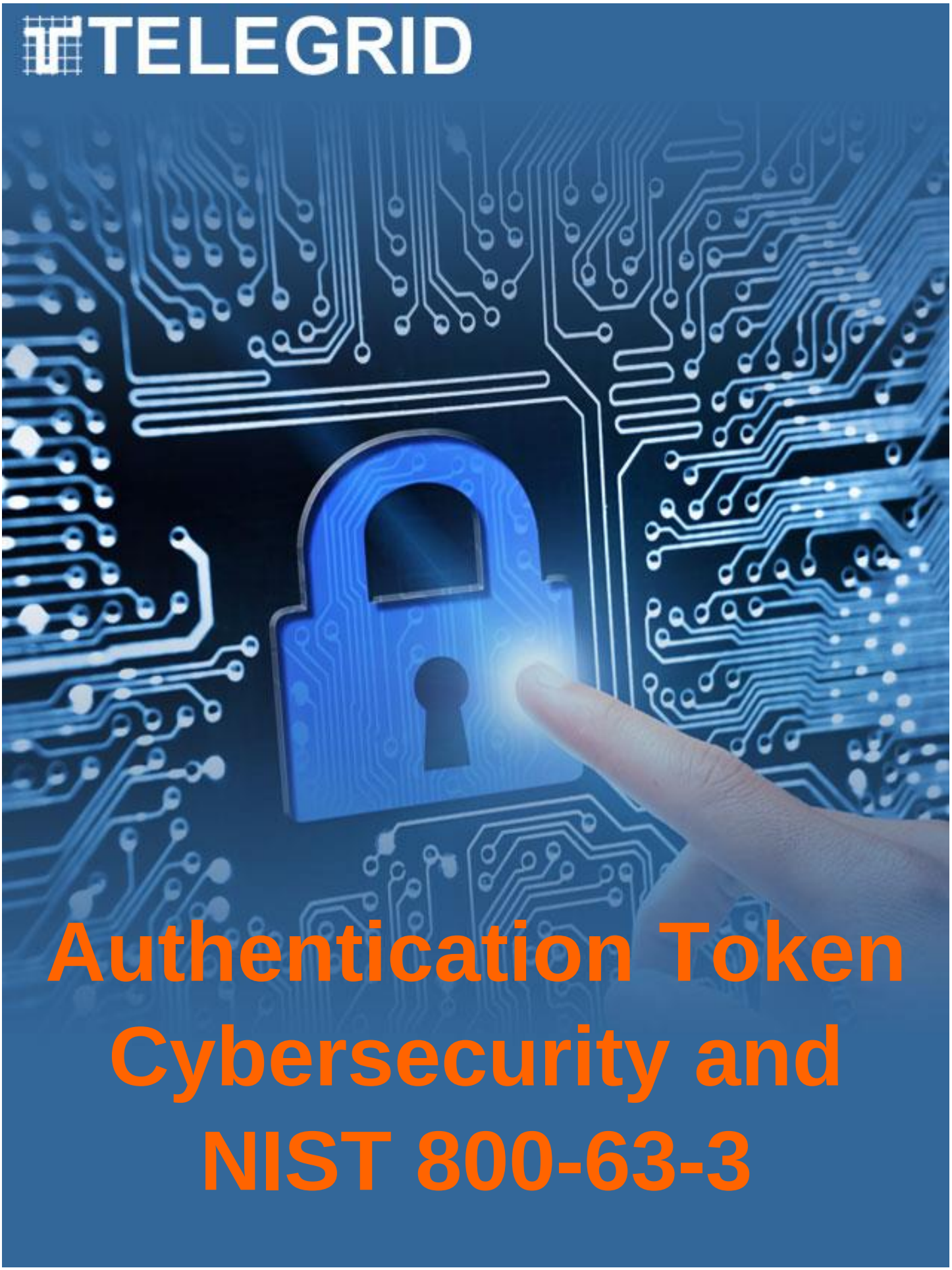
TELEGRID



Authentication Token Cybersecurity and NIST 800-63-3

TABLE OF CONTENTS

TABLE OF FIGURES

1 Abstract

In June 2017 the National Institute of Standards and Technology (NIST) released its updated Digital Identity Guidelines - Special Publication NIST 800-63-3. The result of this revolutionary document is that it will force the Federal Government and the military to adopt the concept of **Holder of Key**. According to NIST, Holder of Key is now a requirement for secure systems in order to protect authentication tokens from interception and manipulation. This creates a problem for most networks. According to the SAML and OAuth standards, the only approved method for implementing Holder of Key is through Public Key Infrastructure (PKI) and TLS with mutual authentication. However, most networks break TLS connections, a process known as “Break and Inspect”, in order to examine message contents. Break and inspect makes it impossible to utilize user PKI certificates to meet Holder of Key.

This paper describes an advanced solution to this problem developed by TELEGRID Technologies, Inc. (TELEGRID) - the SMRTe PKI Proxy (P/N: RWP-1801). The SMRTe PKI Proxy is the **ONLY** product that dynamically generates PKI certificates to satisfy Holder of Key. Adding the SMRTe non-invasively makes a network NIST 800-63-3 compliant by providing the following benefits: automatic generation of PKI certificates, conversion of any authentication credential to a PKI certificate, and network-wide TLS with mutual authentication to allow Holder of Key.

2 Introduction

Gartner Research estimates that by the year 2019 more than 80% of organizational networks will utilize some form of Identity and Access Management (IdAM) software or services. However, Federated Identity and its subset Single Sign-On (SSO) have exposed organizations to new forms of cybersecurity attacks based on the inherently unsecure nature of authentication tokens. Recognizing these issues, in June 2017 the National Institute of Standards and Technology (NIST) released Special Publication NIST 800-63-3 Digital Identity Guidelines which required Holder of Key for the most secure systems. According to NIST, Holder of Key must be employed to secure authentication tokens from interception and manipulation.

According to the SAML and OAuth standards, the only approved method for Holder of Key is via Public Key Infrastructure (PKI). This creates an issue for most organizations since they break the TLS connection to inspect the message contents thereby disallowing PKI internally. The SMRTe PKI Proxy was designed to resolve this issue and is the **ONLY** product that dynamically generates PKI certificates to satisfy NIST's Holder of Key requirement. It can be deployed as a complete SSO solution or as part of an existing IdAM infrastructure to increase overall network security.

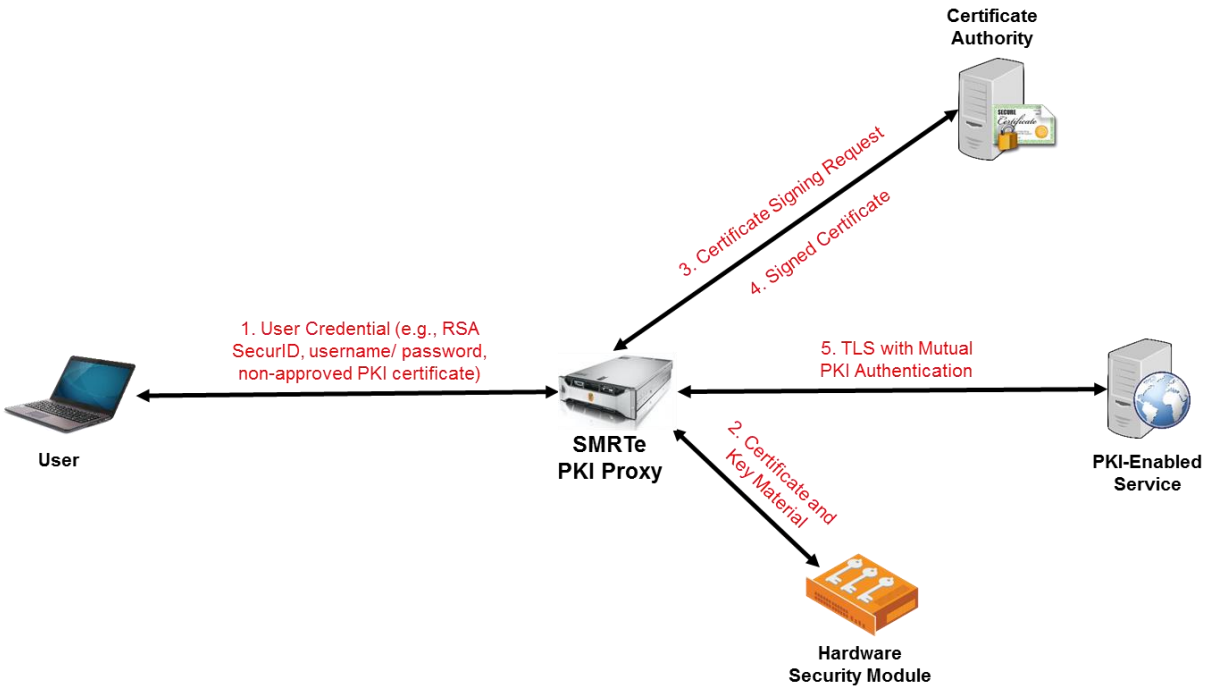


Figure 2-1 SMRTe PKI Proxy Authentication Process

3 Why are NIST Guidelines Important

NIST is a non-regulatory federal agency within the Department of Commerce which issues guidelines across multiple scientific areas including cybersecurity. In 2002 Congress passed the Federal Information Security Modernization Act (FISMA) which was subsequently updated in 2014. FISMA created a requirement for federal agencies to manage information security based on publications that are developed by NIST - FISMA 2014, 44 U.S.C. § 3551 *et seq.*, Public Law (P.L.) 113-283. Based on FISMA requirements, the Office of Management and Budget (OMB) in Circular A-130 stated that federal agencies should implement the security policies in NIST 800 series Special Publications (e.g. SP 800-63-3 Digital Identity Guidelines).

In 2014 the DoD CIO, effectively joining federal agencies, issued Instruction 8510.01 replacing its own DoD Information Assurance Certification and Accreditation Process (DIACAP) risk management process with NIST's Risk Management Framework (RMF). NIST's RMF brings together all of the FISMA-related security standards and guidance. With flow down provisions in most government contracts, contractors are now also subject to NIST guidelines.

NIST's cybersecurity guidelines, such as NIST 800-63-3, are therefore a requirement of the Federal Government, the military, and most government contractors.

4 Single Sign-On Overview

Federated Identity is defined as a standard policy and protocol for management of users' identities and attributes across multiple identity management systems. Single Sign-On (SSO) is a subset of Federated Identity and refers to the method of authenticating a user and providing them with an authentication token or ticket that can be used to access multiple applications and devices.

A SSO infrastructure consists of three main elements, a user, a Service Provider (SP) and an Identity Provider (IdP). As shown in Figure 4-1, when a user attempts to access a SP, they are redirected to an IdP to obtain an authentication token. The IdP authenticates the user based on the credential they provide and responds with an authentication token with specific user attributes. This authentication token is then presented by the user to the SP in order to gain access.

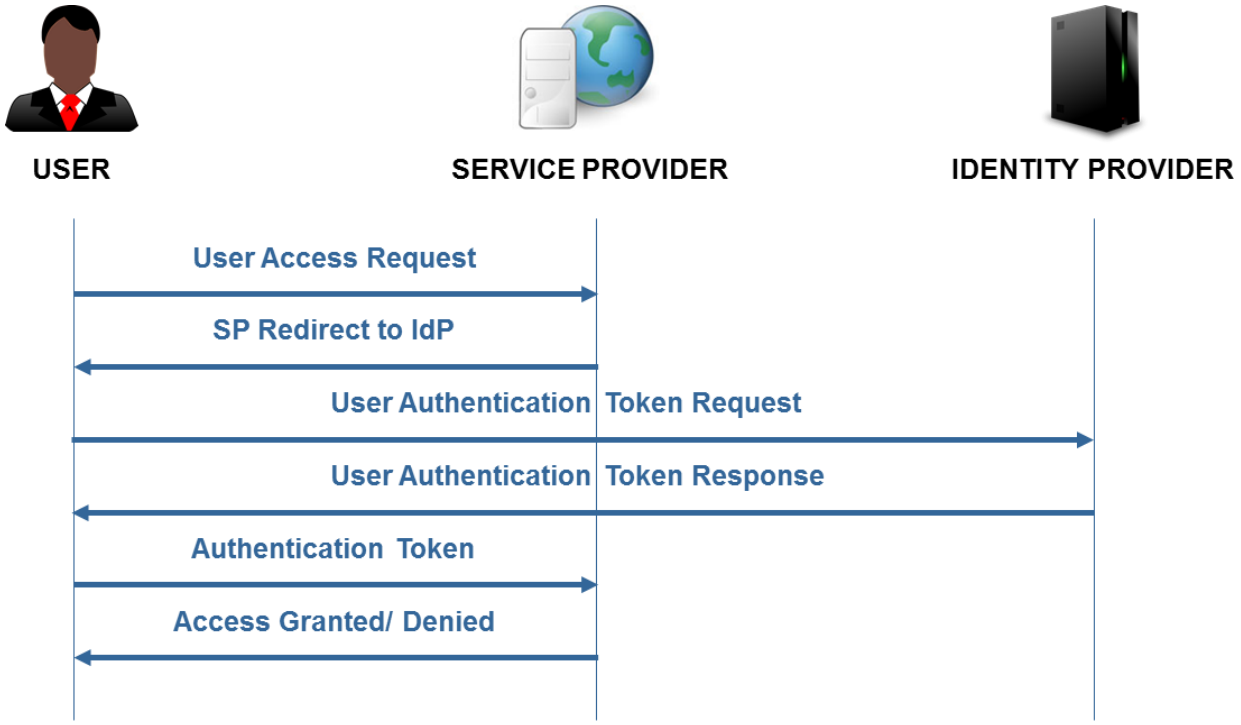


Figure 4-1 Single Sign-On Authentication Flow

A SSO approach can vary in many ways. For instance, the SP can request an authentication token directly from the IdP, a method referred to as back-channel authentication. This however is not the typical method used since it goes against the basic purpose of SSO which is to allow a user to reuse the same authentication token with multiple SPs. Another option is to have multiple IdPs and an IdP proxy which directs user requests to the appropriate IdP. This is typically performed in large disparate networks (e.g., cloud infrastructures). The more IdPs in the network the harder it is to track and verify authentication tokens. This leads to potential cybersecurity attacks as described in Section 5.

The two most prevalent standards for SSO are SAML and OAuth. The Security Assertion Markup Language (SAML) is an open XML based standard developed by the Organization for the Advancement of Structured Information Standards (OASIS). OAuth is also an open standard that is related to OpenID Connect (OIDC), an authentication layer on top of OAuth 2.0. While there are many other standards, most web and mobile applications utilize either SAML or OAuth. Both standards though are susceptible to the cybersecurity attacks described below. Recognizing this threat NIST recommended the implementation of Holder of Key via PKI.

5 Authentication Token Cybersecurity Attacks

Authentication Tokens by their nature are susceptible to cybersecurity attacks. Designed for convenience they are used to gain access to multiple SPs without having to go back to an IdP each time for authentication and authorization. In order to reduce the load on IdPs and maximize their reusability, the earliest versions of authentication tokens did not even include details of the SP being accessed or the IdP issuing the token. Hackers could therefore use existing authentication tokens, or create them, to access any SP on the network. This was limited in later versions of SAML and OAuth but authentication tokens without Holder of Key are still susceptible to the following cybersecurity attacks.

5.1 Man-in-the-Middle

A Man-in-the-Middle attack is a form of "wire-tapping" where a malicious individual intercepts the authentication token being sent from the IdP to the user. As shown in Figure 5-1 the attacker uses the authentication token to gain access to a SP. Holder of Key prevents Man-in-the-Middle attacks by requiring that a user provide proof of their identity along with the authentication token which references them.

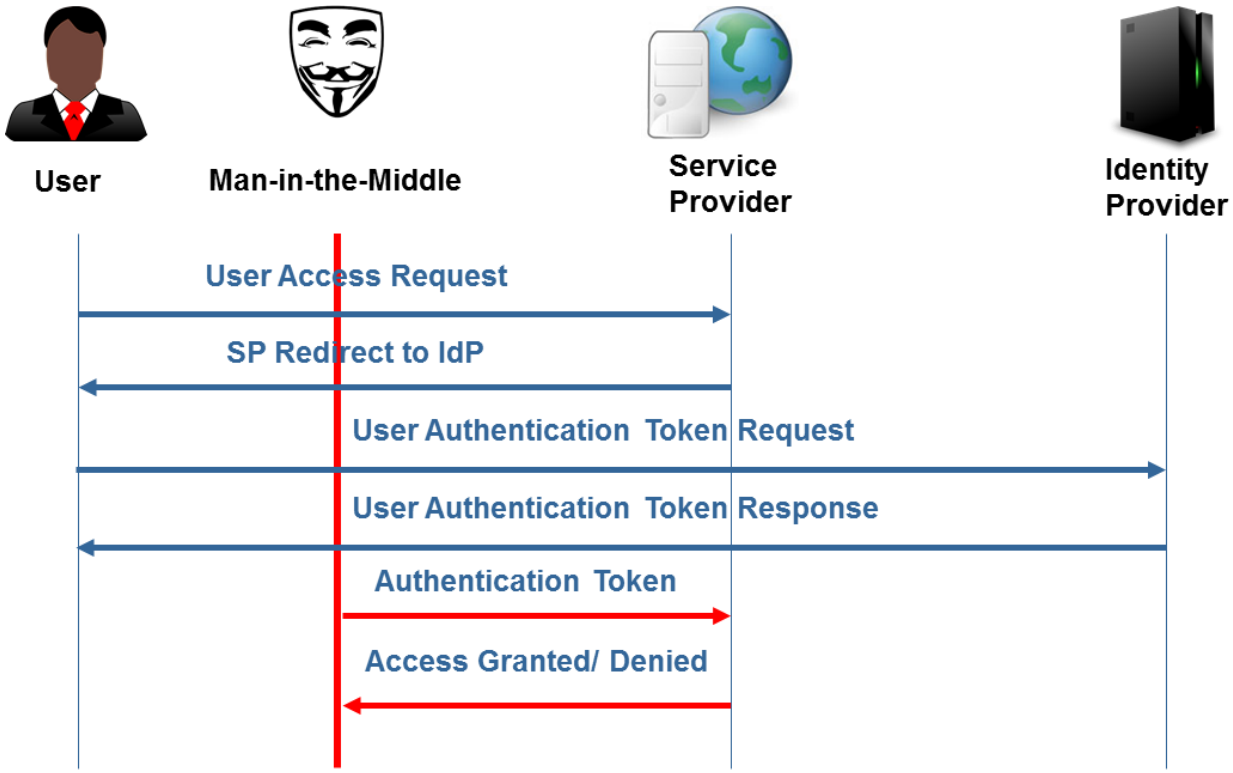


Figure 5-1 Authentication Token Man-in-the-Middle Attack

5.2 Compromised Tokens

Similar to a Man-in-the-Middle attack, this attack also involves a malicious user seeking to impersonate a valid user. In this attack the authentication token is obtained from a website cache or by triggering a buffer overflow from a central server. Indeed this was one of the main vulnerabilities in the Heartbleed attack on OpenSSL. While limiting an authentication token's validity period can prevent this attack, it requires the user to re-authenticate to the IdP more frequently, draining network resources. Additionally this attack must be launched after the authentication token has expired which cannot be guaranteed. Holder of Key is the only true method to prevent this type of attack by requiring that a user provide proof of their identity along with the authentication token which references them to a SP.

5.3 Denial of Service

In this type of attack a malicious user seeks to degrade overall network performance by forcing a SP to validate false authentication tokens. In this attack the user is not concerned with whether the token is validated but with occupying valuable resources.

According to OASIS, "The SAML protocol is susceptible to a denial of service (DOS) attack. Handling a SAML request is potentially a very expensive operation, including parsing the request message (typically involving construction of a DOM tree), database/assertion store lookup (potentially on an unindexed key), construction of a response message, and potentially one or more digital signature operations."

Holder of Key prevents this type of attack by providing a method for the SP to perform user authentication, via TLS with mutual authentication, prior to token validation. Holder of Key provides a method for a SP to authenticate a user prior to handling "expensive" SAML requests.

5.4 Assertion Repudiation

Assertion Repudiation refers to a valid user insisting that they were not the party that delivered an authentication token to a SP. This is not a cybersecurity attack by a malicious user but rather an issue related to accounting. Accounting, which is the third A in an Authentication, Authorization and Accounting (AAA) framework, refers to measuring the resources consumed by a user. An example of Assertion Repudiation is a credit card holder denying a charge by claiming they did not input their credit card number to a specific website. Holder of Key guarantees that the user referenced in the authentication token accessed the service, thereby removing their ability to repudiate the assertion at a later date.

5.5 User Re-authentication

Following initial user authentication, an IdP is not required to re-authenticate a user. Therefore a SP cannot be sure that the authentication token it receives is from a user whose credentials were revoked. If the authentication token has a long validity period the possibility of the credential being revoked increases. Per NIST 800-63C a service provider can request that an IdP re-authenticate the user but there is no direct method for the SP to independently authenticate the user. Holder of Key provides a method for the SP to re-authenticate a user via TLS with mutual authentication.

6 NIST 800-63-3

In June 2017, NIST released the NIST 800-63-3 Digital Identity Guidelines which superseded NIST 800-63-2. NIST 800-63-3 goes further than 800-63-2 in covering all aspects of user authentication from initial risk assessment to deployment of Federated Identity solutions. As opposed to earlier guidelines, which relied solely on authentication type (e.g., single-factor, hard token, etc.) to determine system access, NIST 800-63-3 includes assurance levels for the identity proofing method, the authenticator type and the security level of the federated system being accessed. The image below details the requirements to meet each of the Identity Assurance Levels (IAL), the Authenticator Assurance Levels (AAL) and the Federated Assurance Levels (FAL).

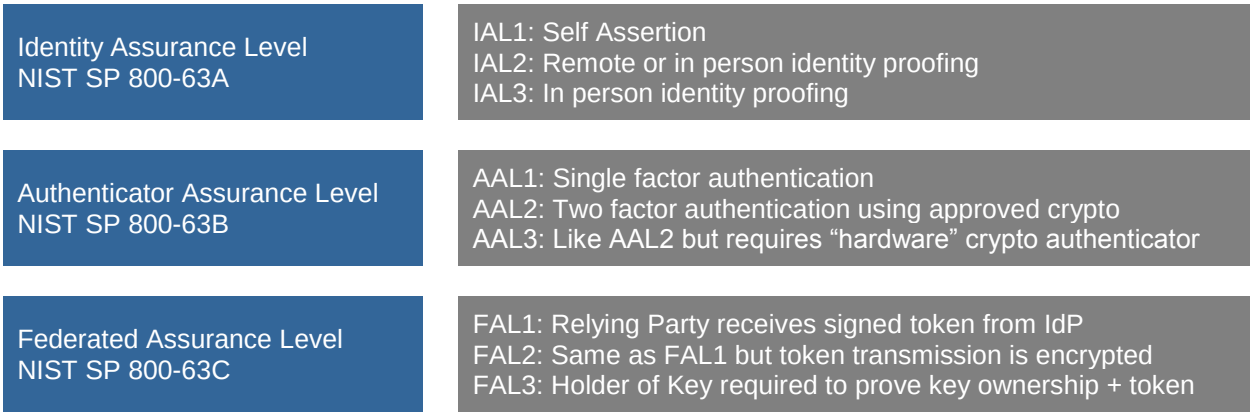


Figure 6-1 NIST 800-63-3 Assurance Level Definition

For the most secure systems, those that are deemed FAL3 for Federated Assurance Level, the NIST guidelines require that a user present a proof that they are the user referenced in an authentication token. This was instituted because relying solely on authentication tokens exposes the network to several cybersecurity attacks, as described in Section 5. Proof of ownership of an authentication token is called Holder of Key and its implementation is described in the following section.

6.1 Holder of Key

According to the SAML 2.0 Holder of Key Profile Definition and the OAuth 2.0 Authorization Framework, currently the only standards-based approach for implementing Holder of Key is with X.509 PKI certificates. While SAML refers explicitly to PKI certificates, OAuth more cryptically refers to an ephemeral asymmetric key pair, of which PKI is the only standards based option.

Both specifications define the process of implementing Holder of Key as follows. The process begins with a user initiating a TLS connection with mutual authentication to an IdP in order to request an authentication token, as shown in Figure 6-2. The IdP then uses the subject fields within the user's PKI certificate (e.g., Subject Name) to create the authentication token. Neither the SAML nor OAuth standards define the exact PKI subject fields which must be selected, but rather leave that decision to the network administrator. The user then initiates a TLS connection with mutual authentication to the SP and passes its authentication token. The SP examines the user's PKI certificate, which it received from the TLS connection, to validate that the authentication token includes the required subject fields. By matching the PKI certificate to the contents of the authentication token, Holder of Key is established.

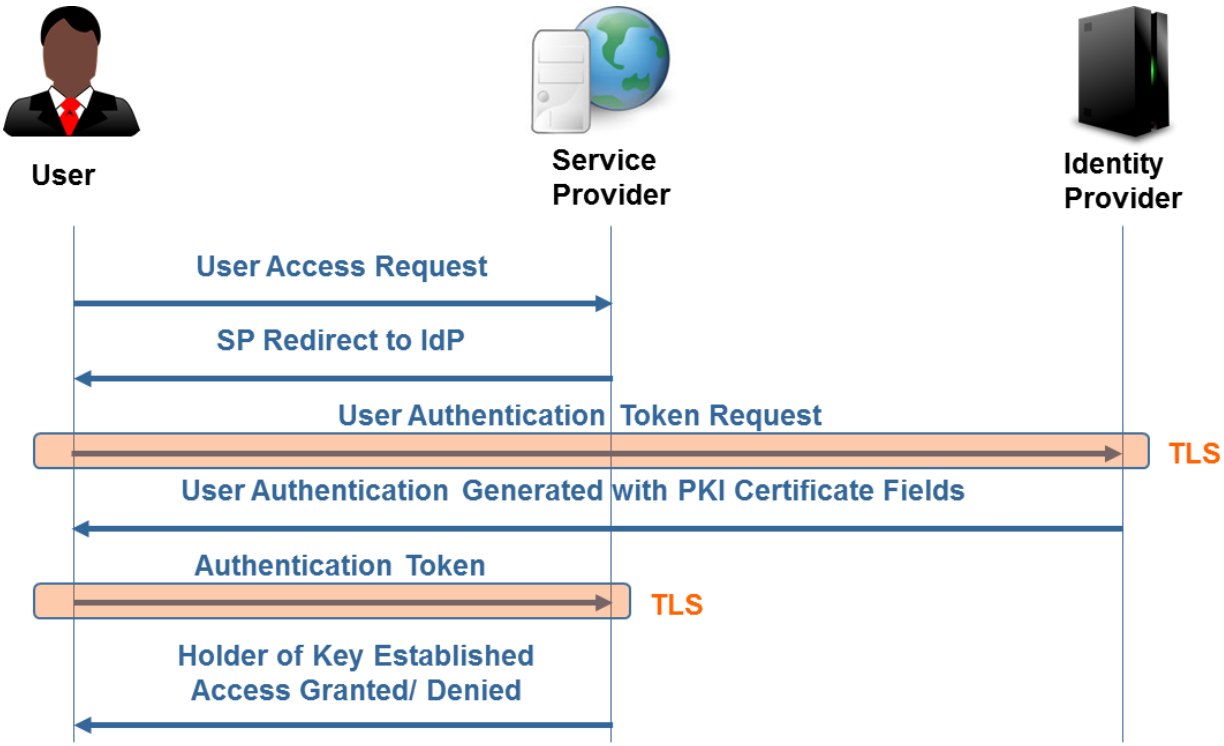


Figure 6-2 NIST 800-63-3 Holder of Key Authentication Flow

7 The Break and Inspect Capability Gap

The implementation of Holder of Key seems straightforward, however, many organizations have a major issue with Holder of Key compliance. The reason is that modern day networks employ "Break and Inspect" either at a network barrier (e.g., firewall) or internally (e.g., gateway). Break and inspect refers to breaking a TLS connection between two parties in order to examine the secure contents of a message. When a secure connection is broken the contents can be sent to a diagnostics tool or data loss prevention system for inspection. Break and inspect is necessary because hackers typically hide their malicious activity from monitoring tools within TLS traffic. Indeed this was the case for the Office of Personnel Management (OPM) hack which was only discovered when a network administrator inspected the contents of a TLS connection and noticed that personal information was leaving the network. For this reason break and inspect has gained in popularity with the Ponemon Institute estimating that 1/3 of organizations now inspect TLS traffic.

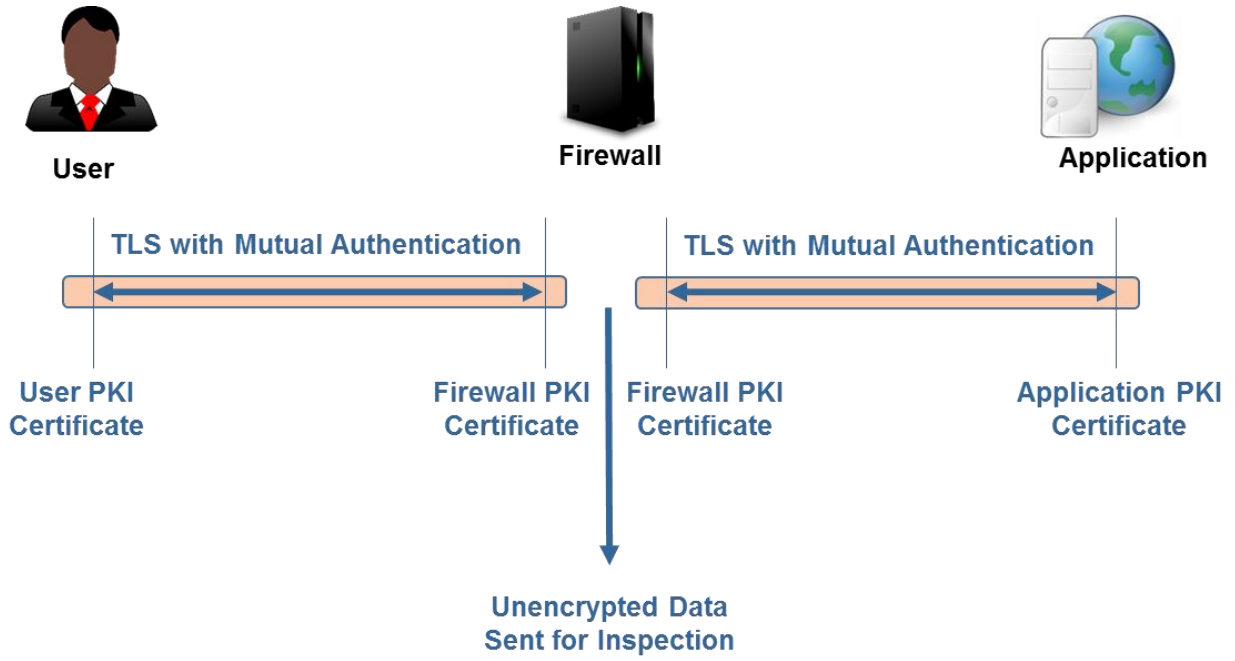


Figure 7-1 Break and Inspect Authentication Flow

Once a TLS connection is broken, it is impossible to reestablish TLS with mutual authentication between the user and the application (i.e., SP). The reason is that the break and inspect tool (e.g., firewall, gateway, etc.) does not store users' private keys in order to reestablish the TLS connection to the application. **This would create a major cybersecurity threat**. Indeed Ponemon also found that for organizations who are looking for a TLS decryption solution, 79% are concerned with how to handle PKI certificate management.

Therefore, rather than storing user's private keys and certificates at the break and inspect tool, the current method is to establish a TLS connection to the application with the break and inspect tool's server certificate, as shown in Figure 7-1. This creates two separate TLS connections making it impossible for the user to provide their certificate to the application. The break and inspect tool can send the user's details, for example for accounting purposes, but it cannot generate a unique PKI certificate for each user which is required for Holder or Key.

8 SMRTe PKI Proxy

A lack of user PKI certificates due to break and inspect creates an issue for the Federal Government, the military and commercial organizations which are required to comply with NIST guidelines. The NIST 800-63-3 guidelines require Holder of Key for authentication and authorization of users to highly secure systems (i.e., FAL3 systems). Based on the SAML and OAuth standards, Holder of Key is only possible through PKI. TELEGRID's SMRTe PKI Proxy was developed specifically to meet this requirement.

The SMRTe accepts any user credential type and automatically generates a unique PKI certificate that can be used for secure authentication and authorization inside of a network. The SMRTe elevates the entire network security level by creating a PKI baseline throughout the network in order to comply with NIST 800-63-3.

The SMRTe is the enterprise version of TELEGRID's SMRT which is deployed globally by the Defense Information Systems Agency (DISA). The SMRTe is FIPS 140-2 and DISA Security Technical Implementation Guides (STIG) compliant and operates on Security Enhanced Linux (SELinux).

8.1 Why is PKI So Important

PKI has been determined by the Federal Government and the military to be the most secure method of providing Multi-Factor Authentication (MFA) and information flow in modern networks. PKI certificates combine an individual's identity information with cryptographic information that is non-forgeable and non-changeable. They, in essence, provide a standards-based representation of the individual's physical identity in electronic form and enable data sharing among appropriate, broad and dynamic communities of interest.

PKI certificates allow authorized users to securely access, process, store, transport, and use information, applications, and networks regardless of technology, organization, or location. PKI-based digital signatures safeguard the integrity of data and information as it moves within a network. Mutual PKI authentication ensures the integrity and confidentiality of devices and resources operating on a network. PKI also enables management of identities operating in groups or certain roles within systems.

8.2 SMRTe Authentication Flow

The SMRTe authentication process is shown in Figure 8-1. When a user attempts to access a FAL3 secure system they are redirected to the SMRTe. The user provides their credential to the SMRTe which, in turn, generates a Certificate Signing Request (CSR) using its FIPS 140-2 approved encryption engine. Certificates can be limited depending on requirements (e.g., time limit, etc.). The SMRTe transmits the CSR to an approved Certificate Authority (CA) for approval and signing. The final signed certificate is then used to log into the PKI-enabled system on behalf of the user. The web traffic is then proxied to the user as a "defense in depth measure".

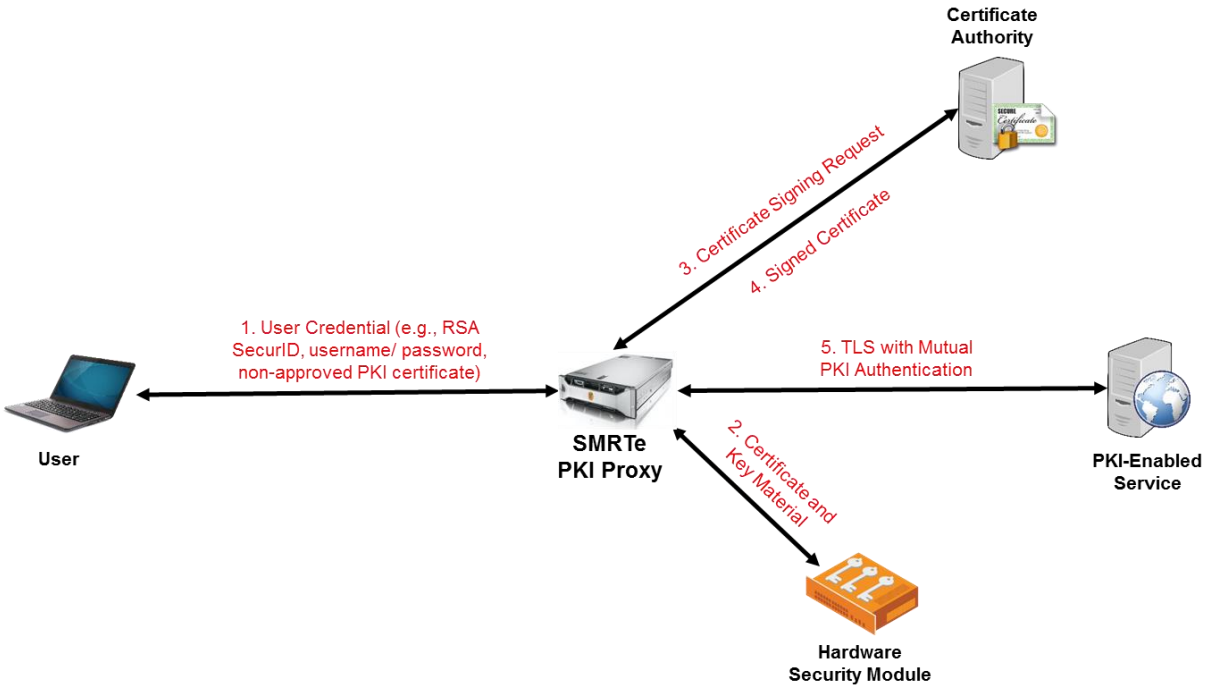


Figure 8-1 SMRTe PKI Proxy Authentication Process

8.3 SMRTe Single Sign-On

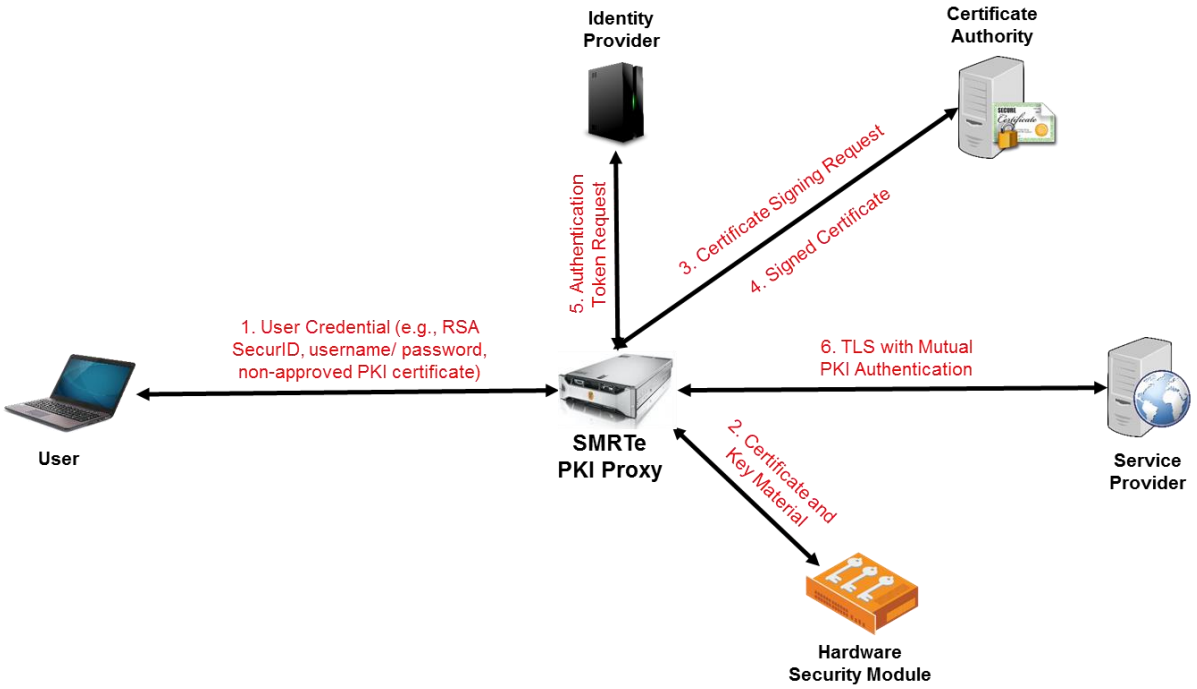


Figure 8-2 SMRTe within a SSO Infrastructure

The SMRTe can be deployed in conjunction with an existing SSO infrastructure, as shown in Figure 8-2. If deployed within a SSO infrastructure, the SMRTe will create a unique PKI certificate and then use it to log into an IdP to request an authentication token. This PKI certificate and associated authentication token will be used by the SMRTe to log the user into a FAL3 SP to satisfy NIST's Holder of Key guidelines.

8.4 SMRTe and Break and Inspect

When deployed in conjunction with a network barrier (e.g., firewall, gateway, etc.), that is performing break and inspect on TLS traffic, the SMRTe will receive user credentials directly from the network barrier. These credentials can be sent to the SMRTe in multiple formats by the network barrier. Since the SMRTe is generating a new user certificate, with a new private key, the network barrier does not need to store the user's existing private key. The SMRTe will use the credentials it receives to generate a CSR which will be sent to a CA to generate a unique PKI certificate. This PKI certificate can be used to log into a SP or be sent to an IdP to generate an authentication token.

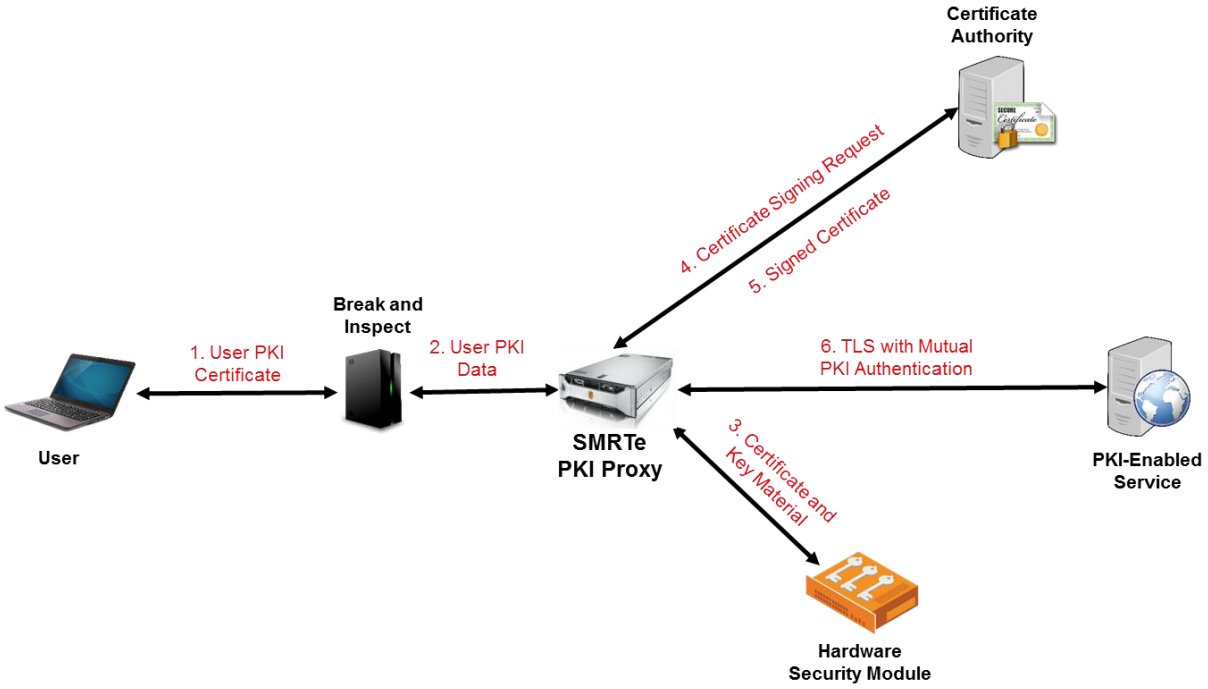


Figure 8-3 SMRTe with Break and Inspect

9 CONCLUSION

The recently released NIST Special Publication 800-63-3 has drastically expanded the importance of its Digital Identity Guidelines to include all facets of an IdAM infrastructure. Once of the most important changes is the requirement for Holder of Key when presenting authentication tokens to FAL3 systems. Based on the existing SAML and OAuth standards, Holder of Key requires the presentation of a user's PKI certificate along with an authentication token. This is an issue for organizations which break the TLS connection at a network barrier for inspection purposes. TELEGRID's SMRTe PKI Proxy was developed specifically to promote PKI, in the most unobtrusive manner possible, with an existing Federated Identity or SSO infrastructure. Network Information Assurance (IA) capabilities enhanced by the SMRTe and its PKI technology enable and promote a common, ubiquitous, and secure network.

Appendix A: Determining Federated Assurance Level

The NIST guidelines define a Federated Assurance Level (FAL) of FAL1 to FAL3 for information systems, with FAL3 being the most secure. NIST has defined a method to determine the appropriate assurance level based upon the risk associated with an adversary impersonating a valid user or maliciously obtaining their credentials. The flow diagram below describes the process of obtaining the FAL of an information system by determining the risk of breach including reputation damage, financial loss, personal safety, etc. When determining the FAL of an information system the NIST guidelines require that an administrator view the risks as they pertain to the organization and not to the individual user. The FAL determination will affect the method that authentication tokens are transmitted throughout the network.

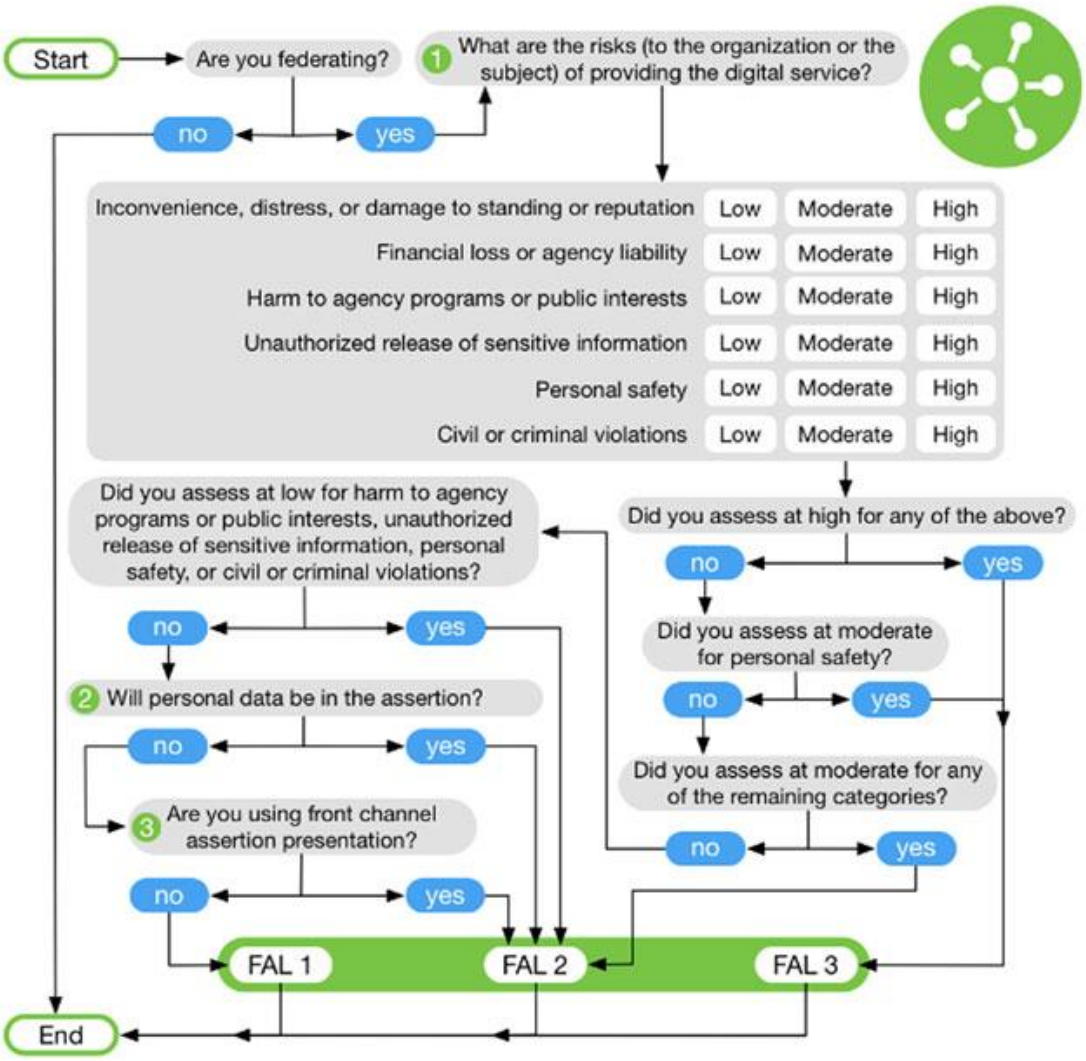


Figure 0-1 Federated Assurance Level Determination

Appendix B: Acronym List

AAA	Authentication, Authorization and Accounting
AAL	Authenticator Assurance Level
CA	Certificate Authority
CSR	Certificate Signing Request
DIACAP	DoD Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DOS	Denial of service
FAL	Federated Assurance Level
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
IA	Information Assurance
IAL	Identity Assurance Level
IdAM	Identity and Access Management
MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
OASIS	Organization for the Advancement of Structured Information Standards
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OTP	One Time Password
PKI	Public Key Infrastructure
RMF	Risk Management Framework
SAML	Security Assertion Markup Language
SELinux	Security Enhanced Linux
SMRTe	Secure Multi-web Resource Tool for the Enterprise
SP	Service Provider
SSO	Single Sign-On
STIG	Security Technical Implementation Guides
TLS	Transport Layer Security