UCA OpenSG Security: Establishing Industry Secure Device Profiles for the Smart Grid

Rohit Khera, rxkw@pge.com

11/03/2010

Agenda

- Establishing Secure Device Profile – Process Overview
- The Need for Smart Grid Secure Device Profiles
- Why Consider Cryptographic Requirements?
- Discussion of Hardware Acceleration Options
- Discussion of Side Channel Attacks
- Key Provisioning
- High Level Deliverables
- Parking Lot Items

Establishing Secure Device Profiles – Process Overview

A — Establish Regulatory & Standards Landscape

Review state / federal statutory and recommended guidelines relevant to device deployment, security, access control & device management

COMMENTARY

- Some FIPS standards relevant for general purpose rather than embedded computing environments
- Others, e.g. NERC CIP, only address protections for infrastructure subsets such as the bulk electric system

B — Evaluate Feasibility of Recommended Guidelines

Establish Implementation feasibility and cost of NIST/ANSI/NSA/FIPS recommended security protocols within constrained environment

COMMENTARY

- Limited processor, memory & comms link capacity in typical remote sensing and industrial control automation type applications.

C — Assess Communications Systems / Link Constraints

Assess security overhead in relation to wireless carrier capacity / latency. Assess incremental power usage characteristics for battery powered devices

COMMENTARY

- Cryptographic padding schemes and added fields (such as HMAC) can lead to larger message sizes requiring greater carrier data capacity.
- Investigate availability / latency impacts of Key establishment/ hashing/ signing & bulk encryption

D — Assess Device Management Strategies

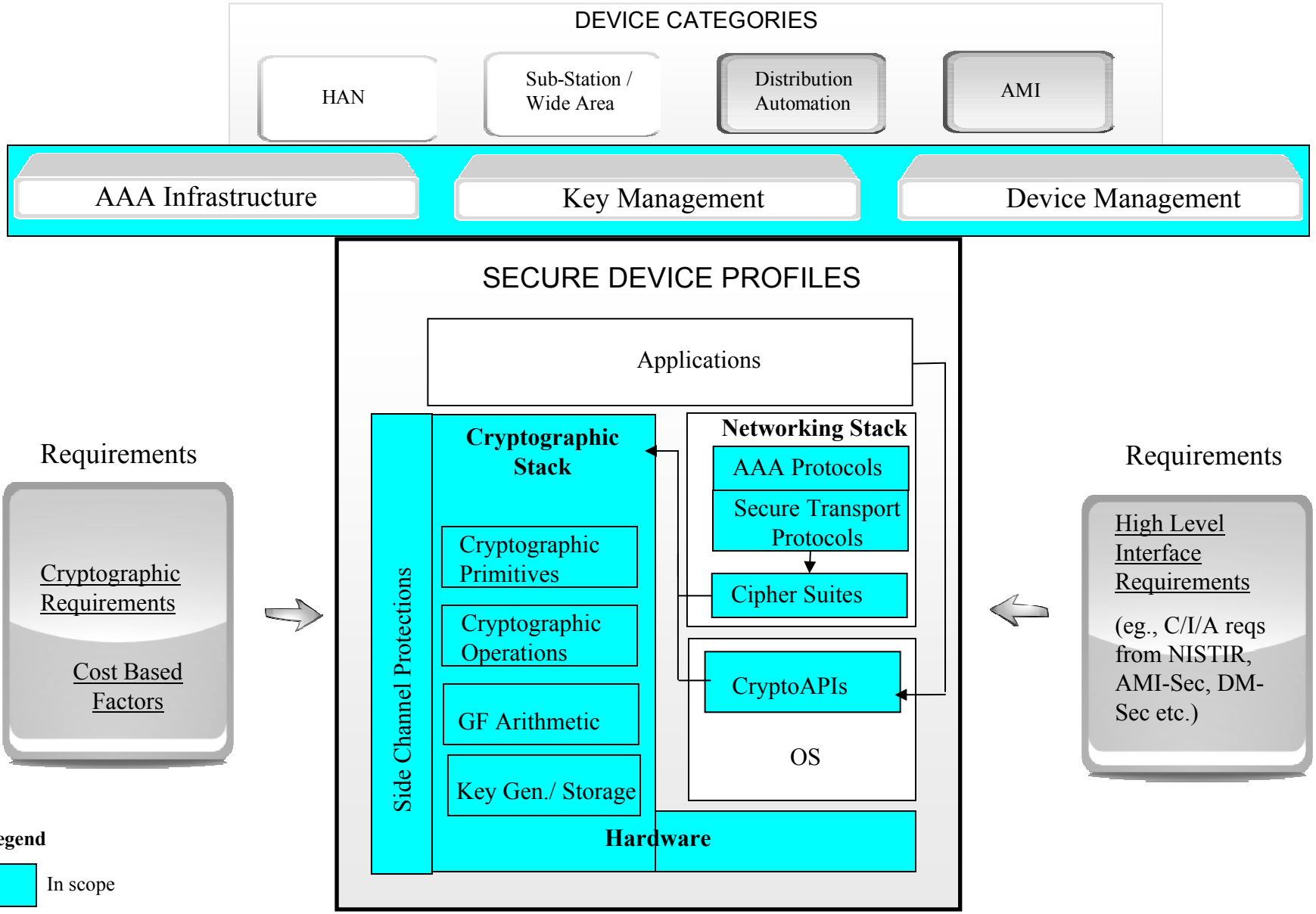
Assess Emerging Device Management technologies

COMMENTARY

- Evaluate if existing IT and device management technologies relevant to general purpose multi-tasking OS'es are applicable to deterministic real time operating system environments connected over low bandwidth networks

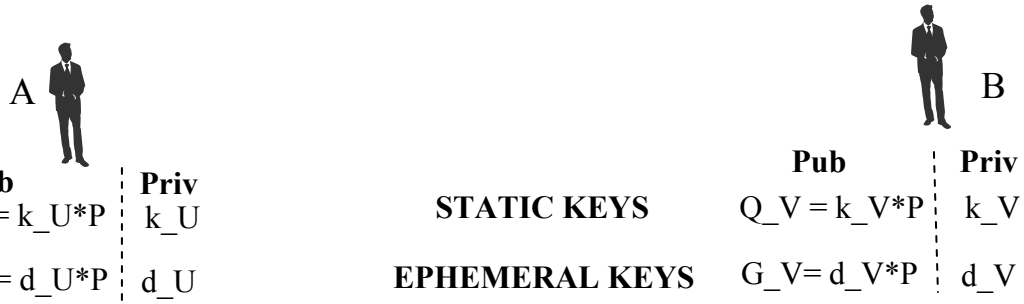
Introducing Secure Device Profiles

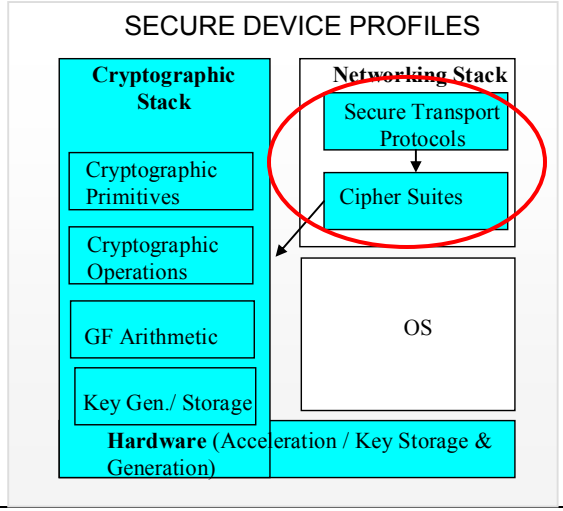
Create multiple secure profiles to address disparate device resource characteristics and communication infrastructures across multiple device categories – leverage existing standards / SDOs



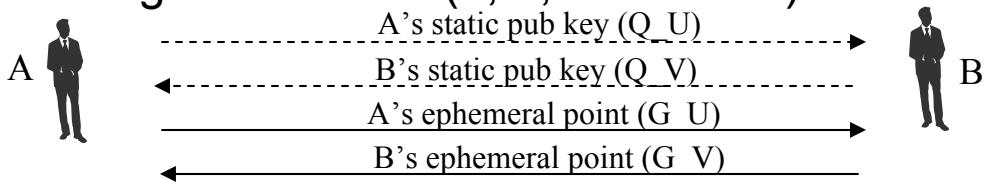
Why Consider Cryptographic Requirements?

Perfect Forward Secrecy, Key Compromise Impersonation Security, Unknown Key Share Security …





Key Exchange Protocol: C(2, 2, ECC CDH)



P = Elliptic Curve Group Base Point

k_U, d_U, k_V, d_V = Scalars

$Z_s = k_U*Q_V = k_U * k_V * P$

$Z_e = d_U*G_V = d_U * d_V * P$

$Z = Z_s \| Z_e$

$Z_s = k_V*Q_U = k_V * k_U * P$

$Z_e = d_V*G_U = d_V * d_U * P$

$Z = Z_s \| Z_e$

Example :KCI

- M sends A an ephemeral point G_V = d_V*P, and B's public key Q_V
- M receives A's public key Q_U and an ephemeral point G_U = d_U*P
- A then computes bitstings Z_s = k_U*Q_V, and Z_e = d_U*G_V and shared secret Z = Z_s || Z_e
- Through knowledge of A's static private key, M can compute
- Z_s = k_U*Q_V and Z_e = d_V*G_U.
- And compute the common shared secret Z = Z_s||Z_e

Why Consider Cryptographic Requirements?

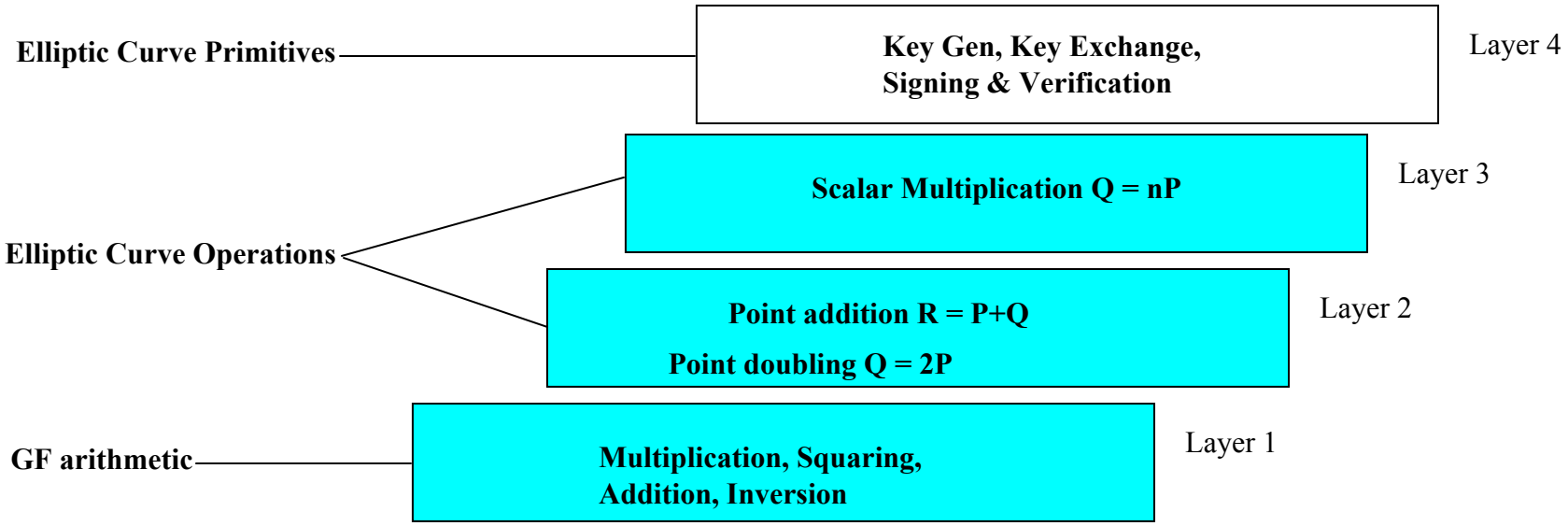
- Secure algorithms necessary but not sufficient – need to address protocol security
- Optionality within specified protocols (eg, IETF, NIST)
- Secure protocols can require additional passes / message exchanges – consider performance / security tradeoffs

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



Multiple ASIC / FPGA based approaches w/ desirable throughput/area characteristics

Legend

Candidate functions for efficient / cost effective hardware implementation

- Differential Power Analysis – utilize statistical correlation to relate specific bits to observed calculation – typically targeting XOR operation between secret keys and temporary data
  - Transition Count Leakage: number of changed bits
  - Hamming Weight Leakage: number of ‘1’ bits being processed
- Timing Attacks – targeting bit wise operations and arithmetic operations

Multiple Mitigation Approaches -

- Constant time algorithms
- Switch gates every clock cycle (regardless of the transmitted data values)

- Symmetric Cryptography
  - Requirements for pairwise symmetric key establishment?
  - Symmetric ‘Needham-Schroeder’ Protocols – eg Kerberos

- Asymmetric Cryptography
  - 802.1AR – Secure Device Identity
  - Require RNG capabilities in the device
  - Supports unique key pairs for distinct security associations

High Level Deliverables/Outputs

- MCUs, chipsets
- Hardware acceleration options
- Hardware based secure key storage & generation options
- Cryptographic primitives, cipher suites & protocols
- Sample cryptographic overhead calculations (hardware dependant)
- Outline of relevant AAA protocols by device category
- Sample power usage analysis
- Key management & provisioning options
- Side channel attack mitigation options
- Cost analysis

Leverage work from existing SDOs

RTOS’es

Software / Firmware Integrity, Formal Methods / Static Analysis

Guidelines for a secure supply chain