Doporučený postup při pořizování USB tokenů nebo čipových karet pro kvalifikovaný podpis podle EU nařízení eIDAS a zákona č. 297/2016 Sb.

Nejčastější dotazy:

Koho se povinnost používat kvalifikovaný elektronický podpis týká?
Zjednodušeně řečeno všech pracovníků státní správy a samosprávy (obecně OVM), kteří ve své pracovní náplni mají podepisování elektronických dokumentů (emailové komunikace) zakládající právní jednání příslušného orgánu. Kvalifikovaný podpis bude také potřebný pro přístup do některých agend Czech POINTu. Pro přesnou definici doporučujeme prostudovat tzv. adaptační zákon č. 297/2016 Sb.

Od kdy je používání kvalifikovaného podpisu povinné?
Pro výše uvedené skupiny osob je používání kvalifikovaného podpisu (založeném na kvalifikovaném certifikátu, který je uložen v bezpečném tokenu/čipové kartě – tzv. QSCD zařízení) povinné od 20. září 2018. Žádná výjimka ani posunutí termínu není možné.

Co pro vytváření kvalifikovaného podpisu potřebuji?
Každý zaměstnanec, který bude opatřovat elektronické dokumenty kvalifikovaným podpisem (= k odesílanému emailu připojí svůj kvalifikovaný podpis) nebo se bude přihlašovat do agend vyžadujících kvalifikovaný podpis, potřebuje:

- bezpečný prostředek pro vytváření elektronických podpisů (tzv. QSCD prostředek), tedy QSCD token nebo čipovou kartu, na kterém bude uložený kvalifikovaný certifikát zaměstnance
- kvalifikovaný certifikát (dále také jen „QC“) vystavený do QSCD prostředku státem uznanou autoritou, např. PostSignum České pošty
- obslužný software (program zvaný SAC) nainstalovaný na počítači před tím, než se na něm začne používat QSCD prostředek s QC

Máme používat USB tokeny nebo čipové karty – co je lepší?
Z pohledu bezpečnosti jsou obě řešení zcela rovnocenné. Důležité je používat QSCD prostředky, které splňují velmi přísné bezpečnostní požadavky evropského nařízení eIDAS.
Těmi jsou např. USB tokeny „SafeNet eToken 5110 CC (940)“ nebo čipové karty „Gemalto IDPrime MD 840“.

USB tokeny jsou velmi praktické, můžeme je připnout na běžný svazek klíčů. Stačí je připojit na standardní USB port, kterým jsou vybaveny všechny počítače. Nevyžadují žádnou speciální čtečku.

Čipové karty potřebují pro používání navíc čtečku čipových karet (doporučujeme osvědčený model Gemalto IDBridge CT30), která se připojuje k USB portu počítače. Výhodou čipové karty je možnost zabudování bezkontaktního čipu do těla karty. Bezkontaktní čip se používá k evidenci docházky, odemykání dveří, vjezdu na parkoviště apod. Na čipové karty je také možné umístit potisk podle požadavků zákazníka.

Co je dobré vědět před pořízením tokenů/karet?

- Kvalifikovaný podpis vytváří vždy fyzická osoba, nikoli právnická. Bezpečný QSCD token/kartu proto musí vlastnit každý zaměstnanec, kterého se to týká. Token není možné sdílet nebo si ho půjčovat.
- Do tokenu/karty není možné naimportovat dosud používané starší QC (i když jsou ještě platné) uložené buď v operačním systému počítače nebo ve starších tokenech SafeNet iKey 4000.
  S nasazením QSCD prostředku souvisí také povinnost pořízení nového QC.

- Zakoupené tokeny/karty mají v sobě nahraný tzv. „Servisní klíč“ České pošty.
  Pozor – pokud dojde ke smazání Servisního klíče, nebude možná vyžádat do tokenu vystavení nového kvalifikovaného certifikátu!
- Tokeny/karty mají nastaveny iniciální hesla (PIN, PUK, QPIN, QPUK) a ta jsou uvedena v dokumentaci. Důrazně doporučujme tato hesla po pořízení tokenu změnit a nahradit dostatečně silným heslem!
- Nově nastavená hesla si pečlivě zaznamenejte a uložte na bezpečné místo. Při zapomenutí hesel PUK a QPUK a jejich opakovaném špatném zadání dojde k nevratnému zablokování tokenu/karty a jejich znehodnocení!

Jak postupovat při zavádění nových tokenů/karet a pořizování nových kvalifikovaných certifikátů?

1) Zjistěte, kolika pracovníků vašeho úřadu se povinnost používat kvalifikovaný podpis bude týkat. Hromadné pořízení QSCD prostředků bývá výhodnější díky množstevním slevám.
2) Objednejte si u svého dodavatele potřebný počet USB tokenů „SafeNet eToken 5110 CC (940)“ nebo čipových karet „Gemalto IDPrime MD 840“ a čteček čipových karet.
3) Po obdržení zásilky tokenů si softwarovou podporu (middleware) tokenů SafeNet Authentication Client (dále jen SAC) stáhněte z odkazu v emailu, který obdržíte nebo z odkazu uvedeného na licenční kartě zakoupené s tokenem / čipovou kartou.
   Při instalaci ovládacího software SAC do počítače postupujte podle Uživatelské příručky.
4) Na této adrese: https://www.postsignum.cz/online_generovani_zadosti.html si stáhnete program iSignum, který slouží k on-line generování žádosti o vydání QC. Podrobný návod k programu iSignum je zde: http://www.postsignum.cz/isignum.html?step=2