Name
Enterprise Key Management Infrastructure TC (EKMI-TC)

Statement of Purpose
Public Key Infrastructure (PKI) technology has been around for more than a decade, and many companies have adopted it to solve specific problems in the area of public-key cryptography. Public-key cryptography has been embedded in some of the most popular tools – web clients and servers, VPN clients and servers, mail user agents, office productivity tools and many industry-specific applications - and underlies many mission-critical environments today. Additionally, there are many commercial and open-source implementations of PKI software products available in the market today.

However, many companies across the world have recognized that PKI by itself, is not a solution. There is also the perception that most standards in PKI have already been established by ISO and the PKIX (IETF), and most companies are in operations-mode with their PKIs – just using it, and adopting it to other business uses within their organizations. Consequently, there is not much left to architect and design in the PKI community.

Simultaneously, there is a new interest on the part of many companies in the management of symmetric keys used for encrypting sensitive data in their computing infrastructure. While symmetric keys have been traditionally managed by applications doing their own encryption and decryption, there is no architecture or protocol that provides for symmetric key management services across applications, operating systems, databases, etc.

While there are many industry standards around protocols for the life-cycle management of asymmetric (or public/private) keys – PKCS10, PKCS7, CRMF, CMS, etc. - however, there is no standard that describes how applications may request similar life-cycle services for symmetric keys, from a server and how public-key cryptography may be used to provide such services.

It is the contention of the author(s) of this TC charter, that key-management needs to be addressed by enterprises in its entirety – for both symmetric and asymmetric keys. While each type of technology will require specific protocols, controls and management disciplines, there is sufficient common ground in the discipline justifying the approach to look at key-management as a whole, rather than in parts. Therefore, this TC will address the following:
Scope

A) The TC will define the request/response protocols for:
   1. Requesting a new or existing symmetric key from a server;
   2. Requesting policy information from a server related to caching of keys on the client;
   3. Sending a symmetric key to a requestor, based on a request;
   4. Sending policy information to a requestor, based on a request;

B) To ensure cross-implementation interoperability, the TC will create a test suite that will allow different implementations of this protocol to be certified against the OASIS standard (when ratified);

C) The TC will provide guidance on how a symmetric key-management infrastructure may be secured using asymmetric keys, using secure and generally accepted practices;

D) Where appropriate, in conjunction with associate standards organizations that focus on disciplines outside the purview of OASIS, the TC will provide input on how such enterprise key-management infrastructures may be managed, operated and audited;

E) It will focus on activities that promote securing sensitive data with appropriate cryptography, and the use of proper key-management techniques and disciplines to ensure appropriate protection of the infrastructure. The TC will do this through educational vehicles such as: white papers, seminars, websites, samples, newsgroups for discussions, etc.

List of Deliverables

1. XSchema Definitions (XSD) of the request and response protocols;
2. A Test Suite that allows for clients and servers to be tested for conformance to the defined protocol;
3. Documentation that explains the communication protocol;
4. Documentation that provides guidelines for how an EKMI may be built, operated, secured and audited;
5. Resources that promote enterprise-level key-management: white papers, seminars, websites, samples, newsgroups for discussions, etc.
Anticipated Audience

Any company that has a need for managing cryptographic keys across applications, databases, operating systems and devices, yet desires centralized policy-driven management of all cryptographic keys in the enterprise. Retail, health-care, government, education, finance – every industry has a need to protect the confidentiality of sensitive data. The symmetric key services protocol will provide an industry standard for protecting sensitive information across these, and other, industries.

All current members of the PKI-TC should be very interested in this new TC, since the goals of this TC overlap the charter of the PKI-TC.

Language

English

IPR Policy

Unlimited use, Royalty Free

[[Non-normative information regarding the startup of the TC, which includes:]]

a. **Identification of similar or applicable work**: To the best of my knowledge, there is no other similar work being carried on in this arena, either within or outside OASIS. However, this TC intends to leverage many OASIS (Web Services Security) and W3C standards (XMLSignature, XMLEncryption) for the creation of the new protocol;

a. **List of contributions of existing technical work**: StrongAuth anticipates providing a DRAFT proposal for the protocol, at the inception of the TC;

a. **Proposed working title and acronym for specification**: Symmetric Key Services Markup Language (SKSML);

a. **Date, time, and location of the first meeting**: First meeting will potentially be in September/October 2006. StrongAuth will be pleased to host this meeting in the San Francisco Bay Area region. If it is infeasible for participants, then the meeting can also be held over the phone.

a. **Projected meeting schedule**: Monthly meetings for the first year. First version of the protocol to be voted on by Spring 2007.
b. Names, electronic mail addresses, of supporters:
   a. Arshad Noor – arshad.noor@strongauth.com
   b.
   c.
   d.
   e.

c. The name of the Convener, and the name of the proposed Chair(s), who must be Eligible Persons.
   a. Arshad Noor (proposed chair)
   b.