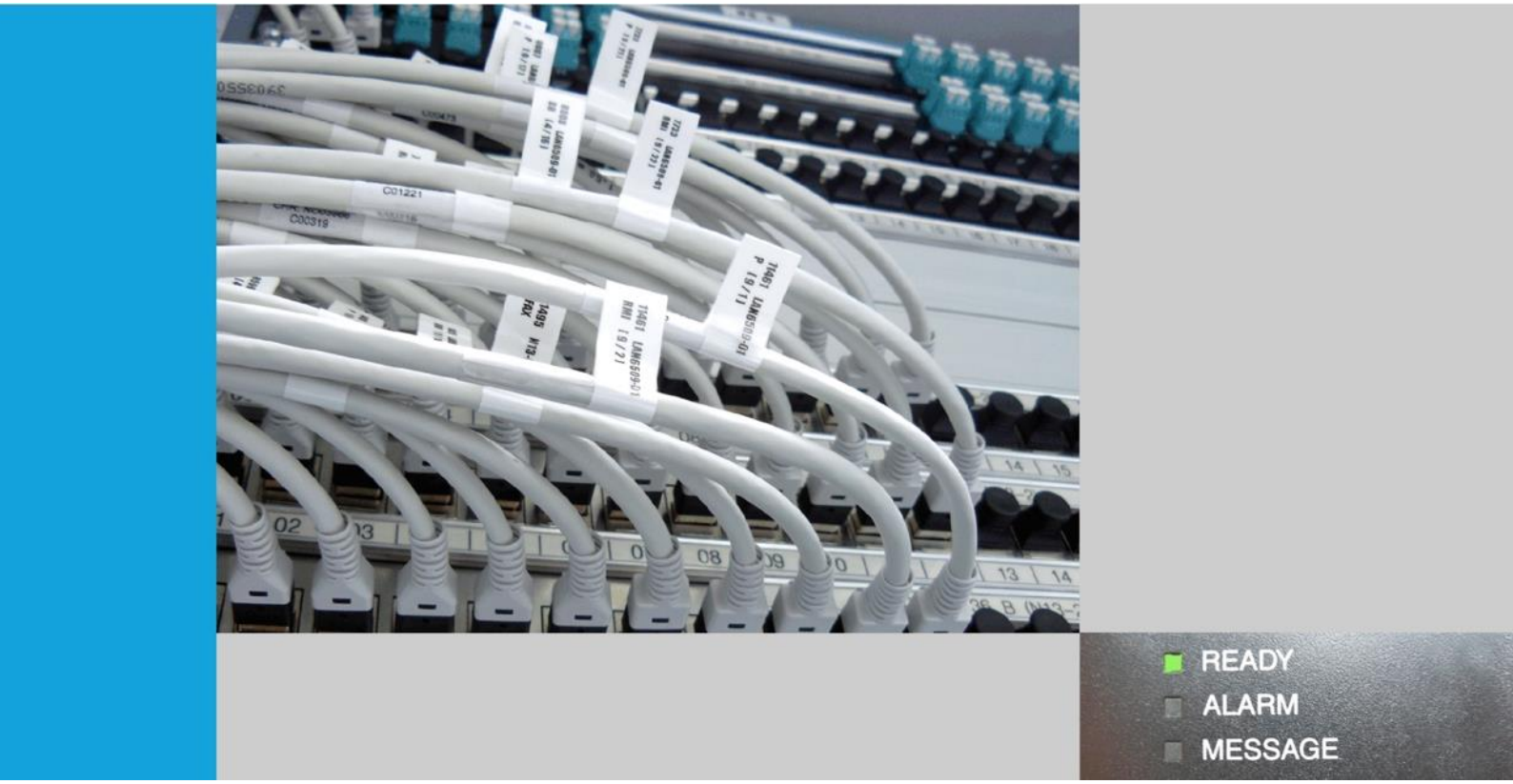
Landesamt für Digitalisierung,
Breitband und Vermessung
<Bavarian State Office for digitalization and measurement>

IT service centre of the Free State of Bavaria



Certificate Policy (CP) and Certificate Practice Statement (CPS) of the public key infrastructure of the Bavarian Administration

for the
X.509 certificate hierarchy of the
Bavarian SSL server PKI

Processing:
Kerstin Ehrhardt

Munich, 12th April 2019

Document development

Version	Date	Processor	Description, QS measure	State *see below
1.0 (ger)	08.01.2013	K. Ehrhardt	Version 1.0 published	Approved
1.2 (ger)	09.02.2018	K. Ehrhardt	New design template; review of contents	Approved
1.2 (en)	08.03.2018	K. Ehrhardt	English translation	Approved
1.3 (en)	12.04.209	K. Ehrhardt	Review of contents; Changes to sections 3.3.1, 4.1.2, 4.3.1, 4.4.1, 4.7.2, 4.7.3, 6.1.1, 6,1,2, 6.1.5, 6.4, 6.4.1	Approved

* The following terms are to be used: in progress, presented, approved

Contents

1 Introduction

The IT service centre in the Bayerisches Landesamt für Digitalisierung, Breitband und Vermessung (LDBV) *<Bavarian State Office for digitalization and measurement>* operates central components and services of the Bayerisches Behördennetz (BYBN) *<Bavarian government network>* on behalf of the Bayerisches Staatsministerium der Finanzen, für Landesentwicklung und Heimat (StMFLH) *<Bavarian state ministry of finance, of state development and home affairs>*. The BYBN is a closed network (intranet) based on internet technology for all state and municipal authorities within the Free State of Bavaria. A Public Key Infrastructure (PKI) is among the service provided by the LDBV.

The PKI issues certificates for natural persons, legal persons, groups of persons, functions and automated IT processes. To the participants, PKI is offered, in order to guarantee confidentiality, integrity and liability of data or of notifications. Participants are employees of state and municipal administrations in Bavaria as well as in exceptional cases confidential third parties.

The PKI operated by the LDBV consists of several independent certificate hierarchies.

The object of this certificate policy is the certificate hierarchy, the root of which is operated by QuoVadis (http://www.quovadisglobal.com/). According to the guidelines of the QuoVadis root CA, in this PKI, the issue of certificates for SSL servers (in the following referred to as SSL certificates) is offered exclusively.

- The company of QuoVadis operates the root CA. This CA certifies subordinate sub-CAs, among others one of the Bavarian administration.
- The root CA is registered as a „trusted root certification authority" in most web browsers and operating systems.
- The LDBV operates a sub-CA in the Bavarian government network.

1.1 Overview

1.1.1 Structure and purpose of the document

With the help of this document, the general conditions for issuing and revoking certificates according to the standards of X.509 are stipulated. This document describes the specifications for the safety level of the Bavarian SSL-PKI and putting them into practice. It shall enable the reader to generally understand the SSL-PKI.

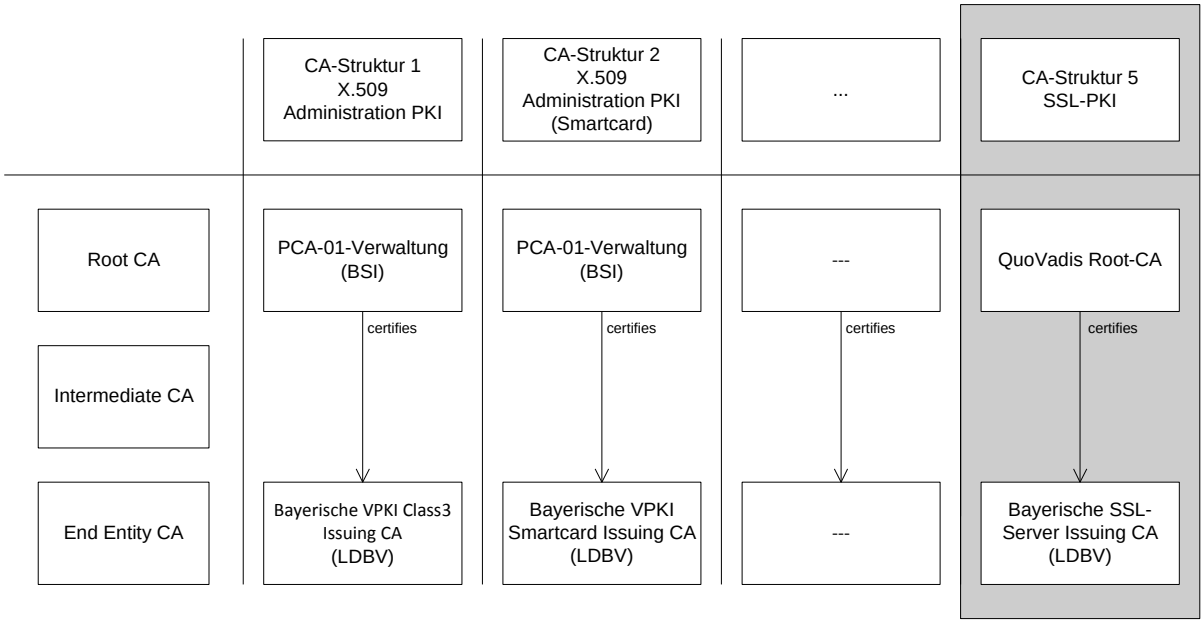
The technical measures and processes are described in detail in the operation manual [1]. The certificate policy is guided by the specifications of RFC 3647. Furthermore, the requirements and guidelines of the CA/ Browser Forum must be considered. These include among others the baseline requirements [3].

This certificate policy must be presented to the company of QuoVadis as the certifying authority. Changes to the contents must be coordinated with the company of QuoVadis.

1.1.2 Structure of the Bavarian Administration PKI

The Bavarian administration PKI consists of several certificate hierarchies according to X.509 which are independent from one another. For each individual hierarchy, different requirements apply, each of which is described in individual certificate policies.

This certificate policy deals with the requirements to the certificate hierarchy X.509 which exclusively makes available SSL server certificates in the state and municipal administration of Bavaria. It is not part of the German administration PKI operated by the BSI.



1.2 Document name and Identification

Name: Certificate Policy of the Bavarian SSL-PKI

Version: 1.3

Date: 12.04.2019

Object identifier (OID): 1.3.6.1.4.1.19266.1.2.3

The SSL-CA meets the requirements of the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates [3]. In case of any inconsistencies between the present policy and the abovementioned baseline requirements, the baseline requirements have priority.

1.3 PKI Participants

1.3.1 Certification authorities

The certification authorities issue certificates to Subscribers. For the SSL-PKI, a maximum three-stage PKI hierarchy is specified. Within this hierarchy the Subscribers form the lowest stage and the root certification authority forms the highest stage.

The route certification authority exclusively certifies subordinate certification authorities. The subordinate certification authorities exclusively issue end entity certificates.

The route certification authority of the SSL-PKI is the QuoVadis Root CA 3 G3. The object identifier (OID) of the route CA certificate is 1.3.6.1.4.1.8024.0.3.

1.3.2 Registration Authorities

For the Bavarian SSL-PKI, the present structure of registration authorities is used, which has already been set-up and used for the Bavarian administration PKI. There is a root registration authority (superior registration authority). This root registration authority registers further registration authorities. Subscribers are not registered by the route registration authority. The root registration authority is operated by the LDBV.

There is a network of registration authorities for safeguarding the identity of Subscribers as well as for verifying proofs of responsibility or proofs of representation. The registration authorities are instructed by the root registration authority on the premises of the LDBV and they are responsible for the correctness of the recorded data. The registration authorities

assure to the LDBV that they comply with this policy and with the certificate practice statement in a written self-declaration form.

1.3.3 Subscribers

Certificates and keys are exclusively handed out to the state and municipal administration in Bavaria.

Subscribers can exclusively be automated IT processes (SSL servers).

Persons responsible for certificates:

For certificates or keys, one individual natural person must always be responsible (in the following referred to as the person responsible for certificates). The person responsible for certificates must provide a proof of responsibility to the registration authority respectively.

1.3.4 Relying Parties

Relying parties verify the authentication of an SSL server according to a certificate of the Bavarian SSL PKI. For the verification, the certificate itself, the certificates superior in the certificate hierarchy, the validity as well as the revocation information available are analysed. A Relying Party can simultaneously be a Subscriber.

1.3.5 Other PKI Participants

Further participants are service providers on behalf of the PKI (e. g. operators of directory services).

1.4 Policy Administration

1.4.1 Organization Administering the Document

The present certificate policy is administered by the LDBV. Changes to the certificate policy are recorded in the section of change history at the beginning of the document. Changes in the certificate policy must be coordinated with the StMFLH. The operator of the root CA (QuoVadis) must be informed about this. In case of serious changes, the operator of the root CA (QuoVadis) should be involved.

1.4.2 Contact person

Bayerisches Landesamt für Digitalisierung, Breitband und Vermessung
<Bavarian State Office for digitalization and measurement>
IT-Dienstleistungszentrum *<IT service centre>*
- Trustcenter - *<Trust centre>*
St.-Martin-Str. 47
81541 München *<Munich>*

Telephone: +49 (0)89/2119-4924
Fax: +49 (0)89/2119-14873
E-mail: pki-support@ldbv.bayern.de

1.4.3 Person determining CPS Suitability for the Policy

By means of regular self-checking, it shall be verified, whether the certificate practice statement appropriately meets the requirements of the certificate policy.

1.4.4 CPS Approval Procedures

The regulations concerning the certificate practice service must be presented to the StMFLH as the principal and to the root certification authority upon request. The root certification authority decides about the certificate practice service afterwards.

1.5 Definitions and abbreviations

See the glossary

2 Publications and Repository Responsibilities

2.1 Repositories

The certification authorities publish the revocation information to a directory service, which is accessible via internet. The information is available by LDAPv3 according to RFC 2251. It shall also additionally be possible to retrieve the revocation information by OSCP.

The certification authorities and the server certificates shall as a standard be filed in the directory service in the point determined by the name of the certificate owner. The restricted list shall be published in the directory service entry of the certification authority. If the certificates of the certification authorities and revocation lists are to be published somewhere else, the reference to this place of the publication must be included in the certificates issued.

2.2 Publication of Certification Information

The following information shall be made available to the Subscribers and to the certificate verifiers:

- Reference to the root certificate and to its fingerprint,
- For each certification authority its certificate and its fingerprint,
- Certificate policy,
- Current revocation lists.

The technical information, in order to connect to the directory services, is published on the internet on http://www.pki.bayern.de.

To the operator of the root CA, all issued terminal certificates are additionally made available. This information is subject to a special protection and it is thus not filed in a directory which is readable to the public. The operator of the root CA exclusively receives the login details of this directory.

Within the scope of certificate transparency, all certificates issued are kept in so-called CT logs. These logs are known to the public and formatted as plain text. They are automatically read out by web browsers and used for verifying a website saved by SSL.

2.3 Time or Frequency of Publication

Certificates and restricted lists shall be published in the directory service immediately after they have been issued.

2.4 Access controls on Repositories to information

The reading access to certificates from certification authorities and to blocking information shall take place anonymously. The reading access to published end entity certificates is determined for the operator of the root CA only. The writing access is limited to authorized persons, or to automated IT processes.

3 Identification and authentication

3.1 Naming

The names used must correspond to the specifications of the standard of X.509, i. e. the attribute of “issuer Distinguished Name (DName)“ in the certificate must be identical to the attribute of “subject DName“ in the certificate of the issuing certification authority, in order to enable the set-up of the certificate path.

The root CA has assigned a unique namespace to the Bavarian administration PKI. This namespace must be used within the SSL-PKI.

3.1.1 Type of names

The following types of names shall be supported:

- DName
- URI
- LDAP names
- Principal name
- DNS name

A clear DName must be assigned to the Subscriber and to the certificate issuer. The URI in the attribute subject shall mark automated IT processes. The LDAP names must refer to the entries, in which the certificate and the revocation list of the Bavarian infrastructure PKI CA are published in the LDAP directory. A principal name is a clear character string (name) in the active directory and it describes, for example, a services instance (service principal name, SPN). If a DNS name is used, it describes a unique name in the network for a machine, for example a server.

In case of the name type of DName, the following stipulations are to be considered:

- In the attribute subject - of a certificate for certification authorities, in the DName, the components of “organizationName“ (o), “stateOrProvince“ (s) and “countryName“ (c) must be included.
- In the attribute subject of a certificate for end entities, in the DName, the components of “commonName“ (cn), “organizationalUnitName“ (ou), “organizationName“ (o), “stateOrProvince“ (s) and “countryName“ (c) must be included.

In case of the name type of DNS name, the following stipulations must be considered:

- In the “baseline requirements“ of the CAB forum [3], it is stipulated that no internal server names or reserved IP addresses may be used. Each server name must be resolvable in the internet by a DNS server.

3.1.2 Need for names

Names must be significant, clear and unique, in order to be able to identify the Subscribers. The following regulations apply:

- Certificates for SSL servers must not be issued to the names of natural persons or of legal persons.
- The name of the server instance must result clearly.
- Wildcard certificates are permitted under specific circumstances (cf. **Fehler! Verweisquelle konnte nicht gefunden werden.** and **Fehler! Verweisquelle konnte nicht gefunden werden.**).

The compliance to the naming conventions is to be made sure by the responsible certification authority.

3.1.3 Anonymity and Pseudonymity of Subscribers

Certificates of the Bavarian SSL PKI are issued for business purposes only. Therefore, anonymity and pseudonymity in the name of the certificate are not permitted within the Bavarian SSL PKI.

3.1.4 Rules for Interpreting Various Name Forms

Distinguished names in certificates shall be interpreted according to the standard of X.500 and to the syntax of ASN.1. In order to do so, the RFC's 2253 and 2616 are relevant.

3.1.5 Uniqueness of names

The clarity of names shall be guaranteed by the certification authority. A wildcard certificate may be used for several instances.

3.1.6 Recognition, Authentication and Role of trademarks

Subscribers are not permitted to use names in their certificates that infringe trademarks or brand names. The Bavarian SSL PKI is not responsible for verifying registered trademarks or brand names when issuing certificates.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of private key

If the private key is generated by the certification authority, the certification authority must encrypt the private key with an appropriate password for transport. It must be assured that the person responsible for certificates only can receive the password. The private key must be transmitted separately from the corresponding password.

If the private key is generated by the Subscriber, this Subscriber must assure the ownership of the private key to the certification authority – for example by an electronical signature of the application for the certificate, when presenting the corresponding public key to the certification authority for certification.

3.2.2 Authentication of Organization Identity

Registration authorities must register at the root registration authority as a function.

Subscribers must authenticate at one of the registration authorities subordinate to the root registration authorities

If the certificates are to be issued for servers, a person responsible for certificates must therefore be appointed by the authority responsible for the use of the certificates vis-à-vis the registration authority. This person responsible for certificates legally corresponds to a Subscriber and it shall thus be identified by the registration authority, or by the root registration authority according to the regulations of chapter 3.2.3. In addition, the registration authority must verify the data necessary for issuing the certificate.

The certification authority may only equip servers known with certificates. The certification authority must verify the authentication of an IT process.

3.2.3 Authentication of Individual Identity

The verification of the identity must take place at a registration authority. In order to do so, the Subscriber must generally appear at the registration authority in person. The registration authority must carry out the identification due to a photo identification (identity card, passport, authority identification card). In addition, the registration authority must verify the data necessary for issuing the certificate.

If the registration authority and the personnel office responsible for the Subscriber are situated in the same authority, it can be refrained from the Subscriber appearing in person as

well as from the verification by means of photo identification and the identification can take place by data synchronization instead.

3.2.4 Non-verified Subscriber Information

No stipulation.

3.2.5 Validation of Authority

No verification by the registration authority takes place, to what extent the appointed person responsible for certificates is indeed responsible for the server applied for.

3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and authentication for Re-Key After Revocation

3.3.1 Identification and Authentication for Routine Re-Key

For the routine certificate renewal, no identification and no registration (authentication) is necessary again, as the registration data remain after the expiry of the certificate and they shall be adapted by the registration authority to changes. The chain of trust is thus not broken.

3.3.2 Identification and Authentication for Re-Key After revocation

After the revocation of a certificate, a new application shall be carried out. An identification at a registration authority is not necessary again.

3.4 Identification and Authentication for Revocation Request

An application for revocation of a certificate shall be carried out by the person responsible for certificates after authentication. The authentication can either be carried out by logging on a web interface of the certification authority or, in case of revocation by telephone, with the help of its revocation password. As an alternative, the person responsible for certificates shall also be able to apply for a revocation of the certificate at the registration authority in charge. The registration authority must identify the person responsible certificates according to the regulations in 3.2.3.

The root certification authority, the root registration authority or the registration authority shall, in justified cases (e. g. in case of resignation, in case of violation of the security policy), also be able to revoke certificates without any application of the person responsible for certificates.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who can submit a Certificate Application

Each applicant, who has been identified and authenticated by a registration authority according to chapter 3.2.2 or 3.2.3, may apply for certificates.

4.1.2 Enrolment Process and Responsibilities

Applicants apply for their required certificates directly at the certification authority. In order to do so, this certification authority provides a web-based interface (web frontend).

Together with the authentication at the responsible registration authority, the applicant receives a letter with his personal login details to the web interface mentioned above. In addition, the letter contains the personal revocation password, with the help of which all or individual certificates issued to the Subscriber can be revoked.

In the course of the first login, the applicant must alter his password at the web interface such that it is known to himself only. The applicant is responsible for the fact that no authority knows his personal login details, not even the registration authorities, the certification authorities or other trust centre employees.

The applicant can apply for personal certificates, he can renew them and he can revoke them via the web interface. Digital forms are offered to the applicant, which he shall completely fill in. Afterwards, the application is transmitted to the certification authority by electronic means.

If certificates are to be applied for legal persons, for groups of people, for functions or for automated IT processes, the registration authority shall also provide the applications required therefore to the authenticated person responsible for certificates via the abovementioned web interface.

When applying, the applicant must accept the certificate policies of the certification authority.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Before the application, the applicant must authenticate at a registration authority. The registration authority enters the details of the applicant into the web interface of the certification authority. The details of the applicant are closely linked to the registration authority afterwards. The registration authority is responsible for the correctness of the data respectively. This also applies for changes in the details (e. g. e-mail-address).

4.2.2 Approval or Rejection of Certificate Applications

The certificate application made by the applicant shall be transmitted to the certification authority immediately.

The certification authority shall verify the application for completeness. Afterwards, a verification of the application details together with the registration data shall take place, so that the applicant can only apply for certificates for servers which have been registered for him by the registration authority beforehand. As a rule, this happens within the web interface during the application.

If, for any reason, an application is rejected, the applicant must be informed about this stating the reasons.

4.2.3 Time to Process Certificate Applications

The certificate applications must be processed by the certification authority within one working day.

4.2.4 Certificate Authority Authorization (CAA)

Currently, no verification of Certification Authority Authorization (CAA) DNS entries (RFC 6844) is in place.

The end entity certification authorities of the SSL PKI underlie technical restrictions, which is why there is no obligation to use CAA.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

Certificate applications shall be processed by the certification authority.

It shall regularly be monitored by the root certification authority, if the certificates applied for have been issued properly.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

If an application for a certificate is rejected, the applicant shall receive a notification respectively. Otherwise, the applicant shall receive the certificate, or the PSE from the certification authority of the Bavarian SSL PKI.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Upon receipt of the certificates, the Subscriber must verify this material. If there is no objection on behalf of the person responsible for certificates, the certificate must be considered accepted.

In case of flawed certificates, the person responsible for certificates must revoke the certificates. The person responsible for certificates himself must apply for a new certificate (new application for a certificate).

4.4.2 Publication of the Certificate by the CA

After issuing the certificates, the certification authority shall publish these certificates in the provided directory services according to section 2.2. A publication of the certificate shall take place independent of the acceptance by its owner, (or by the person responsible for certificates).

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

It is not necessary to notify further involved parties of issuing a certificate.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The person responsible for certificates shall take over the responsibility for appropriately and safely using the certificate and the private key belonging to it. The person responsible for certificates can grant access to the private key to further persons.

The person responsible for certificates especially has the following tasks:

- to apply for a revocation in case of changes of the certificate data,
- to keep the private key safe,
- in case of loss or compromising of the private key, to apply for a revocation of the certificate.

Access to the private key must take place secured by the access protection of the operating system or by organizational measures.

The Subscriber may only use the private key and the certificate belonging to it for the intended purposes stated on the certificate.

4.5.2 Relying Party Public Key and Certificate Usage

Each participant using the certificate of another participant must assure that this certificate is only used for the intended purpose stated in the certificate. In addition, every time the certificate is used, he must verify the validity of the certificate.

4.6 Certificate Renewal

It is not permitted to renew a certificate without renewing the key.

4.7 Certificate Re-Key

4.7.1 Circumstances for Certificate Re-Key

An application for a renewal of a key and of a certificate may only be processed, if

- a certificate has already been issued to this Subscriber and if
- this old certificate is about to expire.

If a certificate has been revoked before its validity has expired, a certificate renewal must not take place. A new application for a certificate must take place.

4.7.2 Who May Request Certification of a New Public Key

New certificates shall be applied for by the person responsible for certificates.

4.7.3 Processing Certificate Re-Keying Requests

The person responsible for certificates shall be informed of the upcoming certificate extension six weeks before the end of the validity.

The person responsible for certificates must care for the re-key and re-certification independently.

A new registration is not necessary.

4.7.4 Notification of New Certificate Issuance to Subscriber

Cf. point 4.3.2**Fehler! Verweisquelle konnte nicht gefunden werden.**

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

Cf. point 4.4.1

4.7.6 Publication of the Re-Keyed Certificate by the CA

Cf. point 4.4.2

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Cf. point 4.4.3

4.8 Certificate Modification

It is not intended to modify a certificate. If application data change, the certificate must be revoked and issued again.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for revocation

A certificate must be revoked, if at least one of the following points is the case:

- The Subscriber demands the revocation of his certificate to his certification authority in writing.
- The Subscriber informs his certification authority that the certificate request was not authorized and that it is thus not valid.
- The Subscriber no longer requires the certificate because
    - he is no longer responsible for the server or
    - the DNS name used in the certificate no longer belongs to him (it has been given to another person / institution).
- The Subscriber is no longer authorized to own a certificate, for example because
    - he does not comply with the certificate policy or
    - the DNS name used in the certificate was given to another person or
    - the certificate was not used according to regulations.
- The details of the certificate are no longer valid (for example change of the DNS name).
- The private key got lost or it was compromised.
- The certification authority has found out that a wildcard certificate is or was fraudulently used.
- The registration authority or the certification authority does not comply with the certificate policy or certificate practise statement.
- The registration authority or the certification authority is cancelled without substitution.
- Compromising of the private CA key.
- The technical content or the format of the certificate bears a not acceptable risk for the providers of application software or for PKI participants (for example, the CA/browser forum can determine that a cryptographic / signature algorithm or a key size that is no longer recommended is a not acceptable risk and that such certificates should be revoked or replaced by the registration authority or by the certification authority within a given length of time respectively).

4.9.2 Who can Request revocation?

The following persons or institutions may apply for a revocation:

- the Subscriber or a person responsible for certificates in case of group certificates and of server certificates,
- the legal representative of the Subscriber,
- the registration authority,
- the root registration authority,
- the certification authority,
- the root certification authority.

4.9.3 Procedure for Revocation Request

Revocations are only carried out by the certification authority which has issued the certificate to be revoked.

The Subscriber must apply for a revocation at the certification authority. In order to do so, there are three opportunities:

- via the web interface (web frontend, as a rule continuously available (24x7), exceptions according to SLA),
- by telephone at the ServiceDesk of the ITDLZ in the LDBV (telephone: +49 (0)89/2119-4924, corresponding to the service catalogue available from Monday until Friday from 7:00 a.m. until 6 p.m.),
- in person at the registration authority.

In order to apply for a revocation via the web interface, the Subscriber must register to it with his personal details. In order to carry out the revocation, the Subscriber must enter his revocation password. The revocation shall take place automatically without any further personnel interaction.

In order to apply for a revocation by telephone, the Subscriber must know his revocation password and he must let it know to the employee of the trust centre hotline in extracts. The employee of the trust centre hotline enters the revocation electronically and passes it on to the certification authority via the web interface which automatically carries out the revocation without any further personnel interaction.

In order to apply for a revocation in person, the Subscriber contacts his registration authority. This registration authority then verifies the identity of the applicant and then immediately passes the application for revocation on to the certification authority. In order to do so, no revocation password is necessary. The employee of the registration authority enters the revocation electronically and passes it on to the certification authority via the web interface which automatically carries out the revocation without any further personnel interaction.

4.9.4 Revocation Request Grace Period

As soon as a reason for a revocation becomes known, the person responsible for certificates must apply for a revocation without delay.

4.9.5 Time Within Which CA Must Process the Revocation Request

The certification authority must carry out the revocation within 24 hours.

4.9.6 Revocation Checking Requirements for Relying Parties

A certificate verifier must verify the validity of the certificates every time they are used. In order to do so, he shall obtain the current revocation list and he shall verify it for the certificate used.

4.9.7 CRL Issuance Frequency

The restricted lists of the certification authorities shall have a duration of validity of 24 hours and shall be issued and published again every 12 hours.

4.9.8 Maximum latency for CRLs

After the generation of the revocation list, it shall be published immediately afterwards without delay.

4.9.9 On-Line Revocation/Status Checking Availability

The revocation lists of the SSL CA shall also be published on an OCSP server.

4.9.10 On-Line Revocation Checking Requirements

All OCSP servers used are operated according to the standard of RFC 2560. OCSP clients shall also work according to this standard, in order to guarantee a correct communication.

4.9.11 Other Forms of Revocation Advertisements available

Except for revocation lists, no other forms of revocation information need to be offered.

4.9.12 Special Requirements re-Key Compromise

When compromising a private key of a participant, the certificate belonging to it must be revoked without delay.

In case of compromising a private key of a certification authority, the certificate of the certification authority must be revoked without delay. In addition, all certificates issued by this certification authority must be revoked.

4.9.13 Circumstances for suspension

Temporarily revocation or suspension of certificates is not permitted.

4.9.14 Who can Request Suspension?

Temporarily revocation or suspension of certificates is not permitted.

4.9.15 Procedure for Suspension Request

Temporarily revocation or suspension of certificates is not permitted.

4.9.16 Limits on Suspension Period

Temporarily revocation or suspension of certificates is not permitted.

4.10 Certificate Status Services (OCSP)

4.10.1 Operational Characteristics

The reference to the OCSP place of publication must be deposited in the certificates issued.

4.10.2 Service Availability

In order to keep the number of technical failures as small as possible, OSCP services should be built up redundantly.

All certificate verifiers should also be able to use the OCSP service, i. e. neither firewalls nor other access restrictions should obstruct the certificate verifier from using the OCSP service.

4.10.3 Operational Features

The OCSP service should verify, if an enquired certificate has been issued by the certification authority deposited in the OCSP. If this is not the case, the OCSP service may not answer with “good”.

4.11 End of Subscription

The contractual relationship can be terminated, if the Subscriber would no longer like to use the service of the Bavarian SSL PKI, or if the Bavarian SSL PKI ceases the service. If the certificates of the Subscriber are still valid during the termination, they must be revoked.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

No depositing of keys shall take place (key backup).

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Session keys are not deposited.

5 Facility, Management, and Operational Controls

5.1 Physical Controls

The components necessary for the operation of the Bavarian SSL PKI must be operated securely and appropriately availably. The components shall be placed in physical protection zones. The access to these protection zones shall be reduced to a closed user group.

The measures for operating the IT infrastructure of the LDBV by the IT DLZ correspond to the BSI IT baseline security according to the security policies [2].

5.1.1 Site Location and Construction

The LDBV operates a large computer centre in the IT service centre with servers for various different purposes of use. The servers can be placed in different protection zones depending on their protection requirements.

The computer centre is monitored in an operation of 24x7h by the staff. This includes among others

- video surveillance of the premises and of the building,
- monitoring of sensors concerning climate, ventilation, temperature, plumbing and electrical engineering,
- monitoring of the fire alarm system,
- monitoring of the water alarm system.

The staff can, if applicable, make further emergency calls, if they do not take place automatically, and it can grant access to relief forces.

5.1.2 Physical access

The servers of the issuing certification authorities are situated in the access controlled rooms of the LDBV.
The physical access to servers in the computer centre is limited to administrators. These administrators look after the hardware used.

5.1.3 Power and Air Conditioning

The general policy of the computer centre applies. In this general policy, it is regulated that the power supply is redundantly configured to all servers. For power cuts, UPSs and an emergency power system (fuel-driven) are available.

The rooms in the computer centre are automatically ventilated.

5.1.4 Water Exposures

The general policy of the computer centre applies. In this general policy, it is regulated that a water warning system is installed.

5.1.5 Fire Prevention and Protection

The general policy of the computer centre applies. In this general policy, it is regulated that a fire alarm system is installed.

5.1.6 Media Storage

Mobile data carriers must be kept safe closed or protected from unauthorized access. The details are regulated in the operation manual [1].

5.1.7 Waste Disposal

The general security policy for the computer centre applies.

It has been pointed out to the administrators that servers from the field of PKI are especially worthy of protection. During the disposal, it must be made sure that data, especially personal details, are certainly deleted.

5.1.8 Off-Site Backup

A backup at another site does not exist.

5.2 Procedural Controls

Authorized personnel only shall be permitted to carry out tasks regarding key management and certificate management or to make changes to the configuration of the CA software / RA software. These rights are to be anchored in a role concept.

5.2.1 Trusted Roles

The following safety-relevant roles are to be determined:

- network administrators,
- server administrators,
- administrators of the PKI operation,
- employees of the root registration authority,
- employees of the registration authorities,
- auditors.

The LDBV, as the operator of the Bavarian administration PKI, installs the PKI operation and the root registration authority. The root registration authority installs the certification authorities and the registration authorities. The root registration authority identifies and authorizes the PKI administrators or the employees of the subordinate registration authorities. The auditors are appointed by the root certification authority.

5.2.2 Number of Persons Required per Tasks

For the sake of safety and availability of the PKI, the relevant tasks are fulfilled according to the four-eye principle. This includes, for example, the recovery of the key material in the cryptographic module as well as all safety-relevant configurations at the CA.

5.2.3 Identification and Authentication for Each Role

The identification with the help of servers, as a rule, shall take place by means of a user name and a password. The general policy for the computer centre applies, which, among others, regulates the password policy.

The identification with the help of the HSM takes place by means of personal admin USB tokens.

The identification for configuration changes in the CA takes place by means of smart cards. All changes (e. g. to certification authorities and certificate templates) are possible in the four-eye principle only.

The identification of the PKI roles (root RA, RA, administrator, applicant) at the web frontend takes place by means of a user name and a password.

5.3 Personnel Controls

The administrators and the employees of the root registration authority and the subordinate registration authorities are instructed by the LDBV before they get started with their work.

New employees of an existing registration authority shall be instructed promptly by the LDBV. Refresher courses and instructions due to larger changes must be offered as required.

5.3.1 Qualifications, Experience, and Clearance Requirements

New PKI administrators are familiarized by means of suitable instructions and briefings by their colleagues.

Employees of trust centres (root RA) are familiarized by means of instructions and briefings by PKI administrators.

Persons who are responsible for or employees of registration authorities are obliged to take part in the instruction offered by the LDBV.

Employees of the service desk are familiarized with their tasks by the trust centre (root RA).

5.3.2 Background Check Procedures

For all employees of the LDBV, the following shall be effected when they are employed:

- the qualifications are verified (school education, training, advanced training, if applicable, job references, if applicable) and
- a security check (including the request of a certificate of good conduct) is carried out.

5.3.3 Training Requirements

Persons working in the field of PKI must meet professional minimum requirements. Depending on the field of activity, these professional minimum requirements can range from technical knowledge and experience to experience in data protection and data security, e. g. in the field of human resources.

New employees in the field of PKI technology and trust centre receive an intensive job training with successive job enlargements and extension of rights.

Employees of registration authorities receive an instruction by employees of the LDBV.

5.3.4 Retraining Frequency and Requirements

All persons involved in the PKI should regularly take part in advanced training and in further education.

5.3.5 Job Rotation Frequency and sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

Appropriate sanctions according to the operation manual [1] are imposed on unauthorized action / activity.

5.3.7 Independent Contractor Requirements

Exclusively registration authorities and their employees are the external service providers of this PKI. These employees are instructed by the LDBV. The root registration authority located in the LDBV monitors the activities of the registration authorities.

5.3.8 Documentation Supplied to personnel

Documentation for PKI administrators are mainly technical manuals for hardware or software, in addition an operation manual [1], an architectural concept [1a], a security concept [1b], a backup recovery concept [1c].

Documentation for registration authorities and for users are issued, developed further and published on the internet by PKI administrators and / or by trust centre employees.

5.4 Audit Logging Procedures

In the security concept [1b], events to be monitored are to be defined such that violations of the present certificate policy can be recognized. The events are to be kept in the records. The records shall be analysed. The analyzation can be supported by suitable filter mechanisms and alarm mechanisms. The mechanisms and the incidental data should be verified and analysed at least every working day.

All components of the Bavarian SSL PKI shall be kept up to date by regular updates. The administrators of the components are responsible for detecting current weak points of the components and for stopping them. Due to the input of the updates or patches, disturbances of the operation shall be expected. The principle of “safety before availability“ stipulated in the security policy (BayITSiLL) applies. The administrators shall keep records of their activities and of their verifications.

In case of serious violations of the present certificate policy and of the certificate practise statement, the person responsible for IT security is to consult directly and without delay.

The measures are to be verified regularly. Records of the verification shall be kept. In doing so, it shall first of all be assured that the current measures meet the specifications. The specifications result from the present certificate policy and from the certificate practise statement. The auditors shall carry out the verification.

5.5 Records Archival

The following data must be archived by the root registration authority:

- All applications concerning a registration authority or a certification authority.

All applications concerning registration authorities and certification authorities shall be archived as long as the registration authority or the certification authority exists and after that for seven further years.

The following data must be archived by the registration authorities:

- All applications concerning a Subscriber.

The data archived by the registration authority shall be archived as long as the Subscriber takes part in the administration PKI and after that for seven further years.

The following data must be archived by the certification authority of the Bavarian SSL PKI:

- certificates of the certification authorities,
- certificates of the Subscribers,
- log files (audit log).

The certificates of the certification authorities shall be archived until the expiry of the validity of the certificate and after that for five further years. The certificates of the Subscribers shall be archived until the expiry of the validity of the certificate and after that for seven further years.

Private keys of Subscribers may be archived.

5.6 Key changeover

A key change at a certification authority shall always take place, if the current key can no longer issue certificates whose validity exceeds the validity period of the CA itself (shell model).

The key change of the certification authority must take place according to the four-eye principle.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

When compromising a certification authority, the operation of this certification authority must be stopped without delay and the certificate of this certification authority must be revoked without delay. All certificates issued by this certification authority must also be revoked. The users affected must be informed in an appropriate manner.

In the certification process for a certification authority, the root certification authority shall receive:

- a revocation password
- the names, telephone numbers and e-mail-addresses of the persons authorized to revoke for this certification authority.

One of the persons authorized to revoke must hand in the revocation to the root certification authority without delay. In order to do so, he / she shall have the following possibilities:

- telephone,
- fax or
- e-mail.

The root certification authority will contact the operator of the certification authority by telephone (main number from the telephone book) afterwards and communicate with at least one person authorized to revoke. The person authorized to revoke must say the revocation password.

The root certification authority shall take acceptable measures in the commercial context respectively [4], in order to revoke the certificate quickly upon receipt and after a successful validation of an application for revocation. A new restriction list is issued and published immediately.

Computing Resources, Software, and/or Data Are Corrupted After compromising, the PK infrastructure can be rearranged under certain framework conditions.

First of all, the causes of compromising must be found.

Technical flaws must be processed and corrected.
Human flaws must be reduced to a minimum risk by means of measures, regulations and the like.
The exact measures are defined in the safety concept [1b]. External auditors can be granted access to this document.

Before a resumption of the PKI operation:

- the technical environment should be verified again for the maximum possible security and
- the certification authority must be equipped with new key material.

5.8 CA or RA Termination

If a certification authority is closed, the certificate of this certification authority and all other certificates issued by it must be revoked. The process corresponds to the process of **Fehler! erweisquelle konnte nicht gefunden werden.**. The revocation list shall be valid until the end of the validity of the certificate of the certification authority.

If a registration authority is closed, the users registered by it can be taken over by another registration authority. If no other registration authority agrees to take over these users, the

users must be logged out. The certificates belonging to this registration authority are to be revoked automatically.

The particulars are regulated by the operation manual [1].

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The key pairs of the certification authorities shall be generated in a cryptographic module (cf. 6.2).

The key pairs for Subscribers may be saved das a file (in software) or in hardware tokens (chip card or USB token).

Private keys for IT processes with wildcard FQDNs, i. e. with a star in the first part of the URI, must be generated in hardware (e. g. HSM or smart card) and they must not leave the hardware (except for backup purposes).

6.1.2 Private Key Delivery to Subscriber

There is no transmission of private keys necessary.

6.1.3 Public Key Delivery to Certificate Issuer

The applicant sends his public key to the certification authority together with his certificate application. During the transmission, the public key must be saved before any changes are made. After the certification of the key, the certification authority publishes the public key corresponding to the publishing regulations.

6.1.4 CA Public Key Delivery to Relying Parties

When handing over the certificates to the Subscriber, a certificate chain is also enclosed.

The certificate of the certification authority of the Bavarian infrastructure PKI is been placed in the directory service and is then available to all communication partners.

6.1.5 Key Sizes

Only combinations of key algorithm and key length should be used, which have been categorized as safe for the validity period by the BSI [5] and which are sufficient to the FIPS standard [6]. The usability of the key algorithms used must be tested regularly. If a key algorithm is no longer categorized as safe enough, no further keys using this algorithm must be issued.

6.1.6 Public Key Parameters Generation and Quality Checking

The quality of the generated public key parameters of the certification authority of the Bavarian SSL PKI should correspond to the cryptographic algorithms [5] categorized as suitable by the BSI. In special cases, the recommendations of the BSI can be considered as not binding for the Bavarian infrastructure PKI. These include, for example, compatibility problems concerning clients corresponding to the standard according to BayITS-11 [7], and which are thus common.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

Certification authority:

The certification authority of the SSL PKI is considered as technically constrained in the sense of baseline requirements of the CAB forum [3]. Requirements to different certificate extensions result from this.

The certificate of the certification authority of the Bavarian SSL PKI contains a key use extension (X.509v3 keyUsage extension) marked as critical with the entries of keyCertSign and

crlSign, i.e. these certificates can only be used for the verification of certificates and of restriction lists.

The extended key use (X.509v3 ExtendedKeyUsage extension) is marked as not critical. In this extension, all intended purposes of keys must be entered, for which the CA issues end entity certificates.

The basic constraints (X.509v3 BasicConstraints extension) also marked as critical make it clear that this is a certificate from a certification authority.

Furthermore, the certificate of the certification authority contains an extension, which is marked as not critical, to name extensions (X.509v3 NameConstraints extension). Here, URIs are permitted or prohibited.

End entities:

The key use extension (X.509v3 keyUsage extension) marked as critical in the certificates for Subscribers, may contain the following entries: DigitalSignature, nonRepudiation, keyEncipherment, dataEncipherment. Therefore, they can only be used for electronic signatures, authentication and encryptment.

Each CA product used offers different certificate templates, which, among others, can differ in their intended use. This policy allows templates for:

- Web servers (mixed together with SSL servers).

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The keys of the certification authority of the Bavarian SSL PKI must be generated and saved in a cryptographic module. Keys of Subscribers do not have to be generated and saved in hardware. Keys with wildcard FQDNs must be generated in hardware (e. g. HSM or Smartcard) and they are not permitted to leave the hardware (except for backup purposes).

Each person responsible for certificates must protect his or her own private key(s) from loss, from changes and from third party access.

6.2.1 Cryptographic Module Standards and Controls

The cryptographic module used at the certification authority has a safety certification according to FIPS 140-2 level 3.

6.2.2 Private Key (n out of m) Multi-Person

The private keys of the certification authority of the Bavarian SSL PKI must be protected according to the four-eye principle.

6.2.3 Private Key Escrow

It is not permitted to deposit the private keys of the certification authorities of the Bavarian SSL PKI.

The deposition of private end-entity-keys takes place as indicated in section 4.12.

6.2.4 Private Key Backup

The private keys of the certification authority of the Bavarian SSL PKI are in the HSM and they must be saved with the help of backup methods of the HSM manufacturer.

A central backup of private end-entity-keys does not take place. Subscribers are permitted to save their keys themselves, if the protection of the private key is not released or dissolved.

6.2.5 Private Key Archival

No stipulation.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

It is not required to retain the private key of the certification authority of the Bavarian SSL PKI after the end of its use any longer.

6.2.7 Private Key Storage on Cryptographic Module

The private key of the certification authority of the Bavarian SSL PKI is placed encrypted in the HSM.

6.2.8 Method of Activating Private Key

For activating the private key of the certification authority for the certification of keys for subordinate certification authorities, it is sufficient to enter a password into the CA server at the start of the certification service. The password required is known to authorized PKI administrators only. It is placed encrypted in a configuration file. All configuration files are protected by system access rights.

Private keys of end users shall be protected by at least a password / PIN, which has to be entered when activating the private key. In addition, private keys of end users are permitted to be saved by means of storage of the private keys on a hardware token (smart card or USB token).

6.2.9 Method of Deactivating Private Key

The private key of the certification authorities of the Bavarian SSL PKI is deactivated as soon as the certification service on the CA server is stopped.

In order to deactivate private keys of end users, the following opportunities are permitted:

1. If the private key remains inactivated for a number of time upon its activation, it will automatically be deactivated.
2. The software for certificate administration offers the possibility to manually deactivate keys again, for example with the help of a button.
3. If the private keys are saved on a hardware token, the deactivation will take place when removing the token from the reader.
4. An activation of the private key shall remain valid for one action only and afterwards, the key is automatically deactivated again.

6.2.10 Method of Deactivating Private Key

Destroying a private key of a CA can come into question from two situations:

- the utilization period of the CA key has expired or
- the key of the CA has been revoked.

The key material on the hardware token must be securely deleted. The exact process depends on the token used and it shall be stipulated in the operation manual [1].

6.2.11 Cryptographic Module Rating

The cryptographic module has a safety certification according to FIPS 140-2 level 3.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Public keys certified by the certification authority of the Bavarian SSL PKI are archived in the database of the certification authority.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The following maximum certificate validities shall apply in the SSL PKI:

- certificate of the root CA of QuoVadis: 20 years
- certificate of the issuing CA of LDBV: 10 years
- server certificates: 3 years (starting from 1.3.2018 2 years)

The validity of the CA certificate must be longer than the period of use of the private key, i. e. it is not permitted to use the private key of the CA for issuing certificates until the end of the certificate validity. In this way, it is assured that the subordinate certificates are no longer valid than the certificate of the issuing instance (shell model).

6.4 Activation Data

The storage of the private key on the PC / system of the Subscriber shall always take place secured, meaning, for example, with a password protection. As soon as the private key is used, the Subscriber must initially release this protection.

6.4.1 Activation Data Generation and Installation

In case of a centralized key generation, the activation data (PIN, password) protecting the private key must be generated by a secured application and they must be transmitted to the user especially protected.

While producing the private kay the Subscriber has to create the activation data (PIN, password).

For the activation data, at least 6 characters of at least 2 groups of characters (capital letters, small letters, numbers and special characters) shall be used.

6.4.2 Activation Data Protection

The activation data shall appropriately be protected against loss, theft, changes, not authorized disclosure or not authorized use.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

All computer systems and server systems taking part in the PKI within the scope of this certificate policy must meet specific safety standards. These include:

- current status of the operating system (current security patches and so on),
- virus scanner (PC: protection from keyloggers),
- user authentication when logging on to the operating system.

For servers additionally:

- penetration test,
- minimum system – required software only is installed,
- in case of safety-critical flaws, the system shall be brought to the current safety level as fast as possible; a temporary shutdown shall possibly be considered,

- safety-relevant processes shall be kept in the records,
- restricted access authorizations and access permissions,
- restricted communication interfaces – required communication interfaces only.

These specifications meet the general policies for servers of the LDBV/ IT-DLZ.

6.5.2 Computer Security Rating

A threat analysis must be carried out and an appropriate security concept must be generated.

6.6 Life Cycle Technical Controls

For software in the field of user administration and certificate administration, standard products shall be used as far as possible, which require most small adjustments to the operating environment.

6.6.1 System Development Controls

The software used must resist generally known threat scenarios.

PKI systems are to be developed such that the manufacturer has no unnoticed access to the operating data (private keys, PINs, user data).

6.6.2 Security Management Controls

The increased security requirements of the PKI components must be pointed out to the system administration. It shall especially be organizationally regulated that the operation data (private keys, PINs, user data) must not be read or passed on by the system administration.

It shall further be (organizationally) regulated that developers of the systems / software shall not have any access to the operating data of the operating environment. If developers, for example when correcting errors, have to work in the operating environment, confidentiality shall be demanded on behalf of the developers.

If records of the system have to be forwarded to developers (e. g. for detecting errors), data which is not required, especially operating data, shall be removed.

Operating system updates and new program versions must undergo functional and quality assuring tests before being imported into the operating environment.

Before launching the PKI components, penetration tests of the operating environment shall be carried out. These tests and similar ones shall be repeated regularly.

6.7 Network Security Controls

For achieving an increased security of the PKI, components generating, processing or saving private keys shall be provided with safety measures respectively, also including network security.

The safety measures put into practice in the network are described in the operating manual [1] or in the security concept [1b]. Among others, this includes that

- PKI servers are placed in their own network area and they are separated from other systems by firewalls,
- that network ports, which are no longer required, are deactivated,
- that communication links to other servers are either required by PKI software or by software necessary for operating a server (e. g. operating system updates, backup software and so on).

6.8 Time-Stamping

A timestamp service is not offered at present.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

The certificates issued correspond to X.509v3 and serve the intended purposes mentioned in **Fehler! Verweisquelle konnte nicht gefunden werden.**.

A Subscriber must own one valid certificate per type of certificate only.

7.2 CRL Profile

The revocation lists issued correspond to CRLv2.

7.3 OCSP Profile

OCSP answers meet the standard according to RFC 2560.

7.4 LDAP profiles

The LDAP directory services are configured according to the standards of LDAP v3 and RFC 4510.

8 Compliance Audit and Other Assessments

The work processes of the certification authorities shall regularly be tested for conformity with the certificate policy and with the certificate practice statement.

8.1 Frequency and Circumstances of Assessment

The first verification shall take place before starting the operation of a certification authority or of a registration authority. Further verifications of a certification authority or of a registration authority shall be carried out regularly. Registration authorities shall be verified at least once a year.

8.2 Identity/ Qualifications of Assessor

The verification of the root registration authority and of the certification authorities shall take place by the root certification authority or by an office commissioned by the root certification authority.

8.3 Assessor's Relationship to Assessed Entity

Self-checking is permitted.

If verification is carried out by an independent verifier, this independent verifier is not permitted to be a member of the office to be verified simultaneously. In this connection, an authority, a department, a unit or a subject area is to be understood as an office.

8.4 Topics Covered by Assessment

All areas relevant to the PKI may be verified.

8.5 Actions Taken as a Result of Deficiency

Detected defects must be removed promptly in consultation with the verifier and with the verified party. If a certification authority does not perform the removal of defects within the agreed period of time, the verifier must induce the root registration authority to close down the registration authority. If a certification authority does not perform the removal of defects within the agreed period of time, the verifier must induce the certificate of the certification authority to be revoked.

8.6 Communications of Results

A publication of the results outside of the offices concerned is not intended.

9 Other Business and Legal Matters

9.1 Fees

No fees are charged at present.

9.2 Financial Responsibility

The financial responsibility for the LDBV shall be taken by the Free State of Bavaria. It shall be held liable for several liabilities.

Moreover, the Free State of Bavaria is not eligible for insolvency. According to § 12 para. 1 no. 1 InsO *<German Insolvency Code>*, it is illegal to open insolvency proceedings concerning the asset of a state.

9.3 Confidentiality of Business Information

All information, which is not published by the LDBV or by any other authority, shall be treated confidentially.

According to § 37 para. 1 BeamtStG *<German status law for officials>*, officials shall remain silent about the business matters they became familiar with during or on occasion of their official duties. This shall also apply beyond the area of an employer as well as beyond the termination of the civil service. Public sector employees shall be sworn to secrecy according to § 3 para. 2 TV-L *<tariff commission of German states>*.

9.4 Privacy of Personal Information

The LDBV and all other authorities involved shall meet all legal requirements concerning data protection.

Personal data shall only be passed on to third parties within the scope of stipulations or due to a legal obligation.

9.5 Intellectual Property rights

The legal requirements for copyright law shall apply. In this certificate policy, no specific regulations deviating from the law shall be made.

9.6 Representations and Warranties

The statutory warranty regulations shall apply.

9.7 Disclaimers of Warranties

An exclusion of warranty is not stipulated.

9.8 Limitations of Liability

Liability is excluded. This shall not apply for

1. Damages caused by injury to life, body or health or for deliberate damages, based on a negligent breach of duty and

2. miscellaneous damages based on a grossly negligent or deliberate breach of duties.

9.9 Indemnities

An exemption from liability shall not take place.

9.10 Term and Termination

This certificate policy shall enter into force the day of its publication. The validity of the certificate policy shall end when publishing a new certificate policy or when ceasing the certification services.

9.11 Individual Notices and Communication with Participants

No regulations shall be made in this certificate policy respectively.

9.12 Amendments

Changes and supplements to the certificate policy shall be proposed by the LDBV and they shall be reconciled with the StMFLH *< Bavarian state ministry of finance, of state development and home affairs>* as the principal. The root certification authority shall only be included in case of serious changes and it shall otherwise be informed only.

New versions of the certificate policy shall be published on the web site of the LDBV. Certification authorities taking part shall be briefed on new versions.

The LDBV shall decide if, in case of changes in the certification authority, a new policy identifier shall be used. This shall especially be the case, if the certificate policy has considerable changes compared to the previous certificate policy.

9.13 Dispute Resolution Provisions

An arbitration in terms of §§ 1025 ff. ZPO *<civil process order>* is not intended.

9.14 Governing Law

The legal place of jurisdiction shall apply.

9.15 Compliance with Applicable Law

German law shall apply.

9.16 Miscellaneous Provisions

If individual provisions of this certificate policy are or become ineffective, the rest of the contents of the certificate policy shall remain unaffected. Incidentally, a gap shall not affect the effectiveness of the certificate policy either. Instead of the ineffective provision, the effective provision shall be deemed agreed, which is closest to the provision originally intended, or which would have been regulated based on the spirit and purpose of the certificate policy, if the point had been considered.

10 Glossary

AIA	*Authority Information Access*, attributein the certificate pointing to publication point of the superordinate CA certificate
BSI	Bundesamt für Sicherheit in der Informationstechnik *<Federal Office for Information Security>*
BYBN	Bayerisches Behördennetz *<Bavarian government network>*
CA	*Certification Authority*
CAB	*CA/Browser Forum*, pool of CA operators and developers of operating systems, web browsers and other applications using certificates https://cabforum.org/
CA policy	Certificate policy of a PKI; the present document
CDP	*CRL Distribution Point*, attribute in the certificate pointing to publication point of the revocation list
Certificate	ensures the allocation of a public key to a participant
Certification Authority	Issues certificates
CPS	*Certificate Practice Statement*, regulations concerning the certificate practice service
CRL	*Certificate Revocation List*
DN	*Distinguished Name, see DName*
DName	*Distinguished Name,* a clear object name in LDAP directories
End entity CA	Certification authority issuing certificates for end entities (e. g. for users or for servers)
FQDN	*Fully Qualified Domain Name*, full name of the server including the domain name
Hardware token	A hardware token is a hardware for the storage of private keys, which, among others, prevents an unauthorized use of the private key.
Internal Server Name	*Internal Server Name*, server name (with or without a not registered domain name), which is not resolvable in the public DNS.
IT-DLZ	*IT service centre*, a plant section of the LDBV and the operator of the Bavarian SSL PKI
HSM	Hardware Security Module, module connected to the CA server for keeping safe encryption keys and signature keys of the CA
Key Backup	Storage of private encryption keys for restoring them later
Key Recovery	Restoring private keys on demand of an owner, e. g., if the private key has got lost and something has to be decrypted
Key Escrow	Restoring private keys on demand of a third party, e. g. in case of longer illness of a user, or if something has to be decrypted during his absence
Key pair	A key pair consists of a private key and of a public key. The private key can only be accessed by the owner and it is subject to special protection. The public key is known to all participants.

LDAP	*Light Directory Access Protocol*, directory service (e. g. for certificates or for restricted lists)
LDBV	*Landesamt für Digitalisierung, Breitband und Vermessung* <*Bavarian State Office for digitalization and measurement*>
OCSP	*Online Certificate Status Protocol*
PGP	*Pretty Good Privacy*
PKI	*Public Key Infrastructure*, organizational and technical entity, the participants of which are certified by a common root CA
PIN	*Personal Identification Number*, secret sequence of numbers or character string (e. g. in order to protect the private key)
PSE	*Personal Security Environment* (e. g. password-protected P12 file)
RA	*Registration Authority*
Registration authority	Authority registering a person as a user and identifying this person
Reserved IP address	*Reserved IP Address*, an IPv4 or an IPv6 address, which has marked the IANA as reserved: http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml
Revocation list	List of issued and signed by a CA and containing revoked certificates
RFC	*Request for Comment*, documents for worldwide standardizations
RFC3647	This RFC shall serve the description of documents describing the operation of the PKI, especially of the CA policy and of the CPS.
RFC-822 Name	e-mail address
Root CA	(also known as root certification authority) the highest certification authority of a PKI
SAN	Subject Alternative Name
SigG	German Digital Signature Act; sets general conditions, under which a digital signature is of equal legal status as a handwritten signature.
SLA	*Service Level Agreement* (agreement concerning the operation & the availability of servers between server administrators and PKI administrators)
S/MIME	*Secure Multipurpose Internet Mail Extensions*, standard for secure e-mails
SSL	*Secure Socket Layer*, protocol for the transport security of a client-server communication
StMFLH	*Staatsministerium der Finanzen, für Landesentwicklung und Heimat* <*Bavarian state ministry of finance, of state development and home affairs*>, an office superior to the LDBV and principal of the Bavarian infrastructure PKI
Trust centre	Certification service provider
UID	*Unique Identifier*, unique number

UPS	Uninterruptible power supply, battery system ensuring the power supply for servers for a short time during a power cut or the like
URI	*Uniform Resource Identifier*, a character string serving for the identification of a resource (e. g. for the denomination of resources on the internet and there, above all, WWW)
Wildcard certificate	Certificate bearing a (*) in part of a FQDN, and which can thus be used for several authorities
X.509v3	Standard for certificates

11 References

[1] Operational concept for the Bavarian administration PKI
documents connected to it:

- [1a] Architectural concept
- [1b] Security concept
- [1c] Backup recovery concept

[2] BSI, IT baseline security manual
http://www.bsi.de/gshb/

[3] “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates“ or “Baseline Requirements”
http://www.cabforum.org

[4] CP/CPS of the QuoVadis root CA
https://www.quovadisglobal.bm/~/media/Files/Repository/QV_RCA1_RCA3_CPCPS_V4_10.ashx

[5] BSI, technical guideline (BSI TR-02102-1), cryptographic process: Recommendations and key lengths

http://www.bsi.de

[6] FIPS (Federal Information Processing Standard), US committee developing standards; in the document, FIPS 140-2 (safety requirements for cryptographic modules) is used
http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[7] BayITS-11, IT standards for the Bavarian administration