UCA Open-SG Security: Embedded Systems Security Task Force Charter

DOCUMENT REVISION HISTORY

Version	Date	Updated By	Description of Changes
0.1	2010.10.15	Rohit Khera	Background Statement
0.2	2010.11.07	Rohit Khera	Scope Statement, Revision to Background Section
0.3	2010.11.19	Rohit Khera	Revisions to Scope Section
0.4	2010.11.21	Rohit Khera	Added Secure Device Profile Diagram and narrative to scope section. Added section on deliverables
1.0	2010.11.30	Rohit Khera	Added section entitled 'Collaboration'
1.1	2010.12.06	Rohit Khera	Incorporated feedback from Mike Ahmadi of GraniteKey and Brad Singletary of Enernex
1.2	2011.01.24	Rohit Khera	Added sections on Device Management, Device Robustness and Random Number Generation
1.3	2011.03.06	Rohit Khera	Updated Secure Device Profile Diagram. Added section on intellectual property rights and assertions relevant to the workings of the task force subsequent to discussion on this topic with Daniel Thanos and Darren Highfill 2/25/2011

1 Background

Significant benefits of the Smart Grid are expected to arise through the deployment of intelligent electronic devices (IEDs) enabling increasing levels of automation and observability of the electric distribution and transmission system as well as the customer premise. The networked, distributed and geographically dispersed nature of these devices raises legitimate concerns around protection, access and control of their critical functions and data. While the overall issue of smart grid security is an expansive subject that spans multiple areas, the scope of work outlined in this document is centered on devices. Traditional approaches to distributed systems security focus on discrete functions around authentication, availability, message confidentiality, integrity and non-repudiation - a consideration of these functions is a legitimate means to examine security requirements related to the deployment of intelligent devices on the grid. An adjacent topic in scope for this effort is the application of PKI in support of authenticated protocols, key agreement / exchange and cryptographic non-repudiation, as well as appropriate key management. Further areas for consideration include hardware and software related topics such as ciphers, cryptographic co-processors, protocols, device identification and authentication.

The proposed designation for this group is ‘Embedded Systems Security’ – the term ‘embedded systems’ warrants a brief definition since it has been stated that the evolution and increasing sophistication of these systems will eventually blur traditional distinctions with general purpose computing architectures. For the purpose of this discussion, the term ‘Embedded System’ refers to a solid state based component incorporating critical control and protection functions – a distinctive aspect of such a component would be its reliance on system features that support the placement of upper bounds on the time required for completion of critical tasks. The remainder of this document shall outline scope and topics for consideration by this task force, and provide a detailed description of proposed deliverables.

2 Goals and Scope

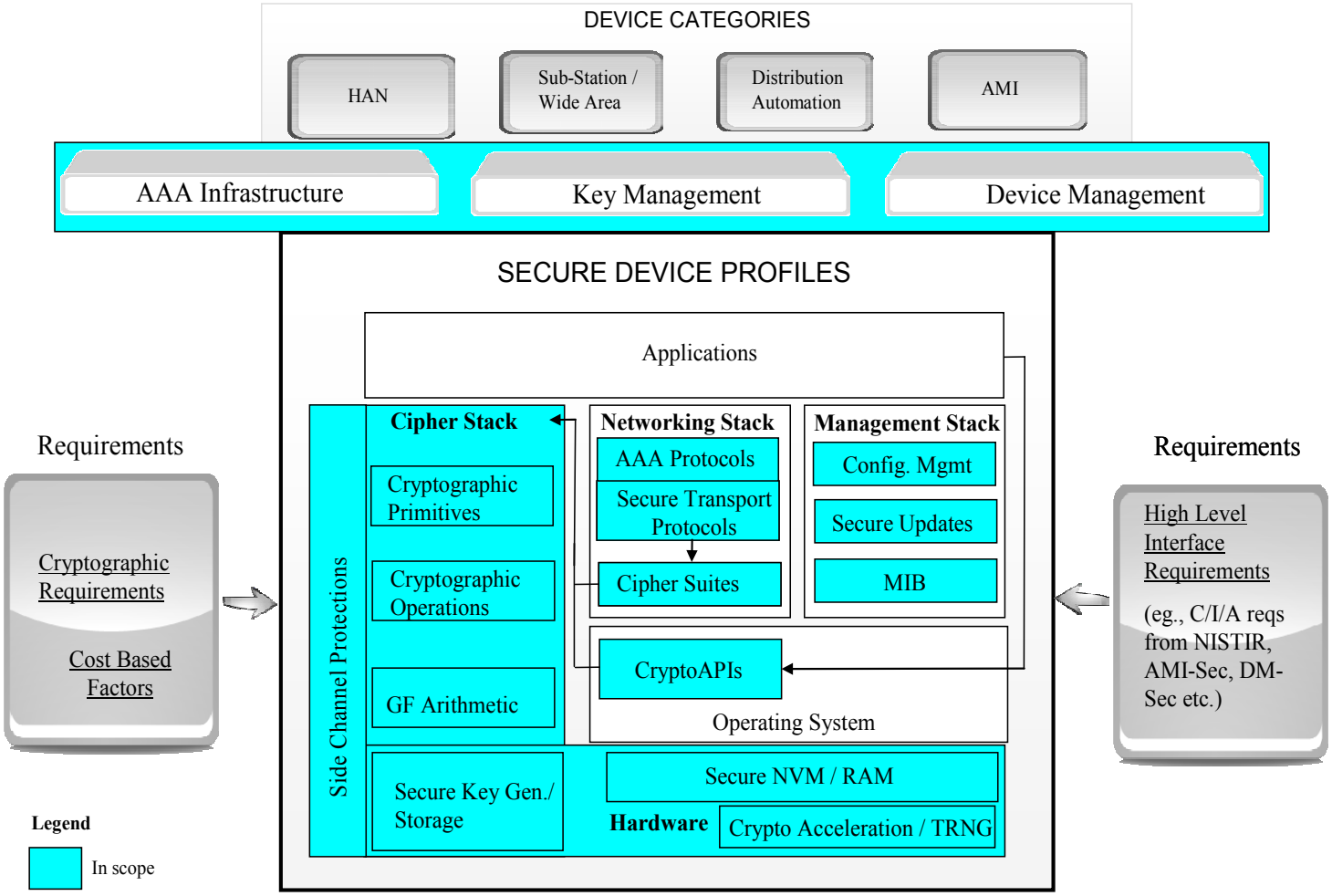
The primary goal of the group is to create multiple 'Secure Device Profiles' addressing the main smart grid domains. These domains identified for this effort are:

1) Distribution
2) Wide Area
3) Sub Station
4) Infrastructure Edge
    - AMI
    - Home Area

It is intended that the final work product contain multiple device profiles for the identified smart grid domains. This is motivated due to the fact that devices in the wide area, distribution and home settings operate under distinct computational resources, constraints and available channel bandwidth requiring tailored profiles to accommodate specific device operating characteristics.

2.1 Secure Device Profiles

The following diagram provides a representation of profiles targeted for this effort:



2.2 Secure Device Profile Components

2.2.1 Cryptographic Hardware

The emergence of cost effective hardware targeted at cryptographic operations offers the possibility for device manufactures to incorporate purpose-built hardware for cryptographic acceleration, random number and key generation, and secure storage of cryptographic materials. The profiles will provide guidance related to the usage and applicability of such hardware for the device types under consideration. They will also address specific design considerations and vulnerabilities associated with the use of such mechanisms –there is a significant amount of work around the design of secure integrated circuits for smart cards and related applications – it is intended to leverage this work to the extent possible. An additional topic for consideration would be specification of standard APIs for applications and software components to access underlying hardware based security functions.

2.2.2 Ciphers

The profiles will provide guidance around cryptographic requirements and FIPS approved ciphers relevant to devices in the identified smart grid domains. The intent is to leverage existing standards around the specification of cryptographic primitives and protocols, such as those specified by standards organizations such as NIST, NSA, IETF and ANSI. In addition, the profile will provide guidance related to the size and relative performance of cryptographic primitives in order to facilitate choices consistent with a device's computational resources, channel bandwidth and availability requirements

2.2.3 Random Number Generation

Since the generation of random numbers is critical for the purposes of creating cryptographic keys on a device, guidance around entropy sources and various mechanisms for true and deterministic random number generation relevant to a constrained device operating environment will be provided

2.2.4 Side Channel Attacks & Mitigation

The profiles will describe typical attacks exploiting hardware and algorithmic characteristics of cipher implementations including power analysis and timing based attacks and the relevance of such attacks to devices within the identified smart grid domains. The profile will also discuss protections that could be employed in order to increase complexity and required resources to successfully mount such attacks

2.2.5 Secure Protocols

The profiles will discuss secure transport and inter-network level protocols to secure communications and provide guidance around the applicability of such protocols to devices in the identified domains. The intent is to address internet and non-internet protocol based communications.

2.2.6 Device Identity

The profiles will address cryptographic mechanisms to associate unique identifying characteristics to a device and provide guidance on protections associated with securing a device's indentifying characteristics. The profiles will also provide guidance around appropriate milestones in the device production, deployment and commissioning lifecycle for provisioning device identifying characteristics.

2.2.7 Device Authentication & Access Control

The profiles will address protocols related to authenticating devices on communication networks and tradeoffs associated with centralized and federated authentication mechanisms, also discussing the applicability of various authentication mechanisms to the classes of devices under consideration.

2.2.8 Device Robustness and Resilience

The intent of this section is to discuss hardware and software related architecture principles related to device robustness and resilience, provide guidance around resistance to denial of service types of attacks (eg. interrupt coalescing and CPU resource conservation) and protocol implementation guidelines.

2.2.9 Key Management

The profiles will provide guidance around management of cryptographic keys

2.2.10 Device Management

The profiles will define a minimal set of security related events generated by the device for the purpose of security event monitoring and correlation. This section will also provide general guidance in the area of managing secure firmware upgrades and updates to device configurations and settings.

2.3 Leverage Existing Standards

Significant aspects of the enumerated secure device profile components can be addressed by leveraging industry work and standards from existing organizations such as NIST, ANSI and the IETF (not an exhaustive list) – it is intended to leverage existing standards to the greatest extent possible and create tailored profiles to address unique device operating characteristics, computational resources and channel bandwidth within the identified smart grid domains.

2.4 Collaboration

Since the topic of embedded systems security requires consideration of device communication capabilities and protocols, it is anticipated that the group will collaborate with the SG-Communications subgroup within UCA OpenSG in order to help identify and promote communications architectures and protocols required for specifying robust security functions in the devices under consideration. It is also intended that the group collaborate with the OpenHAN initiative, NIST CSWG and the Dept. of Homeland Security Industrial Control Systems Joint Working Group

3 Deliverables

The following is a list of proposed deliverables around the specification of Secure Device Profiles. The essential components of the profiles are described in section 4 'Secure Device Profiles – High Level Overview'. Subsequent sections are intended to provide further detail around components identified in section 4.

4 Leadership

Co-chairs: Rohit Khera, Pacific Gas & Electric Co., Daniel Thanos, GE Energy Services

Secretary: TBD

5 Voting and Overall Process

Participants are granted voting rights in accordance with the rules set forth in the Operating Procedures for OpenSG Technical Committee Section 9.2 Working Group and Task Force Voting (http://osgug.ucaiug.org/default.aspx). Voting privileges are contingent upon membership in UCAIug (http://www.ucaiug.org/Pages/join.aspx) and meeting the attendance requirements. The SG Security WG officers will track attendance in group meetings in order to establish a member's voting rights. Only one vote may be cast per entity. Valid votes are as follows:

- YES
- YES with comments
- NO with comments
- ABSTAIN

The work product vote must achieve a quorum (50% of eligible voters casting votes) with a 2/3 majority of cast votes in favor to pass. ABSTAIN votes will not count toward the 2/3 majority calculation.

If the vote passes, comments received with YES votes shall be resolved prior to publication of the work product if and only if they are strictly editorial in nature. All comments received in the voting process with substantive technical impact shall be noted, retained in a separate document, and handled in a future revision of the work product. Approved versions of work products shall contain no comments or mark-up.

5.1.1 Voting Eligibility

To qualify to vote, an entity must be a member in good standing in the UCA International Users Group as of the call for vote and must have representation at 3 of the previous 5 Task Force meetings.

5.1.2 Overall Process

Voting and voting eligibility is described in the sections above. Other items related to the overall working process of the group will draw from existing process defined for listservs, document management, meetings and participation defined in the UCA OpenSG-Security working group charter 1.0.

6 Intellectual Property

The creation of secure device profiles as outlined in sections 2 and 3 of this document require a level of detailed technology specification that necessitates elucidating a position around the incorporation of intellectual property in the body of work.

The task force shall adopt an approach to intellectual property similar to what is found in the workings of the Internet Engineering Task Force (IETF) as outlined in RFC 3979 'Intellectual Property Rights in IETF Technology'.

Task force leadership disclaims all responsibility related to an assessment of the intellectual property status of contributions to this effort. It is expected that all parties contributing toward the specification of device profiles disclose any intellectual property contained within their work. All contributions to the work without an accompanying disclosure around the intellectual property status of the contributions will default under the assumption that the contributions are IP encumbered, i.e., that they contain intellectual property. This will be duly noted as the work is voted upon for incorporation into the profiles. Based on the outcome of the vote, such contributions may or may not be incorporated into the final body of work. It is conceivable that the task force vote in aspects of work that are known to contain intellectual property if such is deemed necessary for specification of the profiles. In this case, it is expected that the IP owner undertake to provide it under RAND licensing terms (Reasonable and Non- Discriminatory).