A-Trust Gesellschaft für Sicherheitssysteme im elektronischen
Datenverkehr GmbH.
Landstraßer Hauptstraße 5
Tel.: +43 (1) 713 21 51 – 0
Fax: +43 (1) 713 21 51 – 350
DVR: 1065181 – FN: 195738a
office@a-trust.at
www.a-trust.at

a.trust

Betriebskonzept Registrierungsstellen

Version: 1.0.2

Datum: 25.10.2004

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

1 Einleitung

1.1 Zweck des Dokuments

Dieses Dokument richtet sich an die Registrierungsstellen der a.trust und beschreibt den Ablauf der Zertifikatsausstellung für Maestrokarten und a.sign Premium Bestellkarten - beide mit ACOS-Chip - sowie auch die Ausstattung derselben mit Bürgerkartenfunktionalität.

1.2 Begriffsbestimmung Signatur- und Bürgerkarte

Ab Dezember 2004 kann jeder Inhaber einer Maestrokarte diese gegen eine Karte austauschen, die über Signatur- und Bürgerkartenfunktion verfügt. Diese Karte wird für die gewohnten Funktionen verwendbar sein und zusätzlich die erforderlichen Daten (insb. Signaturschlüssel) sowie den nötigen Speicherplatz enthalten, um als Signatur- und auch als Bürgerkarte dienen zu können.

Gleichzeitig werden für bestimmte Projekte bereits ab Mitte November 2004 a.sign Premium Bestellkarten mit ACOS-Chip angeboten. Diese werden parallel zu jenen mit Starcos-Chip ausgegeben, welche noch weiterhin für eine befristete Zeitspanne auf spezielle Anforderung ausgestellt werden können.

Eine Bürgerkarte ist eine Signaturkarte (a.sign Premium) mit einem qualifizierten Signaturzertifikat für sichere Signaturen und einem einfachen Zertifikat, basierend auf dem Schlüssel für Geheimhaltung, Authentifizierung und einfache Signatur.

Sie enthält außerdem eine „Personenbindung", mit welcher von der Stammzahlregisterbehörde bestätigt wird, dass der in der Bürgerkarte bezeichneten Person eine bestimmte Stammzahl zur eindeutigen Identifikation zugeordnet ist. Die Stammzahl ist eine durch Verschlüsselung gesicherte Ableitung aus der ZMR-Zahl des Zentralen Melderegisters. Damit wird ausschließlich für Behörden eine eindeutige und unverwechselbare Zuordnung eines elektronisch gestellten Antrags zu einer Person möglich.

2 Ablauf Maestrokarte

Dieses Kapitel beschreibt den organisatorischen Gesamtablauf im Zusammenhang mit der Ausstellung der Maestrokarte an den Signator und der Erzeugung des Signatur- und Geheimhaltungszertifikats sowie des Schreibens der Personenbindung auf die Karte:

1. Die Issuerbank sendet die Maestrokarten-Auftragssätze an Europay Austria.

2. Europay Austria übermittelt die Kartenproduktionsaufträge an AustriaCard. Dort werden die Karten initialisiert sowie mit den Maestro-spezifischen Daten personalisiert und erhalten Layout und Beschriftung.

3. Die Karten werden von AustriaCard an die Issuerbanken oder im Auftrag der Issuerbank gleich direkt an die Kunden übermittelt.

4. Die Issuerbank sendet die Maestrokarte an den Karteninhaber (sofern er sie nicht von Austria Card direkt erhalten hat) oder legt sie in der Filiale zur Abholung bereit. Die Karte ist als Maestrokarte wie gewohnt verwendbar. Wenn der Karteninhaber die Signatur- und Bürgerkartenfunktion nicht nützen will, dann ist für ihn der Prozess hier zu Ende.

5. Will der Karteninhaber die Signaturfunktion der Maestrokarte aktivieren, dann muss er mit der Karte und einem gültigen amtlichen Lichtbildausweis eine Registrierungsstelle aufsuchen.
   Anmerkung: Wenn die Filiale der Issuerbank, bei welcher er seine Maestrokarte erhält (falls er sie nicht zugesandt bekommt), gleichzeitig eine RA-GS der a.trust ist, dann kann er diesen Schritt auch gleich anlässlich der Abholung der Karte erledigen und muss nicht gesondert zu einer RA-GS gehen.

6. Der RO prüft die Identität des Zertifikatswerbers anhand des Lichtbildausweises, nimmt die Belehrung des Signators lt. Signaturgesetz vor und erfasst alle Daten für den Zertifikatsantrag (Details zur Identitätsprüfung siehe Kapitel 5.1). Der RO druckt Antragstellerformular (zwei-fach) sowie das PIN-Infoblatt mit den folgenden PINs aus: Initial-(Signatur)-PIN, Geheimhaltungs- und Infobox-PIN. Die Ausdrucke übergibt er dem Signator. Ein Exemplar des Signaturvertrags wird vom Signator unterschrieben. Der RO scannt und archiviert (mit Signatur durch die RO-Karte) sowohl das vom Signator unterschriebene Antragstellerformular (Zertifikatsantrag und Signaturvertrag) als auch den vorgelegten Ausweis. Die CIN wird neu vergeben oder eine bestehende CIN übernommen (siehe auch Kapitel 5.6).

7. Der RO sendet einen mit seiner RO-Karte signierten Zertifikatsantrag an die a.trust CA. CA-seitig wird das Geheimhaltungsschlüsselpaar generiert bzw. ein bestehendes übernommen (siehe Kapitel 4.2), die Zertifikate für den Sig-

natur- und den Geheimhaltungsschlüssel erstellt und, wenn der Signator zugestimmt hat, im Directory der a.trust veröffentlicht.

8. Die CA liefert das Geheimhaltungsschlüsselpaar und die beiden Zertifikate an die RA-Software, die sie ohne Zwischenspeicherung an die Signaturkarte weitergibt.

9. Die beiden Zertifikate und der Geheimhaltungsschlüssel werden auf die Signaturkarte gespeichert.

10. Der Signator liest die Initial-PIN vom PIN-Infoblatt, gibt sie am Kartenleser ein und ändert sie auf die von ihm selbstgewählte sechs-stellige Signatur-PIN, mit welcher er anschließend signieren kann.

11. Täglich wird von a.trust eine Datei erstellt, in der für die aktivierten Maestrokarten die a.trust Kartennummer (CIN + CSN) einer bankseitig bekannten Kartennummer zugeordnet wird. Diese Datei wird den Bankinstituten, die diese Information benötigen, verschlüsselt und nach erfolgreicher Authentifizierung zur Verfügung gestellt.

12. Von seinem eigenen PC-Arbeitsplatz aus kann der Signator seine Geheimhaltungs- und Infobox-PIN ändern. Er kann, wenn er möchte, auch weiterhin die beiden in der RA-GS ausgedruckten PINs verwenden.

13. Personenbindung

    a. Der Signator kann mittels Web-Applikation, die von der a.trust Homepage aus über http://www.a-trust.at/zmrservice/ gestartet wird, seine Personenbindung beantragen.
    Wenn eine RA das möchte, kann sie dieses Internet-Service optional in ihren GS anbieten.

    b. Aufgrund der CIN der Karte werden die entsprechenden Daten aus der CMS-Datenbank der a.trust gelesen. Aus den persönlichen Daten wird die Anfrage an das Zentrale Melderegister erstellt und abgesandt. Der Signator muss dazu die Geheimhaltungs-PIN eingeben.

    c. Das ZMR sendet die Personenbindung und die Meldeadresse an das a.trust Rechenzentrum (siehe Kapitel 4.3).

    d. Die Personenbindung wird auf die Karte geschrieben. Die Eingabe der Infobox-PIN ist dafür notwendig.

Die zu diesem Ablauf gehörigen Aktivitäten und die ausführenden Systemeinheiten/Personen sind in der folgenden Grafik skizziert.

Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH.
A-1030 Wien, Landstraßer Hauptstraße 5

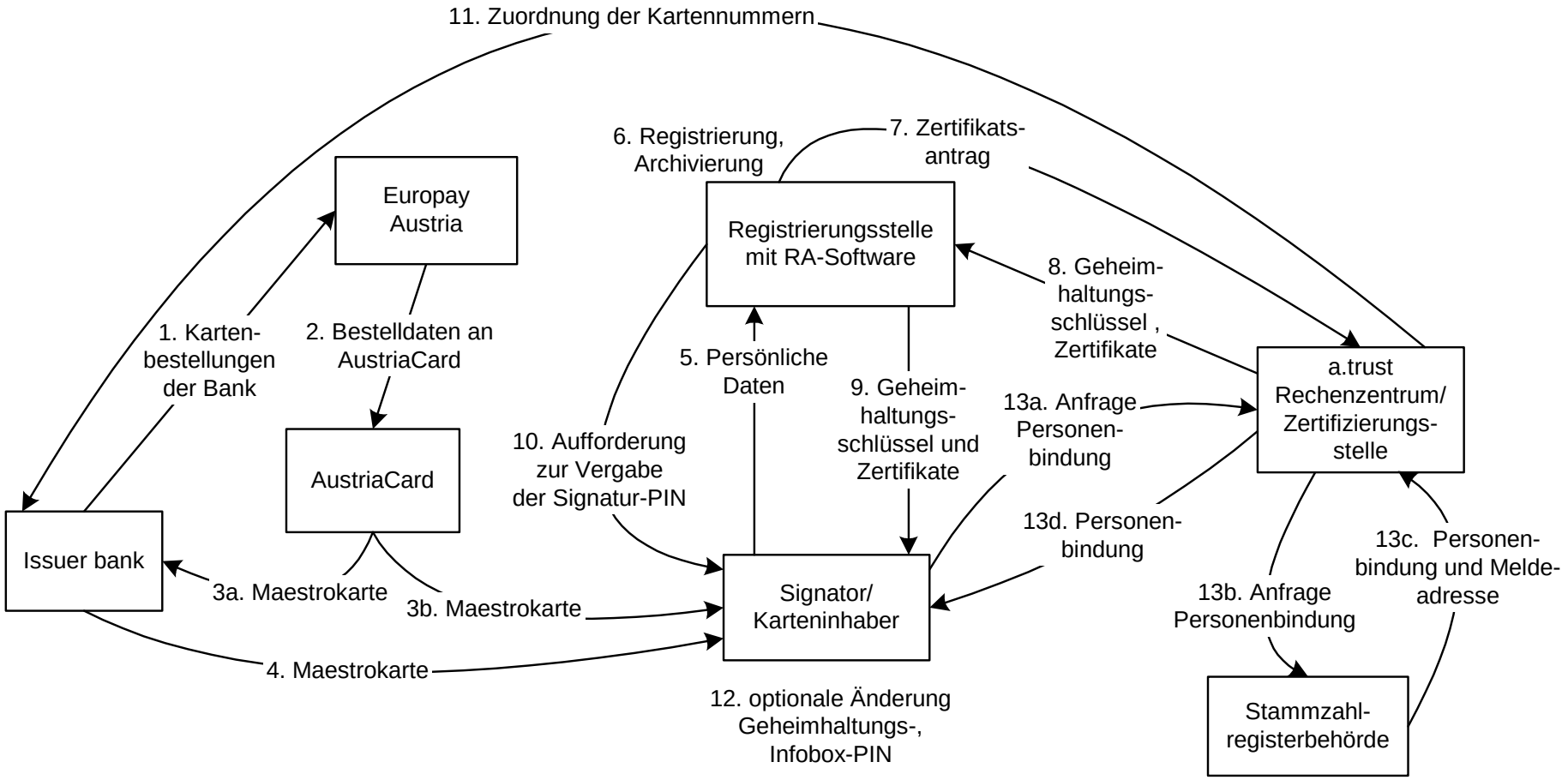

Abbildung 1 Ablauf

3 Ablauf a.sign Premium Bestellkarte

Dieses Kapitel beschreibt den organisatorischen Gesamtablauf im Zusammenhang mit der Bestellung der a.sign Premium Bestellkarte mit ACOS-Chip, der Registrierung des Signators und der Erzeugung des Signatur- und Geheimhaltungszertifikats sowie des Schreibens der Personenbindung auf die Karte:

1. Der Zertifikatswerber bestellt seine Karte über das Web-Formular der a.trust Homepage oder er sucht eine RA auf, die seine Bestellung via CRS an a.trust weiterleitet. Bei größeren Projekten kann die Bestellung mittels eines definierten Datenträgers an a.trust erfolgen. Die CIN wird ermittelt oder übernommen (siehe Kapitel 5.6).

2. Die Kartenbestellungen werden vom a.trust Rechenzentrum an AustriaCard gesandt.

3. Die Karten werden von AustriaCard erzeugt und an die bei der Bestellung definierten RA-GS übermittelt.

4. Der Karteninhaber erhält Antragstellerformular und Merkblatt und besucht mit seinem gültigen amtlichen Lichtbildausweis die ausgewählte Registrierungsstelle nach empfohlener Terminvereinbarung.

5. Der RO prüft die Identität des Zertifikatswerbers anhand des Lichtbildausweises, nimmt die Belehrung des Signators lt. Signaturgesetz vor und gleicht mit dem Zertifikatswerber die Daten ab. (Details zur Identitätsprüfung siehe Kapitel 5.2). Der RO druckt jedenfalls bei einer Änderung der Daten das Antragstellerformular (zwei-fach) sowie das PIN-Infoblatt mit den folgenden PINs aus: Initial-(Signatur)-PIN, Geheimhaltungs- und Infobox-PIN. Die Ausdrucke übergibt er dem Signator. Ein Exemplar des Signaturvertrags wird vom Signator unterschrieben. Der RO scannt und archiviert (mit Signatur durch die RO-Karte) sowohl das vom Signator unterschriebene Antragstellerformular (Zertifikatsantrag und Signaturvertrag) als auch den vorgelegten Ausweis.

6. Der RO sendet einen mit seiner RO-Karte signierten Zertifikatsantrag an die a.trust CA. CA-seitig wird das Geheimhaltungsschlüsselpaar generiert bzw. ein bestehendes übernommen (siehe Kapitel 4.2), die Zertifikate für den Signatur- und den Geheimhaltungsschlüssel erstellt und, wenn der Signator zugestimmt hat, im Directory der a.trust veröffentlicht.

7. Die CA liefert das Geheimhaltungsschlüsselpaar und die beiden Zertifikate an die RA-Software, die sie ohne Zwischenspeicherung an die Signaturkarte weitergibt.

8. Die beiden Zertifikate und der Geheimhaltungsschlüssel werden auf die Signaturkarte gespeichert.

9. Der Signator liest die Initial-PIN vom PIN-Infoblatt, gibt sie am Kartenleser ein und ändert sie auf die von ihm selbstgewählte sechs-stellige Signatur-PIN, mit welcher er an-schließend signieren kann.

10. Von seinem eigenen PC-Arbeitsplatz aus kann der Signator seine Geheimhaltungs- und Infobox-PIN ändern. Er kann, wenn er möchte, auch weiterhin die von der RA-GS erhaltenen Default-PINs verwenden.

11. Personenbindung

    a. Der Signator kann mittels Web-Applikation, die von der a.trust Homepage aus über http://www.a-trust.at/zmrservice/ gestartet wird, seine Personenbindung beantragen.
    Wenn eine RA das möchte, kann sie dieses Internet-Service optional in ihren GS anbieten.

    b. Aufgrund der CIN der Karte werden die entsprechenden Daten aus der CMS-Datenbank der a.trust gelesen. Aus den persönlichen Daten wird die Anfrage an das Zentrale Melderegister erstellt und abgesandt. Der Signator muss dazu die Geheimhaltungs-PIN eingeben.

    c. Das ZMR sendet die Personenbindung und die Meldeadresse an das a.trust Rechenzentrum (siehe Kapitel 4.3).

    d. Die Personenbindung wird auf die Karte geschrieben. Die Eingabe der Infobox-PIN ist dafür notwendig.

Der Ablauf wird durch die folgende Grafik illustriert.

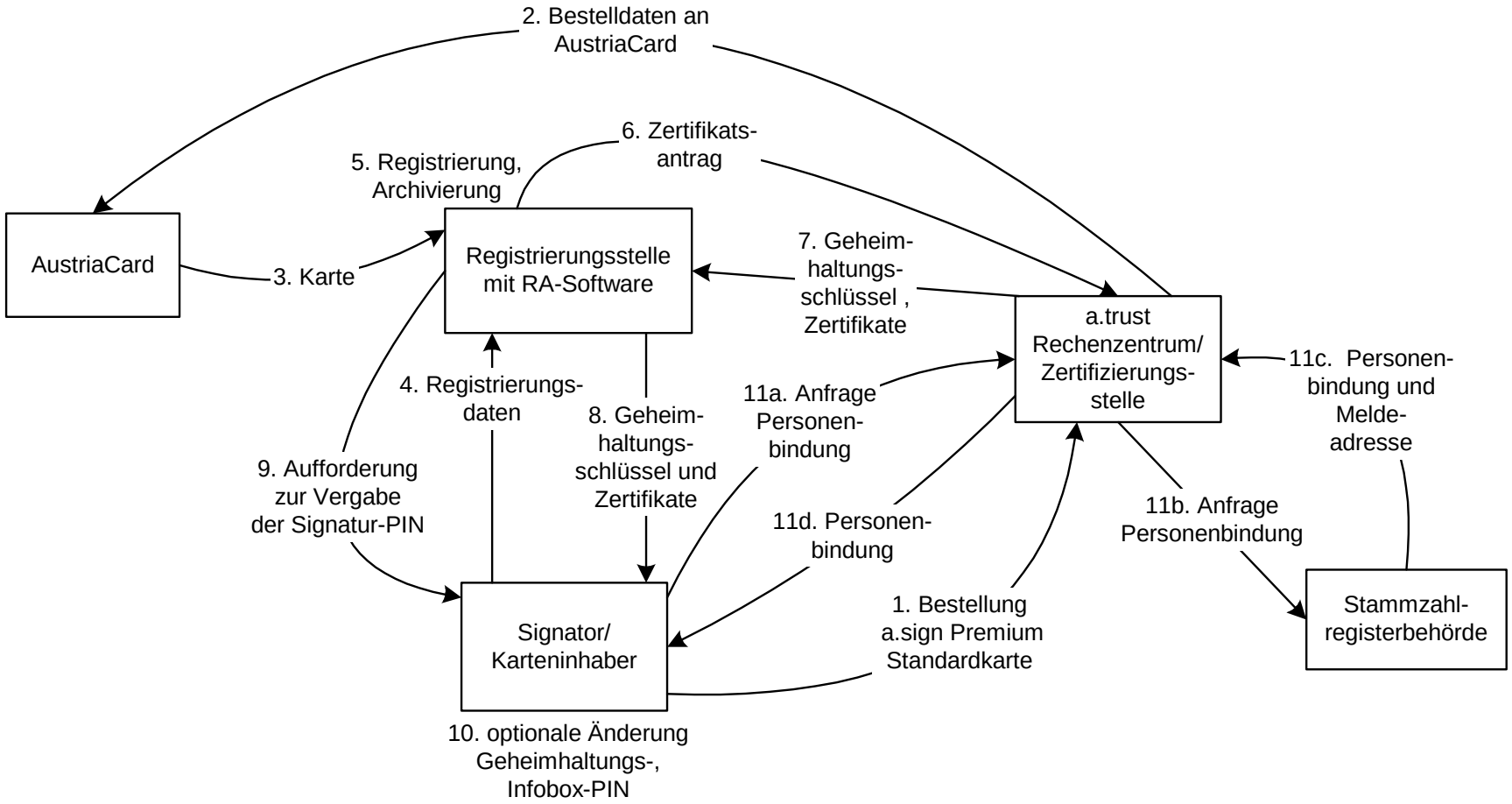

Abbildung 2 Ablauf

4 Darstellung der wesentlichen Systembestandteile

In den folgenden Absätzen werden die wesentlichen Bestandteile der Maestrokarte und der Bestellkarte mit ACOS-Chip zusammengefasst.

4.1 Signaturschlüssel, PIN und PUK

Der Signaturschlüssel, der zur Erstellung sicherer digitaler Signaturen gem. Signaturgesetz geeignet ist, wird während der Initialisierung bei AustriaCard durch die Karte selbst erzeugt.

Die Unterschriftsfunktion der Karte ist durch eine PIN gegen Missbrauch geschützt. Bei der Registrierung muss der Signator die fünf-stellige numerische Initial-PIN (ist für jeden Signator gleich: 12345) dem PIN-Infoblatt entnehmen, in den Kartenleser eingeben und unverzüglich ändern. Der RO hat den Signator ausdrücklich darauf hinzuweisen, dass die Signatur-PIN aus sechs Ziffern bestehen muss. Die Initial-PIN selbst ist nicht zur Signatur geeignet. Bei Eingabe der Initial-PIN zum Zweck der Änderung auf die Signatur-PIN sind drei Fehleingaben möglich.

Bei Eingabe der Signatur-PIN sind zehn Fehleingaben möglich. Nach der zehnten falschen Eingabe wird die Signaturfunktion der Karte blockiert. Sie kann durch Eingabe des Signatur-PUK wieder aufgehoben werden. Der Signatur-PUK ist ein 16-stelliger numerischer Code. Im Falle des Signatur-PUK sind drei Fehleingaben möglich, nach der dritten falschen PUK-Eingabe kann keine Deblockierung mehr vorgenommen werden. Weiters kann nur insgesamt dreimal eine Deblockierung der PIN durch PUK-Eingabe erfolgen.

4.2 Geheimhaltungsschlüssel, PIN und PUK

Der Geheimhaltungsschlüssel, der zur Erstellung einfacher Signaturen, Authentifizierung und Geheimhaltung (Entschlüsselung) Verwendung findet, wird anlässlich der Registrierung in der RA auf die Karte geschrieben. Gleichzeitig wird er auch in verschlüsselter Form in der CMS-Datenbank gespeichert, damit er auf Ersatz-/Folge- und Zusatzkarten übernommen werden kann. Um auf eine andere (nächste) Karte übernommen werden zu können, muss (müssen):

- der Chip der nächsten Karte über dasselbe Betriebssystem verfügen,
- Schlüssellänge und Algorithmus bei der nächsten Karte unverändert sein,

- der Signator diese Option bei der Aktivierung der Karte (mit Gültigkeit für die nächste Karte) auswählen und
- bei Folgekarten der Zusammenhang zur bestehenden Karte berücksichtigt werden (siehe Kapitel 5.6).

Wenn eine Bedingungen nicht zutrifft, so wird bei der nächsten Aktivierung der alte Schlüssel nicht verwendet, sondern auf jeden Fall ein neuer Geheimhaltungsschlüssel generiert und wiederum im CMS gespeichert.

Die Geheimhaltungsfunktion der Karte ist durch die Geheimhaltungs-PIN gegen Missbrauch geschützt, die nach zehn Fehleingaben blockiert ist und mittels Geheimhaltungs-PUK deblockiert werden kann. Die Geheimhaltungs-PIN ist vier-stellig numerisch und wird im Rahmen der Registrierung vom RO zusammen mit den dazu gehörigen Informationen ausgedruckt und so dem Signator übergeben. Diese PIN ist eine Zufallszahl, wird für jeden Signator neu generiert und ist schon zur Auslösung der Geheimhaltungsoperation geeignet. Der Signator kann sie in eine selbstgewählte ebenfalls vier-stellige Geheimzahl ändern. Diese PIN-Änderung nimmt der Signator an seinem eigenen Rechner vor.

Der Geheimhaltungs-PUK ist ein 16-stelliger numerischer Code. Drei Fehleingaben sind möglich, nach der dritten falschen Eingabe kann keine Deblockierung mehr vorgenommen werden. Weiters kann nur insgesamt dreimal eine Deblockierung der PIN durch PUK-Eingabe erfolgen.

4.3 Personenbindung, PIN und PUK

Die Karte enthält sogenannte Infoboxen, in denen Daten, die für die Bürgerkarte relevant sind, abgespeichert werden können. Derzeit wird nur die Infobox für die Personenbindung genutzt. Die Infoboxen sind durch eine gemeinsame PIN, die sogenannte Infobox-PIN geschützt. Dazu gibt es eine Default-PIN (0000 für alle Signatoren), die dem Signator bei der Registrierung in Form eines Ausdrucks auf dem PIN-Infoblatt übergeben wird, unabhängig davon, ob er die Personenbindung aktivieren wird oder nicht. Der Signator kann die Infobox-PIN in einen selbstgewählten Wert ändern, wenn er das möchte, oder den Default-Wert beibehalten. Hinsichtlich Länge, Fehlversuche und weiterer Eigenschaften von Infobox-PIN und -PUK gilt dasselbe wie für Geheimhaltungs-PIN und -PUK.

Die Registrierungsstelle oder a.trust bekommen keine der vom Signator selbst gewählten PINs zu sehen und speichern sie auch nicht, gleichgültig ob er sie in der RA-GS ändert oder an seinem eigenen PC-Arbeitsplatz. Der Signator sollte die Informationsblätter, wenn darauf gültige PINs stehen, gesichert aufbewahren oder (noch sicherer) sich die PINs merken.

Wenn der Signator die Personenbindung über http://www.a-trust.at/zmrservice/ auf die Karte aufbringen lässt, wird die im ZMR eingetragene Meldeadresse in der CMS-Datenbank gespeichert. Dies geschieht bei jeder neuerlichen Personenbindungsabfrage durch den Signator mit der zum Abfragezeitpunkt gültigen Meldeadresse. Diese Speicherung dient dem Nachweis, dass es zu einem bestimmten Zeitpunkt einen eindeutigen Eintrag im ZMR gegeben hat.

4.4 Schlüssellängen und Algorithmen

Der Signaturschlüssel ist ein auf dem ECC-Algorithmus (elliptic curve cryptography) basierender Schlüssel mit 192 bit Länge. Der Geheimhaltungsschlüssel ist ein RSA-Schlüssel mit einer Länge von 1536 bit. Die CA-Schlüssel der Root- und der Zwischenzertifizierungsstellen, die zur Signatur der Signatorzertifikate und Sperrlisten dienen, sind RSA-Schlüssel mit einer Länge von 2048 bit.

4.5 Druck/Nachdruck von PINs/PUKs

Die PUKs für Signatur, Geheimhaltung und Infobox werden nicht standardmäßig ausgedruckt, sondern sie werden nur auf Antrag des Signators, der beim Call Center gestellt und an das a.trust Rechenzentrum weitergeleitet wird, gedruckt. Alternativ kann der Signator das PUK-Kuvert auch über http://www.a-trust.at/pukservice anfordern. Vom Rechenzentrum wird das Kuvert mit den drei PUK-Werten an den Signator versandt.

Die Initial-(Signatur-)PIN, die Geheimhaltungs-PIN und die Infobox-PIN werden in der Registrierungsstelle auf das PIN-Infoblatt gedruckt und dem Signator bei der Registrierung übergeben. Das PIN-Infoblatt muss auf jeden Fall sicher und von der Karte getrennt aufbewahrt werden.

Die Initialwerte der PINs können, wenn das notwendig sein sollte, zu einem späteren Zeitpunkt nachgedruckt werden. Der Signator muss die Anforderung für den Nachdruck dem Call Center bekannt geben; das PIN-Kuvert wird ihm dann an seine Zustelladresse gesandt. Es können nur die Initialwerte gedruckt werden, d. h. vom Signator bereits geänderte, selbst vergebene PINs sind weder der RA-GS noch dem a.trust Rechenzentrum bekannt, weshalb sie sich der Signator selbst merken muss.

4.6 Überblick über die PINs der ACOS-Karte

Die folgende Tabelle veranschaulicht die verschiedenen PINs der Karten mit ACOS-Chip, ihre Verwendungsmöglichkeiten und Eigenschaften.

Anmerkung: Der Maestro-Code (Bankomat-Code) gilt nur für Maestrokarten.

PIN	Mitteilung an Signator	Initialwert	Stellen-anzahl	Verwendung	Anzahl Fehl-ver-suche	PUK	PIN-Änderung
Maestro-Code	PIN-Kuvert	zufällig	vier	Bankanwendungen	vier	nein	nein
Initial-PIN für Signatur	Ausdruck in der RA-GS auf PIN-Infoblatt	12345	fünf	Änderung in Signatur-PIN	drei	nein	verpflichtende Änderung in die Signatur-PIN in der RA-GS
Signatur-PIN	Selbstwahl durch den Signator	siehe Initial-PIN	sechs	sichere Signatur	zehn	ja	jederzeit möglich durch Eingabe der aktuellen Signatur-PIN, empfohlen

Geheimhal-tungs-PIN	Ausdruck in der RA-GS auf PIN-Infoblatt	zufällig	vier	Einfache Signatur, Ge-heimhaltung, Authentifi-zierung	zehn	ja	jederzeit möglich durch Eingabe der aktuellen Geheimhaltungs-PIN, empfohlen
Infobox-PIN	Ausdruck in der RA-GS auf PIN-Infoblatt	0000	vier	Zugriff auf die Info-boxen (Personenbin-dung) auf der Karte	zehn	ja	jederzeit möglich durch Eingabe der aktuellen Infobox-PIN, empfohlen

Tabelle 1 PINs und ihre Eigenschaften

5 Organisatorisches

5.1 Registrierung Maestrokarte

Zur Registrierung besucht der Inhaber der Maestrokarte die RA-GS. Dazu muss er einen gültigen amtlichen Lichtbildausweis und die Karte mitbringen. Der RO identifiziert den Karteninhaber anhand des Ausweises. Er muss den auf der Kartenoberfläche lesbaren Namen des Signators mit dem im Ausweis befindlichen Namen vergleichen. Bei Abweichung beider Namen (Anmerkung: eine Abweichung hinsichtlich eines zweiten Vornamens oder eines Titels stört hierbei nicht) muss der Registrierungsprozess abgebrochen werden. Der Signator darf in diesem Fall kein Zertifikat erhalten, da er entweder eine Karte in der Hand hat, die nicht ihm gehört oder eine erfolgte Namensänderung nicht durchgängig nachvollzogen wurde. Der RO muss dem Signator empfehlen wiederzukommen, wenn die Daten richtig gestellt sind (d. h. der Signator wird bei seiner Bank eine neue Maestrokarte mit korrektem Namensaufdruck bestellen oder bei der Ausweisbehörde einen neuen Ausweis beantragen müssen).

Der Signator erhält Merkblatt und Antragstellerformular bei der Registrierung.

5.2 Registrierung Bestellkarte

Zur Registrierung für eine a.sign Premium Bestellkarte sucht der Zertifikatswerber mit einem gültigen amtlichen Lichtbildausweis und seinem Antragstellerformular, das ihm nach der Bestellung mit dem Merkblatt zugesandt wurde, jene RA-GS auf, die er bei der Bestellung ausgewählt hat. Der RO identifiziert den Karteninhaber anhand des Ausweises. Im CRS muss aufgrund der Bestellung ein Datensatz vorhanden sein, der bei der Aktivierung vom RO mittels des Lichtbildausweises und der Angaben des Signators abzugleichen und ggf. zu korrigieren ist.

5.3 Schreiben der Zertifikate

Bei der Registrierung werden der Geheimhaltungsschlüssel auf die Karte geschrieben und die Zertifikatserstellung für Signatur- und Geheimhaltungsschlüssel in der CA angestoßen. Die Zertifikate werden auf der Karte gespeichert und, wenn gewünscht, im Directory veröffentlicht.

5.4 PIN-Änderungen

Die Vergabe der Signatur-PIN ist unmittelbar in der RA-GS durch den Signator durchzuführen. Nach der Eingabe der Initial-PIN muss der Signator die selbst gewählte Signatur-PIN zweimal eingeben. Diese Signatur-PIN sowie auch die Geheimhaltungs-PIN kann er jederzeit an seinem eigenen Rechner zu Hause oder im Büro ändern.

Wenn der Signator die Bürgerkartenfunktion in Anspruch nehmen will, dann veranlasst er das ebenfalls von seinem eigenen Arbeitsplatz aus über eine von a.trust zur Verfügung gestellte Web-Applikation. Auch seine Infobox-PIN kann er an seinem Arbeitsplatz ändern, wenn er das möchte.

5.5 Sperre, Widerruf und Passwort

Bei der Registrierung einer Maestrokarte wählt der Signator ein Widerrufs- und Sperrpasswort und gibt es dem RO zur Erfassung mit seinen persönlichen Daten bekannt. Bei einer Bestellkarte gibt der Signator das gewählte Passwort bereits anlässlich der Bestellung an.

Das Passwort kann sich der Signator notieren, damit er es nicht vergisst. Falls er es dennoch vergisst, kann er es bei einer RA-GS mit Ausweisleistung erfragen oder, sofern seine Zertifikate gültig sind und die Karte verwendbar ist, das Passwort mit dem Online-Änderungsformular für seine Stammdaten (Authentifizierung mit der Geheimhaltungs-PIN) anzeigen lassen.

Die Sperre und der Widerruf der Zertifikate einer Maestrokarte folgen den gleichen Abläufen wie Sperre und Widerruf von a.sign Premium Bestellkarten. Allerdings kann anlässlich des Widerrufs von Maestrokartenzertifikaten keine Ersatzbestellung einer Maestrokarte durch den Revocation Center Agent erfolgen, da der Signator eine Maestrokarte nur bei seiner Bank bestellen kann. Wenn der Signator mit seiner neuen Maestrokarte in die RA-GS zur Aktivierung kommt, so hat die Registrierung genauso wie die erstmalige Registrierung unter Beachtung von Kapitel 5.6 zu erfolgen. Hinsichtlich der Verrechnung der Zertifikatsgebühr gibt es die Unterscheidung zwischen Ersatzbestellung/-aktivierung und Folgebestellung/-aktivierung.

5.6 Identifikation des Inhabers einer CIN

Auch die Maestrokarte erhält eine a.sign Premium Kartennummer, wenn die Zertifikate ausgestellt werden. Allerdings ist diese nicht auf der Kartenoberfläche sichtbar, sondern nur intern gespeichert und am Antragstellerformular ersichtlich.

Die Kartennummer besteht aus der CIN (12-stellig) und der Kartenfolgenummer (vier-stellig), wobei die CIN für den Signator eindeutig und auch Bestandteil der Inhaberinformationen des Zertifikats ist.

Die CIN bleibt bei jeder der Karten des Signators gleich, falls bei Bestellung/Aktivierung der Zusammenhang zur bestehenden oder vorigen Karte hergestellt wird. Die Folgenummer wird um eins erhöht.

Wenn ein Karteninhaber bereits eine Signaturkarte hat(te) und bei der Aktivierung der Signaturfunktion die CIN beibehalten möchte, so muss eine genaue Identifizierung erfolgen, um die CIN nur einem Signator zuzuteilen, der berechtigt ist, sie zu verwenden.

Es gibt die folgenden Möglichkeiten, die CIN eines Signators zweifelsfrei festzustellen (die Ausweisüberprüfung hinsichtlich Gültigkeit und Lichtbild erfolgt natürlich in jedem Fall):

CIN aus der Karte lesen

Die Voraussetzung dafür ist, dass der Signator die „alte“ Karte noch verwenden kann (intakter Chip und nicht gesperrt/widerrufen) und sie bei der Aktivierung der neuen Karte in die RA-GS mitnimmt.
Die alte Karte wird, mit Authentifizierung durch Eingabe der Geheimhaltungs-PIN, gelesen und die CIN aus der Karte ermittelt. Die folgenden, zur Karte gehörigen, Daten werden mit dem vorgelegten Ausweis abgeglichen: Vorname, Zuname, Geburtsdatum und Geburtsort. Bei Übereinstimmung ist der Signator eindeutig als Berechtigter für die CIN identifiziert.

Übereinstimmung persönlicher und Ausweisdaten

Der Signator nimmt bei der Aktivierung den Ausweis mit, den er auch bei der Aktivierung der letzten Karte vorgelegt hat. Die persönlichen sowie die Ausweisdaten des Signators müssen mit den im CMS gespeicherten Daten übereinstimmen.
Persönliche Daten: Vorname, Nachname, Geburtsdatum, Geburtsort,
Ausweisdaten: Ausweisnummer, Ausstelldatum, ausstellende Behörde.
Mit der Übereinstimmung dieser Daten ist der Signator eindeutig identifiziert.

Wenn der Signator weder die alte Karte noch den zuletzt verwendeten Ausweis mitbringt, dann erhält er eine neue CIN.

5.7 Unterscheidungen

Die folgenden Unterschiede zwischen Maestrokarte und Bestellkarte mit ACOS-Chip wurden identifiziert:

- Die Maestrokarte erhält der Kunde von seiner Bank und kann sie nach Wunsch aktivieren lassen. Die Bestellkarte bestellt er entweder über das Web-Formular der a.trust oder direkt bei der RA-GS oder es wird zur Bestellung ein Datenträger an a.trust übermittelt.

- Eine Bestellkarte erhält der Signator bei der Aktivierung direkt in der RA-GS, eine Maestrokarte muss er üblicherweise in die RA-GS selbst mitbringen.

- Bei der Bestellkarte werden Antragstellerformular und Merkblatt nach der Bestellung an den Signator versandt, bei der Maestrokarte erhält er diese Unterlagen erst bei der Registrierung.

- Eine Ersatzkarte kann im Rahmen eines Widerrufs nur dann beim RCA bestellt werden, wenn es sich um eine Bestellkarte handelt. Eine neue Maestrokarte kann im Zuge ihrer Aktivierung in der RA-GS als "Ersatzaktivierung" abgewickelt werden und hat so hinsichtlich der Zertifikatsverrechnung für den Signator den gleichen Effekt.

Zur Information sind die wichtigsten Unterschiede zwischen Bestellkarte mit ACOS-Chip und Bestellkarte mit Starcos-Chip hier zusammengefasst:

- Auf die Karte mit ACOS-Chip wird eine Kennzeichnung gelasert, die sie für den Signator von der Starcos-Chip-Karte unterscheidbar macht. Diese Kennzeichnung ist ein Bindestrich „-“ zwischen CIN und CSN auf der ACOS-Bestellkarte. In der Dokumentation (CP/CPS) und in der Kommunikation mit dem Signator (Call Center etc.) wird auf diese Unterscheidung Bezug genommen werden.

- Starcos-Chip: Der Signator erhält nach der Bestellung Antragstellerformular, Merkblatt, PIN- und PUK/Passwort-Kuvert zugesandt.
  ACOS-Chip: Der Signator erhält nach der Bestellung nur Antragstellerformular und Merkblatt zugesandt. Die PIN-Informationen werden bei der Registrierung auf das PIN-Infoblatt gedruckt, das Widerrufs- und Sperrpasswort wird nicht gedruckt. Das PUK-Kuvert wird nur, wenn es der Signator benötigt, auf ausdrückliche Anforderung beim Call Center oder nach Bestellung über die Homepage via http://www.a-trust.at/pukservice gedruckt und an ihn versandt.

- Starcos-Chip: Die Signatur-PIN ist sechs- bis acht-stellig.
  ACOS-Chip: Die Signatur-PIN ist exakt sechs-stellig.

5.8 Vertragsdauer

Maestrokarten können unter Umständen länger gültig sein als die zugehörigen Zertfikate; z. B. Austausch der Maestrokarte im Oktober mit unmittelbarer Aktivierung von a.sign Premium, Gültigkeit der neuen Karte bis Ende Dezember + drei Jahre, Gültigkeit der Zertifikate nur bis Oktober + drei Jahre.

In diesem Fall bleibt es dem Signator überlassen, ob er für die verbleibende Restlaufzeit der Karte sein Zertifikat verlängern lässt oder eine neue Maestrokarte bestellt und für diese neue Zertifikate ausstellen lässt.

Wenn die Maestrokarte zum Zeitpunkt der Zertifikatsausstellung kürzer als drei Jahre gültig ist, wird die Gültigkeitsdauer des Zertifikats jener der Maestrokarte angepasst.

6 Anhang

A Dokumentengeschichte

Version	Datum	Autor	Änderungen
1.0	31.08.2004	Stangl/BDC	Erste Version
1.0.1	18.10.2004	Stangl/BDC	Verschiedene Änderungen in den Abläufen
1.0.2	25.10.2004	Stangl/BDC	Finale Version

B Glossar

ASM	a.trust Security Module
CCM	Central Certificate Manager
CIN	Cardholder Identification Number
CMS	Card Management System
CRL	Certificate Revocation List, Liste der gesperrten und widerrufenen Zertifikate
DN	Distinguished Name
DS	Directory Service (Verzeichnisdienst)
ECC	Elliptic Curve Cryptography; asymmetrischer Kryptoalgorithmus basierend auf elliptischen Kurven.
HSM	Hardware Security Module
Kompromittierung	Eine unautorisierte Offenlegung von oder der Verlust der Kontrolle über sicherheitskritische Informationen und geheimzuhaltende Daten
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
Öffentlicher Schlüssel	(Public Key) Öffentlicher Teil eines Schlüsselpaares, Bestandteil eines Zertifikates, wird zur Überprüfung von Digitalen Signaturen und zur Verschlüsselung von Daten verwendet
PIN	Personal Identification Number
Privater Schlüssel	(Private Key, Geheimer Schlüssel) Geheimer Teil eines Schlüsselpaares, der zum digitalen Signieren und Entschlüsseln von Daten erforderlich ist und geheimgehalten werden muss.

Public-Key System	Ein kryptographisches System, das ein Paar von durch einen mathematischen Algorithmus verbundenen Schlüsseln benutzt. Siehe auch Öffentlicher Schlüssel und Privater Schlüssel.
PUK	Personal Unblocking Key
RA	Registration Authority, Registrierungsstelle
RA-GS	Geschäftsstelle einer RA, in der Registrierungen durchgeführt werden
RC	Revocation Center
RCA	Revocation Center Agent, Mitarbeiter des Revocation Centers, der zuständig ist für die Entgegennahme der Sperr-, Widerrufs- und Sperraufhebungsanträge
RO	Registration Officer, Mitarbeiter der Registrierungsstelle und verantwortlich für Registrierung und Abwicklung sämtlicher Bestellungen und Anträge des Karteninhabers
RSA	Asymmetrischer Kryptoalgorithmus für die Erstellung und Verifikation der Elektronischen Unterschrift und Ver- und Entschlüsselungsaufgaben
Signator	a.sign Premium-Karteninhaber; Definition lt. § 2 Abs. 2 [SigG]: „eine natürliche Person, der Signaturerstellungsdaten und die entsprechenden Signaturprüfdaten zugeordnet sind und die entweder im eigenen oder im fremden Namen eine elektronische Signatur erstellt, oder ein Zertifizierungsdiensteanbieter, der Zertifikate für die Erbringung von Zertifizierungsdiensten verwendet“.
ZDA	Zertifizierungsdiensteanbieter
ZMR	Zentrales Melderegister

C Gesetzliche Grundlagen

REF	TITEL
[SigG]	Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG). BGBl. I Nr. 190/1999 (NR: GP XX RV 1999 AB 2065 S. 180. BR: AB 6065 S. 657.)
[SigV]	Verordnung zum Signaturgesetz, BGBl II 2000/30, 02. 02. 2000
[e-govG]	Bundesgesetz, mit dem ein e-Government-Gesetz erlassen wird sowie das Allgemeine Verwaltungsverfahrensgesetz 1991, das Zustellgesetz und das Gebührengesetz 1957 geändert werden 2003-10-28