The following information was posted with the attached DRAFT document:

NIST Released NISTIR 7817, A Credential Reliability and Revocation Model for Federated Identities

November 30, 2012

NIST announces the release of NIST Interagency Report (NISTIR) 7817, A Credential Reliability and Revocation Model for Federated Identities. NISTIR 7817 describes and classifies the different types of identity providers serving federations. For each classification, the document identifies perceived improvements or gabs when the credentials are used in authentication services and recommends counter measures to eliminate some of identified gaps. With the countermeasures as the basis, the document suggests a Universal Credential Reliability and Revocation Services (URRS) model that strives improve authentication services for federations.

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

A Credential Reliability and Revocation Model for Federated Identities

Hildegard Ferraiolo
…..
…..
…..

DRAFT NISTIR 7817

A Credential Reliability and Revocation Model for Federated Identities

Hildegard Ferraiolo

C O M P U T E R S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

December 2011

U.S. Department of Commerce
John E. Bryson, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary for Standards and Technology and Director

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 analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Interagency Report discusses ITL's research, guidance, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Interagency Report
23 pages (2011)

Abstract

A large number of IDentity Management Systems (IDMSs) are being deployed worldwide that use different technologies for the population of their users. With the diverse set of technologies, and the unique business requirements for organizations to federate, there is no uniform approach to the federation process. Similarly, there is no uniform method to revoke credentials or their associated attribute(s) in a federated community. In the absence of a uniform revocation method, this document seeks to investigate credential and attribute revocation with a particular focus on identifying missing requirements for credential and attribute revocation. This document first introduces and analysis the different types of digital credentials and recommends missing revocation-related requirements for each model in a federated environment.

As a second goal, and as by-product of the analysis and recommendations, this paper suggests a credential reliability and revocation service that serves to eliminate the missing requirements and involves all the entities of the federation.

Table of Contents

1. Introduction

Identity providers establish and manage their user community's digital identities. These identities (in the form of digital credentials) are used by the user to authenticate to service providers. The digital identity technology deployed by an identity provider for the population of their users varies and often dictates a specific authentication solution in order for the service provider to authenticate the user.

A federated community accommodates two or more identity provider along with the specific authentication solution. With the diverse set of identity providers, and the unique business requirements for organizations to federate, there is no uniform approach in the federation process. Similarly, there is no uniform method to revoke credentials or their associated attribute(s). In the absence of a uniform method, this document investigates credential and attributes revocation with a particular focus on identifying missing requirements for revocation. As a by-product of the analysis and recommendations, this document also suggests a model for credential reliability and revocation services that serves to eliminate some of the missing requirements.

2. Identity Provider Models and Recommendations

For the purpose of this document, the identity provider and associated authentication solutions can be categorized according to the number of parties involved in an authentication event. The 2-party model, for example, involves only the service provider and the credential holder (user) in the authentication event. The 4-party model, on the far spectrum, involves the credential holder, an independent identity provider, the service provider and one or more independent attributes providers that voucher for attributes requested by the service provider. These and other models are discussed in this section. Where applicable, recommendations are identified to improve credential revocation.

2.1. The Two-Party Model (2 legged)

The two parties in the authentication event are the user and the service provider. In this case, the service provider also acts as the identity provider. The two-party model is the most frequently used scheme of today. The user registers with each service provider separately, and receives a digital credential (usually username and password) after completing the registration process. These credentials are used for subsequent logins to the service providers. With a 2-party model, the user is forced to remember (or carry) credentials for each service he/she subscribes to. The 2-party model is generally not part of federations, except by loose interpretation or by extension, where it is used in an enterprise's single-sign-on (SSO) applications.

> **Recommendation 1:** In enterprise SSO solutions, services providers receive an assertion that asserts a successful prior authentication event by the enterprise's SSO authentication server. In cases where the session has been tampered by an attacker [1]or in cases where the attackers compromised the credential (e.g., pharming or phishing attacks), a service provider or application may detect suspicious activities of the attacker. Based on this knowledge, the service provider may prevent further malicious activities with other service provider by reporting the incident to the enterprise's SSO authentication server, resulting in a suspension of the credential. A reporting and revocation procedure, therefore, is beneficial to protecting the enterprise SSO environment.

2.1.1. Delegation

In some instances, a third party application may provide services by accessing a user's primary service. For example a third party smart phone application may offer a message consolidation service by gathering and displaying email, text messages and instant messaging in one place - its application. The consolidation service requires the username and password for each service it consolidates in order to access, retrieve, and display the messages in its consolidation application.

[1] A session could be subject to man-in-the-middle attack, or session hijacking. Other attacks originate at the service provider may include Cross-Site Request Forgery (CSRF) or Cross-Site Scripting (XSS).

By sharing a password and username (i.e., the credential and its secret) with a third party service, the user gives un-controlled access to the third party application. As much as possible, such services should not be used, as it gives unlimited access to another party. In addition, should malicious activity occur that originated at the third party, the primary service is likely to revoke access privileges; and as a result, block the user out of the primary service.

To disable third party application, a user can simply change the credential (username and/or password) at the primary.

> **Recommendation 2:** In federated communities, delegation technologies should be considered. With delegation technologies, the service provider issues delegation credentials that are tailored for access to data and/or processes limited to third party service, but excludes access rights to anything else, such as user settings and controls. With delegations, and should malicious third party activities occur, the primary service revokes the delegated credential, while the user credential remains valid. At the same time, the user is protected by Denial of Service (DoS) attacks. Delegations of a service should also be time-constraint, by limiting the access of a third party service to the time necessary to perform the delegated service.

> **Recommendation 3:** For time-insensitive delegations, a user or service provider in the federations should have the ability to terminate a delegated service through a delegation revocation procedure.

2.2. The Three-Party Model (3 legged)

A 3-party model involves a user, an independent identity provider, and a service provider. In general, the user authenticates to the identity provider. After successful authentication, the identity provider issues an assertion to the service provider indicating that the user has successfully authenticated to the identity provider. The service provider in this case outsources authentication to the identity provider and accepts the authentication assertion of the identity provider.

A service provider accepts the user's access requests to its service based on successful authentication assertion from the identity provider. As is the case with the two-party model, the service provider needs to protect its resources from unauthorized and malicious access. It employs a variety of defense mechanisms[2] to detect and guard against attacks such as phishing, cross-site scripting, session hijacking as best as possible.

Malicious activities at the service provider are not generally shared with the identity provider. This situation is unfortunate, as the service provider is at the forefront of attacks. It has all audit trails and knowledge of suspicious or malicious account activities. The user could potentially be a victim of a phishing attack by directing the user to a mock identity provider for authentication, and thereby learn the username and/or password. With the phished username and passwords, the attacker authenticates to the actual identity provider to acquire an assertion. The attacker subsequently tries several service providers to access the user's federated services and accounts. Unaware of the attack, a service provider accepts the

[2] SP 800-63-1, section 9 and 10 describes specific threat mitigation techniques for authentication threats.

assertion and grants access. The service provider, however, may detect unusual or suspicious account activities and blocks the user out. With the feedback from the affected service provider, the identity provider could suspend the user and prevent further attacks at other federated services. Service provider feedback is especially useful and indicative in the federations since the feedbacks are likely reported by several service providers in the federation, and thus providing strong evidence of credential compromise. The user as well as the service is saved time, money and damage because of service provider's feedback and identity provider's suspension actions.

> **Recommendation 4:** A reporting service for credential revocation/suspension is necessary in order for the service provider to provide feedback on malicious use of credentials.

2.2.1. Single Sign On Schemes

Service providers in the 3-party model may be part of a federated Single Sign On environment where an identity provider authenticates the user once on behave of the service providers. All service providers accept the authentication assertions and give the user access to their services without the need for the user to re-authenticate for each service individually. The threats from assertion miss-use are limited when identity providers issue short term assertions for the service provider. While short-term assertions are a deterrent for attackers, they do not mitigate threats resulting from the user's long term credential that was used to authenticate to the identity provider. If the long term credential has been compromised, an attacker could use the credential to authenticate to the identity provider and proceed undetected to exploit several service providers. A federated SSO environment therefore can benefit from service providers reporting suspicious or malicious account activities and for identity providers to suspend a credential based on the feedback.

> **Recommendation 5:** The previously described phishing attack and other attacks against long term user credential is a concern in federated single sign-on environment. Based on the service provider's audit trail and risk mitigation techniques, the service provider may be able to prevent further malicious activities for other service providers by reporting incidents to the identity provider. A reporting service for credential revocation/suspension, therefore, is beneficial to protecting the federated SSO environment.

2.2.2. Privacy Enhancing Technologies

Privacy enhancing models seek to minimize the exposure of user attributes and user information; thereby limiting attributes disclosure to service provider based on the "need-to-know" or "least privileged" security mantra. Privacy enhancing protocols also limit the identity provider and service provider's ability to collect and link the user's login habits. There is no transaction handle and the user can register and use pseudonyms with each service provider or even stay anonymity with a service provider. Most privacy enhancing authentication protocols are based on selective disclosure schemes where the user has more control to selectively present some attributes, while hiding (i.e., zero knowledge) other irrelevant attributes in the interaction with the service provider. Other schemes do not disclose an attribute value (say, date of birth) at all. Instead, these privacy enhancing technologies can dynamically calculate and proof a predicate/condition (above 21) for the service provider, instead of revealing user attribute (the date of birth). Privacy enhancing protocols involve the identity provider only minimally. The identity provider signs the user's attributes and issues zero-knowledge enabled credentials to the user. The user,

in turn, establishes a login account with the service provider with a pseudonym or by establishing an anonymous login account. On subsequent login, the user presents the credential with the service without further interaction/authentication with the identity provider. The identity provider therefore is out of the loop and cannot collect user's internet footprint. Similarly, the service provider does not interact with the identity provider beyond simply verifying the identity provider's signature on the credential. No transaction handle is involved.

Recommendation 6: While privacy enhancing schemes offer enhancements to information disclosure, it suffers from the lack of identity provider involvement in the authentication event. Without the identity provider's involvement, the status of a user's credential cannot be determined by the service provider. Where the status of a credential/attribute is important to the federation, therefore, a service provider may benefit from a black-list as part of a federated revocation mechanism.

Recommendation 7: Black lists are posted by the identity provider and constructed primarily based on feedback received from users or based on individuals reporting a lost, stolen, or compromised credential. The black list mechanism is valuable, but seems to exclude service provider feedback. Service providers are the primary entities that have first-hand information about malicious account activities. As is the case in the previous recommendation, with service provider feedback, malicious incidents could be reported by the service provider to the identity provider. As a result, the identity provider could suspend the credential and protect the user from further attacks. To implement this measure, a trusted third party, (the revocation service of the federation) would have to perform the task of anonymity revocation and credential suspension/ revocation.

2.3. The Four-Party Model (4 legged)

In the four-party authentication model, an attribute provider is introduced in addition to the identity provider, service provider and user. The need for attributes, in addition to user identification and authentication stems from existing and newer access control models such as Attribute-Based Access Control (ABAC) or Role-Based Access Control (RBAC), where combinations of attributes (authorization attributes) are evaluated at the access decision point of the service to determine authorized access. The four-Party model can be further sub-categorized in accordance to the source of the attributes: 1) single source, where the service provider relies on a single source to provide attributes in an authentication event, and 2) multi source, where the service provider relies on several independent attribute providers to provide attributes in an authentication and authorization event.

2.3.1. Single Source Attribute Providers

The most common single source attribute provider is the identity provider. Single source attribute provider in a federated communities, have generally pre-agreed authorization attributes. These attributes are maintained by the user's identity provider (issuer) and sent to the service provider as part of an authentication event to provide authorization context in the form of assertions. An example of this model is the Backend Attribute Exchange (BAE), an interagency attribute exchange mechanism used in addition to PIV cardholder authentication, where a federal agency service provider can request additional attributes

about a PIV cardholder from other agencies (e.g., the issuer/identity provider) to enhance authentication and determine access control privileges. Another example is the First/ Emergency Response Official (F/ERO) system where attributes such as knowledge, skills, and abilities of first responders are verified at incident control sites. The arriving first responder presents his/her First Responder Access Card (FRAC) at the incident site, where he or she is authenticated using the digital credentials on the First Responder Access Card. The attributes are pre-loaded from the F/ERO Attribute Repository in the access control station and linked to the FRAC credentials at the authentication event, so that these attribute can be used for informed decision-making (for example, whether the first responder should be allowed access to a particular area during an emergency) .

> **Recommendation 8:** The types of attributes accepted by the federation are defined at federation establishment. Federated attributes, in turn, are assigned to the users at credential enrollment. They can be asserted by the user but validated by the identity provider. Where attributes serve a critical part in the roles or the functions a user is permitted to perform, it is important for attributes to be up-to-date. The identity provider; therefore, should check the authoritive source(s) for attribute updates (e.g., changes in the attribute qualification, revocation, suspension).

2.3.2. Multi-Source Attribute Providers

There are situations, where identity provider is not the attribute provider. Other authoritive sources are consulted independently. These sources may include credit bureaus or a background investigation services. With multi-source attribute providers, therefore, the service provider aggregates attributes from several sources or, receives aggregated attributes from an aggregation service to make an access decision. The multi-source attribute provider model is less common, because of the added complexity and extended trust model required and the lack of a standards based approach to multi source attribute aggregation. The complexity, in part, is due to the lack of a standards based aggregation technique that correlates the different sources to the same user.

2.3.2.1. Attribute Aggregation

An aggregation service collects all service provider-requested attributes. The collection of attributes is subsequently used by the service provider to determine access privileges. Attribute aggregator services are discussed in the next two sections.

2.3.2.2 Service Provider as the Aggregation Agent:

When the service provider aggregated attributes, it accumulates the attributes from the attribute providers at the authentication event in order to determine access privileges to its services. Ideally, the user consents to the release of attributes by authenticating to each attribute provider individually and authorized the release to the service provider. A mechanism to correlate and aggregate the different attribute assertions received for a user has to exist in this model in order for the service provider to link the attribute to the same person. A simple method to correlate attributes is to use the same credential throughout the authentication event – including authentication to the identity provider as well to all attribute providers.

Recommendation 9: As a benefit of using the same credential, and with service provider feedback mechanisms, the authentication decisions by the attribute provider and identity provider is based on the same status of the credential.

2.3.2.3 External Aggregation Agent

In this model, either the identity provider or an independent service acts as the aggregation agent, by collecting the attributes on behave of the service provider from various identity providers or attribute providers sources. The collection of attributes is subsequently provided to the service provider in a single transaction. A federation service (e.g. URRS, section 3), can accumulate or correlate the credential used for authentication of all parties.

3. The Uniform Reliability and Revocation Service (URRS)

In federations, service providers relinquish control of maintaining their own population of user credentials by accepting credential managed by a 3rd party identity provider. These 3rd party credentials are not issued for the sole purpose of one service; they serve other service providers within the federation as well. To accept 3rd party credentials, therefore, involves some risks, even if a trust framework is established. There are threats from other service providers, the 3rd party identity provider and the users. For example, service providers may be vulnerable to cross site scripting, while user may be tricked into phishing schemes or subject to pharming. As a result (and because these credentials are accepted by many service provider), attacks geared at one service and its user is a threat to all other federated services.

The URRS strives to mitigate some of threats identified in section 2 by providing a collaborative tool for all parties of the federated community to contribute to and participate in the credential reliability and revocation service, including the user and the service provider. Involving all parties will enhance acceptance and trust in the credentials by giving the stakeholders with the most risk (e.g., financial lose) the ability to monitor and report credentials. Participation by the user and service provider will lead to closely surveyed credentials and, eventually to more trusted credentials. Attackers, on the other hand, will have limited success in repeat miss-use of a credential because of the monitoring, reporting and revocation features of the URRS.

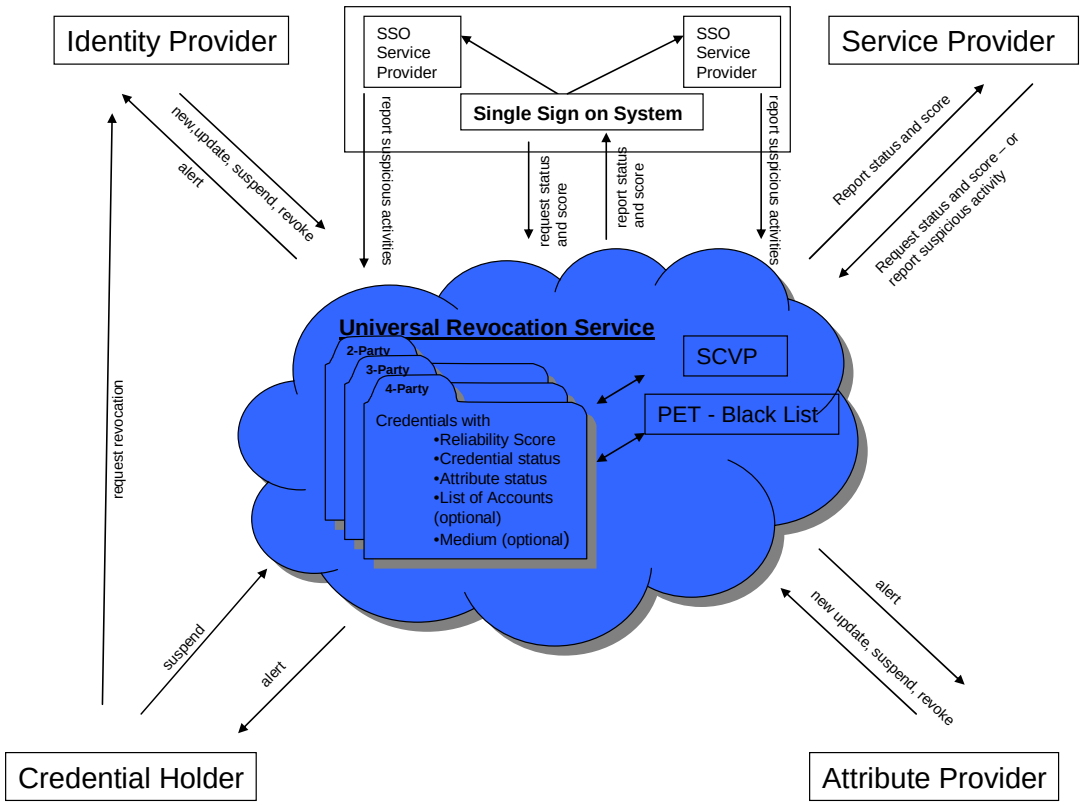
The proposed Uniform Reliability and Revocation Service (URRS) provides revocation status information to and from identity providers, service providers, attribute providers and users. Revocation services include traditional revocation checks such as such as CRL or OCSP check for PKI-based credentials. The URRS also includes credential revocation services that incorporate some of the missing requirements identified in section 2 as a federation service. Inclusion of missing requirements in an URRS will depend on the types of model of the federated community. For example, a federated community without federated privacy enhancing technology would not include recommended features in section 2.2.2.

The service provider feedback to the URRS results in a credential's reliability score that decreases the reliability with each negative feedback, and may cause the URRS to lower the credential status to 'suspended' should the score reach a pre-established low-score. Suspension actions can be initiated by the identity provider or by the user regardless of the reliability score. The reliability score also serves as a tool for service providers to determine the suitability of a presented credential in an authentication event. The service provider may decline the credential, if the reliability score is low. The reliability mechanism will limit, as a result, attacker's success in repeat attack of a credential.

In addition to the credential reliability and revocation service, the URRS also attempts to address revocation to a credential medium where the user has several credential in one medium – e.g., smart card and revocation of derived credentials. Medium revocation and derived credential revocation is discussed in section 4.

The URRS is designed to serve a federated system with diverse set of federated identity types. The entities of the URRS are depicted in Figure 1 and their roles in universal revocation are described in more details in section 3.1 through 3.4.

Figure 1 - Universal Credential Revocation Service



The URRS in figure 1 includes all possible entities in the federation. However, depending on the federation, only a few entities may be involved. For example, a federated community without federated privacy enhancing identities would not include the PET black list.

3.1. Universal Revocation Service's Role:

The URRS is the central information collection and distribution point of credential status information and its reliability. The URRS' role is to:

- Maintain credential status (ACTIVE, SUSPENDED, REVOKED)
- Communicate credential status and reliability scores to service providers and in order for the service provider to make a risk based decision to accept or decline the proposed credential for authentication
- Maintain reliability score for each ACTIVE credential and
    - Lower the reliability score in cases where the pre-established reliability threshold has not been reached. The credential status in this case remains ACTIVE.
    - Update the credential status to SUSPENDED" in cases where pre-established reliability threshold has been reached
    - Update the credential status to REVOKED as requested by the identity provider and/or user.

- Communicate feedback from the service provider to identity provider and user including the resulting actions (Credential status and/or reliability score update)
- Accept immediate SUSPENSION requests from user for credentials that have not reached the pre-established reliability threshold
- Accept immediate 'REVOCATION' requests from identity provider for credentials that have not reached the pre-established reliability threshold.

The URRS automatically updates the reliability score with each feedback from the service provider. These updates are communicated to the identity provider and the user. The URRS automatically suspends the credential if a feedback causes the score to fall below the reliability score threshold. The threshold value is established and agreed upon by the identity providers and service providers when the URRS is setup.

3.2. The User's Role

A user (credential holder) can benefit by monitoring his/her own credential. Monitoring services is a critical function for the user as his/her digital reputation is at stake. By involving the user, he/she can actively monitor the credential status and take actions to suspend or the credential should the reliability score of the credential be un-acceptable to a user. Involving the credential holder will add an extra layer of surveillance and promote early detection of credential misuse, effectively mitigating further attacks as a result of early detection.

The User's responsibility is to:

- Monitor his/her profile of credentials through the user interface of the URRS
- React to alerts sent by the URRS, as necessary and request the URRS to suspend a credential as needed.
- Immediately report lost, stolen, or compromised credentials to identity provider and URRS for suspension or revocation action at the URRS and identity provider.

The user can suspend a credential at any point, even if the reliability threshold has not been reached. Reasons for immediate suspension may be necessary if the user's credential has been lost. A user may also need to request immediate suspension upon detecting an attacker's use of a stolen or compromised credential at a service provider.[3] The attacker may trigger an URRS alert, enabling the user to discover unauthorized use of the credential. In some circumstances, suspended credentials can be re-activated. A lost credential, for example may be recovered by the user, but if no activity has been reported by the URRS for the credential during the suspension period, the credential may be re-activated at the digression of the identity provider.

3.3. The Service Provider's Role:

As recommended in section 2, service provider feedback in the 2 – 4 party models should be part of a revocation service. With a service provider feedback procedure, malicious use of a credential is effectively reported to the URRS. Other service providers are prevented from using the credential because

[3] The user may receive an unexpected out-of-band authentication request from the service or detect changes to the service's user setting/activities.

1) the credential has been flagged as revoked/suspended by the URRS or 2) because the reliability score has been lowered to an unacceptable level. Thus, other service providers are saves time, money and damage because of the URRS's reliability score system and/or suspension / revocation action.

The service provider's role is to:

- Report suspicious account activities to the URRS so that the URRS either
  - Lower the reliability score or update the status the credential status to SUSPENDED" or REVOKED
- Consult the URRS at authentication events for the credential status and reliability score and in order to make a risk based decision to accept or decline the credential for authentication and subsequent login.

3.4. The Single Sign On Systems

With Single Sign On systems, an authentication server or identity provider authenticates the user on behave of the service providers. The service providers accept the authentication assertion and give the user access to their services without the need to re-authenticate.

The service providers unified under the SSO environment should:

- Report suspicious account activities to the URRS so that the URRS can
  - Lower the reliability score or
  - update the status the long term credential status to SUSPENDED" or REVOKED

The authentication server/identity provider's role is to:

- Consult the URRS at each authentication event and retrieve the credential status and reliability score in order to make a risk based decision to accept or decline the proposed credential for authentication and subsequent assertion provisioning for the unified service provider under the SSO environment.

3.5. The Identity Provider and Attribute Provider's Role

In order for the URRS to be effective, the identity provider and attribute provider will interface with the URRS to:

- Provide credential/attribute updates (revoked, suspended) to the URRS in cases where the identity provider received reports of lost, stolen or compromised credentials
- Receive reliability score updates from the URRS in order to alert the user and take revocation actions as needed.
- Issue new credential(s) or attributes after revocation and register the new credential at the URRS.

Revocation procedure for the credential is initiated by the identity provider and communicated to the URRS. At the same time, the identity provider will issue a new credential to the user and register the credential at the URRS.

3.6. Supplementary URRS Feature: Credential Medium (Token) Revocations

Credential medium, such as smart cards, smart phone hold a user's credentials and associated credential secret. Some credential mediums contain several credentials for multi factor authentication used for graduated authentication to access IT resources. An example is a smart card that holds PKI credentials as well as PIN and Biometric credentials of the user. The management of the medium entails updating credentials in the medium, possibly at different times. Updates are necessary, for example, if one credentials has been compromised, while other credentials remain secure and valid. The management of the medium also becomes more complex if there are several credential issuers sharing a medium. For example, an enterprise may have issued smart cards to its employees containing credentials that authenticate employees to the enterprise's IT system. These cards also contain credentials for the cafeteria payment system and credentials to authenticate and pay for fares for the local transit agency. A lost or stolen card, in this situation, needs to be coordinated to the 3 entities or system. The URRS can provide revocation services for lost, stolen or compromised mediums and its credentials as follows:

- Lost/stolen medium: Immediate update of all credential statuses hosted by the medium to SUSPENDED or REVOKED state as requested by identity provider or medium holder.
- Communicate lost/stolen medium to all identity providers that issued a credential for the medium.
- Replace or update one or more credential state in cases where the credentials have been replaced to due to credential compromise.

3.7. Supplementary URRS Feature: Derived Credential Revocation

User mobility enables employees to stay connected with the office while away from the office desktop computing environment. The laptop has been the medium of mobility, but it is slowly taken over by smart phone, tablets and other smaller portable devices. With hard and soft tokens, each of the mobile devices may need to be provisioned with secondary credentials to enable the user's seamless connectivity to the office and its resources regardless of the medium currently in use (smart phone, tablet, etc). These secondary credentials are called derived credentials [4]for the purpose of this document. With derived credentials, a revocation or suspension of the primary credential may affect the derived credential as well.

Derived credentials may contain the primary's credential identifier in addition to its own identifier. This will enable federated services map the set of access control rules/roles to the same user. These types of derived credentials also have their own token/credential secrets. Therefore, a compromised primary credential should not affect the derived credentials as it has its own secret that is different (and in a different device) than the compromised primary credential. However, the derived credential needs to be updated to reflect the new credential identifier of the replacement primary credential, once the compromised credential is replaced. Similarly, re-issuance and renewal of the primary credential triggers the same type of update for the derived credentials.

Termination of the primary credential, on the other hand, should lead to the derived credential's termination. Unlike re-issuance and renewal, termination ends the user's privileges to the primary credential and by inference lead to termination of all other derived credentials embedded in the mobility devices and used for the same application / services as the primary credential.

[4] See SP 800-63-1 for a detailed definition of a derived credential.

The URRS can help maintain the derived credentials association with the primary credential:

- Maintain association primary credential and derived credential for renwal and reissuance
- Update derived credential identifier at each renewal or reissuance of the primary credential as indicated by the identity provider
- Mark all derived credentials as ‘REVOKED” in case there the primary credential has been terminated.

Appendix A—Recommendations

Section 2.1 The Two-Party Model – Enterprise SSO

Recommendation 1: With enterprise SSO solutions, services providers receive an assertion that asserts a successful prior authentication event by the enterprise's SSO authentication server. In cases where the session has been tampered by an attacker [5]or in cases where the attackers compromised the credential (e.g., pharming or phishing attacks), a service provider or application may detect suspicious activities of the attacker. Based on this knowledge, the service provider may prevent further malicious activities with other service provider by reporting the incident to the enterprise's SSO authentication server, resulting in a suspension of the credential. A reporting and revocation procedure, therefore, is beneficial to protecting the enterprise SSO environment.

Section 2.1.1 The Two-Party Model – Delegation

Recommendation 2: In federated communities, delegation technologies should be considered. With delegation technologies, the service provider issues delegation credentials that are tailored for access to data and/or processes limited to third party service, but excludes access rights to anything else, such as user settings and controls. With delegations, and should malicious third party activities occur, the primary service revokes the delegated credential, while the user credential remains valid. At the same time, the user is protected by Denial of Service (DoS) attacks. Delegations of a service should also be time-constraint, by limiting the access of a third party service to the time necessary to perform the delegated service.

Recommendation 3: For time-insensitive delegations, a user or service provider in the federations should have the ability to terminate a delegated service through a delegation revocation procedure.

Section 2.2 The Three-Party Model

Recommendation 4: A revocation/suspension service is necessary in order for the service provider to provide feedback on malicious use of credentials.

Recommendation 5: Phishing attack and other attacks against long term user credential are a concern in federated single sign-on environment. Based on the service provider's audit trail and risk mitigation techniques, the service provider may be able to prevent further malicious activities for other service providers by reporting the incident to the identity provider. A reporting and revocation procedure, therefore, is beneficial to protecting the federated SSO environment.

[5] A session could be subject to man-in-the-middle attack, or session hijacking. Other attacks originate at the service provider may include Cross-Site Request Forgery (CSRF) or Cross-Site Scripting (XSS).

Recommendation 6: While privacy enhancing schemes offer enhancements to information disclosure, it suffers from the lack of identity provider involvement in the authentication event. Without the identity provider's involvement, the status of a user's credential cannot be determined by the service provider. Where the status of a credential/attribute is important to the federation, therefore, a service provider may benefit from a black-list as part of a federated revocation mechanism.

Recommendation 7: Black lists are posted by the identity provider and constructed primarily based on feedback received from users or based on individuals reporting a lost, stolen, or compromised credential. The black list mechanism is valuable, but seems to exclude service provider feedback. Service providers are the primary entities that have first-hand information about malicious account activities. As is the case in the previous recommendation, with service provider feedback, malicious incidents could be reported by the service provider to the identity provider. As a result, the identity provider could suspend the credential and protect the user from further attacks. To implement this measure, a trusted third party, (the revocation service of the federation) would have to perform the task of anonymity revocation and credential revocation.

Section 2.3: The Four-Party Model:

Recommendation 8: The types of attributes accepted by the federation are defined at federation establishment. Federated attributes, in turn, are assigned to the users at credential enrollment. They can be asserted by the user but validated by the identity provider. Where attributes serve a critical part in the roles or functions a user is permitted to perform, it is important for attributes to be up-to-date. The identity provider therefore, should check the attribute authoritive source for roles or qualifications revocation or change.

Recommendation 9: As a benefit of using the same credential, and with service provider feedback mechanisms, the authentication decisions by the attribute provider and identity provider is based on the same status of the credential.

Appendix B—Acronyms

ABAC	Attribute Based Access Control
AP	Attribute Provider
CSF	Cross Site Request Forgery
CXX	Cross Site Scripting
DoS	Denial of Service
FRAC	First Responder Access Card
IdMS	Identity Management System
SSO	Single Sign On
FIPS	Federal Information Processing Standard
ITL	Information Technology Laboratory
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
PET	Privacy Enhancing Technology
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
RBAC	Role Based Access Control
SP	Special Publication

Appendix C—References

[FIPS201] Federal Information Processing Standard 201-1, Change Notice 1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, March 2006. Or as amended
(See http://csrc.nist.gov)

[SP800-63] NIST Draft Special Publication 800-63-1, *Electronic Authentication Guideline*, February 2010 or as amended (See http://csrc.nist.gov