



První certifikační autorita, a.s., (I. CA) was founded at the beginning of year 2001. The use gained in implementation and operation of the project providing of sophisticated services in the Czech Republic is one of the determining factors for high quality of provided services.

The most important step forward was the completion of accreditation process in sense of Law 227/2000 about electronic signature and cohering edicts. The Office for Personal Data Protection confers on První certifikační autorita, a.s a certificate of accreditation provider of certification services in the Czech Republic with effectiveness since 1st of May 2002. In 2006 I.CA get certificate of accreditation provider of certification services in the Slovak Republic too.

In 2011 our company provide the services of remote signing of documents to our clients.

Position on the Market

Our company is currently the biggest provider of digital certificates in the Czech and Slovak Republic. Density of certificates is high. There are more than 100 so-called registration authorities, recently having exceeded the number of 400 in count. Their spread over the whole territory of the country is a notable competitive advantage. These contacting offices thus provide optimum accessibility of our products and services.

The quantity of certificates issued in the Czech Republic is also unmatched. Their number has reached six-digit numbers. These competitive advantages enable the company to continuously develop its product portfolio as well as improve quality of services provided.

Certificates, Qualified certificates

A digital certificate is an electronic version of identity card, it even contains similar set of information. First of all, it explicitly connects physical and electronic identities.

Ing. Roman Kučera is among the information contained in the certificate. This value is of paramount importance. Developments in performing power of computer could in long-term void the reliability of digital certificates. Regularly issued certificates bear 5. 9. 2018 validity of a certificate can be nullified even during the period if required e.g. by disclosure of private key of the certificate.

Nullified certificate is registered in the list of nullified certificates (CRL). The list of void certificates is then formed as a file (list of nullified certificates) with maximum period of validity

Služba vzdáleného pečetění I.CA RemoteSeal



Hovořit budeme o splnění povinnosti veřejnoprávního podepisujícího danou § 8 zákona č. 297/2016 Sb.:

- Nestanoví-li jiný právní předpis jako náležitost právního jednání obsaženého v dokumentu podpis nebo tato náležitost nevyplývá z povahy právního jednání, veřejnoprávní podepisující a jiná právnická osoba, jedná-li při výkonu své působnosti, zapečetí dokument v elektronické podobě kvalifikovanou elektronickou pečetí.
- **Tato povinnost platí nejpozději od 20. září 2018.**

Ve zkratce - kde je dnes značka, musí být pečeť

Co to je kvalifikovaná elektronická pečeť?

- Dle článku 3 bodu 27) eIDAS je to:

Zaručená elektronická pečeť, která je vytvořena pomocí kvalifikovaného prostředku pro vytváření elektronických pečetí a která je založena na kvalifikovaném certifikátu pro elektronickou pečeť.

Kvalifikovaný certifikát pro elektronickou pečeť může vydat pouze kvalifikovaný poskytovatel služeb vytvářejících důvěru, který byl auditován a služba zařazena na TL list státu EU (LoTL).

Seznam kvalifikovaných poskytovatelů v ČR

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Mimo serveru · Textová verze · English · Rozšířené vyhledávání · Ok

Rychlé menu

Úvod · O nás · Služby pro veřejnost · Informační servis · eGovernment · EU · Nabídky a zakázky · Projekty · Legislativa · Kontakty

POVINNÉ ZVEŘEJŇOVANÉ INFORMACE

Úvodní strana / eGovernment / eIDAS, elektronický podpis / Povinné zveřejňované informace

Seznam kvalifikovaných poskytovatelů služeb vytvářejících důvěru a poskytovaných kvalifikovaných služeb vytvářejících důvěru

Ministerstvo vnitra zveřejňuje informace o kvalifikovaných poskytovatelích služeb vytvářejících důvěru a poskytovaných kvalifikovaných služeb vytvářejících důvěru.

Číslo	Kvalifikovaní poskytovatelé služeb vytvářejících důvěru	Kvalifikované služby	Zahájení poskytování
1.	První certifikační autorita, a.s. , IČO 26439395, Podvinný mlýn 2178/6, PSČ 190 00 Praha 9	Vydávání kvalifikovaných certifikátů pro elektronické podpisy (před účinností Nařízení (EU) č. 910/2014 se jednalo o službu vydávání kvalifikovaných certifikátů); Kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů a pečeti; Vydávání kvalifikovaných certifikátů pro elektronické pečeti; Vydávání kvalifikovaných elektronických časových razítek; Vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek.	03/2002 04/2017 08/2017 09/2017 02/2018
2.	Česká pošta, s.p. , IČO 47114603, Politických vězňů 906/4, PSČ 225 96 Praha 1	Vydávání kvalifikovaných certifikátů pro elektronické podpisy (před účinností Nařízení (EU) č. 910/2014 se jednalo o službu vydávání kvalifikovaných certifikátů); Vydávání kvalifikovaných certifikátů pro elektronické pečeti; Vydávání kvalifikovaných certifikátů pro autentizaci internetových stránek; Vydávání kvalifikovaných elektronických časových razítek.	09/2005 08/2017 08/2017 09/2017

Policie ČR

Hasiči ČR

Státní služba

Registr smluv

C T H H
CENTRUM PROTI TERORISMU
A HYBRIDNÍM HROZBÁM

GDPR

<http://www.mvcr.cz/clanek/seznam-kvalifikovanych-poskytovatelu-sluzeb-vytvarejicich-duveru-a-poskytovanych-kvalifikovanych-sluzeb-vytvarejicich-duveru.aspx>

Kde lze zjistit, že se jedná o kvalifikovaný prostředek pro vytváření elektronických pečetí (QSealCD)?

„Compilation of Member States notification on SSCDs and QSCDs“

<https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds>

- Uvedena certifikovaná QSigCDs a QSealCDs podle nařízení eIDAS

První certifikační autorita, a.s., (I. CA) was founded at the beginning of the year 2003. It is based on its own expertise and experience gained in the development and operation of the system that has become the first one in a field of commercial providing of sophisticated services for the design and administration of digital certificates in the Czech Republic. One of the determining factors for high quality of provided services.

The most important step forwards was a successful completion of accreditation in accordance with sense of Law 227/2000 about electronic signatures and other related edicts. The

HSM moduly hodnocené jako QSealCD

List of QSCDs	
Name: Applicant Qualified Signature Creation Device (QSigCD)	PrimeSign Remote Signing Device/Core für qualifizierte Signaturen und Siegel PrimeSign GmbH yes IMPORTANT NOTE: Device aimed to be managed on behalf of the user (signatory) by a QTSP that can be only considered as QSigCD when duly operated by a QTSP in accordance with eIDAS Regulation (EU) 910/2014. Zentrum für sichere Informationstechnologie - Austria (A-SIT) 20.11.2017 Valid up to revocation by A-SIT A-SIT-VIG-17-067 QSigCD designation by QSigCD designation date QSigCD designation expiry QSigCD designation report reference QSigCD designation report Art.30.3.(b) notified alternative certification method CC certification report reference Qualified Seal Creation Device (QSealCD)
QSealCD designation by QSealCD designation date QSealCD designation expiry QSealCD designation report reference QSealCD designation report Art.30.3.(b) notified alternative certification method CC certification report reference	Zentrum für sichere Informationstechnologie - Austria (A-SIT) 20.11.2017 Valid up to revocation by A-SIT A-SIT-VIG-17-067 https://www.a-sit.at/downloads/736 https://www.a-sit.at/pdfs/merkblatt_de.pdf https://www.a-sit.at/pdfs/merkblatt_en.pdf none yes IMPORTANT NOTE: Device aimed to be managed on behalf of the user (seal creator) by a QTSP that can be only considered as QSealCD when duly operated by a QTSP in accordance with eIDAS Regulation (EU) 910/2014. Zentrum für sichere Informationstechnologie - Austria (A-SIT) 20.11.2017 Valid up to revocation by A-SIT A-SIT-VIG-17-067 https://www.a-sit.at/downloads/736 https://www.a-sit.at/pdfs/merkblatt_de.pdf https://www.a-sit.at/pdfs/merkblatt_en.pdf none
Name: Applicant Qualified Signature Creation Device (QSigCD)	Qualified Signature and Seal Creation Device (QSCD) LuxTrust's Qualified Remote Signature and Seal Creation Device, version 1.0 LuxTrust S.A., IVY Building, 13-15 Parc d'activités, L-8308 Capellen, Luxembourg yes IMPORTANT NOTE: Device aimed to be managed on behalf of the user (signatory) by a QTSP that can be only considered as QSigCD when duly operated by a QTSP in accordance with eIDAS Regulation (EU) 910/2014. Zentrum für sichere Informationstechnologie - Austria (A-SIT) 14.12.2017 Valid up to revocation by A-SIT A-SIT-VIG-17-060 QSigCD designation by QSigCD designation date QSigCD designation expiry QSigCD designation report reference QSigCD designation report Art.30.3.(b) notified alternative certification method CC certification report reference Qualified Seal Creation Device (QSealCD)
QSealCD designation by QSealCD designation date QSealCD designation expiry QSealCD designation report reference QSealCD designation report Art.30.3.(b) notified alternative certification method CC certification report reference	Zentrum für sichere Informationstechnologie - Austria (A-SIT) 14.12.2017 Valid up to revocation by A-SIT A-SIT-VIG-17-060 https://www.a-sit.at/downloads/682 https://www.a-sit.at/pdfs/merkblatt_de.pdf https://www.a-sit.at/pdfs/merkblatt_en.pdf HSM (subcomponent) certified by OCSI http://www.ocsi.isticom.it/documenti/certificazioni/thales/rc_thales_nshield_v1.0.pdf yes IMPORTANT NOTE: Device aimed to be managed on behalf of the user (seal creator) by a QTSP that can be only considered as QSealCD when duly operated by a QTSP in accordance with eIDAS Regulation (EU) 910/2014. Zentrum für sichere Informationstechnologie - Austria (A-SIT) 14.12.2017 Valid up to revocation by A-SIT A-SIT-VIG-17-060 https://www.a-sit.at/downloads/682 https://www.a-sit.at/pdfs/merkblatt_de.pdf https://www.a-sit.at/pdfs/merkblatt_en.pdf HSM (subcomponent) certified by OCSI http://www.ocsi.isticom.it/documenti/certificazioni/thales/rc_thales_nshield_v1.0.pdf

The most important step forwards was a successful completion of accreditation in the sense of Law 227/2000 about electronic signatures and e-signing edicts. The

Name:	Qualified Signature Creation Device (QSCD) Protect & Sign, version 4.18
Applicant	DocuSign France, 9-15 Rue Maurice Mallet, 92130 Issy-les-Moulineaux, France
Qualified Signature Creation Device (QSigCD)	yes
	IMPORTANT NOTE: Device aimed to be managed on behalf of the user (signatory) by a QTSP that can be only considered as QSigCD when duly operated by a QTSP in accordance with eIDAS Regulation (EU) 910/2014.
QSigCD designation by	Zentrum für sichere Informationstechnologie - Austria (A-SIT)
QSigCD designation date	20.12.2017
QSigCD designation expiry	Valid up to revocation by A-SIT
QSigCD designation report reference	A-SIT-VIG-17-069
QSigCD designation report	https://www.a-sit.at/downloads/884
Art. 30.3. (b) notified alternative certification method	https://www.a-sit.at/pdfs/merkblatt_de.pdf
CC certification report reference	n.a.
Qualified Seal Creation Device (QSealCD)	no
Name:	Qualified Signature and Seal Creation Device (QSCD) AliasLab CryptoAccelerator, release 3.5.1
Applicant	AliasLab SpA, via Cremona 27/6, 46100 Mantova, Italy
Qualified Signature Creation Device (QSigCD)	yes
	IMPORTANT NOTE: Device aimed to be managed on behalf of the user (signatory) by a QTSP that can be only considered as QSigCD when duly operated by a QTSP in accordance with eIDAS Regulation (EU) 910/2014.
QSigCD designation by	Zentrum für sichere Informationstechnologie - Austria (A-SIT)
QSigCD designation date	20.12.2017
QSigCD designation expiry	Valid up to revocation by A-SIT
QSigCD designation report reference	A-SIT-VIG-17-083
QSigCD designation report	https://www.a-sit.at/downloads/886
Art. 30.3. (b) notified alternative certification method	https://www.a-sit.at/pdfs/merkblatt_de.pdf
CC certification report reference	https://www.a-sit.at/pdfs/merkblatt_en.pdf
Qualified Seal Creation Device (QSealCD)	HSM (subcomponent) certified by OCSI
	http://www.ocsi.isticom.it/documenti/certificazioni/thales/rc_thales_nshield_v1.0.pdf
	yes
	IMPORTANT NOTE: Device aimed to be managed on behalf of the user (seal creator) by a QTSP that can be only considered as QSealCD when duly operated by a QTSP in accordance with eIDAS Regulation (EU) 910/2014.
QSealCD designation by	Zentrum für sichere Informationstechnologie - Austria (A-SIT)
QSealCD designation date	20.12.2017
QSealCD designation expiry	Valid up to revocation by A-SIT
QSealCD designation report reference	A-SIT-VIG-17-083
QSealCD designation report	https://www.a-sit.at/downloads/886
Art. 30.3. (b) notified alternative certification method	https://www.a-sit.at/pdfs/merkblatt_de.pdf
CC certification report reference	https://www.a-sit.at/pdfs/merkblatt_en.pdf
	HSM (subcomponent) certified by OCSI
	http://www.ocsi.isticom.it/documenti/certificazioni/thales/rc_thales_nshield_v1.0.pdf

QSealCD

První certifikační autorita, a.s. (I. CA) was founded at the beginning of the year 2003. It has gained its reputation through its own expertise and experience gained in the development and operation of the system that has become the first one in a field of commercial providing of sophisticated services for the design and administration of digital certificates in the Czech Republic. The determining factors for high quality of provided services.

The most important step forwards was a successful completion of accreditation in the sense of Law 227/2000 about electronic signatures and e-signing edicts.



Name:	Qualifizierte Signatur- und Siegelerstellungseinheit (QSE) des Swisscom All-in Signing Service (AIS), Version 2.3.1
Applicant	Swisscom IT Services Finance S.E., Modecenterstraße 17 / Unit 2, 1110 Wien, Austria
Qualified Signature Creation Device (QSigCD)	yes IMPORTANT NOTE: Device aimed to be managed on behalf of the user (signatory) by a QTSP that can be only considered as QSigCD when duly operated by a QTSP in accordance with eIDAS Regulation (EU) 910/2014. Zentrum für sichere Informationstechnologie - Austria (A-SIT)
QSigCD designation by	16.03.2018
QSigCD designation date	Valid up to revocation by A-SIT
QSigCD designation expiry	A-SIT-VIG-17-076
QSigCD designation report reference	https://www.a-sit.at/downloads/912
QSigCD designation report	https://www.a-sit.at/pdfs/merkblatt_de.pdf
Art.30.3.(b) notified alternative certification method	https://www.a-sit.at/pdfs/merkblatt_en.pdf
CC certification report reference	none
Qualified Seal Creation Device (QSealCD)	yes IMPORTANT NOTE: Device aimed to be managed on behalf of the user (seal creator) by a QTSP that can be only considered as QSealCD when duly operated by a QTSP in accordance with eIDAS Regulation (EU) 910/2014. Zentrum für sichere Informationstechnologie - Austria (A-SIT)
QSealCD designation by	16.03.2018
QSealCD designation date	Valid up to revocation by A-SIT
QSealCD designation expiry	A-SIT-VIG-17-076
QSealCD designation report reference	https://www.a-sit.at/downloads/912
QSealCD designation report	https://www.a-sit.at/pdfs/merkblatt_de.pdf
Art.30.3.(b) notified alternative certification method	https://www.a-sit.at/pdfs/merkblatt_en.pdf
CC certification report reference	none
Name:	Qualifizierte Signaturerstellungseinheit (QSEE) der A-Trust für die Handy-Signatur bestehend aus HSM und HSM Server, Version 1.2
Applicant	A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH, Landstraße Hauptstraße 1b, E02, 1030 Wien, Austria
Qualified Signature Creation Device (QSigCD)	yes IMPORTANT NOTE: Device aimed to be managed on behalf of the user (signatory) by a QTSP that can be only considered as QSigCD when duly operated by a QTSP in accordance with eIDAS Regulation (EU) 910/2014. Zentrum für sichere Informationstechnologie - Austria (A-SIT)
QSigCD designation by	09.04.2018
QSigCD designation date	Valid up to revocation by A-SIT
QSigCD designation expiry	A-SIT-VIG-17-086
QSigCD designation report reference	https://www.a-sit.at/downloads/930
QSigCD designation report	https://www.a-sit.at/pdfs/merkblatt_de.pdf
Art.30.3.(b) notified alternative certification method	https://www.a-sit.at/pdfs/merkblatt_en.pdf
CC certification report reference	HSM (subcomponent) certified by OCSI http://www.ocsi-list.com.it/documenti/certificazioni/thales/rc_thales_nshield_v1_0.pdf
Qualified Seal Creation Device (QSealCD)	no

List of QSCDs:	
Name:	-
Name:	ARX CoSign v8.2
Applicant	ARX (Algorithmic Research, Ltd.)
Qualified Signature Creation Device (QSigCD)	yes IMPORTANT NOTE: Device aimed to be managed on behalf of the user (signatory) by a QTSP that can be only considered as QSigCD when duly operated by a QTSP in accordance with eIDAS Regulation (EU) 910/2014.
QSigCD designation by	OCSI
QSigCD designation date	07.02.2017
QSigCD designation expiry	-
QSigCD designation report reference	OCSI/ACC/ARX/01/2017/RA
QSigCD designation report	http://www.ocsi.isticom.it/documents/accertamenti/arx/ac_rda_eidas_cosign_82_v1.0.pdf
Art.30.3.(b) notified alternative certification method	http://www.ocsi.isticom.it/index.php/dispositivi-di-firma/procedura-di-accertamento
CC certification report reference	OCSI/CERT/IMQ/05/2016/RC
CC certification body	-
CC certification date	12.09.2016
CC certification report	http://www.ocsi.isticom.it/documents/certificazioni/arx/rc_arx_cosign_82_v1.0.pdf
Security Target	http://www.ocsi.isticom.it/documents/certificazioni/arx/st_arx_cosign_82_v2.6.pdf
Qualified Seal Creation Device (QSealCD)	yes IMPORTANT NOTE: Device aimed to be managed on behalf of the user (seal creator) by a QTSP that can be only considered as QSealCD when duly operated by a QTSP in accordance with eIDAS Regulation (EU) 910/2014.
QSealCD designation by	OCSI
QSealCD designation date	07.02.2017
QSealCD designation expiry	-
QSealCD designation report reference	OCSI/ACC/ARX/01/2017/RA
QSealCD designation report	http://www.ocsi.isticom.it/documents/accertamenti/arx/ac_rda_eidas_cosign_82_v1.0.pdf
Art.30.3.(b) notified alternative certification method	http://www.ocsi.isticom.it/index.php/dispositivi-di-firma/procedura-di-accertamento
CC certification report reference	OCSI/CERT/IMQ/05/2016/RC
CC certification body	-
CC certification date	12.09.2016
CC certification report	http://www.ocsi.isticom.it/documents/certificazioni/arx/rc_arx_cosign_82_v1.0.pdf
Security Target	http://www.ocsi.isticom.it/documents/certificazioni/arx/st_arx_cosign_82_v2.6.pdf
Name:	nShield Connect 500, nShield Connect 500+, nShield Connect 1500, nShield Connect 1500+, nShield Connect 6000, nShield Connect 6000+
Applicant	Thales e-Security Ltd.
Qualified Signature Creation Device (QSigCD)	Yes IMPORTANT NOTE: Device aimed to be managed on behalf of the user (signatory) by a QTSP that can be only considered as QSigCD when duly operated by a QTSP in accordance with eIDAS Regulation (EU) 910/2014.
QSigCD designation by	OCSI
QSigCD designation date	05.02.2018
QSigCD designation expiry	-

QSealCD

CERTIFICATION
AUTHORITY

První certifikační autorita, a.s. (I. CA) was established at the beginning of the year 2013. It has gained its own expertise and experience gained in the development and operation of the system that has become the first one in a field of commercial providing of sophisticated services for the issuance and administration of digital certificates in the Czech Republic. The determining factors for high quality of provided services.

The most important step forwards was a successful completion of accreditation in the sense of Law 227/2009 about electronic signature, as pherasing in date 2014.

QSigCD designation report reference	OCSI/ACC/THL/02/2017/RA
QSigCD designation report	http://www.ocsi.isticom.it/documenti/accertamenti/thales/ac_rda_eidas_nshield_v1.0.pdf
Art.30.3.(b) notified alternative certification method	http://www.ocsi.isticom.it/index.php/dispositivi-di-firma/procedura-di-accertamento
CC certification report reference	OCSI/CERT/RES/02/2012/RC
CC certification body	OCSI
CC certification date	10.03.2016
CC certification report	http://www.ocsi.isticom.it/documenti/certificazioni/thales/rc_thales_nshield_v1.0.pdf
Security Target	http://www.ocsi.isticom.it/documenti/certificazioni/thales/st_thales_nshield_v1.0_public.pdf
Qualified Seal Creation Device (QSealCD)	yes
	IMPORTANT NOTE: Device aimed to be managed on behalf of the user (seal creator) by a QTSP that can be only considered as QSealCD when duly operated by a QTSP in accordance with eIDAS Regulation (EU) 910/2014.
QSealCD designation by	OCSI
QSealCD designation date	05.02.2018
QSealCD designation expiry	-
QSealCD designation report reference	OCSI/ACC/THL/02/2017/RA
QSealCD designation report	http://www.ocsi.isticom.it/documenti/accertamenti/thales/ac_rda_eidas_nshield_v1.0.pdf
Art.30.3.(b) notified alternative certification method	http://www.ocsi.isticom.it/index.php/dispositivi-di-firma/procedura-di-accertamento
CC certification report reference	OCSI/CERT/RES/02/2012/RC
CC certification body	OCSI
CC certification date	10.03.2016
CC certification report	http://www.ocsi.isticom.it/documenti/certificazioni/thales/rc_thales_nshield_v1.0.pdf
Security Target	http://www.ocsi.isticom.it/documenti/certificazioni/thales/st_thales_nshield_v1.0_public.pdf
Name:	DocuSign Signature Appliance v8.4
Applicant	DocuSign
Qualified Signature Creation Device (QSigCD)	yes
	IMPORTANT NOTE: Device aimed to be managed on behalf of the user (signatory) by a QTSP that can be only considered as QSigCD when duly operated by a QTSP in accordance with eIDAS Regulation (EU) 910/2014.
QSigCD designation by	OCSI
QSigCD designation date	21.02.2018
QSigCD designation expiry	-
QSigCD designation report reference	OCSI/ACC/DSA/01/2017/RA
QSigCD designation report	http://www.ocsi.isticom.it/documenti/accertamenti/docusign/ac_rda_eidas_docusign_84_v1.0.pdf
Art.30.3.(b) notified alternative certification method	http://www.ocsi.isticom.it/index.php/dispositivi-di-firma/procedura-di-accertamento
CC certification report reference	OCSI/CERT/IMQ/07/2017/RC
CC certification body	OCSI
CC certification date	21.02.2018
CC certification report	http://www.ocsi.isticom.it/documenti/certificazioni/docusign/rc_docusign_84_v1.0.pdf
Security Target	http://www.ocsi.isticom.it/documenti/certificazioni/docusign/st_docusign_84_v2.13.pdf
Qualified Seal Creation Device (QSealCD)	yes
	IMPORTANT NOTE: Device aimed to be managed on behalf of the user (seal creator) by a QTSP that can be only considered as QSealCD when duly operated by a QTSP in accordance with eIDAS Regulation (EU) 910/2014.
QSealCD designation by	OCSI
QSealCD designation date	05.02.2018
QSealCD designation expiry	-
QSealCD designation report reference	OCSI/ACC/THL/02/2017/RA
QSealCD designation report	http://www.ocsi.isticom.it/documenti/accertamenti/thales/ac_rda_eidas_nshield_v1.0.pdf
Art.30.3.(b) notified alternative certification method	http://www.ocsi.isticom.it/index.php/dispositivi-di-firma/procedura-di-accertamento
CC certification report reference	OCSI/CERT/RES/02/2012/RC
CC certification body	OCSI
CC certification date	10.03.2016
CC certification report	http://www.ocsi.isticom.it/documenti/certificazioni/thales/rc_thales_nshield_v1.0.pdf
Security Target	http://www.ocsi.isticom.it/documenti/certificazioni/thales/st_thales_nshield_v1.0_public.pdf

Čipové karty hodnocené jako QSealCD

Name:	Produit Gemalto "IAS Classic V4.4 with MOC Server 1.1 on MultiApp V4" embarqué sur le microcontrôleur M7892 G12 Infineon Technologies AG
Applicant	Gemalto
Qualified Signature Creation Device (QSigCD)	yes
QSigCD designation by	Agence Nationale de Sécurité des Systèmes d'Information (ANSSI)
QSigCD designation date	07.07.2017
QSigCD designation expiry	07.07.2022
QSigCD designation report reference	3341/ANSSI/SDE
QSigCD designation report	-
CC certification report reference	ANSSI-CC-2017/22
CC certification body	ANSSI
CC certification date	16.06.2017
CC certification report	ANSSI-CC-2017/22
Qualified Seal Creation Device (QSealCD)	yes
QSealCD designation by	Agence Nationale de Sécurité des Systèmes d'Information (ANSSI)
QSealCD designation date	07.07.2017
QSealCD designation expiry	07.07.2022
QSealCD designation report reference	3341/ANSSI/SDE
QSealCD designation report	-
CC certification report reference	ANSSI-CC-2017/22
CC certification body	ANSSI
CC certification date	16.06.2017
CC certification report	ANSSI-CC-2017/22

DocuSign Signature Appliance alias ARX CoSign



CERTIFICATION
AUTHORITY

- ARX (Algorithmic Research) CoSign v8.2
- Společnost ARX koupena v roce 2015 společností DocuSign
- Produkt nadále prodáván pod názvem DocuSign Signature



I.CA RemoteSeal



Jaké jsou možnosti pečetění?

1. QSealCD v držení pečetící osoby - pokud jsou data pro vytváření elektronických pečetí uchovávána v prostředí spravovaném zcela, nikoli však výhradně uživatelem = certifikované čipové karty (malí klienti) či HSM (velcí klienti disponující odborným zázemím)
2. QSealCD na dálku - pokud data pro vytváření elektronických pečetí spravuje kvalifikovaný poskytovatel služeb vytvářejících důvěru jménem pečetící osoby = velcí klienti
3. Zahraniční kvalifikovaní poskytovatelé.

Služba I.CA RemoteSeal představuje variantu 2.

I.CA RemoteSeal



Výhody využití služby pečetění na dálku

- uživatelé nemusí mít detailní technické znalosti HSM modulu a jeho ovládání
- není třeba zajistit investiční prostředky na nákup HSM modulu/ů, což znamená výraznou úsporu a minimální technické nároky.

Služba I.CA RemoteSeal byla auditována a orgánem dohledu zařazena na seznam služeb poskytovaných kvalifikovaným poskytovatelem služeb vytvářejících důvěru správním rozhodnutím z 21.6.2018.

Identifikátor této služby (1.3.6.1.4.1.23624.10.1.38.1.0) byl uveřejněn v důvěryhodném seznamu České republiky u služby „(78) I.CA - vydávání kvalifikovaných certifikátů“ společně s identifikátorem „QCQSCDManagedOnBehalf“ podle kap. 5.5.9.2.3 technických specifikací ETSI TS 119 612 v2.1.1.

I.CA RemoteSeal



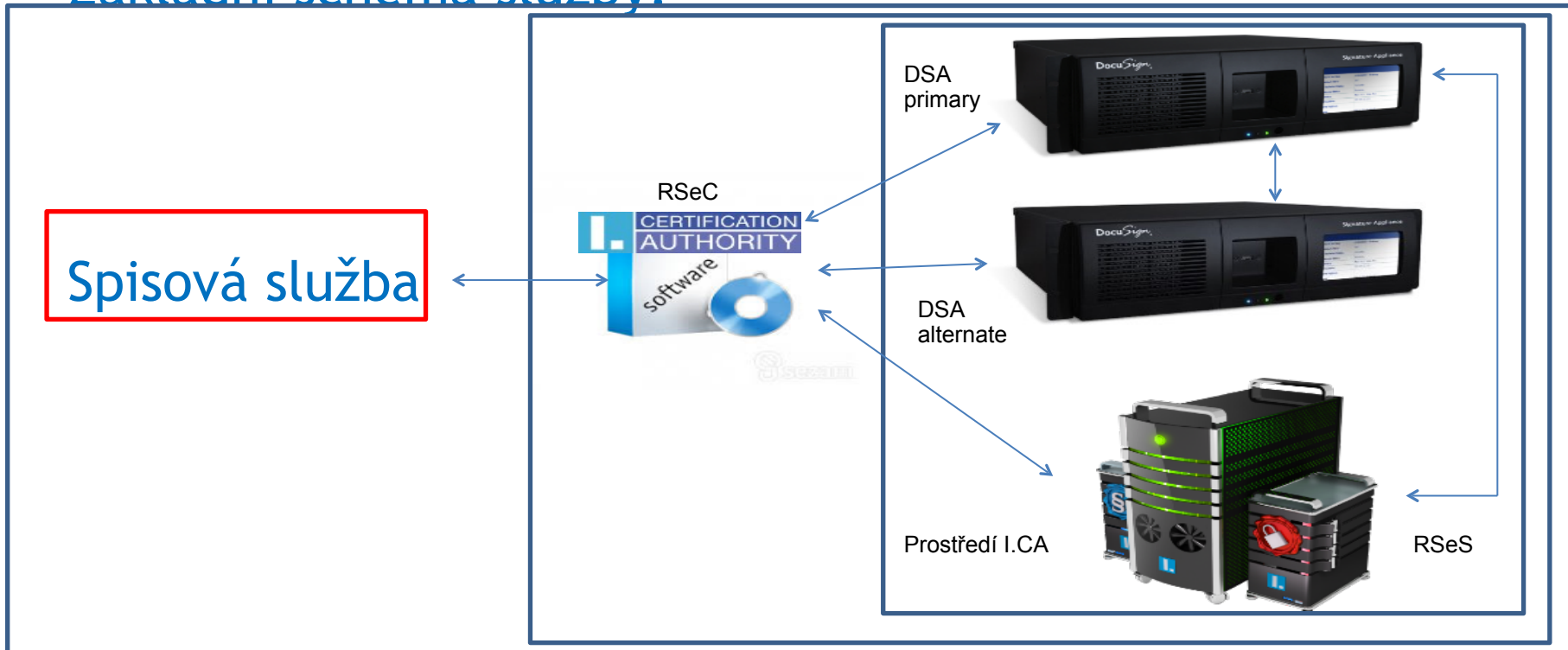
The most important step forwards was a successful completion of accreditation in the sense of Law 227/2000 about electronic signatures and e-signing edicts.

Na TL (https://tsl.gov.cz/publ/TSL_CZ.xtsl) je služba uvedena:

(78) I.CA - issuing qualified certificates	
Service Type	CA/QC
Service Status	TrustedList/Svcstatus/granted
Status valid from	2017-08-16 12:15:00
Service History	▶ 2016-06-30 22:00:00
Service History	▶ 2016-06-15 05:55:00
Qualifications	▼ Qualifications - Service Information Extension
	Critical true
	Qualifiers TrustedList/SvcInfoExt/QCQSCDStatusAsInCert
	Assert At least one
	Policies Object Identifier 1.3.6.1.4.1.23624.10.1.30.1.0
	Policies Object Identifier 1.3.6.1.4.1.23624.10.1.30.1.1
	Policies Object Identifier 1.3.6.1.4.1.23624.10.1.31.1.0
	Policies Object Identifier 1.3.6.1.4.1.23624.10.1.34.1.0
Service Info	▶ Additional Service Information Extension: TrustedList/SvcInfoExt/ForceSignature
Qualifications	▼ Qualifications - Service Information Extension
	Critical true
	Qualifiers TrustedList/SvcInfoExt/QCQSCDManagedOnBehalf
	Assert At least one
	Policies Object Identifier 1.3.6.1.4.1.23624.10.1.38.1.0
Service Certificate	▼ I.CA Qualified 2 CA/RSA 02/2016
	Subject Name ▼ Country CZ
	Common Name I.CA Qualified 2 CA/RSA 02/2016
	Organization První certifikační autorita, a.s.

I.CA RemoteSeal

Základní schéma služby:



Architektura - popis komponent systému



- **RSeC** - RemoteSeal Client - klientská komponenta určená pro integraci do volající aplikace, typicky do spisové služby.
- **RSeS** - RemoteSeal Server - základní aplikační server provozovaný I.CA, který realizuje první vrstvu autentizace volající aplikace a udržuje evidenci provedených transakcí (opečetění).
- **DSA** - DocuSign Signature Appliance - certifikovaný QSealCD HSM modul.
- **RSeActivationUtil** - Aktivační utilita sloužící k aktivaci RSeC pomocí tzv. aktivační karty.

I.CA RemoteSeal



Základní popis:

- Zřízení služby
- Aktivace RemoteSeal klienta
- Opečetění dokumentu
- Automatické prodloužení služby
- Vydání následného kvalifikovaného certifikátu pro elektronickou pečeť
- Cenový model
- Testování služby a produkční prostředí.

Zřízení služby

- Mezi I.CA a klientem bude uzavřena smlouva.
- Oprávněná osoba klienta navštíví pobočku Registrační autority (RA).
- Operátor RA vydá klientovi prvotní autentizační komerční technologický certifikát na aktivační čipovou kartu . Certifikát je zaveden jako autentizační certifikát pro RemoteSeal pro daného uživatele.
- Operátor RA připraví žádost o pečetící certifikát pro uživatele.
- Operátor RA vygeneruje párová data pro pečetící certifikát
 - ICARA pomocí RemoteSeal klienta založí pro klienta uživatele na HSM
 - ICARA provede aktivaci uživatelského účtu v HSM
 - ICARA provede pod účtem uživatele generování párových dat pro vydání prvotního pečetícího certifikátu.
- Operátor RA pomocí ICARA podepíše žádost o vydání pečetícího certifikátu privátním klíčem párových dat na HSM

Zřízení služby

- Oprávněná osoba klienta zadá PIN na pinpadové čteče
- Na základě žádosti proběhne vydání pečetícího certifikátu
- Pečetící certifikát (resp. veřejná část):
 - Je zaslán na e-mailovou adresu uživatele
 - ICARA uloží na čipovou kartu/token uživatele.
 - ICARA uloží do HSM
- Oprávněná osoba klienta odchází z RA s aktivační kartou.

Časová náročnost zřízení služby: po uzavření smlouvy hodiny.

Aktivace RemoteSeal Klienta

- Oprávněná osoba spustí dodávanou utilitu RSeActivationUtil



Aktivace RemoteSeal Klienta



- Pro aktivaci RemoteSeal klienta spustí oprávněná osoba klienta dodávanou GUI utilitu
- Utilita vyzve uživatele k vložení aktivační karty, načtež utilita:
 - Naváže spojení s RemoteSeal serverem pomocí oboustranně autentizovaného HTTPS s prvotním autentizačním certifikátem (uživatel je vyzván k zadání PINu)
 - Automaticky vytvoří žádost o vydání následného autentizačního certifikátu, která je podepsána prvotním autentizačním certifikátem; privátní klíč je generován v RSeActivationUtil (nikoliv na kartě)
 - Žádost je odeslána ke zpracování do I.CA, kde se obratem vydá následný certifikát a ten se stáhne zpět do utility
- Následně utilita vytvoří aktivační soubor, kde bude uložen následný autentizační certifikát včetně privátního klíče
- Uživatel tento aktivační soubor následně načte do aplikace volající RemoteSeal klienta (např. spisové služby).
Časová náročnost aktivace: hodina

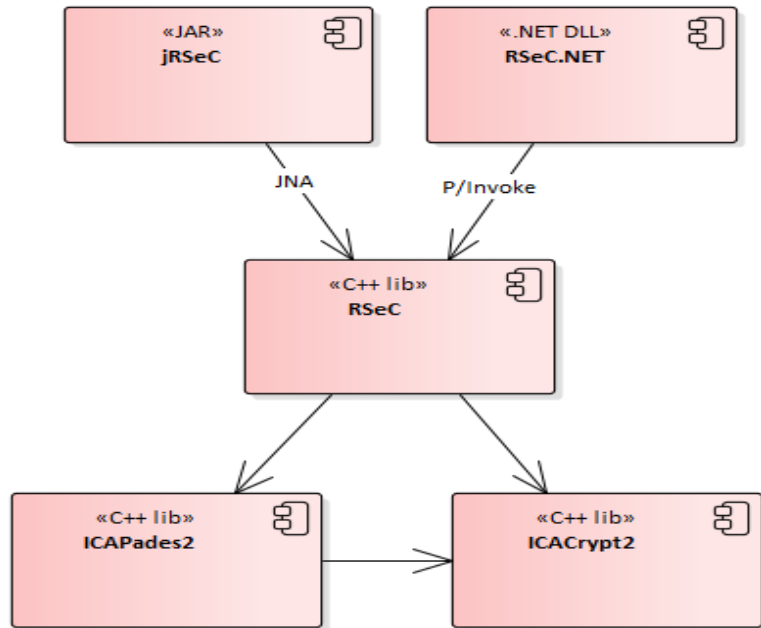
RSeActivationUtil - technické parametry



- Jednoduchá Windows GUI utilita.
- Nemusí být spouštěna na stejném PC, na kterém je provozován RSeC.
- Vyžaduje: .NET 4.5.2

RSeC - Architektura

cmp RSeC - Architektura



- RemoteSeal Client
- Klientská komponenta sloužící k zadávání transakcí (požadavků na opečetění dat) do systému RemoteSeal.
- Nativní C++ jádro
- Distribuováno ve formě:
 - JAR pro Java
 - .NET assembly pro .NET
 - V případě zájmu možno volat přímo nativní jádro.

Implementaci řeší typicky dodavatel spisové služby za podpory I.CA

RSeC - Podporované formáty podpisu



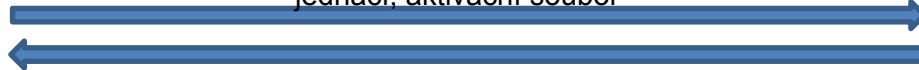
- CAdES-B-B, CAdES-B-T
 - Dle normy EN 319 122, ve variantách:
 - Interní
 - Externí
- PAdES-B-B, PAdES-B-T
 - Dle normy EN 319 142, ve variantách:
 - Neviditelný
 - Viditelný - Text/Obrázek/Text+Obrázek + volitelně obrázek na pozadí
- XAdES-B a XAdES-T
 - dle normy ETSI TS 103 171, a to ve variantě enveloped

Podepisovaná data (business obsah) nikdy neopouští volající systém (komponentu RSeC)!

Proces opečetění dat

Spisová
služba

Dokument k opečetění, parametry požadovaného opečetění, číslo
jednací, aktivační soubor

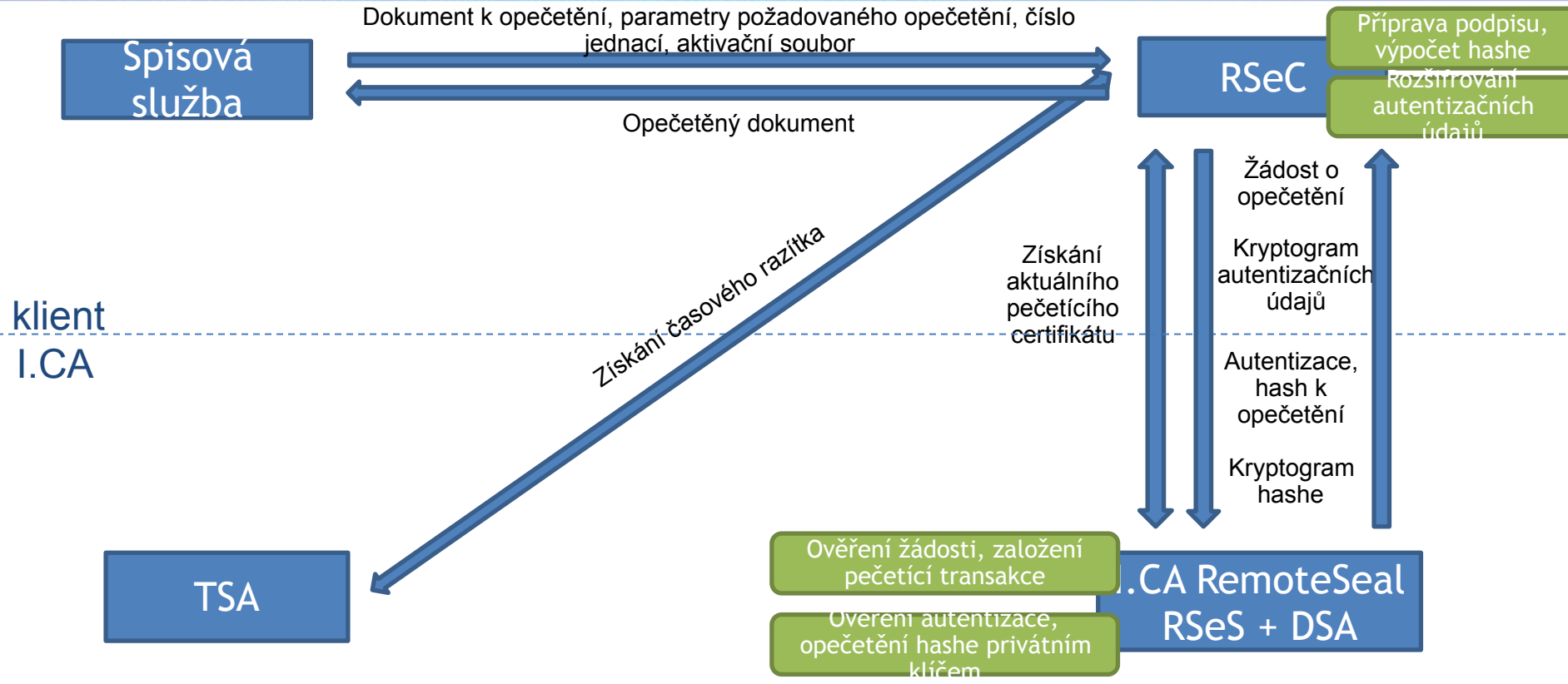


Opečetěný dokument

klient
I.CA

I.CA RemoteSeal

Proces opečetění dat



Automatické prodloužení služby



- RSeC disponuje funkcionalitou automatické obnovy autentizačního certifikátu.
- Před koncem platnosti autentizačního certifikátu je automaticky vytvořena žádost o následný certifikát, která je odeslána na I.CA.
- V rámci odeslání žádosti je veřejný klíč zaregistrován na RSeS a dojde k přešifrování autentizačních dat k DSA pro umožnění přístupu pomocí následného certifikátu.
- Po vydání následného autentizačního certifikátu je tento stažen a automaticky se začne využívat pro autentizaci k RSeS.
- Celý tento proces se děje zcela automatizovaně a transparentně vůči volající aplikaci a probíhá jako součást operace opečetění dat.
- Z hlediska volající aplikace stačí zajistit, aby došlo cca 1x za 14 dní k opečetění libovolného dokumentu.

Automatické vydání následného pečetícího certifikátu

- Před koncem platnosti pečetícího certifikátu dojde prostřednictvím RSeC k vygenerování nového klíčového páru v DSA a vygenerování a opečetění žádosti o následný certifikát původním pečetícím certifikátem.
- Tato žádost je zpracována v I.CA standardní cestou.
- Po vydání certifikátu provede RSeC registraci certifikátu do DSA a RSeS a tento se tímto okamžikem začne automaticky používat pro vytváření kvalifikovaných elektronických pečetí.
- Tento proces je plně automatický a z volající aplikace transparentní.
- Z hlediska volající aplikace stačí zajistit, aby došlo cca 1x za 14 dní k opečetění libovolného dokumentu

Webové uživatelské rozhraní



- Webové uživatelské rozhraní umožňuje oprávněné osobě klienta:

- Procházet a prohledávat seznam provedených opečetění
- Hledat např.: dle data, hashe dokumentu nebo čísla jedacího
- Prohlížet detailní informace zda a kdy a jakým certifikátem byl daný dokument opečetěn.

Nalezené transakce			
VYHLEDÁNO PODLE			
Jednoznačný identifikátor podepsujícího uživatele: U-T-1-10			
Počet nalezených transakcí: 453			
Nové hledání			
VÝPIS TRANSAKČÍ			
Jednoznačný identifikátor transakce	Stav pečeti transakce	Jednoznačný identifikátor dokumentu (např. číslo jednací)	Datum a čas podání žádosti o pečeť
U-T-1-147	Opečetěno	Documentid	11.06.2018 18:58:26.927000
U-T-1-148	Opečetěno	Documentid	12.06.2018 10:14:53.488000
U-T-1-149	Opečetěno		12.06.2018 10:17:16.734000
U-T-1-150	Opečetěno	Documentid	12.06.2018 11:04:36.168000
U-T-1-151	Opečetěno	Documentid	12.06.2018 11:08:30.800000
U-T-1-152	Opečetěno	Documentid	12.06.2018 11:09:04.276000
U-T-1-153	Opečetěno	Documentid	12.06.2018 11:10:49.776000
U-T-1-154	Opečetěno	Documentid	12.06.2018 11:12:01.805000
U-T-1-155	Opečetěno	Documentid	12.06.2018 11:22:16.896000
U-T-1-156	Opečetěno	Documentid	12.06.2018 11:23:21.786000
U-T-1-157	Opečetěno	Documentid	12.06.2018 11:24:11.376000
U-T-1-158	Opečetěno	Documentid	12.06.2018 13:43:49.311000
U-T-1-159	Opečetěno	Documentid	12.06.2018 13:45:54.063000
U-T-1-160	Opečetěno		12.06.2018 14:58:41.443000
U-T-1-161	Opečetěno		12.06.2018 16:01:01.168000
U-T-1-162	Opečetěno	docID: PAdES_002	12.06.2018 16:14:46.081000

- DSA je včetně svého řešení autentizace certifikováno jako řešení pro vytváření Kvalifikované elektronické pečeti.
- Přesto I.CA RemoteSeal přidává další bezpečnostní prvky:
 - Zamezení potenciální možnosti zkopírování autentizačních údajů do DSA mezi návštěvou RA a aktivací služby díky bezpečné aktivační čipové kartě.
 - Zakládání transakcí na RSeS prostřednictvím oboustranně autentizovaného HTTPS kanálu pro zpřístupnění zašifrovaným autentizačních dat k DSA.
 - Runtime kontrola integrity klientské komponenty RSeC (i RSeActivationUtil).
 - Zabezpečení komunikačního kanálu RSeC-DSA pomocí techniky Certificate Pinning.
 - Kontrola integrity konfigurace RSeC proti neoprávněným změnám.
 - Možnost zpětné kontroly seznamu opečetěných dokumentů.

Co se změní z klienta pohledu

Nyní

- Oprávněná osoba požádá na RA o vydání systémového certifikátu
- Ten je instalován v prostředí klienta
- Spisová služba použije systémový certifikát pro označování dokumentu
- Dokument opatřený značkou uloží.

Nově

- Oprávněná osoba požádá na RA o vydání kvalifikovaného certifikátu pro elektronickou pečeť
- Dodavatel spisové služby za pomoci I.CA instaluje v prostředí klienta RemoteSealClienta
- Spisová služba volá RemoteSealClienta
- Opečetěný dokument uloží.

Testovací aplikace

The most important step forwards was a successful completion of accreditation in the sense of Law 227/2000 about electronic signature and signing edicts. The



TestApp - RSeC.NET

Input:

ActivationFile: as byte[]

File to sealed:

Options:

Signature type: CADES PAdES XAdES

Hash algorithm: Document ID (optional): Add TimeStamp

Signature options - PAdES:

Visible signature Location: Reason:

Visible signature options:

Type: Document page:

Description:

Dimension [mm]:

X: Y:

Width: Height:

Background image: as byte[]

Signature image: as byte[]

Cenový model

Jde o kombinaci paušálního poplatku a jednotkové ceny za jedno opečetění v množstevních pásmech (obdobně časovým razítkům).

Ceník pro koncové klienty I.CA RemoteSeal

počet pečetění od - do za měsíc	paušální poplatek Kč bez DPH/měsíc	Cena za 1 ks pečetění Kč bez DPH	Cena celkem za měsíc Kč bez DPH (při max počtu pečetění)	Cena za 1 ks opečetění Kč celkem
1 - 100	1 000	4,00	1 400	14,0000
101 - 300	2 000	3,50	3 050	10,1667
301 - 500	3 000	3,00	4 500	9,0000
501 - 1.000	5 000	2,50	7 500	7,5000
1.001 - 3.000	7 000	2,10	13 300	4,4333
3.001 - 5.000	9 000	1,70	17 500	3,5000
5.001 - 10.000	11 000	1,40	25 000	2,5000
10.001 - 30.000	14 000	1,10	47 000	1,5667
30.001 - 50.000	17 000	0,80	57 000	1,1400
50.001 - 100.000	21 000	0,50	71 000	0,7100
100.001 - 300.000	24 000	0,30	114 000	0,3800
300.001 - 500.000	29 000	0,20	129 000	0,2580
500.001 - 1.000.000	35 000	0,16	195 000	0,1950
1.000.001 - 5.000.000	42 000	0,12	642 000	0,1284
5.000.001 - 10.000.000	49 000	0,08	849 000	0,0849

Cenový model

Druhou možností je plně paušální poplatek v daném množstevním pásmu sjednaný individuálně.

Aktivační čipová karta/token, autentizační certifikáty (prvotní i následné), pečetící certifikáty, pomoc při implementaci RemoteSeal klienta - jsou poskytovány zdarma v rámci služby.

Pokud bude klient přidávat při pečetění časová razítka, je třeba počítat s cenou časových razítek (nejsou součástí služby pečetění).

Je také možné dodat HSM modul (či koupí klient) do prostředí klienta, avšak v módu „black box“ se správou kvalifikovaného poskytovatele.

Testování a produkční prostředí



Služba v testovacím prostředí byla nasazena v dubnu.

Pro zájemce o testování je možné se obrátit na
remoteseal@ica.cz.

V produkčním prostředí je služba k dispozici od konce srpna.

Závěr

První certifikační autorita, a.s., (I. CA) was founded at the beginning of the year 2009. It has gained expertise and experience gained in implementation and operation of the system, which is the first one in a field of commercial providing of sophisticated services in the area of issuing and administration of digital certificates in the Czech Republic. The determining factors for high quality of provided services.

The most important step forwards was a successful completion of accreditation according to sense of Law 227/2000 about electronic signatures and authenticating edicts. The



Děkuji za pozornost.

Ing. Roman Kučera
kucera@ica.cz