Institute of Informatics, Slovak Academy of Sciences

SlovakGrid CA

Certificate Policy and Certification Practice Statement

Translation of user-related parts to Slovak language

Preklad častí pre používateľov do slovenčiny.

Version 2.2
December 2015

Obsah

- 1.3.4 Platnosť

Druhy a možné použitia vydávaných certifikátov sú nasledovné:

a) certifikát pre server: autentifikácia a kryptovanie komunikácie;
b) osobný certifikát: autentifikácia a kryptovanie komunikácie;
c) certifikát pre službu: autentifikácia a kryptovanie komunikácie.

Certifikát vydaný Certifikačnou autoritou SlovakGrid nesmie byť použitý na finančné transakcie ani na iné komerčné účely. Privátny kľúč nesmie byť zdieľaný viacerými osobami alebo servermi a jeho držba automaticky neoprávňuje ku prístupu k výpočtovým prostriedkom Gridu.

– 2.1 Povinnosti

- 2.1.3 Povinnosti majiteľa SlovakGrid certifikátu

a) Prečítať a akceptovať pravidlá a procedúry publikovaní v tomto dokumente;
b) Vygenerovať si dvojicu kľúčov pomocou spoľahlivej metódy;
c) Uchovávať si privátny kľúč v bezpečí a chránený; nesmie byť zdieľaný s inou osobou;
d) Použiť aspoň 12 znakové silné heslo na ochranu privátneho kľúča osobného certifikátu; privátne kľúče pre servery a služby môžu byť uložené bez hesla, ale musia byť adekvátne chránené metódami operačného systému
e) Neodkladne oznámiť certifikačnej autorite (CA) potenciálne zneužitie privátneho kľúča;
f) Oznámiť CA stratu alebo zničenie kľúča;
g) Oboznámiť CA keď už certifikát nepotrebujete;
h) Oboznámiť CA keď sa informácia v certifikáte stane nesprávnou alebo nepresnou.

– 2.2 Ručenie

a) SlovakGrid CA garantuje overenie identity žiadostí o certifikát podľa procedúr popísaných v tomto dokumente;
b) SlovakGrid CA garantuje overenie identity žiadostí o zrušenie platnosti certifikátu podľa procedúr popísaných v tomto dokumente;
c) SlovakGrid CA je prevádzkovaná na základe najlepšej snahy a nezaručuje istotu služby ani jej primeranosť;
d) SlovakGrid CA nie je zodpovedná za žiadne problémy spôsobené jej činnosťou alebo použitím ňou vydaných certifikátov;
e) SlovakGrid CA odopiera akúkoľvek zodpovednosť za škody alebo zhoršenia vyplývajúce z jej činnosti.

- 2.3 Finančná zodpovednosť

SlovakGrid CA odopiera akúkoľvek finančnú zodpovednosť za škody alebo zhoršenia vyplývajúce z jej činnosti.

– 3.1 Prvotná registrácia

– 3.1.2 Význam mien

Formát rozlišovacích mien pre SlovakGrid je nasledovný:
"C=SK, O=SlovakGrid, O=*organizácia*, CN=*meno-subjektu*"
Všeobecné meno (CN) v subjekte certifikátu musí byť odvodené zo skutočného mena subjektu. Aktuálny zoznam vhodných mien pre O je možné nájsť na nasledovnej internetovej adrese: http://ups.savba.sk/ca/ra-list.html. Aspoň jedna medzera má byť použitá v časti CN, ktorá oddeľuje meno od priezviska.

– 3.1.4 Jedinečnosť mien

Rozlišovacie meno musí byť pre každý certifikát jedinečné. V prípade zhody skutočného mena musia byť pridané doplňujúce čísla alebo písmená, aby sa zaručila jedinečnosť mena v certificate. Osoba môže žiadať o vydanie ďalšieho certifikátu, ak sa použije tento princíp. Rozlišovacie meno je spojené s jednou a len jednou osobou počas celej doby životnosti CA, pozri kapitolu 3.1.9c.

– 3.1.7 Metóda na preukázanie držby privátneho kľúča

Neurčená.

- 3.1.8 Preukázanie príslušnosti ku organizácii

Neurčené.

– 3.1.9 Preukázanie totožnosti

Procedúra je odlišná pre žiadosť o certifikát pre osobu a pre server:
Ak osoba žiada o svoj osobný certifikát:

a) Žiadosť o certifikát má byť poslaná na ca.ui@sav.sk z e-mailovej adresy z domény organizácie žiadateľa (kvôli predbežnej kontrole) a musí byť tiež doručená bezpečnou cestou (napr. osobne na prenosnom pamäťovom médiu) registračnej autorite;
b) Žiadateľ musí osobne navštíviť registračnú autoritu (RA);
c) Overenie totožnosti žiadateľa sa uskutoční ukázaním platného oficiálneho preukazu (občiansky preukaz alebo cestovný pas) alebo tým, že RA spoľahlivo danú osobu pozná.

Dátum narodenia žiadateľa a jeho e-mailová adresa sa zapíšu do záznamu o overení totožnosti kvôli zaručeniu nepridelenia jednej identity viacerým osobám počas celej doby životnosti CA.

Ak sa žiada o certifikát pre server alebo službu:

d) Žiadosť musí byť poslaná e-mailom a musí byť podpísaná platným osobným certifikátom vydaným SlovakGrid CA pre príslušného systémového administrátora;
e) Žiadateľ musí kontaktovať RA a preukázať, že má potrebné poverenie.

– 3.2 Bežná zmena kľúčov

Varovania o blížiacej sa expirácii budú posielané držiteľom certifikátov, spravidla 1 mesiac vopred. Zmena kľúčov pred expiráciou môže byť uskutočnená poslaním žiadosti podpísanej súčasným platným osobným certifikátom, ale najviac 5 rokov od poslednej osobnej návštevy u RA.
Zmena kľúčov po expirácii sa vykoná rovnakým postupom preukázania totožnosti ako pri žiadosti o nový certifikát.

- 3.3 Zmena kľúčov po zrušení platnosti certifikátu

Zmena kľúčov po zrušení platnosti certifikátu sa vykoná rovnakým postupom ako prvotná registrácia.

– 3.4 Žiadosť o zrušenie platnosti certifikátu

Žiadosť o zrušenie platnosti certifikátu má byť podaná:

a) E-mailom poslaným na ca.ui@sav.sk podpísaným platným osobným certifikátom vydaným SlovakGrid CA.
b) Keď sa nedá použiť e-mail, žiadosť bude overená vykonaním procedúry popísanej v kapitole 3.1.9 (Preukázanie totožnosti).

- 6.1 Generovanie a inštalácia dvojice kľúčov

– 6.1.1 Generovanie dvojice kľúčov

Každý žiadateľ si musí vygenerovať svoje vlastné kľúče sám. SlovakGrid CA pre neho túto službu nevykonáva.

– 6.1.3 Doručenie verejného kľúča vydavateľovi certifikátov

Verejného kľúče sa doručujú zakryptované e-mailom, SSL cez http, na diskete alebo inom prenosnom médiu.

– 6.1.4 Doručenie verejného kľúča vydavateľa žiadateľom

CA certifikát je stiahnuteľný z webu SlovakGrid CA (http://ups.savba.sk/ca).

– 6.1.5 Dĺžky kľúčov

a) minimálna dĺžka kľúča pre osobný alebo serverový certifikát je 2048 bitov;
b) dĺžka CA kľúča je 2048 bitov.

– 6.1.9 Účely použitia kľúča

Kľúče môžu byť použité na autentifikáciu, kódovanie údajov, zaistenie integrity správ a nadviazanie bezpečného spojenia. Certifikáty a CRL sú podpísané privátnym kľúčom certifikačnej autority.