This work represents a collaborative effort between the OASIS Trust Elevation TC and ITU-T SG 17 Identity Management Question (Q10/17) to provide comments on NIST SP 800-63-2, Electronic Authentication Guideline, pursuant to its 9 April 2015 solicitation. (See <http://csrc.nist.gov/groups/ST/eauthentication/sp800-63-2_call-comments.html>)

**I. General Comments**

* As the solicitation notes, “NIST is considering a significant update to SP 800-63-2 in response to market innovation, evolving federal requirements, and an advanced threat landscape targeting remote authentication.” Plainly that evolving threat landscape exists globally - with significant effects on the United States domestically; thus, any update of this Special Publication should include extensive treatment of the international information security ecosystem within which the provisions are derived and implemented. At present, SP800-63-2 is completely devoid of anything other than U.S. domestic implementations, despite the agency’s extensive international mandates in its Organic Act, the provision of international standards status to its publications, and the global nature of the authentication challenges being faced.[[1]](#footnote-1)
* Levels of Assurance (LoAs) today represents a range of trust depending on the order and the context of the evaluation of related assurance tokens. For example, if an authentication attempt comes from an unexpected location, a system may require the use of several sets of tokens even from the same LoA in order to ensure that the required assurance level is achieved. OASIS Trust elevation TC has taken a close look on how to enahcne trust for these uses cases and we do recommend that NIST try to harmonize with the work.
* Identity Register
* Add to the model the concept of the Identity Register, which is the repository that maintains the binding between tokens and identifiers. This entity has certain privacy and security obligations that come with this role, including the protection of registration data for future dispute resolution balanced with the user risk-mitigation goal of minimizing instances of PII. The Identity Register may provide support for federated authentication and identification and credential reliability and recovery services.
* We recommend that NIST consider the identity and access management architecture to be addressed at a much higher level of abstraction and to separate identity management from access management.

**II. What requirements, processes, standards, or technologies are currently excluded from 800-63-2 that should be considered for future inclusion?**

* NIST should implemt extensively used industry techniques such as the Extended Validation Certificates (EVcerts) pursuant to the CA/B Forum specification or the adaptation and the additional token extension found in ETSI TS 102 042 pursuant to European Union policies as means to combat threats to identity attributes and minize man in the middle attacks. The Forum’s recent inclusion of extensive government entity trust certification provisions in the specification, facilitates the use of EVcerts for a broad array of new government services
* NIST has done a great job in harmonizing its work with other stanadrds and in this siprit we do recommend continued harmonizations with ITU-T X.1254 (also ISO 29115) work that has done extensive extensions to the 800-63 framework . In particular, the ITU-T X.1254 (also ISO 29115) work relating to non-human entities .

**III. Should a representation of the confidence level in attributes be standardized in order to assist in making authorization decisions? What form should that representation take?**

* OASIS Trust Elevation TC has developed three committee draftes that can be used for developing a consistant method for determining, evaluationg and improving on LoA levels in a technology independdent fashion. It is also developing metada data and protocol for expressing and excahning needed trust elevation methods between a verifier and a client.
* Many systems are designed to support flexible authentication based on risk-based access. In many cases, these systems select many tokens from a given LoA to enhance the trust within the authentication step. NIST needs to be more flexible and adapt the work from OASIS Trust Elevation TC in order to piggy-back on the use of common LoA metadata and trust elevation protocols that could work with Oauth, OpenID Connect and SAML.
* At the point of transaction, the environment needs to be evaluated, not just the credential. The threat environment affects the trustworthiness of the transmitted credential.
* NIST needs to start accommodating the latest trends in using a mobile device as part of the authentication process.
	+ As an example, the OASIS Identity-Based Attestation and Open Exchange Protocol Specification (IBOPS) models of enabling the user to authenticate to a device, and then an agent to attest to this fact, changes the dynamics of determining the LoA and the verifier (or CSP).
* Consideration should be given to hacker resistant authentication methods, e.g., where hacking the identity provider server will not result in massive security breaches.
	+ For example, in IBOPS, the server holds a pointer to the client secrets and does not store any credentials locally; client secrets are stored on the clinet device which changes the attack vector whereby hackers will need to hack the server and the associated device to obtain a credential.

**IV. What methods can be used to increase the trust or assurance level (sometimes referred to as “trust elevation”) of an authenticated identity during a transaction? If possible, please share any performance metrics to corroborate the efficacy of the proposed methods.**

* NIST SP 800-63 framework looks at the traditional three categories of authentication factors: something you have, something you are, and something you know. These categories are limiting because they assume strict and static authentication tokens with limited authentication capabilities. In many cases the context around the use of an authentication factor, such as access from a known location or time of day, can change the order of challenges or responses required by an adaptive authentication engine. NIST should enlarge the scope of authentication categories to include context and behavior to enable a wider set of acceptable tokens and devices housing these tokens. For example, a smart phone can house a soft token that is protecting a soft PKI certificate in a Key Chain. The trust level in the token can change based on the device status/health such as rooting or the use of anti-virus software. As such, the achievable LoA from the device can vary with time and could be a function of software on the device and also a function of OS system integrity.
* The use of biometrics in the document needs to be expanded. Currently the scope is very limited to enrollment and second or third factors on hard tokens. However, the trend in the industry is to use biometrics more broadly. For example, biometrics can bind the access request to a user as part of a larger process performed by the verifier through the use of cumulative identity attributes that binds a device, location and behavior to an authorization request.
* The advent of smart devices and the Internet of Things requires the extension of the work to include non-human entities. The assumption that the interaction is a web-based interaction between the user and the verifier is not totally true in the current environments. Given that mobile single sign-on technologies are still primitive, it is important to not rely on cookies or unprotected tokens for Single Sign-On support.

**V. Threats to Authentication**

1. Increasing authentication assurance requires the combination of authentication factors with no (or minimal) overlapping vulnerabilities to enhance assurance. It is not the number of factors that matters, but the reduction in threats that the combination of factors achieves. The way the combination occurs can either reduce or increase threats of context and related vulnerabilities. The OASIS Trust Elevation TC produced two committee drafts based on ITU-T X.1254 (ISO 29115) that include a comprehensive list of authentication methods and a way of computing the authentication strength based on vulnerabilities and their associated mitigation/control. It is recommended that NIST build on this work to ensure that authentication strength is understood by implementers.
2. It is recommended that Trust Elevation techniques be added to the next version of the document. Trust elevation can occur in multiple places. Consider for example a scenario where a Credential Service Provider (CSP) authenticates a user coming from a smart device. The CSP can have the option of using multiple capabilities in the device such as biometric, location, and soft PKI tokens or certificates to authenticate the user. The authentication strength can be consistent with the risk engine requirements. If the CSP is acting as an IDP or attribute provider to other Verifiers or relying parties, these parties can elevate the authentication strength per their own requirements and may be able to ask the CSP to do it on their behalf or combine the CSP tokens into application specific attributes, such as behavior, that they also can do on their own.
	1. A standardized means of requesting a higher assurance level, such as the ones being developed by the OASIS Trust Elevation TC, should be used.
	2. An overlay/tailoring capability similar to SP 800-53 could also be used. Each 800-63 LOA would become a baseline that could be tailored as necessary, consistent with tailoring guidance, to help each community of interest better meet its mission / business needs. In the overlays, authentication strength can be computed using concepts form OASIS Trust Elevation TC.

**VI. Elevation of Biometric to a token**

NIST does not recognize the use of Biometrics as authentication tokens. They are mainly used at enrolment. However, if the right privacy enhancing methods are used, combined with appropriate trust elevation methods (e.g., as in OASIS IBOPS), biometrics can be evolved to provide effective user authentication at least at LoA 2. It is therefore recommended that NIST investigate the use of biometric as a full token.

**References**

1. OASIS Electronic Identity Credential Trust Elevation Methods (Trust Elevation) TC; <https://www.oasis-open.org/apps/org/workgroup/trust-el/>
2. OASIS Identity Based Attestation and Open Exchange Protocol Specification (IBOPS) TC; <https://www.oasis-open.org/apps/org/workgroup/ibops/>
3. X.1254 : Entity authentication assurance framework; <http://www.itu.int/rec/T-REC-X.1254/en>
4. Question 10/17 – Identity management architecture and mechanisms; <http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/q10.aspx>
1. *See* National Institute of Standards and Technology Act, [available at <http://www.nist.gov/director/ocla/upload/NIST-Organic-Act.pdf>. *See also*, Organizations recognized according to Recommendations ITU-T A.4, A.5 and A.6, <http://www.itu.int/en/ITU-T/extcoop/Pages/sdo.aspx>. [↑](#footnote-ref-1)