Bundesministerium
des Innern

S P H I N X

Pilotversuch
Ende-zu-Ende-Sicherheit

PKI Organisationshandbuch

November 1999

Schriftenreihe der KBSt
ISSN 0179-7263
Band 46

KBSt

Koordinierungs- und Beratungsstelle
der Bundesregierung
für Informationstechnik
in der Bundesverwaltung

Schriftenreihe der KBSt
Band 46
ISSN 0179 - 7263

Bundesministerium des Innern
Arbeitsgruppe O 1
O 1 (KBSt) - 195 101/25
11014 Berlin

Homepage der KBSt: http://www.kbst.bund.de

Veröffentlichungen aus der Schriftenreihe der KBSt können von Band 26 bis einschließlich Band 41 bezogen werden bei

Bundesanzeiger Verlagsgesellschaft mbH
Postfach 1005

50455 Köln

SPHINX

Pilotversuch

Ende-zu-Ende-Sicherheit

PKI Organisationshandbuch

Version 3.5
Stand: 24. September 1999

Claus Stark, Holger Mack, Fritz Bauspieß
Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe

Hans-Willi Fell
Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 183
D-53175 Bonn

Klaus Wielandt
Siemens Business Services GmbH & Co. OHG
Vorgebirgsstraße 49
D-53119 Bonn

Thomas Beckmann, Norbert Landwehr
CCI GmbH
Lohberg 10
D-49716 Meppen

Inhaltsübersicht

Abbildungsübersicht

Vorwort

Verschlüsselungs- und Signaturverfahren benötigen als "notwendiges Übel" eine Zertifizierungsinfrastruktur (engl. Public Key Infrastructure, abgekürzt PKI). Dies liegt in der Besonderheit des gewählten Verfahrens begründet: Jeder der moderne kryptografische Verfahren einsetzt, erzeugt mit einem Programm zwei Schlüssel, die über ein ausgeklügeltes mathematisches Verfahren einander zugeordnet sind. Diese Schlüssel sind binäre Texte mit einer Länge die größer ist als 768 Bit (empfohlene Mindestlänge für digitale Signaturen). Einer der Schlüssel ist der private oder geheime Schlüssel. Diesen speichert der Besitzer auf Diskette oder Chipkarte ab, verwahrt ihn sicher auf und gibt ihn niemals an andere Personen weiter. Der zweite Schlüssel ist der sogenannte öffentliche Schlüssel.

Mit dem öffentlichen Schlüssel des Empfängers verschlüsselt der Absender die Nachricht. Nur der Empfänger mit seinem privaten (geheimen) Schlüssel ist in der Lage die Informationen zu entschlüsseln. Der private Schlüssel des Absenders dient zur digitalen Signatur eines Dokuments. Nach Erhalt kann der Empfänger mit dem öffentlichen Schlüssel des Absenders dessen Unterschrift und die Echtheit des Dokuments prüfen.

Ein Schwierigkeit stellt nur der Austausch der öffentlichen Schlüssel dar. Jeder Besitzer muß in einer offenen Kommunikationswelt wie dem Internet, in der jeder mit jedem sicher kommunizieren möchte, seinen öffentlichen Schlüssel bekanntgeben. Angenommen, der Besitzer stellt den öffentlichen Schlüssel im Internet auf seiner Homepage oder in einem Verzeichnis zum Download bereit, bestünde die Gefahr, daß andere Personen die öffentlichen Schlüssel vertauschen, so daß eine Zuordnung von Person zu öffentlichen Schlüsseln nicht sichergestellt wäre. In der Folge können die empfangenen Dokumente für den Empfänger nicht entschlüsselt werden, andere jedoch die vertraulichen Nachrichten lesen..

Ein Zertifikat verhindert die versehentliche Veränderung oder Fälschung der Zuordnung von Person zu Schlüssel. Es besteht im wesentlichen aus Angaben öffentlichen Schlüssel, Namen des Besitzers und Gültigkeitsdauer. Eine Verfälschung der Angaben in den Zertifikaten verhindert die Zertifizierungsstelle, in dem sie das Zertifikat durch ihre digitale Signatur beglaubigt.

Augenscheinlich kann es im Internet nicht nur eine Zertifizierungsstelle geben. Zertifizierungsstellen schließen sich zu einer Zertifizierungshierarchie zusammen. Daher besteht sie aus einer Vielzahl verschiedener Unternehmen, Organisationen und Behörden, die sich über ihr Zusammenwirken verständigen müssen. Erst dann ist es möglich, daß ihre Kunden und Anwender wahlfrei miteinander sicher und authentisch kommunizieren können.

Während es zu den technischen Prozessen von Verschlüsselung und digitaler Signatur einer Vielzahl von Veröffentlichungen gibt, sind die organisatorischen Abläufe eher Gegenstand für die Fachwelt oder nur für den Eigenbetrieb geklärt. Die oben erwähnte Verständigung der Zertifizierungsstellen mit unterschiedlichen Betreibern wird zwar gefordert, ist jedoch in der Praxis noch zu regeln. Diese Regelung reicht jedoch bei weitem nicht aus. Ein Vielzahl von Abläufen zum Beispiel von Teilnehmer zur Zertifizierungsstelle oder zur Registrierungsstelle sowie interne Abläufe bei den unterschiedlichen Stellen einer Zertifizierungshierarchie sind harmonisierungs- manchmal auch regelungsbedürftig.

Im Pilotversuch SPHINX werden die Abläufe in einer kleinen Zertifizierungsinfrastruktur mit ca. 400 Teilnehmern im Sinne von Interoperabilität und Funktionalität getestet. Die gemachten organisatorischen Erfahrungen münden im vorliegenden Organisationshandbuch.

Das Organisationshandbuch wurde rollenbasiert aufgebaut, so daß es unabhängig von einer bestehenden Aufbauorganisation oder von konkreten Personen im Projekt SPHINX modelliert werden konnte. Das hat seine Bewandtnis: es sollte nicht nur für die am Pilotversuch

Beteiligten geeignet sein, sondern auch anderen helfen, die beispielsweise eine Zertifizierungsstelle oder Registrierungsstelle aufzubauen beabsichtigen.

Ein solches Dokument wie das hier vorliegende ist niemals statisch. Konsequente Anwendung der beschriebenen Abläufe, Tests und Einsatz neuer oder verbesserter Produkte sowie die Einführung neuer Verfahren (Internet-Standards) werden als Erfahrungen in das Organisationshandbuch einfließen und es verändern. Daher soll es Anregung und Hilfestellung geben sowie zur Diskussion mit Interessierten auffordern.

1 Ziele des Organisationshandbuchs

Im Rahmen des Projekts SPHINX wird die organisatorische und technische Infrastruktur für eine effiziente Ende-zu-Ende-Sicherheit für den elektronischen Dokumentenaustausch spezifiziert, aufgebaut und betrieben. Die Public Key Infrastruktur (PKI) besteht aus verschiedenen Komponenten, deren Zusammenspiel sowohl technisch als auch organisatorisch den Sicherheitsanforderungen genügen muß. Für einzelne dieser Komponenten sind über organisatorische Regelungen, wie sie in dem vorliegenen Organisationshandbuch (OrgHB) beschrieben sind, hinaus zusätzlich hohe Sicherheitsanforderungen an die Infrastruktur (bauliche Voraussetzungen), an die eingesetzte Technik (Hardware und Software) und an das eingesetzte Personal (besonders ausgebildete und überprüfte Personen) zu stellen. Nur wenn alle diese Aspekte gleichermaßen beachtet werden, kann das realisierte System seine Ziele bzgl. Funktionalität und Sicherheit erreichen. Dieses Zusammenführen der verschiedenen Aspekte zu einem geschlossenen Konzept erfolgt überlicherweise in einem *Sicherheitskonzept*.

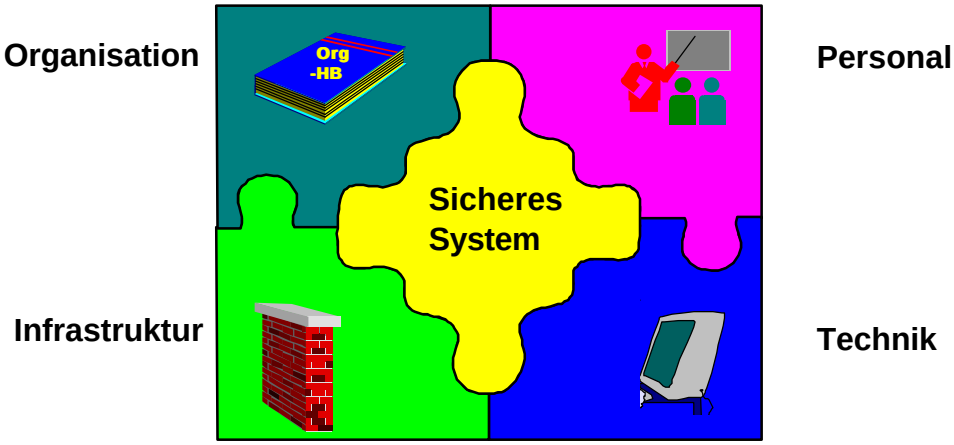


Abbildung 1: Notwendige Voraussetzungen für ein sicheres System

Während das Hauptaugenmerk des Pilotprojektes SPHINX zunächst auf der technischen Fortentwicklung der eingesetzten technischen Komponenten hinsichtlich ihrer Interoperabilität lag, rückt nun verstärkt auch die Organisation ins Blickfeld. Sie leistet einen wichtigen Beitrag für die Sicherheit der PKI.

In diesem Organisationshandbuch werden die Komponenten der PKI und deren organisatorisches Zusammenwirken beschrieben.

Hauptziel des vorliegenden Organisationshandbuchs ist es, das erkannte Defizit bei der Planung einer PKI oder einer einzelnen Instanz, nämlich den Aufwand der organisatorischen Abläufe sowie das Zusammenspiel zwischen Technik und Organisation abschätzen zu können. In dem Pilotversuch SPHINX wird anhand des Organisationshandbuches der beschriebene Ablauf getestet. Für den Wirkbetrieb einer PKI bzw. Instanz muß die Organisation dem geforderten Sicherheitsstandard angepaßt werden.

Dieses Organisationshandbuches hat im Einzelnen folgende Ziele:

- Es definiert die Struktur und die Abläufe der PKI, die sich an die organisatorischen Strukturen des von der Studie „Ende-zu-Ende-Sicherheit für elektronischen Dokumentenaustausch“ vorgegebenen Rahmens anlehnen.
- Es berücksichtigt die organisatorischen Besonderheiten der Bundesverwaltung, der Länderverwaltungen und der Industrie, aber auch die des einzelnen Bürgers.
- Es beschreibt klare, aufeinander abgestimmte Strukturen und Abläufe, damit diejenigen, die mit dem Aufbau einer oder mehrerer Stellen betraut sind (hier sei als Beispiel der organisatorische Ansprechpartner in der Institution genannt), die beschriebenen Organisationsabläufe nutzen können.
- Die Aufbau- und Ablauforganisation ist nicht nur an der aktuellen Projektsituation orientiert, sondern vor allem auch auf einen späteren Produktivbetrieb ausgelegt.
- Die in diesem Organisationshandbuch entwickelten Modelle (PKI- und Rollenmodell) sind flexibel gehalten und erlauben die Anpassung an jeweils gegebene Ziele und Rahmenbedingungen.
- Die Regelungen des Organisationshandbuchs ermöglichen ein selbständiges Arbeiten der beteiligten Instanzen und Personen bei gleichzeitiger Gewährleistung eines sicheren und funktionstüchtigen Gesamtbetriebs. Die Erfahrung aller Beteiligten aus der Anwendungen des Organisationshandbuch soll im Rahmen der Piloterprobung in das Organisationshandbuch zurückfließen und eingearbeitet werden.
- Für das Personal in den einzelnen Stellen (Registrierungsstellen und Zertifizierungsstellen) existieren eigene Betriebshandbücher für die Handlungsanleitung in der Praxis. Sie werden auf der Grundlage des in diesem Organisationshandbuchs dokumentierten PKI- und Rollenmodells erstellt und enthalten speziell auf die Bedürfnisse dieser Stellen ausgerichtetes Material (u.a. benötigte Formulare und Arbeitsanweisungen).

Das Organisationshandbuch konzentriert sich auf die Abläufe und die Rollen, die für einen reibungslosen Verlauf des Piloten notwendig sind und die für die Erreichung der gestellten Ziele benötigt werden. Hierbei ist besonders darauf hinzuweisen, daß die Abläufe und Maßnahmen einen für den zeitlich begrenzten Piloten angemessenen Sicherheitsstandard garantieren sollen.

Die in diesem Dokument beschriebenen organisatorischen Vorgänge sind produktunabhängig und sollen von jedem Produkt, das die technischen Anforderungen dieses Piloten erfüllt, unterstützt werden können. Es wird davon ausgegangen, daß alle im Piloten eingesetzten Produkte die in den Dokumenten „SPHINX-Tailoring“ und „SPHINX-Technische Grundlagen“ für den Piloten festgelegte Funktionalität umfassen. Durch die hier beschriebenen Abläufe dürfen sich keine darüber hinaus gehenden technischen Anforderungen an die Produkte ergeben. Sollten einige Punkte nicht durch die bestehenden technischen Maßnahmen gelöst werden können, so müssen zu Beginn geeignete organisatorische Maßnahmen getroffen werden. Spezielle Funktionalitäten einzelner Produkte werden nicht berücksichtigt.

Da das SPHINX-Projektmanagement sich zunehmend aus den eigentlichen operativen Abläufen zurückziehen und stärker beratende, analytische und dokumentarische Funktionen übernehmen wird, bedarf es einer aktiven Einbindung der teilnehmenden Behörden, Firmen und anderen Institutionen am Aufbau der Strukturen und in der Durchführung der Abläufe. Ein Hauptaugenmerk liegt daher auf den organisatorischen Ansprechpartnern der Registrierungsstellen.

2 Aufbau des Dokuments

Das vorliegende Organisationshandbuch für den Aufbau und Betrieb einer Public Key Infrastruktur (PKI) für die Ende-zu-Ende-Sicherheit beim elektronischen Dokumentenaustauschs ist wie folgt gegliedert:

- Kapitel 3 enthält eine Übersicht über den Aufbau der für den Piloten spezifizierten PKI und eine Beschreibung der spezifischen Ziele, Aufgaben und Rollen der verschiedenen PKI-Teilkomponenten („Instanzen“). In diesem Kapitel werden außerdem die grundlegenden Datenobjekte benannt, die innerhalb der PKI Verwendung finden.
- Kapitel 4 und 5 spezifizieren die Ablauforganisation der PKI: Kapitel 4 stellt die Abläufe und das Zusammenwirken der verschiedenen Stellen innerhalb der PKI insgesamt dar. Detailliert werden die Vorgänge der PKI in Kapitel 5 beschrieben.
- Im Verlauf des Piloten sollen weitere Unternehmen und Behörden in die PKI integriert werden. Dort werden in der Regel lokale Registrierungsstellen eingerichtet. Gegebenenfalls kommen außerdem neue Zertifizierungsstellen hinzu. Diese neuen Stellen (Registrierungs- und Zertifizierungsstellen) müssen bestimmte Voraussetzungen erfüllen, um in das bestehende PKI-System eingebunden werden zu können. Die Einrichtung und Einbindung neu hinzukommender PKI-Stellen wird in Kapitel 6 beschrieben.
- Kapitel 7 enthält Definitionen für die hier verwendeten Begriffe, wie sie im Rahmen dieses Organisationshandbuchs zu verstehen sind.
- Kapitel 8 beschreibt die graphische Darstellungsweise.
- Kapitel 9 enthält eine Übersicht über das Formularwesen.
- In Kapitel 10 finden sich Literaturverweise.

3 Aufbauorganisation

3.1 Ziele der PKI in SPHINX

Die Spezifikation und der Aufbau einer Public Key Infrastruktur (PKI) im Projekt SPHINX hat zum Ziel, eine interoperable und praktischen Anforderungen genügende technische und organisatorische Infrastruktur für die Realisierung von Ende-zu-Ende-Sicherheit beim elektronischen Dokumentenaustausch bereitzustellen. Hauptziel des zu realisierenden Systems ist es, gleichermaßen Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit des elektronischen Dokumentenaustauschs (unter Wahrung der Herstellerunabhängigkeit) sicherzustellen.

Dieses Ziel wird in SPHINX durch eine geeignete Public Key Infrastruktur (PKI) erreicht:

- Vertraulichkeit der Ende-zu-Ende-Kommunikation: Es ist für jeden Endanwender möglich, zu jedem anderen aktiven[1] Endanwender innerhalb der PKI ein gültiges Zertifikat zu erhalten, um elektronische Dokumente für diesen zu verschlüsseln.
- Integrität der Ende-zu-Ende-Kommunikation: Es ist für jeden Endanwender möglich, ein elektronisches Dokument zu signieren. Anhand der Signatur und der im Rahmen der PKI bereitgestellten[2] Zertifikate kann jeder andere Endanwender prüfen, ob das Dokument integer ist oder verändert wurde.
- Authentizität der Ende-zu-Ende-Kommunikation: Anhand von Zertifikaten kann jeder Endanwender auf einfache Weise prüfen, ob eine Signatur vom vermuteten Endanwender stammt oder nicht.
- Offene Standards: Die spezifizierte PKI orientiert sich ausschließlich an veröffentlichten Standards. Dies ermöglicht allen Herstellern von Hard- und Software, entsprechende Produkte zu entwickeln und anzubieten.

Die PKI setzt sich aus verschiedenen Komponenten zusammen, die nur im geeigneten Zusammenspiel die oben genannten Ziele gemeinsam erreichen. Der Aufbau und die Abhängigkeiten der einzelnen Komponenten werden in Kapitel 3 beschrieben, die Abläufe in den Kapiteln 4 und 5.

---

1 Die Sonderfälle, in denen Endanwender inaktiv sind, weil sie entweder noch kein Zertifikat erhalten haben oder weil ihr Zertifikat abgelaufen oder gesperrt ist, werden im Rahmen der PKI ebenfalls berücksichtigt und geeignet behandelt.

2 „bereitgestellt“ besagt hier lediglich, daß der öffentliche Schlüssel des Endanwenders im Rahmen der PKI durch Ausstellung eines geeigneten Zertifikats verwendbar gemacht wurde. Ob die Verteilung von Zertifikaten durch Mitsenden mit Dokumenten und/oder durch Abruf von Verzeichnisdiensten erfolgt, ist dabei offengelassen.

3.2 Modell der PKI

3.2.1 Übersicht über das PKI-Gesamtmodell

Folgendes Gliederungsschema liegt dem PKI-Modell zugrunde:

- Die Gesamt-PKI gliedert sich in ***Stellen*** als organisatorische Einheiten (Kapitel 3.2.2).
- Jede Stelle besteht aus einer oder mehreren ***Instanzen*** und stellt über ihre Instanzen *Dienste* zur Verfügung.
- Jeder Dienst wird in Form von ***Aufgaben*** in Arbeitsschritte zergliedert (Kapitel 3.2.3).
- Jeder ***Instanz*** sind die durch sie erbrachten Dienste der Stelle zugeordnet. Die zur Erbringung dieser Dienste erforderlichen Aufgaben werden innerhalb der Instanz von entsprechenden ***Rollen*** *(Kapitel 3.3)* unter Nutzung der technischen und organisatorischen Infrastruktur der instanz-realisierenden ***Stelle*** erbracht.

Die konkrete Zuordnung von Instanzen zu Stellen (und Rollen) erfolgt in der Praxis in der *Umsetzung* des Modells (Kapitel 3.4).

Institutionen bezeichnet im folgenden Organisationseinheiten wie Behörden oder Firmen, die entweder Stellen der PKI realisieren oder denen Endanwender der PKI zugeordnet sind.

3.2.2 Stellen

Eine Stelle ist eine organisatorische Einheit innerhalb einer Institution, die mit Hilfe ihrer Instanzen Dienste der PKI erbringt.

Die Zuweisung von Diensten bzw. Instanzen zu Stellen erfolgt in der Modellumsetzung unter Beachtung der gegebenen Rahmenbedingungen. Folgende Stellen treten typischerweise in einer PKI auf:

Stelle	**Beschreibung**
Zertifizierungsstelle (ZS)	Stelle, die alle PKI-Dienste erbringt.
Registrierungsstelle (RS)	Stelle innerhalb einer Institution, die als organisatorische Schnittstelle der PKI zu den Endanwendern der Institution dient.

Abbildung 2: Typische Stellen einer PKI

Die genannten Stellen erbringen typischerweise folgende Dienste:

Dienst	Stelle	
	Zertifizierungsstelle	Registrierungsstelle
Service für Teilnehmer	X	X
Registrierung[3]	X	X
Zertifizierung	X	
Verzeichnis	X	
Sperrdienst	X	
Namensraumvergabe[4]	X	

Abbildung 3: Stellen und Dienste

3.2.3 Dienste, Instanzen und Aufgaben

Dienste

Dienste sind Leistungen, die innerhalb der PKI für Personen oder PKI-Komponenten erbracht werden.

Innerhalb der PKI, die im Rahmen von SPHINX realisiert ist, werden folgende Dienste erbracht:

Dienst	Beschreibung
Teilnehmer-servicedienst	Dieser Dienst stellt sicher, daß Teilnehmer (z.B. Personen, Endanwender oder Zertifizierungsstellen) mit der PKI in Kontakt treten können, um sich beispielsweise bei der PKI an- oder abzumelden. Der Teilnehmerservicedienst identifiziert Teilnehmer sicher, nimmt u.a. Zertifizierungs- und Sperranträge entgegen und gibt (bei zentraler Schlüsselgenerierung) das PSE an die Teilnehmer aus. Dieser Dienst weist dem Teilnehmer seinen eindeutigen Namen zu (Namensvergabe). Er steht darüberhinaus den ihm zugeordneten Teilnehmern für alle Fragen in Zusammenhang mit der Nutzung der PKI zur Verfügung.
Registrierungsdienst	Personen, die die PKI im Sinne der Ende-zu-Ende-Sicherheit nutzen wollen, müssen sich zunächst als *Teilnehmer registrieren* lassen. Dieser Dienst umfaßt die Erfassung und Verwaltung der Teilnehmerdaten sowie die Archivierung der zugehörigen Originaldokumente. Zusätzlich stellt dieser Dienst die Sperr-Hotline für den ihm zugeordneten Teilnehmerkreis zur Verfügung.

[3] Die Registrierung der Teilnehmer bzw. Endanwender ist hier auf die beiden Stellen verteilt: Die Identifikation des Antragstellers, die Vorprüfung des Antrags und die Namensvergabe wird durch die lokale Registrierungsstelle vorgenommen, die vollständige Antragsprüfung erfolgt durch die Zertifizierungsstelle.

[4] Die Namensraumvergabe wird als interner Dienst der PKI benötigt, um den Teilnehmern eindeutige Namen zuordnen zu können. Der Namensraumvergabedienst braucht nur von einer der Zertifizierungsstellen realisiert werden, die diesen Dienst dann innerhalb der PKI zentral zur Verfügung stellt. Dieser Dienst kann aber auch beispielsweise durch eine eigene Stelle (Namensraumvergabestelle) oder verteilt über die Zertifizierungsstellen realisiert werden.

Dienst	Beschreibung
	Desweiteren bietet der Registrierungsdienst die Möglichkeit der Registrierung lokaler Registrierungsstellen der Institutionen.
Zertifizierungsdienst	Es sind Zertifikate für Teilnehmer zu erstellen, um eine sichere, d.h. integere und authentische Verteilung der öffentlichen Schlüssel der Teilnehmer im Rahmen der PKI sicherzustellen. Dieser Dienst umfaßt weiterhin die Schlüssel- und PSE-Generierung, die Sperrlistenerstellung sowie die Prüfung von Prototypzertifikaten.
Verzeichnisdienst	Der Verzeichnisdienst stellt Teilnehmern, die Zertifikate anderer Teilnehmer benötigen, bzw. sich über den Gültigkeitszustand von Zertifikaten informieren möchten, diese Informationen zur Verfügung. Er veröffentlicht Zertifikate und Sperrlisten.
Sperrdienst	Teilnehmer, die ein Zertifikat sperren lassen möchten, können dies über den Sperrdienst veranlassen. Der Sperrdienst macht Sperrinformationen integer und authentisch verfügbar. Er führt die Sperrung von Zertifikaten aus und erzeugt Sperrlisten.
Namensraum-vergabedienst	Institutionen, die für ihren Teilnehmerkreis die PKI im Sinne von Ende-zu-Ende-Sicherheit nutzbar machen wollen, müssen einen - bis auf Ebene der Teilnehmerinstitution - eindeutigen Namensraum zugeordnet bekommen. Der Namensraumvergabedienst stellt sicher, daß den Institutionen nach Bedarf eindeutige und disjunkte Namensräume zugeordnet werden.

Abbildung 4: Kurzdarstellung von Diensten

Instanzen

Instanzen sind Untereinheiten von Stellen, die durch ihre spezifischen Aufgabenprofile gekennzeichnet sind.

Die Aufgabenprofile der Instanzen sind weitgehend „orthogonal“ zueinander, so daß sie sich wie Bausteine in einem Baukasten für eine PKI darstellen, die relativ frei kombinierbar sind. In jeder Instanz sind Aufgaben spezifiziert, die durch Rollen erbracht werden. Die Instanzen einer Stelle kooperieren miteinander, um insgesamt die von der Stelle zu erbringenden Dienste zu realisieren.

Dieses Konzept erlaubt es, das PKI-Modell einfach zu erweitern oder umzukonfigurieren. Das Modell kann somit leicht auf die spezifischen Anforderungen der Institutionen der PKI angepaßt werden. So ist es beispielsweise möglich, Stellen neu zu definieren und zu integrieren, die lediglich einen speziellen Dienst (z.B. Verzeichnisstelle) innerhalb der PKI realisieren. Ebenso ist die Integration neuer Dienstleistungen innerhalb der PKI durch die Definition und Integration neuer Instanzen möglich (z.B. Zeitstempeldienst).

Folgende Instanzen werden innerhalb der PKI spezifiziert:

Instanz	**realisiert Dienste**
Zertifizierung (Z)	Zertifizierungsdienst, Sperrdienst
Registrierung (R)	Registrierungsdienst
Verzeichnis (V)	Verzeichnisdienst
Teilnehmerservice (TSV)	Teilnehmerservicedienst
Namensraum-vergabe (NRV)	Namensraumvergabedienst

Abbildung 5: Instanzen und Dienste

3.2.3.1 Aufgaben der Instanz Zertifizierung

Der *Zertifizierungsdienst* und der *Sperrdienst* werden im wesentlichen durch die Instanz Zertifizierung erbracht. Dieses impliziert folgende Teilaufgaben für die diese Instanz:

	Aufgaben	**Beschreibung**	**Rollen**[5]
Zertifi-zierungs-dienst	Technische Prüfung des Zertifizierungsauftrags	Der Zertifizierungsauftrag kommt von der Instanz Registrierung und wird technisch insbesondere in folgenden Aspekten geprüft: • Formale Prüfung der Authentizität und Integrität des Auftrags und seiner Anlagen. • Inhaltliche Überprüfung der Angaben und Parameter (z.B. Schlüssellängen).	ZERTV
	Schlüsselprüfung	Wünscht der Teilnehmer „Dezentrale Schlüssel-generierung“, wird das Vorhandensein geeigneter Schlüssel beim Teilnehmer geprüft (z.B. Prüfung der Selbstsignatur des zur Zertifi-zierung vorgelegten Prototypzertifikats gegen den im Prototypzertifikat enthaltenen öffentlichen Schlüssel zur Prüfung der Verfügbarkeit des zugehörigen privaten Schlüssels beim Teilneh-mer).	ZERT1, ZERT2
	Schlüsselgenerierung	Wünscht der Teilnehmer „Zentrale Schlüssel-generierung“, werden Schlüssel (gem. *Policy*) generiert. Es sind dabei die gültigen Parameter für die Schlüsselgenerierung zu beachten.	PS1, PS2
	PSE-Generierung	Wünscht der Teilnehmer „Zentrale Schlüssel-generierung“, wird das zu den Teilnehmer-schlüsseln gehörige PSE erzeugt (z.B. Software-PSE oder Chipkarte). Das PSE ist PIN-geschützt und enthält u.a. die privaten Schlüssel zur Nutzung durch den Teilnehmer.	PS1, PS2

[5] Vorgriff auf Kapitel 3.3 „Rollenmodell“, in dem die hier eingetragenen Rollen definiert werden.

	Aufgaben	Beschreibung	Rollen[5]
	PIN-Brief-Erstellung	Wenn Teilnehmer „Zentrale Schlüsselgenerierung“ wünschen, werden zum PSE passende PINs erzeugt. Die PINs werden vom Teilnehmer benötigt, um das PSE nutzen zu können. Die PINs werden (gem. *Policy)* erstellt und veteilt.	PS1, PS2
	Zertifikaterstellung	Das Zertifikat zum öffentlichen Schlüssel incl. der zusätzlich durch das Zertifikat zuzuordnenden Angaben (gem. *Policy*) wird ausgestellt. Es sind dabei die gültigen Parameter für Zertifikate zu beachten.	ZERT1, ZERT2
	Verteilung von Zertifizierungsergebnissen	Es erfolgt die Verteilung der Ergebnisse und Datenobjekte, die bei der Zertifizierung anfallen (z.B. Zertifizierungsbestätigung, Zertifikat, PSE, PIN-Brief) gem. *Policy*.	ZERTV
Sperrdienst	Technische Prüfung des Sperrauftrags	Der Sperrauftrag kommt von der Instanz Registrierung und wird technisch insbesondere in folgendem Aspekt geprüft: • Formale Prüfung der Authentizität und Integrität des Auftrags und seiner Anlagen.	ZERTV
	Sperrzustand des Zertifikats ändern	Das Zertifikat ist als „gesperrt“ zu markieren.	ZERT1
	Sperrlisten-Erzeugung	Es werden Listen (gem. *Policy*) erstellt und gepflegt, die über den Sperrzustand der Zertifikate der Zertifizierungsstelle Aufschluß geben. Es sind dabei die gültigen Parameter für Sperrlisten zu beachten.	ZERT1
	Verteilung der Sperrinformation	Sperrlisten sind zeitnah zu veröffentlichen. Daher sind die Sperrlisten zeitnah dem Verzeichnis zur Veröffentlichung zu übermitteln.	ZERTV

Abbildung 6: Dienste, Aufgaben und Rollen der Instanz Zertifizierung

Folgende Aufgaben, die keinem einzelnen Dienst direkt zuzuordnen sind, sind ebenfalls von der Zertifizierung zu erbringen:

Aufgaben	Beschreibung	Rollen[6]
Kommunikation und Vorgangsabwicklung mit angrenzenden Instanzen	Alle Vorgänge, Dokumente und Datenobjekte (z.B. Zertifizierungsauftrag und Protoypzertifikat), die von anderen Instanzen empfangen werden, sind geeignet formal zu prüfen. Diese Prüfung umfaßt u.a. die mathematische Prüfung auf Integrität und Authentizität. Alle Vorgänge, Dokumente und Datenobjekte, die an andere Instanzen übermittelt werden, sind geeignet aufzubereiten und zu schützen.	ZERTV
Beschaffung und Bereitstellung von PSE-Leermaterial	Es ist sicherzustellen, daß ausreichend Leermaterial für die PSE-Generierung bereitsteht (z.B. nichtpersonalisierte Chipkarten).	ZERTV

[6] Vorgriff auf Kapitel 3.3 „Rollenmodell“, in dem die hier eingetragenen Rollen definiert werden.

Aufgaben	Beschreibung	Rollen[6]
Protokollierung	Alle im Rahmen der Zertifizierung durchgeführten Aufgaben sind geeignet zu protokollieren.	betroffene Rollen

Abbildung 7: Weitere Aufgaben und Rollen der Instanz Zertifizierung

Sonderaufgaben der Instanz Zertifizierung einer Zertifizierungsstelle, die als Wurzel-Zertifizierungsstelle betrieben wird

Innerhalb der PKI muß eine Zertifizierungsstelle als Wurzel-Zertifizierungsstelle betrieben werden. Diese hat einige besondere Aufgaben, u.a. das Erstellen der Wurzelzertifikate. Die Sonderaufgaben müssen vom Leiter der Wurzel-Zertifizierungsstelle explizit vorbereitet und unter seiner Aufsicht durchgeführt werden und können nicht allein an Mitarbeiter der Wurzel-Zertifizierungsstelle delegiert werden.

	Aufgaben	Beschreibung	Rollen[7]
Wurzel-Zertifizierung	Erzeugen eines Wurzel-Zertifikats	Der öffentliche Schlüssel der Wurzel-Zertifizierungsinstanz wird von sich selbst zertifiziert. Dieser Vorgang umfaßt u.a. die Schlüssel- und die PSE-Generierung. Die Wurzelzertifizierung muß geeignet protokolliert werden. Hinweis: Um die Integrität und Authentitzität des Wurzelzertifikats für Dritte überprüfbar zu machen, muß entsprechendes *Wurzel-Prüfmaterial* erzeugt und veteilt werden.	LZS u.a.
	Erzeugen von Wurzel-Prüfmaterial zum Wurzelzertifikat (z.B. Fingerprint)	Im Rahmen der Wurzelzertifizierung wird geeignetes Prüfmaterial erzeugt. Dieses wird z.B. auf Papier ausgedruckt (Wahl eines „anderen Mediums“ als das Zertifikatsmedium). Dieses Prüfmaterial kann z.B. ein „Fingerprint“ der Wurzelzertifikate sein.	LZS u.a.
	Verteilung des Wurzelzertifikats und des Wurzel-Prüfmaterials	Das Wurzelzertifikat und das Wurzel-Prüfmaterial wird allen Teilnehmern und sonstigen Personen und Institutionen auf integere Weise zur Verfügung gestellt.	ZERTV

Abbildung 8: Dienste, Aufgaben und Rollen der Instanz Zertifizierung im Rahmen der Wurzelzertifizierung

3.2.3.2 Aufgaben der Instanz Registrierung

Der *Registrierungsdienst* wird durch die Instanz Registrierung mit folgenden Teilaufgaben erbracht:

	Aufgaben	Beschreibung	Rollen[8]
Registrierungsdienst für	Formales und inhaltliches Prüfen von Zertifizierungsanträgen	Der Zertifizierungsantrag kommt von der Instanz Teilnehmerservice und wird formal wie inhaltlich	REG

[7] Vorgriff auf Kapitel 3.3 „Rollenmodell“, in dem die hier eingetragenen Rollen definiert werden.

[8] Vorgriff auf Kapitel 3.3 „Rollenmodell“, in dem die hier eingetragenen Rollen definiert werden.

	Aufgaben	Beschreibung	Rollen[8]
Teilnehmer (Endanwender, Zertifizierungsstellen)		geprüft: • Formale Prüfung der Authentizität und Integrität des Antrags und seiner Anlagen. • Inhaltliche Prüfung der Angaben und Parameter (z.B. Schlüssellängen).	
	Pflege der Teilnehmerdatenbank	Sämtliche Teilnehmer der Zertifizierungsstelle sind in einer Teilnehmerdatenbank zu pflegen. Dazu gehören die Stammdaten der Teilnehmer sowie der Status zu ihren Zertifikaten.	REG
	Archivierung der Originaldokumente	Dokumente in Papierform und Dokumente in elektronischer Form sind geeignet zu archivieren (u.a. Zertifizierungsanträge sind in Papierform im Original zur Beweissicherung zu archivieren).	REG
Sperrdienst	Sperrhotline für Teilnehmer	Entgegennahme, Prüfung und Bearbeitung von Sperranträgen durch Teilnehmer.	REG

Abbildung 9: Dienste, Aufgaben und Rollen der Instanz Registrierung

Der Registrierungsdienst leistet mit der *Registrierung und Betreuung Lokaler Registrierungsstellen* (in der Institution angesiedelte Instanz Teilnehmerservice) neben seinen eigentlichen PKI-Aufgaben noch Aufgaben im Aufbau der PKI.

	Aufgaben	Beschreibung	Rollen[9]
Registrierungsdienst für Teilnehmerservice-Instanzen	Formales und inhaltliches Prüfen von Anträgen für die Einrichtung einer Instanz Teilnehmerservice	Der Antrag auf Einrichtung einer Teilnehmerservice-Instanz wird formal wie inhaltlich geprüft: • Formale Prüfung der Authentizität und Integrität des Antrags und seiner Anlagen. • Inhaltliche Prüfung der Angaben.	REG
	Namensraum-Vergabe für Instanz Teilnehmerservice	Die Registrierungsstelle beantragt einen geeigneten Namensraum bei der Instanz Namensraumvergabe und ordnet diesen Namensraum der Instanz Teilnehmerservice zur Namensvergabe mit (gem. *Policy)*.	REG

Abbildung 10: Dienst, Aufgaben und Rollen der Instanz Registrierung im Rahmen des Aufbaus der PKI

Folgende Aufgaben, die keinem einzelnen Dienst direkt zuzuordnen sind, sind ebenfalls von der Zertifizierung zu erbringen:

Aufgaben	Beschreibung	Rollen[10]

[9] Vorgriff auf Kapitel 3.3 „Rollenmodell“, in dem die hier eingetragenen Rollen definiert werden.

[10] Vorgriff auf Kapitel 3.3 „Rollenmodell“, in dem die hier eingetragenen Rollen definiert werden.

Aufgaben	Beschreibung	Rollen[10]
Kommunikation und Vorgangs-abwicklung mit angrenzenden Instanzen	Alle Vorgänge, Dokumente und Datenobjekte (z.B. Zertifizierungsantrag und PSE), die von anderen Instanzen empfangen werden, sind geeignet formal zu prüfen. Diese Prüfung umfaßt u.a. die mathematische Prüfung auf Integrität und Authentizität. Alle Vorgänge, Dokumente und Datenobjekte (z.B. PSE und PIN-Brief), die an andere Instanzen übermittelt werden, sind geeignet aufzubereiten und zu schützen.	REG
Protokollierung	Alle im Rahmen der Registrierung durchgeführten Aufgaben sind geeignet zu protokollieren.	REG

Abbildung 11: Weitere Aufgaben und Rollen der Instanz Registrierung

3.2.3.3 Aufgaben der Instanz Verzeichnis

Der *Verzeichnisdienst* der Zertifizierungsstelle wird im wesentlichen durch die Instanz Verzeichnis erbracht. Dieses impliziert folgende Teilaufgaben für die diese Instanz:

	Aufgaben	Beschreibung	Rollen[11]
Verzeich-nisdienst	Erstellung und Pflege von Teil-nehmereinträgen im Verzeichnis	Für jeden Teilnehmer ist ein Eintrag im Verzeich-nis vorzunehmen, in das Zertifikate und ggfs. Sperrlisten eingetragen werden können.	VERP
	Pflege von Zertifikatsinforma-tionen im Verzeichnis	Es sind Zertifikate und Sperrlisten gem. *Policy* in das Verzeichnis einzupflegen (Einstellen und Aktualisieren von Zertifikaten, Einstellen und Aktualisieren von Sperrlisten).	VERP

Abbildung 12: Dienste, Aufgaben und Rollen der Instanz Verzeichnis

Folgende Aufgaben, die keinem einzelnen Dienst direkt zuzuordnen sind, sind ebenfalls von der Zertifizierung zu erbringen:

Aufgaben	Beschreibung	Rollen[12]
Kommunikation und Vorgangs-abwicklung mit angrenzenden Instanzen	Alle Vorgänge und Dokumente, die von anderen Instanzen empfangen werden, sind geeignet formal zu prüfen. Diese Prüfung umfaßt u.a. die mathematische Prüfung auf Integrität und Authentizität. Alle Vorgänge und Dokumente, die an andere Instanzen übermittelt werden, sind geeignet aufzubereiten und zu schützen.	VERP
Protokollierung	Alle im Rahmen im Verzeichnis durchgeführten Aufgaben sind geeignet zu protokollieren.	VERP

Abbildung 13: Weitere Aufgaben und Rollen der Instanz Verzeichnis

[11] Vorgriff auf Kapitel 3.3 „Rollenmodell“, in dem die hier eingetragenen Rollen definiert werden.

[12] Vorgriff auf Kapitel 3.3 „Rollenmodell“, in dem die hier eingetragenen Rollen definiert werden.

3.2.3.4 Aufgaben der Instanz Teilnehmerservice

Der *Teilnehmerservicedienst* wird durch die Instanz *Teilnehmerservice* erbracht. Dieses impliziert folgende Teilaufgaben für diese Instanz:

	Aufgaben	**Beschreibung**	**Rollen**[13]
Teil-nehmer-service-dienst	Kommunikation und Vorgangs-abwicklung mit den Teilnehmern	Der Teilnehmerservice stellt die organisatorische Schnittstelle der PKI zum Teilnehmer dar. Neben der Vorgangsabwickung muß hier Support-dienstleistung für die Teilnehmer zur Verfügung gestellt werden.	SERV
	Sichere Teilnehmeridentifikation	Teilnehmer sind eindeutig und sicher zu identifi-zieren (gem. *Policy*).	TID1, TID2
	Entgegennahme von Anträgen	Anträge (z.B. Teilnahme- und Zertifizierungs-anträge) sind entgegenzunehmen und zu prüfen.	SERV
	Sperrhotline für Teilnehmer und autorisierte Personen	Teilnehmer können Eigensperrungen, autorisierte Personen Fremdsperrungen von Zertifikaten vornehmen lassen (gem. *Policy*).	SERV
	Namensvergabe für Teilnehmer	Festlegung des Teilnehmernamens auf der Basis des ihr zugewiesenen Namensraums.	SERV

Abbildung 14: Dienst, Aufgaben und Rollen der Instanz Teilnehmerservice

Folgende Aufgaben, die keinem einzelnen Dienst direkt zuzuordnen sind, sind ebenfalls vom Teilnehmerservice zu erbringen:

Aufgaben	**Beschreibung**	**Rollen**[14]
Kommunikation und Vorgangs-abwicklung mit angrenzenden Instanzen	Alle Vorgänge und Dokumente, die von anderen Instanzen empfangen werden, sind geeignet formal zu prüfen. Diese Prüfung umfaßt u.a. die mathematische Prüfung auf Integrität und Authentizität. Alle Vorgänge und Dokumente, die an andere Instanzen über-mittelt werden, sind geeignet aufzubereiten und zu schützen.	SERV
Protokollierung	Alle im Rahmen des Teilnehmerservice durchgeführten Aufgaben sind geeignet zu protokollieren.	betroffene Rollen

Abbildung 15: Weitere Aufgaben und Rollen der Instanz Teilnehmerservice

3.2.3.5 Aufgaben der Instanz Namensraumvergabe

Der *Namensraumvergabedienst* wird durch die Instanz *Namensraumvergabe* erbracht. Dieses impliziert folgende Teilaufgaben für diese Instanz:

	Aufgaben	**Beschreibung**	**Rollen**[15]

[13] Vorgriff auf Kapitel 3.3 „Rollenmodell“, in dem die hier eingetragenen Rollen definiert werden.

[14] Vorgriff auf Kapitel 3.3 „Rollenmodell“, in dem die hier eingetragenen Rollen definiert werden.

	Aufgaben	Beschreibung	Rollen[15]
Namens-raumver-gabe-dienst	Namensraumvergabe	Die Instanz Namensraumvergabe vergibt Namensräume an Instanzen Teilnehmerservice oder Unternamensräume an Instanzen Namensraumvergabe. Dabei müssen folgende Restriktionen beachtet werden (gem. *Policy*): • Alle Instanzen Namensraum sind untereinander hierarchisch organisiert (Ausnahme nur, wenn es nur eine einzige Instanz Namensraumvergabe gibt). • Einer Instanz Namensraumvergabe wird (durch eine übergeordnete Instanz Namensraumvergabe) ein Namensraum vergeben, den diese verwaltet (Ausnahme bei der Wurzelzertifizierungsstelle). Der zugewiesene Namensraum darf nicht verletzt werden. • Die Instanz Namensraumvergabe muß sicherstellen, daß die Namensvergabe innerhalb ihres Namensraums kollisionsfrei ist (d.h. im Gesamtnamensraum dürfen Namensräume bzw. Namen nicht mehrfach vorkommen).	BNRV

Abbildung 16: Dienst, Aufgabe und Rolle der Instanz Namensraumvergabe

Hinweis zur Umsetzung im SPHINX: Innerhalb der PKI muß eine Instanz Namensraumvergabe realisiert werden, die als *Namensraumwurzel* den gesamten Namensraum verwaltet. Diese kann weitere Unterinstanzen Namensraum bestimmen, die hierarchisch organisiert sind.

Hinweis zur Nutzung bestehender externer Namensraumvergabe-Einrichtungen: Es ist möglich, bereits bestehende Einrichtungen zur Namensraumvergabe zu nutzen. Beispielsweise kann die Namensraumvergabe der Bundesbehörden durch die bereits bestehende X.400-Namensvergabe extern erbracht werden. Sollen externe Namensraumvergabe-Einrichtungen in SPHINX integriert werden, müssen diese sich verpflichten, die in der *Policy* aufgeführten Teilnahmevoraussetzungen zu erfüllen.

Hinweis zu internen und externen Namensraumvergabe-Einrichtungen: Instanzen zur Namensraumvergabe können sowohl PKI-intern (z.B. als Teil einer Zertifizierungsstelle oder als eigenständige Namensraumstelle) oder extern (z.B. die Nutzung bereits bestehender Einrichtungen für Namensraumvergabe) realisiert werden.

Folgende Aufgaben, die keinem einzelnen Dienst direkt zuzuordnen sind, sind ebenfalls von der Namensraumvergabe zu erbringen:

Aufgaben	Beschreibung	Rollen[16]
Kommunikation und Vorgangsabwicklung mit angrenzenden Instanzen	Alle Vorgänge und Dokumente, die von anderen Instanzen empfangen werden, sind geeignet formal zu prüfen. Diese Prüfung umfaßt u.a. die mathematische Prüfung auf Integrität und Authentizität.	BNRV

[15] Vorgriff auf Kapitel 3.3 „Rollenmodell“, in dem die hier eingetragenen Rollen definiert werden.

[16] Vorgriff auf Kapitel 3.3 „Rollenmodell“, in dem die hier eingetragenen Rollen definiert werden.

Aufgaben	Beschreibung	Rollen[16]
	Alle Vorgänge und Dokumente, die an andere Instanzen übermittelt werden, sind geeignet aufzubereiten und zu schützen.	
Protokollierung	Alle im Rahmen der Namensraumvergabe durchgeführten Aufgaben sind geeignet zu protokollieren.	BNRV

Abbildung 17: Weitere Aufgaben und Rollen der Instanz Namensraumvergabe

3.3 Das Rollenmodell

3.3.1 Von der Rollenspezifikation zur Personalbemessung

Rollenspezifikation

Eine Rolle stellt eine Bündelung inhaltlich oder organisatorisch zusammengehörender Aufgaben dar, die typischerweise von einer Person oder einer Gruppe von Personen bearbeitet werden. Die Beschreibung der Rolle abstrahiert dabei von der konkreten Person, die die Rolle übernimmt. Rollen werden bei der Zerlegung einer Gesamtaufgabe oder im Zusammenhang mit der Aufgabenverteilung bei Abläufen definiert. Die Aufgaben einer Rolle dürfen sich nicht widersprechen. Einer Person werden typischerweise eine oder mehrere Rollen zugewiesen.

Es lassen sich „spezifische“ und „begleitende“ Rollen identifizieren:

- Eine **spezifische Rolle** wird eigens für die Stelle besetzt (z.B. der Verantwortliche für die Zertifizierungsstelle). Hier können administrative und operative Rollen unterschieden werden:
  - **Operative Rollen** sind direkt in die Abläufen der Stelle integriert.
  - **Administrative Rollen** sind nicht in die Abläufe der Stelle integriert. Sie sind für die spezifischen administrativen Tätigkeiten in der Stelle verantwortlich.
- Eine **begleitende Rolle** ist unabhängig von der Stelle besetzt (z.B. Datenschutzbeauftragter). Sie ist in der Regel bereits innerhalb der Institution besetzt und ist bei Bedarf von der Stelle in Anspruch zu nehmen.

Funktionstrennung

Rollen werden Personen zugeordnet. Dabei sind Restriktionen bzgl. der Funktionstrennung zu beachten. Rollen können zueinander unverträglich sein. Bei Unverträglichkeit von Rollen dürfen diese nicht einer Person zugeordnet werden. Miteinander verträgliche Rollen sind auf eine Person abbildbar.

Um die Funktionstrennung übersichtlich darzustellen, werden alle Rollenkombinationen betrachtet und tabellarisch dargestellt:

	Rolle A	Rolle B	Rolle C
Rolle A		o	
Rolle B	o		x
Rolle C		x	

Abbildung 18: Beispiel der Funktionstrennung von Rollen

- **Obligatorische Funktionstrennung:** Wenn eine Rolle mit einer anderen Rolle unverträglich ist, wird dieses mit **x** dargestellt. In diesem Fall dürfen diese beiden Rollen nicht einer Person zugeordnet werden.
- **Empfohlene Funktionstrennung:** Das Zeichen **o** wird in der Tabelle verwendet, wenn eine Funktionstrennung *empfohlen* wird. In diesem Falle sollten - müssen aber nicht - die Rollen verschiedenen Personen zugeordnet werden. Es sind bei der Fortschreibung des Rollenmodells allerdings möglich, daß die Empfehlungen in verbindliche Vorgaben abgeändert werden.

- Bei den übrigen Rollenkombinationen (leere Felder) ist eine **Funktionstrennung nicht erforderlich**.

Rollenzuweisung

Die Rollen können nun - unter Berücksichtigung der obligatorischen und empfohlenen Funktionstrennung - *Mitarbeitern* zugeordnet werden. *Mitarbeiter* sind natürliche *Personen*, die in einer oder mehreren Rolle agieren.

Die Rollenzuweisung kann tabellarisch erfolgen:

	Rolle A	Rolle B	Rolle C
Mitarbeiter 1	X		X
Mitarbeiter 2		X	

Abbildung 19: Beispiel einer Rollenzuweisung unter Berücksichtigung der Funktionstrennung

Bei dieser Rollenzuweisung sind weitere Rahmenbedingungen zu beachten (Personalbemessung).

Personalbemessung

Dieses Organisationshandbuch stellt die notwendigen Informationen zur Rollenspezifikation, zur Funktionstrennung und zur Rollenzuweisung zur Verfügung. Das Rollenmodell läßt sich damit als Basis für die Personalbemessung einer Stelle verwenden. Dabei sind neben der Funktionstrennung weitere Rahmenbedingungen zu beachten.

Die Rahmenbedingungen, die für die Stelle gelten sollen, sind anhand einer Schätzung mehrerer Faktoren zu präzisieren.

Zu diesen Faktoren gehören:

- Stellenspezifische Festlegungen und Abschätzungen
    - Welche Dienste sollen von der Stelle zur Verfügung gestellt werden?
    - Bereitschaft der Dienste (z.B. Sperrdienst: 8 oder 24 Stunden am Tag verfügbar?)
    - Erwartete Menge an Vorgängen (z.B. niedrige oder hohe Anzahl an Zertifizierungen zu erwarten?)
    - Läuft der Betrieb kontinuierlich durch oder sind besondere Leistungsspitzen zu erwarten?
    - Einflüsse der verschiedene „Policies (Ist z.B. eine stündliche, tägliche oder wöchentliche Bereitstellung von Sperrlisten erforderlich?)
- Tarifliche Bestimmungen (z.B. Mitarbeiter-Arbeitszeitregelungen).
- Betriebliche Bestimmungen (z.B. Vertretungsregelungen).
- Eingesetzte Technik (Rationalisierung).

Unter Berücksichtigung dieser und weiterer relevanten Größen ist eine Bestimmung des benötigten Personalbedarfs und -profils einer Stelle möglich.

3.3.2 Rollenspezifikation

Die folgende Tabelle zeigt die Rollen auf, die für den Betrieb der einzelnen Instanzen benötigt werden[17]. Es werden sowohl die begleitenden als auch die spezifischen Rollen dargestellt.

3.3.2.1 Begleitende Rollen

Rolle	Abk.	Beschreibung der Aufgaben
IT-Sicherheits-Beauftragter	ITSB	Der IT-Sicherheitsbeauftragte ist gesamtverantwortlich für die Sicherheit in der zugeordneten Stelle. Insbesondere hat er folgende Aufgaben zu erfüllen: • Erstellung, Umsetzung und Fortschreibung des Sicherheits-konzepts • Administration der Zutritts- und Zugangsberechtigungen • Durchführung von Schulungsmaßnahmen und Übungen • Gewährleistung der IT-Sicherheit im laufenden Betrieb (z.B. durch regelmäßige Kontrolle und Fortschreibung der Sicher-heitsmaßnahmen) • Untersuchung sicherheitsrelevanter Vorgänge
Revisor	RV	Überprüft regelmäßig die Aktivitäten in der zugeordneten Stelle. Er kontrolliert die ordnungsgemäße Umsetzung und Beachtung des Sicherheitskonzepts und weiterer relevanter Vorschriften.
Datenschutz-beauftragter	DSB	Kontrolle über die Einhaltung der Datenschutzbestimmungen in der zugeordneten Stelle. Seine Funktion ist die Kontrolle der Verarbeitung personenbezogener Daten. Er schult darüberhinaus die Mitarbeiter der Zertifizierungsstelle und verpflicht sie auf die Einhaltung des Datengeheimnisses.
Beauftragter für den Technischen Dienst	BTD	Der technische Dienst ist für Aufbau, Pflege und Instandhaltung der technischen und der baulichen Infrastruktur zuständig.
Beauftragter für das Notfallmanagement	BNM	Er erstellt das Notfallkonzept und setzt dieses um. Er erstellt Notfallpläne und führt Notfallübungen durch. Er überprüft die praktische Umsetzung des Notfallkonzepts.
Administrator	ADM1	Richtet die Hard- und Softwareplattform ein und betreut diese. Dieses umfaßt neben der allgemeinen Administration auch die Benutzerverwaltung.
Co-Administrator	ADM2	*Aufgaben identisch mit Aufgaben von ADM1.*
Beauftragter für die Eigenverwaltung	BEV	Er ist verantwortlich für die Eigenverwaltung der Stelle. Dieses betrifft u.a. folgende Aspekte: Beschaffung, Raumzuweisung, Personalbewirtschaftung, Öffentlichkeitsarbeit und Marketing

Abbildung 20: Begleitende Rollen

[17] Das vorliegende Rollenmodell stellt eine Empfehlung dar, von dem bei konkreten Bedarf im Einzelfall (entsprechend begründet und unter Wahrung des Sicherheitsniveaus und in Absprache mit dem PKI-Projektleitung) abgewichen werden kann. Ein Beispiel hierfür wäre das Abweichen vom Vier-Augen-Prinzip bei einem Arbeitsschritt.

3.3.2.2 Stellenspezifische administrative Rollen

Rolle	Abk.	Beschreibung der Aufgaben
Leiter der Zertifizierungsstelle	LZS	Er plant und koordiniert die Aktivitäten der Zertifizierungsstelle gesamtverantwortlich. Der Leiter der Zertifizierungsstelle ist neben dem Betrieb auch für die Einrichtung bzw. die Einstellung der Zertifizierungsstelle verantwortlich.
Organisatorischer Ansprechpartner	OA	Er ist gesamtverantwortlich für die Einrichtung und den Betrieb der Lokalen Registrierungsstelle. Er übernimmt die Planung und Koordination der Arbeiten und überwacht diese.
Beauftragter für das Kryptomanagement	BKM	Er plant und koordiniert den Einsatz der kryptographischen Methoden und Technologien. Er meldet sicherheitsrelevante Vorgänge dem IT-Sicherheits-Beauftragten. Diese Rolle wird in der Regel in der Zertifizierungsstelle besetzt.

Abbildung 21: Stellenspezifische, administrative Rollen

3.3.2.3 Operative Rollen der Instanz Zertifizierung

Rolle	Abk.	Beschreibung der Aufgaben
Beauftragter für die Zertifizierungsvor- und -nachbereitung	ZERTV	• Vorgangsabwicklung mit angrenzenden Instanzen • Formale und inhaltliche Prüfung eingehender Dokumente • Beschaffung und Bereitstellung von PSE-Leermaterial
Personalisierer[18]	PS1	• Generiert Schlüssel • PSE-Generierung • PIN-Brief-Erstellung
Co-Personalisierer	PS2	• *Aufgaben identisch mit Aufgaben von PS1.*
Zertifizierer	ZERT1	• Zertifiziert Schlüssel • Zertifikatssperrung • Sperrlisten-Erstellung
Co-Zertifizierer	ZERT2	*Aufgaben identisch mit Aufgaben von ZERT1.*

Abbildung 22: Operative Rollen der Instanz Zertifizierung

3.3.2.4 Operative Rolle der Instanz Registrierung

Rolle	Abk.	Beschreibung der Aufgaben
Registrator	REG	• Vorgangsabwicklung mit angrenzenden Instanzen • Sperrhotline für die Teilnehmer • Formale und inhaltliche Prüfung eingehender Dokumente

[18] Bei „dezentraler Schlüsselgenerierung“ erfolgt Schlüsselgenerierung und PSE-Generierung durch den Teilnehmer selbst und nicht durch den Personalisierer. Die PIN-Brief-Erstellung erübrigt sich dann.

Rolle	Abk.	Beschreibung der Aufgaben
		• Vorgangsbearbeitung • PIN-Brief-Versand an Teilnehmer • Pflege des Teilnehmerdatenbestands (incl. Archivierung von Originaldokumenten)

Abbildung 23: Operative Rolle der Instanz Registrierung

3.3.2.5 Operative Rolle der Instanz Verzeichnis

Rolle	Abk.	Beschreibung der Aufgaben
Verzeichnispfleger	VERP	• Vorgangsabwicklung mit angrenzenden Instanzen • Pflege der Teilnehmer-Grunddaten (Eintrag in Verzeichnis) • zeitnahes Einstellen von Zertifikaten • Zeitnahes Einstellen von Sperrlisten

Abbildung 24: Operative Rollen der Instanz Verzeichnis

3.3.2.6 Operative Rollen der Instanz Teilnehmerservice

Rolle	Abk.	Beschreibung der Aufgaben

Teilnehmerservice-mitarbeiter	SERV	• Ansprechpartner für die Teilnehmer (Beachte: Teilnehmer können sowohl *Endanwender*, als auch *Zertifizierungsstellen* sein)
		• Vorgangsabwicklung mit angrenzenden Instanzen
		• Formale und inhaltliche Antrags- und Dokumentenprüfung (Vorprüfung im Rahmen der Registrierung)
		• Prüfung der Teilnahmevoraussetzungen (Beachte, wenn Teilnehmer = *Zertifizierungsstelle*: Dann muß hier u.a. die erfolgreiche Prüfung des Sicherheitskonzepts nachgewiesen werden)
		• Wenn Teilnehmer = *Endanwender*:
		  • Vergabe des eindeutigen Teilnehmernamens (Namensvergabe)
		• Wenn Teilnehmer = *Zertifizierungsstelle*:
		  • Namensraumvergabe

Beauftragter für die Teilnehmeridentifi-kation	TID1	• Sichere Identifikation des Teilnehmers.
Co-Beauftragter für die Teilnehmeridentifi-kation	TID2	*Aufgaben identisch mit Aufgaben von TID1.*

Abbildung 25: Operative Rollen der Instanz Teilnehmerservice

3.3.2.7 Operative Rolle der Instanz Namensraumvergabe

Die Namensraumvergabestelle sorgt letztendlich dafür, daß innerhalb der PKI jeder Teilnehmer anhand seines Namens eindeutig identifizierbar ist.

Rolle	Abk.	Beschreibung der Aufgaben
Beauftragter für die Namensraumvergabe	BNRV	• Legt Namensräume gem. *Policy* fest. • Vorgangsabwicklung mit angrenzenden Instanzen.

Abbildung 26: Operative Rolle der Instanz Namensraumvergabe

3.3.2.8 Rollen in der Institution

Es sind weiterhin folgende Rollen innerhalb der PKI relevant:

- **Endanwender**
- **Autorisierte Person**

Rolle	Abk.	Beschreibung der Aufgaben
Endanwender	EA	• Nutzt die PKI im Sinne Ende-zu-Ende-Sicherheit für elektronischen Dokumentenaustauschs. • Kann Eigensperrungen veranlassen. **Hinweis:** Auch Mitarbeiter in einer Zertifizierungsstelle agieren in der Rolle des „Endanwenders“.
Autorisierte Person	AP	Person in der Institution, die Fremdsperrungen von Endanwendern veranlassen kann. Die Autorisierte Person muß nicht Teilnehmer sein.

Abbildung 27: Rollen in der Institution

3.3.3 Funktionstrennung der Rollen

Für die Rollen ist folgende Funktionstrennung zu beachten:

	LZS	BKM	OA	ITSB	RV	DSB	BTD	BNM	ADM1	ADM2	BEV	ZERTV	PS1	PS2	ZERT1	ZERT2	REG	VERP	SERV	TID1	TID2	BNRV	EA	AP
LZS					x	x																		
BKM					x																			
OA					x																			
ITSB					x																			
RV	x	x	x	x			x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		
DSB	x						x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x		
BTD					x	x																		
BNM					x	x																		
ADM1					x	x				o														
ADM2					x	x			o															
BEV					x	x																		
ZERTV					x	x											x		o					
PS1					x	x								o	o	o								
PS2					x	x							o		o	o								
ZERT1					x	x							o	o		o								
ZERT2					x	x							o	o	o									
REG					x	x						x												
VERP					x	x																		
SERV					x	x						o												
TID1					x	x															o			
TID2					x	x														o				
BNRV					x	x																		
EA																								
AP																								

Legende:

- x Funktionstrennung obligatorisch
- o Funktionstrennung empfohlen

In allen übrigen Fällen ist eine Funktionstrennung nicht erforderlich.

Abbildung 28: Funktionstrennung der Rollen

Begründung für die Funktionstrennung

Rolle 1	Rolle 2	Begründung für Funktionstrennung
RV	alle anderen Rollen (außer: DSB)	Der Revisor überprüft die Aktivitäten in der Stelle[19]. Dieses schließt aus, daß er selbst eine weitere begleitende oder spezifische Tätigkeit für die Stelle ausübt. Ausnahme: Der Revisor kann zusätzlich die Rolle des Datenschutzbeauftragten übernehmen, da beides die Stelle überprüfende Rollen sind.
DSB	alle anderen Rollen (außer: RV, ITSB und BKM)	Der Datenschutzbeauftragte (DSB) überprüft die Einhaltung der Datenschutzbestimmungen in der Stelle. Dieses schließt aus, daß er selbst eine weitere begleitende oder spezifische Tätigkeit in der Stelle ausübt. Ausnahme 1: Der Datenschutzbeauftragte kann die Rolle des IT-Sicherheitsbeauftragten (ITSB) übernehmen, da sich beiden Rollen auf zueinander disjunkte Aufsichtsbereiche beziehen. Ausnahme 2: Der Datenschutzbeauftragte kann die Rolle des Beauftragten für das Kryptomanagement (BKM) übernehmen, da die Bereiche „Kryptomanagement“ und „Kontrolle der Verarbeitung personenbezogener Daten“ inhaltlich disjunkt zueinander sind und daher keine Rollenkonflikte zu erwarten sind. Ausnahme 3: Zur Verträglichkeit der beiden Rollen DSB und RV: Siehe zur Verträglichkeitsbegründung bei RV.
ADM1	ADM2	Es wird empfohlen, das Vier-Augen-Prinzip bei der Administration durchzusetzen, da der Eingriff in die technische Infrastruktur eine sicherheitsrelevante Tätigkeit darstellen kann. Jeder Veränderung der technischen Infrastruktur kann sicherheitstechnische Veränderungen nach sich ziehen.
PS1	PS2	Es wird empfohlen, das Vier-Augen-Prinzip bei der Personalisierung durchzusetzen, da dieses eine sicherheitsrelevante Tätigkeit darstellt.
ZERT1	ZERT2	Es wird empfohlen, das Vier-Augen-Prinzip bei der Zertifizierung durchzusetzen, da dieses eine sicherheitsrelevante Tätigkeit darstellt.
PSx	ZERTx	Es wird empfohlen, Personalisierung und Zertifizierung zu trennen, wenn das verwendete CA-Produkt keine integrierte Personalisierung/Zertifizierung erlaubt. Der Zertifizierer sollte in diesem Fall icht über die PSE verfügen können.
REG	ZERTV	Durch diese Funktionstrennung wird das Vier-Augen-Prinzip vor und nach der Zertifizierung durchgesetzt. Dieses ist notwendig, um sicherzustellen, daß ausschließlich zulässige Zertifikate erstellt werden können (es dürfen nur Zertifikate erstellt werden, die auf einem gültigen Zertifizierungsantrag basieren).
SERV	ZERTV	Es wird empfohlen, eine Funktionstrennung zwischen dem Teilnehmerservice- und dem Zertifizierungsbereich durch-

[19] Stelle kann z.B. eine Zertifizierungsstelle oder eine Registrierungsstelle sein.

Rolle 1	Rolle 2	Begründung für Funktionstrennung
		zuführen, um Manipulationen auf der gesamten organisatorischen Kette sicher zu unterbinden (6-Augen-Prinzip). Da mindestens eine 4-Augen-Kontrolle des Gesamtvorgangs (Funktionstrennung zwischen REG und ZERTV) gewährleistet ist, auch wenn diese beiden Rollen nicht getrennt würden, wird die Funktionstrennung nicht obligatorisch vorgeschrieben.
TID1	TID2	Die sichere Identifikation eines Teilnehmers stellt die Grundlage des PKI-Systems dar und muß *stets sicher* erfolgen. Daher wird empfohlen, bei dieser Aufgabe das Vier-Augen-Prinzip zu beachten.

Abbildung 29: Begründung der Funktionstrennung der Rollen

3.4

Bei der Umsetzung des PKI- und des Rollenmodells sind die spezifischen Rahmenbedingungen und Anforderungen des Anwendungskontextes zu beachten – sie kann daher sehr

Im Pilotprojekt SPHINX werden Annahmen getroffen, die die Ausgestaltung der PKI vereinfachen. Die Zuordnung der abstrakten Instanzen zu konkreten Betreiberinstitutionen ist daher

Bei einer möglichen Umsetzungs-Fortschreibung der PKI wird diese einfache Struktur entsprechend erweitert werden müssen, da ggf. geänderte Rahmenbedingungen zu beachten sind (siehe Kapitel 3.4.2). Dieses gilt grundsätzlich auch für eine Umsetzung in den Produktivbetrieb.

3.4.1 Umsetzung in SPHINX

3.4.1.1 Zertifizierungshierarchie in SPHINX

Die Zertifizierungshierarchie ist in SPHINX dreistufig angelegt:

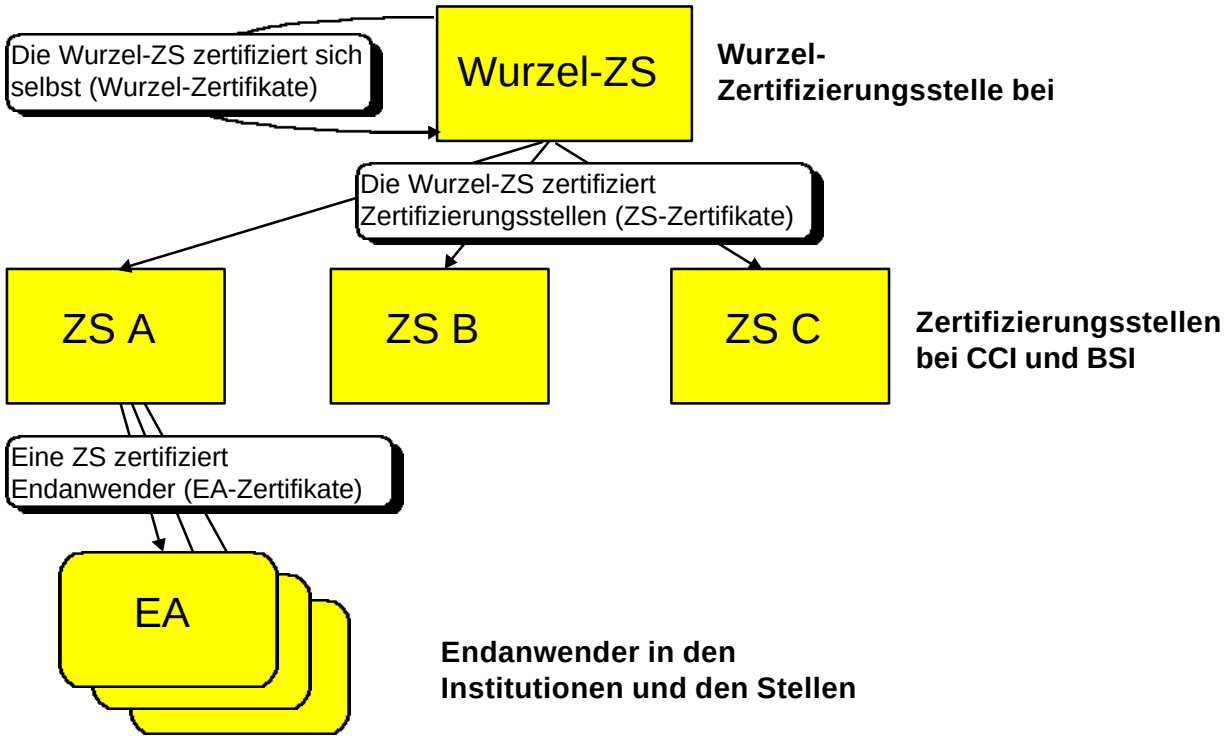
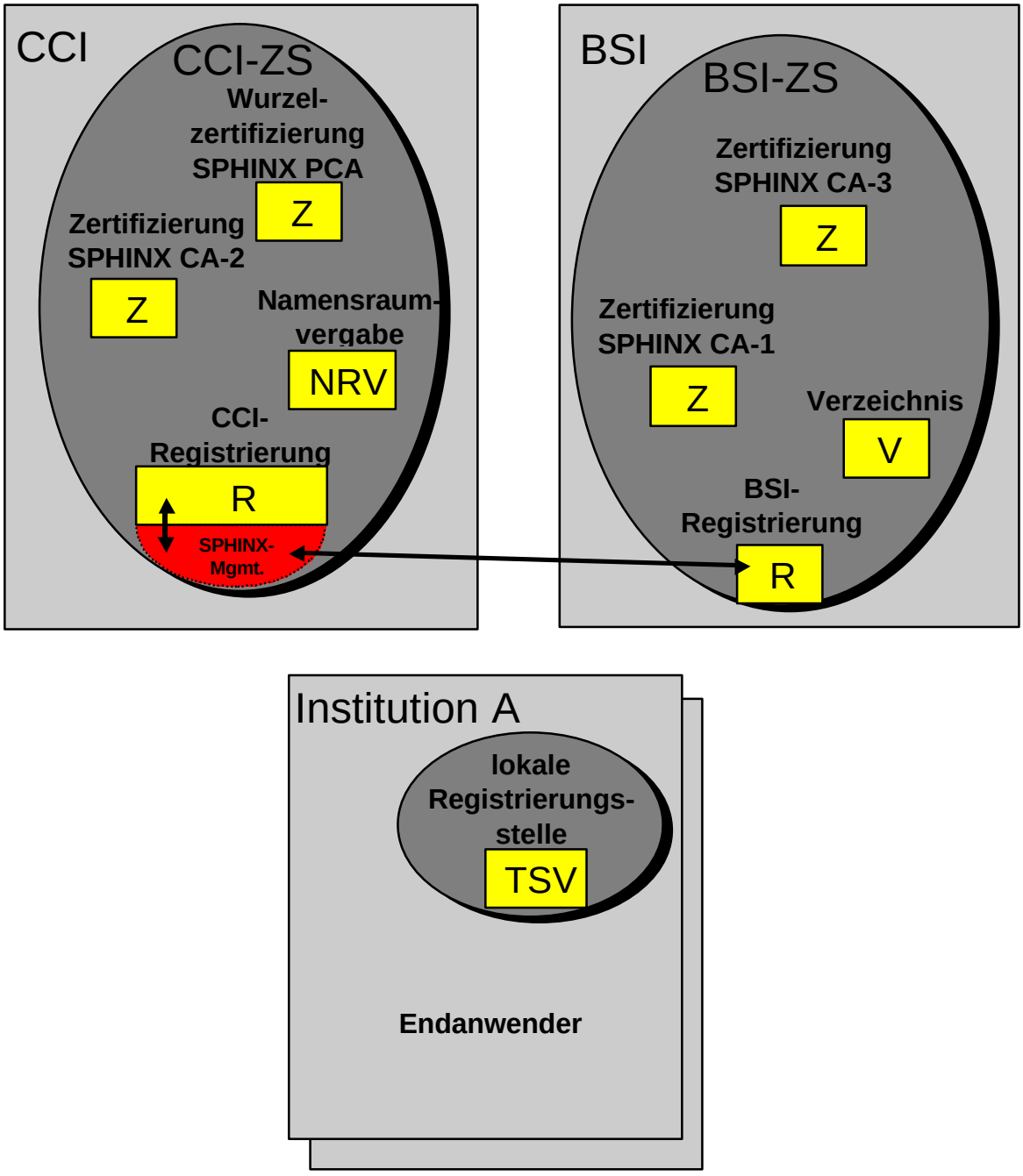


Abbildung 30: Zertifizierungshierarchie in SPHINX

3.4.1.2 Stellen und Rollen in SPHINX



Schema 1: Stellen und Instanzenverteilung im Pilotprojekt SPHINX

CCI-Zertifizierungsstelle (CCI-ZS)

Die CCI-Zertifizierungsstelle unterscheidet sich in wesentlichen Punkten von der Modellvorstellung einer Zertifizierungsstelle:

- Die CCI-Zertifizierungsstelle realisiert sowohl Wurzelzertifizierungsstelle als auch eine Zertifizierungsstelle innerhalb einer organisatorischen Einheit.
- Sie stellt selbst kein Verzeichnisdienst zur Verfügung sondern nutzt dazu den Verzeichnisdienst der BSI-Zertifizierungsstelle.
- Sie stellt eine zusätzliche, projektspezifische Instanz zum SPHINX-Projektmanagement zur Verfügung.

Instanz	**Beschreibung der Aufgaben**
Wurzel-Zertifizierung	Die Wurzel-Zertifizierung[20] SPHINX PCA stellt die Wurzel der PKI dar. Sie zertifiziert die drei Zertifizierungsinstanzen SPHINX CA-1, SPHINX CA-2 und SPHINX CA-3.
Zertifizierung A	Die Zertifizierung SPHINX CA-2 zertifiziert Endanwender.
CCI-Registrierung	Die CCI-Registrierung erbringt die Registrierung für die Wurzel-Zertifizierung SPHINX PCA sowie für die Zertifizierung SPHINX CA-1.
SPHINX-MGMT	SPHINX-MGMT übernimmt zwei projektspezifische Aufgaben: • Projektmanagement-Datenpflege: Dazu werden von allen Instanzen Daten an diese Instanz übermittelt. • Zwischenglied zwischen Registrierungsstellen und Zertifizierungsstellen. ***Hinweis:*** *Diese Instanz ist projektspezifisch und gehört nicht zur originären PKI.*

Abbildung 31: Instanzen der CCI-Zertifizierungsstelle

BSI-Zertifizierungsstelle (BSI-ZS)

Die BSI-Zertifizierungsstelle unterscheidet sich in wesentlichen Punkten von der Modellvorstellung einer Zertifizierungsstelle:

- Die BSI-Zertifizierungsstelle realisiert zwei Zertifizierungsstellen.
- Sie stellt einen zentralen Verzeichnisdienst für alle Zertifizierungsstellen zur Verfügung.

[20] Wenn hier von „Zertifizierungen“ die Rede ist, sind stets *modellhaft* die Zertifizierungs*instanzen* innerhalb einer Stelle (z.B. der *BSI*- oder *CCI-Zertifizierungsstelle*) gemeint.

Instanz	Beschreibung der Aufgaben
Zertifizierung SPHINX CA-1	Die Zertifizierung SPHINX CA-1 zertifiziert Endanwender.
Zertifizierung SPHINX CA-3	Die Zertifizierung SPHINX CA-3 zertifiziert Endanwender.
Verzeichnis	Das zentrale Verzeichnis bedient die Wurzel-Zertifizierung SPHINX PCA und die Zertifizierungen SPHINX CA-1, SPHINX CA-2 und SPHINX CA-3
BSI-Registrierung	Die BSI-Registrierung erbringt die Registrierung für die Zertifizierungen SPHINX CA-1 und SPHINX CA-3.

Abbildung 32: Instanzen der BSI-Zertifizierungsstelle

Registrierungsstellen (RS)

Die Registrierungsstellen unterscheidet sich nicht von der PKI-Modellvorstellung.

Begründung der wichtigsten Umsetzungsentscheidungen in SPHINX Phase II

Es gibt zwei Gründe, Einzelentscheidungen bzgl. der Umsetzung des Modells zu begründen:

- Abweichung vom Modell
- Wahl einer Option innerhalb des Modell

Beide Gründe treffen bei der Umsetzung des Modells in SPHINX Phase 2 zu und werden im folgenden erläutert:

a) Zusätzliche Instanz SPHINX-MGMT in der CCI-Zertifizierungsstelle

Eine Besonderheit im Piloten stellt die zusätzliche Instanz SPHINX-MGMT bei der CCI-Zertifizierungsstelle dar. Diese Instanz ist projektspezifisch und wird im Produktivbetrieb ersatzlos entfallen. Die Instanz übernimmt zum einen die Zuordnung zwischen Registrierungsstellen und Zertifizierungsstellen, sowie die projektspezifische Datenbankpflege (d.h. von den Daten, die lediglich zur Auswertung vom Projektverlauf - und nicht für den Betrieb der PKI - benötigt werden).

Überlicherweise wählt eine Institution ihre Zertifizierungsstelle selbst aus („selbstbestimmte“ Zuordnung). Diese Zuordnung erfolgt im Projekt SPHINX aber nicht selbstbestimmt, sondern projektgesteuert, um innerhalb des Projektes eine gleichmäßige Verteilung der Endanwenderprodukte bei den Endanwendern zu erreichen (es soll kein Endanwenderprodukt bevorzugt oder benachteiligt werden können). Da die (technische) Interoperabilität zwischen den Endanwenderprodukten und den Zertifizierungsprodukten der Zertifizierungsstellen nicht immer gegebeben ist, impliziert die projektgesteuerte Zuordnung von Endanwenderprodukten die projektgesteuerte (d.h. fremdbestimmte) Zuordnung. Um diese „fremdbestimmte“ Zuordnung gegenüber den Registrierungsstellen bzw. den Endanwendern zu vereinfachen, wird innerhalb des Projektes mit der Instanz SPHINX-MGMT nur eine Anlaufstelle aller Registrierungsstellen realisiert. Diese übernimmt die Vermittlung zwischen Registrierungsstellen und zugeordneter Zertifizierungsstellen.

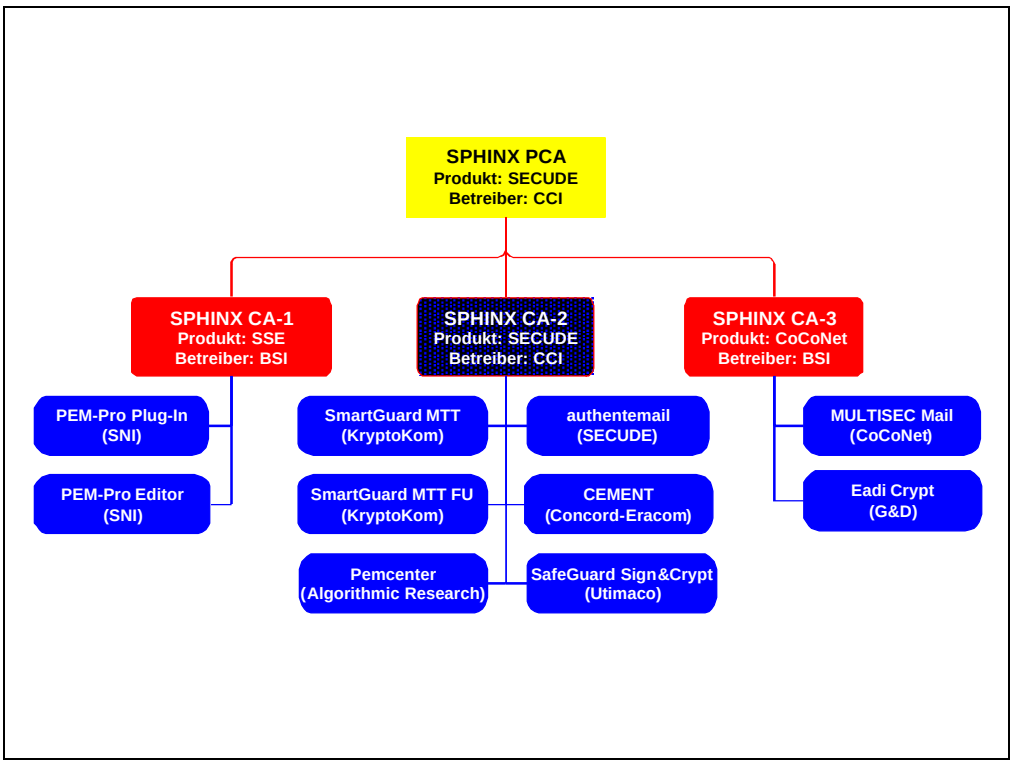


Abbildung 33: Zuordnung von Endanwenderprodukten zu Zertifizierungsstellen in SPHINX

Für die praktische Tätigkeit der einzelnen Institution ist dies ohne Belang, da auf jeden Fall (im Pilot- als auch im Produktivbetrieb) jede Registrierungsstelle genau einer Zertifizierungsstelle zugeordnet ist. Eine mögliche Umstellung auf den Produktivbetrieb zeichnet sich durch den Wegfall der Instanz SPHINX-MGMT aus:

- Für die Institution stellt dieses kein Problem dar, da die Zuordnung der Registrierungstelle zu genau einer Zertifizierungsstelle stets gegeben ist. Es ändert sich für sie lediglich, daß die Zertifizierungsstelle dann direkt zu adressieren ist - Art und Inhalt der Kommunikation ändert sich nicht.
- Die Zertifizierungsstelle selbst hat ebenfalls keine Umstellungsprobleme duch den Wegfall der Instanz, da die Kommunikation nun unmittelbar mit den Registrierungsstellen erfolgt, die sie auch vorher schon (mittelbar) betreut hat.
- Der projektspezifische Anteil der von CCI betreuten Datenbank (PDB, Projektdatenbank) wird bei einem möglichen Übergang vom Pilot- in den Produktivbetrieb ersatzlos entfallen.

b) Zentrales Verzeichnis in der BSI-Zertifizierungsstelle:

Eine weitere Besonderheit ist die zentrale Stellung des Verzeichnisdienstes beim BSI. Nach dem Modell verfügt jede Zertifizierungsstelle über ein eigenes Verzeichnis (eine Veröffentlichung von Zertifikaten und Sperrlisten soll ausschließlich für den eigenen Endanwenderkreis erfolgen). Aus organisatorischen Gründen wurde im Piloten für alle Zertifizierungsstellen gemeinsam ein zentrales Verzeichnis eingerichtet.

Der Wegfall des zentralen Verzeichnisses und der Aufbau von Einzelverzeichnissen hat folgende Auswirkungen auf die betroffenen Stellen:

- Für den einzelnen Endanwender ist dieses von Bedeutung, da bzgl. dem Umgang mit Zertifikaten anstatt nur einem Verzeichnisdienst dann stets mehrere Verzeichnisdienste zu berücksichtigen sind.
- Für die Zertifizierungsstellen hat dieses Auswirkungen, da die Einzelverzeichnisse aller Zertifizierungsstelle geeignet technisch und organisatorisch von den Zertifizierungsstellen koordiniert werden müßten. Diese Koordination betrifft sowohl die Einrichtung (u.a. die Strukturierung des Verzeichnisschemas) als auch den Betrieb (Soll z.B. eine Anfrageweiterleitung erfolgen?) der Einzelverzeichnisse.

c) Multi-Zertifizierung innerhalb einer Zertifizierungsstelle

Jede der beiden Zertifizierungsstellen stellt mehrere Instanzen zur Zertifizierung bereit:

- Die CCI-Zertifizierungsstelle stellt sowohl die Wurzel-Zertifizierung als auch eine Zertifizierung zur Verfügung.
- Die BSI-Zertifizierungsstelle stellt zwei Zertifizierungen zur Verfügung.

Aus pragmatischen Gründen ist im Projekt SPHINX der Aufbau und der Betrieb von 4 eigenständigen Zertifizierungsstellen nicht erwünscht.

d) Keine Teilnahme von Einzel-Endanwendern möglich

Es können ausschließlich Endanwender in Institutionen, die über eine Registrierungsstelle verfügen, teilnehmen. Einzel-Endanwender können nicht teilnehmen.

Dieses ist problemlos, da das Modell diese Variante zuläßt.

3.4.2 Fortschreibung der Umsetzung in SPHINX

Die Fortschreibung der Umsetzung des PKI-Modells in SPHINX wird *kontinuierlich* erfolgen. Der in Kapitel 3.4.1 beschriebene Status (SPHINX Phase 2) dient als Ausgangspunkt für die notwendige Fortschreibung.

Folgende Beispiele deuten an, in welche Richtung sich die PKI-Architektur verändern kann:

- Der Übergang von MailTrusT V.1.1 nach V.2.0, unter Berücksichtigung des unter allen Beteiligten abgestimmten Tailorings.
- Das Einbinden weiterer Zertifizierungsstellen.
- Das Einbinden von Endanwendern, die keiner Teilnehmerinstitution zugeordnet werden können.
- Projektinterne Veränderungen (z.B. eine neue Aufgabenverteilung unter den Betreiberinstitutionen).
- Reduktion der Modellabweichungen, die bisher bestehen (z.B. Eliminierung der Instanz SPHINX-MGMT)
- Änderungen in der Zertifizierungshierarchie (z.B. Erweiterung um eine Hierarchieebene).
- Änderungen in der Namenshierarchie (z.B. Kopplung der Namenshierarchie an die Zertifizierungshierarchie).
- Annäherung an Anforderungen des Signaturgesetzes und der Signaturverordnung.
- Erhöhung der faktischen Sicherheit in Technik, Organisation und Infrastruktur.

Diese Beispiele zeigen, wie groß die Gestaltungsspielräume sind. Ein konkreter Entwurf für eine geeignete PKI-Architektur kann daher erst erfolgen, wenn dessen Ziele und Rahmenbedingungen unter allen Beteiligten abgestimmt worden sind.

3.5 Formulare und Datenobjekte

Zwischen und innerhalb von Stellen und Instanzen werden Formulare und Datenobjekte ausgetauscht. Die konkreten Formulare sind in den Betriebshandbüchern, die konkreten Datenobjekte in der Spezifikation „Technische Grundlagen“ festgelegt. An dieser Stelle soll auf ihre grundlegenden Aspekte eingegangen werden, soweit diese für die globale Ablauforganisation von Bedeutung sind.

- Formulare: Ein Formular legt einen Datensatz logisch fest, der zwischen Instanzen ausgetauscht wird.
- Datenobjekte: Datenblock mit einer genau spezifizierten Struktur und Bedeutung.

3.5.1 Formulare

Um Vorgänge innerhalb der PKI abzuwickeln, sind Informationen strukturiert zwischen den beteiligten Stellen und Instanzen auszutauschen. Die benötigten Daten werden durch Formulare definiert. Es werden folgende Grundarten von Formularen verwendet:

- **Papierformulare**: Es gibt für jede Stelle bzw. Instanz einen Satz Papier-Formulare.
- **Elektronische Formulare**: Es gibt einen Satz von Formularen, die elektronisch verfügbar sind. Diese sind elektronisch über die definierten Schnittstellen zu versenden. Es werden folgende Datenformate verwendet: ASCII, WORD, RTF. Zulässig sind darüberhinaus elektronische Formulare, die z.B. eine geeignet gesicherte Online-Registrierung mittels WWW-Browser ermöglichen (*Policy*).

Grundsätzlich gilt: Alle Formulare sind zu unterschreiben: Papierformulare mit Unterschrift, elektronische Formulare mit individueller digitaler Signatur (unter Verwendung eines EA-Zertifikats). Wenn die Übertragung elektronischer Dokumente auf andere geeignete Weise gesichert sind, kann ggf. auf eine individuelle digitale Signatur verzichtet werden (siehe *Policy*).

Hinweis: Die wesentlichen Formulare sind in den Anhängen dieses Organisationshandbuchs und der Betriebshandbücher enthalten.

3.5.2 Datenobjekte

Hinweis: Alle Datenobjekte werden in dem Spezifikationsdokument „Technische Grundlagen“ ([TechGru]) ausreichend spezifiziert.

3.5.2.1 Zertifikate

Es gibt verschiedene Arten von Zertifikaten innerhalb der PKI, die zwar die gleiche Datenstruktur besitzen, aber verschiedene Aufgaben haben:

- **Wurzel-Zertifikat (W-Z)**: Wurzel-Zertifikat der PKI. Es dient dazu, Zertifizierungsstellen zu verifizieren. Dieses Zertifikat ist mit dem zugehörigen *eigenen* privaten

Signierschlüssel signiert (sog. *Selbstzertifikat*). Es bildet den *Sicherungsanker* im Rahmen der Gültigkeitsprüfung entlang der *Zertifikatskette*.

- **Zertifizierungsstellen-Zertifikat (ZS-Z)**: Es dient dazu, Teilnehmer (i.d.R. Endanwender, aber auch untergeordnete Zertifizierungsstellen) zu verifizieren.
- **Endanwender-Zertifikat (EA-Z)**: Persönliches Zertifikat eines Endanwenders. Es dient dazu, einem Endanwender den Aufbau einer gesicherten Ende-zu-Ende-Kommunikation zu einem anderen Endanwender zu ermöglichen. Die Mitarbeiter innerhalb der PKI besitzen ebenfalls EA-Zertifikate und müssen diese zur gesicherten Kommunikation einsetzen.

Zertifikate dieser drei Arten können zusammen eine **Zertifikatskette** bilden: EA-Z ($\rightarrow$ ZS-Z $\rightarrow$ ... $\rightarrow$ ZS-Z) $\rightarrow$ W-Z .

Daneben existiert folgendes Spezialzertifikat:

- **Prototypzertifikat:** Im Falle der dezentralen Schlüsselgenerierung erstellt der Teilnehmer ein selbsterzeugtes (selbstsigniertes) Zertifikat, das er zusammen mit seinem Zertifizierungsantrag einreicht. Es enthält u.a. Angaben zur Person und zum verwendeten öffentlichen Schlüssel. Darüberhinaus erlaubt das Prototypzertifikat den Stellen und Instanzen der PKI zu verifizieren, ob der Teilnehmer tatsächlich im Besitz des privaten Schlüssels ist, der zum - im Prototypzertifikat enthaltenen - öffentlichen Schlüssels paßt (*Proof of Possession*). Nur in diesem Falle darf die (Wurzel-)Zertifi-zierungsstelle ein Zertifikat (EA- oder ZS-Zertifikat) erstellen.

3.5.2.2 Sperrlisten

Eine wichtige Rolle innerhalb der PKI spielen die Sperrlisten. Diese enthalten Informationen über den Gültigkeitszustand von nicht abgelaufenen Zertifikaten. Die Erstellung der Sperrlisten erfolgt gemäß der für die PKI gültigen *Policy*.

Es sind folgende Sperrlisten innerhalb der PKI realisiert:

- **Wurzel-Sperrliste** (ARL, Authority Revocation List): Enthält Sperrinformationen zu allen von der Wurzel-Zertifizierungsstelle herausgegebenen Zertifikaten (ZS- und WZS-Zertifikate). Die Wurzel-Sperrliste wird von der Wurzel-Zertifizierungsstelle heraus-gegeben und in ihrem Verzeichnisdienst veröffentlicht.
- **Sperrliste** (CRL, Certificate Revocation List): Enthält Sperrinformationen zu Zertifikaten einer Zertifizierungsstelle (EA- und ggf. ZS-Zertifikate). Jede Zertifizierungsstelle gibt eine eigene Sperrliste über ihren eigenen Teilnehmerkreis (Endanwender oder Zertifizierungsstellen) heraus und veröffentlicht diese in einem Verzeichnis.

3.5.2.3 PSE

Zur sicheren Aufbewahung und Nutzung u.a. des privaten Schlüssels ist ein *PSE* (das Personal Security Environment) - auch gelegentlich Token genannt - für den Teilnehmer erforderlich. Im Falle der dezentralen Schlüsselgenerierung wird das PSE durch den Teilnehmer selbst, im Falle der zentralen Schlüsselgenerierung durch die zertifizierende Zertifizierungsstelle erzeugt. Das PSE wird z.B. in Form einer Datei auf Diskette oder in Form einer Chipkarte zur Verfügung gestellt.

3.5.2.4 Fingerprint Wurzel-Zertifikat

Auf vertrauenswürdigem Weg allen Teilnehmern der PKI zur Verfügung gestellte Information, die die Prüfung des Wurzel-Zertifikats auf Integrität und Authentizität erlaubt (*Wurzel-Prüfmaterial*).

3.5.2.5 PIN-Brief

Im Falle der zentralen Schlüsselgenerierung wird in der Zertifizierungsstelle eine zum PSE gehörende Persönliche Identifikationsnummer (PIN) erzeugt und dem Teilnehmer schriftlich – durch den vertraulichen PIN-Brief – auf sichere Weise zugestellt.

3.5.2.6 Protokolle

Jede Instanz hat über ihre Tätigkeit „revisionssicher“ Protokoll zu führen.

Dafür steht ein Satz Protokollformulare zur Verfügung (diese befinden sich als Anlagen in den Betriebshandbüchern). Einträge in Protokollen werden i.d.R. mit Handzeichen des bearbeitenden Mitarbeiters gezeichnet.

Nach Möglichkeit sind die Protokollierungsfunktionen u.a. der Zertifizierungsprodukte und Betriebssysteme zu nutzen. Diese Protokolle sollten manipulationssicher (auf jeden Fall zugriffsgesichert, möglichst auch integrationsgesichert) sein. Je nach Nutzungsprofil der verwendeten maschinengestützten automatischen Protokollierung kann -die manuell geführte Protokollierung verringert werden.

3.5.3 Nutzung der Datenstrukturen durch Stellen und Instanzen

	(W)Z	Z	V	R	TSV	EA
Papier-formulare					X	X
Elektr. Formulare	X	X	X	X	X	X
Wurzel-Zertifikat	E	L, P	V	VW		L, P
ZS-Zertifikat	E		V			L, P
EA-Zertifikat		E	V			L, P
Prototyp-Zertifikat		P			(P)	E
Wurzel-Sperrliste	E		V			L, P
Sperrliste		E	V			L, P
PSE für EA		E				N
PSE für WZS	E, N					
PSE für ZS	E	N				
PIN-Brief EA		E				L
Fingerprint Wurzel-Zertifikat	E	L	L	L	L	L
Protokoll	E	E	E	E	E	

Abbildung 34: Zuordnungsmatrix: Instanz – Datenobjekt

Legende:

Abk.	Bedeutung	Beschreibung
E	Erstellen	Anlegen eines Formulars etc.
L	Lesen	Kenntnisnahme einer Information
N	Nutzen	Anwenden
P	Prüfen	Überprüfen einer Datei auf Integrität und Authentizität
V	Veröffentlichen	Auf öffentlich zugänglichem System bereitstellen
VW	Vertrauenswürdig Weiterreichen	Der Empfänger kann davon ausgehen, daß eine Datei integer und authentisch ist, da die ausgebende Stelle / Instanz vertrauens-würdig ist.
X	Allgemeine Nutzung	Nutzung

4 Instanzübergreifende Ablauforganisation

Dieses Kapitel beschreibt instanzübergreifende Abläufe innerhalb der PKI und schlägt damit die Brücke zwischen dem Modell und Aufbau der PKI gemäß Kapitel 3 und den konkreten Arbeitsschritten, die innerhalb der einzelnen Instanzendurch die Mitarbeiter in den Stellen auszuführen sind.

Hinweis: In diesem Kapitel werden der Einfachheit halber alle für die Zertifizierung relevanten Instanzen (d.h. *alle* Instanzen des PKI-Modells aus Kapitel 3.2) innerhalb einer *Zertifizierungsstelle* angesiedelt (dieses beinhaltet hier auch die Instanzen TSV der lokalen Registrierungsstellen). Werden Instanzen anders auf organisatorische Einheiten verteilt, beschränkt dieses nicht die Allgemeingültigkeit der hier gemachten Aussagen, wenn nur die Verbindungen zwischen den Instanzen untereinander beibehalten werden.

Die Instanzen des PKI-Modells (siehe Kapitel 3.2) sind geeignet zu verbinden, um eine in sich geschlossene PKI zu erhalten:

- Die Verbindungen zwischen den Instanzen innerhalb *einer* Zertifizierungsstelle setzt diese so in Beziehung, daß sie alle Dienste der Zertifizierungsstelle zur Verfügung stellen kann.
- Die Zertifizierungshierarchie setzt die verschiedenen Zertifizierungsstellen *untereinander* in eine Beziehung, sodaß sich hieraus die Gesamt-Architektur der PKI ergibt.

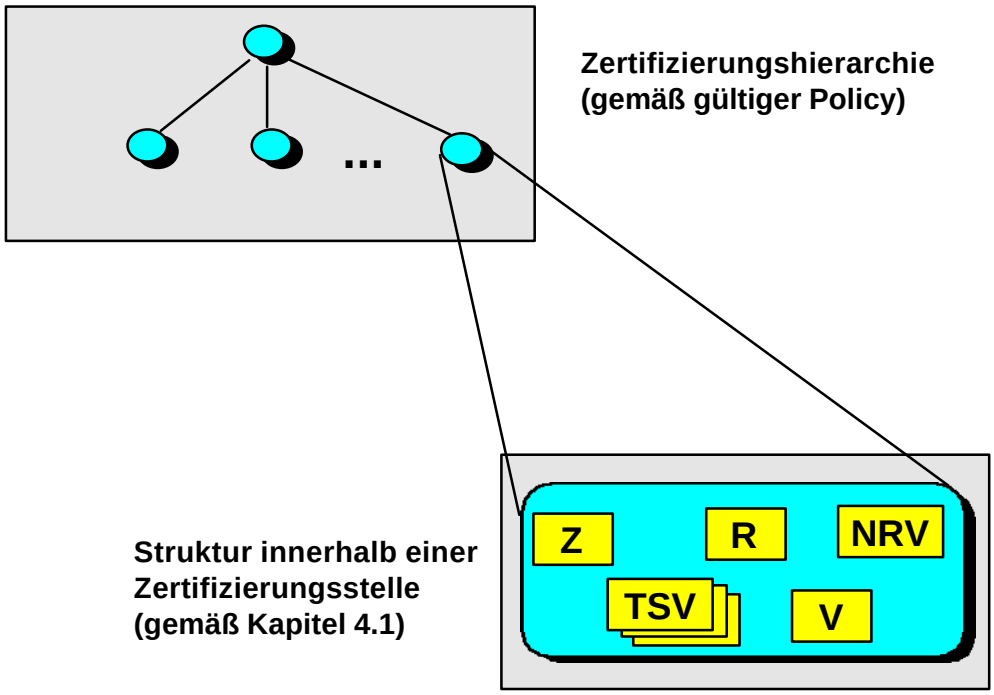


Abbildung 35: Von der einzelnen Instanz zur Zertifizierungshierarchie

In Kapitel 4.1 werden die Instanzen innerhalb der einzelnen Zertifizierungsstelle in Beziehung zueinander gesetzt. Die Zertifizierungshierarchie ergibt sich kanonisch daraus (Verhältnis von „Zertifizierungsstelle zu Teilnehmer“, wobei dann Zertifizierungsstellen die Teilnehmer einer hierarchisch übergeordneten Zertifizierungsstelle sind.). In Kapitel 4.2 werden - auf der in

Kapitel 4.1 entwickelten Kommunikationsstruktur - die Abläufe skizziert, wie sie für die Kernaufgaben vorgesehen sind.

Eine Zertifizierungsstelle besitzt folgende *vier Kernaufgaben*:

1. **Teilnehmerregistrierung**: Innerhalb der PKI wird der organisatorische Rahmen für den einzelnen Teilnehmer geschaffen[21].
2. **Teilnehmerzertifizierung**: Ein Teilnehmer kann zertifiziert werden.
3. **Zertifikatssperrung**: Zertifikate können gesperrt werden.
4. **Registrierung lokaler Registrierungsstellen**: Eine Zertifizierungsstelle hat neue Lokale Registrierungsstellen zu registrieren.

Für jede dieser Kernaufgaben werden in den Kapiteln 4.2.1 - 4.2.4 die Abläufe instanzenübergreifend wie folgt dargestellt:

- Es werden die Schnittstellen und Datenobjekte skizziert, die sich zwischen den Instanzen ergeben.
- Die Aufgaben in den einzelnen Instanzen werden unter ablauflogischen Gesichtspunkten inhaltlich skizziert.
- Dabei wird in der Beschreibungsskizze der Abläufe jeweils auf die Basisvorgänge (siehe Kapitel 5, „instanzspezifischen Ablauforganisation“) referenziert.

4.1 Schnittstellen innerhalb einer Zertifizierungsstelle

Das in Kapitel 3 entwickelte PKI-Modell stellt Bausteine zum Aufbau einer PKI - die Instanzen - zur Verfügung. In diesem Kapitel werden diese Bausteine nun untereinander in Beziehung gesetzt - es werden Schnittstellen zwischen den Instanzen spezifiziert.

Folgende Instanzen (siehe Kapitel 3.2) sind dabei in Beziehung zu setzen:

Instanz	**Beschreibung der grundlegenden Aufgaben**
Zertifizierung (Z)	Leistet die eigentliche Zertifizierung (Zertifikats- und Sperrlistengenerierung, Schlüssel- und PSE-Generierung).
Registrierung (R)	Registrierung der Teilnehmer der Zertifizierungsstelle.
Verzeichnis (V)	Veröffentlicht Zertifikate und Sperrlisten bzgl. zertifizierter Teilnehmer.
Teilnehmerservice (TSV)	Pflegt den Kontakt zu den Teilnehmern (Endanwender, Zertifizierungsstellen), identifiziert diese sicher und führt die Vorprüfung von Anträgen durch. Es können mehrere Instanzen *Teilnehmerservice* realisiert sein (jew. einer Institution als lokale Registrierungsstelle zugeordnet). Die Instanz *Teilnehmerservice*, die bei der Zertifizierungsstelle selbst eingerichtet ist, ist für die Endanwender inner-

[21] Die organisatorische Trennung der Vorgänge *Registrierung* und *Zertifizierung* ist innerhalb der PKI sinnvoll, da diese sehr verschiedene Aufgabenbereiche betreffen. Der einzelne Teilnehmer kann natürlich bei der (Erst-)Antragstellung beide Vorgänge gemeinsam veranlassen (Details hierzu im Hinweis in Kapitel 4.2.2).

Instanz	Beschreibung der grundlegenden Aufgaben
	halb der eigenen Zertifizierungsstelle zuständig. Diese interne Instanz betreut darüberhinaus Institutionen bei der Einrichtung eigener Registrierungs-stellen. Hinweis: Innerhalb der Zertifizierungsstelle selbst ist eine Instanz *Teilnehmerservice* eingerichtet. Die weiteren Instanzen *Teilnehmerservice* sind i.d.R. extern in den lokalen Registrierungsstellen der Institutionen eingerichtet.
Namensraumvergabe (NRV)	Jede Instanz *Teilnehmerservice* muß einen geeigneten Namensraum zugewiesen bekommen. Auf dieser Basis können die Instanzen TSV den Teilnehmer eindeutige Teil-nehmernamen zuordnen.

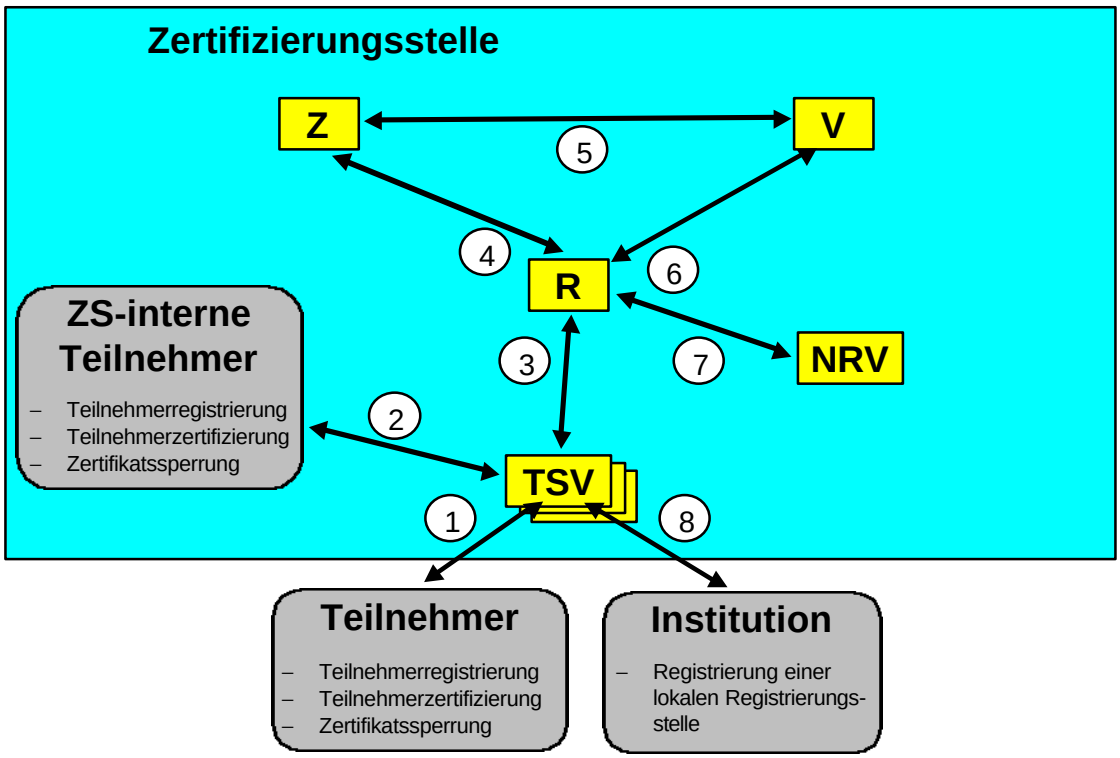


Abbildung 36: Instanzen und Schnittstellen einer Zertifizierungsstelle

Alle Instanzen bilden gemeinsam eine Einheit - Nur wenn diese geeignet zusammenwirken, können die Ziele der PKI erreicht werden. Die Instanzen können dabei nicht beliebig miteinander in Beziehung gesetzt werden. Eine sinnvolle Kommunikationsstruktur der Instanzen wird in der vorangehenden Abbildung dargestellt, die im folgenden kurz begründet wird.

Nr.	Schnittstelle	Begründung für die Einrichtung der Schnittstelle
1	Teilnehmerservice - *Teilnehmer*	Jede Zertifizierungsstelle hat (*externe) Teilnehmer*, die sie zertifiziert (dieses ist letztendlich das Ziel jeder Zertifizierungsstelle). Die Kommunikation zum *Teilnehmer* und seine organisato-

Nr.	Schnittstelle	Begründung für die Einrichtung der Schnittstelle
		rische Betreuung erfolgt durch die Instanz *Teilnehmer-service* (TSV). Es können auch mehrere Instanzen *Teilnehmerservice* innerhalb der Zertifizierungsstelle realisiert sein, die jeweils einen eigenen Teilnehmerkreis betreuen.
2	Teilnehmerservice - *ZS-interne Teilnehmer*	Jede Zertifizierungsstelle hat *ZS-interne Teilnehmer (die eigenen Mitarbeiter)*, die sie zertifiziert. Die Kommunikation zum *internen Teilnehmer* und seine organisatorische Betreuung erfolgt durch die Instanz *Teilnehmerservice* (TSV), die innerhalb der Zertifizierungsstelle selbst eingerichtet ist.
3	Teilnehmerservice - Registrierung	Die Instanz(en) *Teilnehmerservice* werden durch die zentrale Instanz *Registrierung* betreut. Die *Registrierung* stellt ihre zentrale organisatorische Schnittstelle zur Zertifizierungsstelle dar.
4	Registrierung - Zertifizierung	Die *Zertifizierung* wird ausschließlich durch die *Registrierung* veranlaßt und organisatorisch abgewickelt.
5	Zertifizierung - Verzeichnis	Die *zeitnahe* Aktualisierung von Sperrinformationen auf dem Verzeichnis wird durch die direkte Schnittstelle zwischen *Zertifizierung* und *Verzeichnis* sichergestellt.
6	Registrierung - Verzeichnis	Im Rahmen der Teilnehmerregistrierung sind im Verzeichnis Einträge mit Grunddaten der Teilnehmer vorzunehmen. Dieses erfolgt direkt zwischen *Registrierung* und *Verzeichnis*.
7	Registrierung - Namensraumvergabe	Die Instanz *Teilnehmerservice* benötigt einen Namensraum, anhand derer eindeutige Teilnehmernamen (genauer: Endanwendernamen) bestimmt werden können. Die *Registrierung* weist die Instanz *Namensraumvergabe* an, für die Instanz *Teilnehmerservice* einen geeigneten Namensraum zu bestimmen. Dieser Namensraum wird dann der Instanz *Teilnehmerservice* von der Instanz *Registrierung* mitgeteilt (*siehe hierzu auch Punkt 8 dieser Tabelle*).
8	Teilnehmerservice - *Institution*	Zur Integration einer neuen „lokalen Registrierungsstelle“ (die selbst eine neue Instanz *Teilnehmerservice* für die Zertifizierungsstelle einrichten möchte) muß die *Institution* in Kontakt mit der Instanz *Teilnehmerservice* treten, die in der Zertifizierungsstelle selbst eingerichtet ist.

Nach dem PKI-Modell sind nun alle notwendigen Beziehungen zwischen den Instanzen benannt, um die Ziele der Zertifizierungsstelle erreichen zu können. Die Instanzen können ggfs. anders miteinander verbunden werden - im Sinne der Erreichung hoher Sicherheit und Effizienz in der Ablauforganisation wird aber empfohlen, den oben skizzierten Vorschlag umzusetzen.

4.2 Skizzen der Abläufe von Kernaufgaben

Hinweis zur Fehlerbehandlung in den Abläufen: Prinzipiell können in jeder Instanz Fehler auftreten, bzw. Fehler erkannt werden. In diesem Kapitel werden - aus Gründen der Übersichtlichkeit - die Fehlerfälle in den jeweiligen Abläufen *nicht* dargestellt. Im Kapitel 5 „Instanzspezifische Ablauforganisation“ ist die Fehlerbehandlung in den Instanzen enthalten.

Hinweis zu den Teilnehmern: Teilnehmer können sowohl Endanwender als auch Zertifizierungsstellen sein.

4.2.1 Kernaufgabe 1: Teilnehmerregistrierung

Teilnehmer müssen sich - bevor sie zertifiziert werden und die PKI nutzen können - bei der Zertifizierungsstelle registrieren lassen.

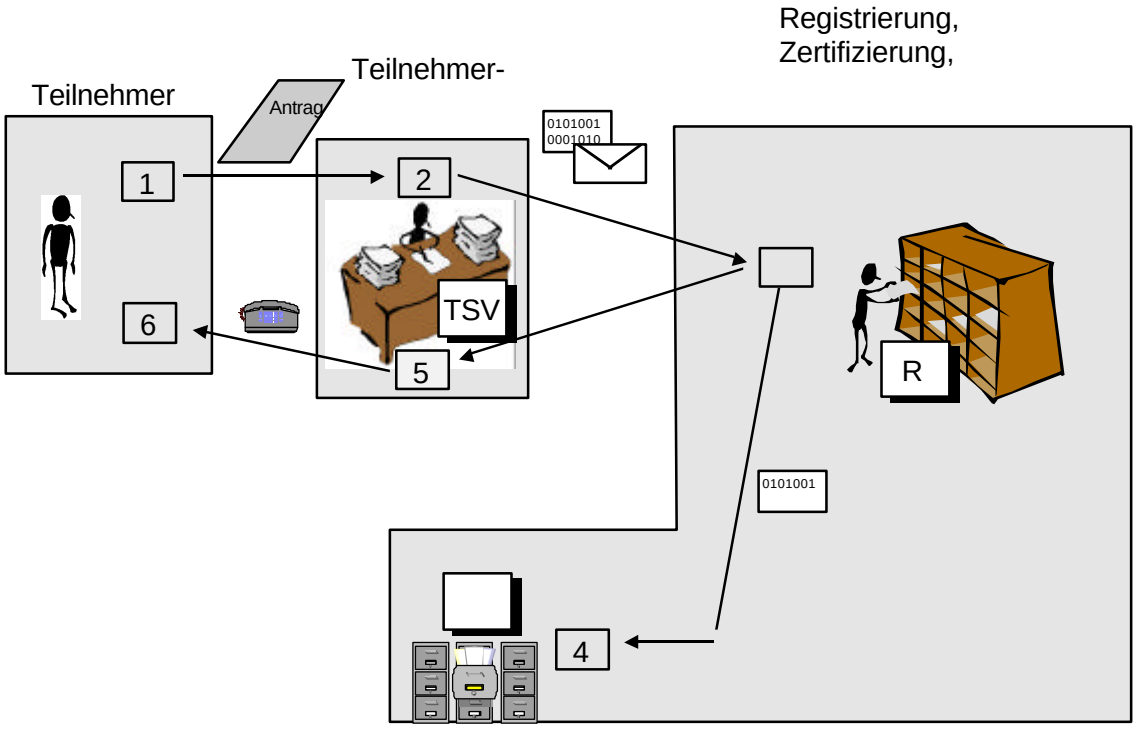


Abbildung 37: Registrierung des Teilnehmers

1. Ein Teilnehmer möchte sich registrieren lassen und wird sich an die Instanz *Teilnehmerservice* wenden [Basisvorgang TSV1].
2. Der *Teilnehmerservice* identifiziert den Teilnehmer, nimmt den Teilnahmeantrag entgegen und führt eine Vorprüfung durch. Ist die Vorprüfung erfolgreich, bestimmt der *Teilnehmerservice* anhand des zugewiesenen Namensraums (der Institution) den *eindeutigen Namen* des Teilnehmers und sendet dann den Registrierungsauftrag an die Instanz *Registrierung* der Zertifizierungsstelle [Basisvorgang TSV1].
3. Die Instanz *Registrierung* prüft den Registrierungsauftrag, registriert den neuen Teilnehmer (u.a. Zuordnung einer eindeutigen Teilnehmer-ID) und veranlaßt ggfs. einen Eintrag im *Verzeichnis* (damit bei der Zertifizierung dann darin seine Zertifikate abgelegt werden

können) [Basisvorgang R1]. Nach Registrierung des neuen Teilnehmers in der Zertifizierungsstelle erfolgt eine Rückmeldung an die Instanz .

4. In der Regel[22]
   Instanz *Verzeichnis*
   nommen [Basisvorgang R1].
5. Nach Eintreffen der Rückmeldung der Instanz *Registrierung* der Zertifizierungsstelle bzgl. der Teilnehmerregistrierung bei der Instanz *Teilnehmerservice* erfolgt eine Benachrichtigung des Teilnehmers über das Ergebnis der Registrierung [Basisvorgang TSV1].
6. Ggfs. erfolgen nun weitere Absprachen zwischen Teilnehmer und Teilnehmerservice über die weiteren Schritte (z.B. über die Zertifizierung des Teilnehmers).

[22] Ein Endanwender muß einer Veröffentlichung seines Zertifikats im Verzeichnis zustimmen. Fehlt diese Zustimmung, erfolgt keine Veröffentlichung - in diesem Falle hat der Endanwender selbst

4.2.2 Kernaufgabe 2: Teilnehmerzertifizierung

Es sind in SPHINX zwei verschiedene Verfahren der Zertifizierung vorgesehen:

Zertifizierung bei zentraler Schlüsselgenerierung

Zertifizierung bei dezentraler Schlüsselgenerierung

sich die Unterschiede in der Ablauforganisation widerspiegeln.

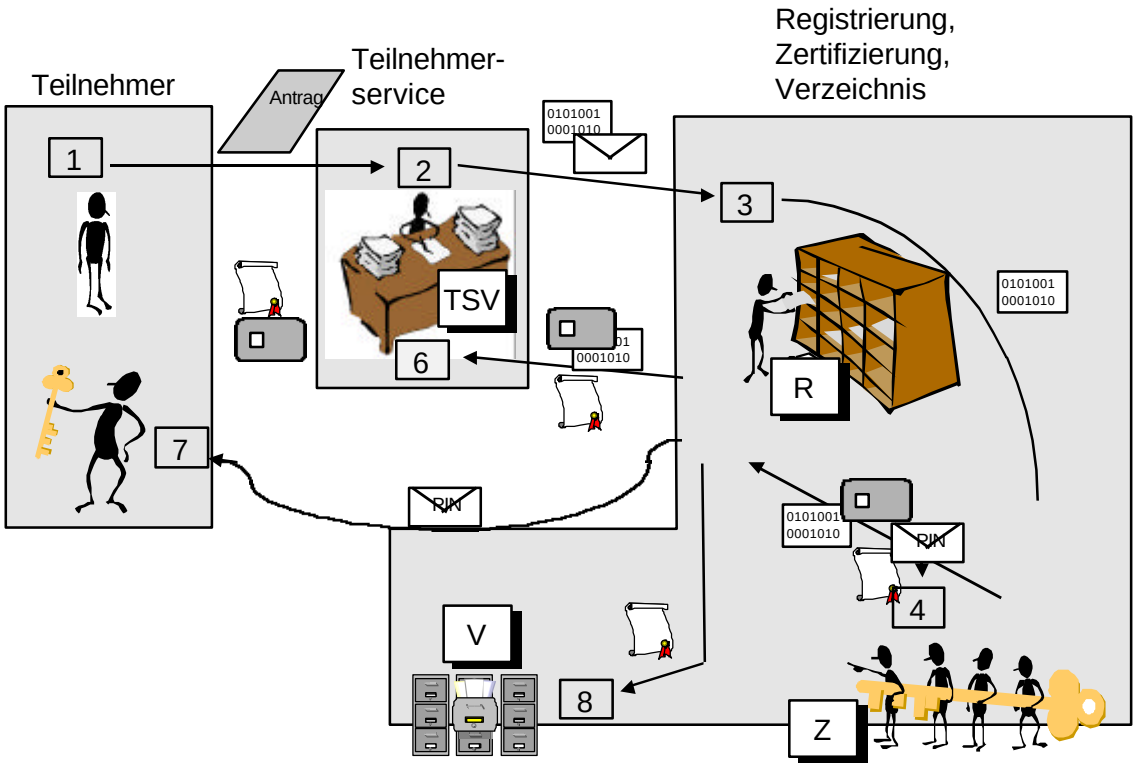
Hinweis: *zentraler Schlüsselgenerierung* Registrierung und Zertifi-

gleichzeitig einen Zertifizierungsantrag beim Teilnehmerservice stellt. Der Teilnehmerservice wird dann beide Anträge an die Registrierung weiterleiten. Die Registrierung hat dieses dann

Teilnehmers wird innerhalb der PKI der organisatorische Rahmen für den Teilnehmer geschaffen, auf den die Zertifizierung dann aufsetzen kann. Bei *gene-rierung* neh-merservice festgelegt und schließlich durch die Zertifizierung im Zertifikat eingetragen wird

4.2.2.1

Bei Zertifizierung mit zentraler Schlüsselgenerierung wird das PSE des Teilnehmers von der Zertifizierungsstelle erzeugt.



38: zierung des Teilnehmers (zentrale Schlüsselgenerierung)

1. Ein Teilnehmer (er ist bereits als Teilnehmer angemeldet [Basisvorgang TSV1]) möchte sich zertifizieren lassen. Der Teilnehmer möchte seine Schlüssel dabei nicht selbst erzeugen. Er wird sich an die Instanz *Teilnehmerservice* wenden, um den Zertifizierungsantrag zu stellen.
2. Der Sachbearbeiter im *Teilnehmerservice* prüft die Identität des Teilnehmers und nimmt den Zertifizierungsantrag entgegen. Er prüft den Antrag und wird ihn dann an die Zertifizierungsstelle weiterleiten (Vorprüfung des Zertifizierungsantrags). Der Antrag muß in Papierform[23] an die *Registrierung* übermittelt werden, da Originaldokumente in der Instanz *Registrierung* der Zertifizierungsstelle archiviert werden müssen. [Basisvorgang TSV2a]
3. Der Sachbearbeiter in der *Registrierung* der Zertifizierungsstelle nimmt den vorgeprüften Zertifizierungsantrag entgegen. Er prüft den Zertifizierungsantrag und archiviert ihn bei sich („Beweissicherung“). Er wird nun die PSE- und Zertifikatserstellung für den Teilnehmer veranlassen. [Basisvorgang R2a]
4. Die *Zertifizierung* erzeugt das PSE und das Zertifikat für den Teilnehmer. Zum PSE wird ein PIN-Brief erstellt. Das Zertifikat, das PSE, der PIN-Brief und Verwaltungsinforma-tionen werden danach an die *Registrierung* übermittelt. [Basisvorgang Z1a]
5. Die *Registrierung* der Zertifizierungsstelle leitet das PSE, das Zertifikat und weitere Verwaltungsinformationen an den *Teilnehmerservice* weiter. Der PIN-Brief wird an den Teilnehmer direkt („persönlich“) vertraulich versandt [Fortführung des Basisvorgangs R2a]. Falls das Zertifikat zur Veröffentlichung vorgesehen ist, wird es an das *Verzeichnis* übermittelt (**Hinweis**: Zur Realisierung des 3-Wege-Protokolls - Veröffentlichung des Zertifikats erst nach Freigabe durch den Teilnehmer - kann das Zertifikat bei der *Registrierung* zwischengelagert werden, bis eine entsprechende Freigabe erfolgt.).
6. Der *Teilnehmerservice* informiert den Teilnehmer über die erfolgte Zertifizierung und hält das PSE und das Zertifikat für den Teilnehmer zur Abholung bereit. [Fortführung des Basisvorgangs TSV2a]
7. Wenn der Teilnehmer über das PSE und die PIN verfügt, kann er die PKI nutzen.
8. Falls das Zertifikat des Teilnehmers dem *Verzeichnis* zur Veröffentlichung übermittelt wurde, wird es dort veröffentlicht. [Basisvorgang V2]

[23] Generell können statt Papierdokumente (die unterzeichnet werden) elektronische Dokumente (die digital signiert werden) verwendet werden. In Fällen, in denen der Unterzeichner kein (im Sinne von SPHINX) gültiges Zertifikat besitzt, ist dieses allerdings nicht möglich (z.B. beim ersten Zertifizierungsantrag eines Teilnehmers) - in diesen Fällen sind Papierdokumente zu verwenden.

4.2.2.2 Teilnehmerzertifizierung bei dezentraler Schlüsselgenerierung

Bei Zertifizierung mit dezentraler Schlüsselgenerierung wird das PSE vom Teilnehmer selbst (mithilfe seines Endanwenderprodukts) erzeugt.

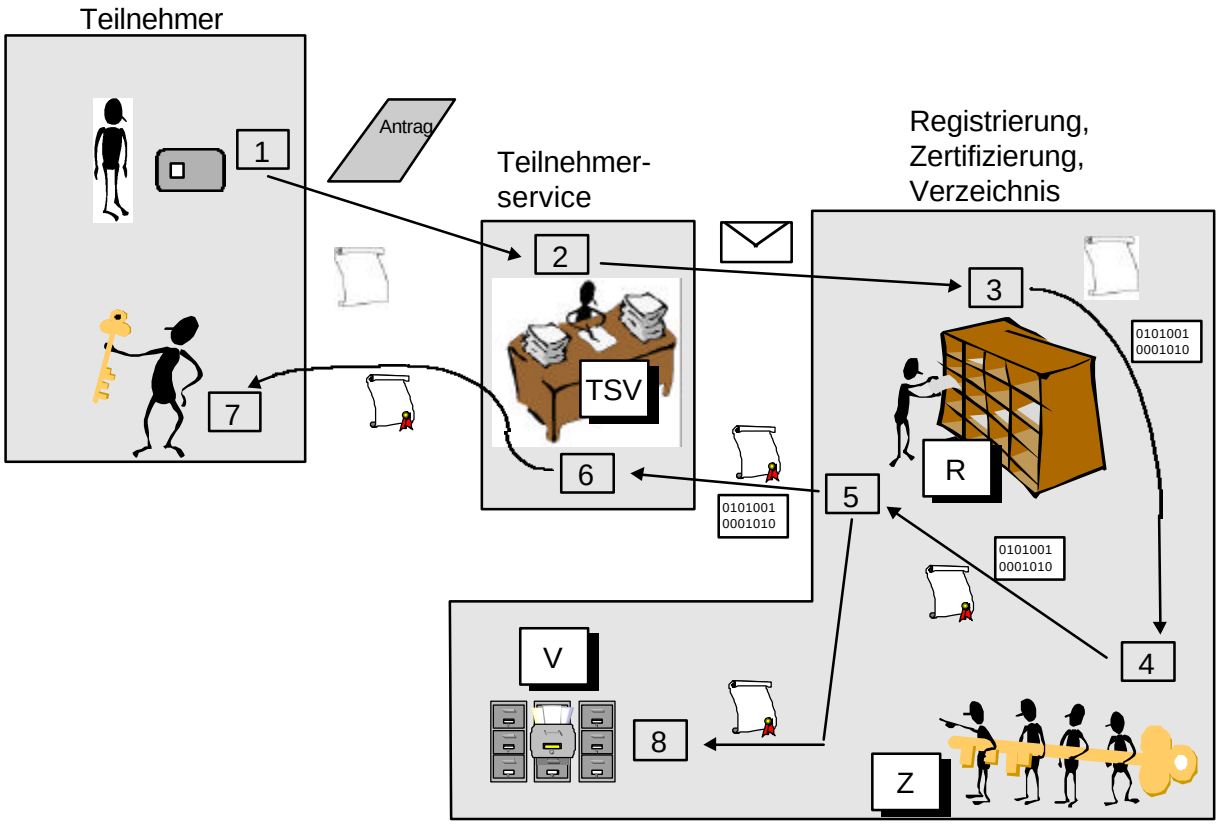


Abbildung 39: Zertifizierung des Teilnehmers (dezentrale Schlüsselgenerierung)

1. Ein Teilnehmer (er ist bereits als Teilnehmer angemeldet [Basisvorgang TSV1]) möchte ein Zertifikat beantragen. Dazu erzeugt er zunächst selbst ein geeignetes Schlüsselpaar (privater und öffentlicher Schlüssel). Der private Schlüssel wird geeignet gesichert in das PSE eingespielt, der (zugängliche) öffentliche Schlüssel wird in eine Schablone für das Prototypzertifikat eingefügt. Die Schablone kann nun noch um weitere Angaben ergänzt werden (z.B. Identifikationsdaten der Person wie den eindeutigen Namen). Die Schablone wird mit dem privaten Schlüssel (unter Nutzung der PSE) signiert und wird so zum Prototypzertifikat (Signatur ist erforderlich aus Gründen der Integritätssicherung und den Nachweis für den „Proof of Possession“), welches selbst wiederum in ein „Certificate Request“ integriert wird. Der Teilnehmer wird sich schließlich an die Instanz *Teilnehmerservice* wenden, um den Zertifizierungsantrag zu stellen. Als Anlage legt er dem schriftlichen Zertifizierungsantrag sein Prototypzertifikat (im „Certificate Request“) auf einem geeigneten Datenträger bei.
2. Der Sachbearbeiter im *Teilnehmerservice* prüft die Identität des Teilnehmers und nimmt den Zertifizierungsantrag sowie das Prototypzertifikat entgegen. Er führt eines Vorprüfung des Antrags und ggfs. des Prototypzertifikats durch und wird beide an die Instanz *Registrierung* der Zertifizierungsstelle weiterleiten. Der Antrag muß in Papierform übermittelt werden, da Originaldokumente in der Zertifizierungsstelle archiviert werden müssen, das Prototypzertifikat kann z.B. auf Diskette beigelegt werden. [Basisvorgang TSV2b]

3. Der Sachbearbeiter in der *Registrierung* der Zertifizierungsstelle nimmt den vorgeprüften Zertifizierungsantrag und das Prototypzertifikat entgegen. Er wird beides prüfen und bei sich archivieren („Beweissicherung“). Er wird nun die Zertifikatserstellung für den Teilnehmer veranlassen und übermittelt dazu den Zerifizierungsauftrag und das Prototypzertifikat an die Instanz *Zertifizierung* [Basisvorgang R2b].
4. Die Instanz *Zertifizierung* prüft die Angaben im Zertifizierungsauftrag. Sie prüft ebenfalls das Prototypzertifikat. Ist beides korrekt, wird das Zertifikat für den Teilnehmer erzeugt. Das Zertifikat wird danach an die *Registrierung* übermittelt [Basisvorgang Z1b].
5. Die *Registrierung* informiert die Instanz *Teilnehmerservice* über das Ergebnis der Zertifizierung [Basisvorgang Z1b]. Falls das Zertifikat zur Veröffentlichung vorgesehen ist, wird es an das *Verzeichnis* übermittelt. (**Hinweis**: Zur Realisierung des 3-Wege-Protokolls - Veröffentlichung des Zertifikats erst nach Freigabe durch den Teilnehmer - kann das Zertifikat bei der Registrierung zwischengelagert werden, bis eine entsprechende Freigabe erfolgt.).
6. Der *Teilnehmerservice* informiert den Teilnehmer über die erfolgte Zertifizierung und hält das Zertifikat für den Teilnehmer zur Abholung bereit. [Fortführung des Basisvorgangs TSV2b].
7. Der Teilnehmer kann nun sein selbsterzeugtes PSE nutzen.
8. Falls das Zertifikat des Teilnehmers dem *Verzeichnis* zur Veröffentlichung übermittelt wurde, wird es dort veröffentlicht. [Basisvorgang V2]

4.2.3 Kernaufgabe 3: Sperrung von Zertifikaten

Eine Zertifikatssperrung wird in der Regel durch den Teilnehmer selbst (Eigensperrung) oder durch eine autorisierte Person (Fremdsperrung) veranlaßt. Es stehen ihnen dafür verschiedene Wege offen.

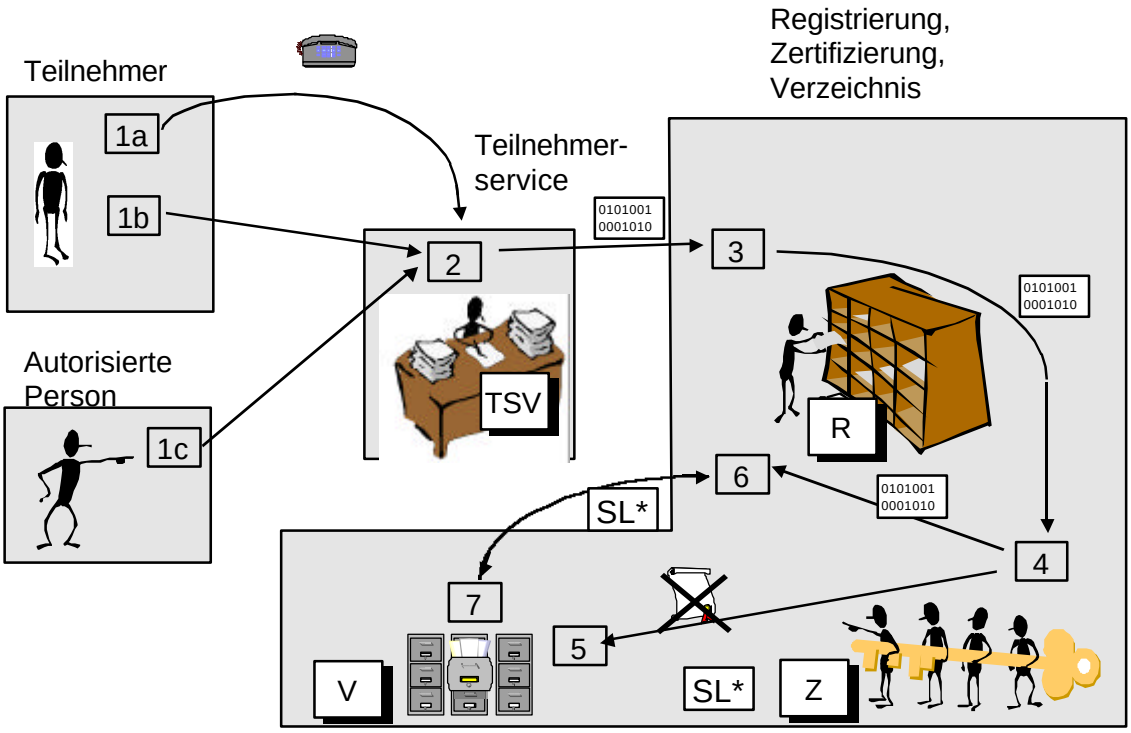


Abbildung 40: Zertifikatssperrung

1. Ein Teilnehmer möchte sein Zertifikat sperren lassen (Eigensperrung). Dazu kann er sich direkt an die Telefonhotline des *Teilnehmerservice* der Zertifizierungsstelle (1a) oder an den für die Institution zuständigen *Teilnehmerservice* („lokale Registrierungsstelle“) (1b) wenden. Möchte die autorisierte Person eine Fremdsperrung veranlassen, muß sie sich an den für die Institution zuständigen *Teilnehmerservice* („lokale Registrierungsstelle“) wenden. Die Sperrung kann (fern)mündlich, schriftlich oder persönlich - nach erfolgreicher Prüfung der Sperrautorisierung - erfolgen. [Basisvorgänge R5a - R5c, TSV4]
2. Der *Teilnehmerservice* prüft, ob alle Sperrvoraussetzungen erfüllt sind. Sind alle Voraussetzungen für die Sperrung gegeben, wird der Sperrungsauftrag an die *Registrierung* der Zertifizierungsstelle weitergeleitet. [Basisvorgang R5d]
3. Liegt der Sperrauftrag bei der *Registrierung* der Zertifizierungsstelle vor, erfolgt die Weiterleitung des Auftrags an die *Zertifizierung* [Basisvorgänge R5a - R5d].
4. Liegt der Sperrauftrag bei der *Zertifizierung* der Zertifizierungsstelle vor, erfolgt die Sperrung des Zertifikats [Basisvorgang Z3a]. Die Sperrung schließt die Generierung und Veröffentlichung einer aktualisierten Sperrliste ein [Basisvorgang Z4].
5. Die Sperrliste wird im *Verzeichnis* aktualisiert. Ein Entfernen gesperrter oder abgelaufener Zertifikate aus dem Verzeichnis erfolgt nicht [Basisvorgang V3].
6. Es erfolgt eine Sperr-Rückmeldung an die *Registrierung* [Basisvorgang Z3a].

7. Es empfiehlt sich zur Qualitätssicherung seitens der *Registrierung*, stichprobenhaft die Aktualität und Korrektheit des Verzeichnisses über die öffentliche Verzeichnis-Schnittstelle zu überprüfen. [Fortführung einer der Basisvorgänge R5a - R5d]

4.2.4 Kernaufgabe 4: Registrierung einer lokalen Registrierungsstelle

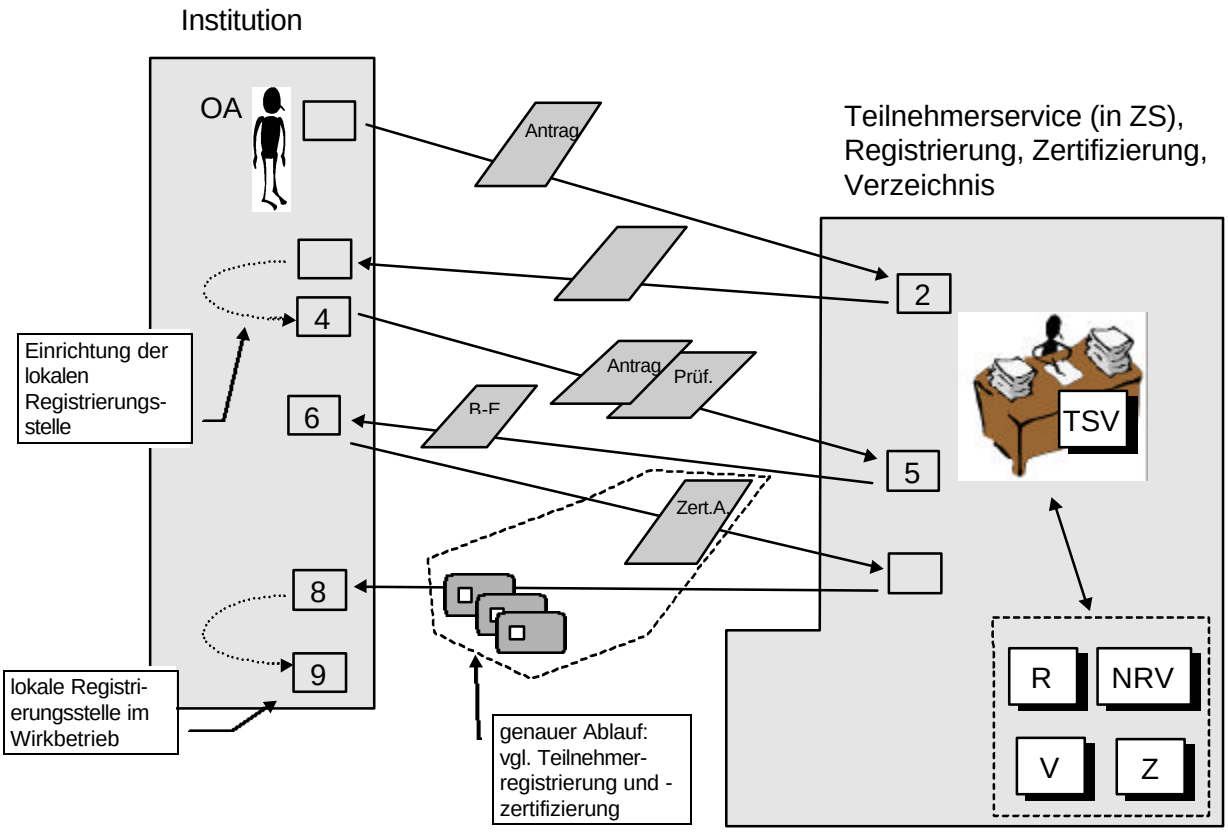


Abbildung 41: Registrierung einer lokalen Registrierungsstelle

1. Der organisatorische Ansprechpartner der Institution stellt einen schriftlichen Antrag auf Einrichtung einer lokalen Registrierungsstelle.
2. Die Instanz *Teilnehmerservice* der Zertifizierungsstelle nimmt den Antrag entgegen und bearbeitet ihn. Bei positiver Prüfung erhält der organisatorische Ansprechpartner eine Teilnahmebestätigung. Mit der Teilnahmebestätigung erhält der organisatorische Ansprechpartner in gemeinsamer Absprache den Namensraum für seinen Teilnehmer-kreis zugewiesen [Basisvorgang R6].
3. Anhand dieser Teilnahmebestätigung hat die Institution die (Investitions-)Sicherheit, daß eine ordnungsgemäß eingerichtete lokale Registstrierungsstelle von der Zertifizierungs-stelle akzeptiert werden wird. Die Institution wird nun die lokale Registrierungsstelle ein-richten.
4. Nachdem die Institution die lokale Registrierungsstelle eingerichtet hat, stellt sie bei der Instanz *Teilnehmerservice* der Zertifizierungsstelle den Antrag auf Betriebserlaubnis. Die Institution legt eine Bescheinigung vor, die besagt, daß alle Teilnahmevoraussetzungen gem. *Policy* erfüllt sind. Dieses wird in der Regel eine geeignete Selbstauskunft der Institution sein, die bei Bedarf beispielsweise durch den Prüfbericht eines Sachverständigen ergänzt werden kann.

5. Die Registrierung der Zertifizierungsstelle prüft, ob alle Teilnahmevoraussetzungen erfüllt sind. Sind sie es, dann erhält der organisatorische Ansprechpartner die Betriebserlaubnis. [Fortführung des Basisvorgangs R6]
6. Liegt die Betriebserlaubnis beim organisatorischen Ansprechpartner vor, wird ein Sammelantrag zur Registrierung und Zertifizierung der Mitarbeiter der lokalen Registrierungsstelle gestellt.
7. Anhand des Sammelantrags werden alle benannten Mitarbeiter der lokalen Registrierungsstelle als Ansprechpartner erfaßt. Für jeden Mitarbeiter wird eine Teilnehmerzertifizierung durchgeführt (Details hierzu: Siehe Teilnehmerzertifizierung). Änderungen im Mitarbeiterstamm sind ebenfalls mit dem Sammelantrag zu melden (z.B. Meldung weiterer Mitarbeiter, Sperrung ausscheidender Mitarbeiter). [Fortführung des Basisvorgangs R6. Details der Teilnehmer-Registrierung und -zertifizierung der Mitarbeiter der lokalen Registrierungsstelle: Siehe entsprechende Basisvorgänge]
8. Die lokale Registrierungsstelle ist nun arbeitsfähig. Es erfolgen nun einige Tests (Abwicklung von Test-Anträgen, die durch die Zertifizierungsstelle vorgegeben werden). [Fortführung des Basisvorgangs R6]
9. Nach erfolgreicher Abwicklung der Tests befindet sich die lokale Registrierungsstelle im Wirkbetrieb.

5 Instanzspezifische Ablauforganisation

Innerhalb einer Stelle (Zertifizierungsstelle, Registrierungsstelle) finden Vorgänge statt, die im wesentlichen durch Mitarbeiter (Personen, die in Rollen agieren) in den Instanzen erbracht werden. Dieses sind Vorgänge, die üblicherweise im Alltagsbetrieb einer Stelle auftreten und die durch ihre Mitarbeiter ausschließlich anhand der Vorgaben des Organisationshandbuchs erbracht werden (***Standardvorgänge***). Daneben gibt es ***Sondervorgänge***, die durch die Leitung der betroffenen Stelle explizit geplant, vorbereitet und ausschließlich unter ihrer Aufsicht erbracht werden. Wechselwirkungen in andere Bereiche sind zu berücksichtigen, ggfs. sind weitreichende Einzelentscheidungen zu treffen. Sondervorgänge betreffen insbesondere die Wurzel-Zertifizierung und die Sperrung von Zertifizierungsstellen-Zertifikaten.

Die ***Standardvorgänge*** setzen sich wiederum aus ***Basisvorgängen*** zusammen. ***Basisvorgänge*** werden durch die einzelnen Instanzen innerhalb der Stelle erbracht.

Die instanzenspezifische Ablauforganisation soll – aus der Perspektive der jeweiligen Instanz heraus – die notwendigen Basisvorgänge beschreiben, die diese zu erbringen hat, um das Gesamtziel einer effizienten und sicheren PKI zu erreichen. Dazu werden die jeweiligen Aufgaben der Instanz dargestellt, die Schnittstellen zu angrenzenden Instanzen spezifiziert und die notwendigen Arbeitsschritte beschrieben.

Es werden zunächst ***Aufgaben*** spezifiziert, die bei Bedarf durch die jeweilige Instanz auszuführen sind. Jede Aufgabe ist durch ein eigenes Kapitel vertreten. Zu jeder Aufgabe wird kurz beschrieben, in welchen Fällen sie notwendig wird.

Es werden die ***Schnittstellen*** zu den jeweils angrenzenden Instanzen betrachtet:

- **Kommunikation:** Mit welchen anderen Instanzen hat eine Instanz zu tun?
- **Eingang:** Welcher Dokumente und Datenobjekte sind von anderen Instanzen entgegenzunehmen?
- **Ausgang:** Welche Dokumente und Datenobjekte sind an andere Instanzen zu übergeben?

Auf dieser Basis werden dann die notwendigen ***Arbeitsschritte*** spezifiziert, damit die Instanz ihrer jeweiligen Aufgabe gerecht werden kann:

- **Eingang**: Entgegennahme von Dokumenten und Datenobjekten (z.B. eines Antrags).
- **Prüfung:** Der Input muß auf Konsistenz (Integrität, Authentizität) überprüft werden („Formale Prüfung“). Weitere Prüfschritte können notwendig sein (ggfs. auch inhaltliche Prüfungen). Output können hier Fehlermeldungen an die betroffenen Instanzen sein. Sollten bei den Prüfungen keine Beanstandungen auftreten, können die eigentlichen Tätigkeiten (die „PKI-Dienstleistung“) ausgeführt werden.
- **PKI-Dienstleistung:** Bei erfolgreicher Prüfung des Inputs wird die Instanz die eigentliche Dienstleistung für die PKI ausführen.
- **Ausgabe**: Ausgabe von Dokumenten und Datenobjekten (z.B. eines Zertifikats).
- **Protokollierung:** Wo notwendig, werden Tätigkeiten einer Instanz - vorrangig zu Zwecken der Revision - von ihr geeignet protokolliert. Anhand der Protokolle können ggf. damit die Ursachen von Problemen identifiziert werden.

Wichtiger Hinweis: Um hier Abläufe spezifizieren zu können ist es notwendig, daß die Schnittstellen zwischen den Instanzen klar definiert sind - die Instanzen und ihre Wechselbeziehungen zueinander bestimmen sehr stark die instanzinternen Abläufe. Hier wird auf die in Kapitel 4 entwickelte ***Modellumsetzung*** referenziert, wie sie in SPHINX auch umgesetzt ist. Wird die Modellumsetzung im Rahmen ihrer Fortentwicklung verändert, sind auch die Abläufe entsprechend der neuen Architektur neu zu spezifizieren.

5.1 Standard- und Basisvorgänge

Innerhalb der PKI finden Vorgänge statt, die durch Mitarbeiter (Personen, die in Rollen agieren) in den Instanzen *Teilnehmerservice*, *Registrierung*, *Zertifizierung*, *Verzeichnis* und *Namensraumvergabe* erbracht werden.

Betrachtet werden hier ausschließlich *Standardvorgänge*. Dieses sind Vorgänge, die üblicherweise im Alltagsbetrieb der Stellen auftreten und die ausschließlich durch die Mitarbeiter auf der Basis des Organisationshandbuchs erbracht werden. Daneben gibt es *Sondervorgänge*, die ausschließlich durch die Leitung der betroffenen Stellen geplant und unter ihrer Aufsicht erbracht werden dürfen. Bei Sonderaufgaben sind Wechselwirkungen in andere Bereiche zu berücksichtigen, ggfs. sind weitreichende Einzelentscheidungen zu treffen. Sondervorgänge betreffen insbesondere die Wurzel-Zertifizierung und die Sperrung von Zertifizierungsstellen-Zertifikaten.

Die innerhalb der PKI auftretenden Standardvorgänge sind in der folgenden Tabelle zusammengefaßt. Jeder Vorgang besteht wiederum aus Basisvorgängen, die schließlich in den Instanzen erbracht werden.

Standardvorgang	Instanz	Basisvorgänge der Instanzen (ablauflogisch sortiert)
Teilnehmerinformation		
Information von interessierten Personen und Institutionen	TSV	• Teilnehmerservice *Nicht explizit modelliert, da Vorgang außerhalb des PKI-Modells liegt und die Sicherheit des Verfahrens nicht direkt betroffen ist. Im Betriebshandbuch lokale Registrierungsstelle werden Hinweise zu diesem Aspekt gegeben.*
Teilnehmer-Registrierung und Zertifizierung		

Registrierung und Zertifizierung von Endanwendern	R, TSV, V, Z	• Teilnehmerservice
		  • Registrierung eines Endanwenders (TSV1a)
		  • Namensvergabe (wird innerhalb TSV1a erbracht)
		  • Teilnehmerzertifizierung (TSV2a/b)
		• Registrierung
		  • Endanwenderregistrierung (R1a)
		• Verzeichnis
		  • Basisdatensatzeintrag für Teilnehmer, (V1)
		• Registrierung
		  • Teilnehmerzertifizierung (zentr. SE) (R2a)
		  • Teilnehmerzertifizierung (dezentr. SE) (R2b)
		• Zertifizierung
		  • Teilnehmerzertifizierung (zentr. SE) (Z1a)
		  • Teilnehmerzertifizierung (dezentr. SE) (Z1b)
		• Verzeichnis
		  • Zertifikatsaktualisierung (V2)

Registrierung und	R, TSV,	• Teilnehmerservice

Standardvorgang	Instanz	Basisvorgänge der Instanzen (ablauflogisch sortiert)
Zertifizierung von Zertifizierungsstellen	V, Z	• Registrierung einer Zertifizierungsstelle (TSV1b) • Namensvergabe (wird innerhalb TSV1b erbracht) • Teilnehmerzertifizierung (TSV2b) • Registrierung • Zertifizierungsstellen-Registrierung (R1b) • Verzeichnis • Basisdatensatzeintrag für Teilnehmer, (V1) • Registrierung • Teilnehmerzertifizierung (R2b) • Zertifizierung • Teilnehmerzertifizierung (dezentr. SE) (Z1b) • Verzeichnis • Zertifikatsaktualisierung (V2) • Sperrlistenaktualisierung (V3)
Änderungsmitteilung durch Teilnehmer		
Änderungsmitteilung durch den Teilnehmer	TSV, R, V	• Teilnehmerservice • Änderungsmitteilung Teilnehmer (TSV1c) • Registrierung • Änderungsauftrag Teilnehmer (R1c) • Verzeichnis • Fehlerkorrektur im Verzeichnis (VF)
Zertifikats-Verlängerung		
Verlängerung von Zertifikaten	R, V, Z	• Registrierung • Zertifikatsverlängerung (R3) • Zertifizierung • Teilnehmerzertifizierung (dezentr. SE) (Z1b) • Verzeichnis • Zertifikatsaktualisierung (V2)
Zertifikats-Sperrung		
Sperrung von Endanwender-Zertifikaten aufgrund eines Sperrauftrags	R, TSV, V, Z	• Teilnehmerservice • Zertifikatssperrung durch EA / AP (TSV4) • Registrierung • Zertifikatssperrung (R4a - R4d) • Zertifizierung • Zertifikatssperrung mit Sperrauftrag (Z2a) • Sperrlistenaktualisierung (Z3) • Verzeichnis • Sperrlistenaktualisierung (V3)
Sperrung von Endanwender-Zertifikaten ohne Sperrauftrag	R, V, Z	• Zertifizierung • Zertifikatssperrung ohne Sperrauftrag (Z2b) • Sperrlistenaktualisierung (Z3) • Verzeichnis • Sperrlistenaktualisierung (V3) • Registrierung • Weitermeldung einer ZS-getriggerten Zertifikats-sperrung (R6)
Sperrlisten-Aktualisierung		
Sperrlisten-Erstellung	R, V, Z	• Zertifizierung • Sperrlistenaktualisierung (Z3)

Standardvorgang	Instanz	Basisvorgänge der Instanzen (ablauflogisch sortiert)

		• Verzeichnis
		  • Sperrlistenaktualisierung (V3)
		• Registrierung
		  • Übernahme der Sperrlistenaktualisierung (R7)

Fehlerkorrektur veröffentlichter Daten		

Fehlerkorrektur im Verzeichnis	R, TSV, Z	• Teilnehmerservice, Zertifizierung
		  • Fehlerkorrekturanforderung Verzeichnis via R (TSVF, ZF)
		• Registrierung
		  • Fehlerkorrekturanforderung Verzeichnis (RF)

Stichprobenhafte Überprüfung des Verzeichnisses	R, V	• Registrierung
		  • Überprüfung des Verzeichnisses (R8)
		• Verzeichnis
		  Kein Basisvorgang notwendig, da Registrierung Daten über öffentliche Verzeichnisschnittstelle anfordert.

Fehlerkorrektur	V	• Verzeichnis • Fehlerkorrektur im Verzeichnis (VF)
Registrierung einer lokalen Registrierungsstelle		

Registrierung einer lokalen Registrierungs-stelle	NRV, R	• Teilnehmerservice
		  • Registrierung einer lokalen Registrierungsstelle (TSV3)
		• Registrierung
		  • Registrierung einer lokalen Registrierungsstelle (R5)
		• Namensraumvergabe
		  • Namensraumvergabe (NRV1)

SPHINX-projektspezifische Vorgänge (SPHINX-MGMT)		
Verteiler	R	• Registrierung • R-Verteiler (R-SPHINX-1)
Projektdatenpflege	R	• Registrierung • Projektdatenpflege (R-SPHINX-2)

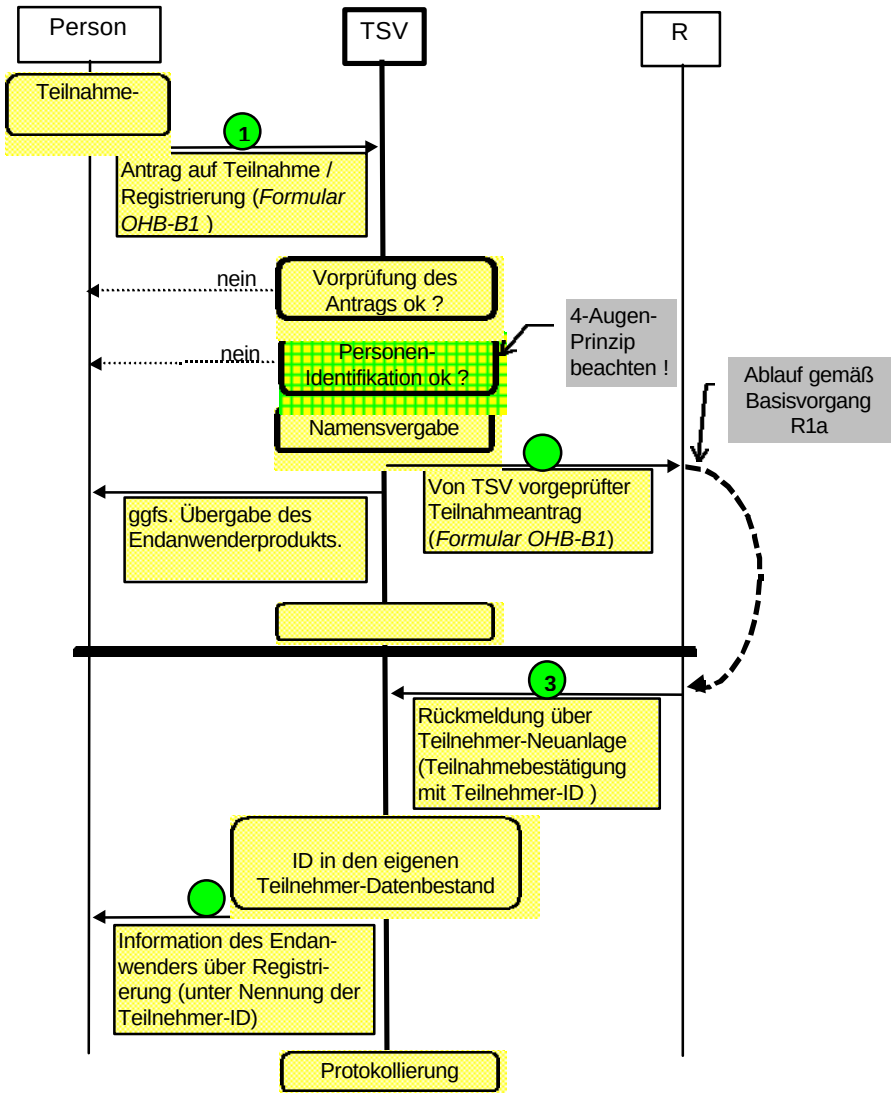
Abbildung 42: Standard- und Basisvorgänge

5.2 Basisvorgänge in der Instanz Teilnehmerservice (TSV)

5.2.1 Registrierung eines Endanwenders (TSV1a)

Der Teilnehmer, der zertifiziert werden möchte, muß sich zunächst registrieren lassen.

Hinweis zur Teilnehmer-ID: Bei der Registrierung erhält jeder Teilnehmer eine Teilnehmer-Kennung, die Teilnehmer-ID, zugewiesen. Sie identifiziert den Teilnehmer innerhalb der PKI eindeutig. Die Teilnehmer-ID wird einem Teilnehmer (Person oder Zertifizierungsstelle) fest zugeordnet und ist nicht mehr veränderbar. Die Teilnehmer-ID ist innerhalb der PKI zur sicheren Zuordnung aller Vorgänge zum Teilnehmer zu verwenden.



Ablaufdiagramm 1: TSV1a: Registrierung eines Endanwenders

5.2.2

Hinweis: Dieser Basisvorgang ist ausschließlich für die Instanz Teilnehmerservice relevant,

Die potentielle Zertifizierungsstelle, die zertifiziert werden möchte, muß sich zunächst registrieren lassen. Diese Registrierung erfolgt mehrstufig:

Informationsphase:
Rahmenbedingungen (insb. über die technischen, organisatorischen, personellen, infrastrukturellen und juristischen Anforderungen) der Teilnahme als Zertifizie-

- Zunächst wird das Teilnahme-
  verfahren eingeleitet. Hierbei werden die organisatorischen Aspekte der Teil
  geklärt (u.a. wer Ansprechpartner der Institution ist). Die Institution erhält eine
  Teilnahmebescheinigung, die ihr die (Investions-)Sicherheit bietet, daß eine gemäß
  Policy) eingerichtete Zertifizierungsstelle in die PKI integriert

- Im Teilnahmeverfahren werden die Teilnahme-voraus-
  setzungen von Teilnehmer umgesetzt, die sie lt. erfüllen muß. Dieses umfaßt
  u.a. die Vorlage eines geeigneten Sicherheitskonzepts und und Aufbau der

- **Betriebserlaubnis"):** Hat der Teilnehmer alle Anforderungen an eine Zertifizie-

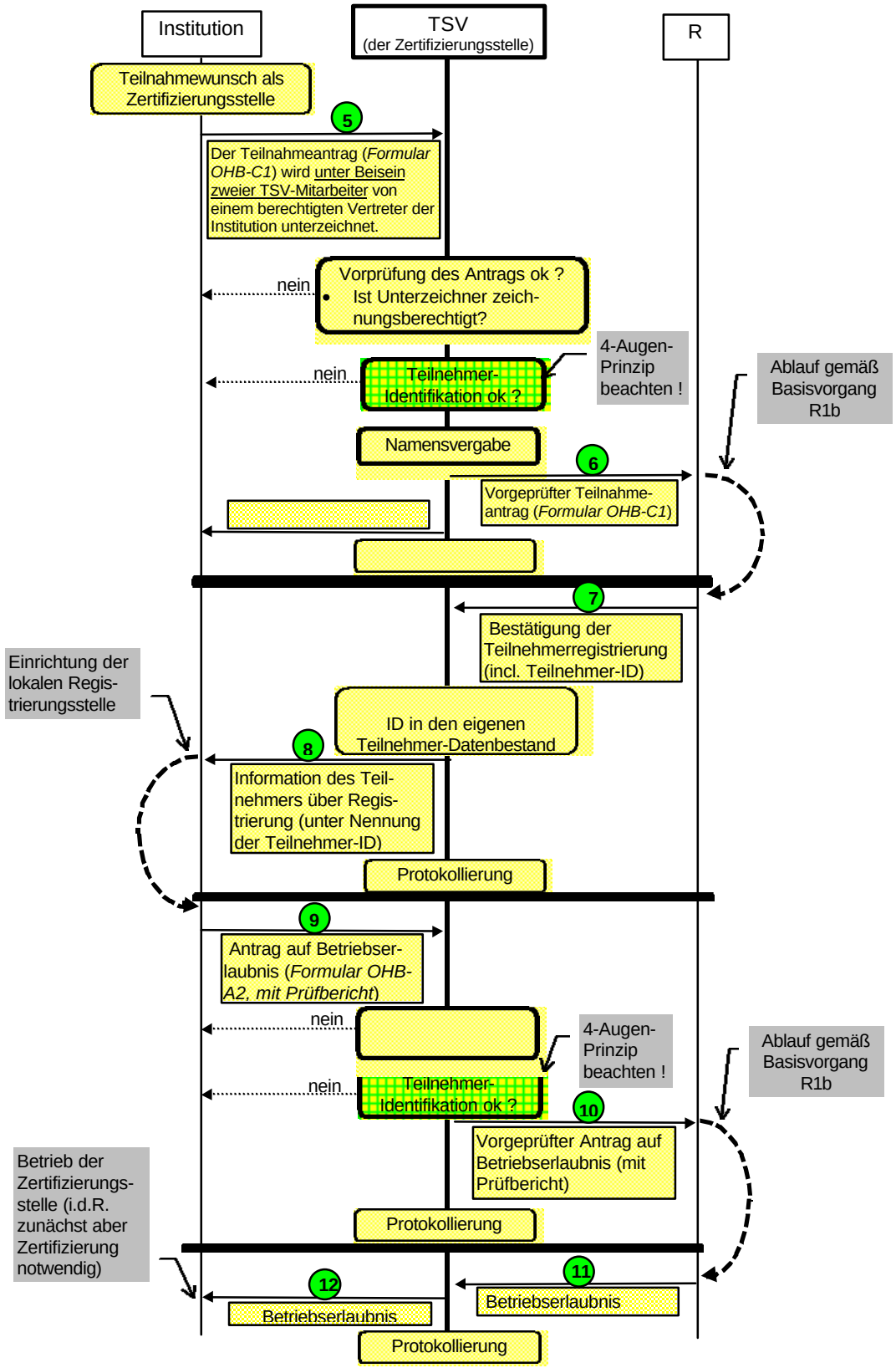
  rungsstelle anerkannten Sachverständigen bescheinigen lassen (Regelungen dazu
  sind in der enthalten) und einen Antrag auf Betriebserlaubnis stellen.

- **Betriebserlaubnis:** Nach erfolgreicher Prüfung des Antrags auf Betriebserlaubnis

  einer Dummy-Sperrliste. Diese Dummy-Sperrliste enthält keinen Sperreintrag und ist
  liste zu ersetzen.
  Nachdem im Verzeichnis ein Eintrag für die Zertifizierungsstelle angelegt wurde,

  Betriebserlaubnis). Die Zertifizierungsstelle kann nun zertifiziert werden
  (Basisverfahren TSV2b).

Siehe Basisvorgang TSV1a.



Ablaufdiagramm 2: TSV1b: Registrierung einer Zertifizierungsstelle

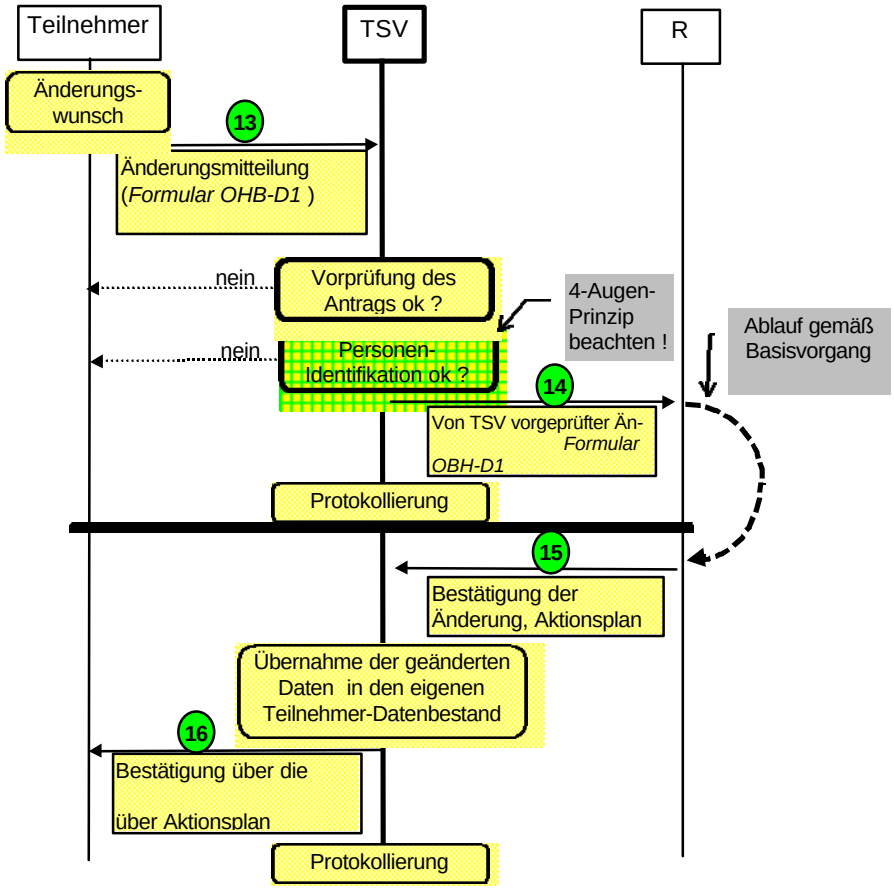
5.2.3 Änderungsmitteilung eines Teilnehmers (TSV1c)

Vom Teilnehmer können jederzeit Änderungen des eigenen Teilnehmerdatenbestandes und des Teilnehmerstatus veranlaßt werden. In diesen Fall wird vom Teilnehmer eine *Änderungsmitteilung* an die Zertifizierungsstelle (über den Teilnehmerservice) eingereicht.

Änderungsmitteilungen sind beispielsweise in folgenden Fällen angezeigt:

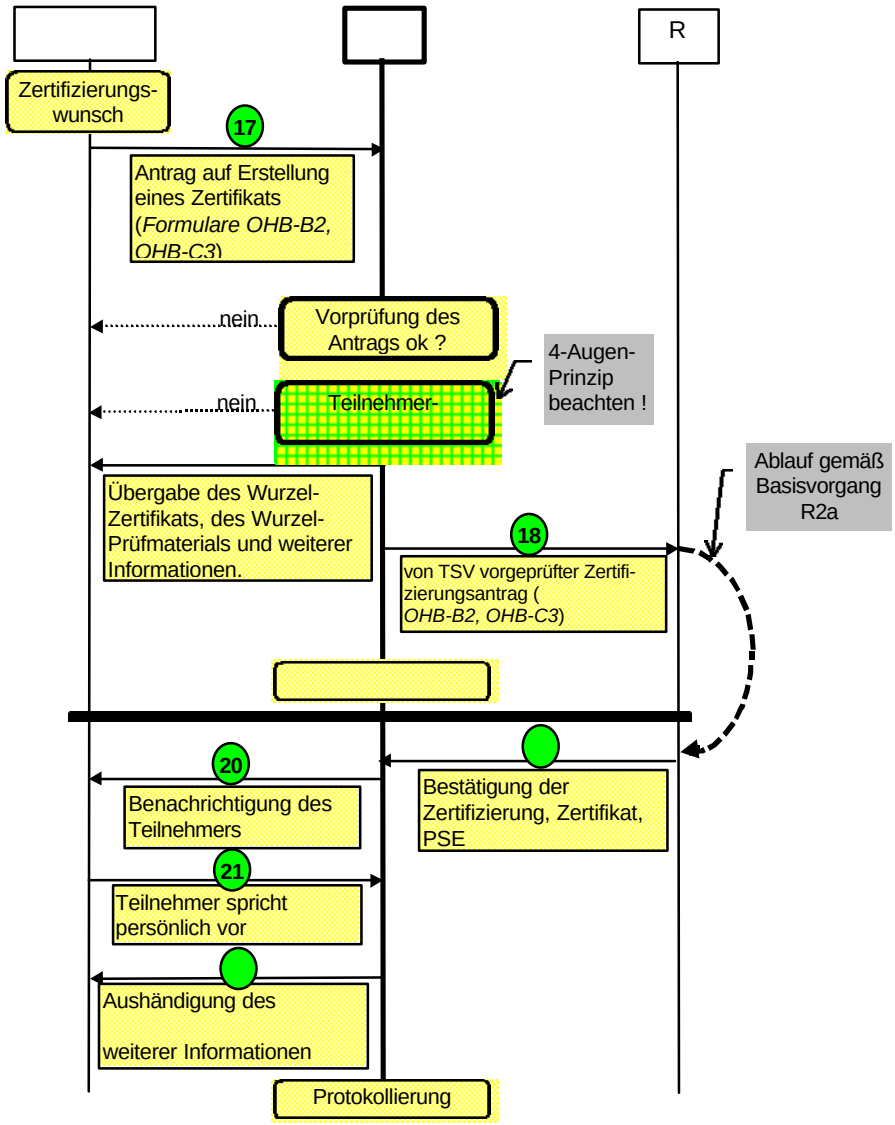
- Namensänderung des Teilnehmers
- Änderungen in den organisatorischen Daten (z.B. Abteilungswechsel)
- Beendung der Teilnahme

Hinweis: Es werden nicht alle an der Änderung implizierten Basisvorgänge automatisch durchgeführt, da die Auswirkungen hier zu komplex sind und z.T. neue Anträge im Original durch den Teilnehmer zu unterzeichnen sind. Der Teilnehmerservice hat nicht die Dokumente verfügbar, um beurteilen zu können, welche Schritte im einzelnen durchzuführen sind. Zur Unterstützung des Teilnehmers und des Sachbearbeiters im Teilnehmerservice wird in der Instanz Registrierung der Zertifizierungsstelle ermittelt, welche Aktionen nun praktisch noch eingeleitet werden müssen.



Ablaufdiagramm 3: TSV1c: Änderungsmitteilung eines Teilnehmers

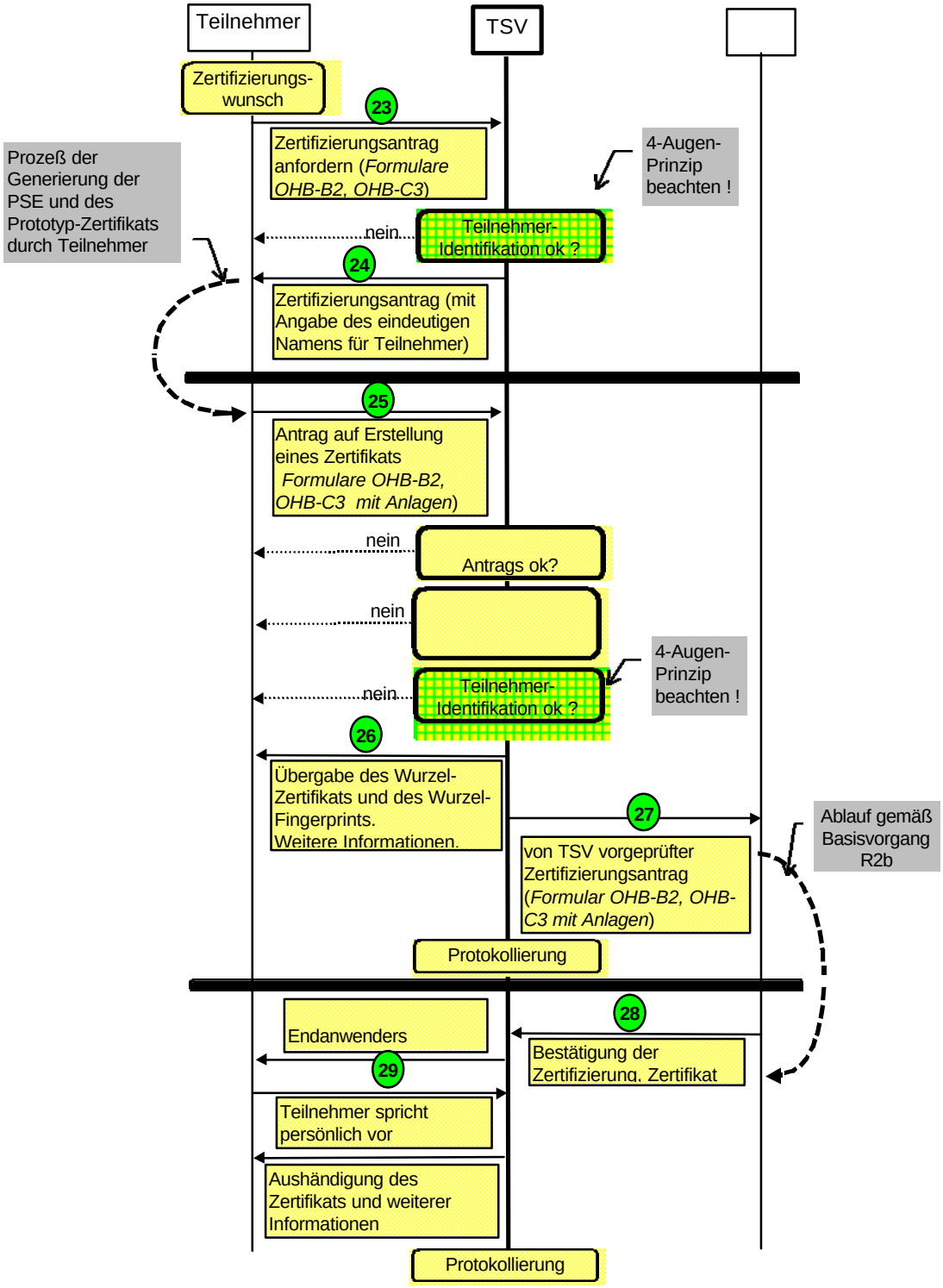
5.2.4



Ablaufdiagramm 4 TSV2a: Teilnehmerzertifizierung (bei zentraler Schlüsselgenerierung)

Teilnehmerzertifizierung bei dezentraler Schlüsselgenerierung (TSV2b)

_____ Wenn eine Zertifizierungsstelle Teilnehmer ist, ist dieser Basisvorgang nur für die Instanz Teilnehmerservice relevant, die in der Zertifizierungsstelle angesiedelt ist.

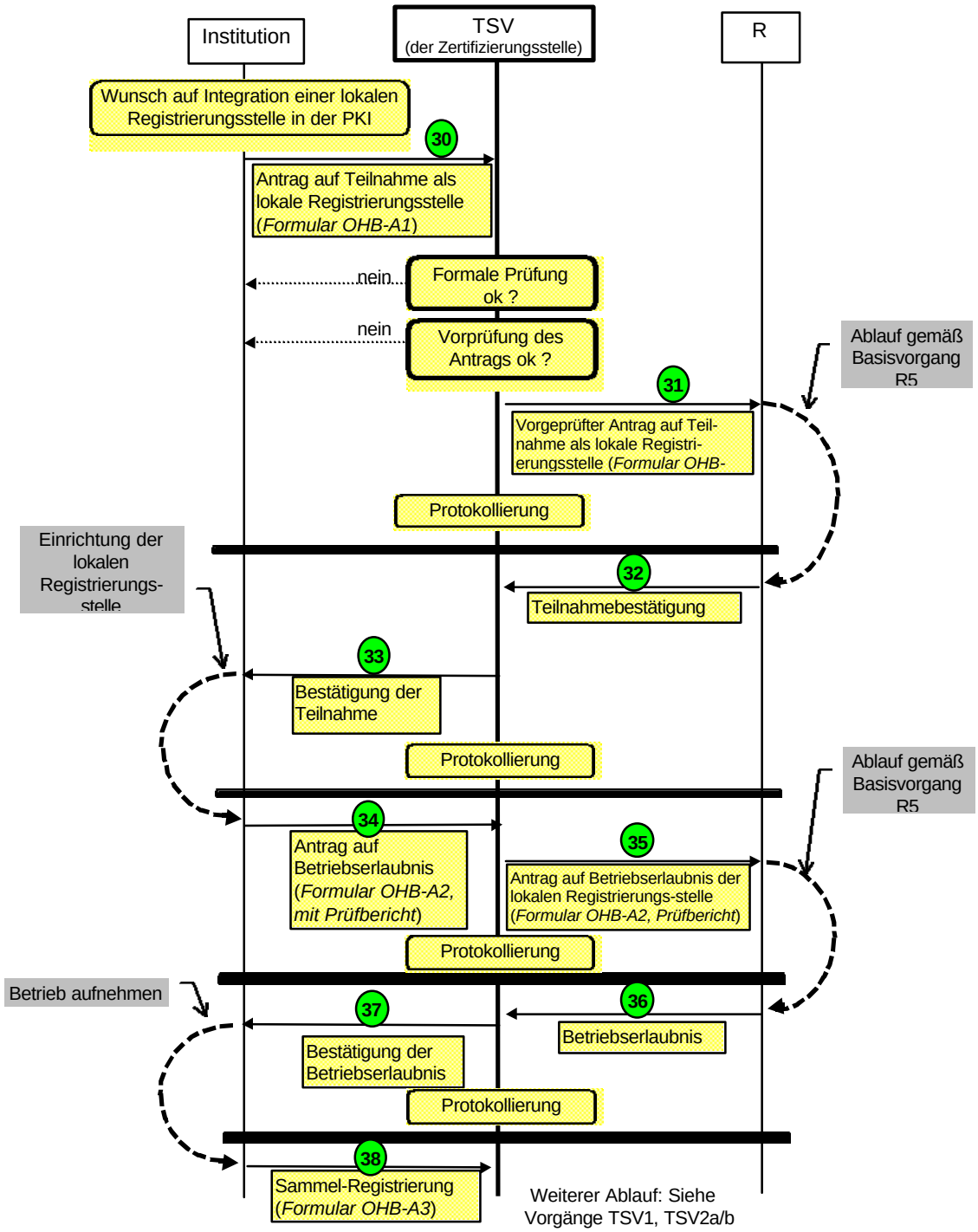


5: 2b: Teilnehmerzertifizierung (bei dezentr. Schlüsselgenerierung)

5.2.6 Registrierung einer lokalen Registrierungsstelle (TSV3)

Hinweis: Dieser Ablauf erfolgt ausschließlich in der Instanz Teilnehmerservice der Zertifizierungsstelle.

Damit die lokale Registrierungsstelle mit der zuständigen Zertifizierungsstelle Vorgänge abwickeln kann, muß sie zunächst bei dieser registriert werden.



Ablaufdiagramm 6: TSV3: Registrierung einer lokalen Registrierungsstelle

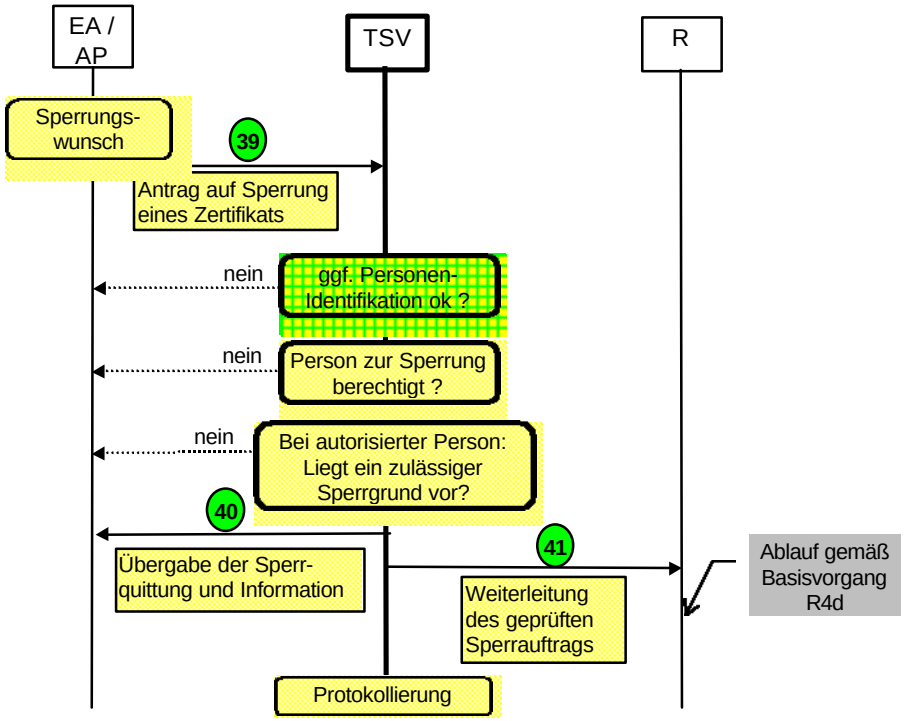
5.2.7 Zertifikatssperrung durch Endanwender oder autorisierte Person (TSV4)

Die Sperrung kann durch den Endanwender selbst [24] (Eigensperrung) oder durch eine für Sperrungen autorisierte Person der Institution (Fremdsperrung) veranlaßt werden.

Der Sperrantrag kann auf verschiedene Weise beim Teilnehmerservice gestellt werden.

Einige Beispiele, wie der Sperrantrag gestellt werden kann:

- Persönliche Vorsprache beim Teilnehmerservice (Identifikation i.d.R durch Vorlage des Lichtbildausweises)
- Via signierter E-Mail (Identifikation i.d.R. durch Prüfung der Signatur)
- Via Telefonanruf unter Nennung des Sperrkennworts (Identifikation nicht notwendig, da die Nennung des Sperrkennworts zur Sperrung autorisiert)
- Via Telefonanruf ohne Nennung des Sperrkennworts (ggfs. mit Rückruf. Bei unsicherer Identifikation ggfs. Aufforderung zur persönlichen Vorsprache)

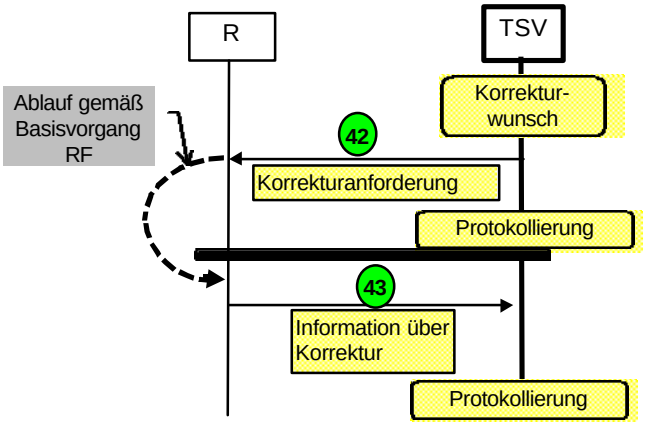


Ablaufdiagramm 7: TSV4: Sperrung eines Endanwenderzertifikats

[24] Der Fall „Sperrung einer Zertifizierungsstellen-Zertifikats“ ist ein *Sondervorgang* und somit von der Leitung der Zertifizierungsstelle zu planen und durchzuführen.

5.2.8 Fehlerkorrektur am Verzeichnis (TSVF)

Ein Fehlerkorrektur bzgl. veröffentlichter Daten (im Verzeichnis) kann durch alle Stellen und Instanzen initiiert werden. Im Falle, daß der Teilnehmerservice Korrekturbedarf erkennt, wird sie einen entsprechenden Korrekturhinweis an die Instanz Registrierung der betroffenen Zertifizierungsstelle übermitteln, die dieses überprüft und ggfs. eine Korrektur initiiert. Die Korrektur kann ausschließlich über die Instanz Registrierung initiiert werden.



Ablaufdiagramm 8: TSVF: Korrekturanforderung

5.3 Basisvorgänge in der Instanz Registrierung (R)

Die Basisvorgänge in der Instanz Registrierung können instanzen-extern (durch Aufträge anderer Instanzen) als auch instanzen-intern (auf eigene Initiative hin) ausgelöst werden.

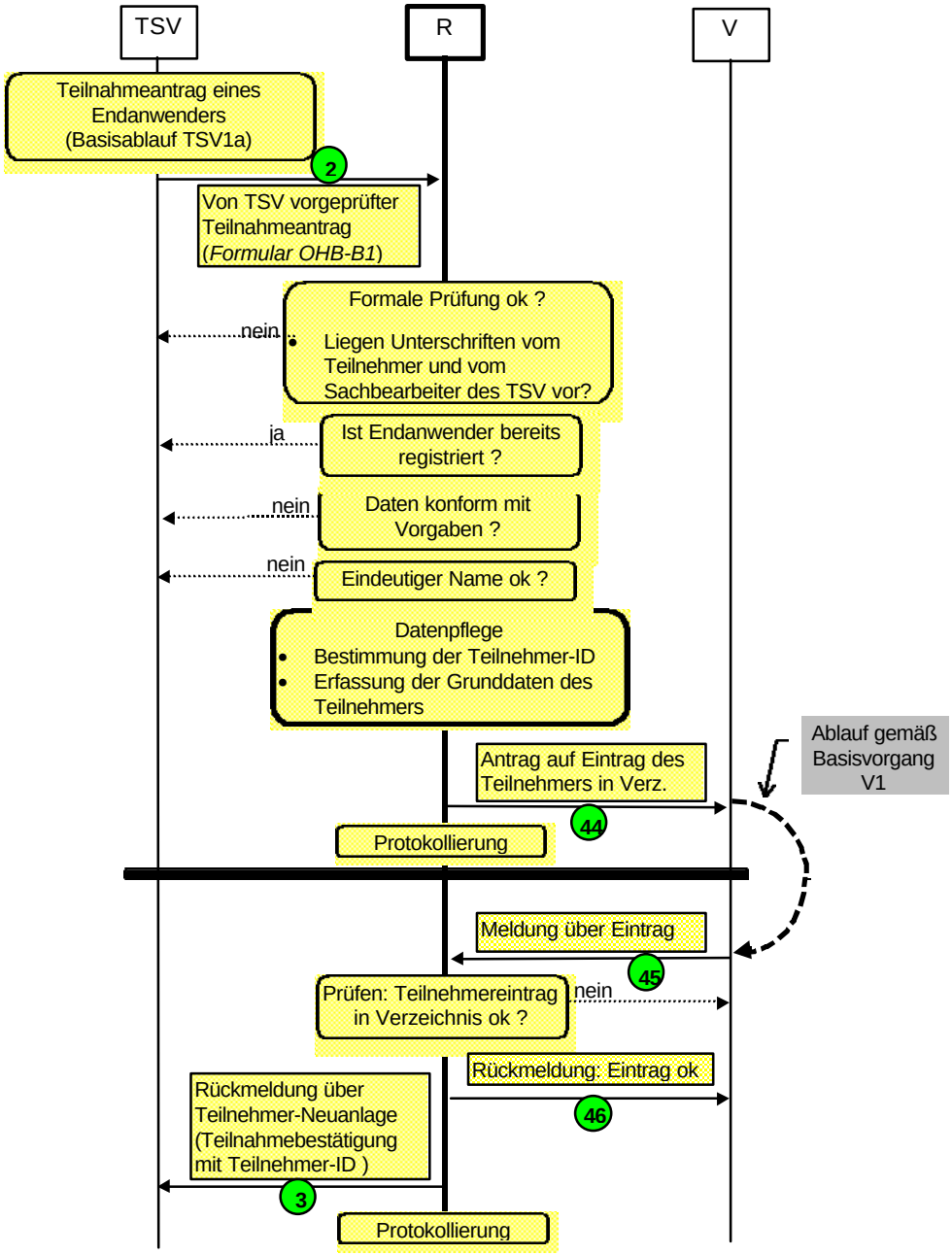
Folgender Basisvorgänge werden instanzen-intern regelmäßig zeitlich angetriggert:

- **Veranlassen von Zertifikatsverlängerungen**: Regelmäßig muß der Datenbestand daraufhin überprüft werden, ob Zertifikate durch Überschreiten des Gültigkeitszeitraums ungültig werden. In diesen Fällen ist zu prüfen, ob eine Zertifikatsverlängerung in Frage kommt (Basisvorgang R3).
- **Stichprobenhaftes Überprüfen des Verzeichnisses** über die öffentliche Verzeichnisschnittstelle durch Abgleich mit eigenem Datenbestand (Basisvorgang R8).

Die Basisvorgänge R-SPHINX-1 und R-SPHINX-2 sind projektspezifisch.

5.3.1 Endanwenderregistrierung (R1a)

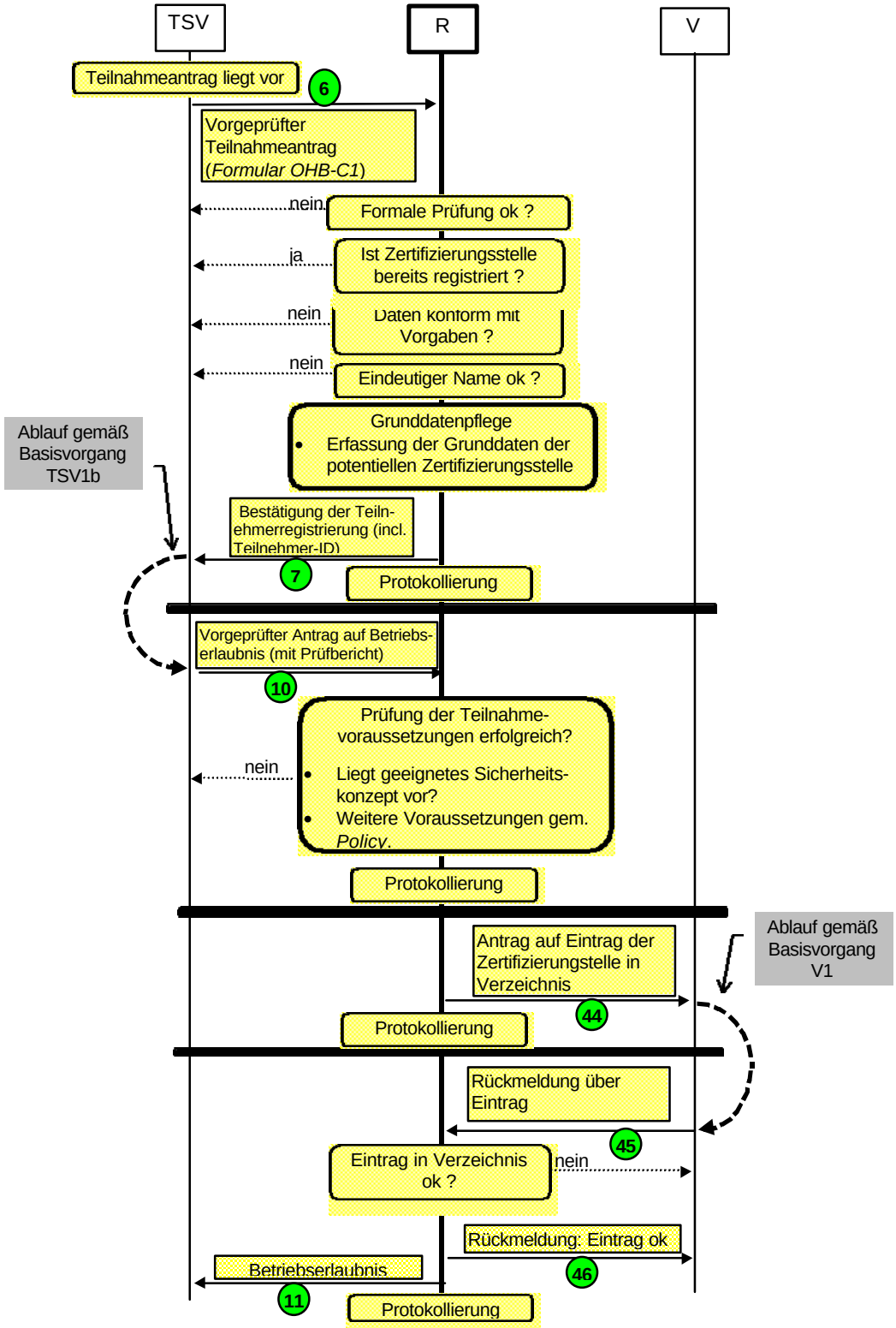
Die Registrierung und die Neuanlage eines Endanwenders wird durch die Instanz Teilnehmerservice vorbereitet und durch die Instanz Registrierung weitergeführt und abgeschlossen.



Ablaufdiagramm 9: R1a: Registrierung eines Endanwenders

5.3.2 Zertifizierungsstellen-Registrierung (R1b)

Die Registrierung einer neuen Zertifizierungsstelle erfolgt mehrstufig (siehe einleitende Bemerkungen zu Basisvorgang TSV1b).

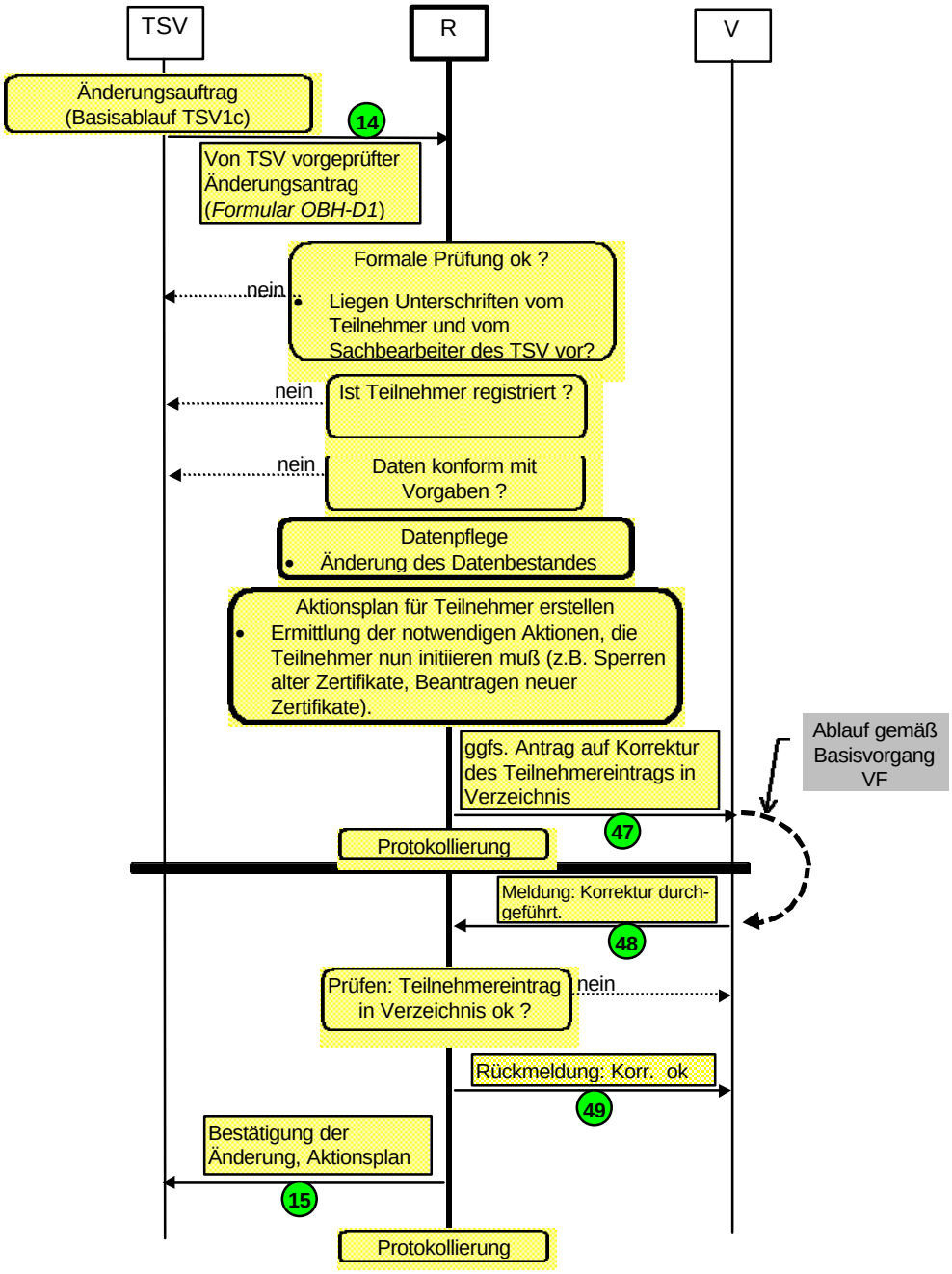


Ablaufdiagramm 10: R1b: Registrierung einer Zertifizierungsstelle

5.3.3 Änderungsauftrag eines Teilnehmers (R1c)

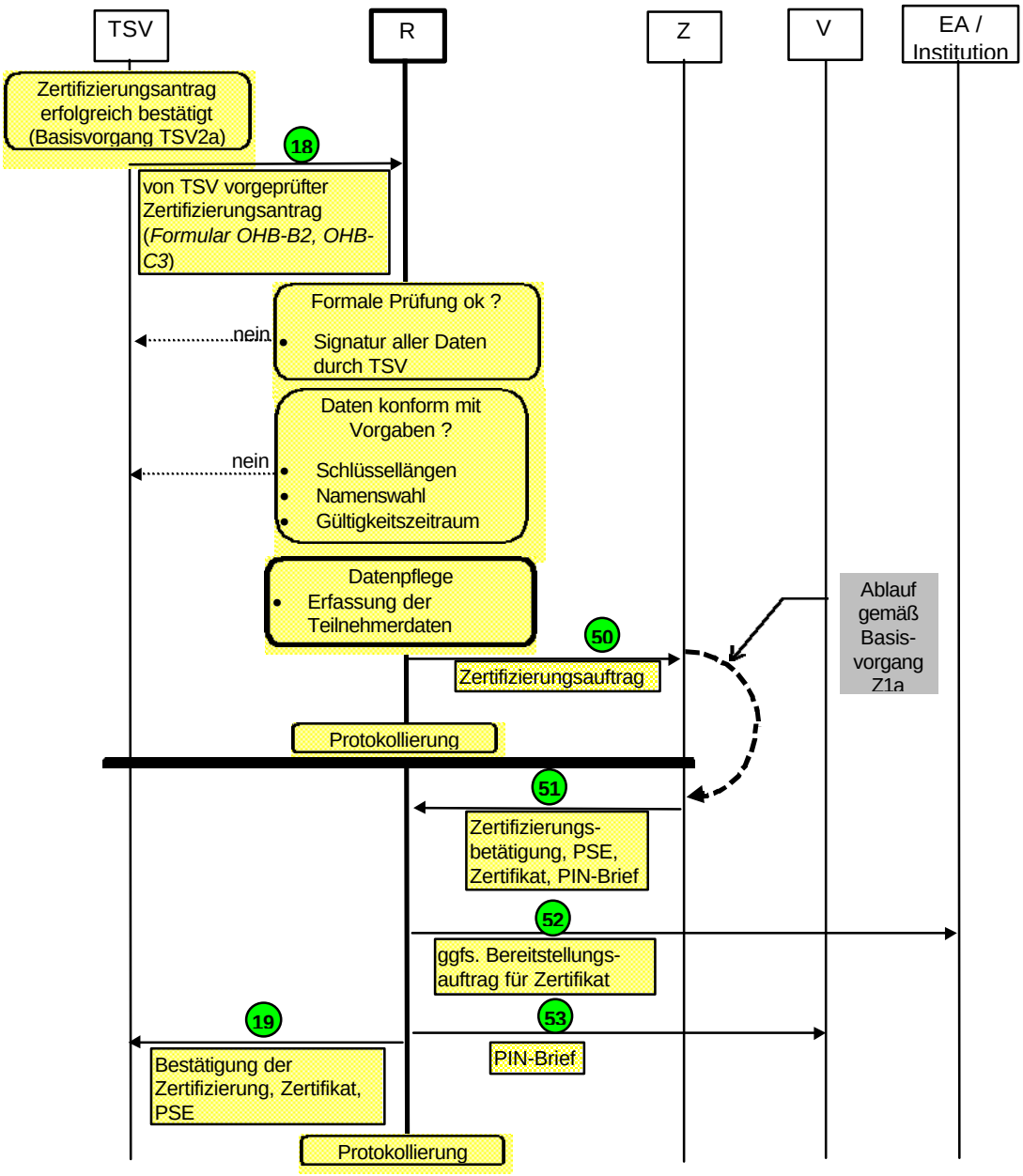
Ein Änderungsauftrag wird durch die Instanz Teilnehmerservice vorbereitet und durch die Instanz Registrierung weitergeführt und abgeschlossen.

Hinweis: Es werden nicht alle an der Änderung implizierten Basisvorgänge automatisch durchgeführt, da die Auswirkungen hier zu komplex sind und z.T. neue Anträge im Original durch den Teilnehmer zu unterzeichnen sind. Zur Unterstützung des Teilnehmers wird ermittelt, welche Aktionen dieser nun praktisch einleiten muß.



Ablaufdiagramm 11: R1c: Änderungsauftrag eines Teilnehmers

5.3.4 Teilnehmerzertifizierung (zentr. Schlüsselgenerierung) (R2a)

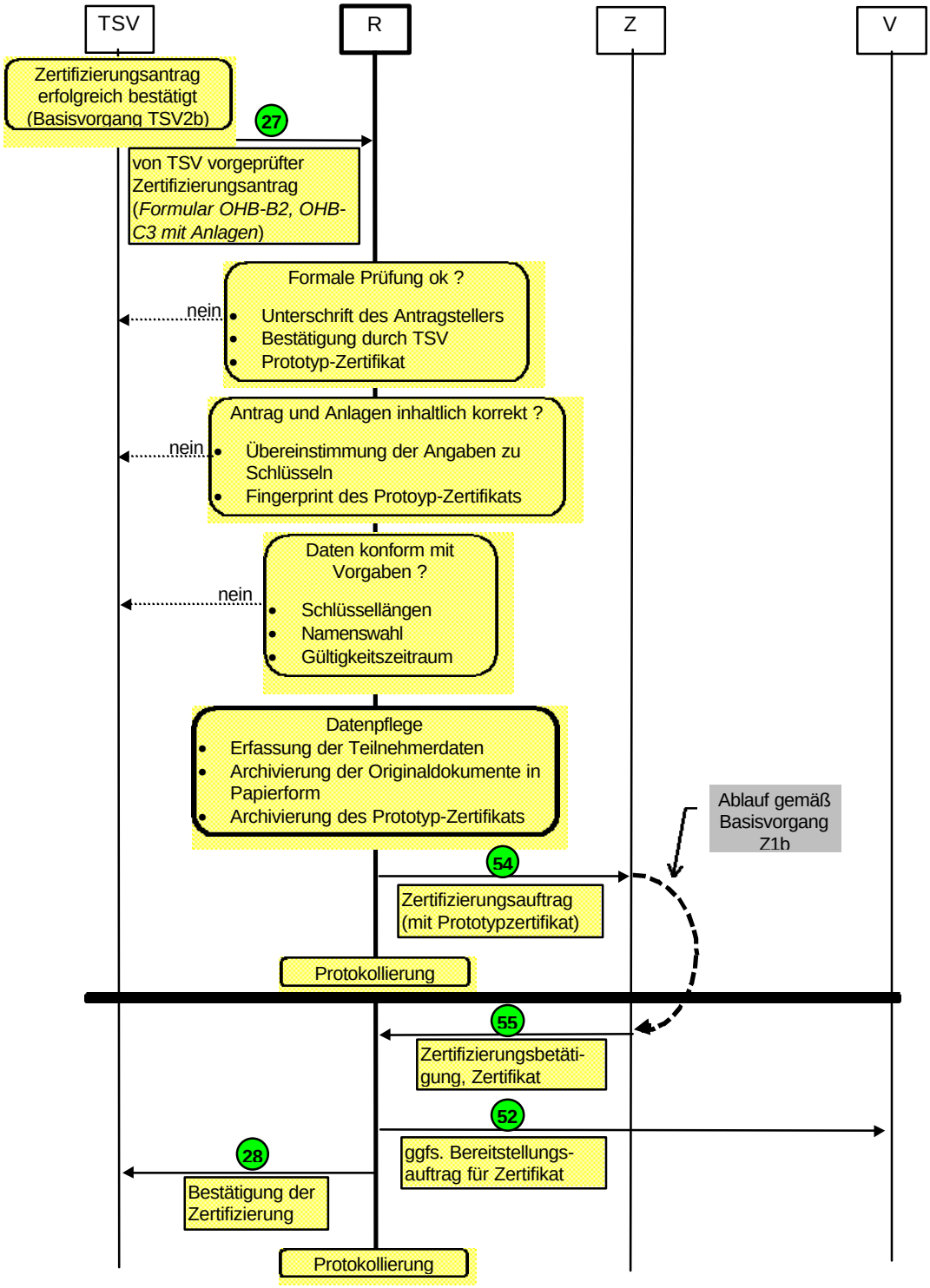


Ablaufdiagramm 12: R2a: Teilnehmerzertifizierung (bei zentraler Schlüsselgenerierung)

5.3.5 Teilnehmerzertifizierung (dezentr. Schlüsselgenerierung) (R2b)

Voraussetzung: Alle Bestandteile einer Teilnehmerzertifizierung liegen vor (Bestätigter Zertifizierungsantrag, Anlagen: Prototyp-Zertifikat des Teilnehmers, ggfs. Schlüsselausdruck). Erst dann wird der Antrag auf Teilnehmerzertifizierung bearbeitet. Sollten nicht alle Bestandteile vorliegen, obliegt es der Registrierungsstelle, geeignete Maßnahmen zur Anforderung dieser Bestandteile festzulegen (zu .a. zeitlichen Limits und der Abläufe).

Festlegung: Der Zertifizierungsantrag muß stets im Original, d.h. in Papierform, vorliegen. D.h. der Teilnehmerservice muß dieses der Registrierung z.B. per gesichertem Postbrief zustellen. Im Rahmen dieser Zustellung sollten alle weiteren Anlagen ebenfalls dieser Sendung beigelegt werden (auf geeigneten Datenträgern wie z.B. Disketten), damit diese stets zusammenbleiben.



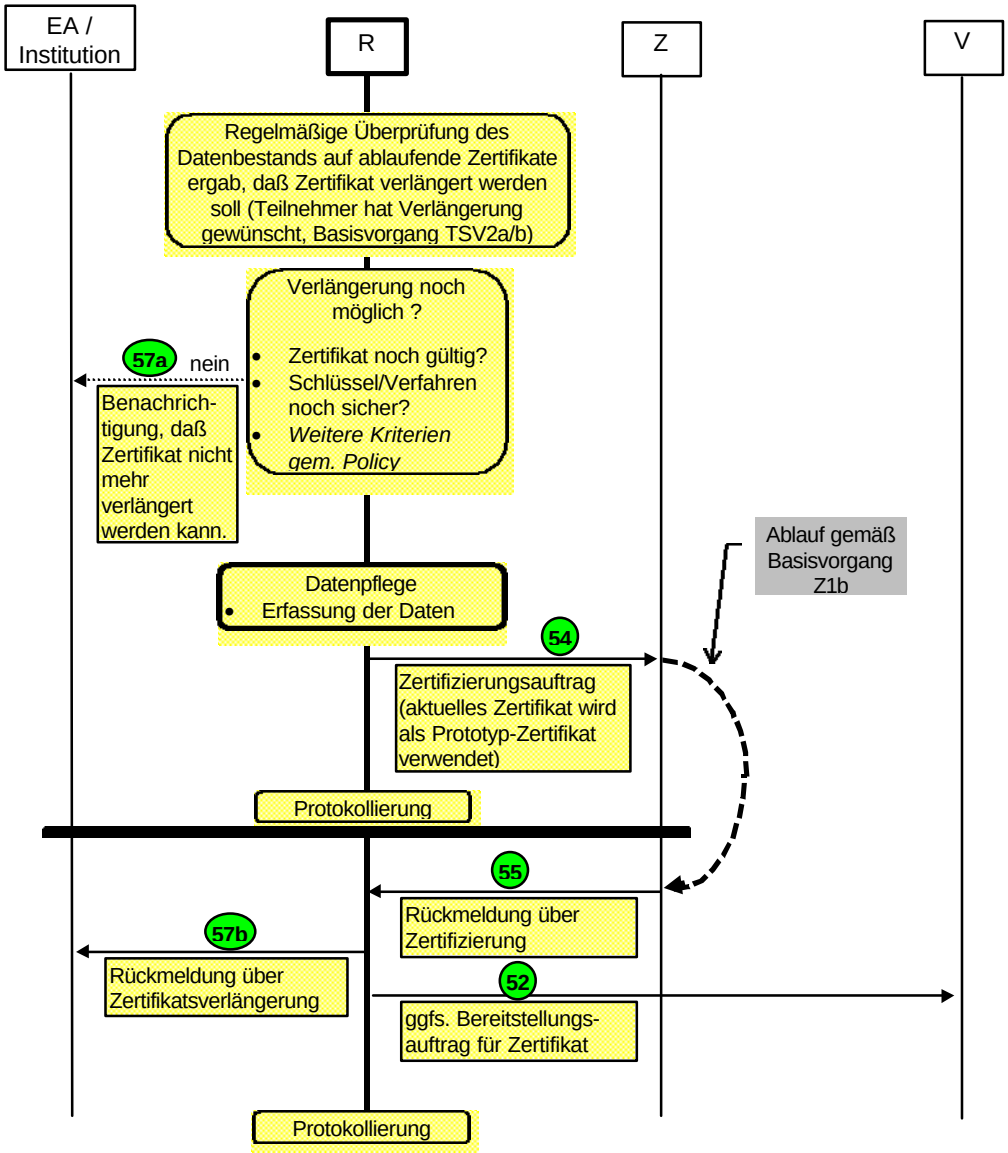
Ablaufdiagramm 13: R2b: Teilnehmerzertifizierung (bei dezentraler Schlüsselgenerierung)

5.3.6 Zertifikatsverlängerung (R3)

Zertifikatsverlängerung erfolgt stets aufgrund des des Wunsches des Teilnehmers, das ablaufende Zertifikat rechtzeitig automatisch verlängern zu lassen (in Formular zur Zertifizierung ankreuzbar).

Die Prüfung auf zu verlängernde Zertifikate erfolgt regelmäßig und automatisch innerhalb der Instanz Registrierung und muß nicht von einer anderen Instanz angestoßen werden.

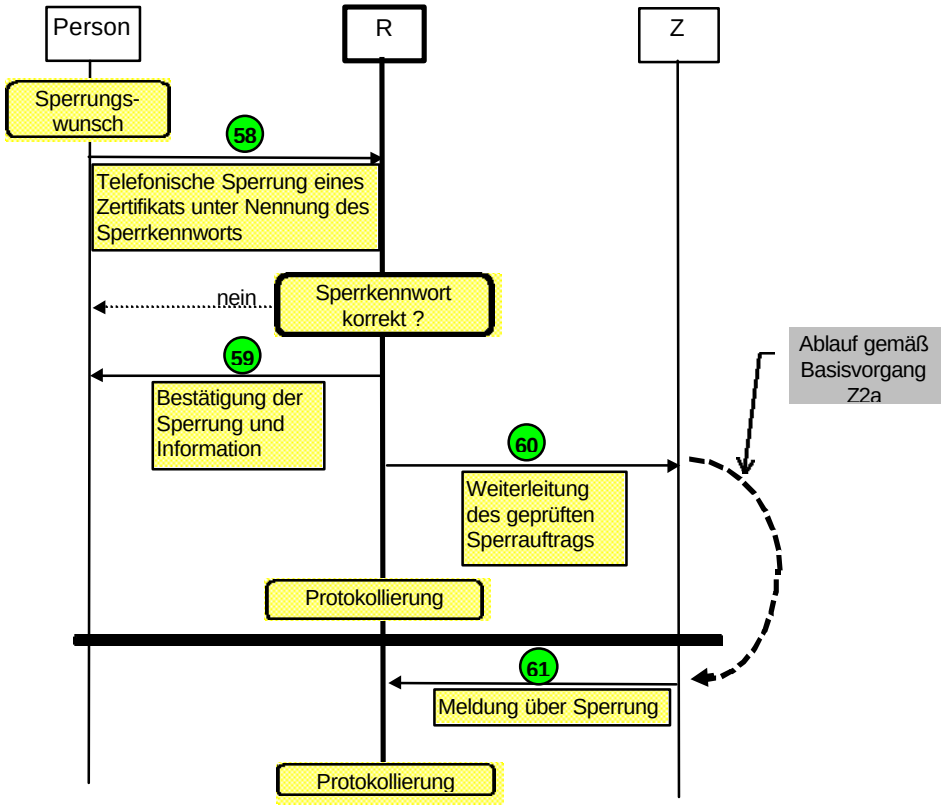
Hinweis: Die Zertifikatsverlängerung erfolgt dabei stets nach dem „dezentralen Verfahren“, d.h. es erfolgt keine neue Schlüssel- und PSE-Generierung (über diese verfügt der Teilnehmer bereits). Dabei ist es unerheblich, nach welchem Verfahren der ursprüngliche Zertifizierungsantrag gestellt wurde.



Ablaufdiagramm 14: R3: Zertifikatsverlängerung

5.3.7 Telefonische Zertifikatssperrung mit Sperrkennwort (R4a)

Ein Zertifikat kann telefonisch durch den Teilnehmer gesperrt werden. Dieser muß sich durch das Sperrkennwort authentisieren.

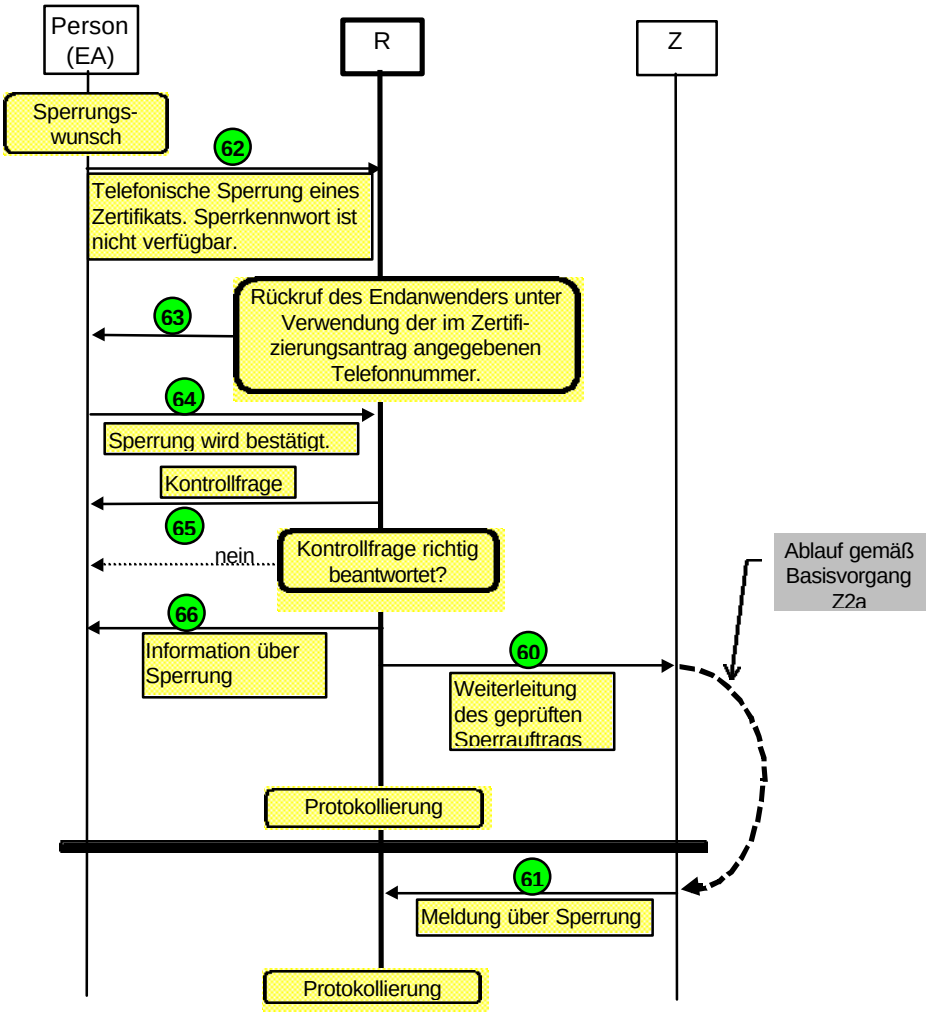


Ablaufdiagramm 15: R4a: Sperrung eines EA-Zertifikats unter Nutzung des Sperrkennworts

5.3.8 Telefonische Zertifikatssperrung durch Endanwender mit Rückruf (R4b)

Ein EA-Zertifikat kann telefonisch durch den Endanwender auch ohne Sperrkennwort gesperrt werden. In diesem Fall muß die Instanz Registrierung den Endanwender zurückrufen - erst dann kann die Sperrung entgegengenommen werden. Eine Sperrung durch die autorisierte Person ist auf diesem Wege nicht möglich (da Sperrberechtigung nicht überprüft werden kann).

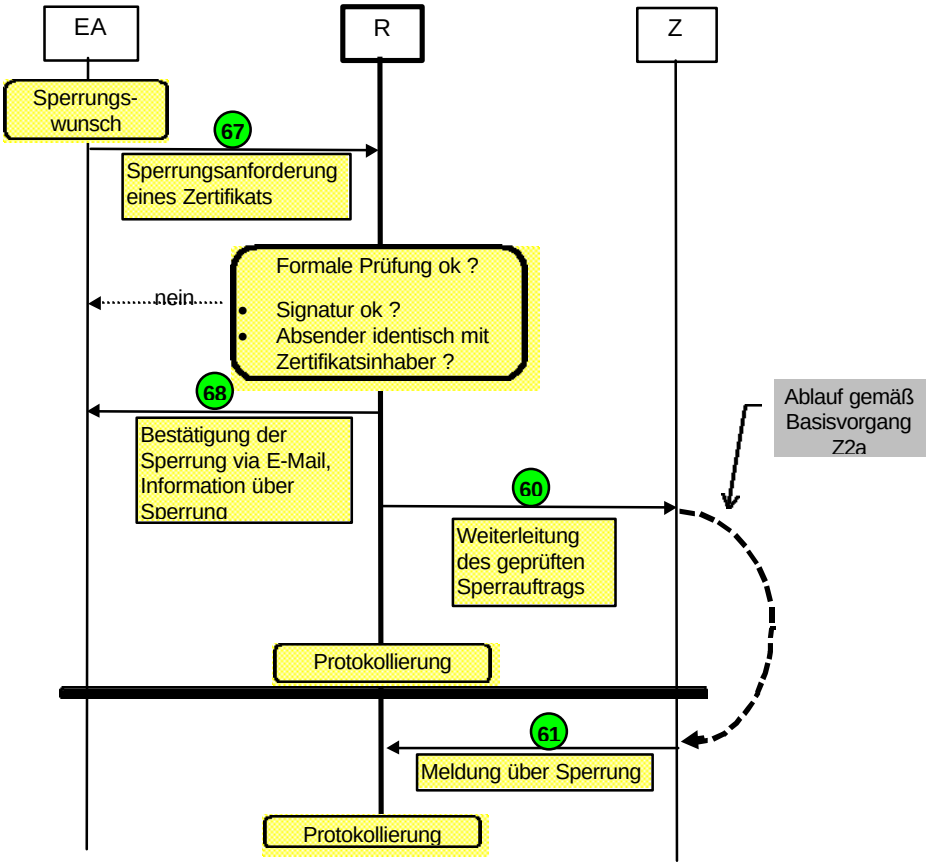
Es ist zur Erhöhung der Sicherheit (nämlich, daß es sich bei der anrufenden Person um den Endanwender handelt) eine *Kontrollfrage* zu stellen. Diese Kontrollfrage kann sich auf beliebige Aspekte aus dem Teilnahme- oder Zertifizierungsantrag beziehen. Nur der Endanwender sollte in der Lage sein, die Kontrollfrage richtig zu beantworten. Das Betriebshandbuch zur Zertifizierungsstelle enthält Hinweise zur korrekten Verwendung von Kontrollfragen.



Ablaufdiagramm 16: R4b: Sperrung eines EA-Zertifikats mit Rückruf

5.3.9 Zertifikatssperrung durch Endanwender via E-Mail (R4c)

Ein EA-Zertifikat kann via E-Mail durch den Endanwender gesperrt werden. In diesem Fall muß die Sperranforderung für das zu sperrende Zertifikat durch den Endanwender selbst signiert sein. Dieses darf auch mit dem Schlüssel erfolgen, welcher mit dem zu sperrenden Zertifikat assoziiert ist. Eine Sperrung durch die autorisierte Person ist auf diesem Wege nicht möglich (da Sperrberechtigung nicht überprüft werden kann).

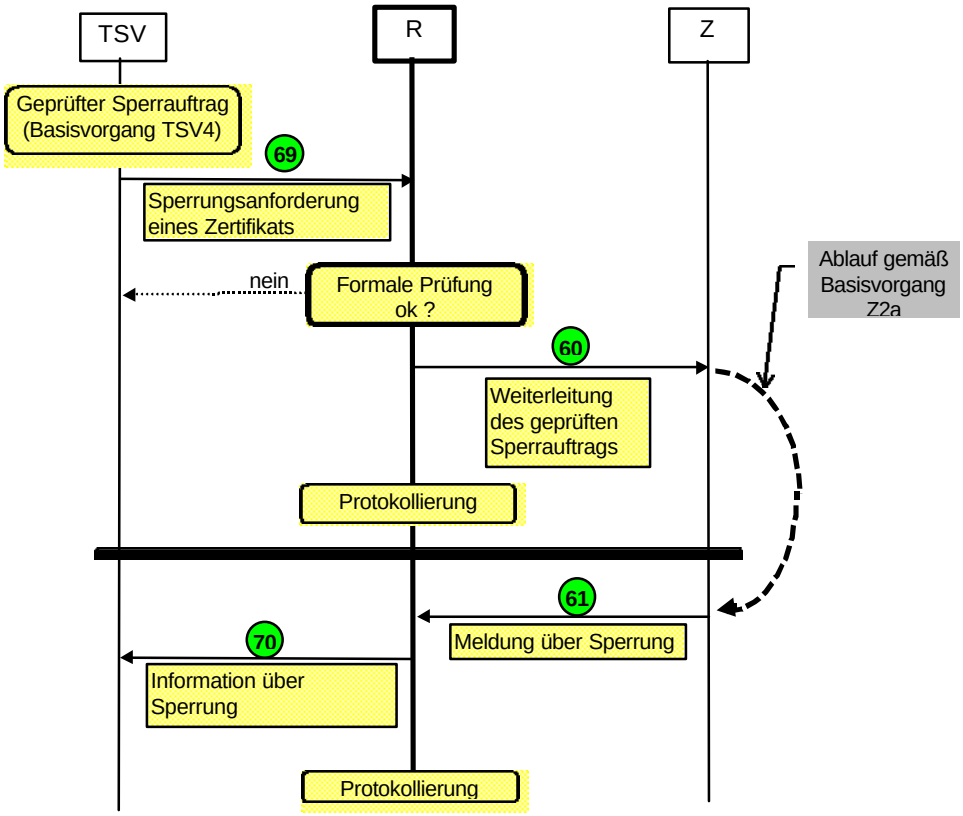


Ablaufdiagramm 17: R4c: Sperrung eines EA-Zertifikats via E-Mail

Hinweis: Bei Kompromittierung des PSE des Endanwenders durch einen Angreifer kann auch der Angreifer die Sperrung des Zertifikats veranlassen. Dieses ist aber hinnehmbar, da in diesem Falle die Verwendung des Zertifikats nicht mehr möglich sein sollte.

5.3.10 Zertifikatssperrung durch Endanwender oder autorisierte Person via Teilnehmerservice (R4d)

Ein Zertifikat kann durch den Endanwender oder eine autorisierte Person via Teilnehmerservice gesperrt werden. In diesem Fall wird die Sperranforderung durch den TSV geprüft und an die Registrierung weitergeleitet.

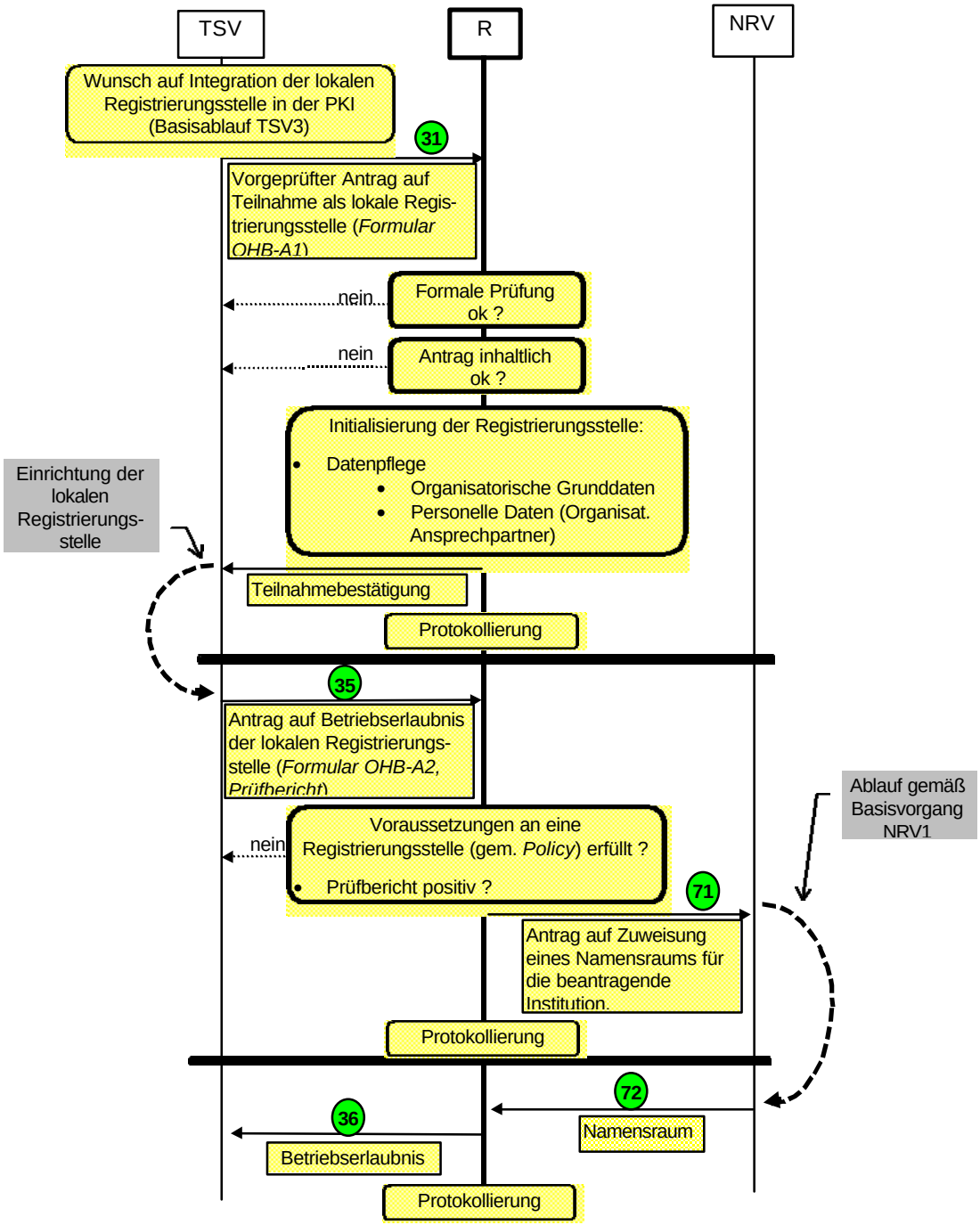


Ablaufdiagramm 18: R4d: Sperrungsanforderung via Teilnehmerservice

5.3.11 Registrierung einer lokalen Registrierungsstelle (R5)

Soll eine neue lokale Registrierungsstelle innerhalb der PKI integriert werden, erfolgt eine feste Zuordnung zur Instanz Registrierung einer Zertifizierungsstelle (*selbst- oder fremdbestimmte Zuordnung*). Diese Instanz wird für die Registrierungsstelle die Schnittstelle zur PKI bilden.

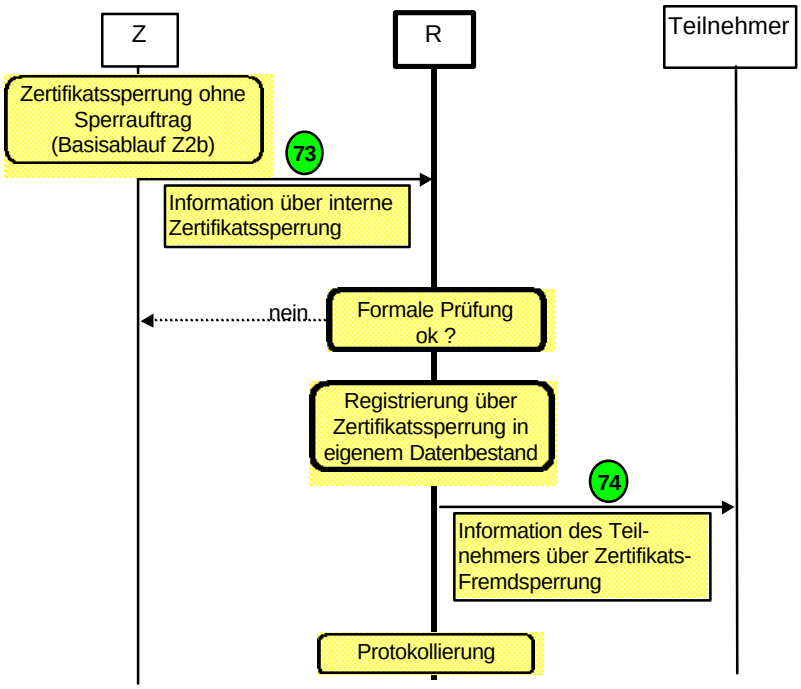
Damit die lokale Registrierungsstelle mit der zuständigen Instanz Registrierung Vorgänge abwickeln kann, muß sie zunächst bei dieser registriert werden.



Ablaufdiagramm 19: R5: Registrierung einer lokalen Registrierungsstelle

5.3.12 Weitermeldung einer ZS-getriggerten Zertifikatssperrung (R6)

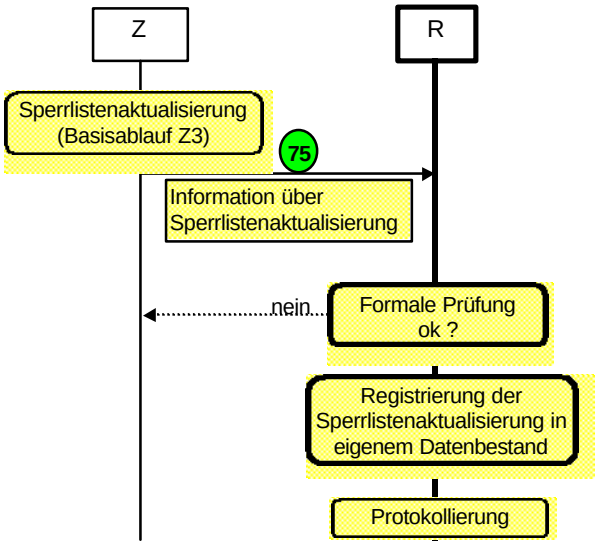
Im Falle einer Zertifikatssperrung, die auf Initiative der Zertifizierungsstelle vorgenommen wurde (Zertifikatssperrung ohne Sperrauftrag, Basisvorgang Z2b), muß der Teilnehmer über diese Fremdsperrung benachrichtigt werden. Die Benachrichtigung erfolgt direkt durch die Instanz Registrierung der Zertifizierungsstelle.



Ablaufdiagramm 20: R6: Weitermeldung einer ZS-internen Zertifikatssperrung

5.3.13 Übernahme der Sperrlistenaktualisierung (R7)

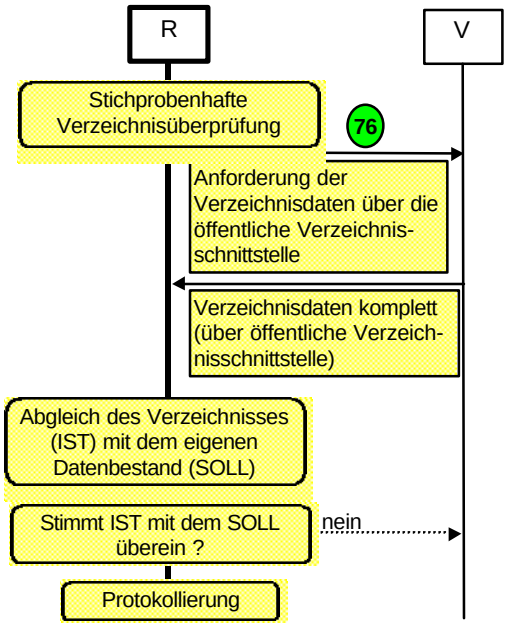
Im Falle einer Sperrlistenaktualisierung, die auf Initiative der Instanz Zertifizierung vorgenommen wurde (Basisvorgang Z3), erfolgt eine Meldung darüber an die Instanz Registrierung. Diese muß in den Datenbestand der Instanz Registrierung eingepflegt werden.



Ablaufdiagramm 21: R7: Information über Sperrlistenaktualisierung übernehmen

5.3.14 Überprüfung des Verzeichnisses (R8)

Die Instanz soll aus Gründen der Qualitätssicherung regelmäßig die Daten des Verzeichnisses überprüfen. Dazu ist es notwendig, die Daten über die öffentliche Verzeichnisschnittstelle (und nicht über die internen Schnittstelle zur Instanz Verzeichnis) anzufordern, um die Überprüfung möglichst realitätsnah durchzuführen.



Ablaufdiagramm 22: R8: Überprüfung des Verzeichnisses

5.3.15 R-Verteiler (R-SPHINX-1)

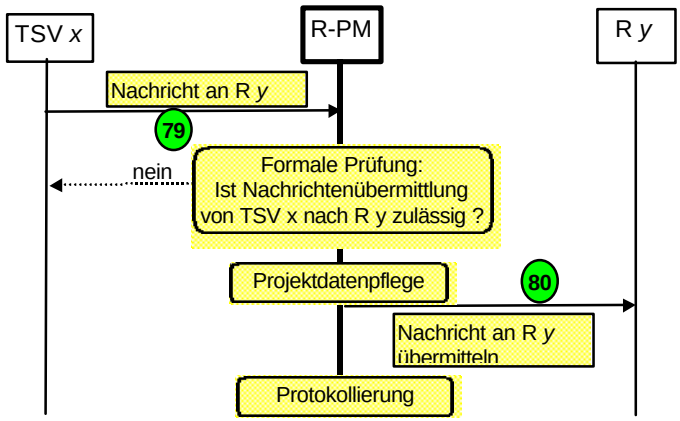
Die Aufgabe „R-Verteiler“ kann einer Instanz Registrierung innerhalb der PKI zugeordnet werden (R-PM: Diejenige Instanz Registrierung, die das Projektmanagement in SPHINX unterstützt), wenn zusätzliche projektspezifische Aufgaben dieses erfordern. Das ist im Projekt SPHINX der Fall:

- Um die zur Zeit teilweise noch fehlende Interoperabilität zwischen den Endanwenderprodukten und den Zertifizierungstools gegenüber den lokalen Registrierungsstellen/Endanwendern transparent (im Sinne von „nicht sichtbar“) zu machen, wurde im Projekt SPHINX mit dem „R-Verteiler“ eine zusätzliche „Zwischenschicht“ zwischen den Instanzen Teilnehmerservice und den Instanzen Registrierung eingeführt. Die gesamte Kommunikation zwischen TSVs und den Rs wird über den R-Verteiler abgewickelt.Es sind an zentraler Stelle projektspezifische Daten zu pflegen.

Der R-Verteiler ist transparent für die beteiligten Instanzen lokale Registrierungsstelle und der Instanzen Registrierung der Zertifizierungsstellen:

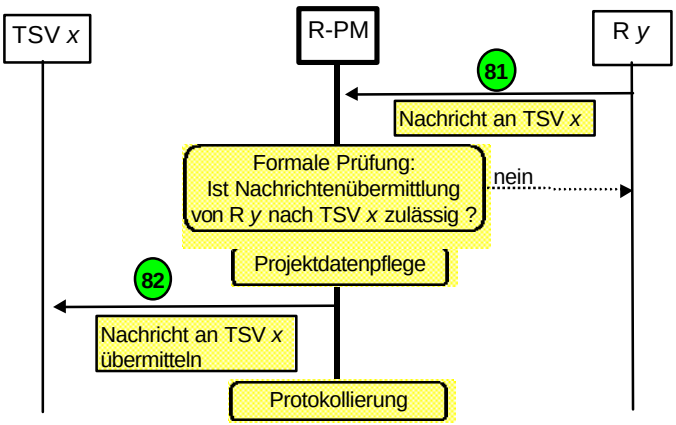
- Transparent ist der R-Verteiler für die lokalen Registrierungsstellen, da diese die ihnen zugeordneten Instanzen Registrierung direkt adressieren, die Nachrichten aber an den R-Verteiler schicken. Fällt der R-Verteiler nach Projektabschluß ersatzlos weg, werden die lokalen Registrierungsstellen ihre Nachrichten direkt an die betreffenden Instanzen Registrierung der Zertifizierungsstellen schicken.
- Transparent ist der R-Verteiler für die Instanzen Registrierung der Zertifizierungsstellen, da diese die ihnen zugeordneten lokalen Registrierungsstellen direkt adressieren, die Nachrichten aber an den R-Verteiler schicken. Fällt der R-Verteiler nach Projektabschluß ersatzlos weg, weden die Instanzen Registrierung der Zertifizierungsstellen ihre Nachrichten direkt an die betreffenden lokalen Registrierungsstellen schicken.

Hinweis: Der „R-Verteiler“ kann ersatzlos entfallen, wenn die mit ihr realisierten „virtuellen“ (d.h. indirekten) Kommunikationsverbindungen „real“ exisitieren. Für die betroffenen Stellen bzw. Instanzen bedeutet diese Umstellung lediglich eine Änderung der Sendeadresse, die Nachrichten selbst bleiben unverändert.



Ablaufdiagramm 23: R-SPHINX-1: Nachricht von TSV *x* an R *y* übermitteln

Bei einer eingehenden Nachricht einer Instanz Teilnehmerservice überprüft der R-Verteiler formal, ob sie der adressierten Instanz Registrierung der Zertifizierungsstelle auch zugeordnet ist. Ist sie es, dann kann die Nachricht weitergeleitet werden. Ist sie es nicht, erfolgt eine entsprechende Fehlermeldung an die Instanz Teilnehmerservice.



Ablaufdiagramm 24: R-SPHINX-1: Nachricht von R *y* an TSV *x* übermitteln

Bei einer eingehenden Nachricht der Instanz Registrierung einer Zertifizierungsstelle überprüft der R-Verteiler formal, ob sie der adressierten Instanz Teilnehmerservice auch zugeordnet ist. Ist sie es, dann kann die Nachricht weitergeleitet werden. Ist sie es nicht, erfolgt eine entsprechende Fehlermeldung an die Instanz Registrierung der Zertifizierungsstelle.

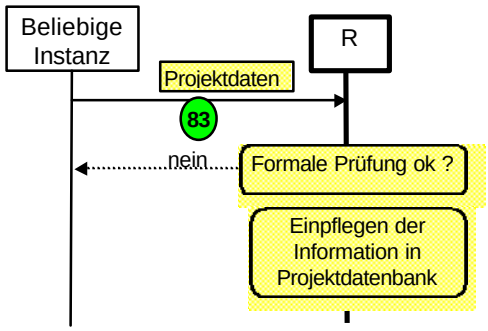
5.3.16 Projektdatenpflege (R-SPHINX-2)

Die Aufgabe „Projektdatenpflege“ kann einer Instanz Registrierung innerhalb der PKI zugeordnet werden, wenn zusätzliche projektspezifische Aufgaben dieses erfordern. Das ist im Projekt SPHINX der Fall: Die Instanz Registrierung, die R-Verteiler zur Verfügung stellt, wird ebenfalls die Projektdaten pflegen.

Projektdaten sind organisatorische Daten und Statusdaten, die innerhalb der PKI anfallen, die aber nicht im Rahmen der normalen PKI-Tätigkeit erfasst und ausgewertet werden.

Projektdaten können von allen Stellen und Instanzen (inkl. des projektspezifischen R-Verteilers) explizit für die Projektdatenpflege übermittelt werden. Welche Daten dafür bereitzustellen sind, ist in den Abläufen der jeweils betroffenen Instanz spezifiziert.

Hinweis: Die Instanz „Projektdatenpflege“ wird ersatzlos entfallen, wenn das Projekt SPHINX beendet wird. Für die betroffenen Instanzen bedeutet diese Umstellung lediglich, daß diese keine Daten mehr für die Projektdatenpflege übermitteln müssen.



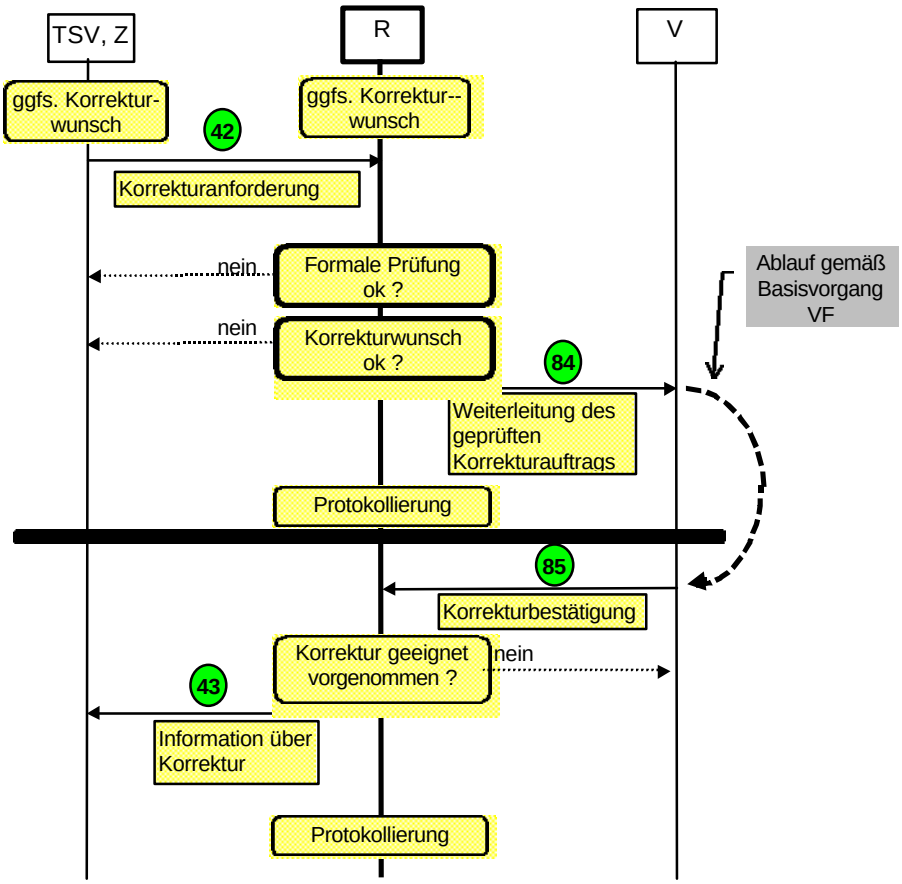
Ablaufdiagramm 25: R-SPHINX-2: Projektdatenpflege

5.3.17 Fehlerkorrekturanforderung bzgl. veröffentlichter Daten (RF)

Ein Fehlerkorrektur bzgl. veröffentlichter Daten (im Verzeichnis) kann durch alle Instanzen initiiert werden. Im Falle, daß die Registrierung Korrekturbedarf erkennt, wird eine Korrektur initiiert.

Hinweis: Alle Korrekturanforderungen werden über die Instanz Registrierung abgewickelt.

Ein Fehlerkorrektur bzgl. veröffentlichter Daten (im Verzeichnis) kann durch alle Instanzen initiiert werden. Im Falle, daß der Teilnehmerservice oder die Zertifizierung Korrekturbedarf erkennen, wird eine entsprechende Korrekturanforderung an die Instanz Registrierung gerichtet.

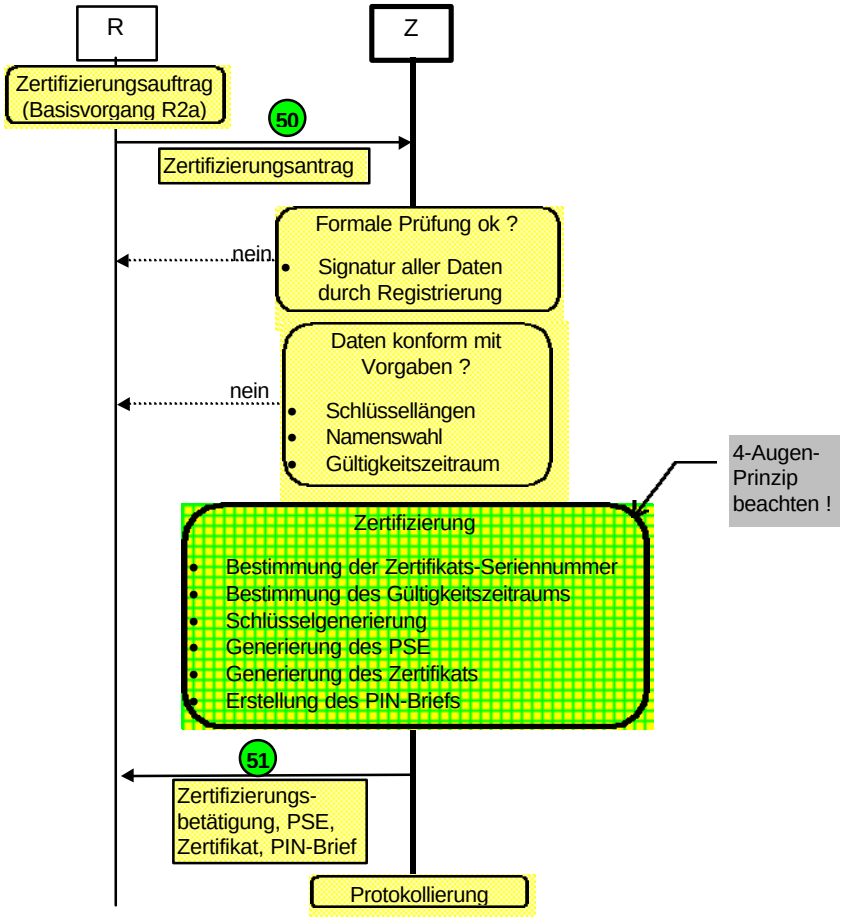


Ablaufdiagramm 26: RF: Korrekturanforderung

5.4 Basisvorgänge in der Instanz Zertifizierung (Z)

5.4.1 Teilnehmerzertifizierung bei zentraler Schlüsselgenerierung (Z1a)

Die Zertifizierung wird für die Teilnehmer der Zertifizierungsstelle durchgeführt. Teilnehmer können Endanwender als auch Zertifizierungsstellen sein.

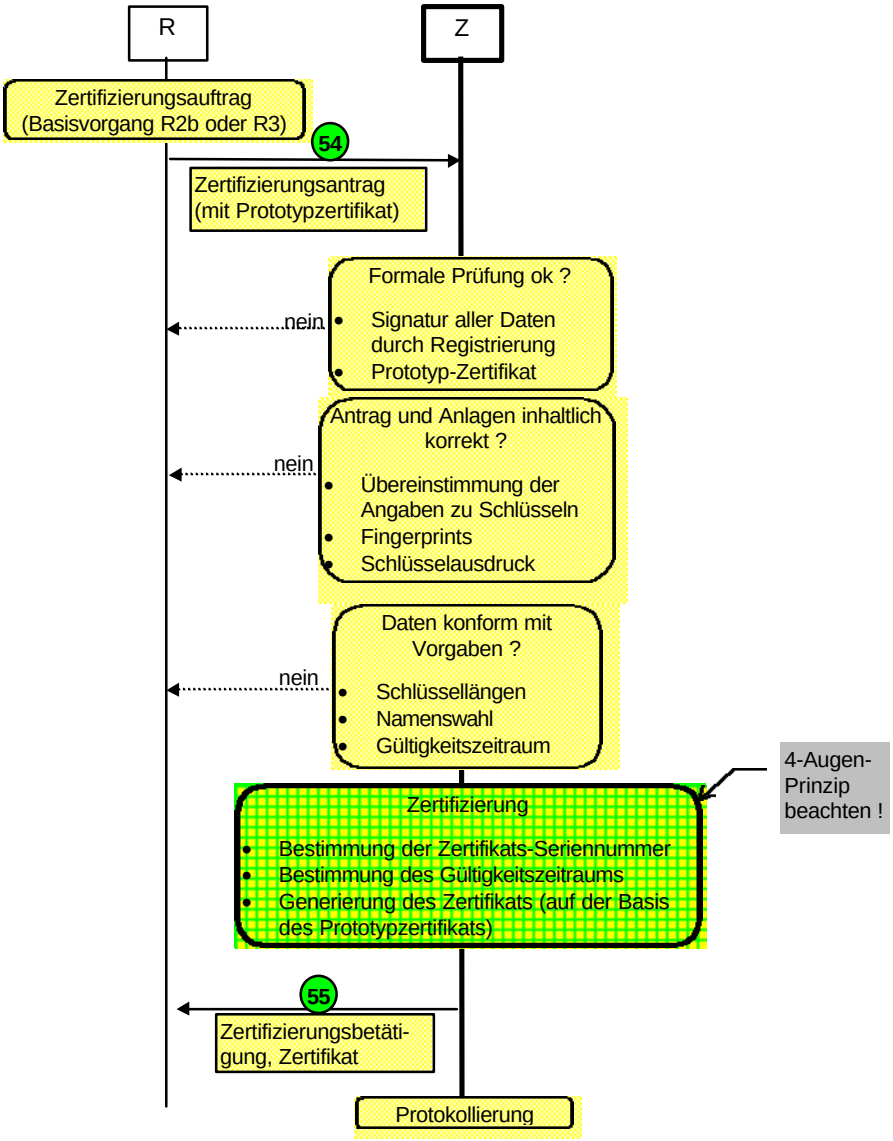


Ablaufdiagramm 27: Z1a: Teilnehmerzertifizierung (bei zentraler Schlüsselgenerierung)

5.4.2 Teilnehmerzertifizierung bei dezentraler Schlüsselgenerierung (Z1b)

Die Zertifizierung wird für die Teilnehmer der Zertifizierungsstelle durchgeführt. Teilnehmer können dabei Endanwender als auch Zertifizierungsstellen sein.

Hinweis zum Vorgang Zertifikatsverlängerung: Die Teilnehmerzertifizierung (dez. SE) wird beim Vorgang „Zertifikatsverlängerung“ (R3) angewandt. Als Prototypzertifikat dient hierbei das ursprüngliche Teilnehmer-Zertifikat („Ur-Zertifikat“). Es ist bei der Zertifikatsverlängerung unerheblich, nach welchem Verfahren (zentrale oder dezentrale Schlüsselgenerierung) das zugrundeliegende Ur-Zertifikat erzeugt wurde, da das dazugehörige PSE nicht betroffen ist (Schlüssel werden nicht verändert).

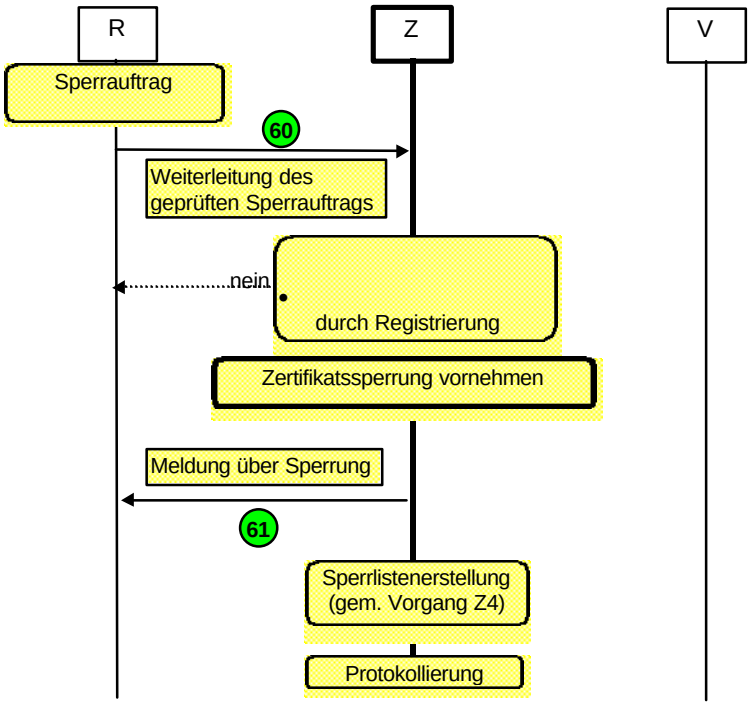


Ablaufdiagramm 28: Z1b: Teilnehmerzertifizierung (bei dezentraler Schlüsselgenerierung)

5.4.3 Zertifikatssperrung mit Sperrauftrag (Z2a)

Eine Zertifikatssperrung kann von der Instanz Registrierung mittels eines Sperrauftrags veranlaßt werden.

Hinweis: Zertifikate, die gesperrt werden oder abgelaufen sind, werden *nicht* aus dem Verzeichnis entfernt.

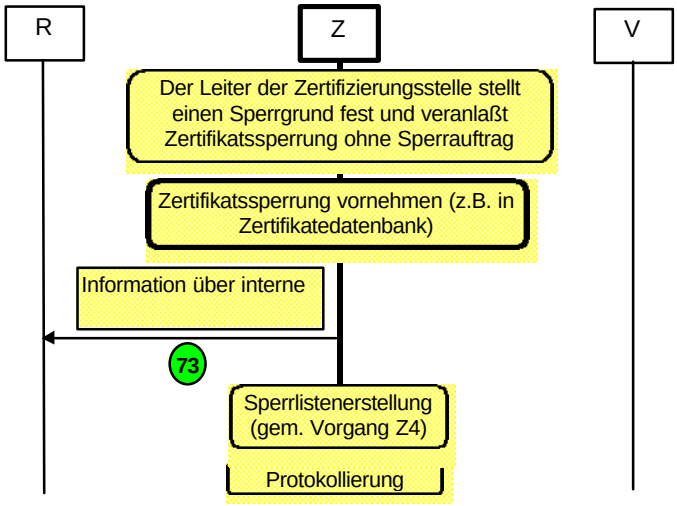


Ablaufdiagramm 29: Z2a: Sperrung aufgrund eines Sperrauftrags

5.4.4 Zertifikatssperrung ohne Sperrauftrag (Z2b)

Eine Zertifikatssperrung ohne Sperrauftrag erfolgt ausschließlich bei *besonderen Ereignissen*, die eine sofortige Sperrung erfordern. Beispielsweise kann der IT-Sicherheitsbeauftragter einen Notfall bzgl. der Schlüsselverwendung feststellen (z.B. Kompromittierung von Schlüsseln der Zertifizierungsstelle oder Wurzelzertifizierungsstelle) und alle Zertifikate eines ganzen Zertifizierungspfads sperren lassen wollen. Dieses ist *kein* Standardvorgang und muß vom Leiter der Zertifizierungsstelle geplant und durchgeführt werden.

Hinweis: Zertifikate, die gesperrt werden oder abgelaufen sind, werden *nicht* aus dem Verzeichnis entfernt.

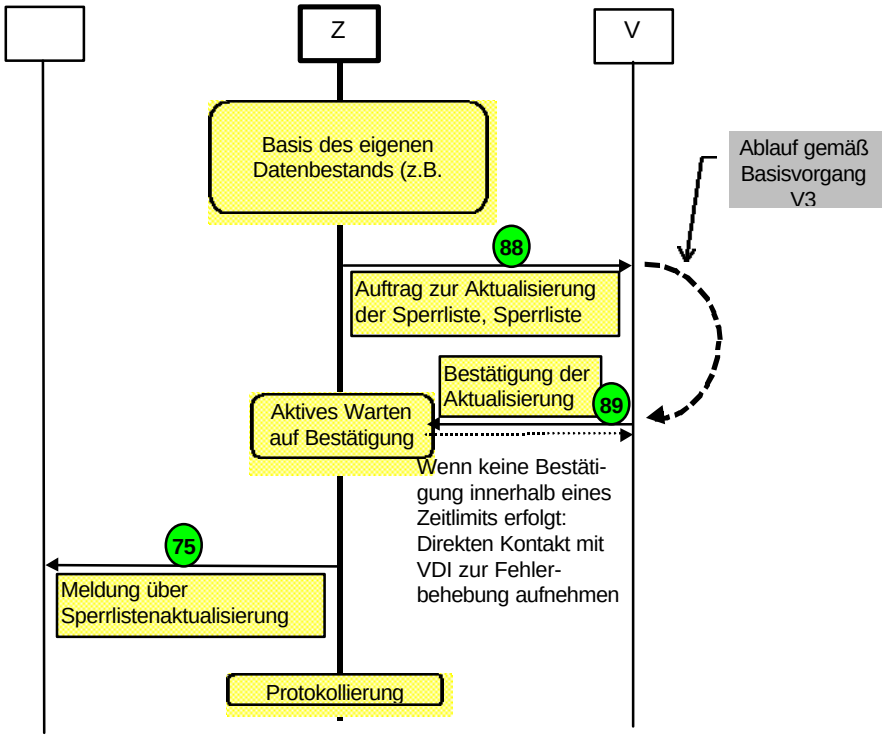


Ablaufdiagramm 30: Z2b: Sperrung durch Zertifizierungsstelle (ohne Sperrauftrag)

5.4.5 Sperrlistenaktualisierung (Z3)

Die Sperrlistenaktualisierung kann instanz-intern als auch -extern veranlaßt werden. Alle *Policy* aufgeführt.

- Aktualisierung der Sperrliste unverzüglich vorgenommen werden (extern veranlaßte
- rechtzeitig eine Aktualisierung vorzunehmen (intern veranlaßte Sperrlisten-erstellung).



31: Z3: Sperrlistenaktualisierung

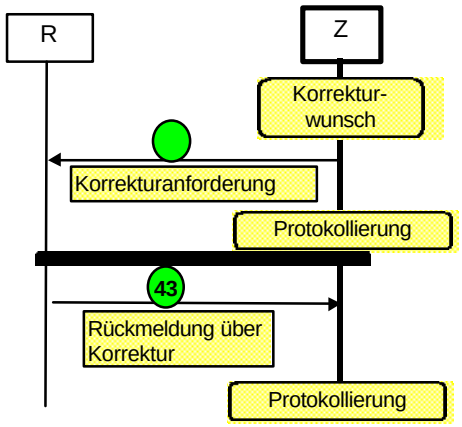
Der Sperrlistenbereitstellung im Verzeichnis wird hohe Priorität zugewiesen. Daher übermittelt die Instanz Zertifizierung der Instanz Verzeichnis die Sperrlisten . Zudem ist ein „aktives Warten“ auf die Bestätigung durch das Verzeichnis unverzichtbar. Sollte keine *Policy* angegeben sein muß) durch das

Maßnahmenempfehlung: Die Zertifizierung sollte nach jeder Sperrlistenaktualisierung die

Darüberhinaus sollte diese Kontrolle auch ohne vorangegangene Aktualisierung stichprobenhaft vorgenommen werden.

5.4.6 Fehlerkorrekturanforderung bzgl. veröffentlichter Daten (ZF)

Ein Fehlerkorrektur bzgl. veröffentlichter Daten im Verzeichnis kann durch alle Stellen und Instanzen initiiert werden. Im Falle, daß die Instanz Zertifizierung Korrekturbedarf erkennt, wird sie einen entsprechenden Korrekturhinweis an die Instanz Registrierung übermitteln, die dieses überprüft und ggfs. eine Korrektur initiiert. Die Korrektur kann ausschließlich über die Registrierung initiiert werden, da sonst Inkonsistenzen bei der Pflege der *Teilnehmer*daten bzw. Projektdaten möglich sind.



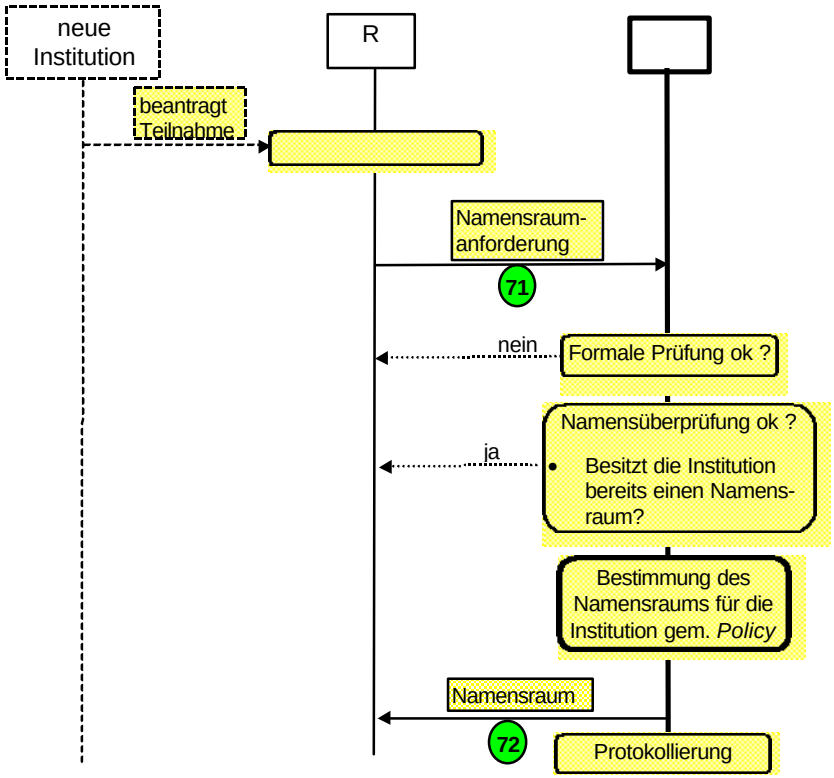
Ablaufdiagramm 32: ZF: Korrekturanforderung

5.5 Basisvorgänge in der Instanz Namensraumvergabe (NRV)

Die Instanz Namensraumvergabe weist einer neuen Teilnehmerinstitution (die einen Teil-

PKI-exklusiven Namensraum zu.

5.5.1 Namensraumvergabe (NRV1)



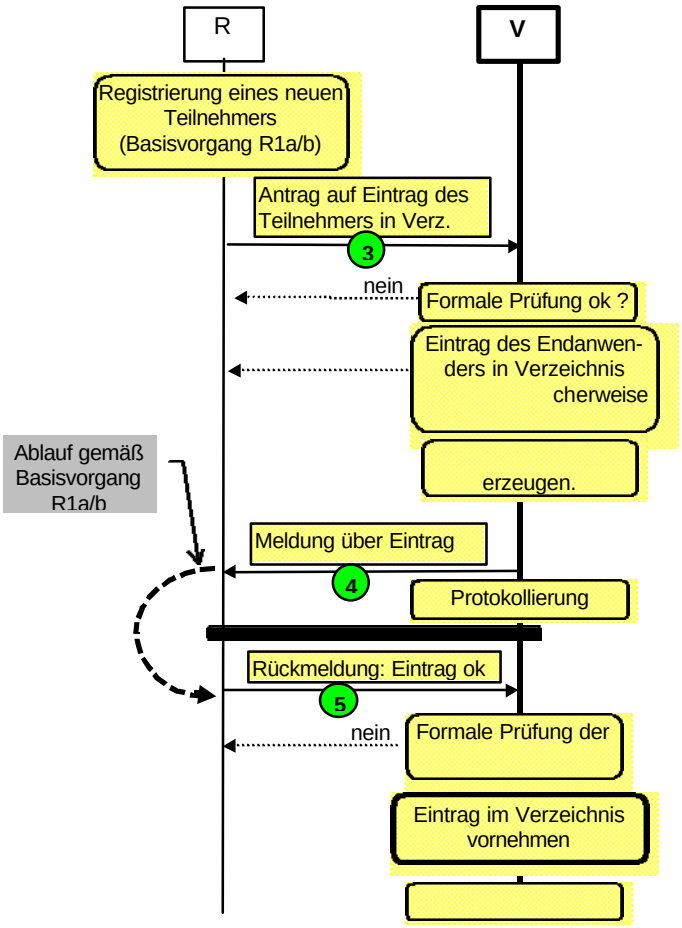
Ablaufdiagramm : NRV1: Namensraumvergabe

5.6 Basisvorgänge in der Instanz Verzeichnis (V)

5.6.1 Basisdateneintrag für Teilnehmer (V1)

Bevor für einen Teilnehmer Zertifikate im Verzeichnis der Zertifizierungsstelle aufgenommen werden können, muß dort ein entsprechender Verzeichnis-Eintrag vorgenommen werden.

Hinweis zum Eintrag einer Zertifizierungsstelle: Beim Eintrag einer Zertifizierungsstelle erfolgt zusätzlich das Anlegen einer Dummy-Sperrliste.



Ablaufdiagramm 34: V1: Basisdateneintrag für Teilnehmer

5.6.2 Zertifikatsaktualisierung (V2)

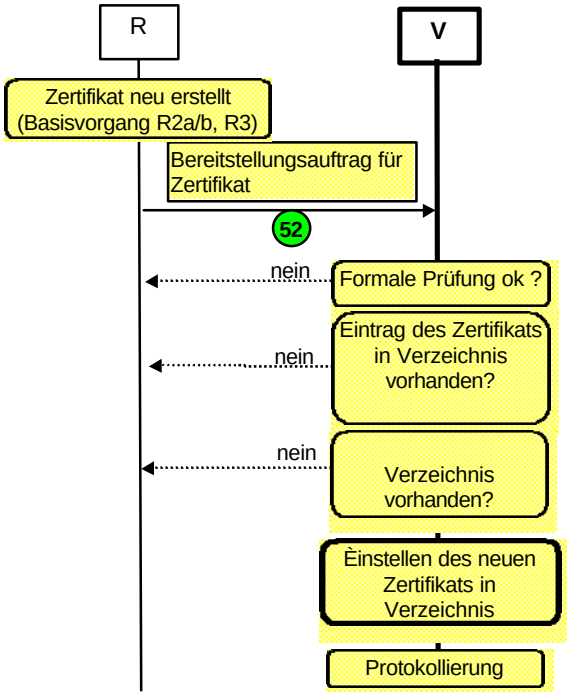
Die Aktualisierung eines Zertifikats ist in folgenden Fällen erforderlich:

- Gültigkeitsdauer wird demnächst ablaufen (oder ist bereits abgelaufen).
- Das bisher gültige Zertifikat wurde gesperrt und wird durch ein neues ersetzt.

Hinweis 1: Eine Aktualisierung kann sowohl mit als auch ohne Schlüsselwechsel auf die gleiche Weise durchgeführt werden, da eine Differenzierung dieser Fälle für das Verzeichnis nicht relevant ist.

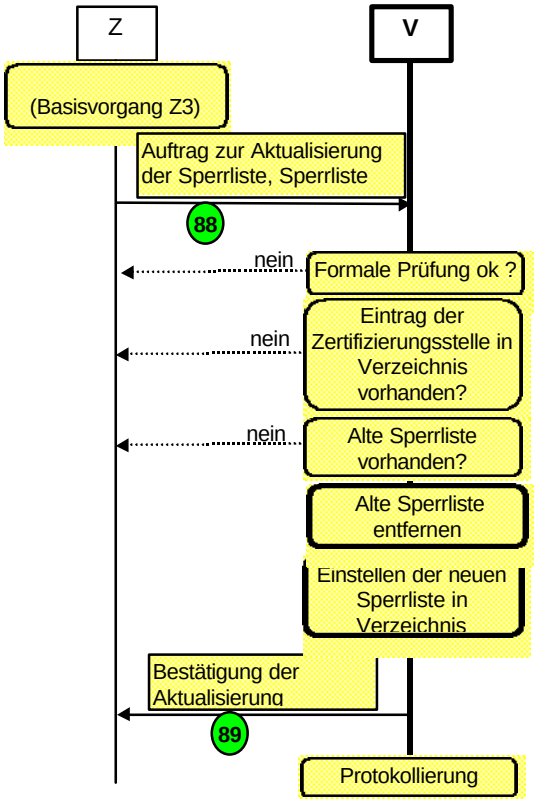
Hinweis 2: Eine Aktualisierung kann sowohl für Endanwender- als auch Zertifizierungsstellen-Zertifikate auf die gleiche Weise durchgeführt werden, da eine Differenzierung dieser Fälle für das Verzeichnis nicht relevant ist.

Hinweis 3: Das alte Zertifikat wird bei Aktualisierung nicht entfernt.



Ablaufdiagramm 35: V2: Zertifikatsaktualisierung

5.6.3 Sperrlistenaktualisierung (V3)



Ablaufdiagramm 36: V3: Aktualisierung einer Sperrliste

5.6.4 Fehlerkorrektur im Verzeichnis (VF)

Die Veröffentlichung von Zertifikaten und Sperrlisten erfolgt z.Z. nicht unter Anwendung des sicheren Drei-Wege-Protokolls (siehe hierzu z.B. MailTrusT Version 2), d.h. auf eine explizite Freischaltung von Zertifikaten und Sperrlisten durch den Auftrageber bzw. Endanwender wird verzichtet. Daher ist es notwendig, eine dazu alternative Möglichkeit der Korrektur falsch veröffentlichter Daten zu spezifizieren.

Das Veröffentlichung von Zertifikaten und Sperrlisten erfolgt in SPHINX grundsätzlich ohne Bestätigung des Auftraggebers allein auf der Grundlage der übermittelten Daten. Dabei können Fehler auftreten. Stellt der Auftraggeber oder der Teilnehmer nach Veröffentlichung im Verzeichnis fest (z.B. durch Anfordern des Zertifikats via Internet), daß die Daten nicht in seinem Sinne veröffentlicht wurden, ist eine Fehlerbehebung notwendig.

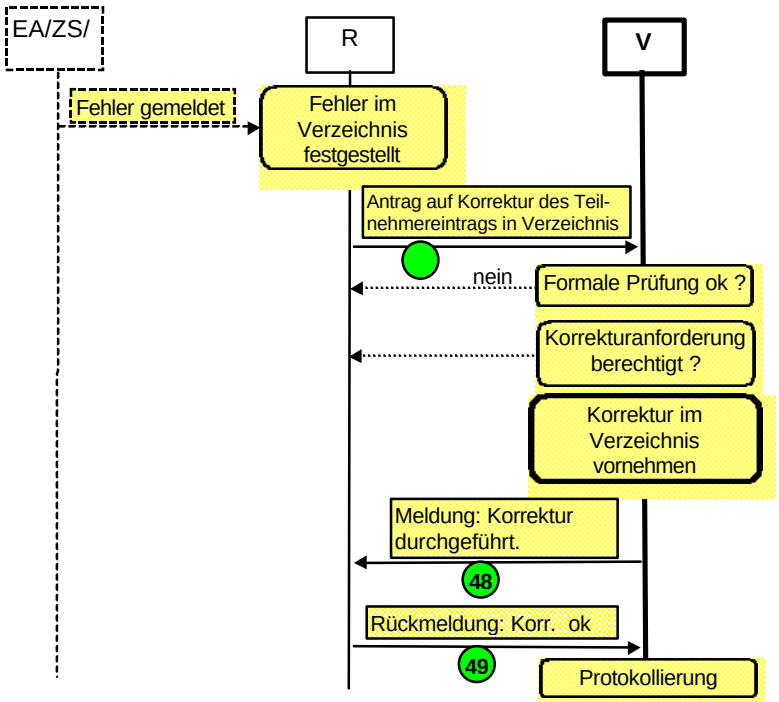
Einige Beispiele fehlerhafter Veröffentlichung:

- Es werden falsche Zertifikatinformationen veröffentlicht.
- Es werden Zertifikatinformationen an der falschen Stelle veröffentlicht.
- Eine Zertifikatsperrung spiegelt sich nicht in der betroffenen Sperrliste wieder.

Korrekturanforderungen werden von den folgenden Stellen initiiert:

- die Zertifizierungsstelle bzgl. fehlerhafter Sperrlisten und Endanwender-Zertifikate
- die Wurzelzertifizierungsstelle bzgl. fehlerhafter Wurzel- und Zertifizierungs-stellenzertifikate und Wurzel-Sperrlisten

Der Endanwender muß sich bei Korrekturanforderung an die lokale Registrierungsstelle wenden, die sich wiederum an die Registrierung der Zertifizierungsstelle wendet. Diese wird dann bei dem Verzeichnis die Korrekturanforderung initiieren.



Ablaufdiagramm 37: VF: Korrektur im Verzeichnis vornehmen

6 Einrichtung von Stellen

6.1 Allgemeine Hinweise zur Einrichtung einer Stelle

1. **Die Integration neuer Stellen grundsätzlich jederzeit möglich**

Die Integration weiterer Stellen in die PKI ist jederzeit möglich. Siehe hierzu auch die Modellierung der PKI in den Kapiteln 3.2.1 (Gesamtmodell), 3.2.2 (Stellen) und 3.2.3 (Dienste, Instanzen, Aufgaben - ohne Unterkapitel 3.2.3.x)

2. **Initiative zur Einrichtung neuer Stellen**

In der Regel wird die Initiative zur Einrichtung neuer Stellen entweder von der PKI-Gesamtleitung oder von einer einzelnen Institution ausgehen. In beiden Fällen wird eine Institution die neue Stelle betreiben.

3. **Auswirkung auf die bestehende Infrastruktur**

Werden typische Stellen (Registrierungsstelle, Zertifizierungsstelle) eingerichtet oder neue Stellen zur Ausgliederung bestimmter, bereits existierender Instanzen aufgebaut, so sind in der Regel keine oder nur geringfügige Auswirkungen auf die übrigen Stellen der PKI zu erwarten.

Sollen jedoch Stellen eingerichtet werden, um neuartige, bislang nicht etablierte Dienste und Instanzen in die PKI einzubringen, so kann dies eine neue Architektur der PKI bedeuten. In diesem Fall muß eine Neubestimmung der Gesamt-PKI erfolgen, die Einfluß auch auf bereits bestehende Stellen und ihre Konfiguration haben kann.

4. **Standard- und Nicht-Standard-Stelle**

Es ist zur Zeit eine *Standard-Stelle* spezifiziert, die problemlos in die PKI zu integrieren ist: Die *lokale Registrierungsstelle*. Ihre Integration ist standardmäßig in der PKI vorgesehen - es gibt hierzu einen eigenen Leitfaden und entsprechende Antragsformulare für interessierte Institutionen (siehe hierzu Kapitel 6.2). Die Integration anderer Stellen (sog. *Nicht-Standard-Stellen*) kann eine funktionale Umstrukturierung der PKI-Gesamtstruktur bedeuten, die nur im Einzelfall zwischen PKI-Management und Institution geklärt werden kann.

5. **Allgemeine Vorgehensweise**

Folgende Schritte sind in der Regel zu unternehmen, um eine neue Stelle der PKI einzurichten:

- ggfs. Vorabklärung der Teilnahme zwischen Institution und PKI-Management (trifft in der Regel nur für Nicht-Standard-Stellen zu)
- Antrag auf Teilnahme
- Bestätigung der Teilnahme
- Antrag auf Betriebserlaubnis
- Betriebserlaubnis
- Betrieb der Stelle

6. **Checklisten**

Um eine neue Stelle in die bestehende Public-Key-Infrastruktur einbetten zu können, müssen diverse Voraussetzungen seitens der PKI-Gesamtleitung und seitens der Institution erfüllt sein. Die Prüfung der Voraussetzungen erfolgt anhand von allgemeinen Checklisten.

6.1 **Allgemeine Checkliste für die Institution, die eine neue Stelle betreiben möchte**

Folgende Checkliste soll es ermöglichen, die allgemein zur Einrichtung einer neuen Stelle erforderlichen Rahmenbedingungen, Voraussetzungen und Arbeitsschritte zu prüfen und zu begleiten:

- Soll eine Standard-Stelle (zur Zeit nur die lokale Registrierungsstelle) oder eine Nicht-Standard-Stelle realisiert werden?
- Falls eine Standard-Stelle realisiert werden soll:
    - Beschaffung der verfügbaren Informationen über die Voraussetzungen an Einrichtung und Betrieb (Leitfaden und Antragsformulare)
    - Klärung in der Institution, ob die geforderten Voraussetzungen erfüllt werden sollen bzw. können:
        - Voraussetzungen an die Zielgruppe: Ist der Teilnehmerkreis, für die diese Stelle eingerichtet werden soll, kompatibel zur Zielgruppe von SPHINX?
        - Technische Voraussetzungen: Die Institution muß für den Betrieb der Stelle einen geeignet ausgestatteten Arbeitsplatz einrichten. Dieses betrifft u.a. die Rechnerausstattung (Hard- und Software, Vernetzung).
        - Organisatorische Voraussetzungen: Die Institution muß bereit und fähig sein, die organisatorische Mindestanforderungen zu erfüllen. Dieses betrifft u.a. die Sicherstellung des Datenschutzes innerhalb der Stelle.
        - Personelle Voraussetzungen: Die Institution muß die Rollen (siehe Rollenmodell), die für die Stelle vorgesehen sind, geeignet durch Personal besetzen.
        - Infrastrukturelle Voraussetzungen: Die Institution muß u.a. geeignete Räume für die Stelle zur Verfügung stellen.
        - Grundschutz des Arbeitsplatzes: Die Institution muß einen angemessenen Sicherheits-Grundschutz des Arbeitsplatzes sicherstellen.
- Falls eine Nicht-Standard-Stelle realisiert werden soll:
    - Vorabklärung mit dem PKI-Management:
        - Welche Funktionalität soll mit der neuen Stelle zur Verfügung gestellt werden?
        - Läßt sich die neue Stelle geeignet in die PKI integrieren?
        - Warum will die Institution die neue Stelle realisieren? Welche Ziele werden verfolgt?
    - Klärung in der Institution, ob die geforderten Voraussetzungen erfüllt werden sollen bzw. können:

  - Aufwandsabschätzung für den Betrieb einer neuen Stelle (betrifft Voraussetzungen an Technik, Organisation, Personal und Infrastruktur).
  - Ist die Institution bereit, diesen Aufwand zu betreiben?

- Ist die Entscheidung für die Einrichtung einer neuen Stelle in der Institution gefallen, sind folgende Dinge zu tun:
  - Bestimmung einer verantwortlichen Person für den Aufbau der Stelle (z.B. organisatorischer Ansprechpartner für die Einrichtung einer lokalen Registrierungsstelle).
  - „Antrag auf Teilnahme“ stellen: Antrag auf Einrichtung einer neuen Stelle stellen. Abwarten der Bestätigung durch einen Vertreter des PKI-Managements („Teilnahmebestätigung“).
  - Aufbau der Stelle gemäß den Anforderungen.
  - „Antrag auf Betriebserlaubnis“ stellen: Nachweis, daß alle Anforderungen an die Stelle umgesetzt wurden (z.B. durch Prüfbericht eines durch das PKI-Management anerkannten Sachverständigten). Abwarten der Bestätigung durch einen Vertreter des PKI-Managements („Betriebserlaubnis“).
- Nach erfolgter Betriebserlaubnis durch das PKI-Management kann der reguläre Betrieb der Stelle aufgenommen werden. Die Stelle verpflichtet sich, die Anforderungen an die Stelle stets einzuhalten (insbes. die *Policy*).
- Es können jederzeit Stichprobenprüfungen auf Einhaltung der Teilnahmevoraussetzungen durch das PKI-Management initiiert werden. Bei gravierenden Mängeln kann die Betriebserlaubnis entzogen werden.

6.2 **Allgemeine Checkliste für das PKI-Management**

Die PKI-Gesamtleitung hat folgende Aspekte zu prüfen:

- Antrag auf Teilnahme
  - Ist die Zielgruppe der Stelle PKI-kompatibel?
  - Ist die neuen Stelle geeignet in die Gesamt-PKI zu integrieren?
  - Funktionalität: Ist die Stelle bzgl. ihrer angestrebten Funktionalität geeignet in die PKI einzubetten? Ergibt sich eine Umstrukturierung innerhalb der PKI? Muß daß PKI- und das Rollenmodell abgeändert werden? Sollen neuartige oder herkömmliche Dienste angeboten werden?
  - Sicherheit: Ist davon auszugehen, daß die Sicherheit der Gesamt-PKI durch die Integration der Stelle nicht gefährdet wird? Ist davon auszugehen, daß die Institution in der Lage ist, alle geforderten Teilnahmevoraussetzungen zu erfüllen?
  - Ist die neue Stelle geeignet in die Zertifizierungs- und Namenshierarchie zu integrieren?
  - Festlegung und Fixierung der konkreten Betriebsvoraussetzungen für die Stelle
  - Sind alle Fragen positiv geklärt, erfolgt die „Teilnahmebestätigung“.
- Antrag auf Betriebserlaubnis
  - Prüfung aller Betriebsvoraussetzungen (u.a. Prüfung auf ein geeignetes Sicherheitskonzept der Stelle).

- Sind alle Betriebsvoraussetzungen erfüllt, erfolgt die „Betriebserlaubnis“.

7. **Betrieb der Stelle**

   - Betreuung der neuen Stelle durch PKI-Management.
   - Stichprobenhaftes Überprüfen der Teilnahmevoraussetzungen der Stelle durch PKI-Management.

6.2 Leitfaden für die Einrichtung einer typischen lokalen Registrierungsstelle

Die Einrichtung einer lokalen Registrierungsstelle in der Institution erfolgt stets auf Initiative der Institution und erfordert die in folgenden beschriebene grundsätzliche Vorgehensweise.

Der organisatorische Ansprechpartner

Einige Teile der PKI, wie die Zertifizierungsstelle und der Verzeichnisdienst, werden durch den Projektbetreiber bereitgestellt, so daß sich eine an der Teilnahme interessierte Institution nicht um deren Realisierung bemühen muß. Eine wesentliche Stelle muß aber jede Institution selbst aufbauen und betreiben: Die lokale Registrierungsstelle LRS.

Da der Aufbau der LRS durch die Vielzahl teilnehmender Institutionen im Projekt SPHINX relativ häufig vorkommt, kommt dem organisatorischen Ansprechpartner im Projekt SPHINX eine besondere Bedeutung zu.

Eine Institution, die sich für die Teilnahme am Projekt SPHINX entschieden hat, wird eine Person bestimmen, die für den Aufbau der notwendigen Strukturen verantwortlich ist (organisatorischer Ansprechpartner, OA). Er ist für den Aufbau und den ordnungsgemäßen Betrieb der LRS verantwortlich.

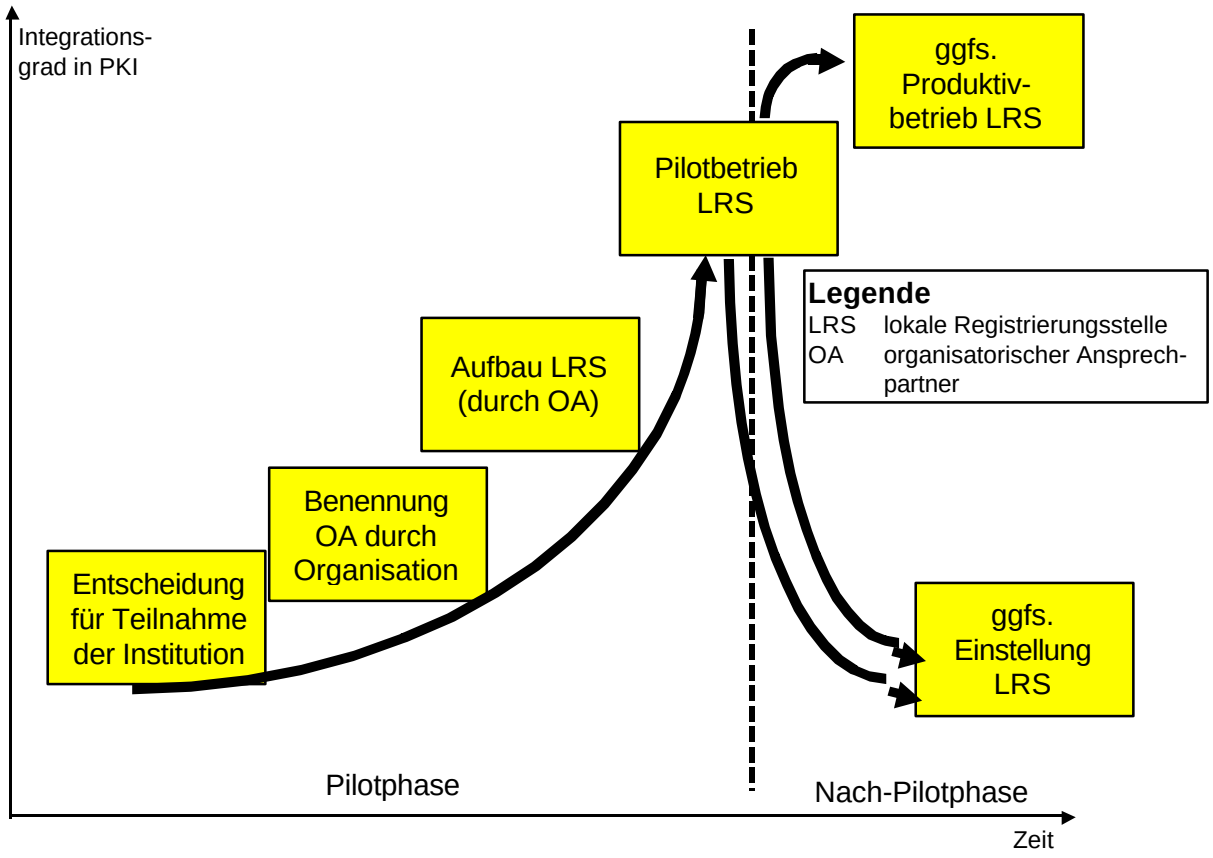


Abbildung 43: Lebenszyklus der lokalen Registrierungsstelle in der Institution

Es werden folgende Erwartungen an den organisatorischen Ansprechpartner gestellt:

- Er ist für den Aufbau der notwendigen Strukturen der PKI innerhalb seiner Institution verantwortlich (siehe Kapitel 6.3).

- Er wird als zentraler Ansprechpartner für die Endanwender und die Mitarbeiter innerhalb der LRS zur Verfügung stehen.
- Er wird als Ansprechpartner der Institution vom übergeordneten PKI-Projektmanagement herangezogen.
- Ggfs. wird er – evtl. nur zeitweise – selbst als LRS-Sachbearbeiter die Vorgangsbearbeitung innerhalb der LRS wahrnehmen.

Hinweise zum Aufbau der Registrierungsstelle

Die Initiative für die Einrichtung einer neuen lokalen Registrierungsstelle geht stets von der Institution aus. Diese muß sich für die Teilnahme am Piloten entscheiden und bereit sein, die benötigte Instrastruktur und Personal bereitstellen.

Voraussetzungen an die PKI:

- Die Wurzelinstanz und eine (für die Institution geeignete) Zertifizierungsinstanz befinden sich im Wirkbetrieb.
- Wurzel- und Zertifizierungsstellen-Zertifikat sind veröffentlicht worden und gültig.
- Wurzelzertifikatinformationen sind geeignet veröffentlicht worden.

Ob diese Voraussetzungen an die PKI erfüllt sind, erfahren Sie beim Leiter der Wurzel-Zertifizierungsstelle.

Voraussetzungen an die Institution:

- Entscheidung der Institution, am Projekt SPHINX teilzunehmen.
- Die Institution kann die technischen, personellen, baulichen, infrastrukturellen und organisatorischen Anforderungen, die an eine lokale Registrierungsstelle gestellt werden, erfüllen (zu den Einzelanforderungen siehe Betriebshandbuch lokale Registrierungsstelle).

Folgende **praktische Schritte** umfaßt die Einrichtung einer lokalen Registrierungsstelle:

- Benennung einer verantwortlichen Person in der Institution (organisatorischer Ansprechpartner, OA).
- OA beantragt formell Teilnahme am Piloten bei der zuständigen Zertifizierungsstelle (Welche Zertifizierungsstelle für die Institution zuständig ist, kann bei der Wurzel-Zertifizierungsstelle erfragt werden).
- Anmeldung als LRS bei der Registrierung der Zertifizierungsstelle. Dazu gibt es ein spezielles Formular (Anhang OHB-A1), das durch die Institution geeignet zu unterzeichnen ist (zeichnungsberechtigte Person, Dienstsiegel).

Nach Bestätigung des Antrags durch die Zertifizierungsstelle:

- Ein Arbeitsplatz für den Betrieb der lokalen Registrierungsstelle wird eingerichtet (Zu den technischen und infrastrukturellen Anforderungen des Arbeitsplatzes: Siehe Betriebshandbuch lokale Registrierungsstelle).

- Bestimmung des Personals, das in der LRS eingesetzt werden soll (*LRS-Sachbearbeiter*).
- Jeder LRS-Sachbearbeiter beantragt ein persönliches EA-Zertifikat bei der Registrierungsstelle (als LRS-Sachbearbeiter). Dazu gibt es ein Formular (Anhang OHB-A2), das durch die Institution geeignet zu unterzeichnen ist (OA als zeichnungsberechtigte Person, Dienstsiegel). In der Zertifizierungsstelle werden die LRS-Sachbearbeiter als Ansprechpartner registriert. Die Zertifizierungsstelle darf nur mit den offiziellen LRS-Sachbearbeitern Vorgänge austauschen.
- Dem LRS-Sachbearbeiter wird sein EA-Zertifikat auf vertrauenswürdigem Wege von der Zertifizierungsstelle zugestellt.
- Dem LRS-Sachbearbeiter werden Wurzelzertifikatinformationen auf vertrauenswürdigem Wege von der Zertifizierungsstelle zur Verfügung gestellt.
- Dem LRS-Sachbearbeiter werden alle benötigten Informationen, Formulare und Unterlagen bereitgestellt (Betriebshandbuch lokale Registrierungsstelle).
- Es erfolgt ein Test der Kommunikationsschnittstelle zwischen Registrierungsstelle und Zertifizierungsstelle. Die Zertifizierungsstelle wird entsprechende Testaufgaben stellen.

Sind alle diese Schritte erfolgreich durchgeführt worden, ist die LRS arbeitsfähig.

- Nachdem die LRS arbeitsfähig ist, ist es nun sinnvoll, die potentiellen Endanwender der Institution über die Einrichtung der lokalen Registrierungsstelle geeignet zu informieren.

Der organisatorische Ansprechpartner benötigt die folgenden **Dokumente und Unterlagen** für seine Tätigkeit:

- Das vorliegende Organisationshandbuch, das über die Gesamtstruktur und Wirkungsweise der PKI informiert.
- Das Formular zur Anmeldung neuer lokaler Registrierungsstellen (Anhang OHB-A1).
- Das Formular zur Zertifizierung von Mitarbeitern der LRS (Anhang OHB-A2)
- Ein Betriebshandbuch der lokalen Registrierungsstelle. Dieses Betriebshandbuch enthält neben der Beschreibung aller erwarteten Vorgänge und dazugehörigen Arbeitsanweisungen die benötigten Formularvorlagen.

6.3 Leitfaden für die Einrichten einer typischen Zertifizierungsstelle

Eine Zertifizierungsstelle (ZS) wird grundsätzlich auf Initiative einer Institution eingerichtet und erfordert die in folgenden beschriebene grundsätzliche Vorgehensweise.

Die Institution, die eine Zertifizierungsstelle im Projekt SPHINX betreiben will, benennt den Leiter der Zertifizierungsstelle (LZS), der für den Aufbau der notwendigen Strukturen und den ordnungsgemäßen Betrieb der ZS verantwortlich ist.

Anschließend können die technischen, personellen, baulichen, infrastrukturellen und organisatorischen Maßnahmen unter Verantwortlichkeit des LZS realisiert werden. Die Betriebserlaubnis wird inklusive des Nachweises über die Erfüllung der Anforderungen beantragt. Nach Erteilung der Betriebserlaubnis wird die Zertifizierungsstelle durch die übergeordnete Wurzelinstanz zertifiziert. Das Zertifikat wird der Zertifizierungsstelle zugestellt und im Verzeichnis veröffentlicht. Letztlich müssen noch die einzelnen Mitarbeiter der Zertifizierungsstelle zertifiziert werden.

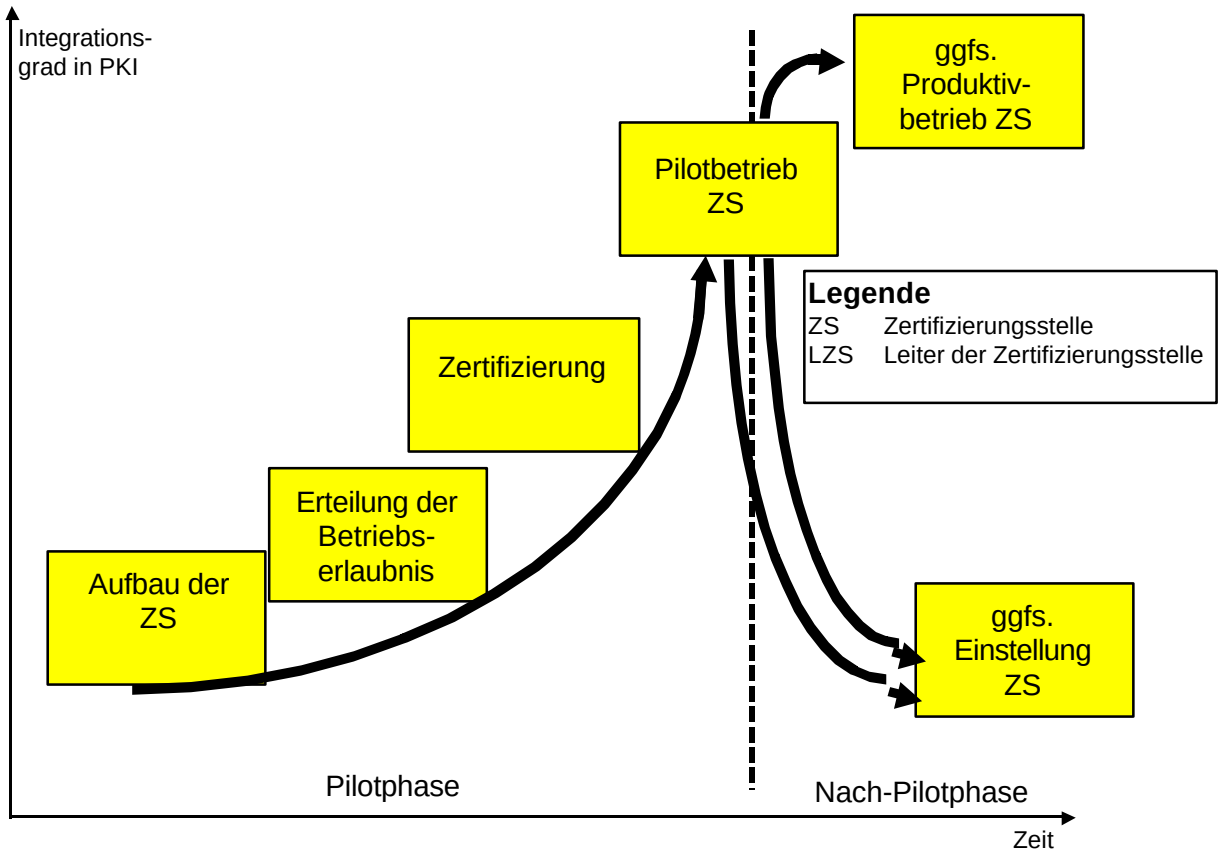


Abbildung 44: Lebenszyklus der Zertifizierungsstelle in der Institution

An den Leiter der Zertifizierungsstelle werden folgende Erwartungen gestellt:

- Er ist für den Aufbau der notwendigen Strukturen der PKI innerhalb seiner Institution verantwortlich.
- Er ist für die Planung und Koordinierung der Aktivitäten der Zertifizierungsstelle verantwortlich.
- Er steht als zentraler Ansprechpartner für die Mitarbeiter der Zertifizierungsstelle zur Verfügung.

- Er ist Ansprechpartner der Institution für das übergeordnete PKI-Projektmanagement.

Hinweise zum Aufbau der Zertifizierungsstelle

Die Initiative für die Einrichtung einer neuen Zertifizierungsstelle geht grundsätzlich von der Institution aus. Diese muß sich für die Teilnahme am Piloten entscheiden und bereit sein, die benötigte Infrastruktur und Personal bereitstellen.

Voraussetzungen an die PKI:

- Die Wurzelinstanz (zur Zertifizierung der Zertifizierungsinstanz) befindet sich im Wirkbetrieb.
- Das Wurzelzertifikat ist veröffentlicht worden und gültig.
- Die Wurzelzertifikatinformationen sind geeignet veröffentlicht worden.

Ob diese Voraussetzungen an die PKI erfüllt sind, erfahren Sie beim SPHINX-Projekt-management.

Voraussetzungen an die Institution:

- Entscheidung der Institution, am Projekt SPHINX teilzunehmen.
- Die Institution kann die technischen, personellen, baulichen, infrastrukturellen und organisatorischen Anforderungen, die an eine Zertifizierungsstelle gestellt werden, erfüllen (zu den Einzelanforderungen siehe Betriebshandbuch Zertifizierungsstelle).

Folgende **praktische Schritte** umfaßt die Einrichtung einer Zertifizierungsstelle:

- Kontaktaufnahme mit dem Projektmanagement.
- Informationaustausch zwischen Projektmanagement und Institution.
- Entscheidung der Institution über die Einrichtung einer Zertifizierungsstelle.
- Benennung einer verantwortlichen Person in der Institution (Leiter der Zertifizierungsstelle) im Teilnahmeantrag für die Zertifizierungsstelle (Anhang OHB-C1).

Nach Bestätigung des Teilnahmeantrags:

- Aufbau der technischen und organisatorischen Infrastruktur (z.B. bauliche Maßnahmen, Rollenverteilung, etc.).
- Erklärung über die Betriebsbereitschaft mit dem Antrag auf Betriebserlaubnis einer Zertifizierungsstelle (Anhang OHB-C2) inklusive dem Nachweis über die Erfüllung der Vorraussetzungen.

Nach Bestätigung der Betriebserlaubnis:

- Beantragung einer Zertifizierung (Anhang OHB-C3) bei der Wurzelinstanz.
- Zertifizierung durch die Wurzelinstanz.
- „Vertrauliche„ Zertifikatszustellung der Wurzelinstanz an die Zertifizierungsstelle.
- Bereitstellung des Zertifikats im (zentralen) Verzeichnisdienst.

- Beantragung der Zertifizierung der Rollenträger (Mitarbeiter der Zertifizierungsstelle) mit dem Registrierungs-/Zertifizierungsantrag für Mitarbeiter derZertifizierungsstelle (Anhang OHB-C4).

Nach der Zertifizierung der Mitarbeiter der Zertifizierungssstelle:

- Test der Kommunikationsschnittstelle zwischen Registrierungsstelle und Zertifizierungsstelle. Die Zertifizierungsstelle wird entsprechende Testaufgaben stellen.

Sind alle diese Schritte erfolgreich durchgeführt worden, ist die Zertifzierungsstelle betriebsbereit. Die potentiellen Endanwender der neue eingerichteten Zertifizierungsstelle sind ggf. über die Bertriebsbereitschaft zu informieren.

Die Zertifizierungsstelle benötigt die folgenden **Dokumente und Unterlagen** für seine Tätigkeit:

- Das vorliegende Organisationshandbuch, das über die Gesamtstruktur und Wirkungsweise der PKI informiert.
- Den Teilnahmeantrag der Zertifizierungsstelle (Anhang OHB-C1).
- Den Antrag auf Betriebserlaubnis einer Zertifizierungsstelle (Anhang OHB-C2).
- Den Zertifizierungsantrag für die Zertifizierungsstelle (Anhang OHB-C3).
- Den Registrierungs-/Zertifizierungsantrag für Mitarbeiter derZertifizierungsstelle (Anhang OHB-C4).
- Das Betriebshandbuch Zertifizierungsstelle. Dieses Betriebshandbuch enthält neben der Beschreibung aller erwarteten Vorgänge und dazugehörigen Arbeitsanweisungen die benötigten Formularvorlagen.

7 Begriffe

7.1 Glossar

Begriff	Beschreibung
Ablauforganisation	Definition der Abläufe innerhalb und zwischen einzelnen Komponenten, aus denen das System besteht. (zur statischen Beschreibung des Systems siehe → *Aufbauorganisation*)
Aufbauorganisation	Festlegung von Aufbau und Struktur eines Systems. Enthält eine Beschreibung der einzelnen Komponenten, aus denen das System besteht sowie eine Beschreibung der Zusammenhänge und Schnittstellen zwischen den Komponenten. (zur Dynamik des Systems siehe → *Ablauforganisation*)
Authentisierung	Prüfung der behaupteten Identität eines Zertifikatinhabers.
Authority Revocation List	→ *Sperrliste*, die Sperrinformationen über WZS- und ZS-Zertifikate enthält. (siehe auch → *Certificate Revocation List*)
Autorisierte Person	Person in einer → *Institution*, die eine → *Fremdsperrung* von EA-Zertifikaten veranlassen darf.
Certificate Revocation List	→ *Sperrliste*, die Sperrinformationen über EA-Zertifikate (und ggf. ZS-Zertifikate) enthält. (siehe auch → *Authority Revocation List*)
Dienst	Leistung, die innerhalb der PKI für Personen oder PKI-Komponenten erbracht wird.
Eigensperrung	Sperrung eines → *Zertifikats*, die durch den Inhaber des Zertifikats selbst veranlaßt wird. (siehe auch → *Fremdsperrung*)
Einrichtung	Vorbereitung und Durchführung des → *Wirkbetriebs* einer → *Stelle*.
Einstellung	Beendigung des → *Wirkbetriebs* einer → *Stelle*.
Endanwender	Eine natürliche Person, die sicheren elektronischen Dokumentenaustausch zu anderen Endanwendern betreiben möchte.
Fingerprint	Kryptographisch sicherer Hashwert eines Datenobjekts, mit Hilfe dessen die Unverfälschtheit des Datenobjekts *per Augenschein* überprüft werden kann. Fingerprints werden im Rahmen der PKI insbesondere für die Überprüfung von Wurzel-Zertifikaten genutzt.
Fremdsperrung	Sperrung eines → *Zertifikats*, die nicht durch den Zertifikats-inhaber selbst, sondern durch eine dritte, dafür → *autorisierte Person* veranlaßt wird. (siehe auch → *Eigensperrung*)
Instanz	Untereinheit einer → *Stelle*, die durch ihre spezifischen

Begriff	Beschreibung
	Aufgaben gekennzeichnet ist und die entsprechende → *Dienste* der → *Stelle* realisiert.
Institution	Organisationseinheit (z.B. Behörde, Firma, o.ä.), die entweder → *Stellen* der PKI realisiert oder der Endanwender der PKI zugeordnet sind.
Lokale Registrierungsstelle	→ *Stelle* in einer → *Institution* mit Endanwendern, die die persönliche und organisatorische Schnittstelle der Endanwender zur PKI bildet.
Organisatorischer Ansprechpartner	Natürliche Person, die für Realisierung und Betrieb der → *(lokalen) Registrierungsstelle* in der → *Institution* verantwortlich ist.
Personal Security Environment	Geschützte Komponente, die u.a. den oder die privaten Schlüssel des Endanwenders enthält. Die Nutzung der PSE (und damit der privaten Schlüssel) ist nur nach erfolgreicher Authentisierung des Endanwenders möglich (z.B. durch PIN-Eingabe). Das PSE kann beispielsweise als Datei auf Diskette oder in Form einer Chipkarte zur Verfügung gestellt werden.
Produktivbetrieb	Wirkbetrieb einer → *Stelle* nach Abschluß des Projektes.
Prototypzertifikat	→ *Selbstzertifikat* eines Teilnehmers, das die im → *Zertifikat* einzutragenden Daten enthält, dem Antrag auf Ausstellung eines Zertifikats beigefügt wird und durch Signatur und ggf. Änderung von Daten von der zuständigen Zertifizierungsstelle in das beantragte Teilnehmerzertifikat umgewandelt wird.
Public Key Infrastruktur	Auf einem asymmetrischen Schlüsselsystem basierende Infrastruktur, die die geforderten Sicherheitsdienste (in SPHINX: Sicherstellung der Integrität, Vertraulichkeit, Authentizität und Verfügbarkeit) erbringt. Zu einer Public Key Infrastruktur im Sinne dieses OrgHB gehören sowohl zentrale Komponenten (z.B. CA-/RA-Komponenten) als auch dezentrale Komponenten (z.B. Plugins und Client-Komponenten). Die Public Key Infrastruktur umfaßt außerdem sowohl technische als auch organisatorische Aspekte.
Rolle	Bündelung inhaltlich oder organisatorisch zusammengehörender Aufgaben, die typischerweise von einer Person oder einer Gruppe von Personen bearbeitet werden.
Selbstzertifikat	→ *Zertifikat*, das mit dem geheimen Schlüssel digital signiert ist, der zu dem im → *Zertifikat* enthaltenen öffentlichen Schlüssel gehört.
Sicherungsanker	Öffentlicher Schlüssel der Wurzelzertifizierungsstelle (enthalten im Wurzelzertifikat), der als Grundlage zur Überprüfung von

Begriff	Beschreibung
	→ *Zertifizierungspfaden* dient.
Sperrliste	Von einer Zertifizierungsstelle signierte Liste gesperrter Zertifikate.
Stelle	Organisationseinheit, die mit Hilfe ihrer → *Instanzen* einen oder mehrere → *Dienste* der PKI erbringt.
Teilnehmer	Oberbegriff für → *Endanwender* und → *Zertifizierungsstellen* der PKI.
Verlängerungs-zertifikat	Zertifikat, das ein anderes (z.B. abgelaufenes) Zertifikat ersetzt, jedoch ohne Schlüsselwechsel für den Teilnehmer.
Wirkbetrieb	Die → *Stelle* ist arbeitsfähig und wird betrieben im Sinne ihrer Ziele (siehe auch → *Produktivbetrieb*).
Wurzel-Prüfmaterial	Vertrauenswürdig übermittelte Information, anhand der die Autentizität eines Zertifikats sicher überprüft werden kann (z.B. → *Fingerprint* des → *Wurzel-Zertifikats*).
Zertifikat	Datenstruktur, die die Zuordnung der Identität (z.B. Personen-name, Institutionsname) des Zertifikatsinhabers zu einem öffentlichen Schlüssel und gegebenfalls weiteren ergänzenden Informationen (z.B. Gültigkeitszeitraum und Name der ausstellenden Zertifizierungsstelle) allgemein nachprüfbar dokumentiert. Ein Zertifikat besteht aus einer Menge von Attributen, deren Unverfälschtheit und Zusammengehörigkeit durch eine digitale Signatur der ausstellenden Zertifizierungsstelle bestätigt wird.
Zertifikatskette	Eine Folge von Zertifikaten *EA-Z Þ ZS-Z ... (Þ ZS-Z Þ ZS-Z ...) Þ W-Z*, wobei eine Verkettung dieser Zertifikate vorliegt: • W-Z als → *Sicherungsanker* in Form eines → *Selbstzertifikats*. • ZS-Z ist mit dem assoziierten geheimen Schlüssel des direkt übergeordneten W-Z oder ZS-Z signiert. • EA-Z ist mit dem assoziierten geheimen Schlüssel des direkt übergeordneten ZS-Z signiert.
Zertifizierungspfad	Synonym für → *Zertifikatskette*.
Zertifizierungsstelle	→ *Stelle*, die Teilnehmerzertifikate und Sperrlisten ausstellt. Eine Zertifizierungsstelle stellt darüber hinaus i.d.R. weitere → *Dienste* zur Verfügung, wie z.B. den Registrierungs- und einen Verzeichnisdienst.

Abbildung 45: Begriffe

7.2 Abkürzungsverzeichnis

Abkürzung	Bedeutung
ADM*x*	Administrator *x* (Rolle)
AP	Autorisierte Person (Rolle)
ARL	Authority Revocation List (Sperrliste für ZS-Zertifikate)
BEV	Beauftragter für die Eigenverwaltung (Rolle)
BKM	Beauftragter für das Kryptomanagement (Rolle)
BTD	Beauftragter für den Technischen Dienst (Rolle)
BMI	Bundesministerium des Innern
BNM	Beauftragter für das Notfall-Management (Rolle)
BNRV	Beauftragter für die Namensraumvergabe (Rolle)
BSI	Bundesamt für Sicherheit in der Informationstechnik
CCI	Competence Center Informatik
CRL	Certificate Revocation List
DSB	Datenschutzbeauftragter
EA	Endanwender (Rolle)
EA-Z	Endanwender-Zertifikat
ID	Identifikations-Kennzeichen
IuKDG	Informations- und Kommunikationsdienste-Gesetz
ITSB	IT-Sicherheitsbeauftragter (Rolle)
LRS	Lokale Registrierungsstelle
LZS	Leiter der Zertifizierungsstelle (Rolle)
NRV	Namensraumvergabe (Instanz)
MGMT	Management
OA	organisatorischer Ansprechpartner (Rolle)
OHB-*xy*	Formular mit der Kennung OHB-*xx*
OrgHB	Organisationshandbuch
PIN	Persönliche Identifikationsnummer
PKI	Public Key Infrastruktur
PSE	Personal Security Environment
R	Registrierung (Instanz)
REG	Registrator (Rolle)
RS	Registrierungsstelle

Abkürzung	Bedeutung
RV	Revisor (Rolle)
SERV	Beauftragter für den Service (Rolle)
SigG	Signaturgesetz
SigV	Signaturverordnung
TID*x*	Beauftragter für Teilnehmer-Identifikation *x* (Rolle)
TSV	Teilnehmerservice (Instanz)
V	Verzeichnis (Instanz)
VERP	Verzeichnispfleger (Rolle)
W	Wurzel
W-Z	Wurzel-Zertifikat
WZS	Wurzelzertifizierungsstelle
Z	Zertifizierung (Instanz)
ZERT*x*	Zertifizierer *x*
ZERTV	Verwalter Zertifizierung (Rolle)
ZS	Zertifizierungsstelle
ZS-Z	Zertifizierungsstellen-Zertifikat

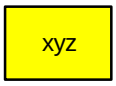
Abbildung 46: Abkürzungen

8 Graphische Darstellungsweise

8.1 Schema

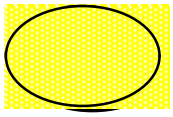
Ein Schema skizziert eine grobe Übersicht über einen Sachverhalt.

Dabei werden folgende graphische Elemente verwendet:



Eine Instanz der PKI

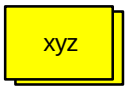
R-Verteiler (SPHINX-spezifisch)



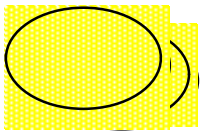
Organisationseinheit

Schnittstelle zwischen Instanzen

Instanzen und Blöcke können einfach oder mehrfach realisiert sein. Ein mehrfaches Auftreten wird durch Überlagern entsprechender Symbole dargestellt:



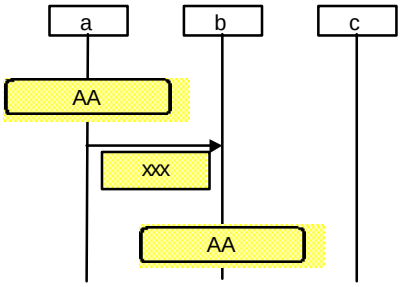
Instanzen können mehrfach realisiert sein.



Blöcke können mehrfach realisiert sein (inkl. aller in

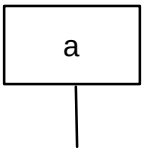
8.2 Ablaufdiagramm

Ein Ablaufdiagramm zeigt den zeitlichen Ablauf eines Vorgangs.



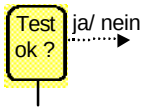
Ablaufdiagramm 38: Beispiel eines Ablaufdiagramms

Dabei werden folgende graphische Elemente verwendet:



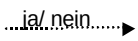
Instanz a (mit Zeitstrahl = Normalpfad)

Aktion A derjenigen Instanz, auf dessen Zeitstrahl bzw. Normalpfad dieses Symbol liegt.



Test eines Sachverhalts: Im Fehlerfall (Testergebnis: „ja“ oder „nein“) wird gestrichelter Pfad verfolgt, im Erfolgsfall der Normalpfad.

Daten-/Informationsübermittlung zw. zwei Instanzen



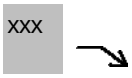
Daten-/Informationsübermittlung zw. zwei Instanzen zur

Referenznummer *xx* für eine Kommunikationsbeziehung. Sie soll das Verfolgen der Kommunikationsbeziehungen, die sich über mehrere Basisvorgänge erstrecken können, erleichtern.

„Virtueller Übergang“: Andere Instanzen bearbeiten den

Vorgang schließlich wieder zurück.

Zeitlicher Schnitt, d.h. der diesem Symbol folgende Ablauf ist unabhängig vom dem Symbol vorangehenden Ablauf.



Erläuterung zu einem Sachverhalt.

Dabei ist der zeitliche Ablauf von oben nach unten zu lesen:

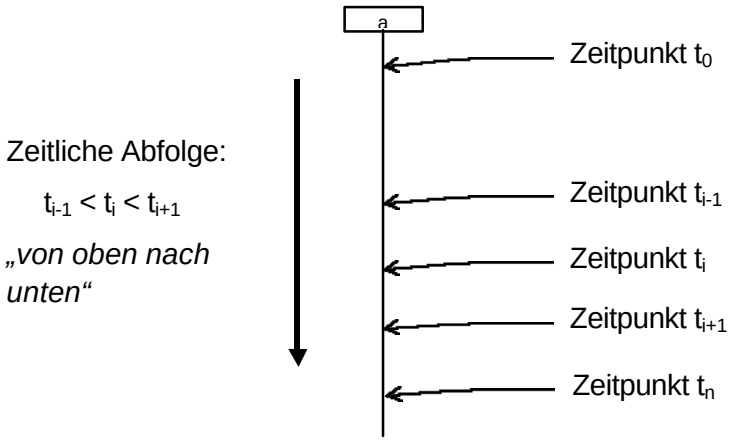


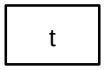
Diagramm 1: Zeitstrahldefinition

8.3 Ablaufschema

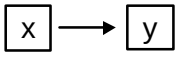
Ein Ablaufschema beschreibt die Instanzen in ihrer Beziehung untereinander. Dabei werden die Datenflüsse, die zwischen den Instanzen existieren, skizziert.

Folgende Grundelemente werden verwendet:

Eine Instanz der PKI: Teilnehmerservice (TSV), Registrierung (R), Zertifizierung (Z), Verzeichnis (V), Namensraumvergabe (NRV)



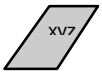
Eine Instanz der PKI zu einem Zeitpunkt t (Durchlaufnummer t). Eine Instanz kann dabei von mehreren Durchlaufnummern betroffen sein.



Übergabe eines Vorgangs mit Datentransfer zwischen zwei Instanzen (von x nach y)

Interner Arbeitsvorgang.

Folgende Datenobjekte werden verwendet:



Papierformular (z.B. Zertifizierungsantrag) (integer, authentisch)

Verschlossener Papierumschlag (mit Dokumenten) (vertraulich, integer, authentisch)

PIN-Brief (vertraulich, integer, authentisch)

gesicherter Datensatz (vertraulich, integer, authentisch)

Sperrliste (integer, authentisch)

Prototyp-Zertifikat (integer)

Zertifikat (integer, authentisch)

PSE (vertraulich, integer)

Telefonat (oder andere ungesicherte Benachrichtigungsform)

Aus Übersichtlichkeitsgründen sind die Instanzen teilweise innerhalb organisatorischer Einheiten eingebettet:

Organisatorische Einheit

8.4 Zertifizierungshierarchie

Symbole, die in der Abbildung zur Zertifizierungshierarchie verwendet werden :

Zertifizierungsstelle

Endanwender

Zertifizierungsbeziehung (zu weiterer Zertifizierungsstelle oder zu Endanwender)

Mögliche Zertifizierungsbeziehung (zu weiterer Zertifizierungsstelle oder zu Endanwender)

9 Übersicht über das Formularwesen

In der folgenden Tabelle wird dargestellt, welche Formulare für die Kommunikation mit den Teilnehmern und Institutionen mindestens benötigt werden. Für die Kommunikation zwischen den Instanzen werden in den Betriebshandbüchern Formularvorlagen bereitgestellt.

Formular-Kennung	Bezeichnung der Formularvorlage	Referenz auf Formularvorlage
Formulare bzgl. lokaler Registrierungsstelle		
OHB-A1	Antrag auf Teilnahme als lokale Registrierungsstelle	OHB_A1.*xx*.doc[25]
OHB-A2	Antrag auf Betriebserlaubnis einer lokalen Registrierungsstelle	OHB_A2.*xx*.doc
OHB-A3	Registrierungs- und Zertifizierungsantrag für Mitarbeiter des Teilnehmerservice	OHB_A3.*xx*.doc
Formulare bzgl. Endanwender		
OHB-B1	Teilnahmeantrag für Endanwender	OHB_B1.*xx*.doc
OHB-B2	Zertifizierungsantrag für Endanwender	OHB_B2.*xx*.doc
Formulare bzgl. Zertifizierungsstellen		
OHB-C1	Teilnahmeantrag für Zertifizierungsstelle	OHB_C1.*xx*.doc
OHB-C2	Antrag auf Betriebserlaubnis einer Zertifizierungsstelle	OHB_C2.*xx*.doc
OHB-C3	Zertifizierungsantrag für Zertifizierungsstelle	OHB_C3.*xx*.doc
OHB-C4	Registrierungs- und Zertifizierungsantrag für Mitarbeiter einer Zertifizierungsstelle	OHB_C2.*xx*.doc
Änderungsformulare		
OHB-D1	Änderungsmitteilung Teilnehmer	OHB_D1.*xx*.doc

Abbildung 47: Formularvorlagen

Hinweis:

Alle Formularvorlagen sind separat auf Anfrage beim Projektbetreiber (BSI) verfügbar.

[25] *.xx*. = Dateifolgenummer der Formularvorlagedatei. Wird eine Formularvorlage geändert, so ist eine neue Dateifolgenummer zu verwenden.

10 Literatur

[TechGru] SPHINX Phase 2 - Technische Grundlagen, Bundesministerium des Innern, Version 3.2, 26.11.1998