Registrierungsstelle Thüringen
Organisationshandbuch
V 1.3

Inhalt

1 Ziel und Inhalt des Dokumentes

Das Land Thüringen plant den Aufbau einer Public Key Infrastruktur für die flächendeckende Einführung und Nutzung der fortgeschrittenen und qualifizierten Signatur zur rechtssicheren digitalen Bearbeitung von Verwaltungsvorgängen.
Der Freistaat Thüringen hat im Rahmen des Projektes „Registrierungsstelle Thüringen“ den Aufbau einer eigenen Verwaltung für die Beantragung von PKI im Land aufgebaut, um die PKI-Dienste zur qualifizierten elektronischen Signatur für verschiedene Fachverfahren anzubieten.

Dieses Dokument soll die spezifischen Prozesse und Vorgaben erläutern, die für die Erstellung von fortgeschrittenen (FeS) und qualifizierten elektronischen Signaturen (QeS) notwendig sind.

Das vorliegende Organisationshandbuch verfolgt nachfolgend genannte Ziele:

- Zu gewährleisten ist der sichere Betrieb der PKI Thüringen und des Verfahrens QeS, in dem die Vorgaben des Zertifizierungsdiensteanbieters aufgegriffen und Strukturen aufeinander abgestimmt werden.
- Das Beschreiben von Abläufen und Prozessen soll zwischen den beteiligten Stellen und Behörden eine effiziente und gleichzeitig selbstständige Durchführung ermöglichen.

Die in diesem Dokument beschriebenen Prozesse und Regelungen basieren auf folgenden Quellen:

- den Vorgabe des Zertifizierungsdiensteanbieters (ZDA) – TeleSec
- den Vorgaben zur Nutzung des PostIdent-Verfahrens der Deutschen Post AG
- dem „Handbuch für Qualifizierte Zertifikate“ als Anlage des Rahmenvertrages über die Nutzung des DOI-Netzes
- der „Leistungsbeschreibung Public Key Service (PKS) für DOI [DOI120]“

2 Aufbauorganisation der PKI Thüringen

Die PKI Thüringen besteht aus verschiedenen Komponenten, Stellen und Behörden, die nur in ihrem Zusammenwirken das oben beschriebene Ziel ermöglichen, dabei sind entsprechend der PKI die beteiligten Stellen und Instanzen in Ebenen gruppiert.

2.1.1 Registrierungsstelle (Thüringer Landesrechenzentrum)

Die Registrierungsstelle (RA) ist zuständig für die Identifizierung und Registrierung der Teilnehmer sowie für die Antragsbearbeitung und –weiterleitung an den Zertifizierungsdiensteanbieter (ZDA). Die Registrierungsstelle Thüringen ist der zentrale Ansprechpartner für die Thüringer Behörden für das Antragsverfahren zur Ausstellung fortgeschrittener und qualifizierter elektronischer Signaturen unabhängig von dem konkreten Verfahren, für welches die Signaturen benötigt werden.

2.1.1.1 Registrierungsstelle TLRZ

Die RA Thüringen ist verantwortlich für:

- Versand der Teilnahmeunterlagen
- Koordinierung des Registrierungsprozesses für die Teilnehmer
- Bereitstellung der Freischaltcodes
- Verwaltung der Signaturstati
- Beschaffung und Versand der Kartenlesegeräte (wenn dies notwendig wird)

- Betrieb, Aktualisierung und Pflege des Web-Portals QeS (http://www.signaturen.thueringen.de)
- Formularserver zur Bereitstellung des Antragsformulars
- Beantragung der Freischaltcodes bei der T-TeleSec
- sichere Archivierung der beim Zertifizierungsprozess anfallenden Unterlagen, Papierunterlagen müssen in einem verschlossenem Schrank aufbewahrt werden
- Rechnungslegungsstelle für ZDA TeleSec und Deutsche Post AG

2.1.1.2 Servicecenter TLRZ

Das Servicecenter im TLRZ als Teil der Registrierungsstelle ist verantwortlich für:

- zentrale Annahme von Service Requests und Störungsmeldungen – Erstlösung
- Koordination der Second Level Supporteinheiten gegenüber den Teilnehmern hinsichtlich der Beantragung der Signaturkarte

2.1.2 Behörde

Die Behörde, Einrichtung oder beteiligte Institution, welche eine QeS benötigt, benennt die entsprechenden Personen. Gleichzeitig überwacht sie die Anzahl der Teilnehmer am Verfahren, die eine Signaturkarte beantragen dürfen. Die Behörden selbst sind auch verantwortlich für die Festlegung der sperrberechtigten Dritten. Die Angabe des jeweiligen sperrberechtigten Dritten im Antragsverfahren erfolgt durch den Antragsteller.

2.1.3 Teilnehmer

Teilnehmer sind Mitarbeiter/innen von Behörden, Landeseinrichtungen oder beteiligten Institutionen, die im Rahmen der Teilnahme am Verfahren QeS die Signaturkarte beantragen und einsetzen. Ein Teilnehmer ist als Zertifikatsinhaber immer eine natürliche Person.

2.1.4 Zertifizierungsdiensteanbieter (ZDA T-TeleSec)

Der Zertifizierungsdiensteanbieter (ZDA) stellt eine eigene geprüfte Registrierungsinfrastruktur zur Verfügung, so dass keine weiteren Organisationseinheiten im Beantragungsprozess benötigt werden. Die Antragsbearbeitung und –weiterleitung sowie die Verwaltung der ausgegebenen Zertifikate übernimmt die Registrierungsstelle Thüringen als zertifizierte Registrierungsstelle des ZDA. Die Registrierungsmitarbeiter des ZDA erbringen alle notwendigen Leistungen für die Erstellung und Ausgabe der Zertifikate für die Zertifikatsinhaber und Teilnehmer des Freistaats Thüringen.

Die PKI Thüringen ist im Bereich der fortgeschrittenen Zertifikate als Master-RA beim Zertifizierungsdiensteanbieter T-TeleSec eingebunden.

2.1.5 Zuständiges Ministerium

Das für ressortübergreifende Informations- und Kommunikationstechnik und E-Government zuständige Ministerium, derzeit das TFM, plant die erforderlichen Haushaltsmittel für die Registrierungsstelle, sofern durch die Anzahl der Teilnehmer kein kostendeckender Betrieb möglich ist. Das Ministerium koordiniert die strategische Weiterentwicklung der PKI-Struktur im Freistaat.

2.1.6 PostIdent Filialen

Die Registrierungsstelle Thüringen bedient sich bei der Identifizierung der Antragsteller im Bereich der qualifizierten und fortgeschrittenen Signaturzertifikate der PostIdent-Filialen der Deutschen Post AG. Die Einbeziehung der PostIdent-Filialen wird über ein zwischen dem Thüringer Landesrechenzentrum, in welchem die Registrierungsstelle Thüringen angesiedelt ist, und der Deutschen Post AG geschlossenen Vertrag gesichert.

2.1.7 Übersicht der beteiligten Instanzen

Die folgende Abbildung soll die an der Beantragung und Ausgabe der Signaturkarte beteiligten Instanzen aufzeigen.

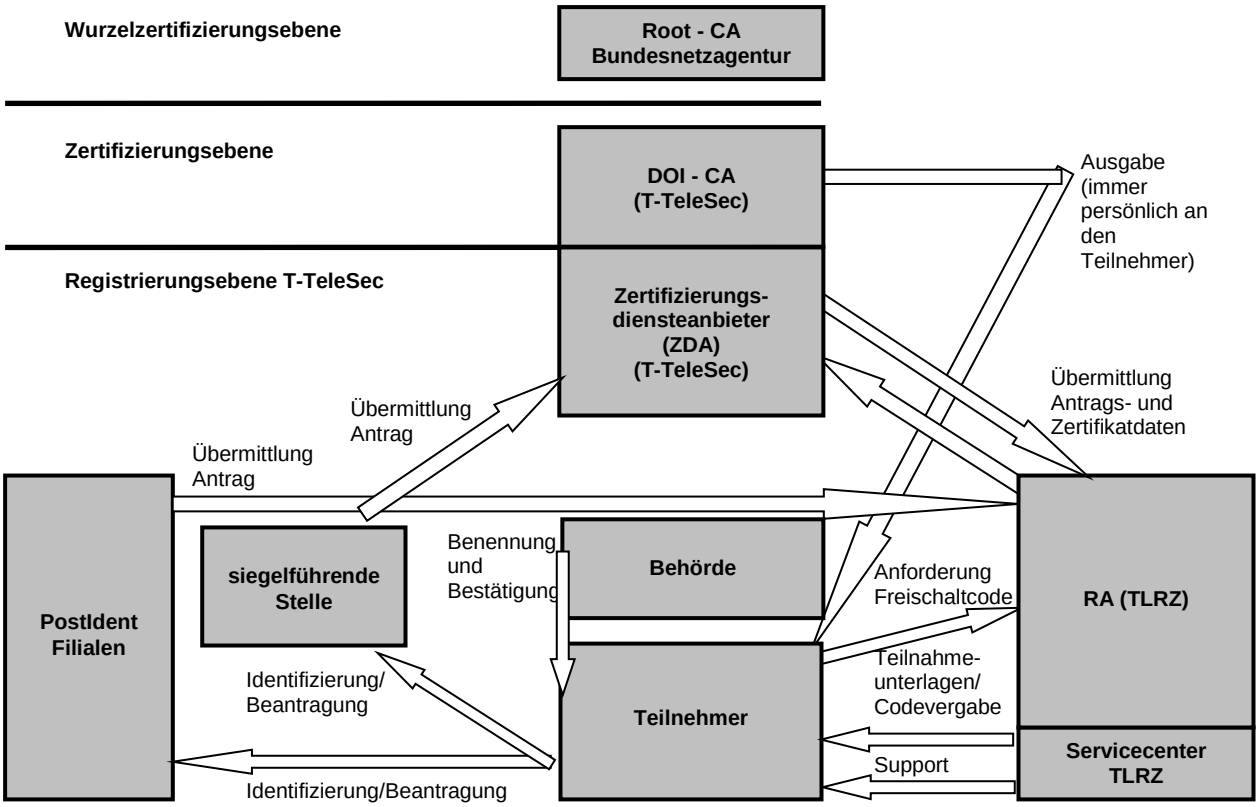


Abbildung 1: Verfahren QeS – beteiligte Instanzen

Die von der PKI Thüringen ausgegebenen Zertifikate werden im Bereich der qualifizierten Signatur von einem akkreditierten Trustcenter nach dem Deutschen Signaturgesetz, dem Trustcenter der T-TeleSec, erstellt. Überwacht wird das Verfahren von der Bundesnetzagentur als höchste Instanz nach dem Deutschen Signaturgesetz. Als oberste Zertifizierungsstelle unterzeichnet sie die Zertifikate des akkreditierten Trustcenters.

3 Ablauforganisation der PKI Thüringen

3.1 Abläufe im Verfahren QeS-EG-DLR

Abläufe sind die Prozesse, in deren Ergebnis die Teilnehmer mit der Signaturkarte für eine qualifizierte elektronische Signatur ausgestattet werden. Diese werden in den folgenden Kapiteln übersichtsartig beschrieben.
Die Darstellung dieser Prozesse in Form von Flussdiagrammen und tabellarisch wird im Organisationshandbuch QeS erfolgen. Die Erstellung und Pflege des Verfahrenshandbuchs QeS wird in der Zuständigkeit des TLRZ und in Abstimmung mit T-TeleSec erfolgen.

Die nachfolgend grafisch dargestellten Abläufe werden als Ereignisgesteuerte Prozessketten (EPK) abgebildet. Eine Beschreibung der Symbole und Begriffe ist in zwei Beispielabbildungen in Anhang dargestellt (siehe 9.1).

Als Anlage zum Organisationshandbuch werden die Prozesse in HTML-Form mitgeliefert.

3.1.1 Teilnehmerzertifizierung

Der Prozess der Teilnehmerzertifizierung ist in fünf Teilprozesse untergliedert, die hier skizziert und beschrieben werden.

Prozessabbildung "Teilnehmerzertifizierung"

Abbildung 2: Ablaufübersicht "Teilnehmerzertifizierung"

Hinweis
Wesentlich für die erfolgreiche Beantragung und Ausgabe der Signaturkarte ist die Verwendung von Freischaltcodes. Das Thüringer Landesrechenzentrum (TLRZ) beantragt beim ZDA (T-TeleSec) ein Budget an Freischaltcodes, welches in der Verwaltungssoftware (siehe 4.3) abgelegt wird. Die Anzahl der beantragten Codes richtet sich nach dem fachlichen Bedarf in Abstimmung mit den Verfahrensverantwortlichen der jeweiligen Behörden.

3.1.1.1 Prozess Anforderung Code

Im Prozess **Anforderung Code** beantragen Behörden, Einrichtungen oder beteiligte Institutionen Freischaltcodes für die Teilnehmer (Benennen diese Teilnehmer), die für ihre Fachverfahren Signaturkarten benötigen. Die Antragstellung erfolgt durch den berechtigten Mitarbeiter der Behörde online über die PKI-Webseite Thüringen (www.signaturen.thueringen.de). In einem ersten Schritt werden die Angaben zur Behörde und die Anzahl der notwendigen Signaturkarten abgefragt und in einem zweiten Schritt die persönlichen Daten für den (die) Signaturkarteninhaber.

Die behördeninterne Vorgehensweise ist nicht Bestandteil des Organisationshandbuches und wird hier nicht näher erläutert.

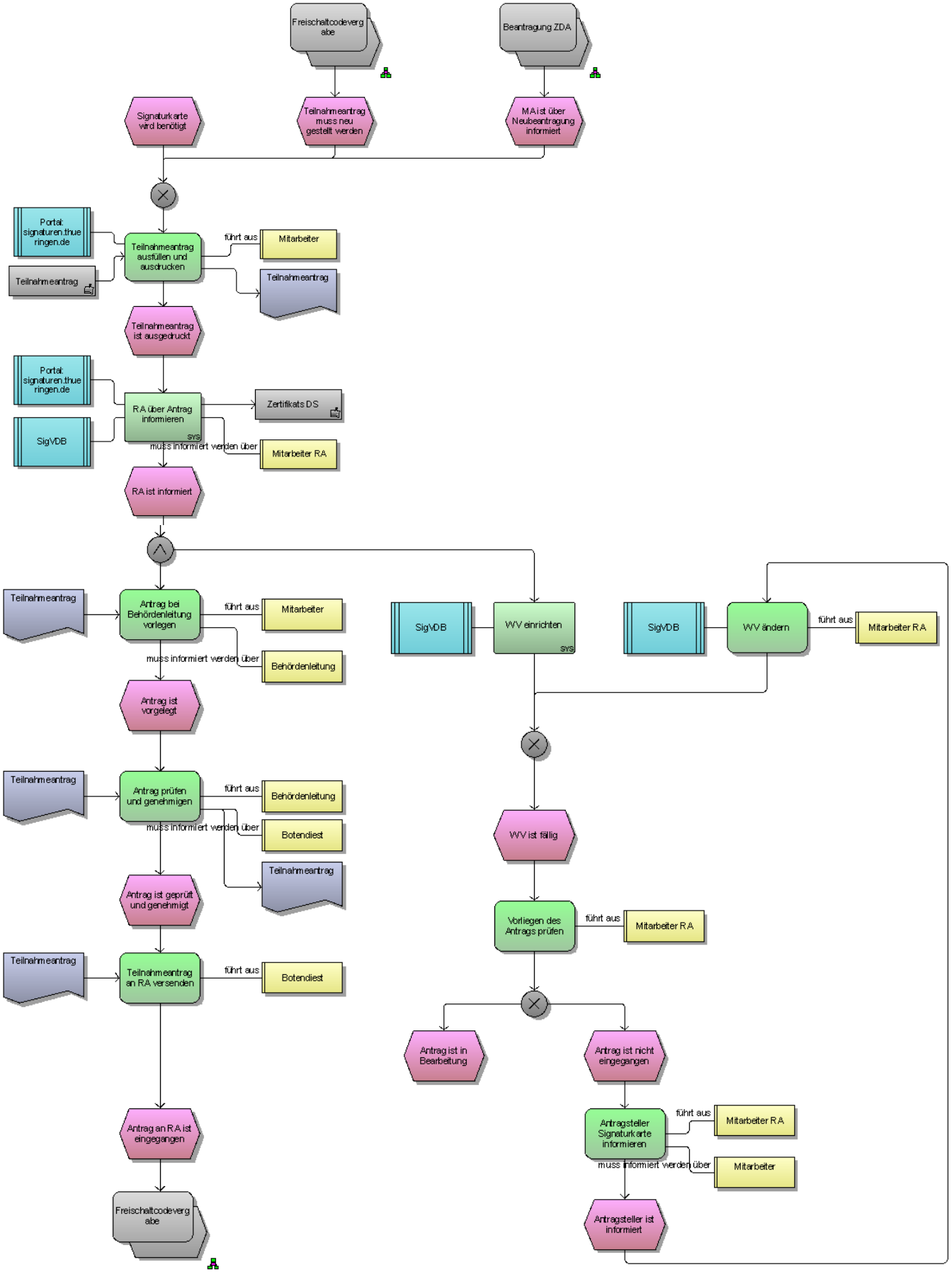
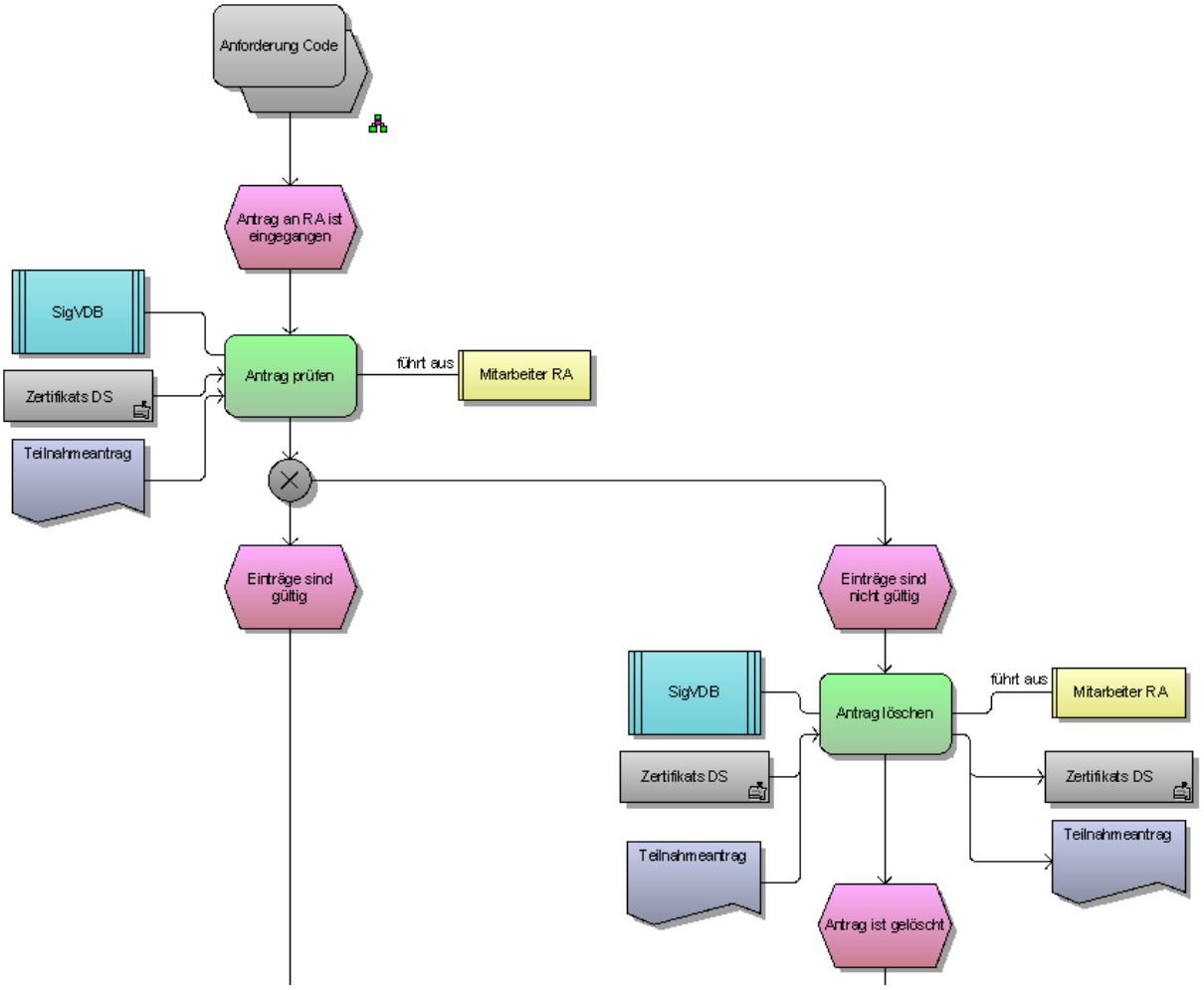


Abbildung 3: Prozessabbildung "Anforderung Code“

3.1.1.2 Prozess Freischaltcodevergabe

Im Prozess **Freischaltcodevergabe** erhalten die benannten Teilnehmer der Behörden, Einrichtungen oder beteiligten Institutionen eine Teilnahmebestätigung mit dem benötigten Freischaltcode vom TLRZ. Der Teilnehmer ist damit selbst in der Lage, die Signaturkarte über die PKI-Webseite Thüringen (www.signaturen.thueringen.de) online zu beantragen.



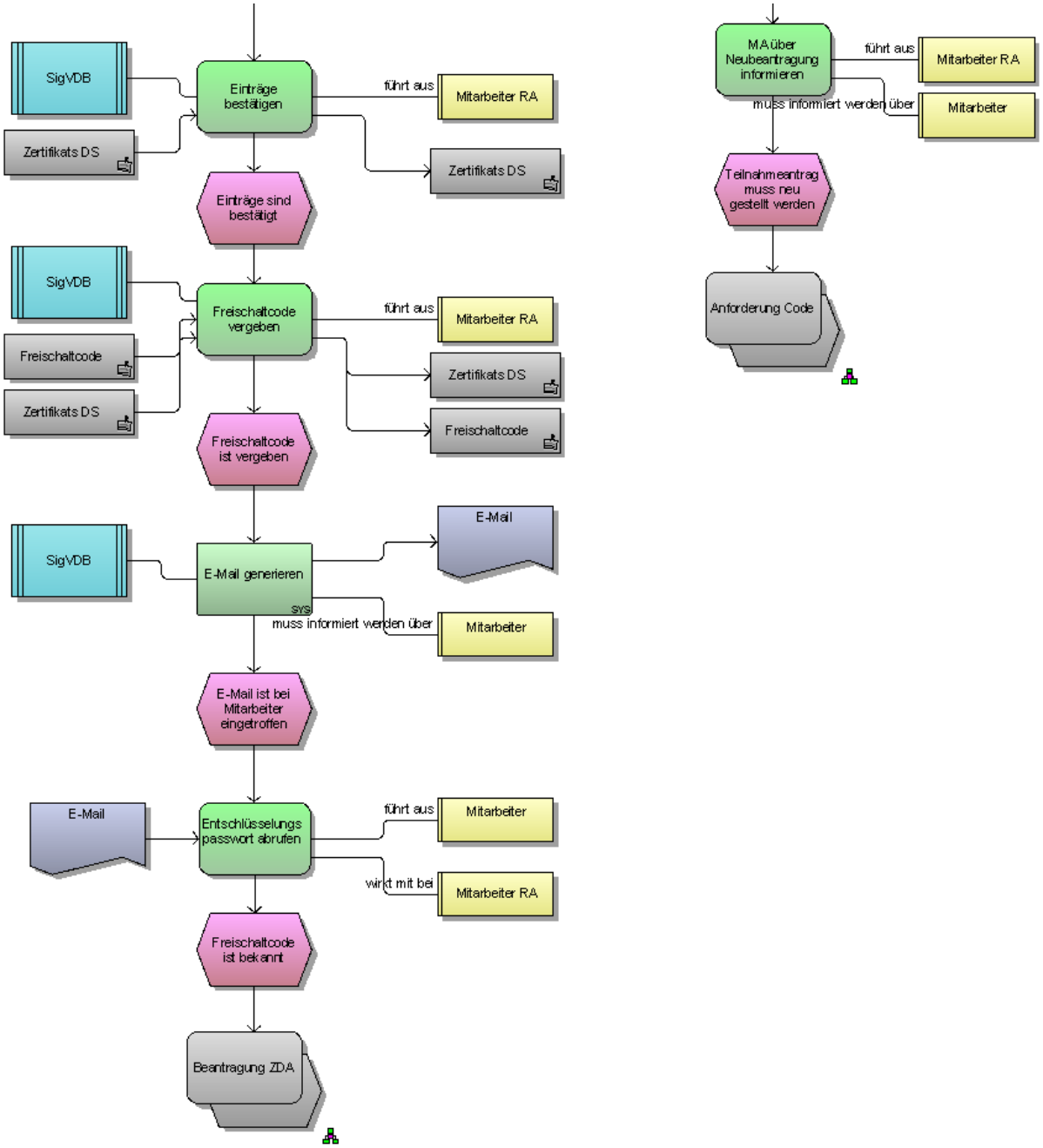


Abbildung 4: Prozessabbildung "Freischaltcodevergabe“

3.1.1.3 Prozess Beantragung ZDA

Der Teilnehmer wird über die PKI-Webseite Thüringen direkt auf die Antragsseite des ZDA TeleSec (https://www.telesec.de/cgi-bin/pksauftrag_doith.pl) geleitet und beantragt dort unter Angabe seines Freischaltcodes die Signaturkarte. Nur mit dem Freischaltcode ist die Onlinebeantragung im Portal möglich. Die Mehrfachnutzung des Codes ist technisch ausgeschlossen.

Der erzeugte Zertifikatsantrag inkl. PostIdent-Coupon wird ausgedruckt und der Antrag wird durch den Teilnehmer unterschrieben. Die Identifizierung des Teilnehmers und Übermittlung der Antragsunterlagen erfolgt abschließend durch das PostIdent-Basic Verfahren. Mittels dieses Verfahrens werden die Antragsunterlagen von der Deutschen Post über die Registrierungsstelle an den Zertifizierungsdienstanbieter (ZDA) T-TeleSec übermittelt.

Alternativ ist auch die persönliche Identifizierung des Antragstellers in der Registrierungsstelle (TLRZ) möglich.

In der Registrierungsstelle werden die in Papierform eingehenden Anträge mit den in der Verwaltungs-DB hinterlegten Antragsinformationen verglichen, die Anträge zur Archivierung eingescannt und anschließend postalisch an den ZDA zur weiteren Bearbeitung weitergeleitet.

Eine Anfrage beim ZDA hat ergeben, dass die Weiterleitung der Antragsunterlagen von der Registrierungsstelle an den ZDA derzeit noch nicht auf elektronischem Wege erfolgen kann.

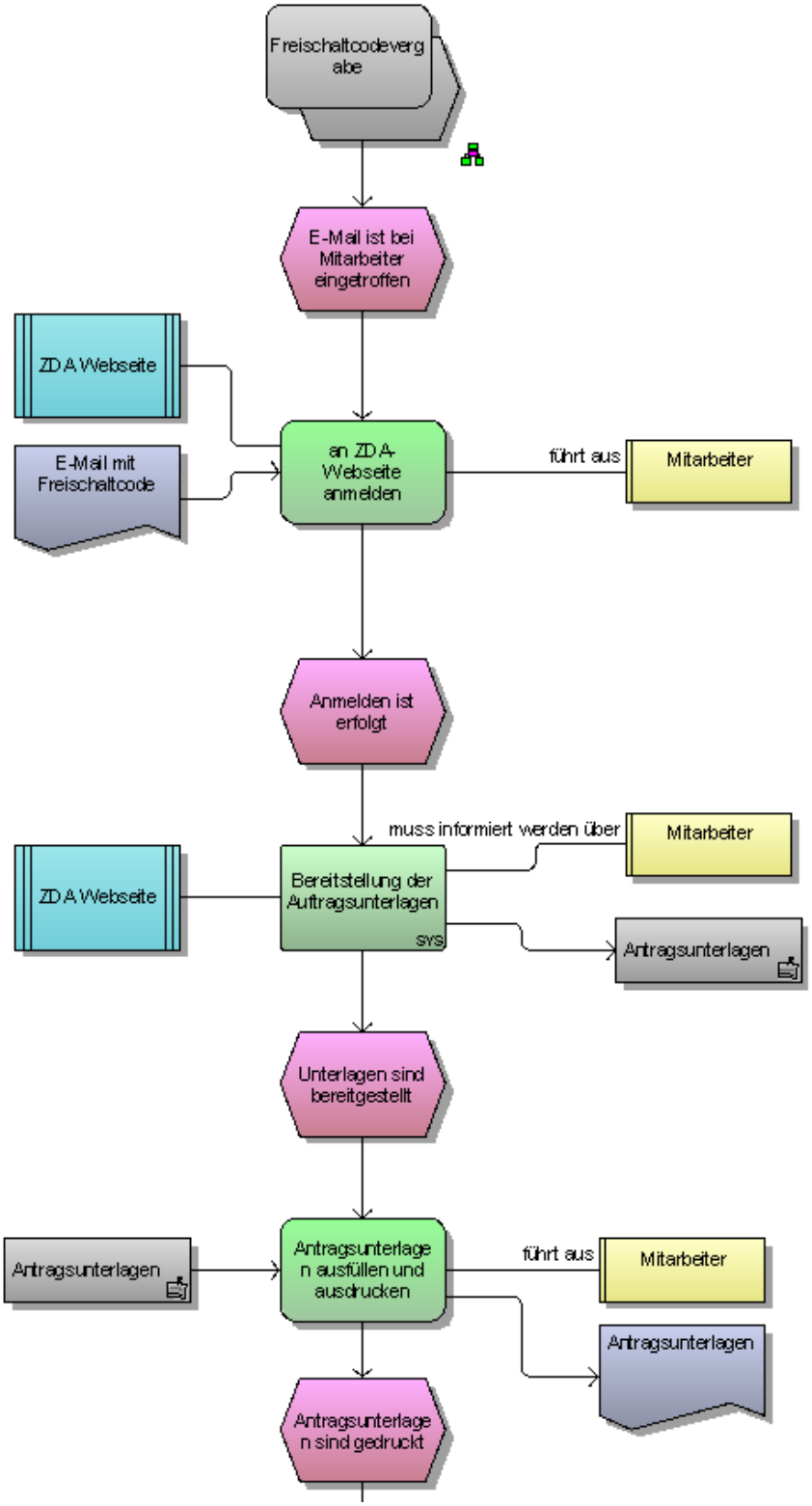


Abbildung 5: Prozessabbildung "Beantragung ZDA (I)“

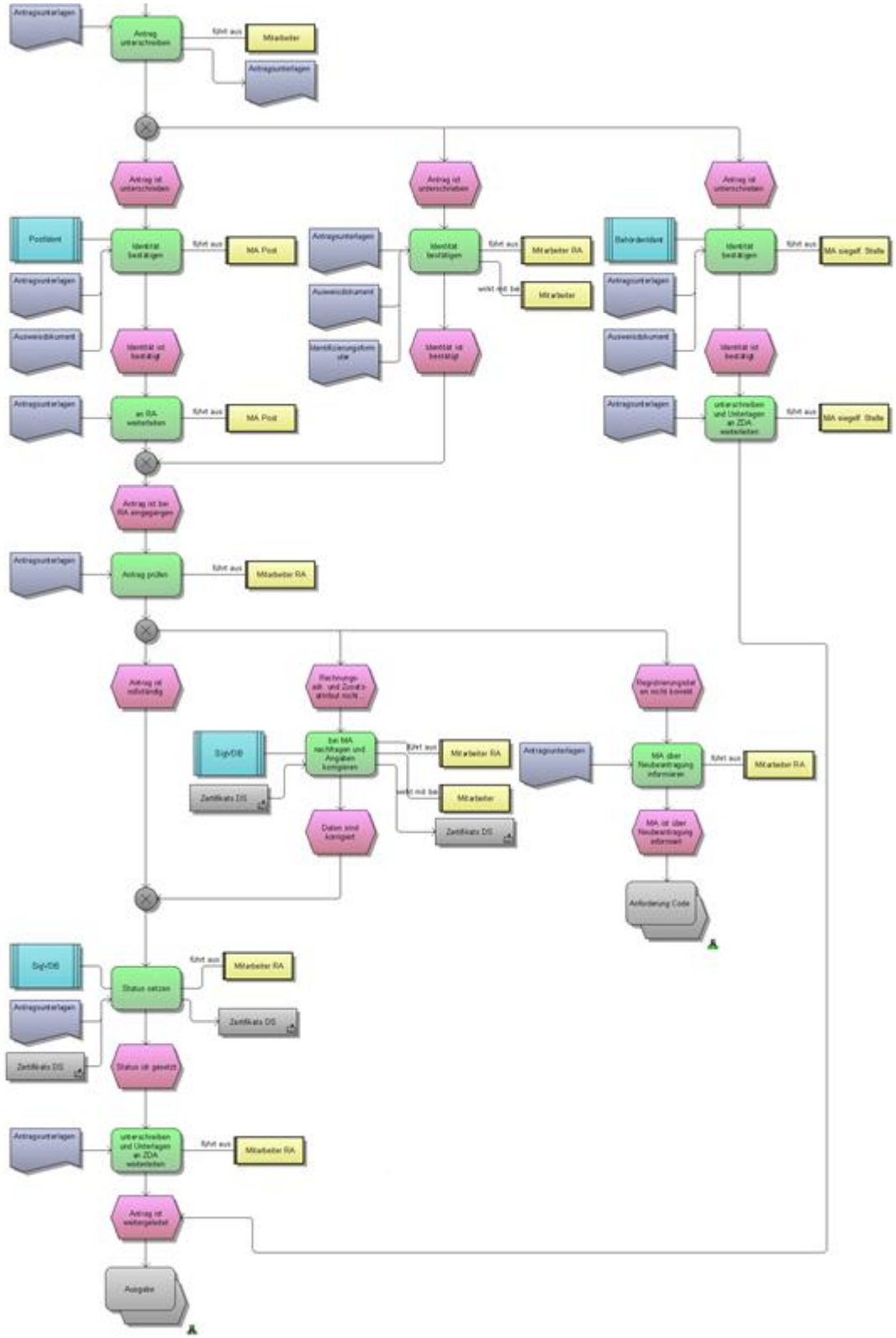


Abbildung 6: Prozessabbildung "Beantragung ZDA (II)“

3.1.1.4 Prozess Ausgabe

Der Herstellungsprozess der Qualifizierten Zertifikate wird durch die Bundesnetzagentur überwacht. Diese Behörde ist die oberste Zertifizierungsstelle und unterschreibt die Zertifikate des akkreditierten Trustcenters.

Der Teilnehmer erhält die beantragte Signaturkarte direkt vom ZDA auf dem Postweg. Dabei befindet sich die unversehrte Signaturkarte im Null-PIN Status. Der Teilnehmer prüft die Unversehrtheit der Karte mittels Null-PIN Verfahren sowie die Korrektheit der Daten (Zertifikat, Name und Behördenbezeichnung) und bestätigt dies gegenüber dem ZDA. Durch den Teilnehmer erfolgt dann die Vergabe von PIN1 und PIN2.

Erst nach Rückmeldung dieser Informationen durch den Karteninhaber erfolgt durch den ZDA das Freischalten des Signaturzertifikates und die Karte ist für qualifizierte elektronische Signaturen einsetzbar.

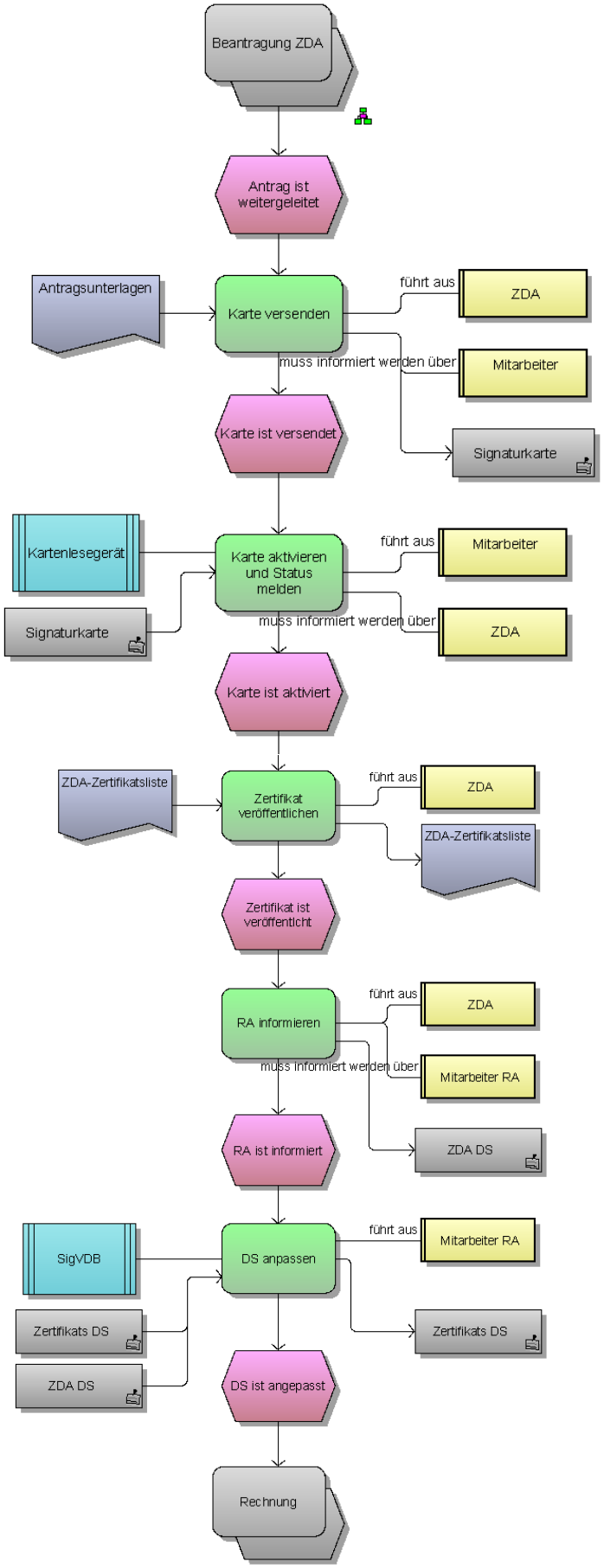


Abbildung 7: Prozessabbildung "Ausgabe“

3.1.1.5 Prozess Rechnung

Gemäß den vertraglichen Regelungen werden die Kosten für die tatsächlich in Anspruch genommenen Identifizierungen des PostIdent-Basic Verfahrens durch die Deutsche Post AG, der Anzahl der ausgestellten Signaturkarten durch den ZDA und der geleisteten Aufwände des TLRZ durch die Registrierungsstelle in Abhängigkeit der Rechnungslegung Dritter gegenüber den beantragenden Ressorts in Rechnung gestellt. Die Teilnahmeanträge für die QeS werden dazu so angepasst, dass bereits bei der Antragstellung jedem Antrag eine konkrete Rechnungsadresse zugeordnet wird. Dies ist entweder über die Zuordnung zu einem konkreten Fachverfahren oder über die explizite Eingabe einer Rechnungsadresse möglich.

Die Bereitstellung der Leistung des TLRZ wird, sofern kein kostendeckender Betrieb möglich ist, dem zuständigen Ministerium (siehe 2.1.5) auf Grundlage einer Servicevereinbarung mit dem TLRZ in Rechnung gestellt.

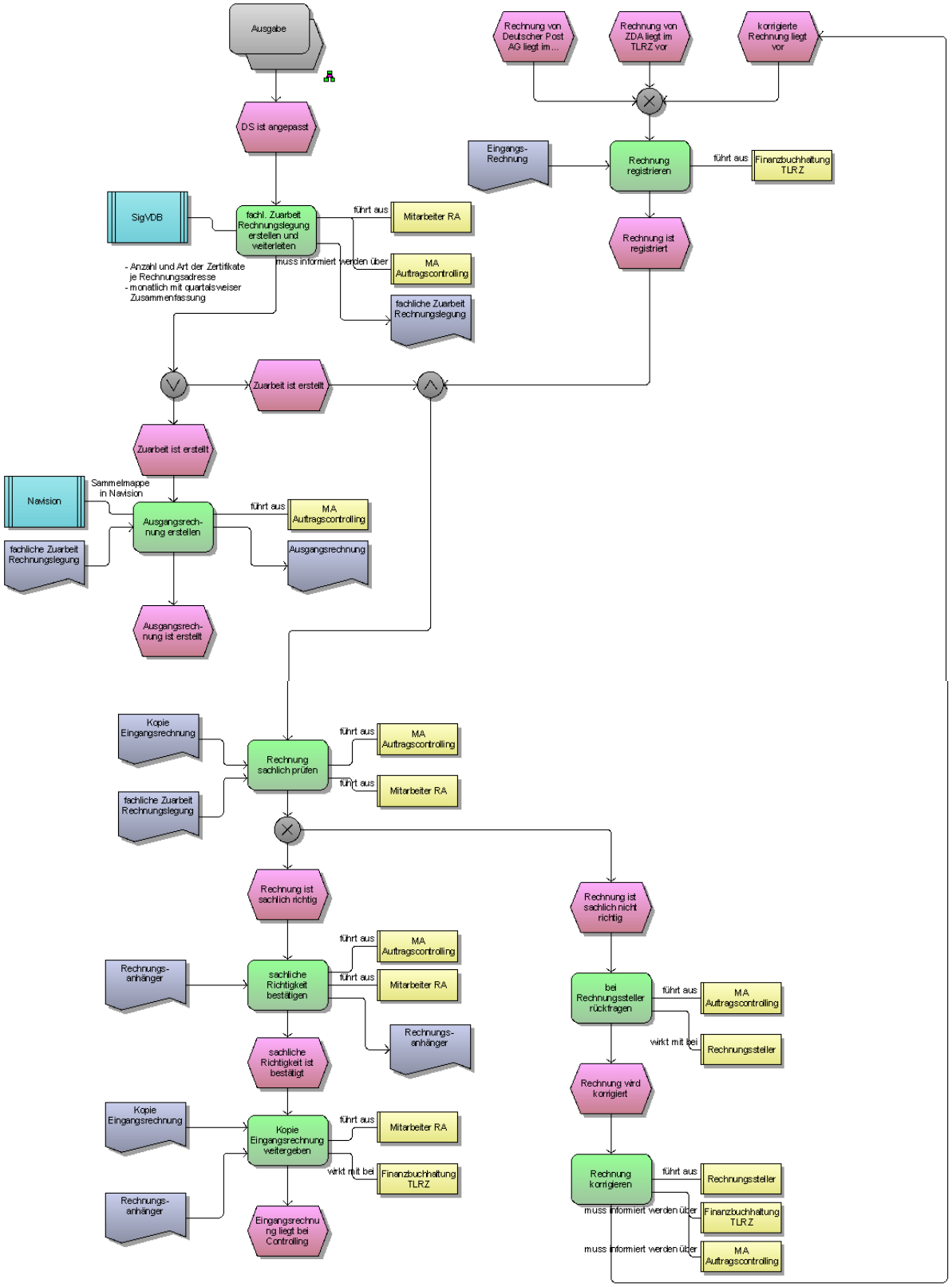


Abbildung 8: Prozessabbildung "Rechnung“

3.1.2 kompletter Ablaufplan für den Erhalt einer Signaturkarte

In der nachfolgenden Tabelle wird der komplette Ablauf für die Beantragung einer Signaturkarte beschrieben:

Vorbedingung	**Aktion**	**Ergebnis**	**Handelnde Person/en** (Ausführende/r – A, Beteiligte/r – B)
1. Eine Signaturkarte wird benötigt.	Stellung Teilnahmeantrag über PKI-Portal (http://www.signaturen.thueringen.de/), Ausfüllen aller notwendigen Angaben zum Antragsteller, der Behörde,… und Ausdruck des Antrags	2. Der Teilnahmeantrag ist ausgefüllt und ausgedruckt.	Mitarbeiter der Behörde (A)
2. Der Teilnahmeantrag ist ausgedruckt.	Die Registrierungsstelle wird über die Antragsstellung informiert, ein Antrags-DS sowie eine Wiedervorlage nach 14 Tagen wird in der SigVDB automatisch angelegt und eine Mail an den Antragsteller mit dem fertigen Antrag und seiner persönlichen Identifikationsnummer versendet.	3. Der Antragsteller erhält eine Mail mit dem Antrag und seiner persönlichen Identifikationsnummer. Die RA ist über den neuen Antrag informiert 8. Eine Wiedervorlage für den RA-Mitarbeiter wurde angelegt	PKI-Portal (A), RA-MA (B)
3. Der Antragsteller erhält eine Mail mit dem Teilnahmeantrag und seiner persönlichen Identifikationsnummer	Der Antragsteller trägt die persönliche Identifikationsnummer in seinen Antrag ein.	4. Der Teilnahmeantrag liegt vollständig dem Antragsteller vor.	MA der Behörde (A)
4. Der Teilnahmeantrag liegt vollständig dem Antragsteller vor.	Den Antrag unterschreiben und bei der Behördenleitung zur Genehmigung vorlegen.	5. Der Teilnahmeantrag ist der Behördenleitung zur Genehmigung vorgelegt.	MA der Behörde (A) Behördenleitung (B)
5. Der Teilnahmeantrag ist der Behördenleitung vorgelegt.	Den Antrag prüfen und genehmigen lassen. Einen Botendienst informieren.	6. Der Teilnahmeantrag ist genehmigt.	Behördenleitung (A) Botendienst (B)
6. Der Antrag ist geprüft und genehmigt.	Versand des Teilnahmeantrages an die Registrierungsstelle.	7. Der Teilnahmeantrag wird an die Registrierungsstelle versendet.	Botendienst (A)
8. Die WV ist fällig (Datensatz ist farbig markiert)	Prüfen, ob ein entsprechender Antrag vorliegt.	Der Antrag ist eingegangen und in Bearbeitung (7.) oder 9. der Antrag ist nicht eingegangen.	RA-MA (A)

Vorbedingung	Aktion	Ergebnis	Handelnde Person/en (Ausführende/r – A, Beteiligte/r – B)
9. Der Antrag ist nicht eingegangen.	Den Antragsteller der Signaturkarte informieren.	10. Der Antragsteller der Signaturkarte wird informiert.	RA-MA (A) MA der Behörde (B)
10. Der Antragsteller ist informiert.	Klärung mit dem Antragsteller, was weiter mit dem Antrag passieren soll. In der SigVDB den Status ändern (neues WV-Datum wird gesetzt) oder, wenn der Antragsteller dies wünscht, den Antrags-DS löschen.	Die WV in der SigVDB hat ein neues WV-Datum. oder: der Antrags-DS wurde gelöscht.	RA-MA (A)
7. Der Antrag ist bei der Registrierungsstelle eingegangen.	Überprüfung der Angaben des eingegangenen Teilnahmeantrags mit denen des Antrags-DS in der SigVVB.	11. Die Einträge sind gültig oder nicht gültig.	RA-MA (A)
11.1 Die Einträge sind nicht gültig.	Den Teilnahmeantrag sowie den Antrags-DS in der SigVDB löschen.	12. Der Antrag-DS wird gelöscht, der Papierantrag wird vernichtet.	RA-MA (A)
12. Der Antrag ist gelöscht.	Den Mitarbeiter der Behörde über die notwendige Neubeantragung informieren.	Der Teilnahmeantrag muss neu gestellt werden.	RA-MA (A) MA der Behörde (B)
11.2 Die Einträge sind gültig.	Die Einträge aus dem Antrags-DS in der SigVDB bestätigen.	13. Der Antrag wird bestätigt.	RA-MA (A)
13. Der Antrag wurde bestätigt.	Einen Freischaltcode aus der Freischaltcode-Liste dem Antrags-DS der SigVDB vergeben. Den Status in dem Antrags-DS der SigVDB entsprechend auf „Freischaltcode vergeben“ setzten	14. ein Freischaltcode wird vergeben.	RA-MA (A)
14. Der Freischaltcode wurde vergeben.	Die SigVDB generiert automatisch eine E-Mail, die dem Mitarbeiter der Behörde den Freischaltcode (in einer verschlüsselten PDF-Datei) übermittelt und ihn über den Link zum Online-Antrag (Weiterleitung auf die TeleSec-Seite) informiert.	15. E-Mail wird abgeschickt.	SYS (A) MA der Behörde (B)
15. Die E-Mail ist bei dem Mitarbeiter eingetroffen	tel. Rückfrage bei der RA, um das Passwort für die PDF-Datei abzurufen. Die PDF-Datei entschlüsseln.	17. Die Datei mit dem Freischaltcode konnte entschlüsselt werden.	MA der Behörde (A) RA-MA (B)
16. Den Status in der SigVDB	Den Status in dem Antrags-DS der SigVDB entsprechend auf „PDF-Passwort	Der Status wird gesetzt.	RA-MA (A)

Vorbedingung	**Aktion**	**Ergebnis**	**Handelnde Person/en** (Ausführende/r – A, Beteiligte/r – B)
anpassen	abgefragt“ setzten		
17. Die Datei mit dem Freischaltcode konnte entschlüsselt werden.	Anmelden und Freischalten mit den Freischaltcodes aus der E-Mail an der ZDA Webseite.	18. Die Anmeldung ist erfolgt.	MA der Behörde (A)
18. Die Anmeldung ist erfolgt.	Die Antragsunterlagen, die von der ZDA Webseite bereitgestellt wurden, ausfüllen und ausdrucken.	19. Die Antragsunterlagen (incl. PostIdent-Antrag) werden gedruckt.	MA der Behörde (A)
19. Die Antragsunterlagen sind ausgedruckt.	Die Antragsunterlagen unterschreiben	20. Der Antrag ist unterschrieben.	
20. Der Antrag ist unterschrieben.	Zur Identifikation des Antragstellers Aufsuchen der Registrierungsstelle oder einer Postfiliale mit PostIdent	21. Antragsteller stellt sich in RA persönlich vor oder 23 Antragsteller stellt sich in einer siegelführenden Stelle persönlich vor oder 23. Antragsteller stellt sich in Postfiliale mit PostIdent persönlich vor.	MA der Behörde (A)
21. Antragsteller stellt sich in RA persönlich vor.	Kontrolle des Ausweisdokuments gem. , Übernahme der Ausweisdaten in Formular „Identitätsfeststellung“ (siehe 7) mit Unterschrift des Antragstellers	22. Die Identität des Antragstellers ist bestätigt.	MA-RA (A)
23 Antragsteller stellt sich in der siegelführenden Stelle mit BehördenIdent und der „Schritt für Schritt Anleitung zum BehördenIdent“ persönlich vor.	Kontrolle des Ausweisdokumentes und ausfüllen des Formulars zum BehördenIdent	24. Die Antragsunterlagen werden zusammen mit der Ausweiskopie und dem ausgefüllten Formular zum BehördenIdent an den ZDA weitergeleitet.	MA der siegelführenden Stelle
25. Antragsteller stellt sich in Postfiliale mit PostIdent persönlich vor.	Die Antragsunterlagen in einen Umschlag verpacken. Diesen zusammen mit dem PostIdent-Antrag und dem zur Identifikation notwendigen Dokument (Personalausweis) dem Post-MA übergeben	26. Der Antragsteller kann identifiziert werden.	MA der Behörde (A)
26. Der Antragsteller	Der Post-MA überprüft die	27. Die Identität wird	MA Dt. Post AG

Vorbedingung	Aktion	Ergebnis	Handelnde Person/en (Ausführende/r – A, Beteiligte/r – B)
kann identifiziert werden.	Identität des Antragstellers mit dem Ausweisdokument und bestätigt dies auf dem geschlossenen Umschlag mit den Antragsunterlagen	bestätigt.	(A)
27. Die Identität ist bestätigt.	Weiterleitung der Antragsunterlagen an die Registrierungsstelle Thüringen	28. Der Antrag wird an die RA Thüringen weitergeleitet.	MA Dt. Post AG (A)
28. Der Antrag ist bei der Registrierungsstelle eingegangen	Die Antragsunterlagen prüfen, ob die Registrierungsdaten korrekt sind (Vergleich der Angaben in Ausweiskopie und im Antrag).	29 Registrierungsdaten sind nicht korrekt.	MA-RA (A)
29. Registrierungsdaten sind nicht korrekt.	Mitarbeiter (Antragsteller) über die Neubeantragung informieren, Status in SigVDB auf Anfangswert zurücksetzen.	Antragsteller wird über Neubeantragung informiert.	MA-RA (A)
25/ 27 der Antragsteller wurde identifiziert	Antrag auf Vollständigkeit prüfen (Gültigkeit der Rechnungsadresse; korrektes Zusatzattribut)	29.1 Der Antrag ist vollständig oder 29.2 die Rechnungs-adresse und Zusatzattribut sind nicht vollständig	MA-RA (A)
29.2 Rechnungsadresse und Zusatzattribute sind nicht vollständig.	Bei Mitarbeiter der Behörde telefonisch nachfragen und die Angaben des Antrags-DS korrigieren.	28 Daten werden in der SigVDB korrigiert und sind vollständig.	MA-RA (A) MA der Behörde (B)
29.1/30 Der Antrag ist vollständig.	Den Status in dem Antrags-DS der SigVDB entsprechend auf „Antrag bearbeitet“ setzten	31 Status wird gesetzt.	MA-RA (A)
31 Der Status ist gesetzt.	Die Antragsunterlagen unterschreiben und die Unterlagen an den ZDA weiterleiten.	32 Die Unterlagen werden weitergeleitet.	MA-RA (A)
33 Die Unterlagen sind beim ZDA eingegangen.	Das beantragte Zertifikat wird erstellt und auf einer Signaturkarte hinterlegt. Die Karte wird per Post an den Antragsteller versendet.	34 Die Karte wird versendet. Informationen über den Versand der Karte werden per E-Mail an die RA weitergeleitet	Telesec (A) MA der Behörde (B)
34.1 Die Karte ist versendet, die Registrierungsstelle ist über den Kartenversand	Den Status in dem Antrags-DS der SigVDB entsprechend auf „Zertifikat versendet“ setzten	35. Der Status wird gesetzt.	MA-RA (A)

Vorbedingung	Aktion	Ergebnis	Handelnde Person/en (Ausführende/r – A, Beteiligte/r – B)
informiert			
34.2 Die Karte ist beim Antragsteller eingegangen	Mit einem Kartenlesegerät wird die Karte aktiviert (Null-PIN-Status wird aufgehoben, PIN 1 und PIN 2 werden vergeben). Auf beiliegendem Schreiben bestätigt der Antragsteller den ordnungsgemäßen Empfang (die Unberührtheit des Null-PIN-Status) der Karte und sendet dieses an den ZDA zurück.	36 Karte wird aktiviert und der Status dem ZDA gemeldet.	MA der Behörde (A) Telesec (B)
36 Die Karte ist aktiviert.	Veröffentlichung der Zertifikatsinformationen in den Listen des ZDA. Darüber wird die Registrierungsstelle informiert.	37 Die Registrierungsstelle wird über die Aktualisierung der Zertifikatslisten durch den ZDA informiert	Telesec (A) MA-RA (B)
37 Die Registrierungsstelle ist informiert.	Der RA-Mitarbeiter aktualisiert die RA-eigene Datenbank SigVDB. Den Antrags-DS und den TeleSec-DS aus der SigVDB anpassen.	38 Der DS wird angepasst und zu einem Zertifikats-DS zusammengefasst. Die SigVDB ist aktualisiert	MA-RA (A)

Tabelle 1: Ablaufdarstellung für die Beantragung einer QeS-Signaturkarte

3.1.3 Änderung Teilnehmerdaten

Eine Änderung von Teilnehmerdaten ist im Rahmen der QeS nicht möglich, hierzu ist in jedem Fall ein Neuantrag erforderlich.

3.1.4 Sperrung von Zertifikaten

Für jedes Zertifikat ist bereits bei der Antragstellung ein sperrberechtigter Dritter anzugeben, welcher neben dem Signaturkarteninhaber die Sperrung des Zertifikates veranlassen kann.

Die berechtigte Sperrung des Zertifikates kann durch die folgenden Stellen initiiert werden:

- a) den Inhaber des Zertifikats
- b) den sperrberechtigten Dritten
- c) die Registrierungsstelle (nach Beauftragung durch a) oder b))

Die Sperrung des Zertifikates kann auf folgenden Wegen erfolgen:

- telefonisch direkt beim ZDA (Sperrhotline **01805 / 26 82 02** unter Angabe des Telepasswortes)
- telefonisch bei der Registrierungsstelle im TLRZ (dieses wird die Sperrung für Sie initiieren) unter Angabe des Telepasswortes
- durch persönlich unterschriebenes formloses Anschreiben an den Zertifizierungsdiensteanbieter Deutsche Telekom AG (z.B. bei vergessenem Telepasswort). Das Schreiben muss in jedem Falle beinhalten:

- die Kartennummer,
- den Karteninhaber und
- den expliziten Sperrwunsch

Sperrinformationen, werden für die Zertifikatsnutzer online, mit einem standard-konformen Verfahren bereitgestellt. Es sind alle von dieser Zertifizierungsstelle gesperrten CA-Zertifikate enthalten. Es stehen Online-Informationen zum Zertifikatsstatus via OCSP unter http://ocsp.telesec.de/ocspr zur Verfügung.

Im Folgenden wird der Prozess zur Sperrung von Zertifikaten ausführlich beschrieben:

3.1.4.1 Sperren von qualifizierten Zertifikaten durch den Zertifikatsinhaber

Der Zertifikatsinhaber kann den Sperrprozess jederzeit gemäß folgender Vorgehensweise durchführen:

- 1.) Anrufen der allgemeinen PKS-Sperrhotline (01805 / 26 82 02)
- 2.) Identifikation über seinen Namen und sein bei der Beantragung des Zertifikats festgelegtes Telepasswort durch die PKS-Hotline
- 3.) Verbale Bestätigung des Sperrwunsches

Nach dieser Bestätigung erfolgt eine sofortige Sperrung des qualifizierten Zertifikats durch die Mitarbeiter der PKS-Sperrhotline und die Veröffentlichung in den unterschiedlichen Sperrlisten und Diensten.

Alternativ zu der Sperrung per Telefon, besteht noch die Möglichkeit das Zertifikat mit einem formlosen Anschreiben an den Zertifizierungsdiensteanbieter Deutsche Telekom AG zu sperren. Aus diesem Schreiben müssen das zu sperrende Zertifikat, d.h. die Angabe

- der Kartennummer,
- des Karteninhabers und
- der explizite Sperrwunsch

erkennbar sein. Dieser Auftrag muss vom Zertifikatsinhaber unterschrieben werden, da auf dieser Basis die Identifikation des Teilnehmers erfolgt. Dieser Prozess ist als Notfall zu sehen, für den Fall, dass der Zertifikatsinhaber sein Telepasswort vergessen hat.

Das genaue Vorgehen ist im Internet auf folgender Seite beschrieben:
http://www.telesec.de/pks/sperren.html

3.1.4.2 Sperren von qualifizierten Zertifikaten durch sperrberechtigte Dritte

Der Sperrprozess kann auf zwei verschiedenen Wegen initiiert werden.

Den Sperrprozess startet der sperrberechtigte Dritte entweder mit einer signierten E-Mail an die RA Thüringen mit der formlosen Aufforderung der Sperrung eines definierten qualifizierten Mitarbeiterzertifikats. Für die eindeutige Verifikation muss der Sperrende dabei folgende Informationen in der E-Mail angeben:

- Name und Vorname des MA, dessen Zertifikat gesperrt werden soll,
- die Aussage, dass es sich um ein qualifiziertes Zertifikat handelt und
- den Sperrgrund, warum das Zertifikat gesperrt werden soll.

Alternativ zu der Zusendung des Sperrauftrages per E-Mail kann auch ein Papierantrag an die RA Thüringen gesendet werden. In diesem Dokument müssen die oben genannten Daten enthalten sein und von dem Sperrberechtigten mit seiner Unterschrift bestätigt werden. Das Dokument muss dabei auf offiziellem Behörden-Briefbogen erstellt und mit einem Dienstsiegel bestätigt werden.

Der MA der RA Thüringen prüft, ob der Sperrauftrag vollständig bzw. eindeutig ist und eine sperrberechtigte Person den Sperrauftrag gestartet hat.

Die eigentliche Sperrung führt der MA der RA gemäß folgendem Arbeitsablauf durch:

1.) Anrufen der allgemeinen PKS-Sperrhotline (01805 / 26 82 02),

2.) Selektion des zu sperrenden Zertifikats über den Namen des Zertifikatsinhabers,

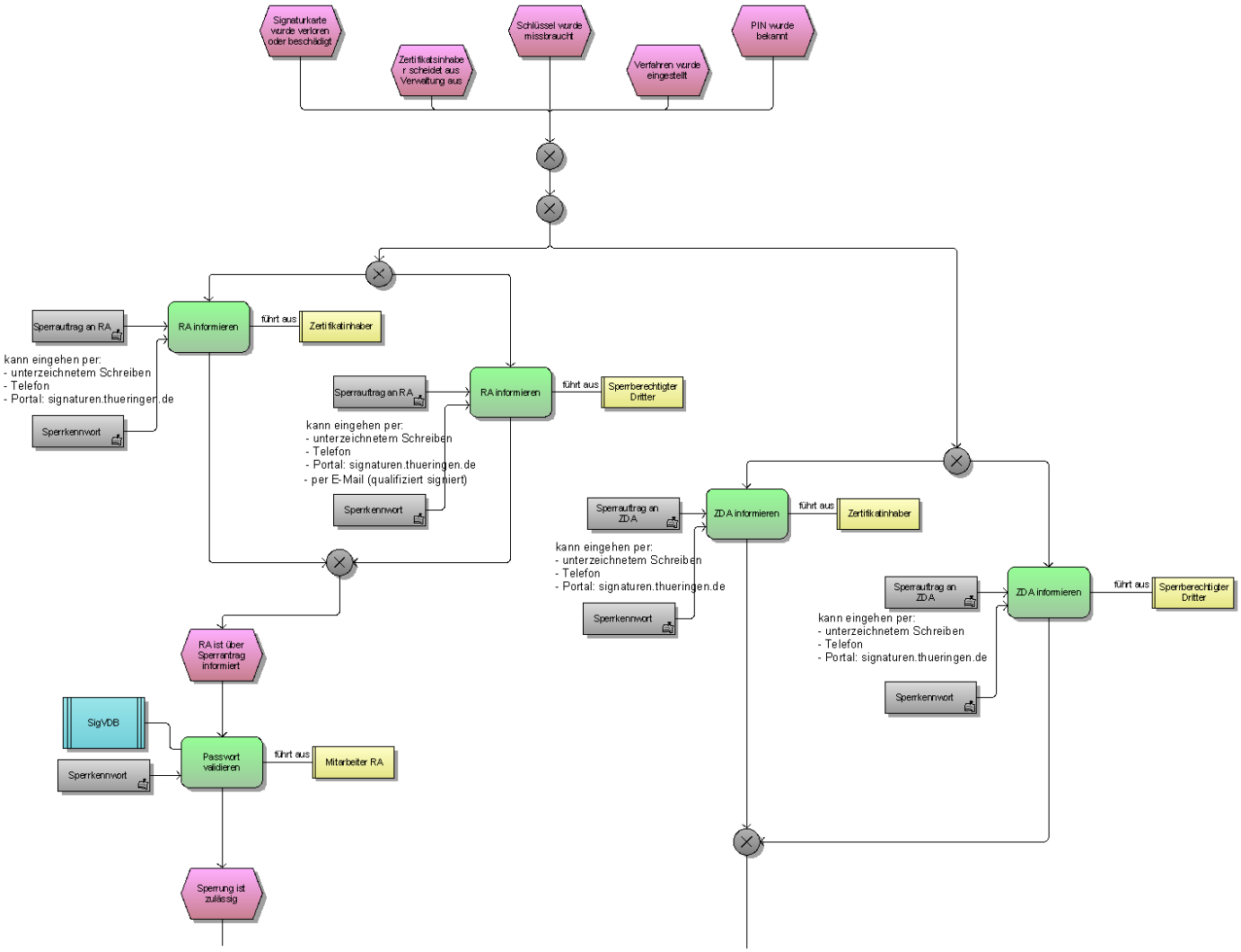
3.) Autorisierung der Sperrung über das bei der Beantragung des Zertifikats festgelegte Telepasswort,

4.) Verbale Bestätigung des Sperrwunsches.

Nach dieser Bestätigung erfolgt eine sofortige Sperrung des qualifizierten Zertifikats durch die Mitarbeiter der PKS-Sperrhotline und die Veröffentlichung in den unterschiedlichen Sperrlisten und Diensten.

Der Mitarbeiter der RA Thüringen schließt den Sperrvorgang über eine Rückmeldung in Form einer E-Mail an den sperrenden Dritten mit der Bestätigung der Sperrung ab.

Alternativ zu der Sperrung per Telefon hat der MA der RA Thüringen ebenfalls die Möglichkeit das Zertifikat mit einem formlosen Anschreiben an den Zertifizierungsdiensteanbieter Deutsche Telekom AG zu sperren. Aus diesem Schreiben müssen das zu sperrende Zertifikat (z.B. identifizierbar über die bekannten Zertifikatsdaten), die sperrende Institution und der explizite Sperrwunsch erkennbar sein. Dieser Auftrag muss dann von einem vertretungsberechtigten Mitarbeiter persönlich unterschrieben und mit einem Dienstsiegel bestätigt werden. Aufgrund der längeren Postlaufzeit ist dieser Prozess nur als Backup zu sehen, falls die entsprechenden Antragsunterlagen nicht mehr verfügbar sind.


Signaturkarte wurde verloren oder beschädigt
Zertifikatsinhaber scheidet aus Verwaltung aus
Schlüssel wurde missbraucht
Verfahren wurde eingestellt
PIN wurde bekannt
Sperrauftrag an RA
RA informieren
führt aus
Zertifikatinhaber
kann eingehen per:
- unterzeichnetem Schreiben
- Telefon
- Portal: signaturen.thueringen.de
Sperrkennwort
Sperrauftrag an RA
RA informieren
führt aus
Sperrberechtigter Dritter
kann eingehen per:
- unterzeichnetem Schreiben
- Telefon
- Portal: signaturen.thueringen.de
- per E-Mail (qualifiziert signiert)
Sperrkennwort
Sperrauftrag an ZDA
ZDA informieren
führt aus
Zertifikatinhaber
kann eingehen per:
- unterzeichnetem Schreiben
- Telefon
- Portal: signaturen.thueringen.de
Sperrkennwort
Sperrauftrag an ZDA
ZDA informieren
führt aus
Sperrberechtigter Dritter
kann eingehen per:
- unterzeichnetem Schreiben
- Telefon
- Portal: signaturen.thueringen.de
Sperrkennwort
RA ist über Sperrantrag informiert
SigVDB
Sperrkennwort
Passwort validieren
führt aus
Mitarbeiter RA
Sperrung ist zulässig

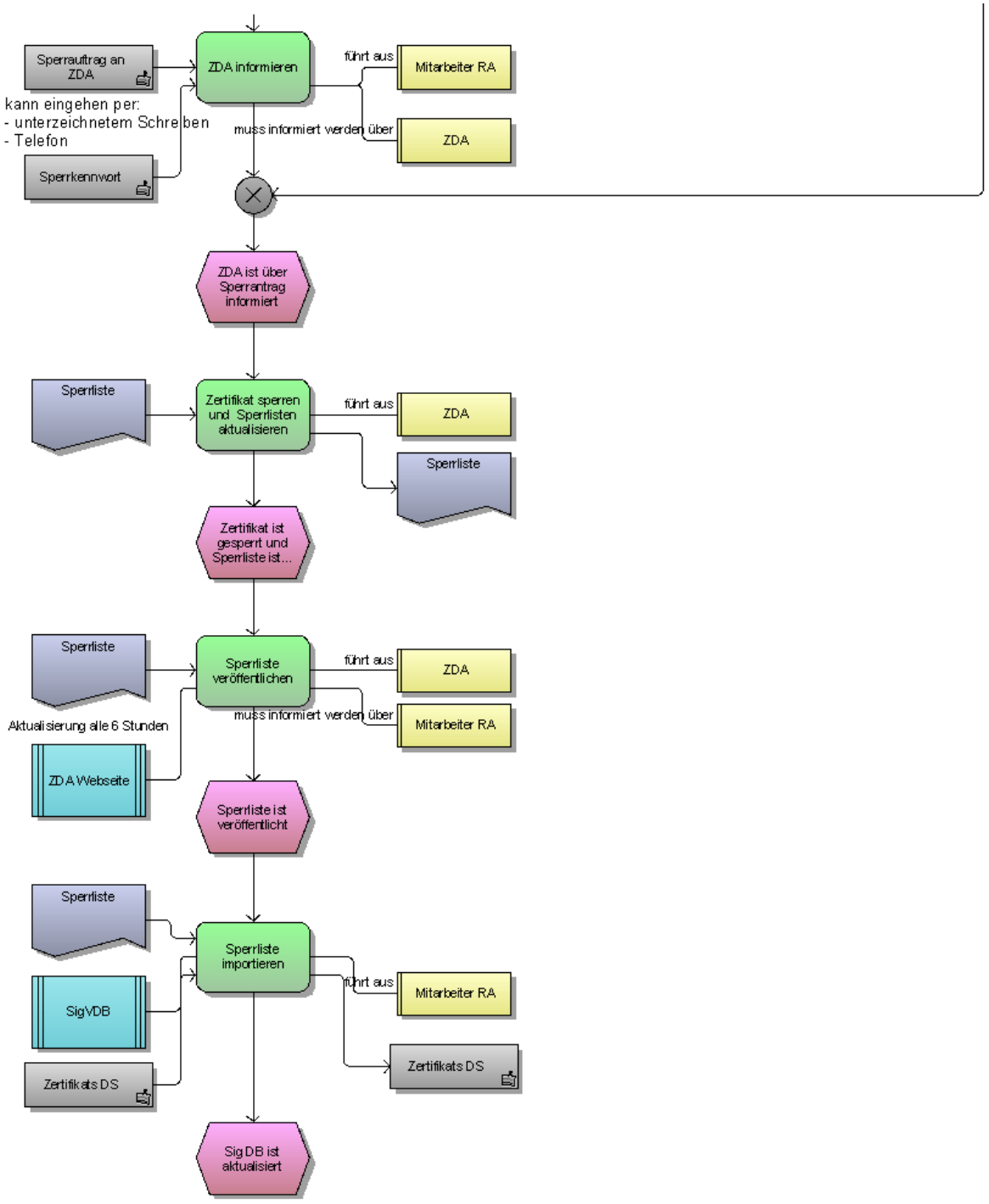


Abbildung 9: Prozessabbildung "Sperrung von Zertifikaten“

3.1.5 Information und Auskunft

Sämtliche Informationen zur Antragsstellung für fortgeschrittene und qualifizierte Signaturen sind online verfügbar und werden auf der PKI-Webseite Thüringen (www.signaturen.thueringen.de) bereitgestellt.

Auskünfte bei technischen Problemen werden im Rahmen des First-Level-Supports durch dasService-Center des TLRZ erteilt.

3.2 Abläufe im Verfahren fortgeschrittene Signatur

Das Verfahren zur Beantragung von fortgeschrittenen Signaturen soll zukünftig ebenfalls über die Registrierungsstelle Thüringen bearbeitet werden. Die Abläufe sind ausführlich in den folgenden zwei Dokumenten beschrieben:

Benutzerhandbuch Master-RA [DOI102] [6]

Benutzerhandbuch Sub-RA [DOI103] [7]

3.3 Die Signaturkarte

Die von der T-TeleSec ausgegebenen qualifizierten Zertifikate werden dem Inhaber auf der Signaturkarte übergeben. Diese Signaturkarte besitzt folgende Eigenschaften[1]:

- Die Schlüsselgenerierung erfolgt in einer gesicherten Umgebung des Trustcenters.
- Die Signaturkarte besitzt einen integrierten Kryptoprozessor, d.h. der private Schlüssel verlässt die Karte nie und alle Operationen mit diesem werden in der Karte durchgeführt.
- Die Signaturkarte trägt qualifizierte Zertifikate.
- Die Signaturkarte kann modular mit den entsprechend benötigten Zertifikaten ausgestattet werden.
- Sicheres PIN-Verfahren
- Die Karte ermöglicht das sog. Null-PIN Verfahren, d.h. die Karte trägt bei erstmaliger Auslieferung die Null-PIN als sicheres Merkmal ihrer Unbenutztheit.
- Sie kann in zwei Varianten für Einzel- oder Massensignatur eingesetzt werden.

3.3.1 Zertifikatsinhalt

Zugehörigkeit zu einer Organisation (hier Behörde)
Die Attribute “Organization” und “Organizational Unit” dienen zur Kennzeichnung der Zugehörigkeit zu einer Verwaltungseinheit, sofern diese direkt mit Hauptzertifikat aufgenommen werden soll.
Hinweis: Mit der Kennzeichnung der Zugehörigkeit zu einer Behörde im Hauptzertifikat wird dargestellt, dass der Zertifikatsinhaber ausschließlich im
Namen der Behörde handelt[2].

Qualifizierte Signaturzertifikate mit Anbieterakkreditierung
Die Unterscheidung von qualifizierten zu fortgeschrittenen Zertifikaten beruht darauf, dass sie auf die Erzeugung digitaler Signaturen eingeschränkt sind, ausschließlich auf einer Signaturkarte und nur für natürliche Personen ausgegeben werden können. Die Erstellung qualifizierter Signaturen muss auf einem zum Zeitpunkt ihrer Erstellung gültigen Zertifikat beruhen.
Weitere Merkmale qualifizierter Zertifikate und Signaturen sind:

- sichere geprüfte Produkte zur Generierung, sichere Signaturerstellungseinheit,
- (Signaturkarte), sichere Schlüsselerzeugung,
- Akkreditierung des Zertifizierungsdiensteanbieters durch die Bundesnetzagentur,
- Sie erfüllen in Verbindung mit den Formanpassungsgesetzen die rechtlichen Anforderungen an eine Unterschrift in gleicher Weise wie eine handschriftliche Unterschrift
- ausschließliche und eindeutige Zuordnung zum Signaturschlüsselinhaber,
- ermöglichen die Identifizierung des Signaturschlüsselinhabers,

[1] Als Signaturkarte kommt die NetKey 3.0-Karte der T-TeleSec zum Einsatz. Die qualifizierten Zertifikate besitzen aufgrund der unterstützten Schlüssellänge von 2048 Bit eine Gültigkeit von 3 Jahren.
[2] „Leistungsbeschreibung Public Key Service (PKS) für DOI [DOI120]“ [8]

- die nachträgliche Änderung der signierten Daten ist erkennbar.

Das Zertifikatsprofil der qualifizierten Signaturzertifikate entspricht dem ISIS-MTT[3] Standard.

Die folgende Tabelle erläutert die wesentlichen Zertifikatsinhalte an einem Beispiel.

Zertifikatsfeld	Bedeutung	Inhalt im qualifizierten Signaturzertifikat
Version	Zertifikatsstandard X.509v3	3 (0x2)
Issuer[4]	Aussteller des Zertifikates	C=DE, O=Deutsche Telekom AG, OU=Produktzentrum TeleSec/0.2.262.1.10.7.20=1, CN=TeleSec PKS SigG CA 13:PN
Validity	Gültigkeit des Zertifikates	
Not Before:	Beginn der Gültigkeit	Dec 6 07:12:17 2005 GMT
Not After:	Ende der Gültigkeit	Nov 6 07:12:17 2008 GMT
Subject	Namensbezeichner Zertifikatinhaber[5]	
C	Land	DE
O	Kennzeichnung der Zugehörigkeit zu einer Organisation	Freistaat Thüringen bzw. Name der Behörde, Einrichtung oder beteiligten Institution
OU	Kennzeichnung der Zugehörigkeit zu einem Ressort[6]	MI
CN	Name des Zertifikatinhabers	Mustermann, Hans
serialNumber	Seriennummer zur Gewährleistung der Eindeutigkeit	2
Erweiterungen des Zertifikates (Extensionen)		
Key Usage	Verwendungszweck des Schlüssels	„Non Repudiation“ (elektronische Signatur)
CRL Distribution Points	Verteilungspunkt(e) für Zertifikatssperrlisten	URI:ldap://pks-ldap.telesec.de/o=Deutsche Telekom AG,c=de URI:http://pks.telesec.de/telesec/servlet/download_crl
qcStatements	Kennzeichnung als qualifiziertes Signaturzertifikat	00.....F..
Subject Alternative Name	alternativer Inhabername	email:hans.mustermann@ressort.thueringen.de

Tabelle 2: Zertifikatsinhalte

Die Angabe im Attribut O (Kennzeichnung der Zugehörigkeit zu einer Verwaltungseinheit

[3] Die genaue Beschreibung des Profils ist zu finden unter http://www.telesec.de/downloads/PKS%20Zertifikatsprofil%202048%20qual%20Sign.pdf

[4] Der Issuer-CN (Name des Ausstellers) kann von den Angaben in der Tabelle abweichen, da durch den ZDA zur Signatur der Signaturzertifikate laufend aktuelle Zertifikate verwendet werden. Im Normalfall kann die als Zähler verwendete Ziffer „13“ im Issuer-CN weitergezählt worden sein. Derzeit (Stand Oktober 2008) werden vom ZDA Zertifikate mit den Ziffern „17“ bis „28“ im Issuer-CN verwendet.

[5] Ressortkürzel des Zertifikatinhabers

oder Organisation) des Zertifikates enthält daher immer der Bezeichnung der juristischen Person für die der Zertifikatsinhaber tätig werden soll. Diese lautet z.B. für Zertifikatinhaber der Landesverwaltung **„Freistaat Thüringen“**. Das Attribut OU enthält z.B.
die Kennzeichnung der Zugehörigkeit zu einer Behörde oder Einrichtung der Landesverwaltung, einem Amt, einer Kommune oder einer Abteilung/Außenstelle in der amtlich abgekürzten Schreibweise.
(Beispiel: TIM= Thüringer Innenministerium)

Attributzertifikate
Zusätzlich zum Namen des Zertifikatinhabers können weitere Eigenschaften des Inhabers in das qualifizierte Signaturzertifikat selbst oder ein dazu gehörendes Attributzertifikat aufgenommen werden. Mögliche Eigenschaften des Zertifikatinhabers können sein:

- Organisationszugehörigkeit des Inhabers,
- Einschränkungen des Verwendungszweckes des qualifizierten Signaturzertifikates,
- ggf. Beschränkung,
- die Berechtigung zur Ausübung bestimmter Tätigkeiten,
- die Vertretungsmacht für einen Dritten.

Zusätzliche Attribute sind projektabhängig bei der Antragsbearbeitung in dem Antrag explizit mit auszuweisen. Im Verfahren der Qualifizierten elektronischen Signatur in Thüringen sind dies z.B. die Attribute „Behörde“ und „Organisationseinheit“.
Werden einschränkende Eigenschaften in einem Attributzertifikat beschrieben, so ist im qualifizierten Signaturzertifikat ein Verweis auf die Existenz dieses Attributzertifikates enthalten. In diesem Fall muss das Attributzertifikat gleichzeitig mit dem Signaturzertifikat beantragt werden. Aufgrund des Verweises im Signaturzertifikat ist eine nachträgliche Beantragung eines beschränkenden Attributzertifikates nicht möglich.
Das Profil der Attributzertifikate entspricht dem ISIS-MTT Standard[7].

Fortgeschrittene Zertifikate
Im Gegensatz zu den qualifizierten Signaturzertifikaten mit Anbieterakkreditierung können fortgeschrittene Zertifikate eingesetzt werden für:

- die Erzeugung digitaler Signaturen,
- die Verschlüsselung von Daten,
- die Authentisierung von Zertifikatinhabern oder Serversystemen.

Kommen fortgeschrittene Signaturen zum Einsatz, erfüllen diese im Gegensatz zu qualifizierten jedoch nicht die rechtlichen Anforderungen an eine Unterschrift in gleicher Weise wie eine handschriftliche Unterschrift.
Sie besitzen eine hohe Flexibilität beim Einsatz in automatisierten Prozessen von Fachverfahren oder beim Einsatz fortgeschrittener Zertifikate für Personengruppen, da sie auch auf alternativen Trägern ausgegeben werden können.
Das Zertifikatsprofil der Fortgeschrittenen Zertifikate entspricht dem ISIS-MTT-Standard. Sie besitzen eine Gültigkeit von 3 Jahren. Serverzertifikate besitzen eine Gültigkeit von 3 Jahren.

4 Personelle und räumliche Ausstattung der RA

4.1 räumliche Ausstattung

Die Registrierungsstelle ist in den Räumlichkeiten des Thüringer Landesrechenzentrums in Erfurt untergebracht. Dabei erfolgt eine Trennung zwischen dem öffentlich zugänglichen

[7] Die genaue Beschreibung des Profils ist zu finden unter
http://www.telesec.de/downloads/PKS%20Zertifikatsprofil%202048%20qual%20Sign.pdf

Bereich zur persönlichen Identifikation der Antragsteller und der Antragsentgegennahme und der eigentlichen Antragsverwaltung in einem nicht öffentlich zugänglichen Bereich.

Die Identifikation der Antragsteller erfolgt in den Räumen der Poststelle des Thüringer Landesrechenzentrums in der 7. Etage (Raum 7.05). Hier besteht die Möglichkeit, den Antrag auf Teilnahme am Verfahren QeS persönlich abzugeben. Die notwendige Identifikation wird durch einen zertifizierten MA der Registrierungsstelle gemäß der Vorgaben des ZDA (siehe Kapitel 9.3: Merkblatt zur Identifizierung durch RA-Mitarbeiter (090915_Checkliste_fuer_RegMA.pdf)) durchgeführt. Bei Bedarf können weitere Mitarbeiter der Registrierungsstelle hinzu gezogen werden.

Die Antragsbearbeitung erfolgt im nicht öffentlich zugänglichen Bereich des TLRZ (8. Etage). Der Zugriffsschutz auf die vertraulichen Antragsdaten ist gewährleistet. Konkrete Festlegungen hinsichtlich des Datenschutzes in der Registrierungsstelle Thüringen werden in Kapitel 6.2 dargestellt.

4.2 Erreichbarkeit

Die Registrierungsstelle Thüringen ist unter folgender postalischen Adresse erreichbar:

Thüringer Landesrechenzentrum
RA Thüringen
Postfach 80 03 05
99029 Erfurt

Weiterhin stehen die folgenden Kommunikationswege zu Verfügung:

Tel.: +49 361 3784 960

Fax: +49 361 3784 9360

E-Mail: TLRZPKI@tlrz.thueringen.de

Die persönliche Antragsstellung und Identifikation wird im Gebäude Ludwig-Erhard-Ring 8, 99099 Erfurt, durchgeführt.

Sie ist zu folgenden Zeiten möglich:

Di: 09:00 bis 12:00 Uhr

Do: 13:00 bis 15:30 Uhr,

oder nach telefonischer Vereinbarung.

Für telefonische Anfragen an die Registrierungsstelle Thüringen sollte die Kernzeitregelung des Thüringer Landesrechenzentrums beachtet werden. Bei Nichterreichbarkeit werden die Anrufe umgeleitet.

Anfragen hinsichtlich der Anwenderbetreuung in PKI-Fachverfahren sowie Problem- und Störungsmeldungen sind gem. Kapitel 8 unter den festgelegten Kommunikationswegen an die RA weiterzuleiten.

4.3 Antragsbearbeitungs- und Verwaltungssoftware

Für die Verwaltung der Antragsdaten und der ausgestellten Zertifikate wurde im TLRZ eine eigene Verwaltungssoftware erstellt.

Diese Software und die konkrete Antragsbearbeitung innerhalb der Software ist ergänzend zu diesem Organisationshandbuch im Dokument „Benutzerhandbuch SigVDB“ (siehe Kapitel 9.3: Benutzerhandbuch SigVDB (Benutzerhandbuch_SigVDB.pdf)) beschrieben.

4.4 Personelle Ausstattung

Eine Registrierungsstelle muss zur Abdeckung eines unterbrechungsfreien Betriebes mindestens aus den folgenden Mitarbeitern (Rollen) bestehen:

- Leiter der Registrierungsstelle
- Stellvertreter des Leiters
- Mitarbeiter Registrierungsstelle

Sämtliche Mitarbeiter müssen vor Aufnahme ihrer Tätigkeit durch den Zertifizierungsdienste-anbieter (ZDA) in einem eintägigen Workshop geschult werden, eine Einweisung in die zur Verwaltung der Anträge und Zertifikate verwendete Software (siehe 4.3) bekommen.

Die RA einer Einrichtung muss immer mit mehreren Personen besetzt sein, damit auch im Urlaubs- oder Krankheitsfall Anträge ohne Verzögerung bearbeitet werden können.

Alle RA Mitarbeiter müssen sich verpflichten, ihre Aufgaben entsprechend der Policy der PKI des Landes Thüringen durchzuführen, welche im Prozess-Handbuch (Anlage 2 zum Vertrag über die Registrierungstätigkeit, siehe 9.3, Dokument [13] sowie im Merkblatt zur Identifizierung durch RA-Mitarbeiter (090915_Checkliste_fuer_RegMA.pdf)) beschrieben ist.

4.4.1 Leiter der Registrierungsstelle

Der Leiter der Registrierungsstelle muss folgende Aufgaben / Zuständigkeiten ausfüllen:

- Zuständig für die Einrichtung und den Betrieb der Registrierungsstelle, ist berechtigt zur Veranlassung der Fremdsperrung von Teilnehmerzertifikaten
- Übermittlung der entsprechenden Nachweise der Fachkunde und Zuverlässigkeit an den ZDA
- Einsatz, Steuerung und Aufsicht der zugehörigen Registrierungsmitarbeiter
- Sicherstellung der gesetzlichen Anforderungen im Betrieb der Registrierungsstelle, insbesondere die Erhaltung und der Nachweis der Zuverlässigkeit und der Fachkunde der Mitarbeiter
- Umsetzung der Vorgaben des ZDA gegenüber den Registrierungsmitarbeitern – dies betrifft die Wahrnehmung von Aufgaben der Zertifizierungstätigkeit als Dritter im Sinne des Signaturgesetzes und der Signaturverordnung
- Ansprechpartner für qualifizierte oder fortgeschrittene Signaturen für die Träger der Fachverfahren und Teilnehmer der PKI Thüringen
- Fremdsperrung von Zertifikaten
- Ist Zuständig für die Erstellung des Notfallkonzeptes

4.4.2 Stellv. Leiter der Registrierungsstelle

Dieser nimmt stellvertretend die Aufgaben des Leiters der Registrierungsstelle Thüringen wahr.

Der stellvertretende Leider der Registrierungsstelle sollte fachlich in der Lage sein, auch die Aufgaben des Registrierungsstellen-Mitarbeiters bei dessen Abwesenheit übernehmen zu können.

4.4.3 Mitarbeiter Registrierungsstelle

Der Mitarbeiter der Registrierungsstelle muss folgende Aufgaben / Zuständigkeiten ausfüllen können:

- Zuständig für die Prüfung der Teilnahmevoraussetzungen, die Identifizierung, Authentifizierung und Registrierung der Teilnehmer
- Antragserstellung, Antragsannahme und – weiterleitung, Antragsüberprüfung
- Unterrichtung des Antragstellers gemäß § 6 SigG i.V.m. den Inhalten in § 6 SigV
- Identifizierung gemäß § 5 SigG i.V.m. § 3 SigV
- Ausgabe der Sicheren Signaturerstellungseinheit (kurz SSEE) (Signaturkarte)
- Aufspielen (Ausgabe) des qualifizierten Zertifikates auf eine geeignete Chipkarte (Signaturkarte)
- Aufspielen (Ausgabe) von qualifizierten Attributzertifikaten auf Datenträger
- Aufspielen (Ausgabe) weiterer Zertifikate (z.B. Verschlüsselung) auf die Signaturkarte
- Übermittlung der Antragsdaten an den ZDA (postalisch) und der Dokumente an die Zentrale Registrierungsstelle.
- Ansprechpartner für die Teilnehmer; Vorgangsabwicklung mit angrenzenden Stellen (Vermittlung Kundenkontakt zum ZDA)
- Zuständig für die Veranlassung der Zertifikatssperrung
- Zuständig für Sub-Registrierungsstellen (nur für fortgeschrittene Zertifikate) und Teilnehmerzertifikate
- Zuständig für die Vergabe von Gruppennamen und der Namensbereiche der Sub-Domänen innerhalb der PKI Thüringen
- Manuelles Erstellen von Sperrlisten
- Sichere Verwahrung der Authentisierungsschlüssel der Master- und Sub- Domänen
- Protokollierung und Nachweisführung in den Abläufen und Prozessen
- fachlicher Ansprechpartner für qualifizierte oder fortgeschrittene Signaturen für die Träger der Fachverfahren und Teilnehmer der PKI Thüringen

4.5 Rollen der PKI Thüringen

Eine Rolle stellt innerhalb der PKI Thüringen eine Bündelung inhaltlich oder organisatorisch zusammengehörender Aufgaben dar, die von einer Person oder einer Gruppe von Personen (Stellvertretung) bearbeitet werden.

Dem Leiter der PKI Thüringen und den Mitarbeitern der Registrierungsstelle werden unter der Beachtung notwendiger Funktionstrennungen bei Unverträglichkeit mehrere Rollen übertragen. Ausgehend von den beschriebenen Funktionen der Rollen und unter Zugrundelegung des Verwaltungsaufbaus, in den die PKI Thüringen eingebettet ist, werden diese in „interne“ und „externe“ Rollen getrennt.

Eine interne Rolle wird für die Registrierungsstelle der PKI Thüringen besetzt, wobei zwischen internen operativen (Tabelle 1 - Intern begleitende Rollen der PKI Thüringen) und externen begleitenden (Tabelle 2 - Extern begleitende Rollen der PKI Thüringen) Rollen unterschieden wird. Die internen operativen Rollen sind direkt und dauerhaft in die Abläufe

der Registrierungsstellen eingebunden. Die externen begleitenden Rollen sind nicht dauerhaft in die Abläufe der Registrierungsstelle eingebunden. Sie sind organisatorisch in der Zuständigen Behörde tätig und werden bei Bedarf von der Registrierungsstelle der PKI Thüringen als Zweitfunktion in Anspruch genommen.

Die folgende Tabelle stellt die intern begleitenden Rollen innerhalb der RA Thüringen dar:

Funktion	**Bündelung der Rollen**	**Aufgaben**
Registrierungsmitarbeiter	• Personalisierer • Registrierer • Sperrberechtigter • Namensvergabe • Organisatorischer Ansprechpartner • Trainer	• Zuständig für die Prüfung der Teilnahmevoraussetzungen, die Identifizierung, Authentifizierung und Registrierung der Teilnehmer • Antragserstellung, Antragsannahme und –weiterleitung, Antragsüberprüfung • Unterrichtung des Antragstellers gemäß § 6 SigG i.V.m. den Inhalten in § 6 SigV • Identifizierung gemäß § 5 SigG i.V.m. § 3 SigV • Ausgabe der Sicheren Signaturerstellungseinheit (kurz SSEE) (Signaturkarte) • Aufspielen (Ausgabe) des qualifizierten Zertifikates auf eine geeignete Chipkarte (Signaturkarte) • Aufspielen (Ausgabe) von qualifizierten Attributzertifikaten auf Datenträger • Aufspielen (Ausgabe) weiterer Zertifikate (z.B. Verschlüsselung) auf die Signaturkarte • Übermittlung der Antragsdaten an den ZDA (elektronisch bzw. postalisch) und der Dokumente an die Zentrale Registrierungsstelle. • Ansprechpartner für die Teilnehmer; Vorgangsabwicklung mit angrenzenden Stellen (Vermittlung Kundenkontakt zum ZDA) • Zuständig für die Veranlassung der Zertifikatssperrung Sub-Registrierungsstellen und Teilnehmerzertifikate • Zuständig für die Vergabe von Pseudonymen, Gruppennamen und der Namensbereiche der Sub-Domänen innerhalb der PKI Thüringen

		• Manuelles erstellen von Sperrlisten • Sichere Verwahrung der Authentisierungsschlüssel der Master- und Sub-Domänen • Protokollierung und Nachweisführung in den Abläufen und Prozessen • Ansprechpartner für die Träger der Fachverfahren und Teilnehmer der PKI Thüringen • Schulung der Registrierungsmitarbeiter
Leiter der RA Thüringen	• Leiter der PKI Thüringen • Organisatorischer Ansprechpartner • Autorisierte Person • Beauftragter für das Notfallmanagement • Trainer	• Zuständig für die Einrichtung, den Betrieb und die Einstellung des Betriebes der Registrierungsstelle, berechtigt zur Veranlassung der Fremdsperrung vor Teilnehmerzertifikaten • Übermittlung der entsprechenden Nachweise der Fachkunde und Zuverlässigkeit an den ZDA • Einsatz, Steuerung und Aufsicht der zugehörigen Registrierungsmitarbeiter • Sicherstellung der gesetzlichen Anforderungen im Betrieb der Registrierungsstelle, insbesondere die Erhaltung und der Nachweis der Zuverlässigkeit und der Fachkunde der Mitarbeiter • Umsetzung der Vorgaben des ZDA an die Registrierungsmitarbeiter – dies betrifft die die Wahrnehmung von Aufgaben der Zertifizierungstätigkeit als Dritter im Sinne des Signaturgesetzes und der Signaturverordnung • Ansprechpartner für die Träger der Fachverfahren und Teilnehmer der PKI Thüringen • Fremdsperrung von Zertifikaten • Ist Zuständig für die Erstellung des Notfallkonzeptes
Stellv. Leiter der RA Thüringen		Nimmt stellvertretend die Aufgaben des Leiters der PKI Thüringen wahr. Der stellv. Leiter der RA übernimmt die Rolle des Mitarbeiters der Registrierungsstelle bei dessen Abwesenheit.

Tabelle 3: Intern begleitende Rollen der PKI Thüringen

Die folgende Tabelle stellt die extern begleitenden Rollen innerhalb der RA Thüringen dar:

Funktion	**Bündelung der Rollen**	**Aufgaben**
IT-Sicherheitsbeauftragter der Zuständigen Behörde [8]*	IT-Sicherheitsbeauftragter	Der IT-Sicherheitsbeauftragte ist gesamtverantwortlich für die Sicherheit aller Registrierungsstellen. Dies beinhaltet die Steuerung der Überwachung der Anwendung des Sicherheitsprozesses in der PKI Thüringen.
Mitarbeiter Funktionsdienste der Zuständigen Behörde	Beauftragter für die Eigenverwaltung	Der Beauftragte für die Eigenverwaltung ist zuständig für die Eigenverwaltung aller Registrierungsstellen; u.a. die Beschaffung benötigter Hard- und Software, die Raumzuweisung und die Personalbewirtschaftung.
Mitarbeiter des Sicherheitsteams der Zuständigen Behörde [9]	Revisor	Der Revisor ist zuständig für die Umsetzung und Einhaltung des Sicherheitskonzeptes der PKI Thüringen.
Datenschutzbeauftragter der Zuständigen Behörde	Datenschutzbeauftragter	Der Datenschutzbeauftragte ist zuständig für die Kontrolle der Einhaltung der Bestimmungen des Datenschutzes in der PKI Thüringen. Er ist für alle Registrierungsstellen der PKI Thüringen gesamtverantwortlich.
Mitarbeiter der Funktionsdienste der Zuständigen Behörde	Beauftragter für den technischen Dienst	Der Beauftragte für den technischen Dienst ist zuständig für Aufbau, Pflege und Instandhaltung der technischen und baulichen Infrastruktur der PKI Thüringen. Hierzu zählt insbesondere die Instandhaltung der Arbeitsräume der PKI Thüringen.
• Administrator AP • Co-Administrator AP • Administrator Netzwerk, E-Mail Services • Co-Administrator Netzwerk, E-Mail Services • Administrator Protokollierserver, Web-Services • Co-Administrator Protokollierserver, Web-Services	Administrator	Die Administratoren sind zuständig für die Einrichtung der Betreuung der Hard- und Software der Stellen. Dabei werden die Aufgaben der Rollen entsprechend der Zuständigkeit der Bereiche der Zuständigen Behörde wahrgenommen.

Tabelle 4: Extern begleitende Rollen der PKI Thüringen

[8] diese Rolle ist im Rahmen des ISMS zur Zeit nicht in jedem Fall besetzt
[9] diese Rolle ist im Rahmen des ISMS zur Zeit nicht in jedem Fall besetzt

5 IT-Sicherheit

Das Thema der IT-Sicherheit wird in dem begleitenden Sicherheitskonzept der Registrierungsstelle Thüringen (siehe Tabelle 5: Dokumente der Registrierungsstelle Thüringen) dargestellt.

6 Datenschutz

6.1 Allgemeine Festlegungen

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Thüringer Landesrechenzentrum erfolgt unter Beachtung der gesetzlichen Vorgaben aus den Bestimmungen des Gesetzes zum Schutz der personenbezogenen Daten der Bürger (ThürDSG) Anwendung.
Aus den vertraglichen Vereinbarungen (DOI Einzelvertrag zwischen dem Freistaat Thüringenund T-Systems) mit dem ZDA ergibt sich der Umfang der zu erhebenden und zu verarbeitenden personenbezogenen Daten und der dazu erforderlichen technischen und organisatorischen Maßnahmen (§§ 19, 20 ThürDSG).
Die in den Paragrafen 19 und 20 festgelegten Regelungen zum Datenschutz und zur IT-Sicherheit dienen gleichzeitig der Umsetzung der erforderlichen technischen und organisatorischen Maßnahmen, die sich bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten aus diesen Paragraphen ableiten.
Personenbezogene Daten der Antragsteller und Zertifikatinhaber werden demnach in erforderlichem Umfang durch die Mitarbeiter/Innen des ZDA erhoben und gespeichert.
Das Thüringer Datenschutzgesetz findet sinngemäße Anwendung.
Bei den erhobenen und verarbeiteten Daten des Inhabers eines qualifizierten Zertifikates handelt es sich um:

- Name, Vorname des Antragstellers/Antragstellerin ggf. Geburtsname, Titel, Initialen[10]
- E-Mail Adresse des Antragstellers/Antragstellerin[11]
- Name der Organisation und ggf. Organisationseinheit[12]
- Personalausweis-/Reisepassnummer (oder Dienstausweis bei fortgeschrittenen Zertifikaten)
- Gültigkeit des Personalausweises/Reisepasses
- Staatsangehörigkeit
- Wohnanschrift des Antragstellers

Bei den erhobenen und verarbeiteten Daten des Inhabers eines fortgeschrittenen Zertifikates handelt es sich um:

- Name, Vorname des Antragstellers/Antragstellerin ggf. Geburtsname, Initialen[13]
- E-Mail Adresse des Antragstellers/Antragstellerin[14]
- Name der Organisation und ggf. Organisationseinheit[15]
- Personalausweis- oder Dienstausweisnummer

[10] werden in das Zertifikat des Antragstellers übernommen
[11] werden in das Zertifikat des Antragstellers übernommen
[12] werden in das Zertifikat des Antragstellers übernommen
[13] werden in das Zertifikat des Antragstellers übernommen
[14] werden in das Zertifikat des Antragstellers übernommen
[15] werden in das Zertifikat des Antragstellers übernommen

Diese Daten werden elektronisch durch den Teilnehmer sowie in Papierform durch das PostIdent Verfahren der Registrierungsstelle, das BehördenIdent-Verfahren der siegelführenden Stelle und von diesen weiter an den ZDA übermittelt.

6.2 spezielle Festlegungen zum Datenschutz

6.2.1 Umgang mit Papierunterlagen

6.2.1.1 Aufbewahrung der Antragsunterlagen (Kopien)

Die dauerhafte Ablage der Antragsunterlagen entsprechend der Gültigkeit der beantragten Zertifikate zum Zwecke der buchhalterischen Abrechnung und Revision erfolgt in einem gesicherten Schrank innerhalb der Registrierungsstelle. Dabei handelt es sich um die Antragsoriginale bei fortgeschrittenen Zertifikaten und die Teilnahmeerklärungen bei qualifizierten Zertifikaten.

Die Antragsunterlagen dürfen nur zur unmittelbaren Antragsbearbeitung auf dem Arbeitsplatz des Registrierungsmitarbeiters abgelegt werden. Verlässt der Mitarbeiter seinen Arbeitsplatz sind diese in jedem Fall wieder in dem gesicherten Büroschrank zu verschließen.

6.2.1.2 Ausdruck von Listen/Statistiken

Für den Ausdruck von Listen oder Statistiken, welche personengebundene Daten der Antragsteller enthalten, steht der Registrierungsstelle ein Drucker mit PIN-geschützer Ausgabe zur Verfügung.

Beim Ausdruck verwendet der RA-Mitarbeiter die Ausgabeoption „Druck vertraulich“. In dieser ist die Angabe eines Benutzernamens und einer selbst definierten PIN möglich, ohne die der Druckauftrag nicht abgerufen werden kann. Anschließend wird der Ausdruck durch den Mitarbeiter persönlich am Drucker unter Eingabe der PIN abgerufen und der Ausdruck abgeholt.

6.2.1.3 Einscannen von Unterlagen

Ist es erforderlich, dass Antragsdaten eingescannt werden müssen, sind die vorhandenen Multifunktionsgeräte zu nutzen. Dabei stellt der RA-Mitarbeiter sicher, dass die Scandatei an das interne Mail-Postfach der Registrierungsstelle (tlrzpki@tlrz.thueringen.de) erfolgt. Alternativ kann der Mailversand auch an seine persönliche Mailadresse erfolgen.

6.2.1.4 Sichtprüfung der Antragsunterlagen

Der MA der Registrierungsstelle prüft den Auftrag und ggf. die weiteren Formulare und Dokumente nach sichtbaren Fälschungsmerkmalen. Er prüft insbesondere, ob Streichungen oder Veränderungen enthalten sind.

Ist nicht mehr nachzuvollziehen, ob eine Manipulation vorgenommen wurde, wird der Auftrag abgelehnt und der Auftragsteller ist zu informieren und zur erneuten Beauftragung in der Registrierungsstelle aufzufordern.

6.2.1.5 Prüfung der Ausweisdokumente

Die Ausweisdokumente werden durch den Registrierungsmitarbeiter gemäß der Vorgaben im Prozesshandbuch des ZDA (siehe 9.3 Dokument [13]) und der Sicherheitsmerkmale im

Merkblatt zur Identifizierung durch RA-Mitarbeiter (090915_Checkliste_fuer_RegMA.pdf) sowie (für den neuen Personalausweis) im Dokument Der neue Personalausweis - Sicherheitsmerkmale (Flyer_Bundesdruckerei_Sicherheitsmerkmale_nPA.pdf) (siehe 9.3, Dokument [14]) überprüft.

Aus dem Ausweisdokument werden die Daten in das Identifikationspapier (siehe Tabelle 6, Formular Identitätsfeststellung PKI.pdf) übernommen, welches anschließend vom Antragsteller im Beisein des RA-Mitarbeiters zu unterschreiben ist.

Im Rahmen der Antragsbearbeitung erfolgt noch eine separate Prüfung des Identifikationspapiers. Der RA-Mitarbeiter vergleicht das Identifikationspapier mit den Daten im Antragsformular.

6.2.2 Umgang mit elektronischen Antragsdaten

Die elektronischen Antragsdaten werden in der eigens für die Registrierungsstelle entwickelten Anwendung SigVDB in einer Datenbank abgelegt. Sie sind innerhalb des TLRZ-internen Netzwerks von den Arbeitsplätzen der Registrierungsmitarbeiter aufrufbar. Der Zugriff auf die Antragsdatenverwaltung ist nur über einen festgelegten Benutzernamen und ein mindestens 8-stelliges Passwort mit Buchstaben und Zahlen möglich.

Der Registrierungsstellen-Mitarbeiter hat sicherzustellen, dass er sich unmittelbar nach Aufgabenerfüllung wieder von dieser Anwendung abmeldet. Ohne Abmeldung wird die Verbindung zur Anwendung nach 30 Minuten automatisch getrennt.

Hinsichtlich der Vergabe sicherer Passwörter und der Sicherstellung des Zugriffsschutzes zum Arbeitsplatz-PC gelten die Festlegungen des TLRZ (Dienstanweisung Datenschutz und Datensicherheit, siehe 9.3 Dokument [15]).

7 Dokumente und Formulare

Die im Freistaat Thüringen für Beantragung und Ausgabe der Signaturkarte notwendigen Dokumente und Formulare werden in der Verantwortung der Registrierungsstelle Thüringen (TLRZ) erstellt und gepflegt.

Bei diesen Dokumenten ist zu unterscheiden zwischen
a) den Dokumenten des ZDA, aus denen sich die konkreten Anforderungen zur Umsetzung der Verfahrensabläufe ergeben und
b) den Dokumenten der Zuständigen Behörde, die die organisatorischen Prozesse der Antragsbearbeitung regeln.

Das Organisationshandbuch QeS des Freistaats Thüringen regelt die Bekanntmachung, Veröffentlichung und Pflege der Dokumente und Formulare.

Die Regelung der organisatorischen Abläufe innerhalb der beantragenden Behörden sind nicht Gegenstand des Projektes „Registrierungsstelle Thüringen“ und werden hier nicht näher betrachtet.

Dokument	Inhalt	Benutzer	Bereitstellung
Organisations-handbuch	Beschreibung der Ablauf- und Aufbauorganisation der PKI Thüringen	Mitarbeiter der RA	Zuständige Behörde

Betriebshand-buch	Arbeitsanweisungen des ZDA für die RM	Mitarbeiter der RA	Zuständige Behörde
Sicherheits-konzept	IT-Sicherheitsteam der Zuständigen Behörde	IT-Sicherheitsteam der Zuständigen Behörde	Zuständige Behörde
Teilnehmer-handbuch	Informationen und Hinweise für Zertifikatinhaber zur Beantragung von Zertifikaten	Zertifikatinhaber	Webseite http://www.signaturen.thueringen.de
Benutzerhandbuch SigVDB	Beschreibung der Verwaltungssoftware für die Zertifikatsverwaltung in der RA	Mitarbeiter der RA	Zuständige Behörde

Tabelle 5: Dokumente der Registrierungsstelle Thüringen

Formular	Inhalt	Benutzer	Bereitstellung
Teilnahmeerklärung zur QeS	Persönliche Angaben des Antragstellers Beantragung des Antragstellers Teilnahmebestätigung der beantragenden Behörde: • Verfahren / Fachanwendung • Dienststelle Freischaltcode	Teilnehmer	Webseite http://www.signaturen.thueringen.de
Teilnahmeantrag beim ZDA	Persönliche Angaben des Antragstellers Angaben zur Behörde: • Verfahren / Fachanwendung • Dienststelle Bestätigung der RA Freischaltcode	Teilnehmer	Website des ZDA https://www.telesec.de/cgi-bin/pksauftrag_doithms.pl (Link wird in Mail an den Teilnehmer übermittelt)
Bestätigung der Identifizierung „Formular Identitätsfeststellung PKI.pdf“	Angaben zum Ausweisdokument (Nummer, Gültigkeitsdatum), Unterschrift des Antragsstellers (bei der Identifizierung im Beisein des RA-MA zu leisten), Unterschrift des RA-Mitarbeiters	Mitarbeiter RA	Dokumentenablage der RA Thüringen
Antragsformular für neue Projekte	Angaben zum Projekt, zur Anzahl benötigter Zertifikate, zur zuständigen Behörde und zur Rechnungslegungsstelle	Thüringer Behörden und Einrichtungen	Webseite http://www.signaturen.thueringen.de
…			

Tabelle 6: Formulare der Registrierungsstelle Thüringen

8 Support und Eskalation

Vorklärung und Kanalisierung der Supportanfragen erfolgen durch das Service Center des Thüringer Landesrechenzentrums (TLRZ).

Gewährleisteter Support:

- für Antragsteller und Zertifikatsinhaber des Freistaats Thüringen das Verfahren QeS zu Fragen der Antragsübermittlung an den ZDA, und zum Freischaltvorgang
- zum PostIdent Verfahren,
- zum BehördenIdent Verfahren und
- für die Verfahrensverantwortlichen Stellen QeS zu Fragen der Prozessgestaltung bei Zertifikatsbeantragung und –ausgabe

und unterstützend (und soweit dies nicht aufgrund der speziellen Regelungen des Freistaats Thüringen durch das Service Center des Thüringer Landesrechenzentrums bzw. durch die Registrierungsmitarbeiter des ZDA erfolgt) zum Service Center des TLRZ bei

- Übermittlung und Ausgabe der Signaturkarten für fortgeschrittene Zertifikate an die Zertifikatsinhaber im Freistaat Thüringen

Der ZDA gewährleistet den Support hinsichtlich Antragsbearbeitung, Kartenproduktion und -versand.

Detaillierte Informationen zum Support des ZDA beinhaltet die „Leistungsbeschreibung DOI-CA [DOI100]“ (siehe Kapitel 9.3, Dokument [10]).

Kontakt ZDA T-TeleSec:

ITN: http://www.telesec.de/pks/index.html

Kontakt Support Center TLRZ:

Telefon: +49 361 37 99 999

E-Mail: support@servicecenter.thueringen.de

ITN: http://www.signaturen.thueringen.de

9 Anhang

9.1 Beispiele zur Erläuterung der Prozessabbildungen als EPK

Nachfolgend werden anhand von zwei Beispielprozessen die in diesem Handbuch verwendeten Prozessdarstellungen als Ereignisgesteuerte Prozessketten (EPK) dargestellt, um Begriffe und Funktionen zu erläutern.

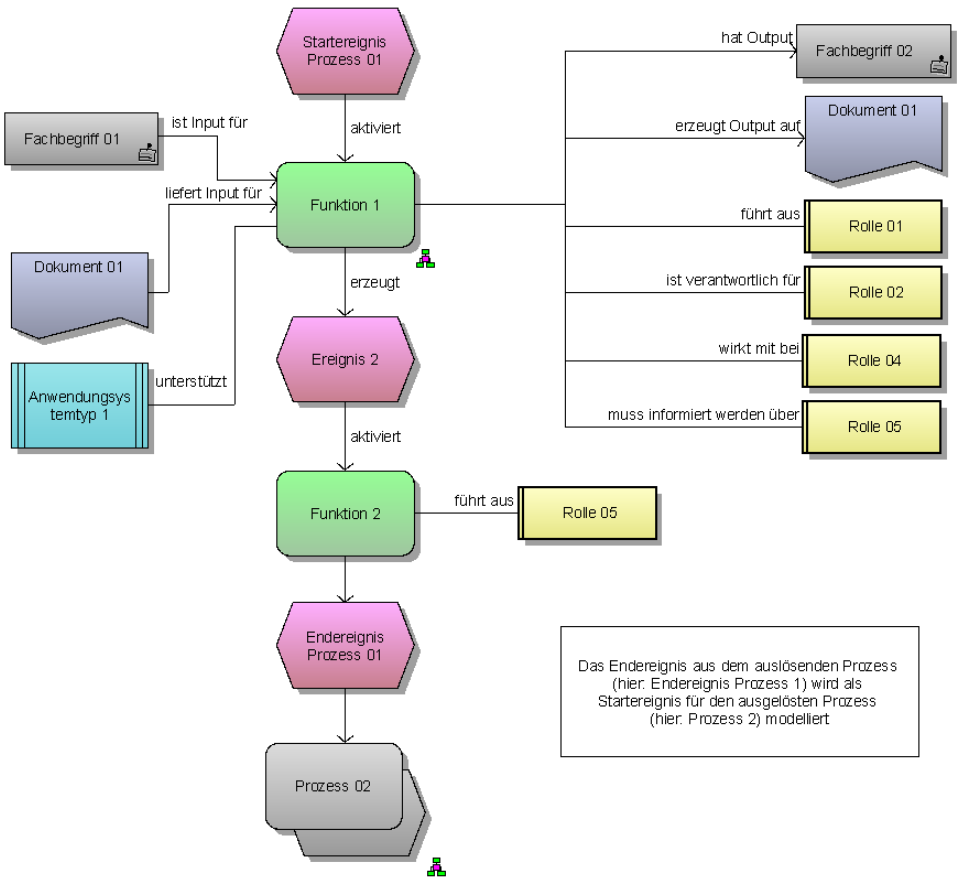


Abbildung 10: Beispiel-EPK "Prozess 01“

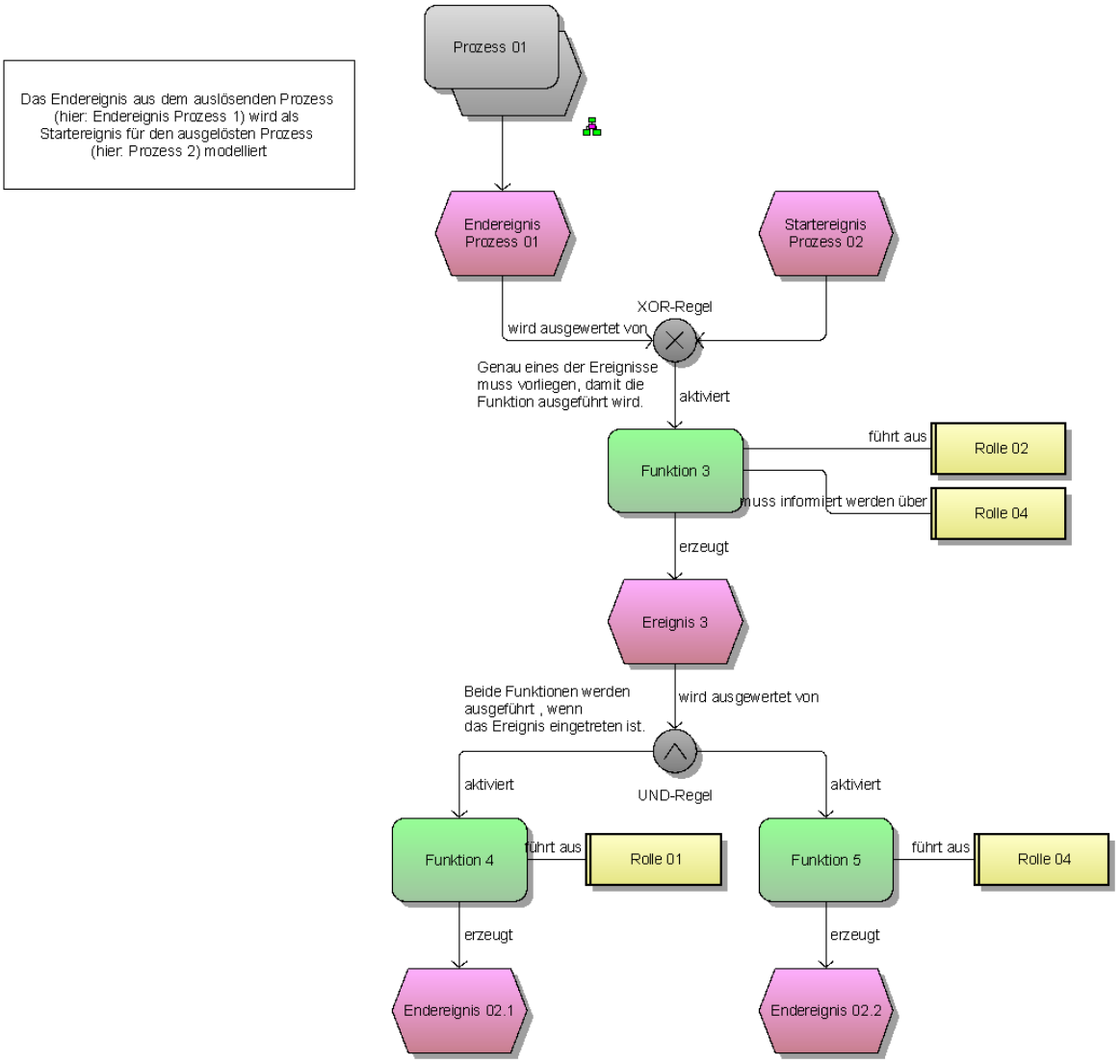


Abbildung 11: Beispiel-EPK "Prozess 02“

9.2 Abkürzungsverzeichnis

Abkürzung	Erklärung
BuE	Behörden und Einrichtungen
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority - Zertifizierungsinstanz
DOI	Deutschland-Online Infrastruktur
EPK	Ereignisgesteuerte Prozessketten
IPSec VPN	Internet Protocol Security Virtual Private Network
MPLS	Multiprotocol Label Switching ermöglicht die verbindungsorientierte Übertragung von Datenpaketen in einem verbindungslosen Netz entlang einem zuvor aufgebauten („signalisierten“) Pfad
PIN	Personal Identification Number, Persönliche Indentifikationsnummer.

	Ein mehrstelliger Zahlen- oder Zeichencode, der zur Authentifizierung verwendet wird. Schützt die Signaturkarte vor unberechtigtem Zugriff, da sie nur im Besitz des Zertifikatsinhabers ist (Ausnahme Gruppenzertifikate)
PKI	Public Key Infrastructure, Technische Einrichtungen und organisatorische Prozesse für die Erzeugung, Verteilung, Verwaltung, Nutzung und Sperrung von öffentlichen Schlüsseln eines asymmetrischen Kryptographieverfahrens
PKS	Public Key Service ein Service im Sinne des SigG von 1997 der T-Systems International GmbH
PUK	Personal Unblocking Key-Nummer (umgangssprachlich auch Super-PIN oder Master-PIN genannt) dient dem Entsperren, z. B. einer SIM-Karte, falls z. B. der PIN-Code mehrfach (üblicherweise dreimal) falsch eingegeben wurde
QeS	Qualifizierte elektronische Signatur
RA	Registration Authority – Registrierungsstelle
RS	Registrierungsstelle der PKI Thüringen
ZDA	Zertifizierungsdiensteanbieter. Dienstleister, der die Zertifikate generiert. Stellt Verzeichnis- und Statusdienste bereit.
MA	Mitarbeiter
DS	Datensatz

Tabelle 7: Abkürzungsverzeichnis

9.3 Referenzierte Dokumente

Dokument	Version/Datum	Referenz
Rahmenvertrag DOI (RV_DOITeil1.pdf - RV_DOITeil4.pdf)	05.03.2009	[1]
Anlage 1 zum Rahmenvertrag Einzelvertrag 2 zwischen dem Freistaat Thüringen (TFM) und T-Systems Enterprise Service GmbH (DOI Anlage 1 zum Rahmenvertrag Oktober 2009.pdf)	12.10.2009	[2]
Vereinbarung zwischen dem Land Sachsen-Anhalt und dem Freistaat Thüringen über die Verwaltung qualifizierter Zertifikate mit Anbieterakkreditierung (Vereinbarung Sachsen-Anhalt-Thüringen-QES-September 2009.pdf)	14.10.2009	[3]
Leistungskatalog DOI-Netz (DOI Leistungskatalog.pdf)	07.10.2009	[4]
Change Request DOI_11 (Einzelvertrag zur Nutzung von DOI Diensten Aktualisierte Service Kataloge) (CR_DOI_11_unterzeichnet.pdf)	29.09.2010	[5]
Benutzerhandbuch Master-RA [DOI102] (DOI102 Handbuch Master-RA v10.pdf)	30.09.2009	[6]
Benutzerhandbuch Sub-RA [DOI103] (DOI103 Handbuch Sub-RA v10.pdf)	30.09.2009	[7]
Leistungsbeschreibung Public Key Service (PKS) für DOI [DOI120] (DOI120 Leistungsbeschreibung PKS für	18.11.2009	[8]

DOI V10.pdf)		
Handbuch für Qualifizierte Zertifikate [DOI121] (DOI121 Handbuch Qualifizierte Zertifikate V10 031109.pdf)	03.11.2009	[9]
Leistungsbeschreibung DOI-CA [DOI100] (DOI100 Leistungsbeschreibung DOI-CA V1.01.pdf)	17.08.2010	[10]
Merkblatt zur Identifizierung durch RA-Mitarbeiter (090915_Checkliste_fuer_RegMA.pdf)		[11]
Benutzerhandbuch SigVDB (Benutzerhandbuch_SigVDB.pdf)		[12]
Prozesshandbuch des ZDA TeleSec (Anlage 2 zum Vertrag über die Registrierungstätigkeit) (Anlage 2 PKS RTV 2008.11.06.pdf)		[13]
Der neue Personalausweis - Sicherheitsmerkmale (Flyer_Bundesdruckerei_Sicherheitsmerkmale_nPA.pdf)	31.10.2010	[14]
DA Datenschutz und Datensicherheit des TLRZ	01.09.2002	[15]

Tabelle 8: Referenzierte Dokumente

9.4 Abbildungsverzeichnis

9.5 Tabellenverzeichnis