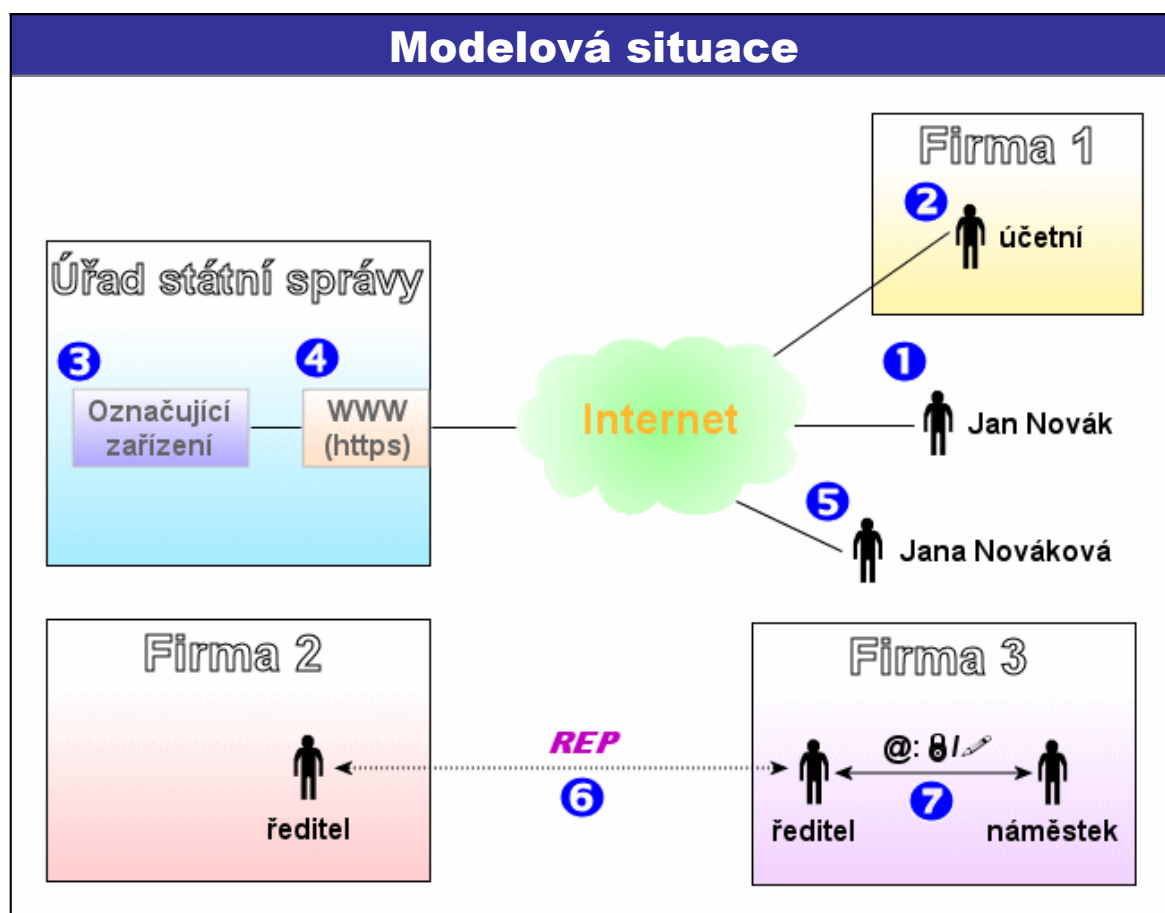


Použití certifikátů vydávaných autoritami PostSignum QCA a PostSignum VCA

(stav od prosince 2005)

Certifikační autorita **Postsignum QCA** vydává čtyři typy kvalifikovaných certifikátů.
Certifikační autorita **Postsignum VCA** vydává pět typů komerčních certifikátů.



Vysvětlivky:

https Pokud se na Internetu setkáte s adresou začínající na **https**, znamená to, že komunikace mezi vámi a daným WWW serverem je při průchodu Internetem (nebo jinou sítí) šifrována, a tedy chráněna před prozrazením přenášeného obsahu.

Tato komunikace se používá zejména tam, kde je potřeba přenášet citlivá data, např. v internetovém bankovníctví.

REP Česká pošta nabízí aplikaci REP, pomocí které si dvě komunikující strany mohou zasílat zprávy a soubory prokazatelným způsobem v podepsané a šifrované podobě. Odesílatel zprávy je informován o jejím vyzvednutí a přečtení příjemcem.

REP lze tak přirovnat k elektronické formě poštovní zprávy s doručenkou.

1 Fyzická nepodnikající osoba chce komunikovat s úřady státní správy.

Jan Novák chce začít komunikovat s úřady státní správy (např. podávat elektronicky daňová přiznání).

Pro tyto účely bude požadovat vydání kvalifikovaného certifikátu autoritou [PostSignum QCA](#) podle certifikační politiky [Certifikáty pro ověření elektronického podpisu fyzické osoby](#).

Další možnosti použití certifikátu:

Tento certifikát lze použít i pro komunikaci s jinými organizacemi (osobami) vyžadujícími (uznávajícími) kvalifikovaný certifikát.

2 Zástupce/zaměstnanec právnické osoby (organizace) chce komunikovat s úřady státní správy.

Ředitel Firmy 1 stanoví, že účetní bude posílat úřadům státní správy požadované informace o zaměstnancích Firmy 1.

Pro tyto účely si účetní nechá vydat kvalifikovaný certifikát autoritou [PostSignum QCA](#) podle certifikační politiky [Certifikáty pro ověření elektronického podpisu zaměstnance](#).

Další možnosti použití certifikátu:

Tento certifikát lze použít i pro komunikaci s jinými organizacemi vyžadujícími (uznávajícími) kvalifikovaný certifikát.

3 Úřad státní správy chce zřídit elektronickou podatelnu.

Úřad státní správy hodlá zřídit elektronickou podatelnu pro příjem a odesílání dat. Aby mohl označovat tato data bez trvalé přítomnosti obsluhy, nechá pro své označující zařízení vydat kvalifikovaný systémový certifikát autoritou [PostSignum QCA](#) podle certifikační politiky [Certifikáty organizace pro ověření elektronické značky](#).

Další možnosti použití certifikátu:

Tento certifikát lze vydat obecně pro všechna zařízení určená k vytváření elektronických značek (ve smyslu definice v zákonu o elektronickém podpisu č. 227/2000 Sb.).

4 Úřad státní správy chce zabezpečit webovou komunikaci se zákazníky.

Občané komunikují s úřadem státní správy prostřednictvím stránek na jeho webovém serveru. Aby byla tato komunikace zabezpečena, aktivuje se zabezpečený kanál. Pro autentizaci webového serveru při otevírání zabezpečeného kanálu se vydá komerční certifikát autoritou [PostSignum VCA](#) podle politiky [Politika pro certifikáty technologických komponent](#).

Další možnosti použití certifikátu:

Tento certifikát lze vydat obecně pro všechna zařízení za účelem zajištění zabezpečené (autentizované a šifrované) komunikace (webové servery, e-mailové servery, adresářové servery a další).

5 Fyzická nepodnikající osoba chce komunikovat s jinou fyzickou nepodnikající osobou.

Jana Nováková chce začít komunikovat s Janem Novákem. Jelikož se jedná o fyzické osoby, postačí pro zabezpečení komunikace vydání komerčního certifikátu autoritou [PostSignum VCA](#) podle certifikační politiky [Politika pro certifikáty fyzických osob](#).

Další možnosti použití certifikátu:

Tento certifikát lze použít i pro komunikaci s jinými organizacemi (osobami) vyžadujícími (uznávajícími) komerční certifikát.

6 Zástupci/zaměstnanci dvou organizací chtějí mezi sebou komunikovat prostřednictvím aplikace REP.

Ředitelé Firmy 2 a Firmy 3 si zakoupí aplikaci REP, aby mohli mezi sebou bezpečně a prokazatelně komunikovat. Pro aplikaci jsou vydávány certifikáty na základě vybrané varianty REP Klienta.

Ředitel Firmy 2 si pořídil [REP Klient Standard](#). Bude potřebovat komerční certifikáty vydané autoritou [PostSignum VCA](#) podle certifikačních politik [Politika pro certifikáty zaměstnanců](#), [Politika pro šifrovací certifikáty skupin osob](#) a [Politika pro certifikáty technologických komponent](#).

Ředitel Firmy 3 si pořídil [REP Klient Lite](#). Bude potřebovat certifikát vydaný autoritou [PostSignum VCA](#) podle certifikační politiky [Politika pro certifikáty zaměstnanců](#).

Další možnosti použití certifikátu:

Aplikaci REP lze používat pro komunikaci s jakoukoliv osobou, která také vlastní REP Klienta.

Certifikát vydaný podle certifikační politiky [Politika pro certifikáty zaměstnanců](#) lze použít pro zabezpečení jakékoliv (například e-mailové) komunikace.

Certifikát vydaný podle certifikační politiky [Politika pro šifrovací certifikáty skupin osob](#) lze použít pro šifrování dat s tím, že k odpovídajícímu soukromému klíči může mít přístup více osob nebo procesů zajišťujících provoz konkrétní služby.

7 Zástupci/zaměstnanci organizace chtějí mezi sebou komunikovat prostřednictvím šifrovaného/podepsaného e-mailu.

Pro zabezpečení e-mailové komunikace (šifrování a podepisování zpráv) si musí obě strany nechat vydat komerční certifikát autoritou [PostSignum VCA](#) podle certifikační politiky [Politika pro certifikáty zaměstnanců](#).

Další možnosti použití certifikátu:

Vydané certifikáty lze používat obecně pro zabezpečení jakékoliv komunikace (založené na certifikátech) s jakoukoliv osobou.