NIST SP 800-63 Rev4 - Pre-Draft Call for Comments: Digital Identity Guidelines

RSA Security Comments

RSA welcomes the opportunity to comment on NIST's Pre-Draft Call for Comments on SP 800-63 Digital Identity Guidelines. Given the importance if the guidelines to the identity and access management market as whole and beyond federal government solution deployments, we would like to see NIST consider modern methods of remote identity proofing and authentication. Decentralized identities, verifiable credentials, and passwordless authentication are in the forefront.

NIST SP 800-63A - Enrollment and Identity Proofing

Capabilities and innovative approaches for remote identity proofing to achieve equivalent assurance as in-person identity proofing.

One of the approaches NIST should consider for identity proofing and provide guidance on is the use of decentralized identifiers and verifiable credentials. An individual with a digital wallet can present a set of tamper-evident credentials and cryptographically proof possession of those credentials at the time of enrollment. Governments and private entities can be Verifiers and/or Issuers of verifiable credentials. As Verifiers, they can consume verifiable credentials issued by trusted entities such as a bank. As issuers, they can issue verifiable credentials to individuals for remote re-proofing purposes after undergoing an in-person or remote proofing process. With the use of verifiable credentials privacy will be enhanced. Individuals are in control of what information they can share at the time of enrollment and Verifiers can limit the data they collect and store about individuals.

NIST SP 800-63B - Authentication and Lifecycle Management

Use of contextual data in conjunction with behavioral characteristics as an authenticator factor

We feel that the push to promote a continuous evaluation of identity will mean more and more focus on contextual authentication methods—methods based on evaluation of several signals that arise from the context of identity-present operations. These methods might include things like locations, presence of known/bound devices, keystroke patterns, etc., and are referenced slightly in 5.2.2.

We would like to see NIST provide some guidance around the use of this kind of method as an authenticator, and around determination of the strength of such methods. In addition, guidance around requirements for privacy and establishment of authentication intent should be established in the document. The stronger the set of contextual information is--i.e. the more that it uniquely identifies a individual—the more important privacy considerations become. In particular, the need to protect things

that are not revocable (keystroke patterns, etc.) should be identified to the same degree as some other “what you are” identifiers.

Section 5.2.9 references the fact that authentication intent is not always established for “behavioral biometrics”, and this is also true for the broader scope of context-based information. The document should probably include guidance for this kind of “continuous authentication” case, to require notification or a cancellation operation when authentications happen, and a distinction between cases that require intent from cases that do not (agents).

Multi-Factor Cryptographic Device definition

The definition of a Multi-Factor Cryptographic Device needs further clarification. NIST should provide more guidance about how general-purpose computing devices with secure processing can achieve the status of "cryptographic device" rather than "cryptographic software", with special emphasis on mobile devices. Mobile applications running in the high-level operating system environment and implementing, for example, user inputs and display functionality can leverage an embedded authenticator to perform cryptographic operations in a restricted operating environment (for example a SE, a TEE or a TPM).

We look forward to further discussions with NIST on this topic and would welcome the opportunity to provide more details and answers to any questions on the above recommendations.

Please contact Salah Machani and Christopher Mclaren with RSA SecurID Access Product Engineering.