POWERs: With all the high-profile stories coming out about data breaches and spying on people's data, there's more pressure than ever for companies to encrypt all their data at rest.

If that was an easy task, everybody would already be doing it. One of the big challenges that companies face -- or, their fears -- is the challenge of managing large number of keys and the fear that they're going to lose a key and therefore lose data.

My guest this week on developerWorks is Michael Guster. He's a software engineer, and he and his coauthor, Stefanie Meile, have just published an article on developerWorks about a standard that will help address some of these fears that companies have.

Michael, welcome to this week on developerWorks. I understand your article is about a standard called Key Management Interoperability Protocol. Tell us a little bit about what this standard is and what it tries to achieve.

GUSTER: Hi, Calvin. Great to be here. Basically, the Key Management Interoperability Protocol -- short, KMIP -- is a single comprehensive protocol which defines the communications between enterprise applications and encryption systems. For example, that could be a key lifecycle management system and its clients.

In the key lifecycle management process are a lot of issues and requirements to consider like key sharing, deployment of keys, long-term availability of a large number of cryptographic objects, and all with different attributes and so on.

Here, KMIP takes the approach to merge all possible objects, attributes, and operations into a single protocol making possible a centralized KLMS. Centralizing the KLMS with one protocol reduces the operating and infrastructure costs and provides a consistent enforcement of security policies. The KMIP specification itself is governed and enhanced by a technical committee of Oasis.

POWERs: Michael, I understand you and Stefanie have created a reference implementation of the KMIP standard. Tell us a little bit about that project.

GUSTER: In a time which data protection is vital and intelligence scandals come to light, the need for data encryption is recognized by the public. However, encryption is only one part of the solution. The keys have to be stored, renewed and distributed. That leads us from data protection to key management.

The Key Management Interoperability Protocol complies with today's requirements of communication between a key lifecycle management system and its clients. But up until now, there are no open source implementations of KMIP. That was the motivation for me and Stefanie to write a reference implementation of KMIP 1.0 in Java. Our project, named KMIP4J, is a complete implementation of the KMIP 1.0 specification, which was successfully tested against two proprietary implementations.

Furthermore, a details test environment with a client and a key management system was built. So, if you want to make your encryption or key management system speak KMIP, you just need to download and embed our KMIP library, configure the server or client stop and you're ready to go.

To get started, we also offer a simple client and server example. For those who are interested in extending and testing our implementation, use our complete test environment. It comes with a graphical user interface and minimal KLMS.

The system architecture is carefully designed to provide extensions and interchangeability. The whole project is available at kmip4j.sourceforge.net. So, check it out and feel free to use and extend it. Comments and suggestions are always very welcome.

POWERs: Thanks, Michael. That sounds like a great way for companies and organizations to get started with KMIP and start using this standard in their software projects. How do you see the KMIP protocol evolving over time?

GUSTER: Using KMIP is an important step toward a better organized and more consistent management of cryptographic objects. Some of the biggest and best know IT companies have recognized the significance and advantages of KMIP and demonstrate support for it by promoting the standard worldwide.

The actual approved version of the specification is 1.1, and version 1.2 is currently under development. These versions of the specification further address the full spectrum of enterprise key management requirements across physical, virtual and
cloud-based deployments.

With our 1.0 open source implementation, we hope to deliver a contribution to the promotion of KMIP and vendors with limited financial resources also the opportunity to join the KMIP club. Thank you.

[ MUSIC ] [END OF SEGMENT]