Background on SKSML

The OASIS Symmetric Key Services Markup Language (SKSML) is the proposed XML-based protocol that defines how a client may request and receive symmetric encryption cryptographic keys, securely, from a key-management service on a network. Clients may consist of:

- Computerized devices such as Personal Digital Assistants (PDA), telephones, laptop, desktop and server-class computers;
- Applications such as office productivity, database, e-commerce, healthcare, financial or other applications; and/or
- Devices such as routers, printers, disks, tape-drives, etc.

Symmetric encryption cryptographic keys currently supported by SKSML include keys based on the Triple Data Encryption Standard (3DES) and the Advanced Encryption Standard (AES).

Background on Mobile Phones

Mobile phones are the most widely deployed computerized device in the world. Their capabilities continue to grow every year, with the current crop out-classing desktop-computer devices of five years ago with built-in features such as WiFi, music-playing, cameras, web-browsing and a wealth of new applications designed for such phones.

However, the non-WiFi bandwidth of mobile-phones continues to remain a bottle-neck, thus requiring that applications constrain system-level downloads/transactions as much as possible. Additionally, the life of the battery on the phone is directly proportional to the CPU processing of the mobile phone – thus requiring minimizing system-level processing where possible.

The growth of new applications on smart-phones, and their significant storage capabilities, is creating a need for securing sensitive data and transactions on the phones through encryption. This requires a network-wide key-management service along the lines of a Symmetric Key Management System (SKMS), as outlined by the OASIS EKMI Technical Committee. And, while it seems that SKSML is a perfect fit for this requirement, this is not feasible in its current form.

Problems with the current form of SKSML for mobile phones

SKSML is designed to cater to a wide variety of business use cases for all classes of computers and applications in an enterprise. However, SKSML – in its current form – is not a perfect fit for mobile phones because:

- SKSML is fairly verbose. Mobile phones will drain their battery charge faster with heavy XML-parsing;
- SKSML payloads are heavy with signed and encrypted messages for every request and response. Mobile phones will need to download and upload larger payloads that choke a carriers’ bandwidth and frustrate customers with real/perceived slowness; and
- SKSML does not fit in with the most popular messaging format for mobile-phones: Short Message Service (SMS).

Proposal

It is proposed that a sub-committee be created within the EKMI TC to define a profile of SKSML for mobile phones to address the above-mentioned short-comings. The “Mobile SKSML” sub-committee will focus on the following:

- Create a compact version of SKSML catering specifically to the constrained mobile-phone environment that can be serviced by the same SKMS as for the enterprise;
- Maintain equivalent security requirements for the messaging protocol so that the authenticity, data-integrity and confidentiality of the payloads are not compromised;

In all other respects, the “Mobile SKSML Sub-committee will operate on the same rules/procedures of the OASIS EKMI TC.