Secure Tamper Resistant Authentication for Anti-Counterfeit Applications

Balaji Badam

Security Architect
Anti-Counterfeit Products

May 2019 | AMF-CIT-T3539

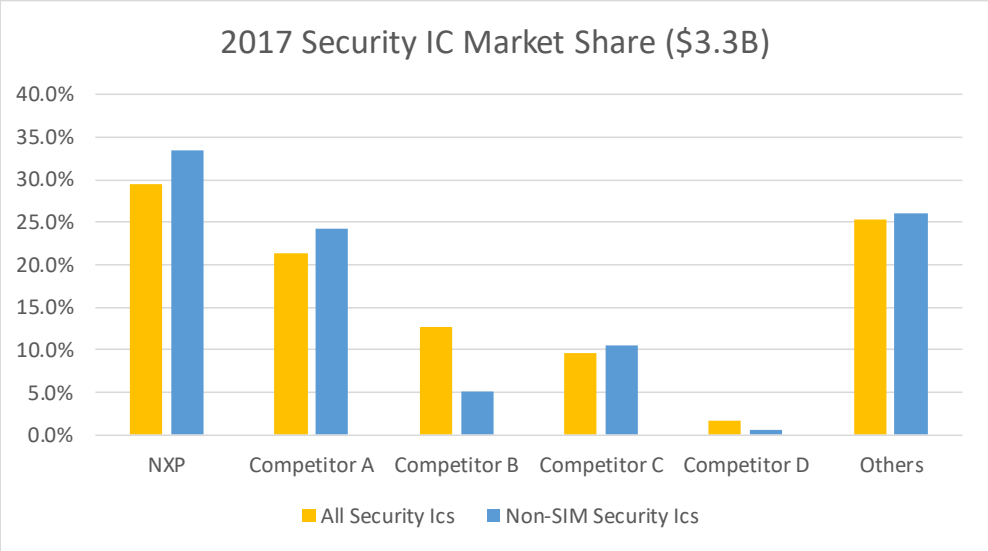
SECURE CONNECTIONS FOR A SMARTER WORLD

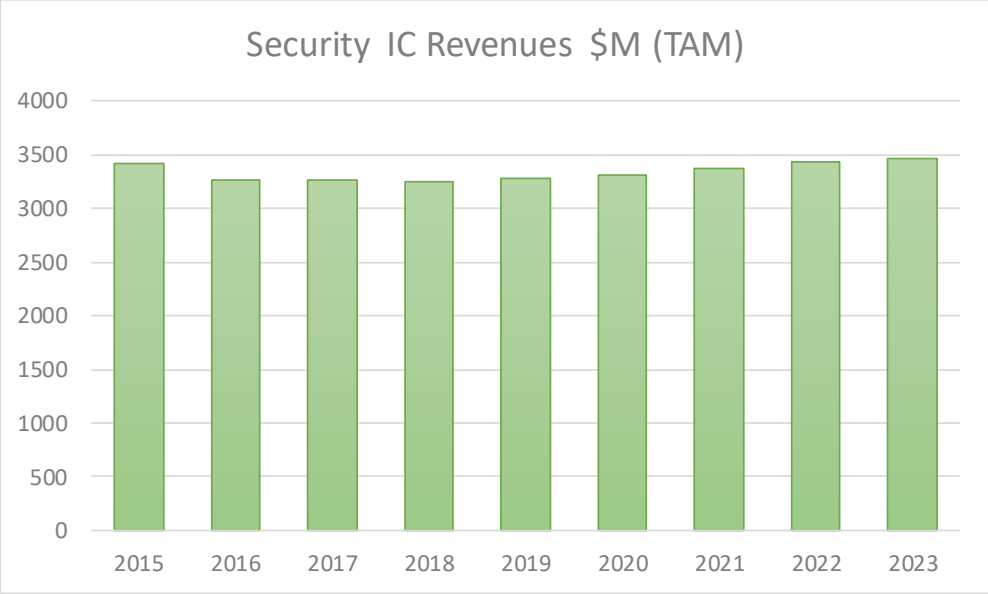
Agenda

- Brief Introduction to NXP Security Offerings
- Anti-Counterfeit Applications and Use Cases
- What to look for in an anti-counterfeit solution
- A1006 Secure Authenticator
- A1007 Preview
- Development Tools and Provisioning Utility

Brief Introduction to NXP Security Offerings

NXP #1 Market Position in Security ICs





Markets include:

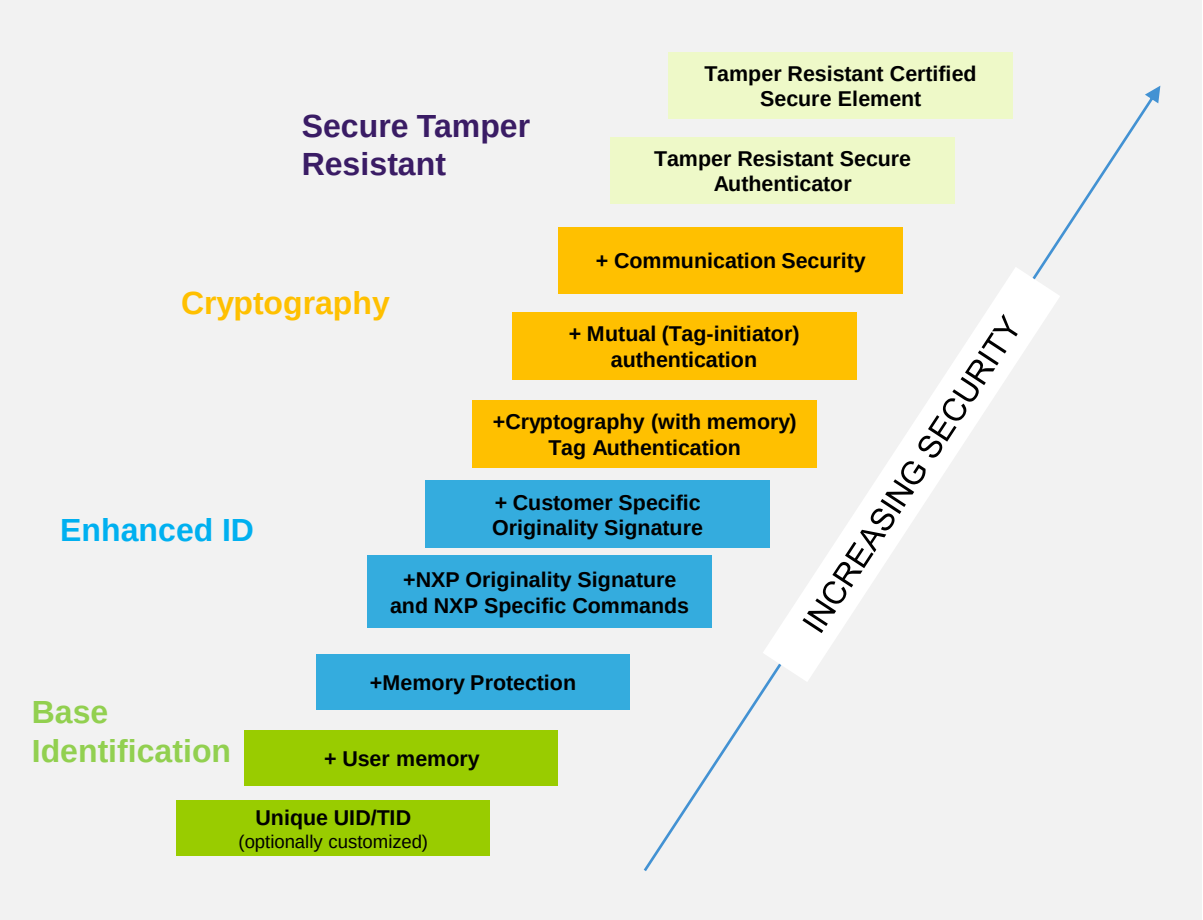
- Authentication & Anti-counterfeiting
- Enterprise ID & Access Management
- Government and Healthcare ID
- NFC Embedded Secure Element
- Payment and Banking
- Pay TV / Conditional Access
- Retail and Loyalty
- SIM card ICs
- Telecom / Payphone card ICs
- Transportation
- Other (includes TPM)

Sources: ABI Research, Q4 2018

NXP Offers a Full Range of Authentication Solutions

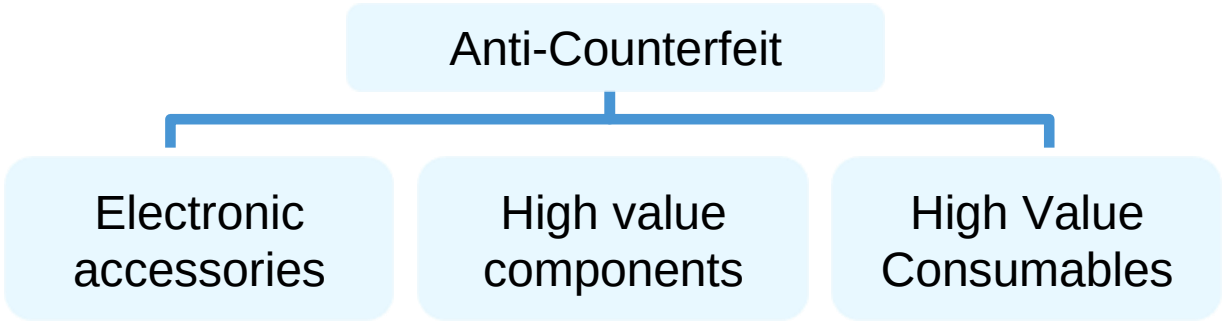
The level and type of security depends on the nature of the product, the logistics channel and possible threats

NXP products address a whole range of security requirements: from base level identification to physically secure tamper resistant cryptographic authentication through to independently certified Secure Elements for applications such as payment and e-government identification



Applications and Use Case Examples

Anti-counterfeit Protection and Proof of Origin



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 and secure production flow

Multiple solutions in development offer range of flexibility, size, and cost

Counterfeited Batteries and Chargers – Serious Problem

- Counterfeit batteries and chargers are very common and difficult to identify
- Significant risk to consumers
- Significant risk to revenue, brand and product liability
- Replaceable batteries, power banks, and all chargers are susceptible to counterfeit
- Xiaomi CEO Lei Jun assessing MI power bank sales
  - "If there were no counterfeits, our sales would be double or triple"
  - Estimated loss of $115 M

Rise of Counterfeits

- Border agents seize $700K in counterfeits at Ranier, The containers held 50 amplifiers, 662 cartons of earbuds and cables, and 57 cartons of sandwich boards and touch lamina.” – Duluth News Tribune, April 16, 2019
- “More than 99% of fake iPhone chargers failed critical safety test – faulty chargers have caused electrical shocks and even fires.” – Underwriters Laboratories study, 2016
- Manufacturing and 3D printing has made it very hard to tell the difference between a super fake and a legitimate product – Steve Shapiro, FBI Intellectual Property Rights
- The US Government accountability Office found that over 2 out of every 5 of supposedly brand name products it purchased were counterfeit” - 2018

Impact of Counterfeit Power Accessories

Mobile Phones

- **"At the end of 2016, Apple claimed that of 100 Apple-branded charging accessories it bought on Amazon, 90 were counterfeits"** – ECN, February 2017
- **"Britain's Chartered Trading Standards Institute reported that of 400 counterfeit chargers it bought from a range of online retailers, 397 failed a basic safety test. "** ECN, February 2017

Electronic cigarettes

- **"A tale of two Juul pods: China's counterfeits pose a threat to US" –** New York Post April 10, 2019
- **"Philadelphia customs agents intercept cases of counterfeit Juul products."** – April 17, 2019
- "**Illicit trade in electronic cigarettes** is on the rise across the developed world … include **bogus batteries** that fail to **recharge** and **liquids containing dangerously high levels of nicotine**." – Wall St. Journal Feb 20, 2015

Medical Supplies

- "According to the World Health Organization (WHO), **more than 8% of the medical devices in circulation are counterfeit** … pose **a significant liability to the manufacturers** and a health risk to both the patients and healthcare providers that **could result in injury, permanent disability, or even death**." – News Medical April 6, 2016

Hoverboards

- **"Thousands of fake hoverboards, worth $1.2 million, seized in Southern California"** – Mercury News September 19th, 2017
- "CBP Seizes Record Amount of Counterfeit Hoverboards … **over 16-thousand counterfeit hoverboards** with an estimated MSRP of over $6 million … **contain batteries that are deemed unauthorized** and therefore counterfeit as well as fake trademark logos." **-** January 27, 2016 – US Customs and Boarder Protection

Power Tools

- **"counterfeit battery … presents significant safety hazards, including an explosion risk …** Black & Decker employees and customers have purchased similar counterfeit batteries on the websites eBay and Amazon." STANLEY BLACK & DECKER, INC. V. D&L ELITE INVS., LLC (US District Court for the Northern District of California (July 19, 2013)

Battery & Charger Auth Applications

All replaceable batteries and high powered chargers (including wireless chargers) should be authenticated for safety, and revenue & brand protection

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

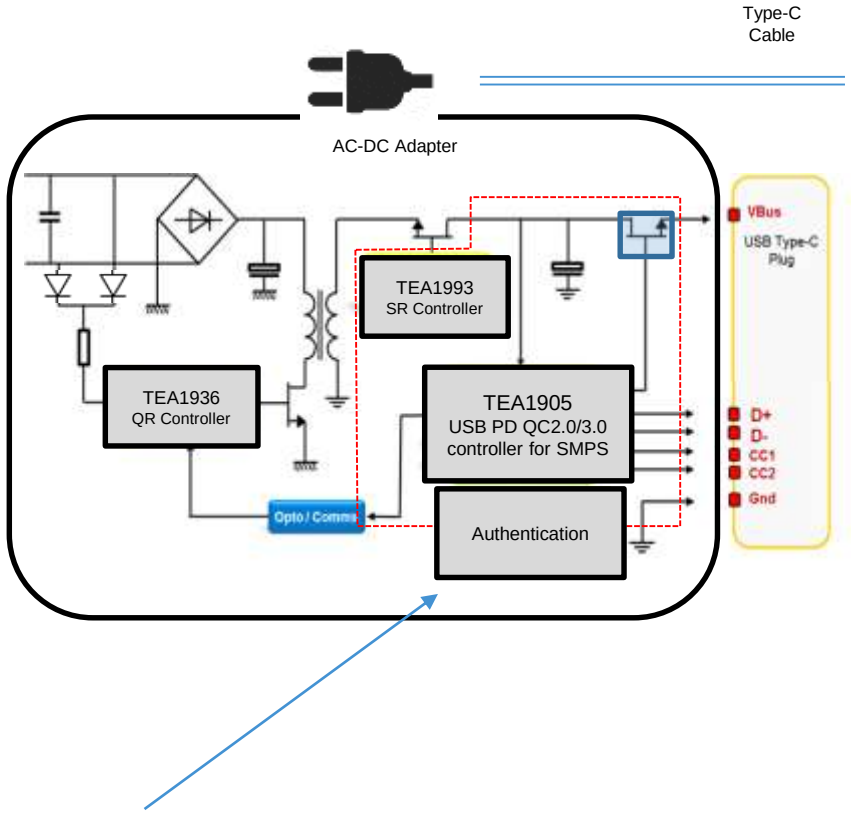
USB charging ports are everywhere – rental car, taxis, airports, …

- 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

NXP USB Type-C Interface & Smart Charging Solutions



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

- NXP USB Type C PD Adapter Solution
- Includes:
  - Primary Controller
  - Secondary Controller
  - PD controller
  - Authentication

Authenticating Electronic Accessories

Mandatory
Authentication IC

- Ecosystem Quality & User Experience
  - Authenticate devices before enabling them
  - Prevent access from rogue devices
- Create licensable ecosystem
  - Embedded secure element is requirement to be a “Made for [OEM]” accessory
  - Accessory makers must agree to OEMs T&C’s and purchase authentication IC from partners
  - Enforces & protects OEM licensing revenue as well as user experience

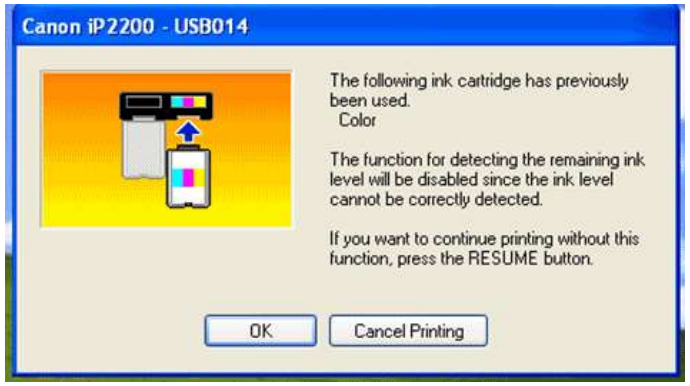
Anti-Counterfeit – Printer Cartridges

Commonly used in both inkjet and laser printers

- Protect revenue source (make money on ink/toner, not printer)

Cartridge Authentication Options

- Only genuine printer cartridges work
- Warn user that cartridge is not genuine
- Allow refills and clones, but potentially reduced functionality



Same business model applies to e-cigarettes, medical consumables, …

What to Look For in Anti-Counterfeit Solutions

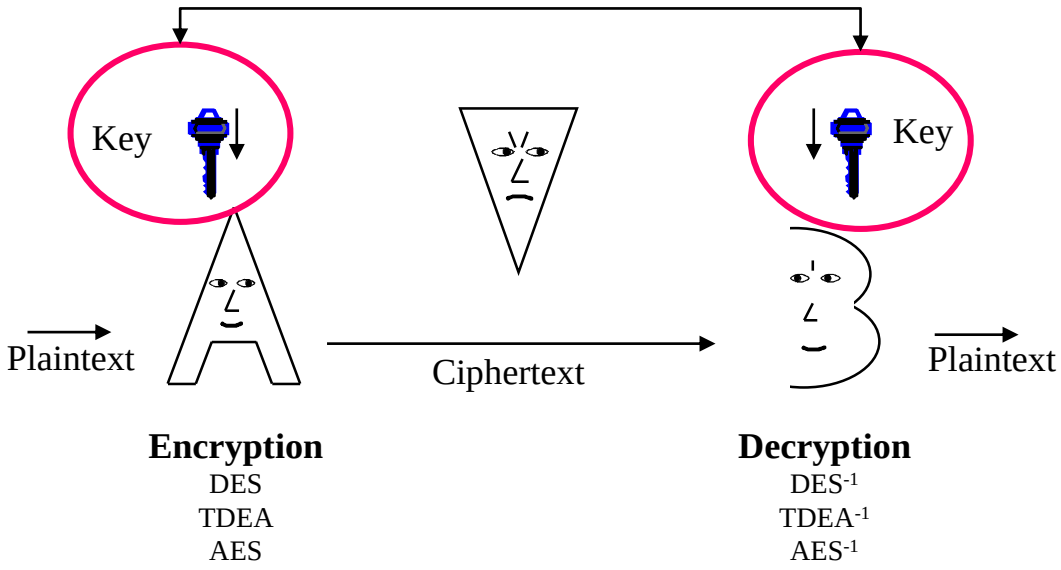
Crypto, tamper resistance, secure manufacturing, personalization

(Trust Provisioning)

Authentication Options

Authentication Option	Description	Advantages	Disadvantages
Silicon Identifier (unique ID)	Unique code in ROM/OTP per device or per application	Simple to implement	Easily cloned
Cryptographic Identifier	Cryptographic challenge-response	Requires slightly more skill to clone than Silicon Identifier	Easily cloned by motivated counterfeiters
Secure Symmetric Crypto Authenticator	Tamper-resistant symmetric authentication (typically SHA or AES)	Simple authentication algorithm	Protecting shared keys (can require two security ICs), break one-break all risk
Secure Asymmetric Crypto Authenticator	Tamper-resistant asymmetric authentication (typically RSA or ECC)	Secure key storage only required on one device, limited attack scalability reduces incentive to counterfeiters	Challenge-response validation can be more compute intensive

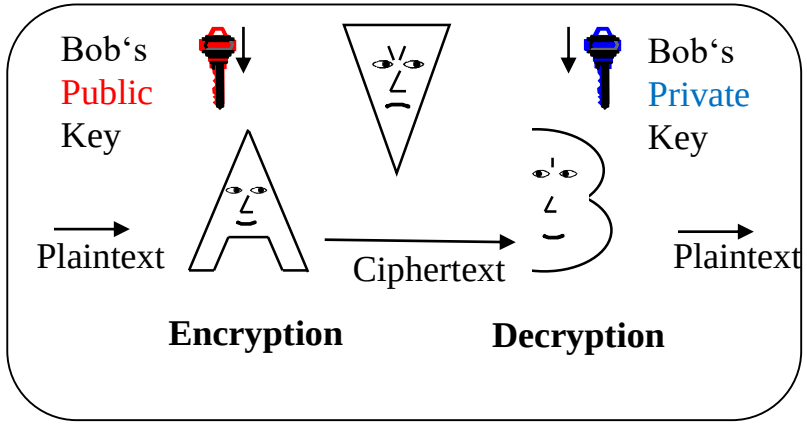
Symmetric Encryption

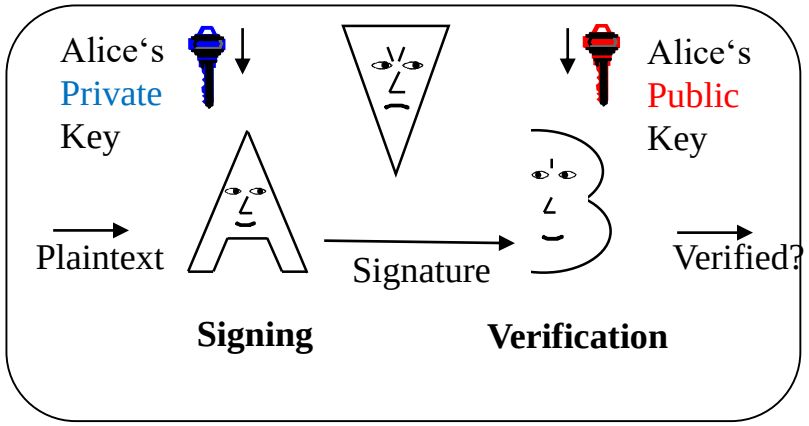


- Efficient algorithms, good for bulk data encryption
- Both parties have a shared secret key
- Challenge 1: How do we get a key securely from A to B?
- Challenge 2: If one device is hacked, then all are hacked (since key is shared)
- Challenge 3: Both sides need secure key storage

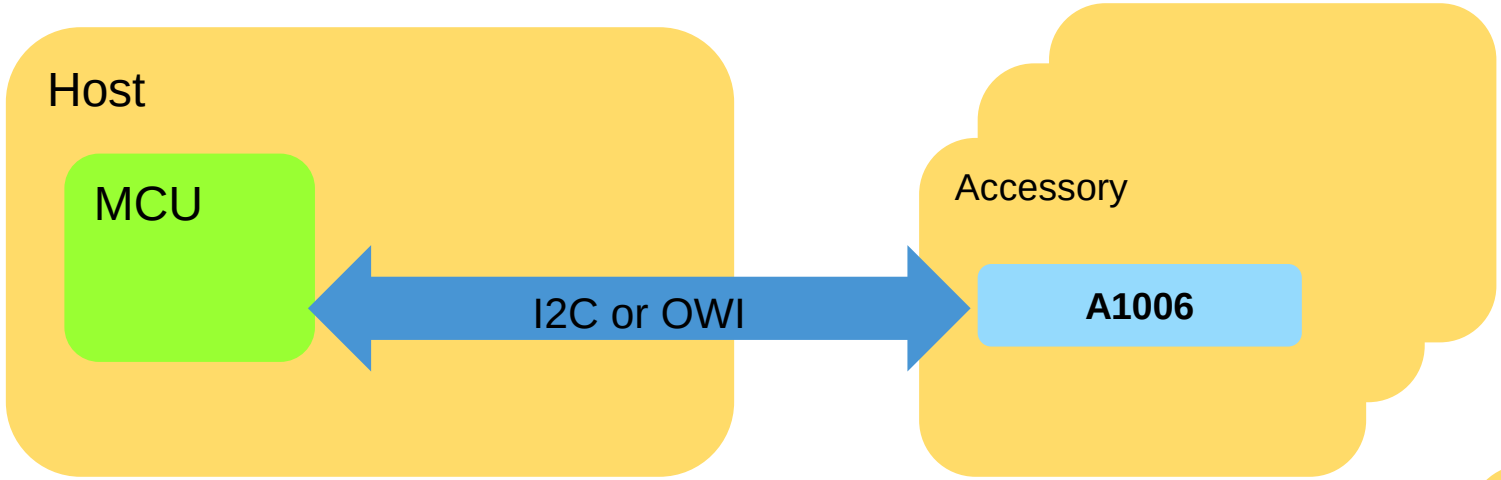
Asymmetric Cryptography

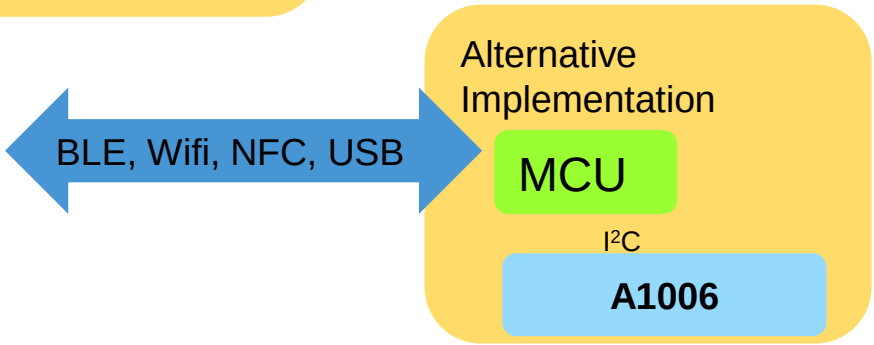
- Based on hard and long-studied mathematical problems
- Each participating party owns a key pair
  - A public key (can be known to everybody)
  - A private key (must stay under the sole control of the owner)
- Only the private key can decrypt something encrypted with the public key
  - Example – encrypted 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





Key Value: Asymmetric Crypto-based Authentication

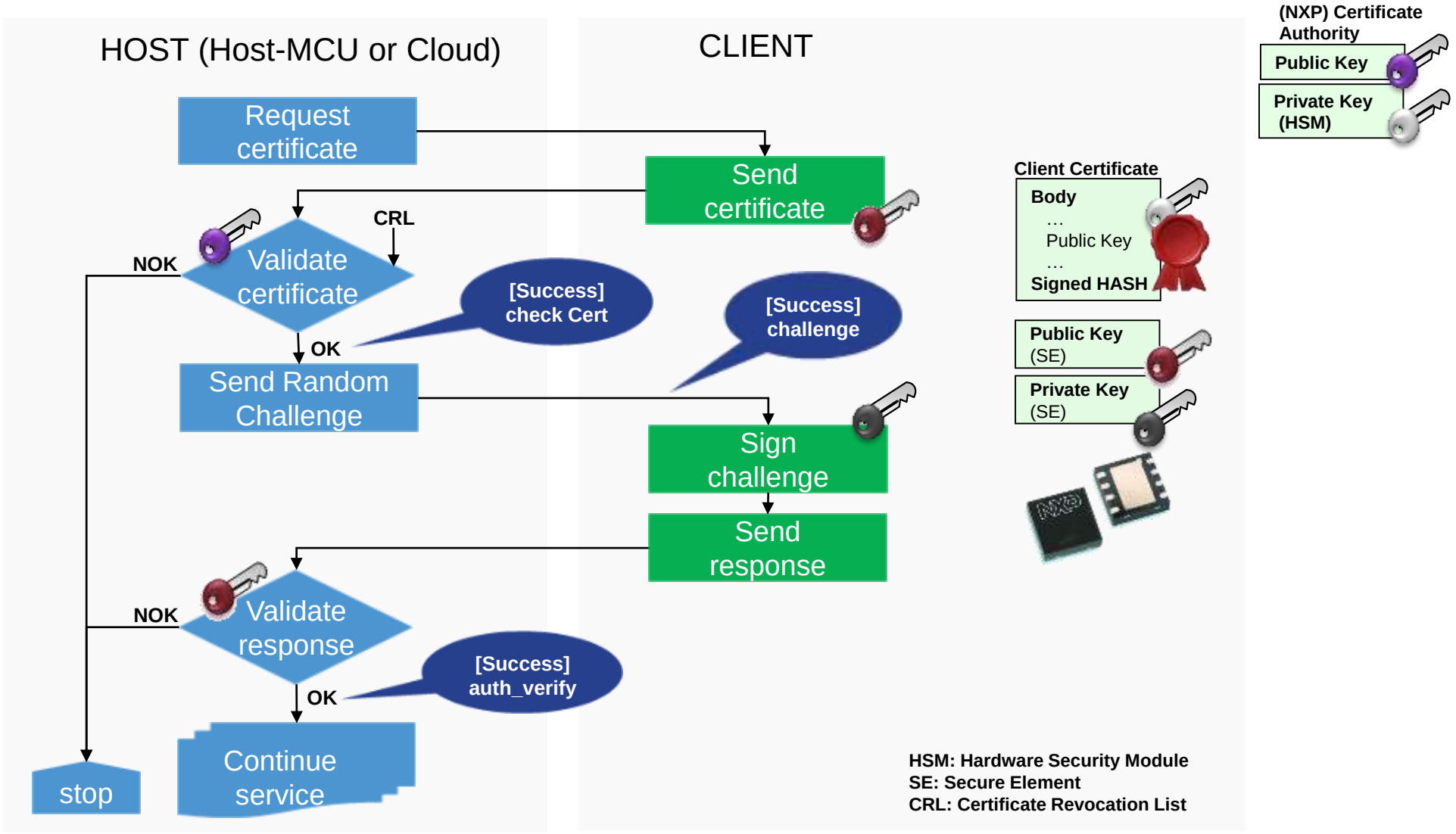




Benefits:

- Unique key pair per accessory
  - Minimized hack scalability
  - Can blacklist/revoke cloned devices without impacting existing infrastructure
- Tamper-resistant IC protects secret key
- One anti-counterfeit IC per accessory
- No need for secure element in the main unit, lower cost of ownership
  - No host secrets, just a single public key needed for validation
- Interface options include I2C, One-wire interfaces

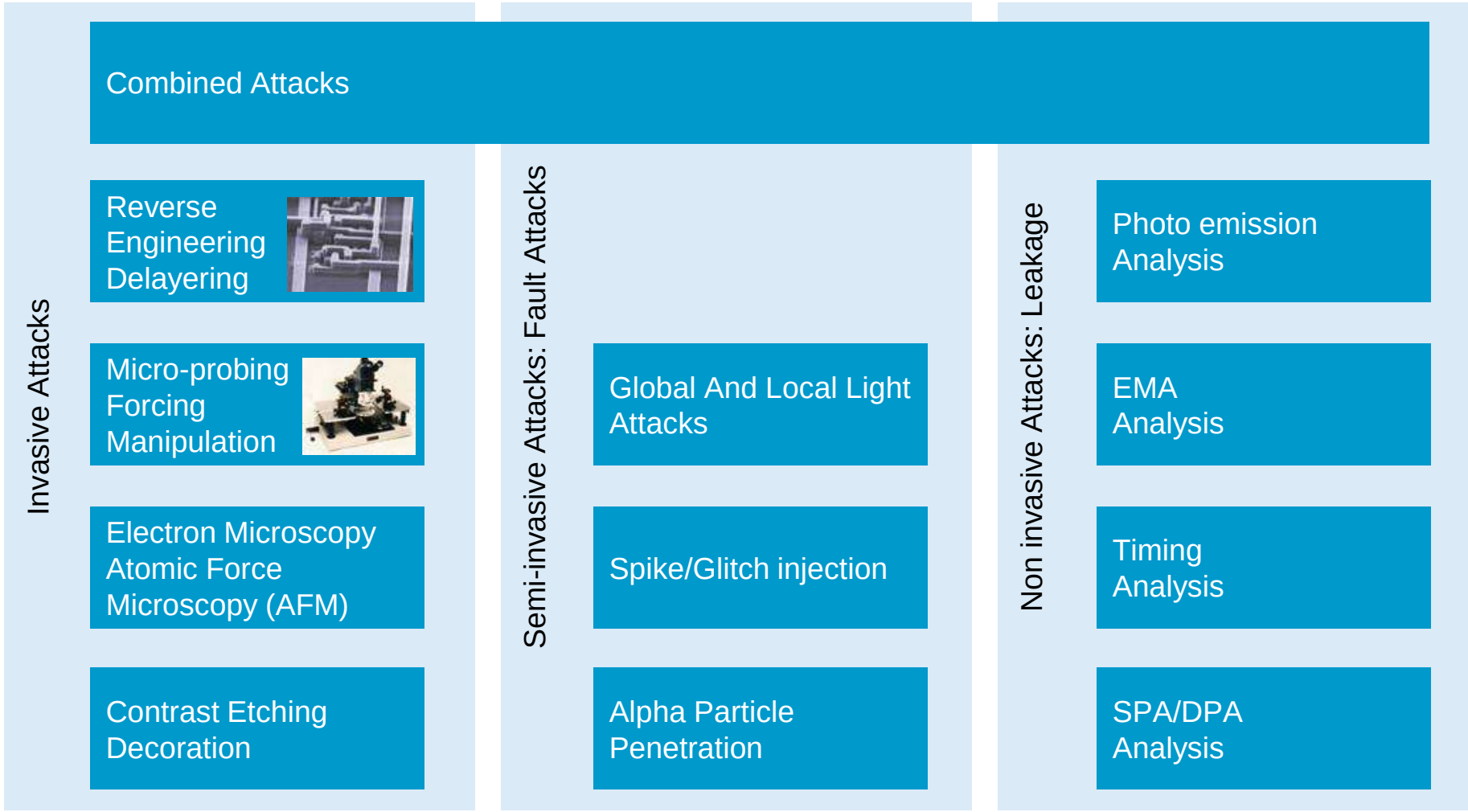
Elliptic Curve Crypto (ECC) Based Authentication



But 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

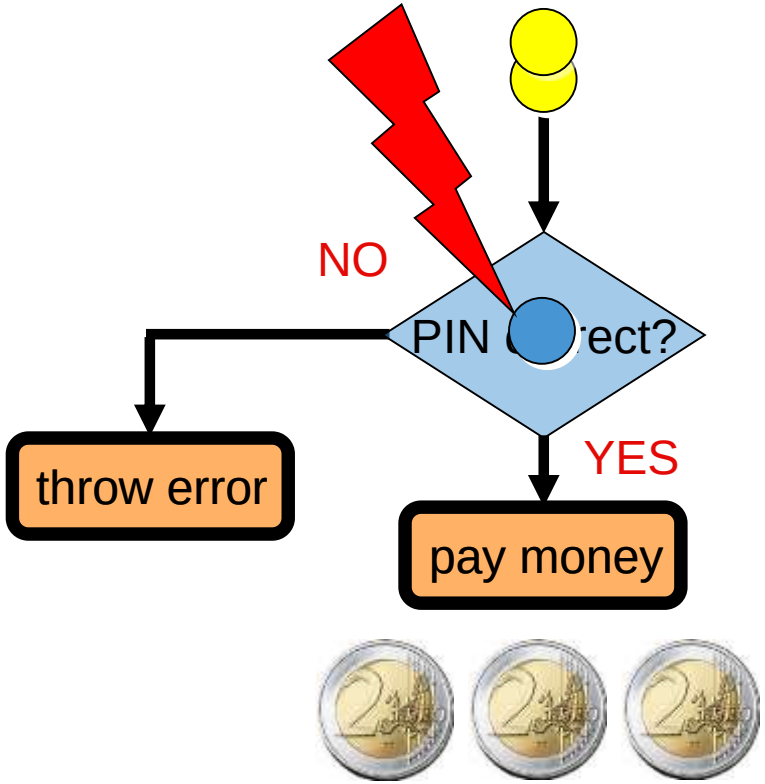


Attacker's goal is to steal the secret key(s)

Fault Attacks with Lasers

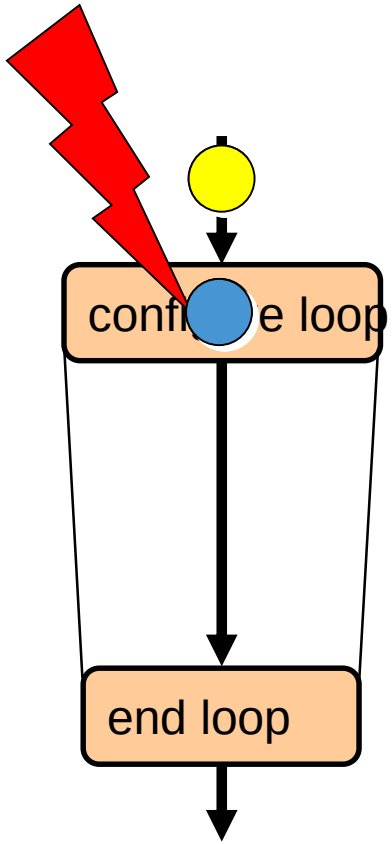
Simple Fault Attacks: Code Execution

attack critical jumps…



Simple Fault Attacks: Code Execution

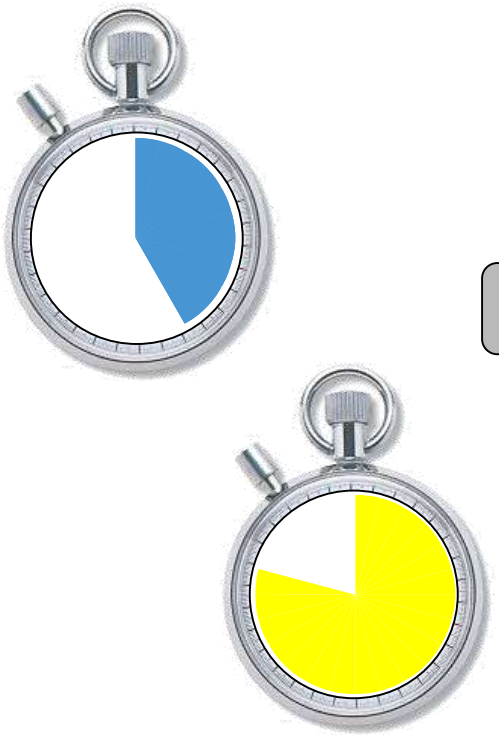
attack I/O loop…
(copy from buffer)

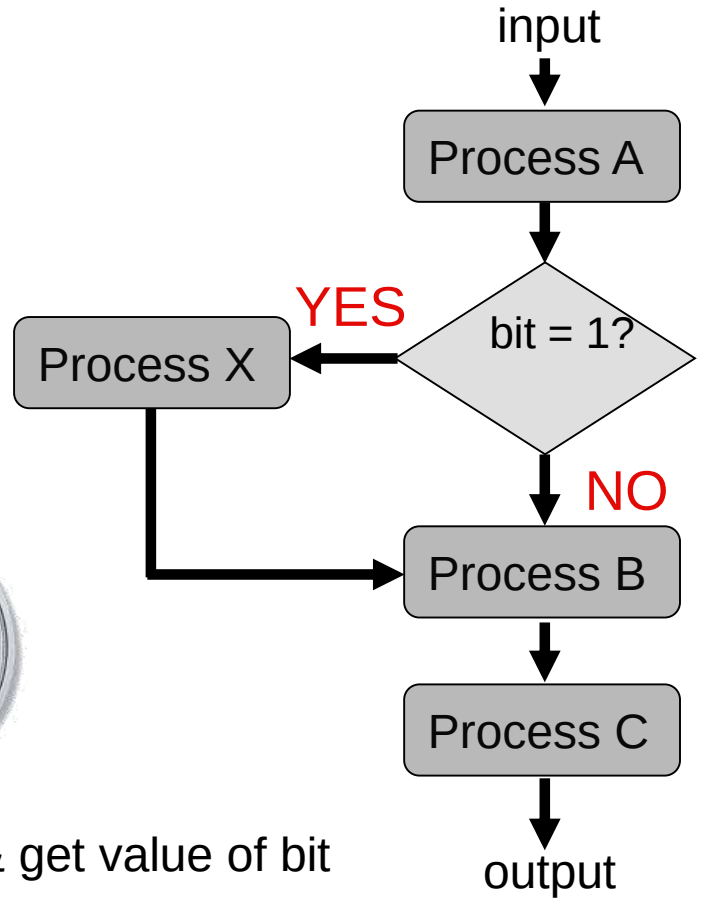


Hello world!

Memory dump: FB AE 04 23 82 F3 D1 …

Timing Attack





measure difference & get value of bit

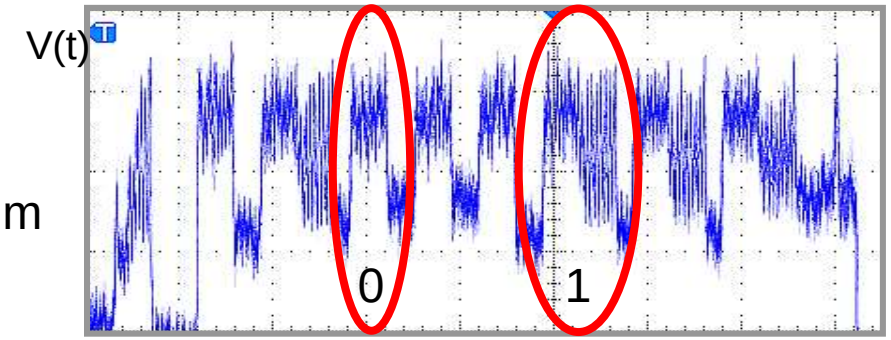
Timing / SPA Attack: Example RSA

Modular exponentiation: $x = m^k \bmod N$

$x = m$
for $i = n-2$ down to 0
  $x = x^2$
  if $(k_i == 1)$ then
    $x = x \cdot m$
endfor
return x

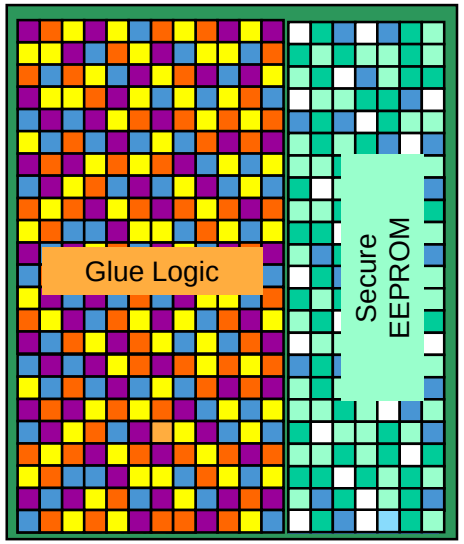
square & multiply algorithm

execution time depends on value of secret bit k_i!



Key Value: 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
- Voltage sensors on the IC
- Active and passive shielding
- Protected true random number generator
- Secured Cores
  - 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)



A1006 Secure Authenticator Product Introduction

A1006 Secure Authenticator – Key Customer Benefits

Targeted for Anti-counterfeit applications…	*… Providing strong asymmetric cryptographic solution coupled with industry leading NXP security technology and services*
Highly Secure …	*… Industry leading tamper resilience and countermeasures against SPA, DPA and other invasive and non-invasive attacks. Die specific key injection preventing scalable attacks.*
Fast, Small and low power…	*… Providing very small package(1x1 mm), very fast authentication (~ 50 ms) and supporting a deep sleep mode consuming very low power(~ 1 uA)*
No secure element in the host…	*… PKI based asymmetric cryptography with private keys never leaving the secure element. No Secure IC needed in the host*
Complete Solution	*… Host reference library, developer kit, certificate provisioning tool, trust provisioning options*

Tamper Resistant Authentication - A1006

- No security IC needed on host side because of PKI (Public Key Infrastructure) authentication
  - Asymmetric/public key based ECDH (Elliptic Curve Diffie-Hellman) explicit authentication protocol with NIST-b163 curve
  - Digitally signed X509v3 certificates using ECDSA signatures with NIST-p224 curve and SHA-224 digest hash
- Industry leading advanced security features include: TRNG, active shielding, security sensors, many more
- 4 kbit EEPROM supports 2 certificates, system memory, and 1kbit for user needs
- Industry's lowest power (550uA max)
  - Deep sleep power < 1 uA at 1.8V Vdd
- Industry's smallest footprint – as small as 1 mm2 in WLCSP
  - Also available in HXSON6 2 x 2 mm package
- Flexible Interfaces: 400 kbps I2C or one wired interface
  - OWI bus powered (no external Vdd needed)
  - OWI interface rated 8kV IEC61000-4-2 ESD protection

A1006 EEPROM Details

4kbit EEPROM split into 4 regions x 1kbit:

1st Certificate area	2nd Certificate area	User memory	System memory
			
NXP Generic Certificate Once this leaves NXP factory, it is read-only.	User-defined certificate injected at the customer manufacturing flow. In “User-mode”: this area is locked, and becomes read only.	Always accessible (RW)	System memory (not accessible by customer ever)

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 550 uA full-on, < 1 uA deep sleep
  - Full certificate validation plus ECC challenge-response in ~50 ms
- Ease of system integration
- Bus-powered one wire interface
  - 8kV IEC61000-4-2 contact ESD protection
  - Demo board and host demo software available
  - Applications support team includes security experts

A1007 Preview

A1007 for Consumables – Launching Soon

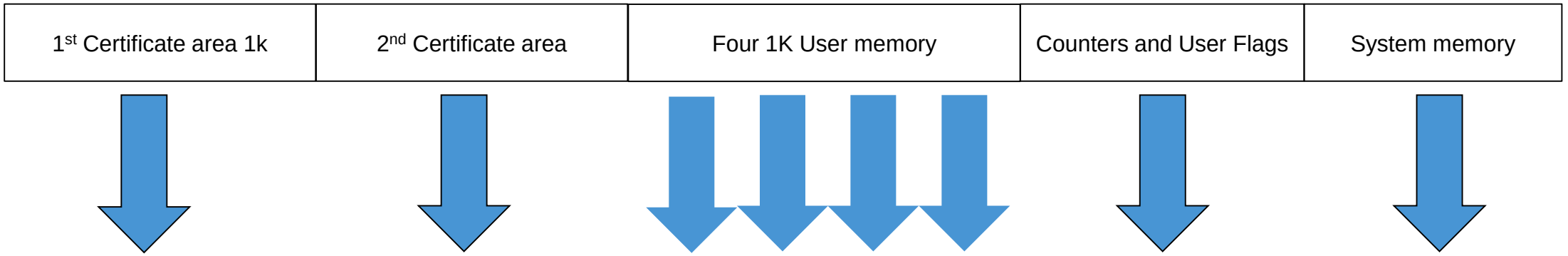
- No security IC needed on host side because of public key authentication (PKI)
  - Asymmetric public/private key Diffie-Hollman authentication protocol based on NIST ECC B-163 curve
  - Digitally signed certificates using ECDSA and NIST ECC P-224 curve
  - PRESENT cipher for locking user memory
- Features for consumables:
  - Two one-way counters
  - 24 non-resettable flags
  - Lockable user space
  - Kill-chip command
- Industry leading advanced security features include: TRNG, active shielding, security sensors, DPA/SPA, many more
- 8kbit EEPROM supports 2 certificates, system memory, and 4kbit for user needs
- Industry's lowest power (550uA max)
  - Deep sleep power < 1 uA at 1.8V Vdd
- Small footprint – available in HXSON6 2 x 2 mm package
  - CSP package - 1.3 x 0.94 mm WLCSP4
- Flexible Interfaces: 400 kbps I2C or one wired interface
  - OWI bus powered (no external Vdd needed)
  - OWI interface rated 8kV IEC61000-4-2 ESD protection

A1007 Secure Authenticator – Key Customer Benefits

Targeted for Consumables markets…	*… Providing strong asymmetric cryptographic solution coupled with industry leading NXP security technology and services*
Highly Secure …	*… Industry leading tamper resilience and countermeasures against SPA, DPA and other invasive and non-invasive attacks. Die specific key injection preventing scalable attacks.*
Fast, Small and low power…	*… Providing very small package(1.3 x 0.94 mm), very fast authentication (~ 50 ms) and supporting a deep sleep mode consuming very low power(~ 1.5 uA)*
No secure element required in the host…	*… PKI based asymmetric cryptography with private keys never leaving the secure element. No Secure IC needed in the host*
Authenticated User Memory and Counters	*… Anti tearing counters; Lightweight symmetric present80 cipher for authenticated reads of user memory and counters*
Kill Command	*… Secure End of Life*
Complete Solution	*… Host reference library, developer kit, certificate provisioning tool, trust provisioning options*

A1007 EEPROM Details

8kbit EEPROM split into 8 regions x 1kbit:



NXP Generic Certificate Once this leaves NXP factory, it is read-only.

User-defined certificate injected at the customer manufacturing flow. In “User-mode”: this area is locked, and becomes read only.

Accessible after unlock (Authenticated Reads and Writes)

Always accessible (Authenticated Reads Increment Counters)

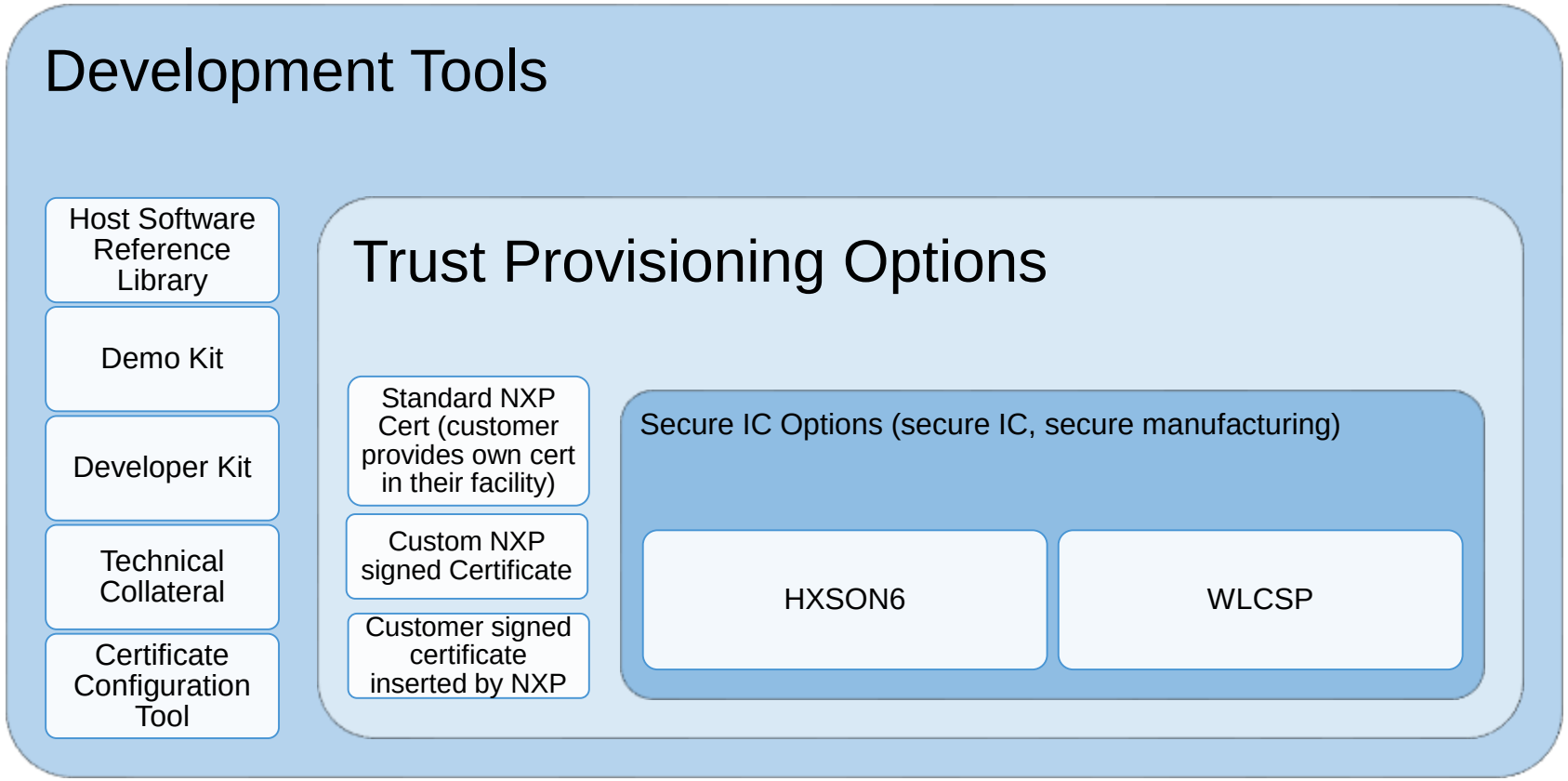
System memory (not accessible by customer ever)

Comparing A1006 vs A1007

Feature	A1006	A1007	Comment
Cryptographic Auth	ECC NIST-B163 ECDH	ECC NIST-B163 ECDH + PRESENT80 cipher MAC	Symmetric cipher MAC added for authenticated data
Authenticated Read/Write	No	Yes	Per flow diagram
Certificate Validation	X509v3 DER certificate signed with ECDSA using ECC NIST-P224 and SHA-224	X509v3 DER certificate signed with ECDSA using ECC NIST-P224 and SHA-224	No change
Authentication Protocol	Explicit using ECDH challenge-response validation	Implicit using per ECDH challenge for key agreement, followed by MAC response validation	See flow diagram
Interfaces	I2C, OWI	I2C, OWI	No change
Package	HXSON6, WLCSP4	HXSON6, WLCSP4	No change
Memory Size	4 kbit (1 kbit user memory + 2 certificate)	8 kbit (4 kbit user memory + 2 certificates)	Increase user data storage
24-bit one-way counter x 2	No	Yes	Eg. measure ink/page consumption
Non-resettable operation flag	No	16-bit individually settable, cannot be cleared	Track different usage states
ESD Level	2kV HBM (8kV IEC on OWI)	4 kV HBM (8kV IEC on OWI)	Improved robustness in high-touch environments
CRC Checksum	No	Yes	Improved data reliability
Kill Chip command	No	Yes	Permanent shut down prevents refills and other illegitimate uses

Development Tools and Provisioning Utility

A1006/A1007 “Whole Product”



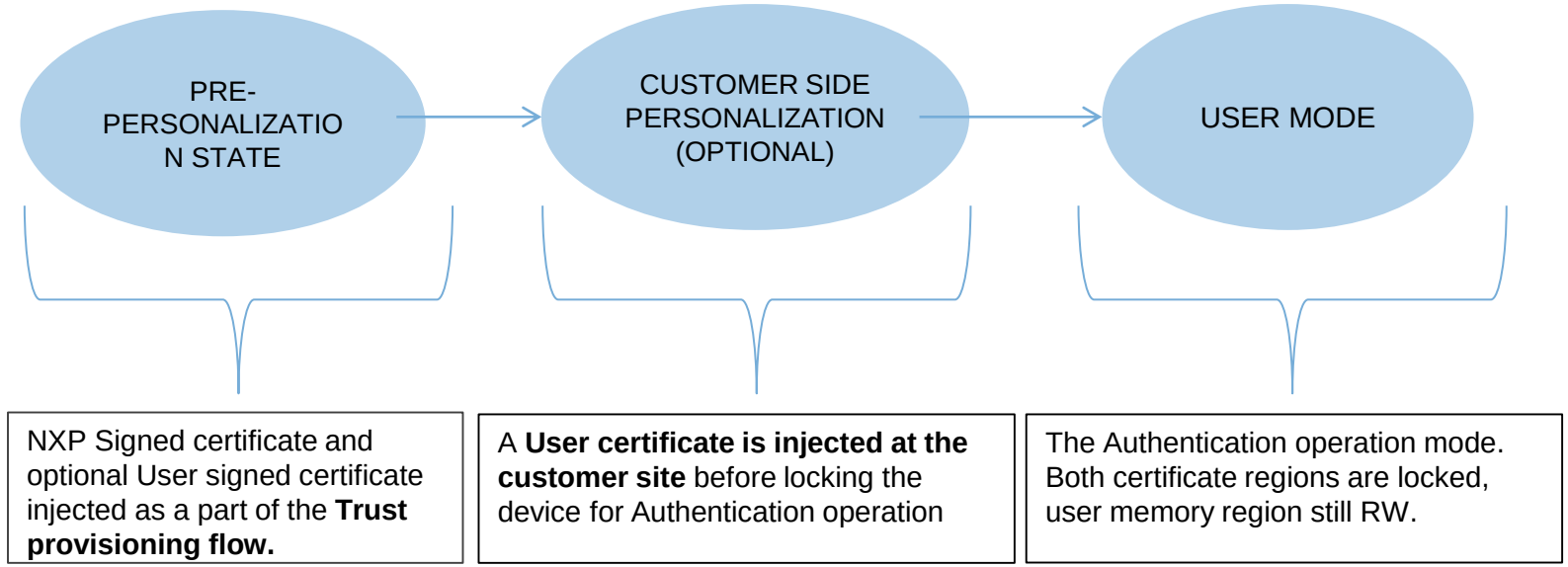
Supplemented by:

- Sales Tools (Demo boards, Collateral, Presentations, White Papers)
- Deep Security Expertise

NXP 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
- 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

A1006 / A1007 Life Cycle stages – Standard Product



Customer side personalization:

- NXP delivers the standard part with a generic NXP digital certificate
- Customers 1) read the public key from the NXP Cert.; 2) create their own Cert. using the same public key and adding customer data; 3) insert the Custom Cert. into the chip in the 2nd Cert. area.
- NXP Smart Card-based Tool to Assist is Now Available

NXP Trust Provisioning Services – Flexible Options

Flexible options available for certificate injection using NXP's Secure Trust Provisioning flow

Standard Product: NXP signed generic Digital Certificate

- NXP acts as "Certificate Authority" and signs a generic NXP certificate. The A1006 IC is supplied in "Customer side personalization" mode to allow additional customer-specific certificate to be inserted.

Customer signed Digital Certificate with customer-specific information

- The A1006 IC ships with a user certificate, containing user-specific information, which NXP signs using the customer signing key within NXP HSM.
- IC can be delivered in either customer provisioning mode (to allow additional data to be locked in 2nd slot) or user mode.

A1006 / A1007 Customer Certificate Provisioning Utility

Use Cases	Specify customer-specific data and signing key for NXP-injected User Certificates
	Provision user-signed certificates in user's factory
	Securely control (limit) certificate provisioning at 3rd party manufacturing sites
Key Features:	Smart-Card for secure storage of signing key and issuance of certificates
	Cross-Platform Web GUI based User Interface
Capabilities:	Create or Import User Certificate Signing Key
	Clone Signing Key to Additional Cards
	Securely provision individual A1006/A1007 with user-signed certificates
	Restrict # of devices that can be provisioned

NXP Trust Provisioning Overview

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 Trust Provisioning: Key Benefits

Value Proposition	Customer Benefit
Reliable Secure Certified Process	- Higher supply chain security - Reduces the security risks and complexity involved in injecting keys and ceriticates at customer site.
Cost savings and faster TTM	- No investment needed for secure equipment, and certified manufacturing facility - Reduced test time in the customer system manufacturing line without the need for key/certificate injection per die - Cost savings and shorter lead times/faster time-to-market
Flexible customization options	- Customized Service – Optional User certificate with User parameters can be injected per die in our Secure manufacturing facilities

$

Supporting Materials

Accessing Datasheet and other Support Materials	These are security documents	
	Encypted secure distribution protects customer and NXP	
	Register in DocStore for documents:	
	https://www.docstore.nxp.com/flex/DocStoreApp.html	
Tools	Demo boards, samples, developer kits are available now	Available through sample store, but need PL approval
	Certificate configuration tool (beta) available now	Contact product line
Additional Info Available on NXP Authentication Web page	Product Brief , White papers, Demo Video	A1007 Launching Soon: 2019
	www.nxp.com/authentication	

SECURE CONNECTIONS
FOR A SMARTER WORLD

www.nxp.com