KRDs and KDHs in the X9.24-2-2016 Norm

Martin Rupp
SCIENTIFIC AND COMPUTER DEVELOPMENT

Introduction

KRDs and KDHs are essential notions in the context of the X9.24-2 norm. A KRD is a key receiving device, while a KDH is a key distribution host.

The X9.24-2-2016 norm deals with the transportation of **symmetric** keys using **asymmetric** cryptography. Therefore, this norm considers two kinds of devices:

1. A KDH that provides the key, which is typically an HSM
2. A device that receives the keys, such as a PED (PIN Entry Device) from an ATM or EFT-POS

The KRD and KDH are the main components in the X9.24-2 norm aside from a possible PKI system with a CA.

KRD

In the scope of the X9.24-2 norm, the KRD is a tamper resistant security module (TRSM) such as a(n)::

- PIN Encrypting Device (PED)
- Encrypting PIN PAD (EPP)
- Hardware Security Module (HSM)

Typically with most implementations of the X9.24-2 norm (like X9 TR-34), the KRD can only respond to commands from a KDH, i.e., the KRD is a slave KRD. KRDs may operate in uncontrolled environments, while KDHs must be used in controlled environments.

Additionally, the usual scenario is the distribution of symmetric keys using asymmetric techniques from a single key distribution host (KDH) to many key receiving devices (KRDs) as described in TR-34. TR-34 also offers the possibility of a peer-to-peer scenario.

KDH

A KDH is a trusted device that sends information to KRDs, e.g., a certificate. It is a processing platform used to securely distribute keys generated by HSMs to KRDs, such as EPPs (encrypting PIN pads) or PEDs (PIN entry devices) and the financial-processing platform communicating with those EPPs/PEDs.

The KDH must use an SCD (secure cryptographic device) to perform cryptographic operations, including the generation of symmetric keys. Usually, a key receiving device (KRD) will be bound/unbound to a key distribution host (KDH).

Authentication between KRD and KDH: Trust Models

The KRD and KDH need to trust each other. Therefore, they need a way to identify each other with some certainty. Mutual trust between KRDs and KHD can be achieved via a PKI. This is the recommended strategy underlined by the norm. The trust models between the parties are an essential aspect of the X9.24-2 norm and should be developed independently.

Conclusion

Key receiving devices and key distribution hosts are the two dual parties in the distribution of symmetric keys using asymmetric cryptography as described by the X9.24-2 norm. Organizations wishing to implement the X9.24-2 norm should understand these terms well since they are fundamental for comprehending the norm.