May 22, 2015

Mr. Paul Grassi
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD  20899


Ref:  Special Publication 800-63-2 Call for Comments

Dear Mr. Grassi:

The International Biometrics & Identification Association (IBIA) is pleased to provide comments on NIST Special Publication (SP) 800-63-2 *Electronic Authentication Guideline* in response to the NIST Call for Comments issued on April 9, 2015.  IBIA is a non-profit trade association based in Washington, DC that promotes the effective and appropriate use of technology to determine identity and enhance security, privacy, productivity, and convenience for individuals, organizations, and governments.

Specifically, IBIA is providing comments in response to the following question raised by NIST in the Call for Comments:  "What requirements, processes, standards, or technologies are currently excluded from 800-63-2 that should be considered for future inclusion?"

The current and prior versions of SP 800-63 define a very narrow role for biometrics in e-authentication.  IBIA believes that a greater role for biometrics, as a legitimate authentication mechanism in e-authentication transactions, is now warranted in light of changes that have occurred since SP 800-63 was first published.  The following rationale is provided for your review and consideration:

• This publication justifies the exclusion of biometrics as an authentication mechanism by stating that it is not "secret" and that the security of biometrics is "often weak or difficult to quantify".  IBIA appreciates that biometric-based authentication systems used for e-authentication must be secure from attack.  We believe that advances in biometric technology, such as anti-spoofing countermeasures, and other well-understood security design approaches, such as server-based matching, digital signatures and encryption, make it possible to design effective systems that include biometrics as a recognized authentication token.
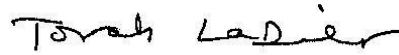
- We believe that biometrics should be designated as an authentication token for assurance levels 1 and 2.  We believe that passwords and PINs are more likely to be compromised than biometrics.  Obtaining a person's biometric template, even in clear text, is not the equivalent risk as obtaining someone's password or PIN since the impersonator is faced with the non-trivial task of inserting the binary biometric template data into the system as if it had been derived from a live image which was presented to a biometric sensor by the legitimate user.  One can easily make the argument that biometrics are more secure than passwords or PINs and provide a significant convenience benefit to the user.

- There are a number of authentication architectures in which biometrics may be applied.  These architectures should be investigated for suitability and included as appropriate, including server-based biometric verification.  For example, NIST funded an NSTIC pilot that provided e-authentication based on specific mobile device possession (cryptographically verified) plus biometrics captured on a mobile device - but matched within a server (i.e., at the verifier).  The biometric data was cryptographically protected during transit and at rest, a comparative token risk assessment was performed, and the solution underwent security and privacy assessments as part of the pilot.

- Today, biometrics are being used in conjunction with mobile devices in multi-factor authentication implementations, not all of which strictly comply with the token definitions within SP800-63-2, but which demonstrate similar (if not better) risk profiles.

- The usability of biometrics has seen a huge improvement in the last decade, with commercial organizations beginning to adopt biometrics specifically for enhanced user experience (in addition to its security features).  Having strong authentication that people can actually use is a significant advantage over many current technologies that are very difficult for people to use – in which case they don't.  Server-based biometric matching has been used successfully as a second authentication factor in mobile banking and other financial services.  Rather than adding "friction", as many strong authentication methods do, biometrics has been found to provide a very quick and easy user experience – even for the elderly.  A recent article about the biometric e-authentication implementation at the United Services Automobile Association (USAA) illustrates this point.  See: http://www.americanbanker.com/news/bank-technology/biometrics-find-support-from-an-unlikely-demographic-seniors-1074341-1.html.

- Biometrics (the 3$^{rd}$, 'what you are' factor) should be elevated to authentication token status.  Where appropriate, suitable protection of the biometric data can be specified.  If necessary, biometrics can be limited to use as a 2$^{nd}$ or 3$^{rd}$ factor only (rather than used alone as a single factor).

IBIA urges NIST to give serious consideration to defining an expanded role for biometrics in e-authentication applications – including server-based matching.  If you have questions, please feel free to contact Tovah LaDier, IBIA's Managing Director at (202) 587-4855 or by email at tovah@cl-law.us.

Sincerely,

Tovah LaDier
IBIA Managing Director