Technischer Bericht

Titel des Dokuments

Bereitstellen einer Public-Key-Infrastruktur (PKI) für Magellan

im Folgenden als **Dokument** bezeichnet

Kurztitel

Magellan PKI

Vorgang

BZ-12366

externe Referenz

ePlanet@ifs-it.de

Das nachfolgende Werk ist geistiges und urheberrechtliches Eigentum der

Name und Anschrift

IFS Informationstechnik München
Trausnitzstraße 8
81671 München

im Folgenden als **IFS** bezeichnet

Die IFS behält sich ausnahmslos alle urheberrechtlichen Ansprüche vor, welche sie gemäß der geltenden Rechtslage in der Bundesrepublik Deutschland sowie aus den jeweiligen Teilen des Werkes, für die die IFS aufgrund von erfinderischer Tätigkeit natürlicherweise die Urheberschaft besitzt, ableiten kann.
Unbeeinflusst davon sind Rechte Dritter, für die die IFS, gemäß den mit diesen Dritten vereinbarten Verträgen und Überlassungen, das vorliegende Werk ggf. auch im Auftrag erstellt hat. Eine Abtretung der Urheberschaft kann daraus dennoch nicht abgeleitet werden.

Name

Felix Fischer — Autor des Dokuments

Datum

20. April 2011 — Erstellungsdatum

Datum

23. Januar 2013 — Datum der letzten Änderung

Nummer

2.0 — Version des Dokuments

IFS Informationstechnik GmbH Trausnitzstraße 8 81671 München
Telefon +49 89 450983 0 Fax +49 89 450983 10 www.ifs-it.de
Kreissparkasse München Konto 10 110 344 BLZ 702 501 50
Amtsgericht München HRB 126547 USt-IdNr: DE203067267
Geschäftsführer: Dr.-Ing. Markus A. Stulle Dipl.-Ing. Thomas Frey

Dokumentinformationen

Status der vorliegenden Version

Bezeichnung

freigegeben

Dieses Dokument unterliegt keinem systematischen Änderungsdienst.

Beteiligte und Rollen

Vorname Nachname	Rolle
Dr.-Ing. Markus A. Stulle	Produktmanager
Dr. Tim-Oliver Paaschen	Vorhabensverantwortlicher
Dimitar Menkov	Qualitätsbeauftragter
Alexander Noé	Gutachter
Bettina von Staden	Lektorin

Speicherort des Dokuments

Pfad

\\ifshome.muc.smarttrust.de\IFS\Produkte\ePlanet\03 Arbeitspakete\BZ-12366 (Bereitstellen einer Public-Key-Infrastruktur für Magellan)\06 Spezifikation\BZ-12366 Bereitstellung PKI für Magellan v2.0.doc

Inhalt

1	Einführung	4
1.1	Glossar	5
1.2	Kryptographie	7
1.3	Public-Key-Infrastruktur PKI	8
1.4	Magellan	10
1.5	ePlanet®	11
2	Szenarien und Anwendungsbeispiele	13
2.1	Akteure von ePlanet®	13
2.2	Referenzbeispiel Baumarkt	14
2.3	Szenario Registrierung und Inbetriebnahme	14
2.4	Szenario Sitzungsaufbau	18
3	Technische Aspekte der Umsetzung	21
3.1	Beschreibung der Abläufe	21
3.2	Prüfen von Zertifikaten	26
3.3	Vorgeschlagene Standards	35
4	ePlanet® Testaufbau	38
4.1	Übersicht	38
4.2	ePlanet® Hintergrundsystem	39
4.3	Verteilung von Zertifikaten	42
Verzeichnisse		44
A	Verzeichnis der Tabellen	44
B	Verzeichnis der Abbildungen	44
C	Referenzen	45

1 Einführung

Magellan definiert ein Verfahren für die sichere Durchführung von Transaktionen bei Kauf und Lieferung von Waren. Grundlage dafür ist die wechselseitige Authentifizierung mittels digitaler Zertifikate. Dazu wird eine *Public-Key-Infrastruktur (PKI)* benötigt, für die in [Magellan] jedoch bewusst wenige Vorgaben gemacht werden.

Das System *ePlanet*® ermöglicht die kostengünstige und breitflächige Versorgung von Fahrzeugen mit Ladestrom. Es verwendet das Verfahren Magellan für die Abwicklung von Angeboten und Bestellungen.

Ziel dieses Dokuments ist es, die besonderen Anforderungen von Magellan an eine PKI darzustellen und technisch zu spezifizieren. Dies erfordert jedoch an vielen Stellen den Kontext der konkreten Umsetzung des Verfahrens für ePlanet®.

In Kapitel 2 werden die Akteure von ePlanet® vorgestellt. Anhand eines praktischen Beispiels wird das Verhältnis zwischen den einzelnen Teilnehmern verdeutlicht. Anschließend werden Anwendungsfälle aus den PKI-relevanten Szenarien „Registrierung und Inbetriebnahme" sowie „Sitzungsaufbau" dargestellt und mithilfe des Referenzbeispiels erklärt.

Kapitel 3 beschreibt die technischen Anforderungen an eine PKI, die sich aus den von Magellan gestellten Auflagen ergeben. Es werden verwendete Standards sowie Erweiterungen erläutert, die für die Umsetzung gezeigter Anwendungsbeispiele relevant sind.

Der Testaufbau von ePlanet® ist das Thema von Kapitel 4. Es enthält eine Übersicht aller Komponenten und beschreibt die Rolle des ePlanet® Hintergrundsystems sowie die Verteilung von Zertifikaten.

1.1 Glossar

Tabelle 1 fasst alle wichtigen Begriffe zusammen, die für dieses Dokument relevant sind.

Begriff	Beschreibung
Anbieter	▪ erzeugt und liefert Güter (Magellan) ▪ Bei ePlanet® übernimmt der Energieversorger diese Rolle.
Anbietersystem	▪ dient der Überwachung und Steuerung von Transaktionen der Güter sowie der Verwaltung von Teilnehmern und deren Daten ▪ kann Leistungsabgabe im Szenario ePlanet® steuern
asymmetrische Verfahren	kryptographische Verfahren, die auf Schlüsselpaaren basieren
Authentifizierung	Überprüfen der erklärten Identität des Kommunikationspartners
Authentisierung	Nachweis der eigenen Identität durch geeignete Verfahren
Authentizität	Urheber bzw. Absender muss identifizierbar sein (s.a. Verbindlichkeit).
Autorisierung	Gewährung von Rechten in Abhängigkeit von der Identität
Basisstation	Begriff aus ePlanet® Sie nimmt die Rolle des Händlers ein (Magellan) und steuert den Ablauf der Transaktionen zwischen Verbraucher und Anbieter.
ePlanet®	System zur kostengünstigen und breitflächigen Versorgung von Fahrzeugen mit Ladestrom: verwendet Magellan als Vertrauensbasis
ePlanet® PKI	dient zur Registrierung von Kunden und zur Erstellung, Verlängerung und Sperrung von Zertifikaten sowie zur Personalisierung von Chipkarten
ePlanet® Steckdose	ermöglicht den leichten Zugang zu Ladestrom für Elektrofahrzeuge und wird durch die Basisstation gesteuert
Händler	▪ verkauft Güter des Anbieters an den Verbraucher ▪ vermittelt Nachrichten zwischen dem verbraucherseitigen und dem anbieterseitigen Kommunikationssystem (Magellan) ▪ Bei ePlanet® übernimmt die Basisstation diese Rolle.
Hash-Funktion	kollisionsfreie Einwegfunktion, die Nachrichten beliebiger Länge auf ein Bitmuster fester Länge abbildet

Begriff	Beschreibung
Leistungsmesser	Sensor, mit dem die elektrische Leistung gemessen werden kann, die ein Verbraucher aufnimmt
Magellan	Verfahren, das der sicheren Durchführung von Transaktionen bei Bestellung und Lieferung von Waren als Vertrauensbasis dient
Nonce	„Number used once“: ▪ zufällig generierter Wert, um Datensätze zu individualisieren ▪ wird z.B. von OCSP als Option genutzt
OCSP	„Online Certificate Status Protocol“ [OCSP]: Protokoll zur Prüfung der Gültigkeit von *Zertifikaten* durch einen *OCSP Responder*
OCSP Responder	▪ Bestandteil einer PKI ▪ Prüfstelle, die OCSP-Anfragen zur Gültigkeitsprüfung von Zertifikaten beantwortet
PLC	Power Line Communication: erforderliche Netzwerktechnologie für ePlanet®
Prüfer	▪ erstellt und prüft Zertifikate im Auftrag des Anbieters (Magellan) ▪ zu realisieren durch eine PKI mit OCSP Responder
Prüfstelle	Teil der ePlanet® PKI: ▪ prüft Zertifikate auf Widerruf ▪ wird auch als Validierungsstelle bezeichnet
Public-Key-Infrastruktur (PKI)	System zum Erstellen, Verteilen und Prüfen von Zertifikaten
Regelleistung	Verfügbarkeit von Regelleistung gewährleistet die Versorgung der Stromkunden mit exakt der benötigten Menge elektrischer Leistung bei unvorhergesehenen Ereignissen im Stromnetz.
Registrierung	Identitätsnachweis mit glaubwürdigen Mitteln bei der Beantragung eines Zertifikats
Registrierungsstelle	registriert neue Teilnehmer von ePlanet® als Verbraucher, Händler, Anbieter oder Prüfer (Magellan).
Signatur	kryptographisches Verfahren, mit dem Authentizität und Integrität von Daten gewährleistet werden
symmetrische Verfahren	kryptographische Verfahren, die auf gemeinsamen Schlüsseln basieren
Verbindlichkeit	Eindeutigkeit der Urheberschaft (s.a. Authentizität)

Begriff	Beschreibung
Verbraucher	▪ Konsument der Güter (Magellan) ▪ bei ePlanet® die Verbraucherstation ▪ verfügt zur Abrechnung über ein Konto im Hintergrundsystem
Verbraucherstation	wird von einem Verbraucher zur Nutzung von ePlanet® benötigt
Verschlüsselung	kryptographisches Verfahren, mit dem die Vertraulichkeit von Daten gewährleistet wird
Vertrauensbasis	Magellan wird als Vertrauensbasis bezeichnet, da das Verfahren die Grundlagen für die sichere Durchführung von Bestellung und Lieferung von Waren beschreibt.
Vertraulichkeit	Schutz von Daten gegen Ausspähen
Verzögerte Bereitstellung	Einzelne Bestell- und Liefervorgänge können durch den Anbieter abgelehnt oder verzögert werden, um auf mögliche Beschränkungen von Transportwegen und Kapazitäten reagieren zu können.
Wurzelzertifikat	In einer PKI mit hierarchischem Vertrauensmodell lassen sich die Zertifizierungsketten aller Zertifikate auf ein gemeinsames Wurzelzertifikat zurückführen.
Zertifikat	strukturierte Daten, die einen öffentlichen Schlüssel und Angaben zu dessen Eigentümer zusammenfassen und von einem Dritten signiert wurden
Zertifikatsperrliste	Liste von Zertifikaten, die zurückgezogen wurden
Zertifizierungsstelle	▪ stellt registrierten Teilnehmern von ePlanet® Zertifikate aus ▪ ist ein Teil der PKI und wird auch Prüfer (Magellan) genannt

Tabelle 1: Glossar wichtiger Begriffe

1.2 Kryptographie

Die *Kryptographie* ([Bless], [JB]) befasst sich mit Informationssystemen, die robust gegen unbefugtes Lesen und Verändern sind. Für Magellan sind die wichtigsten Ziele *Authentizität* und *Integrität*, die mit *asymmetrischen Verfahren* erreicht werden können.

Asymmetrische Verfahren verwenden Schlüsselpaare, bestehend aus einem öffentlichen und einem privaten Schlüssel. Jeder Kommunikationsteilnehmer besitzt sein eigenes Schlüsselpaar. Der private Schlüssel ist geheim. Er wird zum Beispiel zum Erstellen

von digitalen Signaturen verwendet. Der öffentliche Schlüssel ist frei zugänglich und erlaubt zum Beispiel das Prüfen einer Signatur, die mit dem entsprechenden privaten Schlüssel des Schlüsselpaares erzeugt wurde. Mittels digitaler Signaturen können Authentizität und Integrität von Dokumenten geprüft werden.

Der öffentliche Schlüssel kann mit Daten, die die Identifizierung des Besitzers erlauben, in einem Dokument zusammengefasst werden. Wird ein solches Dokument von einem Dritten digital signiert, spricht man von einem *Zertifikat*.

1.3 Public-Key-Infrastruktur PKI

Eine *Public-Key-Infrastruktur (PKI)* ist ein Netzwerk aus Rechnern und Programmen, mit denen Zertifikate erzeugt, verwaltet, geprüft, widerrufen und erneuert werden können.

Tabelle 2 zeigt alle Elemente einer PKI, die für dieses Dokument relevant sind:

Begriff	Beschreibung
Benutzer (Subject)	Teilnehmer der Kommunikation, der ein Zertifikat benötigt oder andere Zertifikate prüfen will
Registrierungsstelle (Registration Authority/RA)	Rolle der PKI: Wichtigste Aufgabe ist die Prüfung der Identität eines neuen Teilnehmers, bevor ein Zertifikat für ihn erstellt wird.
Zertifizierungsstelle (Certification Authority/CA)	Rolle der PKI: ▪ stellt Zertifikate auf Anforderung der RA aus ▪ widerruft Zertifikate ▪ pflegt die Datenbasis zu ausgestellten Zertifikaten
Prüfstelle (Validation Authority/VA)	Rolle der PKI: ▪ verarbeitet Prüfanfragen für Zertifikate auf Grundlage der Datenbasis der CA

Tabelle 2: Bestandteile einer PKI

Im Folgenden werden die Rollen der Registrierungsstelle und der Zertifizierungsstelle nicht weiter unterschieden, da sie in der Regel von der gleichen Institution eingenommen werden.

Die Zertifizierungsstelle ist das Herz einer PKI. Ihre primäre Aufgabe ist es, Benutzern Zertifikate auszustellen. Ein Zertifikat beinhaltet unter anderem:

- Namen des Benutzers
- öffentlichen Schlüssel des Benutzers
- Beginn und Ende der Gültigkeit
- Signatur der Daten durch die Zertifizierungsstelle

1.3.1 Hierarchisches Vertrauensmodell

Globale PKI verlangen nach skalierbaren Strukturen, was komplexe Vertrauensmodelle erfordert. Tatsächlich gibt es nicht nur eine einzelne Zertifizierungsstelle der jeder Benutzer direkt vertrauen kann. In einem hierarchischen Vertrauensmodell lassen sich alle Zertifikate über mehrere Schritte auf ein gemeinsames Stamm- oder Wurzelzertifikat zurückführen. Dieses Vertrauensmodell wird auch als *Top Down* bezeichnet.

Die Zertifikate vom Stammzertifikat bis zum zu prüfenden Zertifikat werden als Zertifikatskette bezeichnet.

1.3.2 Zertifikatsprüfung

Will ein Benutzer das Zertifikat eines anderen Benutzers prüfen, muss er zunächst die Signatur der Zertifizierungsstelle validieren. Abstrakt ausgedrückt muss der Benutzer der Zertifizierungsstelle direkt oder indirekt vertrauen. Er benötigt dafür den öffentlichen Schlüssel der CA oder muss eine Verbindung von seiner vertrauten CA herstellen können.

Die Prüfung eines Zertifikats beinhaltet außerdem die Prüfung des Widerrufstatus. Es gibt zahlreiche Gründe, warum ein Zertifikat vor Ablauf der Gültigkeitsdauer widerrufen wird, zum Beispiel Verlust oder Kompromittierung des privaten Schlüssels zum Zertifikat. Für die Prüfung des Widerrufstatus wird im Rahmen dieses Dokuments [OCSP] verwendet.

Ein *OCSP Responder* stellt die Validierungsstelle der PKI dar. Die Datenbasis über zurückgezogene Zertifikate kann zum Beispiel aus einer Zertifikatssperrliste (Certificate Revocation List/CRL) oder direkt von der Datenbank der Zertifizierungsstelle bezogen werden [Bless].

Abbildung 1 zeigt schematisch die Interaktion zwischen einem Benutzer, der ein Zertifikat prüfen lassen will, und dem OCSP Responder:

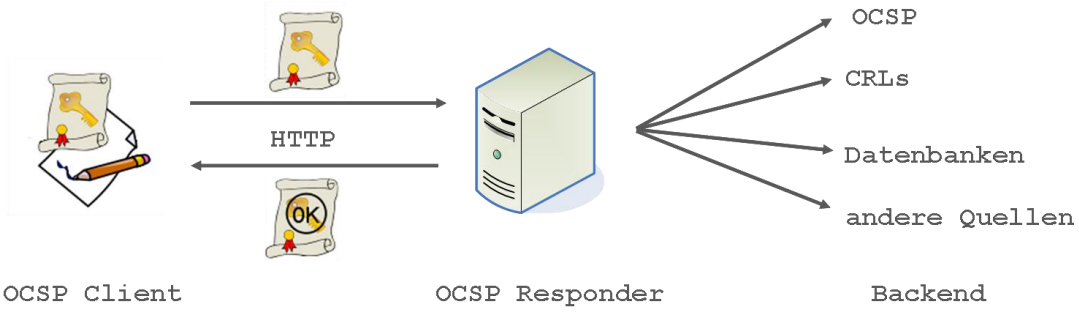

Abbildung 1: OCSP – Online Certificate Status Protocol

Um sich ausweisen zu können, besitzt der OCSP Responder ebenfalls ein Zertifikat, das von der Zertifizierungsstelle ausgestellt wurde und ihn zum Prüfen von Zertifikaten befugt.

1.4 Magellan

Magellan bezeichnet ein Verfahren zur Authentisierung von Transaktionen zwischen Anbietern, Händlern und Verbrauchern mittels Zertifikaten [Magellan]. Es stellt die Vertrauensbasis bei der Abwicklung von Bestellung und Verkauf von Waren dar.

Magellan definiert die folgenden Rollen für die Beteiligten:

- Ein *Verbraucher* (engl. *Consumer*) konsumiert Güter. Er verfügt über ein Konto im System des Anbieters, aber nicht über eine ständige Verbindung zu dessen System.
- Ein *Händler* (engl. *Vendor*) vertreibt die Güter, die vom Verbraucher konsumiert werden. Er vermittelt auch Nachrichten zwischen Verbraucher und Anbieter. Ein Händler ist ständig mit dem Anbietersystem verbunden.
- Ein *Anbieter* (engl. *Supplier*) erzeugt und liefert die Güter, die vom Händler vertrieben und vom Verbraucher konsumiert werden. Er betreibt das Hintergrundsystem, in dem Verbraucher und Anbieter Konten besitzen, und gibt an diese Karten mit den erforderlichen Zertifikaten aus.
- Ein *Prüfer* (engl. *Checker*) erfüllt alle Aufgaben einer PKI.

In Abbildung 2 werden die beteiligten Systeme Magellans und deren Beziehung zueinander gezeigt:

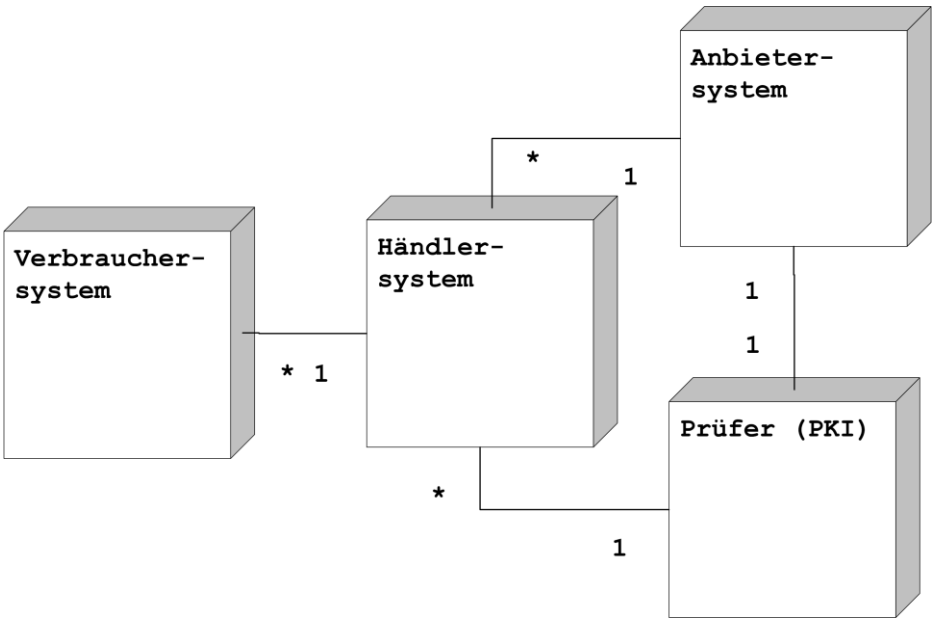

Abbildung 2: Beteiligte Systeme Magellans (aus [Magellan], S.12)

Der höchste Schutzbedarf besteht für Authentizität, Verbindlichkeit und Integrität von Bestell- und Lieferdaten. Die Vertraulichkeit dieser Daten wird hingegen als nicht relevant betrachtet. Dementsprechend sollen diese Daten signiert, aber nicht verschlüsselt werden.

Datensätze, mit denen der Anbieter das Verhalten der Händlersysteme steuert, müssen signiert werden, um Störungen des Betriebs durch Unbefugte zu vermeiden.

1.5 ePlanet®

[ePlanet®] ist ein System zur kostengünstigen und breitflächigen Versorgung von Fahrzeugen mit Ladestrom. Es nutzt Magellan für die Abwicklung von Angeboten und Bestellungen. Des Weiteren sieht ePlanet® eine Möglichkeit für den Energieversorger vor, die Abgabe von elektrischer Energie über ein Hintergrundsystem zu steuern.

Eine ePlanet® Basisstation stellt mehrere ePlanet® Steckdosen (230 V) bereit. Elektrofahrzeuge, die mit einer ePlanet® Verbraucherstation ausgestattet sind, können dort aufgeladen werden. Die Kommunikation zwischen Basis- und Verbraucherstation erfolgt mittels Power Line Communication (PLC) über das

Ladestromkabel. Das Hintergrundsystem wird für den Energieversorger betrieben.

Jede Komponente bei ePlanet® hat eine von Magellan spezifizierte Rolle:

- ePlanet® Verbraucherstation (Verbraucher)
- ePlanet® Basisstation (Händler)
- ePlanet® Anbietersystem (Anbieter)
- ePlanet® PKI (Prüfer)

Die einzelnen Akteure werden genauer in Kapitel 2.1 beschrieben.

2 Szenarien und Anwendungsbeispiele

Die Anwendungsfälle von ePlanet®, die eine PKI betreffen, lassen sich in folgende Szenarien unterteilen:

- Das Szenario *Registrierung und Inbetriebnahme* beleuchtet Vorgänge der Registrierung von Verbraucher, Händler und Prüfstellen.
- Das Szenario *Verbindungsaufnahme* beinhaltet alle für die PKI relevanten Aspekte während der gegenseitigen Authentifizierung zwischen Verbraucher und Händler bzw. zwischen Händler und Anbieter.

Das Szenario *Bestellung und Lieferung* ist bereits in [Magellan] (S. 15 ff.) ausführlich beschrieben und wird an dieser Stelle nicht näher betrachtet.

2.1 Akteure von ePlanet®

An dieser Stelle werden Akteure der ePlanet® PKI vorgestellt. Dies sind Benutzer, die direkt mit Komponenten der PKI in Berührung kommen oder selbst ein Teil von ihr sind.

- Die *ePlanet® Basisstation* wird von einem Händler betrieben und bietet dem Verbraucher Ladestrom an. Sie nutzt Zertifikate, um sich gegenüber Verbraucher und Anbieter auszuweisen.
- Die *ePlanet® Verbraucherstation* ist in einem Fahrzeug integriert und dient der Authentisierung des Verbrauchers und der Abrechnung der Dienstleistung. Sie nutzt Zertifikate, um sich gegenüber Händlern auszuweisen.
- Das *ePlanet® Anbietersystem* autorisiert Verbrauchersitzungen über den Händler. Es nutzt Zertifikate, um sich Händlern gegenüber auszuweisen. Es stellt seinen Händlern ein Web-Portal zur Verfügung.
- Die *ePlanet® Zertifizierungsstelle* registriert Benutzer und stellt Zertifikate aus. Sie besitzt als einzige Komponente ein selbst ausgestelltes Zertifikat, dem alle Benutzer vertrauen müssen. Die Zertifizierungsstelle ist eine zentrale Komponente der PKI (vgl. Tabelle 2).

- Die *ePlanet® Prüfstelle* gibt den Widerrufstatus von Zertifikaten zurück. Sie nutzt selbst ein Zertifikat, um Antworten signieren zu können. Die Prüfstelle ist ein Teil der PKI.

2.2 Referenzbeispiel Baumarkt

Um die Rolle der PKI für ePlanet® zu veranschaulichen, wird ein Referenzbeispiel eingeführt. Jeder Anwendungsfall wird zunächst formal spezifiziert und anschließend anhand des Beispiels erklärt. Der Bezug zum Beispiel wird mit dem Lesezeichen „◈ Referenzbeispiel" eingeleitet.

Dies sind die Teilnehmer des Beispiels mit einem Verweis auf deren Rolle:

- *Baumarkt OGI*: Er nimmt die Rolle des Händlers ein. Für seinen Kundenparkplatz möchte er ePlanet® Steckdosen anbieten. Er betreibt eine ePlanet® Basisstation.
- *Herr Mustermann*: Er möchte mit seinem Elektrofahrzeug Strom überall laden, unter anderem auch bei seinem Lieblingsbaumarkt OGI. Daher lässt er sein Fahrzeug mit einer ePlanet® Verbraucherstation aufrüsten.
- *RWM Strom*: Dies ist im Referenzbeispiel der Energieversorger. Er lässt für seinen Einzugsbereich ein ePlanet® Anbietersystem betreiben.
- *eKom*: eKom betreibt die Hintergrundsysteme für ePlanet®. Dazu gehören Komponenten der PKI, wie Zertifizierungsstelle und Prüfstelle. Die Firma trägt die Registrierung, das Rechnungswesen und das Anbietersystem für RWM.

Herr Mustermann kann nun sein Elektrofahrzeug auf dem Kundenparkplatz von Baumarkt OGI laden, sofern der Strom vonseiten des Anbietersystems von RWM freigegeben ist. Ihm wird die verbrauchte Menge elektrischer Leistung von eKom berechnet. Der Baumarkt bekommt für diesen Betrag einen Bonus gutgeschrieben.

2.3 Szenario Registrierung und Inbetriebnahme

Die Registrierung von Benutzern stellt für eine PKI einen wichtigen Arbeitsschritt dar. Dabei ist vor allem die Identität des Teilnehmers zu prüfen. Das Zertifikat, das für den Teilnehmer ausgestellt wird, enthält Informationen, die eine eindeutige Zuordnung zu der geprüften Identität erlauben.

Auf die Registrierung kann die Freischaltung bzw. Inbetriebnahme erfolgen. Die genauen Abläufe hängen von der Rolle des Benutzers ab.

2.3.1 Anwendungsfall Registrierung ePlanet® Prüfstelle

Beschreibung	Die ePlanet® Zertifizierungsstelle stellt einer neuen ePlanet® Prüfstelle ein Zertifikat aus.
Vorbedingungen	Die neue Prüfstelle wurde akzeptiert.
Nachbedingungen	Das Zertifikat erlaubt das Prüfen von Zertifikaten und erreicht die Prüfstelle auf sicherem Weg in Form einer Chipkarte und PIN.
Hinweis	Das ausgestellte Zertifikat dient nur zur Verbindungsaufnahme mit der Zertifizierungsstelle.

Tabelle 3: Anwendungsfall - Registrierung ePlanet® Prüfstelle

◈ Referenzbeispiel: Eine neue Prüfstelle zu registrieren, bedeutet für die Firma eKom einen internen Wartungsvorgang. Es handelt sich dabei um einen Server, der für die Prüfung von Zertifikaten hinzukommt.

2.3.2 Anwendungsfall Inbetriebnahme ePlanet® Prüfstelle

Beschreibung	Die Prüfstelle wird in Betrieb genommen.
Vorbedingungen	Der Anwendungsfall „Registrierung ePlanet® Prüfstelle" ist erfolgreich verlaufen.
Nachbedingungen	Die Prüfstelle ist in der Lage, Zertifikate auf Gültigkeit zu prüfen.
Hinweis	Die Prüfstelle weist sich mittels des Zertifikats auf der Chipkarte gegenüber der Zertifizierungsstelle aus und erhält daraufhin das Prüferzertifikat für den Betrieb.

Tabelle 4: Anwendungsfall – Inbetriebnahme ePlanet® Prüfstelle

◈ Referenzbeispiel: Das Personal von eKom nimmt den neuen Server in Betrieb.

2.3.3 Anwendungsfall Zertifikat der ePlanet® Prüfstelle erneuern

Beschreibung	Die Zertifizierungsstelle verlängert das Zertifikat der Prüfstelle.
Vorbedingungen	Das Zertifikat der Prüfstelle ist kurz vor Ablauf der Gültigkeit.
Nachbedingungen	Die Zertifizierungsstelle hat das Zertifikat der Prüfstelle verlängert.
Hinweis	In diesem Schritt weist sich die Prüfstelle mit ihren Prüfer-Zertifikat gegenüber der Zertifizierungsstelle aus. Das Zertifikat auf der Chipkarte wird nicht benötigt.

Tabelle 5: Anwendungsfall – Erneuerung Zertifikat Prüfstelle

◈ Referenzbeispiel: Für eKom ist die Erneuerung eines Prüferzertifikats unbedenklich, da keine geheimen Informationen ausgetauscht werden. Die Prüfstelle muss sich mit ihrem aktuellen Zertifikat ausweisen.

2.3.4 Registrierung Händler

Beschreibung	Die Zertifizierungsstelle stellt dem Händler ein Zertifikat für seine ePlanet® Basisstation aus.
Vorbedingungen	Der Händler hat einen Händlervertrag mit ePlanet® abgeschlossen.
Nachbedingungen	Der Händler hat eine ePlanet® Chipkarte mit Händlerzertifikat erhalten; er ist in der Lage, eine ePlanet® Basisstation in Betrieb zu nehmen.
Hinweis	Die Verlängerung des Vertrags erfordert denselben Vorgang.

Tabelle 6: Anwendungsfall – Registrierung Händler

◈ Referenzbeispiel: Baumarkt OGI möchte für seine Kunden ePlanet® anbieten und schließt einen Vertrag mit ePlanet® ab. eKom erzeugt für den Baumarkt ein Zertifikat, das auf einer Chipkarte gespeichert ist. Der Zugriff auf die Chipkarte des Händlers ist nicht mit einer PIN abgesichert, da aus Kostengründen auf die Bereitstellung der erforderlichen Hardware in der ePlanet® Basisstation verzichtet wurde. Es wird angenommen, dass sich die Basisstation an einem Ort befindet, der nicht öffentlich zugänglich ist.

2.3.5 Inbetriebnahme ePlanet® Basisstation

Beschreibung	Die ePlanet® Basisstation des registrierten Händlers wird freigeschaltet.
Vorbedingungen	Der Anwendungsfall „Registrierung Händler" wurde erfolgreich durchgeführt.
Nachbedingungen	Zwischen Chipkarte und Basisstation besteht eine enge Bindung. Durch die Freischaltung weiß das Anbietersystem, an welchem Ort die Basisstation eingesetzt wird. Bei starker Netzauslastung kann die Abgabe von Strom verzögert werden.
Hinweis	Die Freischaltung erfolgt passwortgeschützt über ein Web-Portal des Anbietersystems. Dabei wird eine Kombination aus Kartennummer und Seriennummer der Basisstation übermittelt.

Tabelle 7: Anwendungsfall – Inbetriebnahme Basisstation

◈ Referenzbeispiel: Die Chipkarte wurde mit der Post an den Baumarkt OGI gesendet. Die ePlanet® Basisstation wurde geliefert und von einem Elektriker installiert. Die Freischaltung stellt sicher, dass die gelieferte Basisstation nur mit der Chipkarte von Baumarkt OGI funktioniert.

2.3.6 Servicefall ePlanet® Basisstation

Beschreibung	Der Händler lässt eine beschädigte ePlanet® Basisstation ersetzen und freischalten.
Vorbedingungen	Die defekte ePlanet® Basisstation wurde physikalisch durch eine neue ausgetauscht.
Nachbedingungen	Die neue ePlanet® Basisstation kann ePlanet® Verbraucherstationen mit Strom beliefern.
Hinweis	Die ursprüngliche Kombination aus Kartennummer und Seriennummer wird bei dieser Freischaltung gesperrt.

Tabelle 8: Anwendungsfall – Servicefall Basisstation

◈ Referenzbeispiel: Die ePlanet® Basisstation wurde durch einen Unfall auf dem Kundenparkpatz von OGI beschädigt und wird ausgetauscht. Der Händler kann die neue Basisstation freischalten und danach mit der ursprünglichen, noch intakten Chipkarte verwenden.

2.3.7 Registrierung Verbraucher

Beschreibung	Die ePlanet® Zertifizierungsstelle stellt einem Verbraucher ein Zertifikat für seine ePlanet® Verbraucherstation aus.
Vorbedingungen	Ein Vertrag zwischen Verbraucher und ePlanet® wurde abgeschlossen.
Nachbedingungen	Das Zertifikat des Verbrauchers wird auf einer Chipkarte ausgeliefert. Der Kunde von ePlanet® ist nicht an bestimmte Händler oder Energieversorger gebunden.

Tabelle 9: Anwendungsfall – Registrierung Verbraucher

◈ Referenzbeispiel: Herr Mustermann möchte mit seinem Elektrofahrzeug ePlanet® nutzen und registriert sich bei eKom über einen Vertrag.

2.3.8 Inbetriebnahme ePlanet® Verbraucherstation

Beschreibung	Die ePlanet® Verbraucherstation wird im Fahrzeug des Verbrauchers installiert.
Vorbedingungen	Der Anwendungsfall „Registrierung Verbraucher" wurde erfolgreich durchgeführt.
Nachbedingungen	Der Verbraucher kann ohne Weiteres an jeder ePlanet® Steckdose sein Fahrzeug aufladen.
Hinweis	Bei Verlängerung des Vertrags muss lediglich die Chipkarte ausgetauscht werden.

Tabelle 10: Anwendungsfall – Inbetriebnahme Verbraucherstation

◈ Referenzbeispiel: Herr Mustermann kann mit seinem gerüsteten Fahrzeug beim Baumarkt OGI Strom tanken. Da eKom für ihn abrechnet, kann er auch an seiner Arbeitsstelle ePlanet® nutzen. Dort bezieht die ePlanet® Basisstation von einem anderen Energieversorger Strom.

2.4 Szenario Sitzungsaufbau

Hinsichtlich der Sicherung der Authentizität zwischen Kommunikationsteilnehmern von ePlanet® ist der Aufbau einer Sitzung ein wichtiger Zeitpunkt. Die Identität muss von beiden Seiten mithilfe von Zertifikaten überprüft werden. Die folgenden Anwendungsfälle beziehen sich auf den Sitzungsaufbau zwischen Verbraucher und Händler sowie zwischen Händler und Anbieter.

2.4.1 Gegenseitige Authentifizierung: Verbraucher und Händler

Beschreibung	Die ePlanet® Basisstation authentifiziert sich als gültiger Händler.
Vorbedingungen	Die Verbraucherstation hat Verbindung mit der Basisstation aufgenommen. Die Verbindung ist von Anbietersystem autorisiert.
Nachbedingungen	Die Verbraucherstation hat das Zertifikat des Händlers akzeptiert. Eine Prüfstelle hat den Status des Zertifikats bestätigt.

Tabelle 11: Anwendungsfall – Verbraucher prüft Händler

Beschreibung	Die ePlanet® Verbraucherstation authentifiziert sich als gültiger Verbraucher.
Vorbedingungen	Der Anwendungsfall „Verbraucher prüft Zertifikat des Händlers" wurde erfolgreich durchgeführt.
Nachbedingungen	Die Basisstation hat das Zertifikat des Verbrauchers akzeptiert. Eine Prüfstelle hat den Status des Zertifikats bestätigt.

Tabelle 12: Anwendungsfall – Händler prüft Verbraucher

◈ Referenzbeispiel: Herr Mustermann parkt auf dem Kundenparkplatz von Baumarkt OGI. Er steckt das Ladekabel seines Fahrzeugs in die ePlanet® Steckdose und kann anschließend einkaufen gehen. Bevor der Ladevorgang beginnen kann, startet im Hintergrund die gegenseitige Authentifizierung zwischen Verbraucherstation und Basisstation.

2.4.2 Gegenseitige Authentifizierung: Händler und Anbieter

Beschreibung	Die ePlanet® Basisstation authentifiziert sich als gültiger Händler.
Vorbedingungen	Die ePlanet® Basisstation hat die Verbindung zum ePlanet® Anbietersystem aufgebaut.
Nachbedingungen	Das Anbietersystem hat das Zertifikat des Händlers akzeptiert. Eine Prüfstelle hat den Status des Zertifikats bestätigt.
Hinweis	Die Verbindung zwischen beiden Systemen soll dauerhaft bestehen und die Prüfung der Zertifikate regelmäßig wiederholt werden.

Tabelle 13: Anwendungsfall – Anbieter prüft Händler

Beschreibung	Das ePlanet® Anbietersystem authentifiziert sich als gültiges Anbietersystem.
Vorbedingungen	Der Anwendungsfall „Anbieter prüft Zertifikat des Händlers" ist erfolgreich verlaufen.
Nachbedingungen	Die Basisstation des Händlers hat das Zertifikat des Anbieters akzeptiert. Eine Prüfstelle hat den Status des Zertifikats bestätigt.
Hinweis	Die Verbindung zwischen beiden Systemen soll dauerhaft bestehen und die Prüfung der Zertifikate regelmäßig wiederholt werden.

Tabelle 14: Anwendungsfall – Händler prüft Anbieter

◈ Referenzbeispiel: Damit das Anbietersystem von RWM die Stromlieferung für Herrn Mustermann autorisieren kann, muss es eine Verbindung mit der entsprechenden Basisstation des Baumarkts OGI aufnehmen. Mit dieser Verbindung wird sichergestellt, dass die ausgetauschten Nachrichten auch tatsächlich von OGI bzw. RWM stammen und dass niemand sie verändert hat.

3 Technische Aspekte der Umsetzung

3.1 Beschreibung der Abläufe

Die Vorgänge zwischen den Kommunikationsteilnehmern von ePlanet® geben die grundlegenden Konzepte für die Umsetzung der PKI vor. Dazu gehören im Wesentlichen der Inhalt und die Abfolge der ausgetauschten Nachrichten. In den Kapiteln 2.3 und 2.4 wurden bereits Anwendungsfälle beschrieben. Nun werden die Abläufe durch Sequenz- und Flussdiagramme konkretisiert, wobei auch technische Aspekte mit einfließen.

In den folgenden Kapiteln werden die Anwendungsfälle für ePlanet® erneut aufgegriffen. Die Abläufe werden aus der Sicht einer Komponente beschrieben.

3.1.1 ePlanet® Prüfstelle

Die Prüfstelle für ePlanet® soll mithilfe eines OCSP-Servers [OCSP] umgesetzt werden (vgl. Anwendungsfall 2.3.2, Tabelle 4, Seite 15).

Die Nachrichten eines OCSP-Servers lassen den Empfänger auf widerrufene Zertifikate reagieren. Authentizität und Identität haben dadurch einen hohen Schutzbedarf. Deshalb benötigt die Prüfstelle ein eigenes Zertifikat, mit dem sie sich bei jeder Anfrage ausweisen kann.

Abbildung 3 zeigt, wie ein OCSP-Server in Betrieb genommen wird.

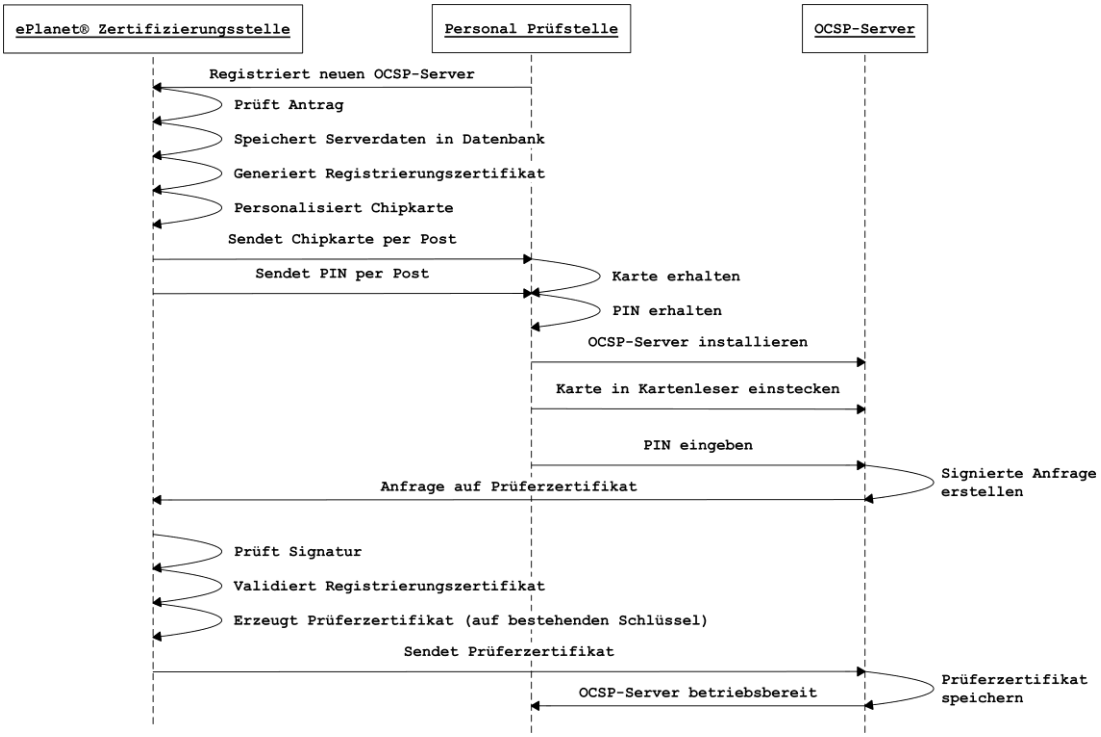

Abbildung 3: Inbetriebnahme eines OCSP-Servers

Das Prüferzertifikat des OCSP-Servers hat eine sehr kurze Gültigkeitsdauer. Die ePlanet® Zertifizierungsstelle muss es regelmäßig erneuern (Abbildung 4).

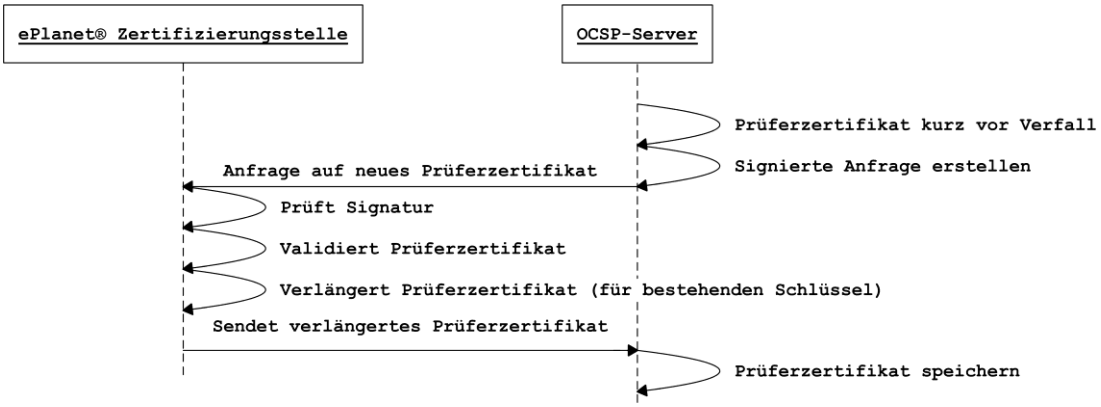

Abbildung 4: Aktualisierung des Prüferzertifikats

3.1.2 ePlanet® Basisstation

Als Bindeglied zwischen Endkunden und Energieversorgern ist der sichere Betrieb der ePlanet® Basisstation wichtig. Ein Energieversorger muss die Abgabe elektrischer Energie möglichst feingranular steuern können, um Überlastungen von Teilen des Stromnetzes zu vermeiden. Dazu muss dem Energieversorger der genaue Standort jeder ePlanet® Basisstation bekannt sein.

Um dies zu erreichen, wird eine Freischaltung der Basisstation über ein Web-Portal des Anbieters vorgesehen. Dabei wird die Verbindung der Daten von Händler, Chipkarte und Basisstation hergestellt. Natürlich setzt dies voraus, dass der Händler seine Chipkarte und ein geheimes Passwort erhalten hat. So kann beim Anbieter die folgende Zuordnung (Abbildung 5) hinterlegt werden:

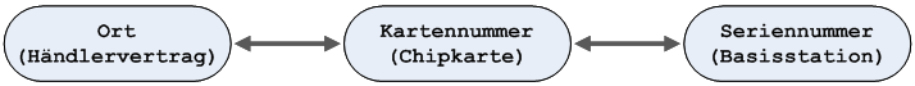

Abbildung 5: Beim Anbieter hinterlegte Zuordnung

Abbildung 6 zeigt die Registrierung und Inbetriebnahme einer ePlanet® Basisstation (vgl. Tabelle 6 und Tabelle 7, Seite 16 f.).

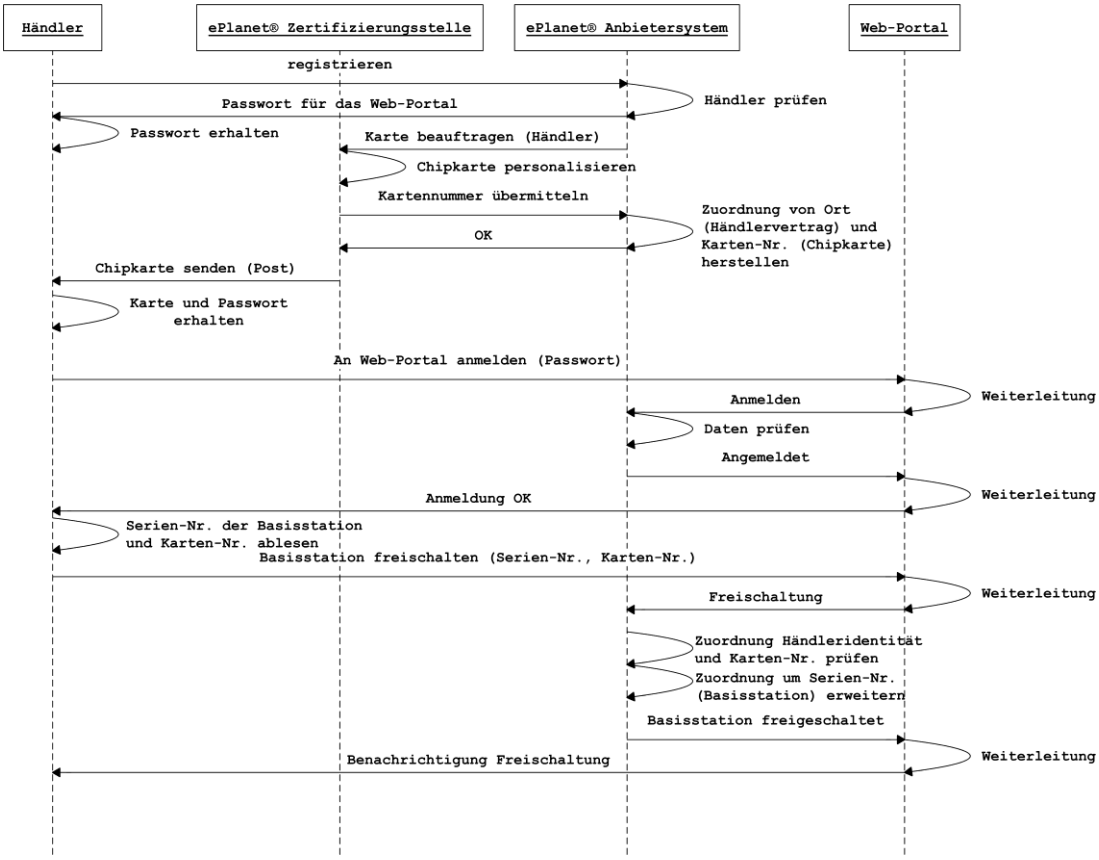

Abbildung 6: Inbetriebnahme einer ePlanet® Basisstation

Falls eine Basisstation ausgetauscht werden muss, kann die Zuordnung zwischen Kartennummer und der neuen Basisstation hergestellt werden. Dieser Vorgang läuft ebenfalls über ein Web-Portal, wie in Abbildung 7 zu sehen ist.

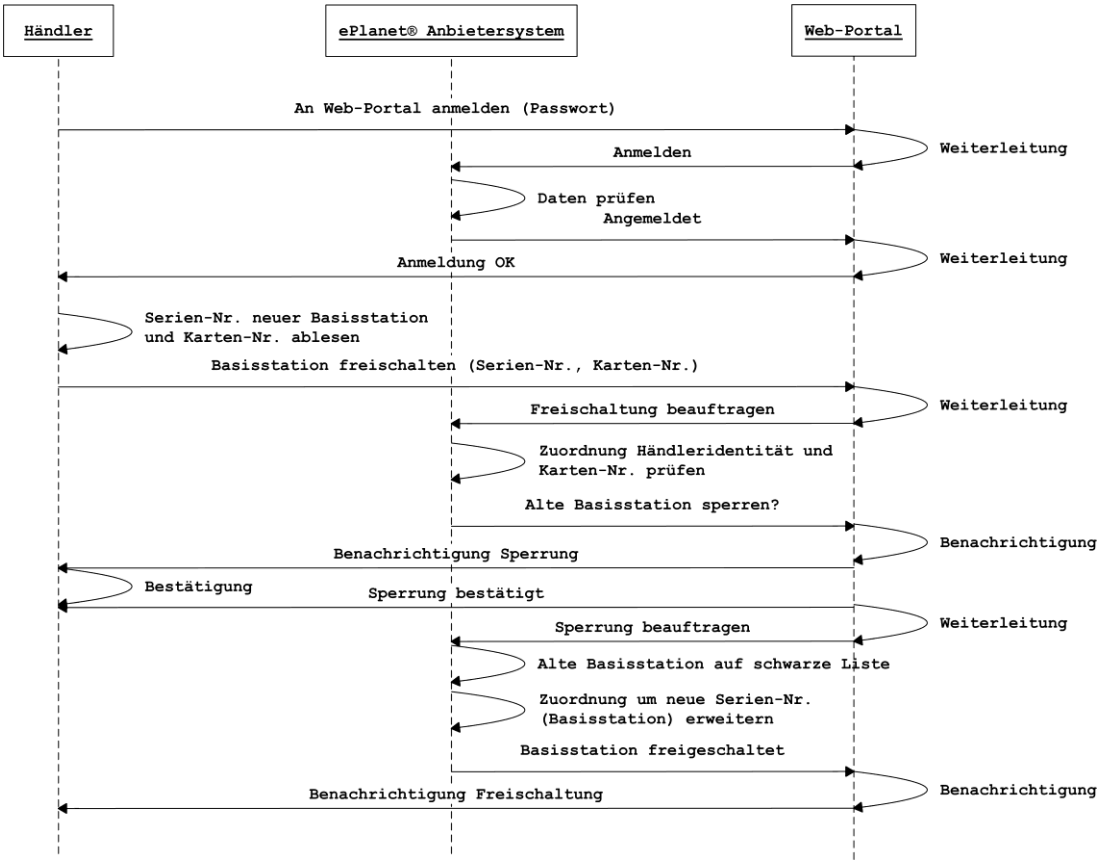

Abbildung 7: Servicefall ePlanet® Basisstation

Lediglich die Zuordnung von Kartennummer und Seriennummer zu hinterlegen, ist jedoch nicht ausreichend. Die Zuordnung muss während des gesamten Zeitraumes der Kommunikation zwischen Basisstation und Anbietersystem bestehen bleiben und zyklisch geprüft werden. Abbildung 8 zeigt diesen Ablauf bei der Verbindungsaufnahme zwischen Basisstation und Anbietersystem.

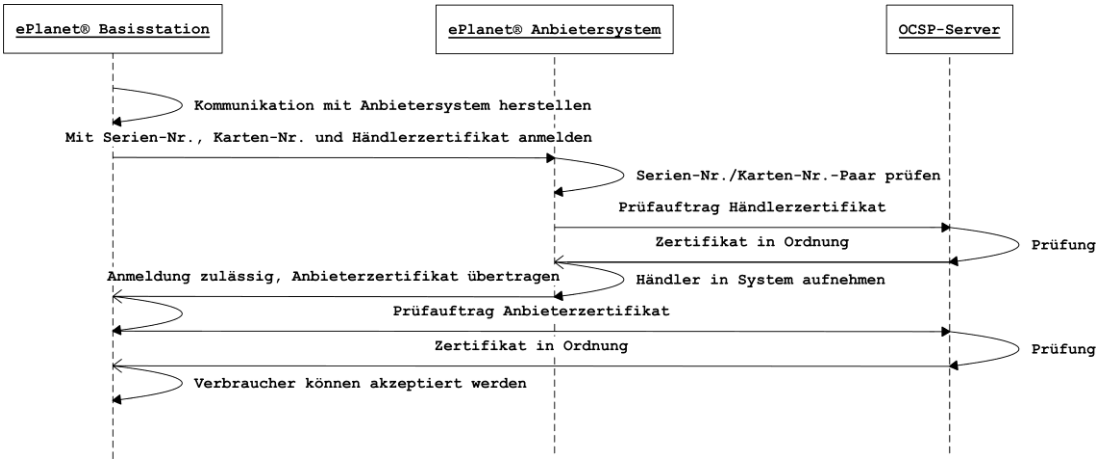

Abbildung 8: Anmeldung Basisstation bei Anbietersystem

3.2 Prüfen von Zertifikaten

Der Ablauf eines Sitzungsaufbaus ist im Dokument [Magellan] (Kapitel 2.2.1, Seite 13 f.) erklärt. Die Aufgabe der PKI ist dabei die Prüfung von Zertifikaten. Sie stellt die Authentizität und Integrität von Nachrichten sicher.

Im Folgenden wird die gegenseitige Prüfung von Zertifikaten zwischen Verbraucher und Händler veranschaulicht.

Dabei werden zuerst die Prüfungen durchgeführt, die ohne direkte Beteiligung der PKI durchführbar sind. Dies schließt die Verifizierung der Signatur ein, sowie die Überprüfung der Gültigkeitsdauer.

Ob ein Zertifikat möglicherweise widerrufen wurde, beantwortet die Prüfstelle der PKI. Dabei wird von einem OCSP Responder ausgegangen. Da dieser qualitative Aussagen über die Gültigkeit eines Zertifikats macht, muss er sich ebenfalls mit einem Zertifikat ausweisen.

Abbildung 9 zeigt eine Übersicht der Prozesse auf der Seite einer ePlanet® Verbraucherstation. Die farblich hinterlegten Teilprozesse werden im Anschluss näher erläutert.

Es wird angenommen, dass die Verbraucherstation keine eigene Zeitbasis hat. Die Prüfung des Gültigkeitszeitraumes eines Zertifikats erfolgt auf Basis der Zeitangabe der OCSP-Antwort.

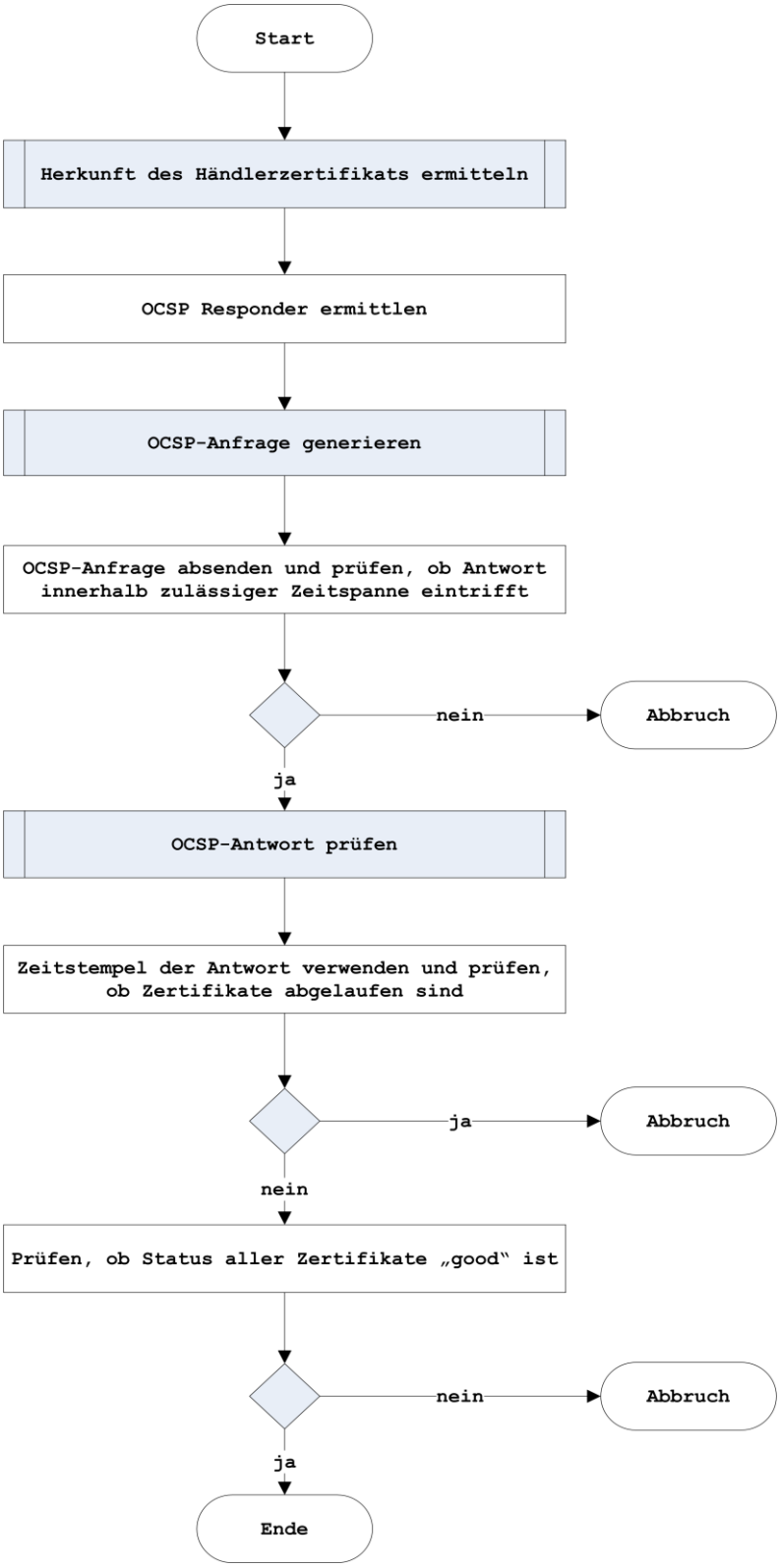

Abbildung 10

Abbildung 11

Abbildung 12

Abbildung 9: Verbraucherstation prüft Händlerzertifikat

Abbildung 10 zeigt, wie zunächst der Ursprung des Händlerzertifikats verifiziert wird. Dieser Ursprung kann die Zertifizierungsstelle sein, die das Zertifikat des Verbrauchers ausgestellt hat. Ebenso möglich ist ein Herausgeber, dem transitiv vertraut werden kann. In diesem Fall kann eine Zertifizierungskette zwischen vertrauter Zertifizierungsstelle und betrachteter Zertifizierungsstelle gebildet werden. Ist dies nicht möglich, besteht keine Basis, auf der den Nachrichten der Basisstation vertraut werden kann, und die Verbindung wird abgebrochen.

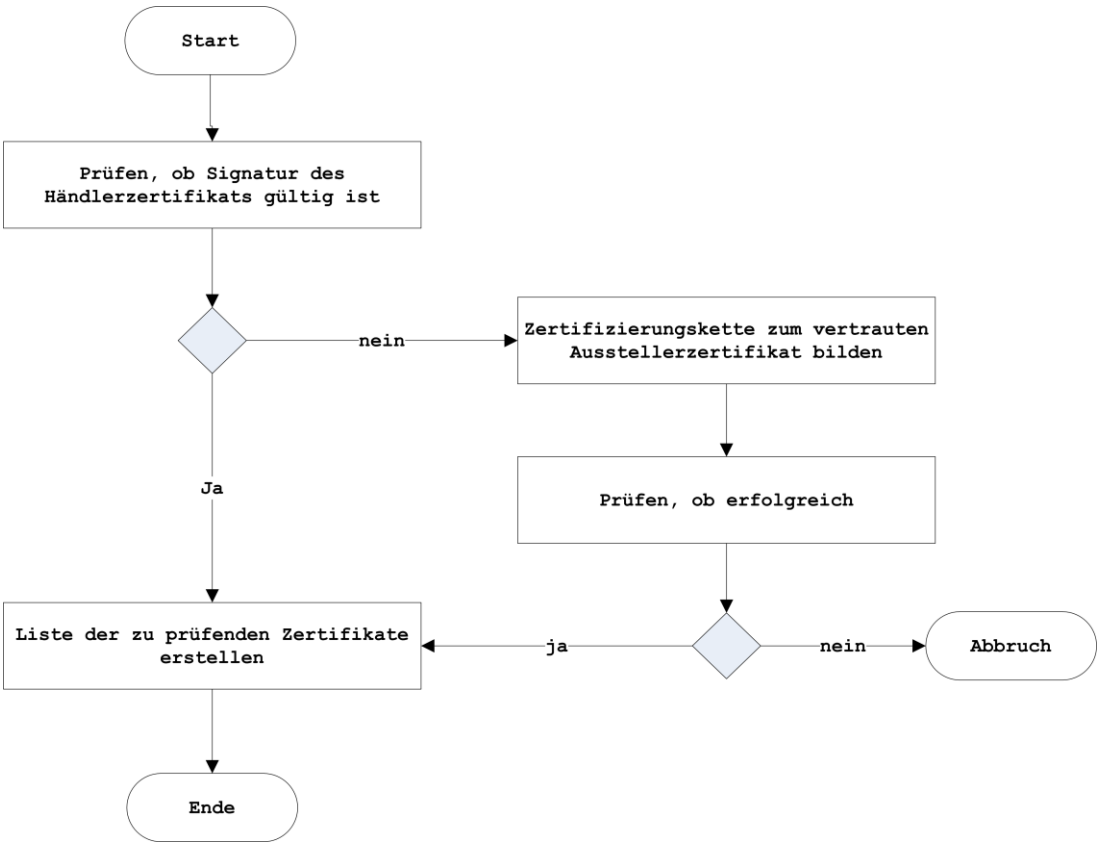

Abbildung 10: Herkunft des Händlerzertifikats ermitteln

Die Signatur des Händlerzertifikats ist nun valide oder eine gültige Zertifizierungskette (mit gültigen Zertifikaten) zum vorliegenden Aussteller kann gebildet werden. Das heißt, es können ein oder mehrere Zertifikate vorliegen, die auf Widerruf geprüft werden müssen. In Abbildung 11 ist zu sehen, wie eine OCSP-Anfrage generiert wird.

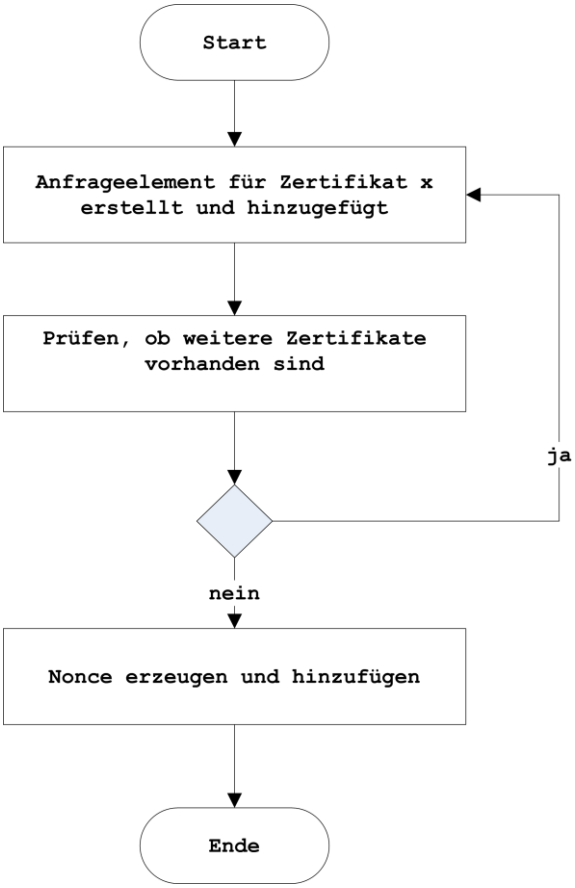

Abbildung 11: Verbraucherstation generiert OCSP-Anfrage

An dieser Stelle ist wichtig, dass die Verbraucherstation mit der OCSP-Anfrage eine Nonce erzeugt und der Nachricht beifügt. Dies liegt daran, dass die Verbraucherstation ihre Nachricht über die ePlanet® Basisstation schicken muss (Abbildung 2). Die Nonce dient zur Absicherung der Integrität der OCSP-Anfrage und -Antwort. Zudem verhindert eine Nonce das Wiedereinspielen älterer Antworten („replay attack"), die das Verwenden des Zeitstempels der Prüfung als Zeitbasis kompromittieren würden.

Erhält die Verbraucherstation daraufhin Antwort vom OCSP-Server, muss die Gültigkeit des Prüferzertifikats und der OCSP-Antwort überprüft werden (Abbildung 12). Stimmt die enthaltene Nonce mit der selbst beigefügten überein, wurde die Nachricht des OCSP-Servers nicht durch einen Dritten verändert.

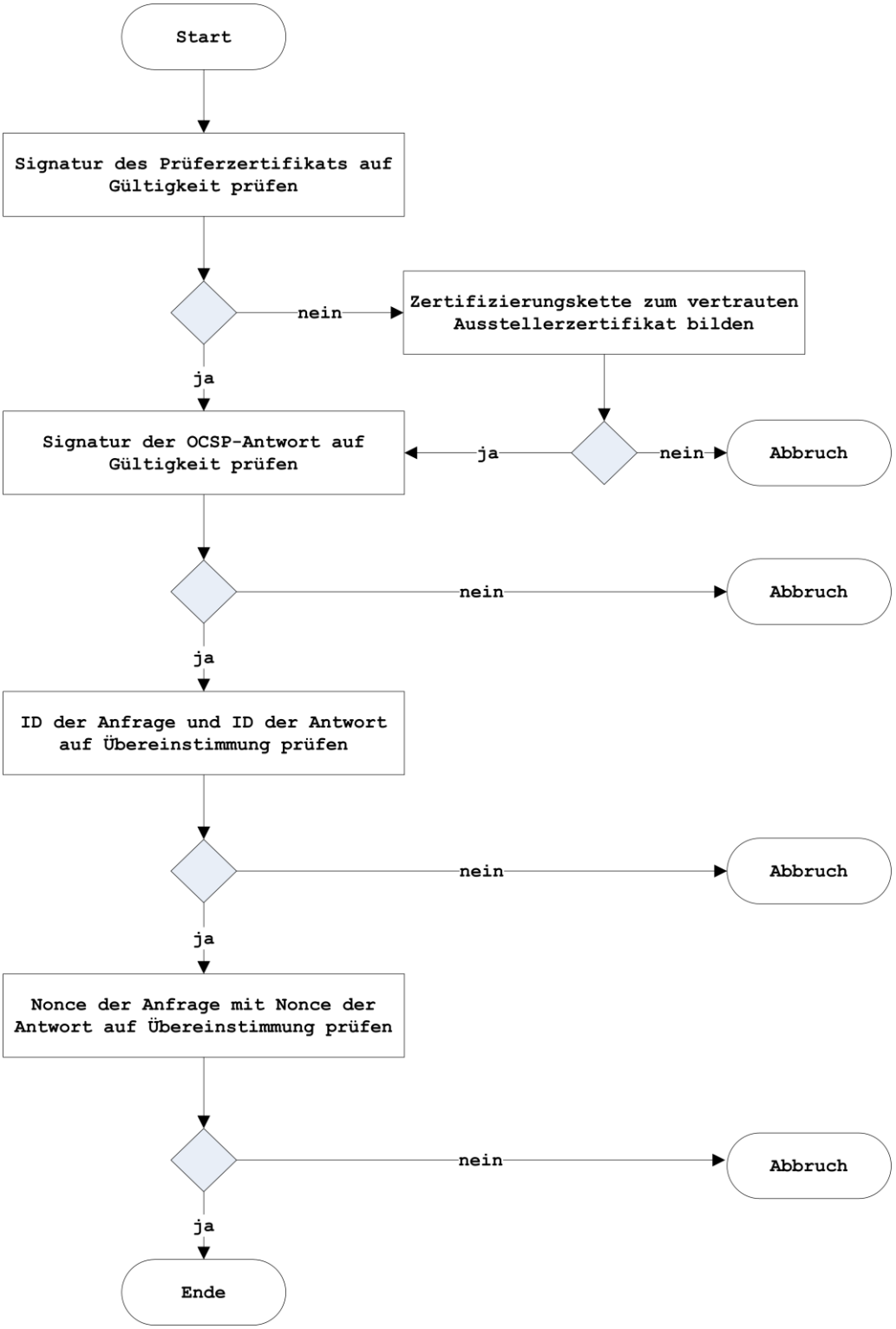

Abbildung 12: Verbraucherstation prüft OCSP-Antwort

Damit ist die Prüfung des Händlerzertifikats abgeschlossen. Einen ähnlichen Ablauf stellt die Prüfung des Verbraucherzertifikats dar. Der Unterschied liegt darin, dass die Basisstation einen direkten Zugang zum Internet hat und eine eigene Zeitbasis. Deshalb kann die Überprüfung der Gültigkeitsdauer vorgezogen werden und eine Nonce ist nicht zwingend erforderlich. Abbildung 13 gibt eine Übersicht über den Prüfvorgang.

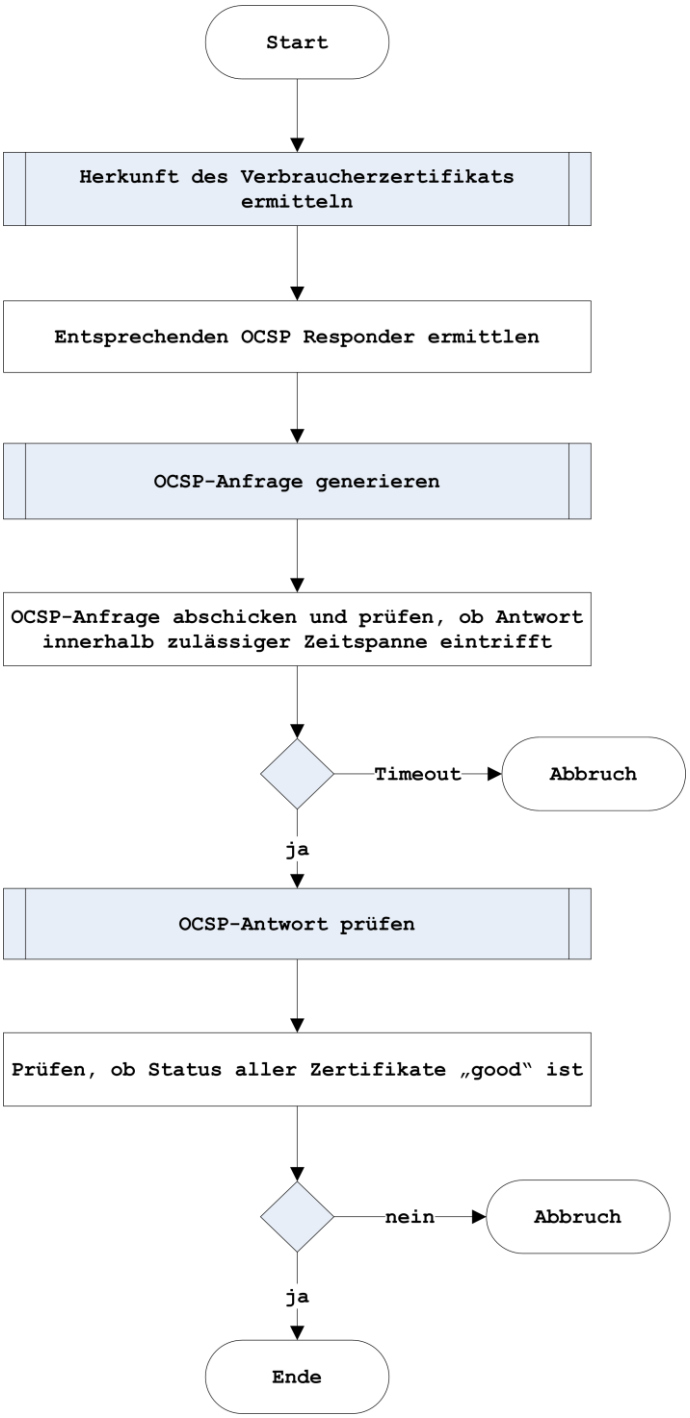

Abbildung 13: Basisstation prüft Verbraucherzertifikat

In Abbildung 14 wird dargestellt, wie der Ursprung des Verbraucherzertifikats ermittelt werden kann. Um die Last auf die Prüfstelle gering zu halten, kann im Vorhinein die Gültigkeitsdauer der Zertifikate überprüft werden.

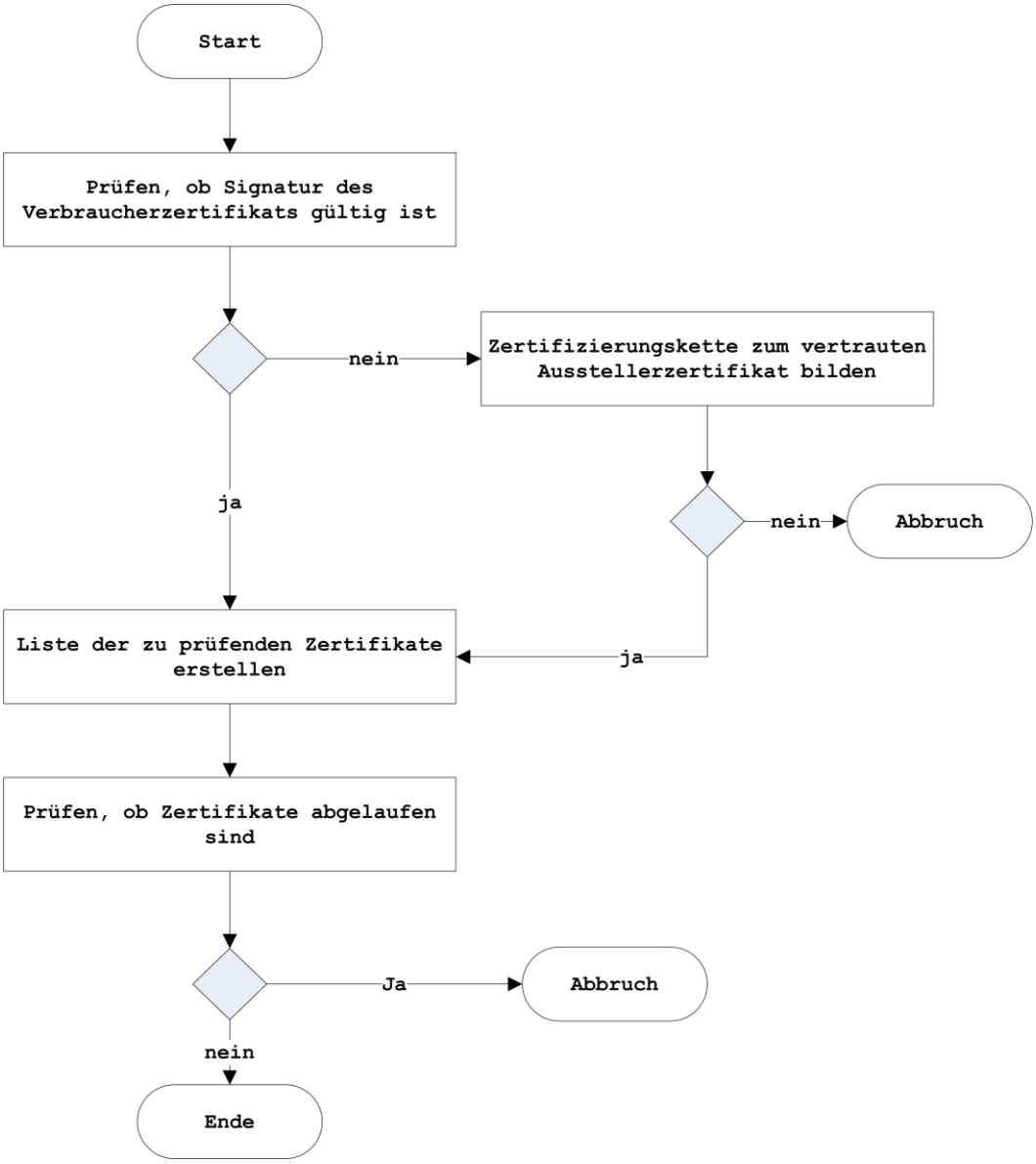

Abbildung 14: Herkunft des Verbraucherzertifikats ermitteln

Für die Erstellung der OCSP-Anfrage muss, wie bereits erwähnt, keine Nonce beigefügt werden (Abbildung 15).

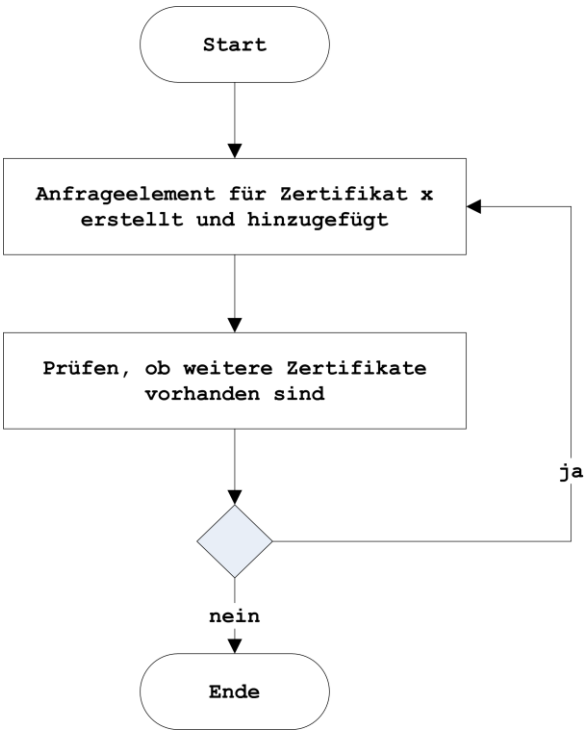

Abbildung 15: Basisstation generiert OCSP-Anfrage

Wird die OCSP-Antwort wie in Abbildung 16 geprüft, ist der Vorgang der wechselseitigen Authentifizierung zwischen Verbraucherstation und Basisstation abgeschlossen.

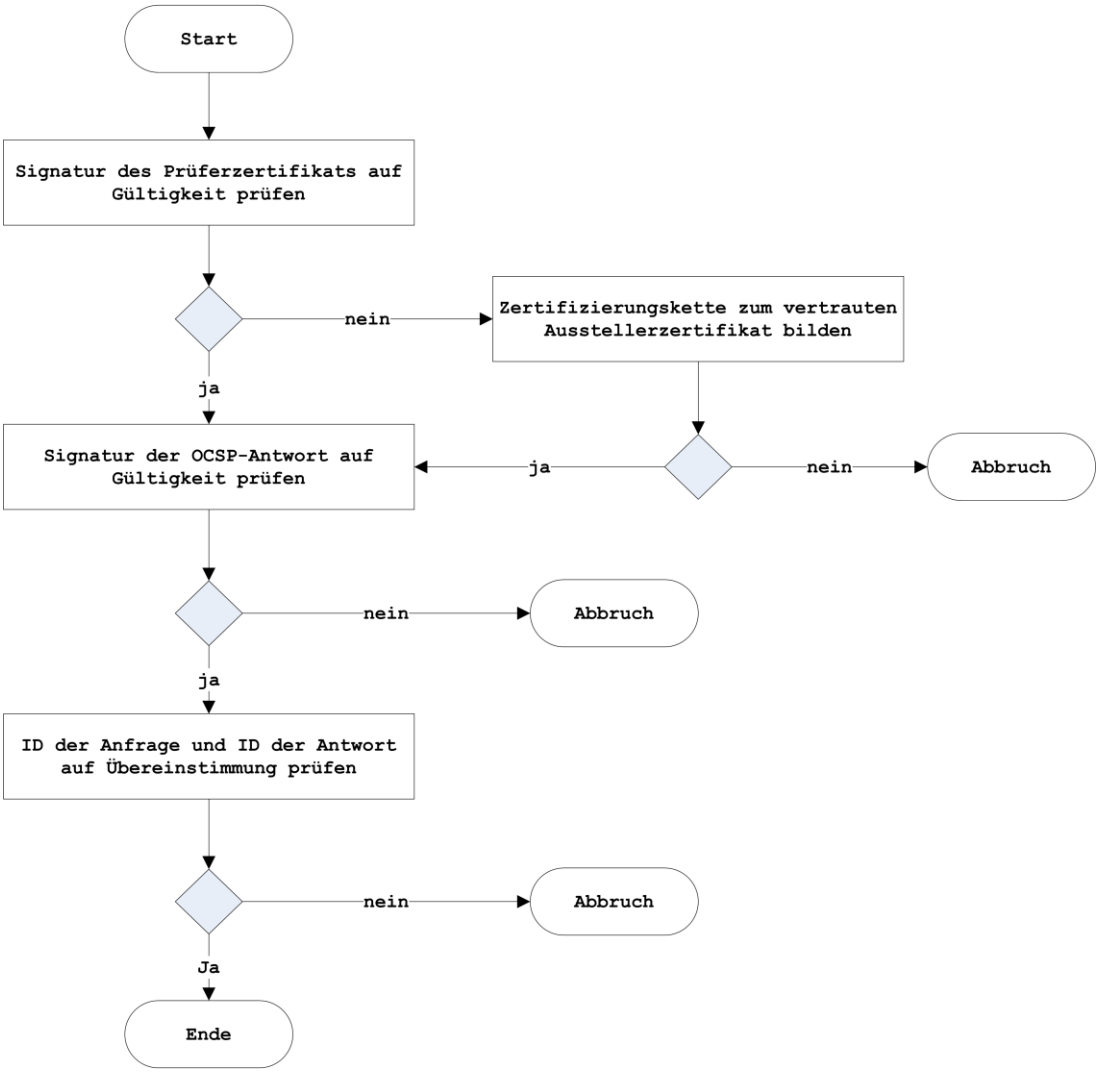

Abbildung 16: Basisstation prüft OCSP-Antwort

Die wechselseitige Authentifizierung zwischen Basisstation und Anbietersystem wird hier nicht mehr detailliert erklärt. Die Abläufe gleichen den oben vorgestellten Vorgängen.

3.3 Vorgeschlagene Standards

Die folgenden Abschnitte stellen vor, mit welchen Standards die PKI für ePlanet® umgesetzt werden soll.

3.3.1 Anforderungen an Zertifikate

In diesem Dokument wird die Verwendung von X.509-Zertifikaten motiviert. Der Standard [X.509] formuliert bereits Richtlinien für eine PKI und ist sehr weit verbreitet. Für ePlanet® ist die Verwendung dieser ID-Zertifikate völlig ausreichend, zumal die Möglichkeit besteht, den Standard zu erweitern. Eine Übersicht zu relevanten Feldern wird in Tabelle 15 dargestellt. ([Bless], Tabelle 9.1, Seite 372)

Feld	Beschreibung
version	Versionsnummer des Zertifikatsformates
serialNumber	Seriennummer, zusammen mit *issuer* eindeutig
issuer	ID des Erzeugers des Zertifikats
signature	für Signatur genutzter Algorithmus
validity	Gültigkeitsdauer des Zertifikats
subject	ID des Zertifikatsbesitzers
subjectPublicKeyinfo	öffentlicher Schlüssel
keyUsage	Zweck des Schlüssels, z.B. *digitalSignature*
extendedKeyUsage	besonderer Zweck des Schlüssels, z.B. *OCSPSigning*
AuthorityInfoAccess	Adresse der verantwortlichen Prüfstelle

Tabelle 15: Struktur des X.509-ID-Zertifikats für ePlanet®

In [Magellan] werden zwei Anforderungen bezüglich Zertifikaten gestellt (Kapitel 2.3, Seite 18 f.):

- Zertifikate enthalten als identifizierbares Merkmal eine Vertragsnummer (z.B. „13816392").
- Zertifikate enthalten eine Angabe über die Rolle des Teilnehmers (z.B. „consumer").

Die beiden Anforderungen können erfüllt werden, indem das Feld *subject* die Vertragsnummer und die Rolle des Teilnehmers als Zeichenkette vereint. Eine ID für ein Verbraucherzertifikat wäre zum Beispiel „13816392-consumer".

3.3.2 OCSP

Wie schon im letzten Kapitel angedeutet, wird für die ePlanet® PKI die Verwendung von [OCSP] vorgeschlagen.

Dies setzt zunächst voraus, dass Zertifikate zwischen den Kommunikationsteilnehmern ausgetauscht werden. Im technischen Bericht [Magellan] wird dieser Vorgang ausführlich beschrieben.

Eine spezielle Anforderung stellt die fehlende Zeitbasis der Verbraucherstation dar sowie die besondere Konstellation zwischen Verbraucherstation, Basisstation und Anbietersystem.

Letztere Tatsache macht eine Erweiterung der OCSP-Nachrichten notwendig: Das Feld *id-pkix-ocsp-nonce* muss hinzugefügt werden, die Erweiterung, um eine Nonce mitsenden zu können.

4 ePlanet® Testaufbau

In diesem Kapitel wird der Testaufbau für ePlanet® beschrieben. Für Verbraucherstation und Basisstation von ePlanet® wird derzeit *embedded PC-Hardware* verwendet, die mit Windows XP betrieben wird. Wie beide Komponenten miteinander interagieren, ist bereits im Dokument [Magellan] spezifiziert.

Der Schwerpunkt dieses Kapitels ist die Umsetzung des Hintergrundsystems. Als Plattform dient ein PC mit Windows als Betriebssystem. Dieser ist über ein LAN mit der Basisstation verbunden. Die Software umfasst mehrere Komponenten und wird in Kapitel 4.2 beschrieben.

4.1 Übersicht

Abbildung 17 zeigt eine Übersicht des Testaufbaus für ePlanet®. Folgende Komponenten sind beteiligt:

- Verbraucherstation - embedded PC mit PLC-Adapter und Kartenleser: Sie verbindet sich automatisch mit der Basisstation, wenn die PLC-Verbindung hergestellt ist, und weist sich mit ihrem Zertifikat der Chipkarte aus.
- Basisstation - embedded PC mit PLC-Adapter und Leistungsmesser: Die Basisstation verfügt über einen Kartenleser mit einer Chipkarte, auf der das digitale Zertifikat des Händlers gespeichert ist. Da Magellan keine Nachrichten erfordert, die vom Händler signiert werden, ist ein privater Schlüssel für das Händlersystem nicht erforderlich. Die Abläufe des Verfahrens Magellan werden für die ePlanet® Basisstation als ereignisdiskretes Modell beschrieben. Die Ausführung dieses Modells erfolgt mit *Heron Didact* [Heron]. Die Anwendung besteht aus der echtzeitfähigen Steuerung *Heron* und dem Werkzeug *Auriga*. Mit Auriga kann die Ausführung des Modells visualisiert und analysiert werden. Eine Erkennung eines parallel verbundenen Stromdiebes ist aufgrund des fehlenden Leistungsmessers in der Verbraucherstation nicht realisiert.
- Hintergrundsystem: Es besteht aus Prozessen für Anbietersystem, Prüfstelle und einer Benutzerschnittstelle.

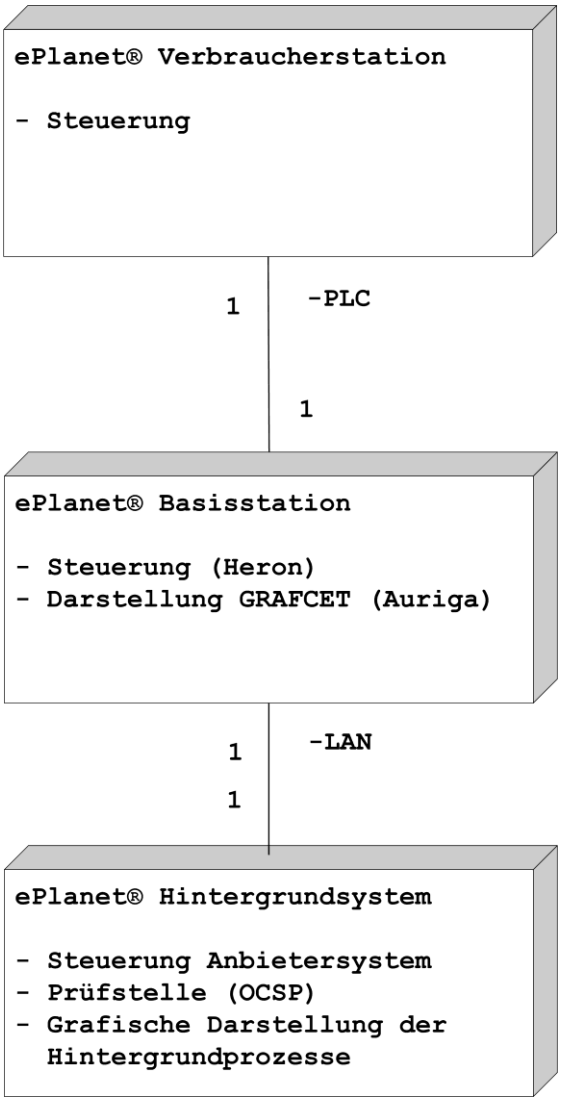

Abbildung 17: Übersicht des ePlanet® Testaufbaus

4.2 ePlanet® Hintergrundsystem

4.2.1 Anbietersystem

Als Hintergrundsystem des Anbieters dient eine Windows-Anwendung mit grafischer Oberfläche. An der Oberfläche werden die Basisstationen aufgeführt, die sich beim Hintergrundsystem registriert haben. Für jede Basisstation kann die Höchstzahl der gleichzeitig zu bedienenden Verbraucher eingestellt werden. Über diese Funktion lässt sich die Sitzungsbeschränkung durch

den Anbieter testen. Abbildung 18 zeigt ein Bildschirmfoto der Bedienoberfläche.

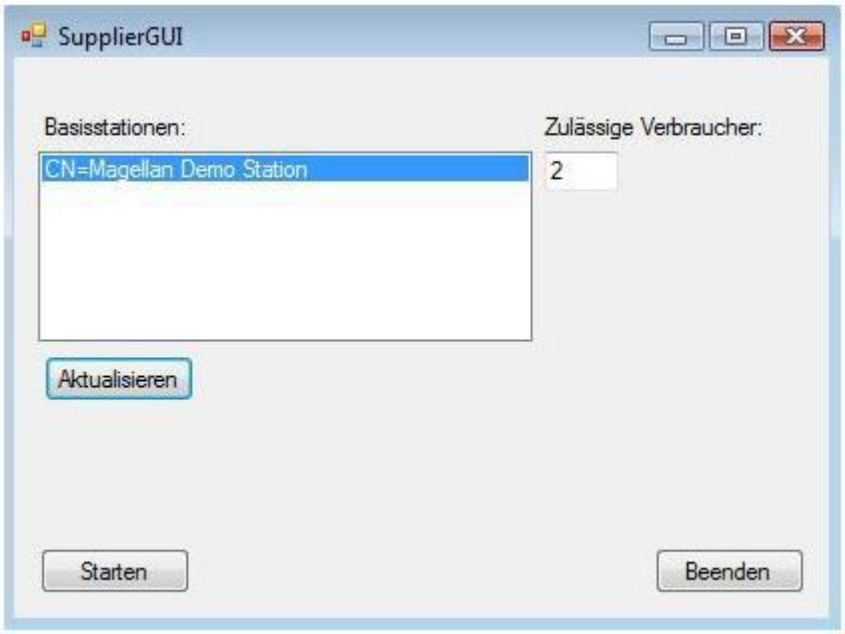

Abbildung 18: Oberfläche der Anbieteranwendung

Der Anwendung fehlen folgende Punkte, um sich in das Hintergrundsystem des ePlanet® Betreibers einfügen zu können:

- Zertifikate mittels OCSP auf Widerruf prüfen
- Anbieterzertifikat auf Chipkarte, da Nachrichten des Anbieters signiert werden müssen
- Datenhaltung mit registrierten Händlern sowie einer Zuordnung von Seriennummern und Kartennummern
- Aufbereitung der Transaktionsdaten: Verbraucher, Strommenge und Kosten
- Schnittstelle zum Abrechnungsprozess des Hintergrundsystems, um relevante Daten zu übertragen

4.2.2 Prüfstelle

Um die Verwendung von OCSP innerhalb von ePlanet® testen zu können, muss für das Hintergrundsystem ein kleiner OCSP-Server entwickelt werden.

Um den Standard [OCSP] zu implementieren, kann die frei verfügbare Bibliothek Bouncy Castle verwendet werden [BCastle].

Abbildung 19 zeigt die Architektur des OCSP-Servers.

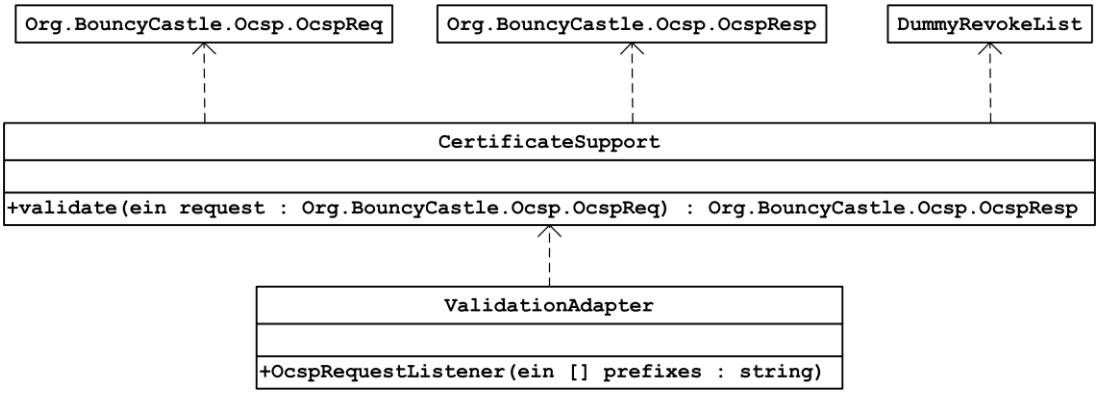

Abbildung 19: Architektur des OCSP-Servers

- *CertificateSupport* implementiert den Prüfalgorithmus für X.509-Zertifikate und verwendet die offene Bibliothek *BouncyCastle*; *OcspReq* und *OcspResp* sind die Datenstrukturen von Bouncy Castle für Anfragen und Antworten des Protokolls.
- *ValidationAdapter* realisiert einen *System.Net.HttpListener* und reicht OCSP-Anfragen weiter an *CertificateSupport*.
- *DummyRevokeList* ist eine zur Laufzeit veränderbare Datenbasis, in der Widerrufsinformation gespeichert wird; sie wird anstelle einer Zertifikatssperrliste oder Datenbank verwendet.

4.2.3 Benutzerschnittstelle

Eine Benutzerschnittstelle kann die Interaktion der verschiedenen Komponenten des Hintergrundsystems veranschaulichen und schafft die Möglichkeit, direkt mit dem System zu interagieren.

Im einfachsten Fall besteht diese Schnittstelle nur aus einer veränderbaren Liste, auf der die Prüfstelle arbeitet. Wird die Liste um einen Eintrag der Verbraucher- oder Basisstation erweitert, muss der OCSP-Server das zu prüfende Zertifikat als widerrufen melden.

Wird mehr Aufwand in die grafische Darstellung des Hintergrundsystems gesteckt, könnte das System auch auf einer Messe vorgeführt werden. Das Konzept für dessen Umsetzung könnte folgende Punkte in Betracht ziehen:

- Gegenseitige Authentifizierung mithilfe von Zertifikaten ist nicht zwingend für jeden Betrachter interessant oder verständlich.
- Das System sollte auf eine leicht verständliche Art die Sicherheit des Verfahrens projizieren. Jedoch sollten gewisse Grundkenntnisse vorausgesetzt werden. Wenn bei einer Demonstration die Chipkarte aus der ePlanet® Verbraucherstation gezogen wird und unmittelbar darauf die Beleuchtung des Exponats erlischt, wirkt das eher inszeniert.
- Die transparente Darstellung der Abläufe schafft Vertrauen in das System. Die Interessen von Verbrauchern, Händlern und Anbietern müssen berücksichtigt werden.
- Die Entwicklung von Bedienoberflächen ist aufwändig und teuer. Möglicherweise bietet sich die Umsetzung als Web-Anwendung an.

4.3 Verteilung von Zertifikaten

Für den Testaufbau benötigen alle beteiligten Komponenten ein eigenes Zertifikat. Damit die Prüfung erfolgreich verlaufen kann, müssen alle Zertifikate von demselben Aussteller stammen (vgl. Zertifizierungsstelle). Für den Testaufbau dient als Wurzelzertifikat ein selbst ausgestelltes Zertifikat.

Mithilfe dieses Wurzelzertifikats werden alle folgenden Zertifikate, die ausgestellt werden, signiert. Möchte ein Benutzer ein anderes Zertifikat prüfen, kann er zunächst diese Signatur des Wurzelzertifikats prüfen. Für den Testaufbau wird daher das Konzept des direkten Vertrauens verfolgt und kein hierarchisches Modell wie in Abbildung 1 gezeigt.

Folgende Felder sind für den Testbetrieb erforderlich:

- Identifikator
- Rolle nach Magellan (consumer, vendor, supplier)
- Gültigkeitsdauer
- Signatur des Wurzelzertifikats

- Kartennummer (womöglich identisch mit Identifikator)
- öffentlicher Schlüssel
- Adresse des zuständigen OCSP-Servers

In Abbildung 20 ist zu sehen, dass für den Testaufbau zumindest fünf Zertifikate erzeugt und verteilt werden müssen.

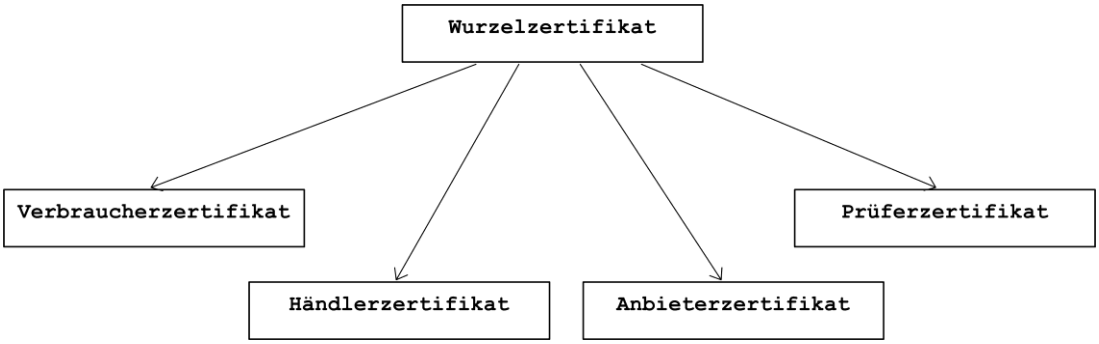

Abbildung 20: Verteilung von Zertifikaten

Verzeichnisse

A Verzeichnis der Tabellen

Tabelle 1: Glossar wichtiger Begriffe 7
Tabelle 2: Bestandteile einer PKI 8
Tabelle 3: Anwendungsfall - Registrierung ePlanet® Prüfstelle 15
Tabelle 4: Anwendungsfall – Inbetriebnahme ePlanet® Prüfstelle ... 15
Tabelle 5: Anwendungsfall – Erneuerung Zertifikat Prüfstelle 16
Tabelle 6: Anwendungsfall – Registrierung Händler 16
Tabelle 7: Anwendungsfall – Inbetriebnahme Basisstation 17
Tabelle 8: Anwendungsfall – Servicefall Basisstation 17
Tabelle 9: Anwendungsfall – Registrierung Verbraucher 18
Tabelle 10: Anwendungsfall – Inbetriebnahme Verbraucherstation ... 18
Tabelle 11: Anwendungsfall – Verbraucher prüft Händler 19
Tabelle 12: Anwendungsfall – Händler prüft Verbraucher 19
Tabelle 13: Anwendungsfall – Anbieter prüft Händler 19
Tabelle 14: Anwendungsfall – Händler prüft Anbieter 20
Tabelle 15: Struktur des X.509-ID-Zertifikats für ePlanet® 36

B Verzeichnis der Abbildungen

Abbildung 1: OCSP – Online Certificate Status Protocol 10
Abbildung 2: Beteiligte Systeme Magellans (aus [Magellan], S.12) . 11
Abbildung 3: Inbetriebnahme eines OCSP-Servers 22
Abbildung 4: Aktualisierung des Prüferzertifikats 22
Abbildung 5: Beim Anbieter hinterlegte Zuordnung 23
Abbildung 6: Inbetriebnahme einer ePlanet® Basisstation 24
Abbildung 7: Servicefall ePlanet® Basisstation 25
Abbildung 8: Anmeldung Basisstation bei Anbietersystem 26
Abbildung 9: Verbraucherstation prüft Händlerzertifikat 27
Abbildung 10: Herkunft des Händlerzertifikats ermitteln 28
Abbildung 11: Verbraucherstation generiert OCSP-Anfrage 29
Abbildung 12: Verbraucherstation prüft OCSP-Antwort 30
Abbildung 13: Basisstation prüft Verbraucherzertifikat 32
Abbildung 14: Herkunft des Verbraucherzertifikats ermitteln 33
Abbildung 15: Basisstation generiert OCSP-Anfrage 34
Abbildung 16: Basisstation prüft OCSP-Antwort 35
Abbildung 17: Übersicht des ePlanet® Testaufbaus 39
Abbildung 18: Oberfläche der Anbieteranwendung 40
Abbildung 19: Architektur des OCSP-Servers 41
Abbildung 20: Verteilung von Zertifikaten 43

C Referenzen

Referenz	auf
[Magellan]	Paaschen, Tim-Oliver (IFS): BZ-11881, Technischer Bericht *Vertrauensbasis Magellan: Wechselseitige Authentisierung von Händlern und Verbrauchern*, http://www.ifs-it.de/de/erfindungskompetenz/eplanet, abgerufen am: 10.05.2012..
[ePlanet®]	IFS: HTML-Dokument *IFS München: ePlanet®*, http://www.ifs-it.de/de/erfindungskompetenz/eplanet, abgerufen am: 10.05.2012.
[OCSP]	Myers, M. u.a. (IETF): *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*, http://www.ietf.org/rfc/rfc2560.txt, abgerufen am: 10.05.2012.
[Bless]	Bless, Roland u.a. (2005): *Sichere Netzwerkkommunikation*, 1. Auflage, Springer-Verlag, Berlin.
[JB]	Buchmann, Johannes (2010): *Einführung in die Kryptographie (Springer-Lehrbuch)*, 5. Auflage, Springer-Verlag, Berlin.
[X.509]	Cooper, D. u.a.: *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, http://tools.ietf.org/html/rfc5280, abgerufen am: 10.05.2012.
[Heron]	IFS: HTML-Dokument *IFS München: Heron Didact*, http://www.ifs-it.de/de/erfindungskompetenz/heron, abgerufen am: 10.05.2012.
[BCastle]	Yang, Kaiser u.a.: *The Legion of the Bouncy Castle*, http://www.bouncycastle.org/csharp/, abgerufen am: 10.05.2012.