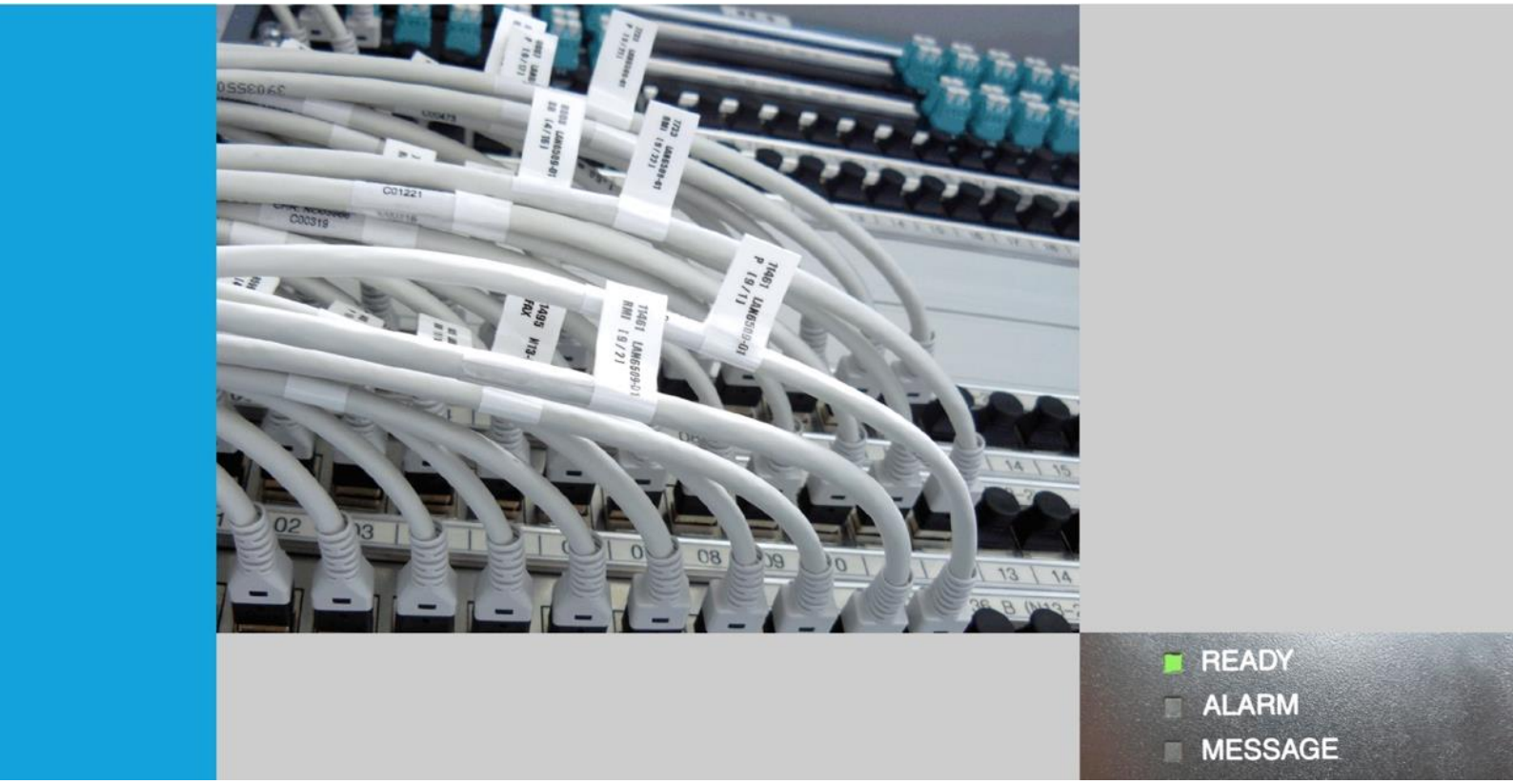
Landesamt für Digitalisierung,
Breitband und Vermessung

IT-Dienstleistungszentrum des Freistaats Bayern



Schulung für Registrierungsstellen der Bayern-PKI

- Einführung und Grundlagen -

München, den 03.07.2019

1 Motivation

Das Landesamt für Digitalisierung, Breitband und Vermessung (LDBV) betreibt für die Bayerischen Verwaltungsbehörden eine kryptographische Infrastruktur bzw. Public Key Infrastruktur (PKI). Ziel dieser Infrastruktur ist die Bereitstellung von kryptographischen Schlüsselmaterial, elektronischen Zertifikate und Zertifikatsstatusinformationen, um ein hohes Maß an Sicherheit für verschiedene IT-Verfahren der bayerischen Verwaltung zu gewährleisten.

Grundvoraussetzung für die vertrauenswürdige Ausgabe von elektronischen Zertifikaten ist ein Registrierungsverfahren für eine verlässliche Registrierung der Nutzerdaten – und falls erforderlich auch eine verlässliche Identifizierung des Nutzers.

Die Registrierungsstellen der Bayern-PKI sind verantwortlich für die Durchführung dieses Registrierungsverfahrens. Diese Schulungsdokumentation unterstützt die Einweisung der Verantwortlichen und Mitarbeiter der Registrierungsstellen als Grundlage für die Wahrnehmung der Aufgaben innerhalb der PKI.

2 Aufbau der Schulung

Diese Schulungsdokumentation vermittelt neben der Motivation für diese Schulung eine allgemeine Einführung in das Thema Public Key Infrastruktur sowie einen Überblick über die organisatorischen und technischen Ausprägungen der Bayern-PKI.

3 Einführung in den Themenkomplex PKI

Public Key Infrastrukturen erfüllen keinen Selbstzweck, sondern werden zur Bereitstellung von Diensten für IT-Anwendungen betrieben. Maßgebliches Ziel dieser Dienste ist die Erhöhung der Sicherheit in verschiedensten IT-Anwendungen, die für die Verwendung von elektronischen Zertifikaten geeignet sind. Das übergeordnete Thema „Sicherheit“ kann dabei auf vier zentrale Anforderungen heruntergebrochen werden:

Anforderung	Erklärung
Vertraulichkeit	Wie stelle ich sicher, dass nur befugte Nutzer Zugriff auf bestimmte Daten erhalten?
Integrität	Wie stelle ich sicher, dass Daten nicht unbefugt verändert werden?
Authentizität	Wie stelle ich sicher, dass ein Nutzer tatsächlich die Person ist, die er vorgibt zu sein?
Verbindlichkeit	Wie stelle ich sicher, dass eine elektronische Kommunikation oder ein elektronischer Prozess tatsächlich stattgefunden hat bzw. nicht abgestritten werden kann?

3.1 Zertifikatsbasierte IT-Anwendungen

Nicht jede IT-Anwendung unterstützt den Einsatz elektronischer Zertifikate. Einige IT-Anwendungen – insbesondere ältere Softwareprodukte oder –versionen – bieten stattdessen alternative Verfahren, mit denen die o.a. angeführten Anforderungen ebenfalls erfüllt werden – meist jedoch nicht auf gleichen Sicherheitsniveau oder dem mit Zertifikaten verbundenen Nutzerkomfort. Beispiele hierfür sind die Verwendung von Passwörtern für die Verschlüsselung von komprimierten Dateien mit WINZIP (Vertraulichkeit), die Verwendung von Prüfsummen (Integrität) oder die Anmeldung mittels Nutzername/Passwort an der Windows Domäne (Authentizität).

Im Bereich der bayerischen Behörden sind zahlreiche IT-Anwendungen im Einsatz die zertifikatsbasierte Prozesse unterstützen:

Anwendung	Erklärung
Sichere E-Mail	Eine verschickte E-Mail passiert auf ihrer Reise mehrere Server Knotenpunkte. Dies können E-Mail Server, Router, Firewalls o.ä. sein. Auf jedem dieser Knotenpunkte sowie unterwegs, durch Belauschen des Netzwerkverkehrs, kann der Inhalt der E-Mail gelesen und auch verändert werden. Um das zu verhindern verwendet man "sichere E-Mail". D.h. um das Mitlesen der E-Mail zu verhindern wird diese verschlüsselt. Um sicherzustellen, dass der Inhalt der Nachricht nicht verändert wurde und um die Identität des Absenders sicherzustellen, wird die Nachricht signiert.
SSL	Sie kennen es vom Online Shopping und Online Banking. Mehrfach übertragen Sie persönliche und höchst schützenswerte Daten (Adresse, Kreditkartennummer, PIN, TAN, ...) über das Internet - ein Medium in dem jeder alle Informationen mitlesen kann. Um die schützenswerten Daten auch vertraulich zu halten und nur dem zugänglich zu machen für den Sie bestimmt sind, wurde SSL entwickelt. Im Wesentlichen geht es darum, dass sich vor Verbindungsaufbau die beteiligten Komponenten gegenseitig ausweisen, d.h. identifizieren, und anschließend nur verschlüsselt kommunizieren.
2 Faktor Authentifizierung	Die 2 Faktor Authentifizierung ist eine Kombination der beiden Authentifizierungsmethoden Besitz und Wissen. Smartcards der Bayern-PKI können anstelle eines RSA-Tokens zur 2 Faktor Authentifizierung, z.B. am NCP Gateway, verwendet werden. Der Besitz ist die Smartcard, das Wissen wird durch die PIN repräsentiert.
IPSec	IPSec stellt eine Sicherheitsarchitektur für die Kommunikation über IP Netzwerke zur Verfügung. So sollen die Schutzziele Vertraulichkeit, Authentizität und Integrität gewährleistet werden. Die Verbindung zwischen PKI und IPSec stellt die zertifikatsbasierte Authentifizierung (ähnlich SSL) der beteiligten Komponenten dar.
Windows LogOn	Das zertifikatsbasierte Windows LogOn ermöglicht es dem Anwender sich anstelle mit Nutzername und Passwort mit einem auf einer Smartcard gespeicherten Zertifikat am PC anzumelden. Voraussetzung ist u.a. ein in das Active Directory integrierter PC und Account.
Server-authentifizierung	Bei der Serverauthentifizierung legt der Server dem Client vor erfolgreichem Verbindungsaufbau sein Zertifikat vor und stellt so seine Authentizität sicher.
Client-authentifizierung	Bei der Clientauthentifizierung legt der Client dem Server vor erfolgreichem Verbindungsaufbau sein Zertifikat vor und stellt so seine Authentizität sicher. Man unterscheidet dabei noch zwischen der Clientauthentifizierung einer Maschine und der einer Person.

Dokumenten-signatur	Wenn Sie von jemandem ein Dokument zugeschickt bekommen, können Sie nicht sicherstellen, ob das Dokument unverfälscht ist und ob es auch derjenige geschrieben hat, der es vorgibt. Durch die Signatur von Dokumenten, d.h. das elektronische Unterschreiben, wie es z.B. in MS Word oder Adobe Acrobat möglich ist, können Sie die Authentizität und Integrität sicherstellen.
Code Signing	Ein Code Signing Zertifikat ermöglichst es ihre Software zu signieren. Dies ist insbesondere für ActiveX Komponenten sinnvoll, die über das Web verteilt werden sollen. Der Nutzer kann sich bei signierten Software-Komponenten versichern wer die Software erstellt hat und ob die Software nachträglich verändert wurde.

3.2 Grundbegriffe der PKI

Seit mehr als 2.000 Jahren verwendet die Menschheit **Mechanismen der Verschlüsselung**, um die Vertraulichkeit von Nachrichten bzw. Informationen gewährleisten zu können. Das bekannteste frühzeitliche Verschlüsselungsverfahren ist das **CÄSAR-CHIFFRE**, ein ***symmetrisches* Verschlüsselungsverfahren**, bei dem ein Buchstabe des Alphabets durch einen anderen Buchstaben ersetzt wird, der um *n Stellen* weiter im Alphabet steht. Eine Verschlüsselung besteht also immer aus einem Verfahren (*verschiebe den Buchstaben um n Stellen des Alphabets*) und einem Schlüssel (*n*). Nur wenn beides bekannt ist, kann der Empfänger einer verschlüsselten Nachricht den ursprünglichen Nachrichtentext wiederherstellen und die geheime Information entnehmen.

Es ist nicht allzu schwer sich vorzustellen, dass entweder durch **bloßes Ausprobieren** („Brute Force“) oder durch das Untersuchen von **Schwachstellen** (z.B. suchen nach Buchstaben, die im Sprachschatz sehr häufig vorkommen) diese einfache Verschlüsselungsform „gebrochen“ wurde und damit nicht mehr als hinreichend sicher betrachtet wurde. Es wurde immer **komplexere Verschlüsselungsverfahren** erfunden, die jedoch immer auf einem symmetrischen Schlüssel basierten (d.h. Empfänger und Sender müssen das gleiche Geheimnis – den Schlüssel – kennen).

Der symmetrische Schlüssel blieb damit auch bis in die Neuzeit ein Grundproblem in der Anwendung von Kryptographie. Zum einen ist der **Schlüsselaustausch** zwischen Sender und Empfänger immer die **größte Schwachstelle** eines Verfahrens, zum anderen steigt der Aufwand der Schlüsselverwaltung mit der Anzahl der unterschiedlichen Empfängergruppen exponentiell an. Im Jahr 1970 wurden schließlich die Grundlagen der **asymmetrischen Kryptographie** entwickelt. Auf der Basis eines nach wie vor ungelösten mathematischen Problems der Primfaktorenzerlegung großer Zahlen lassen sich zwei Zahlen (sprich: Schlüssel) finden, die zwar zueinander gehören (und somit zu einem Schlüsselpaar werden) aber von einem Schlüssel nicht auf den korrespondierenden Schlüssel schließen lassen.

Ein solches ***asymmetrisches* Schlüsselpaar** besteht somit aus einem geheimen Schlüssel (**Private Key**) und einem öffentlichen Schlüssel (**Public Key**). Damit wird sowohl das Problem des Schlüsseltransports (Der öffentliche Schlüssel muss nicht geheim bleiben und kann jedem zugänglich gemacht werden, der dem Besitzer des privaten Schlüssel eine vertrauliche Nachricht zukommen lassen möchte) als auch das Problem der Schlüsselverwaltung gelöst (Mit der Anzahl der Teilnehmer steigt die Anzahl der Schlüssel nur noch linear an).

Um nun einen öffentlichen Schlüssel auch **eindeutig und zweifelsfrei** dem Besitzer des zugehörigen privaten Schlüssels zuordnen zu können, wurden **elektronische Zertifikate** eingeführt. Die Daten des Besitzers (z.B. Name, Vorname, Emailadresse, Unternehmenszugehörigkeit etc.) und der öffentliche Schlüssel werden zusammen als Datenpaket mit dem privaten Schlüssel einer vertrauenswürdigen Instanz (Zertifizierungsinstanz, Certification Authority, CA) verschlüsselt. Das unverschlüsselte Datenpaket und verschlüsselte Datenpaket (eigentlich wird nicht das ganze Datenpaket,

sondern nur ein digitaler Fingerabdruck bzw. Hashwert verschlüsselt) werden zusammen als Zertifikat genutzt.

Möchte sich nun ein Dritter von der Echtheit der Daten des Zertifikats überzeugen, entschlüsselt er den verschlüsselten Teil des Zertifikats mit dem öffentlichen Schlüssel der CA und vergleicht das Ergebnis mit dem Zertifikatsdaten. Sind diese identisch, kann der Dritte von der Echtheit des Zertifikats überzeugt sein und kennt damit zweifelsfrei die Identität des Besitzers des Private Keys. Nun kann dieser Dritte gefahrlos den Public Key des Besitzers nutzen, um vertrauliche Informationen an diesen zu versenden.

Dieses Prinzip der Erstellung eines Zertifikats nennt sich auch **elektronische Signatur**, da es nicht um die Vertraulichkeit geht (der Public Key ist ja für jeden öffentlich zugänglich) sondern um die Integrität der Besitzerdaten. Die Prinzipien für Verschlüsselung und elektronische Signatur sind nachfolgend noch einmal veranschaulicht:

Da **asymmetrische Verschlüsselungsverfahren** bei gleichartigem Sicherheitsniveau etwa **um den Faktor 1.000 langsamer** sind **als symmetrische Verfahren**, sind diese für die Verschlüsselung großer Datenmengen eigentlich nicht geeignet. In der Praxis behilft man sich durch eine Kombination beider Verfahren: Per Zufallsgenerator wird ein symmetrischer Schlüssel generiert (Session Key) und das zu übertragende Datenpaket verschlüsselt. Mit dem asymmetrischen Public Key wird schließlich nur der Session Key verschlüsselt zusammen mit den verschlüsselten Nutzdaten übertragen. Der Empfänger entschlüsselt den Session Key mit seinem Private Key und kann anschließend die Nutzdaten entschlüsseln.

Analog zur praktischen Anwendung der Verschlüsselung wird auch für die elektronische Signatur nicht nur die asymmetrische Verschlüsselung verwendet, da diese für große Datenmengen nicht geeignet ist. Für die Signatur kombiniert man mit einem weiteren kryptographischen Verfahren, dem **Hash-Verfahren** (engl. to hash -> zerhacken).

Aus einem (großen) Quelltext wird mittels einer Hash-Funktion ein Hash-Wert (z.B. von 160 Bit Länge) berechnet. (Als anschauliches Beispiel für eine einfache Hash-Funktion sei hier die Funktion „Bildung einer Quersumme“ genannt). Dieser Hash-Wert dient im Sinne eines **elektronischen Fingerabdrucks** für die Integrität des Quelltextes, d.h. schon geringe Änderungen im Quelltext führen zu einem völlig andren Hash-Wert.

Für die elektronische Signatur wird also zunächst aus der Information (Quelltext) der HashWert gebildet und dieser mit dem Private Key des Nutzers N1 verschlüsselt. Information und verschlüsselter Hash-Wert werden gemeinsam an Nutzer N2 übertragen. Nutzer N2 entschlüsselt nun mit dem Public Key von N1 den Hash-Wert. Schließlich bildet er ebenfalls aus der Information den Hash-Wert. Sind der der generierte und der entschlüsselte Hash-Wert identisch, so ist der Quelltext unverändert und durch den Zertifikatsinhaber N1 auch elektronische signiert worden.

4 Einführung in die Bayern-PKI

Auch die Bayern-PKI baut auf die klassischen Instanzen auf, die im Allgemeinen in Public Key Infrastrukturen zu finden sind:

- Registrierungsinstanz
- Zertifizierungsinstanz
- Veröffentlichungsinstanz

Als Besonderheit der Bayern-PKI wird der Nutzer bzw. Zertifikatsnehmer aktiv in das PKI-Konzept mit einbezogen, da er seine Zertifikate sowie dessen Sperrung selbst beantragen kann.

Für alle Instanzen werden technische Hilfsmittel in Form von IT-Anwendungen eingesetzt. Ebenso wichtig sind jedoch die organisatorischen Regelungen, die in Summe und in Verbindung mit der IT dafür sorgen, dass die Nutzer Vertrauen in die Zertifikate der Bayern-PKI setzen können.

Um einen gleichermaßen sicheren wie effizienten Betrieb der Bayern-PKI zu gewährleisten, werden folgende organisatorischen Rollen definiert:

- Leiter der Bayern-PKI
  Der Leiter der Bayern-PKI ist gesamtverantwortlich für den Betrieb und die Einhaltung der Richtlinien.

- Administratoren
  Die Administratoren sind verantwortlich für Einrichtung und Betrieb der Zertifizierungsstelle und des Zertifikatsmanagementsystems als technische Basis für die Registrierungsstellen. Ebenfalls sind sie verantwortlich für die Einrichtung des Verantwortlichen für die Wurzelregistrierungsstelle.

- Verantwortlicher Wurzelregistrierungsstelle
  Der Verantwortliche registriert die Mitarbeiter der Wurzelregistrierungsstelle und weist Ihnen ihre Rolle im Zertifikatsmanagementsystem zu.

- Mitarbeiter Wurzelregistrierungsstelle
  Die Mitarbeiter richten Registrierungsstellen für Behörden ein, registrieren den jeweiligen Verantwortlichen für die Registrierungsstelle und weisen ihm seine Rolle im Zertifikatsmanagementsystem zu. Zusätzlich weisen sie Service Desk Mitarbeitern ihre Rolle im System zu.

- Verantwortlicher Registrierungsstelle
  Der Verantwortliche registriert die Mitarbeiter seiner Registrierungsstelle und weist Ihnen ihre Rolle im Zertifikatsmanagementsystem zu.

- Mitarbeiter Registrierungsstelle
  Die Mitarbeiter registrieren Nutzer ihrer Registrierungsstelle, pflegen die Daten und können Sperrungen für die Zertifikate der Nutzer beantragen. In besonderen Fällen ist

auch eine Zertifikatsbeantragung für Nutzer durch Registrierungsstellen Mitarbeiter möglich.

- Service Desk
  Die Service Desk Mitarbeiter unterstützen bei technischen Problem und können stellvertretend Sperrungen von Nutzerzertifikaten beantragen.

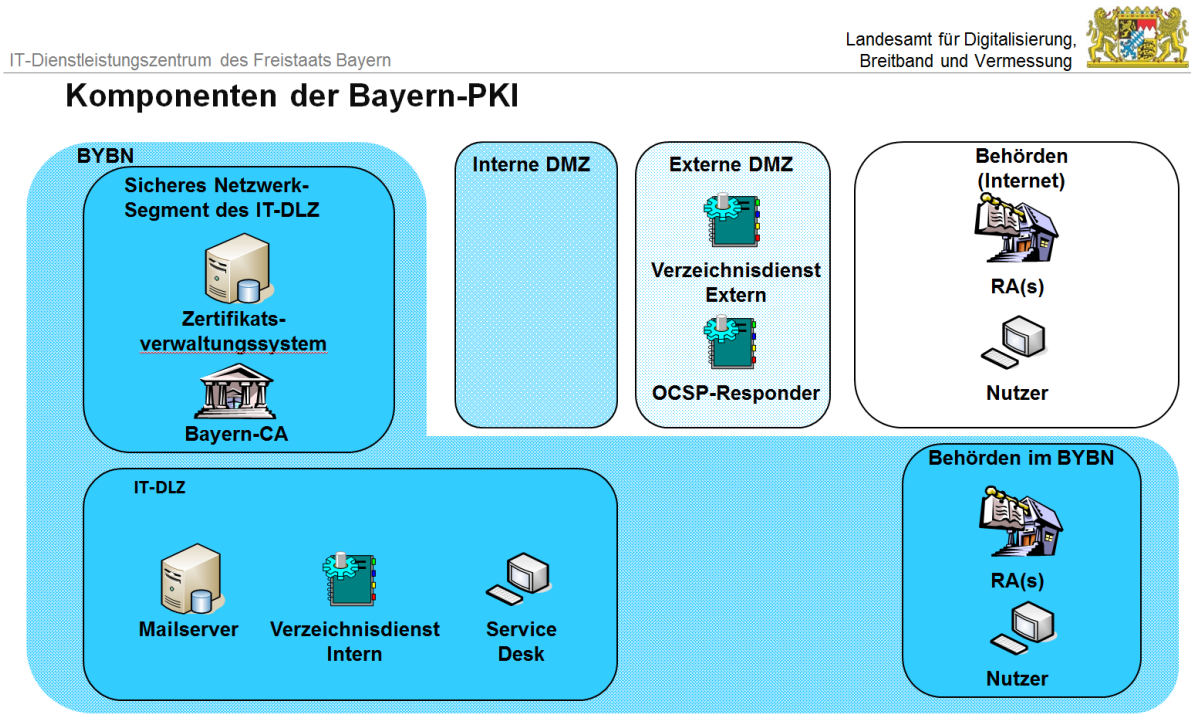
- Nutzer
  Nutzer können im Zertifikatsmanagementsystem Zertifikate beantragen und die Sperrung dieser Zertifikate beantragen. Nutzer gibt es in den Rollen Zertifikatsnehmer (für persönliche Zertifikate), Verantwortlicher für Funktionsstellen, Mitglied von Funktionsstellen sowie Verantwortlicher für Serverzertifikate und Clientverantwortlicher.

5 Komponenten und Prozesse der Bayern-PKI

Das Sicherheitskonzept der Bayern-PKI sieht vor, dass die zentralen Serversysteme der Bayern-PKI – der Application Server des Zertifikatsverwaltungssystems und der Server der Certification Authority bzw. CA-Server – in einem gesondert gesicherten Netzsegment der Bayern-PKI betrieben werden. Der administrative wie operative Web-Client Zugriff auf das Zertifikatsverwaltungssystem erfolgt über einen integrierten Webserver und ist nur innerhalb des Behördennetzes möglich.

Zertifikate können in einem Verzeichnisdienst-Cluster innerhalb des BYBN sowie einem weiteren Cluster in der Externen DMZ gespeichert und veröffentlicht werden. Zertifikatssperrlisten werden ausschließlich im Cluster der externen DMZ veröffentlicht. Ebenfalls in der externen DMZ befindet sich noch der OCSP-Server.

Über den E-Mail Server im BYBN erfolgt die Versendung von Schlüsselmaterial und Zertifikaten.

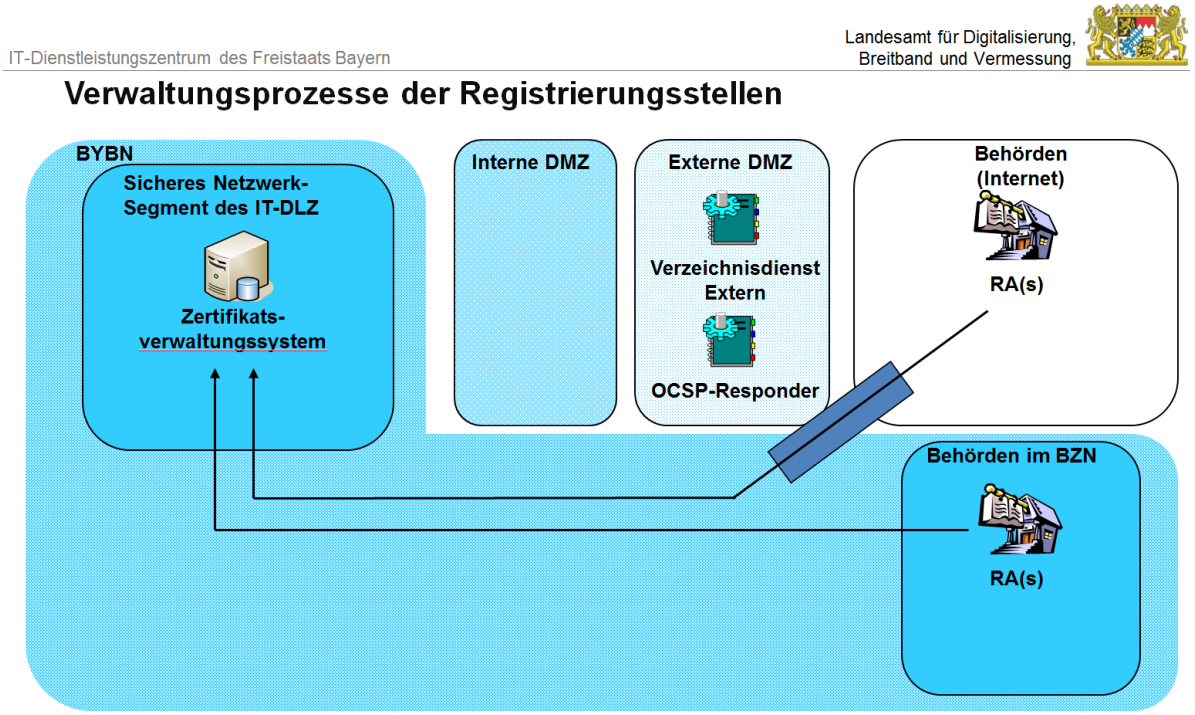


5.1 Verwaltung der Registrierungsstellen

Alle administrativen und operativen Zugriffe der jeweiligen Rolleninhaber

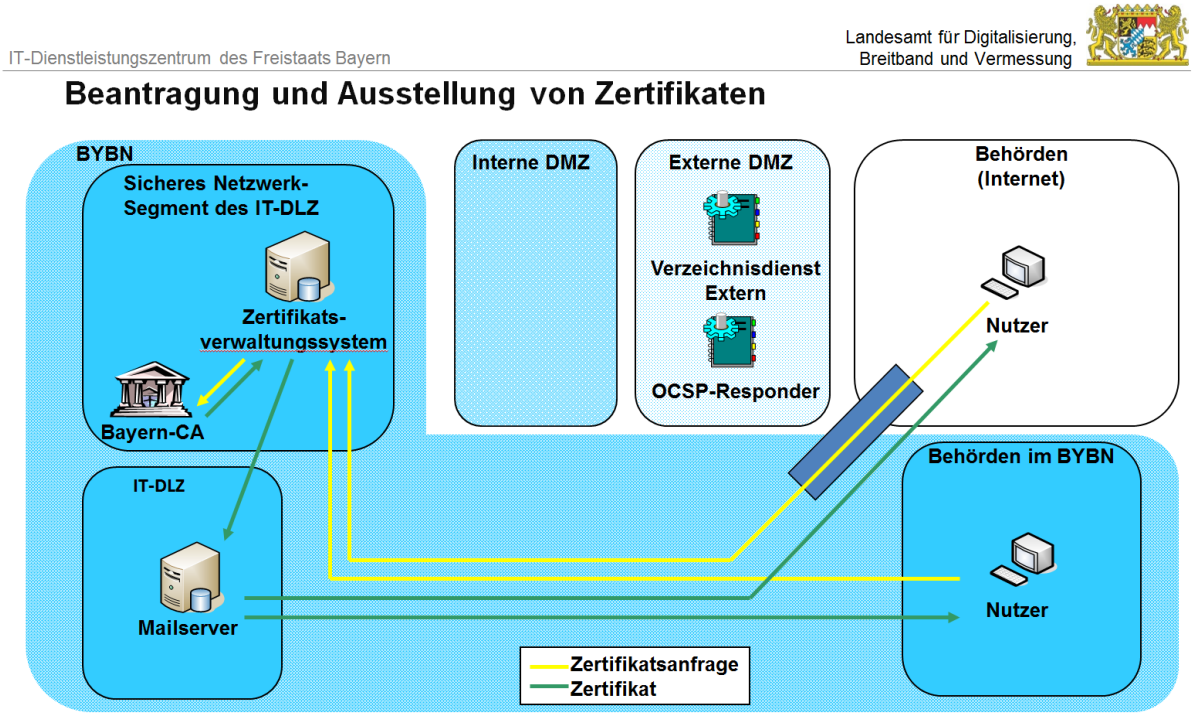
- Administrator
- Verantwortlicher Wurzelregistrierungsstelle
- Mitarbeiter Wurzelregistrierungsstelle
- Verantwortlicher Registrierungsstelle
- Mitarbeiter Registrierungsstelle

erfolgen mit einem Java Web Start Aufruf. Dieser Zugriff ist aus Vorgabegründen nur innerhalb des BYBN möglich und erfolgt verschlüsselt.



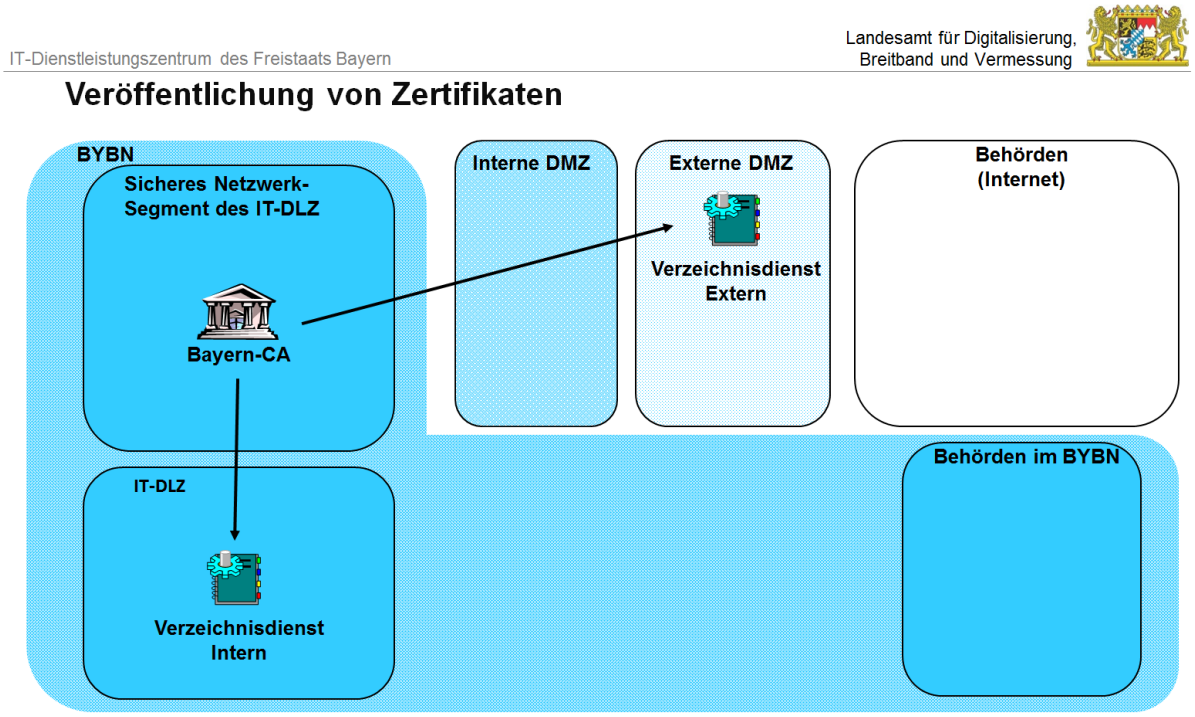
5.2 Beantragung und Ausstellung von Zertifikaten

Analog zum Prozess für die Verwaltung der Registrierungsstellen verbinden sich Nutzer mittels Java Web Start zum Zertifikatsverwaltungssystem, auch hier ist der Zugriff nur von innerhalb des BYBN angesiedelten Systemen möglich. Der Application Server des Systems leitet den Antrag weiter zum CA-Server und erhält als Antwort das Zertifikat des Nutzers. Schlüsselmaterial und Zertifikat werden zu einer Datei zusammengestellt, verschlüsselt und als E-Mail Anhang an den Antragsteller/Nutzer versendet. Der Nutzer kann daraufhin aus dem Zertifikatsverwaltungssystem das Passwort zur Entschlüsselung der Datei und zum Import von Schlüsselmaterial und Zertifikat in den lokalen Zertifikatsspeicher des Clients abfragen. Alternativ ist für Windows Clients auch ein Autoenrollment möglich oder als weitere Alternative die Beantragung von Smartcards.



5.3 Veröffentlichung von Zertifikaten

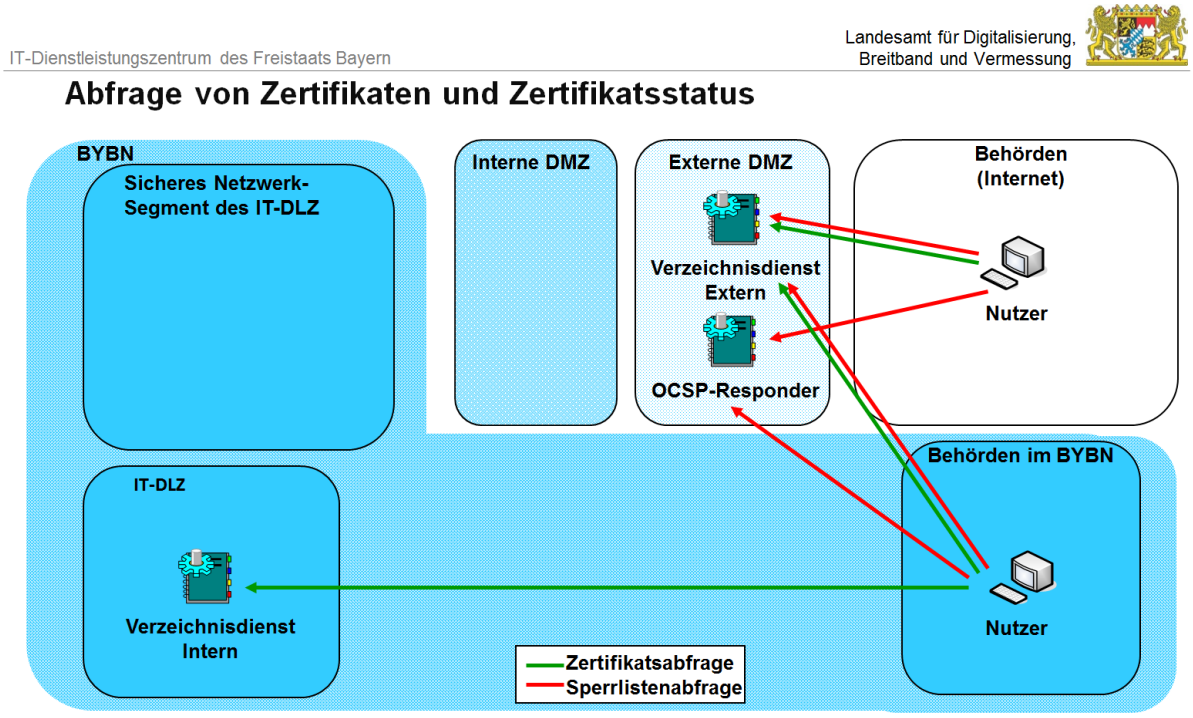
Verschlüsselungszertifikate werden direkt vom CA.-Server in den internen Verzeichnisdienstserver und parallel (wenn der Nutzer der Veröffentlichung nach extern zustimmt) in den externen Verzeichnisdienstserver gespeichert.



5.4 Abfrageprozesse

Die Abfrage des aktuellen Zertifikats eines Zertifikatsnehmers erfolgt in Abhängigkeit vom Standort des Abfragenden entweder auf den Verzeichnisdienstserver intern (Nutzer im BYBN) oder den Verzeichnisdienstserver extern (sonstige Nutzer, angebunden über das Internet).

Statusabfragen bzgl. der Gültigkeit eines Zertifikats erfolgen je nach Verfahren auf den Verzeichnisdienstserver extern (Sperrlistenabfrage) oder den OCSP Server (OCSP Dienst).



5.5 Sperrprozesse

Sperranträge werden von den berechtigten Rolleninhabern

- Nutzer des zu sperrenden Zertifikats
- Mitarbeiter der Registrierungsstelle
- Mitarbeiter des Service Desks

an das Zertifikatsverwaltungssystem und von dort an den CA-Server weitergeben. Der CA-Server fügt die Zertifikatsseriennummer zur Zertifikatssperrliste hinzu, signiert diese elektronisch und speichert die Zertifikatssperrliste in den Verzeichnisdienstserver extern. Der OCSP-Server wiederum greift zur Beantwortung von Statusabfragen auf die veröffentlichte Sperrliste des Verzeichnisdienstservers Extern zu.