Credentials for Smart Objects: A Challenge for the Industry

Alper Yegin
Samsung Electronics
Workshop on Smart Object Security
March 23, 2012
Paris

One of the most challenging areas about designing smart objects and their networks is security. On one hand, smart objects can be extremely constrained -- low processing and battery power, low memory, lack of user a interface. On the other hand, this cannot be an excuse for them to have less security than any other device on the Internet. Smart objects can be assuming very critical roles, such as monitoring as part of a home security system, or controlling as part of an intelligent transportation system. Compromise of such devices can be more catastrophic than compromise of a typical device on the Internet, such as a PC, or a mobile phone.

Security design begins with the selection of credential types. These are the credentials that will be used by the smart objects for getting authorized for network-layer access and then for application-layer access. Certificates, id/password pairs, and UICCs are the possible choices being considered in the industry. Each one of these credential types has their own advantages and disadvantages. Id/password pairs are relatively light-weight when considered in small deployments, yet managing them in large numbers is not practical. Certificates provide a robust and well-established solution for large-scale deployments, but their added cost and dependency on third parties (CA vendors) are concerning to the service providers. UICCs are attractive, especially to 3GPP operators, but they are applicable to only a subset of deployments. Furthermore, they add to the cost of smart objects.

The procedure to provision the devices with such credentials depends on the type of the credential. Id/password pairs can be provisioned by the manufacturer and passed on to the service provider who would be managing the devices. Certificates can be provisioned by the manufacturer, and optionally overwritten by the service provider with another certificate. In addition to the device certificate, one or more root CA certificates need to be provisioned on the device as well. Selection of the Root CA vendor is an issue for the device manufacturer, as the same selection shall also be made by the service providers using those devices. Devices changing service providers may require re-provisioning procedure, which also impacts the choice of credential type. For example, id/password-based credentials cannot be kept the same once the device changes hands.

It appears very difficult for the industry to agree on one type of credential type for all sorts of deployments. It is expected that fragmentation similar to the one in general Internet will be seen for the smart objects, and application-specific (i.e., vertical) profiling will be needed in order to narrow down the possibilities and achieve interoperability. As an example, ETSI M2M Architecture [1][2] supports a variety of credential types – X.509 certificates, PSKs, UICCs, and anything that can be supported by an EAP method.

Secure service provider discovery and service-specific provisioning is another challenge. Lack of a human user behind the device and difficulty in pre-configuring large number of devices make it difficult for device-initiated discovery and selection mechanisms. There is no equivalent of a user interfacing with the device to select an SSID, operator ID, etc. On the other hand, network-initiated discovery and selection mechanism leads to device ownership problems (i.e., how would the device know that it shall really be used by that particular service provider contacting it?).

Dealing with one set of credentials is already difficult. Dealing with multiple credentials due to the separation of network access service and application access service is even harder. Therefore, using the same credential for both types of access seems unavoidable. Furthermore, single sign on schemes are being considered as additional optimization tools. As an example, ETSI M2M Architecture supports use of UICC for both the network-layer and application-layer access.

Architecturally, the network access service provider (e.g., 3/4G, fixed broadband operator) and the application service provider who manages the devices for a specific use (e.g., smart grid) don't have to be the same. Nevertheless, former type sees this as an opportunity to expand its business, hence prepares to act as an integrated service provider. Some of the designs are getting influenced by that aspect (e.g., use of UICC for both of the services).

Finally, smart objects are expected to surround our daily lives. Our activities will be closely monitored and reported by them. Unless proper measures are put in place, our personal privacy will be in a much bigger danger than before. Hiding the real identities from neighboring elements and even intermediaries will be essential. Achieving a water-proof solution for the constrained smart objects presents itself as another challenge.

These are some of the fundamental challenges faced by the smart object architecture designers.

References

[1]http://www.etsi.org/deliver/etsi_ts/102600_102699/102690/01.01.01_60/ts_102690v010101p.pdf
[2]http://www.etsi.org/deliver/etsi_ts/102900_102999/102921/01.01.01_60/ts_102921v010101p.pdf