PUBLIC-KEY CRYPTOGRAPHY ON SMALL DEVICES FROM A PRODUCT POINT OF VIEW

THOMAS PLOS
WORKSHOP ON PKC ON SMALL DEVICES
13, MAY, 2016

PUBLIC

SECURE CONNECTIONS FOR A SMARTER WORLD

OUTLINE

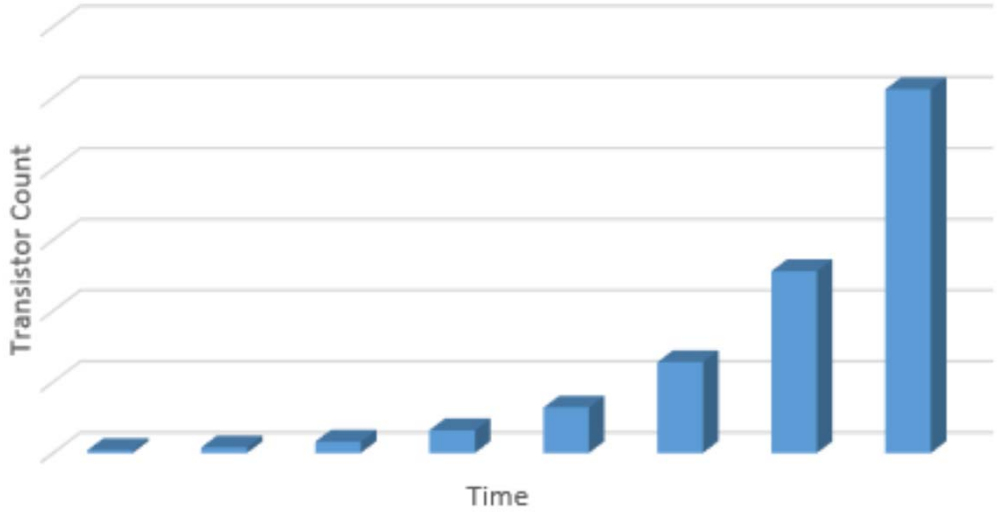
OUTLINE

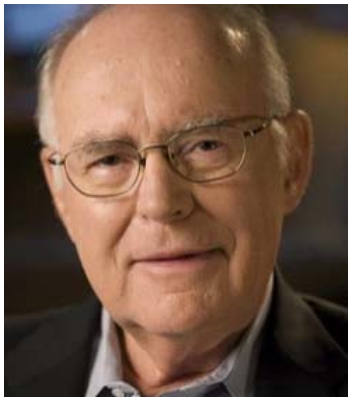
- Motivation
- Product aspects
- PKC standards
- Product certification
- Summary

MOTIVATION

WHAT IS A ‘SMALL DEVICE’ ?

- Moore’s Law
  - In 1970’s
  - Prediction of ‘growth rate’





(C) www.mooreslaw.org

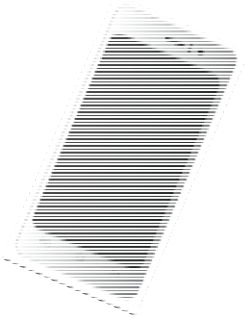
- Self-fulfilling prophecy

Technolgical process ==> enabler for ‘small devices’

WHAT IS A ‘SMALL DEVICE’ (2)

Desktop PC: 1995
- CPU: 90 MHz (1 core)
- RAM: 16MB
- Storage: 1GB
- Power cons: 100W
- Costs: 2000€

Smart phone: 2016
- CPU: 2.3GHz (4 cores)
- RAM: 4GB
- Storage: 32GB
- Power cons: 2W
- Costs: 700€



Sensor (nodes), tags, smart cards
- CPU: some MHz
- RAM: some kB
- Storage: some 100kB
- Power Cons: < 0.1W
- Costs: several €

500 smart and connected devices per houshold in 2022
https://entwickler.de/online/smart-home-givicon-128304.html

PKC ON SMALL DEVICES (1)

- Public-key cryptography (PKC):
  - Encryption (E) and decryption (D) operations
  - Using different keys e, d

$E_e(m) = c$ → $D_d(c) = m$

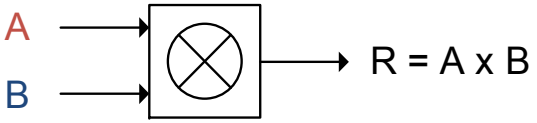
  - Knowing E, e, c → should be difficult to get m or d
  - d as ‘trapdoor’ to allow efficient decryption

- PKC typically more complex and computation/resource intensive than symmetric cryptography (longer keys) – challenging…
  - …to reach performance
  - …to stay within power consumption/energy budget
  - …to not exceed resource limits

PKC ON SMALL DEVICES (2)

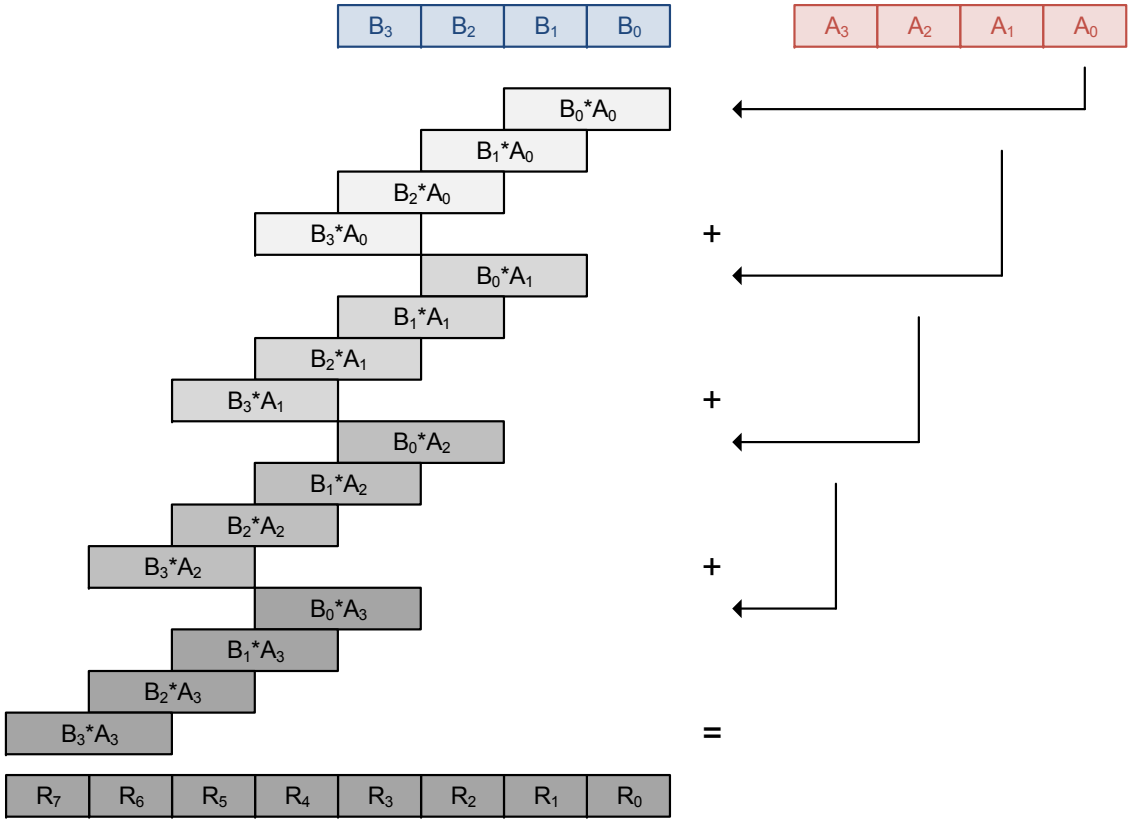
- PKC requires support of multiple-precision (modular) arithmetic

- Example: plain multiplication



  - ‘School book’ method
  - Word size: w bits
  - Operand size: n x w bits
  - Multiplying two n-word operands
  - n^2 w x w multiplication steps

- Modular multiplication even more expensive
  - Certain ‘tricks’ like special representation /reduction techniques



PRODUCT ASPECTS

PRODUCT ASPECTS

Right product @ right time

Fulfills Requirements

- Customer/market demands
- Standards/regulation bodies
- Economic aspects

Available when needed

- Approaching ‘market window’
- Next product generation
- New technology/standard

Technical and non-technical aspects

PRODUCT REQUIREMENTS

Product costs (development/production)

Power/energy budget

Standards/algorithms that have to be supported

Security measures

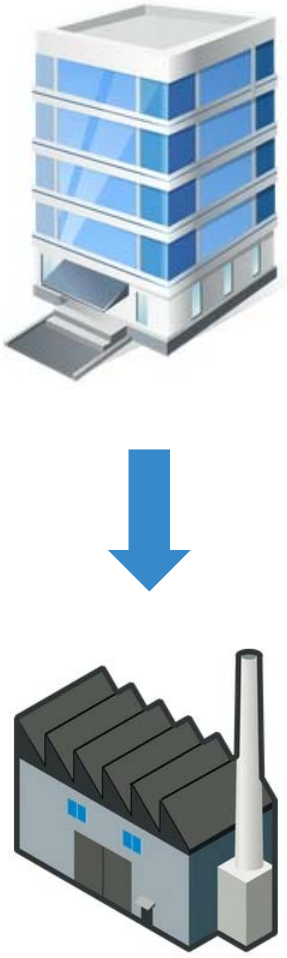
Compliance/certification

Architecture

PRODUCT COSTS (1)

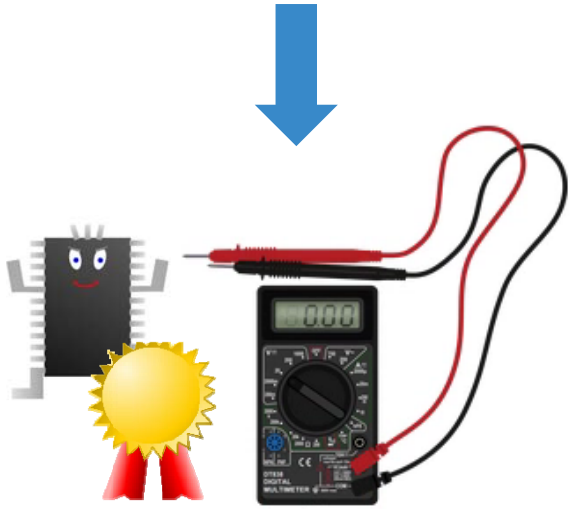
- Development costs
  - Engineers developing architecture/designing product
  - Implementation costs
    - Implement from scratch → longer design time
    - Re-use existing IP/buy IP → licensing costs
  - Platform approach
    - Configurable product platform
    - Design once → re-use for different purposes/markets
  - Infrastructure/ (CAD) tools

- Production costs
  - Used technology
    - Newer process technology → smaller chip size
    - Chip manufacturing more expensive (2nd Moor's Law)
  - Product volume → high volume (cheaper)
  - Packaging/integration



PRODUCT COSTS (2)

- Test/verification/certification costs
  - Testing at multiple stages
    - Test costs can make up significant part of product costs
    - The earlier product defects are found the lower the costs
  - Certifying/testing compliance
    - Fulfills emissions criteria (e.g., CE, FCC)
    - Passes (security) certification required for addressed market (EMVco, CC, FIPS)



ALGORITHM SELECTION

- RSA/Diffie-Hellman:
  - Longer keys (3072 bits for 128-bit security) [NIST]
  - Higher storage requirements/ longer execution times

- Elliptic curve cryptography (ECC)
  - Shorter keys (256 bits for 128-bit security) [NIST]
  - Lower storage requirements/ shorter execution times

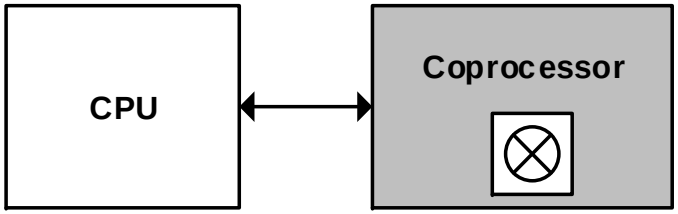
- 3072-bit multiplication vs. 256-bit multiplication
  - Operands 12x shorter
  - 12^2 = 144x faster → energy

[NIST] Recommendation for Key Management, Special Publication 800-57 Part 1 Rev. 3, NIST, 07/2012

ARCHITECTURE SELECTION

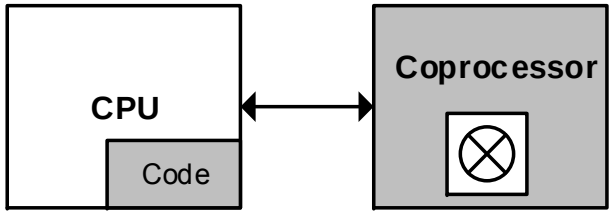
- Different architecture approaches

HW only



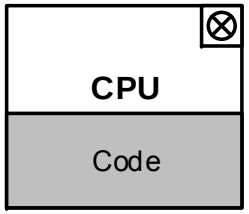
(+) Highly optimized for dedicated purpose (power consumption, execution time, security)
(-) Extra HW costs
(-) Limited flexibility
(-) HW design effort/complexity

HW/SW



(+) Good trade off between optimization/costs (still fast but less design effort/complexity easire to handle)
(+) High(er) flexibility
(-) Not straight-forward to find optimal HW/SW partitioning
(-) Extra HW costs
(-) Less optimized than HW-only (power consumption)

SW only



(+) Limited HW costs (code/data storage)
(+) High flexibility
(+) Minimal HW design effort/eases handling of complexity (programming)
(-) Not optimized (energy consumption, performance)

PKC STANDARDS

(PKC) STANDARDS

- …to ensure interoperability (different applications, vendors)
- …to facilitate deployment
- …to ensure usage of approved security mechanisms

- Different standardization bodies:

International Organization for Standardization (ISO) and the International Electrotechnical Commission standards (ISO/IEC)

Banking and security standards (ANSI, ISO)

Internet Engineering Task Force (IETF) standards and RFCs

U.S. government standards (FIPS)

Public key cryptography standards (PKCS)

- Certain redundancy if standard from one body gets ratified by another one

EXAMPLE: ISO STANDARDIZATION PROCESS

Proposal Stage
- Needed?
- NWIP

Preparatory Stage
- WG
- WD

Committee Stage
- Shared with committee
- CD

Enquiry Stage*
- DIS submitted
- Members vote

Approval Stage
- FDIS submitted
- Members vote

Publication Stage
- Only editorial updates
- Standard published

- Takes typically 3 years
- “Fast-track procedure” possible *

www.iso.org/home/standards_development.htm

ISO/IEC STANDARDS

- International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)
- www.iso.org

- ISO/IEC 9796-2: Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms
- ISO/IEC 9796-3: Digital signature schemes giving message recovery -- Part 3: Discrete logarithm based mechanisms
- ISO/IEC 9798-3: Entity authentication -- Part 3: Mechanisms using digital signature techniques
- ISO/IEC 9798-5: Entity authentication -- Part 5: Mechanisms using zero-knowledge techniques
- ISO/IEC 11770-3: Key management -- Part 3: Mechanisms using asymmetric techniques (e.g., Diffie-Hellman)
- ISO/IEC 13888-3: Non-repudiation -- Part 3: Mechanisms using asymmetric techniques
- ISO/IEC 14888-2: Digital signatures with appendix -- Part 2: Integer factorization based mechanisms
- ISO/IEC 14888-3: Digital signatures with appendix -- Part 3: Discrete logarithm based mechanisms
- ISO/IEC 15946: Cryptographic techniques based on elliptic curves (Part 1: General; Part 5: Elliptic curve generation)
- ISO/IEC 18033-2: Encryption algorithms – Part 2: Asymmetric ciphers
- ISO/IEC 18033-5: Encryption algorithms -- Part 5: Identity-based ciphers
- ISO/IEC 20008-2: Anonymous digital signatures – Part 2: Mechanisms using a group public key
- ISO/IEC 20009-2: Anonymous entity authentication – Part 2: Mechanisms based on signatures using a group public key
- ISO/IEC 29192-4: Lightweight cryptography -- Part 4: Mechanisms using asymmetric techniques
- ISO/IEC 29167-12: Automatic identification and data capture techniques – Part 12: Crypto suite ECC-DH security services for air interface communications
- ISO/IEC 29167-16: Automatic identification and data capture techniques – Part 16: Crypto suite ECDSA-ECDH security services for air interface communications
- ISO/IEC 29167-17: Automatic identification and data capture techniques – Part 16: Crypto suite cryptoGPS security services for air interface communications
- ISO/IEC 29167-19: Automatic identification and data capture techniques – Part 19: Crypto suite RAMON security services for air interface communications

BANKING SECURITY STANDARDS (ANSI)

- Banking security standards used for wholesale/retail banking
- ANSI … American National Standards Institute
- www.ansi.org

- X9.31: Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)
- X9.42: key management using Diffie-Hellman
- X9.44: Public key cryptography for the financial services industry: key establishment using integer factorization cryptography
- X9.57: certificate management standard
- X9.62: Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA).
- X9.63: Key Agreement and Key Management using Elliptic Curve Based Cryptography

U.S. GOVERNMENT STANDARDS (FIPS)

- Developed under the National Institute of Standards and Technology (NIST)
- www.nist.gov
- For use in U.S. federal government departments

- FIPS 186-4: Digital Signatures
  - Discrete log-based: DSA and ECDSA → adoped in ISO/IEC 14888-3
  - Factorization-based: RSA → adoped in ISO/IEC 14888-2

- NIST SP800: Key Establishment Schemes → adopted in ISO/IEC 11770-3
  - 56A - Discrete Logarithm-Based: DHs, MQVs, ECDH (+ ANSI X9.63)
  - 56B - Factorization-Based: RSA based key transport and key agreement

PUBLIC KEY CRYPTOGRAPHY STANDARDS (PKCS)

- Set of standards released by RSA Laboratories
- www.emc.com/emc-plus/rsa-labs/standards-initiatives
- Started in early 1990s → to accelerate deployment
- Not a real industry standard, but a 'de facto' standard (e.g., used in ANSI, IETF)

- PKCS#1- #15
  - PKCS#1: RSA cryptography standard
  - PKCS#3: Diffie-Hellman Key agreement
  - PKCS#5: Password-based encryption standard
  - PKCS#6: Extended-Certificate Syntax standard
  - PKCS#7: Cryptographic Message Syntax Standard
  - PKCS#8: Private-Key Information Syntax Standard
  - PKCS#9: Selected Attribute Types
  - PKCS#10: Certification Request Standard
  - PKCS#11: Cryptographic Token Interface
  - PKCS#12: Personal Information Exchange Syntax Standard
  - PKCS#13: Elliptic Curve Cryptography Standard
  - PKCS#14: Pseudo-random Number Generation
  - PKCS#15: Cryptographic Token Information Format Standard

INTERNET STANDARDS - RFCs

- Requests for Comments (RFCs)
- https://tools.ietf.org/html
- Publications of Internet Engineering Task Force (IETF) and Internet Society (ISOC)

- RFC 2315 PKCS #7: Cryptographic Message Syntax
- RFC 2985 PKCS #9: Selected Object Classes and Attribute Types
- RFC 3447 Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications
- RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC 5958 Asymmetric Key Packages (PKCS #8)
- RFC 5967 The application/pkcs10 Media Type (PKCS #10)
- RFC 6070 PKCS #5: Password-Based Key Derivation Function 2
- RFC 7292 PKCS #12: Personal Information Exchange Syntax

EXAMPLE - ISO/IEC: 29192-4

- Lightweight cryptography -- Part 4: Mechanisms using asymmetric techniques
- Published 2013
- Three lightweight mechanisms:
  - Unilateral authentication mechanism based on ECC (cryptoGPS)
  - Authentication and lightweight key-exchange mechanism (ALIKE) – for authentication and establishing a session key

    (Authenticated Lightweight Key Exchange - SPAKE)
  - Identity based signature mechanism

EXAMPLE - ISO/IEC: 29167

- Automatic identification and data capture techniques, Part 12, 16, 17, 19

- Part 12: Crypto suite ECC-DH security services for air interface communications
  - 2015
  - ECC based Diffie-Hellman key agreement
- Part 16: Crypto suite ECDSA-ECDH security services for air interface communications
  - 2015
  - Crypto suite based on ECC
  - Specifies ECDH key agreement in a secure channel establishment and the use of EC digital signature algorithm in an authentication mechanism (excl. key)
- Part 17: Crypto suite cryptoGPS security services for air interface communications
  - 2015
  - CryptoGPS – low-cost public-key cryptography (coupons)
- Part 19: Crypto suite RAMON security services for air interface communications
  - Under development
  - Rabin Montgomery based crypto system

EXAMPLE - RFC 7748 Elliptic Curves for Security

- Status: *Informational*
- Two elliptic curves over prime fields
- Montgomery curves
- Intended for ECDH usage
- Allows fast implementation

- Curve25519
  - 128-bit security level → prime: $2^{255} - 19$
  - Developed by D. J. Bernstein
- Curve448
  - 224-bit security level → prime: $2^{448} – 2^{224} - 1$
  - Developed by Mike Hamburg

EXAMPLE - PKC in Bluetooth

- Industry standard maintained by Bluetooth Special Interest Group (SIG)
- www.bluetooth.com
- Wireless communication 10 – 100m
- Special LE (low energy) extension
- For connecting smart phones, health/fitness devices, …

- New version (4.2) released in 2014
- Supports now ECDH-based key exchange (pairing)
- Two NIST curves (FIPS 186-3)
  - 96-bit security → P-192 EC
  - 128-bit security → P-256 EC

PRODUCT CERTIFICATION

CERTIFICATION (1)

- Why certifying/evaluating a product?

- Different security evaluations

- FIPS 140-2 (standardized)
  - http://csrc.nist.gov
  - Products in US government/regulated industries (e.g., health care)
  - Cryptographic modules (HW + SW)
  - 4 levels (Level 1 – Level 4)
  - To ensure strength and correct implementation of cryptographic algorithm
  - No vulnerability assessment

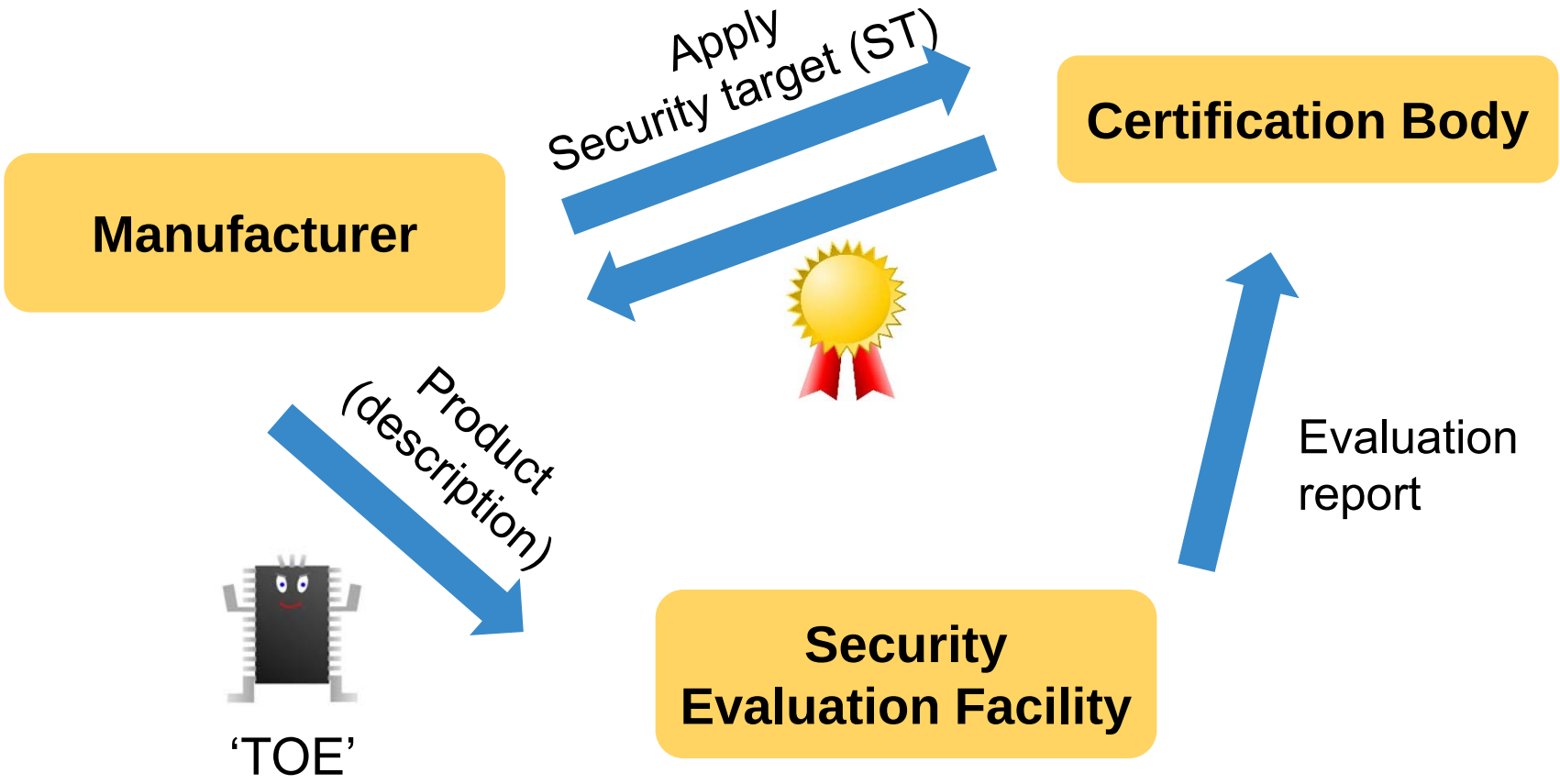
CERTIFICATION (2)

- Common Criteria (CC) (standardized)
  - https://www.commoncriteriaportal.org
  - Products in national identification documents (passport, ID card)
  - ISO/IEC 15408
  - 7 levels (EAL1 – EAL7)
  - Typically EAL4+ for security ICs
  - Correct implementation
  - Exhaustive vulnerability assessment

CERTIFICATION (3)

- EMVCo (proprietary)
  - http://www.emvco.com
  - Products in financial/payment industry
  - Joint venture of American Express, Discover, JCB, MasterCard, UnionPay, and Visa
  - Focus on security and life cycle of product
  - Similar requirements than for CC of security ICs but less formal
  - Renewal 1x per year

EXAMPLE - CC PROCESS



EXAMPLE - CC ASSURANCE LEVELS

EAL 7: formally verified design and tested

EAL 6: semiformally verified design and tested

EAL 5: semiformally designed and tested

EAL 4: methodically designed, tested and reviewed

EAL 3: methodically tested and checked

EAL 2: structurally tested

EAL 1: functionally tested

Higher level → more formal → more details required

SUMMARY

SUMMARY

- Technolgical process as enabler for ‘small devices’

- Product aspects
  - Requirements: technical and non-technical
  - Costs

- (PKC) standards
  - From different standardization bodies
  - Examples for PKC standards focusing on ‘small devices’

- Product certification

SECURE CONNECTIONS
FOR A SMARTER WORLD