17

BPX.

Lukas Fässler
Oliver Sidler

Was Manager wissen müssen!

Elektronische Signatur

Unterschreiben & Verschlüsseln

Praxisleitfaden für die Installation & Anwendung

- Sicher signieren
- Inhalte verschlüsseln
- Einsatz in der Praxis
- Rechtliche Basis Schweiz
- Rechtliche Basis EU
- Technische Grundlagen
- Organisation
- Praxisbeispiele
- Checklisten

Editionspartner:

CABARET

KOBIL secure your identity

swisscom

www.bpx.ch

BPX.

Lukas Fässler
Oliver Sidler

Was Manager wissen müssen!

Elektronische Signatur:
Unterschreiben & Verschlüsseln

Praxisleitfaden für die Installation & Anwendung

BPX-Edition
Rheinfelden/Schweiz

BPX Best Practice Xperts
E-Mail edition@bpx.ch
Internet www.bpx.ch

Lukas Fässler / Oliver Sidler

Elektronische Signatur: Unterschreiben & Verschlüsseln Praxisleitfaden für die Installation & Anwendung

Vorwort von Fulvio Caccia, Präsident asut

Rheinfelden/Schweiz
BPX-Edition, April 2008

ISBN 978-3-905413-03-8

Hinweis: In diesem Booklet wird bei Bezeichnungen die männliche Form verwendet. Dies dient lediglich der Lesefreundlichkeit und schliesst die weibliche Form mit ein.

Aufgrund der technischen Entwicklung können die Anleitungen in diesem Booklet Abweichungen erfahren. Die aktuellen Versionen der Anleitungen sind zu finden unter: www.e-comtrust.ch/signatur

Herstellung: BPX-Edition, Rheinfelden/Schweiz

Druck und Verarbeitung: Druckerei Flawil AG

	Vorwort von Fulvio Caccia, Präsident asut	**4**
1	**Elektronische Signatur**	**5**
2	**Weg zur elektronischen Signatur**	**7**
2.1	Antrag für elektronische Signatur	7
2.2	Erneuerung elektronisches Zertifikat	14
2.3	Ungültigkeitserklärung	16
3	**Elektronische Signatur installieren**	**20**
3.1	Verschlüsselung installieren	24
4	**Unterschreiben und Verschlüsseln**	**30**
4.1	PDF-Dokumente signieren	30
4.2	Signierte PDF-Dokumente lesen	34
4.3	Verwendung der Mail-Verschlüsselung	37
4.4	Prüfung elektronischer Signaturen	43
4.5	Alternative Datenverschlüsselung	45
5	**Rechtsverkehr mit Behörden**	**50**
5.1	Bundesverwaltung	50
5.2	Bundesgericht	52
5.3	Kantonale Gerichte	53
5.4	Weitere Anwendungen	53
6	**Rechtliche Grundlagen Schweiz**	**54**
6.1	Gesetzesbestimmungen	54
6.2	Beweiswert digitaler Dokumente	55
6.3	Haftung und Verantwortung	57
7	**Rechtliche Grundlagen in der EU**	**63**
7.1	Signatur-Richtlinie 1999/93/EG	63
7.2	Deutschland	64
7.3	Italien	66
7.4	Grossbritannien	67
7.5	Österreich	67
7.6	E-Commerce-Richtlinie 2000/31/EG	72
7.7	Beweiswert	72
7.8	Internationale Gültigkeit von Zertifikaten	73
8	**Aufbauorganisation**	**75**
8.1	Akkreditierungsstelle AB	76
8.2	Anerkennungsstelle CB	76
8.3	Bundesamt für Kommunikation Bakom	76
8.4	Zertifizierungsdienstanbieter CSP	77
8.5	Registrierungsstelle RA	77
8.6	Kunde / Antragsteller	78
9	**Technische Grundlagen**	**80**
10	**Glossar und Online-Hinweise**	**82**
11	**Profile der Editionspartner**	**85**
12	**Autorenteam & BPX**	**88**

Vorwort

Schweizerische Unternehmen stehen im dauernden Wettbewerb mit inländischen und ausländischen Konkurrenzunternehmen. Zufriedene Kunden, qualitativ einwandfreie Produkte und Dienstleistungen zu konkurrenzfähigen Preisen sind überlebenswichtig. Der Wettbewerb mit der Konkurrenz erfordert eine stete Überprüfung der eigenen Produktions-, Logistik- und Kundenprozesse. Effizienz und Effektivität sind strategische Erfolgsfaktoren geworden.

Die qualifizierte elektronische Signatur, die nach Art. 14 Abs. 2^{bis} des Schweizerischen Obligationenrechts (OR) seit dem 1. Januar 2005 der eigenhändigen Unterschrift gleichgestellt ist, kann künftig vorab im e-Commerce grosses Potenzial, insbesondere die rechtsverbindliche Automatisierung und Prozessoptimierung, in den Unternehmen freisetzen. Der Anbieter erhält dadurch Rechtssicherheit, weil er sich vollumfänglich auf die digital signierten Bestellungen seiner Kunden verlassen kann. Der ehemals anonyme Kunde wird zum eindeutig identifizierbaren Vertragspartner. Der Kunde kann neu alle seine Rechtsgeschäfte verbindlich auch digital abwickeln.

Jetzt liegt im vorliegenden Booklet, das man auch gut im Regionalzug auf dem Weg zur Arbeit lesen kann, erstmals ein Praxisleitfaden vor, welcher in verständlicher Art und Weise den Einsatz, den Gebrauch und die Installation der erforderlichen Infrastruktur für die Nutzung digitaler Signaturen beschreibt.

Die Anbieter von e-Commerce-Lösungen ermuntere ich, diese neue Technologie in ihre bestehenden Lösungen einzubauen und damit dieser neuen, vertragsbindenden Form zum Durchbruch zu verhelfen. Als Anbieter erhalten Sie dadurch Sicherheit in der Vertragsabwicklung und die Garantie, mit einer eindeutig identifizierbaren natürlichen Person in eine bindende Vertragsbeziehung zu treten. Zudem schaffen Sie sich einen wesentlichen Wettbewerbsvorteil.

Die Konsumenten ermuntere ich, die qualifizierte elektronische Signatur als Ausweis ihres rechtsverbindlichen Handelns einzusetzen und so den Anbietern die Möglichkeit zu geben, die vorhandenen Prozesse zu vereinfachen und dadurch letztlich auch bezüglich Preis konkurrenzfähige Produkte und Dienstleistungen bereitzustellen.

Fulvio Caccia
Präsident der Asut (Schweizerischer Verband der Telekommunikation) und Vizepräsident von ICTswitzerland

1 Elektronische Signatur

Die digitale Signatur ist ein Sicherheitsstandard für den Austausch elektronischer Dokumente und sichert die Authentizität des Absenders und die Integrität des Inhalts eines elektronischen Dokumentes. Die digitale Signatur hat die gleiche rechtliche Relevanz wie die Unterschrift auf einem Papierdokument.

Die digitale Signatur wird durch die Kombination eines geheimen oder privaten Schlüssels (Private Key), der nur dem Schlüsselinhaber selbst bekannt ist, und eines öffentlichen Schlüssels (Public Key), der von Zertifizierungsstellen verwaltet wird, generiert und an ein elektronisches Dokument angehängt.

Der Absender signiert und verschlüsselt sein elektronisches Dokument mit seinem privaten Schlüssel, der sich auf einer Chipkarte oder einem USB-Token befindet. Der Empfänger besitzt nur den öffentlichen Schlüssel und kann das Dokument öffnen und lesen. Er erhält dabei eine verlässliche Information über den Absender und die Authentizität des Inhalts des Dokumentes.

Mit dem öffentlichen Schlüssel kann damit die Echtheit einer Unterschrift überprüft werden, und jede Veränderung an dem unterzeichneten Dokument wird sofort erkennbar. Die öffentlichen Schlüssel werden von autorisierten Stellen zertifiziert. Zertifizierungsstellen speichern die erforderlichen Daten für eine Identifizierung der Eigentümer privater Schlüssel. Über die Zertifizierungsstelle ist es daher möglich, den Eigentümer eines privaten Schlüssels zu ermitteln.

Das Signieren einer Nachricht und deren Verschlüsselung sind nicht dasselbe. Beim Signieren versehen Sie eine Nachricht mit einer Art persönlichem Siegel, das Sie als Absender ausweist und eine nachträgliche Verfälschung der Daten erkennbar macht. Aber: Durch die digitale Signatur wird Ihr Dokument nicht vor unbefugter Einsicht geschützt – eine handschriftliche Unterschrift auf einem Papierdokument schützt ja auch nicht vor Einsichtnahme Dritter. Dazu müssen Sie das Dokument zusätzlich verschlüsseln, was häufig in der Anwendungssoftware als zusätzliche Option vorgesehen ist. Beide Funktionen sind im elektronischen Datentransfer interessant. Sie können sowohl gleichzeitig als auch unabhängig voneinander genutzt werden.

Swisscom Digital Certificate Services Time-Stamping Authority

Swisscom bietet als Dienstanbieter von qualifizierten elektronischen Signaturen gemäss schweizerischem Signaturgesetz ZertES [1] auch Zeitstempel-Services an. Mit diesem Zeitstempel-Service kann die Existenz von digitalen Informationen zu einem bestimmten Zeitpunkt zuverlässig und nachvollziehbar belegt werden. Informationen, die mit einem Zeitstempel eines anerkannten Dienstanbieters für qualifizierte Signaturen versehen wurden, sind vor Veränderungen geschützt, auch wenn diese auf veränderbaren Medien (Disk, Magnetbänder usw.) gespeichert sind. Der von Swisscom angebotene Zeitstempel-Service ist einerseits dazu geeignet, zuverlässig zu belegen, wann eine Signatur an einem Dokument angebracht wurde, und andererseits, damit bei archivierten Daten gesetzeskonform (GeBüV) nachgewiesen werden kann, dass diese nicht verändert wurden (Integritätsnachweis).

Um eine Information mit einem Zeitstempel zu versehen, kann, wie bei der elektronischen Signatur, entweder ein Standardformat gewählt werden (z.B. XML, PDF) oder der Zeitstempel kann als separate Datei aufbewahrt werden. Ein Zeitstempel für ein Dokument wird anhand der Quersumme über das gesamte Dokument erzeugt. So entsteht ein sogenannter «Fingerprint» oder «Hashwert» der Daten. Dieser «Hashwert» wird anschliessend automatisch an den Zeitstempel-Service der Swisscom gesendet. Dieser Dienst generiert daraus ein Zeitstempelobjekt, welches den übermittelten «Hashwert» und die aktuelle Zeit enthält. Dieses Objekt wird elektronisch signiert und an den Anforderer retourniert und zusammen mit der Signatur oder als eigenständiges Element eingebunden. So können die Integrität und der Zeitpunkt, wann die Informationen vorgelegen haben, verbindlich nachgewiesen werden.

Als Zeitquellen werden das GPS-System und das DCF77-System verwendet.

Die GPS-Funkuhr-Zeit wird von der Zeitquelle UTC (USNO, MC) gespiesen. USNO ist das U.S. Naval Observatory. USNO gleicht ihre Zeitserver mit der Referenzzeit des BIPM ab (Bureau International des Poids et Mesures, Frankreich).

DCF77 ist in der Verantwortung der Physikalisch-Technischen Bundesanstalt (PTB) in Deutschland. Mit dem Langwellensender DCF77 werden Normalfrequenz und Zeitsignale sowie kodierte Zeitinformationen gemäss der gesetzlichen Zeit für Deutschland ausgesendet.

Unterscheiden sich die beiden Uhren um mehr als 400 ms, so werden keine Zeitstempel mehr ausgegeben.

[1] ZertES: Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (Bundesgesetz über die elektronische Signatur, ZertES) vom 19. Dezember 2003, auch Signaturgesetz genannt.

Beitrag von Swisscom (Schweiz) AG, Firmenprofil Seite 85

2 Weg zur elektronischen Signatur

Die nachfolgende Darstellung zeigt schematisch und beispielhaft den Prozess, welcher bei der Anmeldung für eine elektronische Signatur bei der Registration Authority (RA; Registrierungsstelle) zu durchlaufen ist.

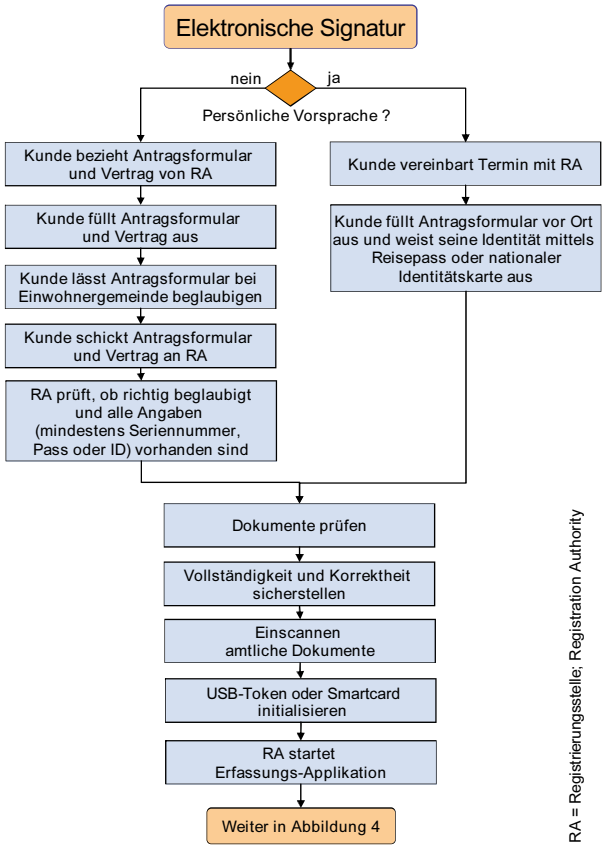


Abbildung 1: Anmeldeprozess für Zertifikatsvergabe (1)

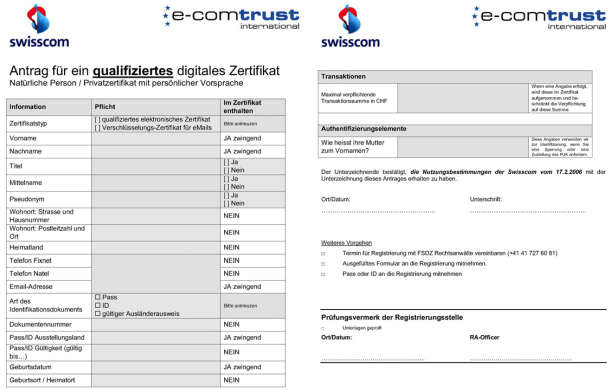
2.1 Antrag für elektronische Signatur

Der Kunde hat die Möglichkeit, entweder persönlich bei der RA vorbeizukommen und die Anmeldung selber vor Ort durchzuführen. Oder er kann die benötigten Unterlagen (Anmeldeformular und Vertrag) aus

dem Internet über die Adresse der RA (z.B. www.e-comtrust.ch/signatur) herunterladen und selber ausfüllen. Damit die Identität sichergestellt ist, braucht es in diesem Falle eine Beglaubigung des Antragsformulares durch die Einwohnergemeinde. Je nach Gemeinde wird dafür eine Bearbeitungsgebühr erhoben.

Persönliche Vorsprache

Das Antragsformular für eine persönliche Vorsprache bei der RA ist vom Antragsteller auszufüllen. Er erhält gleichzeitig mit dem Formular die allgemeinen Nutzungsbestimmungen zur Kenntnis. Der Antragsteller vereinbart mit der RA (z.B. www.e-comtrust.ch/signatur) einen Registrierungstermin und kommt mit dem ausgefüllten Formular sowie dem eigenen Pass oder seiner ID auf den festgelegten Zeitpunkt zur Registrierung bei der RA persönlich vorbei.



swisscom e-comtrust international

Antrag für ein **qualifiziertes** digitales Zertifikat
Natürliche Person / Privatzertifikat mit persönlicher Vorsprache

Information	Pflicht	Im Zertifikat enthalten
Zertifikatstyp	[ ] qualifiziertes elektronisches Zertifikat [ ] Verschlüsselungs-Zertifikat für eMails	Bitte ankreuzen
Vorname		JA zwingend
Nachname		JA zwingend
Titel		[ ] Ja [ ] Nein
Mittelname		[ ] Ja [ ] Nein
Pseudonym		[ ] Ja [ ] Nein
Wohnort: Strasse und Hausnummer		NEIN
Wohnort: Postleitzahl und Ort		NEIN
Heimatland		NEIN
Telefon Fixnet		NEIN
Telefon Natel		NEIN
Email-Adresse		JA zwingend
Art des Identifikationsdokuments	☐ Pass ☐ ID ☐ gültiger Ausländerausweis	Bitte ankreuzen
Dokumentennummer		NEIN
Pass/ID Ausstellungsland		JA zwingend
Pass/ID Gültigkeit (gültig bis…)		NEIN
Geburtsdatum		JA zwingend
Geburtsort / Heimatort		NEIN

swisscom e-comtrust international

Transaktionen

Maximal verpflichtende Transaktionssumme in CHF		Wenn eine Angabe erfolgt, wird diese im Zertifikat aufgenommen und beschränkt die Verpflichtung auf diese Summe.

Authentifizierungselemente

Wie heisst ihre Mutter zum Vornamen?		Diese Angaben verwenden wir für Rückfragen, z.B. bei einer Sperrung oder eine Zustellung des PUK anfordern.

Der Unterzeichnende bestätigt, ***die Nutzungsbestimmungen der Swisscom vom 17.2.2006*** mit der Unterzeichnung dieses Antrages erhalten zu haben.

Ort/Datum: ..... Unterschrift: .....

Weiteres Vorgehen
- ☐ Termin für Registrierung mit FSDZ Rechtsanwälte vereinbaren (+41 41 727 60 81)
- ☐ Ausgefülltes Formular an die Registrierung mitnehmen.
- ☐ Pass oder ID an die Registrierung mitnehmen

Prüfungsvermerk der Registrierungsstelle

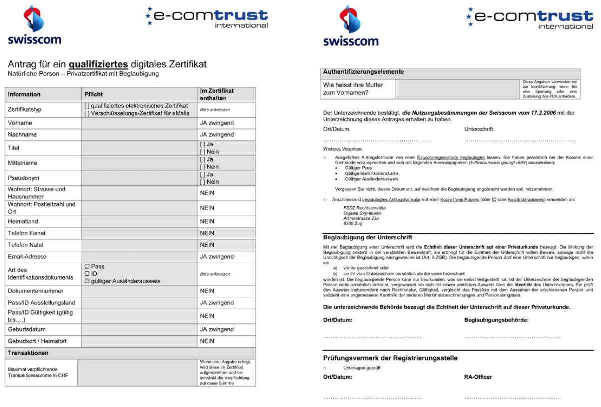
☐ Unterlagen geprüft

Ort/Datum: ..... **RA-Officer** .....

Abbildung 2: Antragsformular für persönliche Vorsprache bei der RA; herunterzuladen z.B. bei www.e-comtrust.ch/signatur

Beglaubigung bei Gemeinde (Einwohnermeldeamt)

Anstelle einer persönlichen Vorsprache bei der RA kann der Antragsteller sein ausgefülltes Antragsformular auf einer Gemeindekanzlei beglaubigen lassen. Er muss dafür seinen Pass, seine ID oder einen gültigen Ausländerausweis mitnehmen. Die Gemeindebehörde bestätigt dann die Übereinstimmung zwischen Unterschrift und Antragsteller sowie die Gültigkeit der Identitätsdokumente des Antragstellers. Anschliessend kann der Antragsteller das beglaubigte Formular an die RA senden. Diese erstellt die Signatureinheit und sendet sie dann zusammen mit dem zugehörigen Passwort an den Antragsteller.



Antrag für ein **qualifiziertes** digitales Zertifikat
Natürliche Person – Privatzertifikat mit Beglaubigung

Information	Pflicht	Im Zertifikat enthalten
Zertifikatstyp	[ ] qualifiziertes elektronisches Zertifikat [ ] Verschlüsselungs-Zertifikat für eMails	*Bitte ankreuzen*
Vorname		JA zwingend
Nachname		JA zwingend
Titel		[ ] Ja [ ] Nein
Mittelname		[ ] Ja [ ] Nein
Pseudonym		[ ] Ja [ ] Nein
Wohnort: Strasse und Hausnummer		NEIN
Wohnort: Postleitzahl und Ort		NEIN
Heimatland		NEIN
Telefon Fixnet		NEIN
Telefon Natel		NEIN
Email-Adresse		JA zwingend
Art des Identifikationsdokuments	☐ Pass ☐ ID ☐ gültiger Ausländerausweis	*Bitte ankreuzen*
Dokumentennummer		NEIN
Pass/ID Ausstellungsland		JA zwingend
Pass/ID Gültigkeit (gültig bis….)		NEIN
Geburtsdatum		JA zwingend
Geburtsort / Heimatort		NEIN
Transaktionen		
Maximal verpflichtende Transaktionssumme in CHF		Wenn eine Angabe erfolgt, wird diese im Zertifikat aufgenommen und beschränkt die Verpflichtung auf diese Summe

Authentifizierungselemente		
Wie heisst ihre Mutter zum Vornamen?		Diese Angaben verwenden wir zur Identifizierung, wenn Sie eine Sperrung oder eine Zustellung des PUK anfordern.

Der Unterzeichnende bestätigt, ***die Nutzungsbestimmungen der Swisscom vom 17.2.2006*** mit der Unterzeichnung dieses Antrages erhalten zu haben.

Ort/Datum: ………………………… Unterschrift: …………………………

Weiteres Vorgehen:

- ☐ Ausgefülltes Antragsformular von einer Einwohnergemeinde beglaubigen lassen. Sie haben persönlich bei der Kanzlei einer Gemeinde vorzusprechen und sich mit folgenden Ausweispapieren (*Führerausweis genügt nicht*) auszuweisen:
  - Gültiger Pass
  - Gültige Identifikationskarte
  - Gültiger Ausländerausweis

  Vergessen Sie nicht, dieses Dokument, auf welchem die Beglaubigung angebracht werden soll, mitzunehmen.
- ☐ Anschliessend beglaubigtes Antragsformular mit einer Kopie Ihres Passes (oder ID oder Ausländerausweis) einsenden an:

  FSDZ Rechtsanwälte
  Digitale Signaturen
  Artherstrasse 23a
  6300 Zug

Beglaubigung der Unterschrift

Mit der Beglaubigung einer Unterschrift wird die **Echtheit dieser Unterschrift auf einer Privaturkunde** bezeugt. Die Wirkung der Beglaubigung besteht in der verstärkten Beweiskraft; sie erbringt für die Echtheit der Unterschrift vollen Beweis, solange nicht die Unrichtigkeit der Beglaubigung nachgewiesen ist (Art. 9 ZGB). Die beglaubigende Person darf eine Unterschrift nur beglaubigen, wenn sie
a) vor ihr gezeichnet oder
b) sie ihr vom Unterzeichner persönlich als die seine bezeichnet
worden ist. Die beglaubigende Person kann nur beurkunden, was sie selbst festgestellt hat. Ist der Unterzeichner der beglaubigenden Person nicht persönlich bekannt, vergewissert sie sich mit einem amtlichen Ausweis über die **Identität** des Unterzeichners. Sie prüft den Ausweis insbesondere nach Rechtsnatur, Gültigkeit, vergleicht das Passfoto mit dem Aussehen der erschienenen Person und vollzieht eine angemessene Kontrolle der anderen Merkmalsbeschreibungen und Personalangaben.

Die unterzeichnende Behörde bezeugt die Echtheit der Unterschrift auf dieser Privaturkunde.

Ort/Datum: ………………………… **Beglaubigungsbehörde:** …………………………

Prüfungsvermerk der Registrierungsstelle

☐ Unterlagen geprüft

Ort/Datum: ………………………… **RA-Officer** …………………………

Abbildung 3: Antragsformular für Beglaubigung durch Gemeindebehörde; herunterzuladen bei www.e-comtrust.ch/signatur

2.1.1 Verifikation

Die Prüfung der Identitätsdokumente ist von grösster Bedeutung, damit die Identität des Antragstellers anlässlich der Registrierung erfasst und die Korrektheit der Angaben im Zertifikat sichergestellt werden können. Die korrekte Durchführung dieses Prozessschrittes gehört zur Sorgfaltspflicht der RA.

Folgende Unterlagen sind zwingend vom Antragsteller vorzulegen:

- Vollständig ausgefüllter Antrag
- Ausweisdokument (Personalausweis, Identitätskarte oder Ausländerausweis)
- Unterzeichneter Vertrag für die Zertifikatsnutzung
- Handelsregisterauszug und Vollmacht bei der Vertretung von juristischen Personen

Die Dokumente werden von der RA auf Echtheit überprüft. Nur bei sicherer Identifikation der Dokumente auf Echtheit darf ein Zertifikat ausgestellt werden.

2.1.2 Registrierungsverfahren

Alle vorgelegten Ausweise und Dokumente werden eingescannt. Bei den Ausweisdokumenten werden alle relevanten Seiten eingescannt: bei der ID beide Seiten, beim Pass oder Ausländerausweis die Hauptseite; wenn dieser bereits verlängert worden ist, zusätzlich die aktuel-