Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartament EFD
Bundesamt für Informatik
und Telekommunikation
Swiss Governmt PKI

NICHT KLASSIFIZIERT

Einrichtung Testaccounts

Klasse B für Bundesexterne (nonBV)

Dieses Dokument beschreibt die Bedingungen für die Erstellung von Testaccount Zertifikate der Klasse B für Bundesexterne auf dem produktiven System

1. Rahmenbedingungen

Die Swiss Government PKI beglaubigt und widerruft digitale Identitäten und steht dazu mit ihrem Namen. Sie unterliegt internationalen Vorgaben sowie der schweizerischen Gesetzgebung. Aus diesen Gründen verlangen wir strikt den korrekten Umgang mit unseren Zertifikaten. Dazu gehört, als wichtigste Komponente der Registrierung, zwingend die zweifelsfreie Feststellung der Identität der Zertifikatsteilnehmer. Wir stellen sicher und weisen aus (CP/CPS), dass die Feststellung der Identität korrekt abläuft.

Ebenso verwaltet die Swiss Government PKI Identitäten, die nicht mehr vertrauenswürdig sind (abgelaufen oder revoziert).

Wichtig: Die Regelwerke der Swiss Government PKI verbieten fiktive Identitäten zu erzeugen und damit produktive Zertifikate auszustellen, die dann zu Testzwecken verwendet werden. Nicht regelkonform ausgestellte Zertifikate werden von der Swiss Government PKI unverzüglich revoziert.

2. Erstellung Testaccount

Bei Bedarf kann jede bundesexterne Organisationseinheit (Kanton/KAPO/STAPO/Gemeinde) Testuser für die Ausstellung von Testzertifikaten der Klasse B auf dem produktiven System erstellen.

Folgende **Voraussetzungen** müssen zwingend erfüllt werden, bzw. ein Testuser muss:

- einer **natürlichen Person** eindeutig zugewiesen werden können
- im **LDAP Verzeichnis** als Testuser sichtbar angelegt sein (Beispiel: in einem eigenen Ast «ou=Test» unter Ihrer eigenen Organisationseinheit)
- im **CN** (Common Name) sowohl den echten Namen der natürlichen Person, wie auch den Vermerkt «Test» im Namen enthalten sein
- über eine **E-Mailadresse** verfügen, die sowohl den echten Namen, wie auch «Test» enthält
- das **gültige Reisedokument** (Beispiel: ID, Pass) der natürlichen Person bei Ausstellung des Zertifikats Klasse B muss im WalkInWizard hinterlegt werden

Beispiel:

- ou=Gemeinde/KAPO/STAPO/Feuerwehr …
    - ou=Test
        - CN: Muster Thomas TEST *Suffix*
        - Email: thomas.muster.test@xxxx.ch
- ou=Kanton X
    - ou=Gemeinde/KAPO/STAPO/Feuerwehr …
        - ou=Test
            - CN: Meier Hans TEST *Suffix*
            - Email: hans.meier.test@xxxx.ch

Sie können auch mehrere Testuser Einträge im LDAP erstellen.

Beispiel:

- CN: Muster Thomas TEST1 *Suffix*
- Email: muster.thomas.test1@kanton.ch
- CN: Muster Thomas TEST2 *Suffix*
- Email: muster.thomas.test2@kanton.ch
- CN: Muster Thomas TESTn *Suffix*
- Email: muster.thomas.testn@kanton.ch

Die Zertifikate Klasse B, welche mit einem solchen Testuser erstellt wurden, sind somit für diesen Verwendungszweck (Test) erkenntlich. Diese Handlungsweise ist mit unseren Auditoren abgesprochen und soll verhindern, dass nichtkonforme produktive Testzertifikate in Umlauf geraten. Siehe auch Rahmenbedingungen in Kapitel 1.

2.1 LDAP Import

Die Angaben für die Testuser sowie den neuen Ast können Sie dem BIT wie gewohnt via LDIF-File (oder CSV-File) zustellen.

3. Mehrfachausstellung

Die Mehrfachausstellung ist generell erlaubt. Mit dem Wechsel auf prestaged Smartcards muss jedoch neu für jedes Zertifikat Klasse B eine separate Smartcard verwendet werden. Dies gilt auch für Testzertifikate.

4. Verrechnung

Pro natürliche Person wird das produktive Zertifikat Klasse B jeweils nur einmal verrechnet. Testzertifikate werden generell nicht verrechnet.