Security Matters.

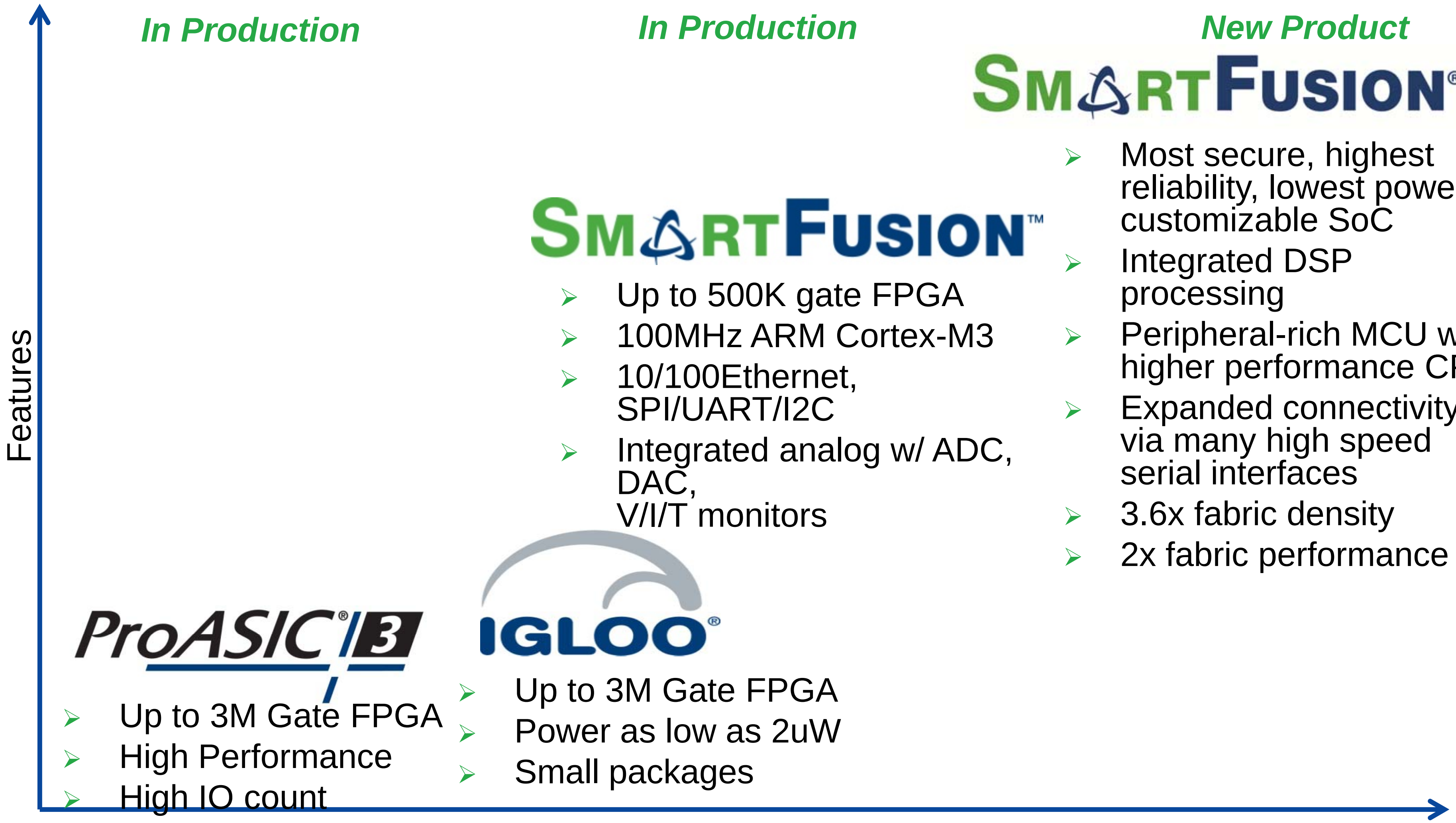
Recent Advances in FPGA Design Security Reduce Insider Threats

Presented by G. Richard Newell
Senior Principal Product Architect

At Cryptarchi 2013
June 24, 2013, Fréjus, France

Microsemi SoC Flash Products

Increasing system features on differentiated flash technology



In Production

ProASIC®3

- Up to 3M Gate FPGA
- High Performance
- High IO count

In Production

SmartFusion™

- Up to 500K gate FPGA
- 100MHz ARM Cortex-M3
- 10/100Ethernet, SPI/UART/I2C
- Integrated analog w/ ADC, DAC, V/I/T monitors

IGLOO®

- Up to 3M Gate FPGA
- Power as low as 2uW
- Small packages

New Product

SmartFusion® 2

- Most secure, highest reliability, lowest power customizable SoC
- Integrated DSP processing
- Peripheral-rich MCU with higher performance CPU
- Expanded connectivity via many high speed serial interfaces
- 3.6x fabric density
- 2x fabric performance

SmartFusion®2 - Flash SoC FPGA w/ ARM Cortex-M3
Most Secure, Highest Reliability, Lowest Power

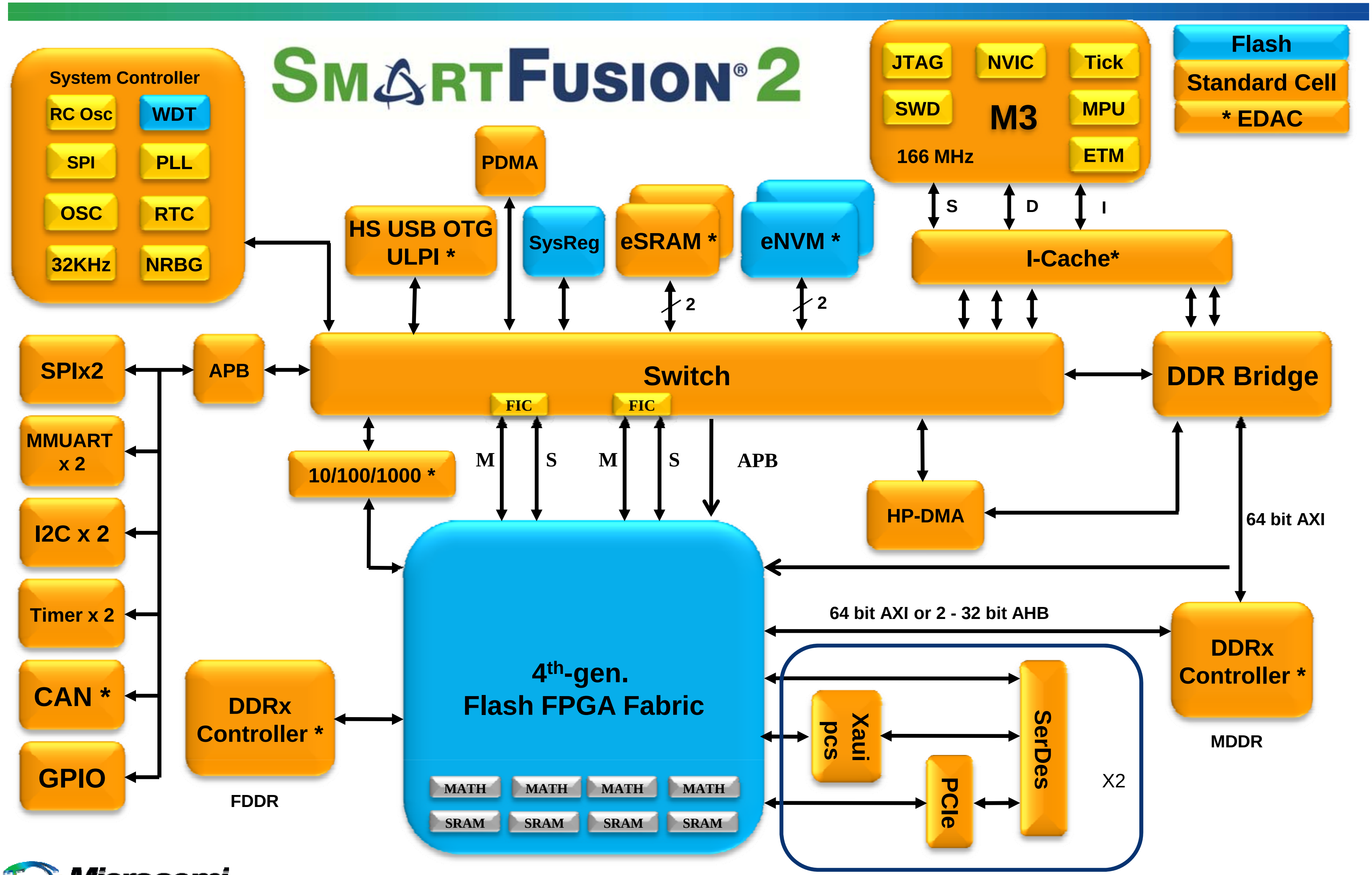
Differentiated, High Value Features

- 166MHz ARM® Cortex™-M3 w/ on board eSRAM & eNVM
  - Includes ETM and instruction cache
  - Extensive peripherals CAN, TSE, USB
- Most secure FPGA
  - DPA hardened, AES256, SHA256, random number generator
- Most reliable FPGA
  - Zero FIT flash FPGA configuration
  - SEU protected memories: eSRAMs, DDR bridges (MSS, MDDR, FDDR), instruction cache, ethernet, CAN and USB buffers, PCIe, MMUART and SPI FIFOs
  - Hard 800 mbps DDR2/3 controllers with SECDED (aka ECC or EDAC) protection
  - Built-in NVM data integrity check
- Lowest power FPGA
  - < 0.5mW in flash-freeze mode
  - 9mW static power during operation

Mainstream Required Features

- 2x fabric performance
- 16x 5Gbps SERDES, PCIe, XAUI / XGXS+ native SERDES
- Integrated DSP processing blocks
- 120K LUT, 5Mbit SRAM, 4Mbit eNVM

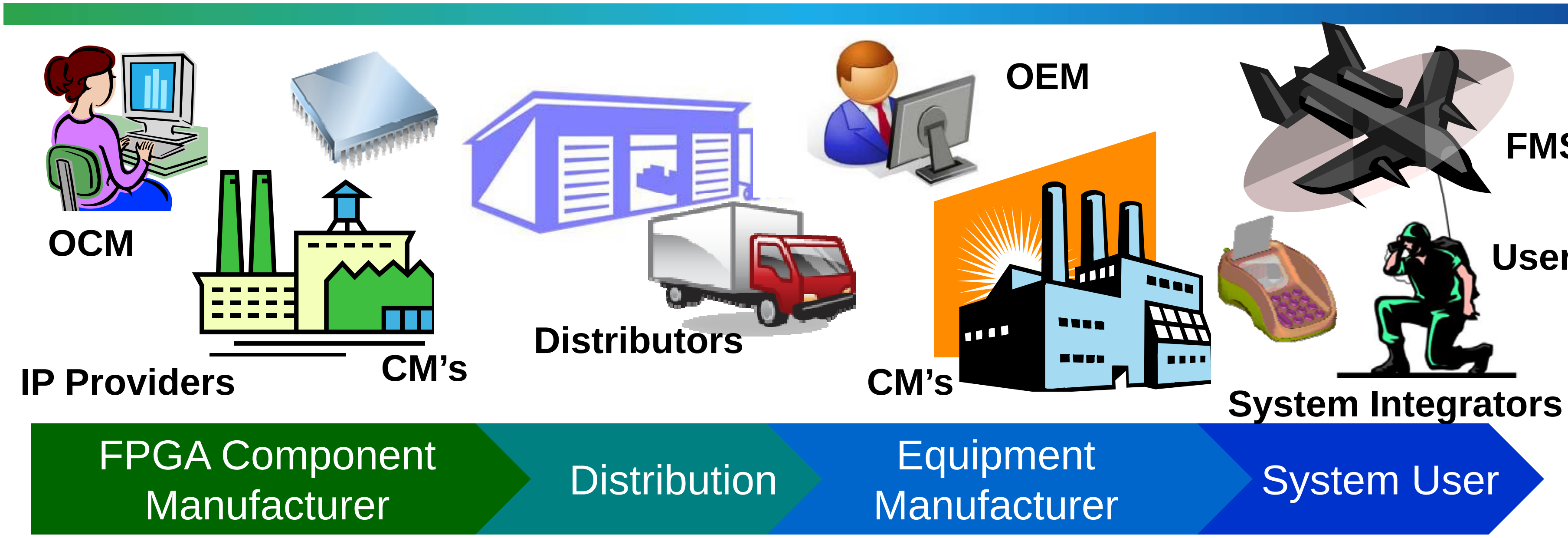
SmartFusion2 SOC FPGA Block Diagram



© 2013 Microsemi Corporation.

Security Matters.

Steps in the FPGA World-Wide Supply Chain



OCM

IP Providers

CM's

Distributors

OEM

CM's

FMS

Users

System Integrators

FPGA Component Manufacturer

Distribution

Equipment Manufacturer

System User

License 3rd-Party IP
Design / Verification
Create Tooling (Masks)
Wafer Fabrication
Wafer-Test / Personalization
Dice / Package
Package-Test / Binning / Marking

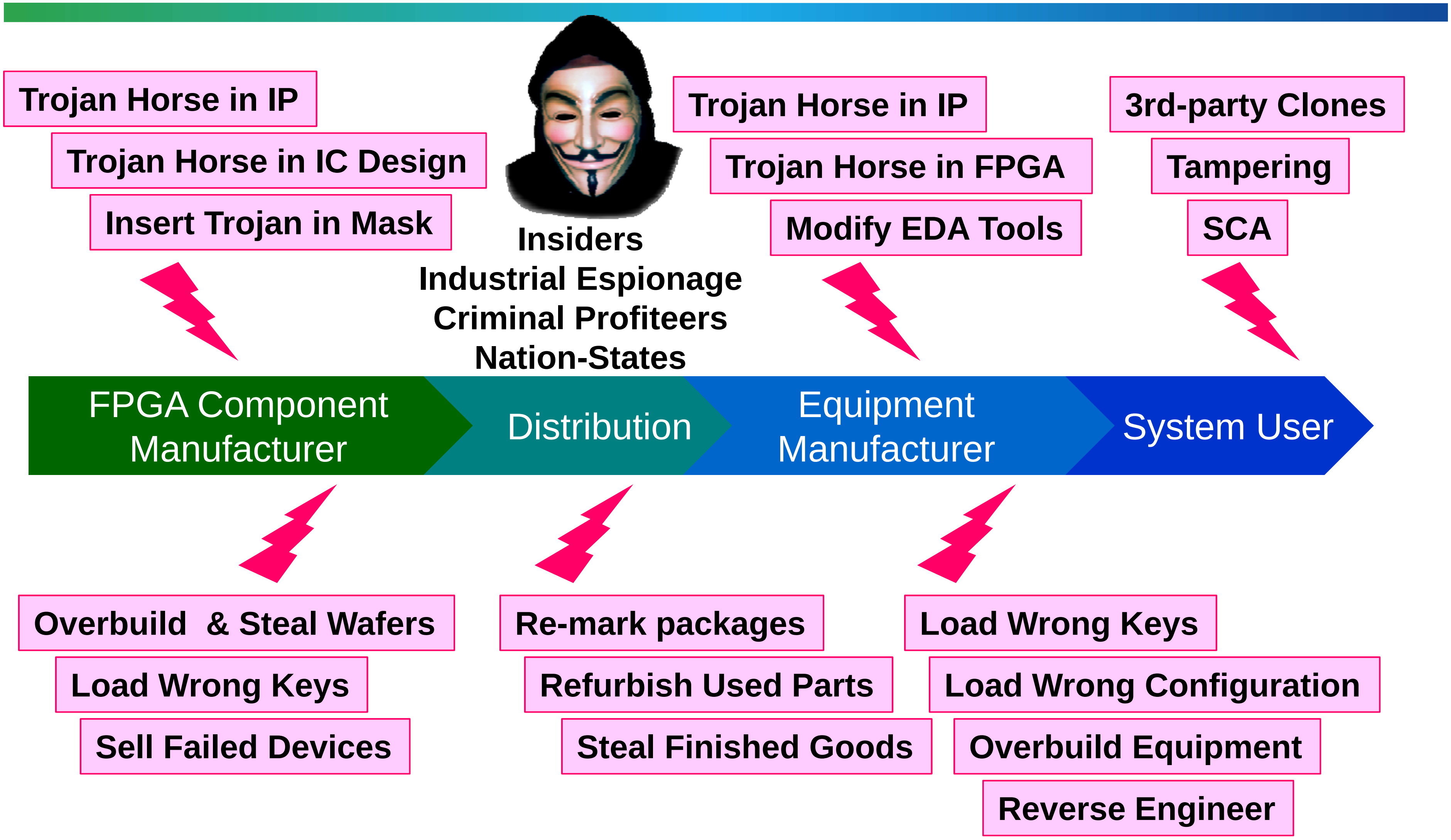
Stock
Ship
Re-Stock

License 3rd-Party IP
Design / Verification
Create Configuration Files
Incoming Inspection
Board Assembly
Program FPGA Configuration
Board-level Test
Equipment Assembly / Test
Personalize / Activate Features

Field Updates

Deploy in Field
Field Updates
Decommission

Threats in the FPGA Supply Chain



Trojan Horse in IP

Trojan Horse in IC Design

Insert Trojan in Mask

Insiders
Industrial Espionage
Criminal Profiteers
Nation-States

Trojan Horse in IP

Trojan Horse in FPGA

Modify EDA Tools

3rd-party Clones

Tampering

SCA

FPGA Component Manufacturer

Distribution

Equipment Manufacturer

System User

Overbuild & Steal Wafers

Load Wrong Keys

Sell Failed Devices

Re-mark packages

Refurbish Used Parts

Steal Finished Goods

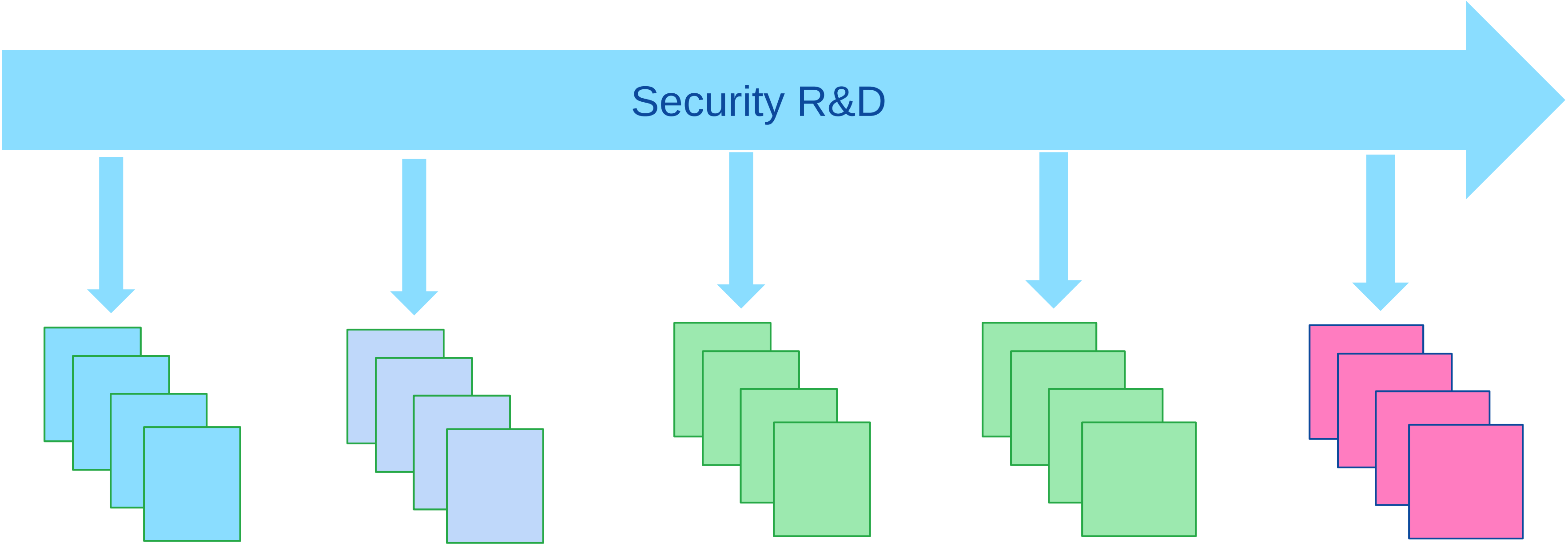
Load Wrong Keys

Load Wrong Configuration

Overbuild Equipment

Reverse Engineer

Security is a Full-Time Job for Microsemi



G2:
Improvements over Anti-Fuse

FlashLock® Passcode

G3:
Major Improvements over G2

Encrypted/Authenticated Bitstream

Security Options

G4
(-005, 010, 025, 050):
Dramatic Improvements over G3

Encrypted Keys

DPA & Active Countermeasures

G4
(-090, -100 & -150)
Additional Improvements

SRAM-PUF

ECC Public Key Algorithms

G5:
Next Generaton Platform

Enhanced Anti-Tamper

Design Security

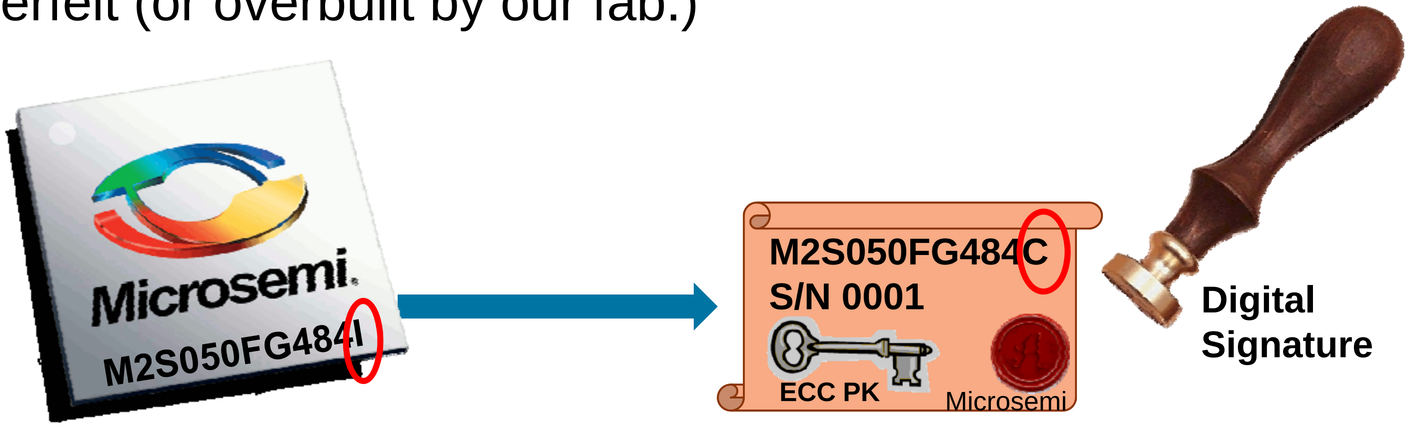
Design Security Features	M2S005 M2S010 M2S025 M2S050	M2GL005 M2GL010 M2GL025 M2GL050	M2S090 M2S100 M2S150	M2GL090 M2GL100 M2GL150
Software Memory Protection Unit (MPU)	x		x	
DPA countermeasures for all design security keys	x	x	x	x
FlashLock™ Passcode Security (256 bit)	x	x	x	x
Flexible security settings using flash lock-bits	x	x	x	x
Encrypted/Authenticated Design Key Loading	x	x	x	x
Symmetric Key Design Security (256 bit)	x	x	x	x
Design Key Verification Protocol	x	x	x	x
Encrypted/Authenticated Configuration Loading	x	x	x	x
Certificate-of-Conformance (C-of-C)	x	x	x	x
Back-Tracking Prevention (a.k.a. versioning)	x	x	x	x
Device Certificate(s) (Identification, Anti-Counterfeiting)	x	x	x	x
Support for Configuration Variations	x	x	x	x
Fabric NVM and eNVM Integrity Tests	x	x	x	x
Information Services (S/N, Cert., USERCODE, etc.)	x	x	x	x
Anti-tamper countermeasures	x	x	x	x
Tamper Detection	x	x	x	x
Tamper Response (incl. Zeroization)	x	x	x	x
ECC Public Key Design Security (384 bit)			x	x
Hardware Intrinsic Design Key (SRAM-PUF)			x	x

Data Security “S” Devices

Additional "S" device Features	M2S005S M2S010S M2S025S M2S050S	M2GL005S M2GL010S M2GL025S M2GL050S	M2S090S M2S100S M2S150S	M2GL090S M2GL100S M2GL150S
CRI Pass-through DPA Patent License	x	x	x	x
Hardware Firewalls protecting access to memories	x	x	x	x
Non-Deterministic Random Bit Generator Service	x	x	x	x
AES-128/256 Service (ECB, OFB, CTR, CBC modes)	x	x	x	x
SHA-256 Service	x	x	x	x
HMAC-SHA-256 Service	x	x	x	x
Key Tree Service	x	x	x	x
PUF Emulation (Pseudo-PUF)	x	x		
PUF Emulation (SRAM-PUF)			x	x
ECC Point-Multiplication Service			x	x
ECC Point-Addition Service			x	x
User SRAM-PUF Enrollment Service			x	x
User SRAM-PUF Activation Code Export Service			x	x
SRAM-PUF Intrinsic Key Gen. & Enrollment Service			x	x
SRAM-PUF Key Import & Enrollment Service			x	x
SRAM-PUF Key Regeneration Service			x	x

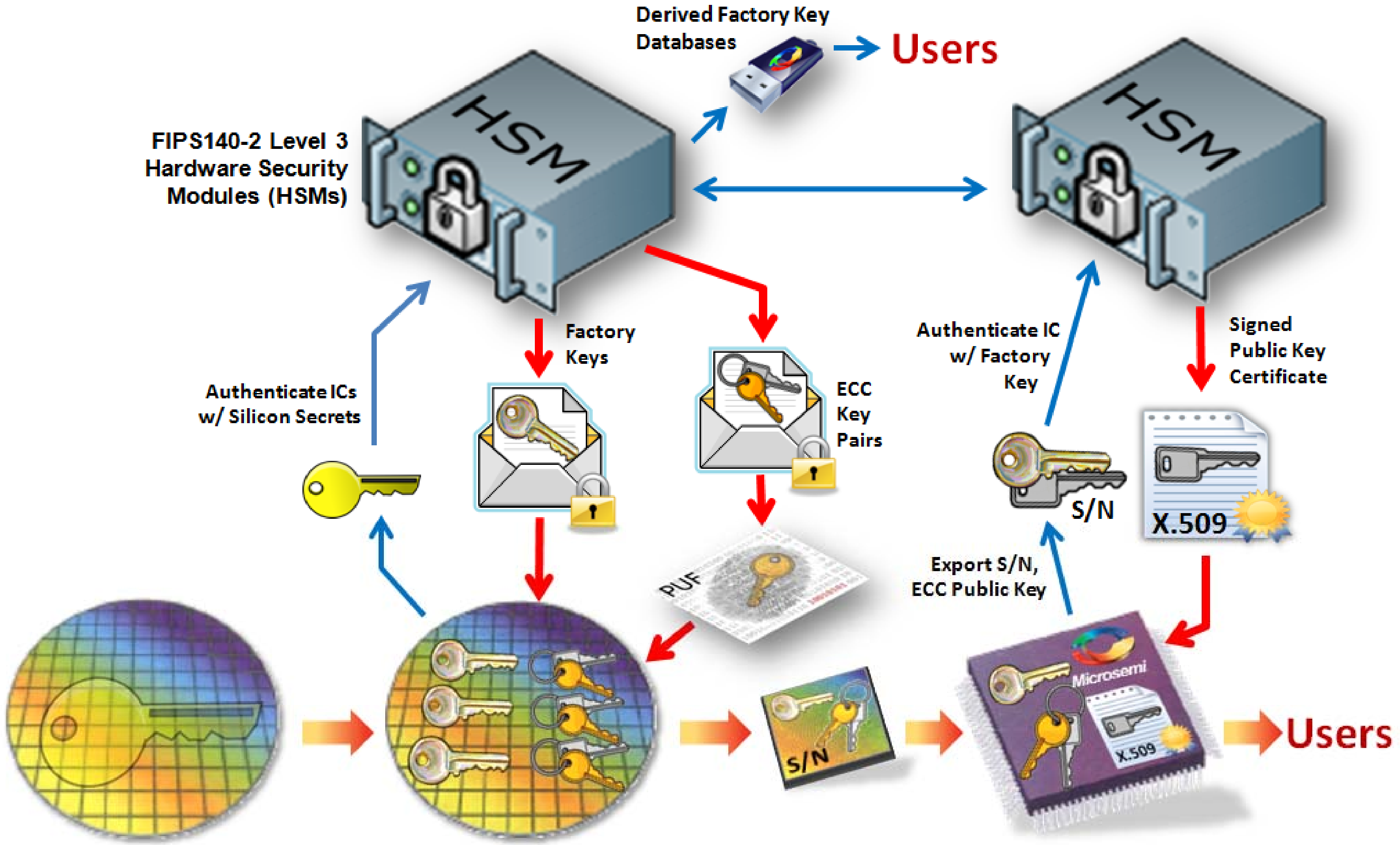
Supply Chain Assurance

- An X.509 conforming certificate digitally signed by Microsemi is stored in each device’s eNVM
- Certifies integrity and authenticity of signed data:
  - Serial number and date code
  - Part Number (with options showing speed grade, screening level, etc.)
  - In larger devices also includes device’s ECC Public Keys
- Key verification protocol binds certificate to secret key(s)
- Cryptographically assures customer that each device is…
  - As marked (speed grade, etc.) – not fraudulently “upgraded”
  - Not counterfeit (or overbuilt by our fab.)



Digital Signature

Device Certificate Chain of Trust


Derived Factory Key Databases
Users
FIPS140-2 Level 3 Hardware Security Modules (HSMs)
HSM
HSM
Authenticate ICs w/ Silicon Secrets
Factory Keys
ECC Key Pairs
Authenticate IC w/ Factory Key
Signed Public Key Certificate
S/N
X.509
PUF
Export S/N, ECC Public Key
S/N
Microsemi
X.509
Users

Fabrication

- Secrets "baked" into Silicon

Wafer Test

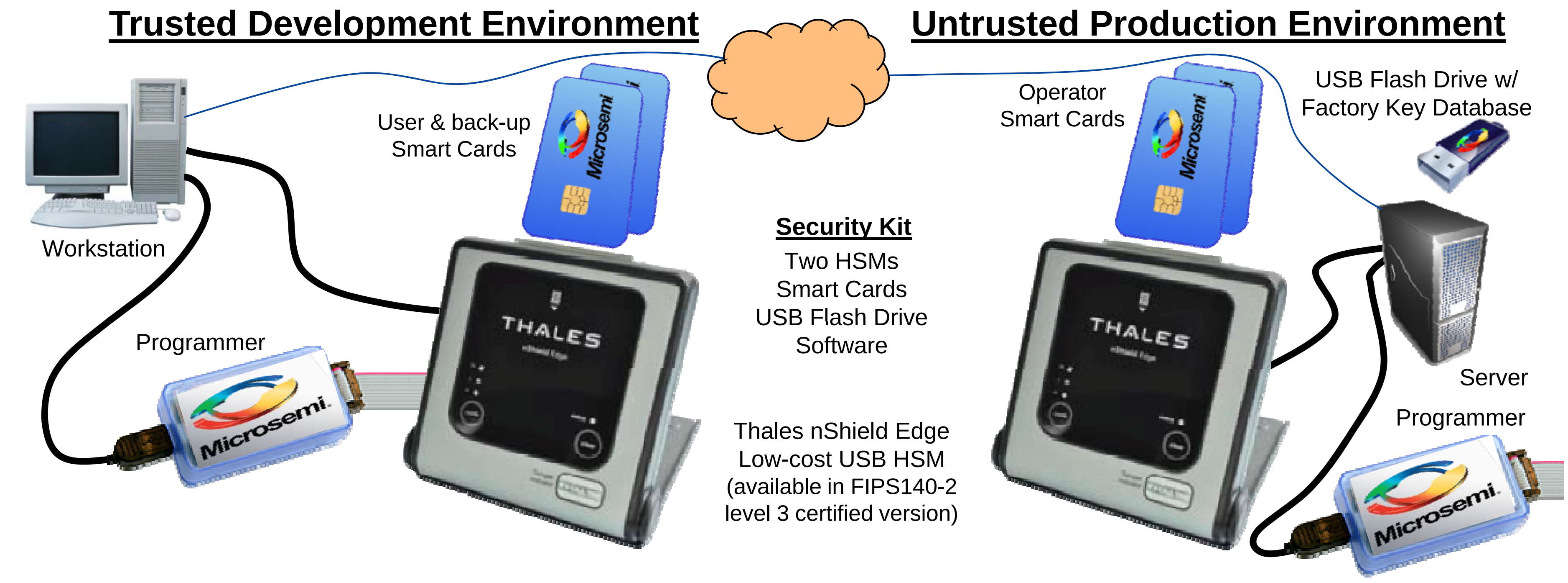
- Authenticate ICs Using Silicon Secrets
- ICs Authenticate Microsemi HSMs, too
- Inject Symmetric Factory Keys & S/Ns
- Inject ECC Key Pairs & Enroll ECC Private Keys with Physically Uncloneable Functions (PUFs)

Dice

Package Test

- Bin IC (e.g., by speed grade)
- Authenticate IC Using Factory Key
- Export ECC Public Key & S/N; Authenticate Key
- Sign & Inject Public Key Certificate

Low-cost secure production programming


Trusted Development Environment
Untrusted Production Environment
Workstation
User & back-up Smart Cards
Programmer
Security Kit
Two HSMs
Smart Cards
USB Flash Drive
Software
Thales nShield Edge
Low-cost USB HSM
(available in FIPS140-2 level 3 certified version)
Operator Smart Cards
USB Flash Drive w/ Factory Key Database
Server
Programmer

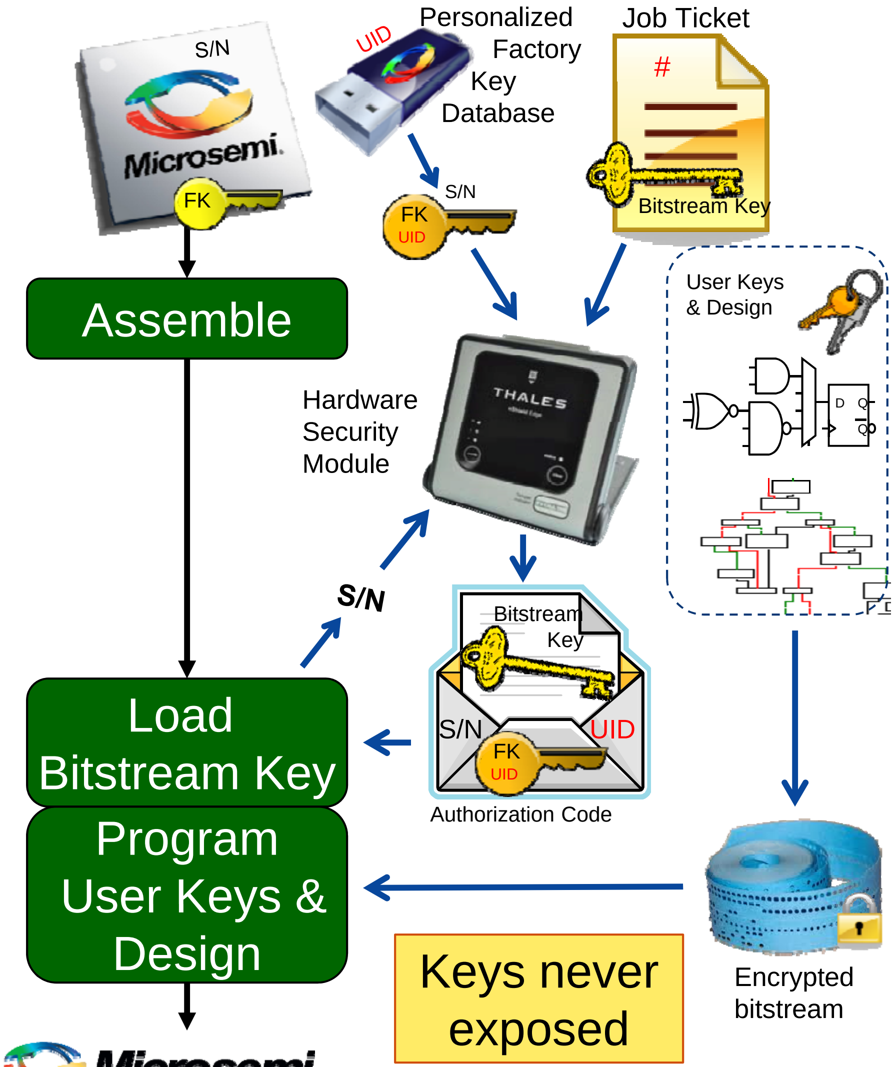
- HSM manages user bitstream keys
- Generates job tickets
- Workstation runs Libero® IDE
  - Synthesis, place-and-route
  - Bitstream generation and encryption

- HSM generates authorization codes
- Decrypts factory key database, or
- Performs Diffie-Hellman key establishment
- Decrypts job ticket
- Keeps track of device count on jobs

SmartFusion®2 User Key Injection
Cloning/Overbuilding Prevention

Microsemi SmartFusion®2

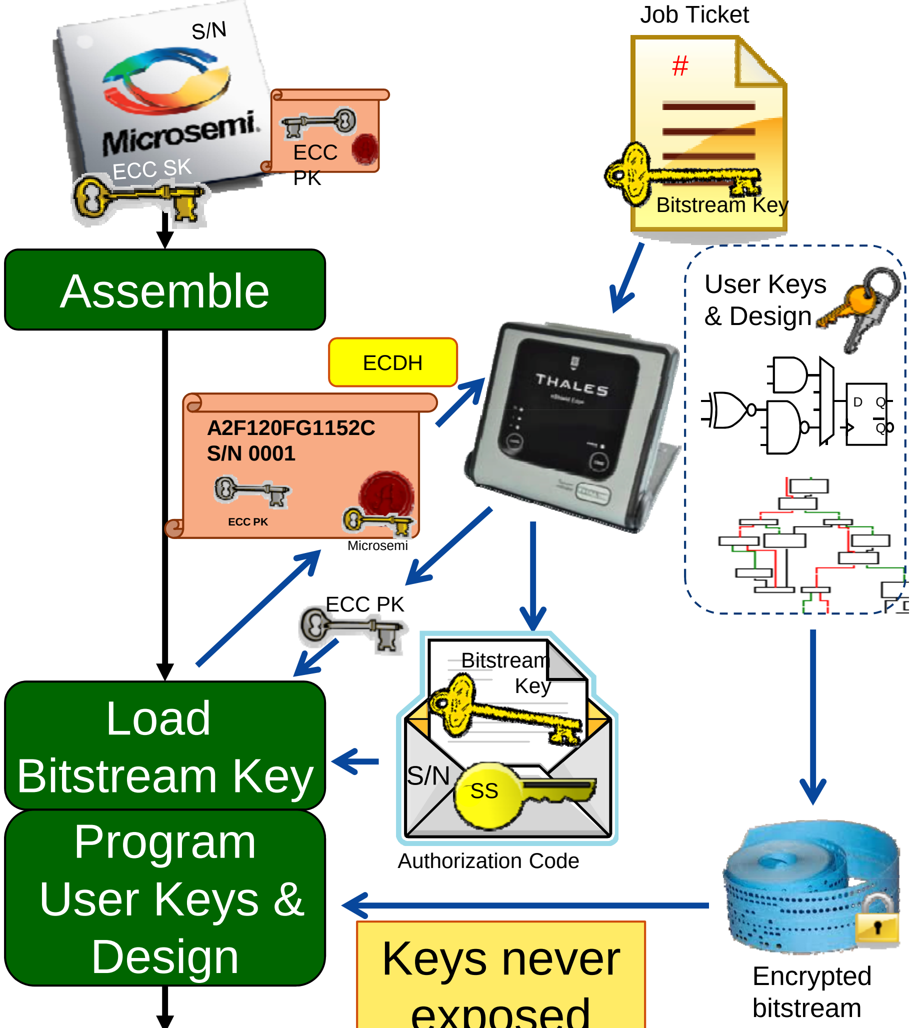
(using symmetric key method)



Keys never exposed

Microsemi SmartFusion2 (-080 & -120 only)

(using optional ECC pubic-key method)



Keys never exposed

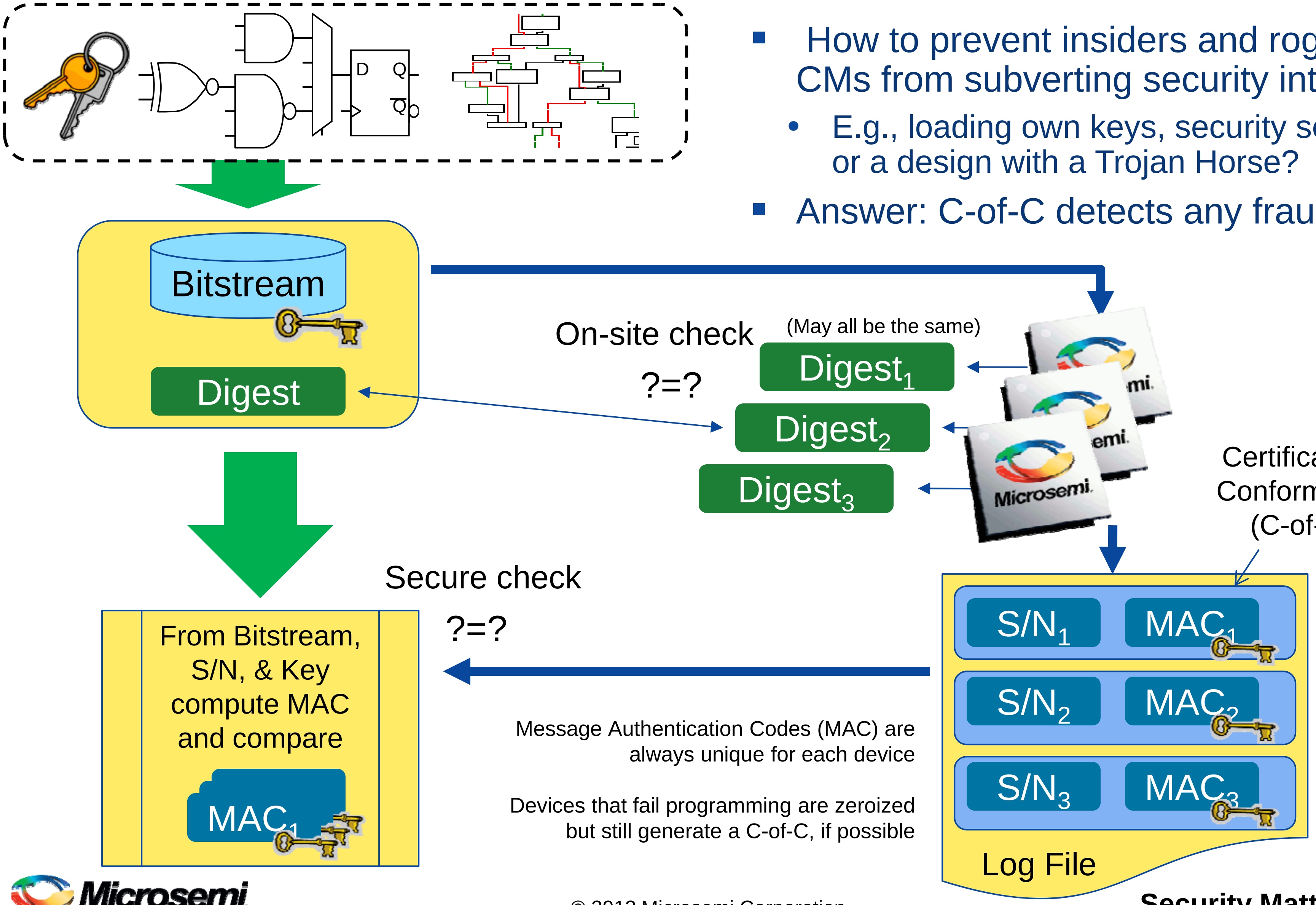
Key Management Comparison

	#1 SRAM FPGA	#2 3G Flash FPGA	#3 Symmetric Key Method	#4 Public-Key Method
Requires Trusted Programming Facility	yes	yes	no	no
Requires Trusted Assembly Facility	yes	no	no	no
Requires Factory Key Database	no	no	yes	no
Requires on-line protocol	no	no	no*	no*
Bitstream key stored statically in device	yes	yes	no	no
Keys Always Protected (by HSM or encryption)	no	no	yes	yes

* Does require reading S/N and/or X.509 certificate, but this can be done offline

Digital Certificate-of-Conformance (C-of-C)

- How to prevent insiders and rogue CMs from subverting security intent?
  - E.g., loading own keys, security settings, or a design with a Trojan Horse?
- Answer: C-of-C detects any fraud



Bitstream

Digest

On-site check

?=?

(May all be the same)

Digest_1

Digest_2

Digest_3

Certificate of Conformance (C-of-C)

Secure check

?=?

From Bitstream, S/N, & Key compute MAC and compare

MAC_1

S/N_1	MAC_1
S/N_2	MAC_2
S/N_3	MAC_3

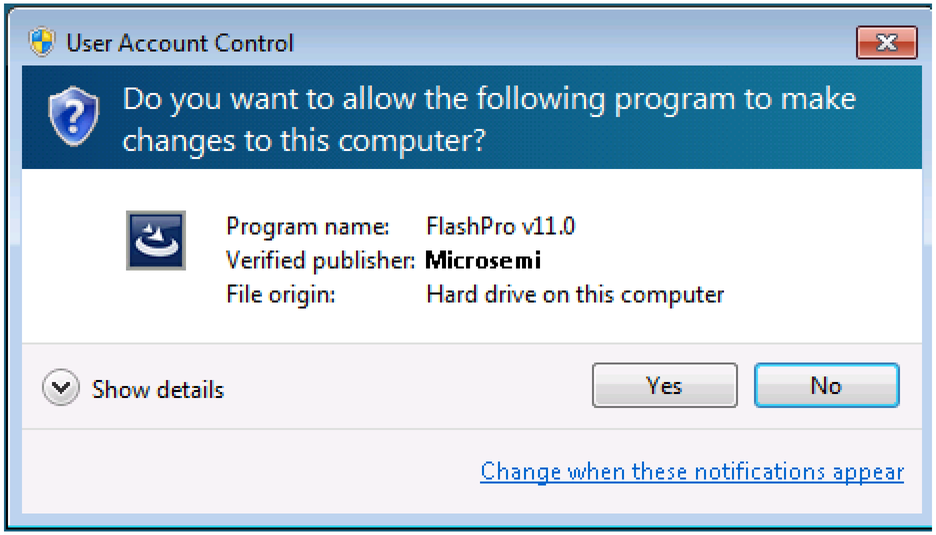
Log File

Message Authentication Codes (MAC) are always unique for each device

Devices that fail programming are zeroized but still generate a C-of-C, if possible

Microsemi SoC Software Code Signing

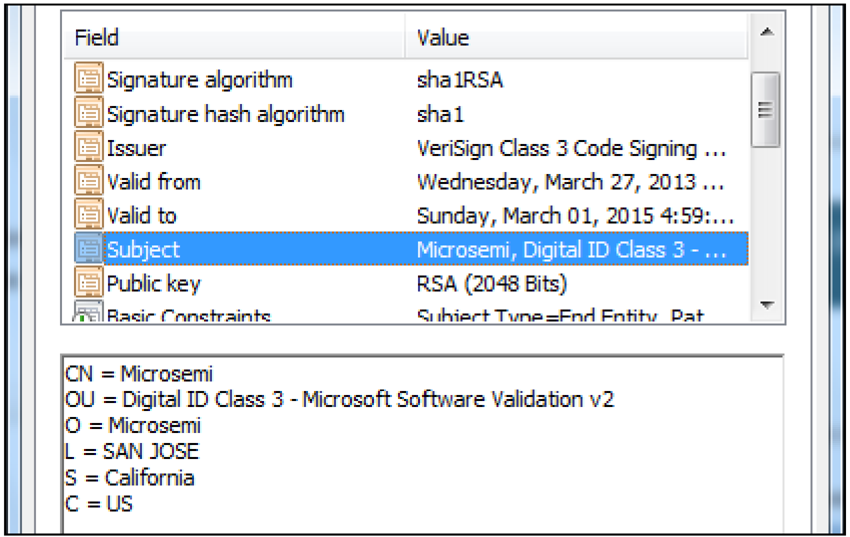
- Microsemi software tools are now digitally signed
- The VeriSign root key should be inherently recognized and trusted on almost all computers



User Account Control

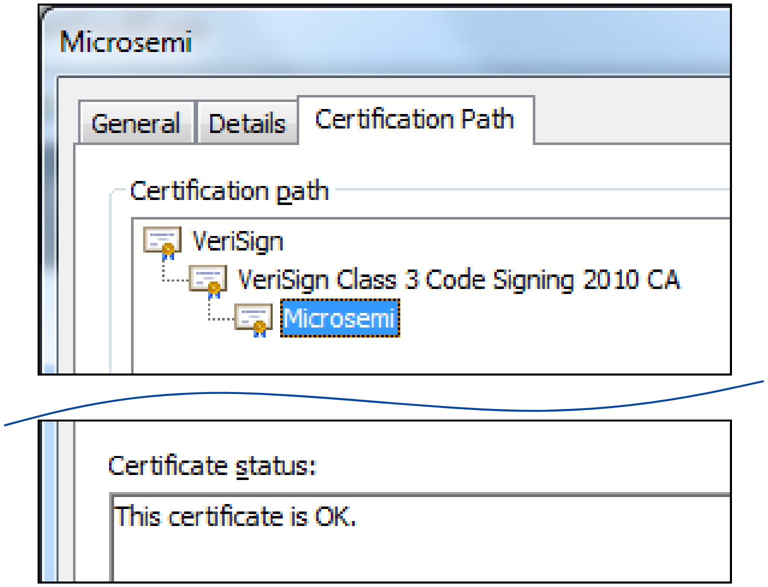
Do you want to allow the following program to make changes to this computer?

Program name: FlashPro v11.0
Verified publisher: **Microsemi**
File origin: Hard drive on this computer



Field	Value
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	VeriSign Class 3 Code Signing ...
Valid from	Wednesday, March 27, 2013 ...
Valid to	Sunday, March 01, 2015 4:59:...
Subject	Microsemi, Digital ID Class 3 - ...
Public key	RSA (2048 Bits)
Basic Constraints	Subject Type=End Entity, Pat

CN = Microsemi
OU = Digital ID Class 3 - Microsoft Software Validation v2
O = Microsemi
L = SAN JOSE
S = California
C = US



Microsemi

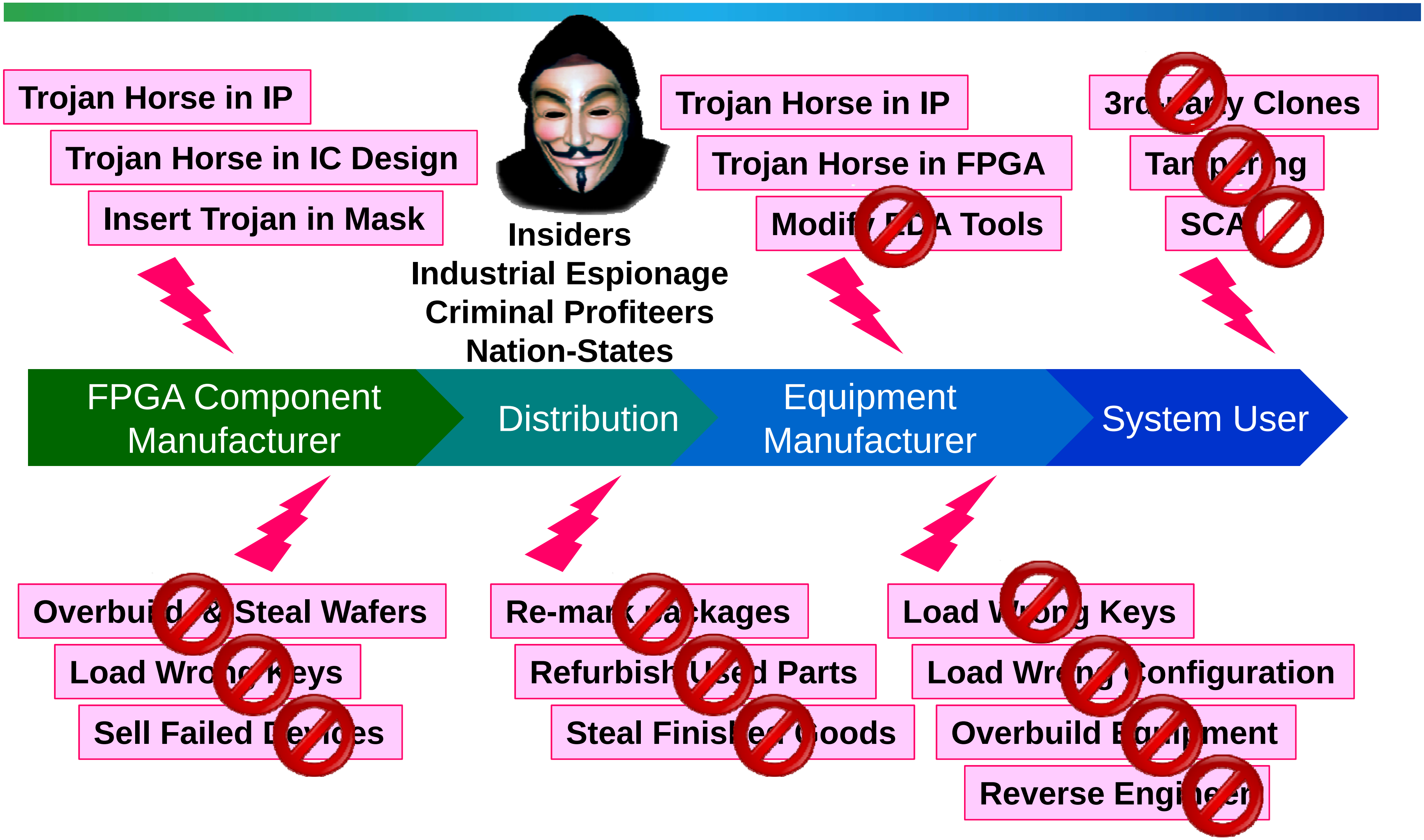
Certification path

- VeriSign
  - VeriSign Class 3 Code Signing 2010 CA
    - Microsemi

Certificate status:

This certificate is OK.

Threats in the FPGA Supply Chain



Trojan Horse in IP

Trojan Horse in IC Design

Insert Trojan in Mask

Insiders
Industrial Espionage
Criminal Profiteers
Nation-States

Trojan Horse in IP

Trojan Horse in FPGA

Modify EDA Tools

3rd Party Clones

Tampering

SCA

FPGA Component Manufacturer → Distribution → Equipment Manufacturer → System User

Overbuild & Steal Wafers

Load Wrong Keys

Sell Failed Devices

Re-mark Packages

Refurbish Used Parts

Steal Finished Goods

Load Wrong Keys

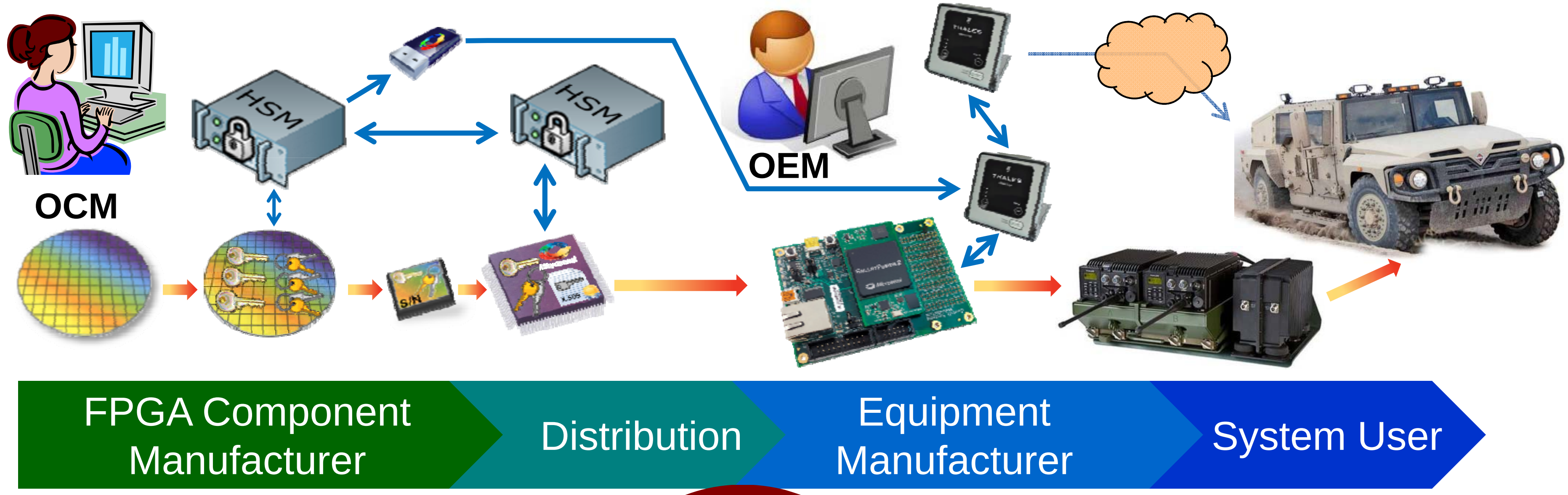
Load Wrong Configuration

Overbuild Equipment

Reverse Engineer

© 2013 Microsemi Corporation.

The Secured Supply Chain



FPGA Component Manufacturer

Distribution

Equipment Manufacturer

System User

The Supply Chain Managed by the OCM & OEM

And not by the Adversaries

Insiders
Industrial Espionage
Criminal Profiteers
Nation-States

Thank You for your Attention!

Questions?

G. Richard Newell
Senior Principal Product Architect
Microsemi Corporation, SoC Group
richard.newell@microsemi.com
+1 (408) 643-6146

Microsemi