the IdP to the subscriber as well as from the subscriber to the RP must be made over an authenticated protected channel.

Security

IdPs, RPs, subscribers, and parties outside of a typical assertions transaction may be malicious or become compromised. An attacker might have an interest in modifying or replacing an assertion to obtain a greater level of access to a resource or service provided by an RP. They might be interested in obtaining or modifying assertions and assertion references to impersonate a subscriber or access unauthorized data or services.

Furthermore, it is possible that two or more entities may be colluding to attack another party. An attacker may attempt to subvert assertion protocols by directly compromising the integrity or confidentiality of the assertion data. For the purpose of these types of threats, authorized parties who attempt to exceed their privileges may be considered attackers.

Common attacks against assertion transmission transactions include the following:

- Assertion Manufacture/Modification: An attacker generates a forged assertion or modifies the content of an existing assertion (such as the authentication or attribute statements), causing the RP to grant inappropriate access to the subscriber. For example, an attacker may modify the assertion to extend the validity period and keep using an assertion; or a subscriber may modify the assertion to have access to information that they should not be able to view.
- Assertion Disclosure: Assertions may contain authentication and attribute statements that include sensitive subscriber information. Disclosure of the assertion contents can make the subscriber vulnerable to other types of attacks.
- Assertion Repudiation by the IdP: An assertion may be repudiated by an IdP if the proper mechanisms are not in place. For example, if an IdP does not digitally sign an assertion, the IdP can claim that it was not generated through the services of the IdP.
- Assertion Repudiation by the subscriber: Since it is possible for a compromised or malicious IdP to issue assertions to the wrong party, a subscriber can repudiate any transaction with the RP that was authenticated using only a bearer assertion.
- Assertion Redirect: An attacker uses the assertion generated for one RP to obtain access to a second RP.
- Assertion Reuse: An attacker attempts to use an assertion that has already been used once with the intended RP.

In some cases, the subscriber is issued some secret information so that they can be recognized by the RP. The knowledge of this information distinguishes the subscriber from attackers who wish to impersonate the them. In the case of holder-of-key assertions, this secret could already have been established with the IdP prior to the initiation of the assertion protocol.

In other cases, the IdP will generate a temporary secret and transmit it to the authenticated subscriber for this purpose. When this secret is used to authenticate to the RP, this temporary

secret will be referred to as a secondary authenticator. Secondary authenticators include assertions in the direct model, session keys in Kerberos, assertion references in the indirect model, and cookies used for authentication.

Threats to the secondary authenticator include the following:

- Secondary Authenticator Manufacture: An attacker may attempt to generate a valid secondary authenticator and use it to impersonate a subscriber.
- Secondary Authenticator Capture: An attacker may use a session hijacking attack to capture the secondary authenticator when the IdP transmits it to the subscriber after the primary authentication step, or the attacker may use a man-in-the-middle attack to obtain the secondary authenticator as it is being used by the subscriber to authenticate to the RP. If, as in the indirect model, the RP needs to send the secondary authenticator back to the IdP in order to check its validity or obtain the corresponding assertion data, an attacker may similarly subvert the communication protocol between the IdP and the RP to capture a secondary authenticator. In any of the above scenarios, the secondary authenticator can be used to impersonate the subscriber.

Finally, in order for the subscriber's authentication to the RP to be useful, the binding between the secret used to authenticate to the RP and the assertion data referring to the subscriber needs to be strong. In assertion substitution, a subscriber may attempt to impersonate a more privileged subscriber by subverting the communication channel between the IdP and RP, for example by reordering the messages, to convince the RP that their secondary authenticator corresponds to assertion data sent on behalf of the more privileged subscriber.

Threat Mitigation Strategies

Mitigation techniques are described below for each of the threats described in the last subsection:

- Assertion Manufacture/Modification: To mitigate this threat, the following mechanisms are used:
  - The assertion is digitally signed by the IdP. The RP checks the digital signature to verify that it was issued by a legitimate IdP.
  - The assertion is sent over a protected session such as TLS. In order to protect the integrity of assertions from malicious attack, the IdP is authenticated.
  - The assertion contains a non-guessable random identifier.
- Assertion Disclosure: To mitigate this threat, one of the following mechanisms are used:
  - The assertion is sent over a protected session to an authenticated RP. Note that, in order to protect assertions against both disclosure and manufacture/modification using a protected session, both the RP and the IdP need to be validated.
  - Assertions are signed by the IdP and encrypted for a specific RP. It should be noted that this provides all the same guarantees as a mutually authenticated protected session, and may therefore be considered equivalent. The general requirement for protecting against both assertion disclosure and assertion manufacture/modification may therefore be described as a mutually authenticated protected session or equivalent between the IdP and the RP.

- Assertion Repudiation by the IdP: To mitigate this threat, the assertion is digitally signed by the IdP using a key that supports non-repudiation. The RP checks the digital signature to verify that it was issued by a legitimate IdP.
- Assertion Repudiation by the subscriber: To mitigate this threat, the IdP issues holder-of-key assertions, rather than bearer assertions. The subscriber can then prove possession of the asserted key to the RP. If the asserted key matches the subscriber's presented key, it will be proof to all parties involved that it was the subscriber who authenticated to the RP rather than a compromised IdP impersonating the subscriber.
- Assertion Redirect: To mitigate this threat, the assertion includes the identity of the RP for which it was generated. The RP verifies that incoming assertions include its identity as the recipient of the assertion.
- Assertion Reuse: To mitigate this threat, the following mechanisms are used:
  - The assertion includes a timestamp and has a short lifetime of validity. The RP checks the timestamp and lifetime values to ensure the assertion is currently valid.
  - The RP keeps track of assertions that were consumed within a (configurable) time window to ensure that an assertion is not used more than once within that time window.
- Secondary Authenticator Manufacture: To mitigate this threat, one of the following mechanisms is used:
  - The secondary authenticator may contain sufficient entropy that an attacker without direct access to the IdP's random number generator cannot guess the value of a valid secondary authenticator.
  - The secondary authenticator may contain timely assertion data that is signed by the IdP or integrity protected using a key shared between the IdP and the RP.
- Secondary Authenticator Capture: To mitigate this threat, adequate protections are in place throughout the lifetime of any secondary authenticators used in the assertion protocol:
  - In order to protect the secondary authenticator while it is in transit between the IdP and the subscriber, the secondary authenticator is sent via a protected session established during the primary authentication of the subscriber.
  - In order to protect the secondary authenticator from capture as it is submitted to the RP, the secondary authenticator is used in an authentication protocol which protects against eavesdropping and man-in-the-middle attacks.
  - In order to protect the secondary authenticator after it has been used, it is never transmitted over an unprotected session or to an unauthenticated party while it is still valid.
- Assertion Substitution: To mitigate this threat, one of the following mechanisms is used:
  - Responses to assertion requests contain the value of the assertion reference used in the request or some other nonce that was cryptographically bound to the request by the RP.
  - Responses to assertion requests are bound to the corresponding requests by message order, as in HTTP, provided that assertions and requests are protected by a protocol such as TLS that can detect and disallow malicious reordering of packets.

Assertion Examples

The following represent three (3) types of assertion technologies: Security Assertion Markup Language (SAML) assertions, Kerberos tickets, and OpenID Connect tokens.

Security Assertion Markup Language (SAML)

SAML is an XML-based framework for creating and exchanging authentication and attribute information between trusted entities over the internet. As of this writing, the latest specification for [SAML] is SAML v2.0, issued 15 March 2005.
The building blocks of SAML include:

- Assertion XML schema which defines the structure of the assertion
- SAML Protocols which are used to request assertions and artifacts
- Bindings that define the underlying communication protocols (such as HTTP or SOAP) and can be used to transport the SAML assertions.

The three components above define a SAML profile that corresponds to a particular use case such as “Web Browser SSO.” SAML assertions are encoded in an XML schema and can carry up to three types of statements:

- Authentication statements include information about the assertion issuer, the authenticated subscriber, validity period, and other authentication information. For example, an authentication assertion would state the subscriber “John” was authenticated using a password at 10:32 p.m. on 06-06-2004.
- Attribute statements contain specific additional characteristics related to the subscriber. For example, subject “John” is associated with attribute “Role” with value “Manager.”
- Authorization statements identify the resources the subscriber has permission to access. These resources may include specific devices, files, and information on specific web servers. For example, subject “John” for action “Read” on “Webserver1002” given evidence “Role.”

Kerberos Tickets

The Kerberos Network Authentication Service [RFC 4120] was designed to provide strong authentication for client/server applications using symmetric-key cryptography on a local, shared network. Extensions to Kerberos can support the use of public key cryptography for selected steps of the protocol. Kerberos also supports confidentiality and integrity protection of session data between the subscriber and the RP. Even though Kerberos uses assertions, since it is designed for use on shared networks it is not truly a federation protocol.

Kerberos supports authentication of a subscriber over an untrusted, shared local network using one or more IdPs. The subscriber implicitly authenticates to the IdP by demonstrating the ability to decrypt a random session key encrypted for the subscriber by the IdP. (Some Kerberos variants also require the subscriber to explicitly authenticate to the IdP, but this is not universal.)

In addition to the encrypted session key, the IdP also generates another encrypted object called a Kerberos ticket. The ticket contains the same session key, the identity of the subscriber to whom the session key was issued, and an expiration time after which the session key is no longer valid. The ticket is confidentiality and integrity protected by a pre-established that is key shared between the IdP and the RP during an explicit setup phase.

To authenticate using the session key, the subscriber sends the ticket to the RP along with encrypted data that proves that the subscriber possesses the session key embedded within the Kerberos ticket. Session keys are either used to generate new tickets, or to encrypt and authenticate communications between the subscriber and the RP.

To begin the process, the subscriber sends an authentication request to the authentication Server (AS). The AS encrypts a session key for the subscriber using the subscriber's long term credential. The long term credential may either be a secret key shared between the AS and the subscriber, or in the PKINIT variant of Kerberos, a public key certificate. It should be noted that most variants of Kerberos based on a Shared Secret key between the subscriber and IdP derive this key from a user generated password. As such, they are vulnerable to offline dictionary attack by a passive eavesdropper.

In addition to delivering the session key to the subscriber, the AS also issues a ticket using a key it shares with the Ticket Granting Server (TGS). This ticket is referred to as a Ticket Granting Ticket (TGT), since the verifier uses the session key in the TGT to issue tickets rather than to explicitly authenticate the verifier. The TGS uses the session key in the TGT to encrypt a new session key for the subscriber and uses a key it shares with the RP to generate a ticket corresponding to the new session key. The subscriber decrypts the session key and uses the ticket and the new session key together to authenticate to the RP.

OpenID Connect

OpenID Connect is an internet-scale federated identity and authentication protocol built on top of the OAuth 2.0 authorization framework and the JSON Object Signing and Encryption (JOSE) cryptographic system. As of this writing, the latest specification is version 1.0 with errata, dated November 8, 2014.

OpenID Connect builds on top of the OAuth 2.0 authorization protocol to enable the subscriber to authorize the RP to access the subscriber's identity and authentication information. The RP in both OpenID Connect and OAuth 2.0 is known as the client.

In a successful OpenID Connect transaction, the IdP issues an ID Token, which is a signed assertion in JSON Web Token (JWT) format. The client parses the ID Token to learn about the subscriber and primary authentication event at the IdP. This token contains at minimum the following claims about the subscriber and authentication event:

- `iss` : HTTPS URL identifying the IdP that issued the assertion
- `sub` : IdP-specific subject identifier representing the subscriber

- `aud` : IdP-specific audience identifier, equal to the OAuth 2.0 client identifier of the client at the IdP
- `exp` : Timestamp at which the identity token expires and after which must not be accepted the client
- `iat` : Timestamp at which the identity token was issued and before which must not be accepted by the client

In addition to the identity token, the IdP also issues the client an OAuth 2.0 access token which can be used to access the UserInfo Endpoint at the IdP. This endpoint returns a JSON object representing a set of claims about the subscriber, including but not limited to their name, email address, physical address, phone number, and other profile information.

While the information inside the ID Token is reflective of the authentication event, the information in the UserInfo Endpoint is generally more stable and could be more general purpose. Access to different claims from the UserInfo Endpoint is governed by the use of a specially defined set of OAuth scopes, `openid`, `profile`, `email`, `phone`, and `address`. An additional scope, `offline_access`, is used to govern the issuance of refresh tokens, which allow the RP to access the UserInfo Endpoint when the subscriber is not present.

Privacy and Security

The minimum specifications established in this document for privacy and security in the use of person information for digital authentication apply the Fair Information Practice Principles (FIPPs).[9] The FIPPs have been endorsed by the National Strategy for Trusted Identities in Cyberspace (NSTIC) and NASCIO in its SICAM Guidance.[10]

The minimum specifications also adhere to the Identity Ecosystem Framework (IDEF) Baseline Functional Requirements (v.1.0) for privacy and security, adopted by the Identity Ecosystem Steering Group (IDESG) in October 2015 (**Appendix 2)**.

The minimum specifications for assertions apply the following FIPPs:

- Transparency: RAs and CSPs should be transparent and provide notice to applicants regarding collection, use, dissemination, and maintenance of person information required during the Registration, Identity Proofing and verification processes.
- Individual Participation: RAs and CSPs should involve the applicant in the process of using person information and, to the extent practicable, seek consent for the collection, use, dissemination, and maintenance of that information. RAs and CSPs also should provide mechanisms for appropriate access, correction, and redress of person information.
- Purpose Specification: RAs and CSPs should specifically articulate the authority that permits the collection of person information and specifically articulate the purpose or purposes for which the information is intended to be used.
- Data Minimization: RAs and CSPs should collect only the person information directly relevant and necessary to accomplish the Registration and related processes, and only retain that information for as long as necessary to fulfill the specified purpose.
- Use Limitation/Minimal Disclosure: RAs and CSPs should use person information solely for the purpose specified in the notice. Disclosure or sharing that information should be limited to the specific purpose for which the information was collected.
- Data Quality and Integrity: RAs and CSPs should, to the extent practicable, ensure that person information is accurate, relevant, timely, and complete.
- Security: RAs and CSPs should protect personal information through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
- Accountability and Auditing: RAs and CSPs should be accountable for complying with these principles, providing training to all employees and contractors who use person information, and auditing the actual use of person information to demonstrate compliance with these principles and all applicable privacy protection requirements.

[9] The term "person information" refers to protected data for person entities. This includes Personally Identifiable Information (PII), Protected Health Information (PHI), Federal Tax Information (FTI), Protected Education Records, and related categories. Specific requirements for the privacy and security of person information should be defined by the identity trust framework for the digital identity system.

[10] The FIPPs endorsed by NSTIC may be accessed at http://www.nist.gov/nstic/NSTIC-FIPPs.pdf . The FIPPs published in SICAM may be accessed at http://www.nascio.org/Portals/0/Publications/Documents/SICAM.pdf.

Appendix 1. IMSAC Charter

COMMONWEALTH OF VIRGINIA
IDENTITY MANAGEMENT STANDARDS ADVISORY COUNCIL
CHARTER

Advisory Council Responsibilities (§ 2.2-437.A; § 2.2-436.A)

The Identity Management Standards Advisory Council (the Advisory Council) advises the Secretary of Technology on the adoption of identity management standards and the creation of guidance documents pursuant to § 2.2-436.

The Advisory Council recommends to the Secretary of Technology guidance documents relating to (i) nationally recognized technical and data standards regarding the verification and authentication of identity in digital and online transactions; (ii) the minimum specifications and standards that should be included in an identity trust framework, as defined in § 59.1-550, so as to warrant liability protection pursuant to the Electronic Identity Management Act (§ 59.1-550 et seq.); and (iii) any other related data standards or specifications concerning reliance by third parties on identity credentials, as defined in § 59.1-550.

Membership and Governance Structure (§ 2.2-437.B)

The Advisory Council's membership and governance structure is as follows:

1. The Advisory Council consists of seven members, to be appointed by the Governor, with expertise in electronic identity management and information technology. Members include a representative of the Department of Motor Vehicles, a representative of the Virginia Information Technologies Agency, and five representatives of the business community with appropriate experience and expertise. In addition to the seven appointed members, the Chief Information Officer of the Commonwealth, or his designee, may also serve as an ex officio member of the Advisory Council.

2. The Advisory Council designates one of its members as chairman.

3. Members appointed to the Advisory Council serve four-year terms, subject to the pleasure of the Governor, and may be reappointed.

4. Members serve without compensation but may be reimbursed for all reasonable and necessary expenses incurred in the performance of their duties as provided in § 2.2-2825.

5. Staff to the Advisory Council is provided by the Office of the Secretary of Technology.

The formation, membership and governance structure for the Advisory Council has been codified pursuant to § 2.2-437.A, § 2.2-437.B, as cited above in this charter.

The statutory authority and requirements for public notice and comment periods for guidance documents have been established pursuant to § 2.2-437.C, as follows:

C. Proposed guidance documents and general opportunity for oral or written submittals as to those guidance documents shall be posted on the Virginia Regulatory Town Hall and published in the Virginia Register of Regulations as a general notice following the processes and procedures set forth in subsection B of § 2.2-4031 of the Virginia Administrative Process Act (§ 2.2-4000 et seq.). The Advisory Council shall allow at least 30 days for the submission of written comments following the posting and publication and shall hold at least one meeting dedicated to the receipt of oral comment no less than 15 days after the posting and publication. The Advisory Council shall also develop methods for the identification and notification of interested parties and specific means of seeking input from interested persons and groups. The Advisory Council shall send a copy of such notices, comments, and other background material relative to the development of the recommended guidance documents to the Joint Commission on Administrative Rules.

This charter was adopted by the Advisory Council at its meeting on December 7, 2015. For the minutes of the meeting and related IMSAC documents, visit:
https://vita.virginia.gov/About/default.aspx?id=6442474173

Appendix 2. IDESG Identity Ecosystem Framework (IDEF) Baseline Functional Requirements (v.1.0) for Privacy and Security

PRIVACY-1. DATA MINIMIZATION
Entities MUST limit the collection, use, transmission and storage of personal information to the minimum necessary to fulfill that transaction's purpose and related legal requirements. Entities providing claims or attributes MUST NOT provide any more personal information than what is requested. Where feasible, IDENTITY-PROVIDERS MUST provide technical mechanisms to accommodate information requests of variable granularity, to support data minimization.

PRIVACY-2. PURPOSE LIMITATION
Entities MUST limit the use of personal information that is collected, used, transmitted, or stored to the specified purposes of that transaction. Persistent records of contracts, assurances, consent, or legal authority MUST be established by entities collecting, generating, using, transmitting, or storing personal information, so that the information, consistently is used in the same manner originally specified and permitted.

PRIVACY-3. ATTRIBUTE MINIMIZATION
Entities requesting attributes MUST evaluate the need to collect specific attributes in a transaction, as opposed to claims regarding those attributes. Wherever feasible, entities MUST collect, generate, use, transmit, and store claims about USERS rather than attributes. Wherever feasible, attributes MUST be transmitted as claims, and transmitted credentials and identities MUST be bound to claims instead of actual attribute values.

PRIVACY-4. CREDENTIAL LIMITATION
Entities MUST NOT request USERS' credentials unless necessary for the transaction and then only as appropriate to the risk associated with the transaction or to the risks to the parties associated with the transaction.

PRIVACY-5. DATA AGGREGATION RISK
Entities MUST assess the privacy risk of aggregating personal information, in systems and processes where it is collected, generated, used, transmitted, or stored, and wherever feasible, MUST design and operate their systems and processes to minimize that risk. Entities MUST assess and limit linkages of personal information across multiple transactions without the USER's explicit consent.

PRIVACY-6. USAGE NOTICE
Entities MUST provide concise, meaningful, and timely communication to USERS describing how they collect, generate, use, transmit, and store personal information.

PRIVACY-7. USER DATA CONTROL
Entities MUST provide appropriate mechanisms to enable USERS to access, correct, and delete personal information.

PRIVACY-8. THIRD-PARTY LIMITATIONS
Wherever USERS make choices regarding the treatment of their personal information, those choices MUST be communicated effectively by that entity to any THIRD-PARTIES to which it transmits the personal information.

PRIVACY-9. USER NOTICE OF CHANGES
Entities MUST, upon any material changes to a service or process that affects the prior or ongoing collection, generation, use, transmission, or storage of USERS' personal information, notify those USERS, and provide them with compensating controls designed to mitigate privacy risks that may arise from those changes, which may include seeking express affirmative consent of USERS in accordance with relevant law or regulation.

PRIVACY-10. USER OPTION TO DECLINE
USERS MUST have the opportunity to decline Registration; decline credential provisioning; decline the presentation of their credentials; and decline release of their attributes or claims.

PRIVACY-11. OPTIONAL INFORMATION
Entities MUST clearly indicate to USERS what personal information is mandatory and what information is optional prior to the transaction.

PRIVACY-12. ANONYMITY
Wherever feasible, entities MUST utilize identity systems and processes that enable transactions that are anonymous, anonymous with validated attributes, pseudonymous, or where appropriate, uniquely identified. Where applicable to such transactions, entities employing service providers or intermediaries MUST mitigate the risk of those THIRD-PARTIES collecting USER personal information. Organizations MUST request individuals' credentials only when necessary for the transaction and then only as appropriate to the risk associated with the transaction or only as appropriate to the risks to the parties associated with the transaction.

PRIVACY-13. CONTROLS PROPORTIONATE TO RISK
Controls on the processing or use of USERS' personal information MUST be commensurate with the degree of risk of that processing or use. A privacy risk analysis MUST be conducted by entities who conduct digital identity management functions, to establish what risks those functions pose to USERS' privacy.

PRIVACY-14. DATA RETENTION AND DISPOSAL
Entities MUST limit the retention of personal information to the time necessary for providing and administering the functions and services to USERS for which the information was collected, except as otherwise required by law or regulation. When no longer needed, personal information MUST be securely disposed of in a manner aligning with appropriate industry standards and/or legal requirements.

PRIVACY-15. ATTRIBUTE SEGREGATION
Wherever feasible, identifier data MUST be segregated from attribute data.

SECURE-1. SECURITY PRACTICES
Entities MUST apply appropriate and industry-accepted information security STANDARDS, guidelines, and practices to the systems that support their identity functions and services.

SECURE-2. DATA INTEGRITY
Entities MUST implement industry-accepted practices to protect the confidentiality and integrity of identity data—including authentication data and attribute values—during the execution of all digital identity management functions, and across the entire data lifecycle (collection through destruction).

SECURE-3. CREDENTIAL REPRODUCTION
Entities that issue or manage credentials and tokens MUST implement industry-accepted processes to protect against their unauthorized disclosure and reproduction.

SECURE-4. CREDENTIAL PROTECTION
Entities that issue or manage credentials and tokens MUST implement industry-accepted data integrity practices to enable individuals and other entities to verify the source of credential and token data.

SECURE-5. CREDENTIAL ISSUANCE
Entities that issue or manage credentials and tokens MUST do so in a manner designed to assure that they are granted to the appropriate and intended USER(s) only. Where Registration and credential issuance are executed by separate entities, procedures for ensuring accurate exchange of Registration and issuance information that are commensurate with the stated assurance level MUST be included in business agreements and operating policies.

SECURE-6. CREDENTIAL UNIQUENESS
Entities that issue or manage credentials MUST ensure that each account to credential pairing is uniquely identifiable within its namespace for authentication purposes.

SECURE-7. TOKEN CONTROL
Entities that authenticate a USER MUST employ industry-accepted secure authentication protocols to demonstrate the USER's control of a valid token.

SECURE-8. MULTIFACTOR AUTHENTICATION
Entities that authenticate a USER MUST offer authentication mechanisms which augment or are alternatives to a password.

SECURE-9. AUTHENTICATION RISK ASSESSMENT
Entities MUST have a risk assessment process in place for the selection of authentication mechanisms and supporting processes.

SECURE-10. UPTIME
Entities that provide and conduct digital identity management functions MUST have established policies and processes in place to maintain their stated assurances for availability of their services.

SECURE-11. KEY MANAGEMENT
Entities that use cryptographic solutions as part of identity management MUST implement key management policies and processes that are consistent with industry-accepted practices.

SECURE-12. RECOVERY AND REISSUANCE
Entities that issue credentials and tokens MUST implement methods for reissuance, updating, and recovery of credentials and tokens that preserve the security and assurance of the original Registration and credentialing operations.

SECURE-13. REVOCATION
Entities that issue credentials or tokens MUST have processes and procedures in place to invalidate credentials and tokens.

SECURE-14. SECURITY LOGS
Entities conducting digital identity management functions MUST log their transactions and security events, in a manner that supports system audits and, where necessary, security investigations and regulatory requirements. Timestamp synchronization and detail of logs MUST be appropriate to the level of risk associated with the environment and transactions.

SECURE-15. SECURITY AUDITS
Entities MUST conduct regular audits of their compliance with their own information security policies and procedures, and any additional requirements of law, including a review of their logs, incident reports and credential loss occurrences, and MUST periodically review the effectiveness of their policies and procedures in light of that data.