Bestätigung

von Produkten für qualifizierte elektronische Signaturen gemäß §§ 15 Abs. 7 und 17 Abs. 4 Gesetz über Rahmenbedingungen für elektronische Signaturen und § 11 Abs. 3 Verordnung zur elektronischen Signatur

TÜV Informationstechnik GmbH
- ein Unternehmen der TÜV NORD Gruppe -
Zertifizierungsstelle
Langemarckstraße 20

45141 Essen

bestätigt hiermit gemäß
§ 15 Abs. 7 Satz 1 Signaturgesetz[1] sowie § 11 Abs. 3 Signaturverordnung[2], dass die

Signaturanwendungskomponente
DATEV Anwenderkomponente GERVA
Version 1.33

den nachstehend genannten Anforderungen des SigG und der SigV entspricht.

Die Dokumentation zu dieser Bestätigung ist unter

TUVIT.93122.TU.09.2005

registriert.

Essen, 23.09.2005

gez. Dr. Gruschwitz
Zertifizierungsstelle

TÜV Informationstechnik GmbH ist, gemäß der Veröffentlichung im Bundesanzeiger Nr. 52 vom 17. März 1999, Seite 4142 und gemäß § 25 Abs. 3 SigG, zur Erteilung von Bestätigungen für Produkte für qualifizierte elektronische Signaturen gemäß § 15 Abs. 7 und § 17 Abs. 4 SigG ermächtigt.

---

[1] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz – SigG) vom 16.05.2001 (BGBl. I S. 876) geändert durch Erstes Gesetz zur Änderung des Signaturgesetzes (1. SigÄndG) vom 04.01.2005 (BGBl. I S. 2)

[2] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) vom 16.11.2001 (BGBl. I S. 3074) geändert durch 1. SigÄndG

Die Bestätigung zur Registrierungsnummer TUVIT.93122.TU.09.2005 besteht aus 8 Seiten.

Beschreibung des Produktes:

1 Handelsbezeichnung des Produktes und Lieferumfang:

DATEV Anwenderkomponente GERVA Version 1.33[3]

Auslieferung:
Als Signaturanwendungskomponente an Endanwender auf einer einmal beschreibbaren CD-ROM (und ggf. zusätzlich auf einem USB-Stick)

Hersteller:
DATEV eG
Paumgartnerstraße 6-14
90429 Nürnberg

2 Funktionsbeschreibung

GERVA ist eine Signaturanwendungskomponente gemäß § 2 Nr. 11 SigG, die elektronische Daten dem Prozess der Erzeugung qualifizierter elektronischer Signaturen durch eine SigG-konform personalisierte DATEV e:secure-Card zuführen kann. Die qualifizierten elektronischen Signaturen können unter Nutzung des Zeitstempeldienstes des Zertifizierungsdiensteanbieters DATEV mit einem Zeitstempel versehen werden. Zusätzlich können mit GERVA erzeugte qualifizierte elektronische Signaturen und qualifizierte Zertifikate auf ihre Gültigkeit hin überprüft und die Ergebnisse der Überprüfung angezeigt werden. GERVA bietet hierzu die Möglichkeit, den Zertifikatstatus online bei einem OCSP-Verzeichnisdienst abzufragen.

OCSP-Anfragen beim Verzeichnisdienst der BNetzA erfolgen nicht, so dass die Gültigkeit der Signaturen und Zertifikate nicht vollständig überprüft werden kann. Für eine vollständige Prüfung muss die Gültigkeit der Zertifikate im Verzeichnisdienst der BNetzA anderweitig überprüft werden.

Zur Prüfung der Gültigkeit von Zertifikaten kann entweder eine online-Prüfung bei einem OCSP-Verzeichnisdienst des DATEV Zertifizierungsdienstes oder eine offline-Prüfung gegen die lokale Zertifikatsdatenbank von GERVA durchgeführt werden. Bei der online-Zertifikatsprüfung wird die aktuelle Systemzeit oder soweit vorhanden die Zeitangabe aus dem Zeitstempel bei der Prüfung der Signatur als Prüfzeitpunkt verwendet. Bei der offline-Zertifikatsprüfung wird die aktuelle Systemzeit verwandt. Bei gesperrten Zertifikaten ist aus der Antwort erkennbar, zu welchem Zeitpunkt die Sperrung erfolgt ist.

Neben den oben beschriebenen Funktionen zum Signieren und zum Prüfen von Signaturen im Sinne des Signaturgesetzes bietet GERVA noch weitere Funktionen zum Ver- und Entschlüsseln, Komprimieren, Signieren mit nicht SigG-konformen Signaturkarten und zur Signaturprüfung von nicht qualifizierten Signaturen. Diese zusätzlichen Funktionalitäten sind **nicht** Gegenstand dieser Bestätigung.

[3] Im folgenden kurz mit GERVA bezeichnet.

GERVA kann sowohl in der Einzelplatzversion als auch in einer Windows Terminal Server (WTS)-Umgebung eingesetzt werden.

Auf einem **Einzelplatzrechner** können von GERVA elektronische Daten dem Prozess der Erzeugung qualifizierter elektronischer Signaturen zugeführt und damit mit Hilfe von Chipkartensystemen (Chipkartenleser und personalisierte Chipkarte als sichere Signaturerstellungseinheit) mit einer qualifizierten elektronischen Signatur versehen sowie erstellte Signaturen verifiziert werden.

In der **WTS-Umgebung** werden die selben Funktionalitäten zur Verfügung gestellt. Im Unterschied zur Einzelplatzversion prägt GERVA in der WTS-Umgebung eine Client-Server Architektur, wobei GERVA als Anwendung auf einem Terminal-Server (WTS-Server) ausgeführt wird und ein Anwender über seinen Terminal Server Client (WTS-Client) diese Anwendung nutzen kann. Dabei werden die Bildschirmdaten vom WTS-Server zum WTS-Client übertragen. Der WTS-Client liefert Tastatureingaben wie auch Mausbewegungen an den WTS-Server zurück. Der WTS-Client präsentiert dem Anwender über ein Bildschirmfenster die gewohnte grafische Windows-Benutzeroberfläche der GERVA-Anwendung und ermöglicht ihm die Interaktion mit der auf dem Server ausgeführten Applikation. Die Aufbereitung der zu signierenden Daten (insbes. die Hashwertbildung) erfolgt auf dem WTS-Server, die Signaturerstellung erfolgt mit dem Chipkartensystem am WTS-Client.

3 Erfüllung der Anforderungen des Signaturgesetzes und der Signaturverordnung

3.1 Erfüllte Anforderungen

GERVA erfüllt die Anforderungen nach § 17 Abs. 2 Satz 1 (eindeutige Anzeige und Feststellbarkeit der Daten bei Signaturerzeugung), 2 (Feststellbarkeit der Daten, des Unverändertseins der Daten, der Zuordnung zum Signaturschlüssel-inhaber, des Inhalts des qualifizierten Zertifikats und des Ergebnisses der Nachprüfung von Zertifikaten bei Signaturprüfung) sowie 3 (bei Bedarf Anzeige des Inhalts der zu signierenden oder signierten Daten) SigG und nach § 15 Abs. 2 Satz 1 (keine Preisgabe der Identifikationsdaten, Signatur nur durch berechtigt signierende Person, eindeutige Anzeige der Signatur vor Erzeugung) und 2 (korrekte Prüfung der Signatur und eindeutige Erkennbarkeit der Gültigkeit der Zertifikate) sowie Abs. 4 (Erkennbarkeit von sicherheitstechnischen Veränderungen) SigV.

3.2 Einsatzbedingungen

Dies gilt unter der Voraussetzung, dass folgende Einsatzbedingungen gewährleistet sind:

Grundlage dieser Bestätigung ist der Einsatz von GERVA in einem ***geschützten Einsatzbereich***. Für den sicheren Einsatz von GERVA und zur Verhinderung von erfolgreichen Angriffen mit den Zielen, dass:

- Daten signiert werden, die nicht signiert werden sollen,
- das Prüfergebnis der Signatur- bzw. Zertifikatprüfung falsch angezeigt wird,

- die Geheimhaltung des Identifikationsmerkmals (PIN) nicht gewährleistet ist,

sind die folgenden Auflagen zu beachten:

3.2.1 Auflagen zur Anbindung an das Internet

Eine Netzverbindung (z. B. mittels Modem, ISDN oder LAN-Anschluss) zum Verzeichnisdienst des Zertifizierungsdienstes DATEV eG ist für die Prüfung der Gültigkeit von Zertifikaten notwendig. Diese Netzverbindung muss so abgesichert sein, z. B. durch eine geeignet konfigurierte Firewall, dass online Angriffe aus dem Internet auf den eingesetzten Personalcomputer erkannt bzw. unterbunden werden. Beim Einsatz von GERVA in der WTS-Umgebung mit Anbindung an das Internet muss gesichert sein, dass online Angriffe auf den Server erkannt bzw. unterbunden werden.

3.2.2 Auflagen zur Anbindung an ein Intranet

Wenn der eingesetzte Personalcomputer in der Einzelplatzversion oder als WTS-Client in einem Intranet betrieben wird, so muss diese Netzverbindung geeignet abgesichert sein, so dass online Angriffe aus dem Intranet auf den Computer erkannt bzw. unterbunden werden. Beim Einsatz von GERVA in der WTS-Umgebung mit Anbindung an das Intranet muss gesichert sein, dass online Angriffe auf den Server erkannt bzw. unterbunden werden.

3.2.3 Auflagen zur Sicherheit der IT-Plattform und Applikationen

Der Benutzer von GERVA muss sich davon überzeugen, dass keine Angriffe von dem Personalcomputer und den dort vorhandenen Applikationen durchgeführt werden. Beim Einsatz von GERVA in der WTS-Umgebung müssen die Administratoren sicherstellen, dass keine Angriffe auf den Server und die dort vorhandenen Applikationen durchgeführt werden. Insbesondere muss gewährleistet sein, dass:

1. die auf dem Personalcomputer und ggf. dem Server installierte Software weder böswillig manipuliert noch in irgendeiner anderen Form verändert werden kann,

2. auf dem Personalcomputer und ggf. dem Server keine Viren oder Trojanischen Pferde eingespielt werden können,

3. die Hardware des Personalcomputers und ggf. des Servers nicht unzulässig verändert werden kann oder

4. der verwendete Chipkartenleser weder böswillig manipuliert noch in irgendeiner anderen Form verändert wurde, um dadurch Daten (z. B. PIN, zu signierende Daten, Hashwerte, etc.) auszuforschen, zu verändern oder die Funktion anderer Programme unzulässig zu verändern. Dieses kann die in Abschnitt 3.2 angegeben Folgen haben.

Die Integrität der GERVA Installation auf dem Personalcomputer und ggf. auf dem Server ist regelmäßig mit dem auf der CD mitgelieferten Programm PrgInt.exe zu überprüfen. Insbesondere kann das Ausforschen der PIN auf dem Personalcomputer nur bei einem Chipkartenleser mit sicherer PIN-Eingabe ausgeschlossen werden.

3.2.4 Auflagen zur Auslieferung und Installation des Produktes

Die Anwenderkomponente GERVA wird vom Hersteller als Produkt auf einer CD ausgeliefert. Zusätzlich zur CD kann das Produkt auf einem USB-Stick geliefert werden, wobei sich das Integritätsprüfprogramm PrgInt.exe ausschließlich auf der CD befindet.

Die Anwenderkomponente GERVA ist für die folgende technische Einsatzumgebung vorgesehen:

- IBM-kompatibler PC lauffähig mit einem der unten genannten Windows Betriebssysteme, mit Anschlussmöglichkeiten für ein Read-Only-Memory-Laufwerk (z.B. CD-ROM) sowie für einen Chipkartenleser (serielle Schnittstelle oder PCMCIA) und mit einer Netzwerkverbindung

- Betriebssysteme (Arbeitsplatzmodus bzw. WTS-Client):
  Windows 98 Second Edition und Windows 2000, Windows XP Home Edition, Windows XP Professional

- Betriebssysteme (WTS-Server):
  Windows 2000 Server, Windows 2000 Advanced Server, Windows 2003 Server

- Betriebssystemzusatz (WTS-Client bzw. WTS-Server):
  Microsoft High Encryption Pack für 128 Bit Verschlüsselung der WTS-Verbindung

- Klasse 2 Chipkartenleser mit PIN-Pad, der die sichere Eingabe der PIN unterstützt. In die Bestätigungstests wurde der Leser SCM SPR 532 pinpad einbezogen. Es werden funktional jedoch auch andere PC/SC oder CT-API Chipkartenleser an der seriellen oder USB-Schnittstelle unterstützt.

- Personalisierte DATEV Signaturkarte e:secure-Card V1.0 (oder Varianten V1.10 bzw. V1.20) mit einer Schnittstelle nach ISO 7816 und Chipkartenbetriebssystem TCOS V2.0 Release 3 der Deutsche Telekom AG

- Netzwerkverbindung zu einem DATEV Zertifizierungsdiensteanbieter (Verzeichnisdienst und Zeitstempeldienst)

Eine Übertragung der Evaluationsergebnisse auf andere Plattformen ist nicht möglich, sondern erfordert ggf. eine Reevaluation. Die Signaturanwendungskomponente GERVA darf deshalb ausschließlich in der oben beschriebenen Hard- und Softwareumgebung eingesetzt werden. Nach der Installation muss die Integritätsprüfung mit dem Programm PrgInt.exe vorgenommen werden.

3.2.5 Auflagen zum Schutz vor manuellem Zugriff Unbefugter

Der Personalcomputer und bei Einsatz in der WTS-Umgebung auch der Server, auf dem GERVA verwendet wird, sowie der verwendete Chipkartenleser müssen gegen eine unberechtigte Benutzung gesichert sein, damit:

1. die auf dem Personalcomputer und ggf. auf dem Server installierte Software weder böswillig manipuliert noch in irgendeiner anderen Form verändert werden kann,

2. auf dem Personalcomputer und ggf. auf dem Server keine Viren oder Trojanischen Pferde eingespielt werden können,

3. die Hardware des Personalcomputers und ggf. die des Servers nicht unzulässig verändert werden kann oder

4. der verwendete Chipkartenleser weder böswillig manipuliert noch in irgendeiner anderen Form verändert wird, um dadurch Daten (z. B. PIN, zu signierende Daten, Hashwerte, etc.) auszuforschen, zu verändern oder die Funktion anderer Programme unzulässig zu verändern. (siehe auch Abschnitt 3.2.3).

Die Unterrichtung durch den Zertifizierungsdiensteanbieter zur Handhabung der Signaturkarte ist zu beachten.

Beim Einsatz von GERVA in der WTS-Umgebung muss sich der Server-Rechner in einer zutrittsgeschützten Einsatzumgebung innerhalb eines verschließbaren und versiegelten Elektroschrankes befinden.

3.2.6 Auflagen zum Schutz vor Angriffen über Datenaustausch per Datenträger

Bei Einspielung von Daten über Datenträger muss gewährleistet werden, dass

1. die installierte Software weder böswillig manipuliert noch in irgendeiner anderen Form verändert werden kann und

2. keine Viren oder Trojanischen Pferde eingespielt werden können,

um dadurch Daten (z. B. PIN, zu signierende Daten, Hashwerte, etc.) auszuforschen, zu verändern oder die Funktion anderer Programme unzulässig zu verändern. (siehe auch Abschnitt 3.2.3)

3.2.7 Auflagen zur Sicherheitsadministration des Betriebes

Eine Sicherheitsadministration des Betriebes von GERVA ist nicht vorgesehen. Eine vertrauenswürdige Administration des Personalcomputers sowie der Internet- bzw. Intranetanbindung muss jedoch sichergestellt werden. Bei Einsatz von GERVA in der WTS-Umgebung muss zusätzlich eine vertrauenswürdige Administration des Servers im 4-Augen-Prinzip gewährleistet sein.

3.2.8 Auflagen zum Schutz vor Fehlern bei Betrieb/Nutzung

Folgende Auflagen sind für den sachgemäßen Einsatz von GERVA zu beachten:

- Für eine vollständige Prüfung der Zertifikatskette muss zusätzlich auf anderem Wege überprüft werden, ob die verwendeten Zertifikate der Zertifizierungsstelle im Verzeichnisdienst der BNetzA vorhanden und nicht gesperrt sind, da hierfür keine online-Prüfung angeboten wird.

- Die authentischen Root CA- und CA-Zertifikate müssen durch den Anwender bereitgestellt sein.

- Es wird eine vertrauenswürdige Eingabe der PIN vorausgesetzt. Der Benutzer hat dafür Sorge zu tragen, dass die Eingabe der PIN weder beobachtet wird noch dass die PIN anderen Personen bekannt gemacht wird.

- Zur Nutzung der GERVA-API dürfen nur vertrauenswürdige externe Applikationen verwandt werden.

- Die Einstellung der Systemzeit des Personalcomputers und ggf. des Servers muss korrekt sein.

- Bei Nutzung eines Terminal Server Clients muss sichergestellt sein, dass dieser über eine entsprechende Netzwerkanbindung verfügt, die es ihm ermöglicht, den Server zu kontaktieren.

- Die Integritätsprüfung mit dem Programm PrgInt.exe ist regelmäßig vorzunehmen.

Folgende Hinweise aus dem Evaluierungsbericht zum Schutz der Einsatzumgebung sind zu beachten:

- Nur bei dem Betrieb eines bestätigten PIN-Pad Lesers im PIN-Pad Modus ist sichergestellt, dass die PIN nur zur SmartCard übertragen wird,

- die GERVA Einstellungen können durch andere Computernutzer auch ohne SmartCard Anmeldung verändert werden,

- nur die qualifizierte Signaturerzeugung über den „GERVA Drucker“ beinhaltet eine sichere Darstellung des Dateiinhalts der zu signierenden Daten,

- für Filesignaturen aus dem Windows Explorer enthält GERVA nur dann eine Referenz auf den Dateinamen, wenn die Anzeige der Statuszeile nicht über „Ansicht – Statuszeile“ abgewählt wurde,

- die GERVA Makros sind verfügbar in Microsoft Word und Microsoft Excel und können nur ausgeführt werden, wenn die Sicherheitseinstellungen für Makros dort unter „Extras – Makros“ nicht auf „hoch“ gesetzt sind.

3.2.9 Anforderungen an das Wartungs-/Reparaturpersonal

Eine Wartung bzw. Reparatur von GERVA ist nicht vorgesehen. Eine Wartung bzw. Reparatur des Personalcomputers ist nur von vertrauenswürdigen Personen durchzuführen. Nach den durchgeführten Arbeiten ist die Integrität des Personalcomputers und aller Applikationen und ggf. des WTS-Servers einschließlich der Integrität von GERVA zu überprüfen (Programm PrgInt.exe auf CD). Beim Einsatz von GERVA in der WTS-Umgebung ist die Administration des Servers im 4-Augen-Prinzip durchzuführen.

3.2.10 Authentisierung des Wartungs-/Reparaturpersonals

Eine Wartung bzw. Reparatur von GERVA ist nicht vorgesehen. Eine Authentisierung des Personals für die Wartung bzw. Reparatur des Personalcomputers und des Servers bei Einsatz von GERVA innerhalb der WTS-Umgebung muss geeignet erfolgen.

3.2.11 Aufbewahrung/Transport der Produkte

GERVA wird vom Hersteller auf einer einmal beschreibbaren CD-ROM und ggf. zusätzlich auf einem USB-Stick auf dem Postweg ausgeliefert. Es ist darauf zu achten, dass die CD-ROM mit dem Integritätsprüfprogramm PrgInt.exe geschützt aufbewahrt werden.

3.3 Algorithmen und zugehörige Parameter

Zur Erzeugung elektronischer Signaturen wird von GERVA die Hashfunktion SHA-1 verwendet.

Die gemäß Anlage 1 Abs. I Nr. 2 SigV festgestellte Eignung reicht mindestens bis Ende des Jahres 2010 (siehe BAnz. Nr. 59 vom 30.03.2005, Seite 4.695).

3.4 Prüfstufe und Mechanismenstärke

Die Signaturanwendungskomponente GERVA Version 1.33 wurde erfolgreich nach der Prüfstufe E2 der ITSEC evaluiert. Die eingesetzten Sicherheitsmechanismen erreichen die Stärke **hoch**.

Ende der Bestätigung