# The Specificity of the Requirements for SCD with Asymmetric Keys According to X9.24-2-2016

**Martin Rupp**
SCIENTIFIC AND COMPUTER DEVELOPMENT

## Introduction

SCDs are secure cryptographic devices compliant with the requirements defined in the ISO 13491-1 and ANS X9.24 Part 1 norms. They are widely used within the scope of the X9.24 standard.

In a previous article, we presented the main concepts of an SCD. Here we focus more on the specific requirements and roles that SCDs must fulfill to be in compliance when using asymmetric cryptography to transport symmetric keys.

If we consider the case of internet-based transaction systems seeking to comply with X9.24-2-2016, then such systems or applications must use SCDs to protect all the private and symmetric keys. The standard states: “"The scope of this part of X9.24 may apply to Internet-based transactions, but only when such applications include the use of a SCD (as defined in section 7.2 of ANS X9.24 Part 1) to protect the private and symmetric keys"

## SCD: PEDs and HSMs

The X9.24 norm mentions specific requirements for two different types of SCDs, a PIN entry device (PED) and a hardware security module (HSM). Here is an example of a typical use case where the norm seeks to emphasize its usage.

1) In the case of a PED, such as a POS Terminal or ATM pinpad device, the norm states that is is mandatory that the PED is provided with secure processing for mutual authentication of the interfacing host (typically an HSM) when the PED is used for the distribution of symmetric key using asymmetric techniques. The PED must have an anti-man-in-the-middle attack system (presumably a strong, secure channel, such as two-ways TLS) and must ensure that the communication with the host will not be tampered or monitored.

2) In the case of an HSM acting as a host system for a PED client, there are similar symmetric requirements, such as an anti-man-in-the-middle attack system and authentication of the client (typically a PED device) so that the key sender and key receiver are identified without any possible ambiguity. Only authorized devices can be allowed to connect to the network. The potential use of a CA (certification authority) by the HSM (acting as an SCD) is then underlined.

# SCDs and Certification Authorities

In the context of retail bank transactions, the X9.24-2 norm underlines that SCDs operated by an acquiring bank may request a digital certificate from a certification authority. This allows for authentication by the other SCDs and provides a secure and trusted manner for exchanging public keys.

The entire network of SCDs that interface with each other can use PKI, digital certificates, and certification authorities judiciously. While this is a recommended use, X9.24-2 doesn’t make it mandatory. Therefore, other types of mutual authentication schemes are possible, provided that they respect the constraints mentioned earlier.

# Cryptographic Keys Stored Inside an SCD

The X9.24-2 norm recommends that symmetric keys and asymmetric *private* keys are stored inside an SCD. If this will not be the case, then strong recommendations are enforced with very precise use cases. Note that some use cases covered by the present norm, such as key management, ban the use of cryptographic keys outside SCDs.

If any SCD is loaded with a temporary private key that is only needed for transferring keys to other SCDs the transient key must be erased completely as soon as the transfer is complete.

# SCDs Used for Key Management

In a key management scheme, all parties *must* use SCDs. In the instance of symmetric key generation inside an SCD, all components involved in the generation must be XORed inside an SCD. According to the X9.24-1-2017 standard, the SCD must reconstruct a key from its fragment using an XOR operation.

SCDs no longer in service (or taken for repair) shall be properly zeroized. In the case of PED, the public keys and certificates must also be erased.

# KHD, KRD and SCDs

Key receiving devices and key host devices have a central role in the norm and must be conceived as devices operating their dedicated SCDs. These SCDs are responsible for the encipherment of KHD keys using the SCD public key.

# Conclusion

In regards to the X9.24-2 norm, secure cryptographic devices (SCDs) are essential components. They are most often mandatory for various cryptographic operations involving the ciphering of symmetric keys via asymmetric keys.