NIST Guidance Tackles Mobile Authentication

Posted At : September 24, 2013 3:20 PM | Posted By : Kyra Fussell

Related Categories: Mobility, Digital Government, Communications Services, Information Security, Telework, Cybersecurity, Department of Commerce, Wireless

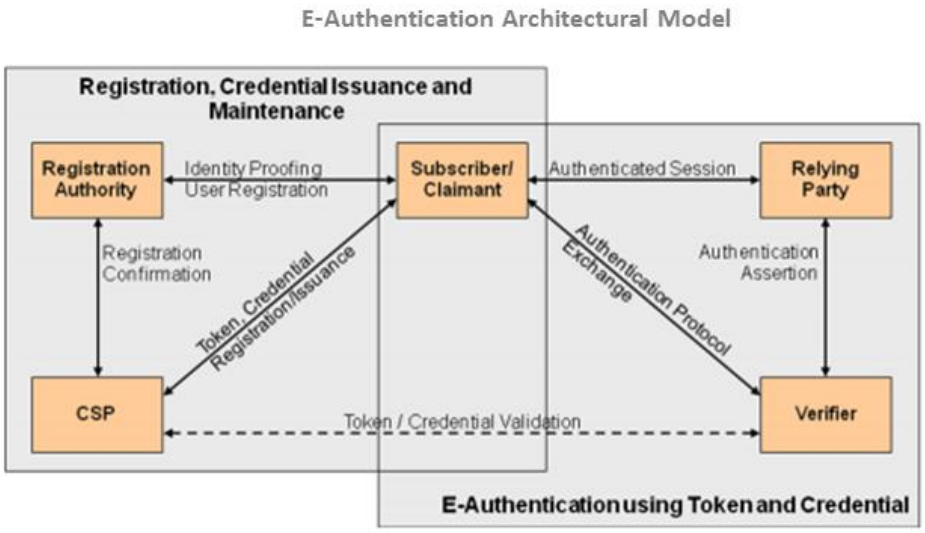
The Commerce Department's National Institute of Standards and Technology (NIST) recently updated its guidance to government agencies for electronic authentication (e-authentication) for federal IT systems and services providers.

NIST's ***Electronic Authentication Guidance*** **(Special Publication 800-63-2)** covers remote authentication of users (e.g. employees, contractors, and private individuals) leveraging open networks to interact with government information systems. As a supplement to the Office of Management and Budget's (OMB) guidance, ***E-Authentication Guidance for Federal Agencies***, the NIST work builds on levels of assurance that are defined by the consequences of authentication errors and credential misuse. The OMB guidance from 2003 provides federal agencies with criteria for determining the level of assurance needed for applications and transactions. These four levels of assurance address identity proofing, registration, tokens, management processes, authentication protocols and related issues.

The guidance from OMB also provides a five step process for agencies to fulfill their e-authentication requirements. The guidelines from NIST target third step in this process, which involves selecting "technology based on e-authentication technical guidance." Outlining specific technical requirements for each of the assurance levels, the NIST document addresses:

- Registration and identity proofing;
- Token (e.g. cryptographic key, password) for authentication;
- Token and credential management mechanisms;
- Protocols to support authentication mechanisms;
- Assertion mechanisms used in communicating remote authentication.

The lowest level achieved in any of the technical areas listed above determines the overall authentication assurance level. Agencies may use additional risk management measures to adjust the level of assurance. In particular, privacy requirements and legal concerns may contribute to a context in which an agency may deem additional authentication measures appropriate.



Source: NIST SP 800-63-1

Previously, NIST released updated guidance that reflected authentication token technologies and restructure the e-authentication architectural model for increased clarity. Among other changes, that revision also added technical requirements for credential service providers, protocols used in transporting authentication data, and assertions related to implementation within the e-authentication model.

The most recent edition provides a more limited update with most of the changes focused on processes for registration and issuance of professional credentials. Two general categories of threats for the registration process are impersonation and compromise of the infrastructure. Since infrastructure threats are addressed by normal security controls, the NIST guidance emphasizes mitigating the threat of impersonation. Two approaches are presented for deterring impersonation: either make it more difficult to accomplish or increase the likelihood of detection. The technical guidance provides several strategies for making impersonation more difficult and describes general requirements for each of the four assurance levels.

Despite budget limitations, agencies continue to look for ways to make information more accessible and empower an increasingly mobile workforce. System risk assessments and technical requirements associated with specific assurance levels will shape the solutions they implement mobile strategies. While assurance requirements will vary across the government, this technical guidance provides a structure for describing agency security requirements and provides vendors with a framework for articulating how solutions will fulfill those needs.

Originally published for Federal Industry Analysis: Analysts Perspectives Blog. Stay ahead of the competition by discovering more about ***GovWinIQ@FIAGovWin.****. Follow me on twitter*