Title:

Performance metrics for knowledge based authentication (KBA) for remote identity proofing.

Proposers:

NSTIC pilots:

CSDII, Criterion, Daon, Resilient, UCAID

Exponent, GTRI, ID.me, PRIVO, TSCP

Commonwealth of Pennsylvania, State of Michigan

The NSTIC pilots were funded by the NIST NSTIC National Program Office (NPO). The NPO and its contractors supported the pilot collaboration meetings in which this work was developed.

Submitted to:

IDESG Standards Coordination Committee

Submission date:

March 26, 2014

Description:

Currently, there is a lack of standard performance metrics regarding the use of knowledge based authentication (KBA) for remote identity proofing. As a result, organizations that rely on these techniques for delivery of services to citizens and customers are forced to make critical authorization decisions with a limited understanding of the risks and benefits of the underlying technologies.

Identity and access management are essential aspects of information security to preserve the availability, confidentiality, and integrity of data, services, and resources. Like all other aspects of information security, selecting effective access control technologies, procedures, and policies requires mature risk management techniques; at the heart of which is an informed awareness of the inherent risks and benefits involved with a particular solution type. Currently, a lack of awareness regarding KBA and remote proofing requires that service providers, government agencies, and other organizations, assume risks that are not clear or well defined.

Note that while this proposal relates solely to KBA use with respect to remote identity proofing, it is believed that base performance metrics derived for that purpose would likely also be beneficial for the purposes of identity authentication or access/authorization decisions.

Business case:

The economic and organizational impacts of errors regarding access controls, whether involving KBA, remote proofing or other aspects of authentication and authorization, are all too clear in today's market.

The results of data breaches—lawsuits, credit monitoring, and loss of sensitive data—can financially affect organizations, damage reputations, and or impact consumer confidence.

Conversely, well established standards around KBA and remote identity proofing will promote expanded and more effective risk-based processes and procedures, thereby increasing market confidence and driving adoption of these solutions. This increased adoption would then allow for a wider range of services to be moved on-line as in-person proofing processes are replaced by remote solutions. In addition, a clear statement of best practices will allow KBA vendors to articulate their solution differentiation.

Existing practice and the need for a standard:

In order to establish a more effective market that is responsive to the complicated requirements that service providers face today, standardized performance metrics and reporting procedures need to be developed. Once created, these standards would allow organizations, government agencies, and other service providers to effectively implement risk-based access solutions to meet cybersecurity needs, protect users, and ensure availability of services.

In order to help establish a common understanding of KBA and remote identity proofing services, it is proposed that standardized approaches are developed to:

1) determine the accuracy and efficacy of KBA and remote proofing techniques. This may include requirements for the currency and validity of the information used in the proofing or the development of the KBA questions; and
2) report failure rates of KBA systems. In addition to standardizing validity criteria for data and processes used in the proofing process or KBA question development, this standard will establish reporting requirements for false acceptance, false rejections, and failure to enroll.

~~(Future KBA-related standards may consider aspects such the validity, currency, and adequacy of the information used, as well as considerations such as service availability and the ability for redress, etc.)~~

Impact on existing or potential markets:

This standard would have a positive impact on the existing identity and access management market by providing a common understanding of KBA and remote proofing standards, improving confidence in solutions, and improving risk-based decision making. Additionally, this standard would improve access to services across multiple markets (health care, financial services, online services that fall under the FTC Children's Online Privacy Protection Act, etc.) that require identity proofing to provide services that require high assurance identity solutions.

Existing standards and related work

No existing standards relating to performance metrics for Knowledge Based Authentication for remote proofing of identity have been identified.

The closest related work discovered is a report by the IDPV Identity Resolution Project on "Establishment of Core Identity Attributes Sets and Supplemental Identity Attributes" (Document No. NASPO-IDPV-060) which analyzed a large database of identity attributes to determine sets of attributes that could be used to resolve individuals from that database. Thus, the NASPO paper's principle purpose was to determine attribute sets for identity resolution, rather than to consider attribute verification for identity proofing. However, to the extent that certain attributes that may be used for KBA were not available within an attribute set (creating what was classified as a "null identity" in the paper), the paper may inform a standard that is developed based on this proposal by identifying one reason for failure in a KBA system. We suggest that the developers of a standard in furtherance of this proposal monitor the ongoing activities of NASPO in regards to ~~Identity Resolution~~the development of NASPO-**IDPV-066** – "Requirements and Implementation Guidelines for Assertion**, Resolution, Evidence, and Verification of Personal Identity**."

.