FTF 2016
TECHNOLOGY FORUM

AUTHENTICATION FOR USB TYPE-C

FTF-MHW-N1910

JOE SALVADOR
MARKETING DIRECTOR, ANTI-COUNTERFEIT PRODUCTS
MAY 19, 2016

AGENDA

- Introduction to NXP Identification and Security
- Authentication for a “Universal” Serial Bus Accessories – Why?
- Authentication Approaches
- Overview of the USB Authentication Specification
- NXP Solutions for USB Authentication

NXP #1 in Security IC Solutions*

#1 PAYMENT CHIP CARDS

CONTACT SECURITY CONTROLLER
DUAL-INTERFACE AND CONTACTLESS SECURITY CONTROLLER
DEBIT, CREDIT, ATM CARDS

#1 MOBILE TRANSACTION

NFC
EMBEDDED SECURE ELEMENTS

#1 TRANSPORT TICKETING /TOLLING

MIFARE SYSTEM SOLUTION
CONTACTLESS SECURE MICROCONTROLLER
CONTACTLESS SECURE MEMORY ICS

#1 CLOSED LOOP PAYMENT

MIFARE SYSTEM SOLUTION
CONTACTLESS SECURE MICRONTROLLER
MICROPAYMENTS, GIFT CARDS, LOYALTY

#1 EGOVERMNENT DOCUMENTS

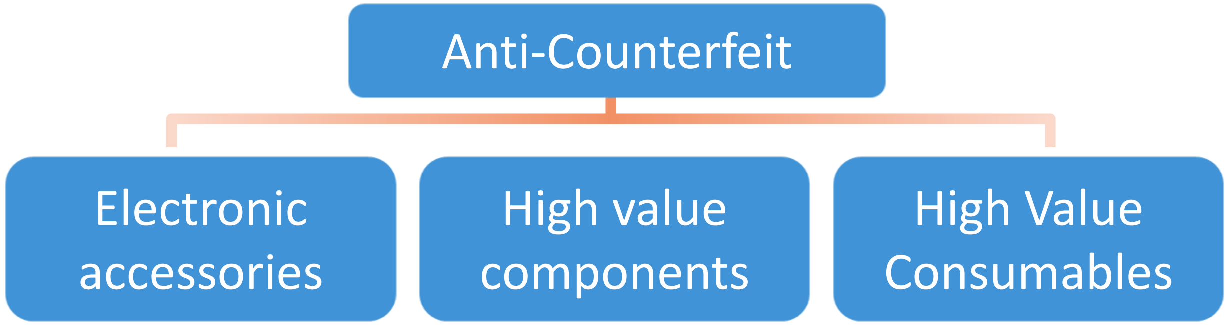
DUAL-INTERFACE AND CONTACTLESS SECURE MICROCONTROLLER
NATIONAL ID CARDS, PASSPORTS, VISAS

#1 POINT OF SALES TERMINAL

NFC
CONTACT READERS
EMVCO COMPLIANT SOLUTIONS
HOST PROCESSOR
TOUCHSCREEN INTERFACE
POWER MANAGEMENT

* Source: IHS 2016

Anti-Counterfeit Protection



Anti-Counterfeit

Electronic accessories

High value components

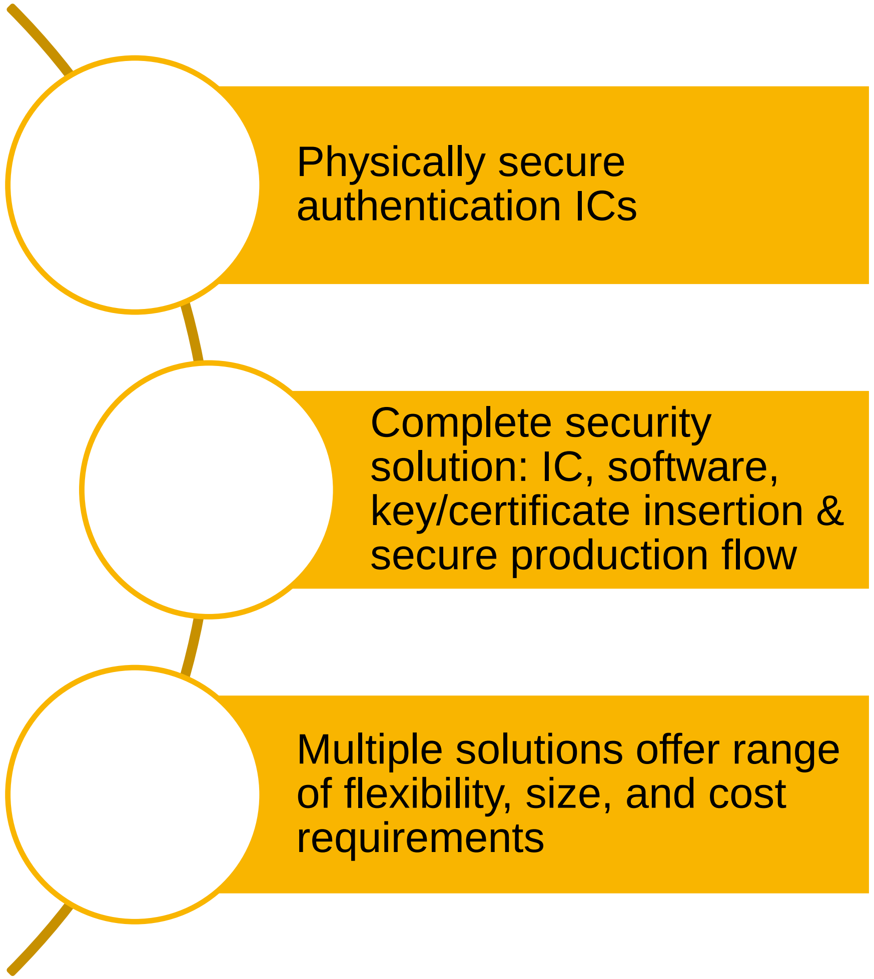
High Value Consumables

Electronic Accessories
- Charger
- Keyboard
- Cables

Game consoles
- Docking Stations.
- Head Set
- Controllers

- Router
- Switches
- Blade server
- Memory boards
- Transceiver

- Printer cartridges
- Batteries
- Medical probes, sensors
- Phone/Tablet Cases.
- Electronic Cig. cartridges



Physically secure authentication ICs

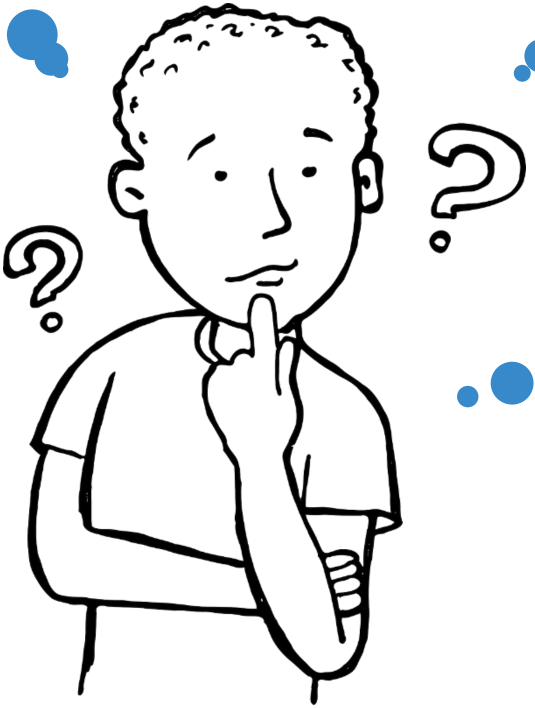
Complete security solution: IC, software, key/certificate insertion & secure production flow

Multiple solutions offer range of flexibility, size, and cost requirements

Secure Authentication for “Universal” Serial Bus Accessories?

Isn’t USB supposed to work with everything?

Can I trust everything that can be plugged in?



Will consumers be upset if some devices don’t fully function?

Can I help protect consumers from unsafe accessories?

USB Trust Challenges

USB Type-C PD chargers can deliver up to 5 amps at 20 volts

- Is the charger one that came with the system?
- Counterfeit chargers are widespread
- Will it damage my system or even possibly cause a fire?

“Faulty USB phone charger blamed for death” – Sydney Morning Herald 2014

USB charging ports are everywhere – rental car, taxis, airports, …

- Is it safe to charge at high power?
- Is it only charging, or doing something else?
- “Bad USB” accessories can present as a network device or keyboard and steal data or worse

Malicious USB devices can even take down other networked systems

- Stuxnet delivered via infected USB storage drives – destroyed a large number of Iranian nuclear centrifuges and was also targeted at their power plant steam turbines

Authentication Options for USB Type-C

USB PD Authentication using Vendor Defined Messaging:

- Advantages:
  - Available immediately, no industry infrastructure required
  - Can be optimized for cost and performance
- Disadvantage: Limited multi-vendor interoperability
- Ok for authenticating branded fast charger or establishing trust with OEM branded peripherals

USB Type-C Authentication Standard:

- Advantage: Support for USB-certified cross-vendor authentication
- Disadvantage: More complex authentication protocol may add unnecessary cost and performance burdens
- Ecosystem support being developed
  - USB as certificate authority
  - Revocation list TBD

USB Authentication Type-C 1.0 Spec Announcement 4/12/2016

Enables host systems to protect and mitigate risks against:

- Non-compliant USB Chargers
- Maliciously embedded hardware/software

Host systems can confirm the authenticity of a USB device or USB charger including product aspects as:

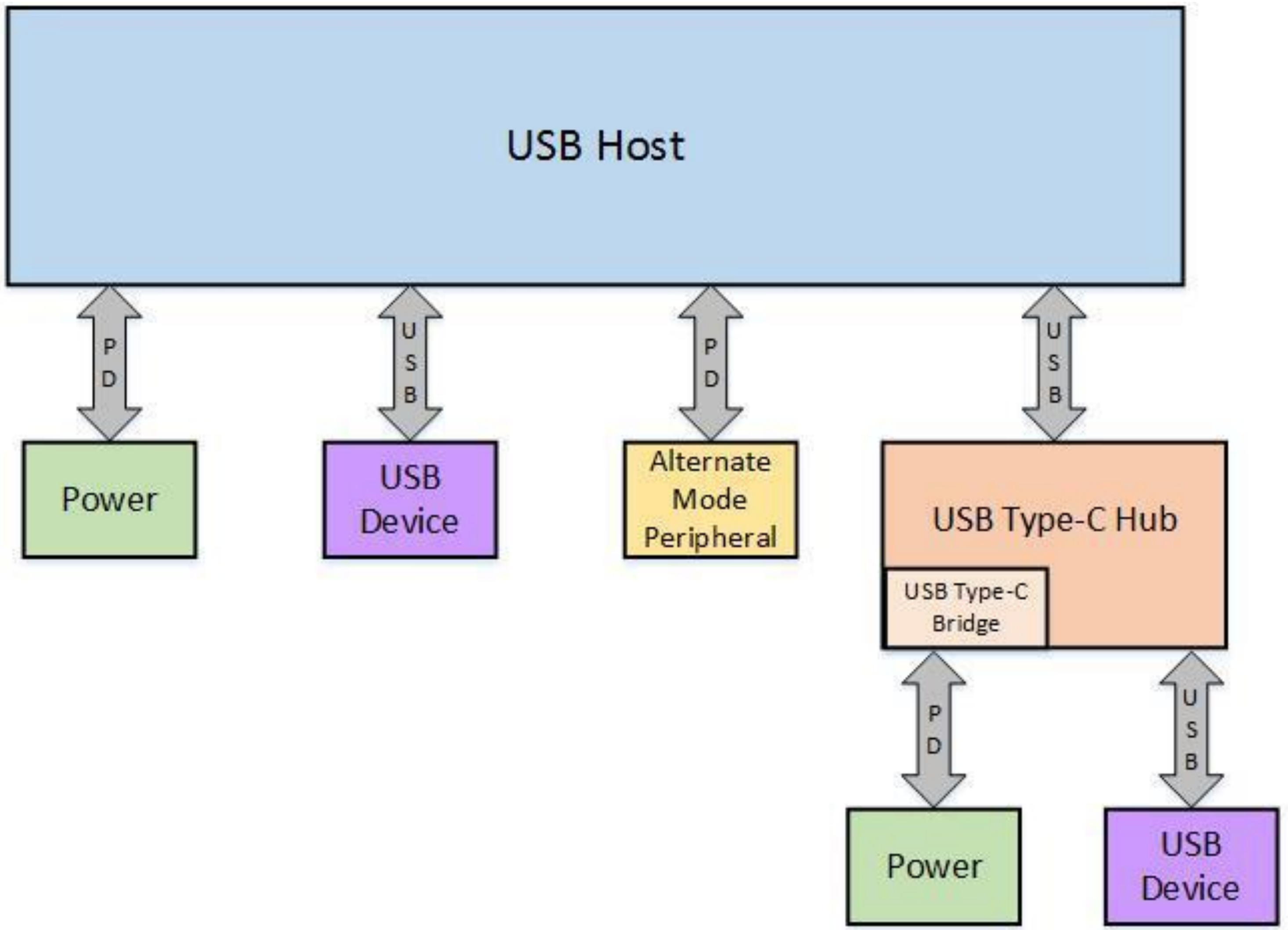
- Descriptors/capabilities
- Certification status

Key Characteristics:

- A standard protocol for authenticating certified USB Type-C™ Chargers, devices, cables and power sources
- Support for authenticating over either USB data bus or USB Power Delivery communications channels
- Products that use the authentication protocol retain control over the security policies to be implemented and enforced
- Relies on 128-bit security for all cryptographic methods
- Specification references existing internationally-accepted cryptographic methods for certificate format, digital signing, hash and random number generation

USB Type-C Example Topology Supporting Authentication

- Supports authentication over data lines and PD
- Supports authentication:
  - Power supply (including cable)
  - USB device
  - Alternate mode peripherals
  - Power and devices connected through a USB Type-C hub



What is Meant by a Security Policy?

What action does system take if an accessory cannot be authenticated?

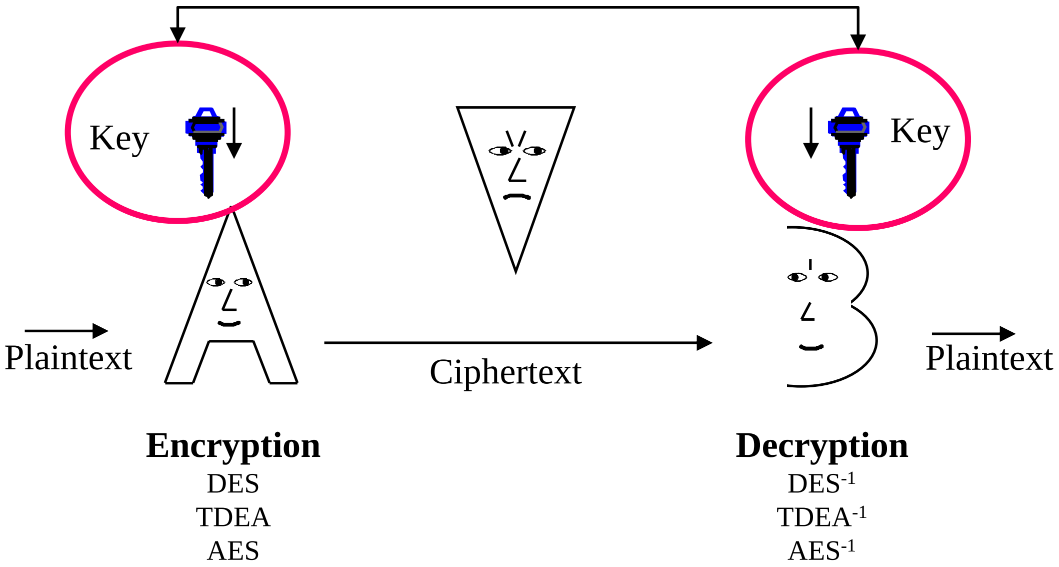
- USB does not define this
- Left to system implementer
- May depend on system implementer, type of accessory and even end-user preferences

Examples:

- “Untrusted” high power charger is only allowed to provide 5V/2A vs. up to 20V/5A for trusted charger
- Alert given to user first time an untrusted charger is plugged in, allowing user to identify counterfeits
- System reports to user that an untrusted accessory wants to act as keyboard, let user confirm or restrict access

AUTHENTICATION FUNDAMENTALS AND USB PROTOCOLS

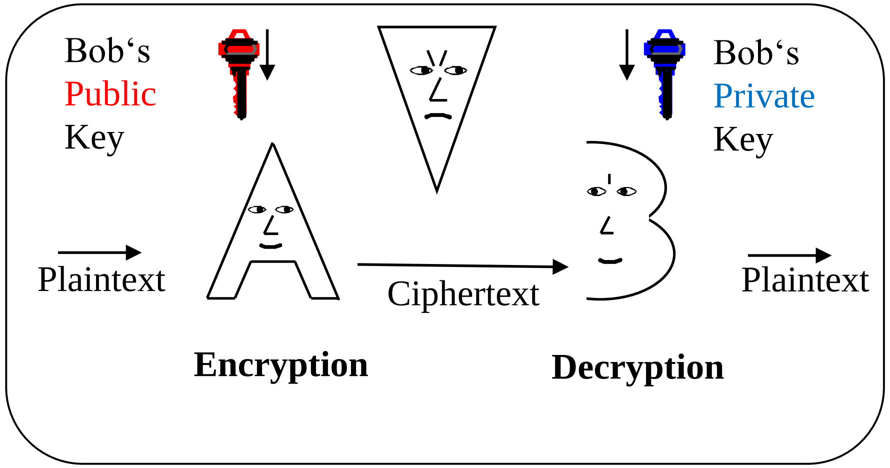
Symmetric Encryption

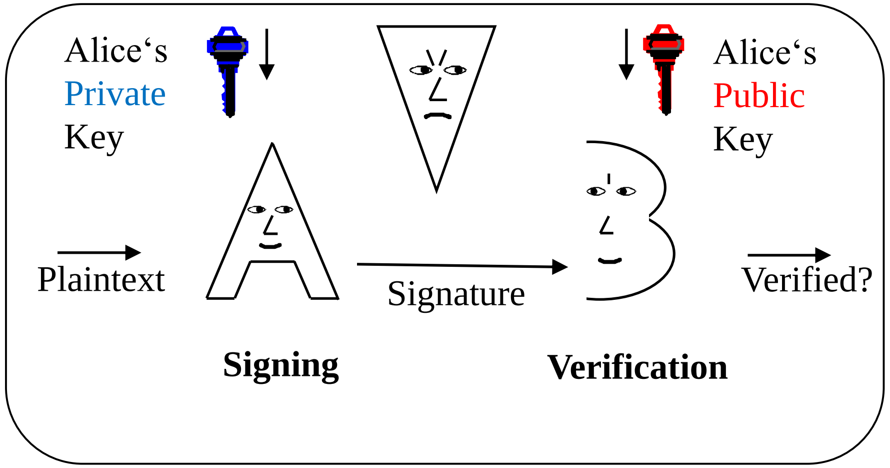


- Efficient algorithms, good for bulk data encryption
- Both parties have a **shared secret key**
- *Challenge 1:* How do we get a key securely from A to B?
- *Challenge 2:* If one device is hacked, then all are hacked (since key is shared)
- *Challenge 3:* Both sides need secure key storage

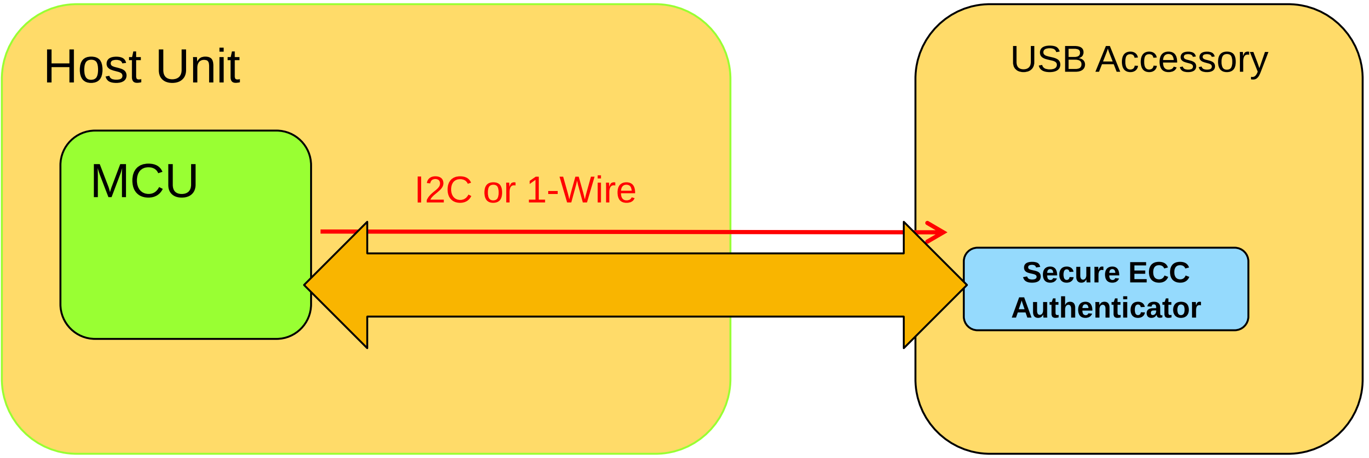
Asymmetric Cryptography

- Based on **hard** and **long-studied** mathematical problems
- Each participating party owns a **key pair**
  - A **public key** (can be known to everybody)
  - A **private key** (must stay under the sole control of the owner)
- Only the private key can decrypt something encrypted with the public key
  - Example – encrypted email – sender uses public key of intended receiver, only the person with the corresponding private key can read message
- Only the public key can decrypt something encrypted with the private key
  - Ensures that the message came from the original sender who had the private key





Asymmetric Crypto-based Authentication



- Benefits:
  - Unique key pair per accessory
    - Minimized hack scalability.
  - Tamper-resistant IC protects secret key
  - One anti-counterfeit IC per accessory
  - Typical interface options include I^{2}C, One-wire interfaces
  - No need for secure element in the main unit, lower cost of ownership

USB Type-C Authentication Uses Standard Security Protocols

Certificate Format Encoding	X.509v3, DER encoding
Digital Signing of Certificates and Auth Messages	ECDSA, using NIST P256, secp256r1
Hash algorithm	SHA256
Random number generation	NIST SP800-90A and NISTSP800-90B

USB Authentication Certificates and Certificate Chains

Definitions:

- **Certificate:** A _digital form of identification_ that provides information about an Entity and certifies ownership of a particular public key.
- **Certificate Chain:** A series of _two or more Certificates_ where each Certificate is _signed by the preceding Certificate_ in the chain.
  - Root Certificate: The first Certificate in a Certificate Chain. This certificate is self-signed.
  - Leaf Certificate: The last Certificate in a Certificate Chain (typically device specific).
  - Intermediate Certificate: A Certificate that is neither Root nor Leaf.

Restrictions:

- Up to 8 Certificate Chains allowed (up to 4 that have USB-IF Root Certificate)
- Maximum Certificate chain size: 4096 bytes

Certificate Contents (Examples, See Spec for Complete Details)

Distinguished Name – unique per entity

- Includes USB VID, PID where appropriate (both mandatory in leaf certificate)
- Organization name
- Serial number

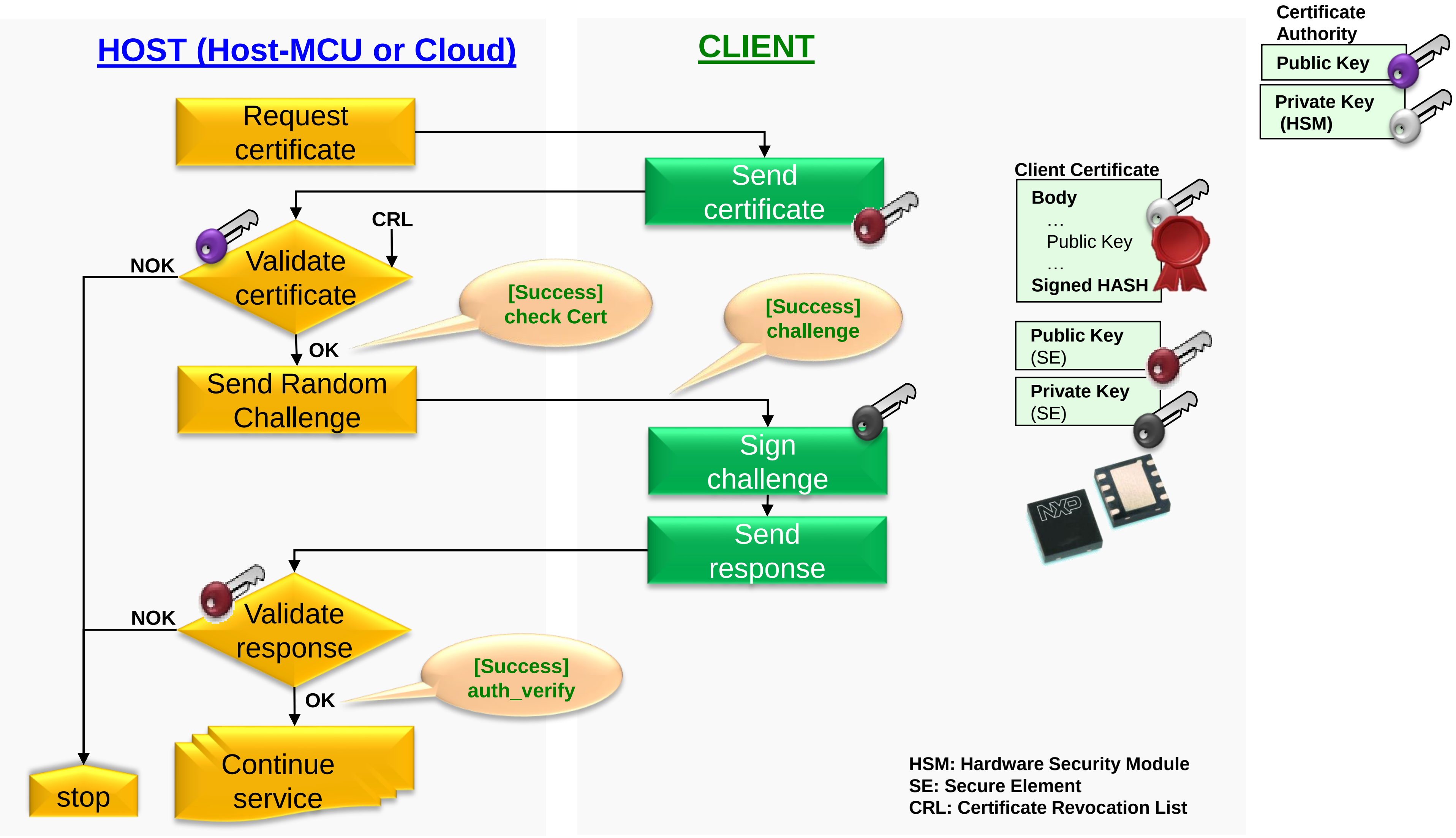
Certificate Validity Dates

Device Capabilities

Security component description

Vendor proprietary information

Simplified Elliptic Curve (ECC) based Authentication



HSM: Hardware Security Module
SE: Secure Element
CRL: Certificate Revocation List

Is Cryptography Enough?

Crypto does not equal security

Even if door lock is impenetrable, if you can find the key it is easy to get in

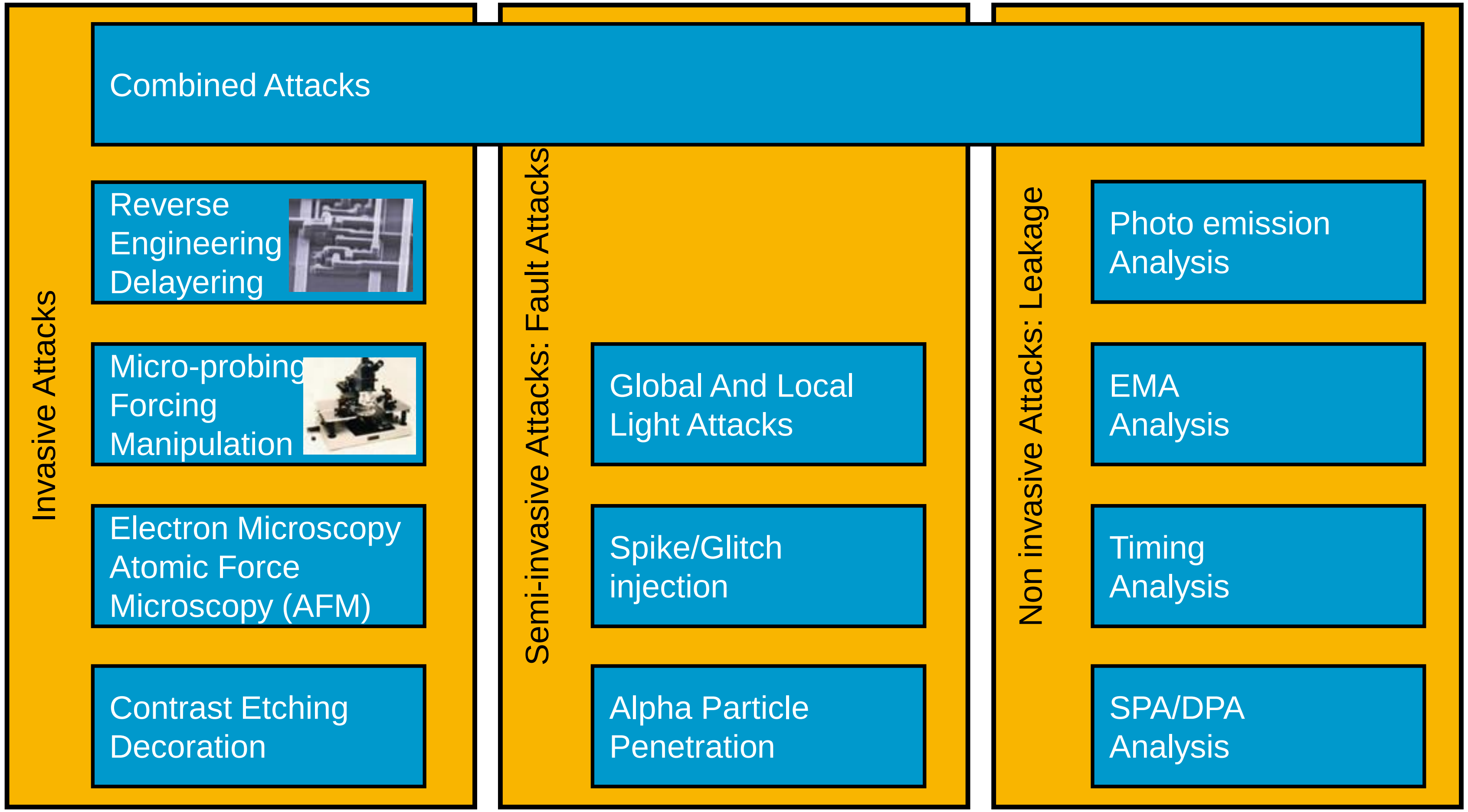
If an attacker can get the keys, they don’t need to break the crypto

Most “secure” micros can be easily hacked if an attacker can get physical access

NXP combines tamper resistant secure ICs with cryptographic authentication for secure authentication

Multilayered security extends beyond the IC to Software, Product Design and Manufacturing

Cracking a Crypto Authentication Device



Combined Attacks

Invasive Attacks

- Reverse Engineering Delayering
- Micro-probing Forcing Manipulation
- Electron Microscopy Atomic Force Microscopy (AFM)
- Contrast Etching Decoration

Semi-invasive Attacks: Fault Attacks

- Global And Local Light Attacks
- Spike/Glitch injection
- Alpha Particle Penetration

Non invasive Attacks: Leakage

- Photo emission Analysis
- EMA Analysis
- Timing Analysis
- SPA/DPA Analysis

Attacker’s goal is to steal the secret key(s)

USB Authentication Spec Security Recommendations

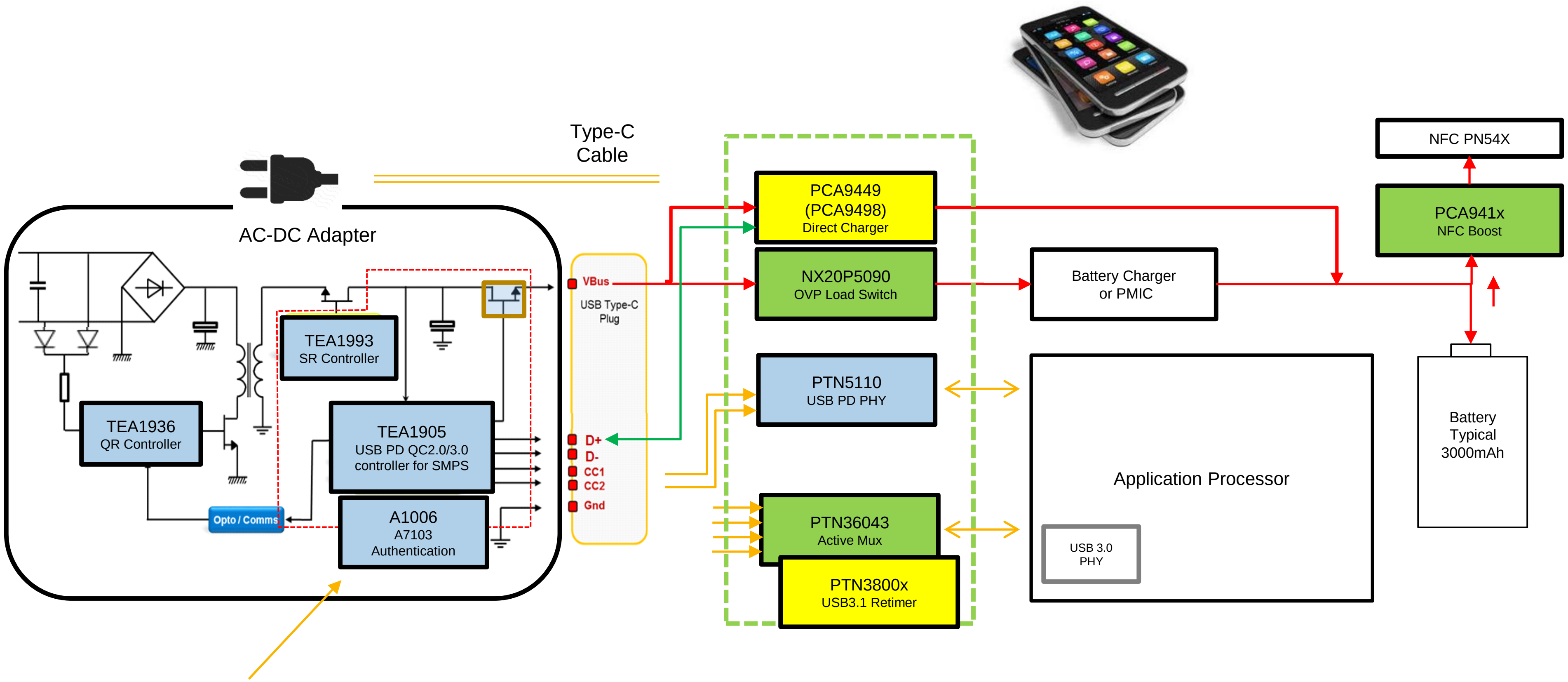
“Vendors of products take appropriate measures to protect the execution of the USB Type-C Authentication protocol and all private keys.”

“Products should **provide protected tamper-resistant operation and storage for the private keys** to prevent them from being read (all or in part), copied or otherwise disclosed.”

“This includes protection against side-channel and fault injection attacks, including software exploits and physical attacks such as leakage, probing, glitching, reverse engineering, and statistical analysis methods.”

NXP PRODUCTS FOR SECURE USB AUTHENTICATION

NXP USB Type-C Interface & Smart Charging – End to End Optimized



Authentication as part of complete end to end USB Type-C Solution

🟩 Released

🟦 In Development

🟨 Concept (New)

NXP’s Recommended Product Options for USB Authentication

	A1006	A7103
Type of Authentication	USB PD Vendor-specific	USB Auth 1.0 Compliant
Crypto Supported	ECC B-163, ECDH	ECC P256, ECDSA
Tamper Resistant	Yes	Yes
EEPROM	4 kbit	20 kByte
Interfaces	I^{2}C, one-wire	I^{2}C, one-wire
Standard Packages	HXSON6 (2 x 2) CSP (1 x 1)	HVSON8 (4 x 4) CSP-12 (2.1 x 2.1)
Status	Sampling, Q3 Production	Production

- A1006 offers industry’s smallest form factor, lowest power secure authenticator
- A7103 offers full USB Authentication 1.0 compliance

Security Threats Landscape

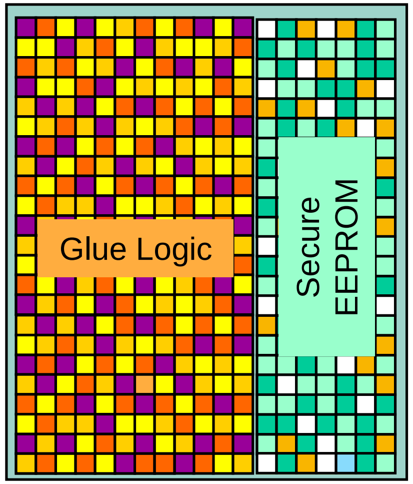
NXP Comprehensive Security Concept

Layered approach protects against all type of attacks
Secure IC & Software
Secure Design
Secure Manufacturing
Secure Key Insertion

Proven by third party security assessments and approvals

Examples of NXP Attack Countermeasures

- Glue Logic
  - Function blocks are chopped up and randomly mixed
- Memory encryption, Memory scrambling
  - For unique placement of data for each IC
- Security routing on all metal layers
- Security sensors on the IC
  - e.g. voltage, temperature
- Active and passive shielding
- Protected true random number generator
- Secured state-machine
  - Secured booting/secured mode control
  - Protection against pertinent fault attacks (robustness)
- Leakage attack countermeasures
  - Protection against timing analysis
  - Protection against Single Power Analysis (SPA), Differential Power Analysis (DPA), Electromagnetic Analysis (EMA)
  - Protection against Differential Fault Analysis (DFA)



NXP Security Management System – Secure Product Delivery

Secure Product Manufacturing

- Certified procedures for ROM code and FabKey data submission
- All sites involved in manufacturing are regularly re-audited according to Common Criteria
- NXP owned manufacturing sites

Security Maintenance

- Dedicated security managers
- Continuous Improvement process installed including regular process reviews

Trustful external Partnerships

- Customer Screening Procedure
- Long lasting trustworthy partnerships with suppliers and vendors

Regularly Assessed by Security Audits

NXP Trust Provisioning Service

Creation of secret keys, certificates & personalization data in HSM

- Only **HSM**’s (Hardware Security Modules) with CC EAL5+ certification have access to Master secrets and unencrypted cryptographic objects

Insertion of key data into NXP chips during production

- Security sealed **Wafer Tester** allocates cryptographic objects into chips

NXP Value Proposition for A1006 Secure Authenticator

Best in class anti-counterfeiting/anti-hacking technology

- Strongest levels of market-proven and certified security
- End to end security includes common criteria certified design environment, production facilities and secure personalization/key insertion per chip

Lowest power, smallest footprint, high performance

- Solutions as small as 1mm2
- Power consumption as low as 500 uA full-on, 50 uA typ, < 1 uA deep sleep
- Full certificate validation plus ECC challenge-response in ~50 ms

Ease of system integration

- Comprehensive end to end USB Type-C solution
- Demo boards and host demo software available
- Applications support team includes security experts and USB experts

SECURE CONNECTIONS
FOR A SMARTER WORLD