Federal Office
for Information Security

Key Lifecycle Security Requirements

Version 1.0.3

Federal Office for Information Security
Post Box 20 03 63
D-53133 Bonn
Phone: +49 228 99 9582-0
E-Mail: eid@bsi.bund.de
Internet: https://www.bsi.bund.de

Document history

Version	Date	Editor	Description
1.0	10.10.2016	BSI	First final version
1.0.1	29.11.2016	BSI	Completion of the introduction by the additional last sentence; editorial work for publication
1.0.2	02.11.2018	BSI	Change on requirements for random number generation.
1.0.3	17.11.2021	BSI	Definition of options within Security Level 2 for End Entities; minor editorial work.

Contents

1 Introduction

This document specifies generic requirements for the key life cycle for cryptographic keys used in Public Key Infrastructures, i.e. keys of Certification Authorities and keys of End Entities.

In general, security and operation of a Public Key Infrastructures are governed by Certificate Policies. This document is intended to be referenced from different Certificate Policies, in order to provide harmonized requirements for the key life cycle and for Cryptographic Modules.

Referencing Certificate Policies MUST declare if the stipulations from this document are REQUIRED or RECOMMENDED for the Certification Authorities and End Entities governed by that Policy.

The referencing Policy MAY provide derogations from this document. The requirements of the referencing Policy take always priority over the requirements of this document.

1.1 Keywords

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

2 Requirements

This document defines two Security Levels for cryptographic keys for use in a PKI (Certification Authorities and End Entities):

- **Security Level 1**
- **Security Level 2**

The referencing Certificate Policy MUST stipulate which Security Level must be fulfilled by which entity.

The following subsections define requirements to be fulfilled for the respective Security Level. The requirements are applicable – unless otherwise stipulated by the Root Certificate Policy – to all entities in the PKI, i.e. to both Certification Authorities and End Entities.

The requirements for Security Level 2 are a superset of the requirements for Security Level 1, i.e. fulfillment of the requirements for Security Level 2 implies compliance to Security Level 1. If a requirement is not marked to belong to one of the Security Levels, it applies to both levels. For End Entities, this document defines optional exceptions within Security Level 1 or 2 that MAY be applied. If applied, this MAY be denoted by Security Level 1_exc(<list of exceptions>) or Security Level 2_exc(<list of exceptions>), respectively, by listing the acronyms of all exceptions that apply and that are given in this document.

2.1 Security Concept

Entities (Certification Authorities and End Entities) SHOULD have a security concept based on established standards, covering the key life cycle and the operation of Cryptographic Modules as described in this document.

2.2 Cryptographic Modules

A Cryptographic Module is a well-defined IT system comprising hard- and software, e.g. a Hardware Security Module (HSM), a Smart Card or a Server.

For the complete life cycle of private keys, Cryptographic Modules fulfilling the requirements from this section MUST be used.

Security Level 1

The access to the Cryptographic Module MUST be protected by two factor authentication.

The number of operators having access to the Cryptographic Module MUST be restricted to the minimum necessary for sustained operations, taking into account requirements relating to business continuity and disaster recovery.

Due care MUST be taken to protect the private key against unauthorized access and compromise.

For random number generation, e.g. for key or signature generation, a random number generator of one of the classes NTG.1, DRG.4 or PTG.3 according to [AIS 20/31] MUST be used.

Security Level 2

The access to the Cryptographic Module MUST be protected by two factor authentication. Access to the Cryptographic Module MUST require at least two separately authenticated operators. For End Entities, the Root Certificate Policy MAY reduce this requirement to a single authenticated operator. If this exception is applied, the Root Certificate Policy MAY denote this by Security Level 2_exc(SAO).

The number of operators having access to the Cryptographic Module MUST be restricted to the minimum necessary for sustained operations, taking into account requirements relating to business continuity and disaster recovery.

The Cryptographic Module SHALL be Common Criteria certified by the BSI according to one of the following Protection Profiles:

- Hardware Security Modules (HSMs):
  - [EN419221-2] (devices with key backup);
  - [EN419221-4] (devices without key backup);
  - [EN419221-5], if the device is operated in a physically separated secure environment. The secure environment, including necessary hard- and software, as well as personal and organizational measures, MUST be certified according to [ISO/IEC 27001]. Access to the secure environment MUST be restricted to the personal necessary for the operation.
- Secure Element / Smart Card:
  - [EN419211-2] (modules including key generation);
  - [EN419211-3] (modules including key import).
- For End Entities, the Root Certificate Policy MAY list additional application specific Protection Profiles. If this exception is applied, the Root Certificate Policy MAY denote this by Security Level 2_exc(AS_PP).

For random number generation, e.g. for key or signature generation, a random number generator of one of the classes DRG.4 or PTG.3 according to [AIS 20/31] MUST be used.

The certification MUST encompass all security functionalities of the Cryptographic Module needed for its operational use according to this guideline and the corresponding Certificate Policy. This implies that all used cryptographic algorithms and key lengths MUST be covered by the certification, as well as functionalities for key backup/key export, if present.

2.3 Key Generation

The following requirements MUST be met for key generation:

- Keys MUST be generated by the entity holding the key.
- Keys MUST be generated in a Cryptographic Module according to Section 2.2.
- If one of the parts of [TR-03116] is applicable to the purpose the key is generated for, the requirements from that part MUST be fulfilled. Otherwise, the requirements from [TR-02102] MUST be fulfilled. The Root Certificate Policy MAY define derogations to this requirement. If this exception is applied, this MAY be denoted by Security Level 1_exc(KG) or by Security Level 2_exc(KG), depending on the Security Level that is otherwise satisfied by the entity.

2.4 Key Export and Import

Private keys MUST NOT be exported from the Cryptographic Module except for the following purposes:

- backup of a private key for recovery after loss of availability of the key (e.g. malfunctioning Cryptographic Module);
- duplication of a key, which means use of the same key in several Cryptographic Modules which are operated as a single unit in order to facilitate resilience or for the purpose of load balancing;
- updates of the hard- and/or software of the Cryptographic Module.

Entities SHOULD carefully weigh the advantages and disadvantages of copying the private key before doing so.

Private keys MUST NOT be archived or escrowed.

2.4.1 Key Export

Exported private keys MUST be handled according to the same Security Level and security requirements as the source key.

Exported private keys MUST be securely encrypted.

Security Level 1
When exporting private keys the encryption of the private key MUST fulfill the requirements of [TR-02102].

Security Level 2
The mechanism for exporting private keys from Cryptographic Modules MUST be covered by the certification of the Cryptographic Module.

2.4.2 Key Import

Importing a private key manually into a Cryptographic Module, e.g. when re-importing the backup key due to a hardware update, MUST require two independently authenticated operators. For End Entities, this requirement MAY be reduced by the Root Certificate Policy to a single authenticated operator for key import only. If this exception is applied, this MAY be denoted by Security Level 1_exc(SAO_KI) or by Security Level 2_exc(SAO_KI), depending on the Security Level that is otherwise satisfied by the End Entity.

2.5 Key Activation

A private key is called activated when it is first used for the intended purpose, e.g. signing or encryption. Using a key to prove possession of the key to a Certification Authority (e.g. signing a certificate request) does not count as key activation.

Each entity MUST NOT have more than one activated key per purpose. In the case of duplication of a key, e.g. for the purpose of load balancing, the original key and its duplicates count as one key.

2.6 Key Usage

Keys MUST NOT be used for purposes other than the purposes foreseen by the Certificate Policy.

2.7 Key Destruction

Private **signing** keys, including all copies and backups, MUST be securely destroyed if

- the validity period has expired, or
- a new key is activated.

The cases and/or dates when private keys used for **encryption/decryption** or **key agreement** shall be securely destroyed SHOULD be defined application specific in the corresponding Certificate Policy.

All kinds of private keys SHALL be securely destroyed as described below.

Security Level 1

Private keys MUST be destroyed by zeroization/overwriting with suitable software.

Security Level 2

Private keys MUST be destroyed

- using the secure mechanism of the Cryptographic Module according to the applicable requirements from the Protection Profile, or
- by physically and irrevocably destroying the Cryptographic Module.

Bibliography

AIS 20/31	BSI: A proposal for: Functionality classes for random number generators, Version 2.0
EN419211-2	CEN: EN 419211-2: Protection profiles for secure signature creation device -- Part 2: Device with key generation
EN419211-3	CEN: EN 419211-3: Protection profiles for secure signature creation device - Part 3: Device with key import
EN419221-2	CEN: EN 419221-2 Protection profiles for Trust Service Provider Cryptographic modules -- Part 2: Cryptographic Module for CSP signing operations with backup - Protection profile (CMCSOB-PP)
EN419221-4	CEN: EN 419221-4 Protection profiles for Trust Service Provider Cryptographic modules -- Part 4: Cryptographic module for CSP signing operations - Protection profile - CMCSO PP
EN419221-5	CEN: EN 419221-5: Protection profiles for Trust Service Provider Cryptographic modules - Part 5: Cryptographic Module for Trust Services
ISO/IEC 27001	ISO/IEC: ISO/IEC 27001:2013, Information technology - Security techniques – Information security management systems - Requirements
RFC2119	IETF: RFC 2119: S. Bradner: Key words for use in RFCs to Indicate Requirement Levels
TR-02102	BSI: Technische Richtlinie TR-02102, Kryptografische Verfahren: Empfehlungen und Schlüssellängen
TR-03116	BSI: Technische Richtlinie TR-03116, Kryptographische Vorgaben für Projekte der Bundesregierung