Landesamt für Digitalisierung,
Breitband und Vermessung
IT-Dienstleistungszentrum

Vorteile der PKI 2.0

» **Verbesserungen des Datenbestands**
- » Hohe Datenqualität und -aktualität
- » Konsistenz der Zertifikatsinhalte durch zentralen Datenbestand für alle PKI-Systeme
- » Verhindern "verwaister" Zertifikate

» **Steigerung der Effizienz**
- » Einheitliche Benutzeroberfläche
- » Automatisierte Aktualisierung der Daten
- » Entlastung und Arbeitserleichterung der Registrierungsstellen

» **Hohes Sicherheitslevel**
- » Orientierung an den einschlägigen technischen Richtlinien (TRs) des BSI (insbesondere der BSI TR-03145)
- » Certification Policy-Vorgaben (CP) des LSI
- » Automatische Pflege der Benutzerdaten durch Anbindung dezentraler Datenbestände (z.B. VIVA)

Bayern-PKI 2.0

» **Automatische Zertifikatsverteilung**

Angebotene Protokolle für die automatische Verteilung (Auto-enrollment):
- » MS WCCE (Microsoft Auto-enrollment)
- » SCEP
- » SCEP-NDES
- » EST
- » ACME

Erfahren Sie mehr

Website der Bayern-PKI 2.0

https:/www.pki.bayern.de/pki20/index.html

Hier finden Sie neben aktuellen Projekt-Informationen auch:
- » FAQ zur Bayern-PKI 2.0
- » Ansprechpartner
- » Newsletterarchiv

Onlineportal des IT-DLZ

https://onlineportal.it-dlz.bybn.de

Hier finden Sie:
- » die PKI im Produktportfolio
- » das Angebot an Vorträgen und Kundenworkshops des IT-DLZ
- » Ein Newsletterarchiv

Sie haben Fragen dazu?

Bei Fragen zur Bayern-PKI 2.0 wenden Sie sich an das IT-DLZ, per E-Mail an:

bayern-pki-2.0@ldbv.bayern.de

oder direkt an das IT-DLZ Kundenmanagement.

Bei IT-sicherheitstechnischen Fragen unterstützt Sie das LSI, beispielsweise zur:
- » Auswahl der Zertifikats-Algorithmen
- » Auswahl von Auto-enrollment-Mechanismen
- » Erfüllung von spezifischen Sicherheits-anforderungen durch die PKI

Wenden Sie sich dafür per E-Mail an:

beratung-staatsverwaltung@lsi.bayern.de
oder:
beratung-kommunen@lsi.bayern.de

Bayern-PKI 2.0

Das neue Produkt des IT-DLZ

Die Bayern-PKI 2.0 löst die bestehende Public Key Infrastructure (PKI) des Freistaats Bayern ab.

Was zeichnet das neue Produkt aus?

Die PKI 2.0 ist modernisiert und an neueste technische Anforderungen angepasst. Sie stellt sicher, dass digitale Prozesse im Freistaat Bayern mittels ausgestellter private-trusted Zertifikate sicher betrieben werden können und gewährleistet damit auf aktuellstem technischen Niveau die Vertraulichkeit, Integrität und Verbindlichkeit von Daten bzw. Nachrichten.

Für wen ist die Bayern-PKI 2.0?

Kommunale und staatliche Behörden können die Bayern-PKI 2.0 nutzen. Die Zertifikate werden für natürliche Personen, juristische Personen, Personengruppen, Funktionen und Assets/Geräte ausgestellt.

Bayern-PKI 2.0

Einführung der PKI 2.0

Die Einführung erfolgt in drei Projektphasen:

» Konzeptionsphase

2024 werden im Projekt Bayern-PKI 2.0 mit dem Dienstleister Architektur, Sicherheitsstruktur und betriebliche Konzepte und Prozesse erarbeitet.

» Implementierungsphase

Es folgt die technische Implementierung des neuen Systems.

» Migrationsphase

Daran schließt sich in den folgenden Monaten die flächendeckende Migration aller Behörden an. An ihrem Ende steht die vollständige Ablösung der Zertifikate der bisherigen Bayern-PKI.

Was dabei für Sie wichtig ist:

- Die bestehende PKI wird parallel betrieben, bis die neue Bayern-PKI 2.0 final eingeführt ist.
- Alle ab März 2024 ausgegebenen "alten" PKI-Zertifikate sind bis März 2027 gültig. Deren Gültigkeitsdauern werden ab Stichtag 12.03.2024 entsprechend verkürzt.
- Alle alten Zertifikate werden mit dem Ende der Migration zurückgerufen.

Was ist die PKI 2.0?

Die Bayern-PKI 2.0 ist eine zentrale Infrastrukturkomponente, die ressortübergreifend durch das IT-DLZ zur Verfügung gestellt wird. Sie besteht aus den folgenden Komponenten:

» IDM (Identitätsmanagement):

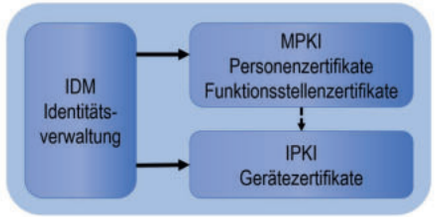
Datenbasis für die MPKI und IPKI. Zentrale Bereitstellung der Identitäten als Akteure innerhalb der Anwendung/Organisation. Korrekte Identifizierung von Teilnehmern (Usern und Funktionsstellen).

» MPKI (Managed PKI):

Erhält Daten aus dem IDM. Stellt Personen- und Funktionsstellenzertifikate (ggf. auf Smartcard) aus.

» IPKI (Infrastruktur-PKI):

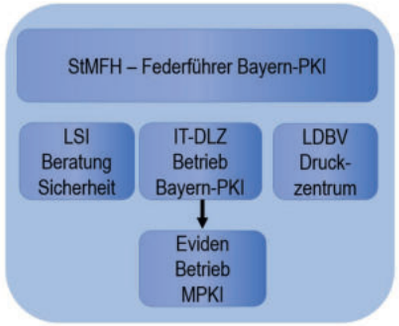
Erhält Daten aus dem IDM und der MPKI.
Stellt Zertifikate für Infrastrukturkomponenten (Server und Clients) im Bay.Behördennetz aus.



» Wesentliche Neuerungen

- Zentraler Betrieb einer IDM-Plattform für die PKI im IT-DLZ
- On-premises Betrieb der IPKI im IT-DLZ
- Betrieb der MPKI durch unseren Partner Eviden
- Zentrales Druckzentrum im LDBV für Smartcards für IT-DLZ-Kunden
- Ausschließliche Unterstützung von Bayern-PKI-spezifischen Smartcards

Betreiber der PKI 2.0



» Wer ist an der PKI beteiligt?

Die Umstellung auf die neue Basiskomponente PKI erfolgt im Rahmen eines Programms, das aus mehreren aufeinanderfolgenden Projekten besteht.
Diese werden in enger Zusammenarbeit zwischen dem StMFH, IT-DLZ, LDBV und LSI sowie dem externen Dienstleister Eviden durchgeführt.

Die Programmleitung für die Bayern-PKI 2.0 liegt beim IT-DLZ.

Das StMFH ist Federführer für die Bayern-PKI.

Das LSI berät in allen sicherheitsrelevanten Fragestellungen zur Bayern-PKI. Darunter fallen beispielsweise die Pflege der Certificate Policy der Bayern PKI 2.0 und die Entscheidung über zugelassene Algorithmen.

Für den technischen Betrieb verantwortlich ist das IT-DLZ, das einen Teil des PKI-Betriebs an den Dienstleister Eviden und das Druckzentrum an das LDBV ausgelagert hat.