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 Software Development Kit 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.02019.TE.05.1999

registriert.

Bonn, den 13.07.1999 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.02019.TE.05.1999 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 Software Development Kit Version 2.0, in deren Lieferumfang folgendes enthalten ist:

- SafeGuard Sign&Crypt Version 2.0,
- CryptWare Client Server API (CCS API) Support Software (ausgeliefert als SafeGuard Sign&Crypt SDK),
- SafeGuard Sign&Crypt User's Guide (Benutzer-Dokumentation),
- SafeGuard Sign&Crypt SDK Technical Reference Manual (Technisches Referenz-Dokument),
- SafeGuard Sign&Crypt SDK Programmer's Guide for Secure Applications (Programmieranleitung).

2. Funktionsbeschreibung

2.1 Allgemein

Das SafeGuard Sign&Crypt Software Development Kit Version 2.0 ist eine Funktionsbibliothek und beinhaltet als Kern Teile des unter debisZERT.02018.TE.03.1999 sicherheitsbestätigten Produktes SafeGuard Sign&Crypt Version 2.0.

Das SafeGuard Sign&Crypt Software Development Kit Version 2.0 stellt eine Schnittstelle für Anwendungsprogramme bereit. Damit können Anwendungsprogramme u.a. die Funktionen „Erzeugung und Verifizierung digitaler Signaturen“ aus SafeGuard Sign&Crypt Version 2.0 nutzen.

Gegenstand dieser Sicherheitsbestätigung sind die beiden genannten Funktionen „Erzeugung und Verifizierung digitaler Signaturen“.

Das SafeGuard Sign&Crypt Software Development Kit Version 2.0 kann desweiteren von Software-Entwicklern genutzt werden: Die Programmieranleitung und die technische Referenz-Dokumentation beschreiben Vorgehensweisen und geben Hinweise, wie sichere Anwendungen mit Hilfe von SafeGuard Sign&Crypt Software Development Kit Version 2.0 zu erstellen sind. Resultierende Anwendungen sind aber nicht Gegenstand dieser Sicherheitsbestätigung; sie sind vielmehr stets zu evaluieren, wenn eine SigG-Konformität angestrebt wird oder erforderlich ist.

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 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 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

SafeGuard Sign&Crypt Software Development Kit Version 2.0 und Anwendungen, die mit Hilfe dieses Produktes entwickelt wurden, laufen auf PC des Industriestandards (mit mindestens Pentium- oder dazu kompatiblem Prozessor).

Für die Nutzung von Chipkarten benötigt der PC einen freien Port für den Anschluß der Chipkarten-Lesegeräte CardMan / CardMan Compact. Das CardMan Keyboard benötigt einen seriellen Port für den Anschluß des Lesers. Für CardMan Mobile wird kein freier serieller Port benötigt, es sollte jedoch einer der vier zur Verfügung stehenden seriellen Port-Anschlüsse frei sein.

Für einen sicheren Betrieb ist eine der folgenden Chipkarten erforderlich:

- SLE CR80S mit T-COS Betriebssystem und 768-Bit RSA auf der Karte oder
- SLE 44CR80S mit CardOS Betriebssystem und 1024-Bit RSA auf der Karte.

Software-seitig benötigt das Produkt als Betriebssystem-Plattform Windows 95 oder Windows NT 4.0 (Workstation oder Server).

Die Funktionen der Funktionsbibliothek können von allen Anwendungsprogrammen aufgerufen werden, die 32-bit Windows DLL Funktionen ansteuern können.

Für die Entwicklung von Anwendungen unterstützt SafeGuard Sign&Crypt Software Development Kit Version 2.0 die folgenden Plattformen:

- alle ANSI kompatiblen, unter Windows 95 oder Windows NT lauffähigen C Compiler,
- Microsoft VisualBasic und
- Borland (Inprise) DELPHI Pascal Entwicklungsumgebung.

3.2 Organisatorische Einsatzumgebung und sachgemäßer Einsatz

Der End-Anwender hat beim Einsatz des Produktes folgende organisatorische Auflagen zu beachten:

- Das Anwendungsprogramm muß eine Anzeigekomponente besitzen, die gemäß den gesetzlichen Vorgaben sicherheitsbestätigt ist.
- Die verwendete Chipkarte muß gemäß den gesetzlichen Vorgaben sicherheitsbestätigt sein.
- Die Räumlichkeiten, in denen der PC mit dem installierten Produkt aufgestellt ist, sind 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 alternativ wie folgt konfiguriert werden:
- MailTrusT V. 1.0 Protokoll mit SHA-1 oder RIPEMD-160, oder
- S / MIME Protokoll mit SHA-1.
- Alle Auflagen an die Einsatzumgebung aus debisZERT.02018.TE.03.1999 sind zu beachten.

Der Programmierer hat für die Erstellung von sicheren Anwendungen die Auflagen aus dem „SafeGuard Sign&Crypt SDK Programmer's Guide for Secure Applications“ zu beachten. Anwendungen, die Signaturgesetz-konform sein sollen, benötigen eine Evaluierung und Sicherheitsbestätigung gemäß SigG / SigV.

4. Eingesetzte Algorithmen und Parameter mit Gültigkeit

Die folgenden von der Funktionsbibliothek in SafeGuard Sign&Crypt Software Development Kit Version 2.0 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 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

In Ergänzung der seinerzeit nach *E2, hoch* durchgeführten Evaluierung von SafeGuard Sign&Crypt Version 2.0 (debisZERT.02018.TE.05.1999) wurde SafeGuard Sign&Crypt Software Development Kit Version 2.0 als Ganzes nach E2 evaluiert. Soweit Komponenten geprüft wurden, die nicht für das Signaturgesetz relevant sind, lag dabei die Mechanismenstärke „mittel“ zugrunde. Alle nach SigG relevanten Komponenten (s. Abschnitt 2.1) besitzen dagegen die Mechanismenstärke „hoch“.

Ende der Sicherheitsbestätigung zu debisZERT.02019.TE.05.1999.