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

Voraussetzungen für die Aufnahme in die Empfehlungsliste der a.trust

Version: 1.0

Datum: 11.02.2005

Inhaltsverzeichnis

© A-Trust GmbH 02/2005

1 Einleitung

1.1 Zweck des Dokuments

Dieses Dokument richtet sich an Hersteller von Komponenten und Verfahren, die zur Erstellung sicherer digitaler Signaturen gem. Signaturgesetz Verwendung finden sollen.

1.2 Haftung der a.trust

a.trust haftet als Zertifizierungsdiensteanbieter für die Sicherheit der digitalen Signatur, die mit den von ihr empfohlenen Komponenten und Verfahren erstellt wurde. Diese Haftung ist einerseits mit einem erheblichen finanziellen Risiko verbunden und andererseits steht auch der Ruf der a.trust als Zertifizierungsdiensteanbieter auf dem Spiel. Vorfälle, die geeignet sind, das Vertrauen in die Zertifizierungsdienste der a.trust zu mindern, sind mit einer erheblichen Imageschädigung in der Öffentlichkeit gleichzusetzen.

Daher ist es für a.trust absolut notwendig, dass die von ihr empfohlenen Komponenten und Verfahren die gem. Signaturgesetz und –verordnung notwendige Sicherheit und Qualität aufweisen. Diese kann nur dadurch gewährleistet werden, dass die entsprechenden Prüfungen unter Beiziehung einer Bestätigungsstelle erfolgen, sodass dem § 18 des [SigG] entsprochen werden kann.

1.3 Gesetzliche Grundlagen

Die Basis für die Empfehlungen der a.trust als Komponenten und Verfahren, die für die sichere digitale Signaturerstellung geeignet sind, bilden das Signaturgesetz und die dazu ergangene Signaturverordnung.

In diesem Abschnitt finden Sie die wesentlichen Passagen aus diesen Rechtsvorschriften aufgelistet.

© A-Trust GmbH 02/2005

Signaturgesetz (siehe [SigG])

§ 18 Technische Komponenten und Verfahren für sichere Signaturen

(5) Die technischen Komponenten und Verfahren für die Erstellung sicherer elektronischer Signaturen müssen nach dem Stand der Technik hinreichend und laufend geprüft sein. Die Erfüllung der Sicherheitsanforderungen nach diesem Bundesgesetz und den auf seiner Grundlage ergangenen Verordnungen muss von einer Bestätigungsstelle (§ 19) bescheinigt sein. Bescheinigungen von Stellen, die von anderen Mitgliedstaaten der Europäischen Union oder von anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum zur Beurteilung der Sicherheitsanforderungen für sichere Signaturerstellungseinheiten nach Art. 3 Abs. 4 der Signaturrichtlinie namhaft gemacht wurden, sind den Bescheinigungen einer Bestätigungsstelle gleich zu halten.

(6) Entsprechen technische Komponenten und Verfahren den allgemein anerkannten Normen, die von der Europäischen Kommission nach Art. 3 Abs. 5 der Signaturrichtlinie festgelegt werden, so gelten die entsprechenden Sicherheitsanforderungen nach diesem Bundesgesetz und den auf seiner Grundlage ergangenen Verordnungen als erfüllt.

§ 19 Bestätigungsstelle

(1) Die nach diesem Bundesgesetz und den auf seiner Grundlage ergangenen Verordnungen einer Bestätigungsstelle zugewiesenen Aufgaben können nur von einer dazu geeigneten Einrichtung wahrgenommen werden.

(2) Eine Einrichtung ist zur Wahrnehmung der einer Bestätigungsstelle zugewiesenen Aufgaben geeignet, wenn sie

1. die erforderliche Zuverlässigkeit aufweist,
2. zuverlässiges Personal mit den für diese Aufgaben erforderlichen Fachkenntnissen, Erfahrungen und Qualifikationen, insbesondere mit Kenntnissen über elektronische Signaturen, angemessene Sicherheitsverfahren, Kryptographie, Kommunikations- und Chipkartentechnologien sowie die technische Begutachtung solcher Komponenten, beschäftigt,
3. über ausreichende technische Einrichtungen und Mittel sowie eine ausreichende wirtschaftliche Leistungsfähigkeit verfügt und
4. die erforderliche Unabhängigkeit, Unparteilichkeit und Unbefangenheit sicherstellt.

(3) Darüber hinaus sind für die Eignung einer Bestätigungsstelle die von der Europäischen Kommission nach Art. 3 Abs. 4 der Signaturrichtlinie festgelegten Mindestkriterien für die Benennung von Bestätigungsstellen maßgeblich. Der Bundeskanzler

© A-Trust GmbH 02/2005

hat diese Kriterien im Einvernehmen mit dem Bundesminister für Justiz mit Verordnung kundzumachen.

(5) Eine Bestätigungsstelle kann zur Erfüllung der ihr nach diesem Bundesgesetz oder der auf seiner Grundlage ergangenen Verordnungen zugewiesenen Aufgaben von anderen Einrichtungen oder Stellen Prüfberichte zu technischen Komponenten und Verfahren einholen.

§ 23 Haftung der Zertifizierungsstellen

(2) Ein Zertifizierungsdiensteanbieter, der sichere elektronische Signaturverfahren bereitstellt, haftet zudem dafür, daß für die von ihm bereitgestellten oder als geeignet bezeichneten Produkte, Verfahren und sonstigen Mittel für die Erstellung elektronischer Signaturen sowie für die Darstellung zu signierender Daten nur technische Komponenten und Verfahren nach § 18 verwendet werden.

(3) Der Zertifizierungsdiensteanbieter haftet nicht, wenn er nachweist, daß ihn und seine Leute an der Verletzung der Verpflichtungen nach den Abs. 1 und 2 kein Verschulden trifft. Kann der Geschädigte als wahrscheinlich dartun, daß die Verpflichtungen nach den Abs. 1 und 2 verletzt oder die zur Einhaltung der Sicherheitsanforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen getroffenen Vorkehrungen kompromittiert wurden, so wird vermutet, daß der Schaden dadurch verursacht wurde. Diese Vermutung ist widerlegt, wenn der Zertifizierungsdiensteanbieter als wahrscheinlich dartut, daß der Schaden nicht durch eine Verletzung bzw. Kompromittierung der im zweiten Satz genannten Verpflichtungen und Vorkehrungen verursacht wurde.

(5) Die Haftung eines Zertifizierungsdiensteanbieters nach Abs. 1 bis 3 kann im vorhinein weder ausgeschlossen noch beschränkt werden.

Signaturverordnung (siehe [SigV])

§ 9 Prüfung der technischen Komponenten und Verfahren

(1) Bei der Prüfung der technischen Komponenten und Verfahren für die Erzeugung sicherer Signaturen sind Sicherheitsvorgaben anzuwenden, die von einer Bestätigungsstelle (§ 19 SigG) als geeignet anerkannt sind. Hiebei können insbesondere Schutzprofile (Protection Profiles) herangezogen werden, die nach den "Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria for Information Security Evaluation - ISO/IEC 15408)" oder nach den "Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (Information Technology Security Evaluation Criteria - ITSEC)" erstellt

© A-Trust GmbH 02/2005

wurden. Das Gleiche gilt für die Prüfung von vertrauenswürdigen Systemen, Produkten und Verfahren, die für die Erstellung von qualifizierten Zertifikaten, für die Speicherung von Signaturerstellungsdaten für qualifizierte Zertifikate oder für sichere Zeitstempeldienste eingesetzt werden.

(2) Bei den Prüfungen nach Abs. 1 sind insbesondere Referenznummern zu beachten, die im Amtsblatt der Europäischen Gemeinschaften nach Art. 3 Abs. 5 der Signaturrichtlinie 1999/93/EG für sichere Signaturerstellungseinheiten (Secure Signature-Creation Devices - SSCD) oder vertrauenswürdige Systeme oder Produkte des Zertifizierungsdiensteanbieters veröffentlicht wurden.

(3) Wenn technische Komponenten und Verfahren in einer kontrollierten Umgebung eingesetzt werden, können Sicherheitsanforderungen, die nach Abs. 1 technisch sichergestellt werden müssen, auch organisatorisch durch Einsatz qualifizierten und vertrauenswürdigen Personals oder technisch-organisatorisch durch Einsatz geeigneter Zugriffs- und Zutrittskontrollmaßnahmen erfüllt werden. Die Erfüllung dieser Sicherheitsanforderungen ist durch eine Bestätigungsstelle zu prüfen.

(4) In der Bescheinigung der Bestätigungsstelle über die Erfüllung der Sicherheitsanforderungen für technische Komponenten und Verfahren für die Erzeugung sicherer Signaturen (§ 18 Abs. 5 SigG) ist anzugeben, für welche Anwendungen, unter welchen Einsatzbedingungen und bis zu welchem Zeitpunkt sie gilt. Ausfertigungen der Bescheinigung und allfällige Prüfberichte sind der Aufsichtsstelle zu übermitteln.

Mit einer weiteren Verordnung (siehe [A-SIT-VO]) wurde die Eignung des Vereins "Zentrum für sichere Informationstechnologie – Austria (A-SIT)" als Bestätigungsstelle festgestellt.

Die Europäische Kommission hat eine Liste von notifizierten Bestätigungsstellen herausgegeben, die unter
http://europa.eu.int/information_society/eeurope/2002/action_plan/safe/esignatures/text_en.htm
einzusehen ist. In dieser Liste befindet sich auch A-SIT als einzige österreichische Bestätigungsstelle.

© A-Trust GmbH 02/2005

2 Aufnahme von Software in die Empfehlungsliste

2.1 Secure Viewer und vertrauenswürdige Datenformate

Unter Secure Viewer zur sicheren Anzeige versteht man Produkte (Software), die gewährleisten, dass nur die dem Signator dargestellten Daten auch tatsächlich signiert werden. Damit verbunden ist auch die Verwendung spezieller empfohlener Dokumentenformate, die von diesen Produkten sicher angezeigt werden können und zugrunde liegender Datenformate, mit denen verhindert wird, dass z. B. für den Signator unsichtbare Daten von ihm unwissentlich signiert werden können. Ein weiterer Bestandteil der Softwarekomponenten zur sicheren Signaturerstellung ist die korrekte Implementierung der zulässigen Hashverfahren.

Einige grundsätzliche und wesentliche technische Requirements an die Secure Viewer-Software sind von a.trust definiert worden. Sie können dem Anhang A des gegenständlichen Dokuments entnommen werden.

2.2 Existenz einer Bescheinigung gem. § 18 SigG

Wenn eine aktuelle Bescheinigung einer Bestätigungsstelle (A-SIT) ausgestellt wurde bzw. ein gleichwertiges Dokument wie ein Sicherheitszertifikat (z. B. von einer deutschen Bestätigungsstelle wie BSI), dann sind die Regelungen des § 18 [SigG] als eingehalten anzusehen.

2.3 Das Produkt ist noch nicht bescheinigt

Der Hersteller einer Software zur sicheren Anzeige muss mit a.trust in einen Dialog eintreten und die Software vorführen sowie ausnahmslos alle technischen Spezifikationen und Beschreibungen inkl. der Benutzerdokumentation und der verwendeten Dokumentenformate an a.trust übergeben.

© A-Trust GmbH 02/2005

Wenn die Überprüfung der Dokumentation durch a.trust eine grundsätzliche Eignung ergibt und aus a.trust-Sicht nichts gegen eine Verwendbarkeit als sichere Signaturerstellungskomponente spricht, wird durch a.trust in Absprache mit dem Hersteller eine Bescheinigung von A-SIT eingeholt, mit der bestätigt wird, dass die Software tatsächlich gem. § 18 (5) [SigG] zur Erstellung einer sicheren digitalen Signatur geeignet ist. Es kann, wenn der Hersteller das vorzieht, auch eine andere dem Signaturgesetz entsprechende Bestätigungsstelle gewählt werden.

Ergeben die Prüfungen, dass die Software nicht geeignet erscheint, dann ist der Hersteller angehalten, die Software gem. den Empfehlungen von a.trust zu verändern. Durch die vorherige Prüfung der Eignung durch a.trust soll verhindert werden, dass ein Hersteller einer Software, die nicht geeignet ist, die kostspielige Überprüfung durch die Bestätigungsstelle mit negativem Ergebnis durchführen lässt.

Trotzdem steht dem Hersteller natürlich immer frei, auf eigene Veranlassung eine Bescheinigung von A-SIT anzufordern. a.trust wird die Bescheinigung einer Bestätigungsstelle, die die Eignung der Software bestätigt, als verbindlich betrachten.

Die Kosten für die Bescheinigung trägt der Hersteller, wenn er sie selbst in Auftrag gegeben hat, aber auch, wenn a.trust sie in Absprache mit ihm beauftragt hat.

Weigert sich ein Hersteller, die Überprüfung gem. § 18 (5) [SigG] erstellen zu lassen sowie die Kosten dafür zu tragen und den Prozess fachlich korrekt zu begleiten, dann wird das Produkt nicht in die Empfehlungsliste aufgenommen, da a.trust in diesem Falle ohne Bescheinigung keine Haftung dafür übernehmen kann und das finanzielle Risiko zu hoch ist.

© A-Trust GmbH 02/2005

3 Aufnahme von Hardware in die Empfehlungsliste

3.1 Sichere Signaturerstellungseinheit

Die sichere Signaturerstellungseinheit (Smartcard) ist die zentrale Komponente für die Erstellung einer sicheren digitalen Signatur. Um diese Eignung festzustellen und zu bestätigen, ist eine Bescheinigung gem. § 18 (5) [SigG] unabdingbar. Die Eigenschaften der Bescheinigung hinsichtlich der Gültigkeit, die in Kapitel 4 angeführt sind, müssen zutreffen.

3.2 Chipkartenleser

Auch um die Eignung des Chipkartenlesers festzustellen und zu bestätigen, ist eine Bescheinigung gem. § 18 (5) [SigG] notwendig. Derartige Bescheinigungen bzw. Zertifizierungen geeigneter Bestätigungsstellen sind für Kartenleserhersteller üblicherweise ohnedies bereit zu stellen, zumal die für die sichere digitale Signaturerstellung verwendeten Kartenleser auch anderen sicheren Anwendungen (z. B. gem. HBCI-Standard) genügen sollen. Die Eigenschaften der Bescheinigung, die in Kapitel 4 angeführt sind, müssen wiederum zutreffen.

© A-Trust GmbH 02/2005

4 Eigenschaften von Bescheinigungen/Zertifizierungen

Eine Bescheinigung/Zertifizierung muss grundsätzlich gültig sein. Wenn sie abgelaufen ist, dann muss nachgewiesen werden, dass eine Verlängerung bereits beantragt wurde. Wenn noch keine Bescheinigung vorliegt, dann muss ebenfalls der Antrag nachgewiesen werden und bestätigt sein, dass aus Sicht der Bestätigungsstelle nichts gegen die Bescheinigung spricht. Es muss a.trust gegenüber glaubhaft gemacht werden können, dass der Antragsteller fachlich und wirtschaftlich in der Lage ist, den Bescheinigungsprozess erfolgreich abzuschließen.

Wenn eine neue Version einer Komponente erstellt wird und sich sicherheitsrelevante Veränderungen darin befinden, dann gilt für den veränderten Teil dasselbe wie für das gesamte Produkt. Die Spezifikationen müssen a.trust vorgelegt werden und die Prüfung durch die Bestätigungsstelle muss über den veränderten Teil stattfinden. Findet kein Upgrade der Bescheinigung/Zertifizierung statt, dann verbleibt die ursprüngliche Version der Komponente in der Empfehlungsliste, die neue Version wird allerdings nicht empfohlen.

© A-Trust GmbH 02/2005

5 Veröffentlichungen in der Empfehlungsliste

Hinsichtlich der Veröffentlichung der Zusatzinformationen zu den Software-Komponenten zur sicheren Anzeige, müssen Formvorschriften definiert und eingehalten werden, um die Empfehlungsliste übersichtlich zu gestalten.

Diese Formvorschriften betreffen insb. die detaillierten Informationen über die verwendeten Datenformate zur sicheren Anzeige.

1) Ein Link zum Download der Software
   (auf der Hersteller- oder der a.trust-Homepage, je nach Vereinbarung/Vertrag).

2) Ein Link zum Download des Benutzerhandbuchs
   (Hersteller und a.trust Homepage)

3) Ein Link zum Download der detaillierten Informationen und Spezifikationen der verwendeten und erlaubten Dokumentenformaten
   (Hersteller und a.trust Homepage).

Die Links müssen unverändert bleiben. Wenn die Links doch geändert werden, dann muss das a.trust vorher angekündigt werden, damit die Änderung rechtzeitig berücksichtigt werden kann.

Die Dokumente müssen auch a.trust in digitaler Form zur Verfügung gestellt werden – immer in der aktuellen Form, damit a.trust sie ggf. selbst auch veröffentlichen und bei Bedarf auch eine Historie der Benutzerhandbücher und Dokumentenformate führen kann, damit Signaturen im gesetzlichen Rahmen auch zu einem späteren Zeitpunkt noch überprüft werden können.

Es wird vorausgesetzt, dass die Hersteller einer Publikation von öffentlichen Dokumenten wie Benutzerhandbuch und Beschreibung der Dokumentenformate durch a.trust zustimmen.

© A-Trust GmbH 02/2005

6 Anhang

A Technische Requirements für Secure Viewer

PIN-Verifikation und PIN-Änderung

Implementiert die gegenständliche Software eine PIN-Verifikation oder eine PIN-Änderung, so sind folgende Anforderungen zu erfüllen:

Verwendung eines Lesers mit PIN-PAD

Zur Verifikation oder Änderung der PIN für die sichere Signatur („Signatur-PIN“) ist dem Karteninhaber die Verwendung eines Lesers mit PIN-PAD zu ermöglichen.

Anzeige des PIN-Typs

Im Zuge der Verifikation einer PIN ist dem Karteninhaber der Typ der einzugebenden PIN (Signatur-PIN, Geheimhaltungs-PIN, Infobox-PIN) anzuzeigen.

Zusätzlich ist die Länge der einzugebenden PIN anzuzeigen.

Beispiele:

Bitte geben Sie Ihre 6-8stellige Signatur-PIN ein. (STARCOS, CARDOS)
Bitte geben Sie Ihre 6stellige Signatur-PIN ein. (ACOS)
Bitte geben Sie Ihre 4stellige Geheimhaltungs-PIN ein. (STARCOS, ACOS, CARDOS).
Bitte geben Sie Ihre 4stellige Infobox-PIN ein. (ACOS).

PIN-Länge bei ACOS Karten

Bei ACOS Karten hat die Software die Länge der Signatur-PIN, die vom Karteninhaber eingegeben oder gewählt werden kann, auf 6 Stellen festzulegen.

Bei Verwendung der CT-API / CT-BCS Schnittstelle ist dies in den Kommandos **PERFORM VERIFICATION** bzw. **MODIFY VERIFICATION DATA** über das „*Control byte for user authentication*“ festzulegen. Dieses Byte ist auf X“61“ zu setzen (Länge der PIN = 6 Stellen, Format ASCII)

© A-Trust GmbH 02/2005

Zugriff auf Infoboxen

Implementiert die gegenständliche Software Zugriffe auf Infoboxen, so sind folgende Anforderungen zu erfüllen:

Default-Infobox-PIN bei ACOS

ACOS-basierende Karten enthalten eine Infoxbox-PIN für das Lesen oder Schreiben der Infobox-Daten. Diese PIN ist im Auslieferungszustand auf „0000“ gesetzt.

Die Client Software darf bei Zugriff auf eine mit Default-PIN versehene Karte keine PIN-Eingabe durch den Kunden verlangen.

Das Feststellen, ob die Karte mit einem Default-Infobox-PIN ausgestattet ist, kann mittels Präsentieren des Default-Wertes mit einem VERIFY-Kommando erfolgen.

Dabei sollte durch geeignete Maßnahmen verhindert werden, dass die Infobox-PIN unbeabsichtigt (durch mehrmaliges Präsentieren des Default-Wertes an eine Karte mit bereits geänderter Infobox-PIN) gesperrt wird.

© A-Trust GmbH 02/2005

B Dokumentengeschichte

Version	Datum	Autor	Änderungen
0.1	09.02.2005	Romana Stangl	Draft-Version
1.0	11.02.2005	Romana Stangl	Anhang techn. Requirements eingefügt

C Referenzdokumente

REF	TITEL
[SigG]	Bundesgesetz über elektronische Signaturen (Signaturgesetz - SigG), BGBl. I Nr. 190/1999, BGBl. I Nr. 137/2000, BGBl. I Nr. 32/2001, BGBl. I Nr. 152/2001
[SigV]	Verordnung über elektronische Signaturen (Signaturverordnung – SigV), BGBl. II Nr. 30/2000, BGBl. II Nr. 527/2004
[A-SIT-VO]	Verordnung über die Feststellung der Eignung des Vereins „Zentrum für sichere Informationstechnologie – Austria (A-SIT)“ als Bestätigungsstelle, BGBl II 2000/31

© A-Trust GmbH 02/2005