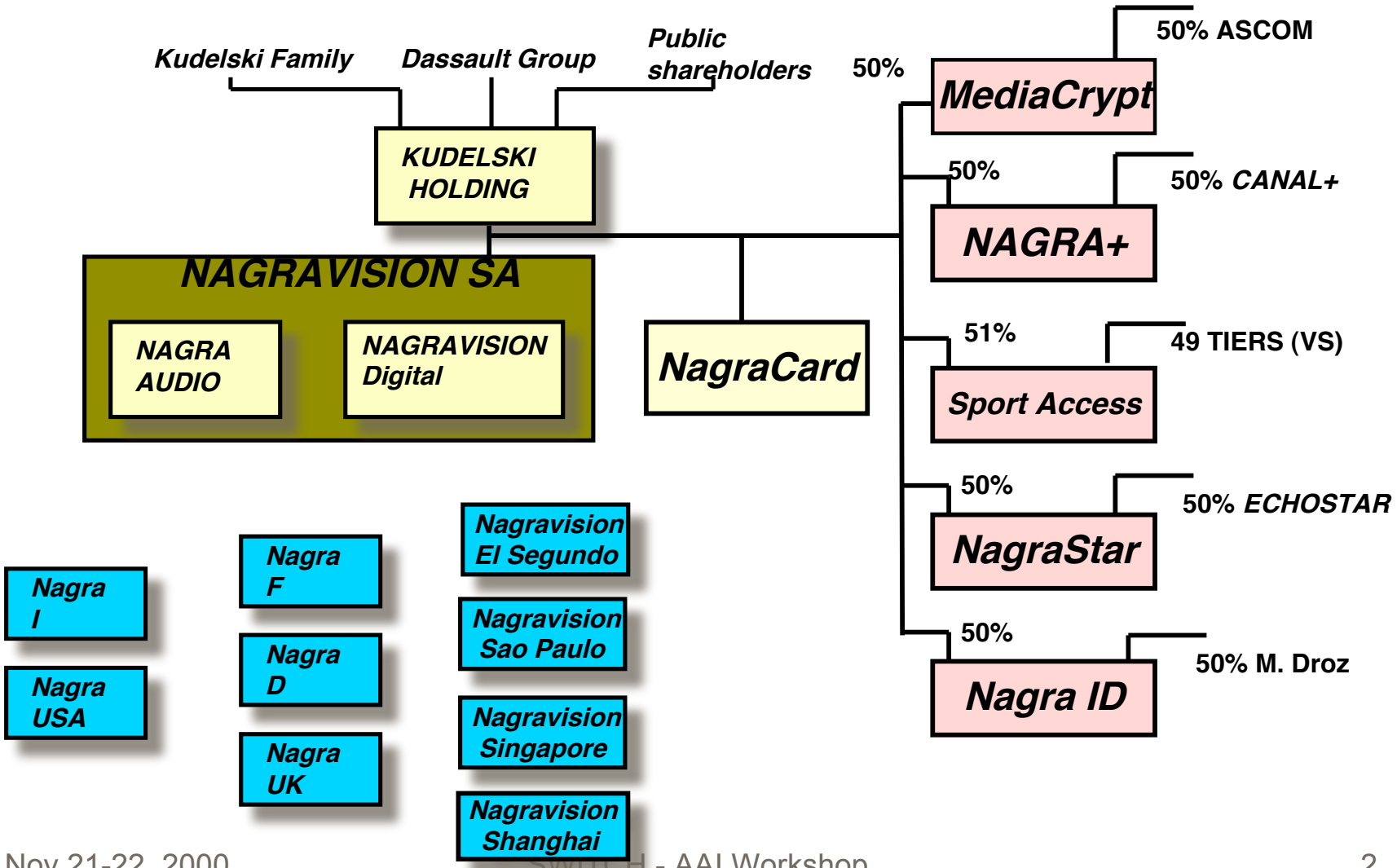
Nagra

The Smart Card Architect

nagra.com

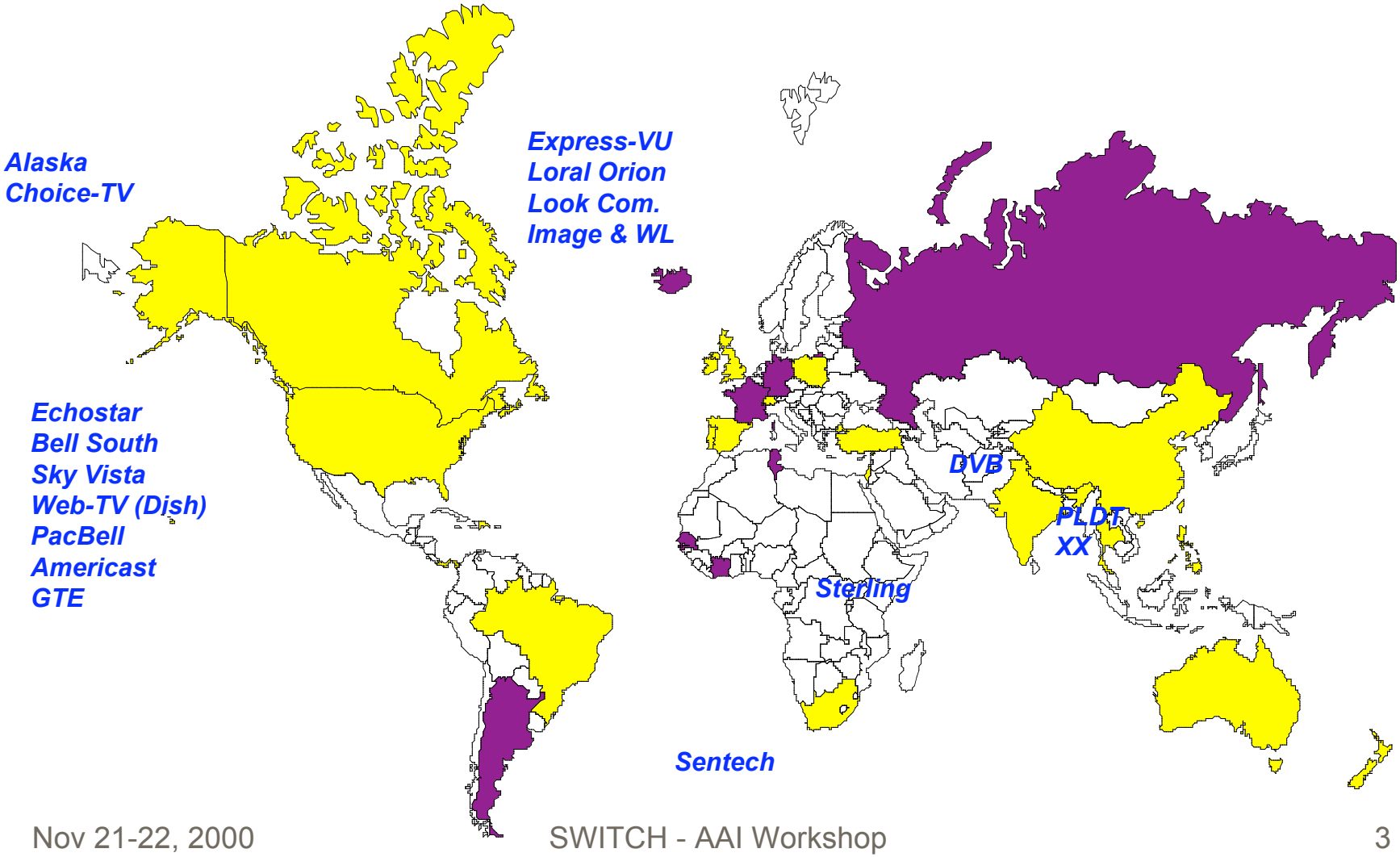
Kudelski Group Structure

Nagra
The Smart Card Architect



Presence Worldwide

Nagra d
The Smart Card Architect



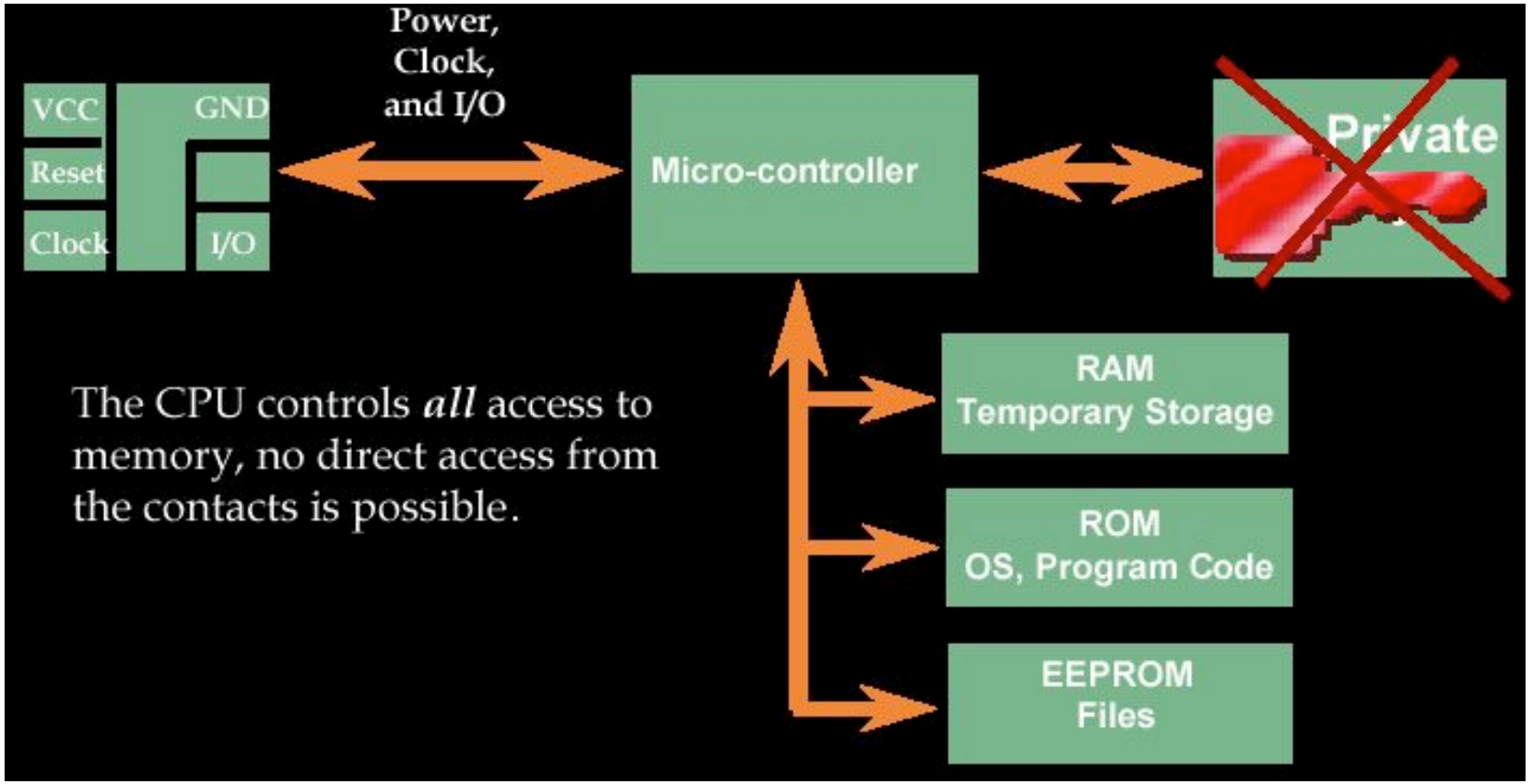
Pay-TV, did you know it's PKI ?

Nagrard
The Smart Card Architect

- Pay-TV systems installed worldwide
  - 22 millions customers
  - pay-per-view
  - electronic purse
  - Internet
- Managed and secured with a very high proprietary secured PKI solution
  - based on a smartcard

Microprocessor based smart card

Nagrard
The Smart Card Architect



Smart Cards and PKI

Nagrard
The Smart Card Architect

- Smart cards are «certificate wallets»

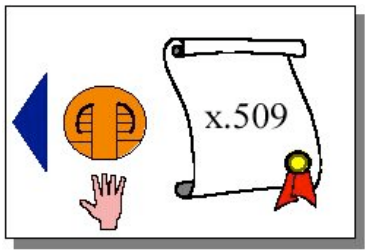
- Secure storage for:
  - Owner private key
  - Trusted root certificates
- Smart Cards are a «PC-in-your-Pocket»
  - Generation of owner's digital signature
- Smart cards provide:
  - Mobility
  - Security
  - Transparency
  - Issuer branding, loyalty

Digital ID

Nagrard
The Smart Card Architect

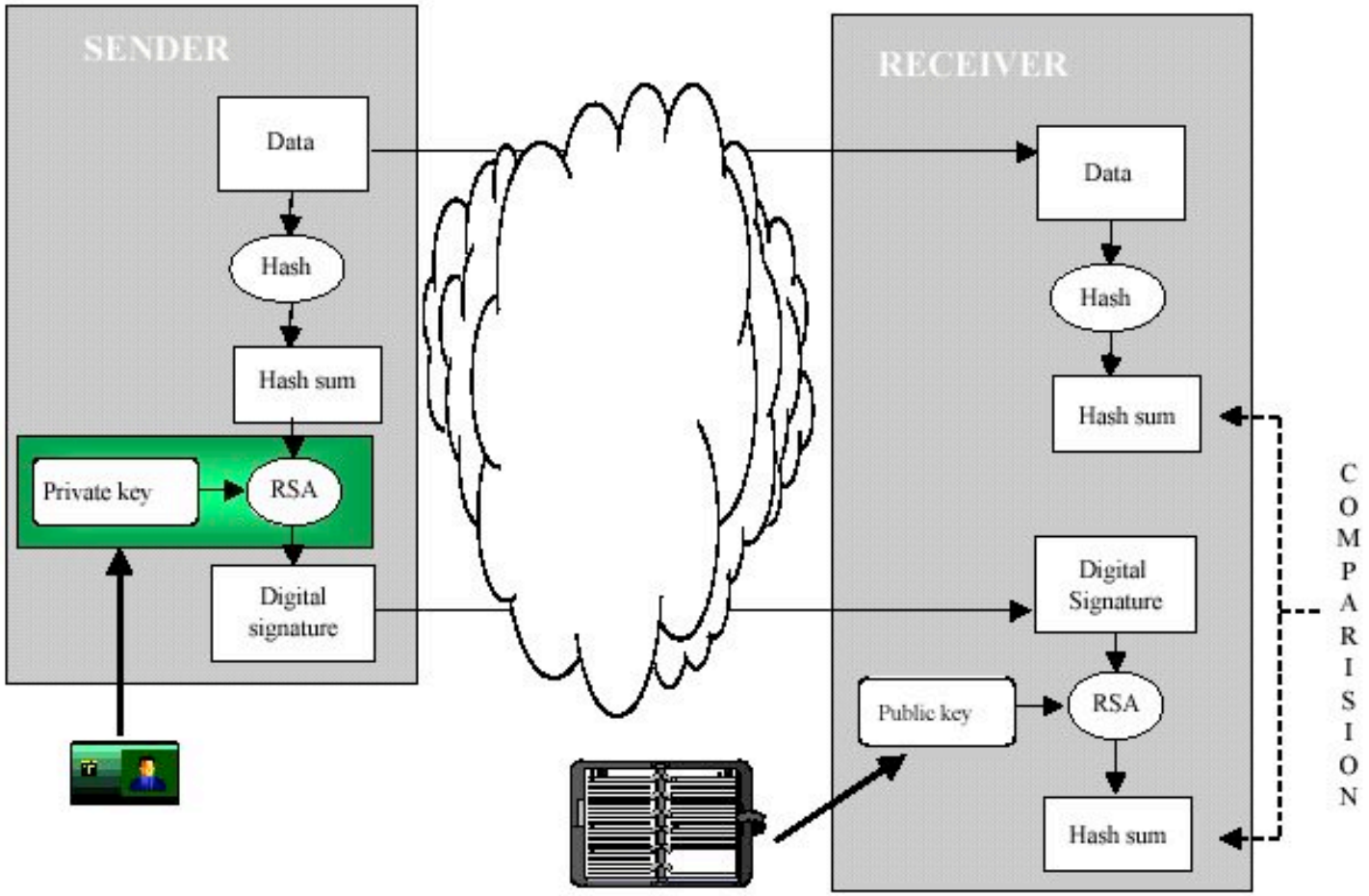
- Asymmetric key-pair
  - public key
  - private key

- X.509 certificate
  - ISO standard
  - public key
  - credentials



Smart card application example: Digital Signature

Nagra d
The Smart Card Architect



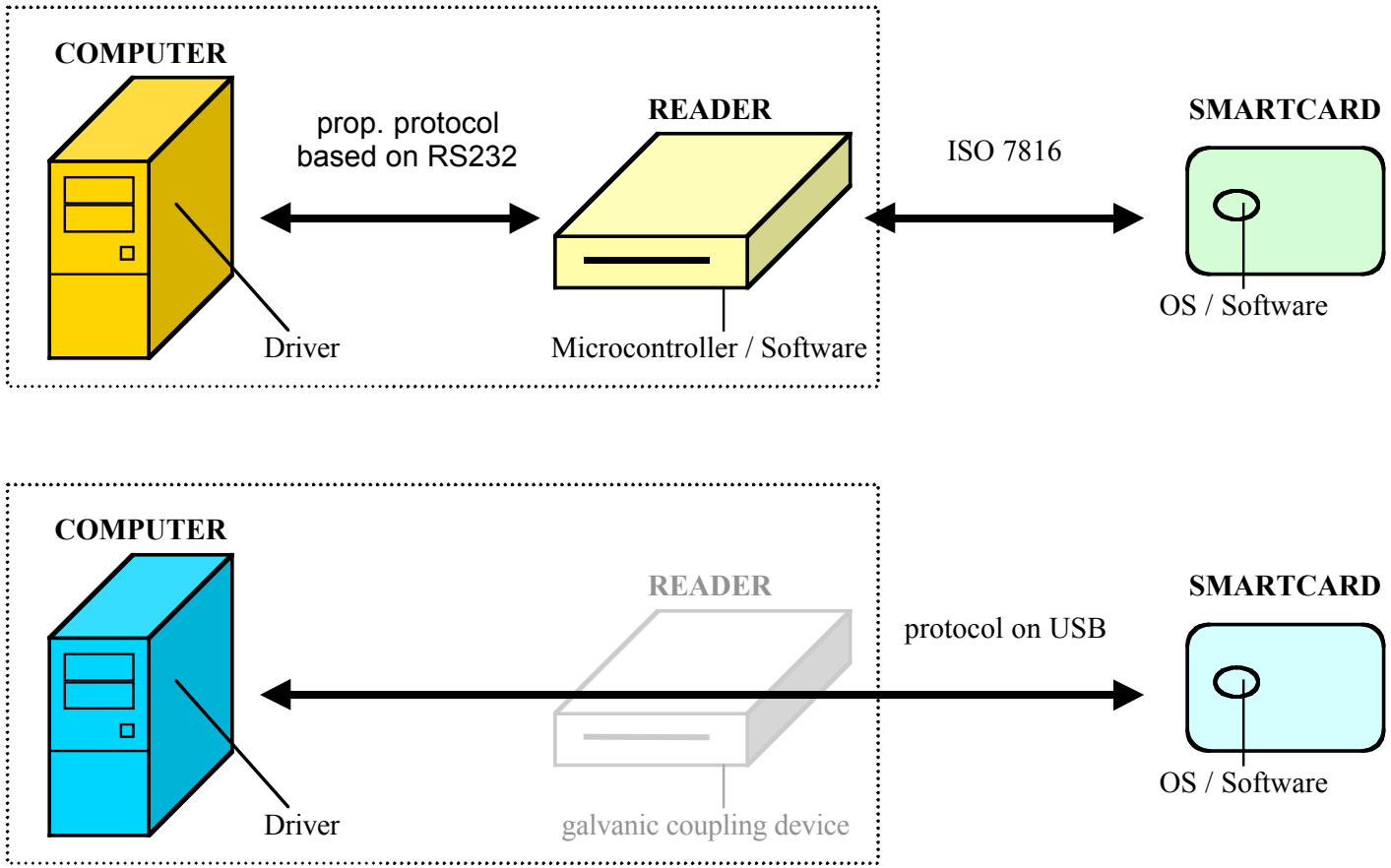
Smart card in heterogeneous environments

Nagrard
The Smart Card Architect

- Smart cards need readers and drivers
- Readers
  - desktop or embedded (keyboard, floppy slot)
  - optional display and keypad
  - PC world ready for installation
  - Mac, Unix & Linux 'waiting' for USB
- Drivers
  - PC/SC standard for Windows PC
  - custom developments

ISO 7816 vs USB

Nagrard
The Smart Card Architect



Certificate Portability: Smart Cards Holding Certificates

Nagrard
The Smart Card Architect

- Pros
  - Tamper-proof device
  - Portable
  - Visible security/theft indicator
  - Upgradeable
  - Branding, Photos,Mag-stripe
  - Biometric cards, readers coming
- Cons
  - More expensive than a pure software solution
  - infrastructure
  - Standards issues
  - Multi-application issues

NagraCard solution

Nagra
The Smart Card Architect

- Based on knowledge of massively-deployed smart card based system management in Pay-TV
  - Nagravision is the #1 player in digital TV, and is an independent company
  - More than 20 millions of smart cards delivered and operating
- NagraCard thinks security at system level
  - To secure the overall security
  - To avoid a breach in the chain
  - To strengthen each element security

Our Mission

Nagrard
The Smart Card Architect

- Smart card architect
  - Security solutions & services
- Smart card R&D
  - Secured and reliable smart card operating systems and applications
- Our approach
  - audit
  - architecture, security
  - implementation

Contact

Nagra
The Smart Card Architect

NagraCard S.A.
Kudelski Group
Route de Genève
CH-1033 Cheseaux

Tel. **+41 21 732 05 60**
Fax **+41 21 732 05 61**
E-mail: **nagracard@nagra.com**
Web-site: **www.nagra.com**