



California Research Bureau RFID Hearing

Sacramento, CA October 31, 2007

Joerg M. Borchert
VP Chip Card & Security ICs



Never stop thinking



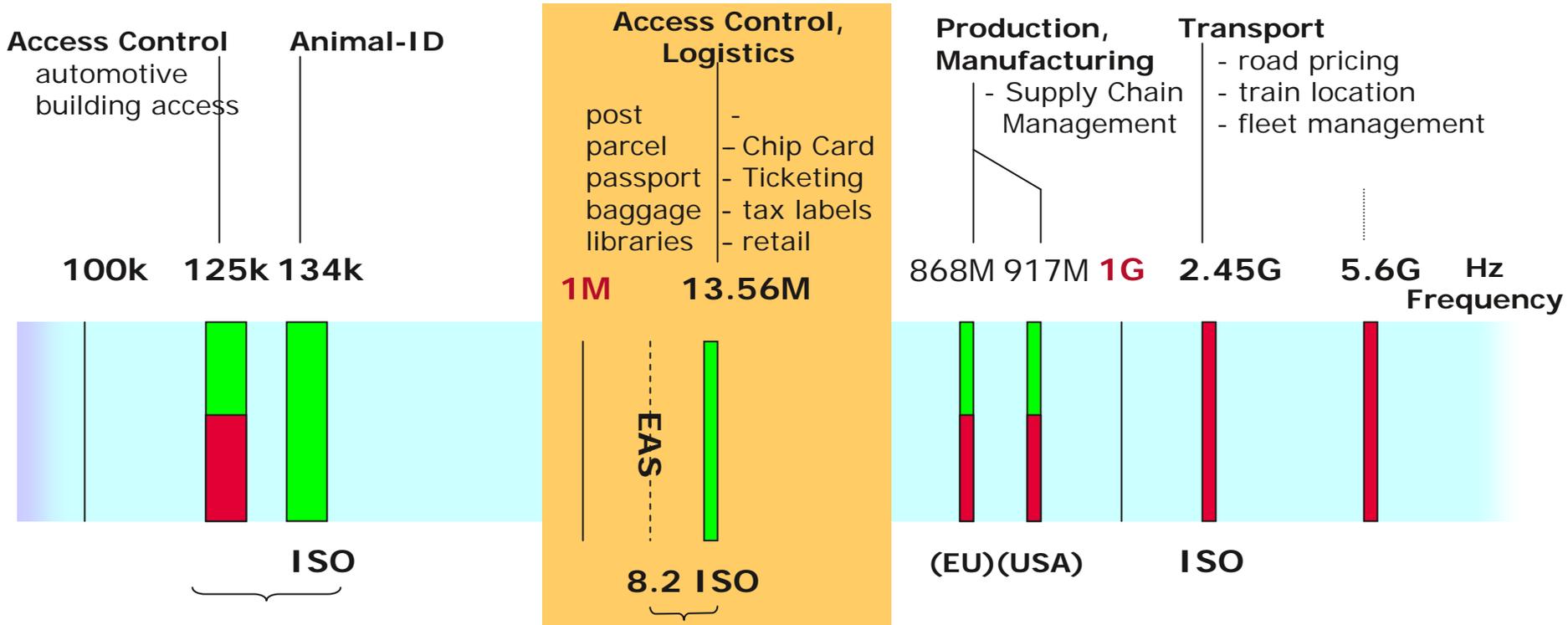
Many types of RFID Technologies



- To discuss RFID technology is the wrong approach
- It is about RFID TECHNOLOGIES, there are many of them
- You can NOT compare a tag for cow with an identity credential/Geneva convention card for a US soldier in the field (which also allows him to access secured IT)



Secure-RF Applications and Frequency Bands



Secure RF applications are based on 13.56Mhz



active tags

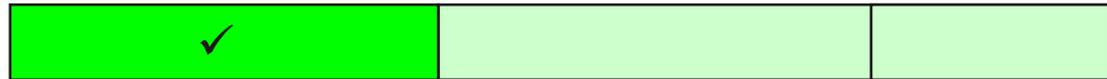


passive tags

Established Standards:



Secure Microcontrollers

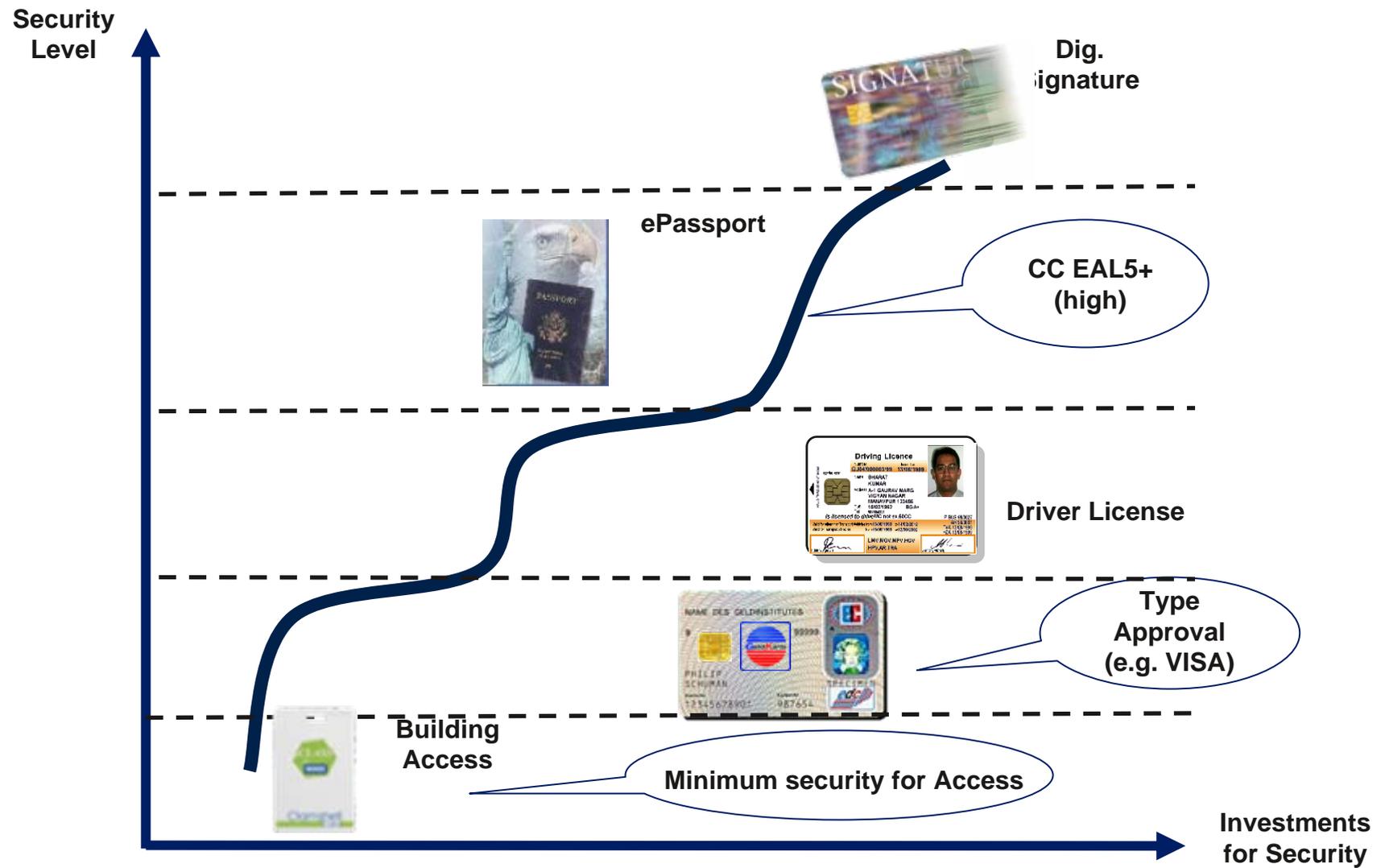


Secure Memory ICs



Digital Signature Requires the Highest Security

Different Applications Require Different Levels of HW Security





Evolution of security in Identification documents

- Fraud has been and will be a real threat
- Raising the bar against adversaries is a constant race
 - Criminals
 - Terrorists
- Innovation in ID document security
 - Signature – secure paper – secure ink/ printing – picture – watermarks – holograms – laser engraving – 2D/ 3D barcode
- Latest innovation: RF security controllers binding biometric identifier electronically to picture on ID of the holder – limits fraudulent production and use of legitimate IDs.
- An identification document has to establish **trust** with the card holder for it to be an effective tool

RF enabled ID Cards: Vulnerabilities and Countermeasures



Potential Vulnerability	Impact	Solution
➤ skimming/ eavesdropping	➤ Man in the middle attack	➤ Basic Access Control Communication Encryption
➤ cloning	➤ Content duplication	➤ electronic signature of content and secure chip technology
➤ replay/ relay	➤ Data collection	➤ one time session key
➤ tracking/ hot listing	➤ Privacy violation "Enemy of State fear"	➤ random chip ID = change at every time used
➤ read range (design dependant)	➤ Data collection	➤ distance is technology dependent Tracking vs. Security

The US Electronic Passport a multi level security approach



➤ Problem

- Fraudulent passports

➤ Impact

- Adversaries can obtain US or 27 visa waiver false travel document
- **Trust** in passport started to erode

➤ Solution

- World wide standardization in ICAO
- Bind first time in history document biometric information (picture) electronically to a contactless security chip
- Listen to the public and introduce shielding to cover privacy concerns

Printing Technology		Electronics Manufacturing	
DESIGN	MATERIALS	DESIGN	PROCESS
Classified Design Software	Embedded Security Threads	Encryption	Secure Physical Plant
Gilloche Pattern	Watermarks	Access Control	Serial Number Tracking
Microprinting	Color-Shifting Ink	Secure Integrated Circuit	High Material Control
Intentional Spelling Errors	Penetrating Ink	Secure Operating System and Applications	Secure Supply Chain
Intaglio			Trusted Vendors

Source: US Government Printing Office

- **Cryptographic Security**
 - Randomized chip serial #
 - Chip data encrypted
- **Physical Security**
 - Shielding
 - New printing features
- **Production Security**



Motivation for eDriver License / ID cards

➤ Problem

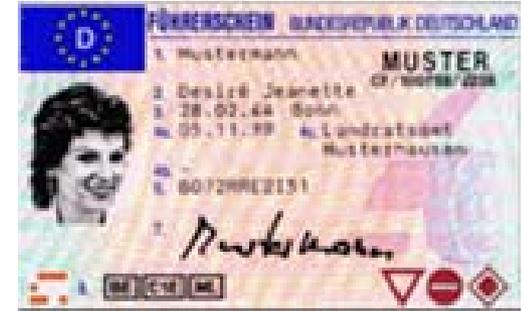
- Fraudulent driver license / ID cards

➤ Impact

- ID theft
- Unlawful social benefits
- Insurance fraud

➤ Solution

- Prevention of counterfeiting & fraudulent documents
- Protection of privacy of drivers (e.g. Japan)
- Streamlining of administration efforts
Optional: Capability for further applications
- Optional: Harmonization (e.g. in India)
- Optional: robust document, compact size
- Optional: Driver's License is the current ID document (e.g. in UK)



(Layout example: Germany)



(Layout example: Japan)



Closing Remarks and Questions

- There is no absolute security in any kind of ID, but there is BETTER security
- Societies/communities need to stay ahead of the bad guys
- The State of California and the chip industry are in the Trust business when it comes to ID documents
- From the economic viewpoint, securing IDs is an insurance model, a question of risk management.



QUESTIONS:

- Can CA allow itself to fall behind the curve by legislating the limits of technology innovation, and setting in stone standards for use in government ID documents?
- Is CA willing to close out the option for the most protected ID documents available?

Any Questions ?

Joerg M. Borchert
joerg.borchert@infineon.com
phone +1 408 503 5608
Fax +1 408 503 2914