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 (LoA) today represents a range of trust depending on the order and the context of the evaluation of related assutance 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 assuranc elevel is achived. In many cases and in particular for knowledge based tokens. The attributes of these tokens losses value as a function of time. The advent of social media makes Knowlede Based Authentication (KBA) information public and waterdown its effective use in the identification process.
* Decouple Identity Binding
* Permit identity proofing to occur after token issuance.
* 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 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.
* Risk Confidence Factors
* Instead of grouping assurance profiles solely as 1,2,3,4 per OMB M-04-04 requirements, permit the expression of risk confidence score with multiple factors including identity proofing, token strength, multiple factors, biometric verification, etc.

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

* NIST should treat extensively used industry techniques such as the Extended Validation Certificates (EVcerts) pursuant to the CA/B Forum specification or the adaptation and extension found in ETSI TS 102 042 as means to combat threats to identity attributes and minize man in the middle attacks.

…..

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)