OASIS RESPONSE TO NIST REQUEST FOR COMMENTS ON ITS ELECTRONIC AUTHENTICATION GUIDELINES (SP 800-63-2, August 2013)

OASIS (the Organization for the Advancement of Structured Information Standards) is pleased to provide this response from one of its technical committees to the request from the US National Institution of Standards and Technology (NIST) for feedback on NIST's announced plans to revise its SP 800-63-2.

PREFACE

Please note that this comment represents only viewpoints from the volunteer expert members of one of our relevant technical committees, the OASIS Trust Elevation TC [1]. OASIS is one of the largest and oldest global open data standards consortia, with approximately 5000 active participants representing about 500 member organizations and individual members in over 80 countries. [2] Our consortium hosts approximately 70 active technical committees, including a large number of open identity management standards projects [3] such as SAML, XACML, WS-Trust, WS-Federation and the Trust Elevation committee, and closely cooperates with interagency and international standards cooperation efforts. [4] However, OASIS as a consortium does not take official positions on public policy matters. Our diverse group of industry, academic and governmental members, who contribute voluntarily to our projects, do not necessarily share the same views on all technical or policy matters, and OASIS emphatically does not speak for them all.

[1] OASIS Trust Elevation committee: https://www.oasis-open.org/committees/trust-el
[2] OASIS generally: https://www.oasis-open.org/
[3] OASIS identity management projects: http://j.mp/OASISidentity
[4] OASIS e-government standards liaisons: https://www.oasis-open.org/liaisons

The following statement represents a collaborative effort between the OASIS Trust Elevation TC, and the Question 10 (subcommittee) of Study Group 17 of the International Telecommunication Union, Telecommunication Standardization Sector (ITU-T), to provide comments on NIST SP 800-63-2, Electronic Authentication Guideline, pursuant to NIST's 9 April 2015 solicitation. [5]
A related statement from ITU-T SG 17's Q10/17 is appended to this submission.

[5] NIST request for comments:
http://csrc.nist.gov/groups/ST/eauthentication/sp800-63-2_call-comments.html

GENERAL COMMENTS

INTERNATIONAL SCOPE 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 the Special Publication should include treatment of the international information security ecosystem within which the provisions are derived and implemented. At present, SP 800-63-2

only addresses US 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. [6]

[6] See National Institute of Standards and Technology Act (http://www.nist.gov/director/ocla/upload/NIST-Organic-Act.pdf), and 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).

ASSURANCE LEVELS AND ELEVATION The concept of Levels of Assurance (LoAs) today represents a range of trust, depending largely 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.

The OASIS Trust Elevation TC is developing specific, open-standards-bazed methodologies for additive actions to improve trust levels and mitigate risks incrementally. We recommend that NIST's assurance model explicitly recognize elevation methodologies in its scheme; and NIST may wish to participate in more detailed specification of standards-based elevation methods in open forums, including the OASIS committee.

IDENTITY REGISTERS We recommend that NIST explicitly add, to its assurance model, a concept and role of "Identity Register", as a repository that explicitly maintains the bindings between tokens and identifiers. Parties acting in that role should have specific, and perhaps-heightened, privacy and security obligations, including the protection of significant stores of registration data retained for future dispute resolution, balanced with the risk-mitigation goal of minimizing instances of personally-identifiable information. The Identity Register role may also be defined to include support for federated authentication and identification, and support for credential reliability and recovery services.

MORE THAN ACCESS CONTROL We recommend that NIST describe and address identity and access management architectures functionally and at a higher level of abstraction, and explicitly separate identity management functions from access management functions.

CYBER RISK AND THREAT INFORMATION SHARING We note that SP 800-63-2 significantly addresses US federal systems for which the US Department of Homeland Security (DHS) also shares some responsiblities. DHS recently transferred several key data specifications for cyber threat intelligence sharing to a new OASIS technical committee for Cyber Threat Intelligence (CTI). [7] The Trust Elevation TC intends to collaborate closely with the CTI TC on implementations to reduce electronic authentication threats. NIST's evolution of the SP 800-63-2 model likely would benefit significantly from explicitly incorporating the availability of data and queries from cyber risk info sharing exchanges (such as those described in CTI specifications) into assurance level selections and trust elevation/risk mitigation transactions.

[7] OASIS CTI TC, STIX, TAXII: https://www.oasis-open.org/committees/cti

ADDITIONAL ELEMENTS FOR 800-63-2

NIST asks what requirements, processes, standards, or technologies, currently excluded from 800-63-2, should be considered for future inclusion.

We appreciate that NIST often harmonizes with and incorporates other relevant open standards very successfully. We recommend continued harmonization with ITU-T Recommendation X.1254 (also published as ISO/IEC 29115), [8] which includes extensions to the 800-63 framework, and in particular, with its treatment of non-human entities.

[8] ITU-T Rec. X.1254: Entity authentication assurance framework (2013): http://www.itu.int/rec/T-REC-X.1254/en

EXTENDED VALIDATION CERTIFICATES NIST's model should recognize recently-evolved, extensively-used industry techniques such as the Extended Validation Certificates (EVcerts) defined by CA/B Forum specifications [9] -- and the adaptation and additional token extensions found in ETSI TS 102 042 [10] -- as appropriate, risk-relevant means to combat threats to identity attributes and to minimize man-in-the-middle attacks. The CA/B Forum's recent inclusion of extensive trust certification provisions in their specification should facilitate the use of EVcerts for a broad array of government services.

[9] The Certification Authorities (CA)/Browser Forum, and its EVcerts specifications: https://cabforum.org/information-for-manufacturers-and-developers/

[10] ETSI Electronic Signatures and Infrastructures: Policy requirements for certification authorities issuing public key certificates (2013). See starting at page 8, and the references to EVCP (Extended Validation Certificates Policy) and EVCP+ (incorporating a secure user device): http://www.etsi.org/deliver/etsi_ts/102000_102099/102042/02.04.01_60/ts_102042v020401p.pdf

BIOMETRIC TOKENS NIST's SP has declined to recognize robust use of biometrics data for authentication, even as the computing environment becomes mobile-first and device-centric. Although biometrics data mainly are used only at enrollment today, these methods can -- with the right privacy-enhancing methods and trust elevation -- can be evolved to provide effective user authentication properly recognized at higher levels of assurance, reaching (at a minimum) what is currently defined as LoA 2. (See, for example, the OASIS iBOPS project [11].) We recommend that NIST reconsider this omission, and fully recognize biometric tokens in its trust model.

[11] OASIS Identity Based Attestation and Open Exchange Protocol Specification (IBOPS) TC and the working drafts posted there: https://www.oasis-open.org/committees/ibops The draft IBOPS model enables a user to authenticate to a device, and then enables an agent to attest to this fact, adding to reliability based on the verifier.

CONFIDENCE LEVELS

LEVEL CALCULATION *NIST's solicitation asks whether representations of the confidence level in attributes should be standardized, in order to assist in making authorization decisions, and what form it should take.*

At the point of transaction, it is no longer enough to evaluate the credential: the environment in which it is recieved also must be evaluated. The threat environment affects the trustworthiness of a transmitted credential. SP 800-63's coarse-grained "levels" may not be sufficiently detailed, or responsive, to support the determination of incremental changes in context-driven trustworthiness.

Many systems and devices in use today are designed to support flexible authentication, based on risk-based access and the foregoing considerations. Some of these systems select from among many tokens, from a defined assurance level, to enhance trust within a specific authentication step. NIST's model should accommodate and represent those flexible practices, and defined trust elevation methodologies, so as to leverage the existence of identity and LoA metadata and token consumption, as can be facilitated by existing data protocols such as SAML, OAuth, OpenID Connect, etc.

The OASIS Trust Elevation TC is developing a detailed methodology, currently published in draft, for determining, indicating, evaluating and improving on assurance levels, in a technology-independent fashion, as described below. The committee also is developing metadata structures to express, and protocols for exchanging, trust-level data and requests between verifiers and clients.

NIST also should consider assigning greater trustworthiness values to hacker-resistant authentication architectures, in cases where hacking is a significant environmental risk. For example, in IBOPS' methodology, the identity provider's server holds only a pointer to the client secrets and does not store any credentials locally; client secrets are stored on the client, which reduces the risk that hacking the identity provider will result in large-scale security breaches.

TRUST ELEVATION AND MULTIFACTOR CALCULATIONS *NIST's solicitation asks what methods can be used to increase the trust or assurance level of an authenticated identity during a transaction.*

The historical SP 800-63 framework looks at three traditional categories of authentication factors: something you have, something you are, and something you know. But these categories are limiting: they assume strict, 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 in its model, to represent the use of context and behavior, and the policy or circumstances that govern when they will be factored into an authentication decision, so to enable a wider set of acceptable tokens and devices

housing these tokens. For example, a smartphone can house a soft token that protects a soft PKI certificate in a Key Chain. The trust level in that token may be able to change, based on the device status or health (such as rooting), the presence and operation of anti-virus software, and perhaps the state messages generated by the latter. With those kinds of determinations, the assurance level achievable from the device can (and should be able to) vary with time, or as a function of various other data, including software on the device and indicia of system integrity.

TAKING THREATS TO AUTHENTICATION INTO ACCOUNT

As noted above, SP 800-63 gives inadequate treatment to biometrics. Currently it recognizes biometrics only in the context of enrollment and as second or third factors on hard tokens. In actual industry practice, however, biometrics indicators are used more broadly as part of a multi-factor scheme: 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 bind a device, location and behavior to an authorization request. Increasingly, the devices involved in the transaction matter; the model's implicit assumption that interactions are web-based between the user and the verifier is long obsolete. Applying those older-fashioned, browser-era methods, such as relying on cookies or unprotected tokens for single sign-on (SSO) support, to current environments may be more likely to result in insecure outcomes, given that many mobile SSO technologies are still at a relatively primitive stage.

COMBINED FACTORS AND COMPLEMENTARY VULNERABILITIES Increases to authentication assurance require the combination of authentication factors *as well as* minimalization of overlapping vulnerabilities. Enhancing assurance is not achieved solely by the number of factors; it also depends on the reduction in threats that a particular combination of factors can achieve. A method of combining factors may either reduce or increase threats from context and related vulnerabilities. The OASIS Trust Elevation TC has produced drafts, based on ITU-T X.1254 (ISO/IEC 29115), of a comprehensive list of authentication methods, and methods for computing their authentication strength, based on the vulnerabilities of each and their associated mitigation/control characteristics. We recommend that NIST consider building on this approach, with the objective of a catalog of factors and combinations that will better ensure that implementers understand (a) options for achieving strength of authentication, and (b) the multiple effects that various factors may have.

PATHS FOR TRUST ELEVATION A well-populated matrix of options for combined factor use also should readily identify paths for trust elevation -- by showing where the addition of a factor or factors will materially improve authentication strength, without introducing new compensating vulnerabilities that undermine it. Trust elevation opportunities can arise in multiple steps in an authentication workflow. For example, when a Credential Service Provider (CSP) authenticates a user coming from a smart device:

- The CSP may 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 identity provider or attribute provider, to other verifiers or relying parties, those parties can elevate the authentication strength per their own

requirements; they may also be able to ask the CSP to do so on their behalf, or combine the CSP tokens into application-specific attributes, such as behavior, on their own.

Parties should have standardized means of requesting stronger assurance, as reflected in the specified transaction patterns under development by the OASIS Trust Elevation TC.

NIST may also wish to consider whether levels of assurance could be approached with an overlay/tailoring capability, similar to that described in NIST's SP 800-53. The revised 800-63 framework could describe a set of baseline assurance levels, each with a minimum set of factors and perhaps environmental or risk conditions – and each of which may be tailored as necessary, consistent with common tailoring guidance provided by the framework, to help each community of interest better meet its mission and business needs. Within each baseline level, adjustments to authentication strength could be approached using the additive approach adopted by the OASIS Trust Elevation TC as described above. Using this approach, it might be possible to compare some alternative factor combinations and transactional patterns, within a given baseline, in a deterministic or arithmetic manner, even if the "larger" steps between the baseline risk levels are not on a linear scale.

Respectfully submitted

James Bryce Clark
<jamie.clark@oasis-open.org>
General Counsel, OASIS

May 22, 2015

INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2013-2016

COM 17 – LS 217 – E

English only

Original: English

Question(s):	10/17	Geneva, 22 May 2015

Ref.:

Source:	ITU-T Study Group 17
Title:	LS with comments on NIST SP 800-63-2, Electronic Authentication Guideline

LIAISON STATEMENT

For action to:	NIST
For comment to:	-
For information to:	OASIS Trust Elevation TC
Approval:	ITU-T SG17 management team by electronic correspondence (22 May 2015)
Deadline:	N/A

Contact:	Abbie Barbir Rapporteur of ITU-T SG17 Question 10/17	Tel: +1 613-291-3253 E-mail: abarbir@live.ca
Contact:	Abbie Barbir Chairman of OASIS Trust Elevation TC	Tel: +1 613-291-3253 E-mail: abarbir@live.ca

This liaison statement represents a collaborative effort between the OASIS Trust Elevation TC and ITU-T Study Group 17, *Security*, in its Question 10/17, *Identity management architecture and mechanisms*, 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)

We also acknowledge and are grateful for the feedback and dialogue we enjoyed from participating experts of OASIS Trust Elevation TC, with whom we collaboratively developed this liaison statement, and who have been informed about this liaison statement.

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, NIST 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]

- Levels of Assurance (LoA) 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. 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 Knowledge Based Authentication (KBA) information public and water-down 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 NIST 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 minimize man in the middle attacks.
- Rec. ITU-T X.1254 (ISO 29115) have done an extensive extension additions to the NIST 800-063 framework and need to be taken into consideration.

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 drafts that can be used for developing a consistent method for determining, evaluating and improving on LoA levels in a technology independent fashion. It is also developing metadata and protocol for expressing and exchanging needed trust elevation methods between a verifier and a client.

---

[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.

- 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 with the authentication step. NIST needs to be 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 IETF Oauth, OpenID Connect and OASIS SAML.
- At the point of transaction, the environment needs to be evaluated, not just the credential. NIST needs to start accommodating the latest trends in using a device as part of the authentication process. In this regard, 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). Emphasis should be given to methods that lead to a hacker resistant authentication method where hacking the identity provider server will not result in massive security breaches. For example, in the OASIS Identity Based Attestation TC (IBOPS) models, the server holds a pointer to the client secrets and does not store any credentials locally. Client secrets are stored on the client device. This changes the attack vector of hackers whereby they will need to hack the server and the associated device to obtain a credential.
- Recommend harmonizing NIST SP 800-63 with work done in Rec. ITU-T X.1254, ISO 29115 and OASIS TRUST Elevation.

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 needs to enlarge the scope of authentication categories to include context and behaviour 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 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 enrolment and second or third factors on hard tokens. However, the trend in the industry is to unlock devices using biometrics with the task of binding the access request to a user to be performed by the verifier through the use of cumulative identity attributes that binds a device, location and behaviour 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 trends. Given that mobile single sign technologies are still primitive, it is important to not rely on cookies or unprotected tokens for Single Sign On support.

V Threats to Authentication

- Increasing authentication assurance requires the combinations of authentication factors with no or minimal overlapping vulnerabilities can result in enhanced 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 Recommendation 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 control. It is recommended that NIST build on this work to ensure that authentication strength is understood by implementers.
- It is recommended that Trust Elevation techniques should 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) can authenticate 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 behaviour, that they also can do on their own.

  – A standardized means of asking for higher assurance such as the ones being developed by OASIS Trust Elevation TC should be used.

  – An overlay/tailoring capability similar to NIST SP 800-53 could also be used. Each NIST SP 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 recommend the use of biometrics as tokens. They are mainly used at enrolment. However, if the right privacy enhancing methods is used combined with appropriate trust elevation methods (like in OASIS IBOPS) biometric can be evolved to provide effective user authentication at least at LoA 2. So it is recommended that NIST investigate the use of biometric as a full token.

References: 4

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. Recommendation ITU-T X.1254: Entity authentication assurance framework; http://www.itu.int/rec/T-REC-X.1254
4. Question 10/17 – Identity management architecture and mechanisms; http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/q10.aspx

_____