Zentrum für sichere Informationstechnologie – Austria
Secure Information Technology Center – Austria

A-1030 Wien, Seidlgasse 22 / 9
Tel.: (+43 1) 503 19 63–0
Fax: (+43 1) 503 19 63–66

A-8010 Graz, Inffeldgasse 16a
Tel.: (+43 316) 873-5514
Fax: (+43 316) 873-5520

http://www.a-sit.at
E-Mail: office@a-sit.at

DVR: 1035461
ZVR: 948166612
UID: ATU60778947

BESCHEINIGUNG NACH § 18 ABS. 5 SIGG

Sichere Signaturerstellungseinheit CardOS V5.3 QES, V1.0

Antragsteller:
Atos IT Solutions and Services GmbH
Otto-Hahn-Ring 6
81739 München, Deutschland

Bescheinigung ausgestellt am: 08.08.2014
Referenznummer A-SIT-1.108

1. Beschreibung der zu bescheinigenden Komponente

Die zu bescheinigende Komponente ist eine Signaturerstellungseinheit (nachstehend Signaturkarte genannt) bestehend aus:

Hardware:

- Prozessorchip Infineon SLE78CFX*P (M7892 B11[1]) mit 3 Chipgrößen SLE78CFX2400P mit 240kByte Flash, SLE78CFX3000P mit 300kByte Flash und SLE78CFX4000P mit 404kByte Flash; Hersteller: Infineon Technologies AG, 81726 München

Eingebettete Software:

- Betriebssystem CardOS V5.3, Version „C903“; Hersteller: Atos IT Solutions and Services GmbH, 81739 München
- EC-library v.1.02.013, SHA-2-library v.1.01, RSA-library v.1.02.013, Toolbox v.1.02.013[2]; Hersteller: Infineon Technologies AG, 81726 München

Personalisierungsskripts zur Installation der Applikation für qualifizierte elektronische Signaturen (QES):

- ConfigAppRSABase.csf: Skript für QES auf RSA Basis
- ConfigAppECBase.csf: Skript für QES auf ECDSA Basis
- ConfigAppADS.csf: Skript zur Finalisierung der Konfiguration
- Vordefinierte Parameter zur Generierung der Signaturerstellungsdaten:
  - Defines_EC_secp256r1.csf (EC-Schlüsselpaar mit secp256r1)
  - Defines_EC_secp384r1.csf (EC-Schlüsselpaar mit secp348r1)
  - Defines_EC_brainpoolP256r1 (EC-Schlüsselpaar mit brainpoolP256r1)
  - Defines_EC_brainpoolP384r1 (EC-Schlüsselpaar mit brainpoolP384r1)
  - Defines_RSA_2048.csf (RSA-Schlüsselpaar mit 2048 Bit Schlüssellänge)
  - Defines_RSA_2560.csf (RSA-Schlüsselpaar mit 2560 Bit Schlüssellänge)
  - Defines_RSA_3072.csf (RSA-Schlüsselpaar mit 3072 Bit Schlüssellänge)
  - Defines_RSA_3584.csf (RSA-Schlüsselpaar mit 3584 Bit Schlüssellänge)
  - Defines_RSA_4096.csf (RSA-Schlüsselpaar mit 4096 Bit Schlüssellänge)

[1] Der Prozessorchip Infineon IC M7892 B11 wurde vom BSI zertifiziert. Der Zertifizierungsreport BSI-DSZ-CC-0782-2012 vom 11.9.2012 weist der Komponente eine Konformität zum Schutzprofil BSI-CC-PP-0035-2007 (Security IC Platform Protection Profile, Version 1.0, 15 June 2007) sowie die erfolgreiche Evaluierung nach der Prüfstufe EAL6+ (Erweiterung: ALC_FLR.1: Life-cycle support – Basic flaw remediation) aus.
[2] Teil der Zertifizierung BSI-DSZ-CC-0782-2012

Mit der Signaturkarte wird die folgende Dokumentation geliefert:

- CardOS V5.3 Chipcard Operating System, User's Manual
- CardOS V5.3 Chipcard Operating System, Packages & Release Notes
- Administrator Guidance 'CardOS V5.3 QES, V1.0'
- User Guidance 'CardOS V5.3 QES, V1.0'
- ADS Description 'CardOS V5.3 QES, V1.0'

Neben der sicheren Signaturerstellungseinheit (CardOS V5.3 QES) können auf der Signaturkarte weitere Applikationen mit weiteren Schlüsselpaaren und Daten vorhanden sein. Diese zusätzlichen Applikationen sind nicht Gegenstand dieser Bescheinigung.

Die kontaktbasierte Schnittstelle der Signaturkarte ist gemäß ISO/IEC 7816-3 implementiert. Diese Schnittstelle wird benutzt, um APDU-Kommandos zur Signaturkarte zu übertragen und die entsprechenden Antwort-APDUs der Signaturkarte gemäß ISO/IEC 7816-4 und ISO/IEC 7816-8 zu empfangen.

Die Signaturkarte erlaubt die Generierung von kryptografisch starken Signaturen basierend auf RSA oder ECDSA über zuvor extern oder intern (einschließlich Berechnung der letzten Runde auf der Karte) berechnete Hashwerte. Das Signaturschlüsselpaar (Signaturerstellungsdaten/ Signaturprüfdaten) wird auf der Signaturkarte generiert, der verwendete Algorithmus und die zugehörigen Parameter können bei der Konfiguration der Signaturkarte aus den oben angegebenen Definitionen ausgewählt werden. Neben der Auswahl des Algorithmus kann auch konfiguriert werden:

- ob ein PUK zur Verfügung gestellt werden soll oder nicht
- ob der PIN-Fehlbedienungszähler fix oder von der PIN-Länge abhängig sein soll

Die Beschränkung der Nutzung der Signaturerstellungsdaten wird durch einen PIN-Mechanismus realisiert.

Die Signaturkarte wird vor der Auslieferung nicht vollständig konfiguriert, sondern es werden nur die ersten Konfigurationsschritte ausgeführt. Diese Basiskonfiguration beinhaltet den Import von kartenindividuellen (von der Seriennummer des Prozessorchips abhängigen) symmetrischen Schlüsseln, die für Authentisierungszwecke und die Erzeugung des Signaturschlüsselpaares verwendet werden. Nach diesem Schritt ist die Applikation für qualifizierte elektronische Signaturen deaktiviert, da der Wert der Transport-PIN noch nicht importiert wurde und der Transportschutz daher nicht aufgehoben werden kann. Die Signaturkarte wird in diesem Zustand an die Signatorinnen und Signatoren ausgeliefert.

Der zweite Konfigurationsschritt wird durch eine (lokale oder Online-) Registrierungsstelle durchgeführt, nachdem die Karteninhaberin oder der Karteninhaber die Ausstellung eines qualifizierten Zertifikats beantragt hat. Diese Konfiguration der Applikation für qualifizierte elektronische Signaturen umfasst den Export des öffentlichen Schlüssels (Signaturprüfdaten), den Import der Transport-PIN und optional die Generierung bzw. das Update von diversen Files unterhalb des Dedicated Files für die Applikation für qualifizierte elektronische Signaturen. Diese optionalen Files können genutzt werden, um Zertifikate abzuspeichern, beispielsweise das qualifizierte Zertifikat für das Signaturschlüsselpaar und das Zertifikat der CA, die das qualifizierte Zertifikat des Signaturschlüsselpaares erzeugt. Nach diesem Schritt ist die Signaturapplikation vorbereitet und kann durch die Signatorin bzw. den Signator aktiviert werden.

Um diesen zweiten Konfigurationsschritt abzusichern, stellt die Signaturkarte einen Authentisierungsmechanismus für die (lokale oder Online-) Registrierungsstelle bereit. Dieser erfordert eine wechselseitige Authentifizierung zwischen Signaturkarte und der Registrierungsstelle und stellt danach einen durch einen Sitzungsschlüssel abgesicherten vertrauenswürdigen Kanal bereit, der die Konfiguration der Applikation für qualifizierte elektronische Signaturen gegen Manipulation und Offenlegung absichert.

Die Signaturkarte bietet die folgenden notwendigen Funktionalitäten für Komponenten, die bei der Erzeugung elektronischer Signaturen involviert sind:

- Erzeugung der Signaturerstellungsdaten und Signaturprüfdaten
- Erzeugung einer einzelnen elektronischen Signatur
  - nach Erlaubnis der Anzeige der zu signierenden Daten, wobei die Anzeigefunktion durch die Systemumgebung der Signaturkarte bereitgestellt werden muss
  - unter Nutzung geeigneter Hash-Funktionen
  - nach geeigneter Authentisierung der Signatorin bzw. des Signators durch die Signaturkarte
  - nach Übertragung der zu signierenden Daten, des Hashwertes oder des Zwischenwertes plus dem Rest der zu signierenden Daten (Hash Last Round) durch Senden einer entsprechenden APDU
  - unter Nutzung einer geeigneten kryptografischen Signaturfunktion mit den geeigneten kryptografischen Parametern und Schlüssellängen

2. Erfüllung der Anforderungen des SigG[3] und der SigV[4]

Die Signaturkarte erfüllt unter nachstehenden Einsatzbedingungen

- Anforderungen nach § 18 Abs. 1[5] und § 18 Abs. 2 zweiter Satz[6] SigG,
- Anforderungen nach § 18 Abs. 6[7] SigG
- Anforderungen nach § 3 Abs. 1[8] und § 3 Abs. 2[9] SigV und
- Anforderungen nach § 6 Abs. 1[10] und § 6 Abs. 2[11] SigV.

Die Signaturkarte ist daher in folgenden Kategorien bescheinigt:

- Komponenten und Verfahren zur Erzeugung von Signaturerstellungsdaten,
- Komponenten und Verfahren zum Speichern von Signaturerstellungsdaten und
- Komponenten und Verfahren zur Verarbeitung der Signaturerstellungsdaten

3. Gültigkeitsdauer der Bescheinigung

Diese Bescheinigung ist für die Dauer von zwei Jahren ab Datum der Ausstellung gültig.

---

[3] Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG, BGBl I Nr. 190/1999 vom 19.August 1999) in der Fassung des Bundesgesetzes BGBl. I Nr. 75/2010 vom 18. August 2010.

[4] Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung 2008 – SigV 2008, BGBl. II Nr. 3/2008 vom 7. Jänner 2008)) in der Fassung BGBl. II Nr. 401/2010 vom 9. Dezember 2010.

[5] Für die Erzeugung und Speicherung von Signaturerstellungsdaten sowie für die Erstellung qualifizierter Signaturen sind solche technische Komponenten und Verfahren einzusetzen, die die Fälschung von Signaturen sowie die Verfälschung signierter Daten zuverlässig erkennbar machen und die die unbefugte Verwendung von Signaturerstellungsdaten verlässlich verhindern

[6] Die Signaturerstellungsdaten dürfen mit an Sicherheit grenzender Wahrscheinlichkeit nur einmal vorkommen, sie dürfen weiters mit hinreichender Sicherheit nicht ableitbar sein; ihre Geheimhaltung muß sichergestellt sein.

[7] 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.

[8] Die technischen Komponenten und Verfahren zur Verarbeitung der Signaturerstellungsdaten müssen in Hinblick auf das Erfordernis der Prüfung nach § 18 Abs. 5 SigG den Anforderungen des § 6 entsprechen.

[9] Es dürfen nur jene Algorithmen und Parameter eingesetzt werden, die die Anforderungen des Anhangs erfüllen. Die Rahmenbedingungen für die technische Sicherheit sind so zu wählen, dass sie dem jeweiligen Stand der Technik entsprechen.

[10] Bei der Prüfung der technischen Komponenten und Verfahren für die Erzeugung qualifizierter Signaturen sind Sicherheitsvorgaben anzuwenden, die von einer Bestätigungsstelle (§ 19 SigG) als geeignet anerkannt sind. Es 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 wurden. (...)

[11] 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 ZDA veröffentlicht wurden.

4. Einsatzbedingungen

Die Gültigkeit dieser Bescheinigung ist an die im Folgenden angeführten Einsatzbedingungen gebunden:

(1) Die mit der Signaturkarte ausgelieferte Dokumentation (siehe Kapitel 1 dieser Bescheinigung) enthält die notwendigen Anweisungen für den sicheren Gebrauch der Signaturkarte. Zusätzlich sind für den sicheren Gebrauch der Signaturkarte die Annahmen über die Einsatzumgebung im Security Target, sowie das Security Target als Ganzes in Betracht zu ziehen. Diesen Anweisungen und Annahmen sowie den Einsatzbedingungen dieser Bescheinigung ist in geeigneter Weise der Wirkung nach zu entsprechen und es sind die getroffenen Maßnahmen
- durch das Sicherheits- und Zertifizierungskonzept des Zertifizierungsdiensteanbieters entsprechend § 12 SigV sicherzustellen,
- in der Belehrung der Signatorin bzw. des Signators entsprechend zu übernehmen
- und deren Wirkung im Wege der Aufsicht sicherzustellen.

(2) Bei der Generierung der Signaturerstellungsdaten auf der Signaturkarte sind der Signaturalgorithmus und die zugehörigen Parameter so zu wählen, dass diese für die gesamte vorgesehene Einsatzdauer der Signaturkarte den gesetzlichen Anforderungen entsprechen.

(3) Der Hersteller der Betriebssystem-Software (Atos IT Solutions and Services GmbH) und der Hersteller des Prozessorchips (Infineon Technologies AG) müssen die Vertraulichkeit des „*PackageLoadKey*“ gewährleisten.

(4) Neben den in der mit der Signaturkarte ausgelieferten Dokumentation enthaltenen Hinweisen bezüglich der Qualität von PIN und PUK (z.B. Länge, Fehlbedienungszähler, etc.) ist die Signatorin bzw. der Signator dazu aufzufordern, eine nicht triviale PIN zu wählen, wenn die Signaturkarte aktiviert wird.

(5) Für die Konfiguration der Applikation für qualifizierte elektronische Signaturen für ECDSA bzw. RSA ist das Konfigurationsskript *ConfigAppADS.csf* im entsprechenden Verzeichnis (*EcQesCfg* bzw. *RsaQesCfg*) zu verwenden.

5. Algorithmen und zugehörige Parameter

Zur Erstellung einer qualifizierten elektronischen Signatur werden von der Signaturkarte die folgenden Algorithmen bereitgestellt:

- ECDSA[12] nach ANSI X 9.62 bzw. ISO/IEC 15946-2 mit Längen der Parameter p, q von 256 oder 384 Bit. Es werden die Kurven P-256 bzw. P-384 nach FIPS PUB 186-4 sowie brainpoolP256r1 bzw. brainpoolP384r1 nach RFC 5639 unterstützt.
- RSA nach PKCS#1 v2.1 (RFC 3447) mit Schlüssellängen von 2048 bis 4096 Bit.

Zur Berechnung des Hashwertes (inkl. Hash Last Round) werden von der Signaturkarte die Algorithmen SHA-256, SHA-384 und SHA-512 nach FIPS PUB 180-4 bereitgestellt.

Dadurch sind die Anforderungen gemäß § 3 Abs. 2 SigV[13] erfüllt.

6. Prüfstufe und Mechanismenstärke

Es liegt das deutsche IT-Sicherheitszertifkat BSI-DSZ-CC-0921-2014 vor, ausgestellt durch die Zertifizierungsstelle des BSI[14], in Bonn am 06.08.2014. Die materiellen Prüfungen sind im Zertifizierungsbericht *„BSI-DSZ-CC-0921-2014 for CardOS V5.3 QES, V1.0 from Atos IT Solutions and Services GmbH“* beschrieben.

[12] DSA basierend auf einer Gruppe $E(F_p)$
[13] Es dürfen nur jene Algorithmen und Parameter eingesetzt werden, die die Anforderungen des Anhangs erfüllen. Die Rahmenbedingungen für die technische Sicherheit sind so zu wählen, dass sie dem jeweiligen Stand der Technik entsprechen.
[14] Bundesamt für Sicherheit in der Informationstechnik, Godesberger Allee 185-189 - D-53175 Bonn

Das Zertifikat weist der Signaturkarte die Konformität mit dem Schutzprofil „*Protection Profile for Secure Signature Creation Device - Part 2: Device with Key Generation, Version 2.01, January 2012, BSI-CC-PP-0059-2009-MA-01*“[15] sowie eine erfolgreiche Evaluierung nach der Prüfstufe EAL4+ (EAL4 mit Zusatz: AVA_VAN.5[16]) der Common Criteria (CC, Version 3.1) aus.

Die Signaturkarte widersteht in ihrer vorgesehenen Einsatzumgebung einem hohen Angriffspotential.

Unterschriften:

SIGNATURE INFORMATION	**Signatory**	Reinhard Posch
	Issuer-Certificate	CN=a-sign-premium-mobile-03,OU=a-sign-premium-mobile-03,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serial-No.	725452
	Method	urn:pdfsigfilter:bka.gv.at:binaer:v1.1.0
	Parameter	etsi-bka-atrust-1.0:ecdsa-sha256:sha256:sha256:sha1
Verification	Signature verification at: http://www.signature-verification.gv.at	
Date/Time-UTC	2014-08-07T16:10:25Z	

Signaturwert	L8QcYBMAal32EHk1DpDeIc/KnVn4MFvmAmrv+KspCkhq620FvsAXPbg4txyheYBRQgzvaDaBtCwR+tlHn63NWQ==	
SIGNATURINFORMATIONEN	**Unterzeichner**	Manfred Holzbach
	Aussteller-Zertifikat	CN=a-sign-Premium-Sig-02,OU=a-sign-Premium-Sig-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	523847
	Methode	urn:pdfsigfilter:bka.gv.at:binaer:v1.1.0
	Parameter	etsi-moc-1.1:ecdsa-sha256@57ac2503
Prüfinformation	Signaturpruefung unter: http://www.signaturpruefung.gv.at	
Hinweis	Dieses mit einer qualifizierten elektronischen Signatur versehene Dokument ist gemäß § 4 Abs. 1 Signaturgesetz einem handschriftlich unterschriebenen Dokument grundsätzlich rechtlich gleichgestellt.	
Datum/Zeit-UTC	2014-08-08T11:24:02Z	

[15] eine CC Version 3.1 entsprechende Weiterentwicklung des CWA 14169 (Protection Profile for the SSCD Type 3) im „Verzeichnis allgemein anerkannter Normen für Produkte für elektronische Signaturen, die von den Mitgliedsstaaten angenommen werden sollen in Übereinstimmung mit den Anforderungen des Anhangs III der Richtlinie 1999/93/EG.“, veröffentlicht im Amtsblatt der Europäischen Union L 175/45 vom 15.7.2003.

[16] Vulnerability Assessment – Advanced methodical vulnerability analysis