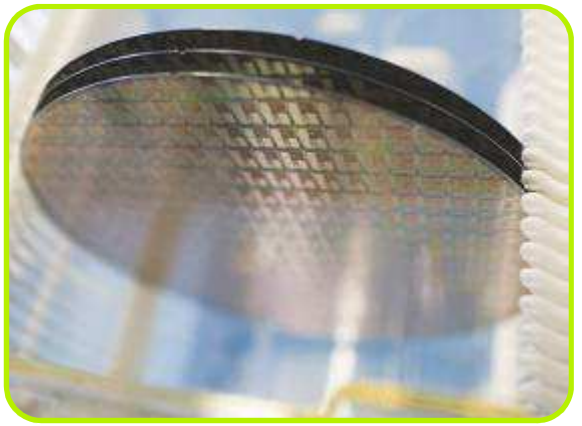
Security in Industry – When is Good Good Enough?

28 November 2013

Mathias Wagner, Fellow, Chief Security Technologist

NXP Semiconductors



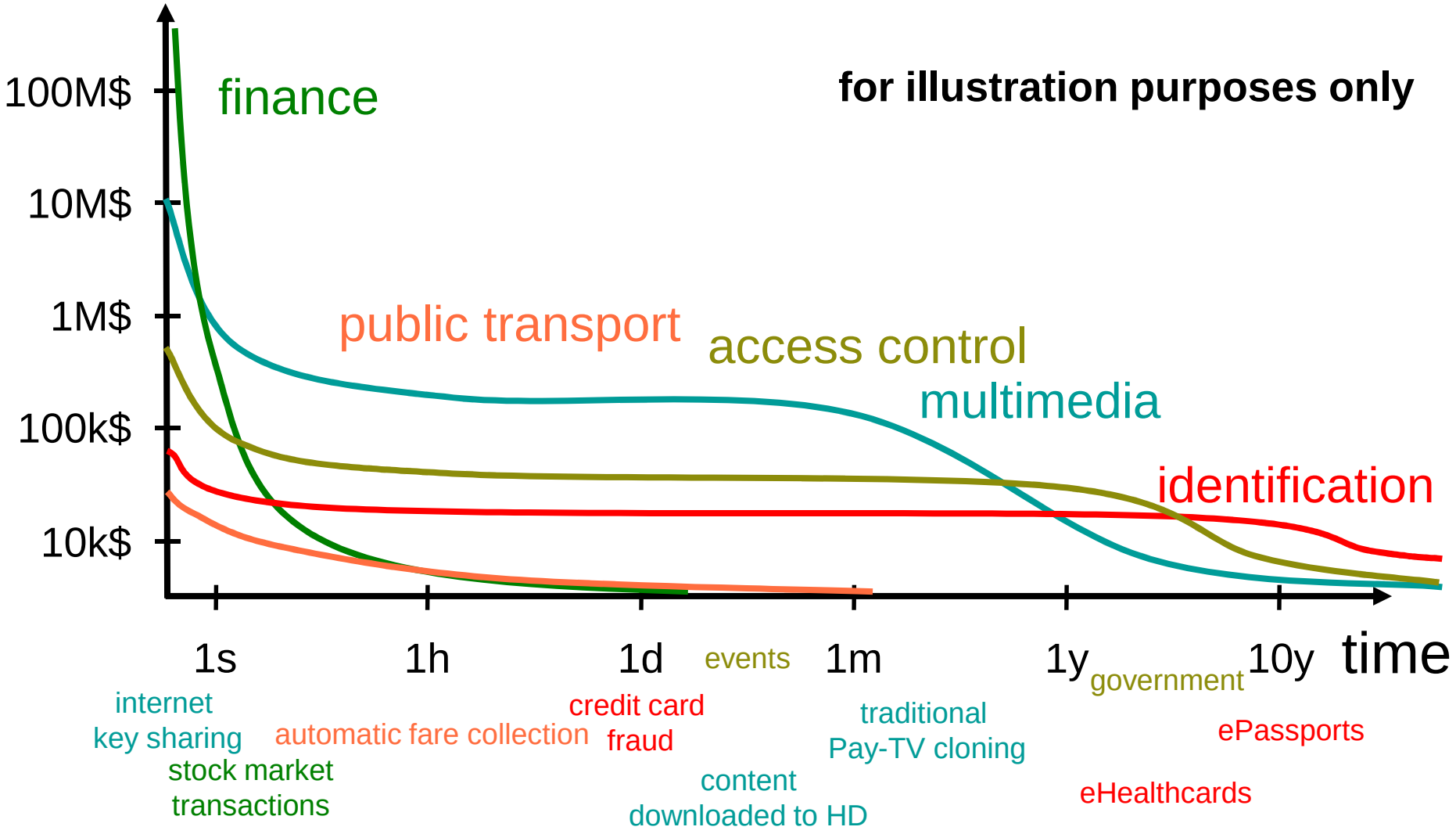
Content

- Introduction
- When is Good Good Enough?
  - Common Criteria – a Primer
  - JHAS – JIL Hardware Attack Subgroup
  - Strategies
- Summary

Introduction

Security Landscape…

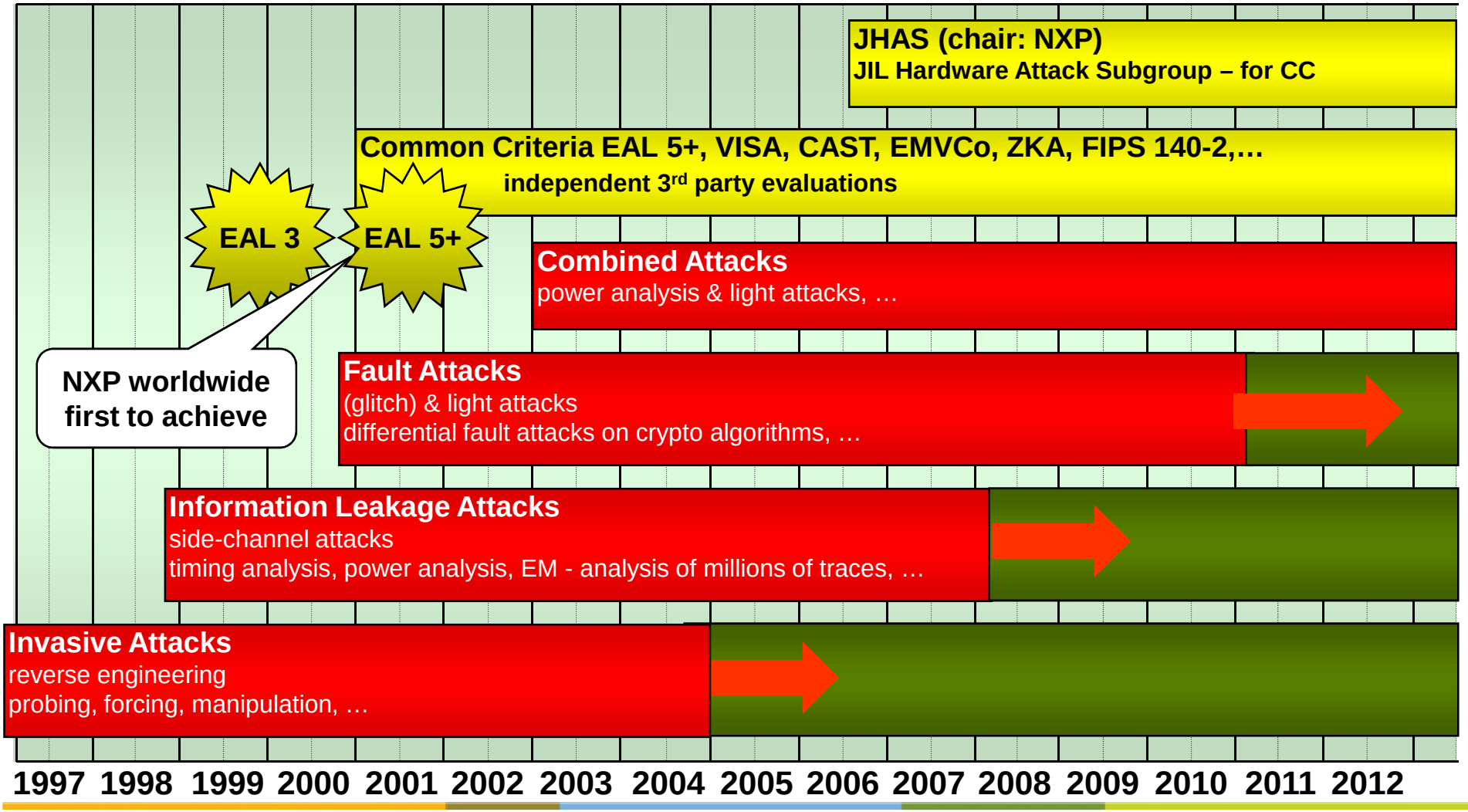
Value of an Attack Depends on Market



Security Roadmap

Attacks on Smart Cards

And what is next…?



How Many Scientific Papers are out there?

- **Academic papers published on attacks (& countermeasures) in the field of secure embedded devices…**
- **A recent survey showed that**
  - **In 2000 about 20 papers**
  - **In 2010 about 100 papers**
- **Estimate as of beginning of 2012:**
  - **In excess of 700 papers have been published since ‘96!!!**
- **OK, not all are new ☺, and there is a lot of redundancy, but still!**

Security is a Moving Target

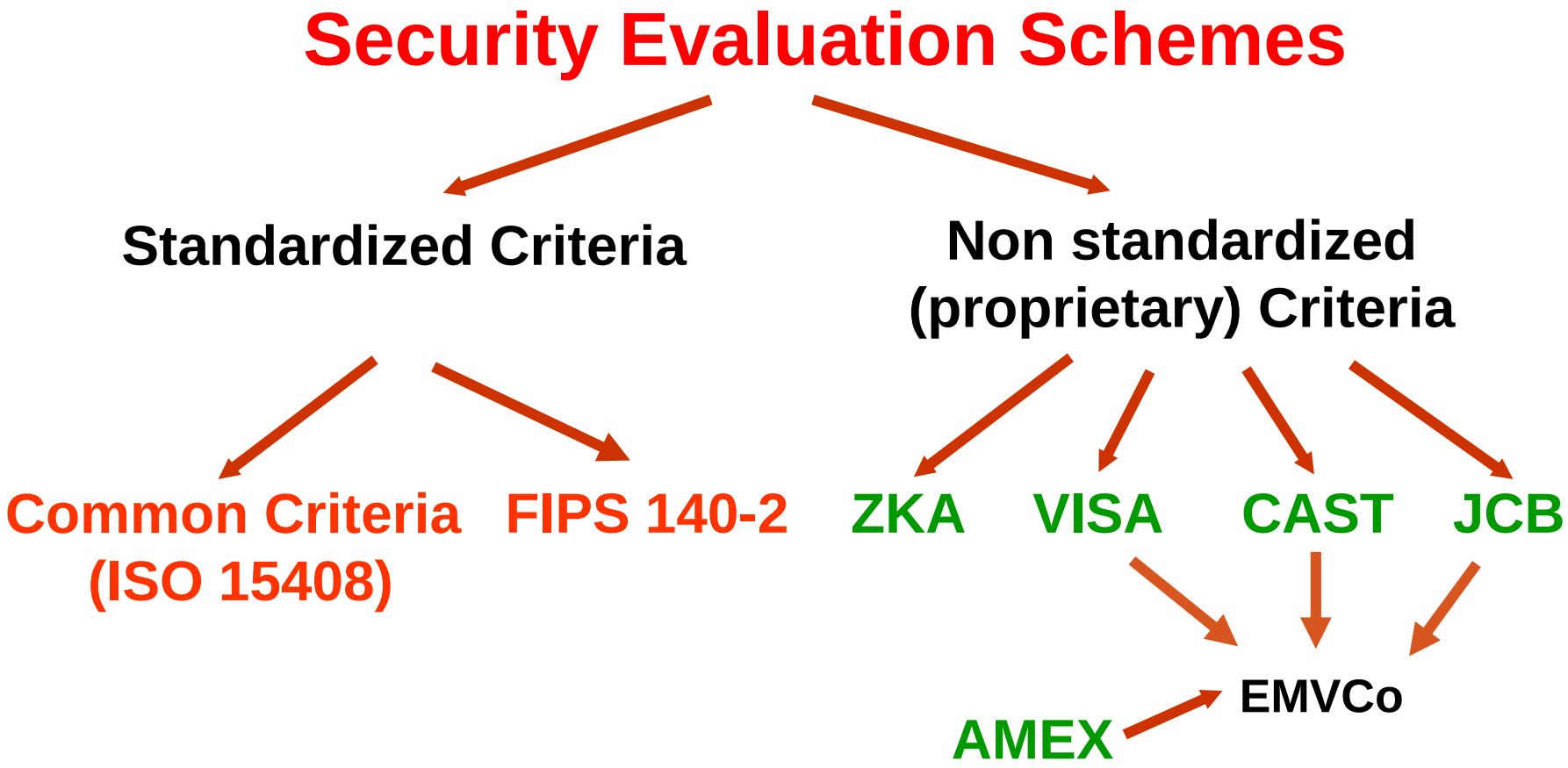
- There is no 100% security – systems can always be successfully attacked, but
    - What type of attackers do I need to consider?
    - How bad is it?
    - How much does it cost?
    - Does it scale?
    - …
- → I need a metric to measure the level of security
- → I need a strategy to reduce risk and impact

Metrics to Measure Security

Overview…

Security Evaluation Schemes – An Overview

Proprietary versus Standardized



FIPS 140 versus Common Criteria

Two fundamentally different approaches...

FIPS 140-2 versus Common Criteria

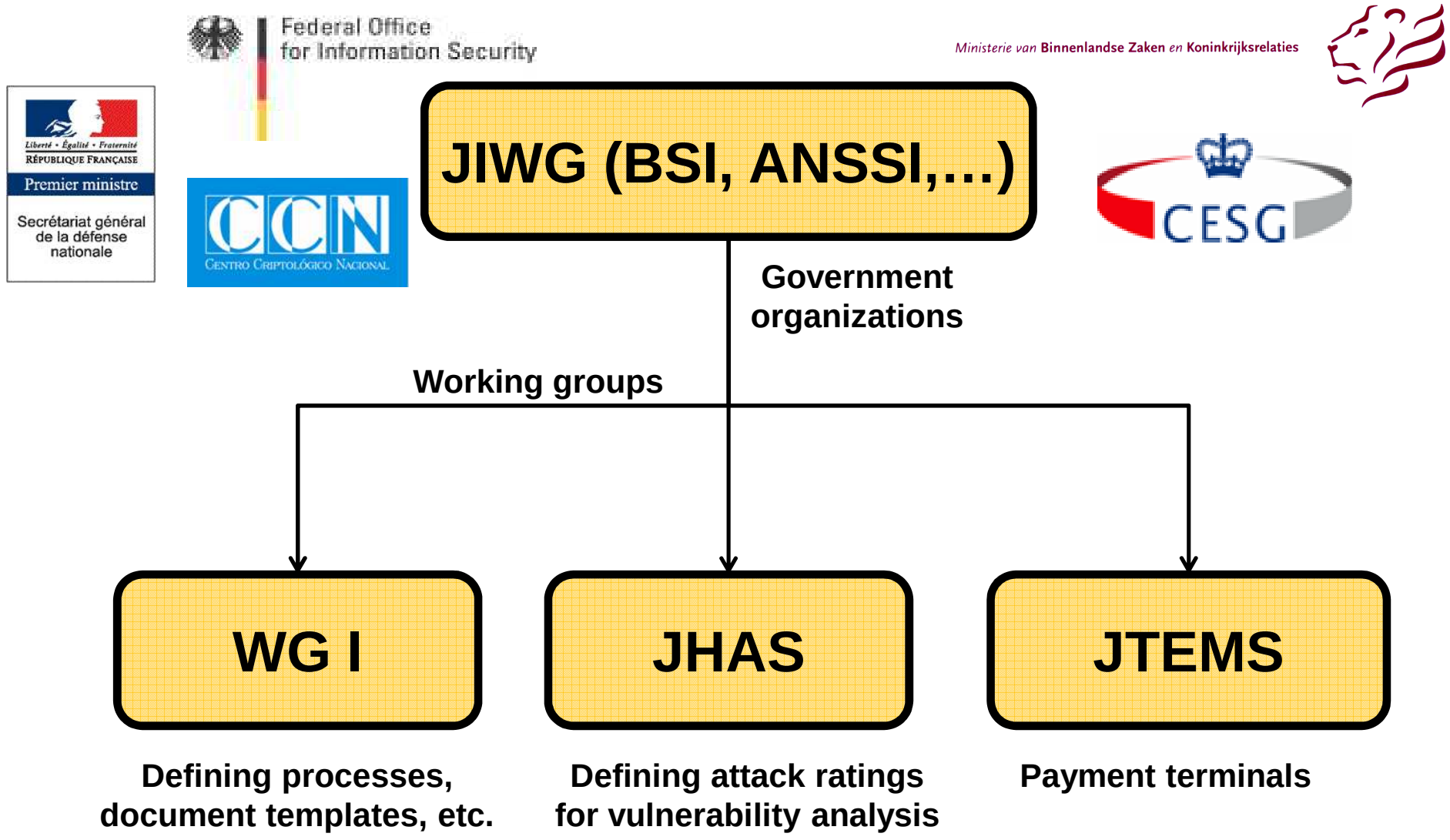
- **FIPS 140-2**
  - Levels 1 – 4
  - Not dedicated to smart cards, so it may also describe physical security measures of a secure letter box… ☺
  - Based on Do's and Don'ts
  - Based on **Checklists**

- **Common Criteria**
  - In practice levels EAL 3 – 5+
  - (Levels 6 & 7 require formal modeling and proofs)
  - Variant dedicated to smart cards available
  - Based on **Assets** that need to be protected like secret keys, user data, user SW

Common Criteria

A high-level introduction

Common Criteria Scheme for Smart Cards



Security Evaluation

Common Criteria – Mission Statement

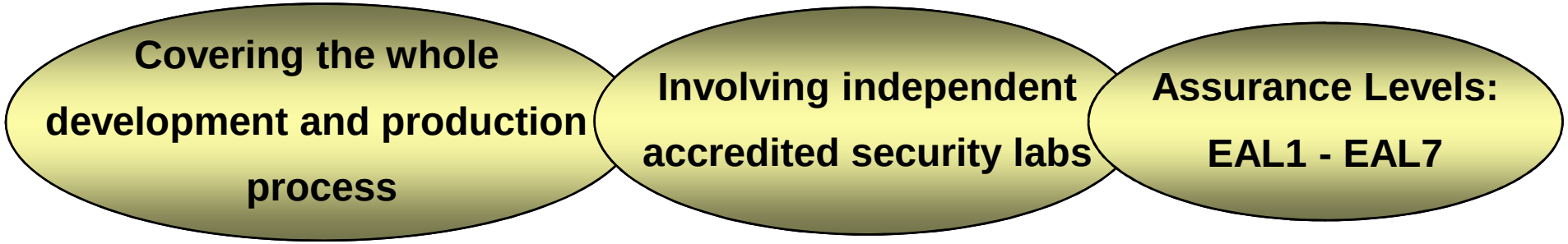
CC Evaluation rates

Correctness

and

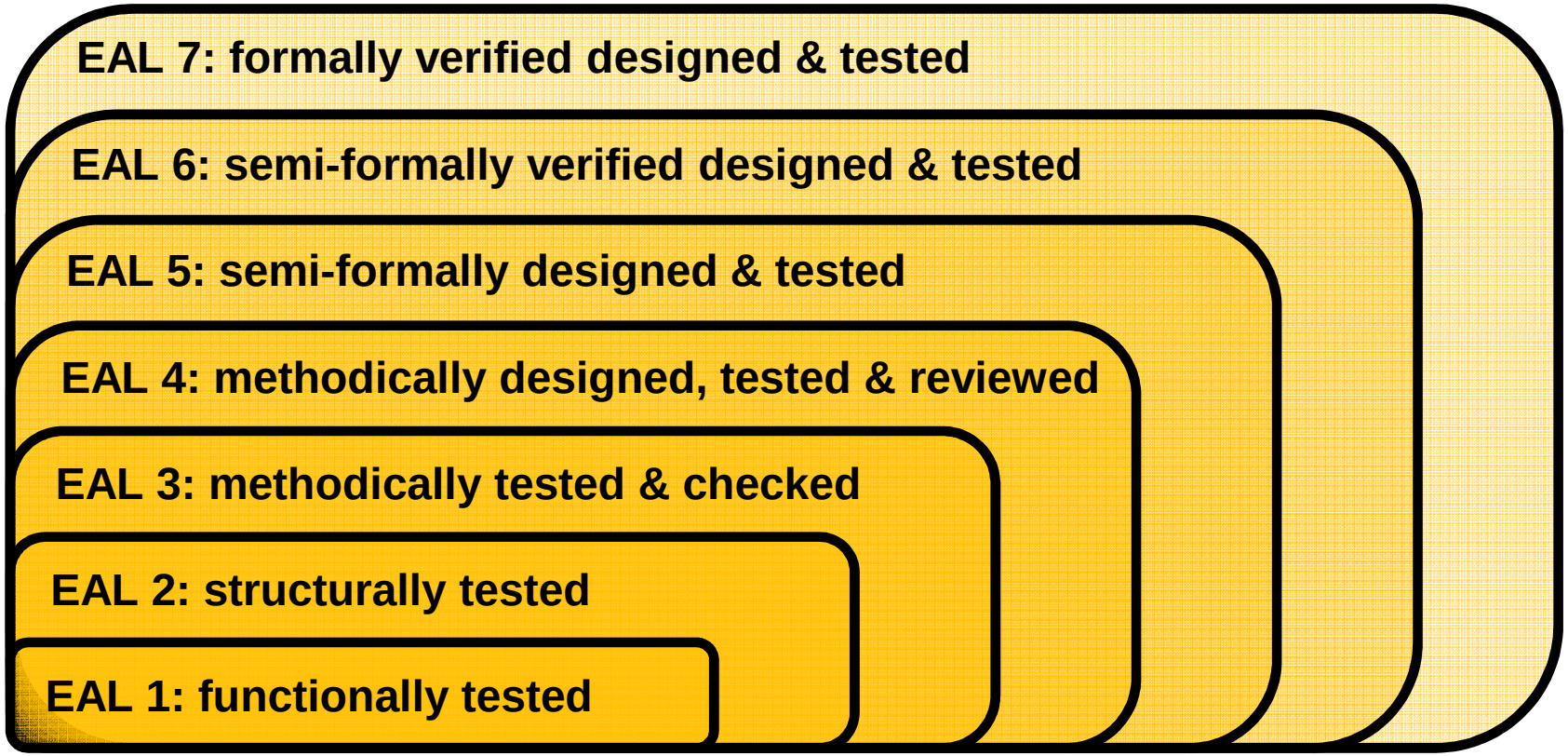
Effectiveness

of *implemented* Security Functions



Security Evaluation

Common Criteria – „EAL“ Assurance Levels



Security Evaluation

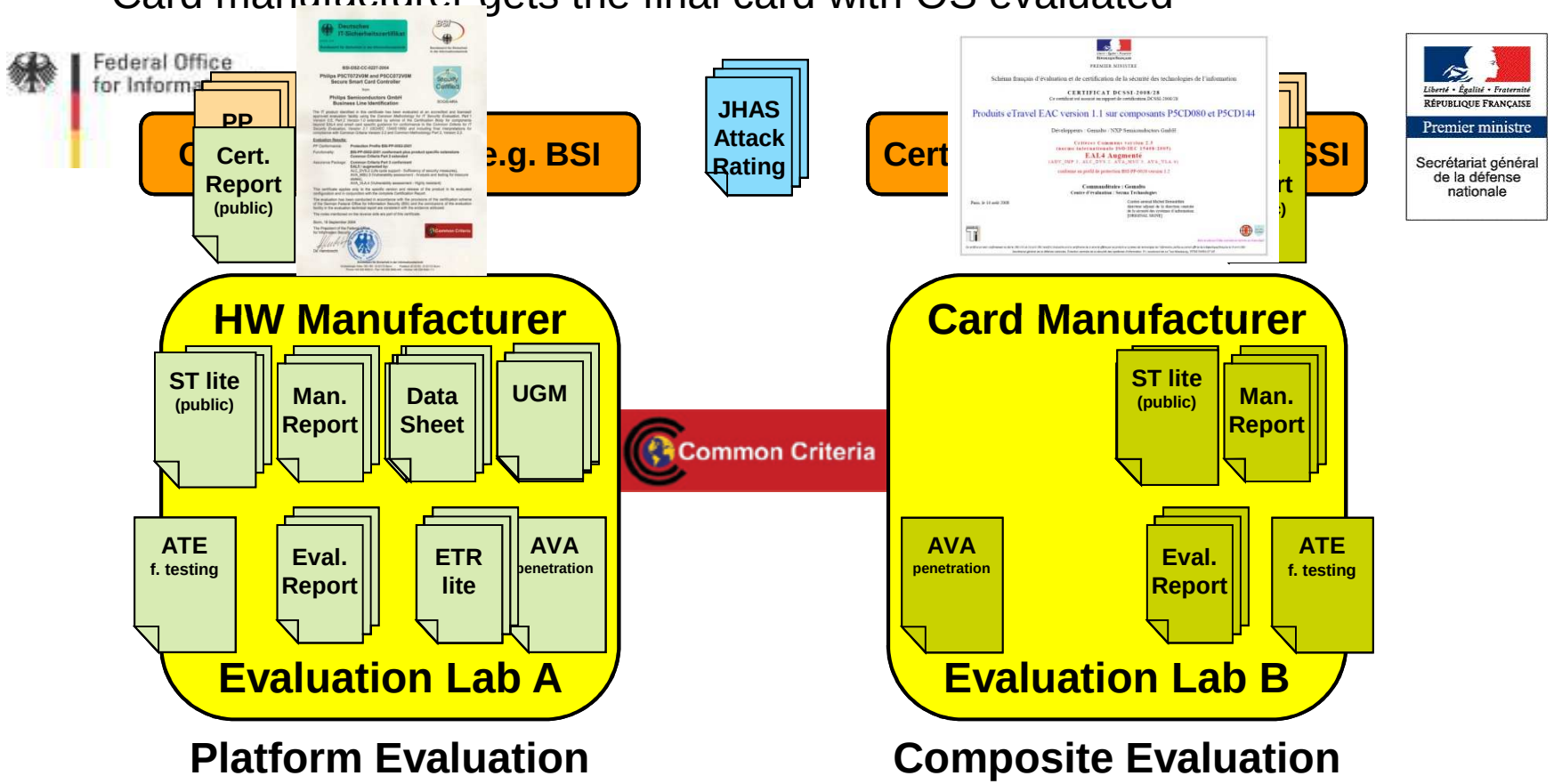
Common Criteria V3.1 - Assurance Levels

- EALn: Predefined Packages…
- Difference is in the component level
  - The higher the number
    - the more formal the description has to be
    - the more details are requested
- EAL5+
  - What is the '+' ?
- '+' = Augmentation
  - At least one component from a higher level has been taken (which one is defined in PP)

Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life-cycle support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	2	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

A Helicopter View on a CC Evaluation

- **Typically, a two-stage approach…**
  - HW manufacturer gets the HW platform evaluated
  - Card manufacturer gets the final card with OS evaluated



JHAS

JIL Hardware Attack Subgroup

Security Evaluation

Common Criteria – JHAS Mission Statement

The JHAS group

- Meets bi-monthly and consists of a wide variety of members
- State-of-the Art: Assess all HW and SW attacks (new and old) that may apply to smart cards and maintain a rating of those that is consistent with the advancements of attacks (published in a confidential document available to all members)
- Quality Assurance: Support evaluating labs to perform & assess attacks uniformly across all members, thereby helping to create a level playing field for all
- Promote the use of CC methodology for vulnerability analysis

JHAS group in CC Scheme – ~36 Members

NXP

Security Evaluation

Common Criteria – JHAS Documents

Application of Attack Potential to Smartcards

- Status: **Public**
- Rating tables and methodology

JIL Attack Methods for Smartcards

- Status: **Confidential**
- List of all attack classes
- Description of many attacks (not exhaustive, though!)
- Example ratings
- Serves as guideline for CBs, evaluation labs and vendors

Security Evaluation

Common Criteria – JHAS Attack Classification

Major attack classes are:

- Physical Attacks (e.g. Reverse Engineering)
- Overcoming Sensors and Filters
- Perturbation Attacks
- Side-channel Attacks
- Exploitation of Test Features
- Attacks on RNG
- Ill-formed Java Card Applications
- Software Attacks
- ...

Security Evaluation

Common Criteria – JHAS Attack Phases

Identification Phase:

- Perform the attack **once** to demonstrate its feasibility and / or achieve a one-time benefit (learning phase)

Exploitation Phase:

- Perform the attack **multiple times** for commercial exploitation

Information Flow between these Phases:

- One of the outcomes of the Identification Phase is a **virtual script** that tells the attacker of the Exploitation Phase how to perform the attack

Common Criteria for Smart Cards – Rating Tables

Range of values CC 3.x	TOE resistant to attackers with attack potential of:
0-15	No rating
16-20	Basic
21-24	Enhanced-Basic
25-30	Moderate
31 and above	High

We need to achieve 31 points for VLA.4 / VAN.5 (part of EAL 4+, 5+, 6+) for each and every attack path!

"Application of Attack Potential to Smartcards" (developed for JIL by JHAS group)

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Multiple Expert	7	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Very critical hardware design	9	NA
Access to TOE		
< 10 samples	0	0
< 30 samples	1	2
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*
Equipment		
None	0	0
Standard	1	2
Specialized	3	4
Bespoke	5	6
Multiple Bespoke	7	8
Open samples		
Public	0	NA
Restricted	2	NA
Sensitive	4	NA
Critical	6	NA

Bellcore Attack on RSA w/ Countermeasures

Factor	Comment	Identification	Exploitation
Elapsed Time	A glitch perturbation is induced. No sample preparation is needed and a straightforward setup is sufficient to obtain an error.	< 1 day (1)	< 1 hour (0)
Expertise	Without any logical countermeasures, considering the chip can be relatively easily disturbed, a proficient could apply the attack in identification, as well in exploitation.	Proficient (2)	Proficient (2)
Knowledge of TOE	According to the protocol, no specific knowledge of the TOE is required.	Public (0)	Public (0)
Access to TOE (number of samples)	Access to TOE will in practice always be of the order of less than 10 samples.	< 10 (0)	< 10 (0)
Open Samples/ Known Key	Samples with known key won't ease this attack.	NA	NA
Equipment	Fault injection equipment based on glitch induction.	Specialized (3)	Specialized (4)
Sub Total		**6**	**6**
Total	**VAN.1 – "No Rating"**	**12**	

Bellcore Attack on RSA: Countermeasures

Countermeasures in Hardware

- Redundancy, check sums, etc. on the chip level
- Example Secure Fetch (NXP)

Countermeasures in Software

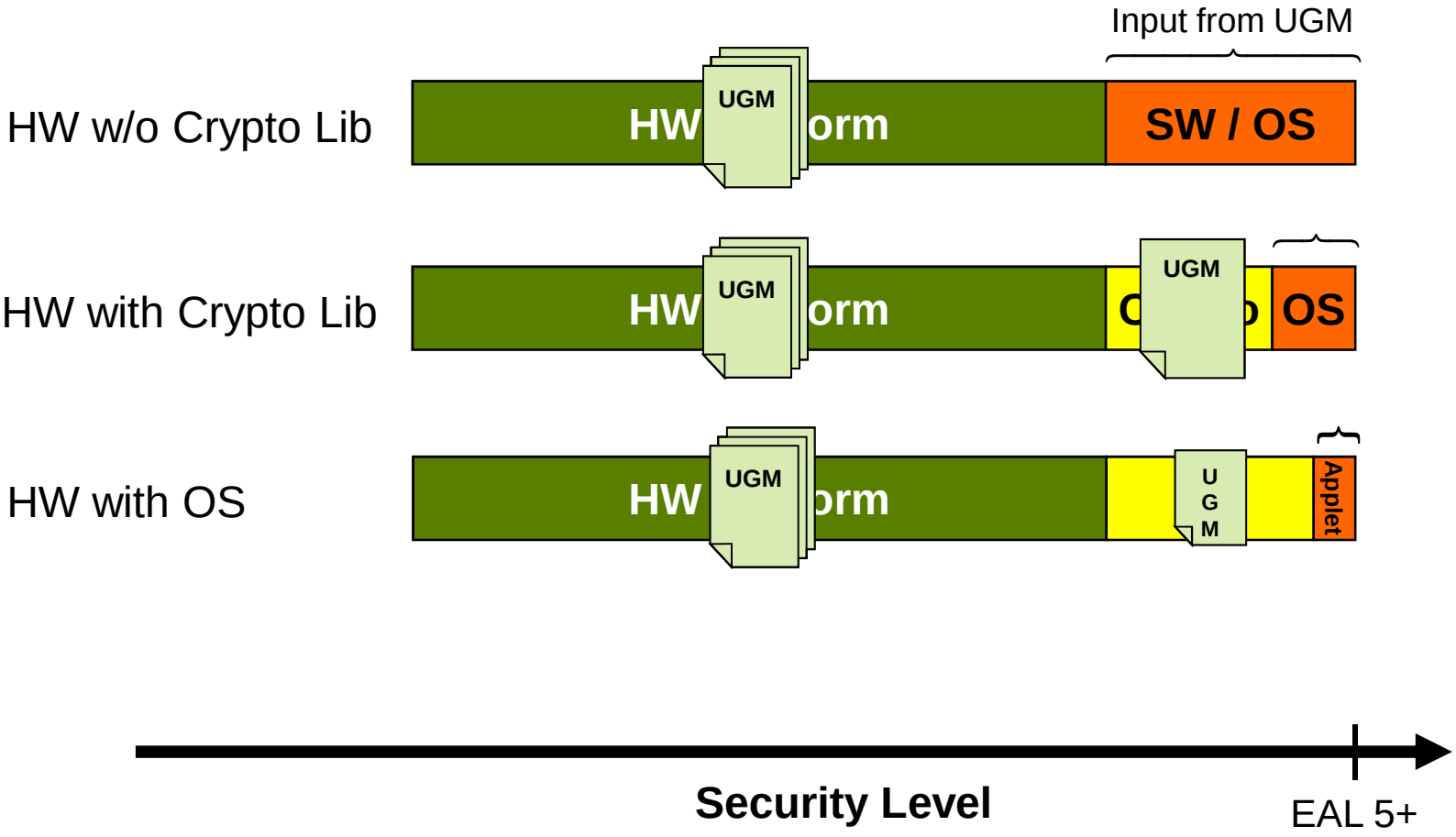
- A guidance on suitable countermeasures in SW may be given in the User Guidance Manual of the HW platform
- The implementation in the customer SW will then have to be tested in the Composite Evaluation
- Example: SW Verification of RSA (and much more…)

Both approaches can lead to an EAL5+ in HW (!)

- It is “simply” a question of where to make the cut in the HW-SW co-design of security features.

HW – SW Co-design

- **Reaching EAL5+ is always a HW/SW co-design effort in CC, so…**
  - EAL5+ != EAL5+… The User Guidance Manual (UGM) does count!



Strategies to Mitigate Risks

Example...

Strategies

- **Make sure the value attached to a single smart card / token is not so large as to make it financially attractive to attack it. This is a system property and not a property of the smart card. Payment systems are a good example for this, with their strong plausibility analysis of financial transactions in the backend.**

- **Develop architectures that defend against entire classes of attacks and not just a single attack (see next slides as an example)**

UMABASA – PUFs Next Gen

Forging an inseparable link between chip and card...

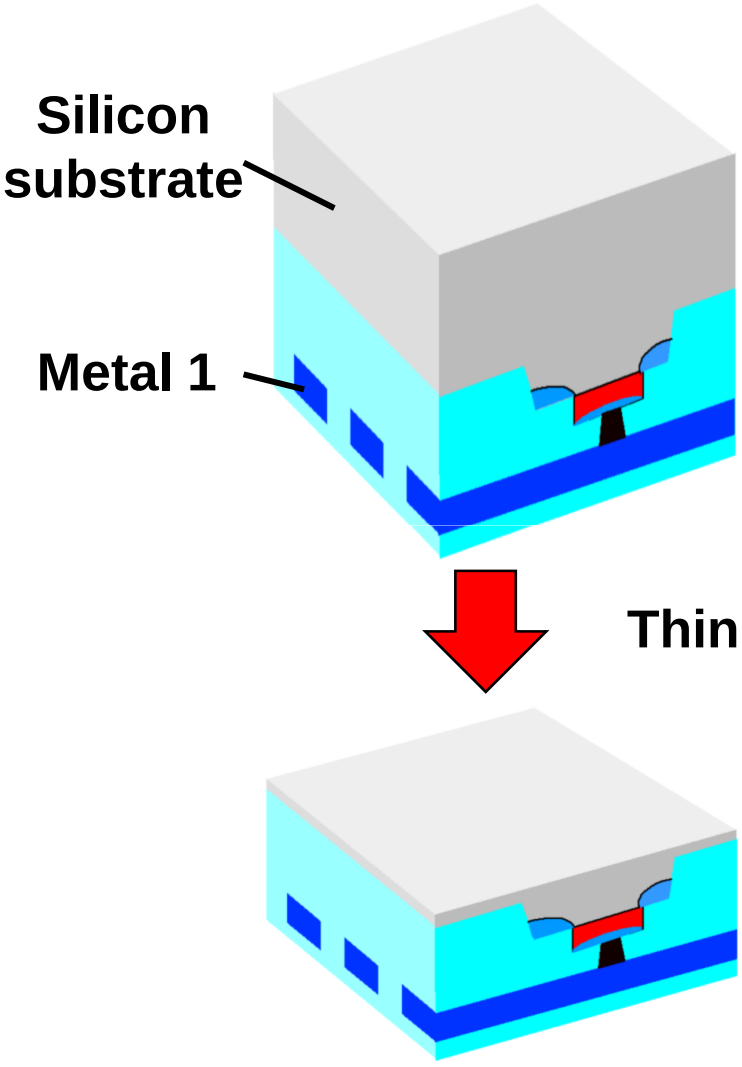
BUNDES DRUCKEREI

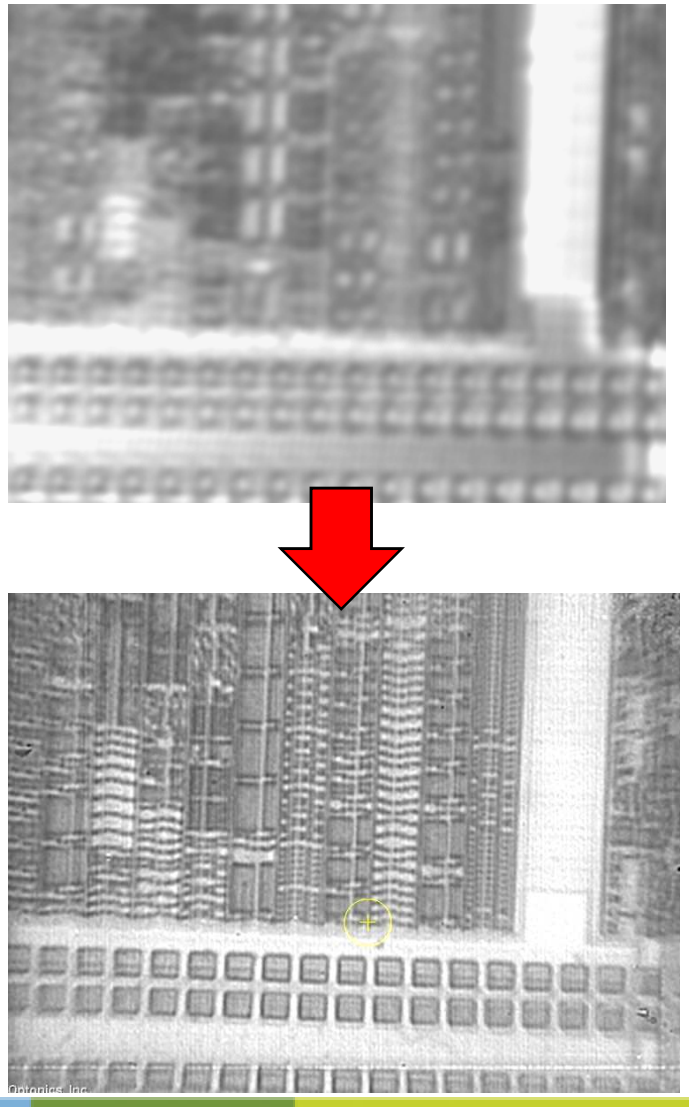
NXP

Fraunhofer SIT Institut Sichere Informations-Technologie

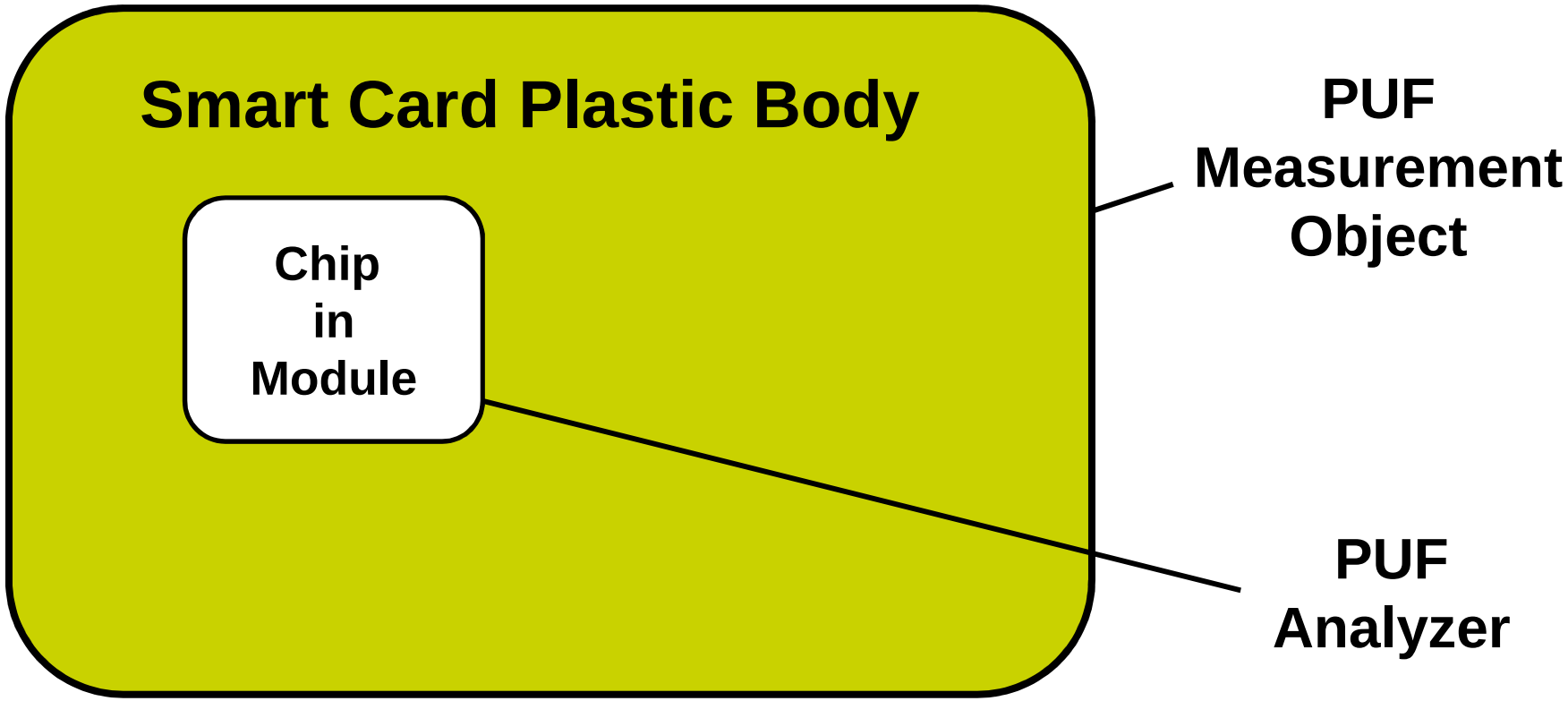
BSI Bundesamt für Sicherheit in der Informationstechnik

Preparation of Chip Backside for Fault Attack



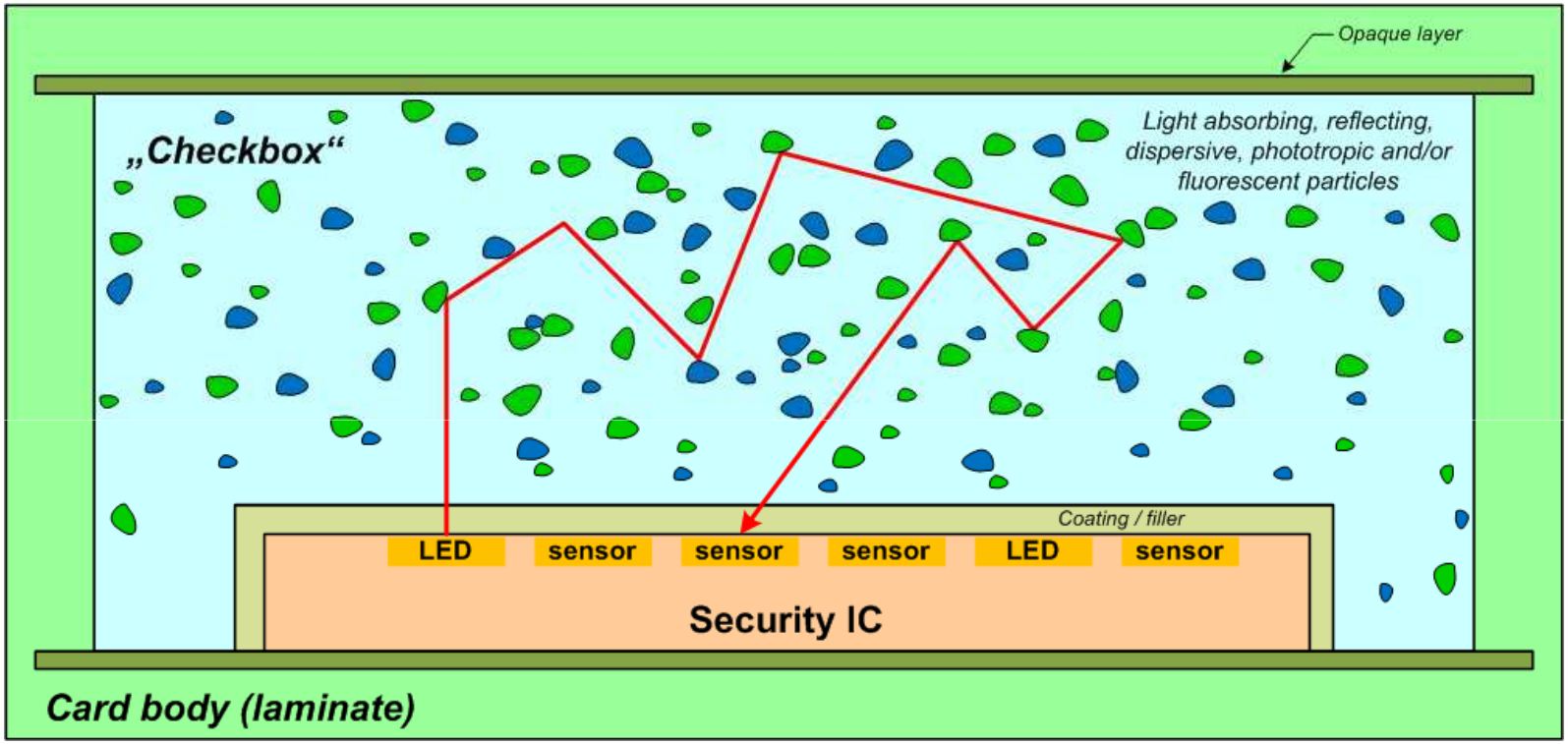


UMABASA Security – Forging the Link



PUF Analyzer & Smart Card Plastic Body are “bound” to each other

UMABASA Security – Forging the Link



PUF Analyzer & Smart Card Plastic Body are “bound” to each other

Summary

Security in Industry – When is Good Good Enough…