Contactless Payments Chip Design
CTST 2009 – New Orleans, LA

Manuel Albers
Director, Business Development & Sales North America
BU A&I – Sales & Marketing - Identification
May 6th, 2009

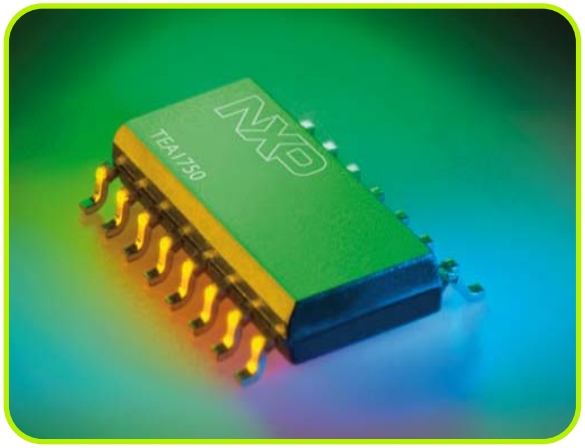
Agenda

1. NXP Semiconductors
2. Setting The Stage
3. Secure Chip Design
4. Secure Chip Environment
5. Secure Chip Evaluation and Certification
6. Conclusion

Company Profile

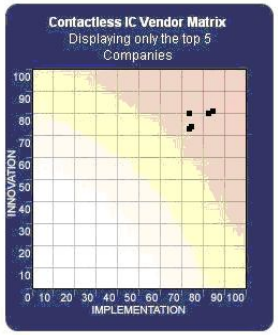
- **President & CEO:** Rick Clemmer
- **Headquarters:** Eindhoven, The Netherlands
- **Net sales:** $5.4 billion in 2008 *)
- Established in 2006 (formerly a division of Philips)
- 50+ years of experience in semiconductors

- **Leadership positions in contactless & security**
  - **Banking solutions**
    - Supplied >500 million banking cards in 35 countries
  - **eGovernment solutions**
    - Supplying 80% of ePassport projects worldwide
  - **Public Transportation**
    - Mifare is used in >70% of the global transport infrastructure
  - **NFC solution**
    - Creator of NFC technology together with Sony
    - NXP products used in about 100 NFC trials worldwide



Contactless IC Vendor Matrix Top 5 Listing:

RANK	COMPANY
1	NXP Semiconductor
2	INSIDE Contactless
3	Infineon Technologies AG
4	Texas Instruments Inc
5	Sony Corporation



Denotes highest rated company along the Implementation scale
Denotes highest rated company along the Innovation scale

Source: ABI Research, 2008

*) These figures include the Mobile & Personal business which was largely part of the ST-NXP Wireless JV in 2008

Agenda

1. NXP Semiconductors
2. Setting The Stage
3. Secure Chip Design
4. Secure Chip Environment
5. Secure Chip Evaluation and Certification
6. Conclusion

Setting the stage

Contactless Payment Chip Design - Objective

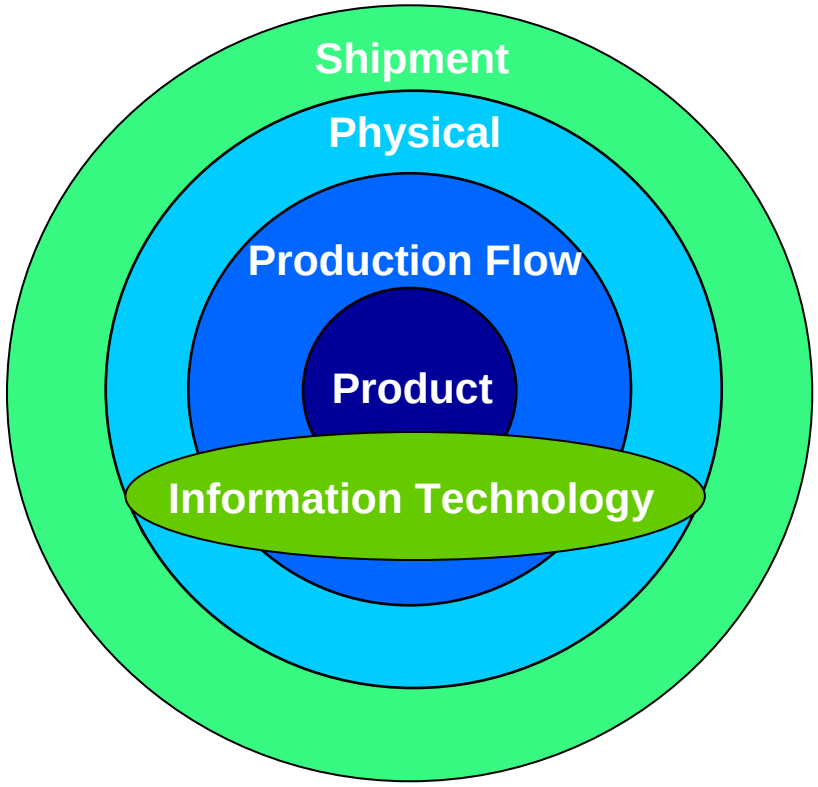
To meet or beat the customer's requirements in the application in terms of

- **Performance**
  - Typically defined in the application specification
  - Analog!
- **Security**
  - Typically defined by the (end-) customer
  - Often referencing standardized or non-standardized security criteria
- **Reliability**
  - Supply
  - Reputation
- **Cost**
  - Competitiveness

Product Security Assessment

General Approach

- **Product**
  To meet the customer's security requirements in the final application.
- **Production Flow**
  To prevent/ detect loss or manipulation of the security product.
- **Shipment**
  To prevent/ detect loss or manipulation of security product.
- **Site Security**
  - Physical Security
    To prevent unauthorized access to security data, products and facilities
  - Logical (IT) Security
    To prevent loss of confidentiality and integrity of security objects/data



Product Security Evaluation & Certification

General Aspects

- **Security** is defined as a state free from unacceptable risk.

- To obtain a **Security Certificate** for a Security Product (Chip), the evaluation comprises the following aspects.

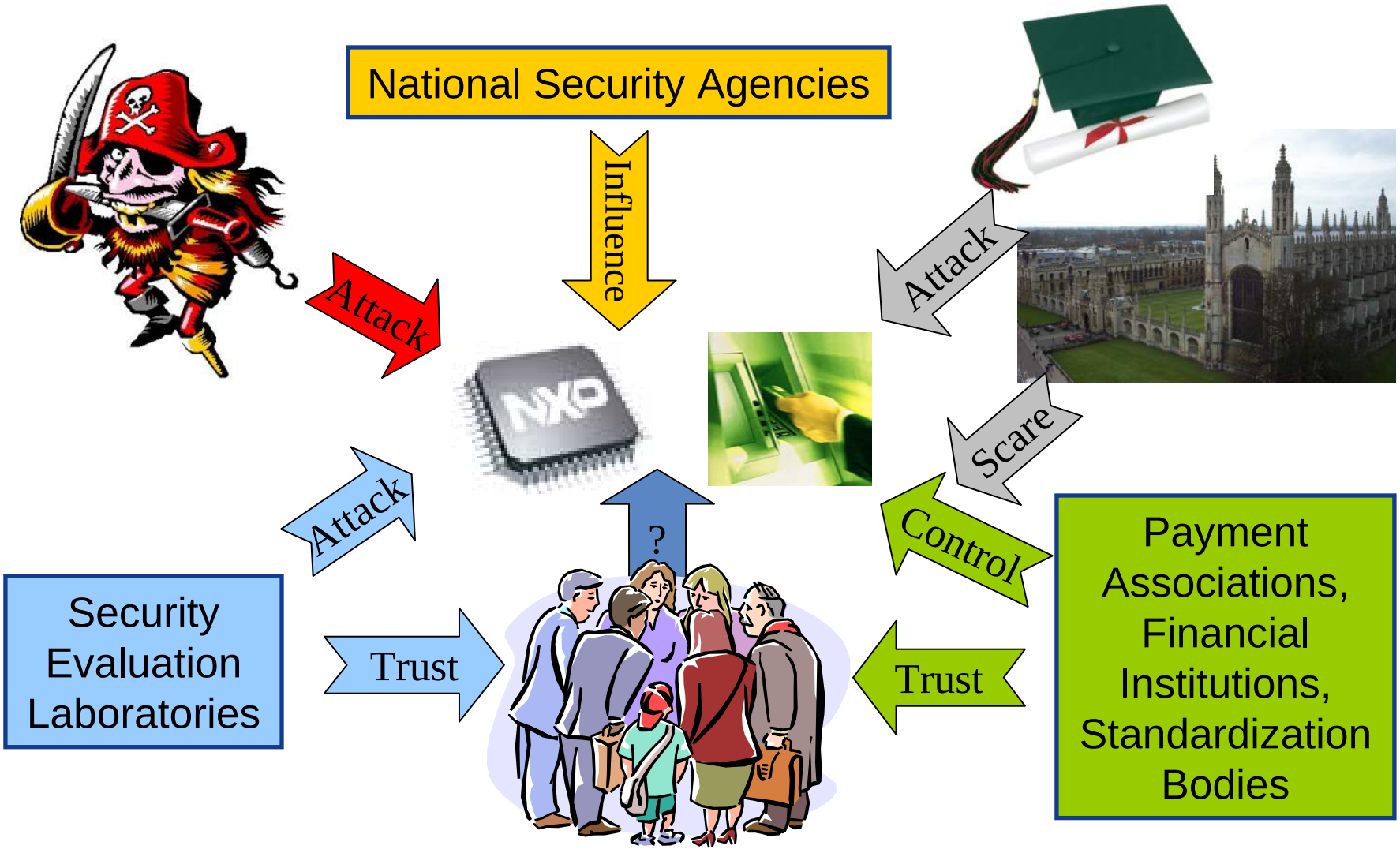
  - **Chip related**
    - Evaluation of the design (including source code)
    - Tests to verify the design
    - Vulnerability Assessment

  - **Chip environment related**
    - Evaluation Audit of the Configuration Management
    - Evaluation Audits of the development environment at the concerned sites
    - Evaluation Audits of the production environment over the entire supply chain

Agenda

1. NXP Semiconductors
2. Setting The Stage
3. Secure Chip Design
4. Secure Chip Environment
5. Secure Chip Evaluation and Certification
6. Conclusion

The Battleground

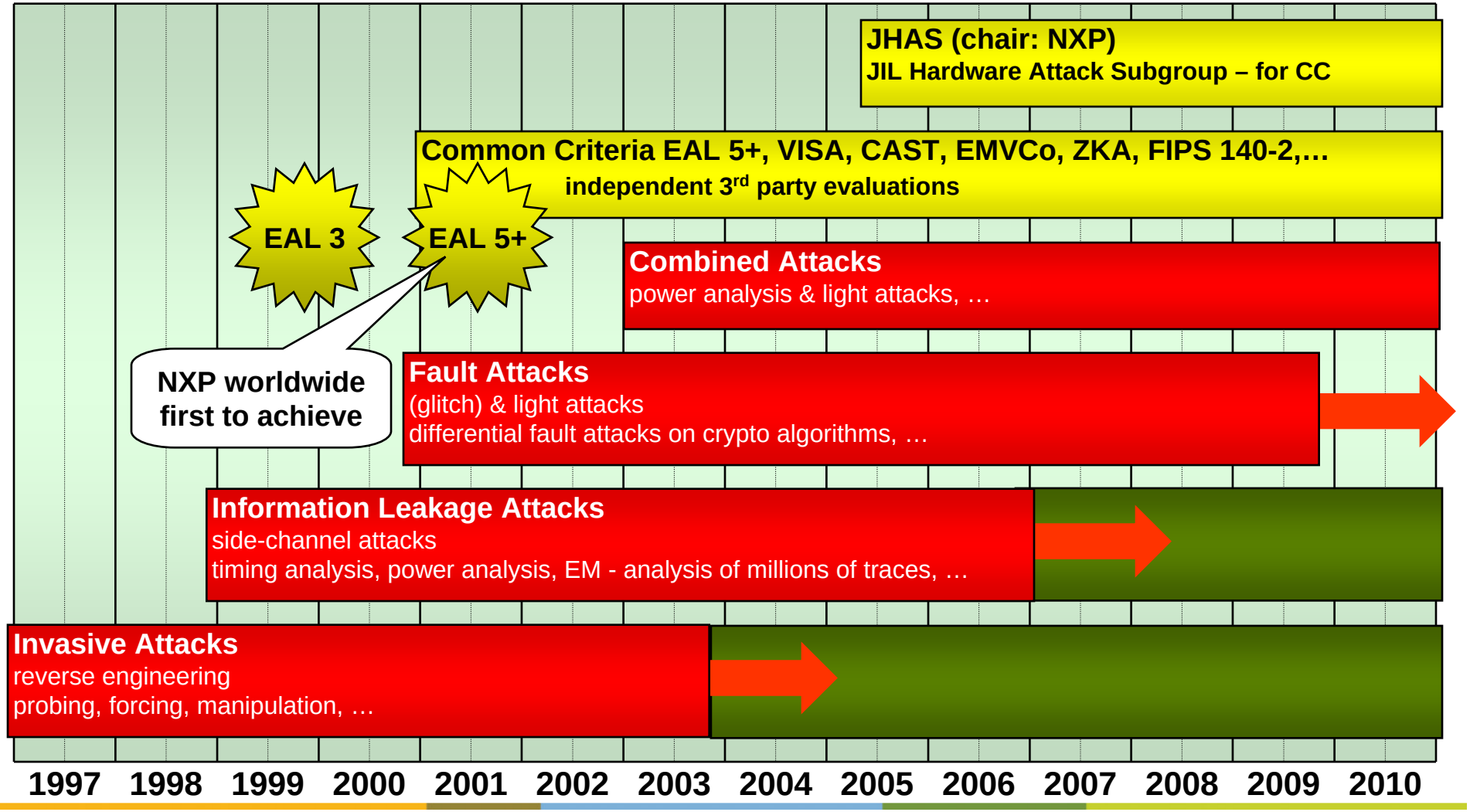


Introduction – Smartcard-based Systems

- **The security of a system is a holistic property**
  - A system usually consists of many components, all of which contribute.
  - The system is only as strong as its weakest link.
- **Light-weight card systems**
  - Are based on relatively cheap cards (e.g. simple ASICs or standard OTS [Off-The-Shelf] CPUs), and a very strong back-end system.
  - Typically used when the number of (to be) deployed consumables is very large (e.g., Public Transport).
- **Heavy-weight card systems**
  - Are based on more expensive, highly secure cards (containing a dedicated high-security CPU core and crypto coprocessors) that “can survive on their own” for a long time in a hostile environment.
  - Typically used when the number of cards is not so large, or no back-channel exists (e.g., Banking, Access Control, eGovernment, Pay-TV).
  - Typically certified with Common Criteria at EAL 4+, EAL 5, or EAL5+

Security Roadmap

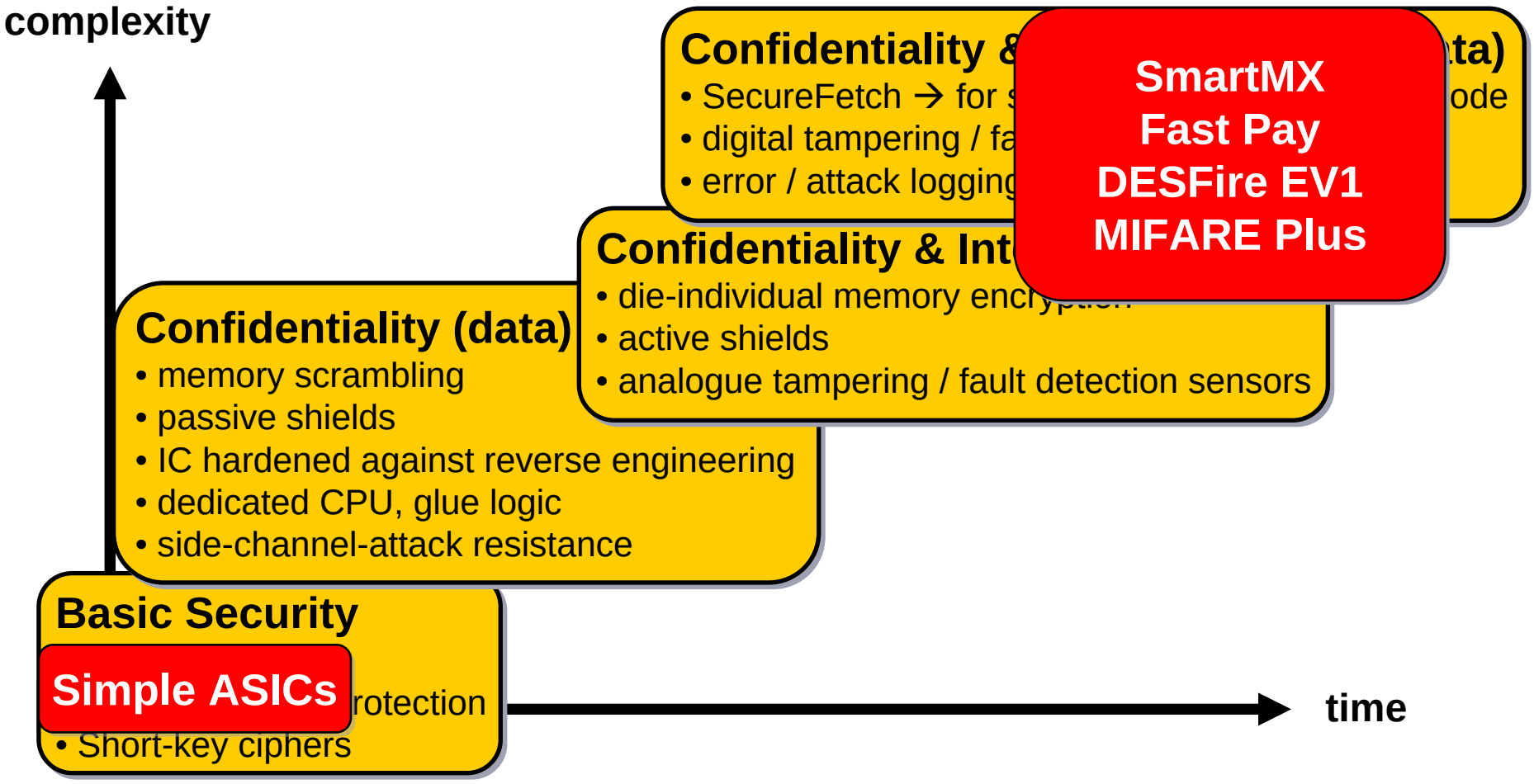
Attacks on Smart Cards



JHAS group in CC Scheme – ~30 Members

Security Roadmap

Evolution of Defences



Security threats landscape – SmartMX

NXP comprehensive Security Concept

More than **100 unique security features** harden the SmartMX.

Licensed Countermeasures against Differential Power Analysis (**DPA**).

Proven by third party security assessments and type approvals:

EMVCo security evaluation
CAST
VISA
Common Criteria EAL5+
ZKA
Approval for German Signature Card


Deutsches IT-Sicherheitszertifikat

BSI-DSZ-CC-0227-2004
Philips P5CT072V0M and P5CC072V0M Secure Smart Card Controller
from
Philips Semiconductors GmbH
Business Line Identification

Evaluation Results:
PP Conformance: Protection Profile BSI-PP-0002-2001
Functionality: BSI-PP-0002-2001 conformant plus product specific extensions Common Criteria Part 2 extended
Assurance Package: Common Criteria Part 3 conformant EAL5 / augmented by: ALC_DVS.2 (Life cycle support - Sufficiency of security measures), AVA_MSU.3 (Vulnerability assessment - Analysis and testing for insecure states), AVA_VLA.4 (Vulnerability assessment - Highly resistant)

Born, 16 September 2004

Common Criteria

Agenda

1. NXP Semiconductors
2. Setting The Stage
3. Secure Chip Design
4. Secure Chip Environment
5. Secure Chip Evaluation and Certification
6. Conclusion

Security Management System

Secure Chip Environment

- **Implementation of a Security Management System (SMS) minimizes the (unacceptable) risks of**

  - Breach of Confidentiality (i.e. information leakage)
  - Integrity (i.e. manipulation of information)
  - Misuse (of information and resources)
  - Economic damages
  - Damage to Reputation

  and supports a close, auditable relationship between Chip Maker, Suppliers, and (End-) Customers.

Security Management System (SMS)

General Requirement

- SMS Implementation throughout the entire development and production process
- Security Policy - Management Team Commitment and assigned responsibilities
- SMS Documentation as integrated part of the Quality System Documentation
- Sufficiency and effectiveness of the SMS need to be checked periodically by 3rd party evaluation site visits.
  - The SMS can e.g. follow security assurance requirements according to Common Criteria (ISO15408)

Agenda

1. NXP Semiconductors
2. Setting The Stage
3. Secure Chip Design
4. Secure Chip Environment
5. Secure Chip Evaluation and Certification
6. Conclusion

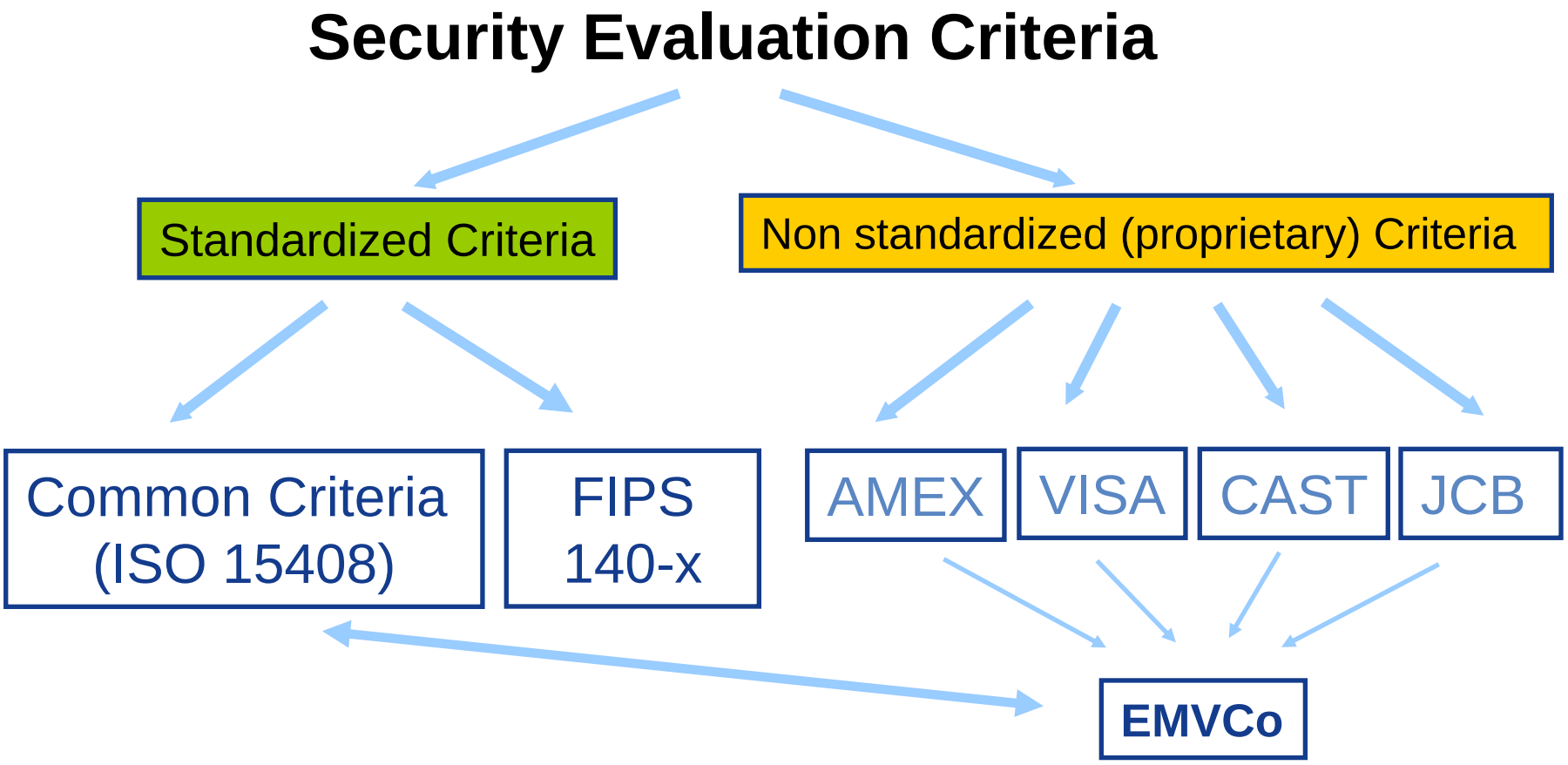
Security Evaluation

Current situation

- Different requirements for different applications
  - Common Criteria
    - German Sig. Law, Passport, Healthcard, Tachograph
    - French banking applications or health card
  - Market driven criteria (banking applications)
    - VISA / MC (CAST) / JCB
    - EMVCo
    - ZKA
  - FIPS 140-2
    - E.g. US Government requirements
  - MULTOS
- Several evaluations of the same HW
  - Time consuming, expensive

Security Evaluation

Current situation



EMVCo approval = H/W approval, Basis for Type Approval

Relevant Formal Card Testing Processes

Example: MasterCard & Visa Type Approval

- **Pre-requisite:** EMVCo. (H/W) Approval
- **MasterCard**
  - Analog Interface Testing
    - Electro-magnetic behavior
  - Digital and Application Testing
  - Performance Testing
  - Combination Testing
    - Card – Reader interaction
  - Card Quality Management
    - Audit of the manufacturing site(s)
  - Compliance Assessment & Security Testing (CAST)
    - Security evaluation of the chip, the OS, and the application
- **Visa**
  - Chip Hardware Security Evaluation Process
    - Not applicable for MSD 1.4.2
  - Functional Testing
    - Analog and Digital Testing
      - magnetic field characteristics
      - timing, anti collision, and protocol
    - Application and/ or Visa GlobalPlatform Testing
  - Risk Testing
    - Security evaluation of the chip, the OS, and the application

Agenda

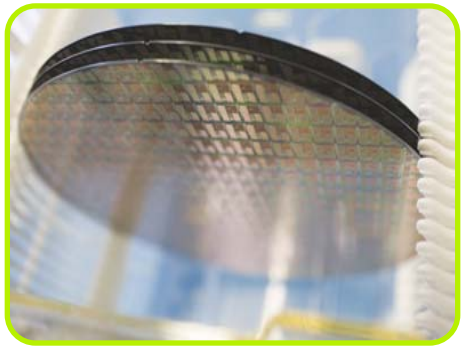
1. NXP Semiconductors
2. Setting The Stage
3. Secure Chip Design
4. Secure Chip Environment
5. Secure Chip Evaluation and Certification
6. Conclusion

Conclusion

- Design of a (secure) Contactless Payment Chip is a very **involved** and **resource-intensive** process.
- Time to market and cost of security evaluations and certifications will continue to drive the **consolidation of non-standard security criteria** to standard security criteria such as Common Criteria.
- Chip Security is a moving target (a race). Market participants contribute to constantly raising the bar for secure chip design. Continuous investments into both **Secure Chip Design Processes** and a holistic **Security Management System** have proven to be a successful and sustainable approach.

Thank You for your attention!

Q & A



manuel.albers@nxp.com

(C) +1 (401) 359-4999