OASIS Enterprise Key Management Infrastructure (EKMI) Technical Committee

Name

OASIS Enterprise Key Management Infrastructure (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.

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 create use-case(s) that describe how and where the protocols it intends to create, will be used;

B) The TC will define symmetric key management protocols, including those 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;
5. Other protocol pairs as deemed necessary.

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

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

E) Where appropriate, and in conjunction with other 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;

F) The TC may conduct other activities that educate users about, and promote, securing sensitive data with appropriate cryptography, and the use of proper key-management techniques and disciplines to ensure appropriate protection of the infrastructure.

List of Deliverables

1. XSchema Definitions (XSD) of the request and response protocols (by August 2007)
2. A Test Suite of conformance clauses and sample transmitted keys and content that allows for clients and servers to be tested for conformance to the defined protocol (by December 2007)
3. Documentation that explains the communication protocol (by August 2007)
4. Documentation that provides guidelines for how an EKMI may be built, operated, secured and audited (by December 2007)
5. Resources that promote enterprise-level key-management: white papers, seminars, samples, and information for developer and public use. (beginning August 2007, continuing at least through 2008)

Anticipated Audiences:

Any company or organization 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 TC's deliverables will provide an industry standard for protecting sensitive information across these, and other, industries.

Security services vendors and integrators should be able to fulfill their use cases with the TC's key management methodologies.

Members of the OASIS PKI TC should be very interested in this new TC, since the goals of this TC potentially may fulfill some of the goals in the charter of the PKI TC.

Language:

English

IPR Policy:

Royalty Free on Limited Terms under the OASIS IPR Policy

TOP

Standards Committees Join News Events Resources Member Sections Policies About

Other sites:
Cover Pages

OASIS Chinese
OASIS Japanese
XML.org

Help us improve OASIS: Send us **feedback!**

Member Sections:
AMQP
Blue
CGM Open
eGov
Emergency
IDtrust
LegalXML
Open CSA
WS-I

XML.org Focus Areas:
BPEL
DITA
ebXML
IDtrust
OpenDocument
SAML
UBL
UDDI