News

Key Management Standards Hit the Fast Track

Greg Goth

It might appear that the technology industry just discovered encryption-key management in 2007. Since the beginning of the year, data-security product vendors, enterprise customers, and standards bodies have embraced efforts to standardize methods for managing encryption keys across disparate encrypted-data storage and exchange systems. With every well-publicized data breach, enterprise customers are more eager for secure storage and key-management technology that won’t require them to start from scratch every time they update applications, switch vendors, or address periodic re-keying requirements mandated by strict new regulations spanning multiple industries and jurisdictions. Across the board, stakeholders in secure networks realize they must define some common ground as quickly as possible.

There are multiple approaches to data storage security, says Steve Norall, senior analyst at the Taneja Group consulting firm. Whether network architects choose software-based backup, a storage-area network (SAN)-based appliance that encrypts data as it traverses a system, or a tape library, Norall says each approach needs key management that lets devices encrypt and decrypt data as necessary.

“In all the survey data we’ve done, no one is standardizing on one approach,” Norall says. “Some companies are using multiple approaches within their own networks. A critical management nexus point is the key-management system. When you need to do a recovery, you need to have the keys to the data, and data is increasingly mobile. Keys have to securely move around.”

And, frankly, Norall says, “Right now, the base level of key exchange is terrible. It needs to get a lot better.”

Working group charters

The question is how quickly that base level of exchange might improve. Three standards bodies—the IEEE, the Internet Engineering Task Force (IETF), and the Organization for the Advancement of Structured Information Standards (OASIS)—have recently chartered working groups on key management. For enterprise technologists, navigating the landscape of vendor-specific key-management solutions and emerging standards efforts might prove to be a daunting task.

“We’re hearing a great deal from customers that that’s a concern,” says Bob Griffin, technical marketing director for RSA Security. He sees two prevailing industry trends precipitating the urgency to create a key-management standard. First is the proliferation of endpoint devices that can share keys to access encrypted data. The second, following naturally from the first, is the increased number of vendors homing in on this market niche.

A third factor, just as important as the technical nuts and bolts, is a regulatory climate that’s becoming ever more security-conscious. Numerous laws, such as California’s Breach Disclosure Law (http://www.auxillium.com/californiaSB1386.shtml), and US federal regulations, such as the US Health Insurance Portability and Accountability Act (http://www.hhs.gov/ocr/hipaa), as well as the Payment Card Industry’s Data Security Standard (https://www.pcisecuritystandards.org), have spelled
out strict requirements for protecting customer and patient data. As a result, security experts increasingly recommend encrypting data stored on any device, not just data in transit. And those devices must be able to share keys efficiently.

“So, interoperability has become extremely important,” Griffin says.

For now, RSA has staked the most of its key-management effort on the IEEE process. The key-management group, IEEE-P-1619.3, is a subgroup of the 1619 Security in Storage Working Group (http://ieee-p1619.wetpaint.com/?t=anon). Griffin is a member of 1619.3, which is focusing on storage encryption.

He’s also serving as an observer and liaison in the OASIS key-management effort, known as Enterprise Key Management Infrastructure (http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ekmi) (EKMI). Griffin characterizes the OASIS effort as “an extremely, extremely large project.” It aims to enable universal encryption and decryption at the application layer. Because this would require every imaginable application to adhere to the same key management standard, both Norall and Griffin see results at least five years away. RSA’s parent company, EMC, is seeking at least some answers much sooner.

“Our very pressing need at EMC is to have interoperability between our storage environment and all the major enterprise key managers emerging on the market,” Griffin says. “It’s clear that this is being driven in IEEE 1619 and that’s the right place for us to be involved at the moment.”

The IETF is also expanding its key-management work. Its 1994 document on Internet authentication, (RFC 1704 http://www.faqs.org/rfcs/rfc1704.html), is prescient on the quandary enterprise IT managers face today in securing data: the prohibitive expense of deploying Kerberos-enabled key servers throughout a large enterprise and the difficulties of ensuring communications across separate administrative domains. More recently, IETF released a “best current practice” RFC on cryptographic key management (RFC 4107 http://www.ipa.go.jp/security/rfc/RFC4107EN.html), and this year it chartered a working group to define a standard protocol for provisioning symmetric keys.

Since the National Institute of Standards and Technology released the Data Encryption Standard in 1977, NIST’s recommendations have often been regarded as the advisory gold standard for the security industry as well as government agencies. NIST experts have also joined the recent tide of key-management activity. They revised the agency’s guidelines for key management (http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf) in March. However, Griffin says conversations he’s had with NIST cryptography experts indicate the agency’s willingness to let the private sector take the lead in the next steps to achieve consensus.

“They felt they were really comfortable leaving the driving of key-management interoperability protocols to a vendor consortium like IEEE 1619,” Griffin says. “They’re very happy about keeping watch on the work rather than taking a leadership or even a strong contributory role.”

No 800-lb. gorillas

Participants and observers have praised the cooperation among the standards groups. EKMI technical committee member Tomas Gustavsson says the Oasis group has conferred with the IETF group and discerned no overlapping effort. And IEEE’s Griffin says the EKMI chair, Arshad Noor, has participated in some of the recent IEEE discussions. Norall says the collaboration is a welcome sight to industry observers and customers clamoring for a standard. “Anybody who can get these guys to the table and coalesce, it would be a positive,” he says. “Just right now, the lack of interoperability and an open API is a very crucial impediment.”
Perhaps one reason why the different efforts seem to be moving along in concert is that nobody has discovered a way to be the industry’s 800-lb. (or 363-kg) gorilla. Norall points out that key management could be “a kind of strategic choke point, especially for storage security,” but so far no big player has decided it can build a dominating de facto solution on that technology alone.

This leaves the solution space open. Bob Lockhart, chief systems architect at security vendor Neoscale, is editor of IEEE 1619.3. “We’ve all kind of presented to each other—or are in the process of presenting to each other—what each one’s target goal is,” Lockhart says.

“When there isn’t an 800-lb gorilla, it’s something that really hasn’t been done before,” he says. “People are trying to figure out which components each of the different bodies are going to do, and how they can all work together.” For example, the IETF keyprov group is focusing more on key provisioning, signaling, and mechanisms between the client and key-provisioning device, and Lockhart says the IEEE group is looking at how to include that information in its deliberations. Conversely, he thinks keyprov might be able to use some of the IEEE group’s work on namespace definitions.

**Nuts and bolts versus “the cloud”**

Lockhart says the IEEE group’s first priority will be focusing on a client-server key-management standard: “That’s what the end users need right now.” He estimates that parts of the specification will be ready for balloting within 12 months. A server-to-server protocol will probably follow a year to 18 months after that.

Meanwhile, the OASIS EKMI group is tackling the more ambitious idea of creating a key-management protocol for the application layer.

“If the cryptographic operation is performed in any other layer of the stack, however efficient it might be in the short-term, residual vulnerabilities in the layers between the cryptographic layer and the application layer will remain,” the group says in its FAQs (http://www.oasis-open.org/committees/ekmi/faq.php). “Given the effort that companies must expend to encrypt sensitive data and manage encryption keys, it behooves them to do it right, and to do it just once. Encrypting in any layer other than the application layer will only require the data owners to revisit the problem again.”

This effort speaks to a vision of a secure and interoperable “cloud” for key management, much like the Domain Name System for Internet addresses. However, both Lockhart and Norall believe such an all-encompassing effort will take longer than customers can wait. “If that’s the requirement, it becomes very much a slow roll,” Norall says, “because you’re expecting the entire application community to embrace and standardize on one API.”

According to Lockhart, existing formats for discrete media types might eventually “work up the stack to where, potentially, applications of a like nature that share common data repositories may go that route. It’s just, you’ve got a five- to 10-year wait before that happens all the way around.”

Meanwhile, Lockhart says the high degree of consensus within and among the standards bodies might lead to the pre-standard release of products that will be viable for the long term by the end of this year. The sense of urgency on all sides is a mix of technical and market factors, he says. Market factors include protecting company brands. When it comes to security breaches, he says, “most people want to keep their name out of the press.”
Related URLs

- US Health Insurance Portability and Accountability Act: (http://www.hhs.gov/ocr/hipaa)
- Payment Card Industry's Data Security Standard: (https://www.pcisecuritystandards.org)
- Enterprise Key Management Infrastructure (EKMI): (http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ekmi)
- IETF RFC 1704 Internet authentication document: (http://www.faqs.org/rfcs/rfc1704.html)

Related Links


Cite this article: