cryptas

we protect identities.

Smart Cards Anno 2020

Stand der Technik und worauf zu achten ist
About & Beyond PKI 2020

Author: DI (FH) Stefan Bumerl
stefan.bumerl@cryptas.com

Document Version: 1.0
Creation Date: 02/2020

CRYPTAS IT-Security GmbH
Franzosengraben 8 . 1030 Wien . Austria . **T** +43 (1) 3 555 3 - 0 . **E** info@cryptas.com

cryptas

we protect identities.

About CRYPTAS

SPECIALIST FOR PKI, STRONG AUTHENTICATION, ENCRYPTION, LAWFUL SIGNATURES AND DIGITAL IDENTITIES

Own solutions around Digital Signatures, Virtual Smart Card, clientless Smart Card access, Self-Service Processes, PKI, OCSP++…

CONSULTING, DEVELOPMENT, INTEGRATION, SERVICES

Topics: eSignature, Smart Cards, PKI, FIM, Key Management, HSM, Encryption…

WIEN, GRAZ, DÜSSELDORF AND STOCKHOLM

Successful in crypto-business since 2003; main markets D/A/CH, Typical Project Size: 1.000 to 300.000 Users

> 40.000 CUSTOMERS / ~100 COUNTRIES /

Verticals: banking, insurance, energy provider, health, industry, government…

Trust Center: Millions Transactions per Day / Thousands Enrollments per Day

eIDAS TRUST CENTER

Qualified Trust Center with focus on Qualified Onboarding, eIDAS Online Contracting, Video-Legitimation, eIDAS Remote Services

CRYPTAS IT-Security GmbH
Franzosengraben 8 . 1030 Wien . Austria . **T** +43 (1) 3 555 3 - 0 . **E** info@cryptas.com

cryptas

we protect identities.

What is a Smart Card

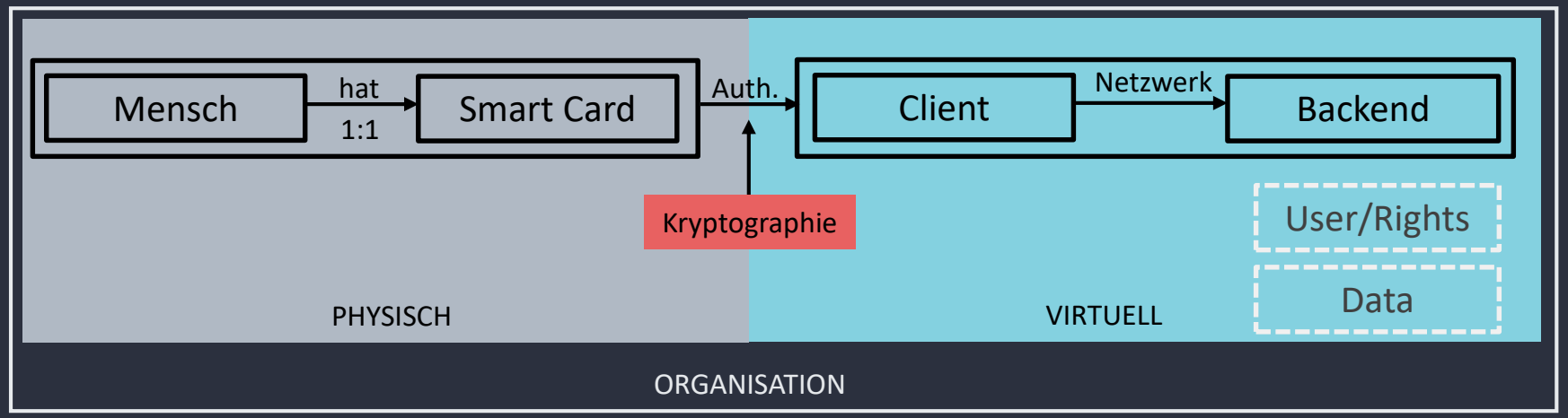
- In an abstract mean
- From a technological view
- Based on the security model
- Practically

cryptas.com . prime-sign.com . cryptoshop.com
Vienna | Graz | Düsseldorf | Stockholm

CRYPTAS IT-Security GmbH
Franzosengraben 8 . 1030 Wien . Austria . **T** +43 (1) 3 555 3 - 0 . **E** info@cryptas.com

cryptas
we protect identities.

Smart Cards from an abstract perspective



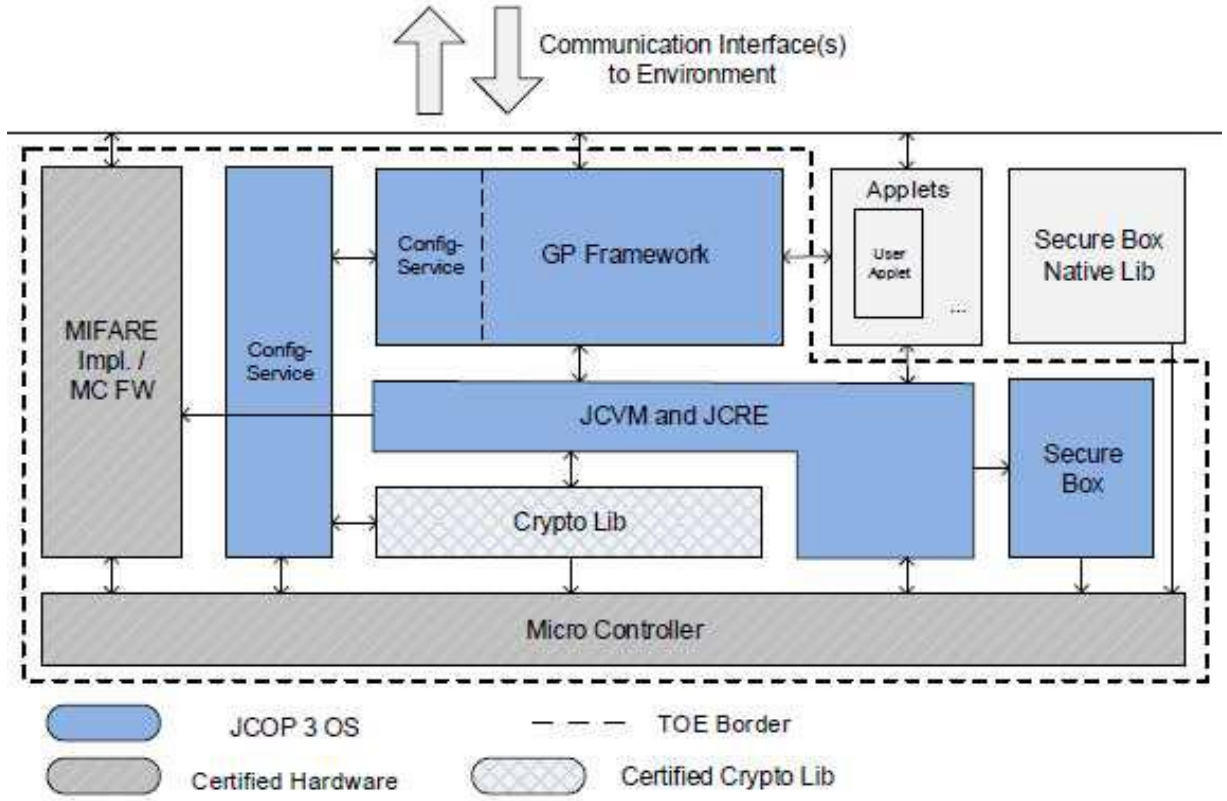
Digital Transformation as main driver

CRYPTAS IT-Security GmbH
Franzosengraben 8 . 1030 Wien . Austria . **T** +43 (1) 3 555 3 - 0 . **E** info@cryptas.com

cryptas
we protect identities.

Technological view

- Computer system (Micro Controller) with CPU, RAM, ROM, EEPROM/FLASH, Crypto-Coprozessor, UART/IO, MMU, Security Sensors
- HW abstraction by virtualization
- Card applications delivered by applets



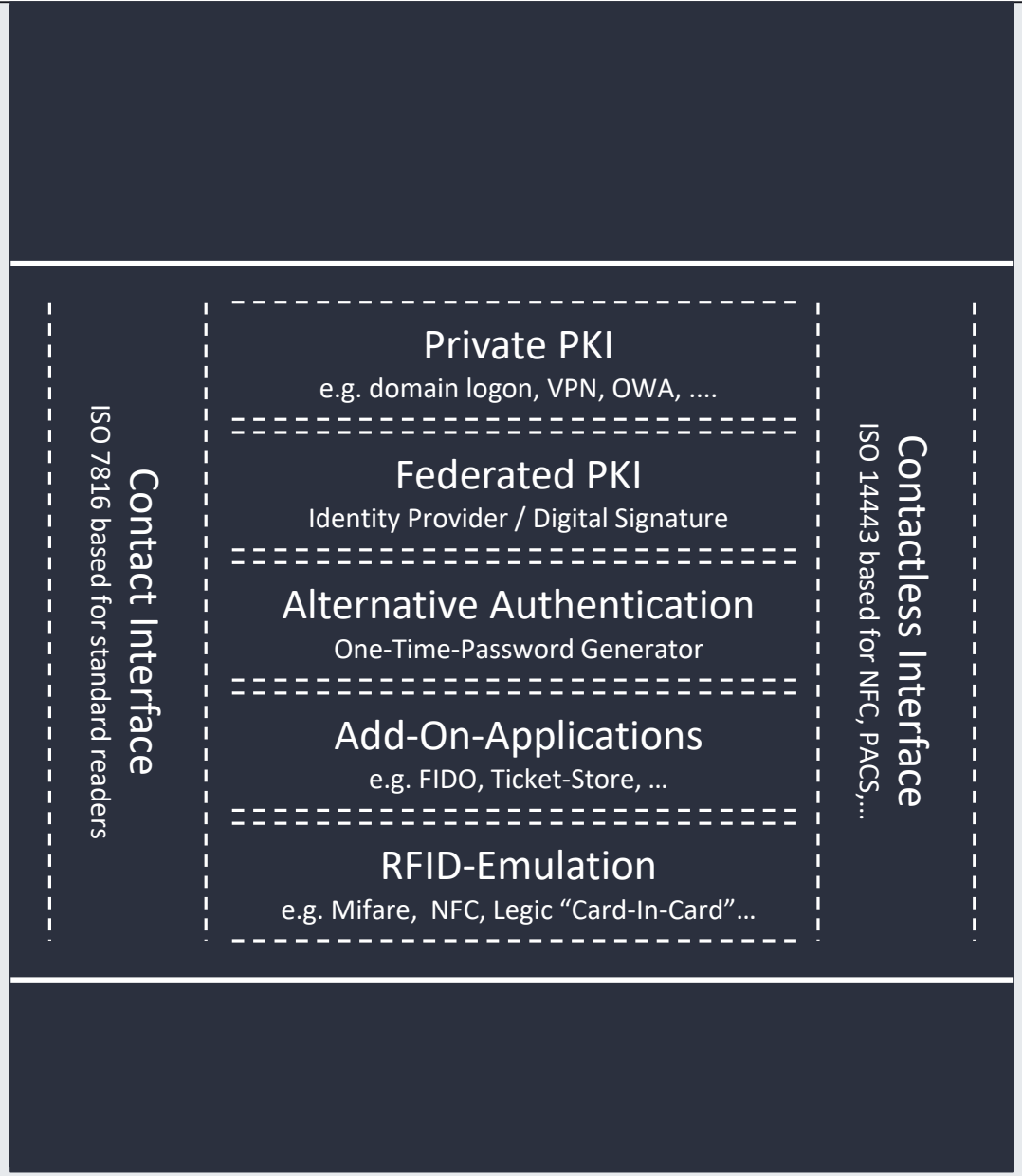
CRYPTAS IT-Security GmbH
Franzosengraben 8 . 1030 Wien . Austria . **T** +43 (1) 3 555 3 - 0 . **E** info@cryptas.com

cryptas

we protect identities.

Functional (typically)

- Dual-Interface (contact/contactless)
- PKI often main application
- Physical access control
- Alternative authentication by OTP / FIDO
- Proprietary applications



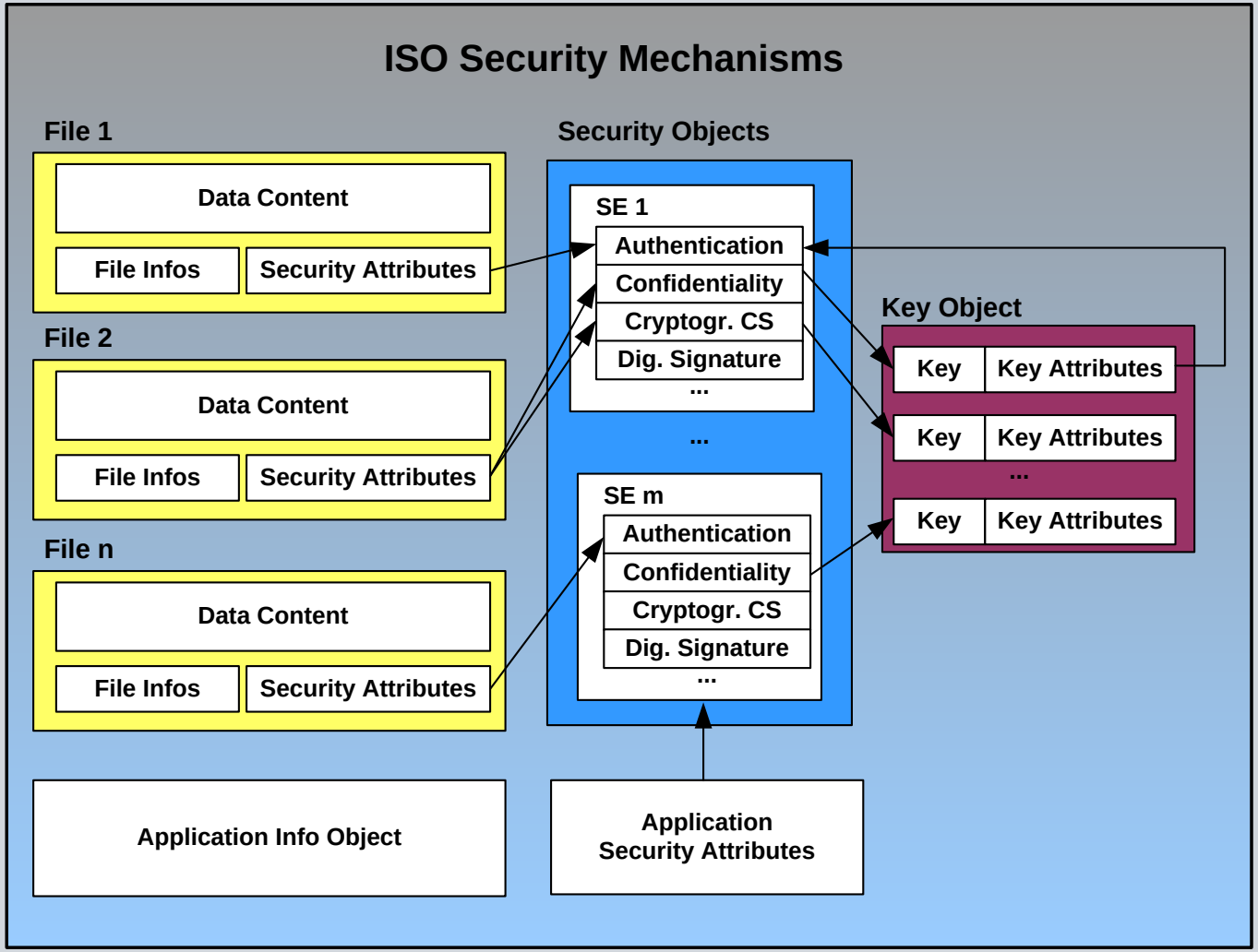
CRYPTAS IT-Security GmbH
Franzosengraben 8 . 1030 Wien . Austria . **T** +43 (1) 3 555 3 - 0 . **E** info@cryptas.com

cryptas
we protect identities.

ISO 7816 Security

- Data container with security attributes
- Reference to SE with mechanisms
- Reference to keys with security attr.

→ Separation of data, mechanisms and keys



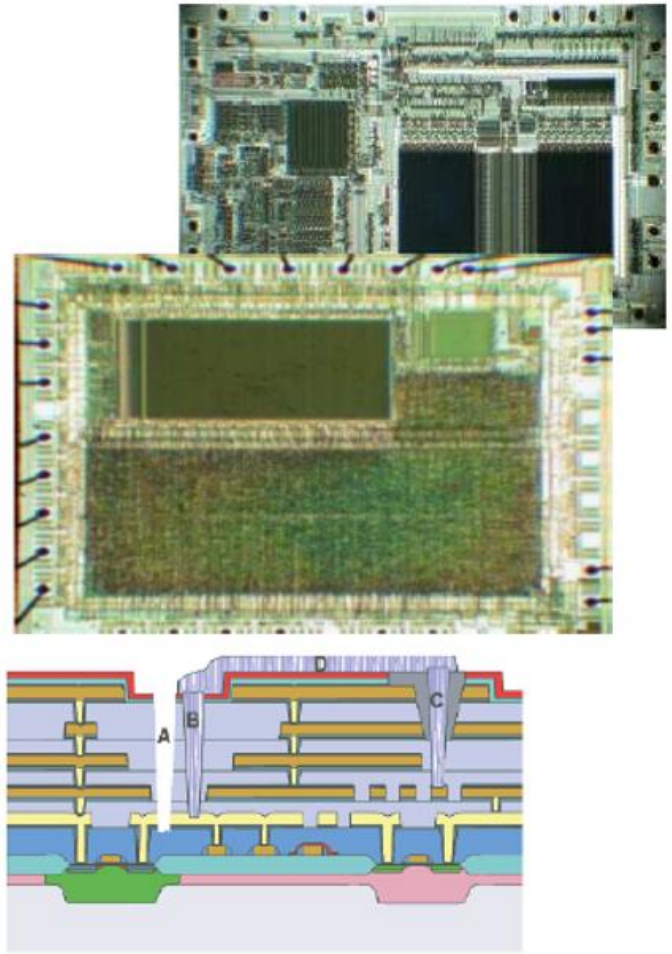
CRYPTAS IT-Security GmbH
Franzosengraben 8 . 1030 Wien . Austria . **T** +43 (1) 3 555 3 - 0 . **E** info@cryptas.com

cryptas

we protect identities.

On-Chip Security

- Sensors
  (voltage, clock, temperature, light)
- Filters (Spikes / Glitches)
- Decoupled clock
- Single Fault Injection detection
- Passive and active Shielding
- Bus and memory encryption
- Dense Multi-Layer Technology
- HW error detection
- True-RNG
- Noise-Generation (against Side Channel)
- …



CRYPTAS IT-Security GmbH
Franzosengraben 8 . 1030 Wien . Austria . **T** +43 (1) 3 555 3 - 0 . **E** info@cryptas.com

cryptas

we protect identities.

Practical Flavors

- Different form factors for different application areas
- Main aspects of choice:
  - mass capabilities
  - costs
  - Individualization
  - robustness
  - delivery options
  - speed
  - size
  - …

CRYPTAS IT-Security GmbH
Franzosengraben 8 . 1030 Wien . Austria . **T** +43 (1) 3 555 3 - 0 . **E** info@cryptas.com

cryptas.com . prime-sign.com . cryptoshop.com
Vienna | Graz | Düsseldorf | Stockholm

cryptas

we protect identities.

cryptas.com . prime-sign.com . cryptoshop.com
Vienna | Graz | Düsseldorf | Stockholm

Smart Card

SW-Architecture

- End-to-end security
- Software Stack
- Integration into the application

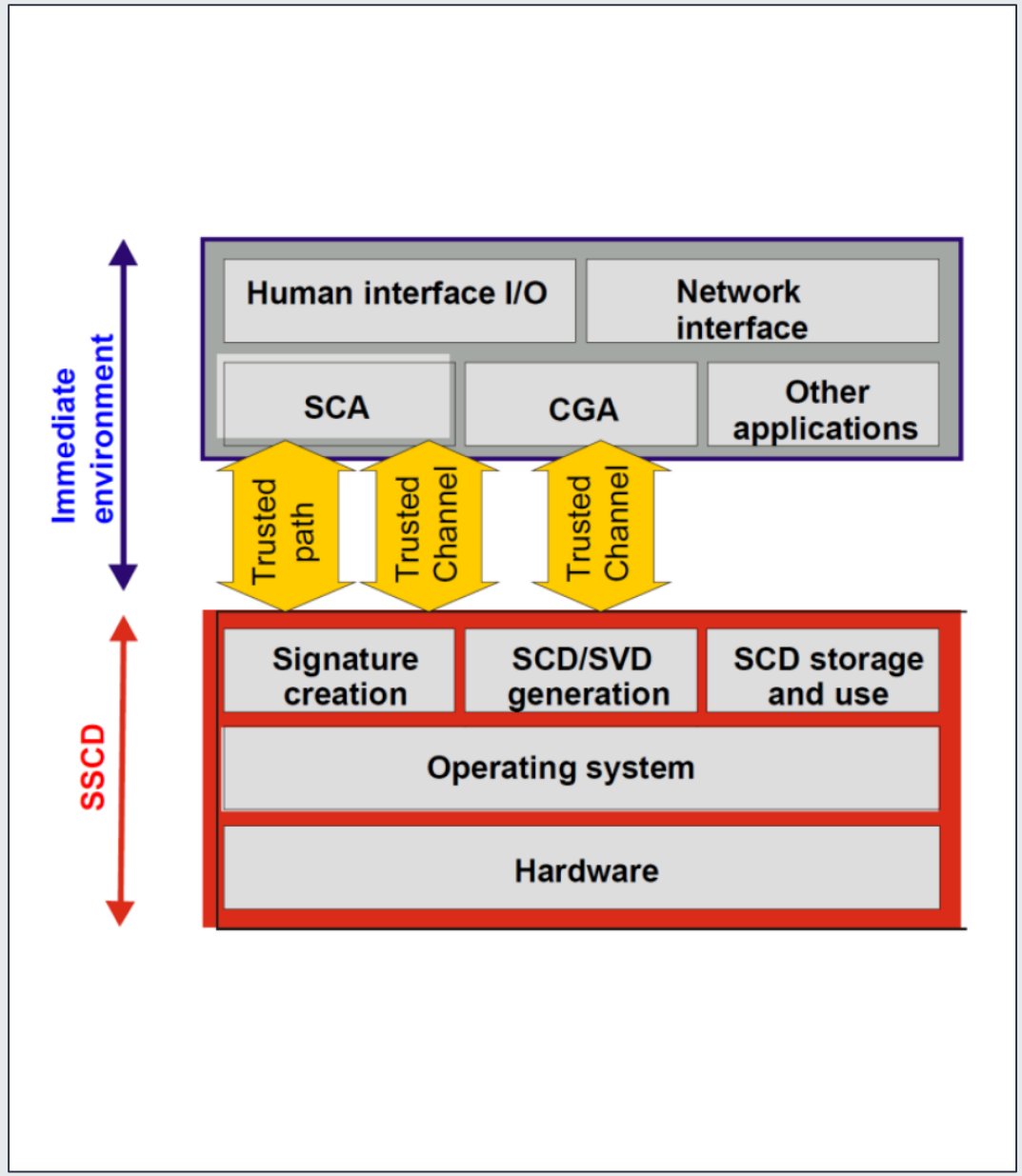
CRYPTAS IT-Security GmbH
Franzosengraben 8 . 1030 Wien . Austria . **T** +43 (1) 3 555 3 - 0 . **E** info@cryptas.com

cryptas

we protect identities.

End to End Security?

- SSCD: Secure Signature Creation Device
- SCA: Signature Creation Application
- SCD/SVD: Signature Creation/Validation Data
- CGA: Certification Generating Authority



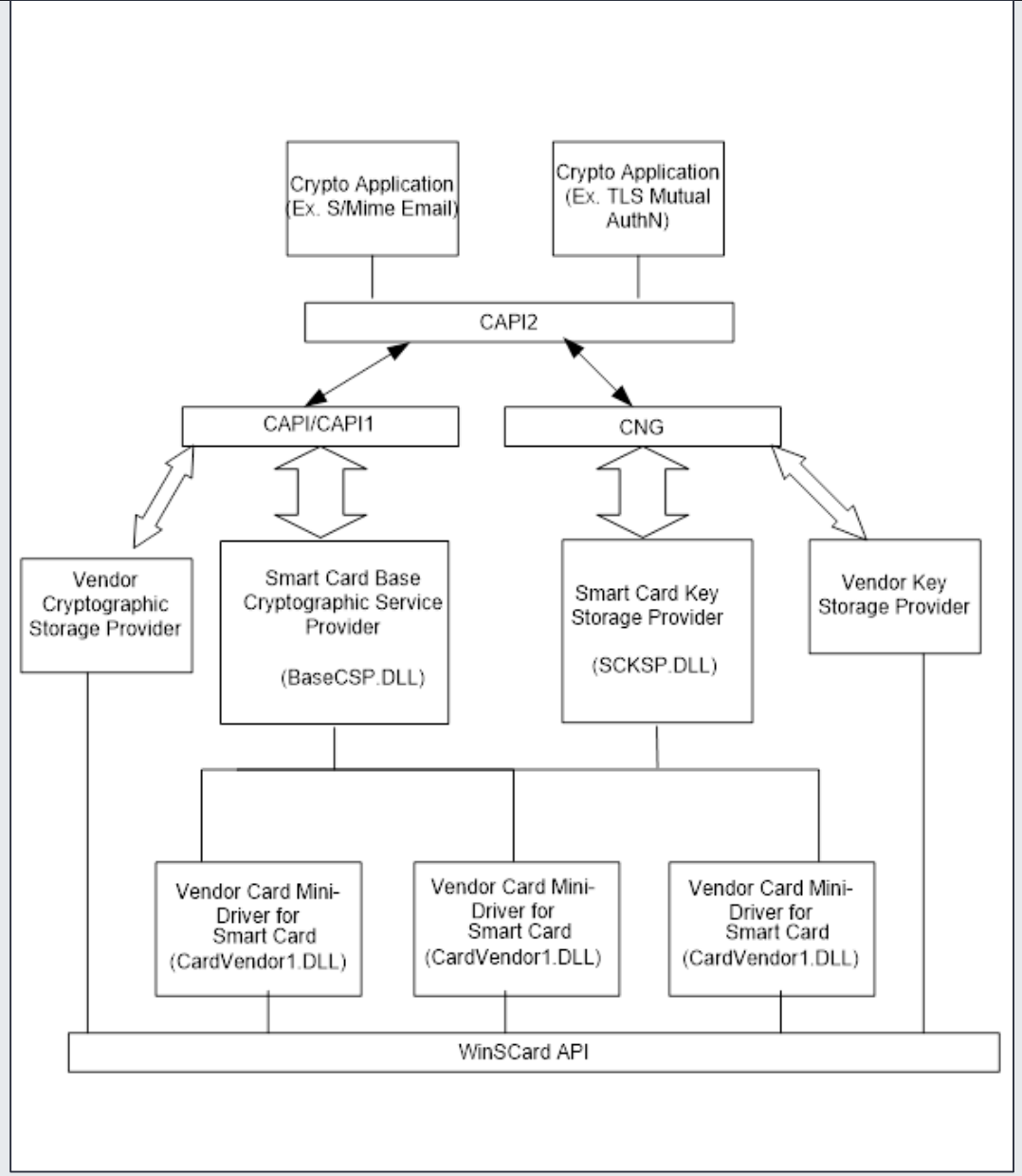
CRYPTAS IT-Security GmbH
Franzosengraben 8 . 1030 Wien . Austria . **T** +43 (1) 3 555 3 - 0 . **E** info@cryptas.com

cryptas

we protect identities.

Software Stack Windows

- Modular, well documented components
- Configured by Windows registry
- Dependent on System integrity / driver integrity
- Smart Card driver Plug and Play
- Responsible for overall performance



CRYPTAS IT-Security GmbH
Franzosengraben 8 . 1030 Wien . Austria . **T** +43 (1) 3 555 3 - 0 . **E** info@cryptas.com

cryptas

we protect identities.

cryptas.com . prime-sign.com . cryptoshop.com
Vienna | Graz | Düsseldorf | Stockholm

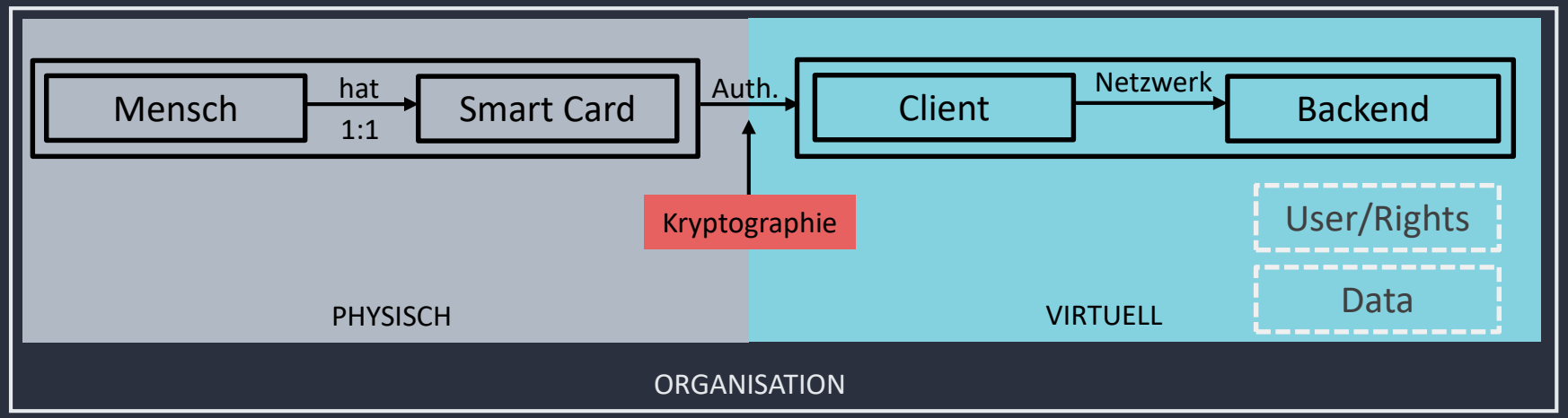
Modern Alternatives?

Mobile, TPM, VSC, FIDO, WH4B…?

CRYPTAS IT-Security GmbH
Franzosengraben 8 . 1030 Wien . Austria . **T** +43 (1) 3 555 3 - 0 . **E** info@cryptas.com

cryptas
we protect identities.

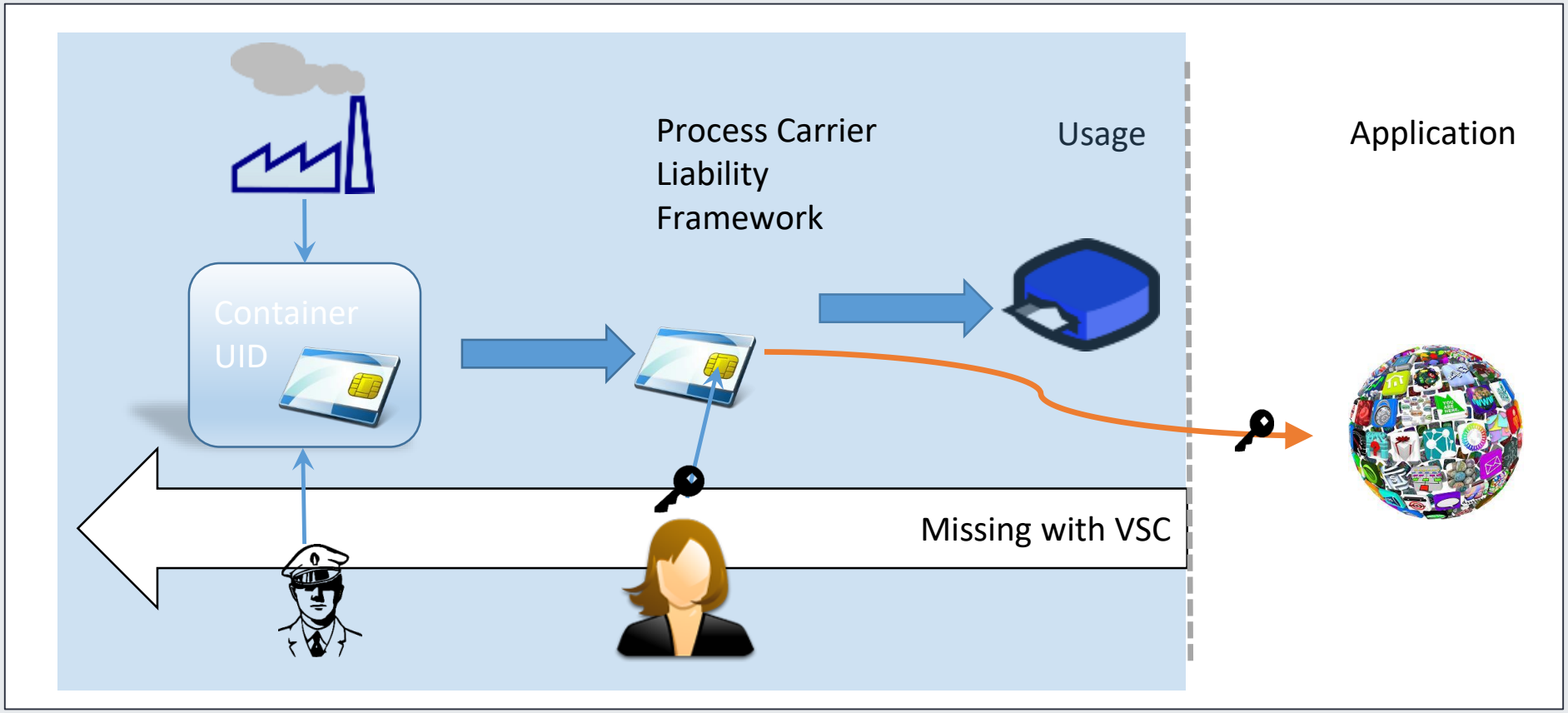
Why Smart Cards – Traditional View



CRYPTAS IT-Security GmbH
Franzosengraben 8 . 1030 Wien . Austria . T +43 (1) 3 555 3 - 0 . E info@cryptas.com
cryptas.com . prime-sign.com . cryptoshop.com
Vienna | Graz | Düsseldorf | Stockholm

cryptas
we protect identities.

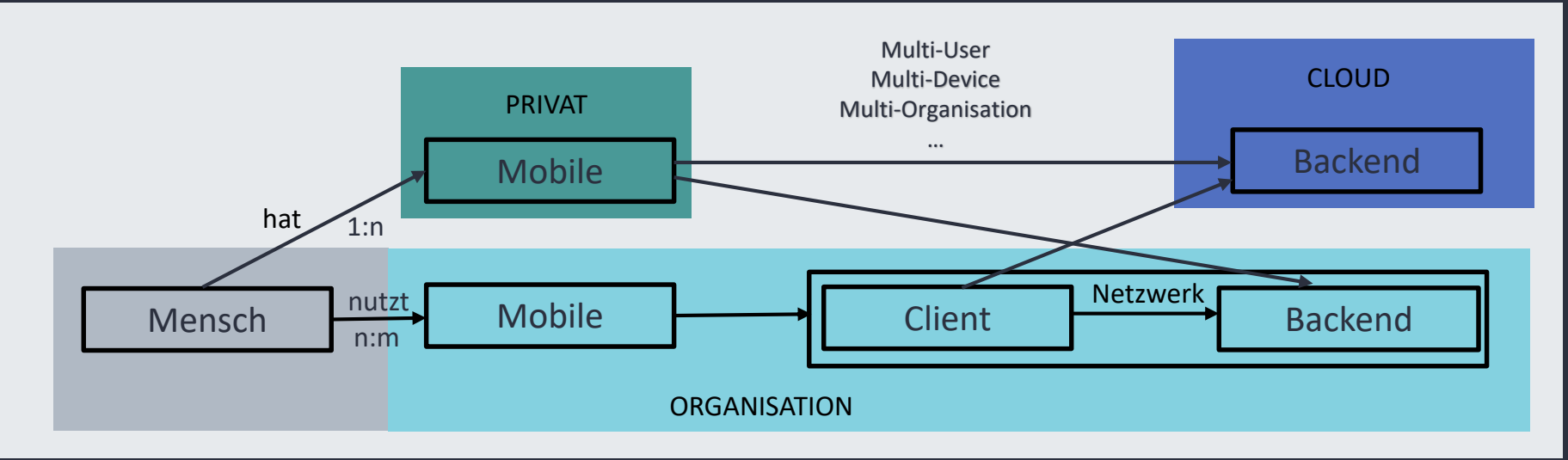
Physical Smart Card compared to virtual ones



CRYPTAS IT-Security GmbH
Franzosengraben 8 . 1030 Wien . Austria . **T** +43 (1) 3 555 3 - 0 . **E** info@cryptas.com

cryptas
we protect identities.

New Goal - Mobile Authentication/Virtual Card?



Transformation des Zugangsschlüssels

CRYPTAS IT-Security GmbH
Franzosengraben 8 . 1030 Wien . Austria . T +43 (1) 3 555 3 - 0 . E info@cryptas.com
cryptas.com . prime-sign.com . cryptoshop.com
Vienna | Graz | Düsseldorf | Stockholm

cryptas
we protect identities.

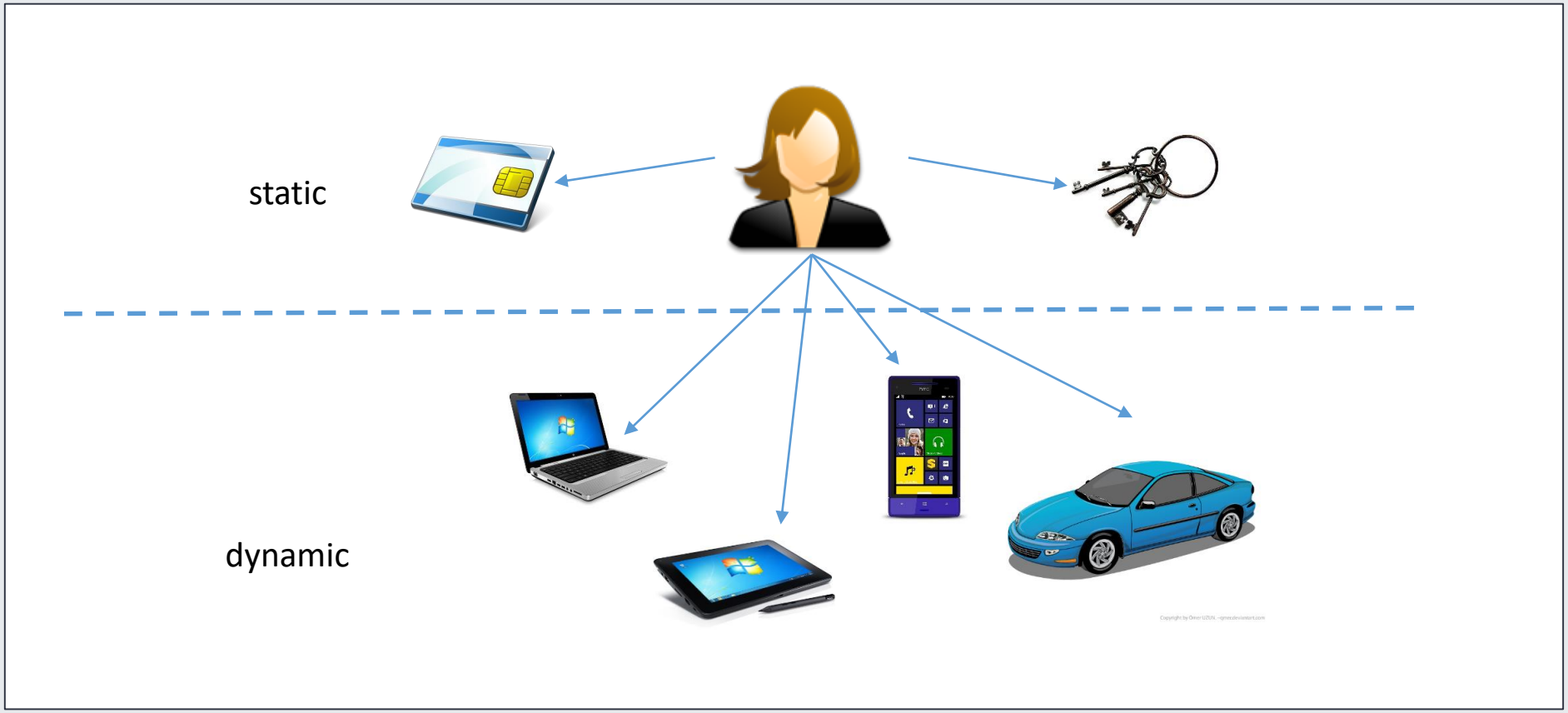
Virtual Smart Card on Mobile as replacement?

CRYPTAS IT-Security GmbH
Franzosengraben 8 . 1030 Wien . Austria . **T** +43 (1) 3 555 3 - 0 . **E** info@cryptas.com

cryptas

we protect identities.

Challenge: Multi-Device.

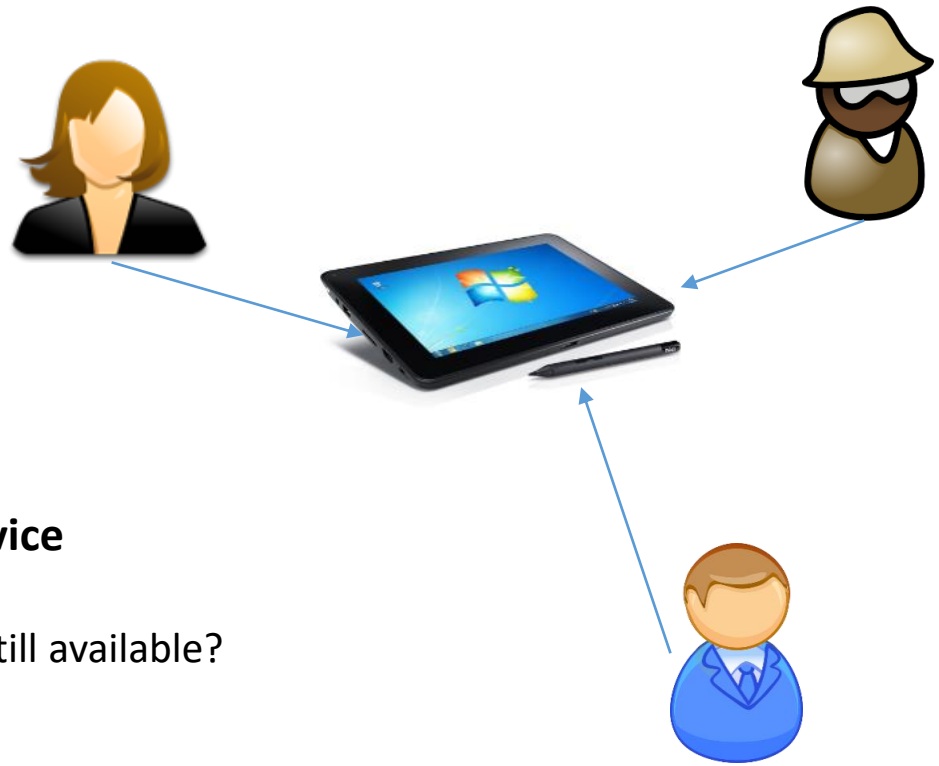


CRYPTAS IT-Security GmbH
Franzosengraben 8 . 1030 Wien . Austria . **T** +43 (1) 3 555 3 - 0 . **E** info@cryptas.com

cryptas

we protect identities.

Challenge: Multi-User.



n to 1 relation : User / Device

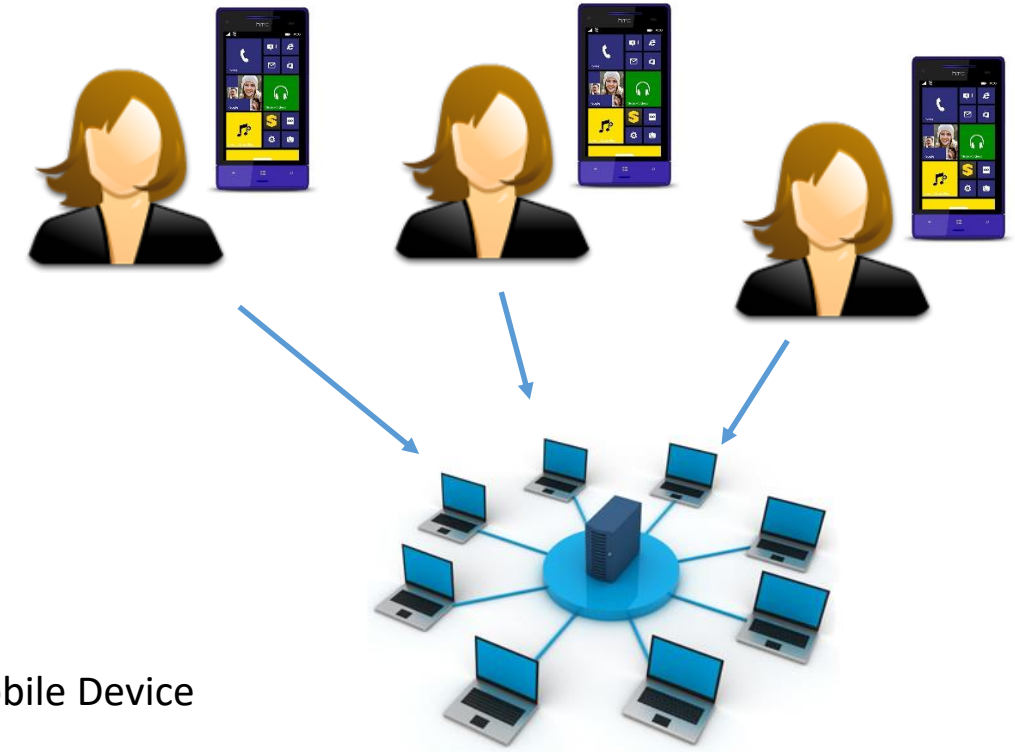
- Additional factor for VSC still available?
- Smart Card / NFC ?
- Smart Card / OTP Reader

CRYPTAS IT-Security GmbH
Franzosengraben 8 . 1030 Wien . Austria . **T** +43 (1) 3 555 3 - 0 . **E** info@cryptas.com

cryptas

we protect identities.

Challenge: Multi-User & Multi-Device.



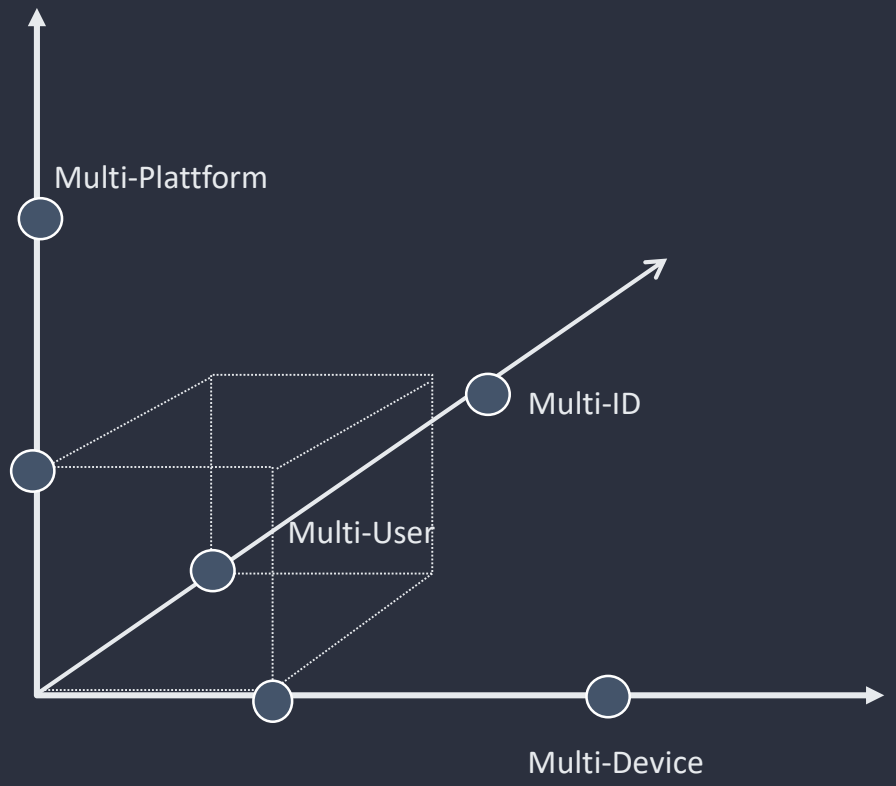
Virtual Smart Cards in VDI Environments

- Identification / Authentification?
- Smart Card /Mobile Reader
- Smart Card OTP to registered Mobile Device

CRYPTAS IT-Security GmbH
Franzosengraben 8 . 1030 Wien . Austria . **T** +43 (1) 3 555 3 - 0 . **E** info@cryptas.com

cryptas
we protect identities.

System complexity dramatically increased!



CRYPTAS IT-Security GmbH
Franzosengraben 8 . 1030 Wien . Austria . **T** +43 (1) 3 555 3 - 0 . **E** info@cryptas.com

cryptas
we protect identities.

Conclusio – Practical Security of the Cryptosystem

+ Mathematical Security

+ Quality of Implementation

+ Quality of Enrollment

+ Quality of Key Storage

+ Quality of the application of the keys

+ Quality of Life-Cycle-Management

→ The weakest Link determines the result

CRYPTAS IT-Security GmbH
Franzosengraben 8 . 1030 Wien . Austria . **T** +43 (1) 355 53-101 . **E** info@cryptas.com