



SPEC-Media-PKI

Version:	1.0.0
Author:	Dr. Joseph Lutgen / VDV ETS
Last changed:	28.09.2023 17:05:00



Table of Contents

List of Tables	3
List of Figures	3
1 Introduction.....	4
1.1 Purpose	4
1.2 Scope	4
1.3 Terminology and Notation	4
1.4 Definitions	4
1.5 Abbreviations	5
2 Structural overview	5
3 Cryptographic algorithms and key sizes	6
4 Planned schedule for CAs in the 2GSI Media PKI	7
5 Concrete parameter values for the initial production and staging roots.....	8
5.1 Production Environment ETS-Root-01	8
5.2 Staging Environment ETS-Root-01	9
6 Appendix: List of References	10



List of Tables

Table 1 : Durations of validity and active phase for Root- and Sub-CAs	6
Table 2 : Key parameters and signature algorithms for 2GSI Media PKI	7

List of Figures

Figure 1 : Structural overview	5
Figure 2 : Planned schedule for CAs in the 2GSI Media PKI	7

1 Introduction

1.1 Purpose

This document is intended to provide the background information and parameters necessary to generate the initial roots for the 2GSI Media PKI, a PKI designed to issue certificates for User Media, SAMs and related entities communicating with User Media and SAMs in the context of eTicket Germany. This will be the successor of the PKI currently in operation.

The intended audience consists of individuals and organisations involved in the development and provision of PKI services for VDV ETS.

1.2 Scope

The goal of the document is to provide the information needed to generate the first Root-CA for the 2GSI Media PKI in a key ceremony. This process will output the root certificate and confidentially archive the private root key for later use in generating certificates over Sub-CAs.

For this PKI the relevant certificate format is specified in the document [SPEC-M2MC]. We refer to these as machine-to-machine certificates. The format is defined as an ASN.1 structure similarly to the compact “card verifiable certificate format”. Certificates for the communication between systems in the “Interoperability Network” of eTicket Germany are not in the scope of this document.

1.3 Terminology and Notation

An octet will be denoted by 0xXY or 'XY' where $X, Y \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F\}$ are hexadecimal symbols.

Octet strings will be denoted by $0xX_1Y_1X_2Y_2 \dots X_nY_n$ (possibly with spaces between octets) or by $'X_1Y_1X_2Y_2 \dots X_nY_n'$ (possibly with spaces between octets). Where relevant and unless otherwise stated, the leftmost octet in this notation will be the most significant.

The significance of octets in an octet string is relevant the order will be most significant octets on the left.

Specific numeric values (Arabic numerals) are decimal.

1.4 Definitions

Term	Definition
Secure Application Module	Secure Application Module refers to a component employed in terminals to perform security operations in the context of an application and to protect critical data like cryptographic keys. Communication between terminal and SAM is initiated strictly by the terminal. The SAM only responds to requests sent by the terminal.
Security level (or strength) of a cryptographic algorithm	The security level is specified as a number S of bits such that it is expected that (roughly) 2^S basic operations are required to break the algorithm.

1.5 Abbreviations

Abbreviation	Definition
2GSI	Second Generation Security Infrastructure
CA	Certificate Authority
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
SAM	Secure Application Module
UM	User Medium
VDV-ETS	Verband Deutscher Verkehrsunternehmen eTicket Service GmbH & Co. KG Translation: Association of German Transport Operators eTicket Service GmbH&Co.KG

2 Structural overview

This chapter defines the basic structural parameters of the planned Media PKI for the second generation security infrastructure (2GSI).

The following figure gives an overview of the hierarchical structure and the entities involved.

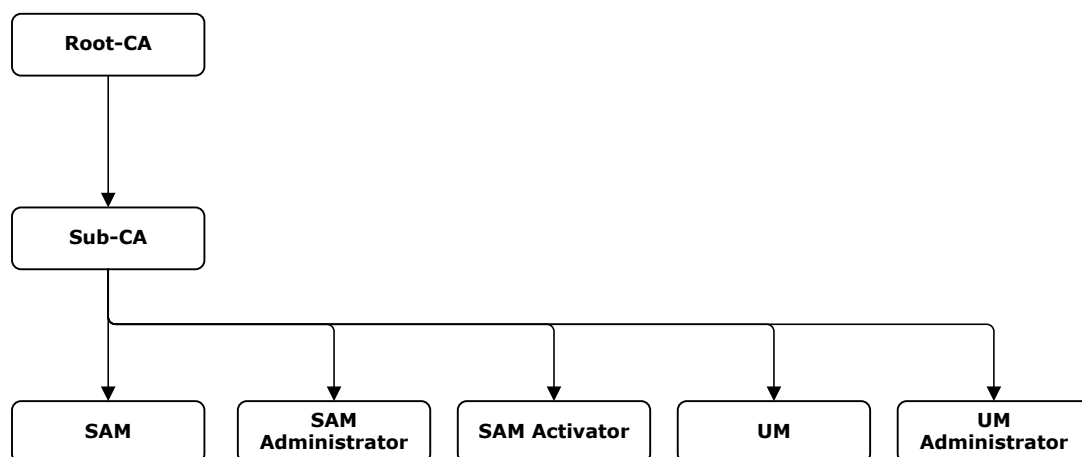


Figure 1 : Structural overview

The 2GSI Media PKI will be implemented as a two-stage hierarchy in which Sub-CAs issue certificates for end-entities and a Root-CA issues certificates for the Sub-CAs.

The Root-CAs themselves will only have a self-certificate, i.e. they will issue their certificates themselves. Trusted channels will be implemented for the delivery of root certificates resp. public root keys to authorized entities and components.

The Root-CAs and Sub-CAs will follow the so called “shell model”, i.e. a key may only be used to verify certificates as long as its own certificate is valid.

In the shell model the period of validity of a CA is therefore divided into an active phase and a passive phase whereby

$$\text{duration of validity} = \text{duration of active phase} + \text{duration of passive phase}.$$

During the active phase the CA may sign new certificates and during the passive phase the CA may only be used to verify already existing certificates. This requires planning from the beginning, but avoids the need to permanently include expired CAs in blocking lists.

The 2GSI Media PKI must allow for validities of up to 5 years for end entity certificates. Therefore, the passive phase of each CA must be at least 5 years.

Generally, the proposed durations of validity for Root- and Sub-CAs depend on the chosen crypto-algorithms and key sizes. The specific algorithm selections for the 2GSI Media PKI are given in chapter 3 and the following table gives an overview of the relevant duration values for Root- and Sub-CAs.

CA	Durations (in years)	
	Validity	Active phase
Root-CA	20	10
Sub-CA	10	4

Table 1 : Durations of validity and active phase for Root- and Sub-CAs

The common format for all of the certificates issued in the 2GSI Media PKI is defined in the specification document [SPEC-M2MC].

The different end entities shown in Figure 1 above will be distinguished by the values of *subjectRole* that are assigned to them according to [SPEC-M2MC]. The data object *SubjectRole* is contained in the data object *Subject* of the certificate.

The 2GSI Media PKI will consist of a staging system (to support integration tests) and a production system. The assignment of a certificate to the staging or production system will be indicated in the *subjectRole* as specified in [SPEC-M2MC].

3 Cryptographic algorithms and key sizes

The collection of crypto-algorithms that are relevant for 2GSI in overall terms is specified in [SPEC-CipherSuite]. The key parameters and signature algorithms selected from this collection for the CAs of the 2GSI Media PKI are as listed in the following table.

CA	Key Type	Standard Curve Parameters	Signature Algorithm
ETS-Root-01	ECC	secp384r1	ecdsa-with-SHA384
ETS-Root-02	ECC	brainpoolP512r1 (expected)	ecdsa-with-SHA512 (expected)
Sub-CAs under ETS-Root-01	ECC	secp384r1	ecdsa-with-SHA384

CA	Key Type	Standard Curve Parameters	Signature Algorithm
Sub-CAs under ETS-Root-02	ECC	secp384r1 or brainpool384r1	ecdsa-with-SHA384

Table 2 : Key parameters and signature algorithms for 2GSI Media PKI

Note: Generally speaking, as we go higher up in a PKI hierarchy key sizes resp. security levels of the algorithms employed should not decrease (see the recommendation e.g. in [FIPS Pub 186-4; Section 6.1.1]). Initially end entity keys will be of type `secp256r1` and may later be stepped up to `secp384r1` or `brainpoolP384r1` as needed.

4 Planned schedule for CAs in the 2GSI Media PKI

The following figure gives an overview of the planned Root- and Sub-CAs showing their short names and key parameters on the left, effective dates, expiration dates, and expected time windows for active and passive phases.

An active phase may be extended by up to 1 year without encountering problems with the fixed expiration dates.

A CA will usually be implemented and made ready for operation before the actual begin of the active phase and the public key may be made available to card production ahead of the actual beginning of the active phase.

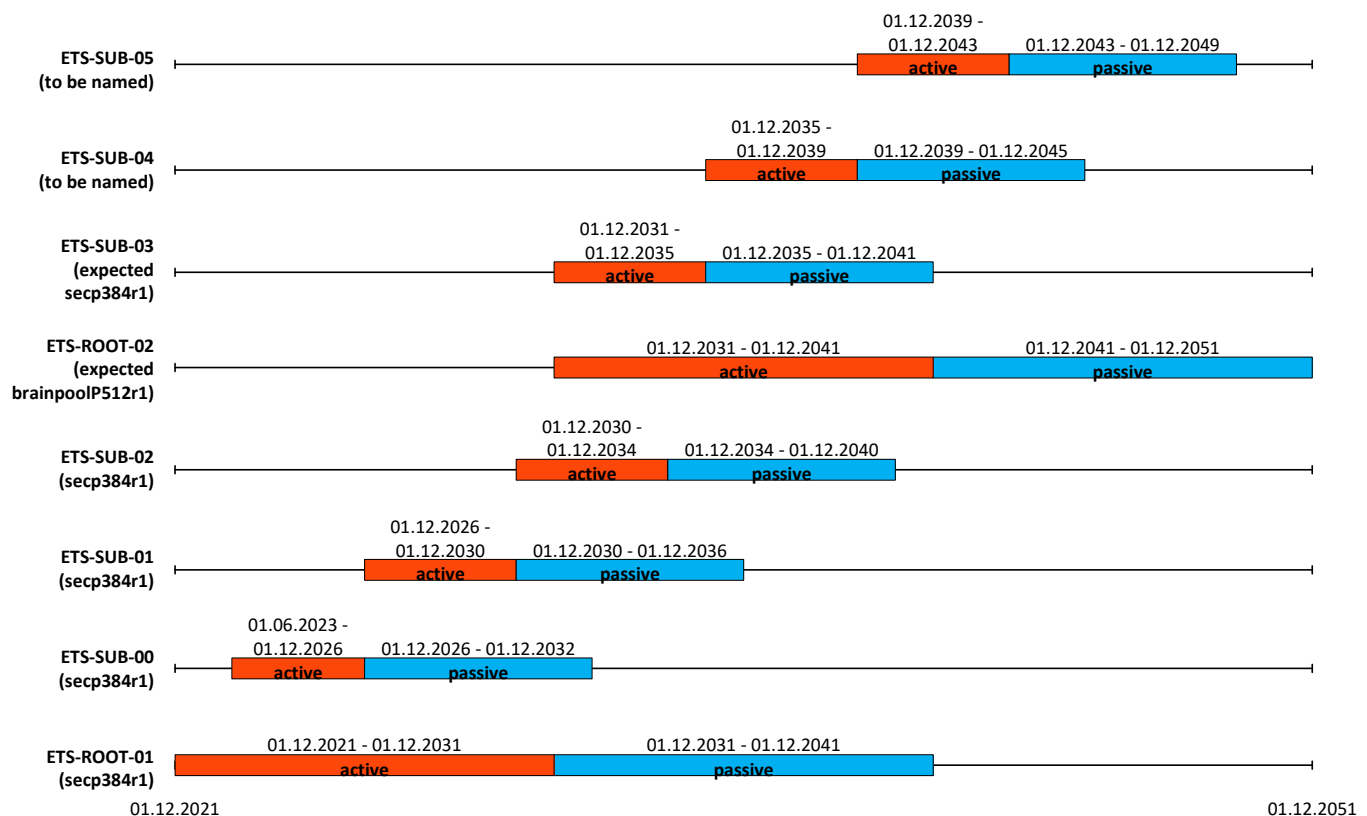


Figure 2 : Planned schedule for CAs in the 2GSI Media PKI



5 Concrete parameter values for the initial production and staging roots

The following two sections define the specific values of attributes to be set in the self-certificates for ETS-Root-01 in the staging and production environments using the data object names and ASN.1 TLV structures specified in [SPEC-M2MC]. Of course the actual values for the public keys and signatures can only be documented after these have been generated.

5.1 Production Environment ETS-Root-01

```
subject
0x7F 20 14
    4D 02 13 88          // registrationAuthorityID = OrgID of VDV-ETS
    80 01 00            // subjectRole = Root Production Environment
    81 0B 45 54 53 2D 52 4F 4F 54 2D 30 31
                        // subjectName = 'ETS-ROOT-01'

subjectAuthorisation
0x7F 4C 10
    4D 02 13 88          // ownerID = OrgID of VDV-ETS
    A0 0A                // AlgorithmIDs
                        06 08 2A 86 48 CE 3D 04 03 03 // ecdsa-with-SHA384

certificateEffectiveTime
0x5F 25 04
    61 A6 AC F0          // Wednesday, 1. December 2021 00:00:00 GMT+01:00

certificateExpirationTime
0x5F 24 05
    00 87 46 9B EF      // Sunday, 1. December 2041 23:59:59 GMT+01:00

certificateAuthorityReference
0x62 14
    4D 02 13 88          // registrationAuthorityID = OrgID of VDV-ETS
    80 01 00            // subjectRole = Root Production Environment
    81 0B 45 54 53 2D 52 4F 4F 54 2D 30 31
                        //subjectName = 'ETS-ROOT-01'

ellipticCurveID in publicKeyParameters
0x06 05
    2B 81 04 00 22          // secp384r1

signatureAlgorithmID
0x06 08
    2A 86 48 CE 3D 04 03 03 // ecdsa-with-SHA384
```




5.2 Staging Environment ETS-Root-01

```
subject
0x7F 20 14
    4D 02 13 88          // registrationAuthorityID = OrgID of VDV-ETS
    80 01 01            // subjectRole = Root Staging Environment
    81 0B 45 54 53 2D 52 4F 4F 54 2D 30 31
                        // subjectName = 'ETS-ROOT-01'

subjectAuthorisation
0x7F 4C 10
    4D 02 13 88          // ownerID = OrgID of VDV-ETS
    A0 0A                // AlgorithmIDs
                        06 08 2A 86 48 CE 3D 04 03 03        // ecdsa-with-SHA384

certificateEffectiveTime
0x5F 25 04
    61 A6 AC F0          // Wednesday, 1. December 2021 00:00:00 GMT+01:00

certificateExpirationTime
0x5F 24 05
    00 87 46 9B EF      // Sunday, 1. December 2041 23:59:59 GMT+01:00

certificateAuthorityReference
0x62 14
    4D 02 13 88          // registrationAuthorityID = OrgID of VDV-ETS
    80 01 01            // subjectRole = Root Staging Environment
    81 0B 45 54 53 2D 52 4F 4F 54 2D 30 31
                        //subjectName = 'ETS-ROOT-01'

ellipticCurveID in publicKeyParameters
0x06 05
    2B 81 04 00 22          // secp384r1

signatureAlgorithmID
0x06 08
    2A 86 48 CE 3D 04 03 03        // ecdsa-with-SHA384
```



6 Appendix: List of References

[SPEC-M2MC] *M2M Certificates Specification*, Version 2.0.2, Dr. Joseph Lutgen.

[SPEC-CipherSuite]

 Cipher Suite Specification, Version 1.0.1, Dr. Joseph Lutgen

[FIPS Pub 186-4]

 Federal Information Processing Standards Publication 186-4, *Digital Signature Standard*, July 2013, National Institute of Standards and Technology.

<https://csrc.nist.gov/publications/detail/fips/186/4/final>