

SYMMETRIC KEY SERVICES MARKUP LANGUAGE (SKSML)

AULA MAGNA. FACULTAT DE DRET

26 d'octubre, 16:00 a 19:00 h

For over two decades, companies have been focused on protecting the perimeter through the use of firewalls, intrusion prevention systems and other access control mechanisms. A few very risk-averse institutions - primarily in the financial and defense sectors - went beyond perimeter-protection and encrypted data at rest, in transit and even while in use. This hard exterior and soft center of the vast majority of companies now haunts the industry as one company after another divulges breaches to sensitive customer data in every consumer-focused sector - financial, retail, healthcare, education and government.

Securing the core - the data - through enterprise-wide encryption has not been an option for most companies due to the lack of standards in symmetric key-management. While asymmetric key-management has a plethora of standards (thank you PKIX), symmetric key-management has suffered from a woeful lack of attention. Until now.

OASIS - the Organization for the Advancement of Structured Information Systems - has taken up the gauntlet and created an Enterprise Key Management Infrastructure Technical Committee (OASIS EKMI TC) with four goals:

1. To standardize on Symmetric Key Services Markup Language (SKSML) - a secure network-based web-service protocol for client applications to request key-management services of a network-based server, much as DNS and DHCP clients request services of their respective servers;
2. To create Implementation and Operations Guidelines for the creation of enterprise-scale EKMI, typically consisting of a Public Key Infrastructure (PKI) for asymmetric key-management, and a Symmetric Key Management System (SKMS) for symmetric key-management;
3. To create Audit Guidelines for Information Security Auditors to audit EKMI's. This goal is being accomplished with the support of members from ISACA - the Information System Audit and Control Association;
4. To create an interoperability test-suite for conformance testing of SKSML implementations.

In this session, you will hear of an architecture and see an open-source implementation of an SKMS implementing the proposed SKSML standard. You will understand how to secure your data across the entire enterprise, while controlling access to its decryption keys from a single focal point. You will hear of the developments at OASIS and determine for yourself why companies like Visa, Wells Fargo, the US Department of Defense, Red Hat, FundServ, Primekey, StrongAuth, Wave, PA Consulting and many security-minded individuals are participating on this effort to advance these goals.

PONENTS

Arshad Noor, CTO of StrongAuth, Inc., a Sunnyvale, California-based company. Chair of the OASIS EKMI Technical Committee.

Antoni Bosch, Director Audit&IT-Governance. Institute of Law & Technology. President ISACA-Barcelona