



# Contactless: The interface of choice for 21st century electronic ID

Rolan Jahn

Segment Marketing Manager eGovernment Solutions

Business Line Identification

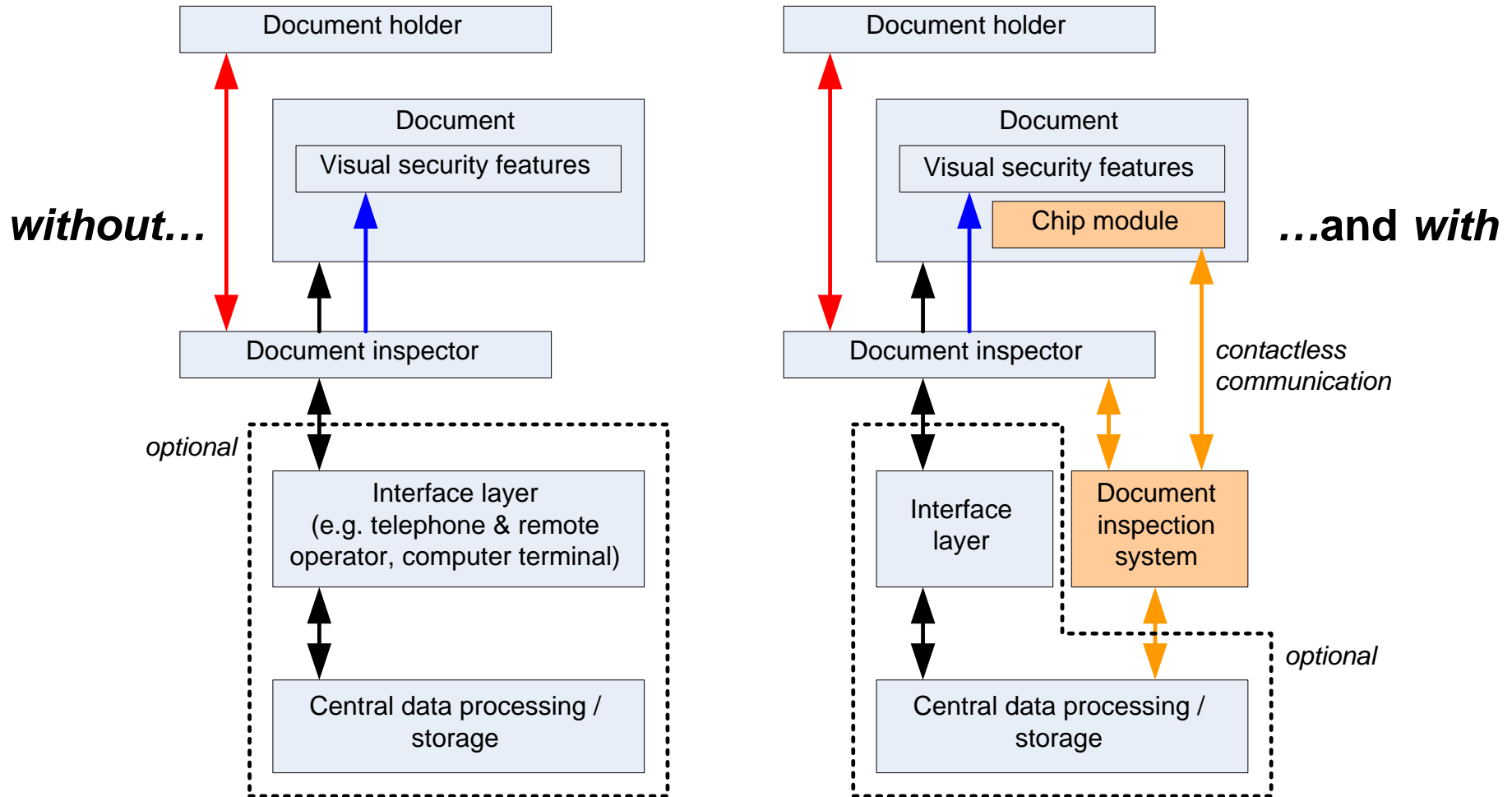
23 September 2008



# Contents

- ▶ Comparison Conventional vs. Electronic ID Schemes
- ▶ Technology Comparison
- ▶ Capabilities of Contactless Technology
- ▶ Security & Privacy with Contactless Technology
- ▶ Contactless Technology - Trends
- ▶ Summary

# Conventional vs. Electronic ID



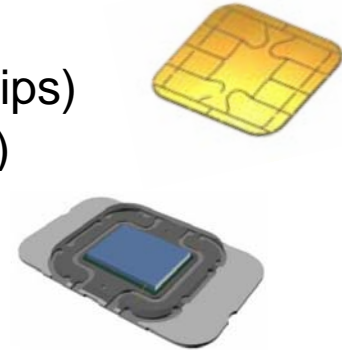
# Conventional vs. Electronic ID (cont.)

- ▶ What does an eID scheme mean on the system level?
  - Issuer benefits
    - Security against document fraud and falsification
  - Inspection process benefits
    - Added security by second inspection path (1st = visual inspection)
    - Second inspection path is bi-directional, active communication
    - Inspection process could potentially be automated
  - Holder benefits
    - control over my data, as they are only on the document I hold (as compared to database solution)
    - Quicker and more reliable inspection process – the inspection agent will bother me less if he has more trust in my identity document
    - Faster inspection time if automated
    - Option to use in the virtual world with home PC-based reader (I can authenticate to the taxpayer internet portal; can prove my age to an online service; ...)



# Technology Comparison

- ▶ Available technologies for electronic identity documents
  - Contact (ISO 7816)
  - Hybrid (ISO 7816 and ISO 14443 as two separate chips)
  - Dual (single chip supporting ISO7816 and ISO14443)
  - Contactless (ISO 14443, ISO 15693)
- ▶ Additional options (future outlook)
  - Display (single shape, dot matrix, graphical display)
  - Input element (type your PIN into the card)



# Technology Comparison (cont.)

		Secure IC in module			Inspection system	
		Contact ISO7816	Dual ISO7816 + ISO14443	Contactless ISO14443	Contact ISO7816	Contactless ISO14443
reliability	Humidity	Contact pad corrosion	Contact pad corrosion	Completely encapsulated	Contact finger corrosion	Completely encapsulated
	Dust	Contact pad abrasion	Contact pad abrasion	No mechanical contact	Contact finger abrasion, dirt	No mechanical contact
	Maintenance				Replace contact fingers, cleanse	No maintenance required
	Convenience				Card / document not visible during reading	Card / document visible at all times
	Integration effort		More complex SW solution required			
	Data rate	Limited by standard ISO7816 – proprietary solutions exist	Up to 848 kbit/s	Up to 848 kbit/s		Up to 848 kbit/s

# Technology Comparison (cont.)

## HF vs. other contactless

- ▶ Nominally, it is just different features
  - ISO14443: proximity coupling = 10cm read distance
  - “other” (ISO15693; 915MHz; ...) = 1m read distance and more
- ▶ The system view shows completely different approaches
  - Proximity coupling (<10cm, ISO14443):
    - Place a document directly next to a reader device and wait for reading (1-10 seconds)
    - Requires conscious act on behalf of document holder
    - 2..145 kbyte of data read from device memory
    - Document provides the actual data storage; no need for central database
    - Classical concept – **identity is defined by what is on and in the document**
  - Vicinity coupling (>>10cm):
    - Document is scanned quickly from the distance (e.g., from a signage bridge above a road)
    - Document holder may not be aware of reading process
    - Power supply from electromagnetic field **very** limited
    - Few bytes of data read from device memory (just about enough to read a single number)
    - No strong encryption possible due to lack of energy (therefore, no sensitive data)

# Capabilities of Contactless Technology

- ▶ Data retention in EEPROM memory  
up to 20 years / 500.000 erase-write cycles
- ▶ Transaction times of several seconds, depending on system choices
  - **Example A:** 4 kB of data, unencrypted transmission, no authentication (“open access”) – 1 second
  - **Example B:** 50 kB of data, transmission encrypted by triple-DES, EAC – 7 seconds
- ▶ Memory sizes between 2 and 145 kbyte
- ▶ Highly sophisticated cryptography co-processors (HW accelerators)
- ▶ Very mature security features (fourth+ generation of design and third-party security certification testing)
- ▶ ...and much more

# Security & Privacy with Contactless Technology

## Privacy concerns

- ▶ Distinguish between two cases
  - Activating a document – limited to about 0.3m distance
  - Eavesdropping on communication – limited to about 3m distance
- ▶ The *eavesdropping* threat –  
“*can anybody’s eID be read from a distance?*”
  - ISO 14443 devices are coupled through the magnetic field
  - Large distances (e.g., meters) require large powers or large loop antenna diameters
  - The loop antenna of the eID document needs to be aligned with reader antennas – turn the document by 90° and the connection breaks down
  - To read a document, the connection must be stable for several seconds

# Security & Privacy with Contactless Technology

## Privacy concerns

- ▶ The risk of eavesdropping is very low
  - Eavesdropping equipment would be big and clunky, has to be well aligned and move with the target
  - ... beware of men with large trunk suitcases?
  - Need to analyze each situation and physical setting for eavesdropping risk
  - Protocol can protect you (e.g.: BAC requires to read printed text from the ePassport to set up a link)



# Security & Privacy with Contactless Technology

## Hardware and Protocol Security

### ▶ Hardware security

- *Smart card processors are not RFID tags* – lots of built-in security features
  - Sensors for e.g. light, temperature, voltage supply anomalies etc.
  - Active shielding and an “edited” topology to disguise certain features
- Processors are security certified by independent third parties (e.g. Common Criteria certification)
- Dedicated, high-performance cryptography coprocessors separate from CPU core

### ▶ Protocol security

- ISO7816-4 offers various standard commands for secure authentication between reader and electronic document (*how to communicate data*)
- Cryptographic algorithms (*what to do with the data*) can be freely chosen by the implementer
- Example: ePassport with BAC or EAC
  - BAC: mutual authentication and encrypted communication, key seeds derived from MRZ data
  - EAC: BAC with additional secret key authentication for some files (biometric data: fingerprints)



# Contactless Technology - Trends

- ▶ Shorter transaction times
  - ...by more powerful processor cores
  - ...by optimized cryptography coprocessors
  - ...by higher transmission data rates (up to 8x)
- ▶ More space for data and applications
  - By Larger non-volatile memory sizes
- ▶ Thinner package types, chip-in-paper, printed loop antennas
  - more space for other security layers in document
  - less specialty materials, more paper-like
  - mechanically more reliable documents
- ▶ Documents with integrated displays
  - Additional, isolated communication channel to document enables new security features (e.g. display one-time passwords, online banking TANs, PACE options...)



# Contactless *is* the interface of choice for 21st century electronic ID

- ▶ Broad range of technology options is available, products are mature
- ▶ Turning Documents into eDocuments offers higher security and additional benefits to document issuer, inspector and holder
- ▶ For eGovernment applications, ISO14443 (proximity coupling, <10cm) is the technology of choice
- ▶ Privacy concerns exist and are healthy – citizens are right to question their governments about data security
  - Technology in itself is very safe – “secret reading” is an unlikely threat
  - Humans are the weakest link – *organization decisions are the key to secure systems*
- ▶ Future technology developments will make contactless technology even more attractive
  - eDocuments will become more “natural”
  - New holder features will become available



