Tony Cox, J Electr Eng Electron Technol 2017, 6:3
DOI: 10.4172/2325-9833-C1-007

Tony Cox

Cryptsoft, Australia

Standardized encryption key management for smart grids with KMIP

With the increased focus on cyber security within our critical infrastructure, the need for encryption as a primary defense is also growing. Wherever encryption is deployed, must the encryption keys be managed? Deploying standard-based key management infrastructure ensures these encryption keys can be managed throughout their entire lifecycle in a secure manner, using commercially available equipment via the KMIP (Key Management Infrastructure Protocol) specification. Developed within OASIS (Organization for the Advancement of Structured Information Standards), KMIP has widespread adoption in storage, information infrastructure and cloud deployments where it underpins the use of many forms of security objects including encryption keys, certificates, tokens, passwords, biometrics and identities. Multiple smart grid technology suppliers are now deploying KMIP conformant technology within their infrastructure to ensure maximum interoperability without sacrificing security. Adopting a well deployed standard means security solutions are readily available from a competitive market, delivering a greater return on investment from cyber security budgets. The KMIP specification has been developed and deployed since early 2009 by members of the KMIP Technical Committee (TC) whose membership includes many well-known brands in the IT and Cyber security industries and is now in its 5th iteration (v1.4) with version 2.0 well on the way. The specification documents cover both the detail of the specification as well as specific deployment profiles, ranging from key foundries, to encrypting storage arrays to post quantum computer cryptography. As smart grid deployments increase, we expect to see more requirements presented to the KMIP TC for inclusion in continued development of the specification.

Biography

Tony Cox has worked with both state and federal government departments on integration of security technology and public key infrastructure, with over a decade experience in both the security and identity management fields. He has an experience in evaluation of multi-million dollar procurement contracts and in the establishment and operation of policy authorities for public key infrastructure for million-plus smartcard token rollouts. He regularly presents to various audiences on interoperable key management and holds the following roles in the security standards space as a Co-Chair-OASIS KMIP Technical Committee, Co-Chair- OASIS PKCS11 Technical Committee and Chair-SNIA-SSIF Governing Board.

tony.cox@cryptsoft.com

Notes: