Issues and Challenges in Provisioning Keys to Smart Objects

Yoshihiro Ohba, Toshiba Corporation
Subir Das, Telcordia Technologies Inc.

In this position paper, we first describe several issues related to key provisioning for smart objects that require further investigations, highlight additional work that may be needed in IETF and then we discuss a Smart Grid use case where we are implementing provisioning of session keys using techniques such as Single Sign On (SSO).

1. Provisioning Authentication Credentials

Smart objects may be manufactured and placed at their intended locations without pre-provisioning authentication credentials (e.g., symmetric or asymmetric keys and identities about key holders) specific to a particular service provider. While for today's service provider-based model (e.g., SIM for cellular providers, Modem for ISPs), pre-provisioning of authentication credentials was not an issue, this is a problem for other emerging use cases where the smart objects may need to be placed before determining their service providers . Moreover, these objects are constrained in terms of memory, power, cost and location where they are placed. In another scenario, the smart objects may change their service providers in the same or a new location. In this use case, new authentication credentials need to be provisioned to smart objects for network access service or application service providers. This is commonly known as re-commissioning and is different from roaming commonly used in cellular networks. For these use cases, an automated remote key provisioning feature would be essential considering that the smart objects installed places may not be physically accessible by humans.

While the IETF Enroll WG was chartered to design an enrollment model but it concluded without producing an outcome before its new demands for smart objects emerge. Dynamic Symmetric Key Provisioning Protocol (DSKPP) [1] defines a key provisioning protocol over reliable transport for provisioning symmetric keys. DSKPP currently supports HTTP/1.1 as its transport. Also Key Management Interoperability Protocol (KMIP) [2] defines key management protocol including asymmetric or

symmetric key provisioning. However, the currently defined transports of DSKPP or KMIP will not work if automated enrollment needs to happen before network entry. To address this problem, for example, a transport protocol for DSKPP or KMIP that works over EAP may be needed.

2. Provisioning Session Keys

For smart objects, it is important to reduce the computational cost as well as the number of message exchanges required for performing peer authentication to provide session keys (a.k.a. ciphering keys) for multiple protocols within a particular layer or across multiple layers ranging from link layer to application layer in order to provide cryptographic protections for the protocols. For example, if an electric meter or a gas meter which is a low processing power device with personal area wireless network technology (e.g., IEEE 802.15.4) has to perform link layer authentication for network access and then execute peer authentication at each higher layer for multiple applications, the device would require more resources and the number of message exchanges over the air will increase. We believe that a Single Sign-On (SSO) mechanism is more appropriate in these scenarios and argue that the most optimized use case of SSO is to integrate network access authentication with peer authentication when network access provider and service providers are same or has business relationship. The security model of ongoing ETSI M2M [3] work proposes the similar concept by the use of key hierarchy generated from a successful authentication either at the network registration or at the service registration level. IETF has defined these keys hierarchies: EAP-generated key hierarchy (a.k.a. EMSK key hierarchy) [4] and TLS-generated key hierarchy (a.k.a., TLS extractor) [5]. It would be useful to have the investigations on SSO for smart objects including requirements done in IETF and then understand if any protocol changes would be required for these environments.

3. Provisioning Group Keys

Smart objects in many scenarios will form a group and will be connected to the Internet via a gateway node. All nodes in that group will use a group communication protocol. A group key for such communications must be securely distributed to the current members of the group both during initial key distribution and subsequent key update. Protocols designed for group key management such as GDOI [6], GSAKMP [7] and MIKEY [8] may be used for group key distribution. Alternatively, key wrap attributes for securely encapsulating group key may be defined in network access authentication protocols such as, PANA [9] and EAP-TTLSv0 [10]. Considering the fact that smart

objects are resource-constrained devices, further investigations are needed for developing more efficient group key management mechanisms or protocols to support group key distribution for a large number of smart objects. For example, the key management scheme based on broadcast encryption such as, [11] can be considered as a candidate group key management mechanism suitable for smart objects since broadcast encryption puts no restriction on how the key is distributed and there is no requirement on key transport security.

4. Experimenting SSO for AMI Networks

We developed an EAP-based SSO mechanism that will be used for a pilot project in AMI (Advanced Metering Infrastructure) networks.

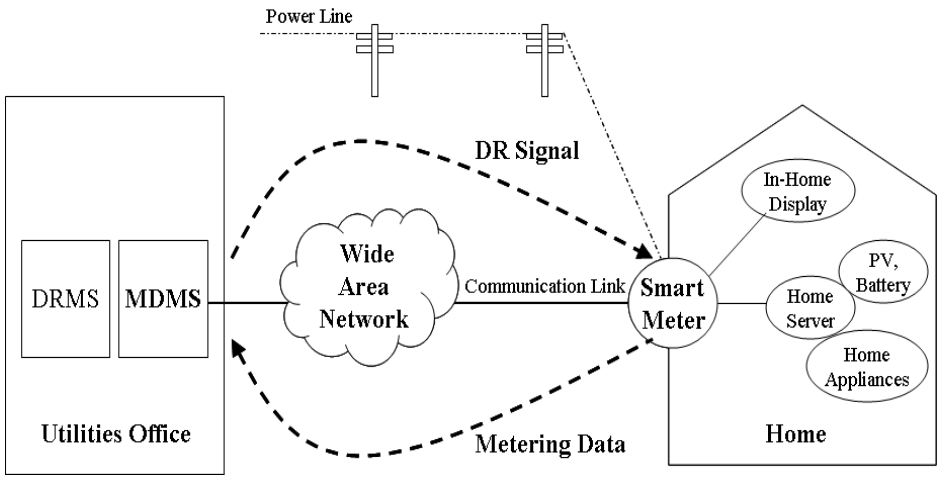

Figure 1 Basic Components of AMI System

A basic AMI system architecture and its components are shown in Figure 1. The smart meter installed in the consumer's house pushes the metering data to the Meter Data Management System (MDMS) in the utility office or the MDMS pulls the metering data from the smart meter. The smart meter could also receive the Demand Response (DR) signal from the MDMS or from the Demand Response Management System (DRMS) via the MDMS. In addition, the smart meter may communicate with the in-home display to show the consumer's energy usage and the home server to coordinate the energy usage in the home.

The smart meter will communicate with the MDMS via public Wide Area Network (WAN) which is probably the Internet for the exchange of the DR signal and the metering data. We are using ANSI C12.22 as an application protocol between the MDMS and the smart meter. ANSI C12.22 provides security mechanism but it lacks from dynamic key management (re-keying) mechanism. In addition, the network access authentication is required in the Neighborhood Area Network (NAN). In order to fulfill these requirements, we apply the architecture as shown in Figure 2

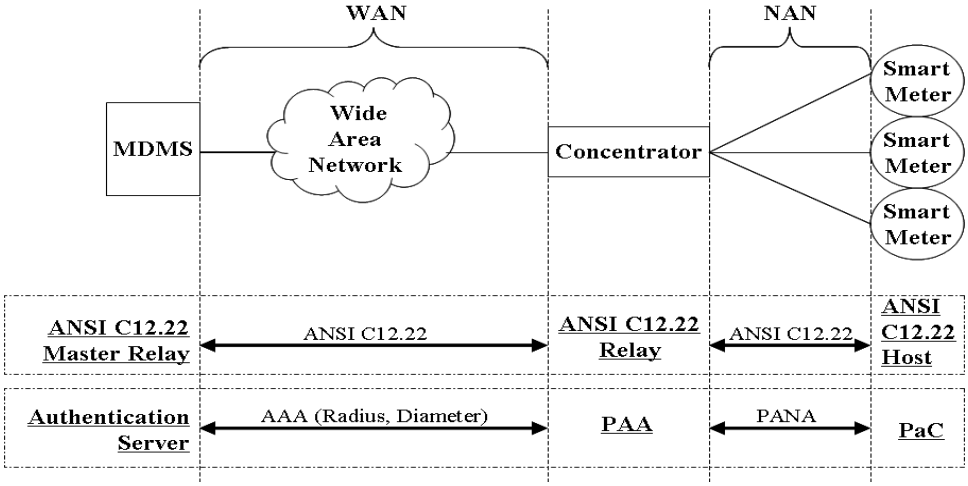

Figure 2 Architecture and Functional Mapping

For our experiment, we use PANA for the network access authentication for the NAN between the concentrator and the smart meter. The concentrator acts as an ANSI C12.22 Relay and PANA PAA (PANA Authentication Agent), and the smart meter acts as an ANSI C12.22 Host and PANA PaC (PANA Client).

The outline of the authentication and key establishment procedures of this model is described below:

- The smart meter starts PANA negotiation with the MDMS at bootstrapping. PANA is used for EAP transport.
- The smart meter shares the ANSI C12.22 ciphering key with the MDMS after EAP authentication is succeeded. The key is generated from EAP EMSK.
- When re-key of ANSI C12.22 ciphering key is needed, EAP re-authentication will be carried out as part of PANA re-authentication before expiration of the ANSI C12.22 ciphering key.

We have started implementing the proposed architecture and functional components for

our test environment. We implemented EAP and PANA on embedded devices with different types of microprocessors including Toshiba TLCS-900. We expect to have test results in near future.

5. References:

[1] A. Doherty, et. al., “Dynamic Symmetric Key Provisioning Protocol (DSKPP),” RFC6063

[2] http://docs.oasis-open.org/kmip/spec/v1.0/cs01/kmip-spec-1.0-cs-01.pdf

[3] “Machine- to- Machine communications (M2M); Functional architecture” Draft ETSI TS 102 690 V 0.9.7, 2010-12

[4] J. Salowey, et al, “Specification for the Derivation of Root Keys from an Extended Master Session Key (EMSK)”, RFC5295

[5] E. Rescorla, **“**Keying Material Exporters for Transport Layer Security (TLS)**,** RFC5705

[6] M. Baugher, et . al., “The Group Domain of Interpretation” RFC3547

[7] H. Harney, et. al., “GSAKMP: Group Secure Association Key Management Protocol” , RFC4535

[8] J. Arkko, et. al., MIKEY: Multimedia Internet KEYing”, RFC3830

[9] Y. Ohba ed. “Protocol for Carrying Authentication for Network Access (PANA)”, RFC5191

[10] B. Funk and S. Blake-Wilson, “Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)” RFC5281

[11]http://www.aacsla.com/specifications/specs091/AACS_Spec_Common_0.91.pdf