Smart Card Alliance Comments: Draft FIPS 201-2

Usage: Authentication

- LaChelle LeVan
- Director, Strategic Alliances - Probaris

NIST FIPS 201-2 Public Workshop
NIST, Gaithersburg, MD – April 18-19, 2011

Usage and Authentication

- **FIPS 201-2 (draft)**
  - Normative reference standard
  - Authentication mechanisms and descriptions are the foundation for requirements and testing scenarios
  - Possible misalignment with best practices and other standards and recommendations

- **Smart Card Alliance comment topics:**
  - Biometrics
  - CHUID
  - Public Key Infrastructure [PKI]
  - Assurance

Protocols, Protocols Everywhere…

➢ Line 553: Add SCVP path validation

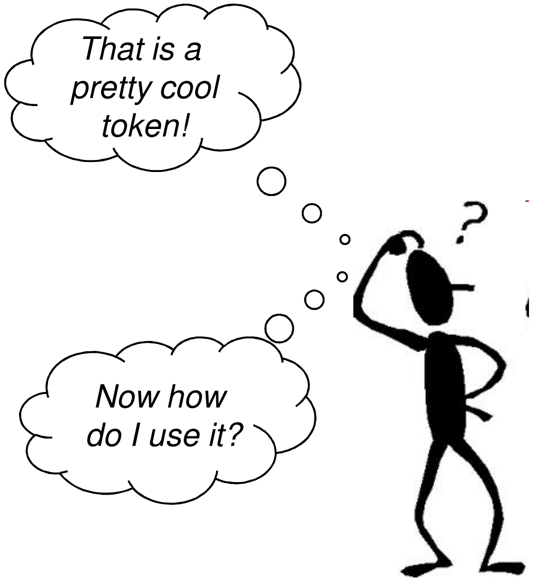
- Change to:
  - Online Certificate Status Protocol (OCSP) *and Server-based Certificate Validation Protocol (SCVP)* responders shall be updated so that queries with respect to certificates on the PIV Card are answered appropriately. *These* may be performed indirectly (by publishing the CRL above) or directly (by updating the OCSP server's internal revocation records).

Biometric Match on Card: What is secure?

- “Secure messaging” is not actionable and interoperable
- Line 1332: Biometric match on card implemented over the contactless interface
  - Require secure messaging to protect the privacy of the contactless transmission of the card holder's presented template from the reader to the card.
  - No current protocols defined
  - Needs extensive discussion, and modification to associated special publications
  - Implementation mechanisms should be further specified in SP 800-78 and SP 800-73.

Section 6…

- Security is only good if it's used
- Security is only great if it's used correctly
- Can we talk the talk, and walk the walk?



Let's just update the entirety of Section 6…

CHUID and Authentication (1 of 2)

CHUID ✚ *SIGNATURE* ≠ PASSWORD

- **The signed CHUID is only an identifier and should be treated as such.**
- **Line 1186:**
  - **Yes, the signature adds entropy to the unsigned CHUID**
  - **Not a good reason to assimilate the signed CHUID into a password**
  - **Any authenticator has to be kept private**
  - **The signed CHUID is a public identifier which can be read over any interface by any reader *without the user's knowledge*.**
- **This paragraph, as written, would tend to suggest that the signed CHUID could be used for authentication.**
- **It may indeed be good practice to store only a hash value of the CHUID in relying systems, but this section should in no way recommend assimilating into, or using the CHUID, as a password.**

CHUID and Authentication (2 of 2)

CHUID − *SIGNATURE* ≠ ONE FACTOR

- **Signature on the CHUID provides validation of integrity, but…**
- **CHUID is only an Identifier**
  - **Can be used to link / index accounts**

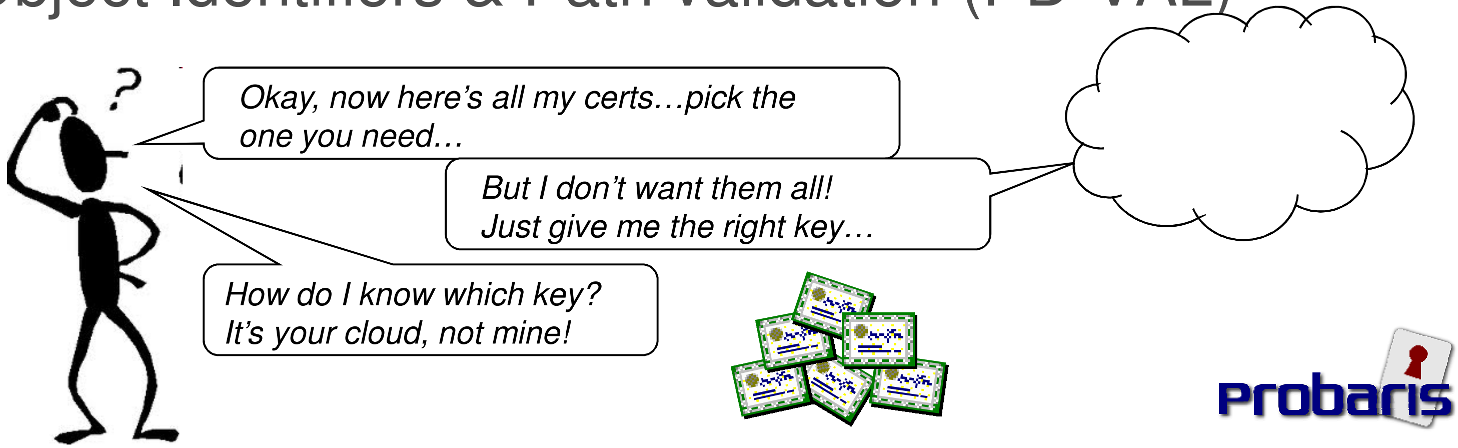
Line	***Comment***
1643	An unsigned CHUID alone shall not be considered one factor.
Line 1840, Table 6.2	An unsigned CHUID alone shall not be considered one factor.
1843, 1845	It is misleading to indicate in this table that VIS or CHUID used alone provide more than "little or no" level of assurance/confidence. In SP800-116, only the combination of VIS and CHUID provides some confidence.

CAK and PACS PIN: Two-Factors!

- **Something I claim? (identifier for linking)**
  - CHUID, FASC-N, UUID
- **Something I have? (One Factor)**
  - CAK (Asymmetric, symmetric)
- **Something I know? (Two Factor)**
  - A secret PACS PIN
- **Add:** PACS PIN + CAK Symmetric, PACS PIN + CAK Asymmetric
- This verifier may be required in normal operation of physical intrusion detection [ID] functions.
  - Provides alignment with common specifications for SCIF access i.e. DCID 6/9 JAFAN 6/9 to name a few.

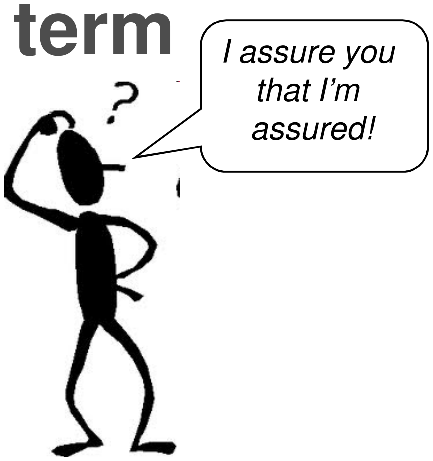
PKI and Authentication: “P what?”

- **Section 6.2 contains recommended validation procedures for use of PKI**
  - Not fully qualified for logical or physical access
  - Further, is very misleading for *remote* logical access
- **Modify to include use of full validation checks and incorporate:**
  - Explicit mention of Revocation checks
  - Policy Object Identifiers & Path validation (PD-VAL)


?
Okay, now here’s all my certs…pick the one you need…
But I don’t want them all! Just give me the right key…
How do I know which key? It’s your cloud, not mine!

Finally: Assurance? Assurance in what?

- **Commonly used yet under-qualified term**
  - Identity Assurance?
  - Cryptographic Assurance?
  - Authentication Assurance?
  - Levels of Assurance?



- **In the entire document:**
  - The term "assurance levels" should be explicitly linked to a given meaning and mechanism
  - Clearly separate and state
    - "Identity Assurance level“
    - “Authentication Assurance level”
    - “Levels of Assurance”
    - Example: Page 68, Table 6-3, Appendix E

Smart Card Alliance

LaChelle LeVan
Probaris, Inc.
llevan@probaris.com

Probaris

- Smart Card Alliance
- 191 Clarksville Rd. · Princeton Junction, NJ 08550 · (800) 556-6828
- www.smartcardalliance.org