Leistungsbeschreibung ***SEN-PKI*** Sub-CA

Datum: 28.05.2015

Trustcenter@VVS-mbH

VVS-Trustcenter

VVS-Trustcenter

Leistungsbeschreibung Smart Energy Cloud Sub-CA

Im Trustcenter der VVS.

Erstellt von:

Versorgungs- und Verkehrsgesellschaft Saarbrücken mbH

Hohenzollernstraße 104 – 106

66117 Saarbrücken

Autor: Christian Schorr

INHALTSVERZEICHNIS

ABBILDUNGSVERZEICHNIS

1 VORWORT

Die CA (Certification Authority) ist einer der wichtigsten Bestandteile der Public Key Infrastructure (PKI) im Smart Energy Network (SEN). Bereits heute bietet VVS-IT im VVS-Trustcenter PKI-Dienste an. Der Link zur offiziellen PKI-Seite lautet:

http://trustcenter.tec-saar.de/

Die Sub-CA der Smart Energy Cloud läuft unter dem Namen: ***SEN-PKI*** (Smart Energy Network - Public Key Infrastructure)

In Kürze finden Sie alles Wissenswerte, Formulare und Informationen rund um die SEN-PKI (Smart Energy Network PKI) im Web unter:

http://www.sen-pki.de

Im Rahmen des Aufbaus der Smart-Energy-Cloud wird das vorhandene Angebot des VVS-Trustcenters um PKI-Dienstleistungen erweitert, die für den Betrieb von Smart-Meter-Infrastrukturen entsprechend den Anforderungen in den Technischen Richtlinien - BSI TR-03109 ff - notwendig sind. Folgende Smart Meter PKI-Dienste werden im Rahmen der aufgebauten und betriebenen BSI-Sub-CA angeboten (BSI TR-030109-4):

- **Zertifikatsmanagementdienste** für das Ausstellen und Verwalten von Smart Meter Zertifikaten für alle externe Marktteilnehmer (**EMT**), Gateway-Administratoren (**GWA**), Hersteller von SMGW's (**GWH**) und Smart Meter Gateways (**SMGW**) für folgenden Verwendungszweck:
  - TLS-Zertifikate zur gegenseitigen Authentisierung zwischen SMGW und autorisierten Marktteilnehmern
  - Verschlüsselungszertifikate für die Ende-zu-Ende-Verschlüsselung von Daten auf der Dateninhaltsebene unabhängig von der TLS-Verbindung
  - Signaturzertifikate
  - Authentifizierungszertifikate
- **Verzeichnisdienste:** Betrieb eines nicht-öffentlichen Verzeichnisdienstes mit allen ausgestellten Zertifikaten, auf den ausschließlich die Teilnehmer der Smart Meter PKI Zugriff haben.
- **Sperrlistenmanagementdienste** für die Erstellung, Pflege und öffentliche, vertrauenswürdige Bereitstellung aktueller Sperrlisten

Spezialisiertes Know How, eine hochredundante RZ-Infrastruktur (Rechenzentrum) und die breitbandige Internetanbindung über ein eigenes Autonomous System (AS) versetzen uns in die Lage den Baustein PKI als Sub-CA (SEN-PKI), angeschlossen an die Root-CA des BSI, mandantenfähig im SEN (Smart Energy Network) zu betreiben und als Dienstleistung anzubieten. Unser SEN-PKI Trustcenter (Smart Energy Network PKI Trustcenter) stellt somit, die vertrauenswürdige dritte Instanz dar um die jeweilige Identität eines berechtigten Marktteilnehmers im SEN (Smart Energy Network) zu bescheinigen. Dies geschieht mit Zertifikaten und sicheren Schlüsselalgorithmen, die nach den Vorgaben des BSI zum Schutze und der Absicherung der Infrastruktur definiert wurden. Hierfür betreiben wir in unsern zertifizierten Rechenzentren spezielle Hard- und Software, welche diesen Anforderungen gerecht wird.

1.1 POC PROOF OF CONCEPT

Mit der Entwicklung und Ausarbeitung eines Implementierungskonzeptes beschäftigen wir uns als VVS bereits seit dem Jahre 2012. Im November des Jahres 2013 haben wir uns mit leistungsfähigen Partnern zusammengeschlossen, um in einem ersten Proof of Concept die Realisierungsphase einzuleiten. Unser Ziel ist es, eine vollumfängliche Lösung für alle Marktteilnehmer bis 2016 bereitzustellen.

1.2 WER SIND WIR

Die Versorgungs- und Verkehrsgesellschaft Saarbrücken mbH kurz VVS, ist einer der größten kommunalen Dienstleister in der Landeshauptstadt Saarbrücken. Insgesamt arbeiten ca. 1.000 Mitarbeiterinnen und Mitarbeiter in diesem Konzern.

Unsere Geschäftsfelder

- Die Energieerzeugung der VVS
  - Heizkraftwerk Süd, Blockheizkraftwerke auf dem Gelände der Saarbahn, am Standort Gasbehälter Ost und am Standort Römerbrücke
- Saarbahn GmbH
  - Die Saarbahn GmbH und die Stadtbahn Saar GmbH leisten unter SaarBahn&Bus den öffentlichen Personennahverkehr auf der Straße und auf der Schiene in der Landeshauptstadt Saarbrücken und im Regionalverband.
- Stadtwerke Saarbrücken
  - Netzwerk für Strom, Erdgas, Fernwärme und Wasser
- Consulting + Bäderbetriebsgesellschaft + Beteiligungen
- Trinkwasser
  - Eigenbetrieb der Wasserwerke in Rentrisch, St. Arnual, Blickweiler und Wolfersheim
- Messwesen
  - co.met GmbH bietet umfassende Dienstleistungen bei der Erfassung, Verarbeitung und Übermittlung von Verbrauchsdaten.
- IT Dienstleistung + Trustcenter + RZ-Betrieb + Consulting
  - Hochverfügbarkeitsplattform für das Hosting von
    - Smart Meter Geräteverwaltungssystemen
    - Meter Data Management (MDM)-Systeme
    - Security Gateway Administrationssysteme
    - Unterstützt die IT-technischen Konzepte des Big-Data Managements und der MDM-Systeme
    - Ermöglicht die wirtschaftliche Verarbeitung umfangreicher Datenmengen
    - Mandantenfähig und Skalierbar
    - Derzeit befinden wir uns in der Zertifizierungsphase entsprechend den gesetzlichen Anforderungen der TR 03109:
      - ISO/IEC 27001 nach BSI Grundschutz
      - Zertifizierung nach TR 03145

1.3 Unsere Partner im Projekt

„…als bundesweiter Metering-Dienstleister für die Energie- und Versorgungswirtschaft betreut co.met aktuell über 300 aktive Vertragskunden und erbringt somit täglich Teilleistungen an über 2,2 Mio. Zählpunkten in ganz Deutschland…“

NEXT LEVEL Integration
B2B by Practice – die Innovative Plattform für Integration und Prozessabwicklung
Next Level Integration hat es sich zur Aufgabe gemacht, Unternehmen und Organisationen aller Größen bei der Vereinfachung und Optimierung ihrer Geschäftsprozesse zu unterstützen.

IBL - Ingenieurbüro Leidner
Effiziente Lösungen für eine moderne Energieversorgung Analyse und Optimierung von Energieversorgungssystemen sowie die Etablierung der hierfür notwendigen IT-Systeme und Geschäftsprozesse. I3L bietet die Integration von Daten und Applikationen.

krügernetwork – Consulting Solution Training
krügernetworks bietet als hersteller- und produktunabhängiges Beratungsunternehmen Dienstleitung bei der Planung und Umsetzung komplexer IT-Infrastruktur Projekte an und ist maßgeblich Verantwortlich für die Leitung und Entwicklung der PKI-Lösung.

1.4 EINSATZBEREICHE EINER PKI

Unsere langjährige Erfahrung im Aufbau und Betrieb einer mandantenfähigen PKI-Infrastruktur befähigen uns die Anforderungen der Technischen Richtlinie, welche durch das BSI definiert wurden, gerecht zu werden. Unsere Mitarbeiter bilden, durch die spezialisiertes Fachwissen, die Säulen der Systemlösung und sorgen für deren reibungslosen Betrieb. Mit unserer Zertifizierung erfüllen wir die Anforderungen nach ISO/IEC 27001 nach BSI-Grundschutz und der TR-03145, welche in den Technischen Richtlinien des BSI gefordert sind. In diesen, vom Bundesamt für Sicherheit in der Informationstechnik, ausformulierten Richtlinien ist beschrieben, wie Sicherheit und Funktionalität im Smart Energy Network implementiert werden muss.

1.5 RISIKOFAKTOREN

Folgende Risikofaktoren können durch den Einsatz einer Public-Key-Infrastruktur abgemildert werden:

- Zentraler Schutz vor ungerechtfertigtem Zugriff
  - Nur autorisierte und authentifizierte Personen erhalten physikalischen Zugriff aufs Netzwerk (802.1x zertifikatsbasierend).
- Gesicherter Zugangsschutz, Zugangskontrolle, Zugangsberechtigung
  - Nur autorisierte, berechtigte Marktteilnehmer haben Zugriff ins SEN (Signaturzertifikate).
- Sicherung sensibler Daten gegen Spionage
  - Filesystemsicherheit (EFS - Encryption File-System)
- Sicherer Datentransport und Datenaustausch (Inhaltsdatenverschlüsselung)
  - Möglichkeiten der Kommunikationskanalsicherung im Transportlayer durch IPSEC Zertifikate usw.
  - Inhaltsdatenverschlüsselung
- Sicherung der Datenintegrität
  - Erkennen von unerwünschter Datenmodifikation
  - Integration eines gesicherten Zeitstempels
- Gewährleistung der Datenunverfälschtheit
  - durch Verschlüsselung durch z. B. S-Mime Kryptografie beim Mailversand.
- Sicherung der Datenauthentizität
  - Sicherstellung, dass der vorgegebene Absender auch der tatsächliche Absender ist (z. B. Signaturzertifikate)

1.6 BEISPIEL 1. – SMART-ENERGY-NETWORK

Ein Beispiel der VVS-Trustcenterdienste in Ihrem Unternehmen definiert sich durch die berechtigte Marktrolle im Smart-Energy-Netwerk der Zukunft. In der durch das BSI erarbeiteten Technischen Richtlinie (BSI TR-03109) werden diese Anforderungen definiert und dienen somit der Gewährleistung der Interoperabilität der verschiedenen in einem Smart-Metering-System vorhandenen Komponenten.

Einsatz einer PKI-Infrastruktur im Smart-Energy-Netzwerk

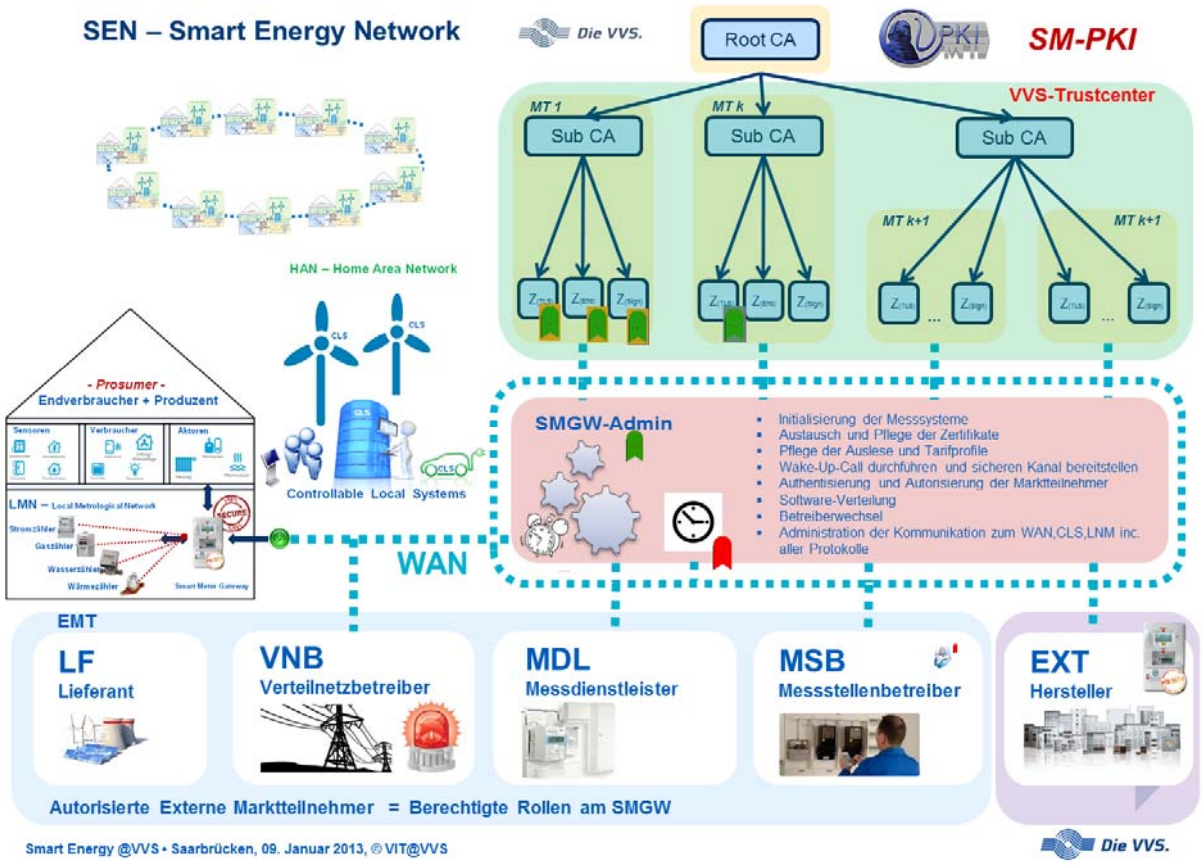

Abbildung 1 - Einsatz einer PKI-Infrastruktur im Smart-Energy-Netzwerk

1.7 BEISPIEL 2. - SMARTCARD

Ein weiteres Beispiel über die Vielfältigkeit und den flexiblen Einsatz unseres VVS-Trustcenters in Ihrem Unternehmen, kann der Einsatz einer Smartcard zur Zwei-Faktor-Authentifizierung (kurz 2FA) sein.

Smartcards mit entsprechenden Zertifikaten kommen überall dort zum Einsatz, wo der Schutzbedarf und die Vertrauenswürdigkeit der Daten mit hoch definiert ist. Sie bilden die Basis einer gesicherten Benutzerauthentifizierung bzw. Autorisierung, vertrauenswürdiger E-Mail Kommunikation über S/MIME und können zum Verschlüsseln sicherheitsrelevanter Daten eingesetzt werden. Die hierfür erforderlichen Schlüsselpaare werden bei der Kartenpersonalisierung in der jeweiligen Smartcard hinterlegt. Dadurch ist sichergestellt, dass der wichtigste Schlüssel, der private Schlüssel, sich zu keinem Zeitpunkt außerhalb der Karte befindet.

Einsatz einer PKI-Infrastruktur im Unternehmensnetzwerk

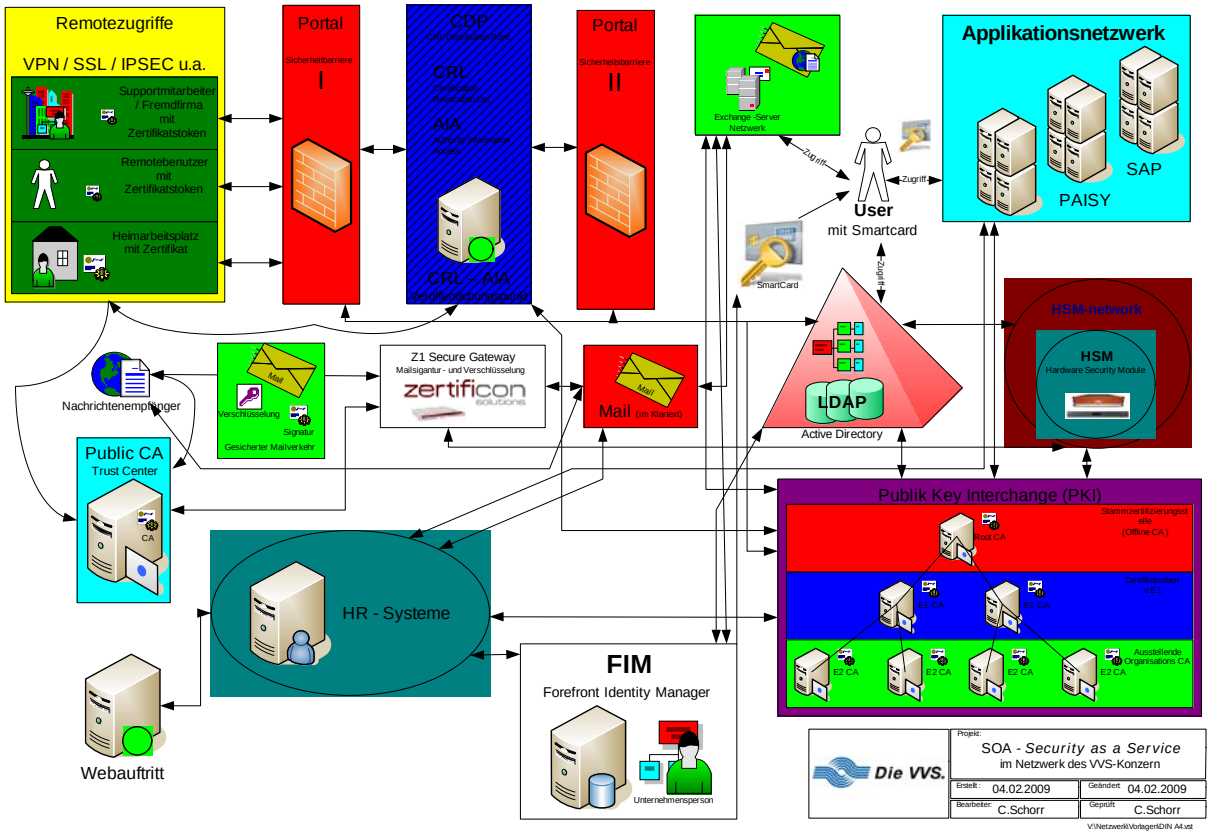

Abbildung 2 - PKI Infrastruktur (Smartcard)

2 DAS VVS – TRUSTCENTER

2.1 DIE INFRASTRUKTUR

Im VVS-Trustcenter befindet sich eine speziell angepasste IT-Infrastruktur für digitale Daten mit definiertem Schutzbedarf ‚*HOCH*'. Alle kryptografischen Operationen, welche in unserm Trustcenter Anwendung finden, werden ausschließlich in dafür bereitgestellten Peripheriegeräten (Hardware-Sicherheitsmodulen = HSM) bereitgestellt. Die Vertrauenswürdigkeit und Integrität von Daten und den damit verbundenen Informationen in geschäftskritischen IT-Systemen ist somit jederzeit sichergestellt. Um diese Infrastruktur abzusichern, sind unsere Rechenzentrums-standorte gegen digitale Angriffe genau so gut geschützt, wie gegen physikalische. So bieten unsere Rechenzentren neben den üblichen Zugangs-, Video-, Brand- und Hochwasserschutzs-zenarien dank unserer Tochtergesellschaft, der Stadtwerke Saarbrücken GmbH, auch eine direkte Integration in die zentrale Netzleitstellenwarte für Niederspannungsanlagen im Saarland. Dank der Vielzahl skalierbarer Funktions- und Integrationsumfänge bieten somit die Systeme von VVS Hochverfügbarkeit von Informationen und Prozessen im 24*7 Stunden-Betrieb. Störungen und Probleme werden zeitnah erkannt und können durch ein Team von Mitarbeitern aus verschiedenen Berufsfeldern schnell und professionell behoben werden.

Der Zugang zur Infrastruktur der PKI ist ausschließlich dem administrativen Fachpersonal vorbehalten. Alle unsere IT-Systeme befinden sich in abgesicherten Geräteschränken und sind über ein Schließsystem mit Alarmgebern geschützt. Alle Anlagen und Aktivitäten unterliegen regelmäßig protokollierten Wartungskontrollen.

Die interne Root-CA wird mit höchstem Schutzbedarf offline betrieben und nur zu operativ definierten Zeitpunkten online geschaltet. Alle administrativen Aufgaben werden workflowgesteuert über integrierte Rollenkonzepte durchgeführt. Ein Desaster Recovery Konzept regelt die Wiederherstellung aller sicherheitsrelevanten Systeme der VVS im Katastrophenfall. Unsere Rechenzentren arbeiten hierzu im Aktiv-Aktiv Betrieb.

Die VVS RZ-Infrastruktur

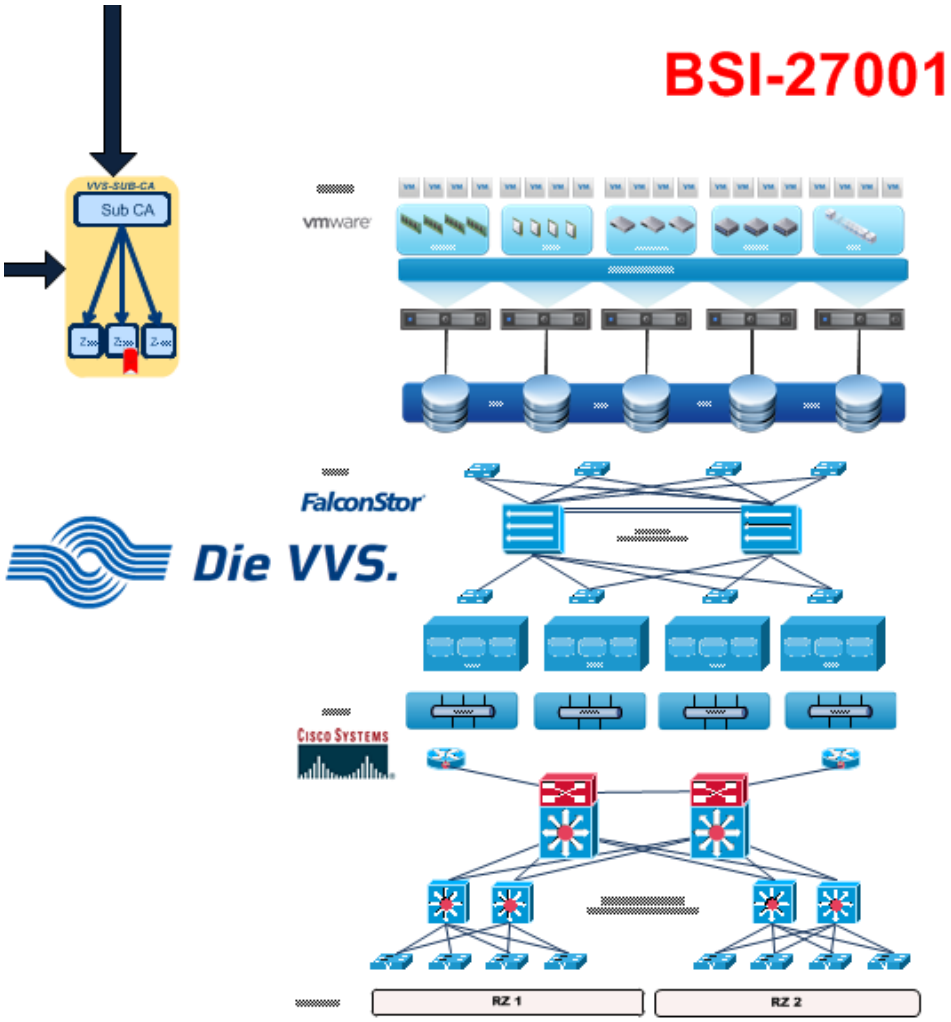

Abbildung 3 - VVS RZ-Infrastruktur

2.2 ARCHITEKTUR EINER INTERNEN PKI

Die Nutzung der Zertifikate steht zur Verwendung von sicherer Authentisierung, elektronischer Signatur sowie der Nachrichtenentschlüsselung zur Verfügung. Zertifikatnutzer sind in der Lage elektronische Signaturen und Nachrichtenverschlüsselung zu nutzen.

Aufbau einer internen PKI-Infrastruktur

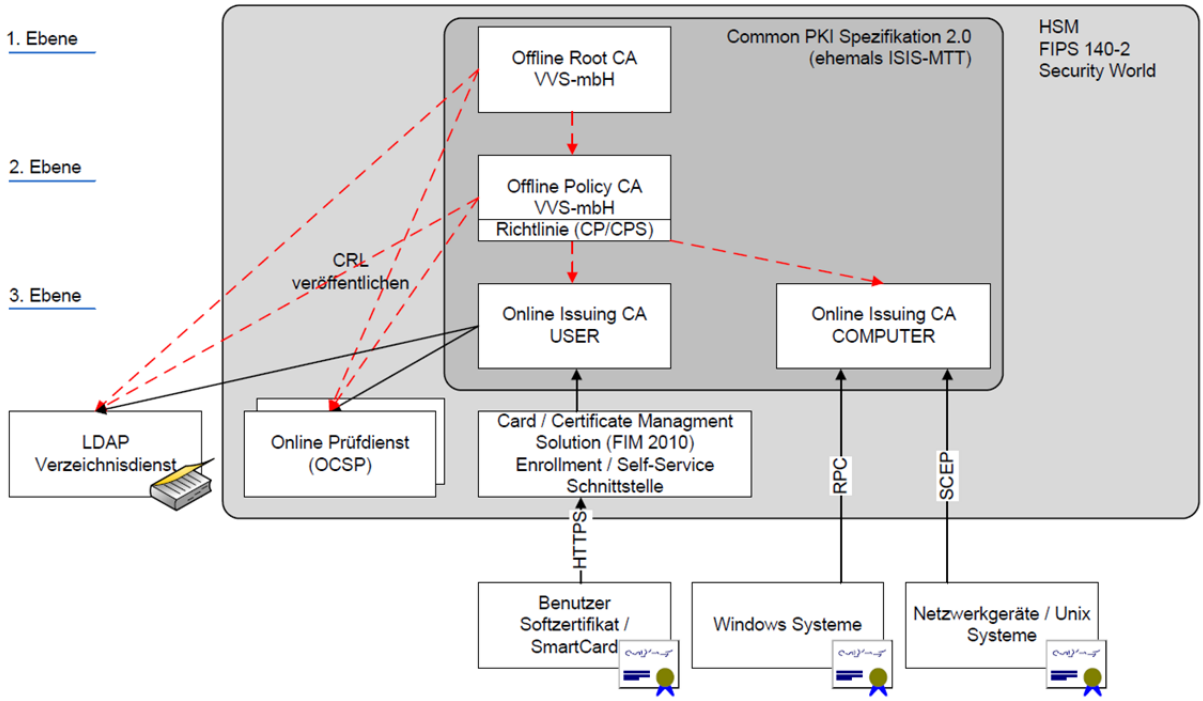

Abbildung 4 - Aufbau einer internen PKI-Infrastruktur

2.3 AUFBAU DER SEN SUB-CA IM TRUSTCENTER DER VVS

Die höchste Vertrauensinstanz, die Root-CA der Smart-Meter-PKI wird durch das BSI betrieben. Alle Sub-CA‘s bilden hierzu einen Vertrauensanker.

Die Bereitstellung der Public Key Infrastruktur für Smart Meter Gateways als Sub-CA erfolgt im Sinne der Technischen Richtlinie TR03109.

Aufbau der Smart-Meter-PKI

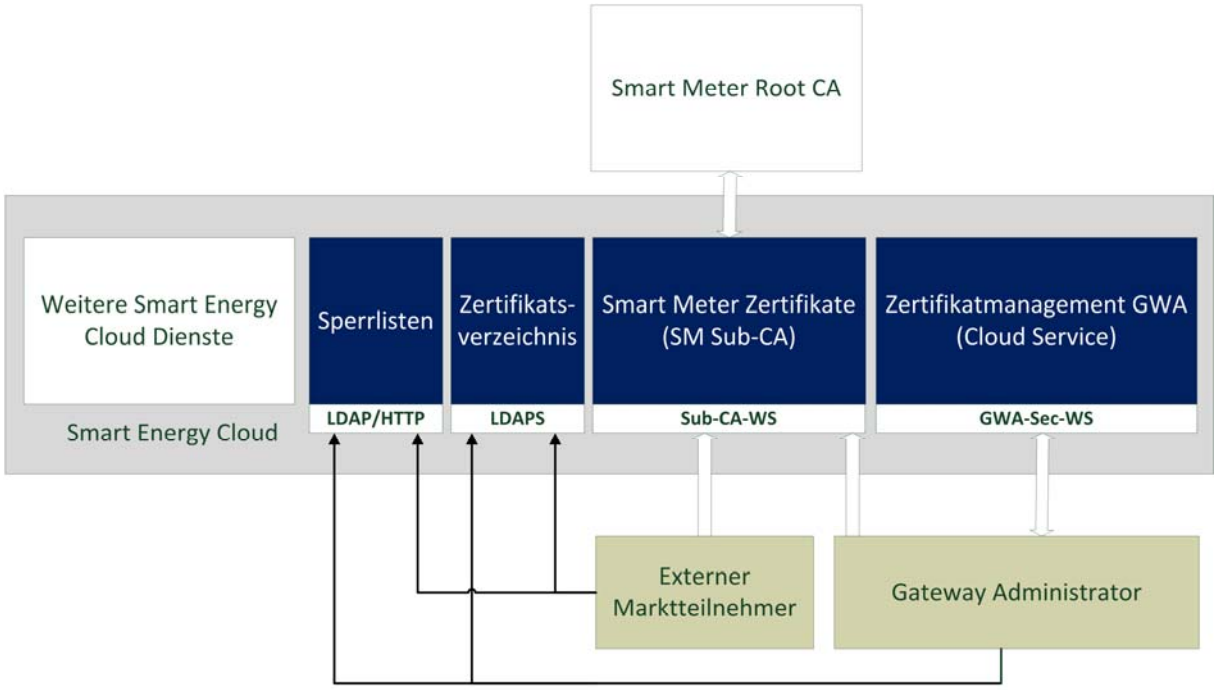

Abbildung 5 - SEC Sub-CA

3 PORTFOLIO DEN SEN-PKI

3.1 DAS LEISTUNGSSPEKTRUM IM VVS-TRUSTCENTER

Unser Portfolio umfasst folgende Leistungen:

- **Endnutzerzertifikate für alle berechtigten Marktrollen. (EMT)**
- **Smart Meter Zertifikate für die WAN-Kommunikation mit Smart Meter Gateways. (SMGW)**
- **Zertifikatsmanagement für Gateway Administratoren gemäß ISO 27001 auf der Basis von IT-Grundschutz und TR-03145 zertifiziertem Cloud Dienst. (GWA)**
- **Zertifikatsmanagement für Gateway Hersteller gemäß ISO 27001 auf der Basis von IT-Grundschutz und TR-03145 zertifiziertem Cloud Dienst. (GWH)**

3.2 MEHRWERTE DER SEN-PKI

Darüber hinaus bietet der Einsatz unserer SEN-PKI für unsere Kunden folgende Mehrwerte:

- **Anbindung externer Firmen-PKI‘s zur Absicherung und Kommunikation mit den CLS-Endgeräten im HAN (Schaltwarte, Netzleitstelle), alternativ die Bereitstellung entsprechender Zertifikate aus einer internen PKI des VVS-Trustcenters**
- **Web-Service-API und Benutzerfrontend mit integrierter Zwei-Faktor-Authentifizierung über Smartcards.**
- **Ausgabe von Informationen ausgegebener Zertifikate über eine separate Web Service Schnittstelle z B. zur Erstellung eines elektronischen Lieferscheins.**
- **Out of Band Registrierung zur Sicherstellung vorab registrierter Seriennummern-zertifikate.**
- **Sperrfunktionalität über Web Service.**
- **Gültigkeitsprüfung von Zertifikaten in der Vorpersonalisierungsphase 2 über Web Service Schnittstelle.**
- **Beratung und Implementierung kryptografischer Verfahren und Standards auf verschiedenen Plattformen sowie beim Einsatz und der Integration von Hardware Security Modulen (HSMs)**

3.2 GEPRÜFTE UND GENORMTE SICHERHEIT „MADE IN GERMANY“

Hochverfügbarer und vollredundanter RZ-Betrieb

- **Aktiv-Aktiv-Betrieb an zwei unabhängigen RZ-Standorten in Deutschland**
- **ISO27001 Zertifizierung auf Basis von IT-Grundschutz (in Kürze verfügbar)**
- **Zertifizierung nach TR-03145 (in Kürze verfügbar)**
- **IT-Grundschutz-Standard - erfüllt die Empfehlungen des BSI zu Methoden, Prozessen und Verfahren sowie Vorgehensweisen und Maßnahmen mit Bezug zur Informationssicherheit auf Basis von:**
    - **BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS).**
    - **BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise.**
    - **BSI-Standard 100-3: Risikoanalyse auf Basis von IT Grundschutz.**
    - **BSI-Standard 100-4: Notfallmanagement.**

Technologie- und Innovationsvorsprung durch Software-Defined Datacenter (SDDC)

- **V-Netzwerk = Hochverfügbarkeit, Redundanz und strikte Mandantentrennung der Netztopologie.**
- **V-Storage = heterogene Speichervirtualisierung und synchrone Spiegelung aller Daten für Kapazitätsoptimierung und Business-Continuity.**
- **V-Server = schnelle Serverprovisionierung und erhöhte Verfügbarkeit auf Plattformebene.**
- **V-Security = kontextdefinierte Fehler- Ressourcen- und Sicherheitsisolation.**
- **V-Client = Bereitstellung von Desktop as a Service.**
- **Big Data Management = Realtime Data Analytics designed für Smart Energy Netzwerke und Netzsteuerung.**

4 LEISTUNGSBESCHREIBUNG IM DETAIL

4.1 DIENSTE

- **Smart Meter Zertifikate** für die WAN-Kommunikation mit Smart Meter Gateways im Sinne der TR-03109. Externe Marktteilnehmer (EMT), Gateway Administratoren (GWA) und Gateway Hersteller (GWH) können Zertifikate für sich und ihre SMGW's (SMGW) im eigenen Verantwortungsbereich über eine BSI-konforme Schnittstelle (WSDL) beziehen – inklusive LDAP Verzeichnis und Sperrlistenverteilerpunkt.
- **Zertifikatsmanagement und Schnittstelle für Gateway Administratoren** aus ISO/IEC 27001 auf Basis von BSI Grundschutz und TR-03145 zertifiziertem Cloud Dienst (in Kürze verfügbar). Der Dienst bietet alle notwendigen Verwaltungsfunktionen für Zertifikate die im Rahmen, der Gateway Administration erforderlich sind inklusive dem Zertifikatsverzeichnis des Administrators.
- **Zertifikatsmanagement und Schnittstelle für Gateway Hersteller** aus ISO/IEC 27001 auf Basis von BSI Grundschutz und TR-03145 zertifiziertem Cloud Dienst. Der Dienst bietet alle notwendigen Verwaltungsfunktionen für Zertifikate, die im Rahmen der Vorpersonalisierung von Gateways beim Hersteller anfallen.

4.2 ZERTIFIKATE

Externe Marktteilnehmer, SMGW-Hersteller und Gateway Administratoren können Smart Meter Zertifikate und Kommunikationszertifikate im Sinne der Technischen Richtlinie TR-03109 aus der SEN-PKI Sub-CA (Smart Energy Cloud Sub-CA) des VVS-Trustcenters beziehen.

Die SEN-PKI Sub-CA der VVS stellt hierfür einen nach BSI definierten Web Service zur Verfügung (WSDL Schnittstelle).

Die Authentifizierung am Web Service der SEN-PKI Sub-CA erfolgt über TLS mit beidseitigen Kommunikationszertifikaten.

Die Erstbeantragung von Zertifikaten über die Registration Authority, kurz RA des VVS-Trustcenters, erfolgt über einen anderen Weg, z. B. S/MIME – hierzu werden weitere Details in der Zertifikatsrichtlinie (CP – Certification Policy) der SEN-PKI Sub-CA definiert.

4.3 ZERTIFIKATSVERZEICHNIS (LDAP'S)

Externe Marktteilnehmer und Gateway Administratoren die im Smart Meter Verbund registriert sind d. h. über ein gültiges Kommunikationszertifikat, im Sinne der TR-03109-4 einer vertrauten Sub-CA verfügen, dürfen die von der SEN-PKI Sub-CA des VVS-Trustcenters ausgestellten Zertifikate in einem in der SEN-PKI bereitgestellten Verzeichnis abrufen. Die Kommunikation zum Dienst erfolgt über LDAPS mit zertifikatsbasierter Clientauthentifizierung.

4.4 SPERRLISTENBEZUGSPUNKT

Die SEN-PKI Sub-CA des VVS-Trustcenters, stellt einen allgemein zugänglichen HTTP-Dienst zur Verfügung um Sperrlisten zu beziehen.

4.5 CLS ZERTIFIKATE IM HAN FÜR SCHALTWARTEN

Die SEN-PKI Sub-CA des VVS-Trustcenters, stellt auf Wunsch interne Zertifikate zur Absicherung der CLS-Devices an der HAN-Schnittstelle zur Verfügung.

4.6 ZERTIFIKATSMANAGEMENT FÜR GWA UND GWH

Die Smart Energy Cloud bietet für Gateway Administratoren und Gateway Herstellern das notwendige Zertifikatsmanagement um Gatewayadministrations- und Konfigurationsaufgaben wahrzunehmen bzw. unterstütz Gatewayhersteller bereits in der Vorpersonalisierungsphase 1. Für Gatewayhersteller bieten wir die Möglichkeit, Wirk-Zertifikate der Vorpersonalisierungsphase 2 (VP2) bereits im Herstellungsprozess aufzubringen was die Herstellung des Endproduktes in Produktionszyklen erheblich vereinfacht.

Für jeden Gateway Administrator (Client) bietet das Zertifikatsmanagement einen isolierten Kontext. In diesem Kontext werden alle SMGW-Zertifikate verwaltet, welche vom GWA installiert oder hinterlegt wurden. Die Wichtigsten, dem GWA zur Verfügung stehenden Funktionalitäten sind:

- Abruf aller im eigenen Kontext hinterlegten Zertifikate.
- Auskunft über Zuordnung von Zertifikat/Gateway.
- Fremdzertifikate im LDAP Verzeichnissen abrufen und im eigenen Kontext hinterlegen.

- Weiterleitung von Zertifikatsanfragen für administrierte Gateways an die eigenen Sub-CA und Entgegennahme der bereitgestellten Zertifikate.
- Zertifikate im Kontext importieren.
- Zertifikate im Kontext ersetzten.
- Zertifikate aus dem Kontext löschen.
- Konfiguration von Vertrauenswürdigen CA‘s (für nicht Smart Meter Zertifikate, z. B. HAN Zertifikate oder Zertifikate für CLS-Devices).
- Konfiguration der anzusprechenden Smart Meter Sub-CA.
- Konfiguration regelmäßiger Zertifikatsvalidierungen (Gültigkeitsprüfung inklusive Sperrprüfung).
- Push-Benachrichtigungsdienst für abgelaufene und gesperrte Zertifikate
- Explizites Triggern von Zertifikatsvalidierungen.
- Back-up und Restore des Kontexts (Zertifikatsbestand).
- Protokollierung aller Aktionen im eigenen Kontext und Abruf der Protokolle.
- Einrichtung einer Prüfer-Rolle (Leseberechtigung auf Protokolle und Zertifikatsbestand = Revisor).

Die vom Zertifikatsmanagement durchgeführten Zertifikatsvalidierungen erfüllen die Anforderungen der TR03109-4, ins besondere auch hinsichtlich der Aktualität der für die Sperrprüfung zugrunde liegenden Sperrlisten.

Das Zertifikatsmanagement wird als Dienst zur Verfügung gestellt. Es exponiert eine Web Service Schnittstelle mit einer WSDL-Beschreibung.

Ein GWA wird am Zertifikatsmanagement authentifiziert und identifiziert anhand eines gültigen SAML Tokens (Security Assertions Markup Language). Der SAML Token muss von einem von der SEN-PKI Sub-CA des VVS-Trustcenters vertrauten Identity Providers ausgestellt werden.

Die Kommunikation zwischen Zertifikatsmanagement und den weiteren GWA-Systemen erfolgt über einen TLS-Kanal mit beidseitiger zertifikatsbasierter Authentifizierung – hierfür werden Kommunikationszertifikate im Sinne der TR03109-4 eingesetzt.

4.7 ZERTIFIZIERUNG

Die SEN-PKI Sub-CA des VVS-Trustcenters ist eine Smart Meter Sub-CA, abgeleitet von der hoheitlichen Smart Meter Root-CA. Die SEN-PKI Sub-CA wird die Anforderungen aus der Zertifikatsrichtlinie der Smart Meter Root-CA erfüllen. Die SEN-PKI Sub-CA des VVS-Trustcenters wird außerdem eine eigene Zertifikatsrichtlinie haben. Alle Zertifikatsnehmer wie Marktteilnehmer oder

Gateway Administratoren müssen die Anforderungen aus der Zertifikatsrichtlinie der SEN-PKI Sub-CA erfüllen.

Die SEN-PKI Sub-CA des VVS-Trustcenters, das Zertifikatsverzeichnis, der Sperrlistenbeziehungspunkt und das Zertifikatsmanagement des GWA/GWH werden einer ISO 27001 Zertifizierung nach IT Grundschutz unterzogen.

5 ANSPRECHPARTNER

Ihre Ansprechpartner zu allen Fragestellungen im Zusammenhang mit dem vorliegenden Dokument sind:

Name	Dr.-Ing. Thomas Klein
Bereich	VIT – Informationstechnik PKI-Trustcenter
Funktion	Fachbereichsleiter
e-mail	t.klein@vvs-konzern.de
Telefon	+49 681 587 2017
Mobil	+49 160 369 4211
Fax	+49 681 587 2344
Name	Christian Schorr
Bereich	VIT – Projektleitung PKI-Trustcenter
Funktion	Sachgebietsleiter
e-mail	c.schorr@vvs-konzern.de
Telefon	+49 681 587 2390
Mobil	+49 171 3320011
Fax	+49 681 587 2641