Introducing A1006 Secure Authenticator
Tamper-Resistant Anti-Counterfeit Solution

NXP

SECURE CONNECTIONS
FOR A SMARTER WORLD

NXP SECURITY OVERVIEW

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

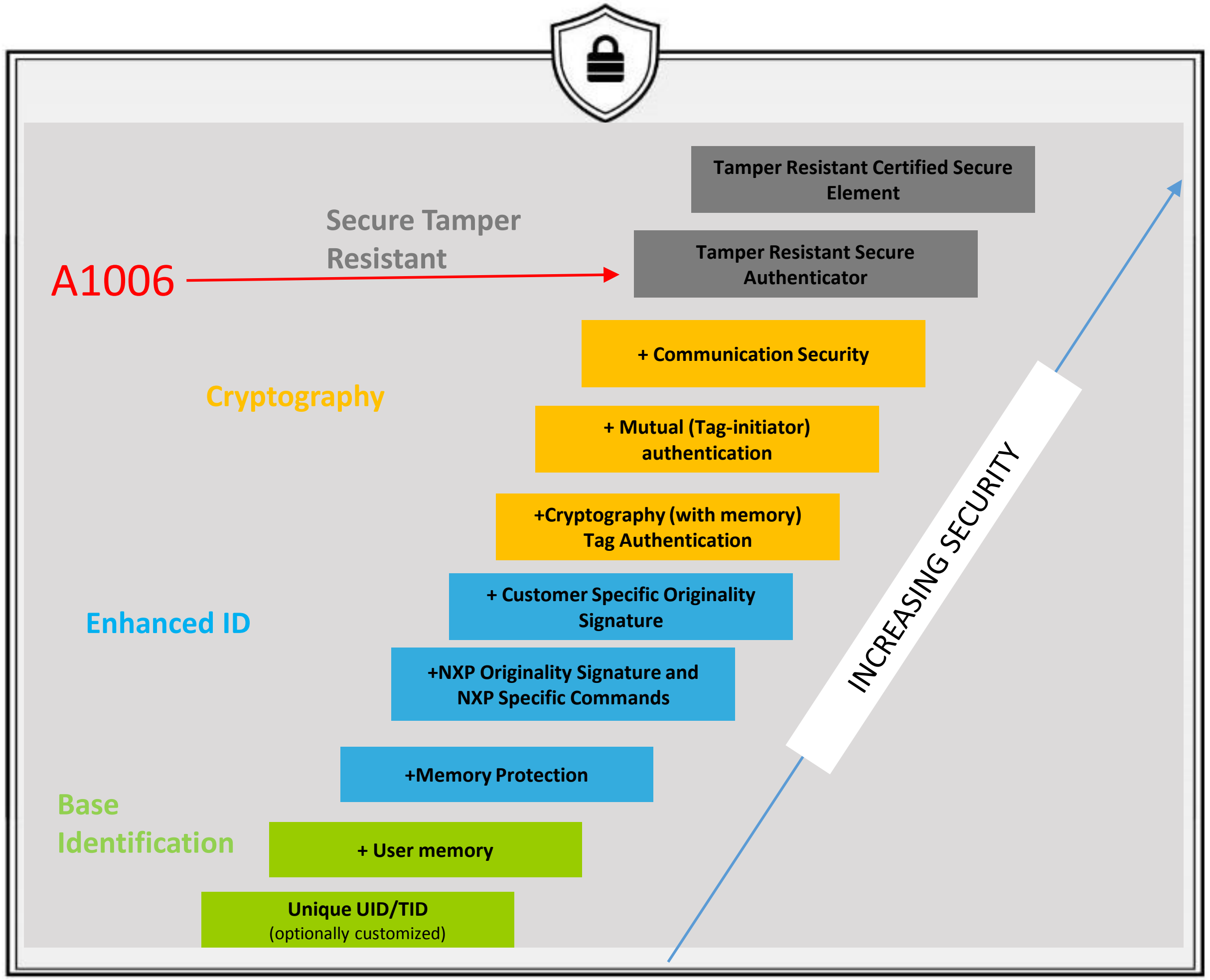
* Source: IHS 2016

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



Tamper Resistant Certified Secure Element

Secure Tamper Resistant

A1006

Tamper Resistant Secure Authenticator

Cryptography

+ Communication Security

+ Mutual (Tag-initiator) authentication

+Cryptography (with memory) Tag Authentication

Enhanced ID

+ Customer Specific Originality Signature

+NXP Originality Signature and NXP Specific Commands

+Memory Protection

Base Identification

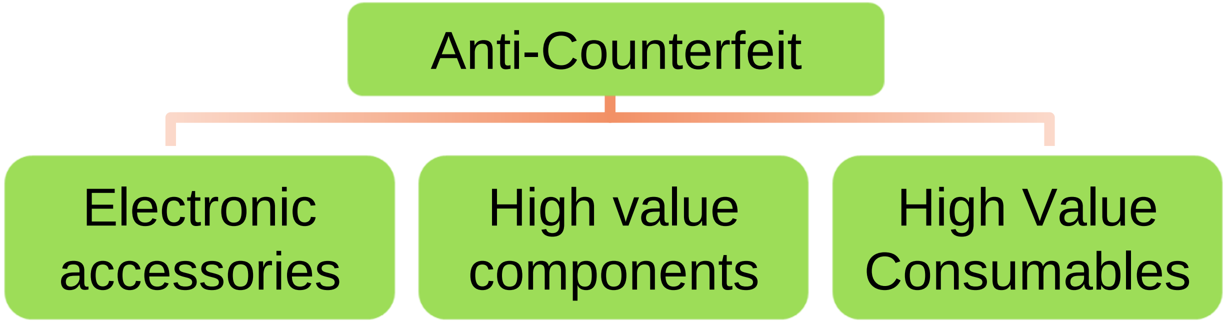
+ User memory

Unique UID/TID (optionally customized)

INCREASING SECURITY

USE CASES

Anti-counterfeit Protection



Electronic Accessories

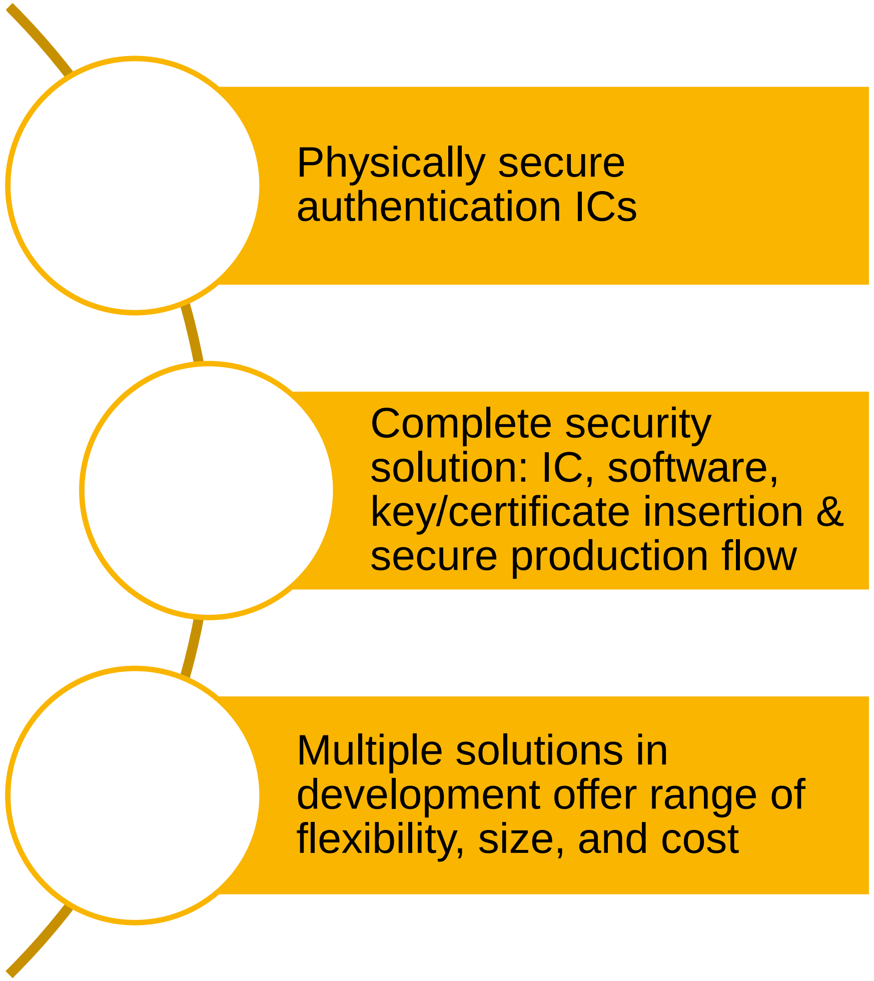
- Charger
- Keyboard
- Cables

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 in development offer range of flexibility, size, and cost

Counterfeited Batteries and Chargers Are a 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

But Will That Affect My Products?

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

- “**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

- “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

Consumer

Cameras

DVs

Wireless
Power

Hoverboards

Smartphones

Power Banks

Drones

Tablets

Portable Audio
Speakers

Notebooks/
Ultrabooks

Medical

Handheld
Medical

Fitness
Watches

Medical Tablets

Portable
Doppler
Imaging

Barcode
Scanners

Blood Glucose
Monitoring

Surgical Systems

Industrial

Portable
Industrial
PDAs

Portable Industrial PCs

Power Tools

Uninterruptable
Power Supply (UPS)

All replaceable batteries and high powered 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 the 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

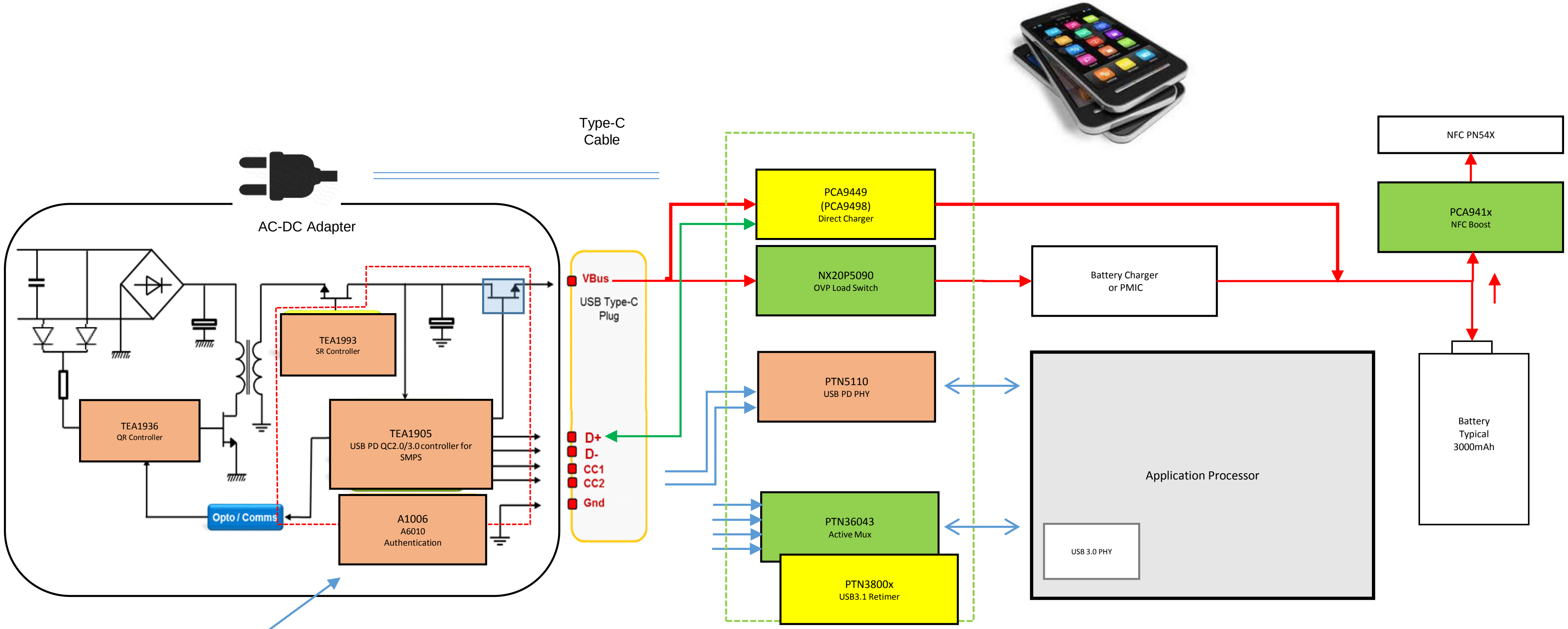
USB charging ports are everywhere – rental car, taxis, airports, …

- 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 – End to End Solutions



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

🟩 Released

🟧 In Development

🟨 Concept (New)

Working demo of USB PD VDM-based Authentication with TEA1905 and A1006 is available

Authenticating Electronic Accessories

Mandatory
Authentication IC

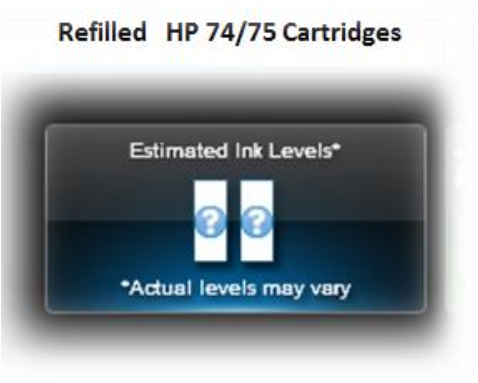
Official
Licensed
Product

- 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

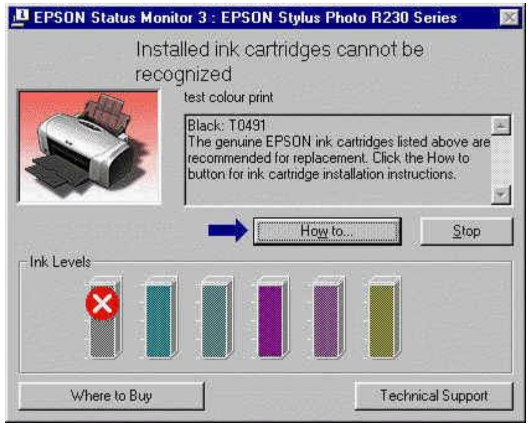
- Commonly used in both inkjet and laser printers
  - Protect revenue source (make money on ink/toner, not printer)
- Cartridge Authentication Options
  - Only genuine printer cartridges work
  - Warn user that cartridge is not genuine
  - Allow refills and clones, but potentially reduced functionality

Refilled HP 74/75 Cartridges



Estimated Ink Levels*

*Actual levels may vary

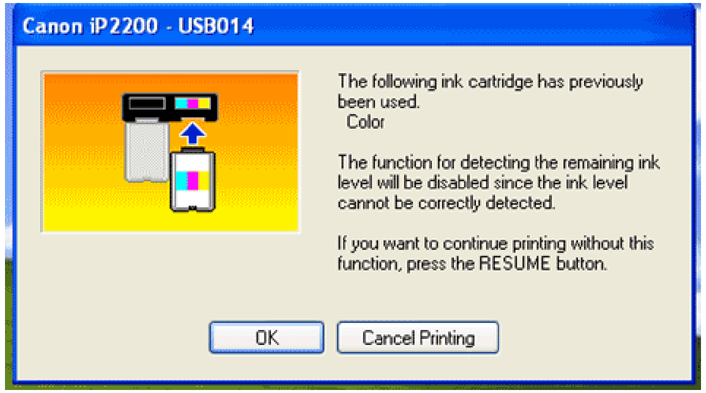


EPSON Status Monitor 3 : EPSON Stylus Photo R230 Series

Installed ink cartridges cannot be recognized

test colour print

Black: T0491
The genuine EPSON ink cartridges listed above are recommended for replacement. Click the How to button for ink cartridge installation instructions.

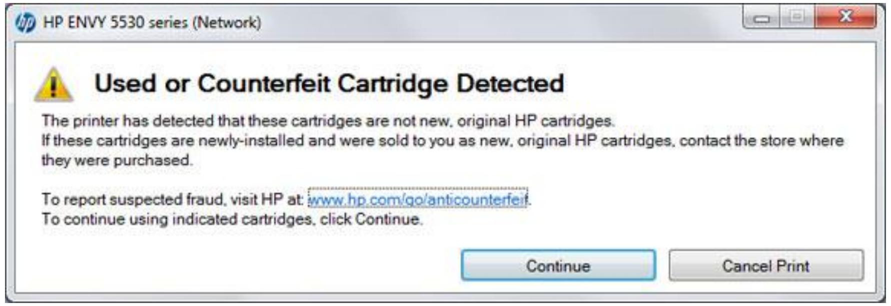


Canon iP2200 - USB014

The following ink cartridge has previously been used.
Color

The function for detecting the remaining ink level will be disabled since the ink level cannot be correctly detected.

If you want to continue printing without this function, press the RESUME button.



HP ENVY 5530 series (Network)

Used or Counterfeit Cartridge Detected

The printer has detected that these cartridges are not new, original HP cartridges.
If these cartridges are newly-installed and were sold to you as new, original HP cartridges, contact the store where they were purchased.

To report suspected fraud, visit HP at: www.hp.com/go/anticounterfeit.
To continue using indicated cartridges, click Continue.

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

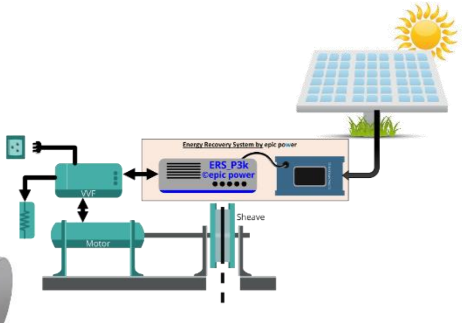
Other applications – More than 150 open opportunities!

Consumables – consumer, medical

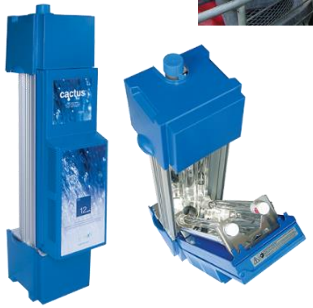
Accessories

Access Control

Revenue enforcement



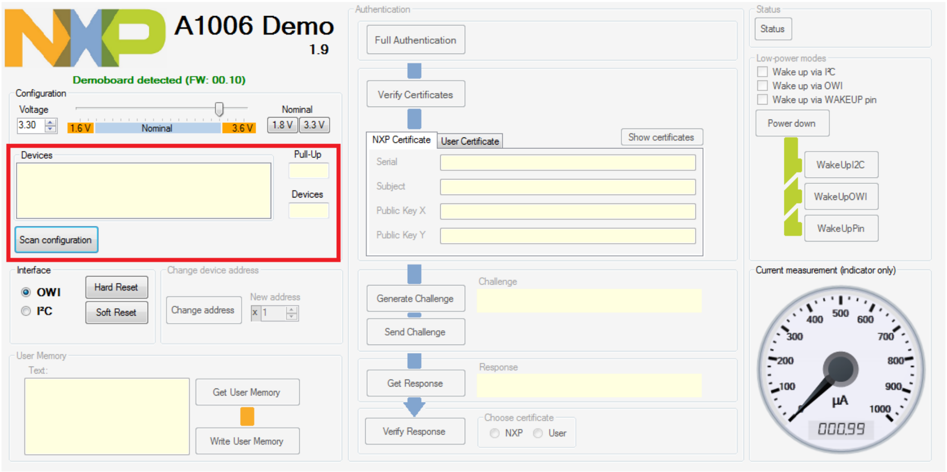
Industrial



PRODUCT OVERVIEW

Tamper Resistant Authentication - A1006

- No security IC needed on host side because of public key authentication (PKI)
  - Asymmetric public/private key Diffie-Hollman authentication protocol based on ECC B-163 curve
  - Digitally signed certificates using 224-bit ECDSA 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 (500uA max)
  - Deep sleep power < 1 uA at 1.8V Vdd
- Industry's smallest footprint – as small as 1 mm^2 in WLCSP
  - Also available in HXSON6 2 x 2 mm package
- Flexible Interfaces: 400 kbps I^{2}C or one wired interface
  - OWI bus powered (no external Vdd needed)
  - OWI interface rated 8kV IEC61000-4-2 ESD protection



A1006 Demo 1.9

Demoboard detected (FW: 00.10)

Configuration — Voltage: 3.30

Interface: ● OWI ○ I²C

Change device address — New address: x 1

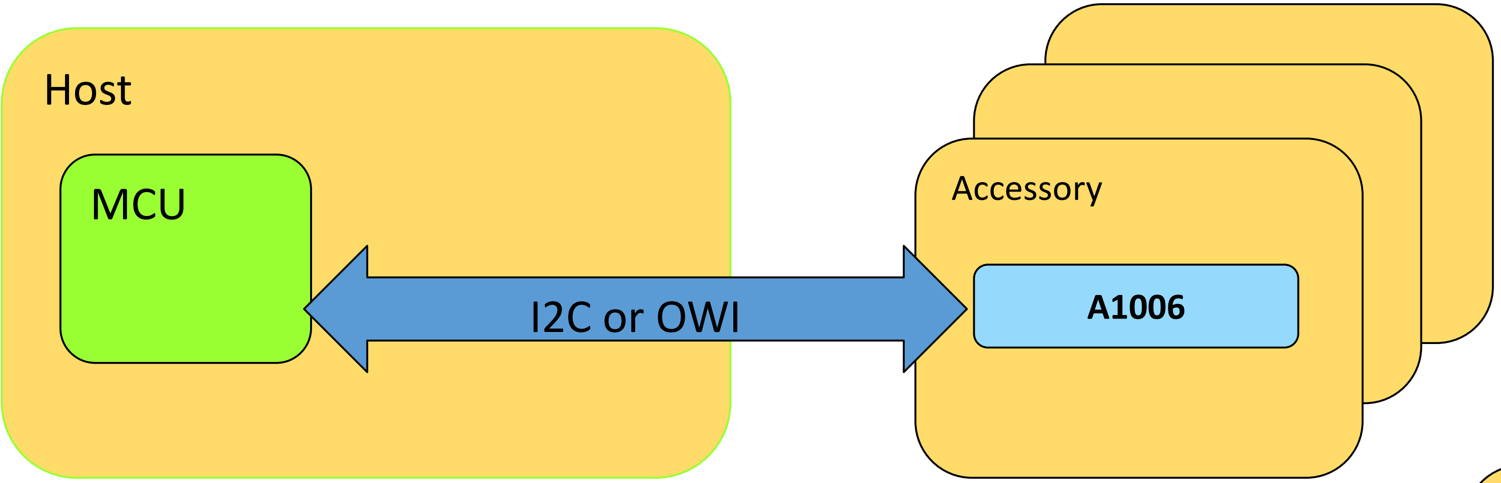
Low-power modes: □ Wake up via I²C □ Wake up via OWI □ Wake up via WAKEUP pin

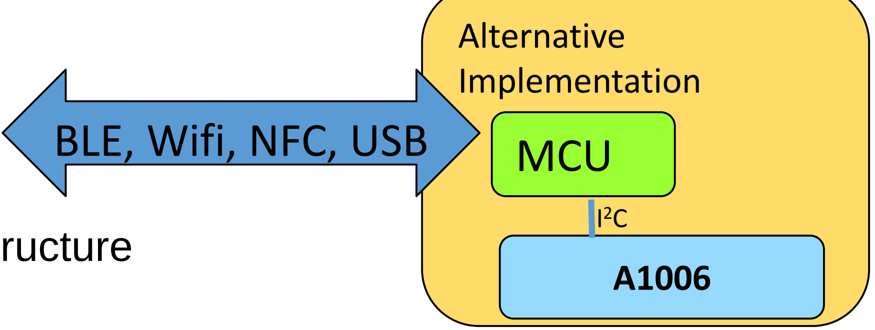
Choose certificate: ○ NXP ○ User

Current measurement (indicator only): 000.99 µA

Production Released

Key Value: Asymmetric Crypto-based Authentication

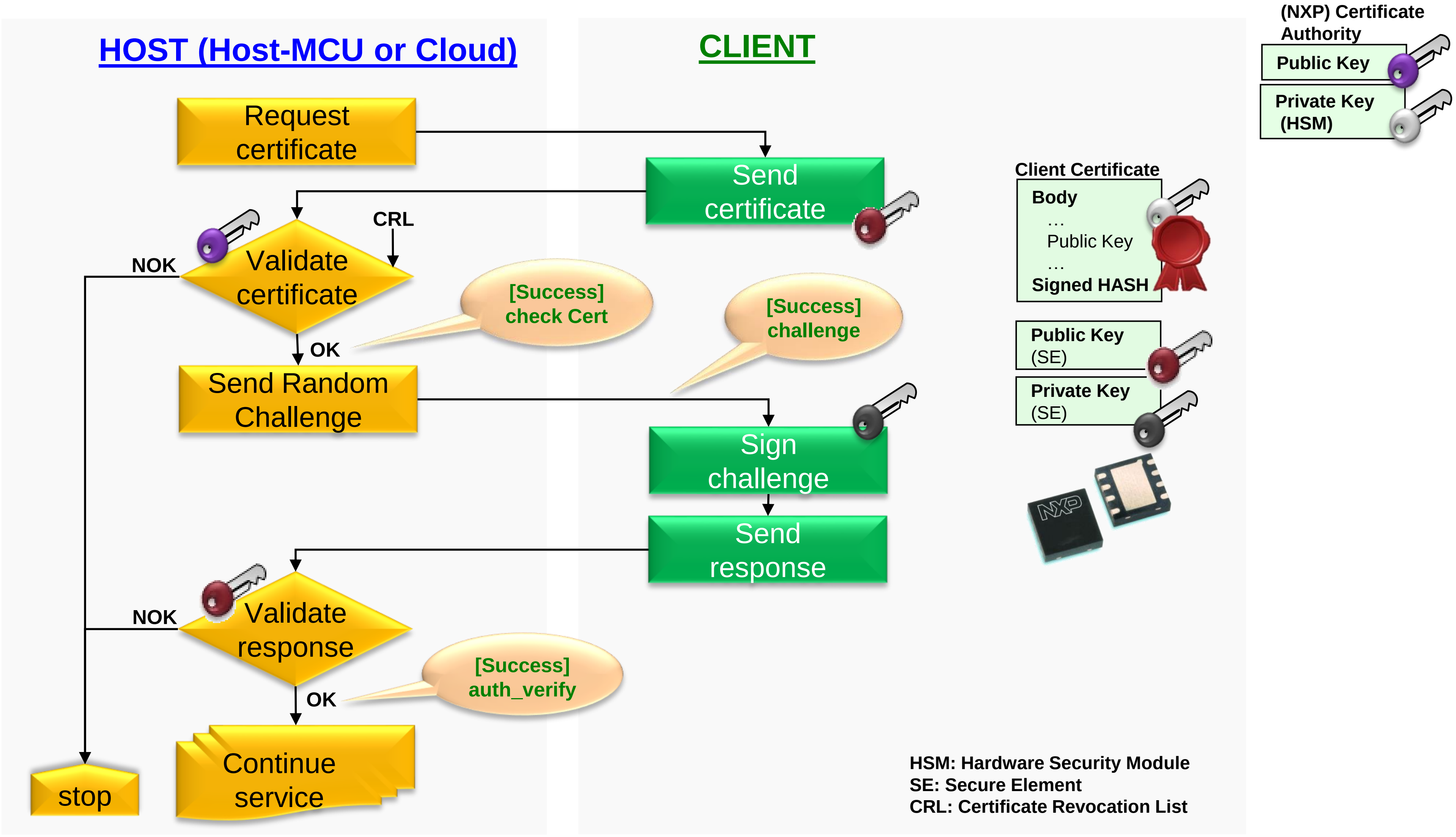




Benefits:

- 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



HOST (Host-MCU or Cloud)

CLIENT

Request certificate

Send certificate

Validate certificate

CRL

NOK

OK

[Success] check Cert

Send Random Challenge

[Success] challenge

Sign challenge

Send response

Validate response

NOK

OK

[Success] auth_verify

stop

Continue service

(NXP) Certificate Authority

Public Key

Private Key (HSM)

Client Certificate

Body

…

Public Key

…

Signed HASH

Public Key (SE)

Private Key (SE)

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

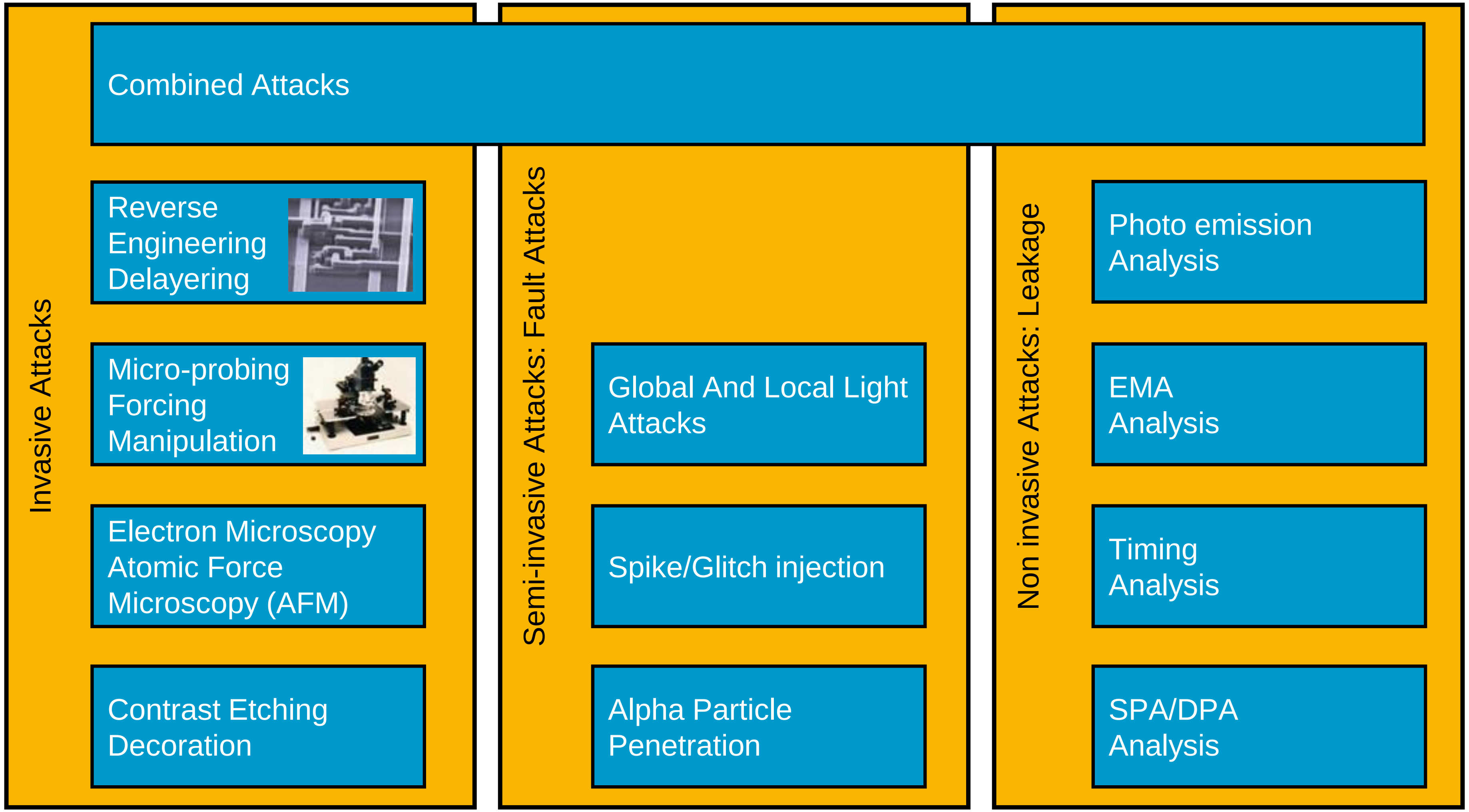
If an attacker can get the keys, they don’t need to break the crypto

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

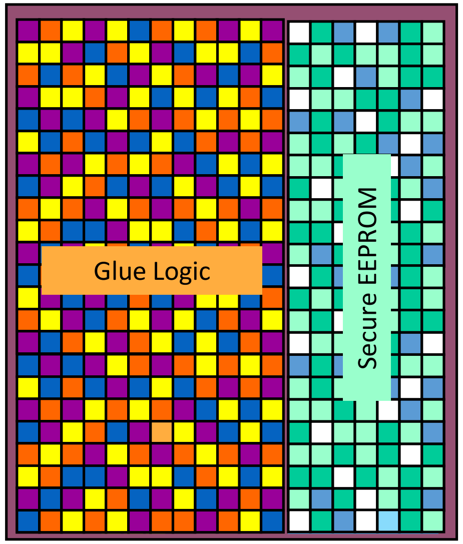
Timing Analysis

SPA/DPA Analysis

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

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)



TRUST PROVISIONING

Key Value: NXP Trust Provisioning Service

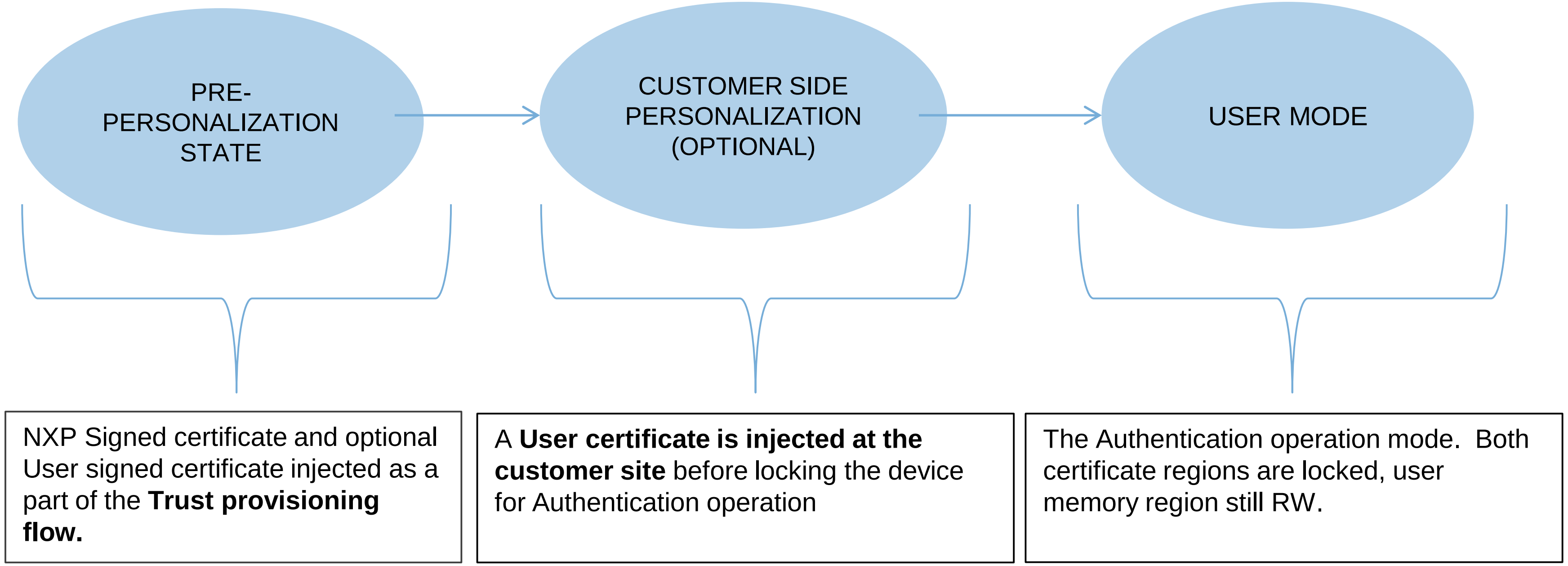
Creation of secret keys, certificates & personalization data in HSM

- Only **HSM**’s (Hardware Security Modules) with CC EAL5+ certification has 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

A1006 Life Cycle stages – Standard Product



PRE-PERSONALIZATION STATE

CUSTOMER SIDE PERSONALIZATION (OPTIONAL)

USER MODE

NXP Signed certificate and optional User signed certificate injected as a part of the **Trust provisioning flow.**

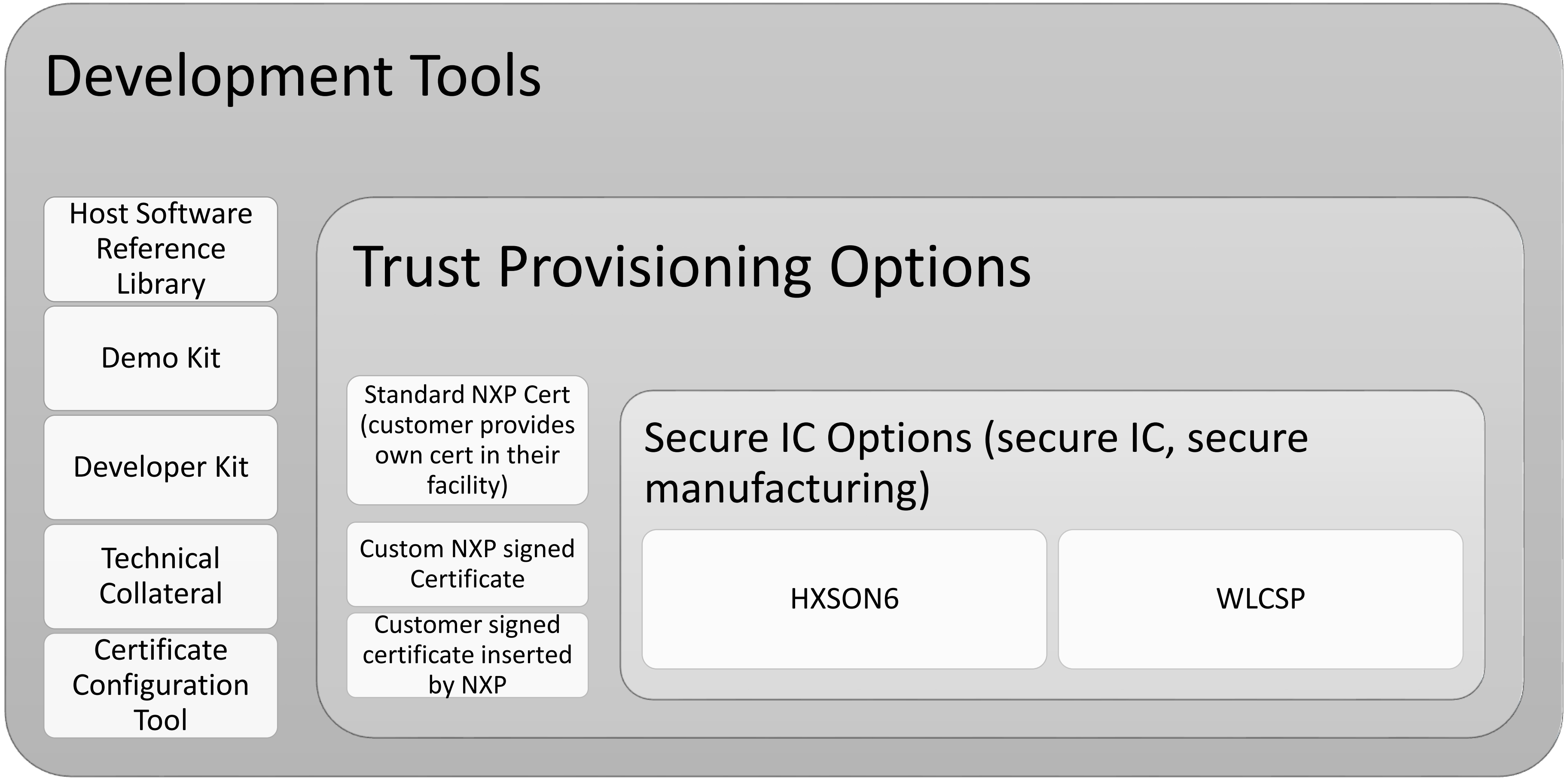
A **User certificate is injected at the customer site** before locking the device for Authentication operation

The Authentication operation mode. Both certificate regions are locked, user memory region still RW.

- 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

SUPPORT MATERIALS

A1006 “Whole Product”



Development Tools

Host Software Reference Library

Demo Kit

Developer Kit

Technical Collateral

Certificate Configuration Tool

Trust Provisioning Options

Standard NXP Cert (customer provides own cert in their facility)

Custom NXP signed Certificate

Customer signed certificate inserted by NXP

Secure IC Options (secure IC, secure manufacturing)

HXSON6

WLCSP

Supplemented by:

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

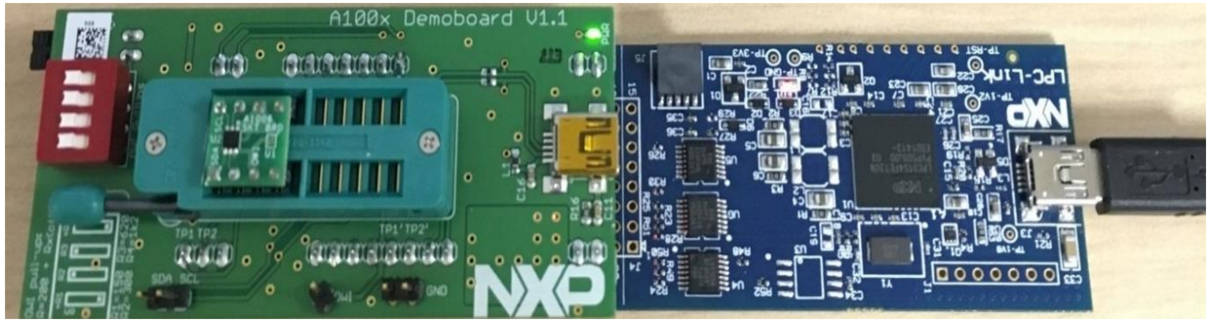
Supporting Materials

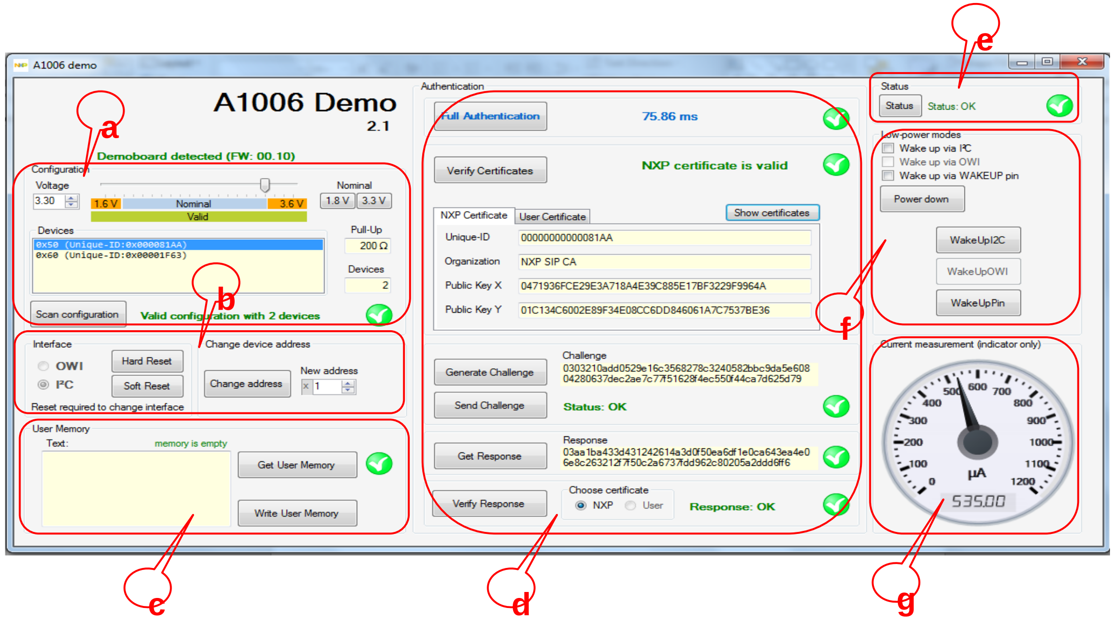
Accessing Datasheet and other Support Materials	These are security documents
	Encypted secure distribution protects customer and NXP
	Register in DocStore for documents:
	https://www.docstore.nxp.com/flex/DocStoreApp.html
Tools	Demo boards, samples, developer kits are available now
	Certificate configuration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

A1006 – Demo Platform

PC based Demo Platforms available.

- HW Demo on OWI and I2C
- Host authentication is running from PC.
- Based on LPC1769




A1006 demo

A1006 Demo
2.1

Demoboard detected (FW: 00.10)

Configuration
Voltage: 3.30
Nominal
Devices:
```
0x50 (Unique-ID:0x000081AA)
0x60 (Unique-ID:0x00001F63)
```
Pull-Up: 200 Ω
Devices: 2
Valid configuration with 2 devices

Interface
○ OWI
● I²C
Reset required to change interface

Change device address
New address: x 1

User Memory
Text: memory is empty

Authentication
Full Authentication: 75.86 ms
Verify Certificates: NXP certificate is valid

NXP Certificate	User Certificate
Unique-ID	00000000000081AA
Organization	NXP SIP CA
Public Key X	0471936FCE29E3A718A4E39C885E17BF3229F9964A
Public Key Y	01C134C6002E89F34E08CC6DD846061A7C7537BE36

Challenge
0303210add0529e16c3568278c3240582bbc9da5e608
04280637dec2ae7c77f51628f4ec550f44ca7d625d79
Status: OK

Response
03aa1ba433d431242614a3d0f50ea6df1e0ca643ea4e0
6e8c263212f7f50c2a6737fdd962c80205a2ddd6ff6

Choose certificate
● NXP ○ User
Response: OK

Status
Status: OK

Low-power modes
□ Wake up via I²C
□ Wake up via OWI
□ Wake up via WAKEUP pin

Current measurement (indicator only)
535.00 µA

NXP

SECURE CONNECTIONS
FOR A SMARTER WORLD