Eigentümer: co.met www.co-met.info

co.met GmbH
Hohenzollernstraße 75
66117 Saarbrücken
www.co-met.info

Betreiber: Stadtwerke Saarbrücken

Stadtwerke Saarbrücken GmbH
Hohenzollernstraße 104-106
66117 Saarbrücken
www.sw-sb.de

Zertifikatsprozesse der SEN

Version	1.0		
Geltungsbereich	SEN		
Klassifizierung	Öffentlich		
Dokumenteneigner	Yvonne Kühn		
Genehmiger	Natalia Götz		
Empfängerkreis/ Verteilerliste	Öffentlich		
Dokumentenstatus	Entwurf		
Dokumententyp	Dokument (DOK)		
Autor/FB/ORGA	Kuehn Yvonne	C7	Co.met
Gültig ab	16.07.2018		

Historie

Version	Datum/Stand	FB/ORGA	Änderungsbeschreibung
V 0.01	16.07.2018	C7/co.met	Erstellung des Dokumentes
V 0.02	26.07.2018	C7/co.met	Korrektur des Dokumentes
V 0.03	30.07.2018	C7/co.met	Einarbeiten der Korrekturen
V 0.04	02.08.2018	C7/co.met	Anpassung einiger Screenshots
V 0.05	10.09.2018	C7/co.met	Änderungen beim Vorgang zum Hochladen der Zertifikate
V 0.06	01.10.2018	C7/co.met	Hinzufügen des fünften Kapitels

Prüfung/Freigabe

Version	Datum	Autor/FB/ORGA	geprüft / freigegeben
V 1.0	14.11.2018	C7/co.met	Natalia Götz

Inhalt

Abbildungsverzeichnis

1. Einleitung

Durch die Inbetriebnahme der Hardware-Sicherheitsmodule wird der PKI Ansprechpartner, der in den Antragsformularen zur Teilnahme an der SEN.CA ausgewählt wurde, in die Zertifikatsprozesse einbezogen. Hierzu zählen die Prozesse zur initialen Zertifikatserstellung, dem routinemäßigen Folgeantrag (Zertifikatserneuerung) und dem Sperren eines Zertifikats. In diesem Dokument werden die Aufgaben des PKI Ansprechpartner bezüglich der initialen Zertifikatserstellung und der Zertifikatserneuerung beschrieben. Weiterhin folgt im letzten Kapitel eine Checkliste zu den Anforderungen, die der SEN.CA Teilnehmer in der Testumgebung zu erfüllen hat, damit der Eintritt in die Produktivumgebung gewährt werden kann.

Die Schaubilder zu den Prozessen sind aufgrund der Größe im Anhang dargestellt. Bei Bedarf können diese als Prozessexport oder Bild zur Verfügung gestellt werden.

2. Prämissen

1. Der PKI Ansprechpartner muss einen Benutzer in der Green- und/oder BlueBox haben. Der Zertifikatsrequest für die zu generierenden EMT und/oder GWA Zertifikate muss in der entsprechenden Anwendung erzeugt werden.
2. Werden Zertifikate für die Test- oder Produktivumgebung benötigt, muss ein Thin Client, der den Zugang zu den Umgebungen ermöglicht, funktional beim Kunden installiert sein. Smartcard und PIN des SEN Benutzers müssen vorliegen.

3. Aufgaben des PKI Ansprechpartners zur initialen Zertifikatserzeugung

3.1. Kurzbeschreibung des Prozesses

Sobald die Anträge zur Teilnahme an der SEN.CA eingehen, wird mit der Ausprägung des Mandanten und Benutzers begonnen. Ist der Mandant erzeugt und der erste Benutzer angelegt, wird ein Systemadministrator den Antrag zur Erstellung eines initialen Zertifikats generieren. Von der Software wird ein initialer Zertifikatsrequest erzeugt. Der PKI Ansprechpartner muss diesen Request prüfen und bei Richtigkeit genehmigen. Das macht er, indem der Inbox Eintrag bearbeitet wird. Dieser Inbox Eintrag kann nur von den beiden im Antrag angegebenen PKI Ansprechpartnern bearbeitet werden. Somit wird das von der Certificate Policy geforderte Vier-Augen-Prinzip und die Zuständigkeit des PKI Ansprechpartners für Zertifikatsangelegenheiten gewährleistet.

3.2. Zertifikatsrequest bearbeiten

Um den Zertifikatsrequest zu genehmigen, öffnet der PKI Ansprechpartner seine Blue- oder GreenBox. Sollen EMT und GWA Zertifikat erstellt werden, muss der Vorgang jeweils in der Blue- und GreenBox durchgeführt werden. Der PKI Ansprechpartner wird über eine Mail informiert, wenn

er den Inbox Eintrag „generateprivatekey“ mit der Meldung „Authorize Private Key generation“ (vgl. Abbildung 1) bearbeiten kann.

ABBILDUNG 1: INBOX EINTRAG

Der Eintrag wird über den Aktionsbutton geöffnet und es erscheint die Ansicht zur Autorisierung der Zertifikatsbeantragung (vgl. Abbildung 2). Dieser wird nach Prüfung autorisiert oder abgelehnt.

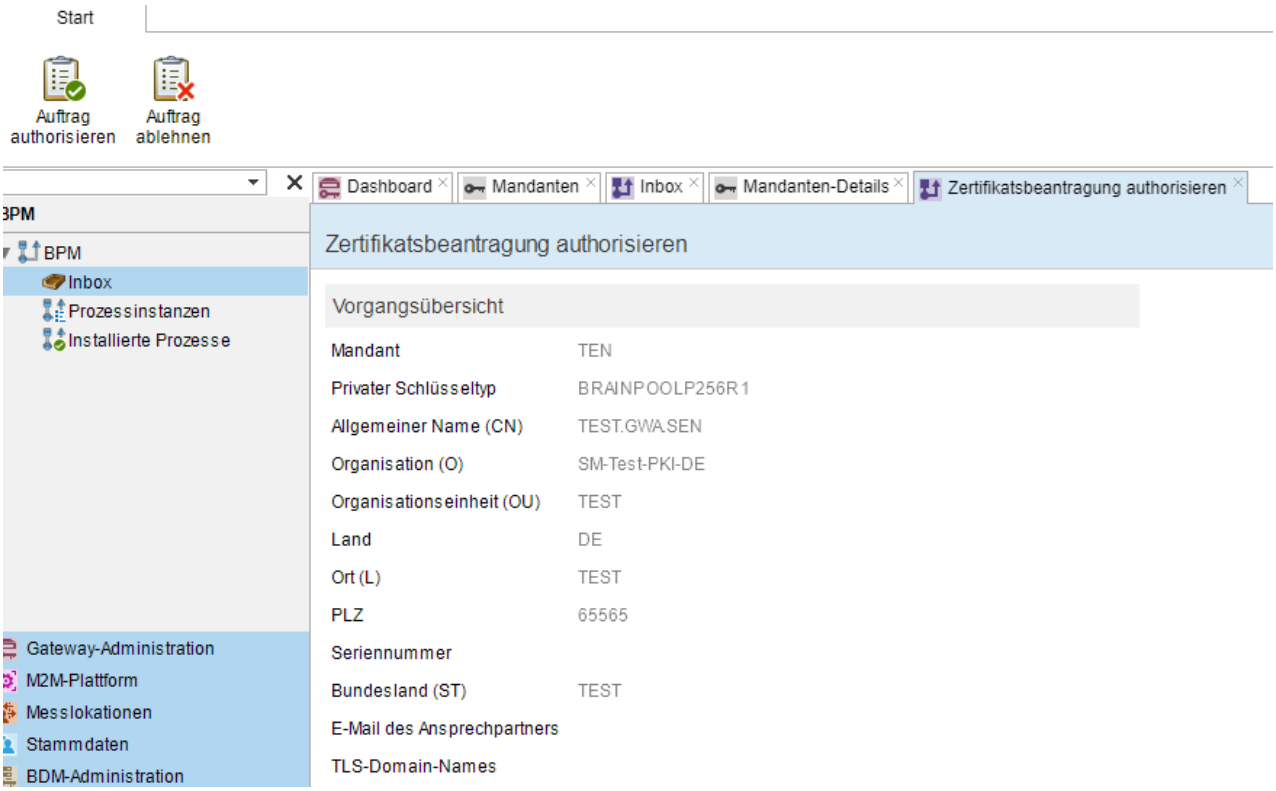

ABBILDUNG 2: AUTORISIERUNG DER ZERTIFIKATSBEANTRAGUNG

Der Antrag muss gewissenhaft geprüft werden, da sich bei der Erstellung Fehler einschleichen können und das Vier-Augen-Prinzip eingehalten werden muss. Somit wird verhindert, dass fehlerhafte Anträge zur Zertifikatserstellung an die SEN.CA gesendet und folglich falsche Zertifikate erstellt werden. Die einzelnen Felder müssen wie folgt ausgefüllt sein:

Mandant	Name des Mandanten, wie in den Formularen gewählt
Privater Schlüsseltyp	Vorausgefüllt; BRAINPOOLP256R1
Allgemeiner Name	Name Mandant.Rolle.SEN (bspw.: comet_gmbh.GWA.SEN)
Organisation (O)	Vorausgefüllt; SM-Test-PKI-DE

Organisationseinheit (OU)	Name des Hauptmandanten, wie in den Formularen angegeben
Land	Vorausgefüllt; DE
Ort (L)	Sitz des Mandanten (bspw. Saarbruecken)
PLZ	Postleitzahl des Ortes (bspw. 66117)
Seriennummer	Kann leer sein, wird von der Registrierungsstelle vergeben
Bundesland (ST)	Bundesland des Mandanten (bspw. Saarland)
E-Mail des Ansprechpartners	Vorausgefüllt; trustcenter@sen-pki.de
TLS-Domain-Names	Rolle.Umgebung.sen-cloud.de (bspw. gwa.test.sen-cloud.de)

Danach ist der nun erzeugte Inbox Eintrag „generatePrivateKey“ mit der Meldung „View generated CSR“ zu öffnen. In der nächsten Ansicht wird dieser angezeigt (vgl. Abbildung 3). Der Request in der roten Box muss herauskopiert und gespeichert werden.

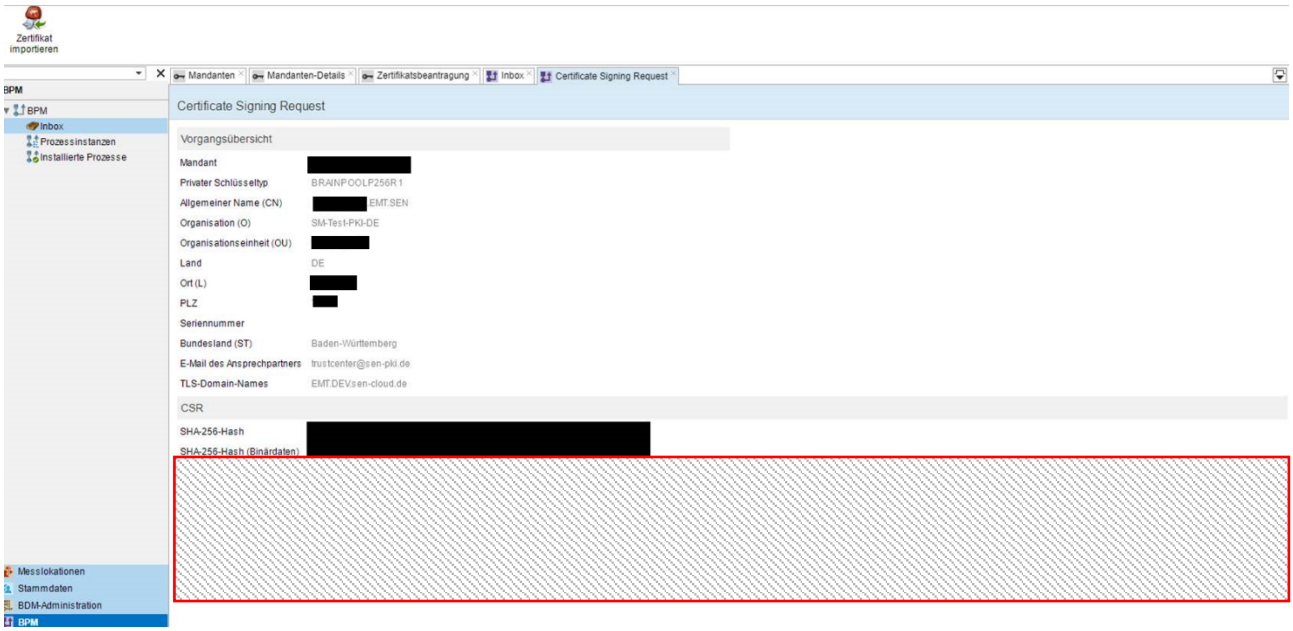

ABBILDUNG 3: ZERTIFIKATSREQUEST

Dazu bitte den Inhalt des rot umrandeten Kastens (siehe Abbildung 3) und den HASH-Wert (direkt über dem roten Kasten) aus der Bluebox herauskopieren und in eine Datei einfügen und speichern. Dies ist der Zertifikatsrequest.
Der Zertifikatsrequest muss in den beiden folgenden Formen und Wegen bei der SEN.CA eingereicht werden:

- Base64-codierter Ausdruck inkl. Unterschrift des PKI Ansprechpartners und Hash-Wert per Post an
  co.met GmbH
  Hohenzollernstraße 75
  66117 Saarbrücken

oder
das unterschriebene Dokument einscannen und als pdf an trustcenter@sen-pki.de

- Base64-codierte Datei (kein pdf, die Werte müssen am Rechner herauskopierbar sein) per S/MIME Mail an trustcenter@sen-pki.de mit dem Betreff: *Changenummer* (wird in einer Mail mitgeteilt) – Erstantrag SM-PKI Zertifikate *Mandantenname* (wie in den Antragsformularen gewählt)

Wichtig: Der Zertifikatsrequest wird bereits im Base64-codierten Format in der Inbox angezeigt. Der Request muss nur herauskopiert und als .txt Datei gespeichert werden. Hierfür sollte möglichst nicht das Programm Word verwendet werden, da häufig Zeilenumbrüche hinzugefügt werden, die in der späteren Verarbeitung Probleme bereiten. Der Hash-Wert muss nur auf dem Ausdruck aufgeführt werden.

Hinweis: Alle Dateien müssen über das SEN-Cloud E-Mail-Postfach an das Trustcenter gesendet werden. Das Postfach kann über https://exchange.vvs-konzern.de/owa vom normalen Arbeitsplatzrechner geöffnet werden. So kann die eingescannte Datei direkt versendet werden, ohne die Datei vorher mit dem Kryptostick auf den Thin Client übertragen zu müssen.

Der Auftrag wird anschließend in der entsprechenden Box abgeschlossen.
Nachdem der Request bei der SEN.CA eingegangen ist, werden die Zertifikate erstellt und an den Antragsteller per S/MIME versendet.

3.3. Zertifikate hochladen

Die von der SEN.CA gesendeten Zertifikate müssen in der entsprechenden Anwendung hochgeladen werden. Hierfür wird der Inbox Eintrag „View generated CSR“ geöffnet und die Zertifikate über den Button „Zertifikate importieren“ hochgeladen. Alle drei Zertifikate (TLS, ENC, SIGN) müssen gleichzeitig hochgeladen werden.

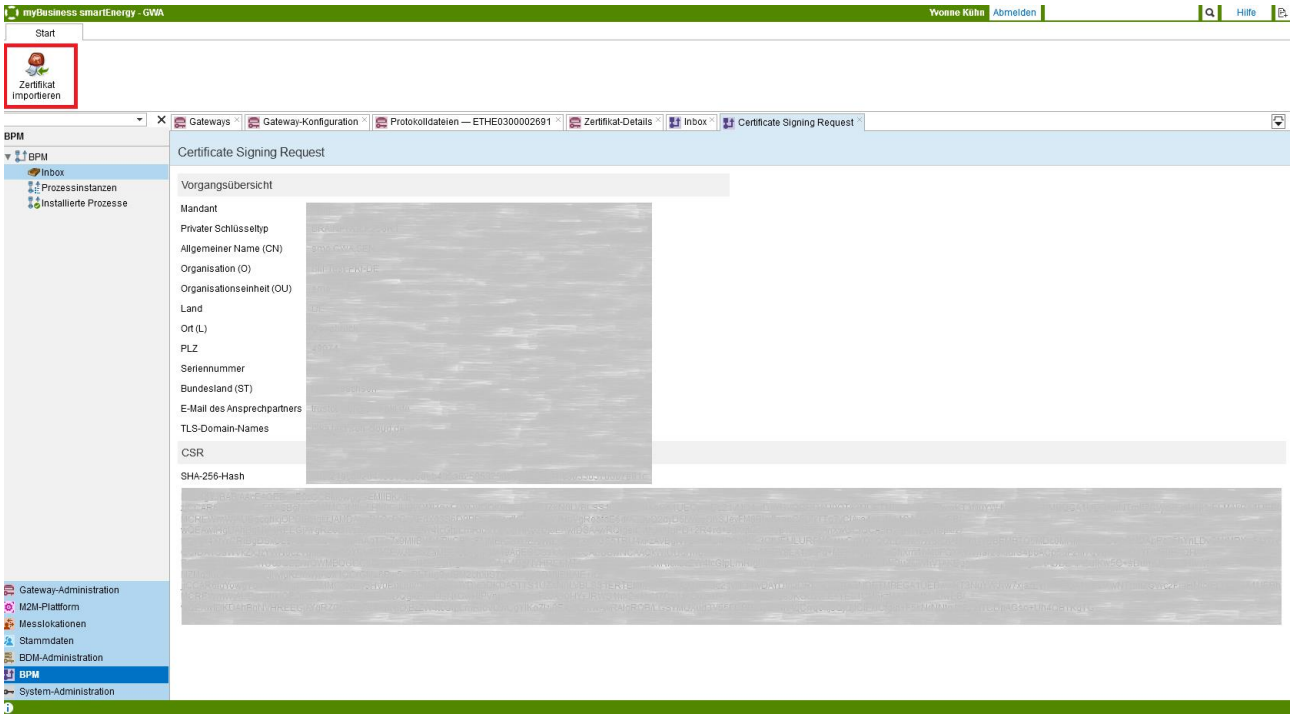

ABBILDUNG 4: ZERTIFIKATE HOCHLADEN

3.4. Schlüsselkennung mitteilen

Für die Konfiguration der Headends müssen die Schlüsselkennungen der hochgeladenen Zertifikate an sen@sen-cloud.de gesendet werden. Die Schlüsselkennung ist pro Zertifikatstyp (TLS, ENC, SIGN) den Zertifikatsdetails (vgl. Abbildung 5) zu entnehmen. Die Übertragung der Schlüsselkennung an die Administratoren der SEN-Cloud stellt sicher, dass die richtigen Zertifikate auf den Headends hinterlegt werden.

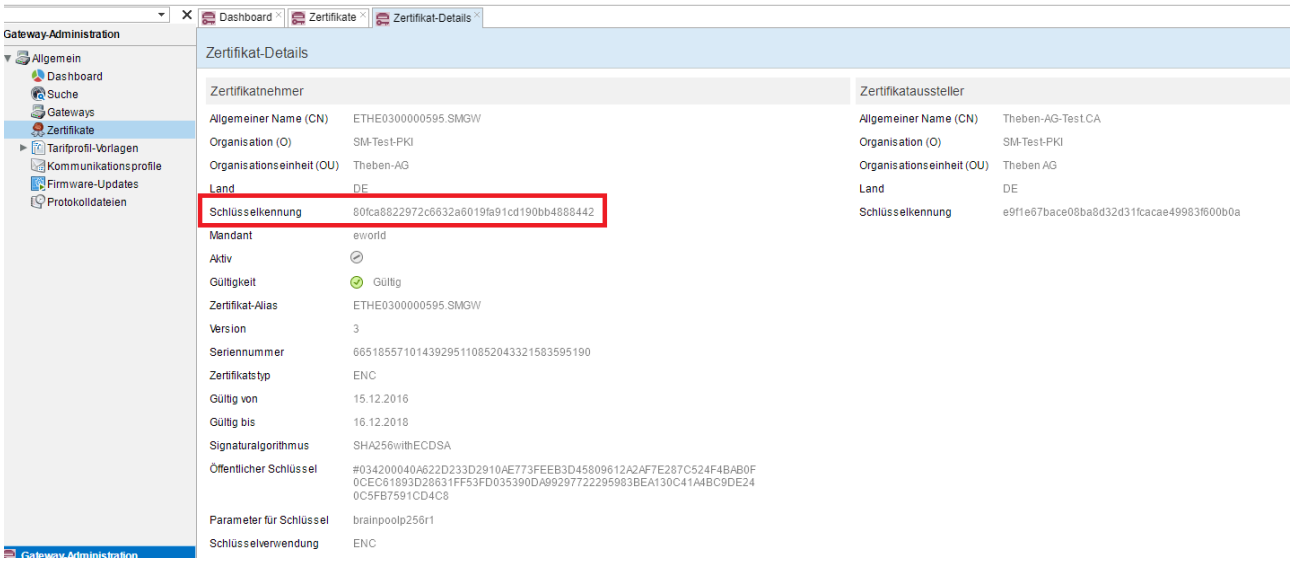

ABBILDUNG 5: SCHLÜSSELKENNUNG EINES ZERTIFIKATS

Die Zertifikate werden anschließend den Headends zugeordnet. Sobald der komplette Prozess abgeschlossen ist, wird eine Fertigmeldung an den Kunden versendet.

4. Aufgaben des PKI Ansprechpartners zum Einreichen eines routinemäßigen Folgeantrags

4.1. Kurzbeschreibung des Prozesses

Der routinemäßige Folgeantrag zur Erneuerung eines Zertifikats muss gemäß den Vorgaben der Certificate Policy einmal in der Testumgebung durchlaufen werden. Ansonsten wird der Prozess angewendet, wenn die Gültigkeitsdauer eines Zertifikats kurz vor dem Ablaufen ist oder das Zertifikat kompromittiert wurde und ausgetauscht werden muss.

Die Zertifikatserneuerung wird durch den Kunden mittels Einreichen des Antrags zum Erneuern eines Zertifikats angestoßen. Die Administratoren der SEN-Cloud werden anhand dieses Antrages die Generierung eines Folgezertifikats einleiten. Der Antrag muss ebenso dem initialen Antrag zur Einhaltung des Vier-Augen-Prinzips vom PKI Ansprechpartner in der Inbox genehmigt werden. Anschließend werden die Zertifikate erzeugt.

4.2. Zertifikatsrequest bearbeiten

Die ersten Schritte der Zertifikatsrequestbearbeitung sind analog dem Prozess der initialen Zertifikatsgenerierung. Der Eintrag wird in der Inbox geöffnet (vgl. Abbildung 1) und angenommen oder abgelehnt (vgl. Abbildung 2). Nachdem der Request angenommen wurde, wird dieser automatisch an die PKI übermittelt. Die Zertifikate werden direkt erzeugt und in der Green- oder BlueBox hochgeladen.

4.3. Schlüsselkennung mitteilen

Nachdem die Zertifikate vollautomatisch generiert und in der Software hinterlegt wurden, wird der PKI Ansprechpartner mittels automatisch generierter E-Mail aufgefordert, die Schlüsselkennung (vgl. Abbildung 5) der Zertifikate mitzuteilen. Die neu generierten Zertifikate können somit auf den Headends hinterlegt werden.

4.4. Nacharbeiten

Zum Abschluss der Zertifikatsprozesse für den Zugang zur Produktivumgebung muss ein Zertifikat gesperrt werden. Die Sperrung wird durch Einreichen des Dokuments „Antrag zum Sperren oder Suspendieren von Zertifikaten der SEN.CA“ initiiert. Es ist darauf zu achten, dass die neuen Zertifikate auf allen Smart Meter Gateways eingespielt wurden und kein Smart Meter Gateway mehr mit den alten Zertifikaten betrieben wird.

5. Bestätigung der Teilnahme an der Testumgebung

Bevor der Mandant in der Produktivumgebung ausgeprägt werden darf, müssen die Voraussetzungen aus der Certificate Policy des BSI[1] erfüllt sein. Sind alle notwendigen Prozesse durchlaufen, wird die erfolgreiche Testteilnahme mittels signierter E-Mail von der SEN.CA bestätigt.

In diesem Kapitel werden die Anforderungen an die verschiedenen Marktrollen mittels Checklisten beschrieben.

5.1. Passiver EMT

- ✓ Registrierung und Zertifikatsbeantragung
  - Die Registrierung und Zertifikatsbeantragung erfolgt mit Einreichen des Antrages zur Teilnahme an der SEN.CA inkl. Anlagen. Der Antragssteller bekommt im Verlauf seine Zertifikate ausgestellt. Die Anforderungen an die Registrierung gemäß der Certificate Policy S. 22 f werden komplett mit den Antragsformularen abgefragt.
- ✓ Sicherheitskonzept ist erstellt
- ✓ Zertifikatserneuerung (routinemäßiger Folgeantrag) des EMT-Zertifikats
  - Für die Zertifikatserneuerung muss wie in Kapitel 4 beschrieben das Formular zur routinemäßigen Erneuerung der Zertifikate eingereicht werden.
- ✓ Zertifikatssperrung eines EMT-Zertifikats
  - Für die Durchführung einer Zertifikatssperrung muss das in Kapitel 4.4 beschriebene Formular eingereicht werden. Bspw. kann das initial ausgestellte Zertifikat gesperrt werden, da nach der Ausstellung des Folgezertifikats mit diesem gearbeitet wird.

5.2. Aktiver EMT

- ✓ Registrierung und Zertifikatsbeantragung
  - Die Registrierung und Zertifikatsbeantragung erfolgt mit Einreichen des Antrages zur Teilnahme an der SEN.CA inkl. Anlagen. Der Antragssteller bekommt im Verlauf seine Zertifikate ausgestellt. Die Anforderungen an die Registrierung gemäß der Certificate Policy S. 22 f werden komplett mit den Antragsformularen abgefragt.
- ✓ ISO 27001 Zertifikat liegt vor
- ✓ Zertifikatserneuerung (routinemäßiger Folgeantrag) des EMT-Zertifikats
  - Für die Zertifikatserneuerung muss wie in Kapitel 4 beschrieben das Formular zur routinemäßigen Erneuerung der Zertifikate eingereicht werden.
- ✓ Zertifikatssperrung eines EMT-Zertifikats
  - Für die Durchführung einer Zertifikatssperrung muss das in Kapitel 4.4 beschriebene Formular eingereicht werden. Bspw. kann das initial ausgestellte Zertifikat gesperrt werden, da nach der Ausstellung des Folgezertifikats mit diesem gearbeitet wird.

[1] Vgl. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03109/PKI_Certificate_Policy.pdf?__blob=publicationFile&v=3 , S. 22ff

5.3. GWA

- ✓ Registrierung und Zertifikatsbeantragung
  - Die Registrierung und Zertifikatsbeantragung erfolgt mit Einreichen des Antrages zur Teilnahme an der SEN.CA inkl. Anlagen. Der Antragssteller bekommt im Verlauf seine Zertifikate ausgestellt. Die Anforderungen an die Registrierung gemäß der Certificate Policy S. 22 f werden komplett mit den Antragsformularen abgefragt.
- ✓ ISO 27001 inkl. TR-03109-6 Zertifikat liegt vor
- ✓ PKI Ansprechpartner haben sich persönlich bei der First-Level-RA der SEN.CA identifiziert und authentifiziert
- ✓ Zertifikatserneuerung (routinemäßiger Folgeantrag) des GWA-Zertifikats
  - Für die Zertifikatserneuerung muss wie in Kapitel 4 beschrieben das Formular zur routinemäßigen Erneuerung der Zertifikate eingereicht werden.
- ✓ Zertifikatssperrung eines GWA-Zertifikats
  - Für die Durchführung einer Zertifikatssperrung muss das in Kapitel 4.4 beschriebene Formular eingereicht werden. Bspw. kann das initial ausgestellte Zertifikat gesperrt werden, da nach der Ausstellung des Folgezertifikats mit diesem gearbeitet wird.
- ✓ Zertifikatserneuerung eines SMGw-Zertifikats
  - In diesem Schritt muss der Wechsel von Gütesiegel- auf Wirkzertifikate durchgeführt werden. Es muss also mind. ein Gateway zur Durchführung dieses Prozesses in der Testumgebung installiert sein. Der Prozess kann direkt im GWA-Modul angestoßen werden.
- ✓ Zertifikatssperrung eines SMGw-Zertifikats
  - Die Sperrung eines SMGw-Zertifikats kann direkt im GWA-Modul angestoßen werden. Bspw. kann der Prozess der Zertifikatserneuerung zweimal durchgeführt werden. So kann das initial ausgestellte Wirkzertifikat ohne Verlust der Kommunikation zum Gateway gesperrt werden.

Anhang

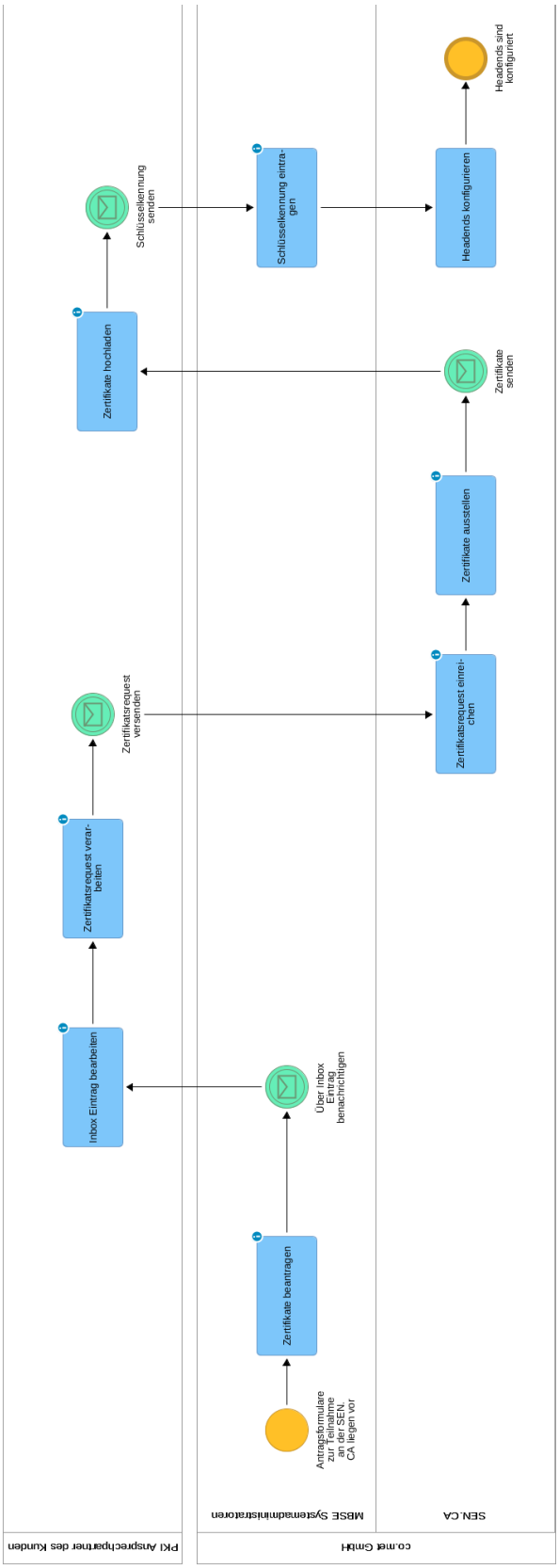

ABBILDUNG 6: PROZESS ZUR INITIALEN ZERTIFIKATSERZEUGUNG

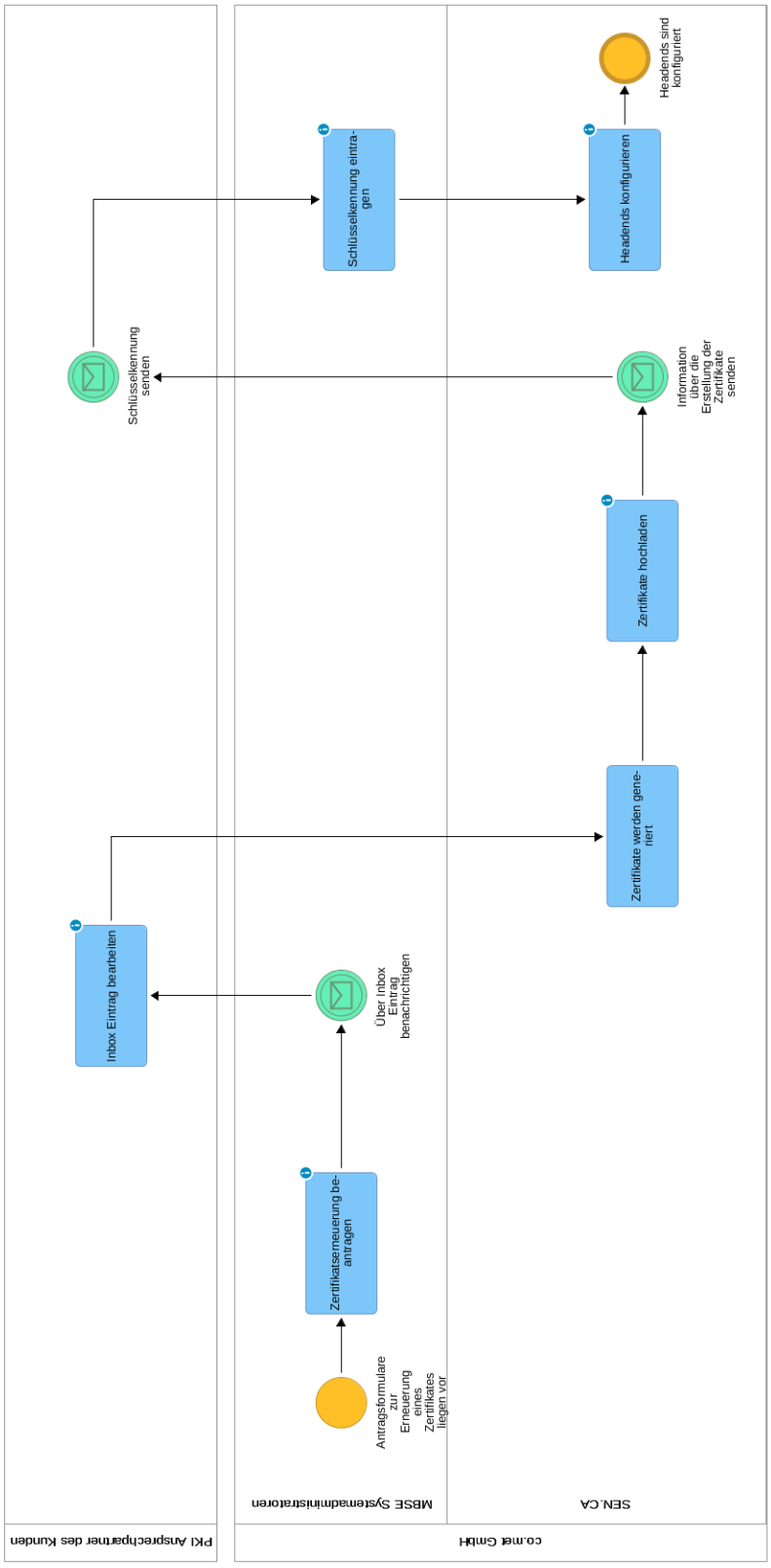

ABBILDUNG 7: PROZESS ZUR ERZEUGUNG EINES FOLGEZERTIFIKATS