ICMC2017

CC for Smart Cards and Mobile Security

Wouter Slegers


Common Criteria

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

brightsight®
the number one security lab in the world

TÜVRheinland®

NLNCSA | Brightsight | Commercial certifier

Your Creative Solutions

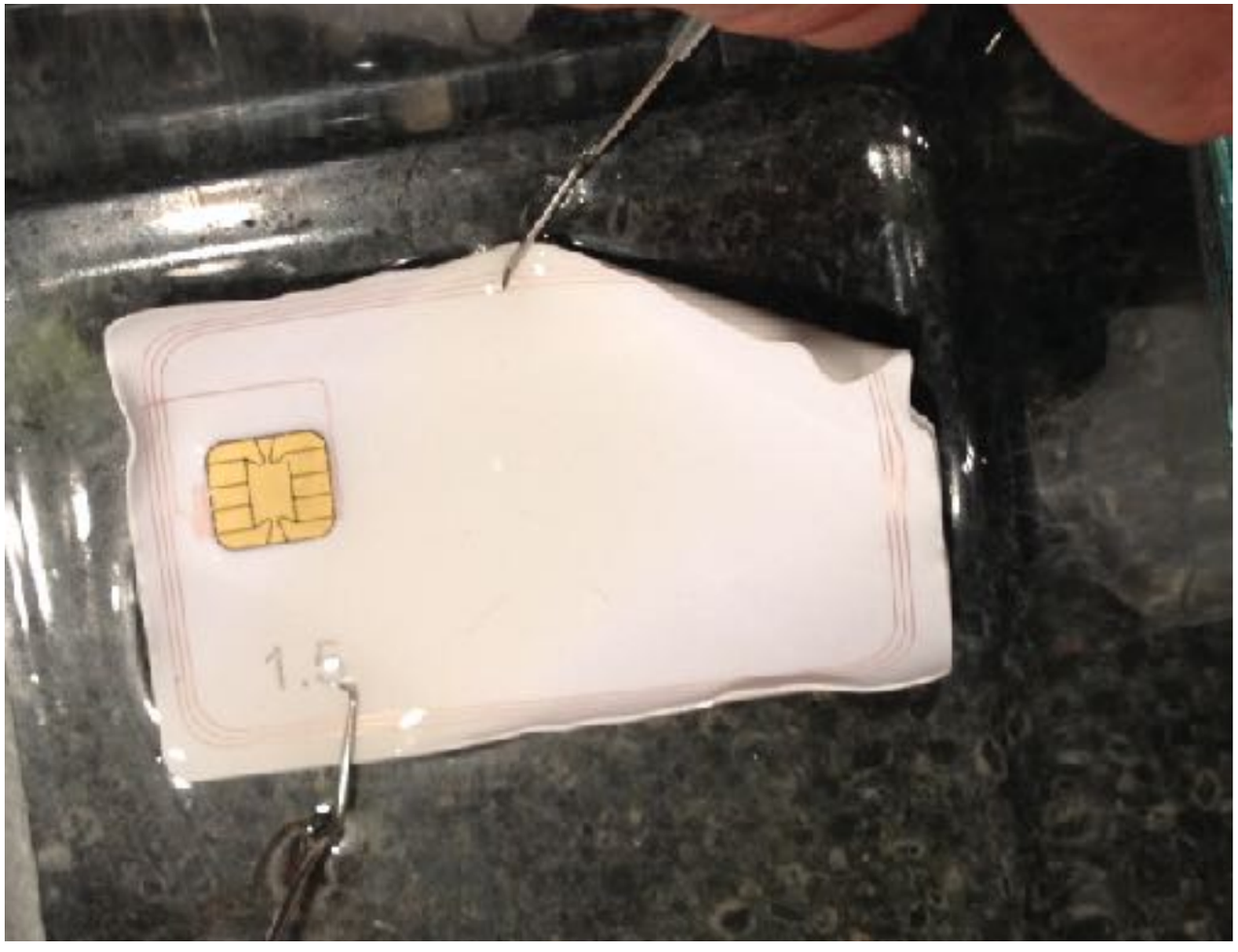
1997 | 2002 | 2009

Accreditation
National Security
Evaluation
NATO
Policy

Common Criteria
Evaluation
Consultancy

EMVco
Courses

Common Criteria
Consultancy
Tools
Training
Smartcards
Certification
Help

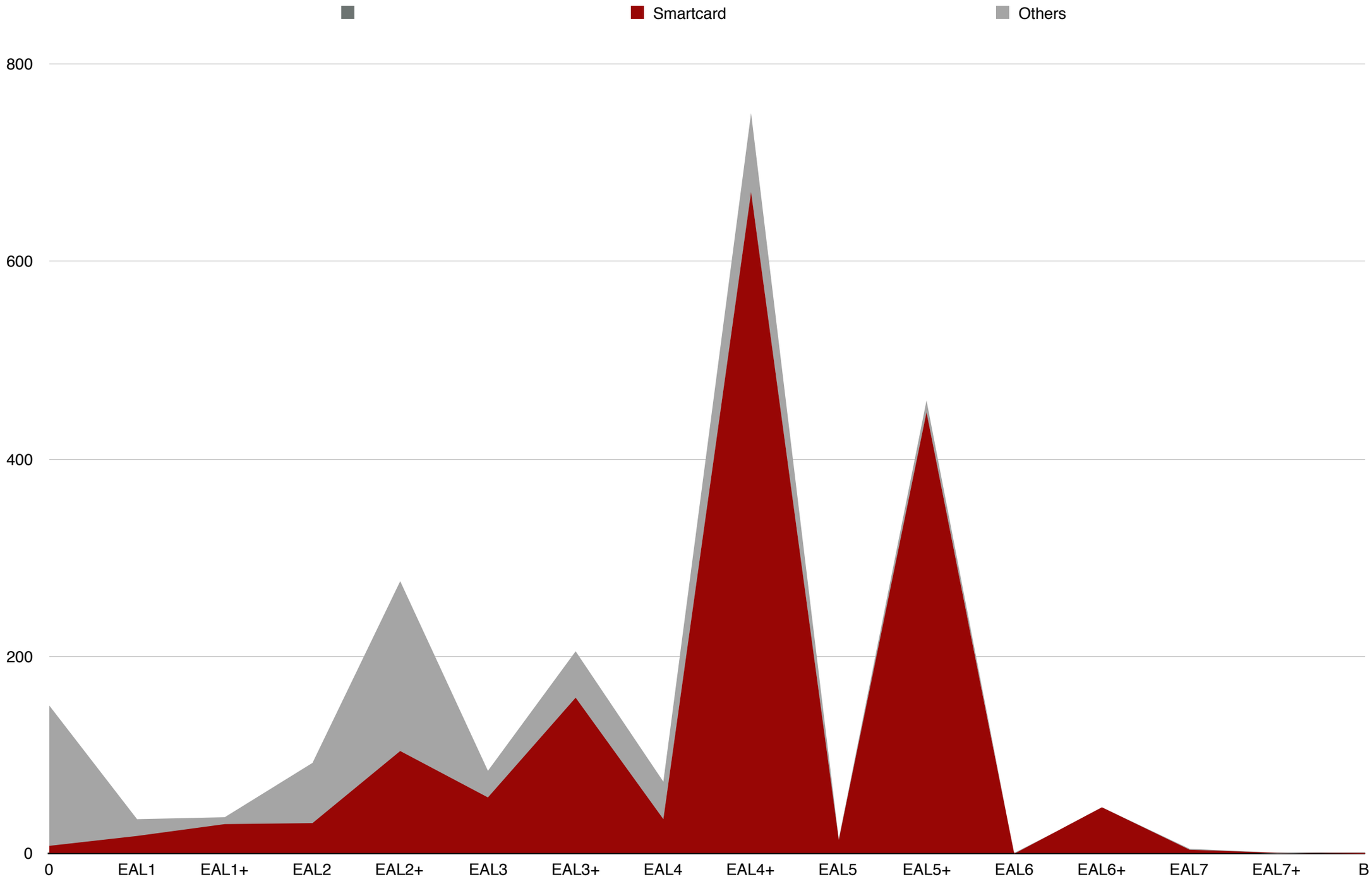


	Smartcard* (1999-now)	last 5 years	last 1.5 years
All	52%	46%	41%
≧EAL4+**	79%	89%	86%
VAN.5***	98%	92%	92%

* excludes smartcards in the “Other devices” (i.e. EU Tachograph), “Products for Digital Signatures” (i.e. EU digital signature cards), “Trusted Computing” (i.e. TPMs format smartcards) etc

** Only impactful augmentations: ALC_FLR.x excluded

*** not all entries specify AVA_VAN levels


Smartcard
Others
800
600
400
200
0
0
EAL1
EAL1+
EAL2
EAL2+
EAL3
EAL3+
EAL4
EAL4+
EAL5
EAL5+
EAL6
EAL6+
EAL7
EAL7+
B

Federal Office for Information Security

TÜVRheinland®

National

EMVCo

VISA

MasterCard Worldwide

Financial

CBs

Federal Office for Information Security

TÜVRheinland®

EMVCo

VISA

MasterCard Worldwide

TSE

CCN

IPA

NSM

CESG

CBs

Federal Office for Information Security

TÜVRheinland®

EMVCo

VISA

MasterCard Worldwide

TSE

CCN

IPA

NSM

CESG

Labs

brightsight

your partner in security approval

T · · Systems ·

SERMA SAFETY & SECURITY

Trusted Labs

Applus LGAI

TÜVIT

Riscure

leti

cea

UL

CBs

Federal Office for Information Security

TÜVRheinland®

EMVCo

VISA

MasterCard Worldwide

TSE

CCN

IPA

NSM

CESG

Labs

brightsight

your partner in security approval

T · · Systems ·

SERMA SAFETY & SECURITY

Trusted Labs

Applus LGAI

TÜVIT

Riscure

leti

cea

UL

Developers

NXP founded by Philips

SAMSUNG

Giesecke & Devrient

life.augmented

gemalto

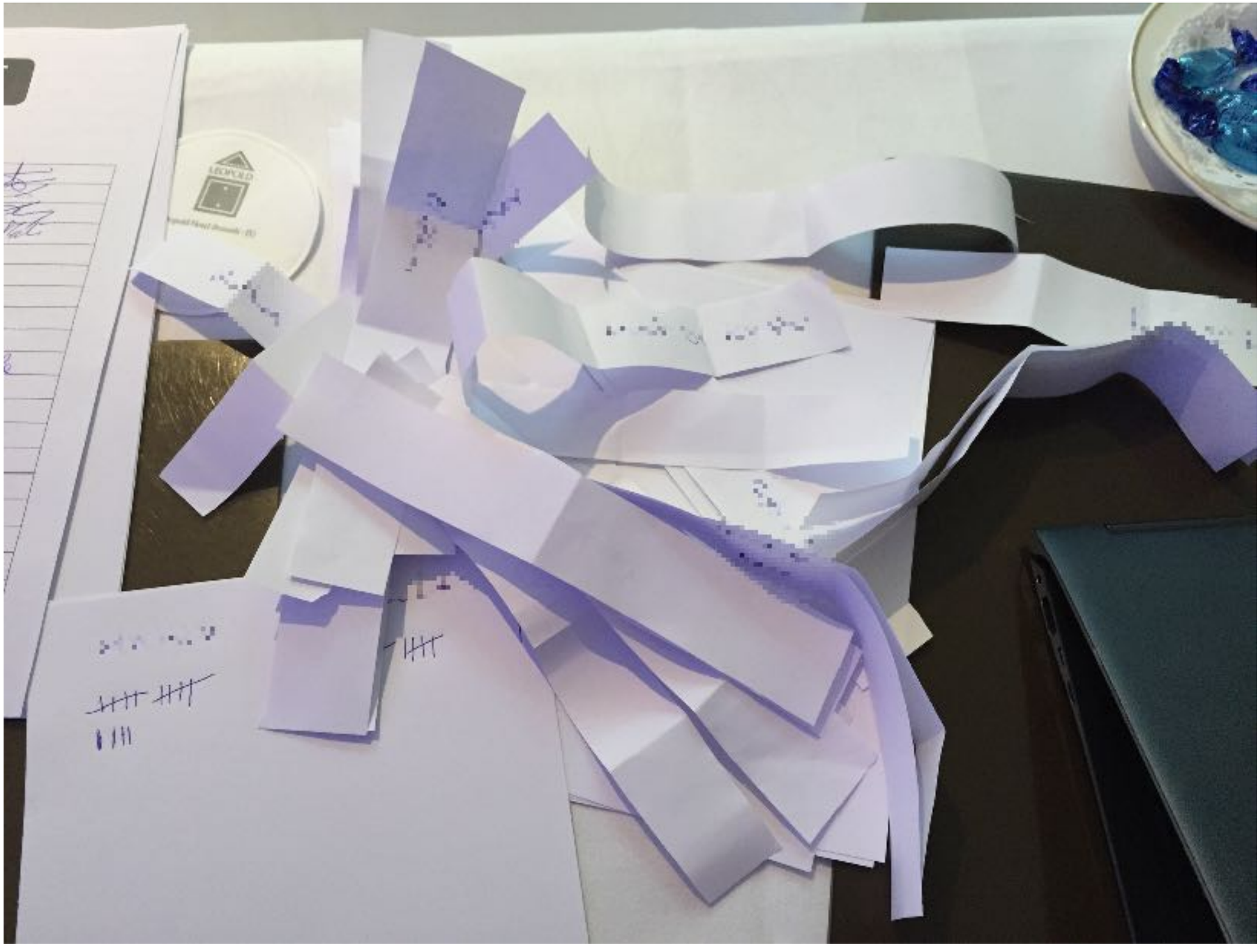
SRC security consulting

inside secure

infineon

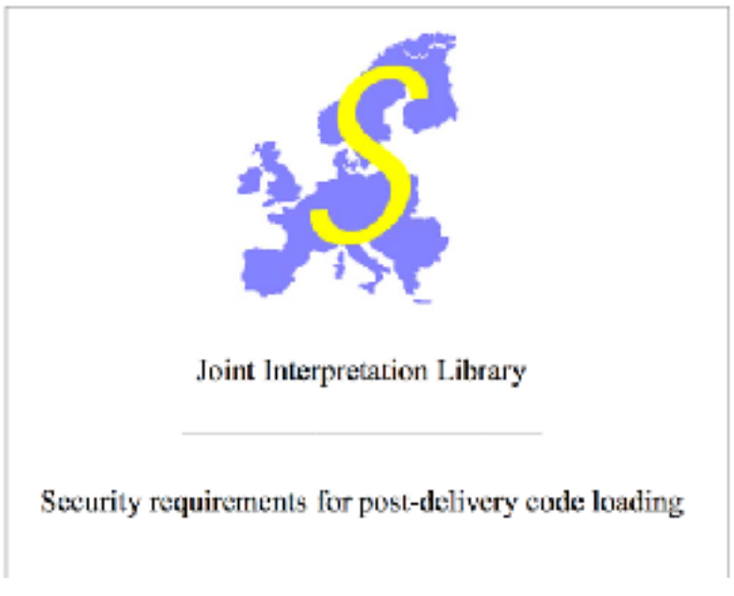
oberthur TECHNOLOGIES THE M COMPANY

SAFRAN Morpho



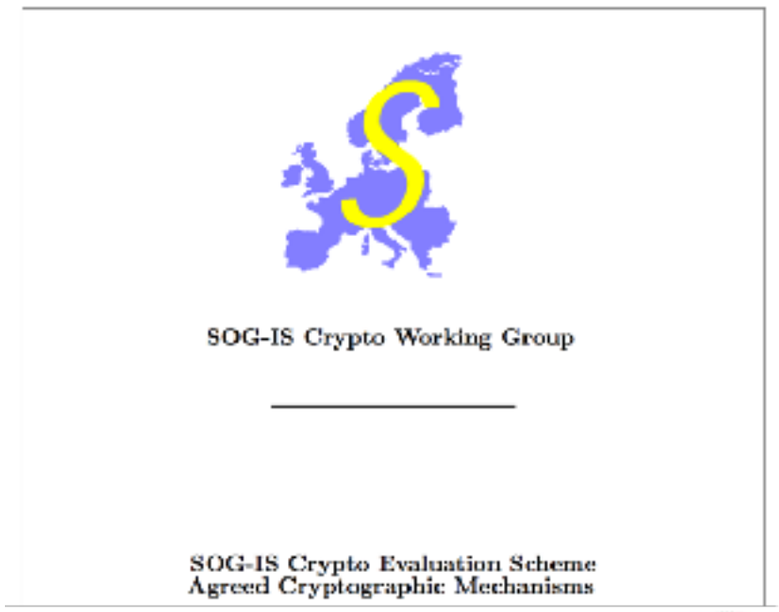

Joint Interpretation Library
Application of Attack Potential to Smartcards


Joint Interpretation Library
Attack Methods for Smartcards and Similar Devices


Joint Interpretation Library
Security requirements for post-delivery code loading


Joint Interpretation Library
Minimum Site Security Requirements

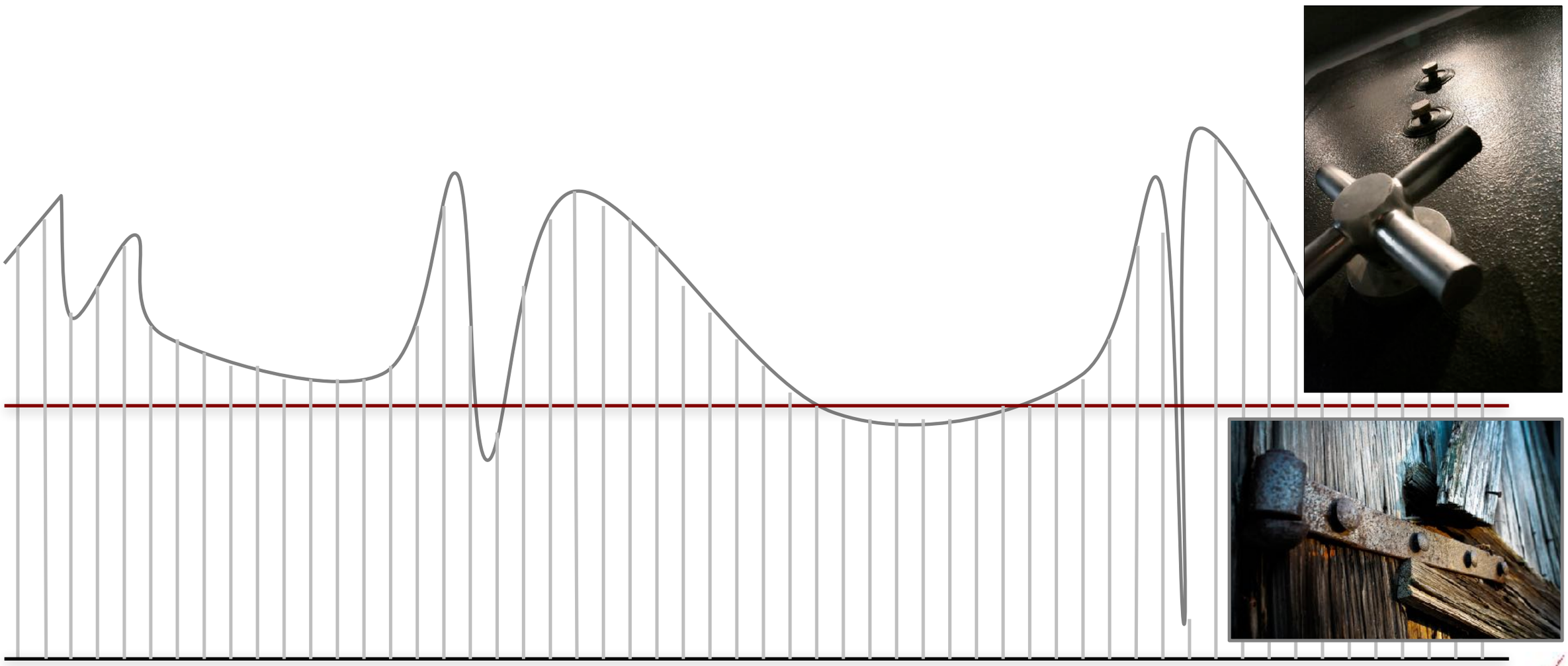

Joint Interpretation Library
Collection of Developer Evidence


SOG-IS Crypto Working Group
SOG-IS Crypto Evaluation Scheme
Agreed Cryptographic Mechanisms

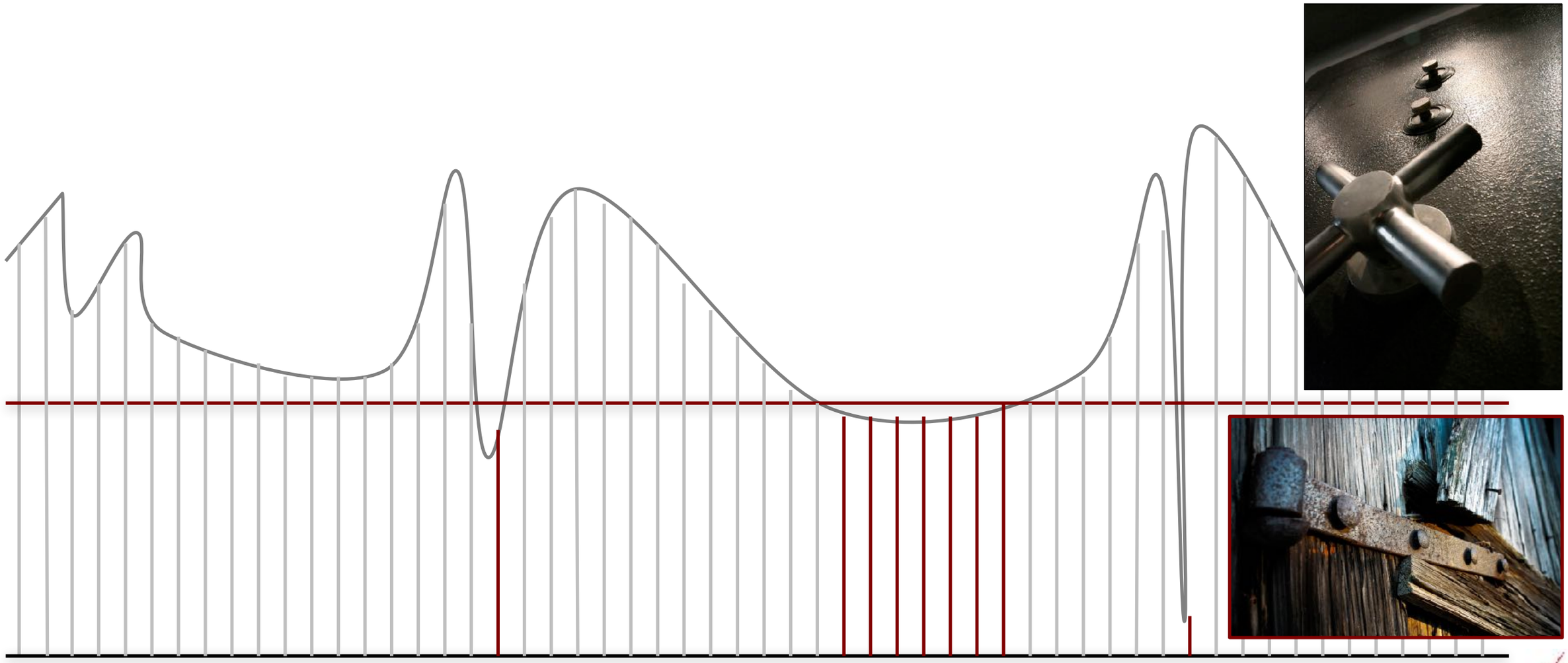

LAWNS
AVAILA

Attacks and ratings

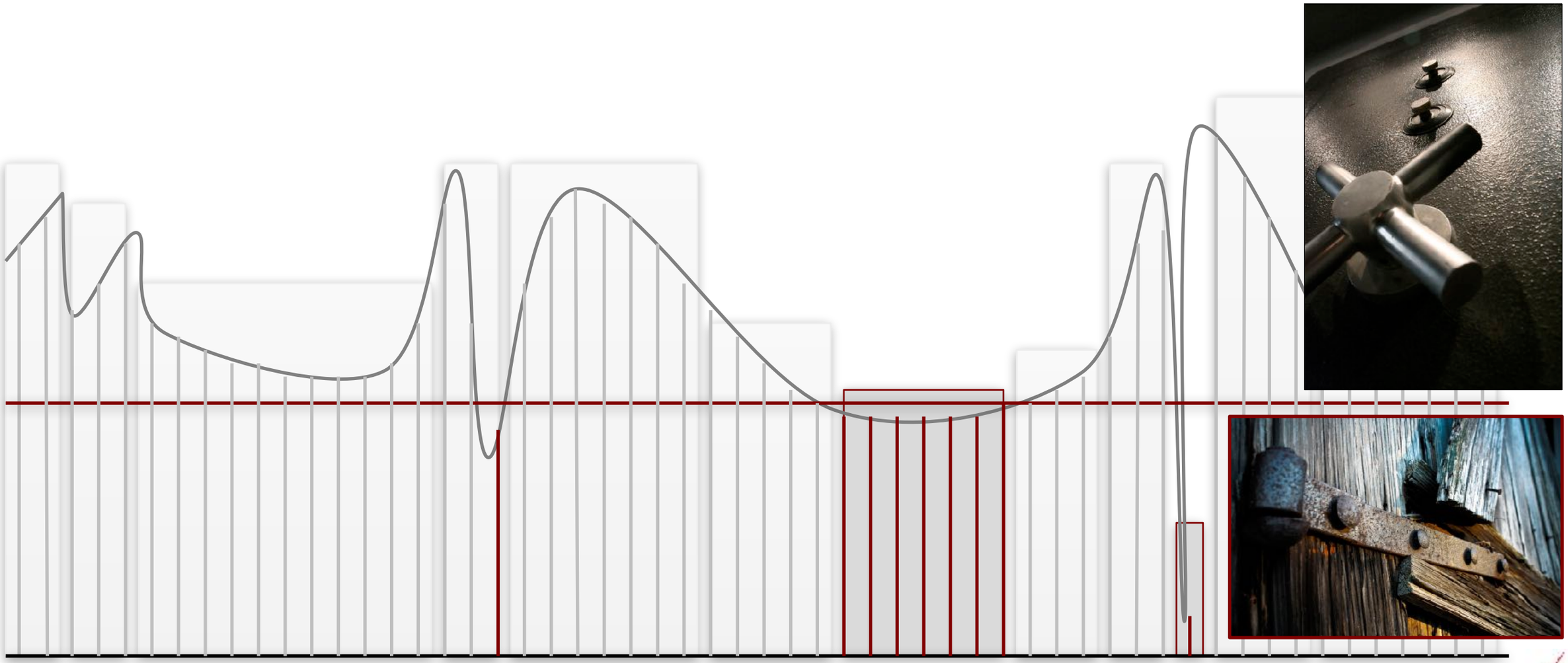
Separating weak from strong



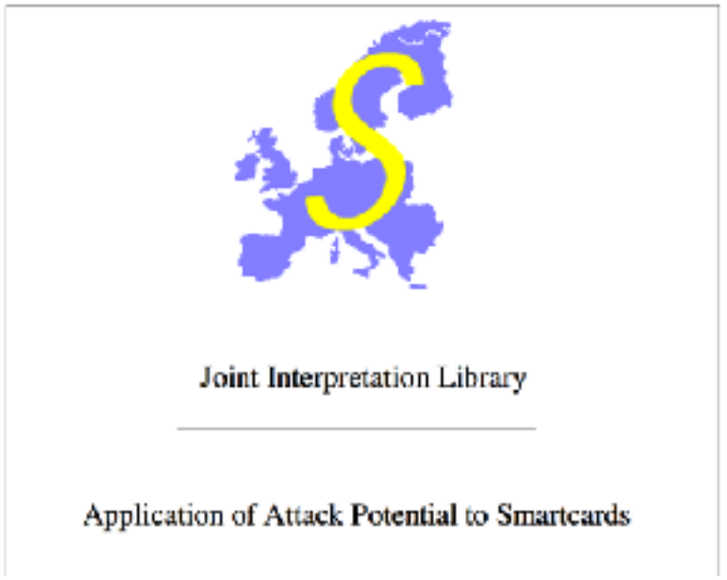
Separating weak from strong



Separating weak from strong



JHAS:
Attack methods and Attack Potential



February 2, 2010

Deconstructing a 'Secure' Processor

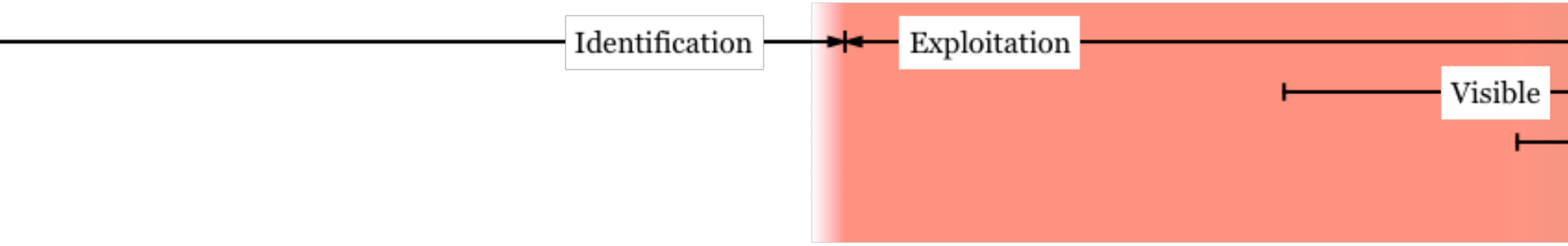
Black Hat – Washington D.C.

Christopher Tarnovsky
Flylogic, Inc.
chris@flylogic.net – http://www.flylogic.net

Black Hat Briefings

Beyond limit of the attacker (31 points)?

	Identification		Exploitation	
	Name	Points	Name	Points
Time	6+ months	5 – ∞	<1 day - <1 week	3 – 6
Expertise	Expert	5	Expert	4
Knowledge	Public - Sensitive	0 - 7	Public	0
Access	< 1000	0 – 3	<10 - <100	0 – 4
Equipment	Specialized-bespoke	3 – 5	Specialized - bespoke	4 – 6
Open samples	None	0	-	-
Sub total		13 – ∞		11 – 20
			Total	24 – ∞


Identification
Exploitation
Visible

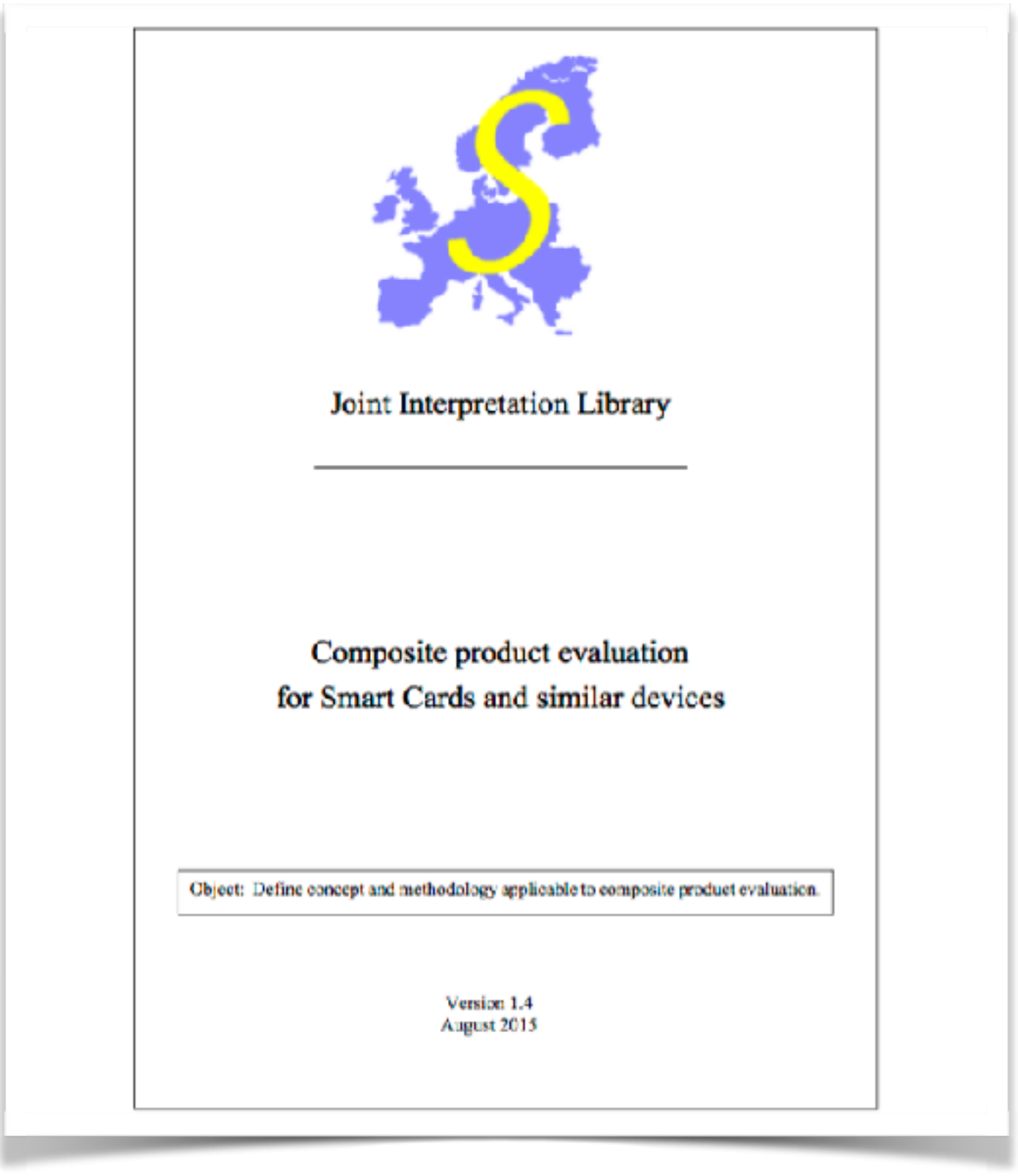
Joint Interpretation Library

Minimum Site Security Requirements

SOG-IS Crypto Working Group

SOG-IS Crypto Evaluation Scheme
Agreed Cryptographic Mechanisms


EUROPESE UNIE
KONINKRIJK DER NEDERLANDEN
PASPOORT

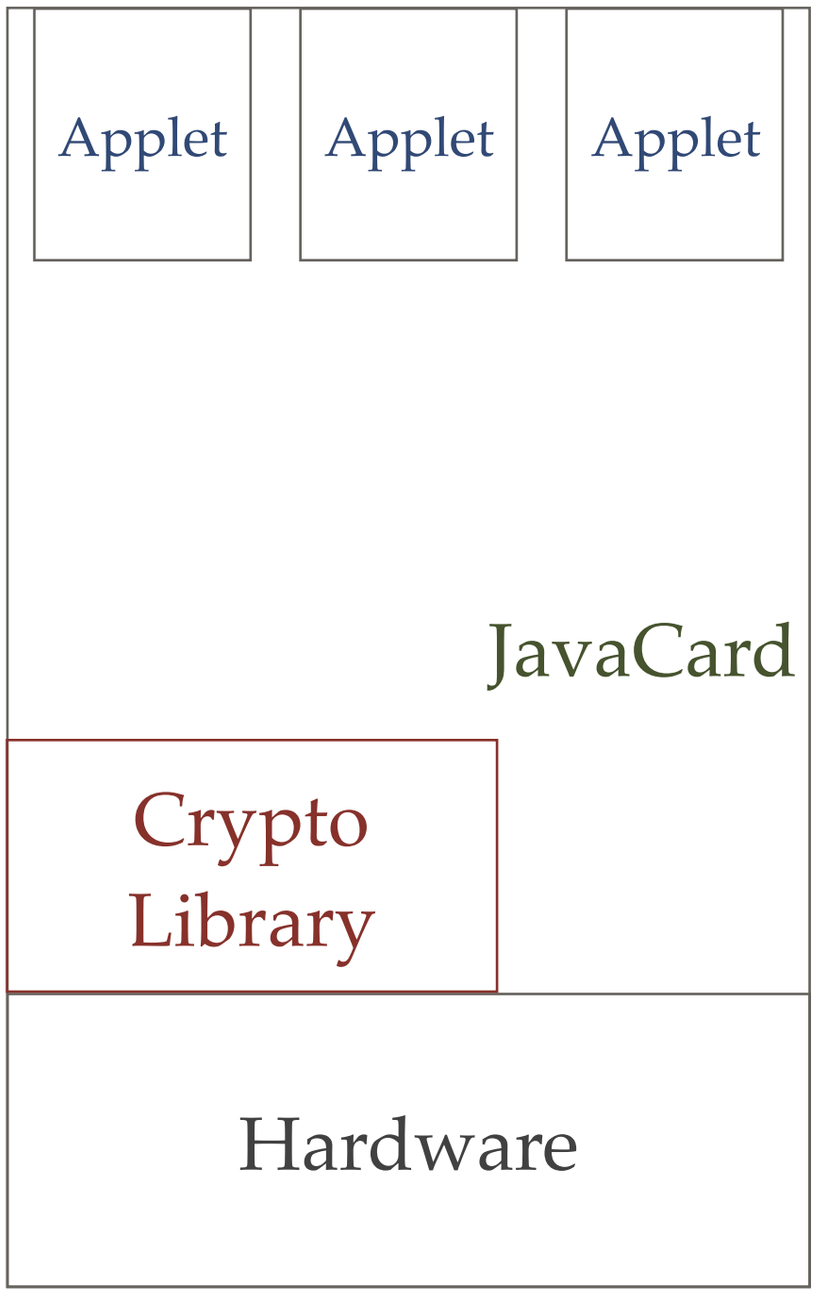


Joint Interpretation Library

Composite product evaluation
for Smart Cards and similar devices

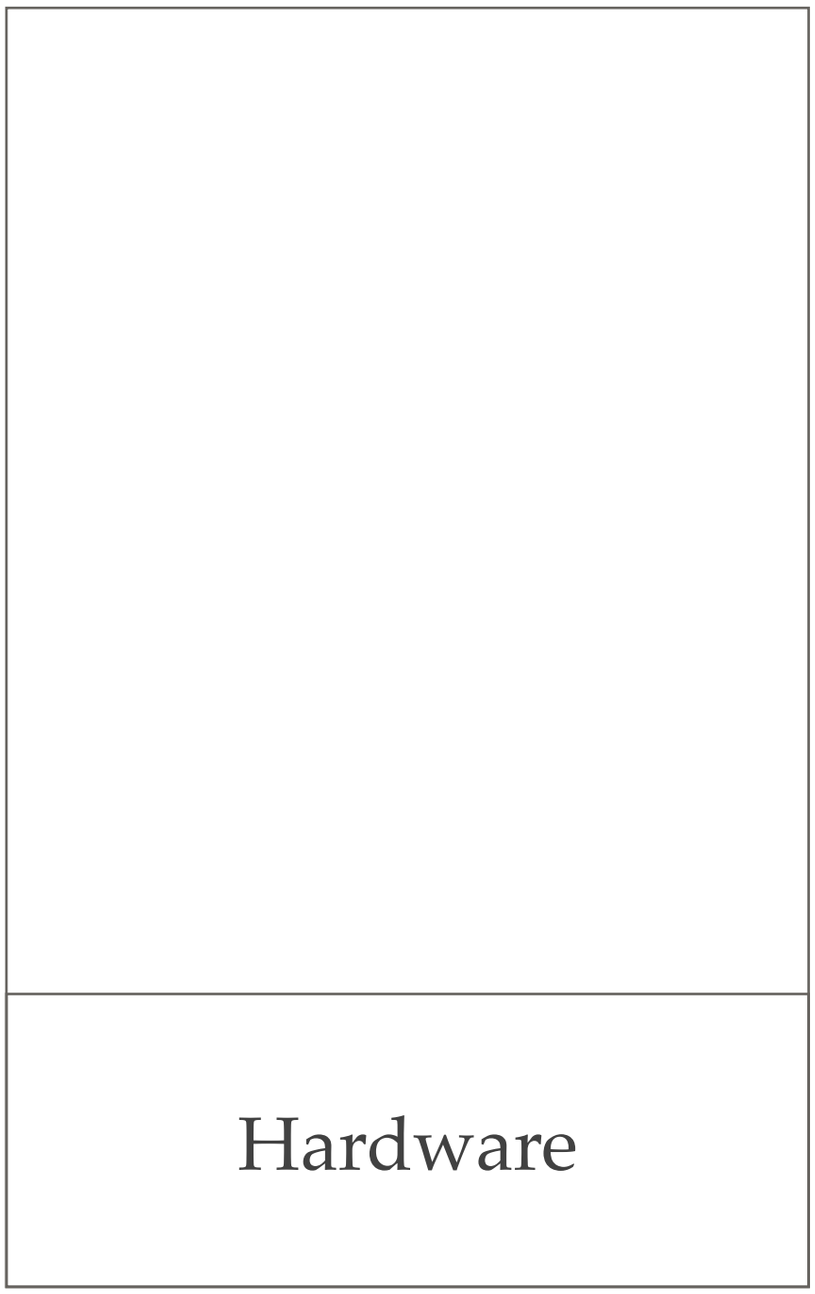
Object: Define concept and methodology applicable to composite product evaluation.

Version 1.4
August 2015



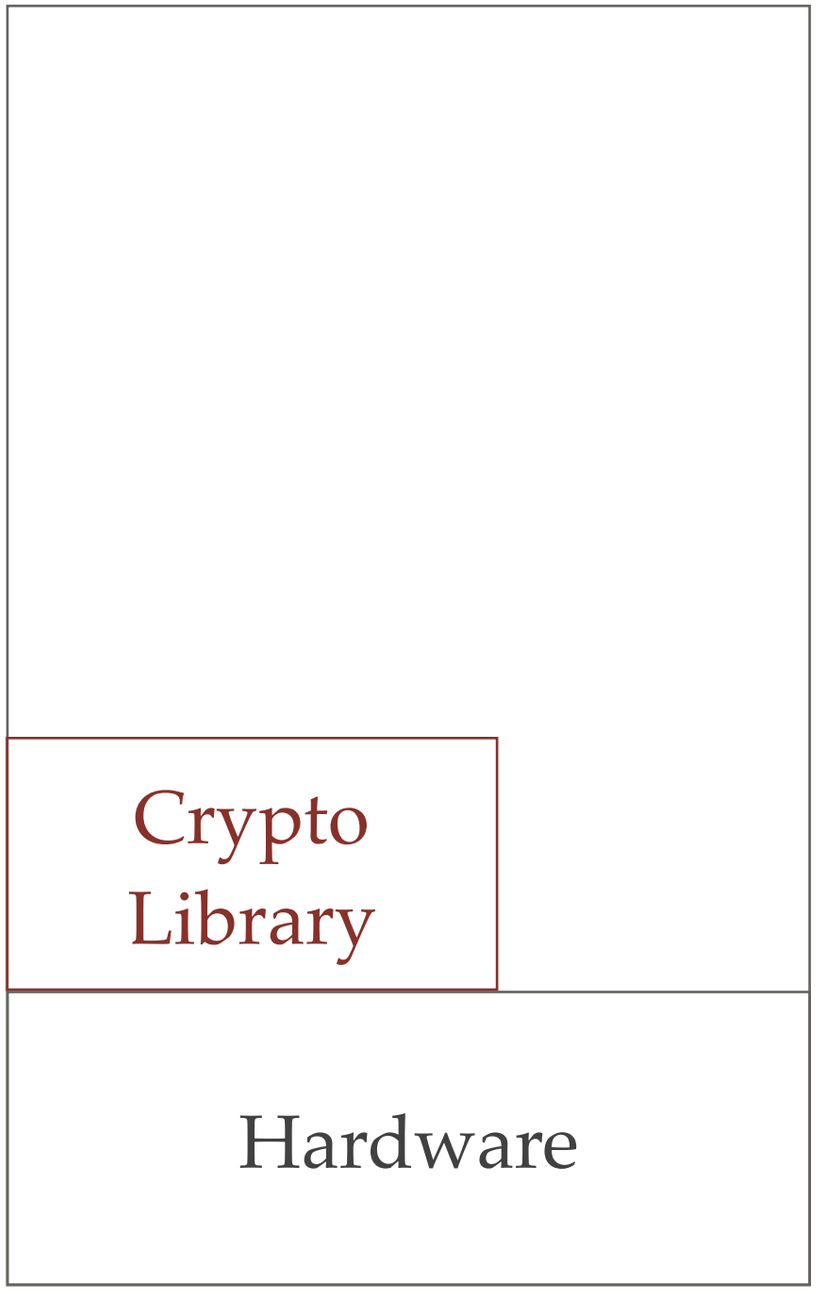
Hardware:

- PP-0035/0084
- Promises:
  - Protection from outside*
  - Crypto does not leak*
  - Possibility to make secure software*



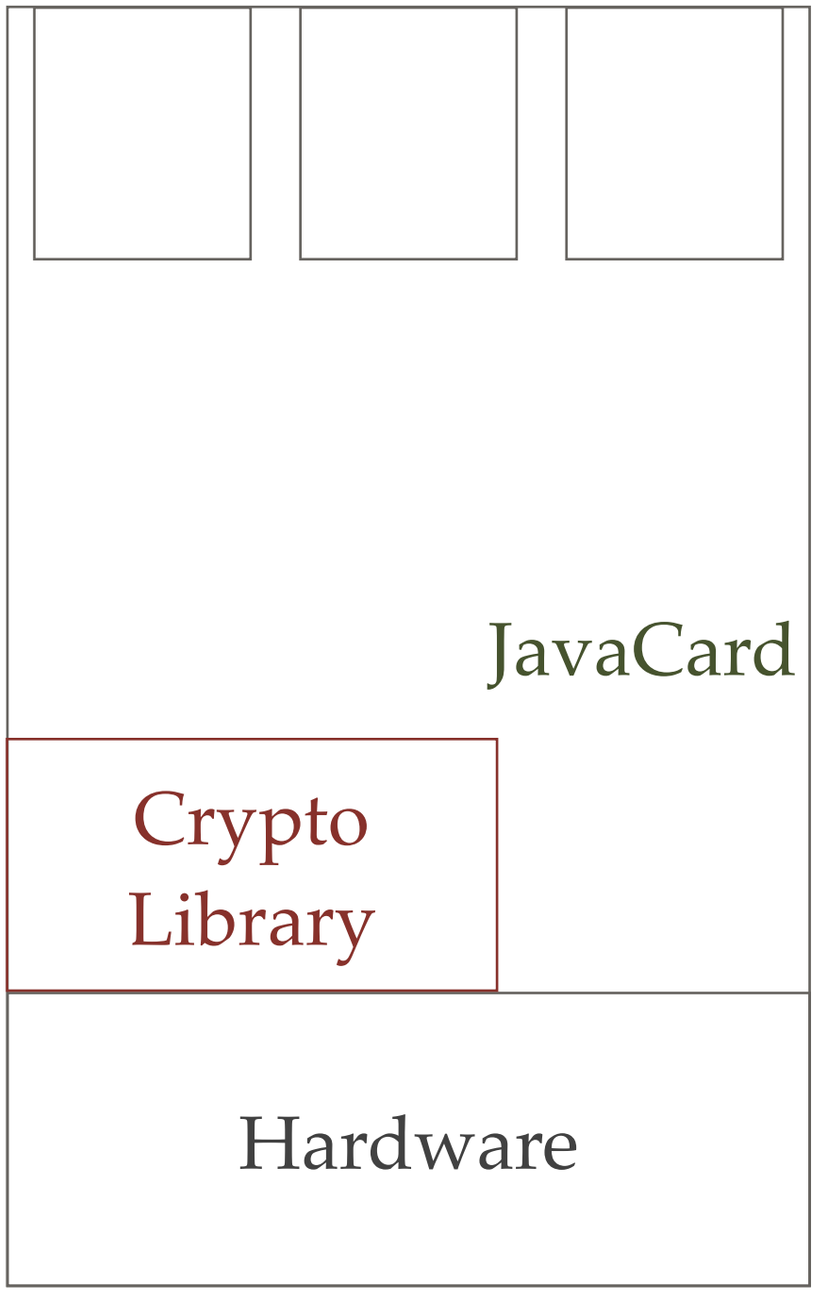
IC+Crypto lib:

- PP-0035/0084
  - + Packages
- Promises:
  - Protection from outside*
  - Crypto does not leak*
  - Possibility to make secure software*



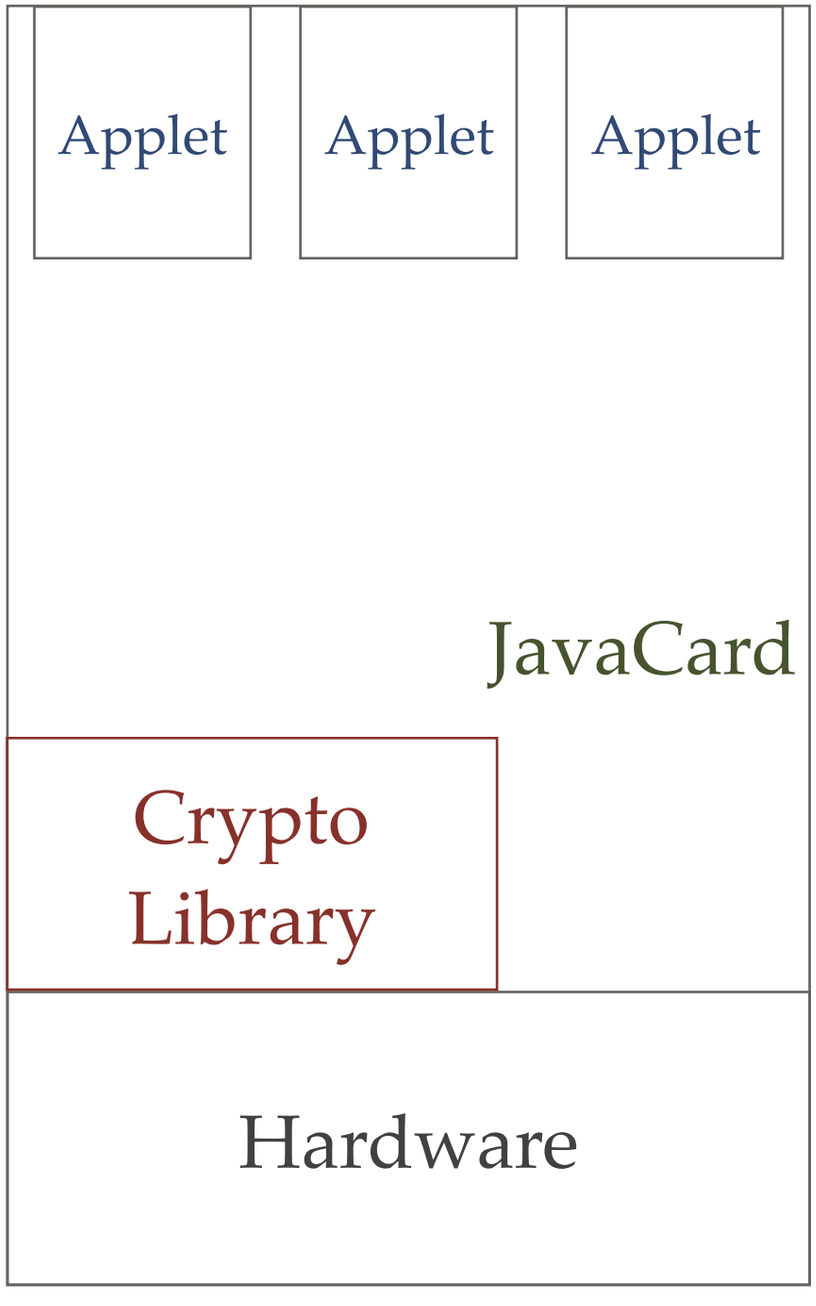
JavaCard:

- HW+Crypto Library+JavaCard
- Java Card PP (Open/Closed configuration)
- Promises:
  - Applets are protected from each other*
  - Applets are protected from outside*
  - Standard crypto is available



Full smart card:

- ePassport (“MRTD”: Machine Readable Travel Document)
- Digital Signature cards (“SSCD”: Secure Signature Creation Device)
- Digital Tachograph
- Travel systems (Mifare)
- Payment cards

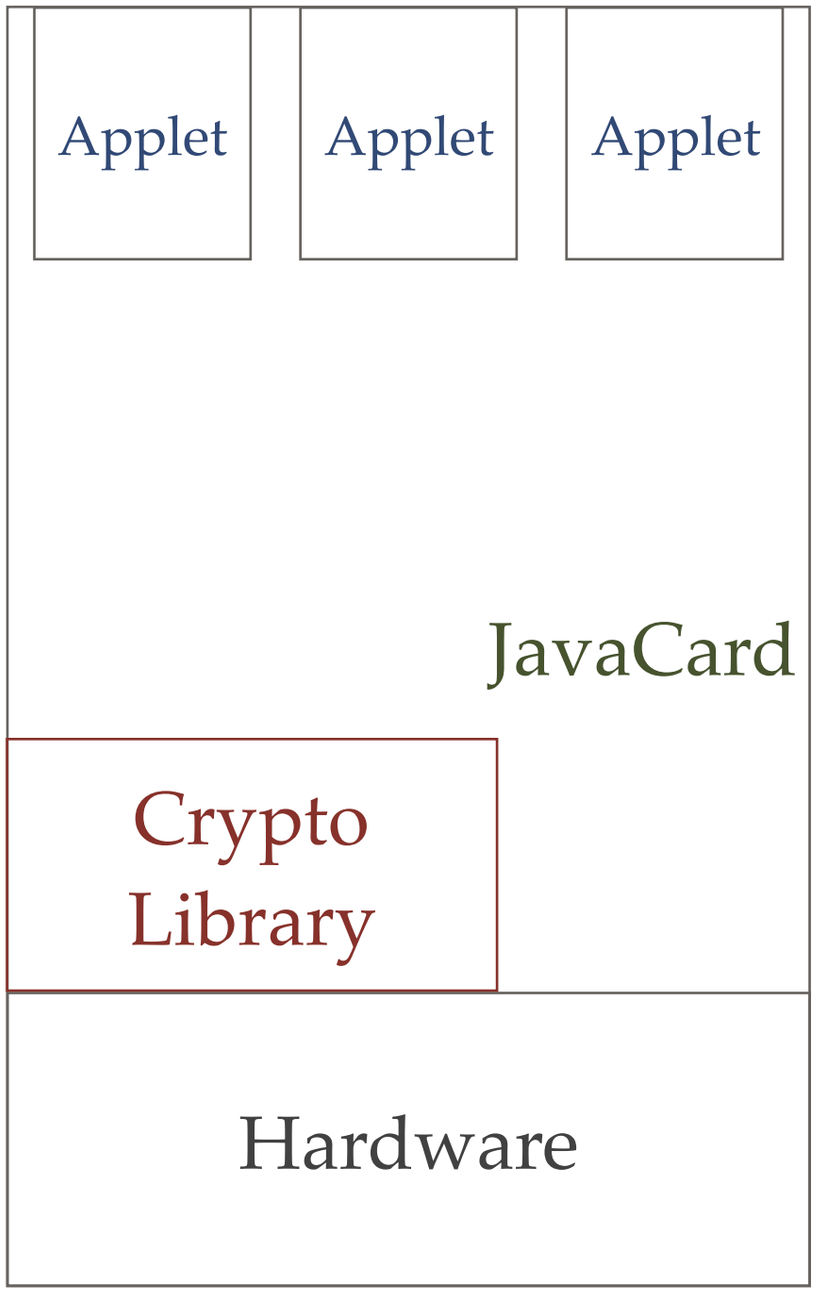


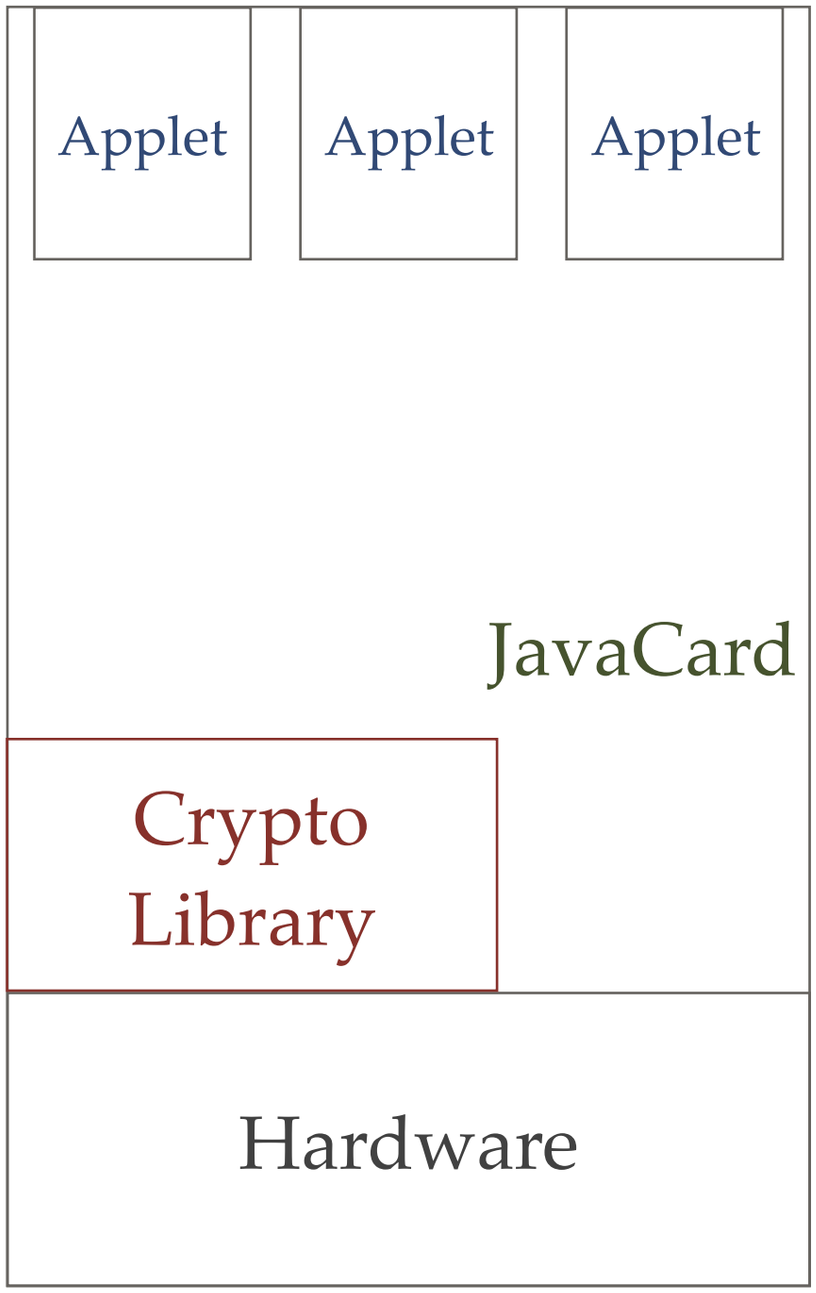
Composition advantages:

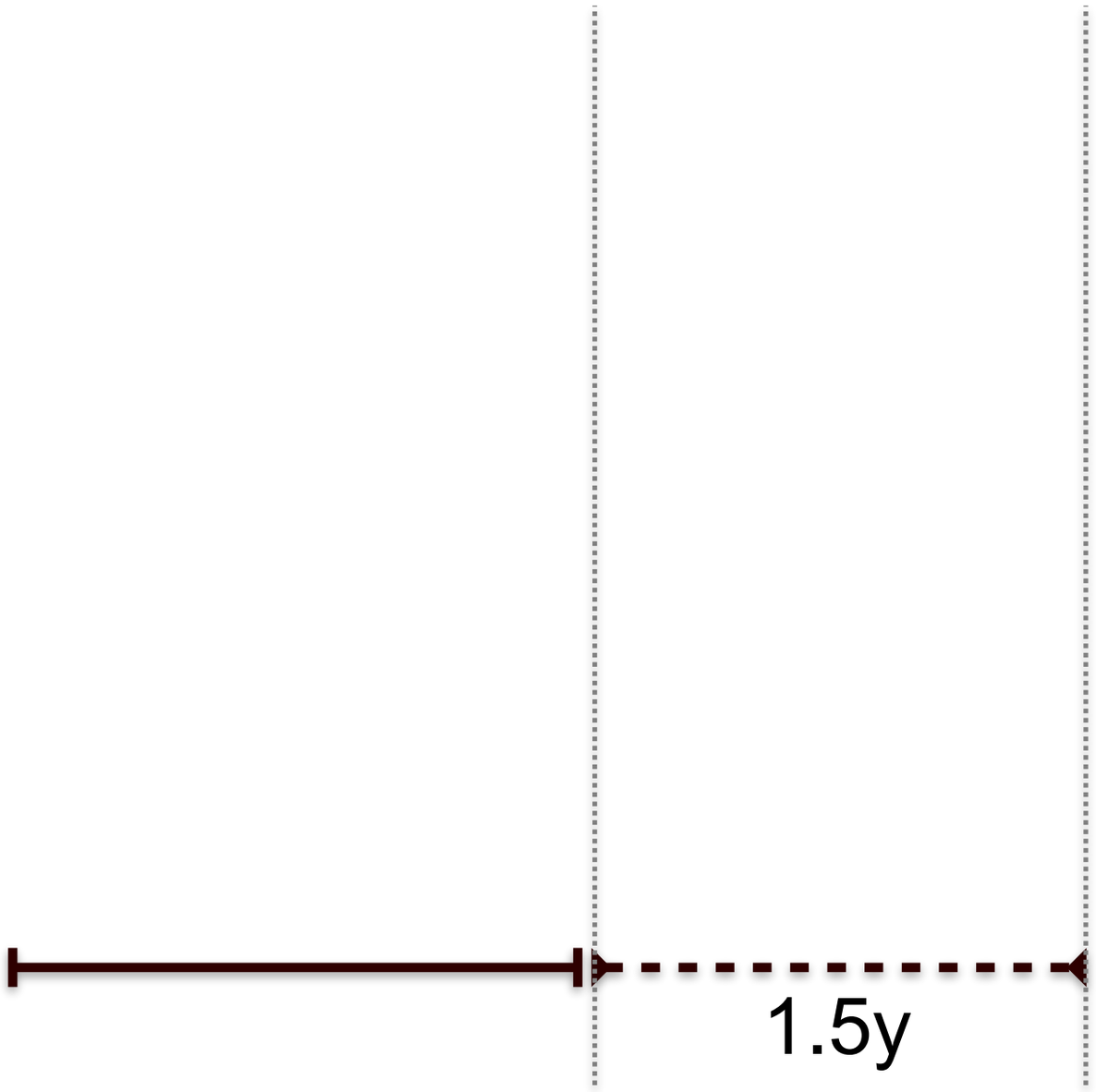
- Efficient re-use of certifications
- Different developers / labs / certification bodies possible

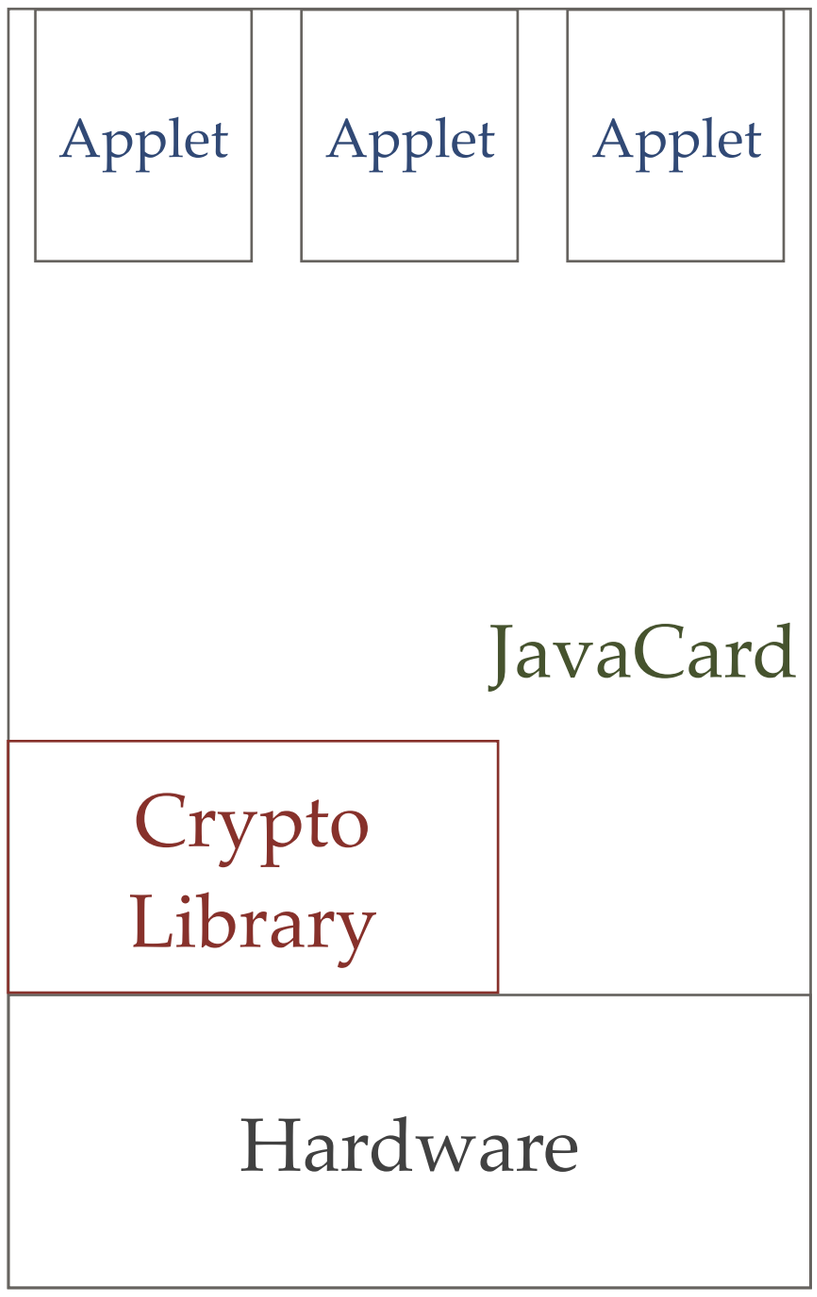
Costs

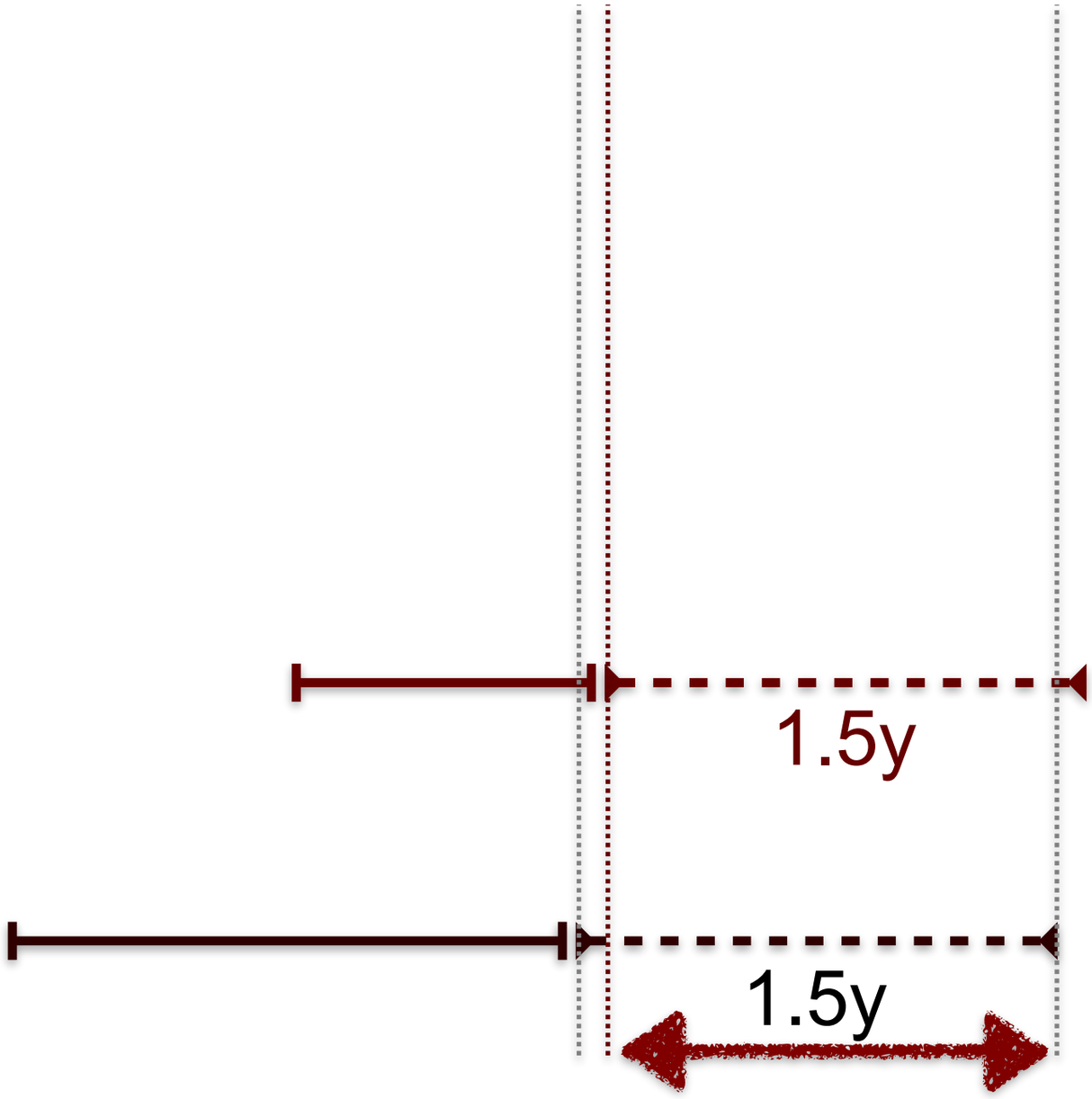
- Dependencies between projects

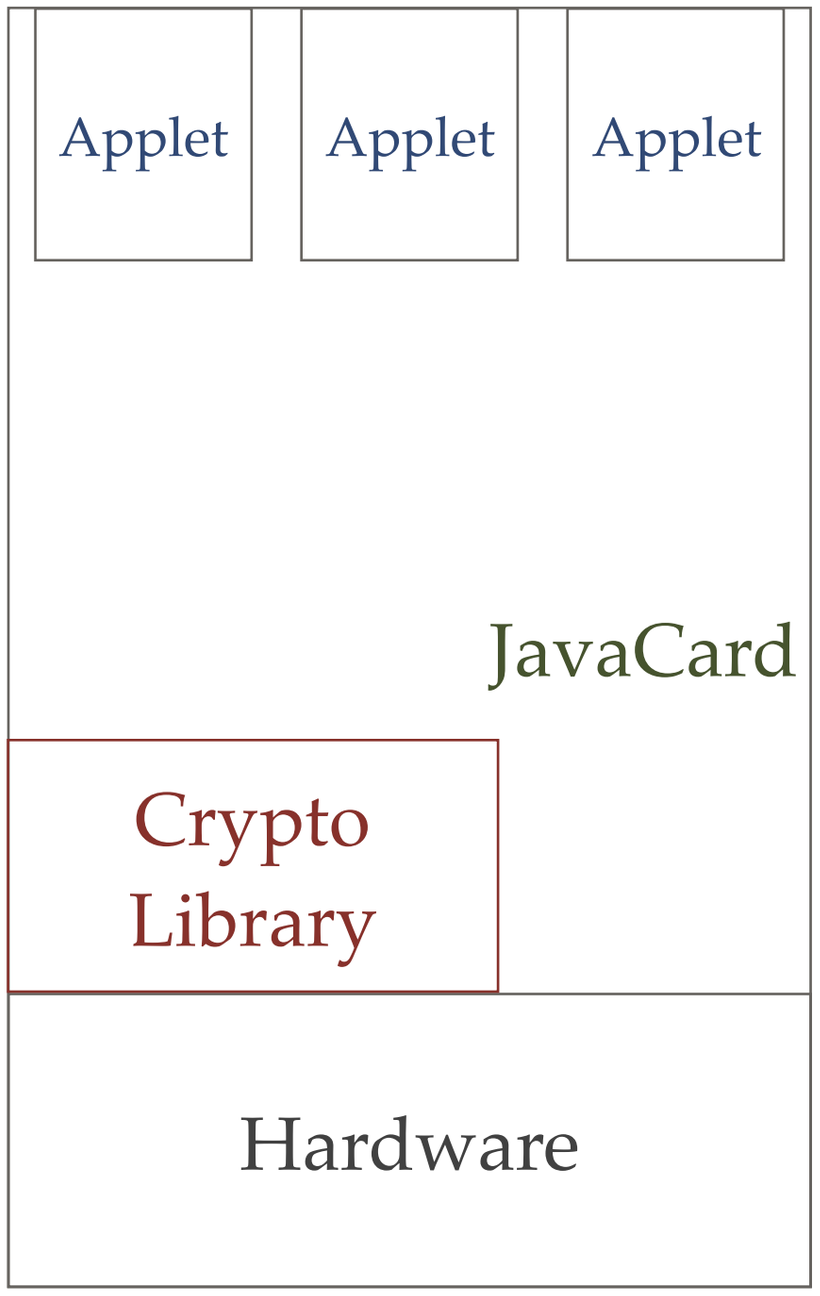


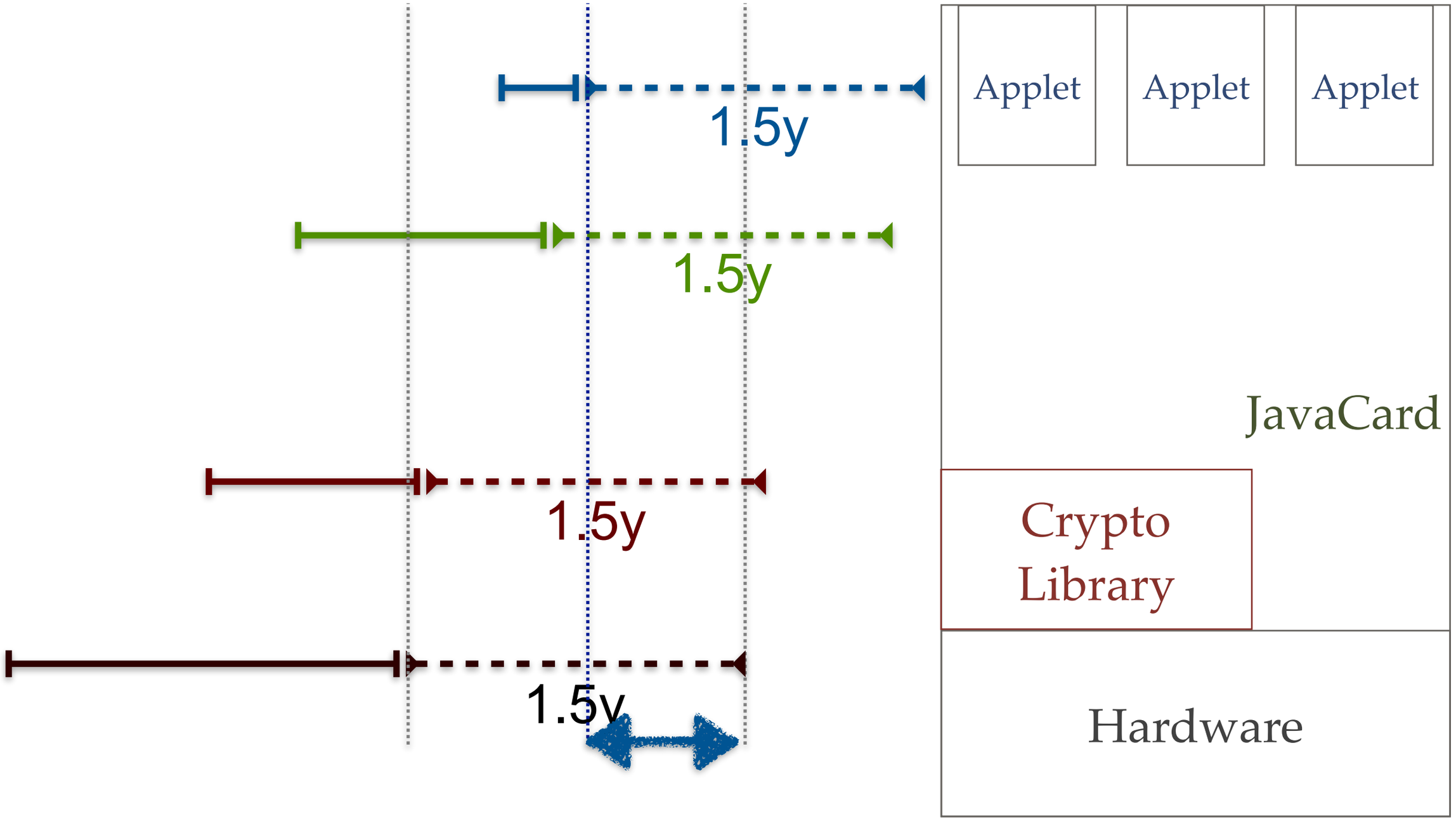

Applet
Applet
Applet
JavaCard
Crypto
Library
Hardware

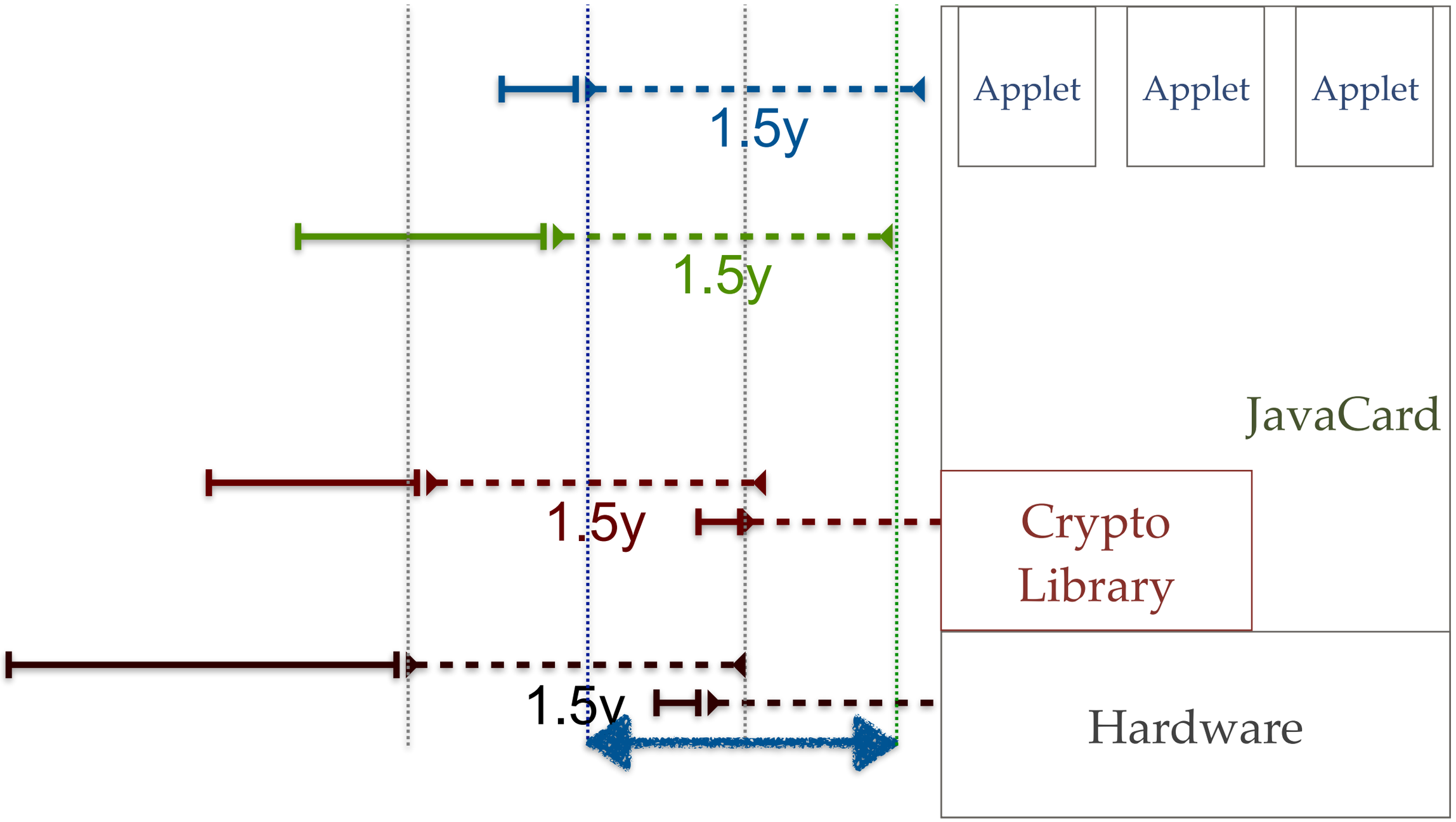

1.5y


Applet
Applet
Applet
JavaCard
Crypto
Library
Hardware

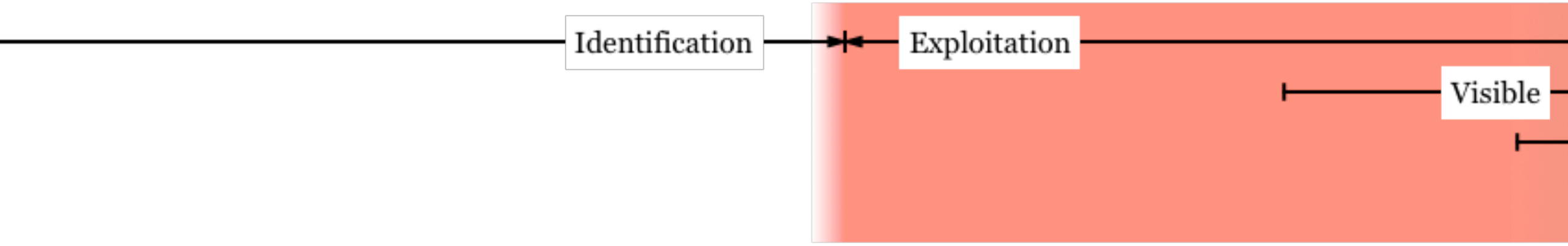

1.5y
1.5y

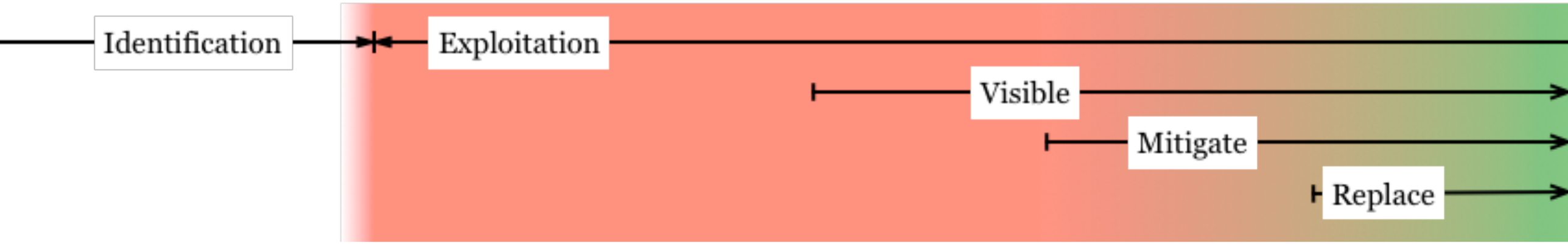

Applet
Applet
Applet
JavaCard
Crypto Library
Hardware

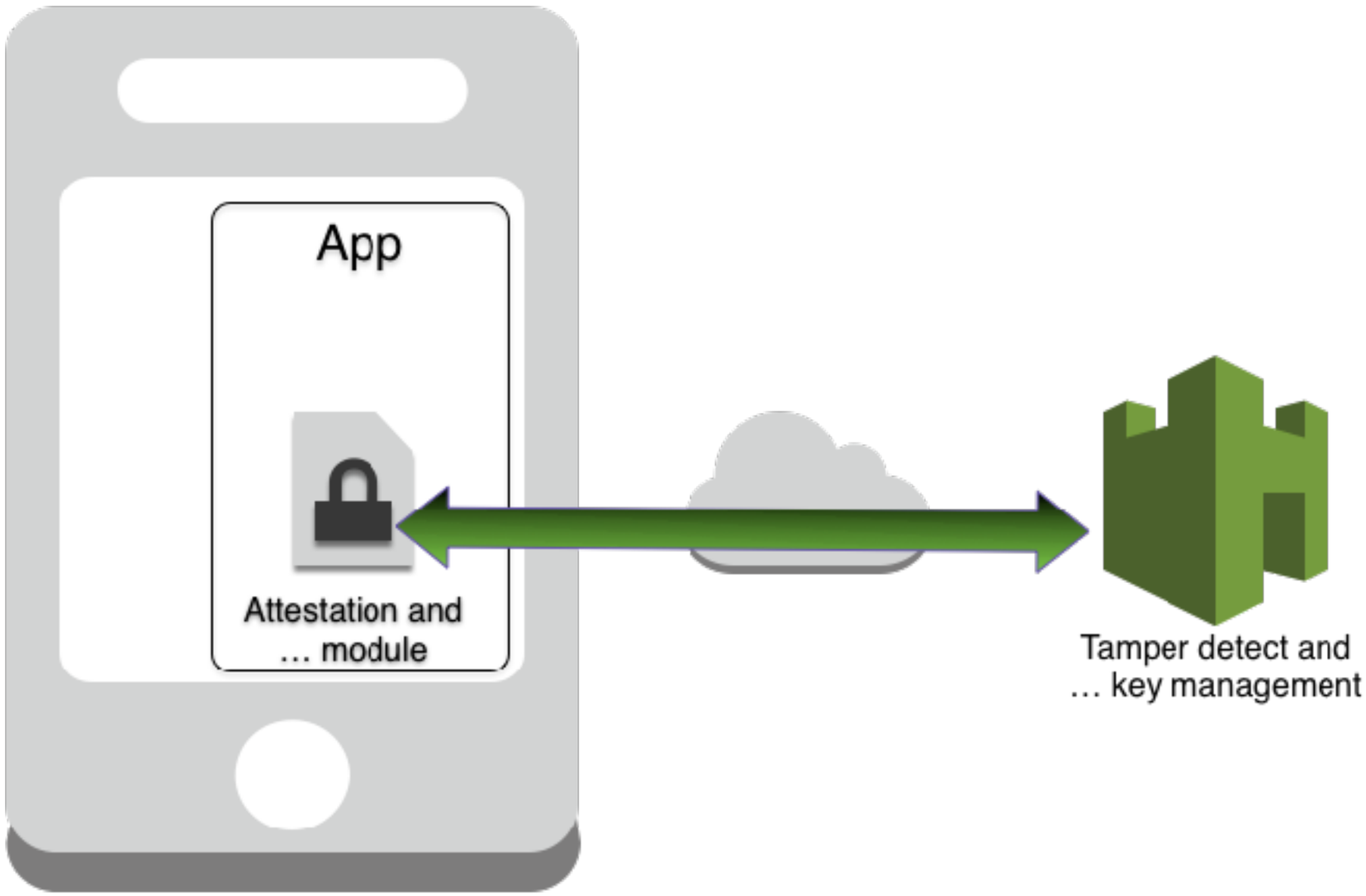

1.5y
1.5y
1.5y
1.5y
Applet
Applet
Applet
JavaCard
Crypto
Library
Hardware

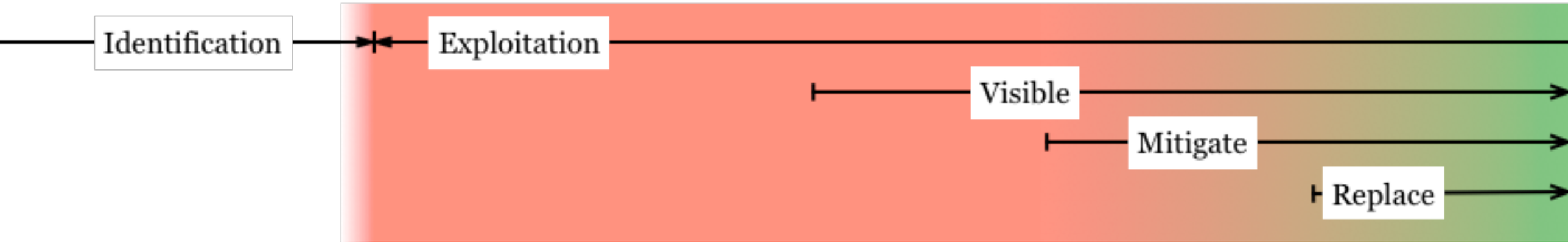

1.5y
1.5y
1.5y
1.5y
Applet
Applet
Applet
JavaCard
Crypto
Library
Hardware

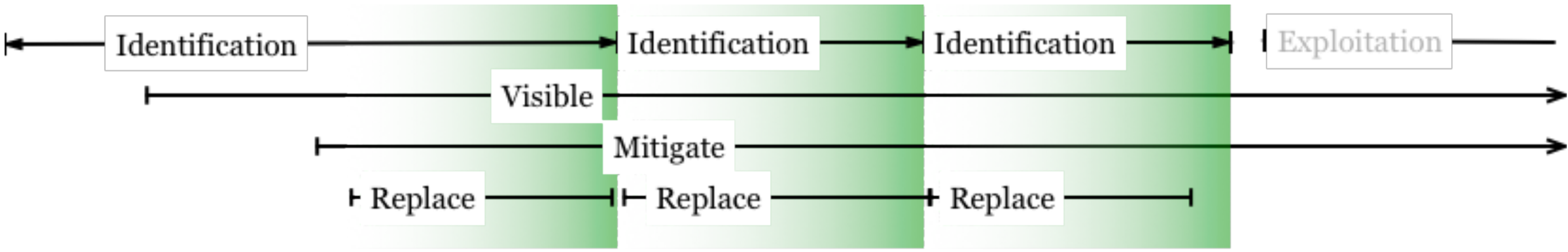

No key needed to access the mezzanine level
access the elevator
use Digital Key in the Hilton Honors app
Elevator
7
8
5
6
3
4
L
M


Identification
Exploitation
Visible


Identification
Exploitation
Visible
Mitigate
Replace


App
Attestation and
… module
Tamper detect and
… key management


Identification
Exploitation
Visible
Mitigate
Replace


Identification
Identification
Identification
Exploitation
Visible
Mitigate
Replace
Replace
Replace

Beyond **time** limit of the attacker (>3 months)?

	Identification		Exploitation	
	Name	Points	Name	Points
Time	not practical	∞	<1 day - <1 week	3 – 6
Expertise	Expert	5	Expert	4
Knowledge	Public - Sensitive	0 - 7	Public	0
Access	< 1000	0 – 3	<10 - <100	0 – 4
Equipment	Specialized-bespoke	3 – 5	Specialized - bespoke	4 – 6
Open samples	None	0	-	-
Sub total		13 – ∞		11 – 20
			Total	∞

WOUTER@
YOURCREATIVESOLUTIONS.NL
+31-6-24721971

Wouter Slegers