Služba vzdáleného pečetění I.CA RemoteSeal

Ing. Roman Kučera
První certifikační autorita, a.s.
5. 9. 2018

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

I.CA RemoteSeal

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

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

QSealCD

HSM modulyy hodnocené jako QSealCD

List of QSCDs	
Name:	**PrimeSign Remote Signing Device/Core für qualifizierte Signaturen und Siegel**
Applicant	PrimeSign GmbH
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	20.11.2017
QSigCD designation expiry	Valid up to revocation by A-SIT
QSigCD designation report reference	A-SIT-VIG-17-067
QSigCD designation report	https://www.a-sit.at/downloads/736
Art.30.3.(b) notified alternative certification method	https://www.a-sit.at/pdfs/merkblatt_de.pdf 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.
QSealCD designation by	Zentrum für sichere Informationstechnologie - Austria (A-SIT)
QSealCD designation date	20.11.2017
QSealCD designation expiry	Valid up to revocation by A-SIT
QSealCD designation report reference	A-SIT-VIG-17-067
QSealCD designation report	https://www.a-sit.at/downloads/736
Art.30.3.(b) notified alternative certification method	https://www.a-sit.at/pdfs/merkblatt_de.pdf https://www.a-sit.at/pdfs/merkblatt_en.pdf
CC certification report reference	none

Name:	**Qualified Signature and Seal Creation Device (QSCD) LuxTrust's Qualified Remote Signature and Seal Creation Device, version 1.0**
Applicant	LuxTrust S.A., IVY Building, 13-15 Parc d'activités, L-8308 Capellen, Luxembourg
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	14.12.2017
QSigCD designation expiry	Valid up to revocation by A-SIT
QSigCD designation report reference	A-SIT-VIG-17-060
QSigCD designation report	https://www.a-sit.at/downloads/882
Art.30.3.(b) notified alternative certification method	https://www.a-sit.at/pdfs/merkblatt_de.pdf https://www.a-sit.at/pdfs/merkblatt_en.pdf
CC certification report reference	HSM (subcomponent) certified by OCSI http://www.ocsi.isticom.it/documenti/certificazioni/thales/rc_thales_nshield_v1.0.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	Zentrum für sichere Informationstechnologie - Austria (A-SIT)
QSealCD designation date	14.12.2017
QSealCD designation expiry	Valid up to revocation by A-SIT
QSealCD designation report reference	A-SIT-VIG-17-060
QSealCD designation report	https://www.a-sit.at/downloads/882
Art.30.3.(b) notified alternative certification method	https://www.a-sit.at/pdfs/merkblatt_de.pdf https://www.a-sit.at/pdfs/merkblatt_en.pdf
CC certification report reference	HSM (subcomponent) certified by OCSI http://www.ocsi.isticom.it/documenti/certificazioni/thales/rc_thales_nshield_v1.0.pdf

QSealCD

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 https://www.a-sit.at/pdfs/merkblatt_en.pdf
CC certification report reference	n.a.
Qualified Seal Creation Device (QSealCD)	no

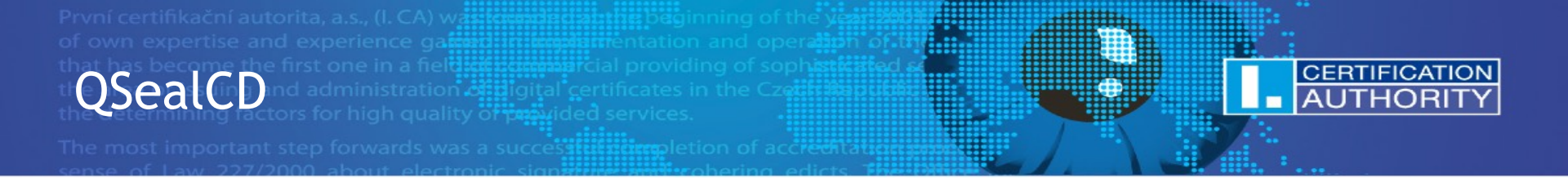
Name:	Qualified Signature and Seal Creation Device (QSCD) AliasLab CryptoAccelerator, release 3.5.1
Applicant	AliasLab SpA, via Cremona 27/6, 46100 Mantova, Italy
Qualified Signature Creation Device (QSigCD)	yes IMPORTANT NOTE: Device aimed to be managed on behalf of the user (signatory) by a QTSP that 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 https://www.a-sit.at/pdfs/merkblatt_en.pdf
CC certification report reference	HSM (subcomponent) certified by OCSI http://www.ocsi.isticom.it/documenti/certificazioni/thales/rc_thales_nshield_v1.0.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	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 https://www.a-sit.at/pdfs/merkblatt_en.pdf
CC certification report reference	HSM (subcomponent) certified by OCSI http://www.ocsi.isticom.it/documenti/certificazioni/thales/rc_thales_nshield_v1.0.pdf

QSealCD

Name:	Qualifizierte Signatur- und Siegelerstellungseinheit (QSEE) 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.
QSigCD designation by	Zentrum für sichere Informationstechnologie - Austria (A-SIT)
QSigCD designation date	16.03.2018
QSigCD designation expiry	Valid up to revocation by A-SIT
QSigCD designation report reference	A-SIT-VIG-17-076
QSigCD designation report	https://www.a-sit.at/downloads/912
Art.30.3.(b) notified alternative certification method	https://www.a-sit.at/pdfs/merkblatt_de.pdf 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.
QSealCD designation by	Zentrum für sichere Informationstechnologie - Austria (A-SIT)
QSealCD designation date	16.03.2018
QSealCD designation expiry	Valid up to revocation by A-SIT
QSealCD designation report reference	A-SIT-VIG-17-076
QSealCD designation report	https://www.a-sit.at/downloads/912
Art.30.3.(b) notified alternative certification method	https://www.a-sit.at/pdfs/merkblatt_de.pdf 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, Landstraßer 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.
QSigCD designation by	Zentrum für sichere Informationstechnologie - Austria (A-SIT)
QSigCD designation date	09.04.2018
QSigCD designation expiry	Valid up to revocation by A-SIT
QSigCD designation report reference	A-SIT-VIG-17-086
QSigCD designation report	https://www.a-sit.at/downloads/930
Art.30.3.(b) notified alternative certification method	https://www.a-sit.at/pdfs/merkblatt_de.pdf https://www.a-sit.at/pdfs/merkblatt_en.pdf
CC certification report reference	HSM (subcomponent) certified by OCSI http://www.ocsi.isticom.it/documenti/certificazioni/thales/rc_thales_nshield_v1.0.pdf
Qualified Seal Creation Device (QSealCD)	no

QSealCD



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/documenti/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/documenti/certificazioni/arx/rc_arx_cosign_82_v1.0.pdf
Security Target	http://www.ocsi.isticom.it/documenti/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/documenti/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/documenti/certificazioni/arx/rc_arx_cosign_82_v1.0.pdf
Security Target	http://www.ocsi.isticom.it/documenti/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

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

QSealCD

CERTIFICATION AUTHORITY

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 (QSigCD)	**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

- 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.

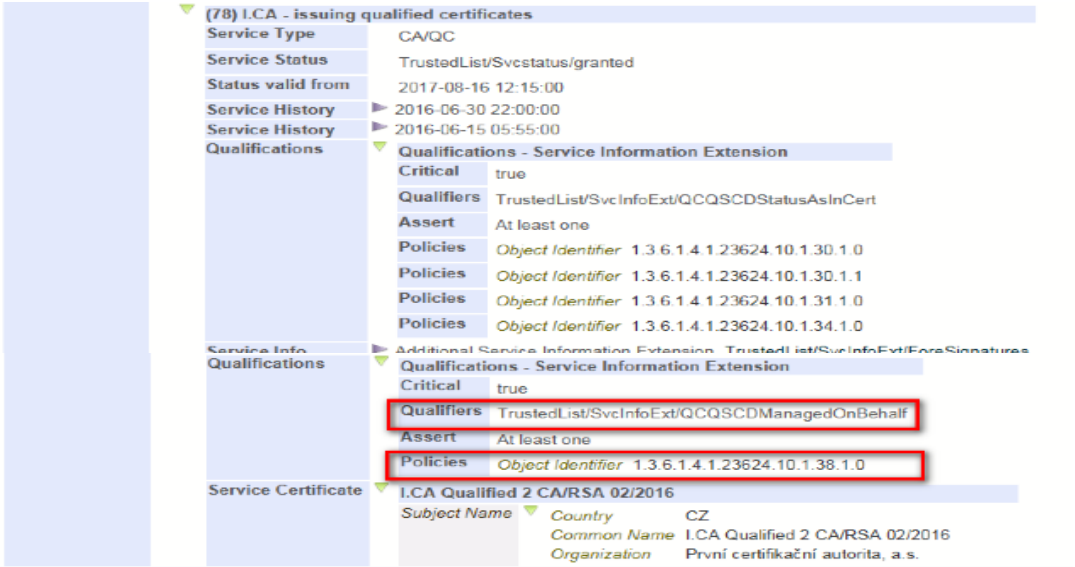
I.CA RemoteSeal

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

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



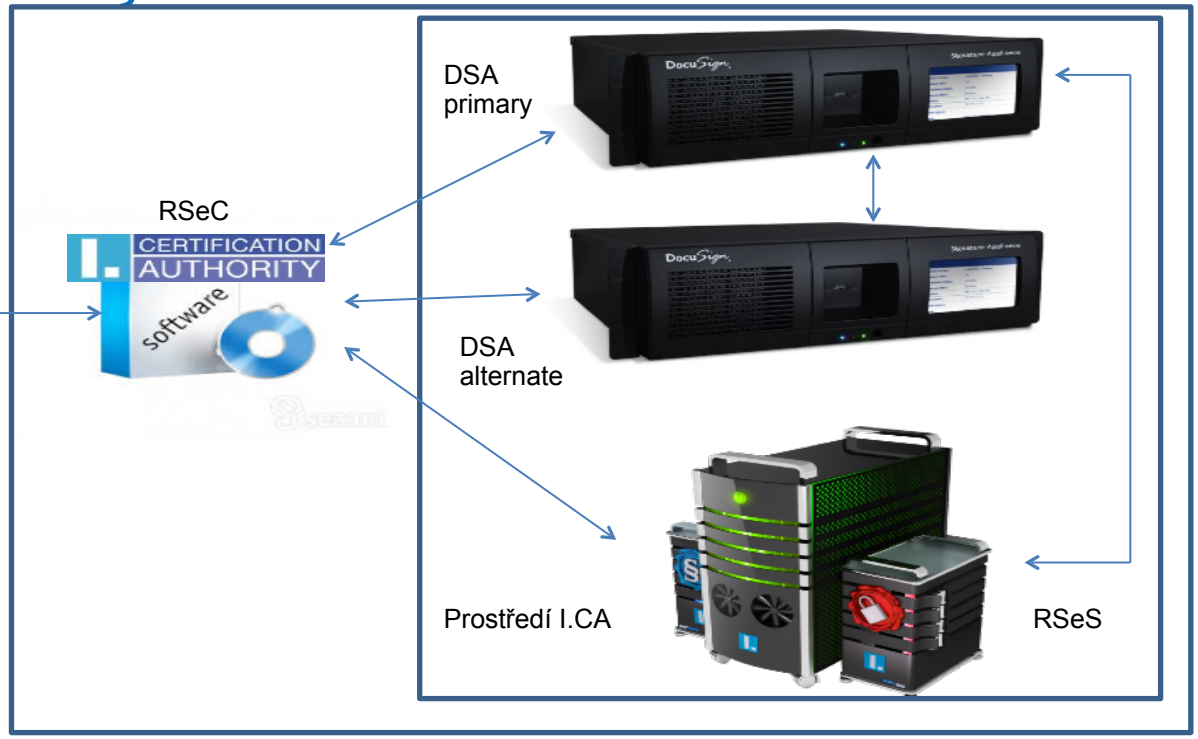
(78) I.CA - issuing qualified certificates

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/ForeSignatures
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:

Spisová služba



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 čtečce
- 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 Clienta

- Oprávněná osoba spustí dodávanou utilitu RSeActivationUtil

Aktivace RemoteSeal Clienta

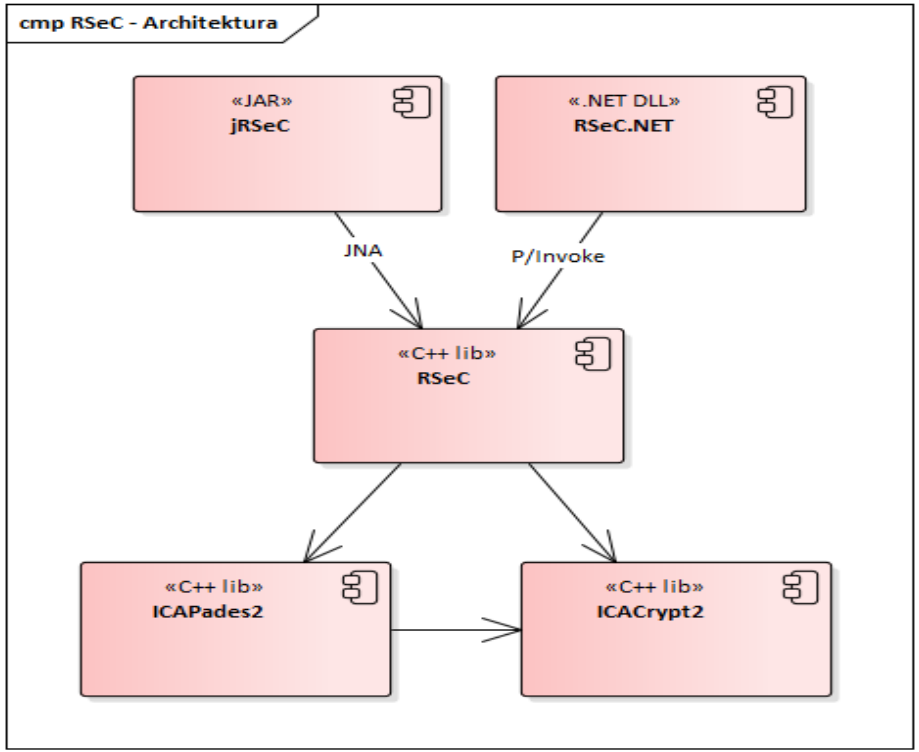
- Pro aktivaci RemoteSeal klienta spustí oprávněná osoba klienta dodávanou GUI utilitu
- Utilita vyzve uživatele k vložení aktivační karty, načež utilita:
  - Naváže spojení s RemoteSeal serverem pomocí oboustranně autentizovaného HTTPS s prvotním autentizačním certifikátem (uživatel je vyzván k zadání 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



- 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.

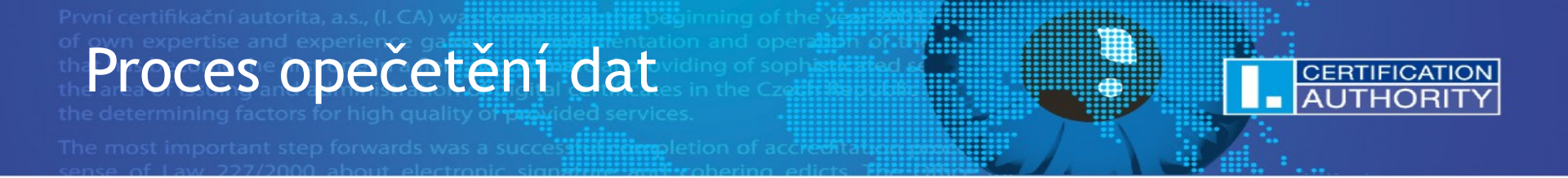
Implementaci řeší typicky dodavatel spisové služby za podpory I.CA

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

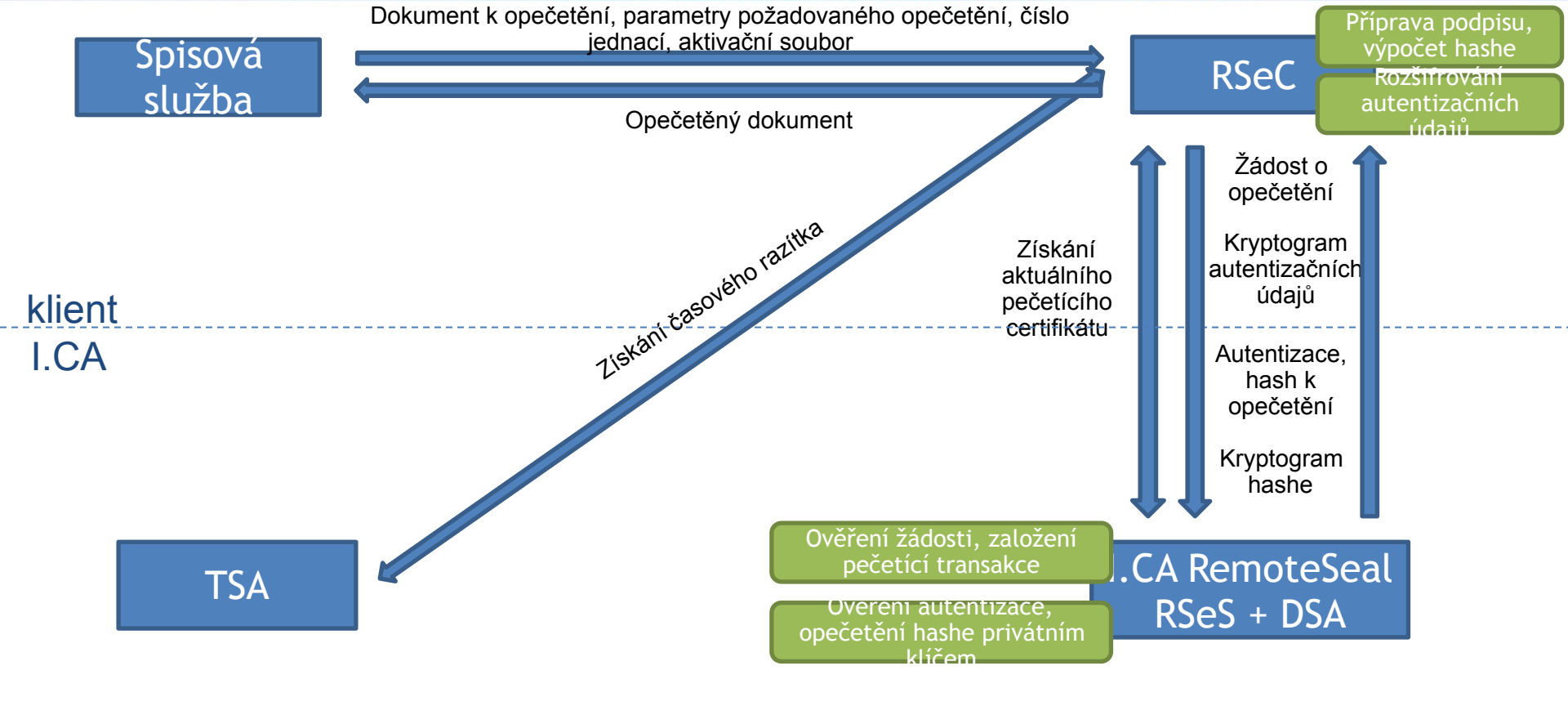
Opečetěný dokument

klient

I.CA

I.CA RemoteSeal

Proces opečetění dat



Automatické prodloužení služby

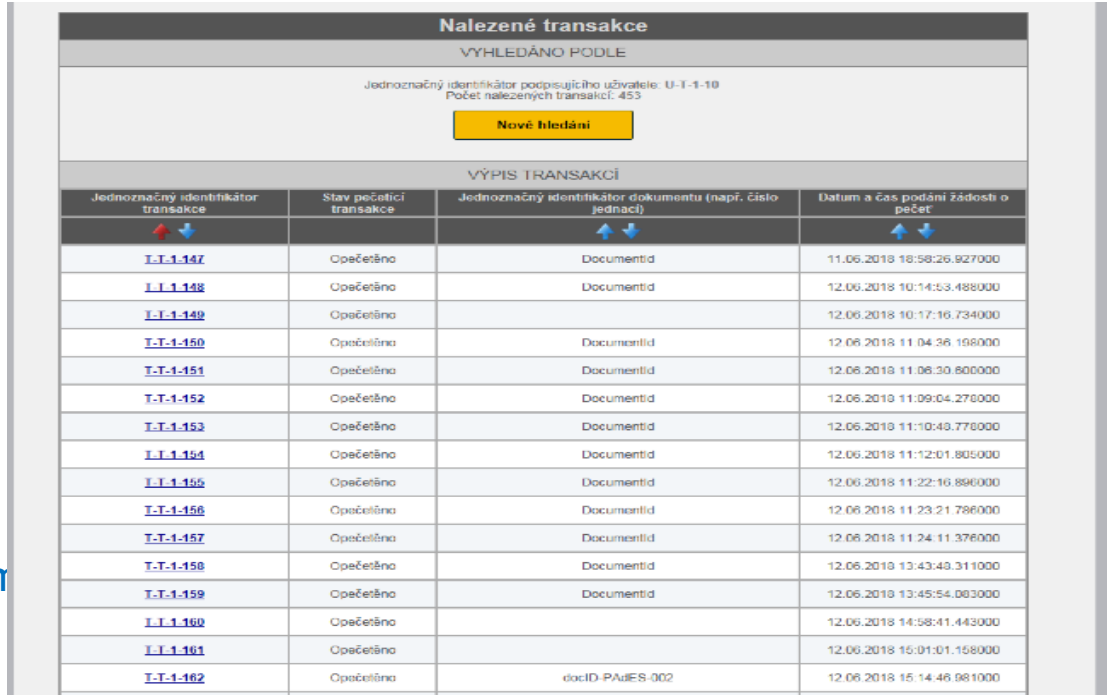
- RSeC disponuje funkcionalitou automatické obnovy autentizačního certifikátu.
- Před koncem platnosti autentizačního certifikátu je automaticky vytvořena žádost o následný certifikát, která je odeslána na I.CA.
- V rámci odeslání žádosti je veřejný klíč zaregistrován na RSeS a dojde k přešifrování autentizačních 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 jednacího
  - Prohlížet detailní informace zda a kdy a jakým certifikátem byl daný dokument opečetěn.



Nalezené transakce

VYHLEDÁNO PODLE

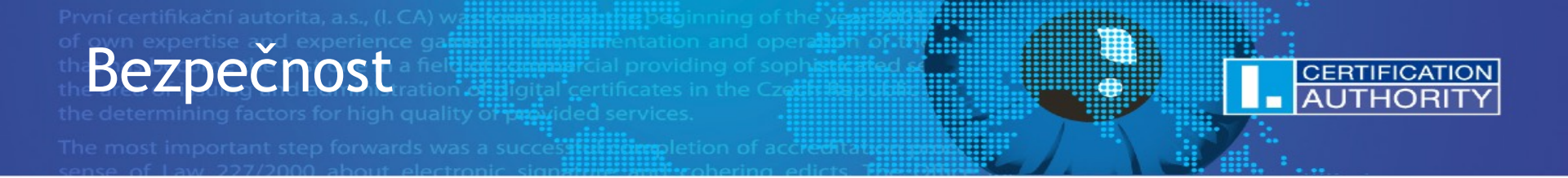
Jednoznačný identifikátor podpisujícího uživatele: U-T-1-10
Počet nalezených transakcí: 453

Nové hledání

VÝPIS TRANSAKCÍ

Jednoznačný identifikátor transakce	Stav pečetící transakce	Jednoznačný identifikátor dokumentu (např. číslo jednací)	Datum a čas podání žádosti o pečeť
T-T-1-147	Opečetěno	DocumentId	11.06.2018 18:58:26.927000
T-T-1-148	Opečetěno	DocumentId	12.06.2018 10:14:53.488000
T-T-1-149	Opečetěno		12.06.2018 10:17:16.734000
T-T-1-150	Opečetěno	DocumentId	12.06.2018 11:04:36.198000
T-T-1-151	Opečetěno	DocumentId	12.06.2018 11:06:30.600000
T-T-1-152	Opečetěno	DocumentId	12.06.2018 11:09:04.278000
T-T-1-153	Opečetěno	DocumentId	12.06.2018 11:10:43.778000
T-T-1-154	Opečetěno	DocumentId	12.06.2018 11:12:01.805000
T-T-1-155	Opečetěno	DocumentId	12.06.2018 11:22:16.896000
T-T-1-156	Opečetěno	DocumentId	12.06.2018 11:23:21.786000
T-T-1-157	Opečetěno	DocumentId	12.06.2018 11:24:11.376000
T-T-1-158	Opečetěno	DocumentId	12.06.2018 13:43:43.311000
T-T-1-159	Opečetěno	DocumentId	12.06.2018 13:45:54.083000
T-T-1-160	Opečetěno		12.06.2018 14:58:41.443000
T-T-1-161	Opečetěno		12.06.2018 15:01:01.158000
T-T-1-162	Opečetěno	docID-PAdES-002	12.06.2018 15:14:46.981000

Bezpečnost



- DSA je včetně svého řešení autentizace certifikováno jako řešení pro vytváření Kvalifikované elektronické pečetě.
- 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 klientského pohledu

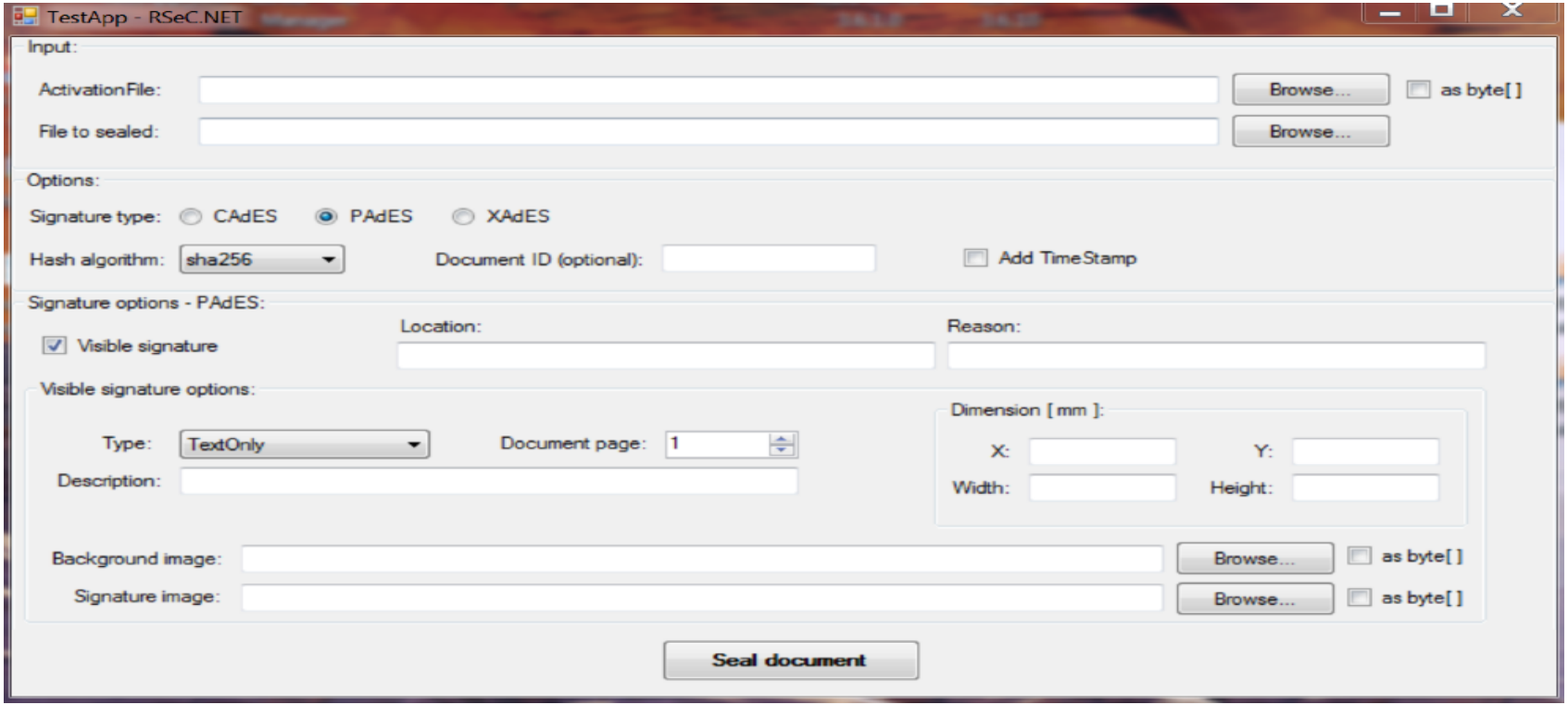
Nyní

- Oprávněná osoba požádá na RA o vydání systémového certifikátu
- Ten je instalován v prostředí klienta
- Spisová služba použije systémový certifikát pro označkování 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



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.

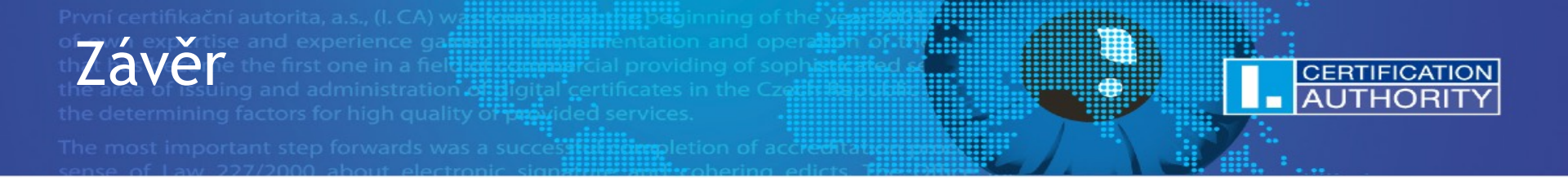
Testování a produkční prostředí

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



Děkuji za pozornost.

Ing. Roman Kučera

kucera@ica.cz