Smart Card Alliance Comments: Draft FIPS 201-2

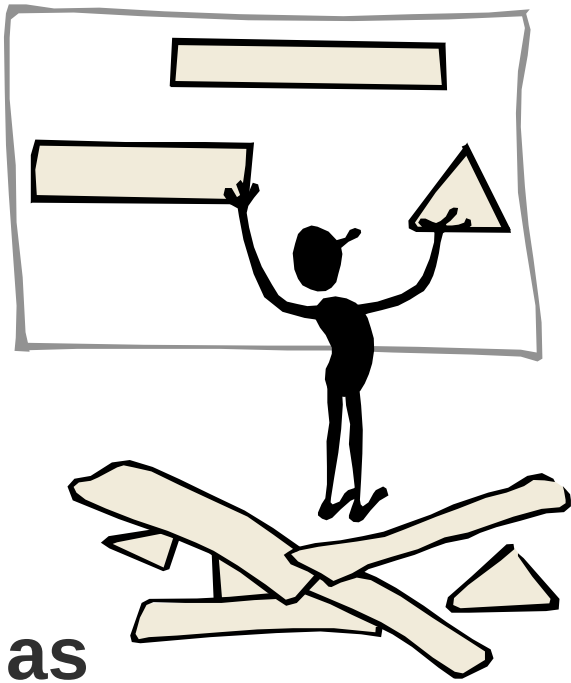
Change Management

- Gilles Lisimaque
- Identity Technology Partners, Inc

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

Change Management

- The following comments are grouped together as the changes proposed in FIPS 201-2 have consequences on systems, terminals, relevant software, and related procedures.
- SCA believes it is important to get some guidance on how to handle such management in a coherent and coordinated manner, as well as minimizing the consequences of the transition for components and systems already in place.



Change Management (Line 270)

- **Comment: The** PIV Application Identifier (AID) is not used to manage version changes. Many terminals today are calling for the full AID on 11 bytes.

- **Suggested change:** The PIV AID (PIX) should be used to indicate the version a given card is compliant with. All terminals should call the AID on 9 bytes only and check the full AID returned by the card (11 bytes). For versions fully backward compatible the last byte of the AID should change, for modifications changing options (e.g. CAK), the byte before last should change

Change Management (Line 276)

- **Comment:** Systems (e.g. PACS) are assumed to accommodate all options of the PIV standard. As such when an option is added (e.g. CAK or MOC or a new cryptographic algorithm) they have to be updated and re-certified

- **Suggested change:** Add sentence: System changes may affect current FISMA and C&A status.

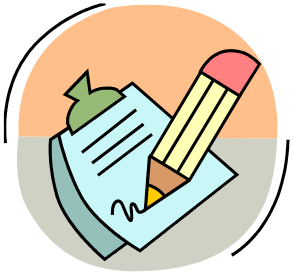
Change Management (Line 287)

- **Comment:** Components that may be affected by version management include, for example, PIV Cards, PIV middleware software, and card issuance systems. The current language does not include relying subsystems and possible consequence of change.

- **Suggested change:** Change sentence to: Components that may be affected by version management include, for example, PIV Cards, PIV middleware software, card issuance systems *as well as relying subsystems. Such system changes may affect current FISMA and C&A status on applicable system components. It is assumed that OMB will issue guidance indicating the requirement for iris recognition, as an alternative to fingerprint matching, will be effective following an update to SP 800-76.*

Change Management (line 525)

- **Comment:** Renewal of card**:** The digital signature must be recomputed with the new FASC-N. **A new FASC-N may require re-registration in relying subsystems.**



- **Suggested Change: Add sentence:** The re-issued card will have a new Credential Number (CN). This results in a new FASC-N. The digital signature must be recomputed with the new FASC-N *and the new credential must be re-registered/re-enrolled into the relying subsystem*

Change Management (Line 583)

- **Comment:** This paragraph should mention that the Security Data Object may also have to be updated as a consequence of other updates.

- **Suggested change:** Suggested to add a sentence saying:
  "The Security Data Object in the card shall be updated to reflect any changes made by such modifications".

- Note: Another possibility is to drop the use of the security data object all together.

Change Management (Line 1298)

- **Comment:** The paragraph about symmetric keys clearly indicates there are commands and containers (and tags) which are not (and will not be) specified in the FIPS 201 standard.

- **Suggested change:** Suggested to modify the last sentence: "This standard does not specify key management protocols or infrastructure requirements, *but will provide naming spaces as well as card commands avoiding collisions with future releases of this standard."*

Change Management (Line 1856)

- **Comment:** Table 6-3 assumes the client (local workstation) on which such verifications are made has not been subject to any kind of attack or malware invasion. This should be mentioned as it is VERY important that the PIN or the Biometric data is not captured, cached and replayed in a rogue client.
- **Suggested change:** Add a note under the table:
  "This table assumes the workstation software and its middleware have not been compromised."

Smart Card Alliance Comments: Draft FIPS 201-2

Card Usage Data

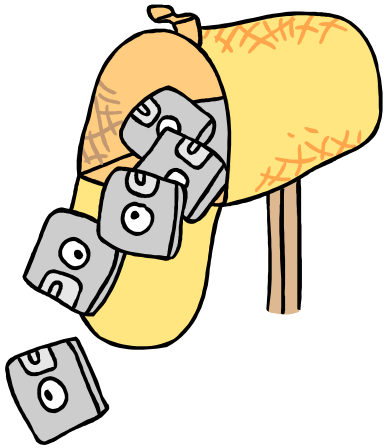
- **Gilles Lisimaque**
- **Identity Technology Partners, Inc**

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

Usage Card Data

The following comments are grouped together as they relate to changes in data structures, their content, their protection or the policies to which they relate.

The following highlights some of the important impacts of such changes identified the Smart Card Alliance.



Usage Card Data (Line 583)

Already mentioned in change Management

- **Comment:** This paragraph should mention that the Security Data Object may also have to be updated as a consequence of other updates.

- **Suggested change:** Suggested to add a sentence saying:
  "The security Data Object in the card shall be updated to reflect any changes made by such modifications".

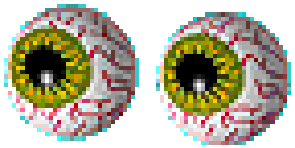
- Note: Another possibility is to drop the use of the security data object all together.

Usage Card Data (Line 615)

- **Comment:** The inclusion of the option to allow the cardholder to provide a primary identity source document to receive the credential after a PIV Card Verification Data Reset (e.g. PIN reset etc) undermines the security and intent of other identity vetting processes.

- **Suggested change:** ...or require the cardholder to provide a primary identity source document (see Section 2.3). If a biometric match is performed, then the type of biometric used for the match shall not be the same as the type of biometric data that is being reset. *If a primary identity source document is provided, then the primary identity source document must match one of the identity source documents used to enroll the cardholder.*

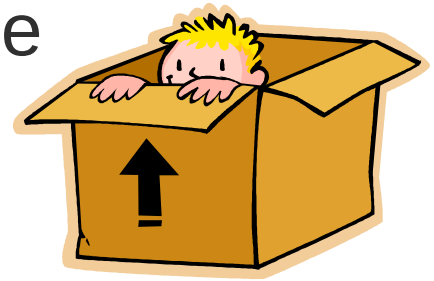
Usage Card Data (Line 1186)



- **Comment:** What ever its entropy is, **the signed CHUID is a public identifier (user name)** 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 and as such should be protected for security reasons.
- **Suggested change:** Replace the whole paragraph with the following: "*The CHUID may be read and used by the relying system and should be treated as an identifier*. It provides information about the CHUID issuer and cannot be modified or altered because of its digital signature. But even so, the CHUID cannot be used as an authenticator as it can be duplicated, cloned or replayed even without the legitimate cardholder's knowledge or consent. It can be used as an index pointer in relying systems; *but used alone, should not be considered as an authentication factor regarding the user or his/her card."*

Usage Card Data (Line 1335)

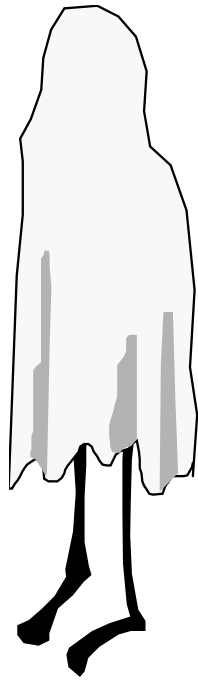
- **Comment:** Is there a policy related to the export of the biometric data on the PIV credential to other relying parties?



- **Suggested Change:** Provide a reference to clarify biometric information export to readers or relying systems.
- **Note:** Such policy may also impact the card data management aspects when it says in the document the Reference biometric used for match-on-card shall never live the card (see next)

Usage Card Data (Line 1335)

- **Comment:** "*The PIV Card shall not permit exportation of the on-card biometric comparison data*". This sentence seems to assume the on-card biometric reference data is different from the biometric data stored in the PIV data object available on the contact interface. **If this must be the case, this should be explained in more detail**.



- **Suggested Change:** Indicate if the On-Card-Biometric data must be different from the information stored in the PIV biometric data object which can be exported outside the card.

Usage Card Data (Line 1769)

- **Comment:** The Subject Distinguished Name (DN) and unique identifier from the authentication certificate are extracted and passed as input to the access control decision. This does clearly indicate the FASC-N can be used as input to PACS for authorization.

- **Suggested Change:** Change as follow:
  The Subject Distinguished Name (DN) and unique identifier *(e.g. FASC-N)* from the authentication certificate are extracted and passed as input to the access control decision**.**

Usage Card Data (general)

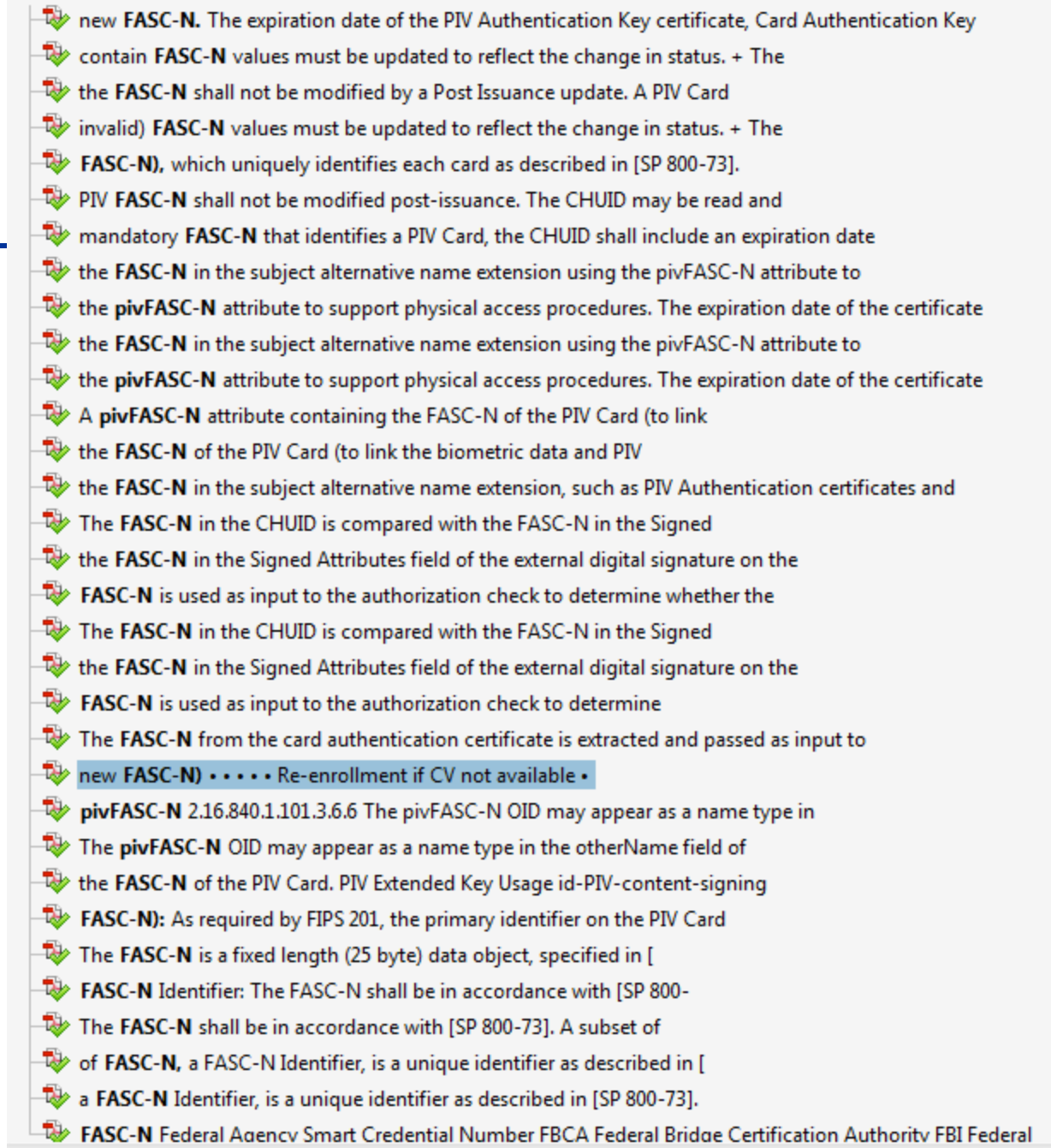
- **Comment:** The entire document is using the term FASC-N all over the place which works only for PIV cards. PIV-I cards are using UUID and PIV may do the same one day.

- Suggested change: Define the term “Unique Credential Number” used to bind the various data objects of the same credential. Define this is the FACS-N in PIV once in the document and use the term “Unique Credential Number” there after.

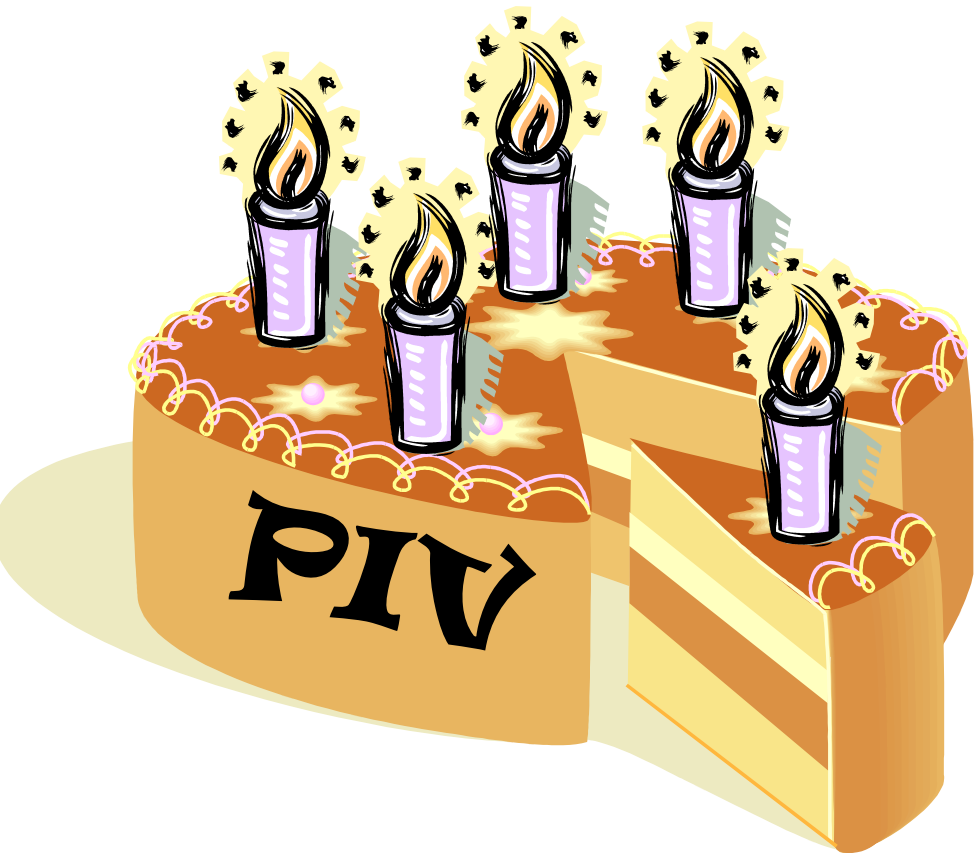
Note: The tern FACS-N or pivFASC-N is used 32 times in the document.

FASC-N term used 32 times in FIPS 201-2

The FASC-N is the PIV credential Identifier



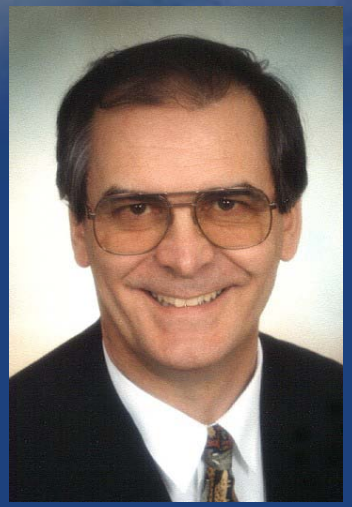
CAK is mandatory!



With FIPS 201-2, it is now possible to have your CAK and eat it too….

Smart Card Alliance

Speaker Contact Information



Gilles Lisimaque
Glisimaque@idtp.com

ID TECHNOLOGY PARTNERS

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