From

NSTIC Pilot Collaboration Group

To

IDESG Standards Coordination Committee

Date

March 17th 2015

Background

On March 27, 2014 the NSTIC pilot collaboration group forwarded a proposal regarding *Performance metrics for knowledge based authentication (KBA) for remote proofing* to the IDESG Standards Coordination Committee (SCC).

We understand that the SCC conducted a call for standards organizations to solicit their interest in developing a standard based on the proposal, but they have not yet identified an organization that meets the IDESG SCC selection criteria.

As a consequence, last month the SCC asked the pilot collaboration group to provide supporting material for the proposal that could be forwarded to appropriate organizations.

This response to the SCC request comprises the observations from several of the NSTIC pilots. The pilot collaboration group would be pleased if the IDESG SCC would forward this response directly to the standards organizations that the SCC deems appropriate.

In this document, we use the term *integrator* as the organization that is relying on the KBA technology, the term *user* to denote the individual who is using the integrator's application, and the term *vendor* to denote the provider of the KBA technology.

Pilot response

Overview

In general, the comments from the pilots fall into two categories:

> Integrators need to know that they are optimizing the efficacy and population coverage of the KBA technology, based on the population of interest, and;
>
> Integrators need to know what residual risk they are assuming, based on the KBA system performance. This will allow the integrators to implement alternate means as fallbacks or as compensating controls.

Thus, the pilots suggested that guidance on configuring the KBA technology would be useful, as would standardized performance metrics which would help them understand their residual risk.

Suggested Guidance

- KBA technologies for remote identity proofing tend to be highly configurable. It is therefore desirable for the KBA vendors to provide standardized guidance for the configuration of the technology to the integrators. This could be accomplished by the integrator selecting from a standardized series of configuration parameters that relate to characteristics of the population of interest, such as expected range of credit history, expected address stability, etc. This would enable the integrator to reliably establish the optimal vendor technology configuration. The vendor could also provide guidance on other aspects, such as: under what conditions should a secondary set of questions be invoked; how soon after a failure a user should be entitled to re-attempt the KBA process; what is the expected reliability of KBA data for these population characteristics; are there specific settings in support of a particular Level of Assurance?

KBA technologies tend to operate on a two-step process.

> KBA step 1. The user provides a minimal set of user information which is used by the KBA vendor to determine the uniqueness of the presented data set and whether it matches a person known to the vendor, as well as the availability of associated historical data to generate the KBA questions.
>
> - It would be helpful to know the expected performance of a KBA system as a function of the provided user data set. This would allow the integrator to invoke KBA at the correct stage in their process, and using the minimal level of requested information. Too early there may not be enough data to meaningfully resolve individuals; too late and more than the necessary amount of data may have been requested of the user. In addition, guidance about the expected availability and reliability of KBA data as a function of the provided user data set would be useful.

KBA step 2. The KBA questions are posed to the user and, based on their responses, the KBA vendor provides a response to the integrator, to indicate whether the user is the valid holder of the data set of user information presented in step 1.

- Based on the system configuration, what is the expected ratio of real to diversionary questions that will be presented in step 2? How does this ratio of real to diversionary questions relate to system performance?
- It would be helpful to have a standardized way of displaying questions across vendors and devices, to enhance usability.
- What types of questions are asked when there is minimal financial or address history?

Desired reportable performance metrics:

Based on the population set selected by the integrator:

- What is the percentage of that population set for which sufficient identity resolution data is unavailable and who would therefore fail KBA step 1 above?
- For the population for which there is sufficient identity resolution and KBA data, what is the expected false rejection rate (i.e. legitimate users who fail the KBA step 2)?
- For the population for which there is sufficient identity and KBA data, what is the expected false acceptance rate (i.e. users who are misclassified as other legitimate users in KBA step 2)? This metric would indicate the degree of confidence or assurance to the integrator to allow them to manage their risk appropriately.

These performance metrics should be reported, along with a statement of the database and other testing characteristics used to generate the expected values for the population set.

Additional recommendation

- It is our understanding that the NASPO IDPV committee that was identified in the proposal is a possible target organization for this additional material. We suggest that an additional body for consideration would be the Accredited Standards Committee X9 (ASC X9). As you likely know, ASC X9 has a history of developing identity related standards for financial transactions, such as ANSI X9.84 *Biometric Information Management and Security for Financial Services Industry* and ANSI X9.117 *Secure Remote Access Mutual Authentication*. Due to the financial sector's historical use of KBA, X9 committee members may be sufficiently motivated and knowledgeable to develop the standard proposed by the NSTIC pilots.