



PODMÍNKY PRO VYDÁVÁNÍ A POUŽÍVÁNÍ ELEKTRONICKÝCH CERTIFIKÁTŮ PRO ZAMĚSTNANCE A HOSTY ČVUT

I.

Úvod

1. Vydavatelem a správcem certifikátů je **certifikační autorita** CESNET Personal Signing CA (dále jen „CESNET“), kterou provozuje CESNET PKI - CESNET, a. l. e., Zikova 4, 106 00 Praha 6, ČR. Certifikační autorita CESNET používá podpisový certifikát vydaný kořenovou certifikační autoritou *CESNET CA Root*. Certifikační autorita CESNET vydává certifikáty pouze koncovým uživatelům.
2. Výpočetní a informační centrum ČVUT v Praze (dále jen „VIC“) zastupuje roli **registrační autority** (dále jen „RA“). Úkolem registrační autority je:
 - ověřování identity žadatele o certifikát
 - nahrání a zašifrování certifikátu na čipovou kartu s kontaktním čipem
 - přijímání žádostí o odvolání certifikátu
3. Výdej a správa certifikátů se řídí pravidly certifikační politiky (dále jen „CP“) a certifikačních směrnic (dále jen „CPS“) vydávaných CA.
4. Certifikační politika a certifikační prováděcí směrnice jsou zveřejněny na stránkách sdružení CESNET na adrese: http://pki.cesnet.cz/CP/Root/1.1/CESNET_Root_CA_CP_CPS-1.1.pdf
5. **Držiteli certifikátů** jsou osoby, kterým byl vydán certifikát certifikační autoritou CESNET.
6. **Spoléhající se strany** jsou subjekty, které se při činnosti spoléhají na certifikáty vydané CESNET.

II.

Použití certifikátu

1. Certifikáty vydané CESNET jsou určeny k ověření digitálních podpisů a k ověření identity držitele certifikátu.
2. Certifikáty CESNET se nesmí používat v rozporu s účelem, ke kterému byly vydány.
3. Použití daného certifikátu je uvedeno v rozšiřujícím parametru keyUsage. Jakékoliv jiné použití než toto uvedené je na vlastní nebezpečí spoléhající se strany.
4. Soukromý klíč vztahující se k certifikátu vydanému CESNET může být použit pouze v souladu s certifikační politikou a k účelům, ke kterým byl certifikát vydán.
5. Certifikát CESNET není uznávaný státem Česká republika
6. Držitel certifikátu je povinen:
 - chránit soukromý klíč před neoprávněným zneužitím a ztrátou;
 - poskytovat správné informace registrační autoritě;
 - používat certifikáty pouze pro legální účely;
 - okamžitě požádat o odvolání certifikátu v případě podezření ze zneužití certifikátu.
7. Spoléhající se strana je povinna:
 - užívat certifikáty vydané podle certifikační politiky v souladu s certifikační politikou;
 - spoléhat pouze na certifikáty, u nichž ověřila, že nebyly odvolány;
 - spoléhat na digitální podpisy, které byly vytvořeny v době platnosti certifikátu a v souladu s účelem, ke kterému byl certifikát vydán.

III.

Vydávání certifikátů

1. Vydání osobního certifikátu CESNET (dále jen „certifikát“) zprostředkuje VIC, jakožto registrační autorita na pracovišti k tomu určeném (dále jen „vydavatelství průkazů“).
2. Na certifikát má nárok zaměstnanec nebo host organizace ČVUT Praze, který je oprávněným držitelem osobního průkazu ČVUT s kontaktním čipem (dále jen „průkazu“). Vydávání tohoto průkazu se řídí dle podmínek pro vydávání a používání průkazů typu osobní ČVUT.
3. Před vydáním osobního certifikátu je osoba povinna prokázat svoji totožnost, a to předložením občanského průkazu nebo jiného platného osobního dokladu, vydaného příslušným správním úřadem.
4. Při vydání certifikátu je generován klíčový pár na kontaktním čipu karty ve vydavatelství průkazů. Čip neumožňuje export soukromého klíče. Výměna informací mezi certifikační autoritou a registrační autoritou je realizována zabezpečenou elektronickou cestou.
5. Převzetím průkazu s certifikátem osoba písemně potvrdí na předepsaném formuláři, v němž svým podpisem zároveň stvrdí, že se seznámila s podmínkami pro vydávání a používání certifikátů a s certifikační politikou CA a zavazuje se je dodržovat.
6. Vydání osobního certifikátu není zpoplatněno.

IV.

Platnost certifikátu

1. Převzetím průkazu s certifikátem vzniká jeho oprávněnému držiteli právo na používání certifikátu po dobu jeho platnosti.
2. Certifikát pozbývá platnosti:
 - a. uplynutím data platnosti certifikátu v něm uvedeného;
 - b. přestanou-li data uvedená v certifikátu odpovídat skutečnosti;
 - c. ukončením posledního vztahu k ČVUT, který ho opravňuje k držení průkazu s certifikátem;
 - d. odvoláním certifikátu.
3. Doba platnosti certifikátu je stanovena na **1 rok** od data vydání.
4. Pokud není certifikát po dobu jeho platnosti nutné zneplatnit, skončí jeho platnost v časovém okamžiku uvedeném v certifikátu. Každý vydaný certifikát zůstává po ukončení své platnosti nadále uložen v databázi vydávající certifikační autority.

V.

Následné vydání certifikátu

1. CESNET neposkytuje službu obnovení certifikátu. Pod službou obnovení certifikátu je myšleno vydání nového certifikátu se stejným veřejným klíčem a novou dobou platnosti.
2. Držitel certifikátu žádá o vydání následného certifikátu následujícími způsoby:
 - a. Žádost o vydání následného certifikátu může držitel **platného** certifikátu podat pomocí webového rozhraní zpravovaného registrační autoritou. V takovém případě musí být žádost podepsána **platným** osobním certifikátem vydaným CESNET.
 - b. Vydání následného certifikátu držiteli již **neplatného** certifikátu CESNET se řídí dle pravidel odstavce III – Vydávání certifikátů.

VI.

Odvolání certifikátu

1. Certifikát vydaný CESNET musí být odvolán, nastane-li některá z následujících skutečností:
 - existuje-li důvodné podezření, že soukromý klíč odpovídající certifikátu byl kompromitován;
 - přestanou-li data uvedená v certifikátu odpovídat skutečnosti;

- je-li certifikát použit v rozporu s certifikační politikou nebo dalšími pravidly upravujícími používání certifikátů CESNET;
 - byl-li certifikát vydán jako důsledek podvodu nebo zanedbání;
 - jestliže by neodvolání certifikátu ohrozilo důvěryhodnost CESNET;
 - požádá-li o odvolání certifikátu jeho držitel.
2. V případě, že nastane jedna nebo více skutečností uvedených v odstavci 1, je držitel průkazu povinen o tom ve vlastním zájmu neprodleně informovat vydavatelství průkazů.
 3. Skutečnost může držitel certifikátu ohlásit osobně ve vydavatelství průkazů, telefonicky, elektronickou poštou (prukazy@victoria.cvut.cz).
 4. Při oznámení je třeba sdělit údaje, podle kterých je možné daný certifikát identifikovat (tj. číslo průkazu, jméno držitele průkazu a jeho rodné číslo), a oznámit všechny okolnosti, které jsou známy o podezření z jeho zneužití. Držitel odpovídá za škody způsobené zneužitím osobního certifikátu neoprávněnou osobou, jeho odpovědnost však končí dnem následujícím po dni, kdy bylo oznámení o skutečnosti vydavatelstvím průkazů přijato.
 5. V případě blokace na základě hlášení o ztrátě nebo zneužití je certifikát odvolán automaticky.
 6. Po ohlášení skutečnosti provede vydavatelství průkazů okamžité zaslání žádosti o odvolání na CESNET. Odvolání certifikátu se projeví nejpozději následující pracovní den po ohlášení.
 7. Odvolaný certifikát nelze obnovit. Nový certifikát bude vydán ve vydavatelství průkazů.
 8. Seznam odvolaných certifikátů vydaných CESNET je publikován na adrese: <http://crl.cesnet-ca.cz/PersonalSigning.crl>.

VII.

Závěrečná ustanovení

1. Podmínky pro vydávání a používání osobních certifikátů jsou podřízené certifikační politice a prováděcím směrnici CESNET CA Root. Certifikační politika a certifikační prováděcí směrnice jsou dostupné na internetu na adrese <http://pki.cesnet.cz>.
2. Tyto podmínky nabývají účinnosti dnem 13. 12. 2013, VIC si vyhrazuje právo podmínky pro vydávání a používání osobních certifikátů měnit a doplňovat, nebo je zrušit vydáním nových podmínek. Platné podmínky jsou k dispozici ve vydavatelství průkazů a na internetu na adrese <http://prukazy.cvut.cz> a <http://pki.cvut.cz>.


Ing. Marek Kalika, Ph.D.
ředitel

V Praze dne 13.12. 2013