



SEMINÁŘ: KVALIFIKOVANÉ PEČETĚNÍ - NÁHRADA ELEKTRONICKÝCH ZNAČEK

SITUACE A ŘEŠENÍ OVM



Povinnost používání kvalifikovaných elektronických pečetí VS

Zákon č. 297/2016 Sb. - §8:

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. Povinnost použití pro VS nejpozději od 20. září 2018.

Kvalifikovaná elektronická pečeť dle nařízení eIDAS:

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



Proč je stanovena povinnost kvalifikovaného el. pečetění pro VS

- Zajištění autenticity elektronických dokumentů obsahujících právní jednání veřejné správy, pro které není stanovena povinnost podpisu nebo povinnost podpisu nevyplývá z povahy právního jednání.



Pozn. společně s kvalifikovanou elektronickou pečetí je nutné opatřit dokument kvalifikovaným elektronickým časovým razítkem.



Proč právě kvalifikovaná elektronická pečeť ?

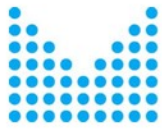
- Nařízení eIDAS: „Kvalifikovaná elektronická pečeť založená na kvalifikovaném certifikátu vydaném v jednom členském státě se uznává jako kvalifikovaná elektronická pečeť ve všech ostatních členských státech“.
- Nařízení eIDAS: „U kvalifikované elektronické pečeti platí domněnka integrity dat a správnosti původu těch dat, s nimiž je kvalifikovaná elektronická pečeť spojena“.



UZNATELNOST
V RÁMCI



EVROPSKÁ UNIE



Co je potřeba pro vytvoření kvalifikované el. pečeti

Kvalifikovaná elektronická pečeť dle nařízení eIDAS:

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

- ✓ V ČR existují tři kvalifikovaní poskytovatelé služeb vytvářejících důvěru, kteří vydávají / mohou vydávat kvalifikované certifikáty pro elektronické pečeti.

➤ Kvalifikovaný prostředek pro vytváření elektronických pečetí

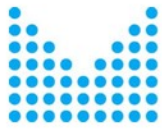
- ✓ Seznam kvalifikovaných prostředků pro vytváření elektronických pečetí je zveřejněn na unijním seznamu SSCD/QSCD: <https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds>.



Typy kvalifikovaných prostředků pro vytváření elektronických pečetí

Dva typy:

- Kvalifikovaný prostředek v držení pečetící osoby (pokud jsou data pro vytváření elektronických pečetí uchovávána v prostředí spravovaném zcela, nikoli však nutně výhradně uživatelem).
- Kvalifikovaný prostředek na dálku (pokud data pro vytváření elektronických pečetí spravuje kvalifikovaný poskytovatel služeb vytvářejících důvěru jménem pečetící osoby).



Kvalifikovaný prostředek pro vytváření el. pečeti

Kvalifikovaný prostředek pro vytváření elektronických pečetí

✓ Na unijním seznamu SSCD/QSCD: <https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds> je zveřejněno několik kvalifikovaných prostředků pro vytváření el. pečetí:

✓ Čipové karty.

✓ Kvalifikované prostředky pro vytváření elektronických pečetí na dálku, které se považují za kvalifikované, pouze pokud jsou spravovány jménem pečetící osoby kvalifikovaným poskytovatelem.



Bohužel se aktuálně na seznamu nenachází HSM modul s certifikací pro vytváření kvalifikovaných elektronických pečetí, kdy HSM modul je spravován přímo pečetící osobou (HSM modul

je v držení pečetící osoby)

Kvalifikovaný prostředek musí být podporován rovněž ze strany kvalifikovaného poskytovatele. Samotné jeho uvedení na seznamu ještě neznamená, že jej poskytovatel musí podporovat



Unijní seznam SSCD/QSCD prostředků.

Kvalifikovaný prostředek v držení pečetící osoby k 2.4.2018:

- **SafeNet eToken 7300 v.9.1.2 (Athena IDProtect/OS755 Java Card on INSIDE Secure AT90SC25672RCT-USB Microcontroller). Software platform: IDSign applet – Java Card application for e-seal/-stamp. Estonsko. Token se již nevyrábí.**

Name:	Digital stamp (issued from 16.06.2016): (Conformity assessed as SSCD, used also for signing by legal entities) Hardware platform: SafeNet eToken 7300 v.9.1.2 (Athena IDProtect/OS755 Java Card on INSIDE Secure AT90SC25672RCT-USB Microcontroller) Software platform: IDSign applet – Java Card application for e-seal/-stamp
Applicant	AS Sertifitseerimiskeskus
SSCD designation expiry	Valid until revocation by Estonian Ministry of Economic Affairs and Communications
SSCD designation report reference	16-0183
SSCD designation report	https://www.mkm.ee/sites/default/files/table_of_sscd_in_estonia.pdf
CC certification report reference	ANSSI-CC-2011/45
CC certification report	https://www.commoncriteriaportal.org/files/epfiles/ANSSI-CC_2011-45en.pdf



Unijní seznam SSCD/QSCD prostředků.

Kvalifikovaný prostředek v držení pečetící osoby k 2.4.2018 :

- **ID.me 1.28 on IDeal Citiz MOSID v2.1.1. - SAFRAN IDENTITY & SECURITY. Francie.**

Name:	ID.me 1.28 on IDeal Citiz MOSID v2.1.1
Applicant	SAFRAN IDENTITY & SECURITY
Qualified Signature Creation Device (QSigCD)	yes
QSigCD designation by	Agence Nationale de Sécurité des Systèmes d'Information (ANSSI)
QSigCD designation date	01.04.2017
QSigCD designation expiry	01.04.2022

Qualified Seal Creation Device (QSealCD)	yes
QSealCD designation by	Agence Nationale de Sécurité des Systèmes d'Information (ANSSI)
QSealCD designation date	01.04.2017
QSealCD designation expiry	01.04.2022
QSealCD designation report reference	2448/ANSSI/SDE
QSealCD designation report	-
CC certification report reference	ANSSI-CC-2016/70
CC certification body	ANSSI
CC certification date	15.11.2016
CC certification report	ANSSI-CC-2016/70



Unijní seznam SSCD/QSCD prostředků.

Kvalifikovaný prostředek v držení pečetící osoby k 2.4.2018 :

- **Applet ID.me 1.12 sur la plateforme IDEal Citiz v2.I. - SAFRAN IDENTITY & SECURITY. Francie.**

Name:	Applet ID.me 1.12 sur la plateforme IDEal Citiz v2.I
Applicant	SAFRAN IDENTITY & SECURITY
Qualified Seal Creation Device (QSigCD)	yes
QSealCD designation by	Agence Nationale de Sécurité des Systèmes d'Information (ANSSI)
QSealCD designation date	01.04.2017
QSealCD designation expiry	01.04.2022
QSealCD designation report reference	2447/ANSSI/SDE
QSealCD designation report	-
CC certification report reference	ANSSI-CC-2016/64
CC certification body	ANSSI
CC certification date	11.10.2016
CC certification report	ANSSI-CC-2016/64



Unijní seznam SSCD/QSCD prostředků.

Kvalifikovaný prostředek v držení pečetící osoby k 2.4.2018 :

- **Produit Gemalto "IAS Classic V4.4 with MOC Server 1.1 on MultiApp V4" embarqué sur le microcontrôleur M7892 G12**

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 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

Předpokládáme, že v dohledné době budou čipovou kartu někteří z kvalifikovaných poskytovatelů služeb vytvářejících důvěru v ČR podporovat.



Unijní seznam SSCD/QSCD prostředků.

Kvalifikovaný prostředek v držení pečetící osoby v držení pečetící osoby k 2.4.2018 :

- NXP ASEPCOS-CNS v1.84 in SSCD configuration on NXP P60D080PVG dual interface microcontroller - NXP Semiconductors Germany GmbH. Francie.

Name:	NXP ASEPCOS-CNS v1.84 in SSCD configuration on NXP P60D080PVG dual interface microcontroller
Applicant	NXP Semiconductors Germany GmbH

Qualified Seal Creation Device (QSigCD)	yes
QSealCD designation by	Agence Nationale de Sécurité des Systèmes d'Information (ANSSI)
QSealCD designation date	19.01.2018
QSealCD designation expiry	02.11.2026
QSealCD designation report reference	10248/ANSSI/SDE
QSealCD designation report	-
CC certification report reference	ANSSI-CC-2016/63
CC certification body	ANSSI
CC certification date	02.11.2016
CC certification report	ANSSI-CC-2016/63



Unijní seznam SSCD/QSCD prostředků.

Kvalifikovaný prostředek pro vytváření el. pečetí na dálku k 2.4.2017 :

- PrimeSign Remote Signing Device/Core für qualifizierte Signaturen und Siegel. Rakousko.
- Qualified Signature and Seal Creation Device (QSCD) LuxTrust's Qualified Remote Signature and Seal Creation Device, version 1.0. Rakousko.
- Qualified Signature and Seal Creation Device (QSCD) AliasLab CryptoAccelerator, release 3.5.1. Rakousko.
- ARX CoSign v8.2. Itálie.



Jak splnit požadavky zák. č. 297/2016 Sb. ?

- Využití služby vytváření kvalifikovaných elektronických pečetí na dálku, kterou plánuje nasadit jeden z kvalifikovaných poskytovatelů služeb vytvářejících důvěru v ČR.
- Využití certifikovaných čipových karet jako kvalifikovaných prostředků pro vytváření elektronických pečetí (určeno spíše pro subjekty, které potřebují vytvořit řádově několik kvalifikovaných elektronických pečetí denně - nutnost zadání PIN pro vytvoření kvalifikované elektronické pečeti).
- Využít služby poskytované kvalifikovanými poskytovateli služeb vytvářejících důvěru usazenými v zahraničí:
 - možnost využití služeb vytváření kvalifikovaných elektronických pečetí na dálku,
 - možnost vydání kvalifikovaného certifikátu pro elektronickou pečeť společně s kvalifikovaným



Služba vytváření kvalifikovaných elektronických pečetí na dálku.

Dle hledání na webu:

- Lucembursko -LuxTrust S.A. - <https://www.luxtrust.com/trust-services/e-seal/>
- Polsko - Asseco Data Systems S.A. Certum - CA (https://www.tuvit.de/fileadmin/Content/TUV_IT/zertifikate/en/9756UE_s_01.pdf)
- Pravděpodobně existují i další kvalifikovaní poskytovatelé nabízející službu vydávání kvalifikovaných elektronických pečetí na dálku.



Vydávání QC pro el. pečeť a QSealCD v zahraničí

Dle hledání na webu:

- Řecko, TSP ADACOM (<https://eshop.adacom.com/e-seal.html>).
Prostředek Safenet 5110.
- Estonsko, TSP SK ID Solutions AS (<https://www.sk.ee/en/services/Digital-stamp/e-seal-on-qscd/>). Prostředek SafeNet eToken 7300 – nahlášen v unijním seznamu. Už se ale nevyrábí.
- Slovensko, např. TSP DISIG (<http://disig.sk/sk/produkty/elektronicky-podpis/kvalifikovany-certifikat/>), pro kvalifikovanou el. pečeť vyžadováno: „KC je možné uložit na certifikovanou čipovou kartu alebo do HSM modulu“
- Pravděpodobně existují i další kvalifikovaní poskytovatelé nabízející službu vydávání kvalifikovaných elektronických pečetí na dálku.



[Průběžně aktualizované informace k problematice kvalifikovaných el. pečeti:](http://www.mvcr.cz/clanek/informace-k-problematice-kvalifikovanych-el-pecti)

<http://www.mvcr.cz/clanek/informace-k-problematice-kvalifikovanych-elektronickych-peceti.aspx>



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Děkujeme Vám za pozornost.