Bestätigung
für technische Komponenten
gemäß § 14 (4) Gesetz zur digitalen Signatur und §§ 16 und 17 Signaturverordnung

debis Systemhaus Information Security Services GmbH
- Zertifizierungsstelle debisZERT-

Rabinstraße 8
53111 Bonn

bestätigt hiermit, daß

SafeGuard Sign&Crypt, Version 2.0

der

Utimaco Safeware AG
Dornbachstr. 30, 61440 Oberursel

den nachfolgend beschriebenen Anforderungen des Artikels 3 des Gesetzes zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Gesetz zur digitalen Signatur) vom 01. August 1997 bzw. der Signaturverordnung vom 01. November 1997 entspricht und bei sachgemäßem Einsatz im Wirkungsbereich der genannten Rechtsvorschriften eingesetzt werden kann.

Die Dokumentation zu dieser Bestätigung ist unter

debisZERT.02018.TE.03.1999

registriert.

Bonn, den 19.04.1999 gez.

(Dr. Heinrich Kersten)

debis Systemhaus Information Security Services GmbH –Zertifizierungsstelle- ist, gemäß der Veröffentlichung im Bundesanzeiger Nr. 31 vom 14. Februar 1998, Seite 1787, zur Erteilung von Bestätigungen für technische Komponenten gemäß § 14 Abs. 4 des Gesetz zur digitalen Signatur ermächtigt.

Die Bestätigung zur Registrierungsnummer debisZERT.02018.TE.03.1999 besteht aus 5 Seiten.

Beschreibung der technischen Komponente:

1. Handelsbezeichnung der technischen Komponente und Lieferumfang

Gegenstand dieser Bestätigung ist die technische Komponente SafeGuard Sign&Crypt, Version 2.0, in deren Lieferumfang folgendes enthalten ist:

- SafeGuard Sign&Crypt Software,
- CardMan Chipkarten-Lesegerät, und zwar alternativ nach Kundenwunsch
  - CardMan Chipkarten-Lesegerät für die serielle Schnittstelle oder
  - CardMan Compact Chipkarten-Lesegerät für die serielle Schnittstelle oder
  - CardMan Mobile PC-Card (PCMCIA) Chipkarten-Lesegerät oder
  - CardMan Keyboard,
- ein Integritätsprüfprogramm,
- SafeGuard Sign&Crypt User's Manual (Benutzerhandbuch in gedruckter Form) sowie ergänzende Informationen auf einer Diskette.

2. Funktionsbeschreibung

2.1 Allgemein

SafeGuard Sign&Crypt ist ein Produkt, das die Erzeugung und Verifizierung digitaler Signaturen und die Darstellung einer sicheren Dokumentenanzeige auf PC des Industriestandards ermöglicht.

Das Produkt benötigt die Plattformen Microsoft Windows 95 oder Microsoft Windows NT 4.0.

Das Produkt beinhaltet eine Komponente zur sicheren *Anzeige* zu signierender Daten, eine Teilkomponente zur *Erzeugung* von digitalen Signaturen, eine Komponente zur *Prüfung* digitaler Signaturen (s. Abschnitt 2.2) sowie ein Chipkarten-Lesegerät. Für die Erzeugung gesetzeskonformer digitaler Signaturen ist die Verwendung einer gesetzeskonformen Chipkarte erforderlich, die nicht im Produktumfang enthalten ist. Das Produkt unterstützt z.Zt. die Chipkarten

- SLE CR80S mit dem Betriebssystem TCOS und 768-bit RSA und
- SLE 44CR80S mit dem Betriebssystem CardOS mit 1024-bit RSA.

Zusätzlich zu den Anforderungen aus SigG / SigV kann das Produkt Daten bei der Übertragung durch Einsatz symmetrischer Verschlüsselung gegen den Verlust der Vertraulichkeit schützen; diese Funktion ist aber nicht Gegenstand dieser Sicherheitsbestätigung.

2.2 Funktionen im Sinne des Gesetz zur digitalen Signatur bzw. Signaturverordnung

Die Anforderungen an die hier betrachteten Komponenten ergeben sich aus §16 (2) Satz 1, 2, 3, 5 und 6 und §16 (3) Satz 1, 2, 3, 4 und 6 der Signaturverordnung:

„(2) Die zur Erzeugung oder Prüfung digitaler Signaturen erforderlichen technischen Komponenten müssen so beschaffen sein, daß aus der Signatur nicht der private Signaturschlüssel errechnet oder die Signatur auf andere Weise gefälscht werden kann. Der private Signaturschlüssel darf erst nach Identifikation des Inhabers durch Besitz und Wissen angewendet werden können und bei der Anwendung nicht preisgegeben werden. (...) Die zum Erfassen von Identifikationsdaten erforderlichen technischen Komponenten müssen so beschaffen sein, daß sie die Identifikationsdaten nicht preisgeben und diese nur auf dem Datenträger mit dem privaten Signaturschlüssel gespeichert werden. Sicherheitstechnische Veränderungen an den technischen Komponenten müssen für den Nutzer erkennbar werden.

(3) Die zum Darstellen zu signierender Daten erforderlichen technischen Komponenten müssen so beschaffen sein, daß die signierende Person die Daten, auf die sich die Signatur erstrecken soll, eindeutig bestimmen kann, eine digitale Signatur nur auf ihre Veranlassung erfolgt und diese vorher eindeutig angezeigt wird. Die zum Prüfen signierter Daten erforderlichen technischen Komponenten müssen so beschaffen sein, daß die prüfende Person die Daten, auf die sich die digitale Signatur erstreckt, sowie den Signaturschlüssel-Inhaber eindeutig feststellen kann und die Korrektheit der digitalen Signatur zuverlässig geprüft und zutreffend angezeigt wird. Die technischen Komponenten zum Nachprüfen von Zertifikaten müssen eindeutig erkennen lassen, ob die nachgeprüften Zertifikate im Verzeichnis der Zertifikate zu einem angegebenen Zeitpunkt vorhanden und nicht gesperrt waren. Die technischen Komponenten müssen nach Bedarf den Inhalt der zu signierenden oder signierten Daten hinreichend erkennen lassen. (....) Sicherheitstechnische Veränderungen an den technischen Komponenten müssen für den Nutzer erkennbar werden.“

3. Beschreibung der Anforderungen an die Einsatzumgebung

3.1 Technische Einsatzumgebung

Das Produkt benötigt einen Standard PC mit Intel Pentium Prozessor (60 MHz) oder höher und genügend Ressourcen zur Installation des Produktes (s. Benutzerhandbuch). Für die Chipkarten-Lesegeräte CardMan (seriell) oder CardMan Compact oder CardMan Keyboard benötigt der PC eine freie serielle Schnittstelle, für CardMan Mobile wird zumindest eine der vier verfügbaren seriellen Port-Verbindungen benötigt. Weitere Hardware-Anforderungen bestehen nicht.

Software-seitig benötigt das Produkt als Betriebssystem-Plattform Windows 95 oder Windows NT 4.0 (Workstation oder Server). Das Produkt unterstützt insbesondere die Dokumentenformate folgender Applikationsprogramme:

- Microsoft Word 95 (=Word for Windows Version 7.0) und Microsoft Word 97,
- Microsoft Exchange Version 4.0,
- Microsoft Outlook.

Desweiteren werden alle Applikationen unterstützt, die das Standard Windows Print Interface nutzen.

3.2 Organisatorische Einsatzumgebung und sachgemäßer Einsatz

Der Anwender hat beim Einsatz des Produktes SafeGuard Sign&Crypt folgende organisatorische Auflagen zu beachten:

- Die Räumlichkeiten, in denen der PC mit dem installierten Produkt aufgestellt ist, ist gegen unbefugten Zutritt zu sichern; alternativ kann der PC durch Einsatz eines zertifizierten Sicherheitsproduktes mit einer sicheren Identifikation und Authentisierung abgesichert werden.

- Das Produkt muß mit folgenden Parametern installiert werden: auszuwählende Hash-Funktion ist RIPEMD-160 oder SHA-1; die CardMan Unterstützung ist zu aktivieren; die Option “geheime Schlüssel der Chipkarte nutzen” ist zu wählen.

- Die Nutzung des Produktes (und der erforderlichen Chipkarte) ist auf die Personen zu beschränken, die signierte Dokumente erzeugen oder empfangen dürfen.

- Falls der betreffende PC mit einem Netz (z.B. dem Internet) verbunden ist, muß der Nutzer dafür Sorge tragen, daß durch die Verbindung die Integrität des Produktes (Software-Anteile) und seiner technischen Einsatzumgebung nicht beeinträchtigt wird, insbesondere

  - soll die Konfiguration des installierten Produktes nicht geändert werden,

  - soll keine Software auf dem PC installiert werden, die nicht hinreichend vertrauenswürdig ist,

  - sollen keine Netzapplikationen (Internet Browser etc.) simultan zur Nutzung des Produktes laufen,

  - soll die Integrität der Software-Anteile des Produktes mit dem mitgelieferten Integritätsprüfprogramm geprüft werden, sobald zwischen der letzten Integritätsprüfung und der erneuten Nutzung eine Verbindung mit einem Netz bestanden hat.

4. Eingesetzte Algorithmen und Parameter mit Gültigkeit

Die folgenden vom Produkt verwendeten Algorithmen und Parameter sind für Verwendung bei gesetzeskonformen digitalen Signaturen durch die Regulierungsbehörde für Telekommunikation und Post freigegeben, und zwar

- Hash-Algorithmen RIPEMD-160 und SHA-1 bis 31.12. 2003,

- asymmetrische Verschlüsselungsalgorithmen RSA 1024-Bit bis 31.12.2003 und RSA 768-Bit bis 31.12.2000.

Die asymmetrischen Verschlüsselungsalgorithmen werden im Produkt lediglich bei der *Prüfung* von empfangenen Signaturen verwendet.

Andere Funktionen der hier betrachteten technischen Komponente sind von Vorgaben in SigG bzw. SigV hinsichtlich der Verwendung bestimmter Algorithmen und Parameter nicht betroffen.

Diese Sicherheitsbestätigung ist gültig bis zum 31.12.2003; sie kann jedoch verlängert werden, wenn zu diesem Zeitpunkt keine neuen Erkenntnisse hinsichtlich der Sicherheit der technischen Komponente oder der Algorithmen vorliegen.

5. Prüfstufe und Mechanismenstärke

Den gesetzlichen Vorgaben entsprechend sind die hier betrachteten Komponenten gemäß der Evaluationsstufe E2 und der Mechanismenstärke „hoch“ evaluiert worden.

6. Hinweis

Die als Bestandteil des Produktes ausgelieferten Chipkarten-Lesegeräte wurden bereits unter der Registriernummer debisZERT.02013.TE.05.1998 getrennt (evaluiert und) sicherheitsbestätigt. Alle in der diesbezüglichen Sicherheitsbestätigung enthaltenen Auflagen und Einsatzbedingungen sind in Abschnitt 3 dieser Sicherheitsbestätigung logisch enthalten.

Auch wenn die Gültigkeit der Sicherheitsbestätigung debisZERT.02013.TE.05.1998 auf den 15.9.2003 beschränkt ist, bestehen seitens der Bestätigungsstelle keine Bedenken, für das Produkt SafeGuard Sign&Crypt als Ganzes den Gültigkeitszeitraum für die vorliegende Sicherheitsbestätigung auf den 31.12.2003 festzulegen.

Ende der Sicherheitsbestätigung zu debisZERT.02018.TE.03.1999.