**Peter Brügger**, 18.06.2015

# Manuelles Enrollment Domain Controller Zertifikate

## Template BVerwE-KerberosAuthentication-viaPKI

**Version:** **V1.01**

| Status | in Arbeit | in Prüfung | genehmigt zur Nutzung |
|---|---|---|---|
| | ☐ | ☒ | ☒ |

| **Beteiligter Personenkreis** | |
|---|---|
| Autoren: | Peter Brügger |
| Genehmigung: | |
| Benützer/Anwender: | |
| zur Information/Kenntnis: | |

| **Änderungskontrolle, Prüfung, Genehmigung** | | | |
|---|---|---|---|
| **Wann** | **Version** | **Wer** | **Beschreibung** |
| 18.06.2015 | X0.85 | Peter Brügger | Ersterfassung |
| 29.06.2015 | X0.86 | Peter Brügger | Input von Pascal Joye eingearbeitet<br>Template von BVerwE-KerberosAuthentication-no-ManApp auf BVerwE-KerberosAuthentication-viaPKI umbenannt |
| 09.07.2015 | X0.88 | Peter Brügger | Input von Review mit Jürgen Weber u. Pascal Joye eingearbeitet und Prüfkriterien erweitert, Dokument umbenannt |
| 13.07.2015 | X0.90 | Peter Brügger | Input von Mario Muster eingearbeitet |
| 14.07.2015 | V1.0 | Peter Brügger | Zur Freigabe auf www.pki.admin.ch |
| 21.07.2015 | V1.01 | Peter Brügger | Template Namen in den Prüfkriterien berichtigt |

## Inhaltsverzeichnis

# 1 Einleitung

Domain Controller Zertifikate werden in folgenden drei Fällen benötigt

- Smart Card Logon (Interactives Logon)
- Ldap/s abfragen des Active Directories
- SMTP e-mail Replikation zwischen Domänen innerhalb eines Forest
  Mit autoenrollment wird für SMTP e-mail Replikation das Template Directory Email Replication eingesetzt. Ein Zertifikat für SMTP e-mail Replikation benötigt im SAN die Server GUID des Domain Controllers

Für die anderen Verwendungszwecke ist heute für autoenrollment das Template Kerberos Authentication , der Standard. In diesen Zertifikaten wird im SAN die GUID des DC nicht benötigt

In dieser Anleitung werden Zertifikate vom Template KerberosAuthentication als Domain-Controller Zertifikate DC-Zertifikate bezeichnet

# 2 Manuelles Enrollment von BVerwE-KeberosAuthentication-viaPKI Template

Diese Anleitung beschreibt das manuelle Enrollment eines Zertifikates für Domain Controller ohne Server GUID des DC im Subject Alternative Name. Dieses Zertifikat kann damit nicht für SMTP e-mail Replikation zwischen Domänen in einem Forest eingesetzt werden

## 2.1 Templates Konfiguration

Template Namen: BVerwE-KerberosAuthentication-noManApp
← US-intraCA-CaAdmin read / enroll
**Nur die Mitglieder der Gruppe US-intraCA-CaAdmin bekommen das Recht ein enrollment von diesem Template auszuführen.**
Subject Name Supply in the request “aktiviert”
Issuance Requirements: CA Certificate Manager approval nicht „aktiviert“
Laufzeit des Zertifikates: 3 Jahre

## 2.2 Unterstützte Domänen für manuelles Enrollment von DC-Zertifikaten

BFS-BFK Service & Design PKI und BFS-BFO PKI Operation entscheiden ob für einen fremden Forest/ Domäne DC-Zertifikate ausgegeben werden oder nicht. Diese Abmachung muss vorgängig stattgefunden haben. Unterstützte Forest/ Domänen werden im Dokument in der Template-Beschreibung CertTemplateSpec-BVerwE-KerberosAuthentication-viaPKI im Kapitel General unter „Unterstützte Forest oder Domänen“ aufgeführt.

Wird der Antrag für die Ausstellung von Domain Controller Zertifikate unterstützt, bezeichnet der Kunde 1-2 Personen, welche einen Antrag für das Ausstellen von Domain Controller Zertifikate stellen können, diese Namen werden auch im Dokument der Template-Beschreibung CertTemplateSpec-BVerwE-KerberosAuthentication-viaPKI im Kapitel General unter „Unterstützte Forest oder Domänen“ aufgeführt.

## 2.3 Voraussetzungen

Der Forest muss für Smart Card Logon vorbereitet sein
Der 1. CDP Pfad des Zertifikats www.pki.admin.ch/crl/Admin-CCE-Intra01.crl muss aufgelöst werden konnen.

## 2.4 Prozess manuelles Enrollment KerberosAuthentication Zertifikate

1. Der Zertifikatsbezüger erstellt auf seinem DC mit dem Powershell Script NewDCReq-10.ps1 ein Requestfile
   Das Powershell Script ist von www.pki.admin.ch -> Zertifikatstypen → Klasse E → auf der rechten Spalte herunterladbar, die Integrität des Scripts muss überprüft werden und von *.txt auf *.ps1 unbenannt werden
   Das Script erstellt das Request-File DCReq.req
2. Der Antragsteller meldet sein Anliegen mittels einem **signierten** E-Mail an pki-info@bit.admin.ch.
   Folgende Angaben werden im Bestellungsmail erwartet:
   Das unter Punkt 1 erstellte Requestfile als Anhang
   Im Mail den vollständigen Namen der Domäne des DCs, für welchen dieses DC-Zertifikat ausgestellt werden soll
3. PKI-Info stellt sicher, dass die Prüfkriterien Teil 2 eingehalten sind.
4. Der CA-Betreiber kopiert diese Datei in ein Verzeichnis auf der CA
5. In diesem Verzeichnis auf der CA führt der CA-Betreiber das Script submit-10.ps1 aus
   Das Powershell Script ist von www.pki.admin.ch -> Zertifikatstypen → Klasse E → auf der rechten Spalte herunterladbar, die Integrität des Scripts muss überprüft werden und von *.txt auf *.ps1 unbenannt werden
   Das signierte Zertifikat wird in dieses Verzeichnis mit Namen NewDC.cer gespeichert.
6. Der CA-Betreiber sendet dem Zertifikatsbezüger mittels signiertem E-Mail das Zertifikat zu, sofern die Prüfkriterien Teil 1 eingehalten sind
7. Der Zertifikatsbezüger speichert dieses Zertifikat in einem Verzeichnis auf dem DC, auf welchem er den Request erstellt hat.
8. In diesem Verzeichnis führt der Zertifikatsbezüger das Powershell Script „InstallCert-10.ps1“ aus.
   Das Powershell Script ist von www.pki.admin.ch -> Zertifikatstypen → Klasse E → auf der rechten Spalte herunterladbar, die Integrität des Scripts muss überprüft werden und von *.txt auf *.ps1 unbenannt werden
9. Der Zertifikatsbezüger stellt sicher, dass unter Computerzertifikaten ein neues Zertifikat sichtbar ist. Statt einem Templatenamen ist im Zertifikat eine OID angegeben.)
10. pki-info@bit.admin.ch. legt das Bestellungsmail Mail des Antragstellers in einem definierten Folder ab.

## 2.5 Vorhandene Einschränkungen

Der 2. CDP Pfad zeigt auf das Active Directory intra.admin.ch und ist für Server die sich nicht im Forest INTRA befinden nicht auflösbar. Der 1. CDP Pfad ist www.pki.admin.ch/crl ist überall auflösbar

Es steht also nur ein gültiger CDP Path zur Verfügung.

## 2.6 Lifecycle

**ACHTUNG**: Zertifikat Ablauf nicht verpassen! Das Zertifikat ist 3 Jahre gültig und wird nicht automatisch erneuert!
Der Server-Betreiber ist für den Lifecycle des Zertifikats zuständig.

## 2.7 Prüfkriterien für Zertifikate des Templates BVerwE-KerberosAuthentication-viaPKI

### Teil 1 - CA-Betrieb

Der Domain Suffix in Subject und SAN im Zertifikat entsprechen dem Namen , welcher der Zertifikatsbezüger im Bestellungsmail gemäss Punkt 2 im Prozess angegeben hat

### Teil 2 - PKI-Info

Ist der Antragsteller berechtigt ein signieren von einem Domain Controller Zertifikat zu verlangen, sichtbar in der Template-Beschreibung CertTemplateSpec-BVerwE-KerberosAuthentication-viaPKI in im Kapitel General unter „Unterstützte Forest oder Domänen“

Pki-info stellt sicher dass für die im Bestellungsmail angegeben Domäne unter den genehmigten Domänen für manuelles Enrollment von DC-Zertifikaten aufgeführt ist, sichtbar in der Template-Beschreibung CertTemplateSpec-BVerwE-KerberosAuthentication-viaPKI in im Kapitel General unter „Unterstützte Forest oder Domänen“

Im Requestfile überprüft PKI-Info, dass der Domain Suffix in Subject und SAN im Zertifikat dem Namen entsprechen, welcher der Zertifikatsbezüger im Bestellungsmail gemäss Punkt 2 im Prozess angegeben hat