

Zertifizierungsrichtlinie der EKKW – PKI

KABl. 2011 S. 28

Das Landeskirchenamt hat in seiner Sitzung am 21.12.2010 gem. § 6 Verordnung über die Intranet- und Internetnutzung in der Evangelischen Kirche von Kurhessen-Waldeck vom 12.11.2010 die folgende Richtlinie beschlossen:

1. Einleitung

1Die Evangelische Kirche von Kurhessen-Waldeck betreibt ein System zur Ausstellung digitaler Zertifikate, die EKKW-PKI (Public Key Infrastructure), um eine gesicherte elektronische Kommunikation und eine Authentifizierung zu ermöglichen. 2Sie stellt als Zertifizierungsinstanz nach dieser Richtlinie „fortgeschrittene elektronische Zertifikate“ aus. 3Die Zertifikate dienen der Nutzung als digitale Signatur und der Verschlüsselung von E-Mail- und Datei-Verkehr.4Diese Zertifizierungsrichtlinie regelt die Abläufe innerhalb der EKKW-PKI und legt dabei die Rahmenbedingungen für die Ausstellung und Nutzung von Zertifikaten fest. 5Sie ist für alle Teilnehmer an der EKKW-PKI verbindlich.

2. Zertifizierungsinstanz

2.1 Zertifizierungsstellen

In der EKKW-PKI gibt es drei Zertifizierungsstellen (CA, Certification Authority). Die Stammzertifizierungsstelle wird offline und zwei weitere als ausstellende Stellen betrieben. Ihre Namen lauten:

EKKW RootCA LKA; EKKW SubCA01 LKA; EKKW SubCA02 LKA

Die Zertifizierungsstellen erstellen alle Zertifikate innerhalb der EKKW-PKI. Die EKKW-PKI wird vom Sachgebiet Informations- und Kommunikationstechnik im Landeskirchenamt betrieben.

Die EKKW-PKI erfüllt folgende Bedingungen:

- Für die Signierung aktiver Zertifizierungsstellen wird eine dedizierte Maschine eingesetzt, die vom restlichen Netzwerk getrennt ist.
- Die zur elektronischen Signatur ausgestellten Zertifikate enthalten ein asymmetrisches Schlüsselpaar.
- Der Zertifizierungsschlüssel hat eine Mindestlänge von 2048 Bits.

- Die Zertifikate für fortgeschrittene elektronische Signaturen werden im PKCS#10/12 Format ausgegeben. Einfache Zertifikate als PKCS#7 (Public Key Cryptography Standards).
- Der selbstsignierte Schlüssel der Stammzertifizierungsstelle und die signierten Schlüssel der ausstellenden Zertifizierungsstellen werden vor unbefugten Personen geschützt aufbewahrt.

Die EKKW-PKI ist bei der zuständigen Behörde (IANA) registriert.

Die Identifikationsnummer dieser Richtlinienerklärung lautet: 1.3.6.1.4.1.34210.100.10.1

2.2 Zertifikatnehmer

Zertifikatnehmer sind natürliche und juristische Personen, einschließlich ihrer Untergliederungen, sowie deren technische Einrichtungen, die ein Zertifikat der EKKW-PKI ausgestellt bekommen.

2.3 Zertifikatsinhalte

Die von EKKW-PKI ausgestellten Zertifikate enthalten regelmäßig folgende Angaben:

- Name des Zertifikatinhabers
- Name der ausstellenden Zertifizierungsstelle
- Seriennummer des Zertifikats
- Gültigkeitszeitraum
- Name des Signatur Algorithmus
- Öffentlicher Schlüssel
- Version
- Fingerprint (elektronische Kennung)
- folgende Erweiterungen:
 - EMail-Adresse: vorname.nachname@ekkw.de
 - Prinzipalname des Zertifikatsinhaber
 - Key Usage (Verwendungszweck)
 - Extended Key Usage (erweiterter Verwendungszweck)
 - Sperrlistenverteilungspunkte
 - Zugriff auf Stelleninformationen

Abhängig vom Verwendungszweck des jeweiligen Zertifikats können weitere Angaben hinzukommen oder entfallen.

3. Namen

¹Die ausgestellten Zertifikate tragen den Namen des Zertifikatinhabers, sowie eine zugeordnete Organisationseinheit. ²Optional können weitere Zuordnungsmerkmale enthalten sein. ³Durch den zugeordneten Namen muss der Zertifikatnehmer innerhalb der Landeskirche eindeutig identifizierbar sein. ⁴Die weiteren Bezeichnungen müssen geläufigen Organisationseinheiten innerhalb der Landeskirche entsprechen. ⁵Zertifikate für Personen dürfen nur auf einen zulässigen Namen des Zertifikatnehmers ausgestellt werden. ⁶Anonyme Zertifikate werden nicht ausgestellt. ⁷Die Eindeutigkeit von mehreren Zertifikaten eines Zertifikatnehmers wird durch die Zertifikatsseriennummer erreicht.

4. Zertifizierungsvorgang

4.1. Antrag und Ausstellung

¹Zertifikate können für eine bestimmte Gruppe Zertifikatnehmer ausgestellt oder von einzelnen Zertifikatnehmern beantragt werden. ²Antragsberechtigt ist jeder Zertifikatnehmer innerhalb der EKKW-PKI. ³Der Antrag ist an das Sachgebiet Informations- und Kommunikationstechnik im Landeskirchenamt zu stellen. ⁴Über Anträge wird entsprechend den Anwendungsmöglichkeiten für den jeweiligen Zertifikatnehmer entschieden. ⁵Das Sachgebiet Informations- und Kommunikationstechnik im Landeskirchenamt prüft die Berechtigung des Antragstellers, sofern dieser ihr nicht bekannt ist.

⁶Die Ausstellung der Zertifikate kann auf elektronischem Wege auch webbasiert erfolgen.

4.2. Teilnehmererklärung

Mit Verwendung des Zertifikats erklärt sich der Zertifikatsinhaber mit der geltenden Richtlinie der EKKW-PKI einverstanden.

5. Sperrung / Sicherheit

5.1 Nutzungsbedingungen

¹Der Zertifikatsinhaber ist für den Schutz des Zertifikats und des privaten Schlüssels, auch auf anderen technischen Geräten, verantwortlich. ²Private Schlüssel in ausgestellten Zertifikaten können exportiert werden. ³Bei einem Zertifikatsexport mit privatem Schlüssel muss für die PFX-Datei (Personal Information Exchange File -kann privaten Schlüssel beinhalten-) ein komplexes Kennwort verwendet werden.

⁴Bei Bekanntwerden eines Missbrauchs bzw. ⁵Verlust eines Zertifikats informiert der Zertifikatsinhaber unverzüglich das Sachgebiet Informations- und Kommunikationstechnik im Landeskirchenamt.

5.2 Sperrgründe

Zertifikate können von EKKW-PKI aus folgenden Gründen gesperrt werden:

- o Missbrauch bzw. Verlust/Diebstahl des privaten Schlüssels
- o Änderung personenbezogener Daten oder sonstiger zertifikatsrelevanter Angaben
- o Ausscheiden des Mitarbeiters
- o Verstoß gegen diese Richtlinie
- o Sperrantrag des Zertifikatsinhaber
- o Einstellen des Zertifizierungsbetriebs
- o Verlust/Diebstahl der PIN (Persönliche Identifikationsnummer) einer PFX-Datei

6. Inkrafttreten

1Diese Richtlinie tritt mit Beschlussfassung des Landeskirchenamtes in Kraft. 2Sie ist im kirchlichen Amtsblatt zu veröffentlichen.