



Informationstag "Elektronische Signatur"

Gemeinsame Veranstaltung von TeleTrust und VOI

Berlin, 17.09.2015

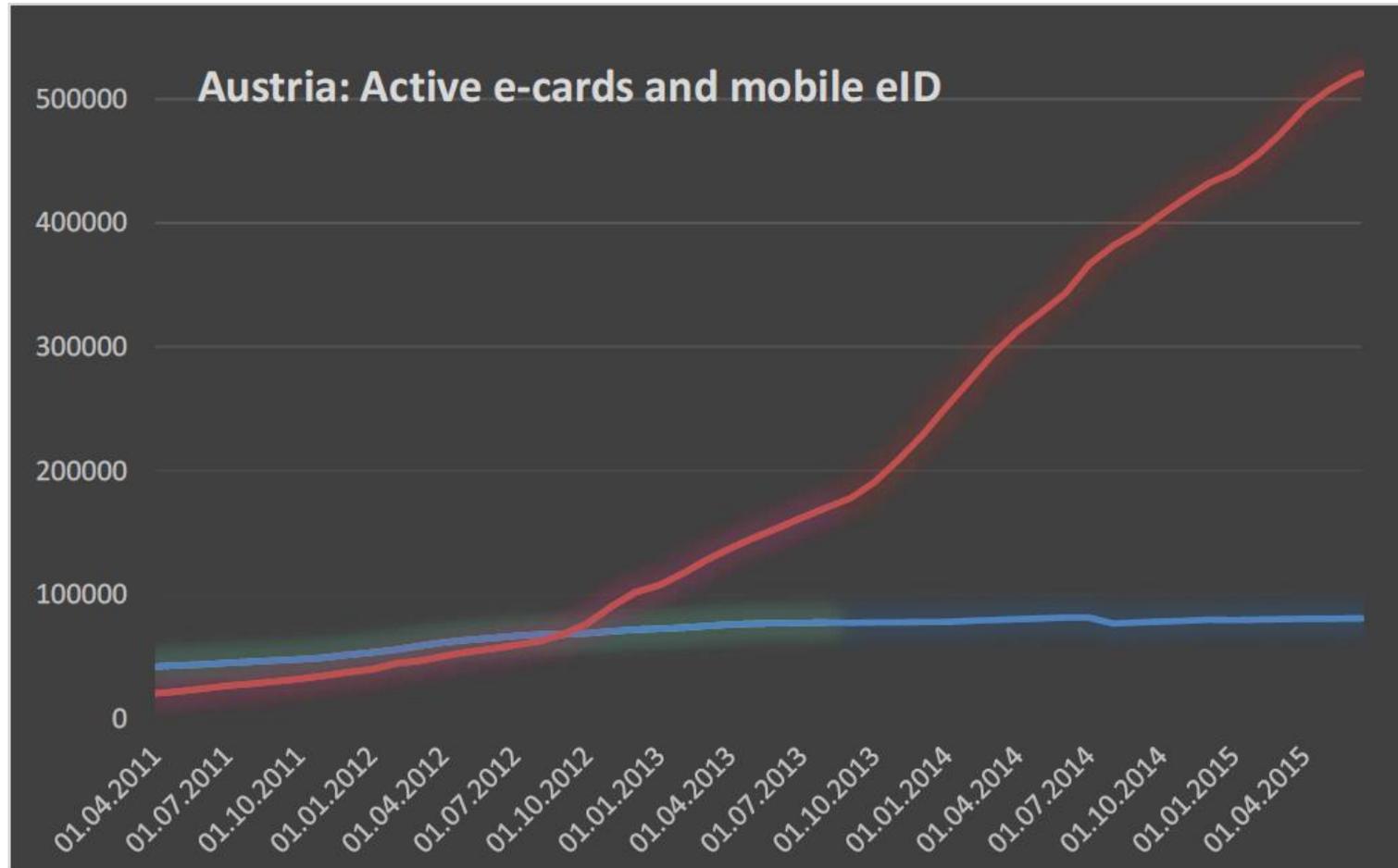
Mobile qualifizierte elektronische Signatur – Fact or Fiction?

Dr. Detlef Hühnlein (ecsec GmbH)

Agenda

- **Motivation**
- Mobilisierung der QES
- Fact or Fiction?

e-cards und Mobile eID in Österreich



Quelle: M. Kubach, H. Leitold, H. Roßnagel, C. H. Schunck, M. Talamo: **SSEDIC.2020 on Mobile eID**, erscheint bei Open Identity Summit 2015, 10.-11. November 2015, Berlin

2015
ISSE

10th & 11th November
Hotel Palace Berlin, Germany
www.isse.eu.com



Countdown: 54 days 11 hours 39 mins

[Home](#) [Programme](#) [Delegates](#) [Speakers for 2015](#) [Supporters](#) [Event Partners](#) [Press](#) [Location](#) [Contact Us](#)

Welcome to ISSE 2015

Co-located with
the Open Identity
Summit 2015

www.openidentity.eu



Click here to
register!



Subscribe to our
mailing list

Click here to download your
Justification letter

ISSE 2015 Programme Topic areas

- Trust Services, eID and Cloud Security
- BYOD and Mobile Security
- Cybersecurity, Cybercrime, Critical Infrastructures

Tweets

[Follow](#)



ISSE conference
@ISSEconference

2 Sep

Nothing like an impromptu conference
brain storm #london #business
#eventmanagement

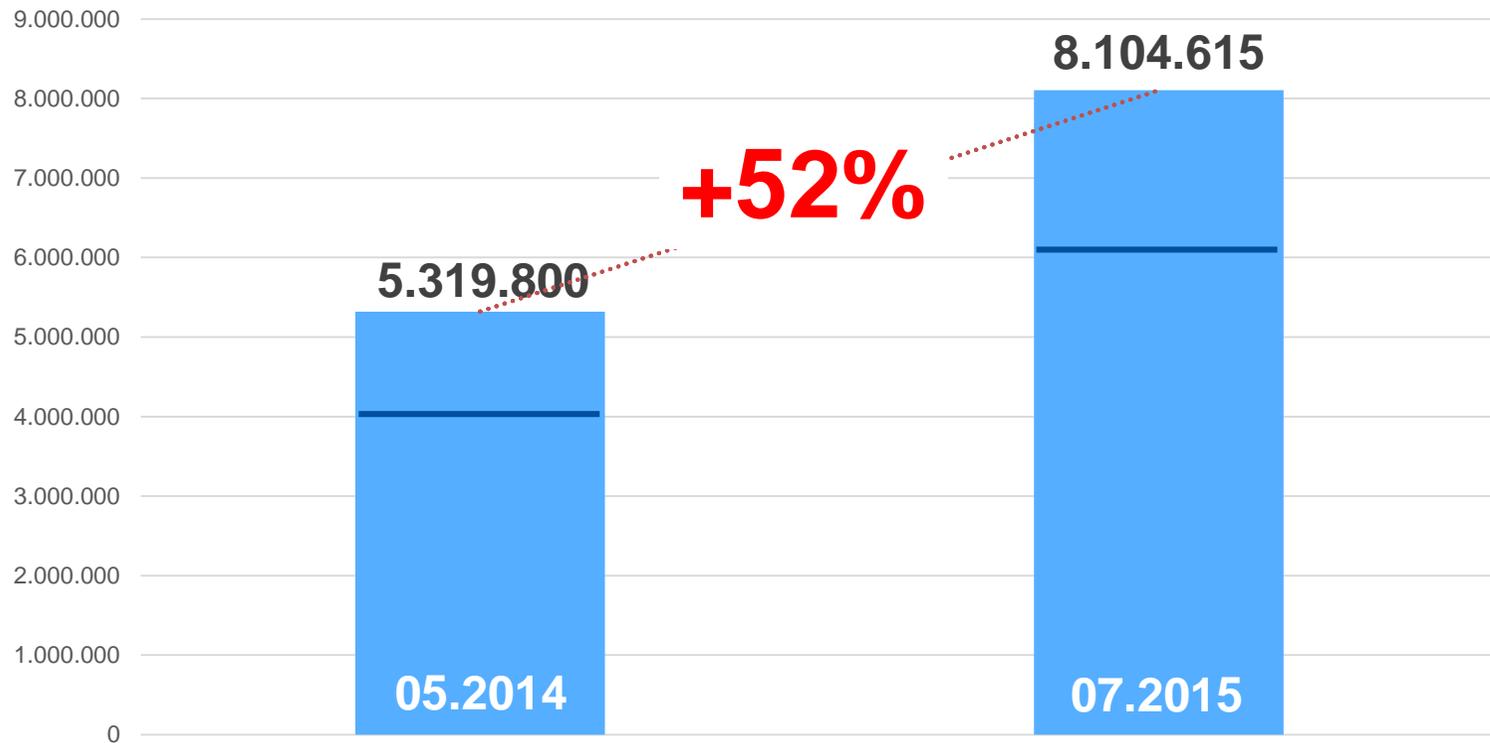
2015
ISSE

Co-locating with



QES in Italien

Anzahl gültiger qualifizierter Zertifikate



Quelle: <http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/firme-elettroniche> (06.08.2015)

eIDAS-Verordnung (2014/910/EU)

I. Allgemeine Bestimmungen (Artikel 1-5)

II. Elektronische Identifizierung (Artikel 6-12)

eIDAS

III. Vertrauensdienste

1. Allgemeine Bestimmungen (Artikel 13-16)

2. Aufsicht (Artikel 17-19)

3. Qualifizierte Vertrauensdienste (Artikel 20-24)

4. Elektronische Signaturen (Artikel 25-34)

5. Elektronische Siegel (Artikel 35-40)

6. Elektronische Zeitstempel (Artikel 41-42)

7. Dienste für die Zustellung elektronischer Einschreiben (Artikel 43-44)

8. Website-Authentifizierung (Artikel 45)

eIDAS

IV. Elektronische Dokumente (Artikel 46)

V. Befugnisübertragungen und Durchführungsbestimmungen (Artikel 47-48)

VI. Schlussbestimmungen (Artikel 49-52)

Agenda

- Motivation

- **Mobilisierung der QES**

- Fact or Fiction?

Rahmenbedingungen für Mobile QES aus SigG / SigV (1)

- § 2 Nr. 3 SigG (QZ+SSEE)
- § 17 Abs. 1 SigG + § 15 Abs. 1 SigV
(Anf. an SSEE = 1999/93/EU Anlage III + ε)
- § 17 Abs. 4 SigG (Bestätigung der SSEE)
- Anlage 1 SigV (CC EAL 4+)

➤ **SSEE = Signaturkarte**
(<http://tinyurl.com/SSEE-BNetzA>)

Rahmenbedingungen für Mobile QES aus SigG / SigV (2)

§ 23 Abs. 3 SigG

(3) **Produkte für elektronische Signaturen**, bei denen in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum festgestellt wurde, dass sie den Anforderungen der Richtlinie 1999/93/EG in der jeweils geltenden Fassung entsprechen, **werden anerkannt**. Den nach § 15 Abs. 7 geprüften Produkten für qualifizierte elektronische Signaturen werden Produkte für elektronische Signaturen aus einem in Satz 1 genannten Staat oder aus einem Drittstaat gleichgestellt, wenn sie nachweislich gleichwertige Sicherheit aufweisen.



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

A-1000 Wien, Seidngasse 22/9 A-1010 Wien, Seidngasse 46a
Tel.: +43 1 503 19 630 Fax: +43 1 503 19 630
Tel.: +43 1 503 19 630 Fax: +43 1 503 19 630

BESCHEINIGUNG NACH § 18 Abs. 5 SigG

Sichere Signaturerstellungseinheit der A-Trust für die mobile Signatur bestehend aus HSM und HSM Server

Antragsteller:
A-Trust Dienstleistungs für Sicherheitsysteme im elektronischen Datenverkehr GmbH
Landstrasser Hauptstraße 5
1030 Wien

Bescheinigung ausgestellt am: 10.07.2014
Referenznummer: A-SIT-1.010

1. Beschreibung der zu bescheinigenden Komponente
Teilkomponenten:
Die Signaturerstellungseinheit besteht aus einem Rechner (HSM-Server), in dem sich ein Hardware Security Modul (HSM) vom Typ "Shield 500e F3" befindet. Dieser Rechner wird in Hochsicherheitsgehäusen des Rechenzentrums der A-Trust in einem Safe betrieben, zu dem nur Sicherheitspersonal der A-Trust Zugriff hat.
Die Funktionalität der mobilen Signatur (Bestellung der zu signierenden Daten, Kontrolle über die Auslösung der Signaturfunktion) ist in dem Programm *HSMServerApplication.exe* implementiert, welches auf dem HSM-Server läuft, und die Funktionen des HSM zur Erzeugung der Signaturerstellungsdaten, zur Erstellung von qualifizierten elektronischen Signaturen und zur Entschlüsselung der gespeicherten Signaturerstellungsdaten nutzt.
Erzeugung und Speicherung der Signaturerstellungsdaten:
Nach der Identifikation der Signatur bzw. des Signaturs müssen von dieser bzw. diesem ihre bzw. seine Mobiltelefonnummer angegeben und ein Signaturpasswort festgelegt werden. Der Nutzer der Mobiltelefonnummer und mittels eines Einmalpassworts, das über eine Verifikations-SMS übermittelt wird, überprüft. Dann werden die Signaturerstellungsdaten im HSM generiert. Die Signaturerstellungsdaten werden durch einen nur im HSM verfügbaren Schlüssel und durch einen vom Signaturpasswort und der Mobiltelefonnummer abgeleiteten Schlüssel verschlüsselt abgespeichert, wodurch die Anwendung der Signaturerstellungsdaten nur innerhalb des HSM und nach Eingabe des Signaturpassworts durch die Signatur bzw. den Signaturer möglich ist.
Signaturerstellung:
Zum Anfügen einer qualifizierten elektronischen Signatur müssen von der Signatur bzw. vom Signatur zuerst Mobiltelefonnummer und Signaturerstellungsdaten in einem Webportal eingegeben werden, woraufhin die Mobiltelefonnummer eine SMS mit einem vom HSM generierten, zeitlich begrenzt gültigen Einmalpasswort und dem Hashwert der zu signierenden Daten gesendet wird. Das Einmalpasswort ist über eine Signatur des HSM mit dem Hashwert der zu signierenden Daten verknüpft. Nach erfolgreicher Prüfung des Einmalpassworts werden im

Modellnr.: HC40320-030, Firmware-Version: 2.08, Serial #: 0100, Modem-ID: 0100, FIPS 140-2 Level 3 (Modem-Identifikation)
Hersteller: PkBox Security, Inc., 200 South First Street, Suite 1117, San Jose, CA 95128, USA
© A-SIT, Partner für Sichere Informationstechnologie

<http://tinyurl.com/SSEE-A-Trust>



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

A-1000 Wien, Seidngasse 22/9 A-1010 Wien, Seidngasse 46a
Tel.: +43 1 503 19 630 Fax: +43 1 503 19 630
Tel.: +43 1 503 19 630 Fax: +43 1 503 19 630

CONFIRMATION PURSUANTO § 18 PAR. 5 SIGG

**Secure Signature Creation Device
PkBox, Version 3.0.3**

Applicant:
Intsig Group SpA
Via Torino 48
I-20123 Milano, Italy

Confirmation issued on: 2015-02-03
Reference number: A-SIT-1.111

Preliminary Remarks
Zentrum für sichere Informationstechnologie – Austria (A-SIT) is declared by the Federal Chancellor's Ordinance B 018 II 31/2000 as a confirmation body pursuant to § 19 of the Austrian Signature Act (Signaturgesetz – SigG), B 018 II 30/1999 as amended by B 018 II 17/2010. A-SIT is notified as a designated body under the European Signature Directive (1999/93/EC) article 3 para. 4.
A-SIT is thus made responsible for confirming the compliance of secure signature creation devices with the security requirements laid down in the Austrian Signature Act as transposition of the Annex III requirements of Directive 1999/93/EC into Austrian legislation.

1. Product Description
PkBox is a product for electronic signatures intended to be used as a Secure Signature Creation Device (SSCD) in a secure operational environment. It implements a Trustworthy System Supporting Server Signing (TWS4S) in accordance with CEN TS 419241:2014. When used in combination with qualified certificate PkBox generates qualified electronic signatures as defined in Directive 1999/93/EC with the legal effects of article 5 para. 1.
Subcomponents:
An HSM device (Dedicated Shield, or nShield Connect) is used as an cryptographic module for the generation and protection of the signature creation data (SCD). The HSM is operated according to its FIPS 140-2 level 3 certification.
The HSM device is accessed only through PkBox CDD ("Credential On Database") which uses a secure mechanism provided by the HSM for storing private keys outside the HSM in a database. The PkBox CDD module is also responsible for the validation of the one-time passwords (OTP) to ensure that the SCD can be reliably protected by the legitimate signatory against the use of others.
The Signature Creation Application (SCA) sends the entire document to be signed either directly to PkBox CDD or uses a PkBox Remote module that is installed in the same IT infrastructure with the SCA. PkBox Remote is then responsible for the last computation and

Firmware Version: 2.08.7.0, Modem/Modem-ID: 0100, Serial #: 02, Modem-ID: 0100, FIPS 140-2 Level 3 (Modem-Identifikation)
Hersteller: PkBox Security, Inc., 200 South First Street, Suite 1117, San Jose, CA 95128, USA
© A-SIT, Secure Information Technology Center – Austria

<http://tinyurl.com/SSCD-PkBox>



Ministero delle Sviluppo Economico
Dipartimento delle Certificazioni e della Tecnologia delle Informazioni

DCSI
Organismo di Certificazione della Sicurezza Informatica

Il Sistema nazionale per la valutazione e la certificazione della sicurezza di sistemi prodotti ICT (SISTEMA) del 30 ottobre 2010 (G.U. n. 254) del 12 aprile 2010.
Organismo designato ai sensi del comma 1 dell'articolo 2 della Direttiva 1999/93/CE nella sua versione attuale, e notified in the name of the state of Italy in accordance with the article 11 della Direttiva stessa, come ente responsabile in Italia per l'accertamento della conformità di un dispositivo di firma a requisiti di sicurezza espressi nell'Allegato III alla suddetta direttiva.

Procedura di Accertamento di Conformità di un Dispositivo per la Creazione di Firme Elettroniche ai Requisiti di Sicurezza Previsti dall'Allegato III della Direttiva 1999/93/CE

Attestato di Conformità n. 2/14

Dispositivo: CoSign v.1.1

Sviluppato da: ARX

Il Dispositivo per la creazione di firme elettroniche indicato in questo attestato è risultato conforme ai requisiti di sicurezza previsti dall'Allegato III della Direttiva 1999/93/CE

Roma, 30 settembre 2014

Il Direttore
Dipartimento delle Certificazioni e della Tecnologia delle Informazioni
Antonio

Il presente Attestato di Conformità è stato emesso dall'Organismo di Certificazione della Sicurezza Informatica (DCSI) su richiesta di un sistema di certificazione di cui al D.L. n. 170 del 2010, n. 62, sezione "Indice dell'attestazione" depositato e pubblicato al ministero delle Infrastrutture e dei Trasporti il 20/09/2014.
La validità del presente Attestato di Conformità è soggetta alle condizioni di alle norme applicative ed al rispetto di: Sicurezza Informatica (DCSI) e CERT (CERT) ed altro allegato che si possono trovare sul sito internet del DCS.

<http://tinyurl.com/SSCD-CoSign>

MOBIIL 




TELE2
MILIEU nakata sokken

TeleTrust Services Ltd. is a registered company in the UK. www.teletrust.com

<http://mobiil.id.ee/>

Rahmenbedingungen für Mobile QES aus SigG / SigV (3)

§ 23 Abs. 1 SigG

(1) **Elektronische Signaturen**, für die ein **ausländisches qualifiziertes Zertifikat** aus einem anderen Mitgliedstaat der Europäischen Union oder aus einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum vorliegt, sind, soweit sie **Artikel 5 Abs. 1 der Richtlinie 1999/93/EG** des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen (ABl. EG 2000 Nr. L 13 S. 2) in der jeweils geltenden Fassung entsprechen, qualifizierten elektronischen Signaturen **gleichgestellt**.

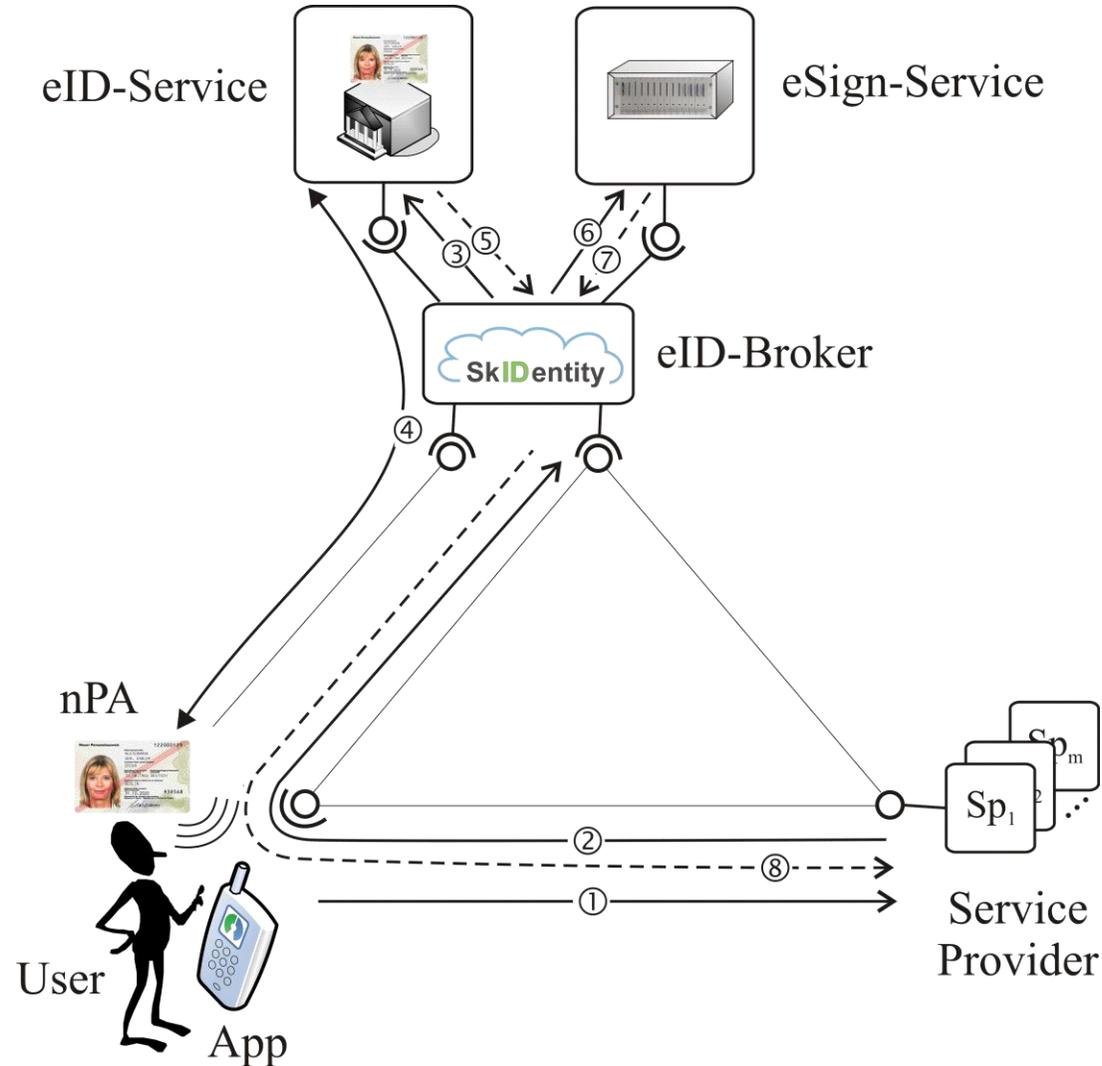


Directory of Signature Creation Devices

Austria		  
		
	A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH	
Italy		  
		
	Actalis S.p.A.	
	Aruba Posta Elettronica Certificata S.p.A.	
	Bank of Italy	

<http://opensignature.org/devices/>

„Bevollmächtigte QES“ http://www.ecsec.de/pub/2012_DuD.pdf



Rahmenbedingungen für Mobile QES aus eIDAS (1)

Artikel 26

Anforderungen an fortgeschrittene elektronische Signaturen

Eine fortgeschrittene elektronische Signatur erfüllt alle folgenden Anforderungen:

- a) Sie ist eindeutig dem Unterzeichner zugeordnet.
- b) Sie ermöglicht die Identifizierung des Unterzeichners.
- c) Sie wird unter Verwendung elektronischer Signaturerstellungsdaten erstellt, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner alleinigen Kontrolle verwenden kann.
- d) Sie ist so mit den auf diese Weise unterzeichneten Daten verbunden, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Rahmenbedingungen für Mobile QES aus eIDAS (2)

Artikel 29

Anforderungen an qualifizierte elektronische Signaturerstellungseinheiten

(1) Qualifizierte elektronische Signaturerstellungseinheiten müssen die Anforderungen des **Anhangs II** erfüllen.

≈

**1999/93/EU Anhang III
+ "Fernsignatur"**

- **EN 419 211 (Part 1-6)**
- **EN 419 221 (Part 1-5)**
- **EN 419 241 (Part 1-3)**

(2) Die Kommission kann im Wege von Durchführungsrechtsakten **Kennnummern für Normen** für qualifizierte elektronische Signaturerstellungseinheiten festlegen. Bei qualifizierten elektronischen Signaturerstellungseinheiten, die diesen Normen entsprechen, wird davon ausgegangen, dass sie die Anforderungen des Anhangs II erfüllen. Diese Durchführungsrechtsakte werden nach dem in Artikel 48 Absatz 2 genannten Prüfverfahren erlassen.

Rahmenbedingungen für Mobile QES aus eIDAS (3)

- (51) Es sollte dem Unterzeichner möglich sein, qualifizierte elektronische Signaturerstellungseinheiten der Obhut eines Dritten anzuvertrauen, sofern angemessene Mechanismen und Verfahren bestehen, die sicherstellen, dass der Unterzeichner die alleinige Kontrolle über die Verwendung seiner eigenen elektronischen Signaturstellungsdaten hat und bei der Verwendung der Einheit die Anforderungen an qualifizierte elektronische Signaturen erfüllt werden.
- (52) Die Erstellung elektronischer Fernsignaturen in einer von einem Vertrauensdiensteanbieter im Namen des Unterzeichners geführten Umgebung soll aufgrund der vielfältigen damit verbundenen wirtschaftlichen Vorteile ausgebaut werden. Damit elektronische Fernsignaturen tatsächlich rechtlich in gleicher Weise anerkannt werden können wie elektronische Signaturen, die vollständig in der Umgebung des Nutzers erstellt werden, sollten die Anbieter von elektronischen Fernsignaturdiensten jedoch spezielle Verfahren für die Handhabung und Sicherheitsverwaltung mit vertrauenswürdigen Systemen und Produkten anwenden, u. a. durch abgesicherte elektronische Kommunikationskanäle, um für eine vertrauenswürdige Umgebung zur Erstellung elektronischer Signaturen zu sorgen und zu gewährleisten, dass diese Umgebung unter alleiniger Kontrolle des Unterzeichners genutzt worden ist. Für qualifizierte elektronische Signaturen, die mit Einheiten zur Erstellung elektronischer Fernsignaturen erstellt werden, gelten die in dieser Verordnung festgelegten Anforderungen an die Vertrauensdiensteanbieter.
- (55) Eine auf internationalen Normen wie der Norm ISO 15408 und damit verbundenen Evaluierungsmethoden und Regelungen für die gegenseitige Anerkennung beruhende IT-Sicherheitszertifizierung ist ein wichtiges Instrument, um die Sicherheit qualifizierter elektronischer Signaturerstellungseinheiten zu prüfen, und sollte gefördert werden. Innovative Lösungen und Dienste wie Mobil- oder Cloud-Signierung stützen sich indes auf technische und organisatorische Lösungen für qualifizierte elektronische Signaturerstellungseinheiten, für die Sicherheitsstandards unter Umständen noch nicht zur Verfügung stehen oder die erste IT-Sicherheitszertifizierung im Gange ist. Nur wenn die Sicherheitsstandards nicht zur Verfügung stehen oder die erste IT-Sicherheitszertifizierung im Gange ist, könnte das Sicherheitsniveau solcher qualifizierter elektronischer Signaturerstellungseinheiten durch alternative Verfahren evaluiert werden. Diese Verfahren sollten mit den Standards für die IT-Sicherheitszertifizierung vergleichbar sein, soweit ihre Sicherheitsniveaus gleichwertig sind. Diese Verfahren könnten durch eine gegenseitige Begutachtung erleichtert werden.

Agenda

- Motivation
- Mobilisierung der QES
- **Fact or Fiction?**

Mobile QES – Fact or Fiction?

- Mobile QES ist in vielen EU-Mitgliedstaaten (z.B. EE, AT, IT) schon seit einigen Jahren möglich
- Umsetzung in Deutschland steht noch aus, ist aber schon auf Basis von SigG/SigV möglich
- eIDAS-Verordnung eröffnet zusätzliche Realisierungsoptionen



Unverbindliche Interessensbekundung für die Mitwirkung am Pilotprojekt "QES2go"

Vorname*	Name*	
<input type="text"/>	<input type="text"/>	
Straße*	Nr.*	
<input type="text"/>	<input type="text"/>	
Postleitzahl*	Wohnort*	Telefon (tagsüber)
<input type="text"/>	<input type="text"/>	<input type="text"/>
Organisation/ Firma	E-Mail*	
<input type="text"/>	<input type="text"/>	

50% Einführungsrabatt sichern? Nutzen Sie hierfür die eID-Registrierung 

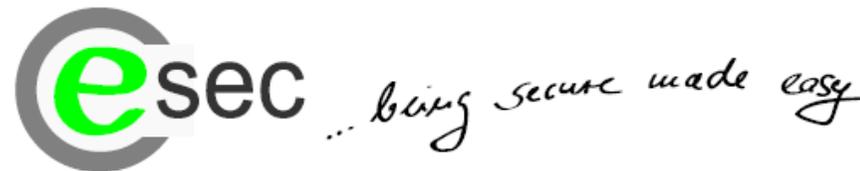


Herzlichen Dank für Ihre Aufmerksamkeit!

Deutschland
Land der Ideen



Ausgezeichneter Ort 2013/14



ecsec GmbH

Sudetenstr. 16
96247 Michelau, Germany
Telefon + 49 9571 896479
Mobil + 49 171 9754980
detlef.huehnlein@ecsec.de
<http://www.ecsec.de>

Dipl.-Inform. (FH)
Dr. Detlef Hühnlein
Geschäftsführer