Derived PIV Credentials Token Form Factors – Giesecke & Devrient's Activities

FIPS 201-2 Supporting Special Publications Workshop

NIST, Gaithersburg
March 3rd & 4th, 2015
Werner Ness

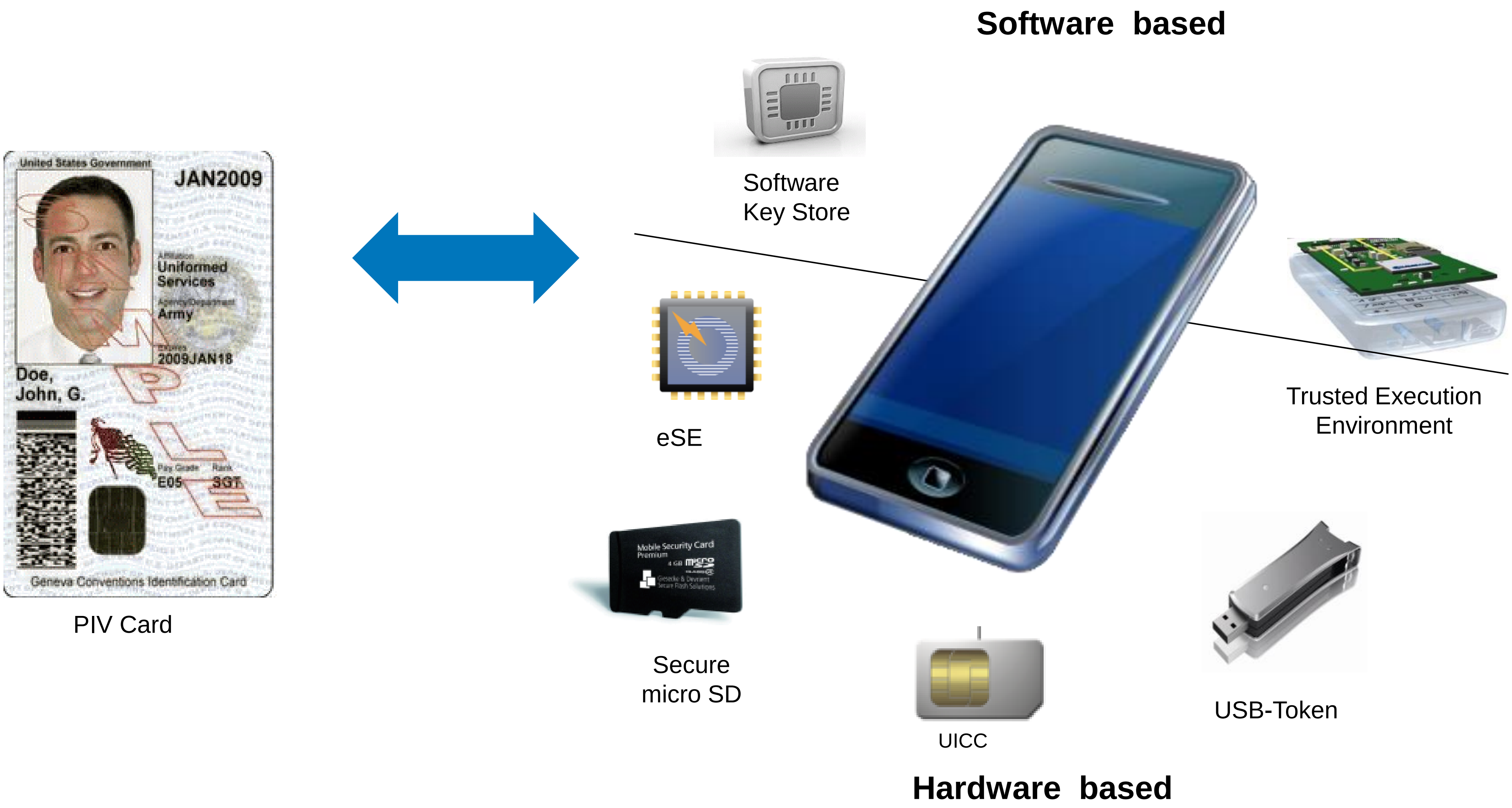
Giesecke & Devrient
Creating Confidence.

Agenda

- Introduction
- G&D Products
- G&D Activities
- Conclusion

1 Introduction

Concept of Derived PIV Credentials Tokens



PIV Card

Software based

Software Key Store

eSE

Trusted Execution Environment

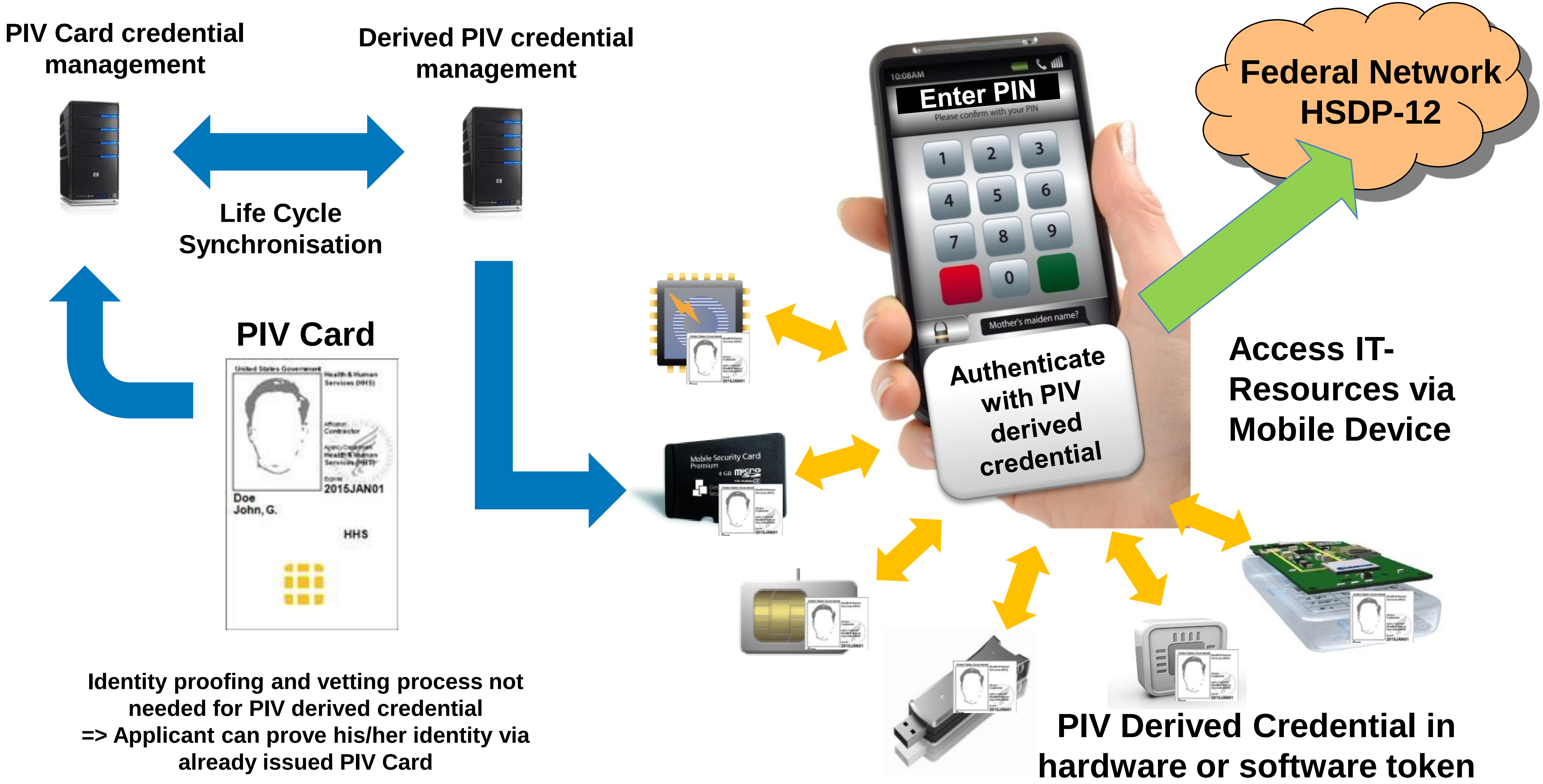
Secure micro SD

UICC

USB-Token

Hardware based

Purpose and Scope



PIV Card credential management

Derived PIV credential management

Life Cycle Synchronisation

PIV Card

Authenticate with PIV derived credential

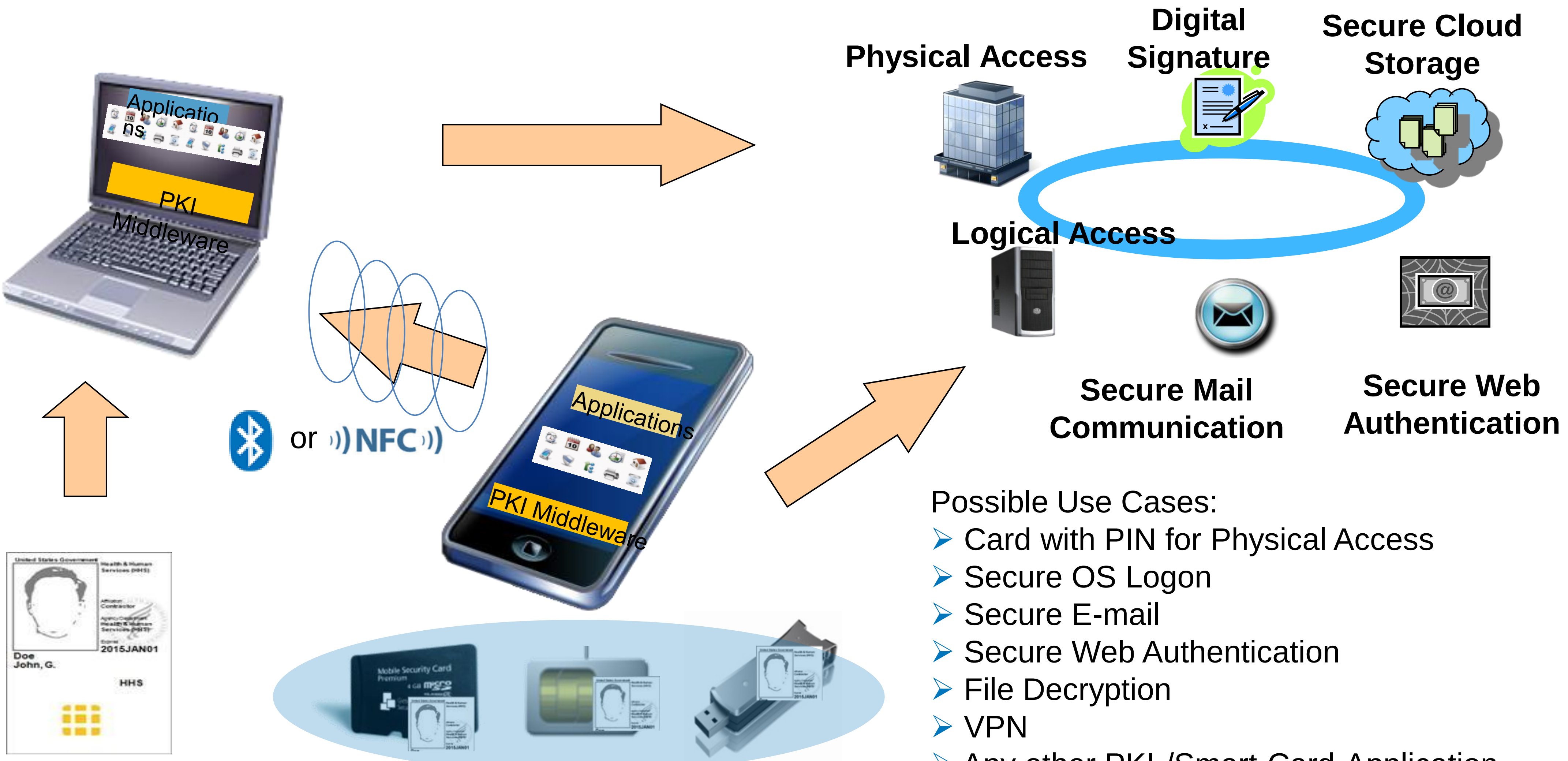
Federal Network HSDP-12

Access IT-Resources via Mobile Device

PIV Derived Credential in hardware or software token

Identity proofing and vetting process not needed for PIV derived credential
=> Applicant can prove his/her identity via already issued PIV Card

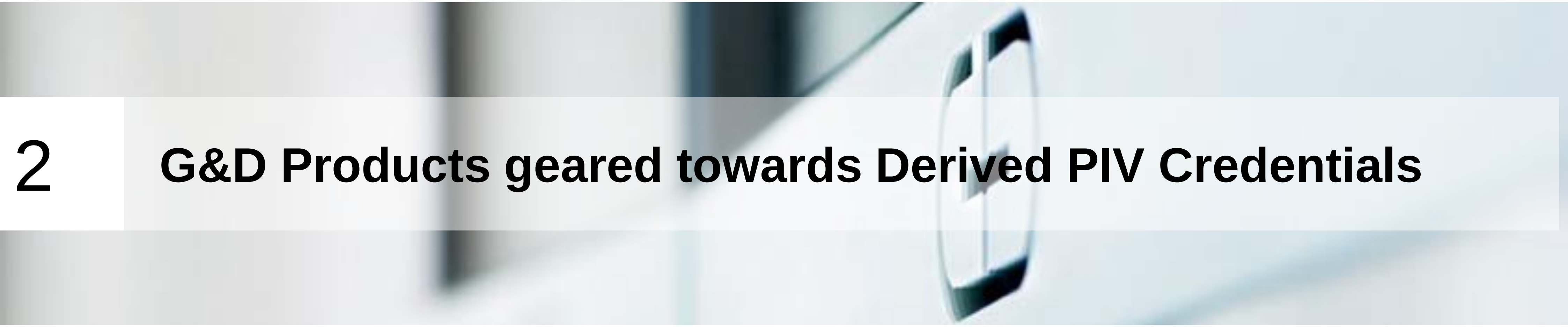
Use Cases with Derived PIV Credentials



Possible Use Cases:

- Card with PIN for Physical Access
- Secure OS Logon
- Secure E-mail
- Secure Web Authentication
- File Decryption
- VPN
- Any other PKI-/Smart-Card-Application

NIST SP800-157, Guidelines for Personal Identity Verification (PIV) Derived Credentials



2 G&D Products geared towards Derived PIV Credentials

Secure Java Platforms: Sm@rtCafé Expert

- Java Card Classic 3.0.4
- GlobalPlatform 2.2.1
- FIPS 140-2, level 3 certified: “Security Requirements for Cryptographic Modules”
- CC certified according to EAL 5+
- Dual Interface with communication speeds,
  - Contact up to 223 kbit/s
  - Contactless up to 848 kbit/s

- Encryption:
  - AES up to 256 bits
  - RSA up to 3072 bits
  - ECC up to 521 bits
  - Hash up to SHA-512
  - On-Board RSA and ECC Key Generation

SkySIM CX: G&D UICC for High-End SIMs/eSE

- SkySIM is a highly efficient and configurable Java Card platform
- Operating system usable regardless of the mobile network (GSM, UMTS, CDMA or LTE)
- Certification: CC-certified (EAL 4+)
- Mobile ID Solution in use: Vodafone Secure SIM
  - Supports Secure Login
  - Supports Secure Data
- Portfolio of applets for UICC available
  - E.g. Mobile Payment, Identity, Transit, Access
- Aspects of FIPS140-2 for an UICC, e.g. performance, algorithms and application management, being analysed

Common Criteria

INFORMATION TECHNOLOGY SECURITY
SOGIS
IT SECURITY CERTIFIED
MUTUAL RECOGNITION AGREEMENT

StarSign Crypto USB Token

- Token OS Sm@rtCafé Expert
- FIPS 140-2, level 3 certified
- Supports several USB standards
- Interfaces include CCID and PC/SC
- Solution depends on smart card chip technology

Secure Micro-SD-Card

- **Availability**
  - Micro-SD card is physically supported in most handsets.
- **Management**
  - requires Admin Agent Apps on mobiles
  - Communication over TCP/IP
- **Driver**
  - Some Handset OS‘s need additional driver support
- **FIPS/CC-certified**

3 G&D Activities

G&D‘s Activities for usage of derived PIV credentials

Supporting Standardisation

- **Support of standardisation of the SIMalliance Open Mobile API.**
- **As a Member of GSMA Mobile ID Task Force to define and describe an architecture and solution together with US MNOs and other UICC manufacturers.**

Providing Solutions

- **Providing Open Source implementation of Open Mobile API (SEEK).**
- **Providing Mobile ID solutions with UICC in several customer and technology projects (e.g. Vodavone Secure SIM).**
- **Token combination based on TEE with eSE. Application can be loaded remotely.**
- **Proof of concepts for implementation of Derived Credential Technologies.**

4 Conclusion

Conclusion

- SP 800-157 defines Derived PIV Credential Hardware Form Factors
  - Token operating systems are similiar to PIV-Cards.
  - Application can be derived from PIV.
  - APIs and interfaces in mobiles available (e.g. GP).
  - Technology of tokens available and deployed.
  - Certification is the same as for a PIV-Card.

- Open Questions
  - Additional Driver for specific tokens has to be provided (e.g. µSD)
  - Several interfaces are required to establish the eco-system
  - Requirements for existing technologies like UICC may be in contradiction to FIPS 140-2 (e.g. POST)

Questions?

Contact:

Jatin Deshpande	jatin.deshpande@gi-de.com
Werner Ness	werner.ness@gi-de.com