NIST special publication expands government authentication options

December 21 2011

A newly revised publication from the National Institute of Standards and Technology (NIST) expands the options for government agencies that need to verify the identity of users of their Web-based services. Electronic Authentication Guideline (NIST Special Publication 800-63-1) is an extensive revision and update of the original document, released in 2006, and it recognizes that times, and technologies, have changed.

"Changes made to the document reflect changes in the state of the art," explains NIST computer security expert Tim Polk, Cryptographic Technology Group manager at NIST. "There are new techniques and tools available to government agencies, and this provides them more flexibility in choosing the best authentication methods for their individual needs, without sacrificing security."

When SP 800-63 was first released, its authors assumed that most agencies would handle the business of figuring out if users were who they claimed to be in-house. But since that time, an industry has grown around providing authentication services, and it is often in the best interest of agencies to take advantage of commercial systems or those of other government entities. And while passwords are still the leading mechanism for authenticating user identity, a growing number of systems rely on cryptographic keys or physical tokens.

The revision broadens the discussion of technologies available to agencies and gives a more detailed discussion of these technologies. The guideline applies whether agencies choose to handle authentication directly or leverage services provided by other parties, including commercial companies.

Government agencies have the option of using the services of companies that have had their authentication systems certified through the Federal Chief Information Officer Council's Trust Framework Provider Adoption Process (TFPAP). This program assesses credentialing processes against federal requirements, including those established in 800-63. To ensure consistency and avoid redundant analysis, NIST strongly encourages agencies to leverage the TFPAP process.

SP 800-63-1 is the official implementation guidance for the Office of Management and Budget (OMB) Memorandum 04-04, "E-Authentication Guidance for Federal Agencies.*" Polk stresses that the revised NIST guideline may inform but is not intended to restrict or constrain the development or use of standards for implementation of the National Strategy for Trusted Identities in Cyberspace (NSTIC). NIST SP 800-63-1 is specifically designated as a guideline for use by federal agencies for electronic authentication. NSTIC, in contrast, has a broader charge: the creation of an Identity Ecosystem, "an online environment where individuals and organizations will be able to trust each other because they follow agreed upon standards to obtain and authenticate their digital identities."

More information: NIST SP 800-63-1, Electronic Authentication Guideline, is available at www.nist.gov/manuscript-public … ch.cfm?pub_id=910006 . For more NIST computer security publications, see csrc.nist.gov/publications/PubsSPs.html

* The Office of Management and Budget's guidance, "E-Authentication Guidance for Federal Agencies" [OMB 04-04] can be found at www.whitehouse.gov/sites/defau … anda/fy04/m04-04.pdf

Provided by National Institute of Standards and Technology (NIST)

Citation: NIST special publication expands government authentication options (2011, December 21) retrieved 9 April 2024 from https://phys.org/news/2011-12-nist-special-authentication-options.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.