Derived PIV Credential Token Form Factors

March 4, 2015

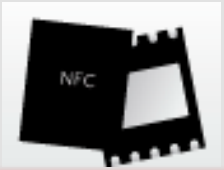
Christophe J. Goyet
c.goyet@oberthur.com

Oberthur Technologies – Identity Business Unit

Smart, Secure Devices -Form factors

- Contact and contactless technologies
- Employee ID (with Photo ID)
- Physical and Logical access applications

- Contact and Contactless (with built-in card reader)
- No Photo ID
- Physical and Logical access applications



- Mainly for Secure Mobile Device applications
- Physical and Logical access applications

Mobile device use cases

E-mail Encryption | E-mail Signature

Physical Access | VPN

Example Use cases

1. Secure Mobile device applications using external Card

E-mail Encryption | E-mail Signature

Physical Access | VPN

Example Use cases

2. Secure Mobile device applications + Use Phone as a Card

Same applications, but different form factors to carry credentials

Form factors- Implications

eSE

UICC /SIM

MicroSD

Card –External SE

Handset Manufacturer	Telecom Operator	Issuing organization
Fused to the device hardware	Plugged-in by the Subscriber	Removable Item
Device Manufacturer involved in the ecosystem	Telecom operator involved in the ecosystem	issuing organization
Credential tied to the device	Credential may be Portable	Credential Portable
Lifecycle management platform can be outsourced	Lifecycle management platform can be outsourced	Lifecycle management typically uses In-House Infrastructure

Embedded

Removable / External

Card Form factor: Physical Security

- Visual Verification of the Card /Cardholder
- Augment electronic verification
- Fall Back Mechanism (Situations where Electronic Verification not possible) :
  - Verification equipment unavailable
  - Verification equipment outage -Technical Issues
  - Non functioning Chip
  - Untrained personnel performing the verification

This is an extra layer not available to Derived Credentials

Typical Types of Fraud: Could they apply to Derived Credentials?

Counterfeit Card

- Copy of a genuine card entirely produced by a forger

Forged Card

- Modification of a genuine card, also called falsification : include photo substitution, data modification

Un-authorized Issuance

- False card based on a stolen non personalized original card – a stolen blank - personalized by a forger

Pseudo Card

- False document entirely invented by a forger and without any connection whatsoever to an existing original document
  - E.g.. Syldavia, Nuevo Rico, United World Nation

Physical Security Features for cards
How do they apply to non card form factors?

- Level 1 security features
  - For naked-eye inspection at point of usage, without any tools


hand


eye

- Level 2 security features
  - For examination by trained personnel with simple equipment

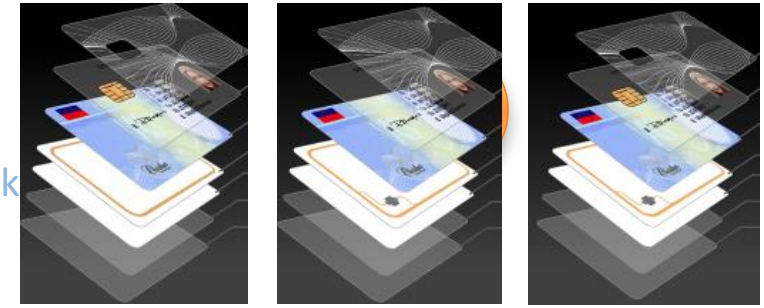

magnifier


UV lamp

- Level 3 security features
  - For inspection by informed forensic specialists with special equipment


microscope

- Level 4 security features
  - Only known to the customer and the ink supplier



Embedded Secure Element