Standards Coordination Committee
www.idecosystem.org

Identity Ecosystem Steering Group

To: Standards Developers

Subject: Solicitation for a new standards project

The Standards Coordination Committee (SCC) of the Identity Ecosystem Steering Group (IDESG) is soliciting Standards Developers to accept and execute on a new project proposal on "Performance metrics for Knowledge-Based Authentication (KBA) for remote identity proofing". KBA for remote identity proofing refers to the dynamic generation of a series of questions from existing sources of person information, such as credit, mortgage, financial, or utilities data, for the purpose of determining if the identity the person is claiming to be who they actually are. KBA, for the purposes of this proposal, does not refer to static KBA used by online services to recover passwords, such as 'What is your mother's maiden name?' We are seeking Standards Developers to establish a standard based on the attached proposal.

As an introduction to the IDESG (www.idecosystem.org), we are a 501(c)3 non-profit organization created to cultivate and promote an environment that gives individuals and organizations greater choice, convenience, and confidence in online transactions. We are working to develop an identity ecosystem framework supporting the vision of an online environment where individuals and organizations will be able to trust each other because they follow agreed upon standards. The IDESG does not intend to become a standards development body, but rather an organization that promotes the development of standards by existing Standards Developers and develops policies that serve to accelerate the development and adoption of the Identity Ecosystem.

The IDESG follows the guiding principles of the National Strategy for Trusted Identities in Cyberspace (NSTIC, http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf), namely that identity solutions will be:

- Privacy enhancing and voluntary
- Secure and resilient
- Interoperable, and
- Cost effective and easy to use

Our intent is to identify interested Standards Developers that we will work with in a liaison capacity to develop the proposed standard. The process we intend to follow is to solicit expressions of interest in the project, obtaining information that will allow us to make an informed decision regarding who to work with based on a set of criteria delineated in our draft Standards Adoption Policy*, namely:

- Qualifications related to the subject matter
- Adequate personnel to progress the work
- Adherence to principles and processes, to include:
    - Participatory openness
    - Fairness and due process
    - Transparency
    - Function-oriented description

    - Affordability
- Public review procedures
- Stable hosting arrangements
- Intellectual property rules

Further, we would expect any resulting standard to be consistent with the NSTIC guiding principles.

*A copy of the draft SAP can be found at https://www.idecosystem.org/filedepot/folder/10?fid=1296. See section 4 for criteria.

In response to this solicitation, interested Standards Developers are asked to provide a written expression of interest and statement of qualifications by **22 September 2014**. Please state why you believe your organization to be the best choice for this project and briefly state how you meet the criteria listed above. We may ask selected submitters to discuss their response with the SCC or a subgroup thereof.

Responses should be submitted via email to the SCC chair at cathy.tilton@daon.com. Likewise, any questions regarding this solicitation should be so addressed.

Please note that this is the first standards proposal issued by the IDESG; however, it is our expectation that as other gaps are identified within the corpus of identity-related standards, other such proposals will be developed. Also note that the IDESG will also be considering existing standards for adoption as-is into the Identity Ecosystem Framework as it evolves.

The scope of this project proposal has purposely been kept focused on a particular aspect of KBA. We realize that a) there are some applications for which KBA is not appropriate and b) there are other areas of KBA for which additional standardization is needed and we do not preclude any Standards Developer from extending that scope. We ask that the Standards Developer(s), in the process of developing the KBA Performance Standard, consider the potential impacts of the following:

- Privacy enhancing techniques including use of attributes,
- Availability, adequacy, currency and validity of data,
- Universal accessibility of questions and answers,
- Incentives to induce disclosure,
- Ability for end users to understand the consequences of answers and of disclosing personal information,
- Vulnerability to data breach or social engineering processes, and
- Reporting of service availability, failure rates, correction of and updating of misinformation, and ability for redress.

We appreciate your consideration of our solicitation. We are hopeful that over time we will establish relationships with a number of standards developers who will help us meet our goal of seeing the emergence of a vibrant Identity Ecosystem.

Regards,

Catherine J. Tilton
Chair, IDESG SCC

New Work Item Proposal

Title:

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

Proposer:

IDESG Standards Coordination Committee (SCC)

Submission date:

7 August 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.

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.

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.