Power Matters.™

Securing the IoT with Low Power, Small Form Factor Programmable Devices

Tim Morin
Director Product Line Marketing
Microsemi SoC Product Group
tim.morin@microsemi.com

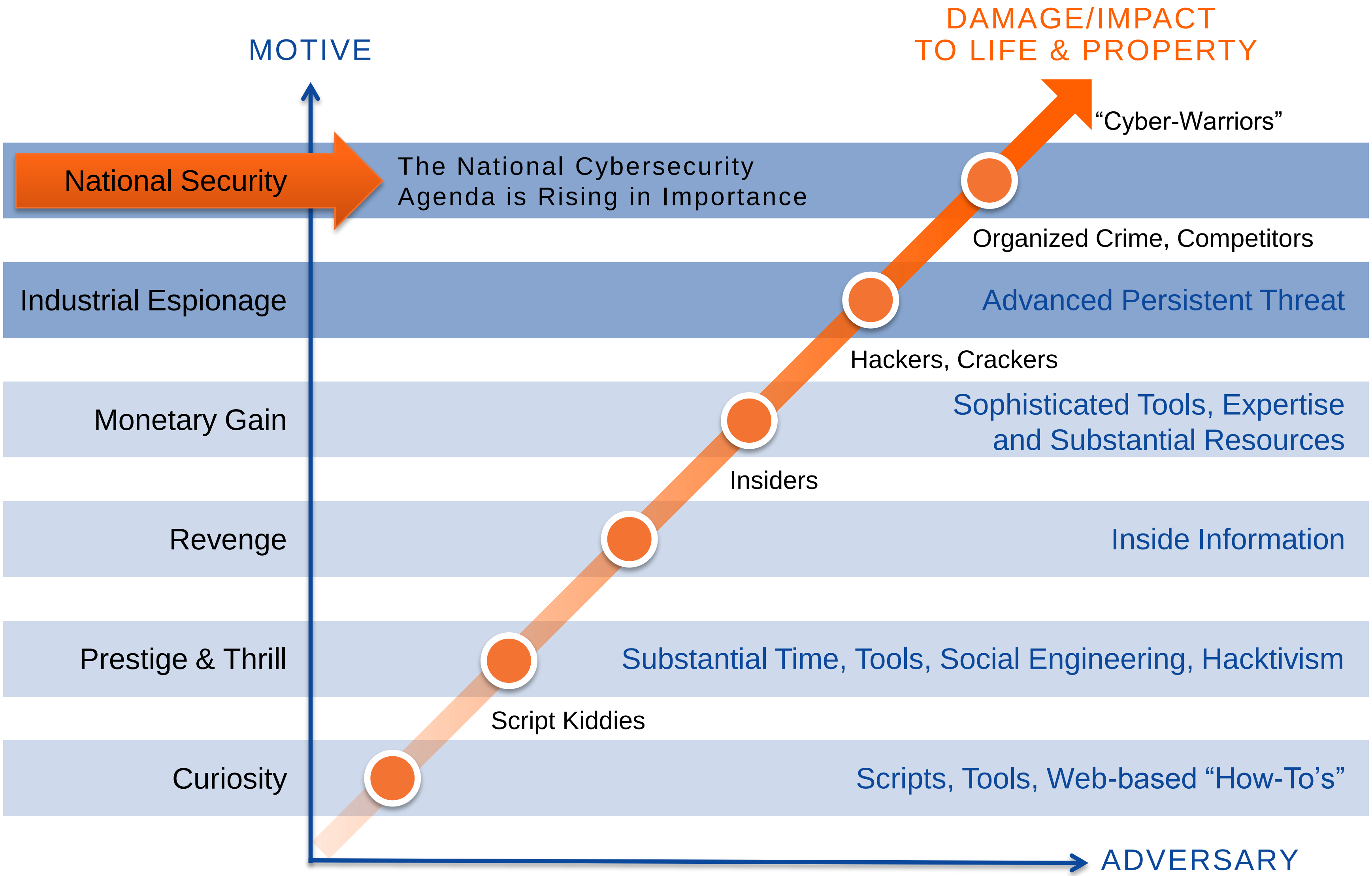
12/9/2014

Agenda

- Why the IoT needs to be secure
- Secure Supply Chain Management and Secure Devices
- Public Key Infrastructure and its pitfalls
- The Microsemi / Escrypt reference design
- Low Power, Small Form Factor, Secure SoC FPGA’s

Adversaries

Cyber Threats/Motives



MOTIVE

DAMAGE/IMPACT
TO LIFE & PROPERTY

National Security

The National Cybersecurity Agenda is Rising in Importance

"Cyber-Warriors"

Organized Crime, Competitors

Industrial Espionage

Advanced Persistent Threat

Hackers, Crackers

Monetary Gain

Sophisticated Tools, Expertise and Substantial Resources

Insiders

Revenge

Inside Information

Prestige & Thrill

Substantial Time, Tools, Social Engineering, Hacktivism

Script Kiddies

Curiosity

Scripts, Tools, Web-based "How-To's"

ADVERSARY

HW Eavesdropping Attack

Smart meter

KrebsonSecurity

In-depth security news and investigation

http://tinyurl.com/boqz8hz

FBI: Smart Meter Hacks Likely to Spread

A series of hacks perpetrated against so-called “smart meter” installations over the past several years may have cost a single U.S. electric utility hundreds of millions of dollars annually, the **FBI** said in a cyber intelligence bulletin obtained by KrebsOnSecurity.

The hacks described by the FBI do not work remotely, and require miscreants to have physical access to the devices. They succeed because many smart meter devices deployed today do little to obfuscate the credentials needed to change their settings, said according to Tom Liston and Don Weber, analysts with InGuardians Inc., a security consultancy based in Washington, D.C.

Liston and Weber have developed a prototype of a tool and software program that lets anyone access the memory of a vulnerable smart meter device and intercept the credentials used to administer it. Weber said the toolkit relies in part on a device called an optical probe, which can be made for about $150 in parts, or purchased off the Internet for roughly $300.

“This is a well-known and common issue, one that we’ve warning people about for three years now, where some of these smart meter devices implement unencrypted memory,” Weber said. *“If you know where and how to look for it, you can gather the security code from the device, because it passes them unencrypted from one component of the device to another.”*

Persistent Access

Routers and Switches

http://www.wired.com/2013/09/nsa-router-hacking/

WIRED **NSA Laughs at PCs, Prefers Hacking Routers and Switches** By Kim Zetter 09.04.13

According to the *Post*, the government … preferred hacking routers to individual PCs because it gave agencies access to data from entire networks of computers instead of just individual machines.

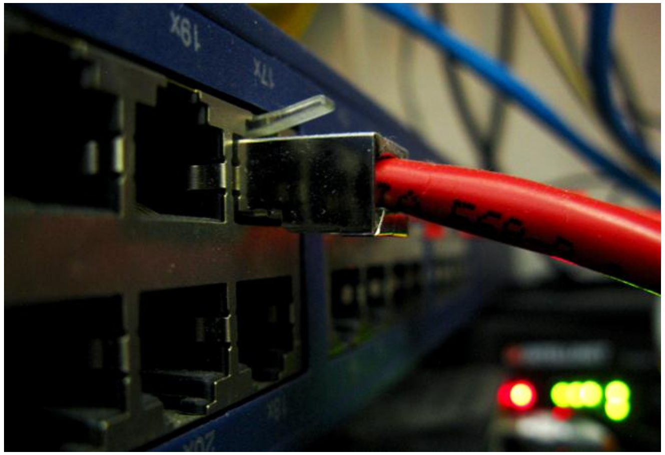


Photo: Santiago Cabezas/Flickr

The NSA’s focus on routers highlights an often-overlooked attack vector with huge advantages for the intruder, says Marc Maiffret, chief technology officer at security firm Beyond Trust. Hacking routers is an ideal way for an intelligence or military agency to maintain a persistent hold on network traffic

According to the budget document, the CIA’s Tailored Access Programs and NSA’s software engineers possess “templates” for breaking into common brands and models of routers, switches and firewalls.

COMPUTERWORLD

http://blogs.computerworld.com/cybercrime-and-hacking/23347/17-exploits-nsa-uses-hack-pcs-routers-and-servers-surveillance

The ANT catalog [circa 2008] specifies persistent backdoor router exploits that target Huawei, Juniper J, Juniper M, and Juniper T series

Energetic Bear / Crouching Yeti / Dragon Fly

- Cyber Espionage – Data gathering
  - Industrial/Machinery (main area of interest)
  - Manufacturing
  - Pharmaceutical
  - Construction
  - Education
  - IT
- Targeted ~2800 victims

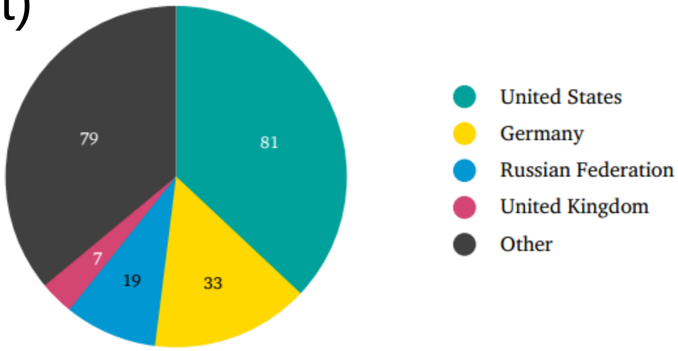
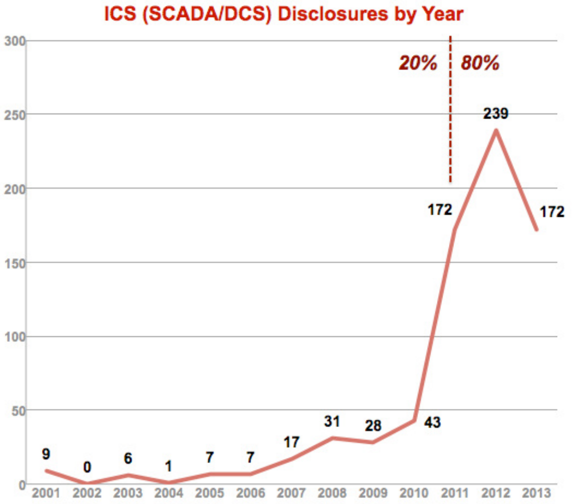


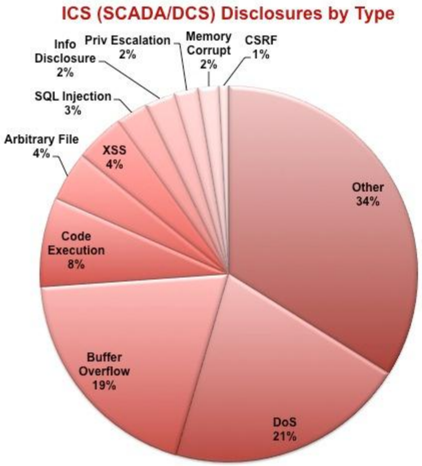
Figure 5. C&C country distribution

Advanced Persistent Threat Campaign

Specifically targeting
SCADA and Industrial Control Systems

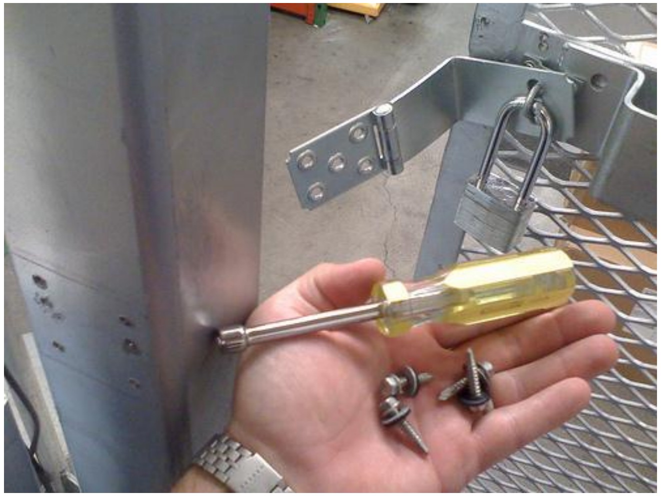
Active and ongoing since 2010

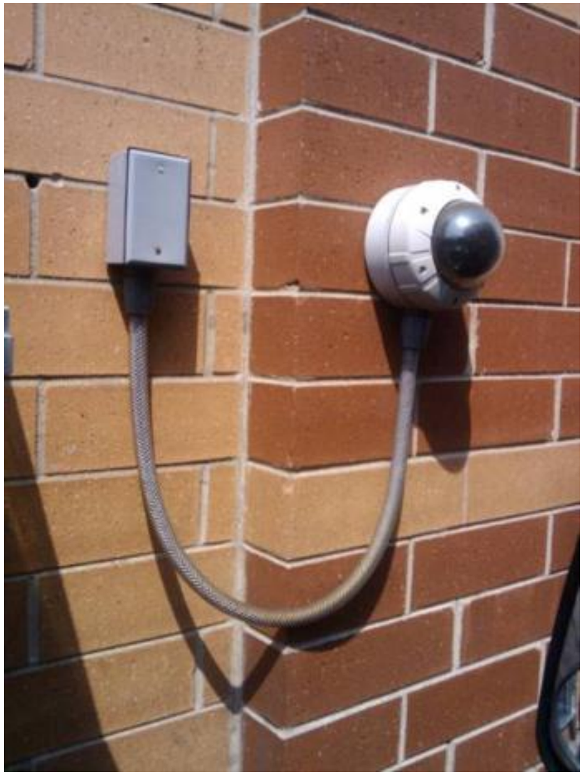


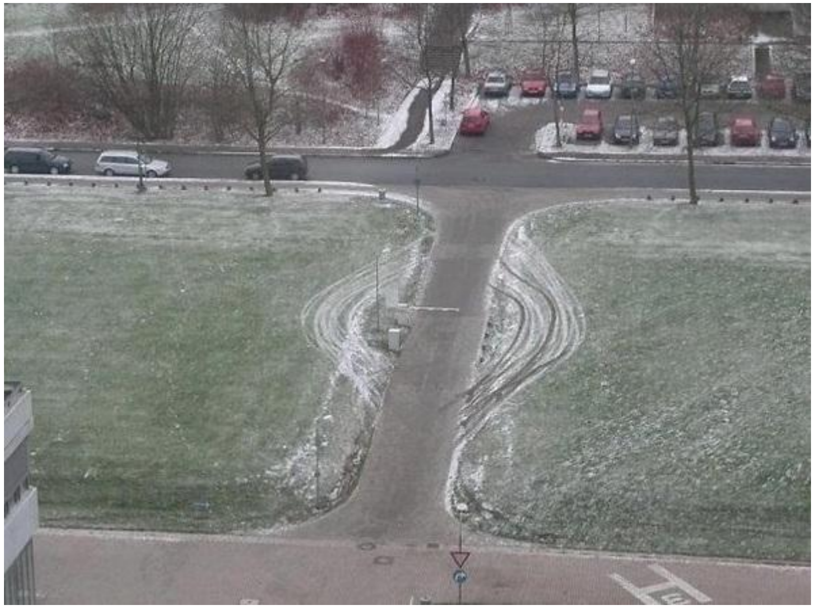


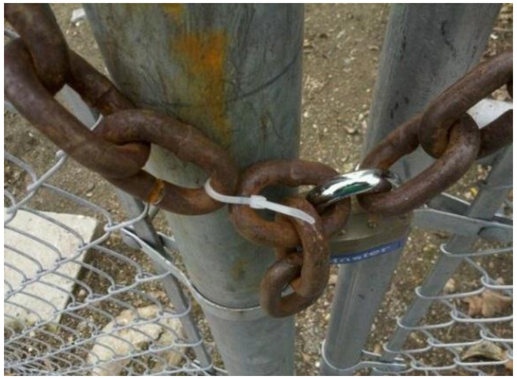
Source : scadahacker.com

Bad Physical Security Examples

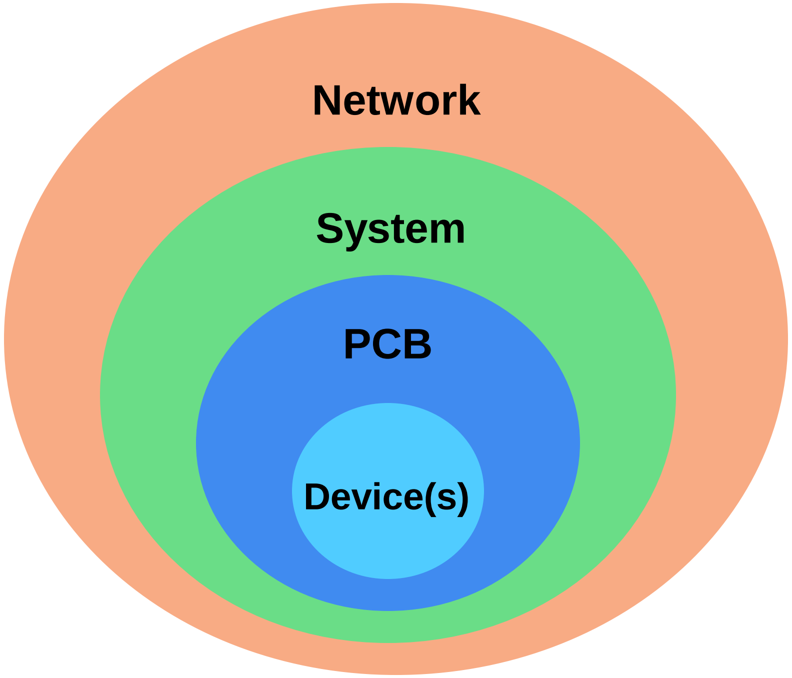






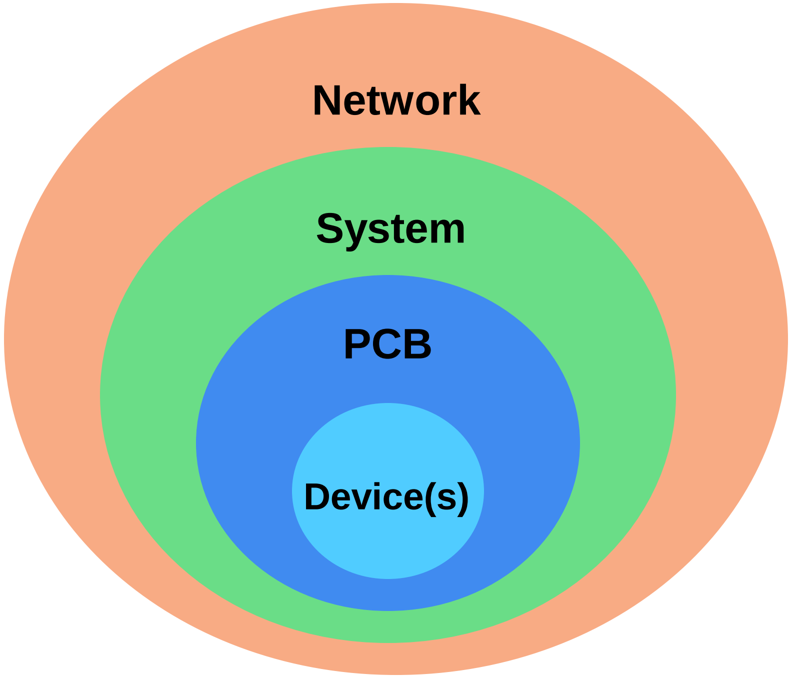


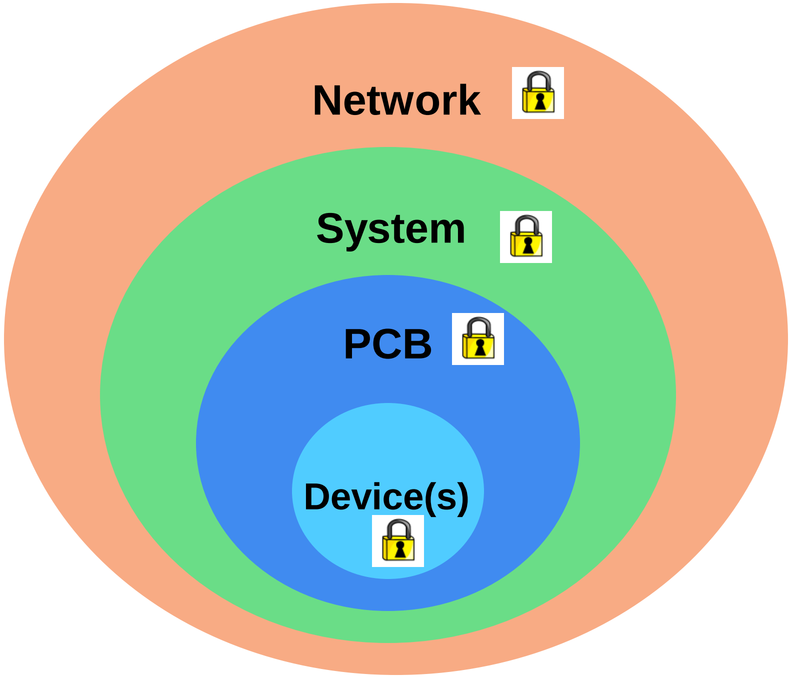
The IoT is a collection of Electronic Networks



- Layers of electronic systems
- Starting with devices on a Printed Circuit Board (PCB)
- With Multiple PCBs creating a system
- With networks between systems
- All designed to make our lives better

The IoT is a collection of Electronic Networks





What is needed is end to end layered security

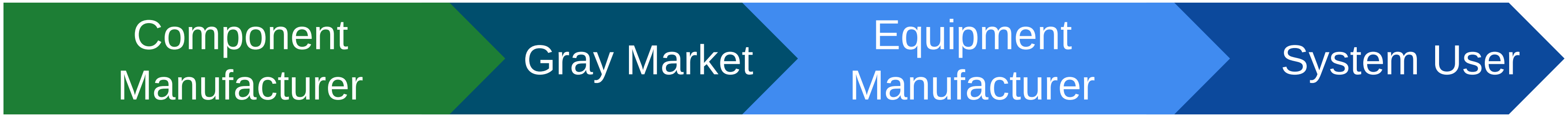
Beginning at the Device

Secure Supply Chain Management and Secure Devices

Secure Hardware

Potential Threats in Your Supply Chain

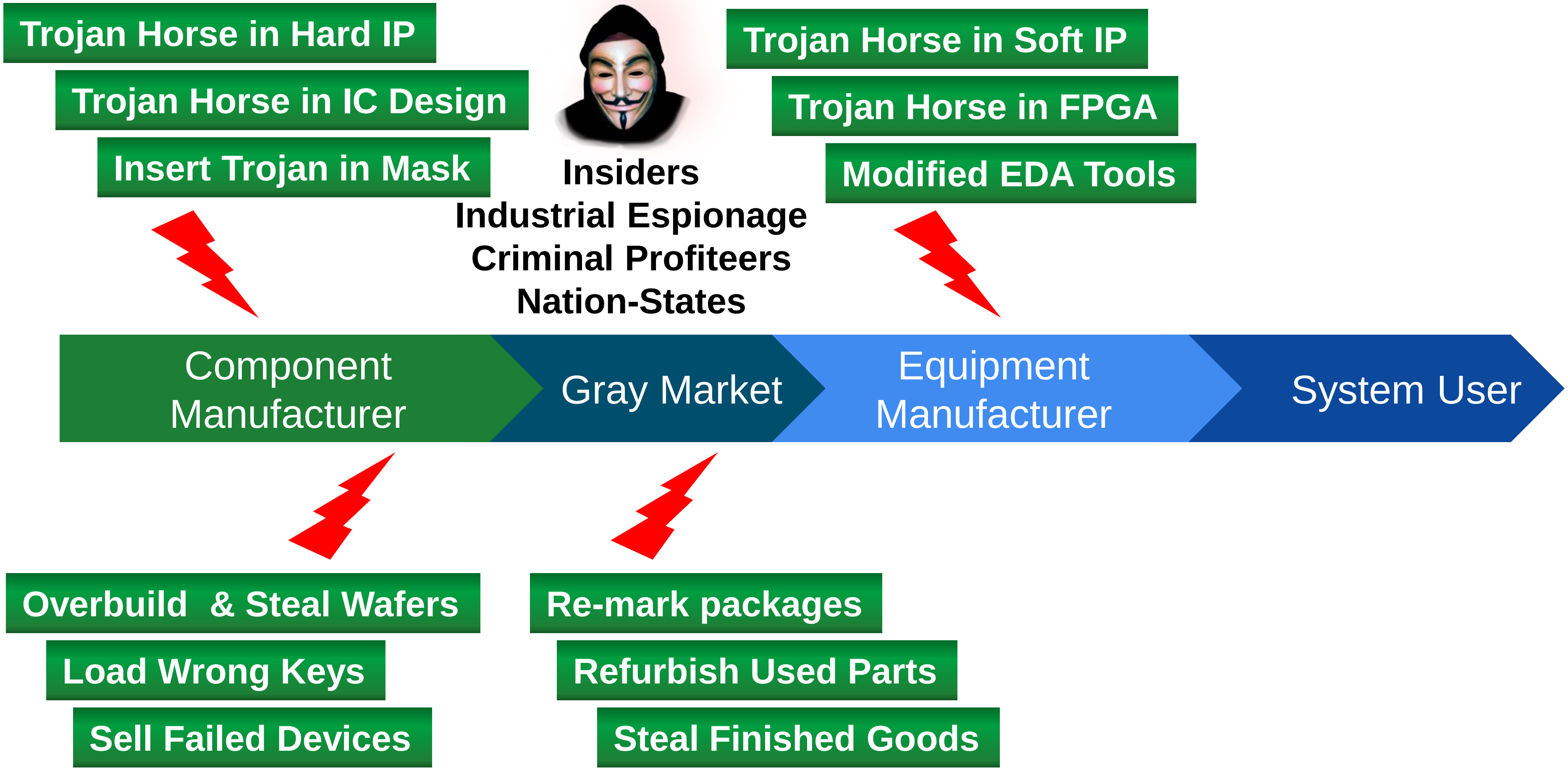
Insiders
Industrial Espionage
Criminal Profiteers
Nation-States



Component Manufacturer → Gray Market → Equipment Manufacturer → System User

Secure Hardware

Potential Threats in Your Supply Chain



Trojan Horse in Hard IP

Trojan Horse in IC Design

Insert Trojan in Mask

Trojan Horse in Soft IP

Trojan Horse in FPGA

Modified EDA Tools

Insiders
Industrial Espionage
Criminal Profiteers
Nation-States

Component Manufacturer → Gray Market → Equipment Manufacturer → System User

Overbuild & Steal Wafers

Load Wrong Keys

Sell Failed Devices

Re-mark packages

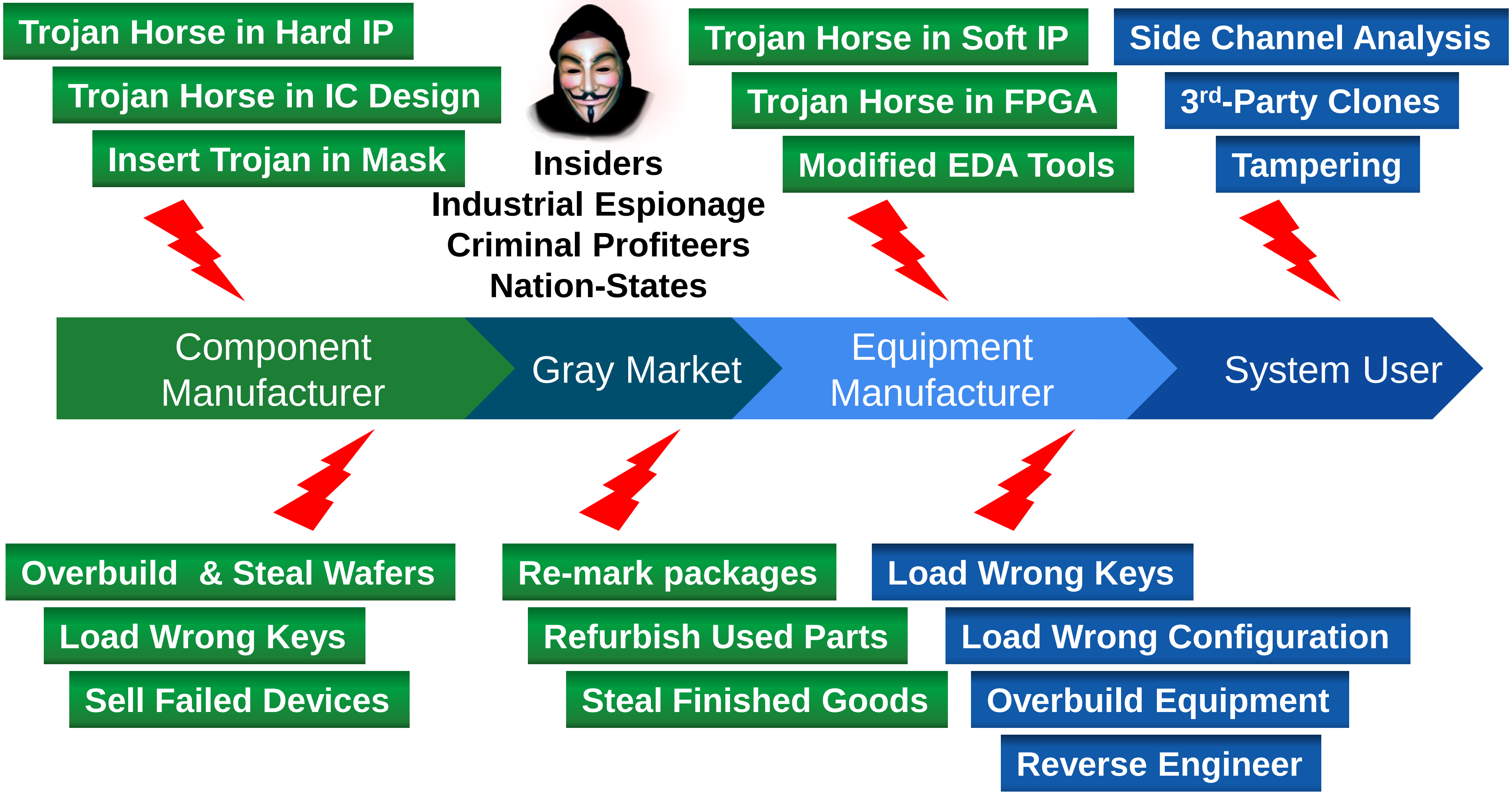
Refurbish Used Parts

Steal Finished Goods

Secure Hardware and Trust

Secure Hardware

Potential Threats in Your Supply Chain



Trojan Horse in Hard IP

Trojan Horse in IC Design

Insert Trojan in Mask

Insiders
Industrial Espionage
Criminal Profiteers
Nation-States

Trojan Horse in Soft IP

Trojan Horse in FPGA

Modified EDA Tools

Side Channel Analysis

3rd-Party Clones

Tampering

Component Manufacturer → Gray Market → 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

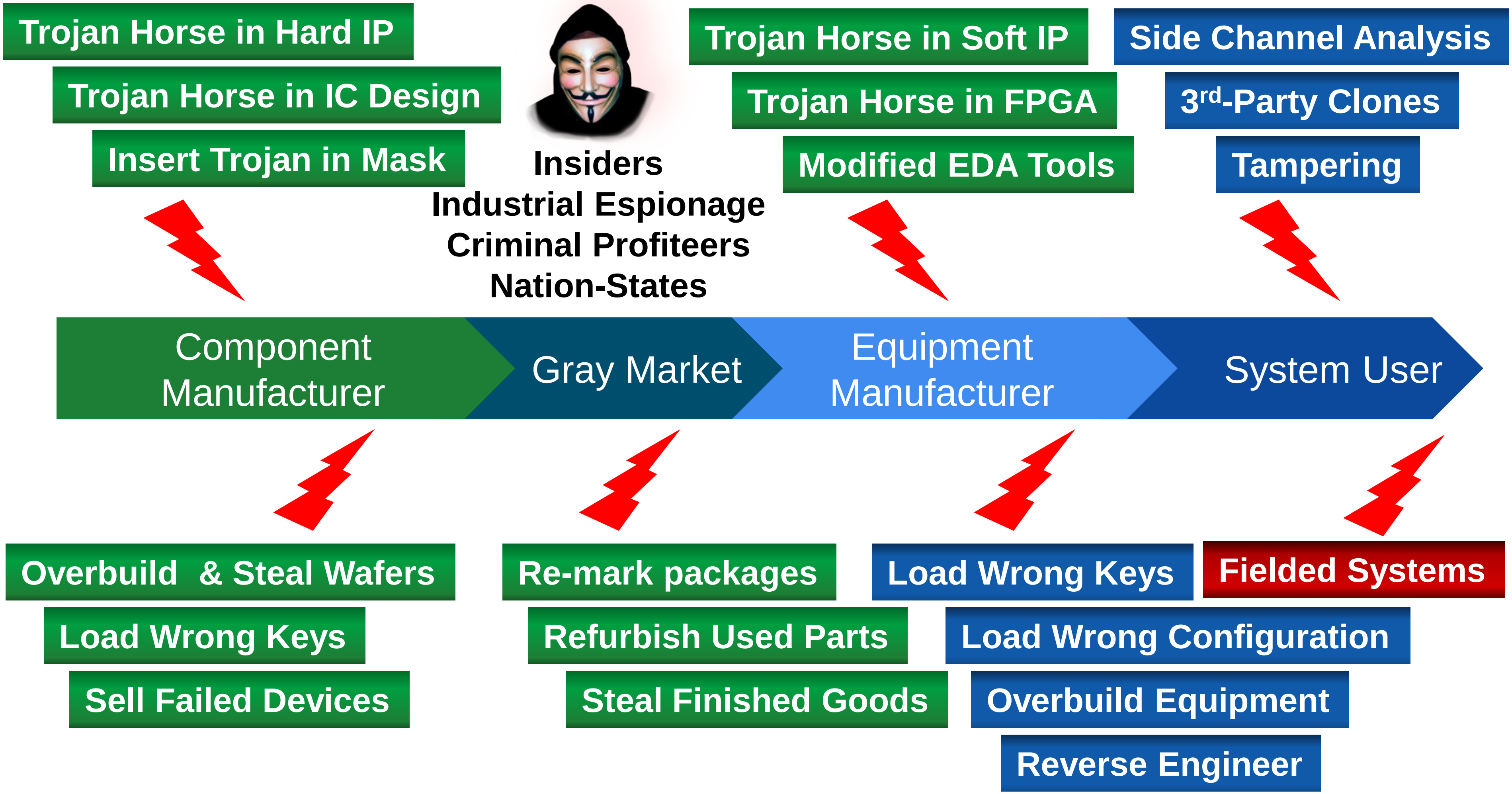
Overbuild Equipment

Reverse Engineer

Secure Hardware and Trust	Design Security & Anti-Tamper

Secure Hardware

Potential Threats in Your Supply Chain



Trojan Horse in Hard IP

Trojan Horse in IC Design

Insert Trojan in Mask

Insiders
Industrial Espionage
Criminal Profiteers
Nation-States

Trojan Horse in Soft IP

Trojan Horse in FPGA

Modified EDA Tools

Side Channel Analysis

3rd-Party Clones

Tampering

Component Manufacturer → Gray Market → 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

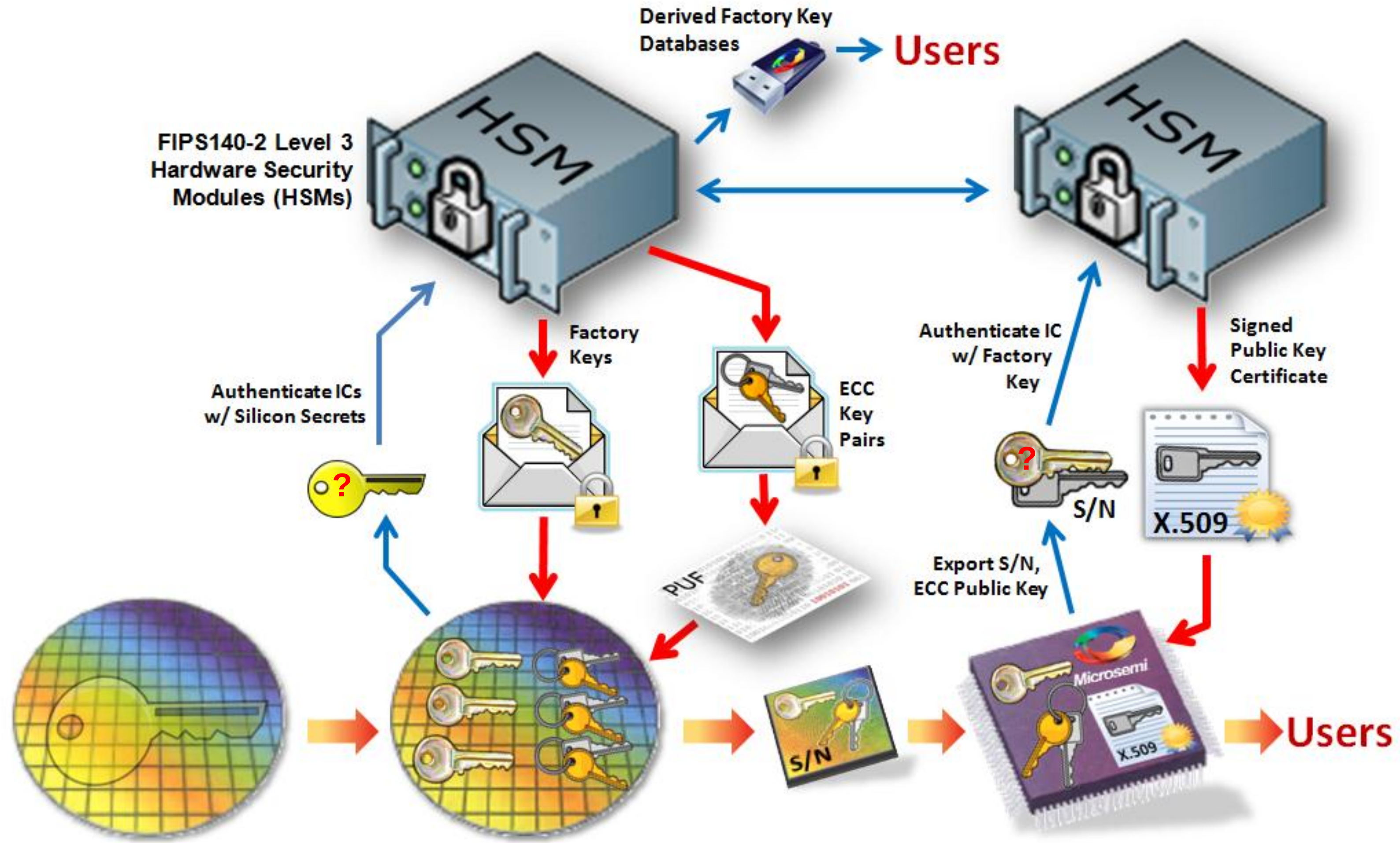
Reverse Engineer

Fielded Systems

Secure Hardware and Trust	Design Security & Anti-Tamper	Data Security & Information Assurance

If your Supply Chain is not secure how can your systems be?

SmartFusion®2 Device Certificate Chain of Trust



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)

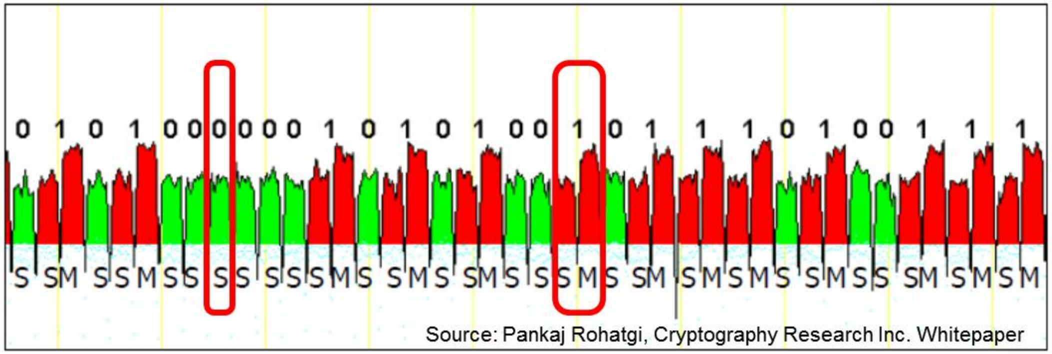
Dice

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

Is your IP / System Protected?

Simple and Differential Power Analysis (SPA/DPA) can extract secret keys by measuring power consumption during cryptographic operations like bitstream loading

Power Trace: RSA “Secret” Exponentiation Operation



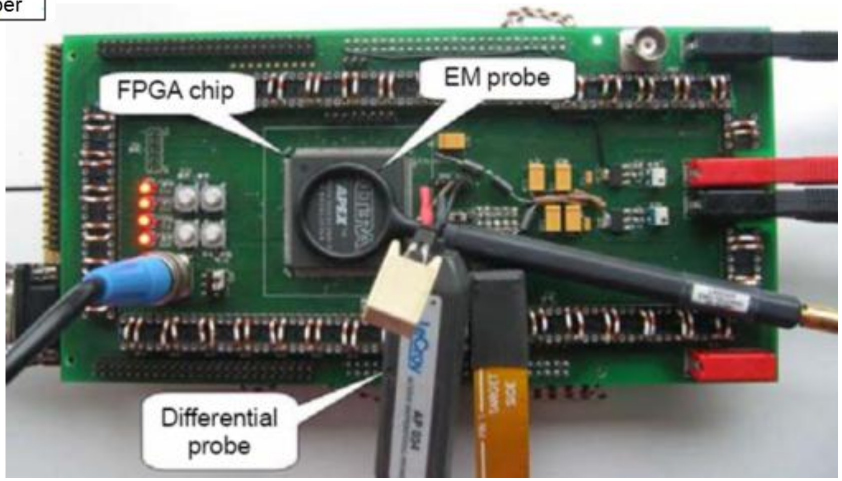
Source: Pankaj Rohatgi, Cryptography Research Inc. Whitepaper

Secret Exponent {0 or 1}

S = Square
M = Multiply

If Secret Exponent = 0
Square
Else
Square + Multiply

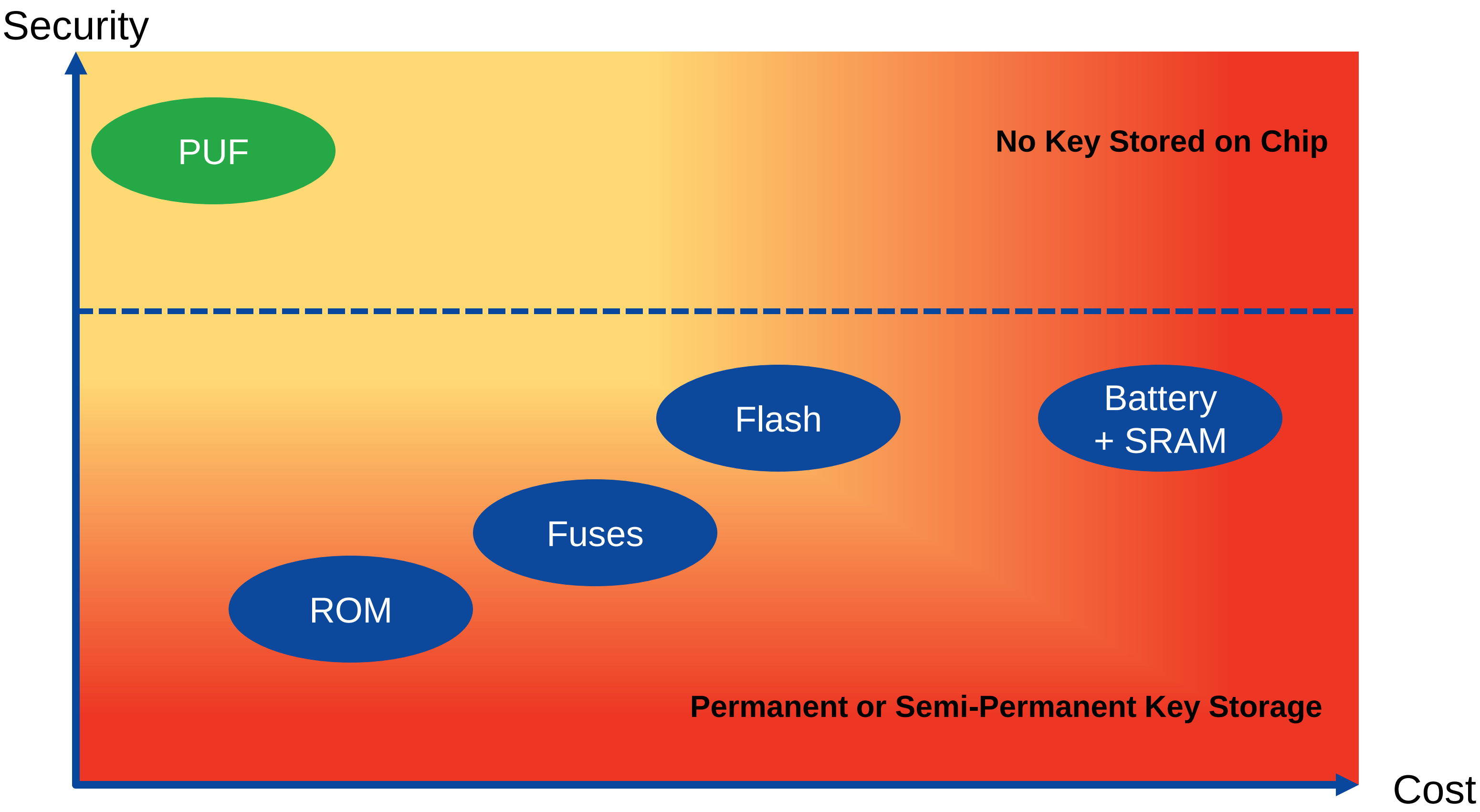
A $400 setup can cost you millions



Without Licensed DPA countermeasure protection your IP is vulnerable!

LICENSED DPA COUNTERMEASURES™

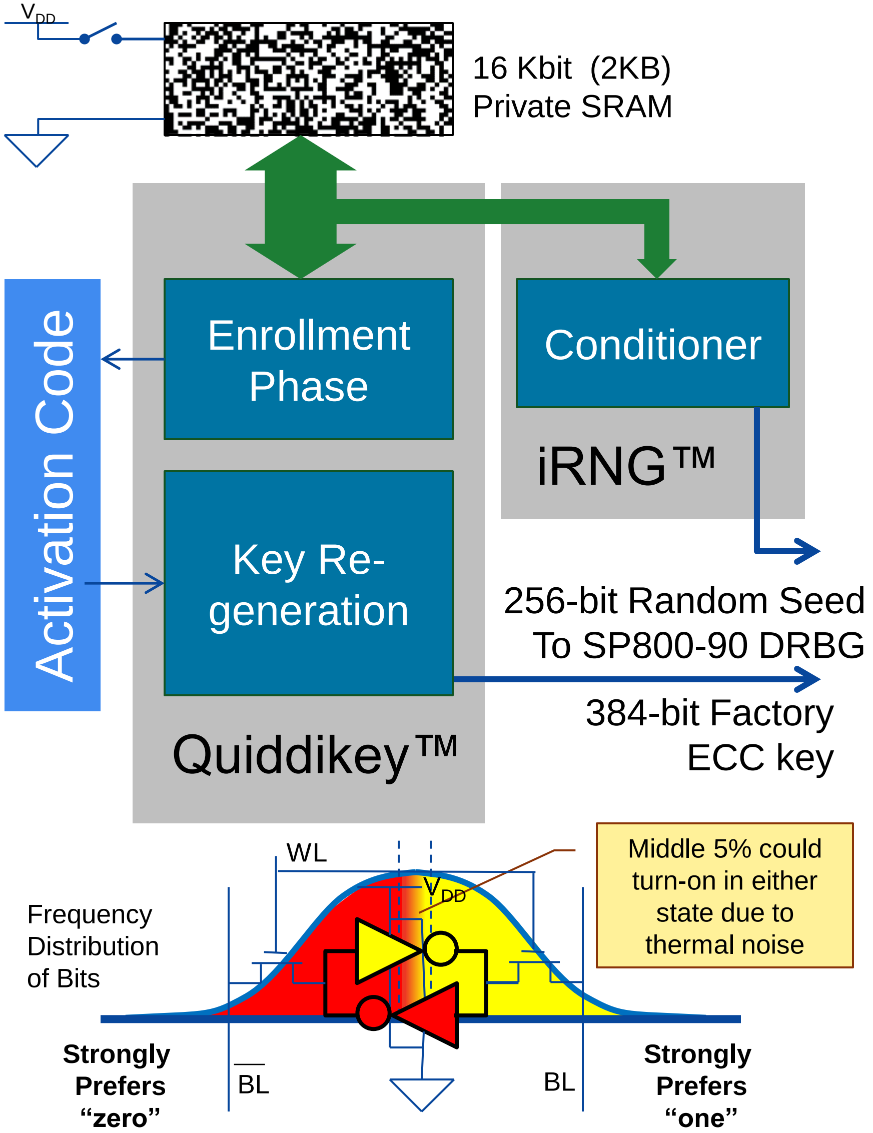
Security Requires Keys



Cost Versus Security for Various Key Storage options

SmartFusion®2 SRAM-PUF (060/090/150 KLE devices)

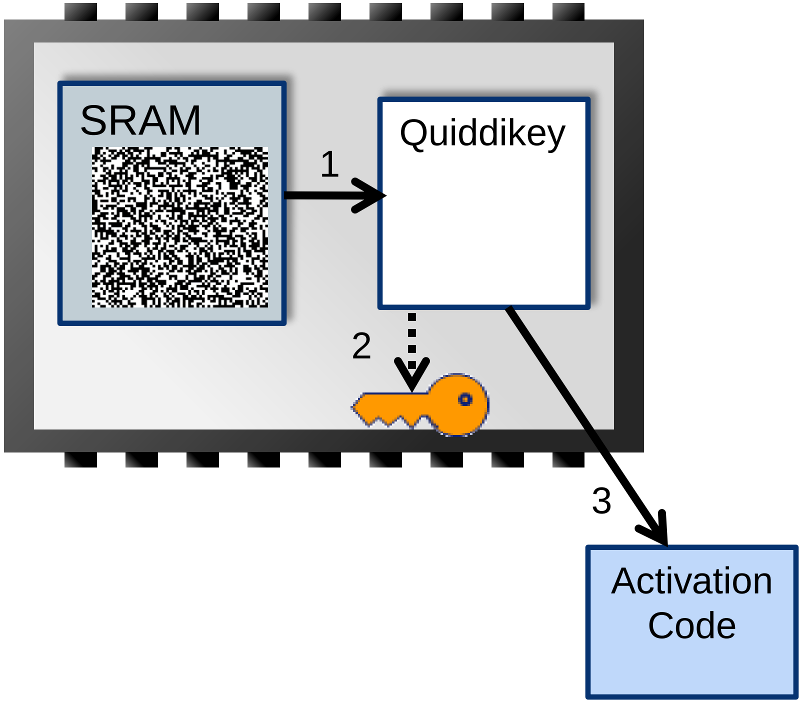
- PUF → a “biometric” identifier unique to each device
  - Analogous to a human fingerprint
    - No two alike, considered unclonable
- Licensed from Intrinsic-ID
- Based on quasi-static random start-up behavior of SRAM bits
  - Each cell independent
    - 50:50 chance of being a 1 or 0
  - But, largely repeatable
    - Typ. 95% of bits start-up same each power-up cycle (~5% noise at amb.)
    - Up to 20% noise over temp/life
- Most secure authentication and key storage mechanism



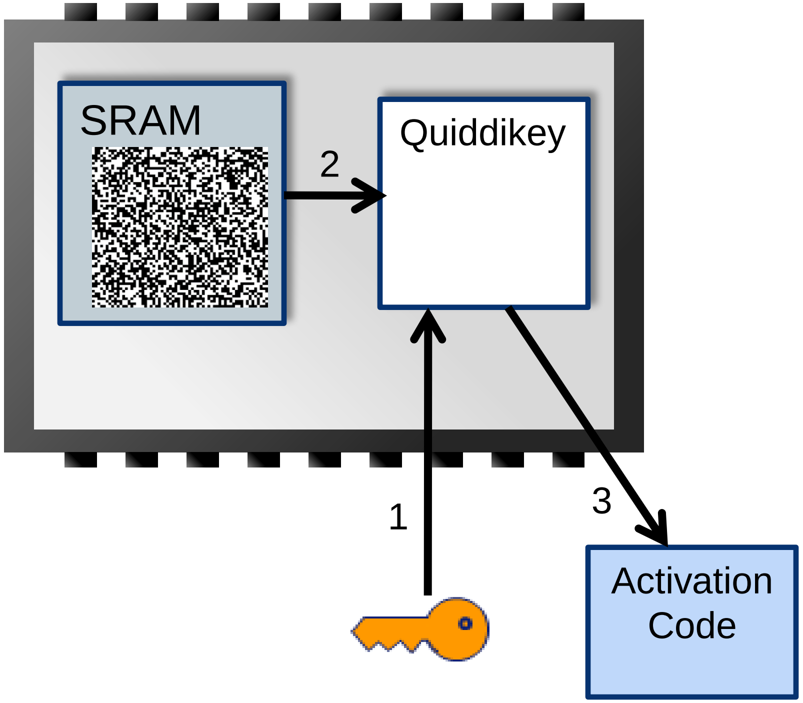
PUF = Physically Unclonable Function

SRAM PUF On-chip Enrollment

Enrollment of random device-unique key

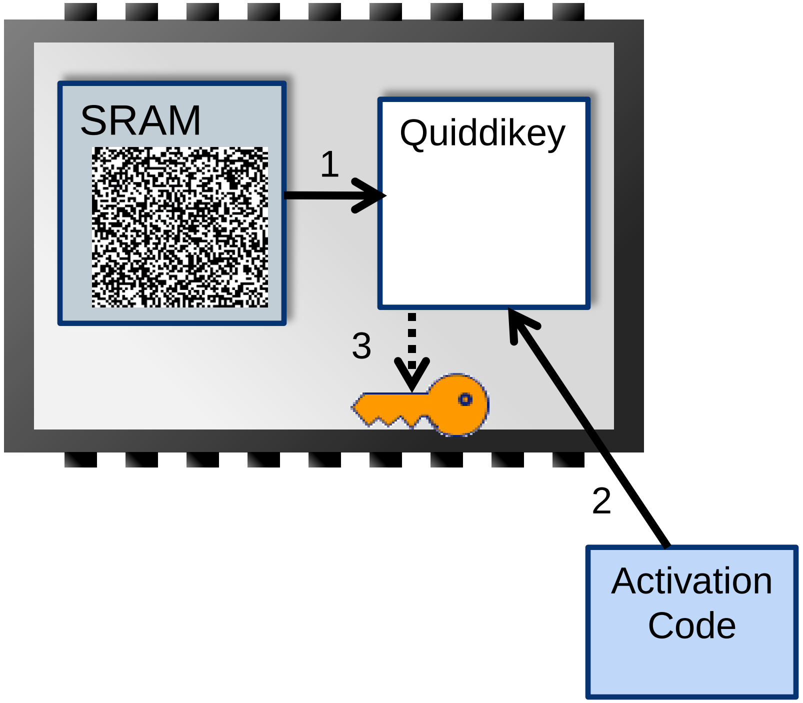


Enrollment of user-defined key

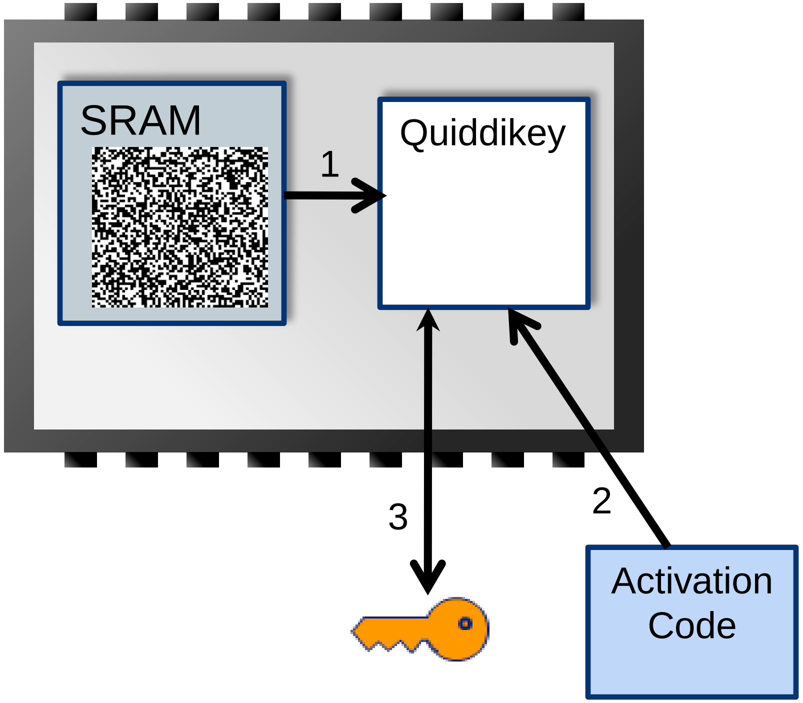


SRAM PUF Reconstruction

Reconstruction of random device-unique key

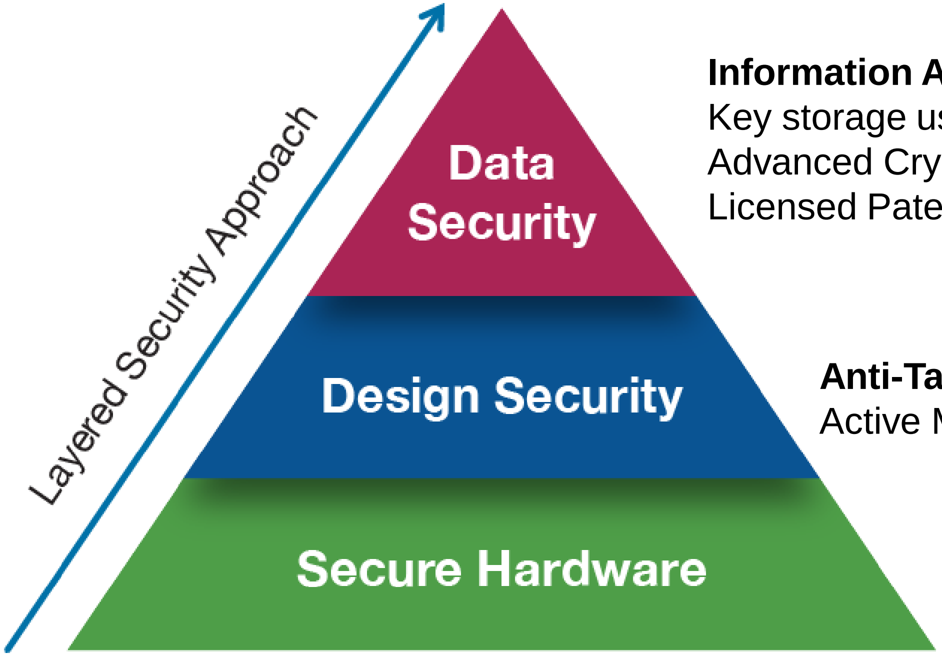


Reconstruction of user-defined key



Device Security is All About Layers

To protect your information you need
Secure Hardware, Design Security and Data Security



Information Assurance:
Key storage using Physically Unclonable Function (PUF)
Advanced Crypto Accelerators with a TRNG
Licensed Patent Protected DPA Resistance Pass through License

Anti-Tamper: Secure Bitstream, Tamper Detection, Active Mesh, No Copying. Cloning, or Reverse Engineering

Trust: Licensed Patent Protected DPA Resistance, NIST Certified Crypto Accelerators, Secure Supply Chain

LICENSED DPA COUNTERMEASURES™

Microsemi FPGAs provide
a solid foundation for your security needs

The DPA logo is a trademark of Cryptography Research, Inc. used under license

Public Key Infrastructure and its Pitfalls

Problem: Authenticated M2M Communications

- Desire to limit communications over a public network (i.e., the Internet) to authentic machines in the User’s private sub-network
  - Using authenticated encryption to also provide confidentiality, integrity
  - Other secure services also require entity authentication

Problem: Authenticated M2M Communications

- Desire to limit communications over a public network (i.e., the Internet) to authentic machines in the User’s private sub-network
  - Using authenticated encryption to also provide confidentiality, integrity
  - Other secure services also require entity authentication
- Symmetric key methods don’t scale well to large numbers of nodes
  - A single key shared by all is simple, but dangerously insecure
  - Individual (per device) symmetric keys are difficult to manage

Problem: Authenticated M2M Communications

- Desire to limit communications over a public network (i.e., the Internet) to authentic machines in the User’s private sub-network
  - Using authenticated encryption to also provide confidentiality, integrity
  - Other secure services also require entity authentication
- Symmetric key methods don’t scale well to large numbers of nodes
  - A single key shared by all is simple, but dangerously insecure
  - Individual (per device) symmetric keys are difficult to manage
- Solution: Asymmetric (and hybrid) cryptography methods
  - Each node has a unique public key pair {secret key, public key}
  - Public keys are certified using a public key infrastructure (PKI)
  - Communication is initially established by sharing the public keys
  - Bulk communication is done using symmetric keys, for efficiency

PKI Examples

M2M authenticated communication is especially interesting

Smart Grid

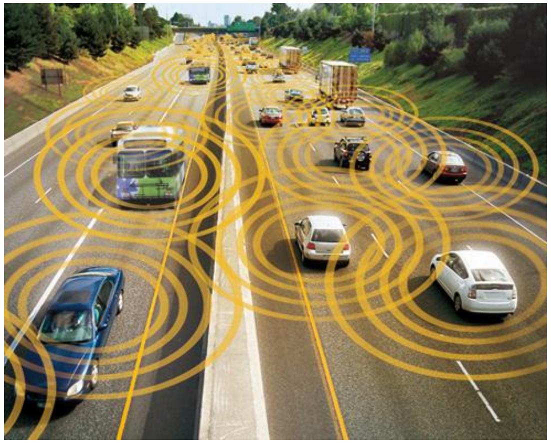
(Homes, Meters, Power Sources, Vehicles, Servers, etc.)

Medical

(Devices & Programmers)

Vehicles-to-Vehicle

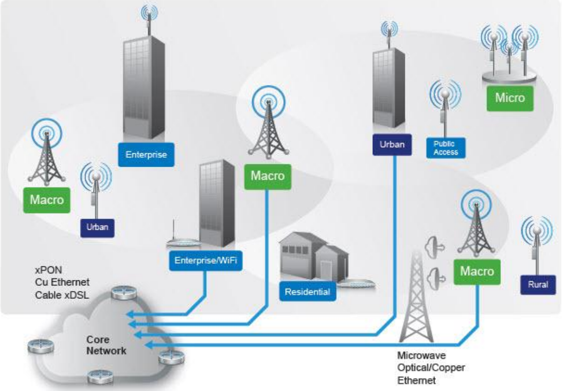
(V2V, and Vehicle-to-Infrastructure, V2I)



Field Sensors

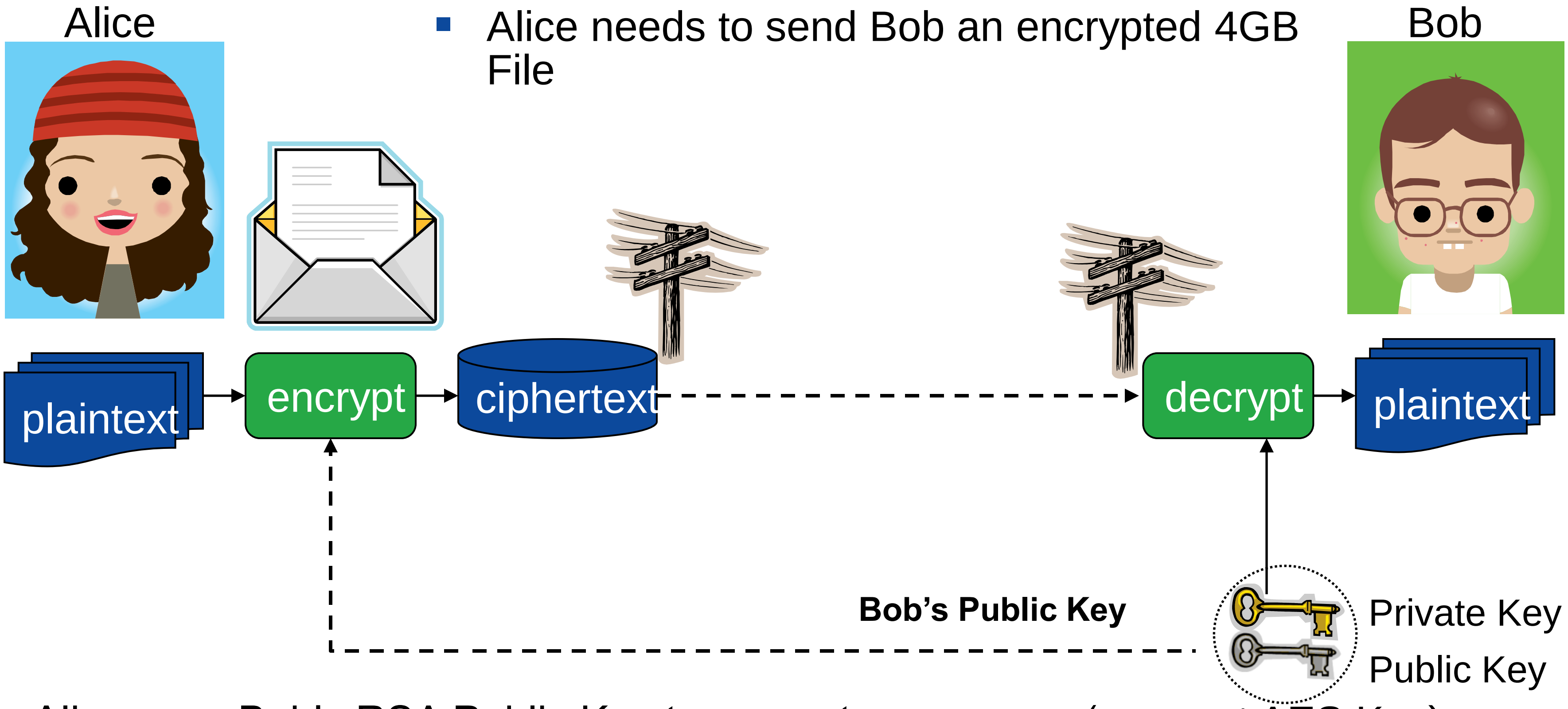
(e.g., Remote Flow Meters, Actuators)

Wired and Wireless Communications



Public Key Cryptography

- Alice needs to send Bob an encrypted 4GB File

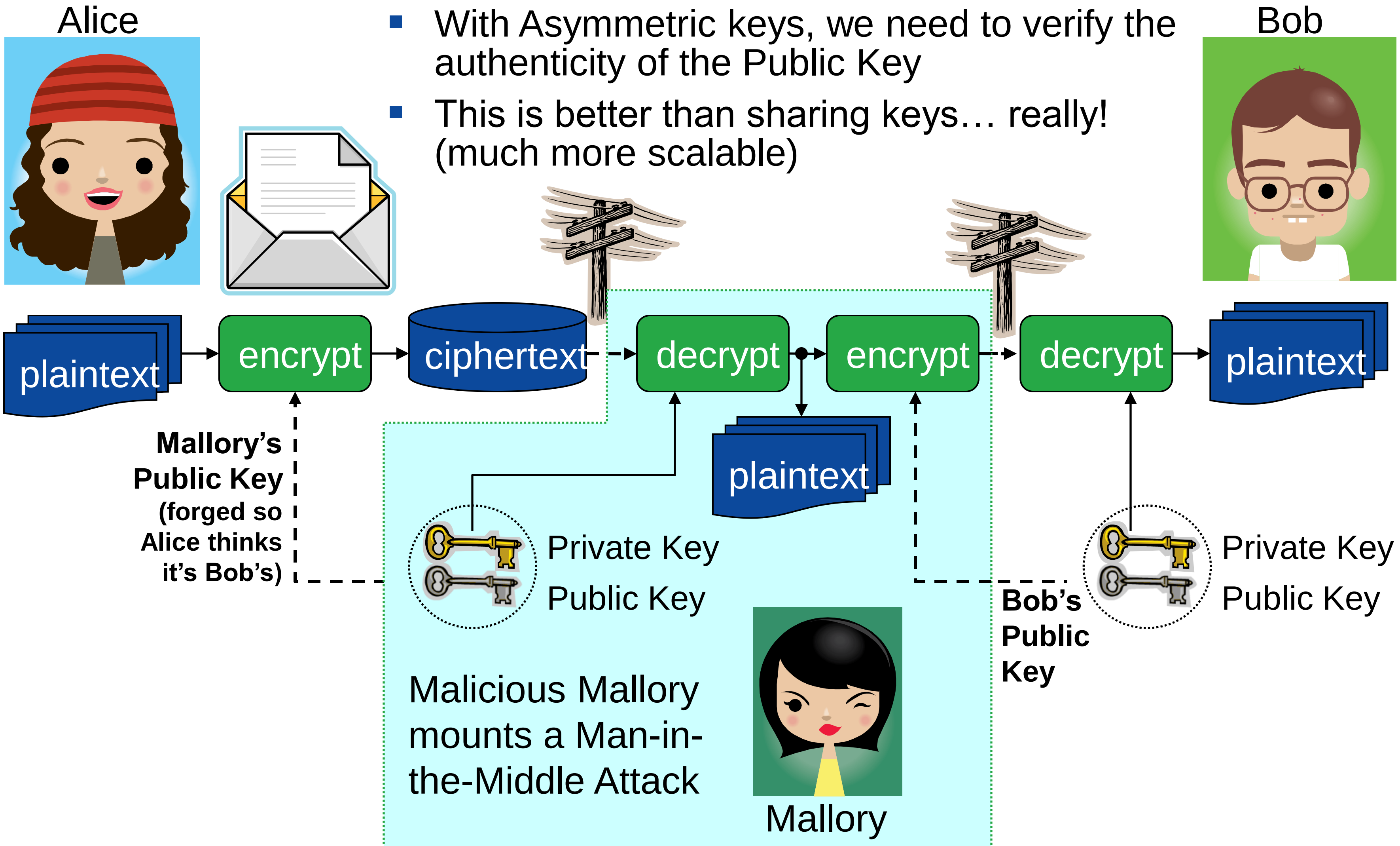


- Alice uses Bob's RSA Public Key to encrypt a message (a secret AES Key)
- Bob Decrypts Alice's message with his RSA Private Key (Bob now has the AES key)
- Alice sends the file, encrypted with the secret AES key to Bob
- Bob decrypts file with the secret AES Key
- Everyone is Happy?

Public Key Cryptography

New Problem – Key Authenticity (Binding)

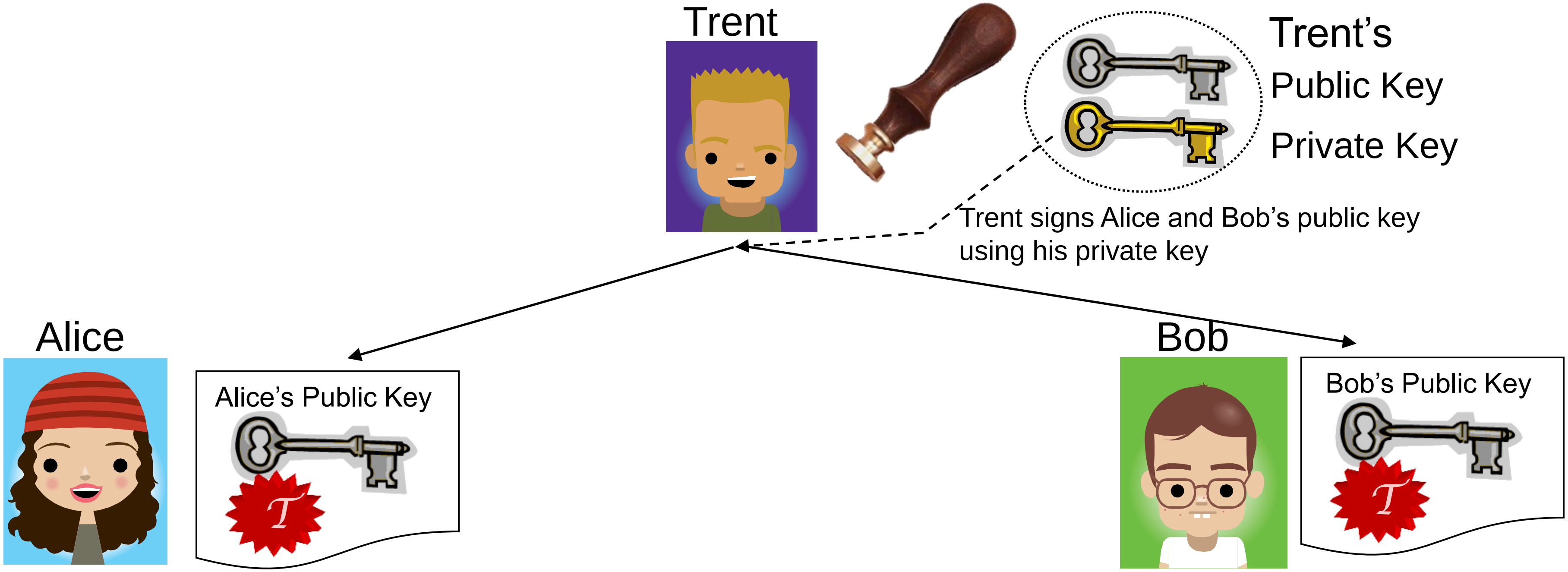
- With Asymmetric keys, we need to verify the authenticity of the Public Key
- This is better than sharing keys… really! (much more scalable)



- Alice should have called Bob on the phone and confirmed she had an authentic key!

Public Key Infrastructure (PKI)

Solves key binding problem



Trent

Trent's

Public Key

Private Key

Trent signs Alice and Bob's public key using his private key

Alice

Alice's Public Key

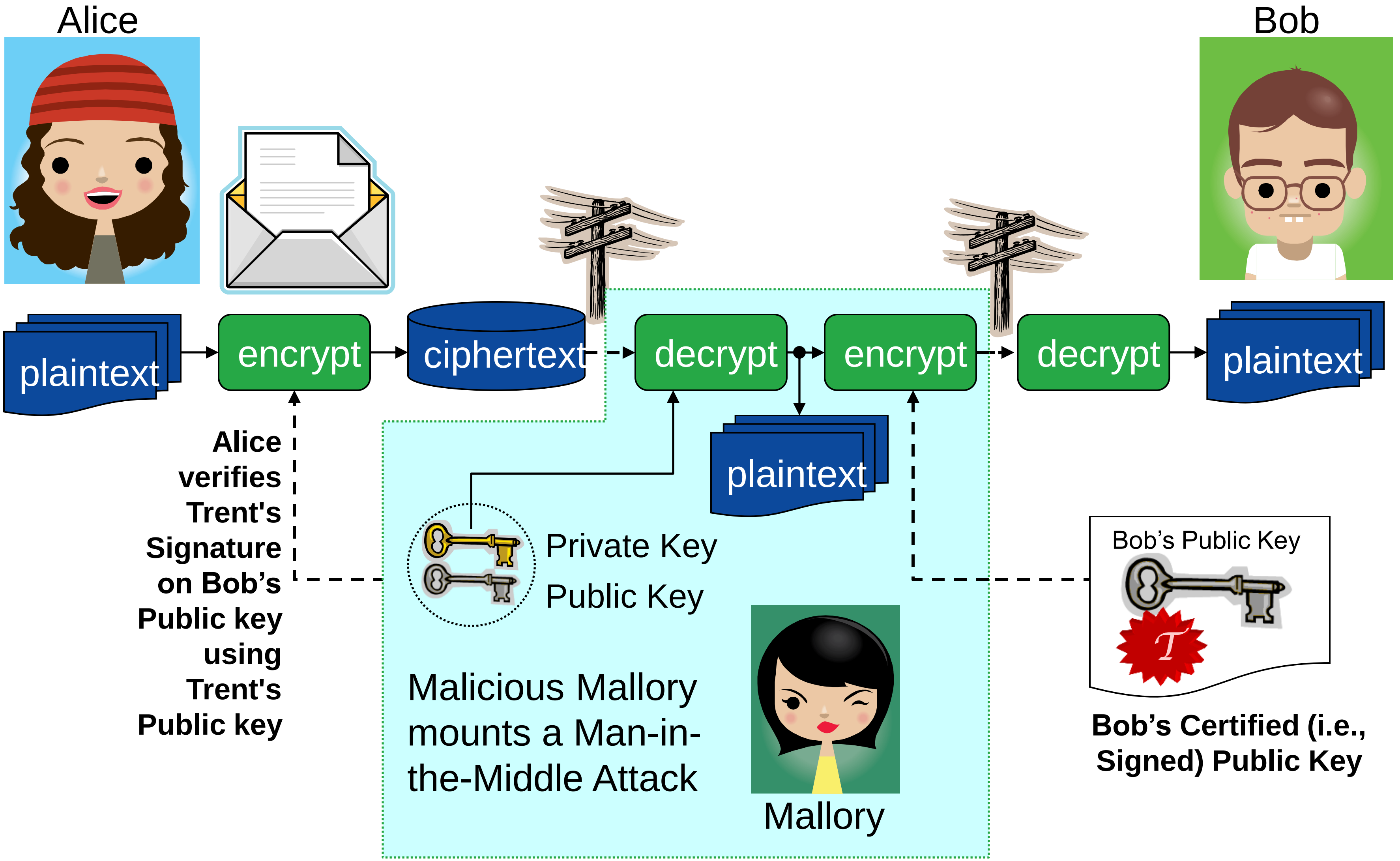
Bob

Bob's Public Key

- Trent's public key is trusted since it is well known to everyone

- Trent is careful to only sign anyone's public key after verifying that they are who they say they are

Public Key Cryptography with Key Authenticity

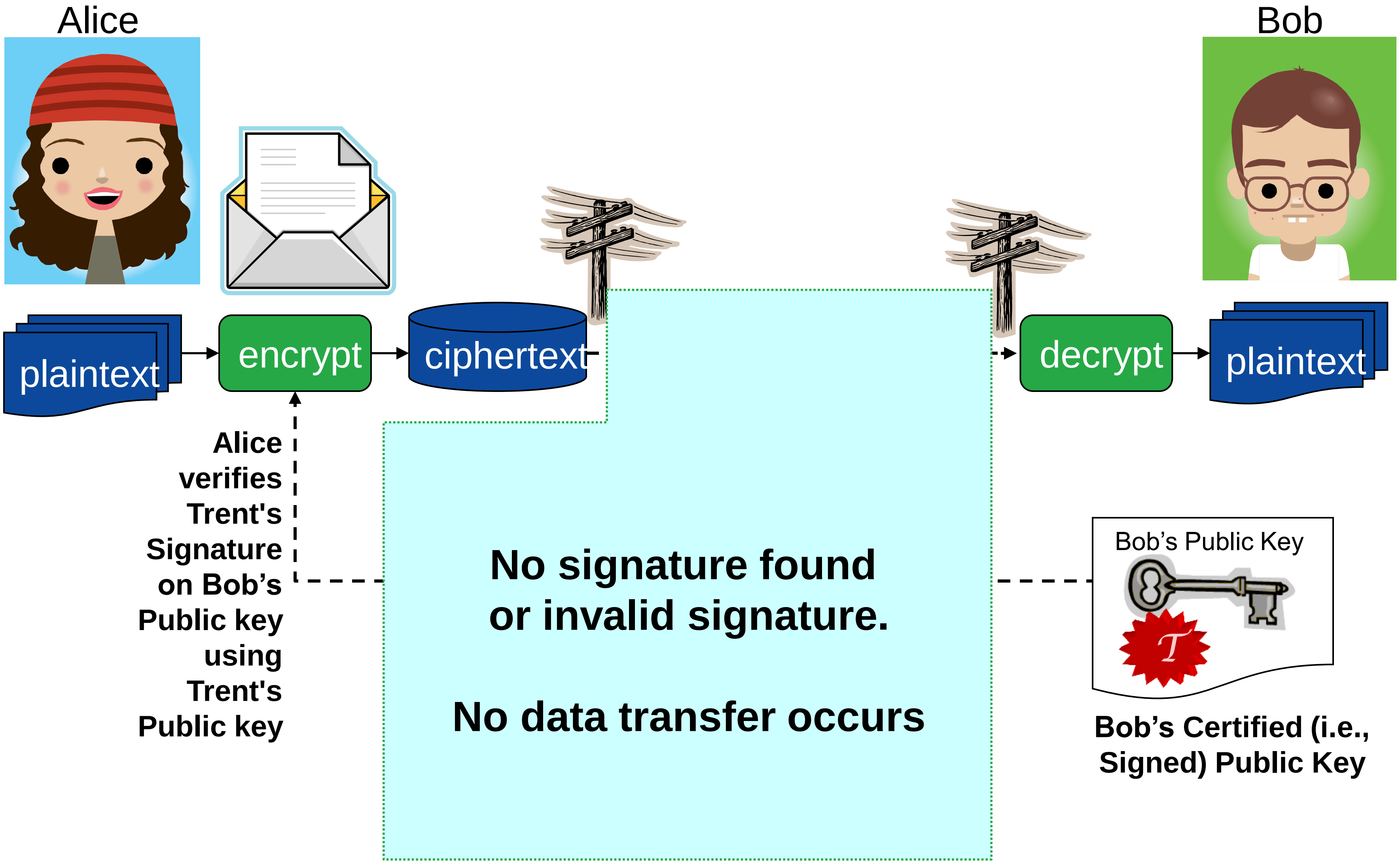


Alice verifies Trent's Signature on Bob's Public key using Trent's Public key

Malicious Mallory mounts a Man-in-the-Middle Attack

Bob's Certified (i.e., Signed) Public Key

Public Key Cryptography with Key Authenticity



Alice

Bob

plaintext → encrypt → ciphertext → decrypt → plaintext

Alice verifies Trent's Signature on Bob's Public key using Trent's Public key

No signature found or invalid signature.

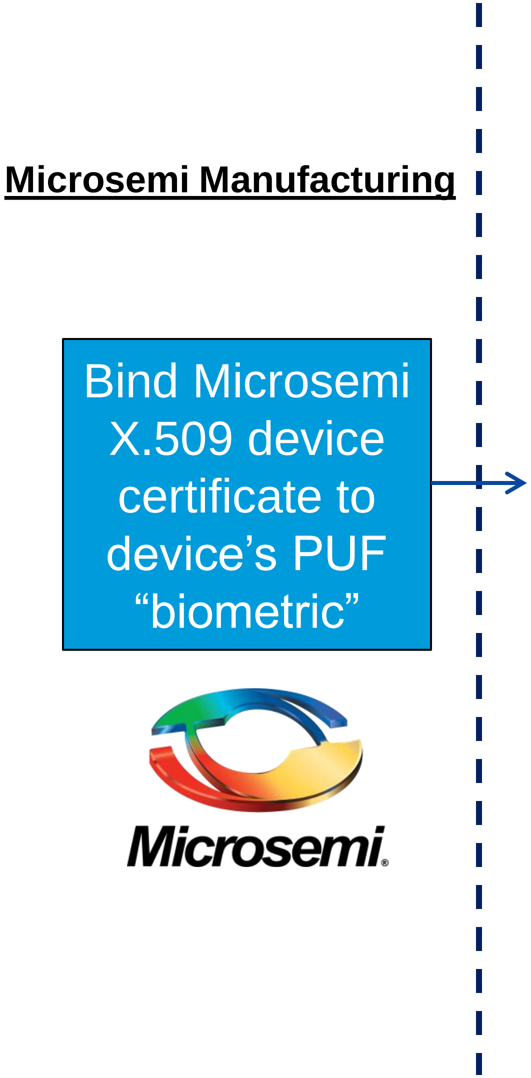
No data transfer occurs

Bob's Certified (i.e., Signed) Public Key

Microsemi / Escrypt PKI Reference Design

Secure M2M Enrollment & Run-Time Services

Extending the Trust Chain to End Applications

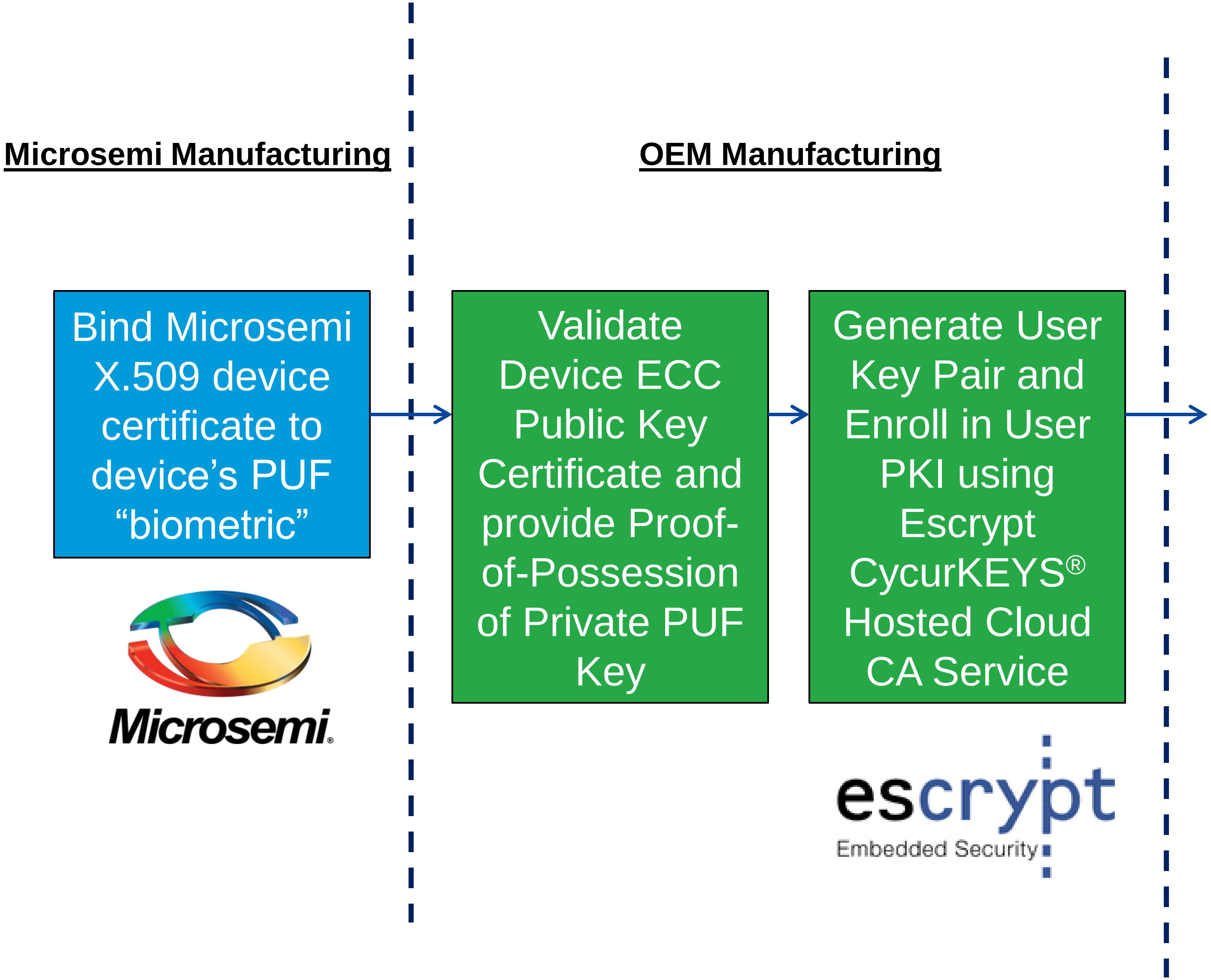


Microsemi Manufacturing

Bind Microsemi X.509 device certificate to device's PUF "biometric"

Secure M2M Enrollment & Run-Time Services

Extending the Trust Chain to End Applications



Microsemi Manufacturing

OEM Manufacturing

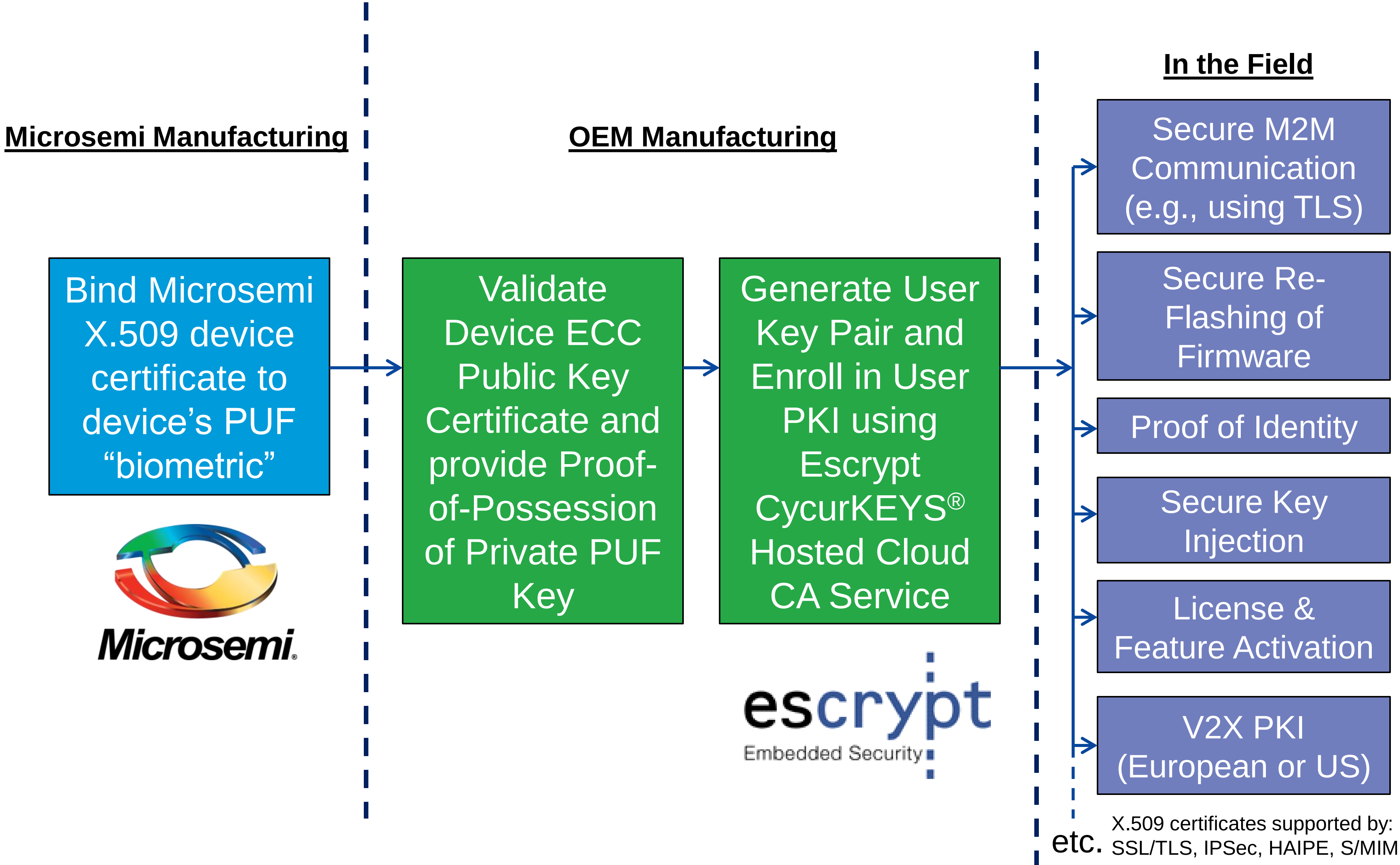
Bind Microsemi X.509 device certificate to device's PUF "biometric"

Validate Device ECC Public Key Certificate and provide Proof-of-Possession of Private PUF Key

Generate User Key Pair and Enroll in User PKI using Escrypt CycurKEYS® Hosted Cloud CA Service

Secure M2M Enrollment & Run-Time Services

Extending the Trust Chain to End Applications



Microsemi Manufacturing

Bind Microsemi X.509 device certificate to device's PUF "biometric"

OEM Manufacturing

Validate Device ECC Public Key Certificate and provide Proof-of-Possession of Private PUF Key

Generate User Key Pair and Enroll in User PKI using Escrypt CycurKEYS® Hosted Cloud CA Service

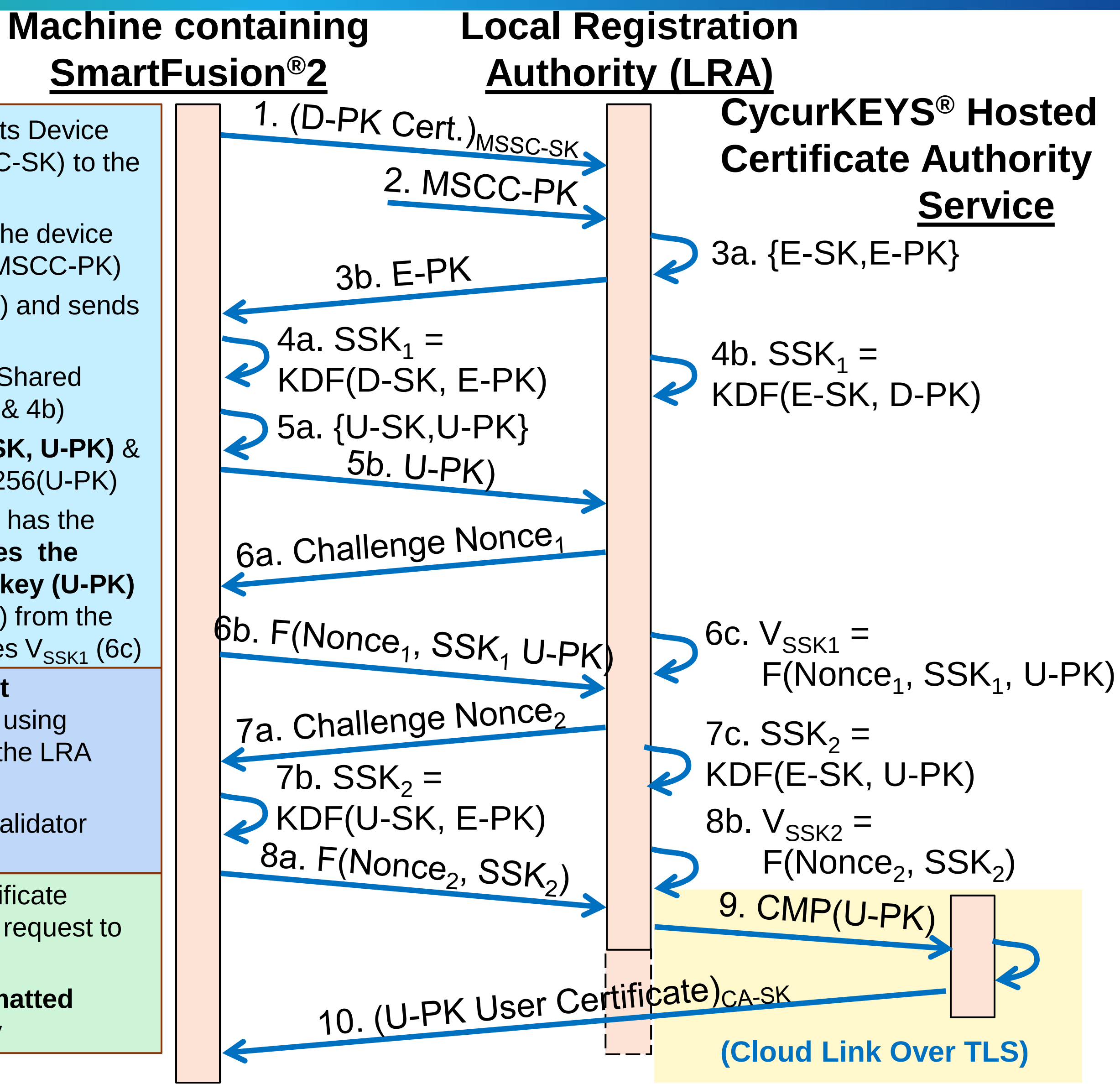
In the Field

- Secure M2M Communication (e.g., using TLS)
- Secure Re-Flashing of Firmware
- Proof of Identity
- Secure Key Injection
- License & Feature Activation
- V2X PKI (European or US)
- etc.

X.509 certificates supported by: SSL/TLS, IPSec, HAIPE, S/MIME, SSH, EAP, LDAP, XMPP, etc.

User PKI Enrollment Phase (Detail)

1. The device **exports its certificate** containing its Device Public Key (D-PK) signed by Microsemi (MSCC-SK) to the LRA
2. The LRA **verifies** the Microsemi signature on the device certificate with the trusted MSCC Public Key (MSCC-PK)
3. The LRA generates an ephemeral key pair (3a) and sends the public key to the device (3b)
4. Both the LRA and Device compute the ECDH Shared Secret Key using a key derivation function (4a & 4b)
5. The device **generates the User Key Pair (U-SK, U-PK)** & sets up to compute a validator (V_{SSK1}) w/ SHA256(U-PK)
6. The LRA challenges the device (6a) to prove it has the same shared secret, thus **proving it possesses the Device Secret Key (D-SK) & the new public key (U-PK)** required to compute it by computing V_{SSK1} (6b) from the SSK1 and the hash of U-PK. The LRA matches V_{SSK1} (6c)
7. The LRA challenges the device (7a) to **prove it possesses the new User Secret Key** (U-SK) using ECDH (7b & 7c) with the new User key pair & the LRA ephemeral key pair from step 3, above
8. The device and LRA compute and match the validator V_{SSK2} (8a & 8b)
9. The **LRA approves the request**, sends a certificate message protocol (CMP) -formatted certificate request to the cloud-based certificate authority (CA)
10. The **CA generates and signs the X.509 -formatted certificate** using the User Root CA Secret Key



Machine containing SmartFusion®2

Local Registration Authority (LRA)

CycurKEYS® Hosted Certificate Authority Service

1. $(\text{D-PK Cert.})_{\text{MSSC-SK}}$

2. MSCC-PK

3a. {E-SK,E-PK}

3b. E-PK

4a. SSK_1 = KDF(D-SK, E-PK)

4b. SSK_1 = KDF(E-SK, D-PK)

5a. {U-SK,U-PK}

5b. U-PK)

6a. Challenge Nonce_1

6b. $F(\text{Nonce}_1, SSK_1\ \text{U-PK})$

6c. V_{SSK1} = $F(\text{Nonce}_1, SSK_1, \text{U-PK})$

7a. Challenge Nonce_2

7b. SSK_2 = KDF(U-SK, E-PK)

7c. SSK_2 = KDF(E-SK, U-PK)

8a. $F(\text{Nonce}_2, SSK_2)$

8b. V_{SSK2} = $F(\text{Nonce}_2, SSK_2)$

9. CMP(U-PK)

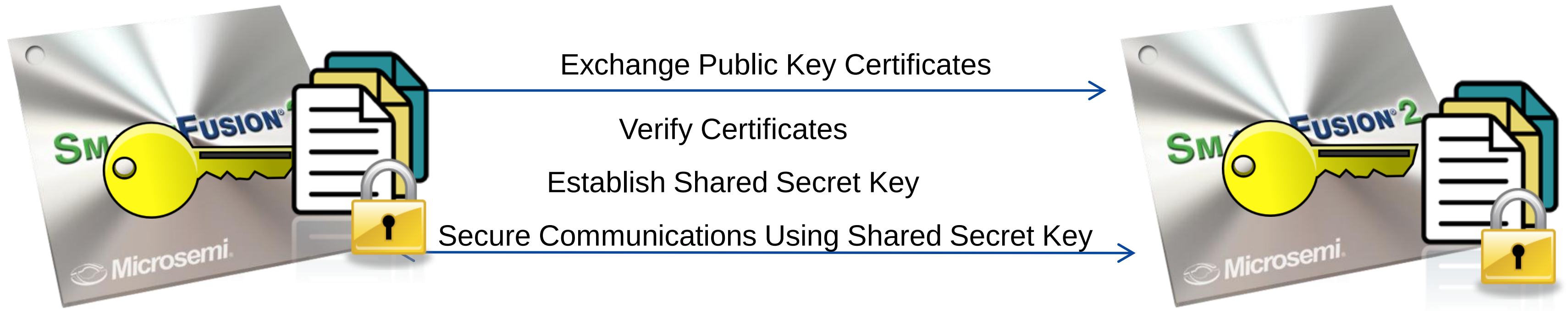
10. $(\text{U-PK User Certificate})_{\text{CA-SK}}$

(Cloud Link Over TLS)

PKI Run-Time Communication Phase

Machine containing
SmartFusion®2 TLS Client

Machine containing
SmartFusion®2 TLS Server



Exchange Public Key Certificates

Verify Certificates

Establish Shared Secret Key

Secure Communications Using Shared Secret Key

User-certified Device-unique
ECC Key Pair {U-SK, U-PK}
(As enrolled, signed by CA-SK))

Inherently Trusted User
Root CA Public Key (CA-PK)

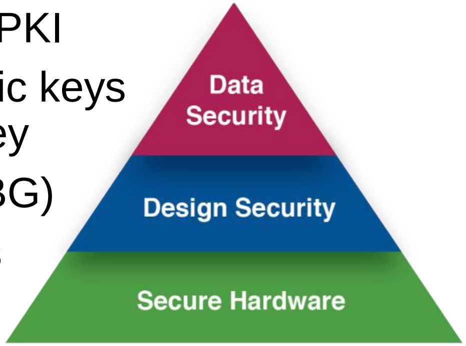
Ditto
(but device-unique)

Ditto

Demo display showing
web browser images

Features of SmartFusion®2/CycurKEYS® Flow

- Microsemi Value-Added Features
  - Layered device security
  - SmartFusion®2's SRAM-PUF provides unforgeable "biometric" identity for devices
  - PUF ECC P-384 key pair certified as part of the Microsemi device PKI
  - Ability to generate new key pairs and bind the newly exported public keys to the silicon "biometric" using the Microsemi-certified PUF ECC key
  - Extensive built-in cryptographic capabilities (AES, SHA, ECC, NRBG)
  - State-of-the-art PUF-based key storage and management features

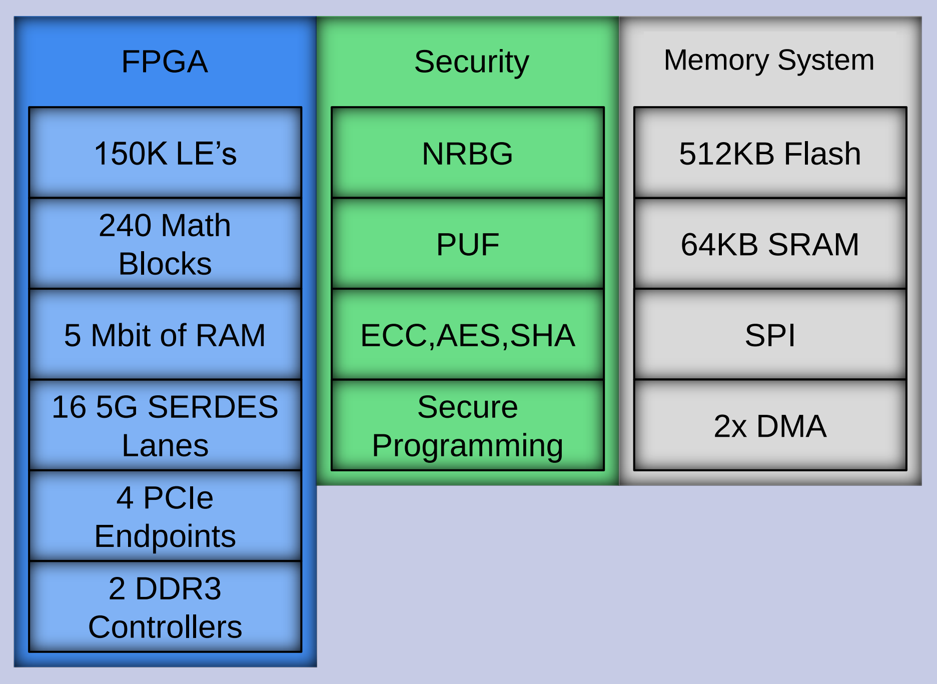


- Escrypt Value-Added Features
  - CycurKEYS® hosted certificate authority (CA) service "in-the-cloud" eliminates the requirement for the OEM to develop and stand-up a secure, reliable private certificate authority infrastructure – or provides the SW tools to do so
  - All required PKI services using the industry-standard Certificate Management Protocol (CMP) per RFC 4210 and using the X.509v3 entity certificate and certificate revocation list (CRL) formats
- Microsemi/Escrypt Partnership
  - Free reference design shows how to tie all the pieces together (March 2015)
  - Expert services also available

Microsemi Mainstream FPGAs

IGLOO2 and SmartFusion2

IGLOO2 – Differentiated Mainstream FPGA



FPGA	Security	Memory System
150K LE’s	NRBG	512KB Flash
240 Math Blocks	PUF	64KB SRAM
5 Mbit of RAM	ECC,AES,SHA	SPI
16 5G SERDES Lanes	Secure Programming	2x DMA
4 PCIe Endpoints		
2 DDR3 Controllers		

- All the historical benefits of using a flash based FPGA like Low power, Reliability and Security are now available in a mainstream FPGA with IGLOO2. Expect more!
  - *More* 5G SERDES Channels
  - *More* GPIO and PCI Compliant 3.3V I/O
  - *Highest Integration* of ASIC Based Functionality
  - *Lowest* Total System Cost
  - *Smallest* Form Factor
  - *Lowest* Power
  - *Highest* Reliability
  - *Unrivaled* Security

LICENSED DPA COUNTERMEASURES™

Libero System-on-Chip

Competitive Landscape < 150K LEs

Features	Microsemi IGLOO2	Competitor A Low-end	Competitor B Low-end
Logic Elements (K)	150	131	150
Max I/O	**574**	300	480
Max SERDES Lanes	**16**	8	9
Max Hard PCI Express Endpoints	**4**	1	2
Hard DDR3 Controllers	**2**	0	2
Max DSP Blocks	240	240	312
Max RAM Mbits	5	5	7
High Performance Memory Subsystem	**Yes**	No	No
Embedded Flash (eNVM)	**Yes**	No	No
Low Power	**Yes**	No	No
Instant-On	**Yes**	No	No
Security	**Yes**	No	No
Reliability	**Yes**	No	No
External Configuration Device	**Not Required**	Required	Required
Power Supplies	**2**	3	3

Competitive Offerings Are Underserving Key Requirements

More Resources Available on Devices

IGLOO2 Higher Max I/O per LE Density

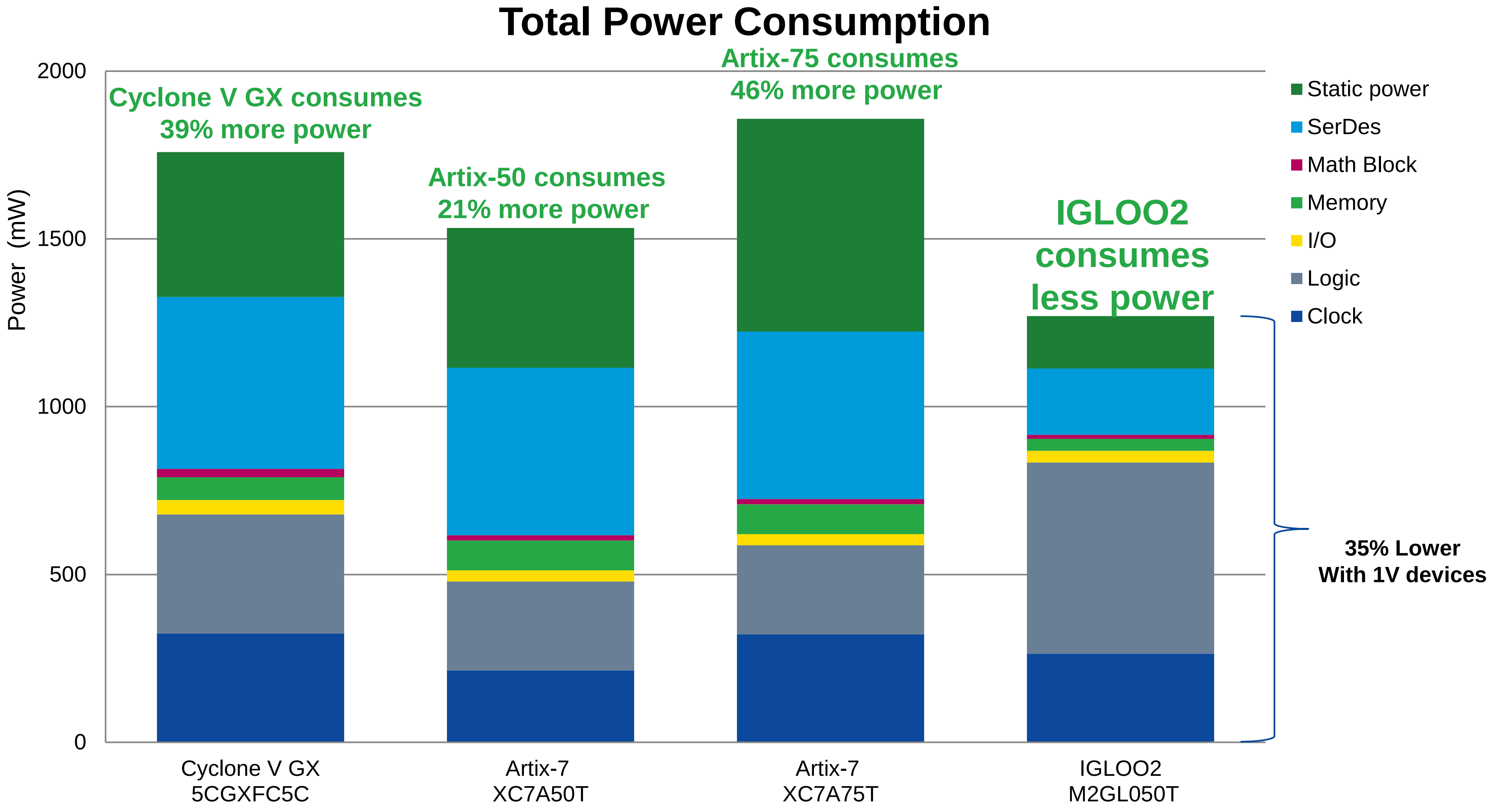
K LE	IGLOO2	Max I/O	Cyclone V-GT	Max I/O	Artix-7	Max I/O
10	M2GL010T	233	-	-	XC7A20SLT	216
25	M2GL025T	267	-	-	XC7A35SLT	216
50	M2GL050T	377	-	-	XC7A50SLT/75	300
90	M2GL090T	412	5CGTD5	336	XC7A100T	300
150	M2GL150T	574	5CGTD7	480	XC7A100T	300

IGLOO2 More SERDES channels at smaller Densities

K LE	IGLOO2	Max 5G SERDES Channels	Cyclone V-GT	Max 5G SERDES Channels	Artix-7 SLT	Max 5G SERDES Channels
10	M2GL010T	4	-	-	-	-
25	M2GL025T	4	-	-	XC7A20/35SLT	4
50	M2GL050T	8	-	-	XC7A50SLT/75	8
90	M2GL090T	4	5CGTD5	6	XC7A100T	8
150	M2GL150T	16	5CGTD7	9	XC7A200T	16

Customers Forced to Buy Larger LE Count Devices
To Meet Application Requirements

IGLOO2: Consumes 17-31% Less Power



Measured at T_j = 100C, worst case conditions

Note: Flash*Freeze mode will yield larger differences

SmartFusion®2 SoC FPGA

Microcontroller	FPGA	Security
166MHz ARM Cortex-M3	150K LE's	NRBG
512KB Flash 64KB SRAM	240 Math Blocks	PUF
8KB I Cache	5 Mbit of RAM	ECC,AES,SHA
10/100/1000	16 5G SERDES Lanes	Secure Programming
HS USB OTG	4 PCIe Endpoints	
CAN	2 DDR3 Controllers	
2x SPI, UART, I2C, Timer		
2x DMA		
Watch Dog		
RTC		

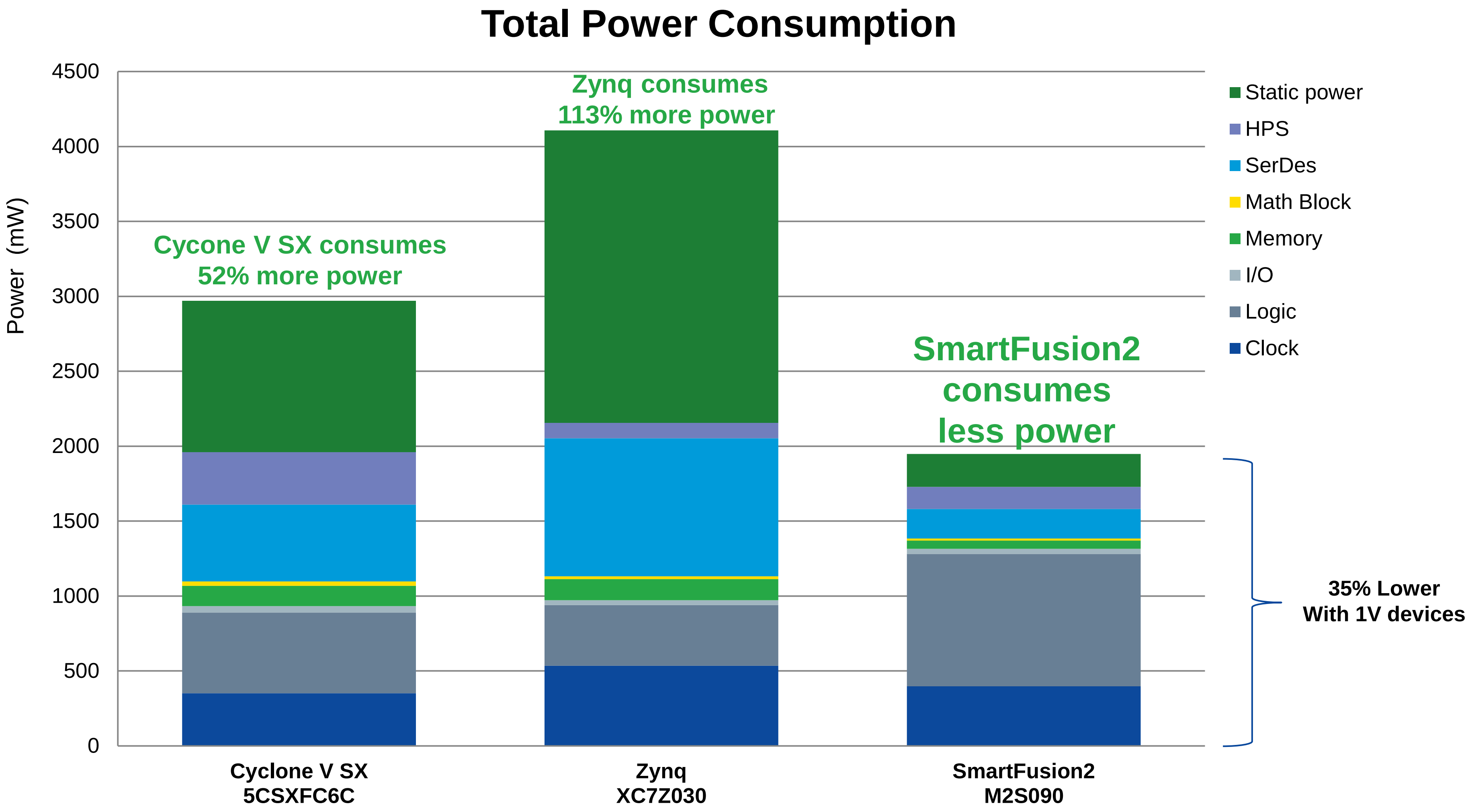
- SmartFusion2 integrates the industry standard real time Cortex-M3 microcontroller with standard communications interfaces. Included in SmartFusion2 are advanced security features like DPA resistant bitstream programming, Physically unclonable function, random number generator and Elliptical curve Cryptography all in the lowest power SoC FPGA device available.

Libero
System-on-Chip

Secure Boot

LICENSED DPA COUNTERMEASURES™

SmartFusion2: Consumes 34-53% Less Power

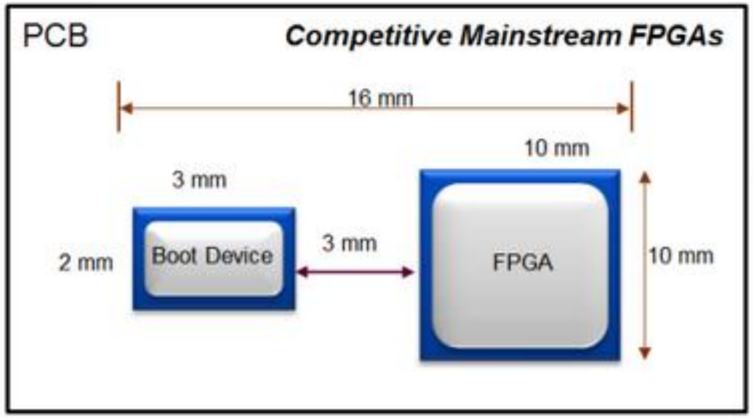


Measured at T_j = 100C, worst case conditions

Note: Flash*Freeze mode will yield larger differences

Small Form Factors

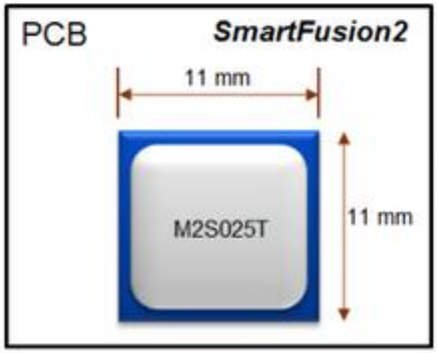
- Microsemi FPGAs and SoC FPGAs enable new applications with small packages and no requirement for an external configuration memory



Total real-estate required is 160 mm^2

+

PROM Cost



Total real-estate required is 121 mm^2

❖ *Applicable to I/O centric applications*

IGLOO2 & SmartFusion2 Families

	Features	M2GL005 M2S005	M2GL010 M2S010	M2GL025 M2S025	M2GL050 M2S050	M2GL060 M2S060	M2GL090 M2S090	M2GL150 M2S150
Logic / DSP	Maximum Logic Elements (4LUT+DFF)	6,060	12,084	27,696	56,340	56,340	86,316	146,124
	Math Blocks (18x18)	11	22	34	72	72	84	240
	PLLs and CCCs	2		6				8
	MSS or HPMS	1 each						
	Security	AES256, SHA256, RNG				AES256, SHA256, RNG, ECC, PUF		
Memory	eNVM (K Bytes)	128	256				512	
	LSRAM 18K Blocks	10	21	31	69	69	109	236
	uSRAM1K Blocks	11	22	34	72	72	112	240
	eSRAM (K Bytes)	64						
	Total RAM (K bits)	703	912	1104	1826	1826	2586	5000
High Speed	DDR Controllers	1x18			2x36	1x18	1x18	2x36
	SERDES Lanes	0	4		8	4	4	16
	PCIe End Points	0	1		2			4
User I/Os	MSIO (3.3V)	115	123	157	139	271	306	292
	MSIOD (2.5V)	28	40	40	62	40	40	106
	DDRIO (2.5V)	66	70	70	176	76	66	176
	Total User I/O	209	233	267	377	387	425	574

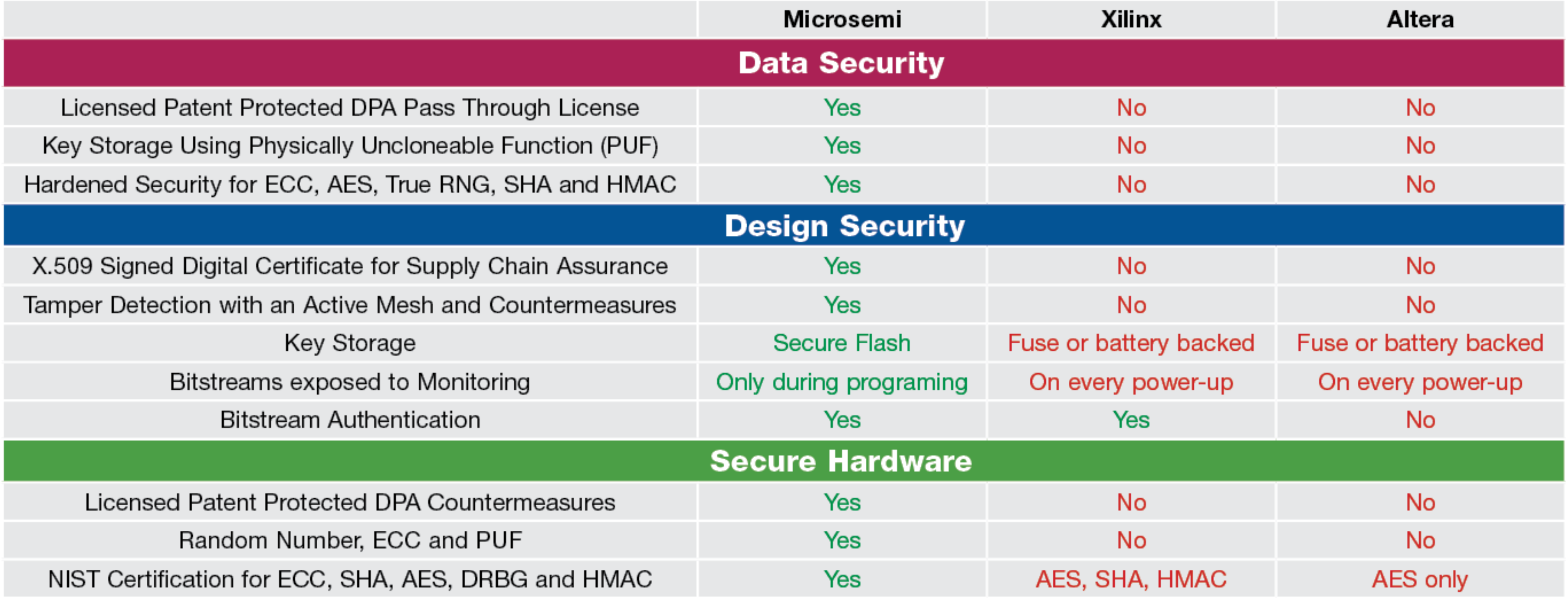
Total logic may vary based on utilization of DSP and memories in your design. Please see the IGLOO2 and SmartFusion2 Fabric User Guides for details
Feature availability is package dependent

IGLOO2 & SmartFusion2 Packages

	Package Options																			
Type	FCSG325		VFG256		FCSG536		VFG400		FCVG484		TQG144		FGG484		FGG676		FGG896		FCG1152	
Pitch (mm)	0.5		0.8		0.5		0.8		0.8		0.5		1.0		1.0		1.0		1.0	
Length x Width (mm)	11x11		14x14		16x16		17x17		19x19		20x20		23x23		27x27		31x31		35x35	
Device Density	I/O	Lanes	I/O	Lanes	I/O	Lanes	I/O	Lanes	I/O	Lanes	I/O	Lanes	I/O	Lanes	I/O	Lanes	I/O	Lanes	I/O	Lanes
005			161	-			171	-			84	-	209	-						
010			138	2			195	4			84	-	233	4						
025	180	2	138	2			207	4					267	4						
050	200	2					207	4					267	4			377	8		
060	200	2					207	4					267	4	387	4				
090	180	4											267	4	425	4				
150					293	4			248	4									574	16

090 is 11x13 in FCS325 pkg type
All packages available in leaded – drop the “G” before the pin count VF400 for example

Comparing Security Capabilities of FPGAs



	Microsemi	Xilinx	Altera
Data Security			
Licensed Patent Protected DPA Pass Through License	Yes	No	No
Key Storage Using Physically Uncloneable Function (PUF)	Yes	No	No
Hardened Security for ECC, AES, True RNG, SHA and HMAC	Yes	No	No
Design Security			
X.509 Signed Digital Certificate for Supply Chain Assurance	Yes	No	No
Tamper Detection with an Active Mesh and Countermeasures	Yes	No	No
Key Storage	Secure Flash	Fuse or battery backed	Fuse or battery backed
Bitstreams exposed to Monitoring	Only during programing	On every power-up	On every power-up
Bitstream Authentication	Yes	Yes	No
Secure Hardware			
Licensed Patent Protected DPA Countermeasures	Yes	No	No
Random Number, ECC and PUF	Yes	No	No
NIST Certification for ECC, SHA, AES, DRBG and HMAC	Yes	AES, SHA, HMAC	AES only

Microsemi FPGAs have the most extensive security feature set of any FPGA on the market

Microsemi

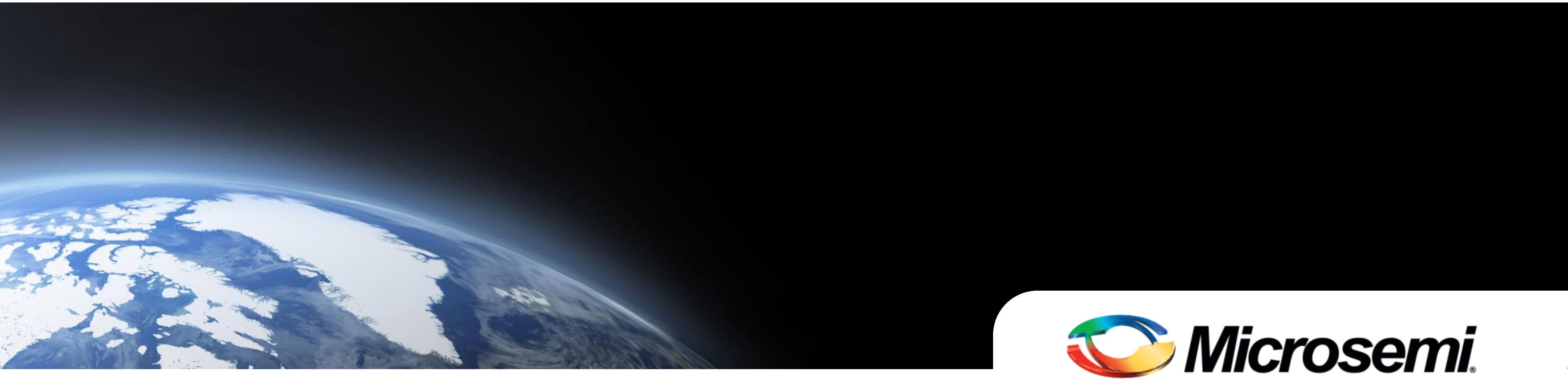
Summary

- Connectivity is not going away
  - Threats are increasing across all applications and market segments

- Security must be layered within a device and across systems and networks
  - Microsemi and Escrypt reference design does much of the heavy lifting for enabling PKI in applications

- Microsemis Mainstream SoC FPGAS, and FPGAs provide a low power, small form factor programmable security solution

Power Matters.^{TM}



Thank You For Attending

http://www.microsemi.com/products/fpga-soc/security