What are the main differences between X9.24-2-2016 and X9.24-1-2017?

Martin Rupp
SCIENTIFIC AND COMPUTER DEVELOPMENT (SCD)

Introduction

The X9.24 norm “Retail Financial Services Symmetric Key Management“ is split into three distinct parts. Part 1 (2016) deals with symmetric key management using symmetric cryptography techniques, while Part 2 (2017) deals with symmetric key management using asymmetric cryptography. Lastly, Part 3 (2017) is an aside that deals with the derived unique key per transaction (DUKPT) algorithm.

In what follows, we explain the main differences between the management of symmetric keys using respectively symmetric and asymmetric techniques, according to the X9.24 norm.

Key Management of Symmetric and Asymmetric Key Encryption Keys

In X9.24 Part 1, secure cryptographic devices (SCDs) are clearly mentioned much more than in Part 2. In Part 1, physical storage devices such as tamper-evident and authenticable (TEA) bags are essential, while in Part 2, they are not of any use. Instead, in Part 2, key host devices (KHDs) and key receiving devices (KRDs) are discussed.

Another critical difference is that Part 2 deals a lot with PKI and especially certification authorities. In Part 1, these are of very little interest.

Additional differences include:

- In Part 1, SCDs acting as key injection devices or portable key loader devices (PKLD) are described. However, the concept of key injection is not considered as necessary in Part 2.

- Part 2 describes the Diffie-Hellman process for key transportation extensively. Part 1 doesn't deal with it since Diffie-Hellman isn't necessarily based on PKI at all.

- The trust model is a concept specific to Part 2 and has no equivalent in Part 1.

Lastly, the concept of public keys is unique to Part 2. Such keys are not managed as all the other secret and private keys since they are usually not protected. For instance, their integrity and authenticity may be enforced by other cryptographic mechanisms such as cryptograms and MACS.

This table show some of the equivalent concepts between the two parts of the norm:

Part 1	Part 2
Tea bag	*(no equivalent)*
SCD	SCD
PKLD	KHD & KRD
(no equivalent)	Public key
secret key	Private key
(no equivalent)	Diffie-Hellman
(no equivalent)	Trust model
(no equivalent)	Certificate

Key Shares and Key Reconstruction in the X9.24 Norm

In both Parts 1 and 2 of the X9.24 norm, the notion of key share and split secret is essential. Key share and split secrets in X9.24 Part 1 has already been described in a previous article. In general, most of the concepts are similar regarding this between the two parts of the X9.24 norm.

In Part 2, in the case where the private key part of an asymmetric key pair is non-encrypted and stored outside an SCD, then it must be stored as key shares using a key fragmentation algorithm such as Blum Shamir (similar to Part 1)/

Additionally:

- In Part 2, the non-automated (manual) distribution of private keys must be done using dual control and split knowledge.

- The storage of key shares must be performed so that no single party can reconstruct the key from its own knowledge of the fragment. Again we find similar requirements in Part 1 of the X9.24 norm.

- Part 2 requires less audit and less dual control than Part 1. Nevertheless, it is emphasized that the rotation of individuals sharing key fragments should be considered a best practice.

Key Management

In Parts 1 and 2, key management shares many common aspects, especially in the event of a compromised key and the way key custodians must react to this. Paragraphs *7.11 Key Replacement* and *7.12 Key Destruction* in Part 2 deal specifically with these notions.

Conclusion

Parts 1 and 2 of the X9.24 norm have differences, similarities, and equivalent concepts. However, they both share a common philosophy based on concrete concepts of secure key management.