Detailný postup pre získanie následného certifikátu

Verzia dokumentu: **1.0**

Dátum: **15. 4. 2004**

Vytlačené v Bratislave, Slovenská republika

Tento dokument neprešiel jazykovou úpravou.

Detailný postup na získanie následného osobného certifikátu PSCA

Definícia následného certifikátu

Za **následný** osobný certifikát sa považuje taký osobný certifikát, ktorý bol vydaný počas posledných 30 dní platnosti iného osobného certifikátu patriaceho danej osobe, pričom **následný certifikát má rovnaké hodnoty vo všetkých položkách** (t.j. položkách Štát, Mesto, Firma, Útvar vo firme, Meno a Priezvisko, Email) **rozlišovacieho mena** (DN, distinguished name) **certifikátu** ako daný certifikát, ktorý sa blíži ku koncu svojej platnosti. **Osobitný dôraz sa pritom kladie na zhodu hodnôt položiek "Meno a Priezvisko" (t.j. položka CN, Common Name) a "Email" (t.j. položka E).**

K certifikátu pre server nie je možné vydať následný certifikát.

Zákazník (žiadateľ o následný certifikát) vykoná nasledovné kroky ako prípravu na získanie následného certifikátu:

- oboznámi sa s týmto postupom, prípadne s princípmi a návodmi pre získanie certifikátu

- zákazník musí mať platný osobný certifikát PSCA, ktorého doba platnosti skončí do 30 dní od podania žiadosti o následný certifikát a musí mať možnosť podpisovať e-maily s použitím tohto certifikátu (t.j. musí mať prístup k svojmu privátnemu kľúču patriacemu k danému certifikátu)

- zákazník si **na svojom počítači** pomocou vyhovujúceho prehliadača vygeneruje prostredníctvom webu PSCA (www.psca.sk) **novú** žiadosť o osobný certifikát, ktorá spĺňa podmienky na vydanie následného certifikátu uvedené vyššie v definícii následného certifikátu, a zazálohuje si ju. (Upozorňujeme, že žiadosť o certifikát resp. v nej sa nachádzajúci verejný kľúč, pre ktorý už bol vydaný certifikát, nemôže byť z bezpečnostných dôvodov použitá opakovane na vydanie iného certifikátu a bude na RA odmietnutá!)

  Pritom si treba poznačiť údaj SessionId – je to číselný reťazec, pred ktorým je reťazec „psca-„ , ktorý jednoznačne identifikuje vygenerovanú žiadosť o certifikát. Prehliadač tento údaj vypíše po tom, čo úspešne vygeneruje žiadosť o certifikát. Žiadosť musí povinne obsahovať vhodne vyplnené položky "Meno a Priezvisko" a "Email". Jednotlivé položky pritom vyplní tak, aby zadané hodnoty boli v súlade s Certifikačným poriadkom PSCA s dôrazom na jeho časť 3.1.2.

  Aby sa vyhol zamietnutiu žiadosti o certifikát na RA, pri zadávaní hodnôt do položiek žiadosti o certifikát by mal žiadateľ o certifikát mať na zreteli, že RA bude skúmať žiadosť o certifikát s ohľadom na hodnoty položiek ešte platného certifikátu žiadateľa,

t.j. či sa daná žiadosť o certifikát dá považovať za žiadosť o následný certifikát v zmysle definície následného certifikátu. Všetky údaje sa musia zadávať bez diakritiky (mäkčene, dĺžne a pod.). Použitie špeciálnych znakov (napr. čiarka, pomlčka, =, / a iné) treba obmedziť na minimálnu nutnú mieru, odporúčame prípadne tieto znaky použiť až po dohode s PSCA, v opačnom prípade si PSCA vyhradzuje právo odmietnuť takúto žiadosť o certifikát.

V poli Firma sa nesmie použiť znak čiarka.

- Zákazník (žiadateľ o certifikát) pošle na RA žiadosť o následný certifikát **podpísaným e-mailom, pričom na podpis e-mailu musí použiť svoj platný osobný certifikát PSCA (resp. presnejšie povedané privátny kľúč patriaci k tomuto certifikátu)**. E-mail adresa RA je daná touto konvenciou: raxx@psca.sk kde xx je autoznačka sídla danej RA, teda napr. raba@psca.sk v prípade RA Bratislava. Podpísaný a prípadne aj šifrovaný e-mail so žiadosťou o následný certifikát **musí obsahovať nasledovné údaje (žiadosť o certifikát s neúplnými údajmi RA odmietne)**:
  - Jednoznačný prejav vôle, že odosieľateľ si želá, aby mu PSCA vydala následný osobný certifikát, napr. text: ”žiadam o vydanie následného osobného certifikátu PSCA”
  - Ako prílohu mailu (binary attachment) žiadosť o certifikát vygenerovanú prehliadačom
  - údaj SessionId – je to číselný reťazec, pred ktorým je reťazec „psca-„ , ktorý jednoznačne identifikuje vygenerovanú žiadosť o certifikát. Prehliadač tento údaj vypíše po tom, čo úspešne vygeneruje žiadosť o certifikát.
  - Jednoznačné prehlásenie, že osobné a kontaktné údaje (t.j. meno a priezvisko, úplná adresa, PSČ, číslo telefónu, číslo občianskeho preukazu resp. pasu) žiadateľa o certifikát sa nezmenili, vo forme textu: ”Potvrdzujem týmto, že moje osobné ani kontaktné údaje sa nezmenili”
    Ak od vydania platného osobného certifikátu žiadateľa došlo k zmene niektorého vyššie uvedeného osobného a/alebo kontaktného údaja, žiadateľ je povinný uviesť v maile tieto všetky osobné a/alebo kontaktné údaje, **ktoré sa zmenili**:

    meno a priezvisko,
    úplná adresa vrátane PSČ,
    číslo telefónu a prípadne aj faxu,
    údaje o svojich dvoch osobných dokladoch totožnosti podľa ustanovení Certifikačného poriadku PSCA (občiansky preukaz, pas, vodičský preukaz, rodný list, preukaz vojaka), konkrétne číslo dokladu, kto doklad vydal a dokedy je doklad platný (ak je tento údaj v doklade uvedený)

- Odporúča sa, aby si zákazník ešte pred odoslaním žiadosti na RA overil a vyjasnil prípadné pochybnosti a problémy, najmä tie, ktoré týkajú vhodnosti hodnôt jednotlivých položiek v žiadosti o certifikát.

- Po upovedomení od RA, že si môže prevziať svoj certifikát, si zákazník dohodne termín návštevy RA (telefonicky, e-mailom). Zákazník si môže prevziať svoj následný certifikát len na RA, prostredníctvom ktorej podal žiadosť o daný certifikát.

Zákazník v dohodnutom termíne príde na RA, pričom vezme so sebou a predloží:

- 3,5" disketu na prevzatie certifikátu, v prípade vzájomnej dohody mu RA certifikát môže zaslať e-mailom

- občiansky preukaz alebo iný doklad totožnosti resp. aj úradne overená plná moc na prevzatie certifikátu v prípade zastupovania zákazníka na RA podľa ustanovení časti 3 Certifikačného poriadku PSCA

- príslušnú peňažnú čiastku, ak nebola vopred dohodnutá iná forma platby za certifikát

Podmienkou prevzatia certifikátu je, aby zákazník (resp. ním poverená osoba) pri návšteve RA podpísala dokumenty „Zmluva o vydaní a používaní certifikátu PSCA" a „Potvrdenie o vydaní certifikátu a jeho odovzdaní žiadateľovi o certifikát".

Žiadosť o certifikát s chýbajúcimi alebo neúplnými údajmi RA odmietne s uvedením dôvodu odmietnutia zaslaním podpísaného mailu žiadateľovi.

Len čo CA vytvorí certifikát, RA vyzve žiadateľa o certifikát prostredníctvom email správy zaslanej na dohodnutú email adresu (štandardne na email adresu nachádzajúcu sa v certifikáte), aby sa dostavil na RA kvôli prevzatiu svojho certifikátu a podpísaniu dokumentu „Zmluva o vydaní a používaní certifikátu PSCA" a potvrdenia o vydaní certifikátu a jeho odovzdaní žiadateľovi o certifikát, ktoré tvorí prílohu zmluvy o vydaní a používaní certifikátu PSCA. Tieto dokumenty sa vyhotovia v troch exemplároch – jeden pre žiadateľa a dva zostanú na RA.

Žiadateľ o certifikát sa pri preberaní svojho certifikátu môže dať zastupovať na RA inou fyzickou alebo právnickou osobou za rovnakých podmienok ako pri podávaní žiadosti o certifikát.

Vytvorený certifikát bude nahraný na 3,5" disketu majiteľa certifikátu alebo subjektu, ktorý ho zastupuje, spolu s certifikátom CA PSCA a certifikačným poriadkom PSCA.

Sú dve možnosti ako nahrať novovytvorený osobný certifikát do prehliadača, aby mohol byť prehliadačom priradený k príslušnému privátnemu kľúču, ktorý sa vytvoril a uschoval na danom osobnom počítači v priebehu generovania žiadosti o certifikát:

- otvorením htm súboru, ktorý žiadateľ o certifikát dostal od RA, prostredníctvom prehliadača, ktorým bola vygenerovaná žiadosť o daný certifikát, sa certifikát nahrá do osobného počítača. Musí to byť ten istý počítač, na ktorom bola predtým vygenerovaná žiadosť o certifikát, z ktorej bol daný certifikát vytvorený.

- po odovzdaní osobného certifikátu pošle RA majiteľovi certifikátu cez email oznam o vytvorení certifikátu na email adresu, ktorá sa nachádza v položke Email v rozlišovacom mene novovytvoreného osobného certifikátu. Oznam bude obsahovať hypertextový odkaz (link) na URL adresu, kliknutím na ktorú si prostredníctvom prehliadača majiteľ nahrá svoj certifikát do svojho osobného počítača. Musí to byť ten istý počítač, na ktorom bola predtým vygenerovaná žiadosť o certifikát, z ktorej bol daný certifikát vytvorený. Prenos certifikátu zo servera PSCA do osobného počítača majiteľa certifikátu sa uskutoční zabezpečeným spôsobom prostredníctvom protokolu https.