



Intelligence Community Technical Specification

Web Security Standards Guidance for Token Services

Version 2014-DEC

December 22, 2014

Distribution Notice:

This document has been approved for Public Release and is available for use without restriction.

Table of Contents

Chapter 1 - Introduction	1
1.1 - Purpose	1
1.2 - Scope	1
1.3 - Background	1
1.4 - Enterprise Need	2
1.5 - Audience and Applicability	2
1.6 - Conventions	3
1.6.1 - Language	3
1.6.2 - Typography	3
1.7 - Dependencies	3
1.8 - Conformance	3
Chapter 2 - Development Guidance	5
2.1 - Token Services	6
2.1.1 - Token Services Guidance	7
2.1.2 - Token Services Considerations and Constraints	8
2.2 - Use Case 1 – Web SSO	9
2.2.1 - Web SSO Guidance	10
2.2.2 - Web SSO Considerations and Constraints	11
2.3 - Use Case 2 – Identity Propagation	12
2.3.1 - Identity Propagation Guidance	13
2.3.2 - Identity Propagation Considerations and Constraints	14
2.4 - Use Case 3 – Token Transformation	14
2.4.1 - Token Transformation Guidance	15
2.4.2 - Token Transformation Considerations and Constraints	16
2.5 - Use Case 4 – Filtered Identity Provisioning	16
2.5.1 - Filtered Identity Provisioning Guidance	17
2.5.2 - Filtered Identity Provisioning Considerations and Constraints	17
2.6 - Use Case 5 – Cross-Security Boundaries Token Service	18
2.6.1 - Cross-Security Boundaries Token Service Guidance	19
2.6.2 - Cross-Security Boundaries Token Service Considerations and Constraints	20
Appendix A - Feature Summary	21
A.1 - WSS-TS Feature Comparison	21
Appendix B - Change History	22
Appendix C - List of Abbreviations	23
Appendix D - Bibliography	25
Appendix E - Points of Contact	28
Appendix F - IC CIO Approval Memo	29

List of Figures

Figure 1 - Token Services	8
Figure 2 - Use Case 1 – Web SSO	11
Figure 3 - Use Case 2 – Identity Propagation	13
Figure 4 - Use Case 3 – Token Transformation	15
Figure 5 - Use Case 4 – Filtered Identity Provisioning	17
Figure 6 - Use Case 5 – Cross-Security Boundaries	19

List of Tables

Table 1 - Token Services Considerations and Constraints	8
Table 2 - Web SSO Considerations and Constraints	12
Table 3 - Identity Propagation Considerations and Constraints	14
Table 4 - Token Transformation Consideration and Constraints	16
Table 5 - Filtered Identity Provisioning Considerations and Constraints	18
Table 6 - Cross-Security Boundaries Considerations and Constraints	20
Table 7 - Feature Summary Legend	21
Table 8 - WSS-TS Feature comparison	21
Table 9 - DES Version Identifier History	22

Chapter 1 - Introduction

1.1 - Purpose

This document provides the guidance to recognize types of problems where token services should be considered as a solution, and the considerations that such solutions will entail. The representative use cases reflective of the problem solutions in this document include Web Single Sign-On (SSO), Identity Propagation, Token Transformation, Filtered Identity Provisioning, and Cross-Security Boundaries Token Service. These use cases are not mutually exclusive, i.e. problems conditions can support application of token services to solve multiple of those problems simultaneously. The approach of presenting them independently is to provide clarity regarding the problem/solution set.

1.2 - Scope

This information guidance document addresses general concepts of what functionality a token service provides, addresses general guidance, and gives specific guidance on the use of the technology in context of the representative use cases and consistent use and exchange of the information involved in those connections.

This information guidance is applicable to the Intelligence Community (IC) and information produced by, stored, or shared within the IC. This document may have relevance outside the scope of the IC enterprise. However, prior to being applied outside of this defined scope, the document should be closely scrutinized and environmental differences separately documented and assessed for applicability.

1.3 - Background

The Intelligence Community Chief Information Officer (IC CIO) is leading the IC's enterprise transformation to an "interoperable federated architecture." Intelligence Community Directive (ICD) 500, *Director of National Intelligence Chief Information Officer* [\[3\]](#) grants the IC CIO the authority and responsibility to:

- Develop an Intelligence Community Enterprise Architecture (IC EA).
- Lead the IC's identification, selection, development, and management of IC enterprise standards.
- Incorporate technically sound, de-conflicted, interoperable enterprise standards into the IC EA.
- Certify that IC elements adhere to the architecture and standards.

In the area of enterprise standardization, the IC CIO is called upon to establish common IT standards, protocols, and interfaces, to establish uniform information security standards, and to ensure information technology infrastructure, enterprise architecture, systems, standards, protocols, and interfaces support the overall information sharing strategies and policies of the IC as established in relevant law, policy, and directives.

Enterprise standards facilitate the information exchanges, service protocols, network configurations, computing environments, and business processes necessary for a service-enabled federated enterprise. As the enterprise develops and deploys shared services employing approved

standards, not only will information and services be interoperable, but significant efficiencies and savings will be achieved by promoting capability reuse.

1.4 - Enterprise Need

The IC CIO funds and oversees a number of critical enabling projects, including the IC Information Technology Enterprise (IC ITE). The IC ITE makes extensive use of web services (a standardized way of integrating Web-based applications using open standards) and distributed processing, yet each individual program providing services therein requires explicit guidance on building secure, interoperable web services.

This document provides general and prescriptive guidance for the development of secure and interoperable web service security solutions in support of the following Office of the Director of National Intelligence (ODNI) policies and implementation guidance.

- IC Information Technology Enterprise (IC ITE):
 - Intelligence Community Information Technology Enterprise (IC ITE) Increment 1 Implementation Plan^[2]
- 500 Series:
 - Intelligence Community Directive (ICD) 500, Director Of National Intelligence Chief Information Officer^[3]
 - Intelligence Community Directive (ICD) 502, Integrated Defense of the Intelligence Community Information Environment^[4]
 - Intelligence Community Directive (ICD) 503, Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation^[5]
 - Intelligence Community Policy Guidance (ICPG) 500.1, Digital Identity^[6]
 - Intelligence Community Policy Guidance (ICPG) 500.2, Attribute-based Authorization and Access Management^[8]
 - Intelligence Community Standard (ICS) 500-21, Tagging of Intelligence and Intelligence-Related Information^[11]
 - Intelligence Community Standard (ICS) 500-27, Collection and Sharing of Audit Data^[12]
 - Intelligence Community Standard (ICS) 500-29, IC Digital Identifier^[13]
 - Intelligence Community Standard (ICS) 500-30, Enterprise Authorization Attributes: Assignment, Authoritative Sources, and Use for Attribute-Based Access Control of Resources^[14]

1.5 - Audience and Applicability

The intended audience of this information guidance document is project managers, software architects, network architects, and developers who have requirements to do authentication¹ and authorization² in the IC. This document is geared toward any projects requiring access control, needing solutions related to enterprise web identity³, or providing and protecting identity or authorization attributes for applications and services.

¹Authentication is the process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device).^[1]

²Authorization is the access privileges granted to a user, program, or process or the act of granting those privileges.^[1]

³An identity is the set of attribute values (i.e., characteristics) by which an entity is recognizable and that, within the scope of an identity manager's responsibility, is sufficient to distinguish that entity from any other entity.^[1]

This document provides guidance related to the use of token services and will be important in satisfying web security requirements and information security goals in a secure and interoperable manner.

The applicability of this information guidance document is defined in the IC Enterprise Standards Baseline (IC ESB). Additional applicability and guidance may be defined in separate IC policies as necessary.

ICS 500-20, Intelligence Community Enterprise Standards Compliance,^[10] defines the IC ESB and its applicability to IC elements. The IC ESB defines the compliance requirements associated with each version of a technical specification. Each version will be individually registered in the IC ESB. The IC ESB defines the location(s) of the relevant artifacts, prescriptive status, and validity period, all of which characterize the version and its utility.

1.6 - Conventions

Certain technical and presentation conventions were used in the creation of this document to ensure readability and understanding.

1.6.1 - Language

The keywords “MUST,” “MUST NOT,” “REQUIRED,” “SHALL,” “SHALL NOT,” “SHOULD,” “SHOULD NOT,” “RECOMMENDED,” “MAY,” and “OPTIONAL” in this technical specification are to be interpreted as described in the IETF RFC 2119.^[15] These implementation indicator keywords are thus capitalized when used to unambiguously specify requirements over protocol and application features and behavior that affect the interoperability and security of implementations. When these words are not capitalized, they are meant in their natural-language sense.

1.6.2 - Typography

Certain typography is used throughout the body of this document to convey certain meanings, in particular:

- *Italics* – A title of a referenced work or a specialized or emphasized term
- Underscore – An abstract data element
- **Bold** – An XML element or attribute

1.7 - Dependencies

This information guidance document contains no external dependencies.

1.8 - Conformance

For an implementation to conform to this specification, it **MUST** adhere to all normative aspects of the specification. For the purposes of this document, normative and informative are defined as:

- *Normative*: considered to be prescriptive and necessary to conform to the standard.
- *Informative*: serving to instruct, enlighten or inform.

The use of keywords defined in IETF RFC 2119^[15] is considered normative within the scope of the sentence. All other parts of this document are informative.

Chapter 2 - Development Guidance

Over the past decade, organizations have been challenged with securely conveying identity and attributes of subjects¹ in and across web-based environments. For that reason, several specifications such as WS-Trust^[22], WS-Federation^[20], SAML 2.0^[17], SAML 2.0 Attribute Sharing^[18], and OpenID Connect^[16] have been developed that enable applications to construct trusted message exchanges through the issuance, exchange, and brokering of security tokens² using "token services." These specifications are implemented in various product suites and applied to different sets which are generically defined in this specification as use cases. While these use cases refer to a number of technical mechanisms or capabilities provided by such solutions, it is important to understand the tradeoffs, risks and benefits of doing so. From a security and interoperability perspective, it is critical that security mechanisms, such as token services, are applied and managed in a consistent manner.

A token service provides a standardized mechanism for issuing security tokens which provide the credentials³ and other information needed to support identification, authentication, and authorization. A token service solution enables service providers to support and augment digital identity and authentication across authentication authorities and resources, leveraging them within a federation. This enables service providers to receive trusted information about a user without having to integrate the user's clients with each and every web service and without the user having to log in and provide authentication information multiple times.

Web service (and service-based) technologies have emerged as promising developments to address cross-security, cross-platform, cross-vendor integration, and trust domains. The representative use cases reflective of the problem solutions in this document include Web Single Sign-On (SSO)⁴ issues. Web Services with a token service represent a practical and proven approach for a secure, standards-driven, and trusted enterprise. Web services from an enterprise perspective can provide real value and include federation to simplify identity, authorization, and trust management across boundaries. This can result in improved agency security, integration, communication, and information exchange between service consumers, service providers, mission partners, and communities of interests. Used appropriately, this will aid in achieving lower enterprise costs, improving message integrity⁵, non-repudiation⁶, confidentiality⁷, and maximize efficiency in mission operations.

A token service can be a direct response to the following problem sets:

- Integrating systems using different identity and authentication systems

¹A subject is an active entity (generally an individual, process, or device) that causes information to flow among objects or changes the system state. ^[1]

²A security token comprises a collection of assertions. Data produced by a token service regarding (i) authentication performed by a subject, (ii) attribute information about the subject, (iii) authorization information for the subject, or a combination of all three.

³Credentials are a set of claims used to prove the identity of a client.

⁴Single Sign-On is a technical consolidation of authentication functionality within a group of systems. Specifically, once an end user has authenticated their identity at an Identity Provider (IdP), he or she may, by their choice, move among other clients that interoperate with the IdP without re-authenticating.

⁵Integrity is the property whereby an entity has not been modified in an unauthorized manner. ^[1]

⁶Non-repudiation is the assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information. ^[1]

⁷Confidentiality is the property that information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information. ^[1]

- Integrating systems using different message protocols and content layouts
- Loss of integrity or spoofing of passed identity and request information
- Trusted brokering of credentials across domains
- Exposure of sensitive identity information during transit or in use
- Lack of effective time-to-live⁸ management of identities and messages

2.1. Token Services

Customary access control solutions tightly couple identification, authentication, and authorization functions, especially when utilizing Attribute Based Access Control (ABAC) ⁹in organizational IT infrastructure and software architectures. IC and DoD communities are moving toward a service-based model of interacting consumer and provider services that require these functions be decoupled from access control to realize the value of this model.

There are many benefits that a token service solution can assist in addressing:

- Establishing clear enterprise trust domains¹⁰ that contain multiple security domains¹¹. Trust relationships must be established, assessed, and brokered.
- Creating identity federation¹² and/or authentication authorities that enable enterprise trust¹³ and are a part of and integrate with a token service.
- Establishing a security token translation service that can transform trust assertions¹⁴ from one registered web application or service to another registered web application/service.
- Establishing a token service that can be flexible enough to receive and issue tokens containing identity, and authorization information in order to support additional functionality such as authorization, auditing, and local authentication.
- Handling of security tokens issued by the token service must be suited to efficient handling and filtering of any boundary devices resulting in enterprise standardization of protocols and bindings.
- Establishing token service registration of participating web services/applications/service providers to include partnership of other token services (in other trust domains) to enable a

⁸The time-to-live for a token would be the date and time the token is no longer valid.

⁹Attribute Based Access Control is an access control based on attributes associated with and about subjects, objects, targets, initiators, resources, or the environment. An attribute-based access control rule set of an access control policy defines the combination of attributes under which an access may take place.^[1]

¹⁰A trust domain is an environment or context that contains or defines one or more security domains. A trust domain may encompass a single site or multiple sites. Trust domains may interact and enter into agreements for providing and /or consuming services across administrative domain boundaries.^[19]

¹¹A security domain is a domain that implements a security policy and is administered by a single authority.^[1]

¹²Identity federation enables the portability of identity information across otherwise autonomous security domains enabling the entities (persons and non-persons) of one domain to seamlessly access data or systems of another domain.

¹³Trust is the characteristic that one system entity is willing to rely upon a second system entity to execute a set of actions and/or to make a set of assertions about a set of subjects and/or scopes.

¹⁴An assertion is a claim that is propagated to a service provider for the purpose of informing an access control decision. In the case of Security Assertion Mark-up Language(SAML), an assertion is a token.

flexible federated capability that improves request and response message integrity and confidentiality, exposing only necessary information when propagating identity between service hops¹⁵ as needed.

- Establishing third-party trust on which all components can rely for independent verification of message identities and content non-repudiation, integrity, and, where needed, confidentiality.

2.1.1. Token Services Guidance

A token service is a mechanism that passes authentication and/or identity information from a requester, which uses the token service to create a token, to a service provider in a form that web services and applications can understand, and use a token service to validate and manage what is provided to the service provider (as illustrated in [Figure 1](#)). In essence, a token service is a “trusted” broker, with which the requester sends a Request Security Token (RST) and receives a Request Security Token Response (RSTR). A token service has the ability to communicate trust to service providers, end users / clients, devices, and an organization’s security mechanisms. A token service provides a standards-based mechanism for extensible authentication to ensure interoperability between different security domains and platforms.

A token service can address difficulties in communicating between components using a variety of methods and mechanisms by leveraging authenticated information (to include identifiers and identity attributes) and using a token that can be interpreted by the token service to meet the technical and security needs of the various service requesters and providers. This trusted third party, “trusted broker”, approach can provide for those needs within a single trust domain where differentiation must be fostered and supported, or across trust domains where controls are even more stringent.

¹⁵A “hop” is the path between a client and service or application.

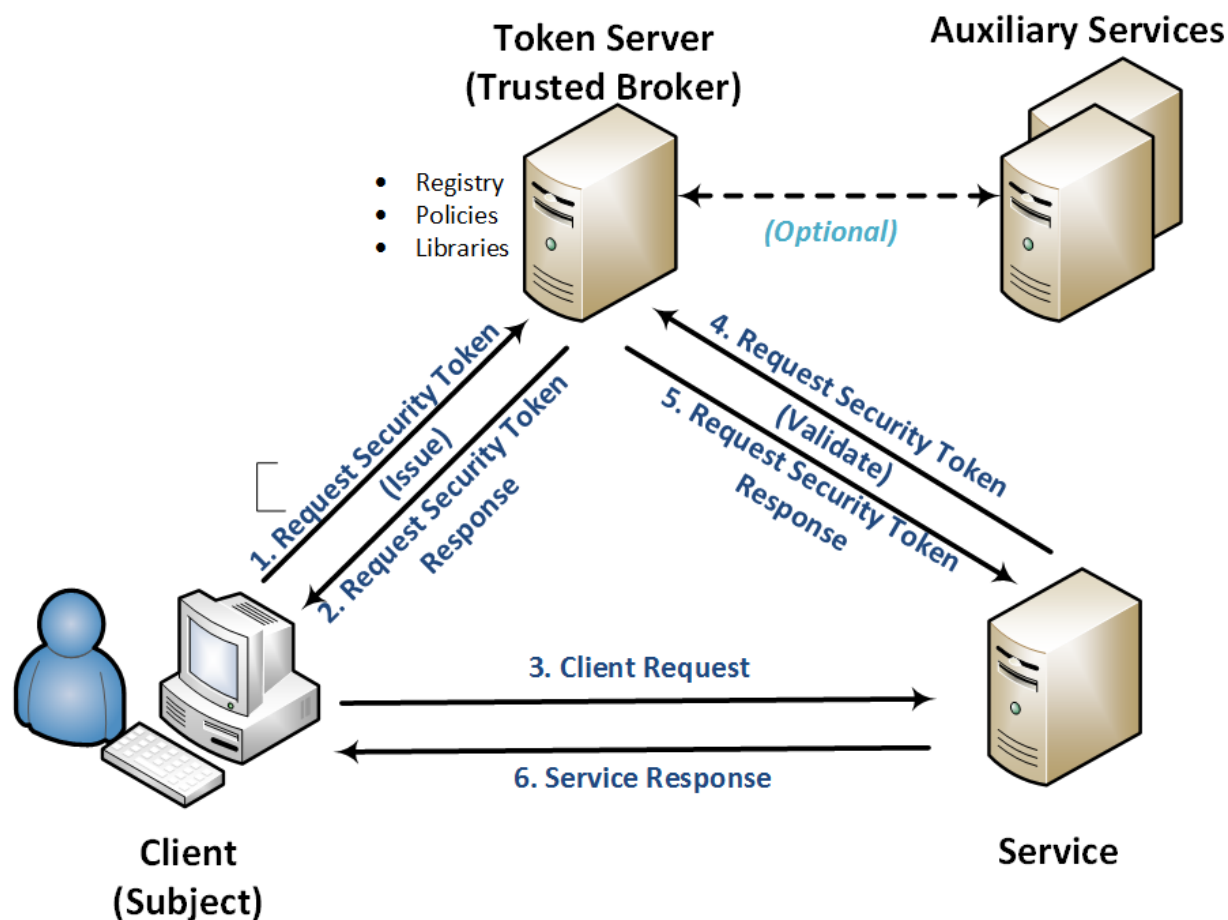


Figure 1 : Token Services

2.1.2. Token Services Considerations and Constraints

This information guidance specification provides the following high-level consideration and constraints, shown in [Table 1](#).

Table 1 - Token Services Considerations and Constraints

Token Services Considerations and Constraints
A token service MUST issue and validate standardized security tokens.
All entities MUST be approved to exchange information by the program's Authorizing Official (AO) ^a This approval may be in the form of an authority to operate (ATO).
Each exchange with the token service MUST be encrypted using Transport Layer Security (TLS), version 1.2.
Each token service transaction MUST be mutually authenticated using valid Public Key Infrastructure (PKI) digital certificates.

Token Services Considerations and Constraints
Each service provider MUST check the validity of the token service's PKI certificate (including the certificate's revocation status).
The token service MUST initiate mutual authentication with the Subject using valid PKI certificates.
The token service MUST check the validity of the Subject's PKI certificate (including the certificate's revocation status).
A service provider MUST reject any request bearing a security token from a token service that has not been authenticated and is not explicitly trusted.
Any security token issued by a token service MUST be signed, and MUST have explicit conditions of use ^b , including an expiring time period.
A token service MUST not validate or transform a security token that has expired.
Upon receipt of a token, a service provider MUST validate the token service's signature and the token's conditions of use, rejecting requests that do not comply with those conditions.
Security Tokens MUST not be reused. Refresh tokens for the purpose of assertion propagation, should be requested from the service provider to the token service and propagated to the next service.
Each service interfacing with token services MUST be registered for the actions and information to be provided by the token service.
Authentication SHOULD be decoupled from Authorization to enable trust in the flexible propagation and use of identity.
A token service MAY add local attributes to support a service provider business operations or calls to another web service.
A token service MAY send user or web service / application identity between different enterprise trust and security domains.
A token service solution MAY use auxiliary services for additional identity or credential functionality.
Validating the integrity of a message MAY use digital signatures, Message Authentication Codes or hash algorithms.
A token service MUST ensure that it meets audit trail requirements

^aAn Authorizing Official is an official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations, agency assets, or individuals.

^bA security token MAY have re-issuance criteria such as re-verifying the user.

2.2. Use Case 1 – Web SSO

Historically, distributed systems have been assembled from components that act as independent security domains. These components comprise individual platforms with associated operating systems, applications, and account management functions. These components act as independent security domains in the sense that a service consumer or end-user has to identify and authenticate independently to each of the security domains with which they wish to interact. An end-user has to conduct a separate sign-on dialogue with each secondary domain that the end-user requires to accomplish the end-user's task. From the management perspective, the legacy approach requires independent management of each security domain and the use of multiple user

account management interfaces and authorization mechanisms. Considerations of both usability and security give rise to a need to harmonize and, where possible, integrate user sign-on functions with token services for the multitude of different domains now found within an enterprise. Being able to interact across such diverse environments is one of the strengths of web services, but it has a price: it becomes difficult to secure such systems and distorts the line between "inside" and "outside" users. It is hard to find a common standard for all involved technologies.

The following is a list of benefits that a Single Sign-On (SSO) solution can address:

- The need to establish standardized enterprise trust domains that contain multiple security domains.
- Identity federation authentication solution which can traverse security, technology, or authority boundaries.
- The need to enable SSO, Reduced Sign-On (RSO), and Single Log-Off (SLO) where possible.
- Reduction in the time taken by users in sign-on operations to individual security domains, including reducing the possibility of such sign-on operations failing.
- Improved security through the reduced need for a user to handle and remember multiple sets of authentication information.
- Reduction in the time taken and improved response by system administrators in adding and removing users to the system or modifying their access rights
- Improved security through the enhanced ability of system administrators to maintain the integrity of user account configuration including the ability to inhibit or remove an individual user's access to all system resources in a coordinated and consistent manner.
- Extending the existing trust model of Secure Socket Layer (SSL) and Public Key Infrastructure (PKI).
- Integrates with identity federation, is standards based, and supports encrypted and signed token service that ensures non-repudiation.
- Integrates with federation into the administration of security tokens.
- Provide consistent and predictable audit capabilities.
- Prevent losing information between a web service consumer and web service provider to maintain end-to-end traceability.

2.2.1. Web SSO Guidance

An SSO service initiates a session for a user that will include an authentication process that requires a user to assert their identity claim by one or more means (factors) that can be physical or logical in nature, in order to access multiple web services or applications. The process authenticates the user for all the web services or applications they have been given rights to within that session and eliminates further prompts when they switch web services during a particular session within a trust or security domain.

In the past, agencies have implemented proprietary mechanisms making service invocation using single sign-on technically challenging. A good solution to SSO in a trust environment is using the WS-* standards (WS-Security^[21] and WS-Trust^[22], SAML 2.0^[17]), and/or X.509. The SAML specification also provides a model for features and functions provided through other forms of information packaging to support secure communications by other tool, protocols, and interfaces. Another good solution to SSO in a trust environment is the use of OpenID Connect^[16]. Implementers must weigh the pros and cons of any SSO solution based on the needs of the organization.

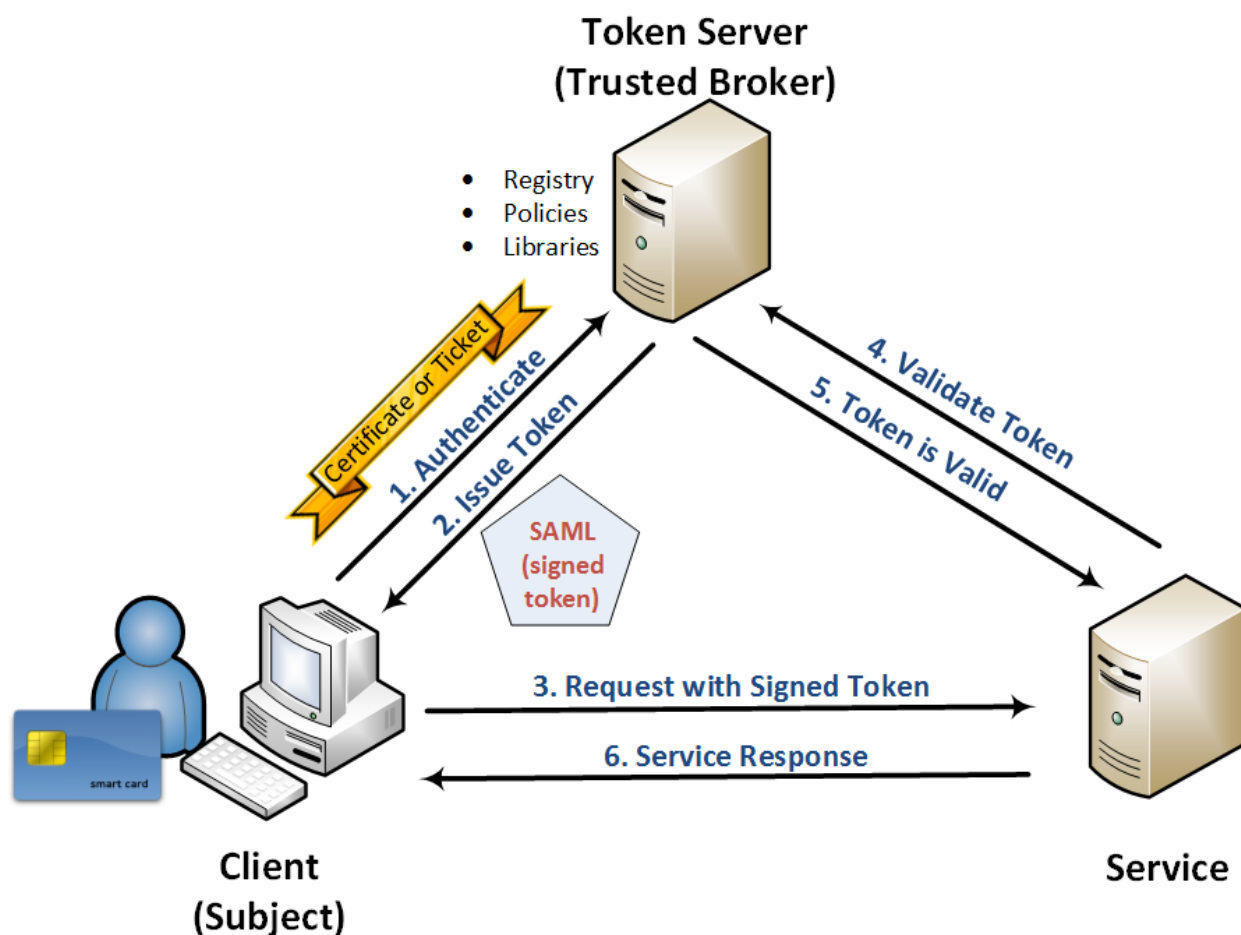


Figure 2 : Use Case 1 – Web SSO

2.2.2. Web SSO Considerations and Constraints

This information guidance specification provides the following high-level constraints, shown in [Table 2](#).

Table 2 - Web SSO Considerations and Constraints

Web SSO Considerations and Constraints
An SSO service MUST authenticate to an authorized token server using a PKI certificate if the SSO service is decoupled from the authorized token service.
An SSO session MUST stay within the trust domain where it has validity. A new SSO session MAY be initiated by the SSO service but the SSO service MUST request a security token refresh from the token service.
An SSO session MUST have a valid signed token issued by an authenticated token service and will have explicit conditions of use, including an expiring time period.
An SSO service MUST initiate mutual (two-way) authentication with the web service consumer using Public Key Cryptography.
The token service MUST check the validity of the SSO service using PKI certificates (including the certificate's revocation status).
An SSO service MUST request a token service security token refresh for the purpose of service "hops".
An SSO "hop" that is destined for a service or domain using a different logon identifier MUST leverage the token services to refresh the token and provide the appropriate credentials for the target service.
An SSO service MAY be a service within the token service or identity federation service.
An SSO service MAY include RSO and SLO functions or services.
An SSO service MAY manage multiple sessions with potentially different identities that request and cancel tokens from a token service.
A new SSO session MAY be initiated to traverse trust domains.
An SSO service MUST ensure that it meets audit trail requirements.

2.3. Use Case 2 – Identity Propagation

Traditional federated identity management relies on a centralized identity control paradigm overlooking service orchestration and organizational ownership boundaries. Service chaining and cross-mission responsibilities within organizational boundaries constitute an expanded execution context and a challenge for legacy identity control methods. This is particularly true when working in a service consumer / provider environment that crosses the line from technology to business where values, intents, and solutions have different reasoning and justification and where the value of mission prevails over the value of technical dexterity. This is specifically true where there are concerns over passing information that asserts the identity of the requesting party or parties (persons and non-persons) that are subject to integrity demands of the services that handle that information across the "hops". The identity propagation occurs when an identity is created and passed across components ("hops").

The following is a list of benefits that an identity propagation solution can address:

- The need for a standardized enterprise identity propagation mechanism to pass authorized identities between trust and security domains.

- Establishing identity federation as a structure of distributed trust domains that serve only their own members, but can federate an authentication request based on trust relationships between them.
- Support and use of trust domain components that rely on their own authentication mechanisms.
- The need for an identity federation authentication solution that can traverse security, technology, or authority boundaries.
- Support of an identity federation and/or authentication authorities that enable enterprise trust through use of a standardized token service.
- The difficulties and risks encountered in acquiring and propagating both enterprise identity and agency identity data across the enterprise

2.3.1. Identity Propagation Guidance

During the identity propagation, an identity originates outside of the identity propagation mechanism, which is never the source of the identity, but is capable of propagating the identity onwards to other security, technology, and authority domains. The token services act as a trusted third-party for the identities of those participating in the conversation across those "hops," guaranteeing the integrity of the information passed and, where the form of the message package itself must change or protocols used, the integrity of that information.

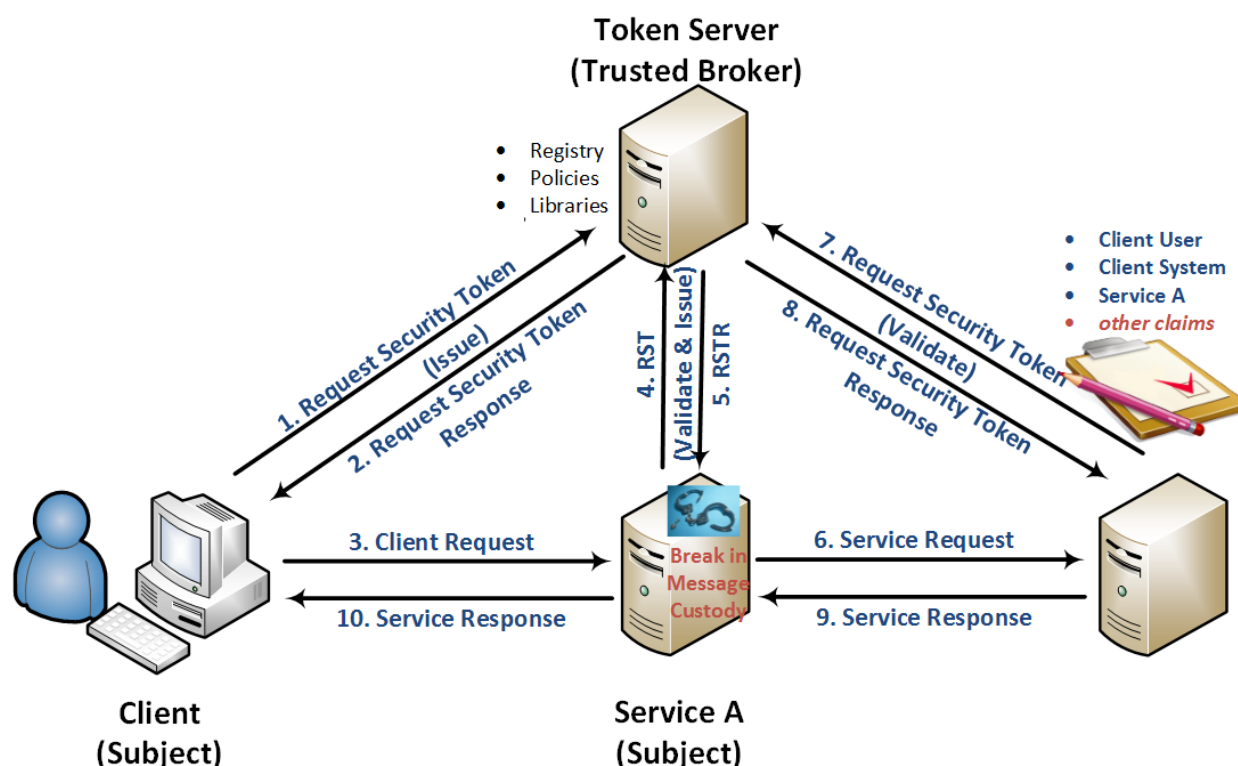


Figure 3 : Use Case 2 – Identity Propagation

2.3.2. Identity Propagation Considerations and Constraints

This information guidance specification provides the following high-level constraints, shown in [Table 3](#).

Table 3 - Identity Propagation Considerations and Constraints

Identity Propagation Considerations and Constraints
Identity propagation MUST not be the service that creates the user's identity.
Identity propagation MUST ensure non-repudiation of participating clients and services.
Identity propagation MUST ensure an audit trail that enables end-to-end traceability.
Identity propagation MUST ensure end-to-end integrity of message content.
Identity propagation MUST request a token service security token refresh for the purpose of service "hops".
Identity propagation MAY be used with SSO, RSO, and SLO.
Identity propagation MAY include security token translation.
Identity propagation MAY enable undisclosed message content across transport services.
Identity information MAY be passed through a token service.

2.4. Use Case 3 – Token Transformation

Consumers crossing multiple security domains are often required to deal with multiple systems utilizing different forms of tokens and identities contained within them. Service providers and consumers are spread over different security domains using different token types or different security token implementation technologies that don't support a common set of token formats. The same is true even within a single security domain where there are multiple contributors of services that use different standards and specifications based on their original construction or for specific functional or security needs that mandate different approaches. Using custom access control methods to convey entrenched user authentication methods is not sufficient to ensure authentication interoperability between consumers and providers. Instead, one beneficial solution would be to leverage a transparent mechanism to perform token transformation with a token service for both consumers and service providers.

The following is a list benefits that a token transformation solution can address:

- The need for a standardized enterprise token translation mechanism to pass authorized security tokens between trust and security domains is critical to enable enterprise trust relationships.
- A key benefit of the token service is the reduced complexity for web application developers and service providers. The benefit to the Service Provider is a reduction in administrative and technical overhead. Support for legacy and acquired systems using different token and identity forms can be transparently supported.
- Adherence to protocol standards is a requirement of token transformation and improves standards compliance because it targets message protocol implementation and contents. This

includes facilitating transition to standards and when the standards themselves change and require system migration.

2.4.1. Token Transformation Guidance

While OASIS^[22] (extension of WS-Security) envisioned token processing occurring at both the client and at the service provider, the underlying token services framework has no such restriction. As a result, larger organizations with multiple security domains have recognized the value of a trusted token service as a “universal token translator” that can convert one type of security token into another type of security token even if there are no web services being used. In other words, users with multiple client applications can use a universal token translator service (e.g. trusted token service) to authenticate to multiple web services / service providers improving SSO/ RSO/ SLO, supporting changes for those services without disruption, and enabling enterprise identities.

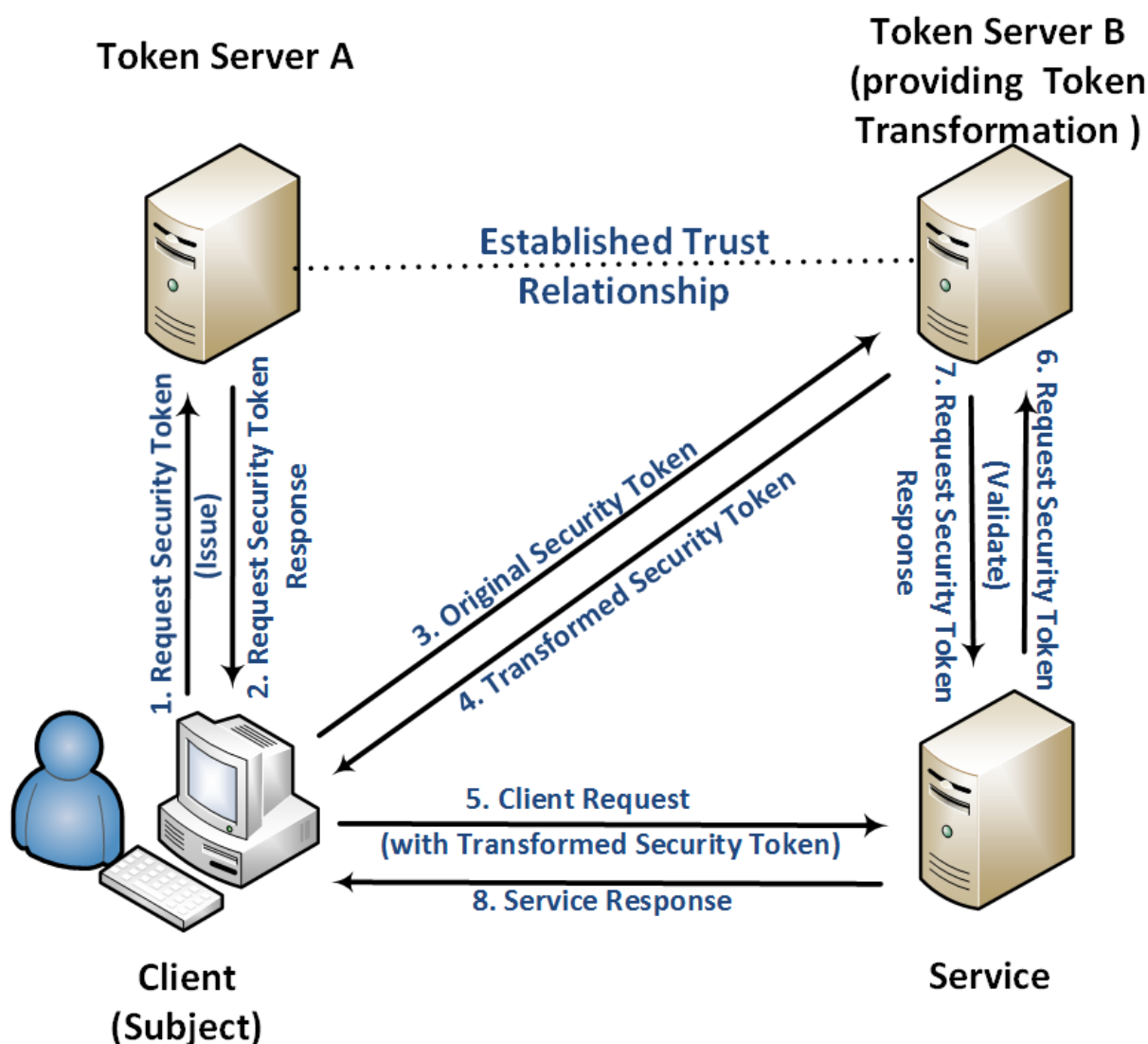


Figure 4 : Use Case 3 – Token Transformation

2.4.2. Token Transformation Considerations and Constraints

This information guidance specification provides the following high-level constraints, shown in [Table 4](#).

Table 4 - Token Transformation Consideration and Constraints

Token Transformation Considerations and Constraints
Token transformation MUST include tokens the token service can recognize and can transform.
A token service MUST have a policy for issuing a token from the service provider for the web service or resource.
A service provider MUST reject any request bearing a token from a token service that has not been authenticated and/or is not explicitly trusted.
Upon receipt of a token transformation request, the token service MUST validate the token's signature and the token's conditions of use, rejecting requests that do not comply with those conditions.
A token service MUST be able to input user identities in a standardized, secure form.
A service MUST be registered with the token service and contain information regarding the type of token and the means of exchange to ensure proper transformation and delivery.
Token transformation MAY be used with both web services or non web-based solutions.
Token transformation MAY support specific operational needs, e.g. access control decisions.
A token service MAY be able to consume identities from many resources.
A token service MAY restrict token transformation access to message content and signatures.
A token service MAY restrict registered services from interrogating message content and signatures.
Token Transformation MUST ensure that it meets audit trail requirements.

2.5. Use Case 4 – Filtered Identity Provisioning

In a diverse environment with multiple levels of security, a token service may need to send identity information that may be incomplete, highly sensitive, or burdensome to the transport mechanism. A token service with filtered identity provisioning would act as an IdP and be able to provide the service provider an identity with only those attributes and values that the service provider is allowed to receive. In some cases a smaller set of information, possibly just an identity key is passed.

A filtered identity provisioning token service solution has all of the benefits that a token service solution has with the following additions:

- Enabling the restriction of the acquired and provisioned identity information to authorized service providers.

2.5.1. Filtered Identity Provisioning Guidance

A filtered identity provisioning token service solution follows the same guidance as a token service with the following addition:

- Upon token validation, the token service will send the identity consisting of only those attributes and values that the service provider is allowed to receive.

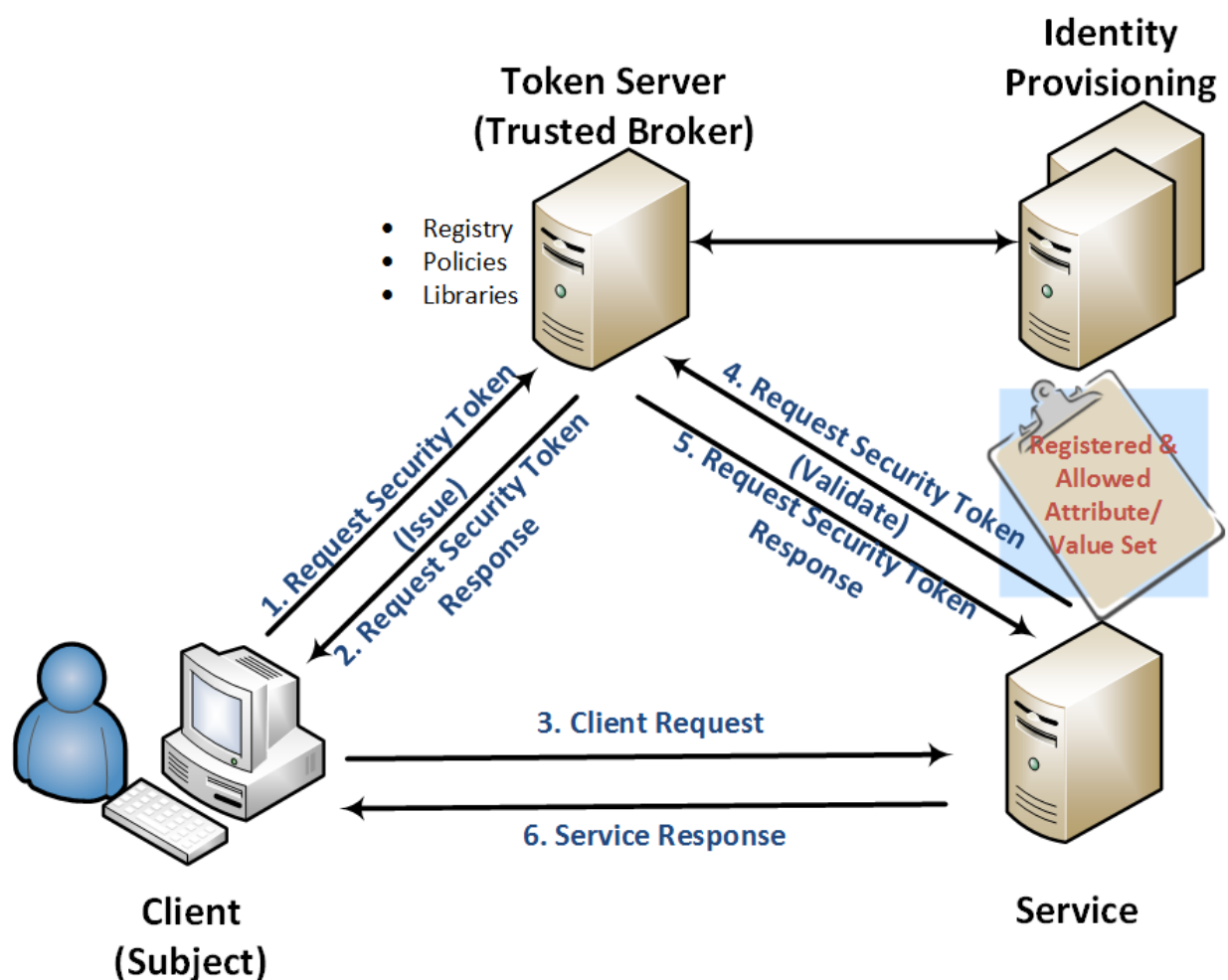


Figure 5 : Use Case 4 – Filtered Identity Provisioning

2.5.2. Filtered Identity Provisioning Considerations and Constraints

This information guidance specification provides the following high-level constraints, shown in [Table 5](#).

Table 5 - Filtered Identity Provisioning Considerations and Constraints

Filtered Identity Provisioning Consideration and Constraints
All web services MUST be registered with the token service for the token service to propagate filtered identities.
Filtered identity MUST enable a token service to provide non-repudiation of participating client and services.
Filtered identity MUST ensure that a token service can provide and meet audit trail requirements.
Filtered identity MUST be provided by an authorized token service.
Filtered identity MUST ensure a token service can provide end-to-end integrity of message content. Integrity of token between the token service used to create the token, and that which is used to validate.
Filtered identity MUST interact with identity provisioning sources to act as an identity provider ^a
Filtered identity MAY restrict message content in whole or in part.
Filtered identity MAY encrypt identity data until end-point delivery.
Message content MAY be protected from exposure wholly or in part.
Filtered identity MAY combine identities to meet service context requirements.

^aAn identity provider is services and data that provide access to information about the identities of people, systems, services and devices.

2.6. Use Case 5 – Cross-Security Boundaries Token Service

IC and DoD IT and security professionals can no longer assume that they will be managing and securing in-house computing assets in a context of their ownership and control. While the operation in a trust or security domain becomes more diverse, its reach is also extended across and into other "domains". IT and security professionals will have a harder time distinguishing "trusted" insiders from "untrusted" outsiders. The IC and DoD communities need clearly defined trust domains to enable authentication federation.

The following is a list of benefits that a cross-security boundaries token service solution can address the need to:

- Leverage an identity which traverses enterprise organizational boundaries.
- Propagate identity along service chains and across domain boundaries exposing limited information along each service "hop", as needed.
- Establish organizational trust domains and negotiate trust relationships.
- Bridge clients and web services authentication on a variety of platforms within the enterprise.
- Leverage enterprise identity and authentication federations within and across domain boundaries.
- Foster interoperability through standardization of protocols that use token services.

2.6.1. Cross-Security Boundaries Token Service Guidance

A trust domain is a collection of systems, personnel, and controls constrained by the technologies, processes, and policies that both define and manage it in a consistent manner. A trust domain may contain or define one or more security domains. A trust domain may encompass a single site or multiple sites.

Establishing trust across domains can be enabled using token services to place multiple third-party trust brokers in the different domains and establishing trust between them. This trust can be established as either a one or two-way trust to control the flow of information. They can also leverage identity systems that cross the boundaries or only those within the boundaries and provide identities reflecting a user or systems as they exist in those domains, or collectively across them, in a trusted fashion.

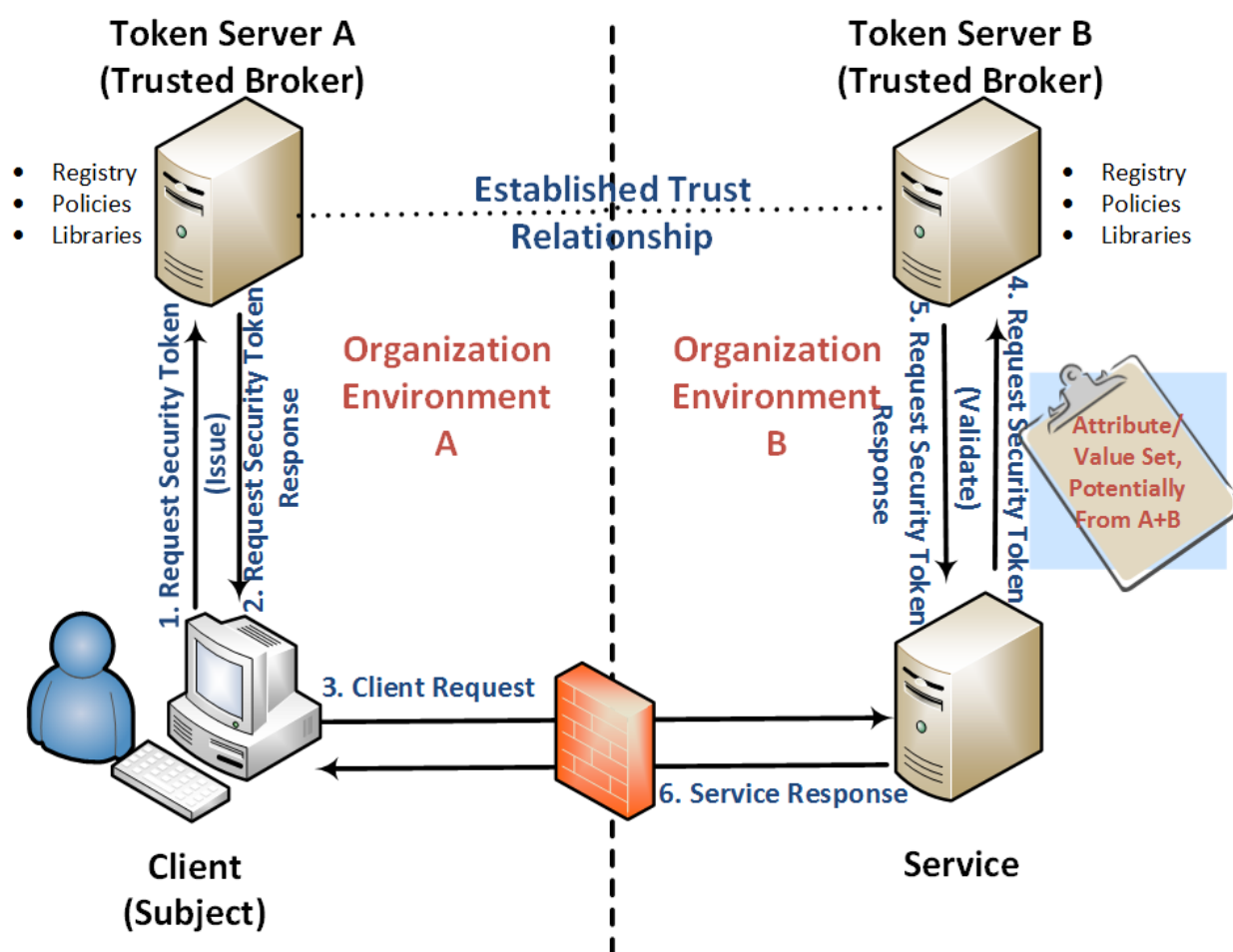


Figure 6 : Use Case 5 – Cross-Security Boundaries

2.6.2. Cross-Security Boundaries Token Service Considerations and Constraints

This information guidance specification provides the following high-level constraints, shown in [Table 6](#).

Table 6 - Cross-Security Boundaries Considerations and Constraints

Cross-Security Boundaries Considerations and Constraints
Token services operating out of different trust domains MUST establish trust between the token services which can be a one-way trust or bi-directional based on the requirement for information flow and security.
All entities MUST be approved to exchange information by the program's AO. This approval may be in the form of an ATO.
Each exchange with the token service MUST be encrypted using TLS, version 1.2.
Each token service transaction MUST be mutually authenticated using PKI certificates.
Each service provider MUST check the validity of the token service's PKI certificate (including the certificate's revocation status).
The token service MUST initiate mutual authentication with the Subject or using Public Key Cryptography
The token service MUST check the validity of the Subject's PKI certificate (including the certificate's revocation status)
A service provider MUST reject any request bearing a token from a token service that has not been authenticated and is not explicitly trusted.
Any token issued by a token service MUST be signed, and it MUST have explicit conditions of use, including an expiring time period.
Upon receipt of a token, a service provider MUST validate the token service's signature and the token's conditions of use, rejecting requests that do not comply with those conditions.
Tokens MUST not be reused. Refresh tokens for the purpose of assertion propagation, should be requested from the consumer to the token service and propagated to the next service.
A token service MAY be used to bridge user/app identity between different security or trust domains.
A Cross-Security Boundaries Token Service MUST ensure that it meets audit trail requirements.

Appendix A Feature Summary

The following table summarizes major features by version for WSS-TS and all dependent specs. The "Required date" is the date when systems should support a feature based on the specified driver. For those changes driven by the IC Markings System Register and Manual, the date is often one year after the date of publication. Executive Orders, ISOO notices, ICDs, and other policy documents have a variety of effective dates.

Table 7 - Feature Summary Legend

Key	Description
F	Full (able to comply and verified by spec to some degree)
P	Partial (Able to comply but not verifiable)
N	Non-compliance (Can't comply)
N/A	Not Applicable. Feature is no longer required.
Cell Colors represent the same information as the Key value	

A.1. WSS-TS Feature Comparison

Table 8 - WSS-TS Feature comparison

WSS-TS Feature Comparison		
Required date	Feature	V1
	Bridge user/app identity between enclave and different security/technical domains	F
	Issue and validate security tokens in single security/technical domain	F
	Issue and validate security tokens in a cross boundary security / technical domain	F
	Enable single sign-on to bridge access across diversity of end-point systems	F
	Enable stronger authentication or re-authentication to assert a higher degree of trust	F
	Bi-directional query to discover subject attributes in support of authorization	F
	Query to acquire subject attributes in support of Authorization	F
	Single authentication that bridges multiple authentication mechanisms (PKI, Kerberos, etc.)	F
	Federated Identity to support subject attribute access	F

Appendix B Change History

The following table summarizes the version identifier history for this DES.

Table 9 - DES Version Identifier History

Version	Date	Purpose
2014-DEC	4 December 2014	Initial Release

Appendix C List of Abbreviations

This appendix lists all the acronyms and abbreviations referenced in this encoding specification.

ABAC	Attribute Based Access Control
AO	Authorizing Official
ATO	Authority To Operate
CIO	Chief Information Officer
CVE	Controlled Vocabulary Enumeration
DES	Data Encoding Specification
DNI	Director of National Intelligence
DOD	Department of Defense
IC	Intelligence Community
IC CIO	Intelligence Community Chief Information Officer
IC EA	Intelligence Community Enterprise Architecture
IC ESB	Intelligence Community Enterprise Standards Baseline
IC ITE	Intelligence Community Information Technology Enterprise
ICD	Intelligence Community Directive
ICPG	Intelligence Community Program Guidance
ICS	Intelligence Community Standard
IdP	Identity Provider
IETF	Internet Engineering Task Force
IT	Information Technology
OCIO	Office of the Intelligence Community Chief Information Officer
ODNI	Office of the Director of National Intelligence
PKI	Public Key Infrastructure
RFC	Request for Comments
RSO	Reduced Sign-On
RST	Request Security Token

RSTR	Request Security Token Response
SAML	Security Assertion Markup Language
SLO	Single Log-Off
SSL	Secure Sockets Layer
SSO	Single Sign-On
TLS	Transport Layer Security
XML	Extensible Markup Language
XSL	Extensible Stylesheet Language

Appendix D Bibliography

Bibliography

[1] CNSSI 4009

Committee on National Security Systems. *National Information Assurance (IA) Glossary*. 4009. 26 April 2010.

Available online at: http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

[2] IC ITE INC1 IMPL

Office of the Director of National Intelligence. *Intelligence Community Information Technology Enterprise (IC ITE) Increment 1 Implementation Plan*. July 2012.

Available online Intelink-TS at: <http://go.ic.gov/HvBHBmY>

[3] ICD 500

Office of the Director of National Intelligence. *Director of National Intelligence Chief Information Officer*. Intelligence Community Directive 500. 7 August 2008.

Available online Intelink-TS at: <http://go.ic.gov/enm8L9x>

Available online at: http://www.dni.gov/files/documents/ICD/ICD_500.pdf

[4] ICD 502

Office of the Director of National Intelligence. *Integrated Defense of the Intelligence Community Information Environment*. Intelligence Community Directive 502. 11 March 2011.

Available online at: http://www.dni.gov/files/documents/ICD/ICD_502.pdf

[5] ICD 503

Office of the Director of National Intelligence. *Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation*. Intelligence Community Directive 503. 15 September 2008.

Available online Intelink-TS at: <http://go.ic.gov/b1ZONju>

Available online at: http://www.dni.gov/files/documents/ICD/ICD_503.pdf

[6] ICPG 500.1

Assistant Director of National Intelligence for. *Digital Identity*. Intelligence Community Policy Guidance 500.1. 7 May 2010.

Available online Intelink-TS at: <http://go.ic.gov/3rfgL6D>

[7] ICPG 500.1

Assistant Director of National Intelligence for Policy and Strategy. *Digital Identity*. Intelligence Community Policy Guidance 500.1. 23.

Available online Intelink-TS at:

Available online at:

[8] ICPG 500.2

Assistant Director of National Intelligence for Policy and Strategy. *Attribute-Based Authorization and Access Management*. Intelligence Community Policy Guidance 500.2. 23 November 2010.

Available online Intelink-TS at: <http://go.ic.gov/ha2FxyZ>

Available online at: http://www.dni.gov/files/documents/ICPG/icpg_500_2.pdf

[9] ICPG 710.1

Director of National Intelligence. *Application of Dissemination Controls: Originator Control*. Intelligence Community Policy Guidance 710.1. 25 July 2012.

Available online Intelink-TS at: <http://go.ic.gov/yAqVQ0H>

[10] ICS 500-20

Director of National Intelligence Chief Information Officer. *Intelligence Community Enterprise Standards Compliance*. Intelligence Community Standard 500-20. 16 December 2010.

Available online Intelink-TS at: <http://go.ic.gov/sLKNq3N>

Available online Intelink-U at: <http://www.purl.org/ic/standards/policy/ICS500-20>

[11] ICS 500-21

Director of National Intelligence Chief Information Officer. *Tagging of Intelligence and Intelligence-Related Information*. Intelligence Community Standard 500-21. 28 January 2011.

Available online Intelink-TS at: <http://go.ic.gov/cWYv9nw>

Available online Intelink-U at: <http://www.purl.org/ic/standards/policy/ICS500-21>

[12] ICS 500-27

Director of National Intelligence Chief Information Officer. *Intelligence Community Standard for Collection and Sharing of Audit Data*. Intelligence Community Standard 500-27. 2 June 2011.

Available online Intelink-TS at: <http://go.ic.gov/5yamXTu>

[13] ICS 500-29

Director of National Intelligence Chief Information Officer. *Intelligence Community Digital Identifier*. Intelligence Community Standard 500-29. 12 July 2012.

Available online Intelink-TS at: <http://go.ic.gov/aCTDYKI>

[14] ICS 500-30

Director of National Intelligence Chief Information Officer. *Intelligence Community Enterprise Authorization Attributes: Assignment, Sources, and Use for Attribute-Based Access Control of Resources*. Intelligence Community Standard 500-30. 24 April 2014.

Available online Intelink-TS at: <http://go.ic.gov/sTPgT9Y>

[15] IETF-RFC 2119

Internet Engineering Task Force. *Key words for use in RFCs to Indicate Requirement Levels*. March 1997.

Available online at: <http://tools.ietf.org/html/rfc2119>

[16] OpenID Connect

The OpenID Foundation (OIDF). *OpenID Connect*. Version 1.0.

Available online at: <http://openid.net/connect/>

[17] SAML 2.0

Organization for the Advancement of Structured Information Standards. *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*. 27 March 2008.

Available online at: <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>

[18] SAML 2.0 Attribute Sharing

OASIS Security Services Technical Committee. *SAML 2.0 Attribute Sharing Profile for X.509 Authentication-Based Systems, Version 1.0, [Encrypted Mode]*. 27 March 2008.

Available online at: <http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-x509-authn-attrib-profile-cd.html>

[19] SAML 2.0 Glossary

Organization for the Advancement of Structured Information Standards. *Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0*. March 15, 2005.

Available online at: <http://docs.oasis-open.org/security/saml/v2.0/saml-glossary-2.0-os.pdf>

[20] WS-Federation

The Organization for the Advancement of Structured Information Standards (OASIS). *Web Services Federation Language*. V 1.2 22 May 2009.

Available online at: <http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.html>

[21] WS-Security

The Organization for the Advancement of Structured Information Standards (OASIS). *OASIS Web Services Security: SOAP Message Security*. V1.1.1 May 2012.

Available online at: <http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-SOAPMessageSecurity-v1.1.1-os.html>

[22] WS-Trust

The Organization for the Advancement of Structured Information Standards (OASIS). *WS-Trust*. V1.4 25 April 2012.

Available online at: <http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/ws-trust.html>

Appendix E Points of Contact

The Intelligence Community Chief Information Officer (IC CIO) facilitates one or more collaboration and coordination forums charged with the adoption, modification, development, and governance of IC technical specifications of common concern. This technical specification was produced by the IC CIO and coordinated with these forums, approved by the IC CIO or a designated representative, and made available at DNI-sponsored web sites. Direct all inquiries about this IC technical specification to the IC CIO, an IC technical specification collaboration and coordination forum, or IC element representatives involved in those forums.

Public Website: <http://purl.org/ic/standards/public>

E-mail: ic-standards-support@ugov.gov [mailto:ic-standards-support@ugov.gov].

Appendix F IC CIO Approval Memo

An Office of the Intelligence Community Chief Information Officer (OCIO) Approval Memo should accompany this enterprise technical data specification bearing the signature of the Intelligence Community Chief Information Officer (IC CIO) or an IC CIO-designated official(s). If an OCIO Approval Memo is not accompanying this specification's version release package, then refer back to the authoritative web location(s) for this specification to see if a more complete package or a specification update is available.

Specification artifacts display a date representing the last time a version's artifacts as a whole were modified. This date most often represents the conclusion of the IC Element collaboration and coordination process. Once the IC Element coordination process is complete, the specification goes through an internal OCIO staffing and coordination process leading to signature of the OCIO Approval Memo. The signature date of the OCIO Approval Memo will be later than the last modified date shown on the specification artifacts by an indeterminable time period.

Upon signature of the OCIO Approval Memo, IC Elements may begin to use this specification version in order to address mission and business objectives. However, it is critical for IC Elements, prior to disseminating information encoded with this new specification version, to ensure that key enterprise services and consumers are prepared to accept this information. IC Elements should work with enterprise service providers and consumers to orchestrate an orderly implementation transition to this specification version in concert with mandatory and retirement usage decisions captured in the IC Enterprise Standards Baseline as defined in Intelligence Community Standard (ICS) 500-20.^[10]