KPMG

Regulatory Alert

Regulatory Insights

February 2026

Cybersecurity: NIST/CISA Draft Report on Protecting Tokens and Assertions

KPMG Regulatory Insights:

- ***Draft Guidance Issued:*** *Voluntary draft guidance with recommendations for protecting digital identity tokens and assertions; directed toward cloud service providers and federal agencies (CSP customers) though the guidance would be useful to other entities making use of tokens and cryptographic keys.*
- ***Enhanced Security Controls:*** *Sets out principles and controls for identity management, including cryptographic key protection, token lifecycle management, and Zero Trust architectures.*
- ***Early Implementation Encouraged:*** *Follows recent high-profile incidents involving token theft, forgery, and misuse; entities are encouraged to consider implementing certain elements prior to final guidance such as reviewing token validation processes, mapping key signing token inventory, reviewing/updating audience restrictions, and clarifying responsibilities with CSPs.*
- ***More to Come:*** *Additional guidance tailored to AI agents will be forthcoming.*

The U.S. Department of Commerce's National Institute of Standards and Technology (NIST), in conjunction with the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), has released an "initial public draft" of the NIST Interagency Report, "Protecting Tokens and Assertions from Forgery, Theft, and Misuse" (NIST IR 8587). The agencies indicate the report responds to Executive Order 14306, *Sustaining Select Efforts to Strengthen the Nation's Cybersecurity,* which directs them to focus on critical protections against foreign cyber threats, and enhancements to secure technology practices.

The report outlines draft implementation guidance for cloud service providers (CSPs) and federal agencies (their customers) regarding the protection of tokens and assertions. It covers:

- Management Responsibilities and Principles
- Tokens and Assertions Overview
- Security Controls

The agencies acknowledge a number of recent high-profile cyberattacks where tokens have been stolen, forged, or misused, creating widespread access to sensitive information. The draft release is designed to provide technical recommendations to help to reduce, prevent or mitigate related harm.

Management Responsibilities and Principles

The draft report is intended to provide clear, actionable guidance for government agencies and cloud companies to protect the digital tokens used in their systems.

Managing Responsibilities: The agencies suggest that security in the cloud is a shared responsibility between the CSPs and their customers (in this instance, federal agencies) and outlines fundamental principles for digital identity security:

- **CSPs.** CSPs would be responsible for securing the underlying infrastructure and would be expected to adhere to key principles, including:
  - **Secure Design:** Building security into their products from the beginning.
  - **Transparency:** Being open about how their security works so customers can assess risks.
  - **Configurability:** Allowing customers to adjust security settings to match specific needs.
  - **Interoperability:** Using common standards so their systems can work securely with other services.
  - **Continuous Monitoring:** Constantly monitor their systems to detect, analyze, and respond to potential threats.

- **Customers.** Customers/Agencies are responsible for correctly configuring security settings, managing user access, and monitoring for threats. They would be expected to:
  - **Assess Risk:** Understand the sensitivity of their data and choose security controls that provide adequate protection.
  - **Tailor Controls:** Customize the security settings offered by the cloud provider to fit their unique operational and threat environments.
  - **Secure Configuration:** Take responsibility for correctly setting up their cloud environment.
  - **Continuous Monitoring:** Constantly monitor their systems to detect, analyze, and respond to potential threats.

Tokens and Assertions Overview

The document explains tokens and assertions and how they work as the core components of authentication systems such as Single Sign-On (SSO), where a user logs in once to access multiple applications. Key elements include:

- **Terms and Concepts:** Defines the key players in a token-based system:
  - **End User:** The person or system trying to access something.
  - **Client:** The software the end user is using (e.g., a web browser or mobile app).
  - **Authorization Server (or Identity Provider):** The trusted service that verifies a user's identity and issues the digital token.
  - **Protected Resource:** The application, data, or service a user wants to access.

- **Types of Assertions and Tokens:** There are three main types:
  - **Identity Tokens:** Prove an individual's identity and contain basic identity information.
  - **Access Tokens:** Act as a key that grants permission to access a specific resource for a limited time.
  - **Refresh Tokens:** A special token used to get a new access token when the old one expires, so that the user does not need to log in again.

- **Uses of Tokens and Assertions:** The two primary scenarios are:
  - **Single Sign-On (SSO) and Federation:** Allowing a user to log in once and access multiple different services across different organizations.
  - **API Access Scenarios:** Allowing computer applications to securely communicate with each other and access data on behalf of a user.

The recommendations in the draft report are intended to mitigate the primary threats to tokens and assertions, which include:

- **Assertion/Token Forgery:** An attacker creates a fake token, usually after stealing a signing key.
- **Assertion/Token Redirect:** An attacker steals a legitimate token and uses it to access a different resource than it was intended for.
- **Assertion/Token Replay:** An attacker intercepts a token and re-uses it to impersonate the legitimate user.
- **Signing Key Compromise:** An attacker steals the master key, allowing them to forge any token and gain widespread access.

Security Controls - IA-13: Identity Providers and Authorization Servers

A key area of focus is the NIST security control IA-13, *Identity Providers and Authorization Servers,* which is part of the NIST Special Publications Series 800-53 and mandates the use of dedicated systems to manage and issue tokens. Recommended controls for identity providers and authorization servers (i.e., the service that verifies a user's identity and issues the digital token) include:

- **Architecture and Design:** Organizations must make critical design choices, such as use of a stateful architecture (where a central server tracks all logins) or a stateless one (where the token itself contains all the needed information). They must also choose the right protocols (e.g., modern OpenID Connect (OIDC) is often preferred over the older Security Assertion Markup Language (SAML)).
- **Risk Assessment and Management:** The level of security must match the level of risk. Agencies must determine the sensitivity of their data and apply the appropriate security and assurance levels.
- **Security Policy and Documentation:** Organizations must create and maintain clear documentation outlining the rules for everything related to tokens: their lifespan, how they are validated, how the keys that sign them are managed, and what to do in case of an incident.
- **Authorization and Zero Trust:** In a Zero Trust model, a valid token is not enough to grant access. The system should also check other aspects of context, such as device health, the user's location, and that user's normal or usual behavior, before making a decision on whether to grant access.

Security Controls - Enhancements

The report also details specific ways to strengthen the security of token-based systems, including:

- **Protection of Cryptographic Keys:** Master keys are used to digitally sign, and thus create, tokens, and are therefore critically important. If stolen, an attacker can forge any token desired. Guidance is provided for the entire lifecycle of these keys:

- **Generation:** Keys must be created using secure, approved methods.
- **Distribution:** Keys must be shared securely between systems.
- **Storage and Isolation:** Keys must be protected from theft, ideally by storing them in specialized, tamper-resistant hardware like a Hardware Security Module (HSM).
- **Rotation:** Keys should be replaced on a regular schedule (e.g., every 30 days or every year, depending on the risk) defined by the sensitivity of the system and scenario of use.
- **Revocation and Destruction:** Old or compromised keys must be securely destroyed.

— **Verification of Identity Assertions and Access Tokens:** The application receiving a token must verify it properly. This includes checking that the token's digital signature is valid, came from a trusted source, is intended for that specific application (audience), and has not expired.

— **Token Management:** Covers managing the lifecycle of the tokens themselves.

- **Token Validity Length:** Tokens should have short lifespans (e.g., under an hour) to minimize the window of opportunity for an attacker if one is stolen.
- **Token Revocation:** Systems must have a way to cancel, or revoke, a token or session if a compromise is suspected.
- **Audience Restriction:** A token issued for one application should not be accepted by another.
- **Session Monitoring:** All token activity should be logged and analyzed to detect suspicious patterns.

Security Controls - Other Considerations

Other covered topics for building a secure system include:

— **Secure Integration:** Cloud providers should offer secure, pre-configured templates to help customers avoid common setup mistakes.

— **Presentation Methods:** It is much more secure for systems to exchange tokens directly (back-channel) rather than passing them through a user's browser (front-channel).

— **Token Encryption:** The contents of a token should be encrypted if they contain any sensitive information, such as user roles or personal data.

— **FAL3 Assertions:** For very high-risk applications, the system should not just trust the token but should require an additional and independent proof of identity, such as proof of a physical smart card.

— **Device-Bound Session Credentials:** An emerging technology that cryptographically binds a login session to a specific physical device, making it more difficult for an attacker to hijack the session from another machine.

— **Risk Signal Frameworks:** Protocols that allow different online services to share threat information in real-time. For example, if a user's password is changed for one service, a signal can be sent to all connected services to automatically log out active sessions, containing the impact of an account takeover.

Request for Comment

NIST seeks feedback from government and industry stakeholders on the entirety of the initial public draft, and particularly on these topic areas:

— **Signing Key Validity Periods:** Input on the length of validity and structure of scenarios.

— **Token Validity Periods:** Opinions on token validity lengths and related controls.

— **Key Protection and Isolation:** Feedback on the clarity of key management definitions and their mapping to FISMA system levels.

— **Key Scoping:** Operational considerations, implementation challenges, and best practices.

— **Emerging Standards:** Comments on new standards that could support token and assertion protection.

For more information, please contact Rik Parker.

Contact

Laura Byerly
Managing Director
Regulatory Insights
lbyerly@kpmg.com

Brian Hart
Principal
Risk, Regulatory and Compliance
bhart@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: in **kpmg.com**