Digitální
a informační
agentura

Certifikáty a jejich použití

Verze 2.3

Digitální a informační agentura
Na Vápence 915/14, 130 00 Praha 3
posta@dia.gov.cz

Úvod

Vydávání certifikátů pro přístup do produkčního prostředí základních registrů a ISSS (Informační systém sdílených služeb) se řídí Certifikační politikou DIA pro certifikáty vydávané pro AIS (dále jen Certifikační politika). Tato politika je uveřejněná na webu DIA.

Tento dokument pouze vysvětluje některé aspekty vydávání a používání certifikátů, ale nenahrazuje žádná ustanovení Certifikační politiky.

DIA nevydává Certifikační politiku pro testovací prostředí základních registrů, ale dodržuje obdobná pravidla jako pro produkční prostředí.

Jako AIS (Agendový informační systém) jsou v tomto dokumentu označovány informační systémy, které mají podle platných zákonů nárok na přístup do základních registrů a do dalších informačních systémů, které tvoří tzv. referenční rozhraní veřejné správy. Pokud je v dokumentu uvedeno "AIS", myslí se tím jak AIS, tak SSVÚ (soukromoprávní systém pro využívání údajů).

Vydání certifikátu pro AIS

Aby mohl AIS volat služby základních registrů, nebo služby ISSS (Informační systém sdílené služby) musí mít povolen přístup k vnějšímu rozhraní ISZR (Informační systém základních registrů) anebo ISSS. Přístup povoluje DIA na žádost správce AISu. Výsledkem úspěšného vyřízení žádosti je mj. vydání serverovového certifikátu pro AIS. Jde o serverový certifikát v tom smyslu, že je vydáván pro aplikaci, a ne pro osobu. Při navazování spojení mezi ISZR, respektive ISSS a AIS ho lze použít jak jako klientský (spojení navazuje AIS), tak serverový (spojení navazuje ISZR, respektive ISSS).

DIA vyžaduje podání žádosti o certifikát ve formátu PKCS#10. Správce AISu posílá žádost o certifikát spolu s vyplněným formulářem z aplikace RAZR, která je dostupná z prostředí KIVS a Internet. Žádost ve formátu **musí** obsahovat:

- IČO správce AIS, který o registraci AISu žádá. V případě, že správce AIS nemá IČO, uvádí žadatel identifikátor správce AIS z RPP.
- Identifikátor (číslo) AISu v RPP.
- Indikaci, zda se jedná o přístup do produkčního nebo testovacího prostředí ISZR, respektive ISSS.
- Veřejný klíč RSA, který má být certifikován.

Návod na vygenerování dvojice klíčů a vytvoření žádosti o certifikát veřejného klíče ve formátu PKCS#10 je na webu DIA. V návodu je uvedený postup při použití software GeneratorCertRAZR a knihovny OpenSSL. Je možné použít i jiný software, jehož výstupem bude žádost o certifikát v požadovaném formátu a s požadovaným obsahem. DIA vytvořila aplikaci pro generování žádostí o certifikát. Tuto aplikaci je možné stáhnout z webu DIA a volně používat.

Pro podávání žádostí o přístup AISu k základním registrům určila DIA aplikaci RAZR (Registrační autorita základních registrů). Postup pro podání žádosti je na webu DIA.

Certifikáty vydává Certifikační autorita (CA) DIA, a to odděleně pro testovací a produkční prostředí. Pro každé prostředí je jiná CA a každá CA používá jinou řadu sériových čísel. Identifikačním údajem certifikátu je:

- identifikace vydávající CA a sériové číslo certifikátu, **nebo**
- identifikace vydávající CA a otisk (hash) certifikátu, ***nebo***
- identifikace vydávající CA a předmět certifikátu (Subject).

CA DIA vydává certifikáty pro:

- ISZR.
- ISSS.
- AISy. Co AIS, to certifikát. Nelze použít jeden certifikát pro více AISů.

CA DIA certifikuje pouze veřejné klíče vygenerované algoritmem RSA. Požadovaná minimální délka klíče je pro testovací i produkční prostředí 3072 bitů. Certifikáty vydává pro testovací i produkční prostředí na 3 roky. CA používá při podpisu vydávaných certifikátů hash funkci SHA384.

Pro každou žádost je nutné vygenerovat novou dvojici klíčů. Není povoleno certifikovat jeden veřejný klíč víckrát, tj. není možné prodlužovat platnost jednoho klíčového páru.

Certifikát se vydává pro konkrétní AIS, který je identifikovaný svým číslem a IČO správce nebo identifikátorem správce v RPP. Při změně kteréhokoliv z uvedených údajů je nutné požádat o zneplatnění všech dosud platných certifikátů pro AIS a požádat o nové certifikáty pro AIS. Při změně agend anebo IP adres AISu není nutné žádat o nový certifikát.

Žadatel o certifikát (správce AISu) je povinen zkontrolovat, že ve vydaném certifikátu jsou údaje, které uvedl v žádosti o certifikát. Pokud tomu tak není, znamenalo by to, že dostal certifikát patřící jinému subjektu anebo AISu.

Použití klíčového páru a certifikátu AIS

Certifikáty vydávané CA DIA pro AISy je možné použít pouze pro vzájemnou autentizaci a navázání SSL spojení mezi AIS a ISZR, respektive AIS a ISSS, nebo vzájemnou autentizaci a navázání SSL spojení mezi dvěma AIS. Není povoleno je používat pro jiné účely.

Při rozhodování, zda je možné párový klíč a certifikát v určité situaci použít, je nutné brát v úvahu všechna ustanovení Certifikační politiky, podle které byl certifikát vydaný. Je nutné respektovat jak organizační opatření, tak přípustná použití definovaná v certifikátu (Key Usage a Enhanced Key Usage). To, že párový klíč a certifikát lze technicky k nějakému účelu použít, ještě neznamená, že takové použití je povoleno.

Správce AISu zajistí instalaci certifikátu a odpovídajícího soukromého klíče na všechna zařízení (servery, firewally, komunikační sběrnice, SSL koncentrátory, HSM apod.) tak, aby AIS mohl komunikovat s ISZR anebo s ISSS anebo s jinými AIS. Jeden AIS, a tedy i jeho certifikát (a soukromý klíč) může být nainstalován na více zařízeních a na jednom zařízení může být zakončená SSL komunikace více AISů a tedy i více certifikátů (a soukromých klíčů) různých AISů. Podstatné je, aby správci všech AISů zajistili splnění požadovaných podmínek pro provoz AISů a aby AIS při každém volání služby základních registrů použil správný certifikát.

Certifikační politika povoluje předat soukromý klíč a certifikát jinému subjektu (typicky provozovateli AISu, nebo poskytovateli cloud služeb). Požaduje, aby v takovém případě měl správce AISu s příslušným subjektem uzavřenou smlouvu. V Certifikační politice jsou uvedené pouze minimální požadavky na takovou smlouvu a na zacházení se soukromým klíčem. Tzn. že správce AISu má uvést v příslušné smlouvě takové požadavky, které budou vyhovovat jeho požadavkům na bezpečnost AISu, ale v každém případě bude smlouva obsahovat požadavky z Certifikační politiky.

Je odpovědností správce AISu zajistit takovou bezpečnost soukromého klíče, která vyhovuje požadavkům na bezpečnost AISu. Z hlediska DIA za bezpečnost soukromého klíče v každém případě odpovídá správce AISu.

Každý AIS má v testovacím i produkčním prostředí maximálně 2 platné certifikáty. Tj. takové, jejichž platnost trvá a nebyly zneplatněny (odvolány). Zablokovaný certifikát (viz dále) je stále platný. Certifikační politika povoluje mít souběžně 2 platné certifikáty pro jeden AIS maximálně po dobu 3 měsíců. Pokud správce překročí maximální lhůtu 3 měsíce souběhu platnosti dvou certifikátů pro jeden AIS, DIA mu jeden z certfikátů zneplatní.

V testovacím prostředí může mít AIS výjimečně i více platných certifikátů, ale musí vyšší počet zdůvodnit a DIA má právo počet omezit.

ISZR, ISSS i AISy používají certifikáty a příslušné soukromé klíče pro vzájemnou autentizaci a pro ustavení šifrovaného spojení (https).

Pokud spojení s ISZR, respektive ISSS navazuje AIS, identifikuje se a autentizuje se vůči ISZR, respektive ISSS svým certifikátem. ISZR, respektive ISSS se vůči AISu identifikuje svým certifikátem vydaným také CA DIA. AIS má povinnost autentizovat ISZR, respektive ISSS. Může to provést tak, že kontroluje vydavatele certifikátu a k tomu předmět certifikátu ISZR / ISSS, sériové číslo certifikátu ISZR / ISSS, nebo otisk (hash) certifikátu ISZR / ISSS. Vždy musí kontrolovat vydavatele a platnost certifikátu. K ověření platnosti se používá CRL, který vydává CA DIA. CA DIA neumožňuje možnost ověření protokolem OCSP.

Správce AISu musí být připraven na situaci, že pro ISZR nebo ISSS bude vydaný nový certifikát.

ISZR, respektive ISSS bude komunikovat s AISem, pokud jsou současně splněny následující podmínky:

- AIS se prokáže platným certifikátem vydaným CA DIA.
- Certifikát byl skutečně vydán pro autentizující se AIS.
- Pro certifikát AISu nebyl zablokován přístup k základním registrům. Zablokování se používá pro dočasný zákaz přístupu AISu. Certifikát AISu zůstává v tomto případě v platnosti.

Pokud spojení s AIS navazuje ISZR, respektive ISSS, umožňuje svoji identifikaci a autentizaci vůči AISu svým certifikátem, tentokrát z hlediska navazování spojení v roli klientského certifikátu. AIS požádá ISZR / ISSS o certifikát a ISZR / ISSS mu ho poskytne.

AIS i ISZR a ISSS používají **při obou směrech navazování spojení** stejný certifikát. AIS tedy nepotřebuje pro každý směr navazování spojení jiný certifikát. AIS nepotřebuje různé certifikáty ani v případě, že pro komunikaci s ISZR / ISSS používá různé servery, protože ISZR / ISSS nekontroluje, že jméno z certifikátu je stejné, jako jméno serveru.

AIS může stejný certifikát používat při komunikaci s ISZR přes KIVS i přes Internet. Komunikace s ISSS je možná pouze přes KIVS.

Vzájemná autentizace AIS pomocí certifikátů vydaných CA DIA je povolená, ale pro jejich skutečné použití vždy musí být zváženo, zda certifikáty splňují požadavky důvěryhodnosti pro použití v konkrétní situaci. Speciálně je nutné uvážit možné zpoždění při zařazení sériového čísla certifikátu do seznamu zneplatněných certifikátů, viz dále kapitolu „Zneplatnění certifikátu“ v tomto dokumentu a kapitolu 4.9.3.1 Certifikační politiky. Popis podmínek pro vydání certifikátu a obsah certifikátu jsou uvedeny v Certifikační politice.

DIA doporučuje uvádět v žádostech o certifikát v položce CommonName (CN) nebo Subject Alternative Names (SAN) DNS jméno (FQDN) počítače, který bude přijímat zpětná volání v případě,

kdy ISZR vrací odpověď na asynchronní dotaz v aktivním režimu. Pokud bude spojení navazováno v KIVS, mělo by jít o jméno, pod kterým je počítač dosažitelný v síti KIVS. Pokud bude spojení navazováno v Internetu, pak by mělo jít o veřejné DNS jméno. Pokud AIS asynchronní volání v aktivním režimu nebude používat, doporučuje DIA uvádět DNS jméno AISu v KIVS, respektive v Internetu. Pokud je potřeba mít v certifikátu více jmen, je možné druhé a další jména uvést v položce SAN.

Pokud má informační systém vystupovat vůči ISSS jako publikační, vyžaduje ISSS jméno serveru, které je součástí URL, na kterém ISSS s AIS komunikuje v položce Subject Alternative Name (SAN). Jméno serveru musí být z domény cms2.cz a obsahovat pravidla, která určila DIA, tj.

Jméno serveru v případě produkčního prostředí:

- aisAAA.bbb.ccc.cms2.cz, nebo
- aisAAA.ccc.cms2.cz

Jméno serveru v případě testovacího prostředí:

- aisAAA-test.bbb.ccc.cms2.cz, nebo
- aisAAA-test.ccc.cms2.cz

Kde AAA = číslo AIS, bbb = zkrácený název aplikace, ccc = zkrácený název OVM.

Více informací v návodech na vytvoření žádostí o certifikáty na webu DIA.

Zneplatnění certifikátu AIS na žádost správce AIS

Zneplatnění certifikátu je trvalá **nevratná** operace, po jejímž provedení již nelze certifikát používat pro přístup do základních registrů ani do ISSS ani pro komunikaci s jiným AIS. O zneplatnění certifikátu typicky žádá správce AIS v situaci, kdy došlo ke kompromitaci soukromého klíče, nebo když ruší AIS, nebo když se mění správce AIS.

Správce AISu má dvě možnosti, jak požádat o zneplatnění certifikátu:

- Pokud správce AISu při žádosti o vydání certifikátu specifikoval heslo pro komunikaci, může požádat o zneplatnění telefonicky, nebo osobně při návštěvě DIA. V tomto případě musí správce AISu žádost potvrdit zasláním žádosti z aplikace RAZR.
- Podat žádost o zneplatnění z aplikace RAZR.

Žadatel o zneplatnění nějakého certifikátu musí uvést:

- IČO nebo identifikátor správce AIS v RPP, pokud správce AIS nemá IČO.
- Identifikaci (číslo) AIS.
- Sériové číslo certifikátu.

Součástí žádosti o zneplatnění certifikátu může být také určení důvodu zneplatnění. V případech, kdy je zneplatnění certifikátu požadováno z důvodu vyzrazení soukromého klíče nebo existujícího podezření z neoprávněného použití soukromého klíče, musí žadatel tento důvod uvést.

DIA zablokuje přístup AIS k ISZR s použitím dotyčného certifikátu (ale zatím ho nezneplatní) a provede jednu z následujících akcí:

- Pokud DIA obdržela žádost o zneplatnění certifikátu prostřednictvím aplikace RAZR, zahájí proces zneplatnění certifikátu.

- Pokud DIA obdržela žádost o zneplatnění certifikátu osobně nebo telefonicky, čeká na zahájení procesu zneplatnění do doby, než dostane z aplikace RAZR žádost o zneplatnění certifikátu. Pokud z RAZR takovou žádost nedostane do 3 pracovních dnů, DIA certifikát odblokuje.

Pokud je výsledkem procesu zneplatnění certifikátu rozhodnutí, že certifikát bude zneplatněn, je požadavek co nejrychleji zpracován a identifikace příslušného certifikátu je umístěna do seznamu zneplatněných certifikátů (CRL) a žadateli je datovou schránkou odesláno rozhodnutí. CRL je standardním způsobem publikován do KIVS a do Internetu ve standardním časovém intervalu definovaném Certifikační politikou.

Zneplatnění certifikátu AIS z iniciativy DIA

Situace, ve kterých dojde ke zneplatnění certifikátu z iniciativy DIA, jsou vyjmenovány v Certifikační politice. Např. zánik správce AIS, nebo kompromitace některého z privátních klíčů vydávajících CA DIA, nebo porušování Certifikační politiky. DIA certifikát zneplatní a informuje o tom správce příslušného AISu.

Zablokování certifikátu AIS

Zablokování certifikátu je dočasná **vratná** operace. Znamená, že ISZR bude odmítat spojení s AIS, který použije zablokovaný certifikát. Používá se ve dvou situacích:

- Při zneplatňování certifikátů vydaných AIS v době do publikace CRL, ve kterém je zneplatněný certifikát uveden.
- Při vážných bezpečnostních problémech způsobených AISem.

Zablokovaný certifikát obecně zůstává v platnosti a jeho blokaci lze zrušit.

Z hlediska jiných AIS a ISSS je zablokovaný certifikát stále platný.

Výměna certifikátu ISZR / ISSS

Pokud se blíží konec platnosti certifikátu vydaného pro ISZR / ISSS, vydá DIA nový certifikát a nahradí starý certifikát novým.

DIA také uveřejní na svém webu údaje o novém certifikátu ISZR / ISSS**.**

Zneplatnění certifikátu ISZR / ISSS

Pokud je z nějakého důvodu zneplatněn certifikát ISZR / ISSS, vydá DIA nový certifikát a nahradí starý certifikát novým. Sériové číslo starého certifikátu je umístěno do CRL a CRL je publikován do KIVS a do Internetu. Nečeká se tedy na standardní čas publikace CRL.

AISy se tedy dozví o zneplatnění certifikátu ISZR / ISSS bez prodlení, respektive mají možnost se o něm dovědět bez prodlení.

Výměna certifikátu Certifikační autority DIA

Pokud se blíží konec platnosti certifikátu (a tedy i privátního klíče) používaného některou Certifikační autoritou DIA pro vydávání certifikátů pro AIS, vygeneruje DIA nový klíčový pár pro příslušnou CA,

k veřejné části vydá nový certifikát a nahradí starý klíč novým. Od té chvíle bude používat pro vydávání certifikátů nový privátní klíč. DIA tak učiní v dostatečném předstihu před ukončením platnosti certifikátu (a privátního klíče) vydávající CA. Lhůta činí několik let v závislosti na době, na jakou CA vydává certifikáty.

DIA uveřejní nový certifikát vydávající CA na standardních místech dostupných z Internetu a z KIVS.

Po určitou dobu tedy budou v platnosti certifikáty vydané pro AISy, respektive ISZR, respektive ISSS stejnou CA s použitím různých privátních klíčů. Nejjednodušší způsobem pro ověřování certifikátů je pro důvěřující stranu (tj. AIS) zařadit mezi důvěryhodné CA oba certifikáty příslušné CA.

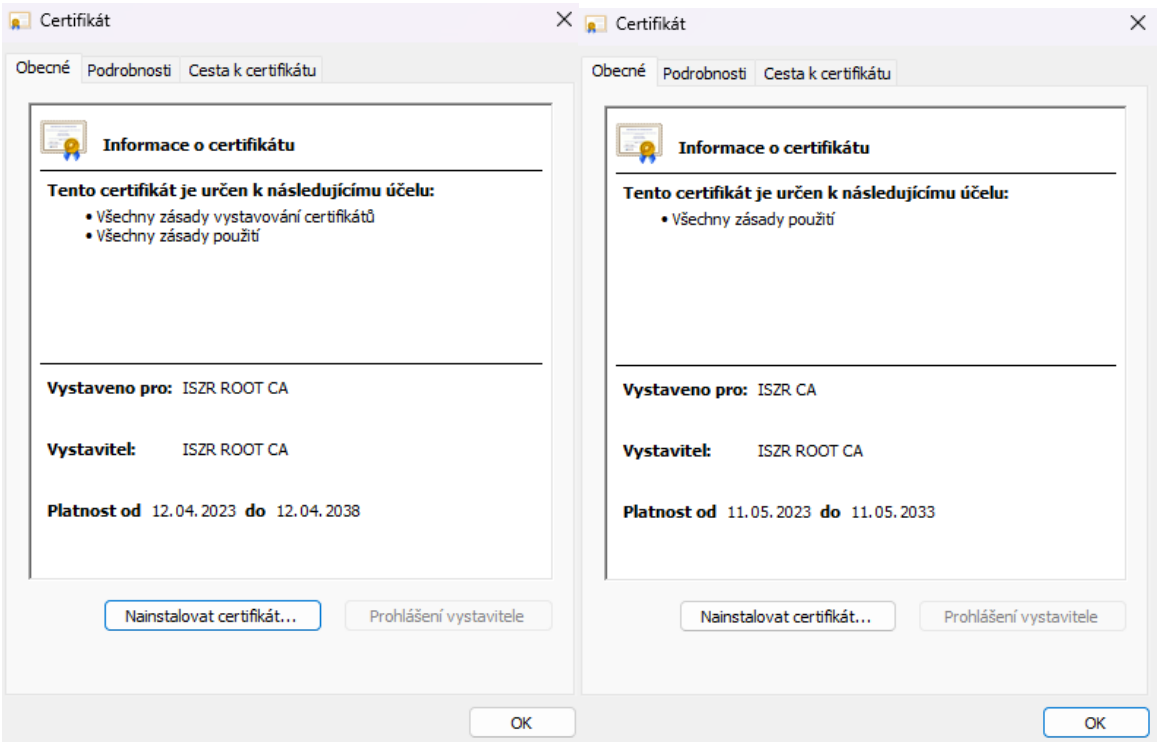
Ověřování certifikátů vydaných CA DIA

Vazba je přes položky „Subject Key Identifier“ v certifikátu vydávající CA a „Authority Key Identifier“ v certifikátu, který tato CA vydala.

Poznámka: Všechny příklady jsou provedeny na PC, které nemá certifikáty certifikačních autorit DIA mezi důvěryhodnými (trusted).

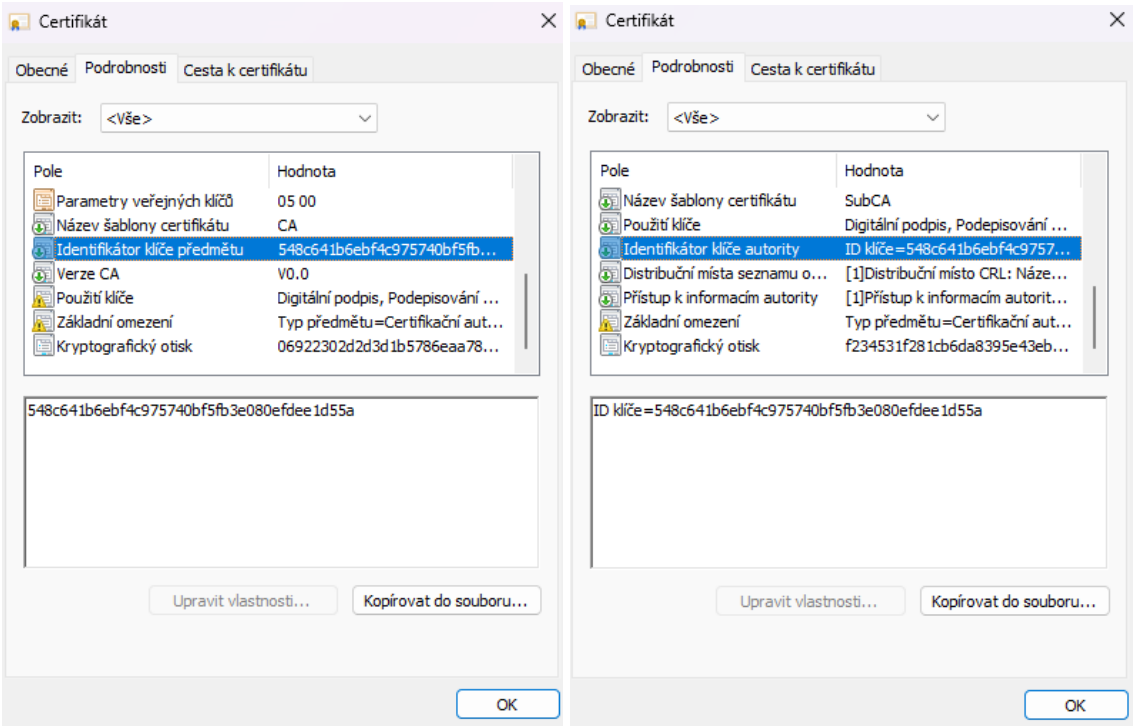
Produkční prostředí základních registrů

Root CA vydala certifikát pro podřízenou CA:



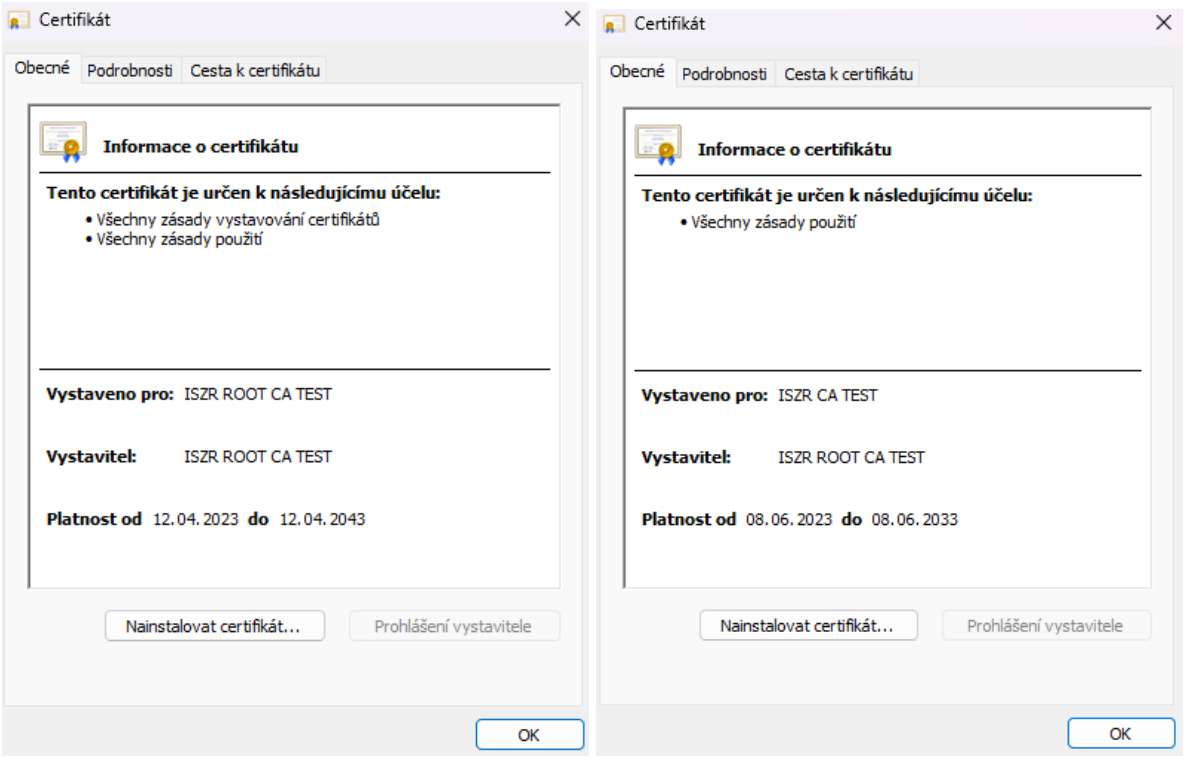
„Subject Key Identifier“ = „Authority Key Identifier“:

(Identifikátor klíče předmětu = Identifikátor klíče autority)



Testovací prostředí základních registrů

Root CA vydala certifikát pro podřízenou CA:



„Subject Key Identifier“ = „Authority Key Identifier“:

(Identifikátor klíče předmětu = Identifikátor klíče autority)

