OASIS Members Advance Interoperability Standard for Enterprise Encryption Key Management

IBM, Axway, BeCrypt, Brocade, Cisco, EMC, Emulex, HP,
PGP Corporation, Red Hat, SafeNet, Skyworth TTG, Symantec, Thales,
U.S. National Institute of Standards and Technology (NIST), Venafi, and Others
Collaborate on Open Standard for IT Security, Compliance, and Data Recovery

Boston, MA, USA; 6 May 2009 – The international open standards consortium, OASIS, has formed a new group to enable interoperability of key management services and clients. The new OASIS Key Management Interoperability Protocol (KMIP) Technical Committee will work to define a single, comprehensive protocol for communication between encryption systems and a broad range of new and legacy enterprise applications, including email, databases, and storage devices.

"As encryption technologies become more pervasive across the enterprise, key management quickly becomes a mission critical activity for protecting the sensitive data. Without a standard way to integrate encryption technologies and key management systems, data confidentiality and integrity may actually degrade," said Jon Oltsik, Principal Analyst at the Enterprise Strategy Group. "To address this issue, I've long been a strong proponent of key management standards and did what I could to push leading security vendors in this direction. I'm happy to say that the OASIS KMIP effort may finally fill this void."

KMIP will enable key lifecycle management, including the generation, submission, retrieval, and deletion of cryptographic keys. Designed for use by both legacy and new encryption applications, KMIP will support symmetric and asymmetric keys, digital certificates, and other "shared secrets."

"Our goal is to dramatically simplify the way companies encrypt and secure information," said Robert Griffin of EMC, co-chair of the OASIS KMIP Technical Committee.

“By removing redundant, incompatible key management processes, KMIP will provide better data security while at the same time reducing expenditures on multiple products,” added Anthony Nadalin of IBM, co-chair of the OASIS KMIP Technical Committee.

“KMIP is being advanced as an open standard in direct response to customers' needs to enable the widespread use of encryption,” noted Laurent Liscia, executive director of OASIS. “The effort already has the backing of major stakeholders in this area, and we welcome others to join and have their views represented as this specification moves through the standardization process.”

Participation in KMIP is open to all interested parties. Archives of the Committee's work will be accessible to both members and non-members, and OASIS will offer a mechanism for public comment.

Support for KMIP

IBM
"Interoperability across encryption and key management systems is a significant advancement that will enable acceptance of data protection on all types of devices from mainframes to banking devices to sensors. KMIP will allow customers to encrypt data with confidence anywhere in the enterprise or Cloud, knowing that it is not only secure, but can also be accessed when needed."
-Anthony Nadalin, Distinguished Engineer and Chief Security Architect, IBM Tivoli Software

Axway
“Through its recent merger with Tumbleweed, Axway brought together two companies with a long-standing commitment to developing highly secure, reliable messaging protocols for multi-enterprise collaboration. We’re committed to helping companies reduce risk, increase security and lower costs as they interact with their trading communities. As such, we fully support KMIP’s ability to consolidate and simplify key management across a variety of business-critical collaborative applications.” -Dr. Taher Elgamal, chief security officer for Axway

Brocade
“The amount of sensitive corporate information continues to grow exponentially, so organizations need a broader deployment of encryption technologies across data centers in order to protect data confidentiality and privacy. The reality is that these organizations operate in an increasingly complex, multivendor environment. As a result, interoperability and open standards are critical to successful deployments. Brocade is dedicated to interoperability across encryption and key management systems and is pleased to be working with OASIS in creation of the KMIP Technical Committee. Brocade will continue to actively participate in the group's valuable work on standardizing communication between encryption and key management systems.”
-Jose Carreon, Product Marketing Manager for Security Technologies, Brocade.

EMC
“KMIP has the three key attributes that are true of all important standards: it solves a significant customer problem; that problem can't be solved by just one vendor; and the right vendors are working together to solve the problem. We at RSA and EMC are happy to be working with the key players in the industry to drive this important interoperability standard.”
-Bob Griffin, Director, Solutions Design at RSA, The Security Division of EMC

Emulex
“Compliance and regulatory pressures have made encryption an essential pillar for next-generation data center architectures. One of the key challenges we have heard from our end user customers is the complexity of managing keys. Emulex fully supports KMIP, because it simplifies key management for secure encryption devices, such as the Emulex Secure HBA technology. Emulex's host-based encryption technology maximizes security protection and minimizes its cost for virtualized and converged data center deployments.” -Steve Daheb, senior vice president and chief marketing officer, Emulex.

HP
"Customers are looking for advancements to secure information and, at the same time, reduce cost, complexity and risk. HP supports creating a standard for encryption technologies to help companies protect sensitive data." -Chris Whitener, chief strategist, Secure Advantage, HP

PGP Corporation
“PGP Corporation has long been a proponent and supporter of the standardization of key management services and is pleased to join the OASIS KMIP Technical Committee to help drive this effort. By providing a standard way to manage encryption keys across multi-vendor applications, we are in effect helping customers increase the value of their encryption solutions."
-Jon Callas, Chief Technology Officer of PGP Corporation

Red Hat
“Delivering secure open source software is one of Red Hat's top priorities. By collaborating with industry partners through OASIS we are able to support standards in Key Management such as KMIP. These efforts directly effect our customers and ensure that they are deploying secure and hardened solutions." -Mark Little, Sr. Director of Engineering, Middleware, Red Hat

SafeNet
“SafeNet is excited to play a significant role in contributing to and shaping the KMIP standard. We continue to work with leading technology vendors to offer core key management capabilities with the SafeNet DataSecure and HSM product lines.” -Derek Tumulak, vice president, product management, SafeNet

Symantec
“The OASIS KMIP efforts will help to establish the interoperability our customers need to simplify encryption key management. These efforts will help to enhance our customers' choices for securing and managing their information." -Gary Phillips, senior director, standard tools and technologies, Symantec

Thales
“Organizations increasingly understand the need to encrypt data, but often hold back from doing so out of fear of losing access to the data or the prospect of managing multiple non-interoperable key

management systems. As the premier provider of encryption and key management systems, Thales' goal is to empower customers to encrypt data with confidence anywhere in the enterprise, knowing that it is not only secure, but also available when needed. Today's announcement of an official KMIP Technical Committee by OASIS is a crucial step towards that goal, enabling the deployment of effective, consistent information security policies not just in small areas of the datacenter but across the entire enterprise." -Jon Geater, Director of Technical Strategy for Thales information systems security activities

Venafi
"Venafi has been helping organizations who want to centrally manage encryption systems and keys across a broad range of applications and platforms for several years. The industry is long overdue for a single key management standard to allow for greater scalability and control across all of the different encryption scenarios world class entities have. Venafi is committed to contributing to the development of, and rapidly implementing support for KMIP." -Peter D. Bartok, CTO & Chief Architect of encryption management company, Venafi

Additional information:

OASIS KMIP Technical Committee
http://www.oasis-open.org/committees/kmip/

Cover Pages Technology Report:
http://xml.coverpages.org/keyManagement.html

About OASIS:

OASIS (Organization for the Advancement of Structured Information Standards) is a not-for-profit, international consortium that drives the development, convergence and adoption of open standards for the global information society. OASIS promotes industry consensus and produces worldwide standards for security, Web services, XML conformance, business transactions, electronic publishing, and other applications. OASIS open standards offer the potential to lower cost, stimulate innovation, grow global markets, and protect the right of free choice of technology. OASIS members broadly represent the marketplace of public and private sector technology leaders, users and influencers. The consortium has more than 5,000 participants representing over 600 organizations and individual members in 100 countries. http://www.oasis-open.org

Press contact:
Carol Geyer
OASIS Director of Communications
carol.geyer@oasis-open.org

+1.978.667.5115 x209 (office)
+1.941.284.0403 (mobile)