PHILIPS

Security of Identification Products - how to manage?

CHES, Edinburgh, Sept.2005

Thomas Wille
Business Line Identification
Philips Semiconductors

About us

- Philips Semiconductors (5,500 M€ sales, 32,000 employees)

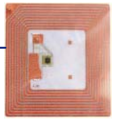
- Business Line Identification: we are in the ID business for about 10 years starting with
  - » car immobilizers
  - » smart cards for banking applications
- in both segments we are holding the No. 1 position

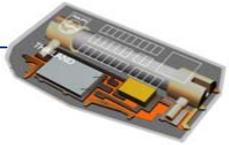
- our markets are:
  - » car immobilizers
  - » cards for public transport
  - » RFID tags
  - » RFID labels
  - » smart cards for banking, mobile com, payTV
  - » IC for passports
  - » Near Field Communication (NFC)
  - » reader ICs

- all segments in common are dominated by contactless interface technology

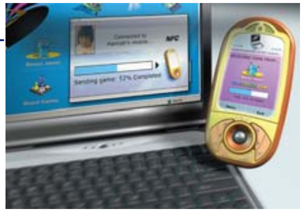
Identification products

- labels
- tags
- immobilizer





- banking cards
- SIM cards
- payTV cards
- public transport cards
- Near Field Communication (NFC)



- e-passport
- e-IDcards

- contactless
- contact

What is the purpose of ID - products?

- labels
- tags
- immobilizer

- identify objects or **rights on objects**

- banking cards
- SIM cards
- payTV cards
- public transport cards
- Near Field Communication (NFC)

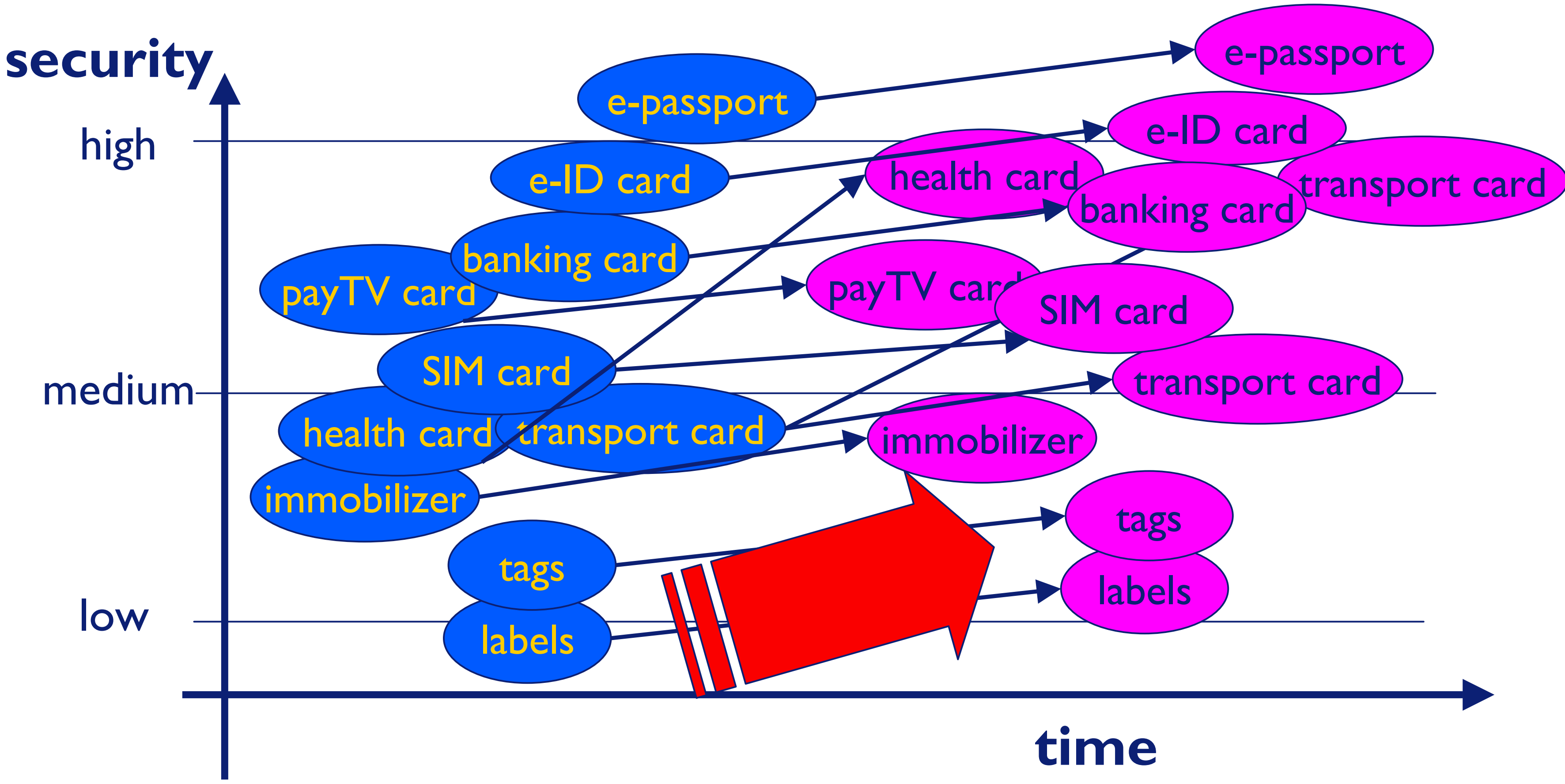
- access **rights to services**

- e-passport
- e-IDcards

- **persons rights**

- *contact?*
- *contactless?*

Evolution of Security Requirements



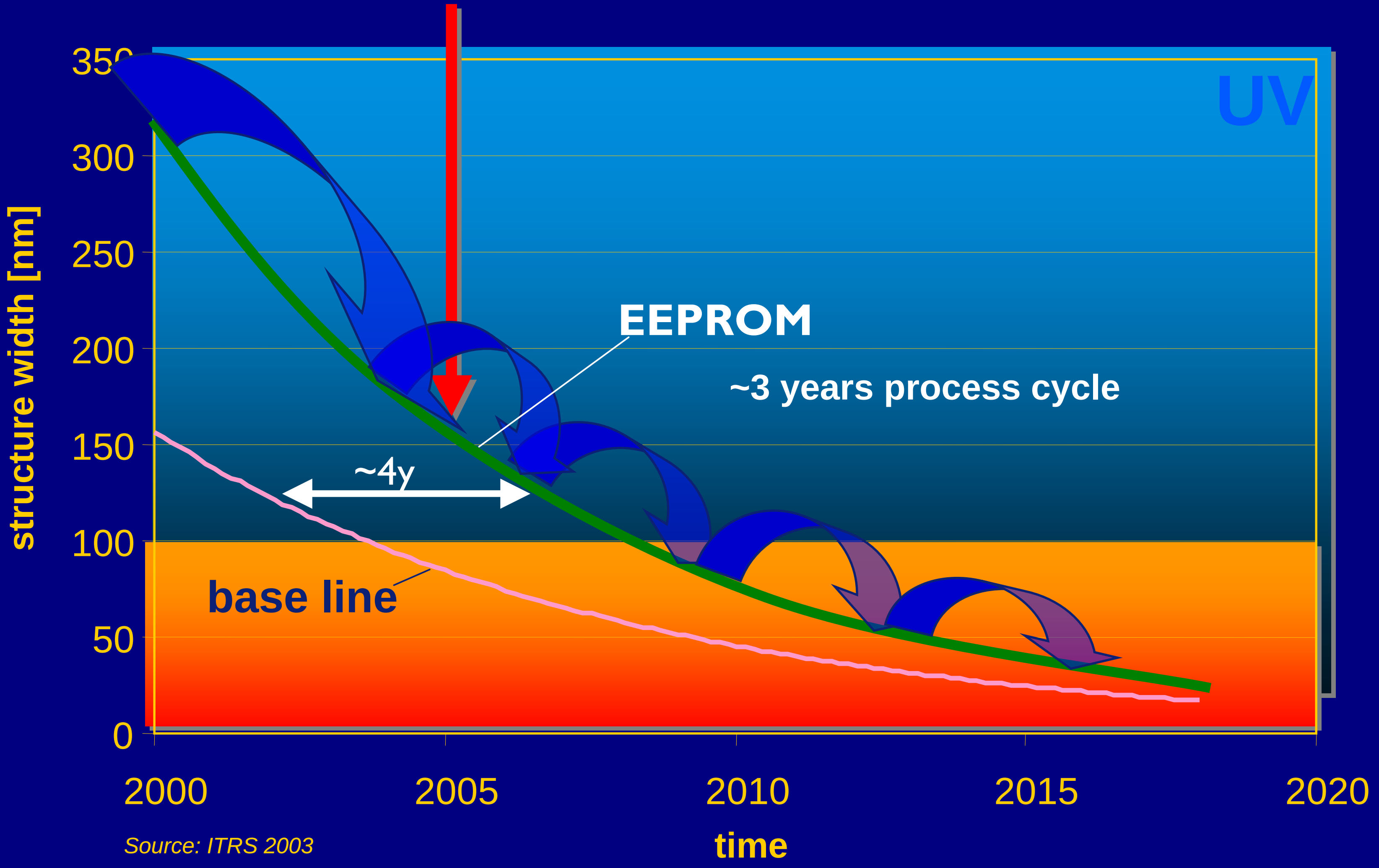
- **security requirements increase over time!**

Why does security increase over time?

- technology progresses in terms of complexity and miniaturization of structures
- features of analysis tools are growing along this trend as kind of pre-condition of technology development enabling smarter attacks

PHILIPS

ITRS – International Technology Roadmap for Semiconductors



Source: ITRS 2003

Security level of Hardware products

- the increase of security for hardware products can mainly be driven in synchronicity with silicon technology development
- This leads to nearly the same 2-3 years cycle time (reaction time) where silicon manufacturers are able to introduce significant changes in security designs

……. if there is a severe problem!!

- product lifetime is about twice the silicon cycle time →5 years
- new designs need to fulfill security requirements over their complete lifetime of up to 5 years
- **if we only can improve security significantly within the silicon cycle time –** which is far too long for timely reaction **– we need to find other methods to manage and enable state-of-the-art security in our products!**

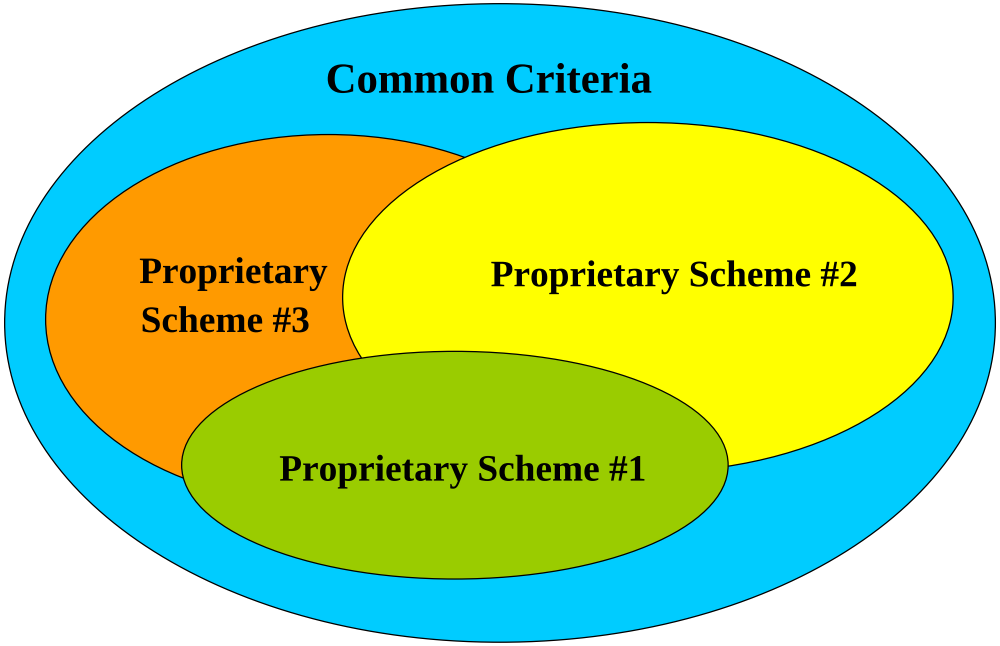
Is the security level of ID products too low?

- it depends!
- designers may underestimate the skills of hackers
- designers of security products may have a ‘blind spot’
- some people in the community suffer from ‘security paranoia'
- we sometimes recognize that not all security features provided by hardware are utilized in the operating software on system level

How to define security?

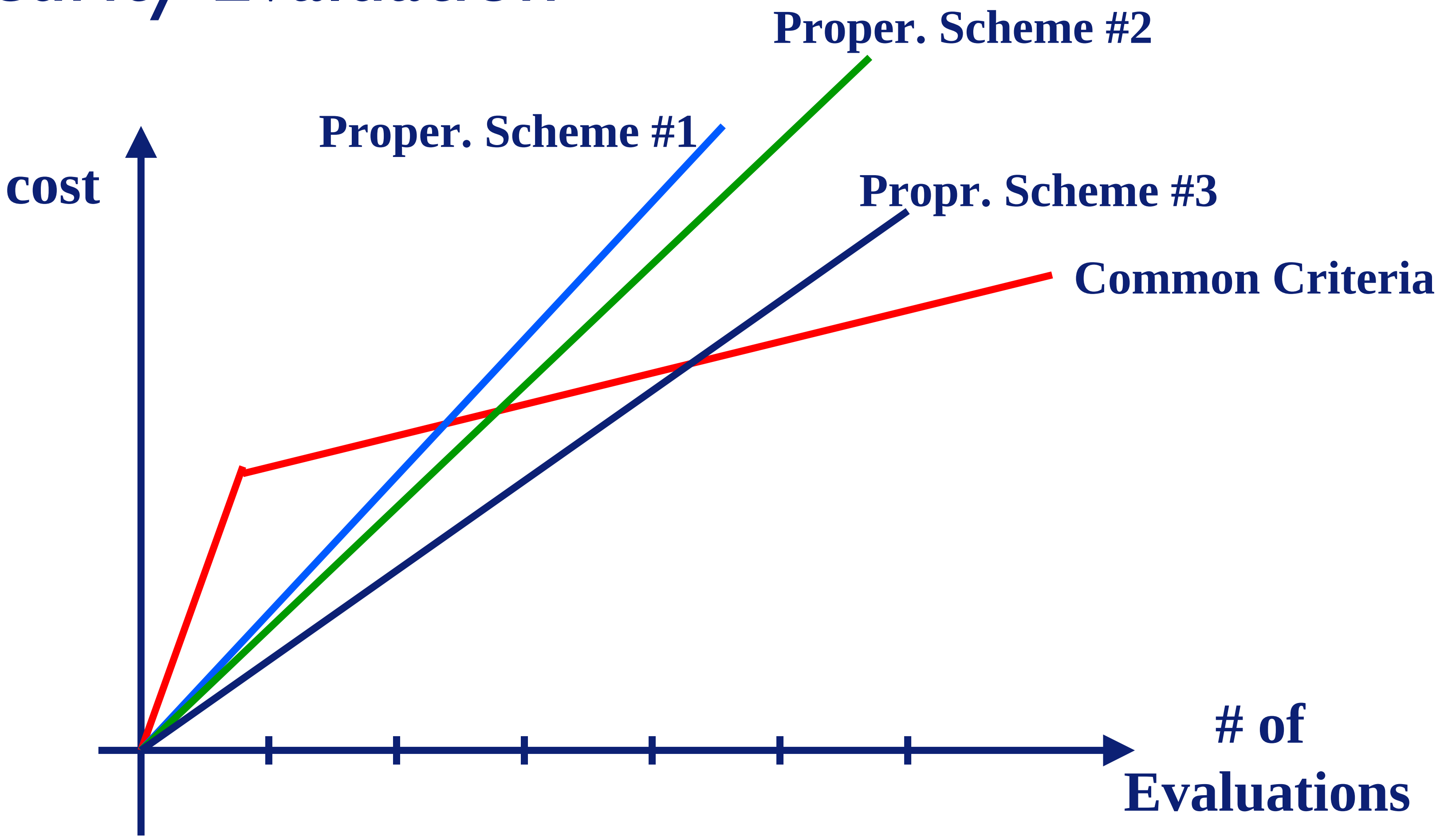
- ‘When I do a risk assessment of smart card use in banking applications I assume that the smart card is instantaneously broken without any effort’ - a banker, who must not be named (’96)
- The security level of products has to be
  ‘Fit for Purpose’
- obviously it was very difficult to define an appropriate security level for a product!

How to define security? Evaluation schemes



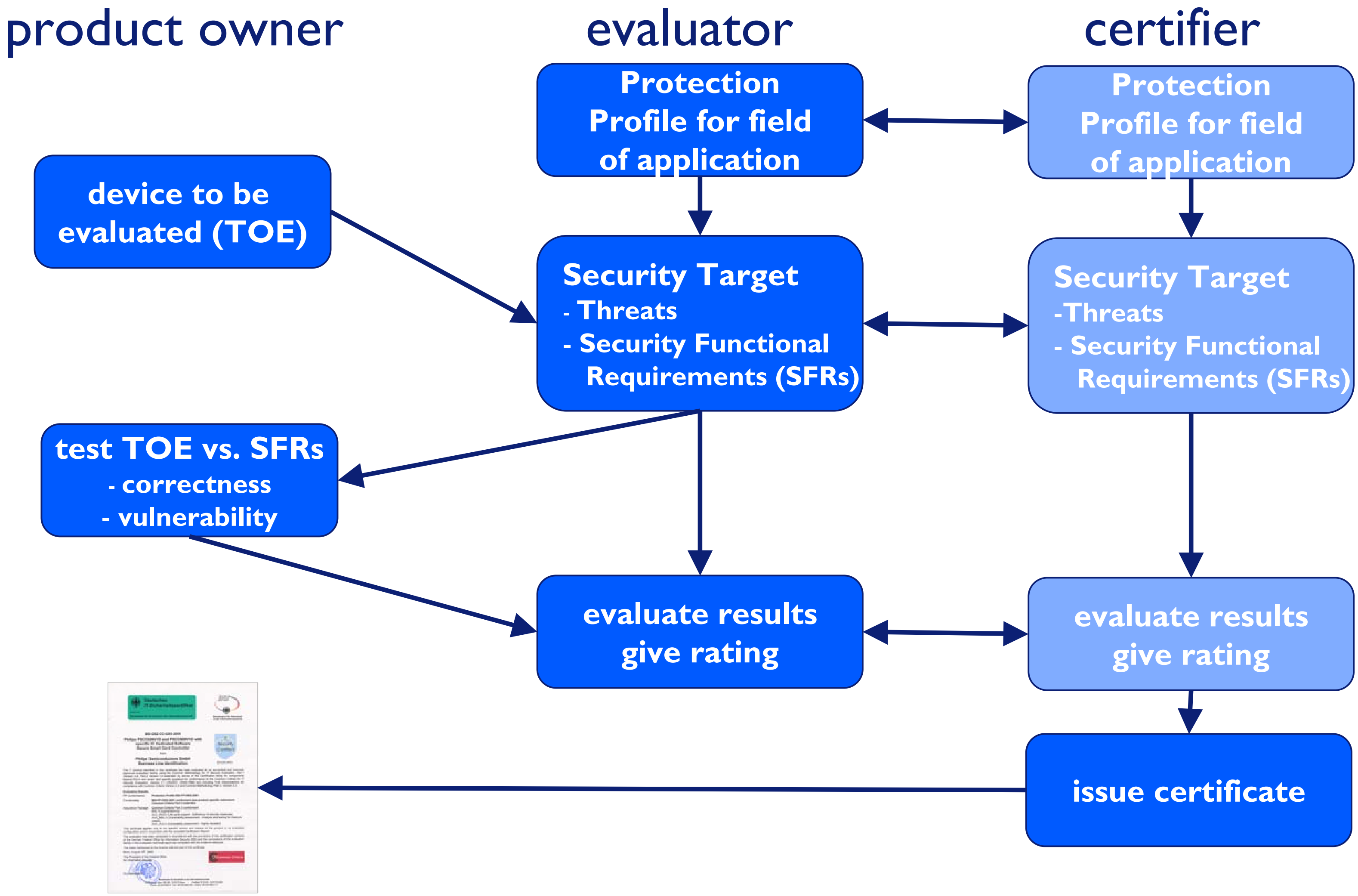
- CC covers all requirements
- modular in SW and HW
- re-useable
- combine new SW with av. HW

Security Evaluation



- **modularity and re-use of CC saves cost**

How does CC work?



product owner

evaluator

certifier

Protection Profile for field of application

Protection Profile for field of application

device to be evaluated (TOE)

Security Target
- Threats
- Security Functional Requirements (SFRs)

Security Target
-Threats
- Security Functional Requirements (SFRs)

test TOE vs. SFRs
- correctness
- vulnerability

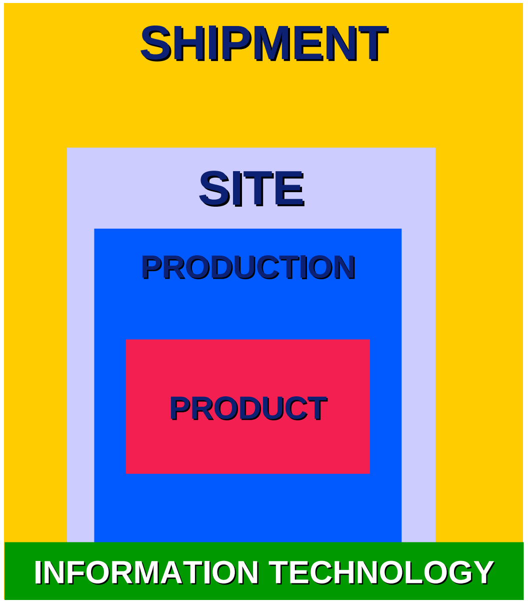
evaluate results give rating

evaluate results give rating

issue certificate

What other elements are covered by CC

- Product-Development
  - **state of the art silicon - NV-technology**
  - **cryptographic co-processors, random number generators**
  - **product design hardened against attacks**
- Production, life cycle management
- Site security
- Shipment
- Security Management



Track record of security evaluations

Common Criteria

Certified Smart card controller hardware

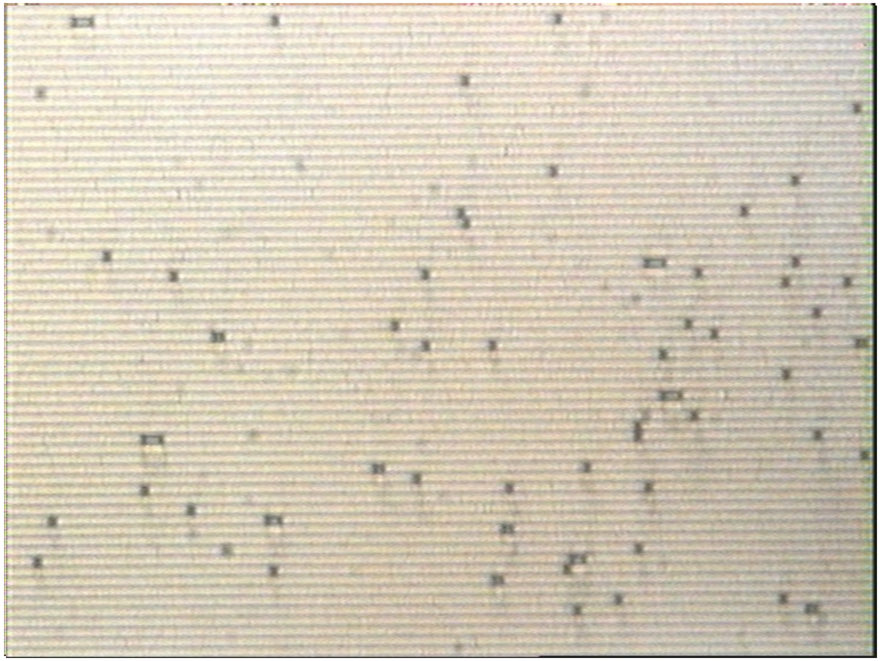
based on Smartcard IC Platform Protection Profile (BSI-PP-0002-2001)

PRODUCT	LEVEL	DATE	EVALUATOR / CERTIFICATION BODY	REMARKS
P8WE5032	**EAL3**	11/99	debis/BSI	
P8WE6017	**EAL5+**	07/01	debis/BSI	worlds 1st smart card controller at EAL5+. Highest level ever reached. also used as basis for formal composite evaluation, re-evaluation 2003 & 2005
P8WE6004	**EAL5+**	03/02	T-Systems/BSI	also used as basis for formal composite evaluation
P8WE5033	**EAL5+**	08/02	T-Systems/BSI	
P16WX064	**EAL5+**	06/03	T-Systems/BSI	worlds 1st 16 bit smart card controller EAL5+ certified P16 Crypto Library 08/03, re-evaluation 2005
P5CT072	**EAL5+**	09/04	T-Systems/BSI	worlds 1st Secure Triple Interface smart card controller EAL5+ certified
P5CC072	**EAL5+**	09/04	T-Systems/BSI	also used as basis for formal composite evaluation
P5CC009	**EAL5+**	09/04	T-Systems/BSI	also used as basis for formal composite evaluation
P5CC036	**EAL5+**	10/04	T-Systems/BSI	also used as basis for formal composite evaluation
P5CD036	**EAL5+**	02/05	T-Systems/BSI	particularly suitable for e-Passport application
P5CD072	**EAL5+**	02/05	T-Systems/BSI	particularly suitable for e-Passport application
P5CD009	**EAL5+**	02/05	T-Systems/BSI	

Further information can be found at: **http://www.bsi.bund.de/zertifiz/zert/report.htm**

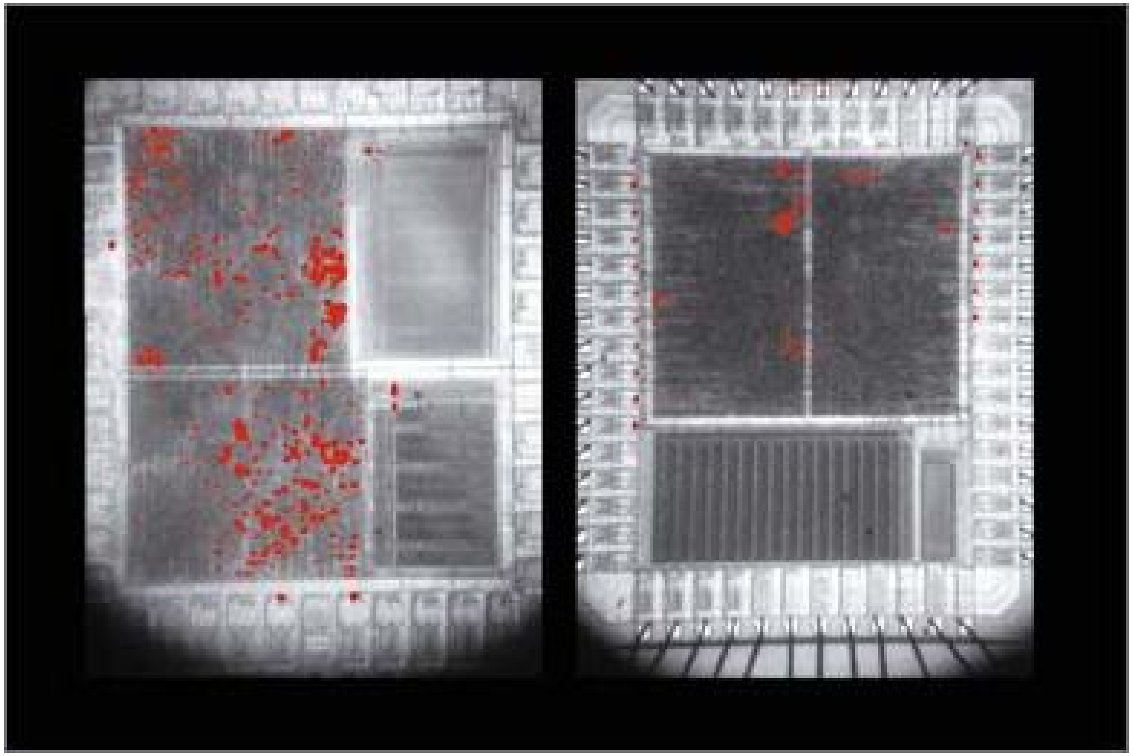
some examples of state of the art security measures

- example Layout
  - with shielding (Anti-Probing Layer)



Low Power

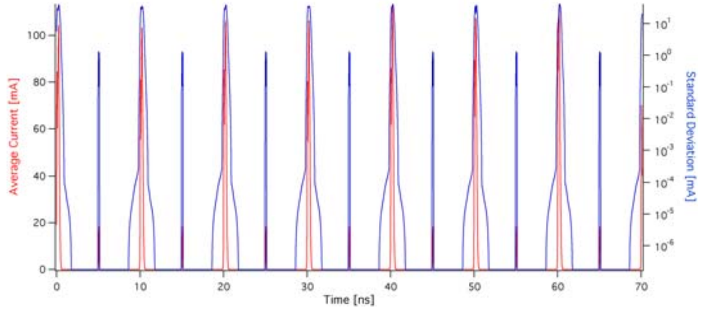
Synchronous 80c51



Asynchronous 80c51

Power Consumption

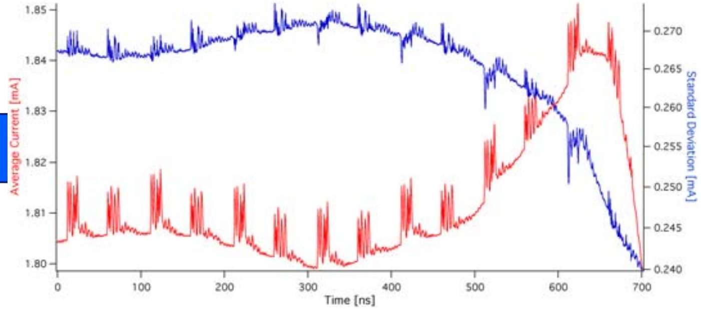
old design



average current

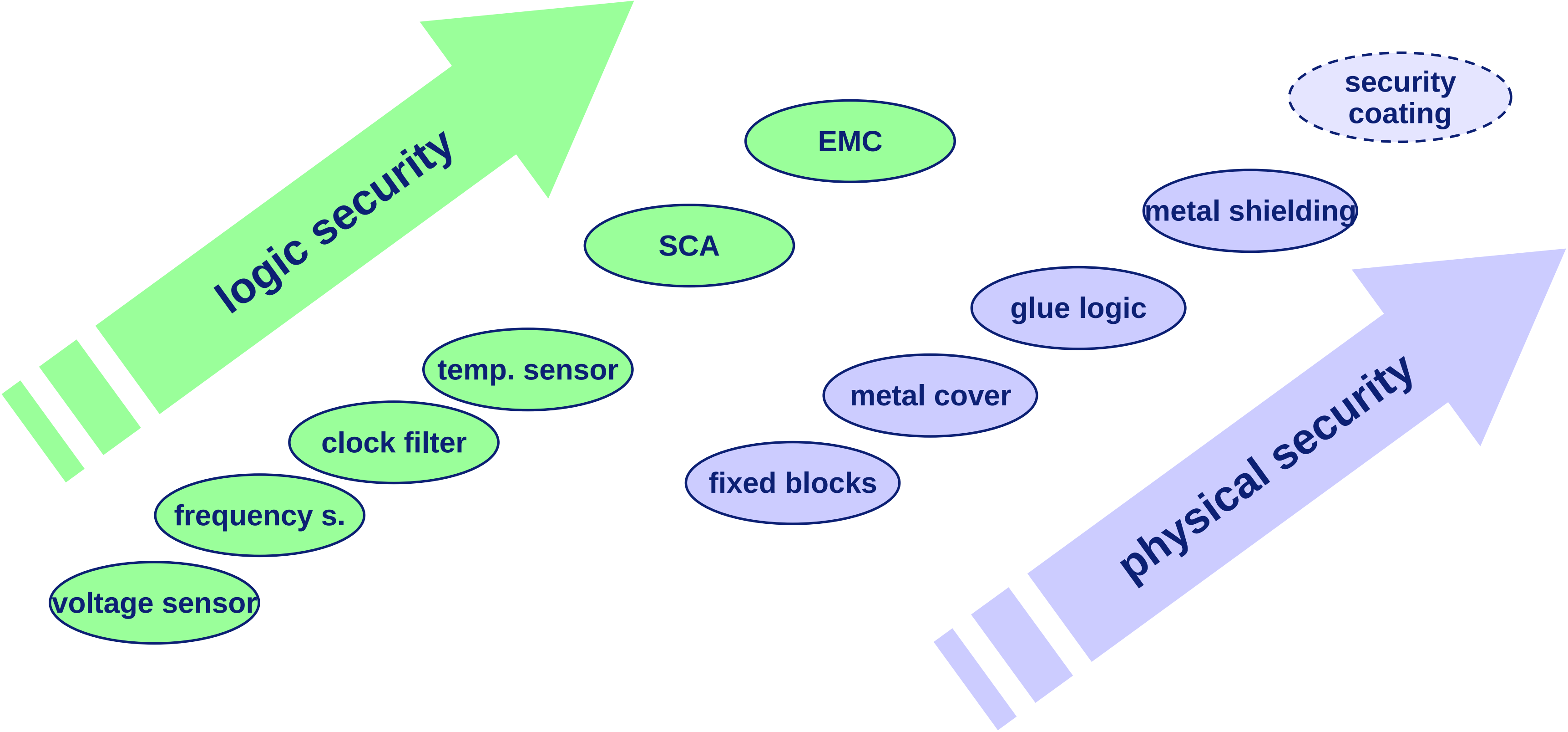
standard deviation

state-of-the-art



reduced by factor of 700

security roadmap



How to define security?

- Common Criteria evaluation scheme provides best known method to define security level for a product

- certificate assures that Security Functional Requirements are correctly implemented and the device delivers the security level given by the rating

Is there still a problem with security of products?

- we can now define a requirement specification using the CC system
- the products can be designed according to requirements, then tested
- …. and we have done our job.

- But don't forget the problem with the silicon cycle time (2-5 years)

➔ consequently the security target need to take into account this timeline

➔ yes, this is possible! … (hardly for new applications!)

Is there still a problem with security of products?

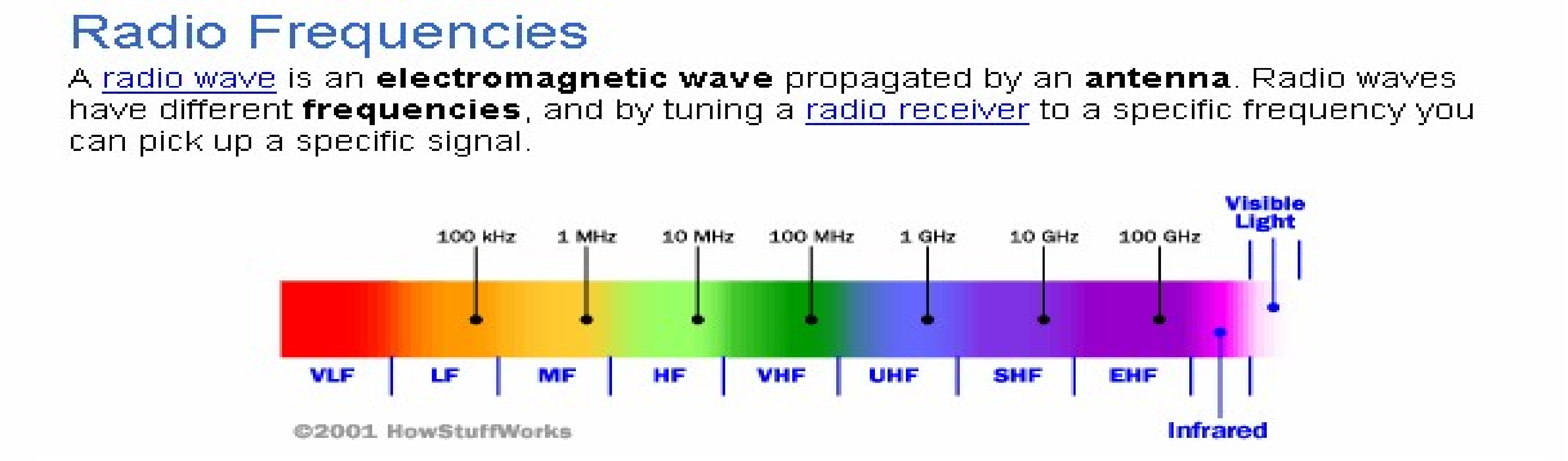
no, if we

- do own internal security evaluation of devices
- do 3rd party security evaluation of devices

**continously,
as improvement
process**

Contactless Interfaces - RFID

- RFID = Radio Frequency IDentification uses radio frequencies between 100kHz and today up to 2,45 GHz for contactless communication to identify objects or person’s rights. Radio frequencies are used as data transmission link.

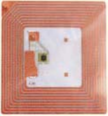


Radio Frequencies

A radio wave is an **electromagnetic wave** propagated by an **antenna**. Radio waves have different **frequencies**, and by tuning a radio receiver to a specific frequency you can pick up a specific signal.

©2001 HowStuffWorks

Standards for Contactless Data Links for ID products

Smart Labels, Cards				
	tags mainly for animal identification	labels for goods ID, electronic barcode	cards for public transport, access control, NFC	pallet identifcation goods flow, warehouse mgmt
	125 kHz	13.56 MHz		860 MHz – 2.45 GHz
Interface	ISO 11784/85 ISO 18000-2	ISO 18000-3 HF EPC Class 1	ISO 14443	ISO 18000-6 UHF EPC Class 1 Gen2
Reader	Vicinity	Vicinity	Proximity	Long Range
	≤ 1,0 m	≤ 1,5 m	≤ 0,1 m	≤ 5 m

other standards of wireless connectivity

Bluetooth®

The Official Blue

ZigBee™ Alliance

Wireless Control That Simply Works

Wireless

Yet another wireless link to grow the zoo?

reless LAN

Infrared Data Association

Wi Fi™

NFC vs. wireless technologies

Wireless	NFC	Bluetooth	ZigBee	WLAN	WUSB	IrDA
carrier [MHz]	13,45	2400	2400	2400, 5000	UWB radio	light
Speed [kbit/s]	< 424	< 721	<250	<2000 <11000	<480 (initial) <1000000	115
Range [m]	0,1	< 10	>10	<100m	<10	< 1
set up time [s]	< 0,1	6	>1	>1	>1	0,5
Network Configuration	peer to peer	point to multi-point	point to multi-point	point to multi-point	point to point	peer to peer
Security	yes, HW	yes, protocol level	no	yes, protocol	yes, protocol	no (except IFRM)
Communication modes	active - active active - passive	active - active	active - active	active - active	active - active	active - active
Usebility	fast & simple touch & go	selction process, long setup time	?	easy	?	easy to use, directivity is a problem
Cost	low	moderate	?	moderate	?	low
Applications	RFID compatible, data exchange connectivity	data exchange head Sets	control & commands	notebook PCs	home entertainement office connection cluster connection	remote control data exchange
Infrastructure	C'less Ticketing e-payment	mobile phones, PDAs	no	hotspots	?	CE, PCs mobile phones

Wireless Connectivity

- What determines *SIMPLICITY* for connectors?

difficult to use ←→ looking for connector or connection point
indentify orientation of connector
is the base station on?
how to initialize data link
- looking for application
- trying out
- manipulating setup
- ok, if not - give up

**If we don‘t have
all these problems
then
it must be simple!!**

Wireless Connectivity

- What are the requirement of such link?

  → quite small defined interaction range – size of human hand
  → isotropic field of interaction
  → easy identifiable point of interaction – „Touch Point“
  → automatic init of communication
  → fast reaction time

  → good security, peer to peer
  → low energy… no battery

NFC vs. wireless technologies

Wireless	NFC	Bluetooth	ZigBee	WLAN	WUSB	IrDA
carrier [MHz]	13,45	2400	2400	2400, 5000	UWB radio	light
Speed [kbit/s]	< 424	< 721	<250	<2000 <11000	<480 (initial) <1000000	115
Small Interaction Range [m]	0,1	< 10	>10	<100m	<10	< 1
set up time [s], fast init/reaction	< 0,1	6	>1	>1	>1	0,5
Network Configuration	peer to peer	point to multi-point	point to multi-point	point to multi-point	point to point	peer to peer
Security	yes, HW	yes, protocol level	no	yes, protocol	yes, protocol	no (except IFRM)
Communication modes	active - active active - **passive**	active - active	active - active	active - active	active - active	active - active
Usebility - touch point identifiable	fast & simple touch & go	selction process, long setup time	?	easy	?	easy to use, directivity is a problem
degree of isotropic interaction field	ISOTROPIC	ISOTROPIC	ISOTROPIC	ISOTROPIC	ISOTROPIC	directed
automatic initialization	🟩	🟨	?	🟩	?	🟩
Cost	low	moderate	?	moderate	?	low
Applications	RFID compatible, data exchange connectivity	data exchange head Sets	control & commands	notebook PCs	home entertainement office connection cluster connection	remote control data exchange
Infrastructure	C'less Ticketing e-payment	mobile phones, PDAs	no	hotspots	?	CE, PCs mobile phones

🟩 **helps for ‚Easy setup‘**

🟨 **makes ‚Easy setup‘ difficult**

NFC as close coupling interface

- support setup of other wireless links due to peer to peer
- hand down it‘s inherent security to other wireless links
- will make communication setup much simpler and more secure

What‘s special of RFID with respect to security?

- contactless links have a certain distance of propor operation
- since the link radiates more or less isotropic it distributes also the data isotropic

- moreover:
  beyond the range of proper function eavesdropping is possible depending on the measurement effort up about 10 times the range of proper function

➔ RF link itsself cannot be controlled!

What‘s special of RFID with respect to security?

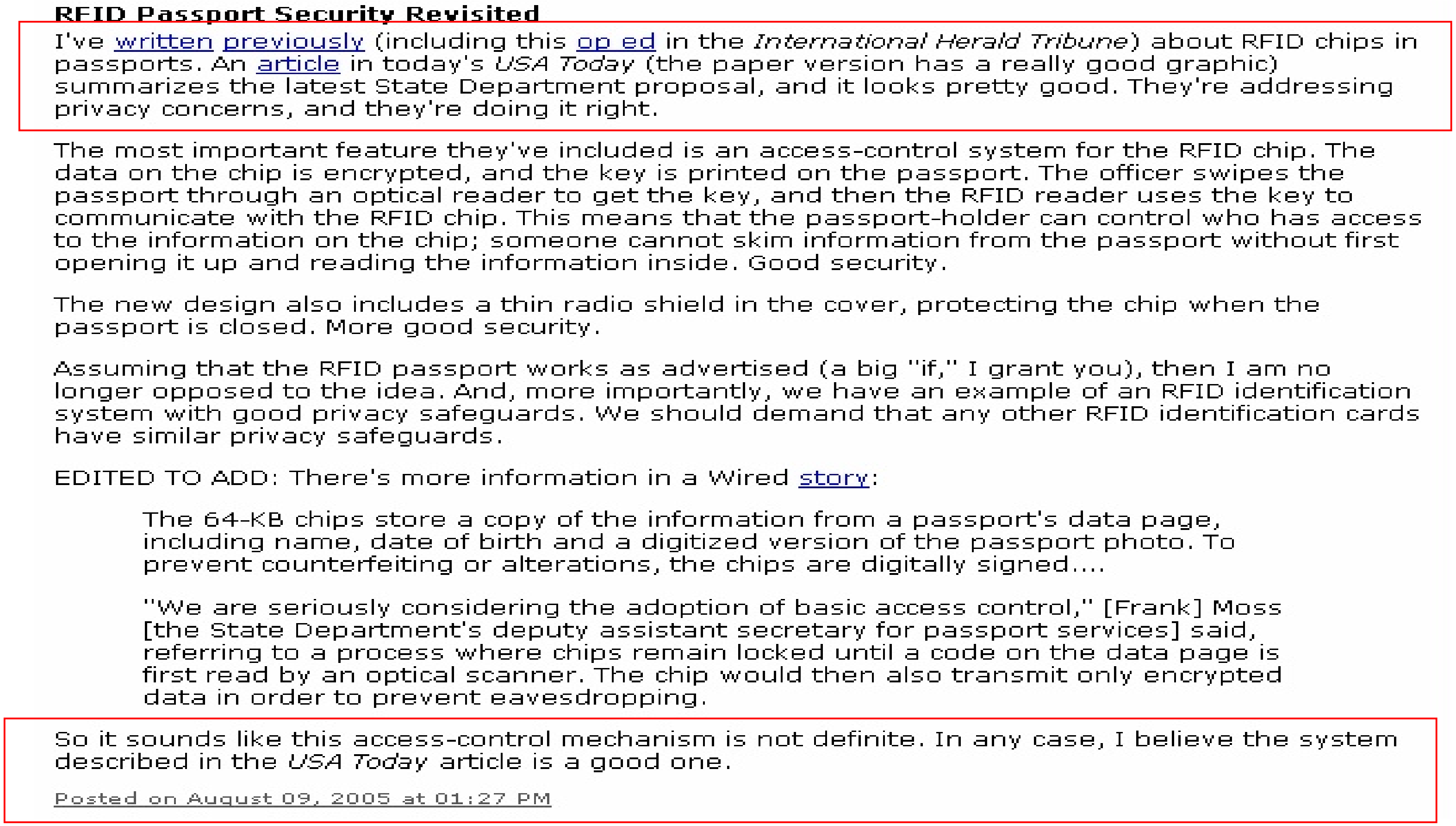
- all measures securing a contact data link can also be applied to an RF link like
  - proper authentication (bi-directional) via challenge response
  - appropriate data encryption

- all recent discussions in the public about RFID were focussing on the question of abuse and/or attack the ‚application‘

  ➔ passports equiped with RFID (e-passport)

What‘s special of RFID with respect to security?

- discussion on e-passport on Bruce Schneier‘s home page



RFID Passport Security Revisited

I've written previously (including this op ed in the *International Herald Tribune*) about RFID chips in passports. An article in today's *USA Today* (the paper version has a really good graphic) summarizes the latest State Department proposal, and it looks pretty good. They're addressing privacy concerns, and they're doing it right.

The most important feature they've included is an access-control system for the RFID chip. The data on the chip is encrypted, and the key is printed on the passport. The officer swipes the passport through an optical reader to get the key, and then the RFID reader uses the key to communicate with the RFID chip. This means that the passport-holder can control who has access to the information on the chip; someone cannot skim information from the passport without first opening it up and reading the information inside. Good security.

The new design also includes a thin radio shield in the cover, protecting the chip when the passport is closed. More good security.

Assuming that the RFID passport works as advertised (a big "if," I grant you), then I am no longer opposed to the idea. And, more importantly, we have an example of an RFID identification system with good privacy safeguards. We should demand that any other RFID identification cards have similar privacy safeguards.

EDITED TO ADD: There's more information in a Wired story:

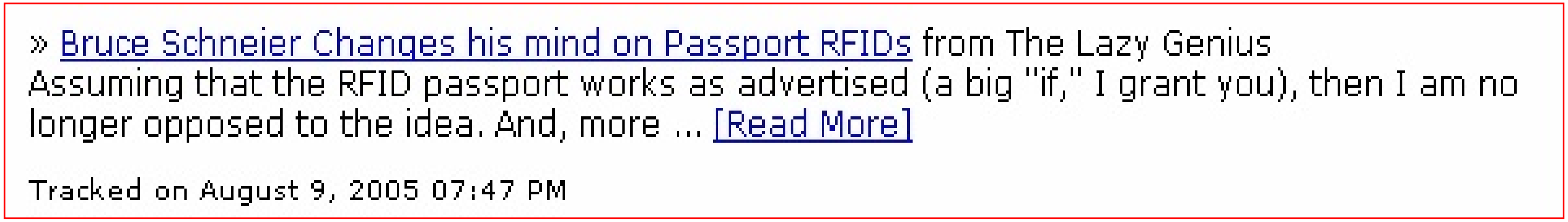
> The 64-KB chips store a copy of the information from a passport's data page, including name, date of birth and a digitized version of the passport photo. To prevent counterfeiting or alterations, the chips are digitally signed....
>
> "We are seriously considering the adoption of basic access control," [Frank] Moss [the State Department's deputy assistant secretary for passport services] said, referring to a process where chips remain locked until a code on the data page is first read by an optical scanner. The chip would then also transmit only encrypted data in order to prevent eavesdropping.

So it sounds like this access-control mechanism is not definite. In any case, I believe the system described in the *USA Today* article is a good one.

Posted on August 09, 2005 at 01:27 PM

What‘s special of RFID with respect to security?

- discussion on e-passport on Bruce Schneier‘s home page



» Bruce Schneier Changes his mind on Passport RFIDs from The Lazy Genius
Assuming that the RFID passport works as advertised (a big "if," I grant you), then I am no longer opposed to the idea. And, more ... [Read More]

Tracked on August 9, 2005 07:47 PM

In summary that was a good discussion – why?

- such discussions are necessary to
  - reveal potential weaknesses of the system
  - increase level of acceptance

- it showed that Semiconductors provided the right solution already before the discussion started

Conclusion

Security of Identification Products - how to manage?

- establish and maintain a good link into security/crypto community to ensure state-of-the-art know how
- support public discussions and provide solutions acceptable by all
- do own internal security evaluation of devices
- do 3rd party security evaluation of devices

continous improvement process

….. to provide state-of-the-art security technology for the people!

PHILIPS