UCA OpenSG Security: Update on Embedded Systems Security Task Force Activities

Rohit Khera, rxkw@pge.com

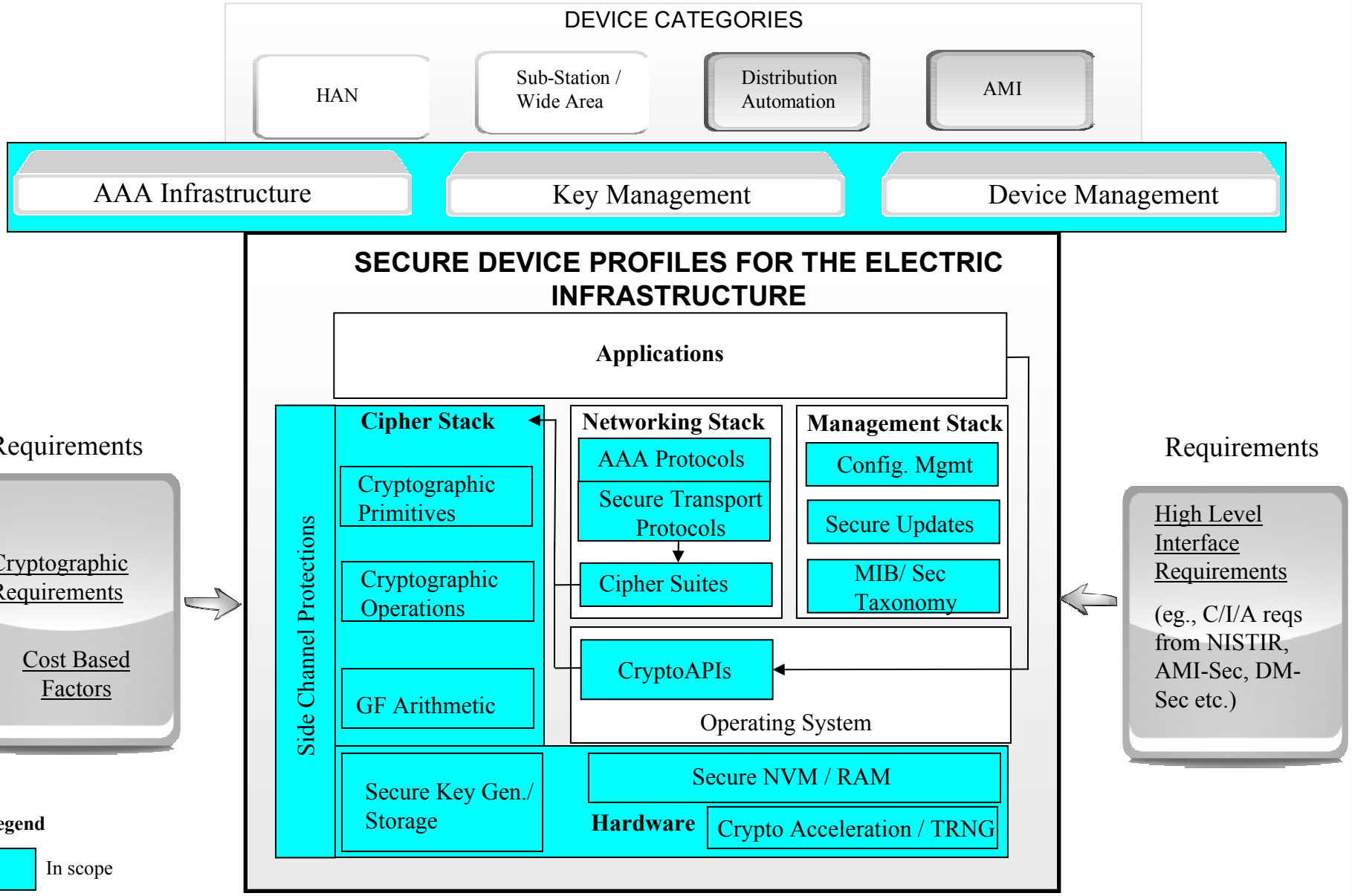
03/09/2011

Agenda

- Update on Secure Device Profile Components
- Deliverables and Progress
- Some Questions Around Hardware
- Intellectual Property Rights Considerations
- Constraint Characterization
- Organization & Contact Info

Secure Device Profile Components

Create multiple secure profiles to address disparate device resource characteristics and communication infrastructures across multiple device categories – leverage existing standards / SDOs



Deliverables and Progress

Topic	Primary Owner/s	Secondary Owner/s	Start Date / Status	Est. Completion
Cryptographic Hardware	Shrinath Eswarahally (Infineon)		Underway (first draft submitted)	
Ciphers (refer to NISTIR 7628 Crypto Section)	Rohit Khera (PG&E)	Daniel Thanos (GE)	Underway	
Random Number Generation	Sami Nassar (NXP)	Rohit Khera (PG&E)		
Device Identity	Sami Nassar (NXP) Marc Auclair (NXP) Mike Ahmadi (GraniteKey/NXP)	Sadu Bajekal (IBM)		
Device Authentication & Access Control	None			
Device Robustness & Resilience	Bora Akyol (PNNL) Daniel Thanos (GE)			
Key Management	David Sequino (Green Hills Software) Chris Dunn (Safenet) Gib Sorebo (SAIC)			

Deliverables and Progress

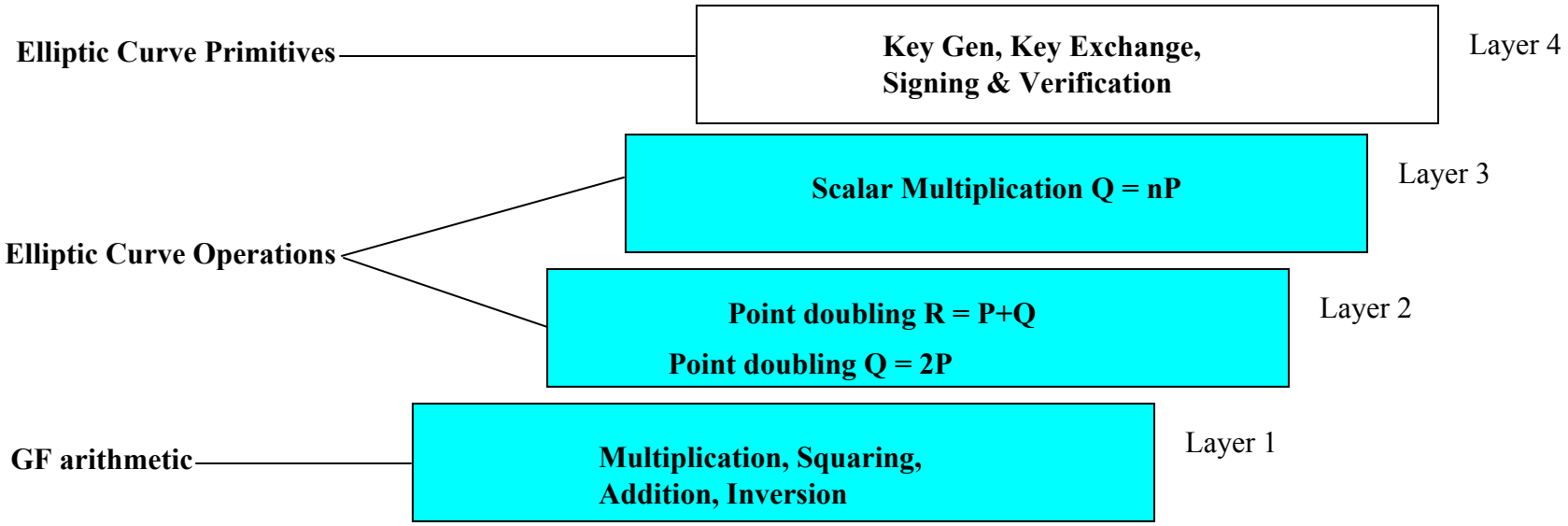
Topic	Primary Owner/s	Secondary Owner/s	Start Date / Status	Est. Completion
Device Mgmt	Sadu Bajekal (IBM) Steve Dougherty (IBM)			
Secure Protocols	None			
Device Authentication and Access Control	None			

Acceleration for public key cryptography – Sample Applications

Modular Multiplication

- Multiple efficient acceleration approaches for modular multiplication in Z/nZ - (i) multiply and reduce (ii) interleaving (Karatsuba Ofman, Booth-Barrett, Montgomery method)
- Multiple efficient acceleration approaches for modular multiplication in GF(2^m) – basis dependant / independent

Acceleration techniques for ECC



- ***Monolithic / Single Die***

  Example – Smart Cards (Cryptographic / Security boundary encompasses the entire system)

  Advantages – Entire system contained within boundary

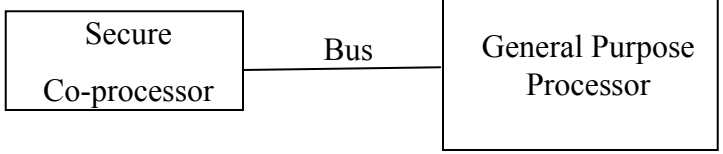
  Dis-Advantages – Low word size (typically 16 bit) and clock rating

- ***Co - Processor***

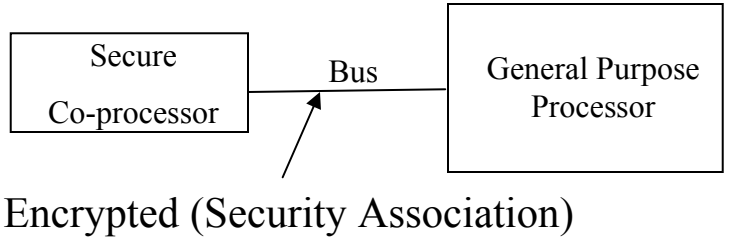
  Advantages – Augment security functions, secure key storage (how about oracle based attacks?), acceleration, side channel protections etc.

  Dis-Advantages – Cleartext traverses bus to general purpose MCU?

A



B



Typical Secure MCU Layout

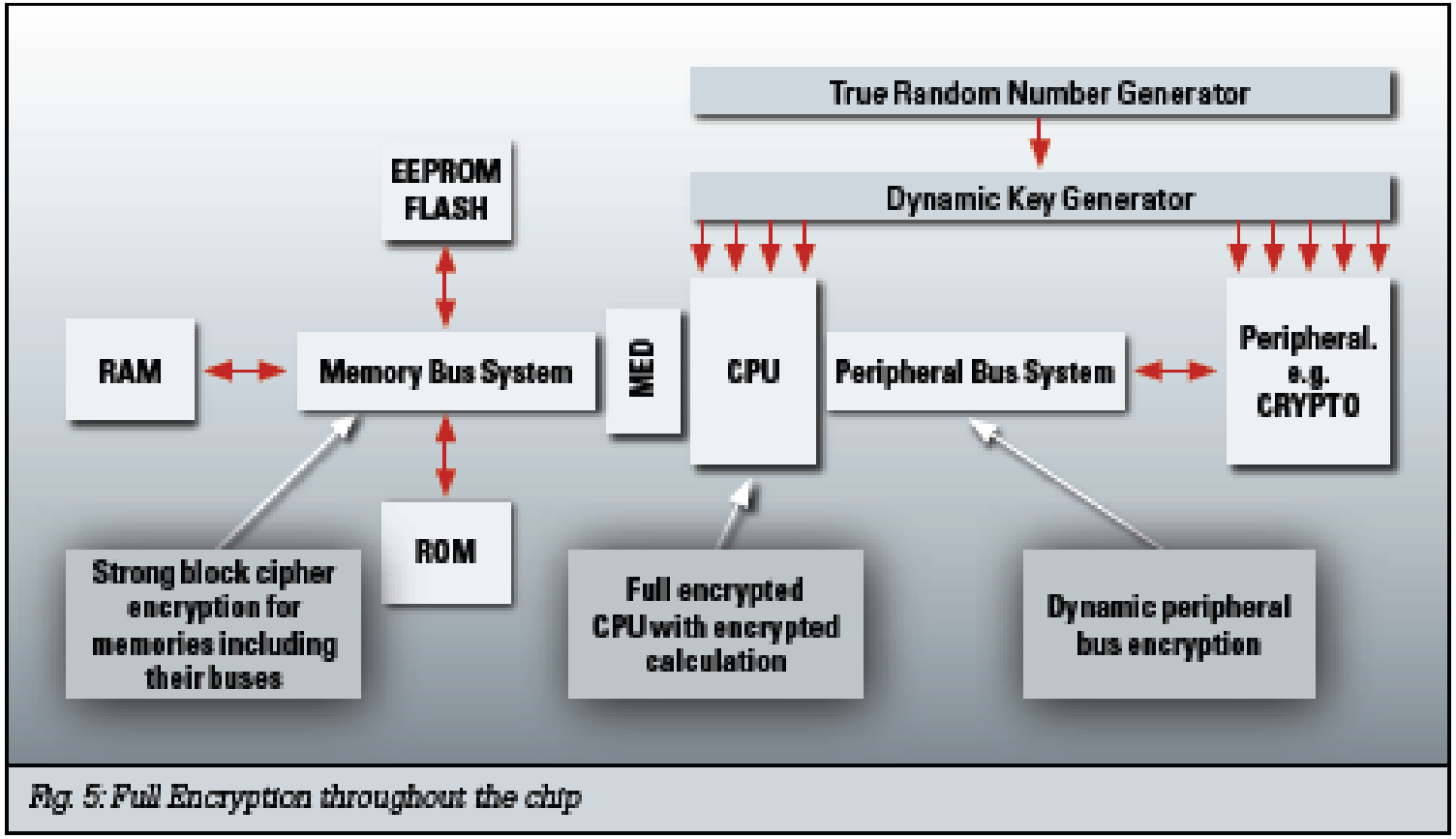


Fig. 5: Full Encryption throughout the chip

- Robust Cryptography possible on constrained systems

Table 7: Estimated time and power consumption for signature generation/verification and key exchange for the client and server side on a TelosB

Cryptosystem	Signature	
	Generation	Verification
RSA-1024	68.97 mWs 5.66 s	2.70 mWs 0.22 s
ECC-160	6.26 mWs 0.52 s	12.41 mWs 1.02 s
RSA-2048	523.10 mWs 42.89 s	12.20 mWs 1.00 s
ECC-224	16.93 mWs 1.39 s	33.55 mWs 2.76 s

Cryptosystem	Key exchange	
	Client	Server
RSA-1024	3.51 mWs 0.29 s	68.97 mWs 5.66 s
ECC-160	6.15 mWs 0.51 s	6.15 mWs 0.51 s
RSA-2048	12.98 mWs 1.06 s	523.10 mWs 42.89 s
ECC-224	16.62 mWs 1.37 s	16.62 mWs 1.37 s

From ref(3) on Intel Core 2 1.83 GHz processor under Windows Vista in 32-bit mode Milliseconds/Operation

RSA 2048 Signature
6.05
RSA 2048 Verification
0.16
ECDSA over GF(p) 256 Signature 2.88
ECDSA over GF(p) 256 Verification 8.53
ECDHC over GF(p) 256 Key-Pair Generation 2.87

Secure MCUs
33MHz

RSA 2K signatures – 1000 fold increase for generation and verification over 16bit TI MSP430 (8Mhz)
ECC 224 signatures – 300 fold increase for generation and verification over 16bit TI MSP430 (8Mhz)

References

- 1) Energy Analysis of Public Key Cryptography for Wireless Sensor Networks, S. Wander, N. Gura et. al.
- 2) Comparing Elliptic Curve Cryptography & RSA on 8 – bit CPUs, N. Gura, A. Patel et. al., CHES 2004
- 3) Crypto++ 5.6.0 Benchmarks, http://www.cryptopp.com/benchmarks.html (on Intel Core 2 1.83 GHz processor under Windows Vista in 32-bit mode)
- 4) Krzysztof Piotrowski, Peter Langendoerfer, Steffen Peter , How Public Key Cryptography Influences Wireless Sensor Node Lifetime, SASN ACM 2006

Intellectual Property

- TF will adopt IETF IPR model
- IETF IP position stated in RFC 3979 ‘Intellectual Property Rights in IETF Technology’
- Task force leadership disclaims responsibility for assessments of the intellectual property status of contributions to this effort
- Expected that contributions accompanied by IP disclosures explicitly stating whether or not contributed materials contain IP
- Contributions without accompanying IP disclosures will be assumed IP encumbered
- All contributions will be voted into the spec., IP encumbered items will be flagged as such during time of vote
- If IP encumbered technology is voted into spec, its expected that owner provide technology under RAND licensing terms

Chairs

- Rohit Khera – rxkw@pge.com
- Daniel Thanos - Daniel.Thanos@ge.com

- Sharepoint

http://osgug.ucaiug.org/utilisec/embedded/default.aspx

- Email Reflector –

'OPENSG-SGSEC-EMBSYSSEC-TF@SMARTGRIDLISTSERV.ORG'

Bi-Weekly Co-ordination and status calls