SPRÁVA ZÁKLADNÍCH REGISTRŮ

Certifikáty a jejich použití

Verze 1.21

Vydávání certifikátů pro AIS (agendový informační systém) pro produkční prostředí základních registrů se řídí Certifikační politikou SZR (Správa základních registrů) pro certifikáty vydávané pro AIS. Tato politika je uveřejněná na webu SZR.

Tento dokument pouze vysvětluje některé aspekty vydávání a používání certifikátů, ale nenahrazuje žádná ustanovení Certifikační politiky SZR pro certifikáty vydávané pro AIS.

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

Slovem AIS jsou v tomto dokumentu označovány informační systémy, které mají podle platných zákonů nárok přístup do základních registrů a do dalších informačních systémů veřejné správy (ISVS), které tvoří tzv. referenční rozhraní ISVS.

Vydání certifikátu pro AIS

Aby mohl AIS volat služby základních registrů, nebo služby ISSS (Informační systém sdílených služeb) musí mít povolen přístup k vnějšímu rozhraní ISZR (Informační systém základních registrů) anebo ISSS Informační systém sdílených služeb). Přístup povoluje SZR 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 počítač (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).

SZR 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 PKCS#10 **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.
- 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 SZR. V návodu je uvedný postup při použití software OpenSSL. Je možné použít i jiný software, jehož výstupem bude žádot o certifikát v požadovaném formátu a s požadovaným obsahem.

Postup pro podání žádosti o přístup AISu k základním registrům je na webu SZR.

Certifikáty vydává Certifikační autorita (CA) SZR 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**
- otisk (hash) certifikátu, **nebo**
- identifikace vydávající CA a předmět certifikátu (Subject). Atributy, zajišťující rozlišení, je v předmětu certifikátu kombinace IČO a číslo AIS. RA SZR kontroluje, aby v žádostech o certifikát bylo vždy uvedeno IČO a číslo AIS a tyto dva atributy také jsou ve vydaných certifikátech.

CA SZR vydává certifikáty pro:

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

CA SZR certifikuje pouze veřejné klíče vygenerované algoritmem RSA. Požadovaná délka klíče je pro testovací i produkční prostředí 2048 bitů. Certifikáty vydává pro testovací i produkční prostředí na 3 roky.

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

Je možné žádat o certifikát pro AIS pro produkční prostředí základních registrů, i když AIS nemá certifikát pro testovací prostředí základních registrů.

Certifikát se vydává pro konkrétní AIS, který je identifikovaný svým číslem a svým správcem (ten je identifikovaný svým IČO). 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.

CA SZR používá při certifikaci veřejných klíčů pro AISy a ISZR algoritmus SHA256.

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.

Použití klíčového páru a certifikátu AIS

Certifikáty vydávané CA SZR 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 všechny servery AISu, které komunikují s ISZR anebo ISSS. Jeden AIS a tedy i jeho certifikát (a soukromý klíč) může být nainstalován na více serverech a na jednom serveru může být 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. SZR doporučuje instalovat certifikáty a soukromé klíče pouze na nezbytně nutné servery.

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, SZR mu jeden z certfikátů zneplatní.

V testovacím prostředí může mít AIS výjimečně i více platných certifikátů, ale musí vyšší počet zdůvodnit a SZR 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 se vůči AISu identifikuje svým certifikátem vydaným také CA SZR. AIS má povinnost autentizovat ISZR. Může to provést tak, že kontroluje sériové číslo certifikátu ISZR, nebo kontroluje otisk certifikátu ISZR, nebo kontroluje předmět certifikátu ISZR. Vždy musí kontrolovat vydavatele a platnost certifikátu.

ISSS používá certifikáty vydané jinou CA, než je CA SZR.

Správce AISu musí být připraven na situaci, že pro ISZR bude vydán nový certifikát.

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

- AIS se prokáže platným certifikátem vydaným CA SZR.
- 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, se kterým je problém. Certifikát AISu zůstává v tomto případě v platnosti.

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

AIS i ISZR 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 používá různé servery, protože ISZR nekontroluje, že jméno z certifikátu je stejné, jako jméno serveru.

AIS může stejný certifikát používat při komunikaci s ISZR přes KIVS i přes Internet.

Vzájemná autentizace AIS pomocí certifikátů vydaných CA SZR je povolená, ale pro jejich skutečné použití vždy musí být zváženo, zda certifikáty vydané CA SZR pro AIS 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 SZR pro vydávání certifikátů pro AIS.

SZR doporučuje uvádět v žádostech o certifikát v položce CommonName DNS jméno 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 SZR uvádět DNS jméno AISu v KIVS, respektive v Internetu. Pokud neexistuje jednoznačné DNS jméno, které by bylo možné AISu přiřadit, SZR doporučuje uvést buď jméno DNS domény, ve které je AIS umístěn, nebo nějaký text charakterizující AIS. Pokud je potřeba mít v certifikátu více jmen, je možné druhé a další jména uvést v položce Subject Alternative Name (SAN).

Pokud má AIS vystupovat vůči ISSS jako publikační, vyžaduje ISSS jméno serveru v položce Common Name (CN) v předmětu certifikátu a nebo v položce Subject Alternative Name (SAN). Jméno serveru musí být navíc z domény cms2.cz, tj. např. server.ovm.cms2.cz. Tzn. že v žádosti o certifikát musí být obsažena správná hodnota parametru / parametrů CN a nebo SAN.

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. 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 zneplatnění, může požádat o zneplatnění telefonicky, nebo osobně při návštěvě SZR. 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, případně certifikátu, musí žadatel tento důvod uvést.

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

- Pokud SZR obdržela žádost o zneplatnění certifikátu prostřednictvím aplikace RAZR, zahájí proces zneplatnění certifikátu.
- Pokud SZR 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 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 způsebem publikován do KIVS a do Internetu ve standardním časovém intervalu definovaném Certifikační politikou SZR.

Zneplatnění certifikátu AIS z iniciativy SZR

Situace, ve kterých dojde ke zneplatnění certifikátu z iniciativy SZR, jsou vyjmenovány v Certifikační politice SZR. Např. zánik správce AIS, nebo kompromitace některého z privátních klíčů vydávajících CA SZR, nebo porušování Certifikační politiky. SZR 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 eGSB a jiných AIS je zablokovaný certifikát stále platný.

Výměna certifikátu ISZR

Pokud se blíží konec platnosti některého certifikátu vydaného pro ISZR, vydá SZR nový certifikát a nahradí starý certifikát novým. Jde o certifikát, kterým se ISZR prokazuje AISům, které se k němu připojují.

SZR také uveřejní na svém webu údaje o novém certifikátu ISZR v sekci „Pro správce AIS“ v odstavci **„**Platné certifikáty CA“**.**

Zneplatnění certifikátu ISZR

Pokud je z nějakého důvodu zneplatněn certifikát ISZR, vydá SZR 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 bez prodlení, respektive mají možnost se o něm dovědět bez prodlení.

SZR také uveřejní na svém webu údaje o novém certifikátu ISZR v sekci „Pro správce AIS“ v odstavci **„**Platné certifikáty CA“**.**

Výměna certifikátu Certifikační autority SZR

Pokud se blíží konec platnosti certifikátu (a tedy i privátního klíče) používaného některou Certifikační autoritou SZR pro vydávání certifikátů pro AISy nebo ISZR, vygeneruje SZR nový klíčový pár pro CA,

k veřejné části vydá nový certifikát a nahradí starý klíč novým. Od té chvíle bude používat pro vydávání certifikátů nový privátní klíč. SZR 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.

SZR uveřejní nový certifikát vydávající CA na standardních místech na Internetu.

Po určitou dobu tedy budou v platnosti certifikáty vydané pro AISy, respektive ISZR 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.

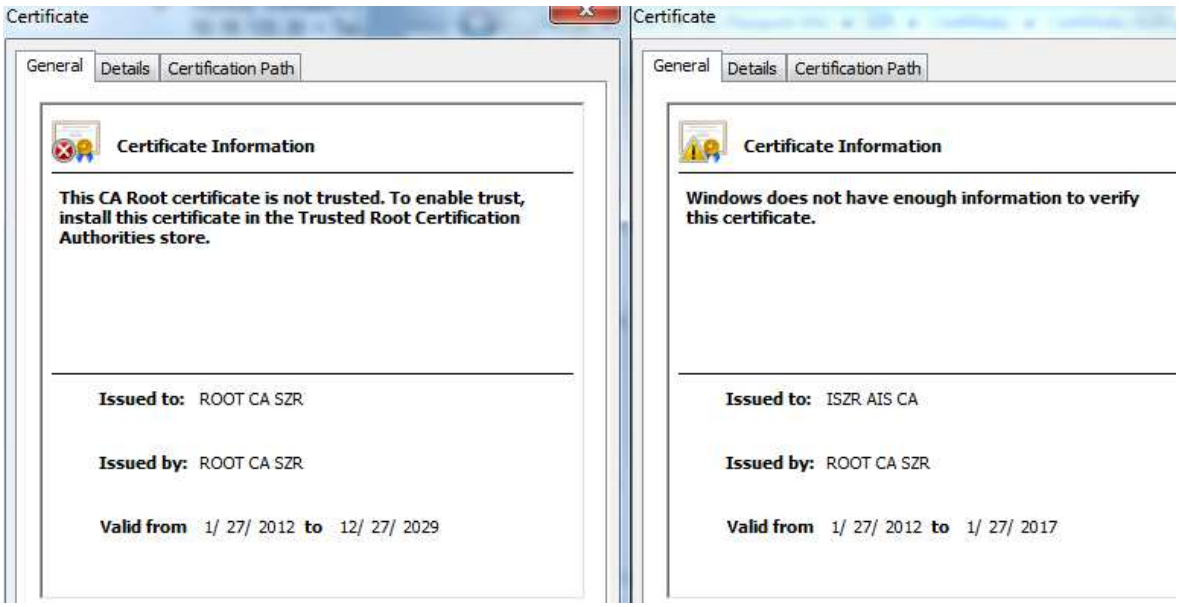
Ověřování certifikátů vydaných CA SZR

Vazba je přes položky „Subject Key Identifier“ v certifikátu vydávající CA a „Authority Key Identifier“ v certifikátu vydaném CA.

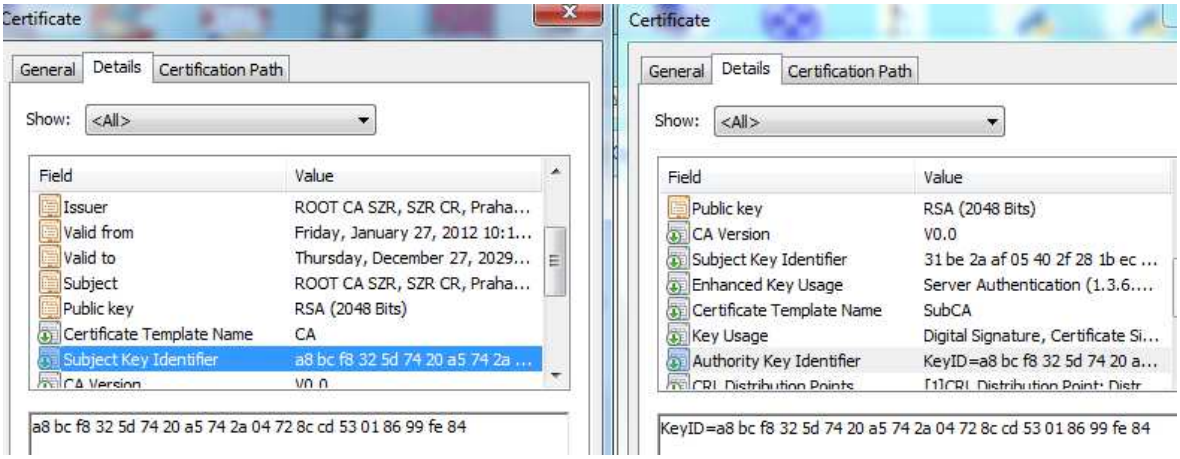
Poznámka: Všechny příklady jsou provedeny na PC, které nemá certifikáty certifikačních autorit SZR mezi důvěryhodnými (trusted).

Produkční prostředí základních registrů

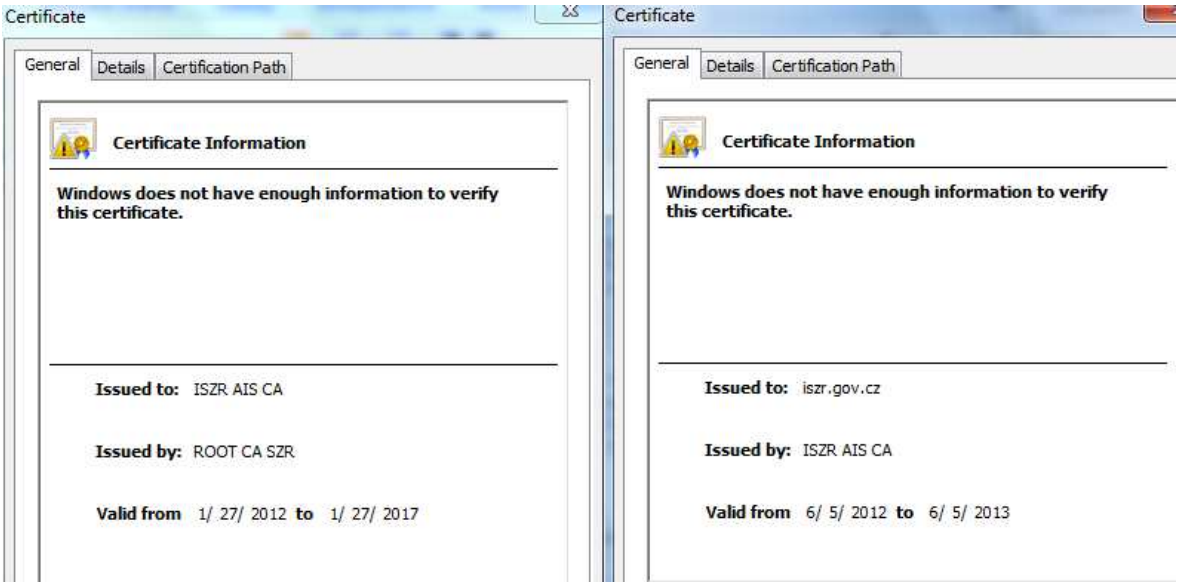
Root CA vydala certifikát pro podřízenou CA:



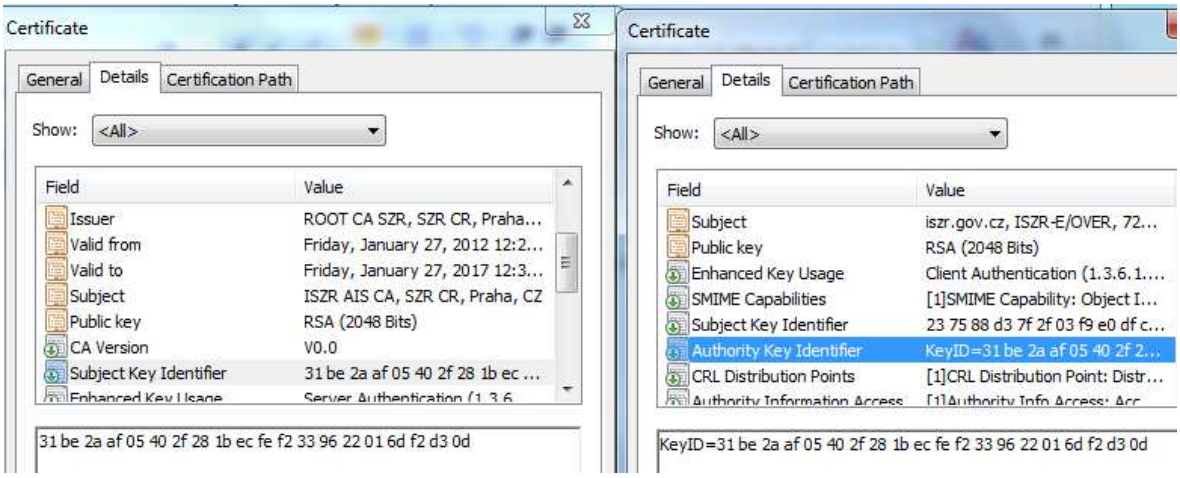
„Subject Key Identifier“ = „Authority Key Identifier“:


Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Issuer
ROOT CA SZR, SZR CR, Praha...
Valid from
Friday, January 27, 2012 10:1...
Valid to
Thursday, December 27, 2029...
Subject
ROOT CA SZR, SZR CR, Praha...
Public key
RSA (2048 Bits)
Certificate Template Name
CA
Subject Key Identifier
a8 bc f8 32 5d 74 20 a5 74 2a ...
a8 bc f8 32 5d 74 20 a5 74 2a 04 72 8c cd 53 01 86 99 fe 84
Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Public key
RSA (2048 Bits)
CA Version
V0.0
Subject Key Identifier
31 be 2a af 05 40 2f 28 1b ec ...
Enhanced Key Usage
Server Authentication (1.3.6....
Certificate Template Name
SubCA
Key Usage
Digital Signature, Certificate Si...
Authority Key Identifier
KeyID=a8 bc f8 32 5d 74 20 a...
KeyID=a8 bc f8 32 5d 74 20 a5 74 2a 04 72 8c cd 53 01 86 99 fe 84

Podřízená CA vydala certifikát pro AIS, respektive ISZR:

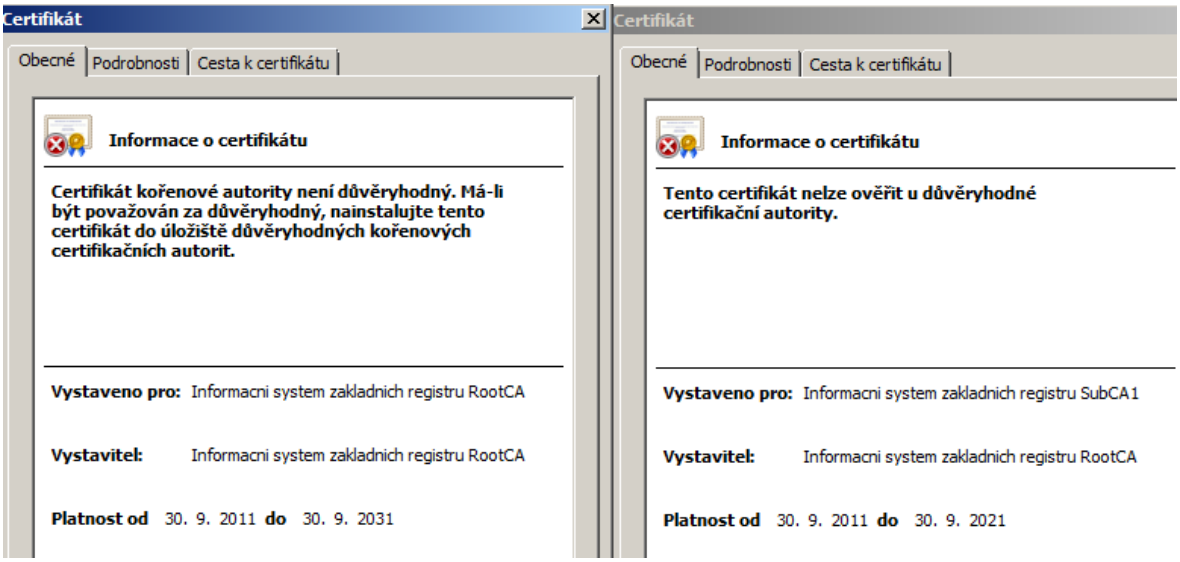


„Subject Key Identifier“ = „Authority Key Identifier“:

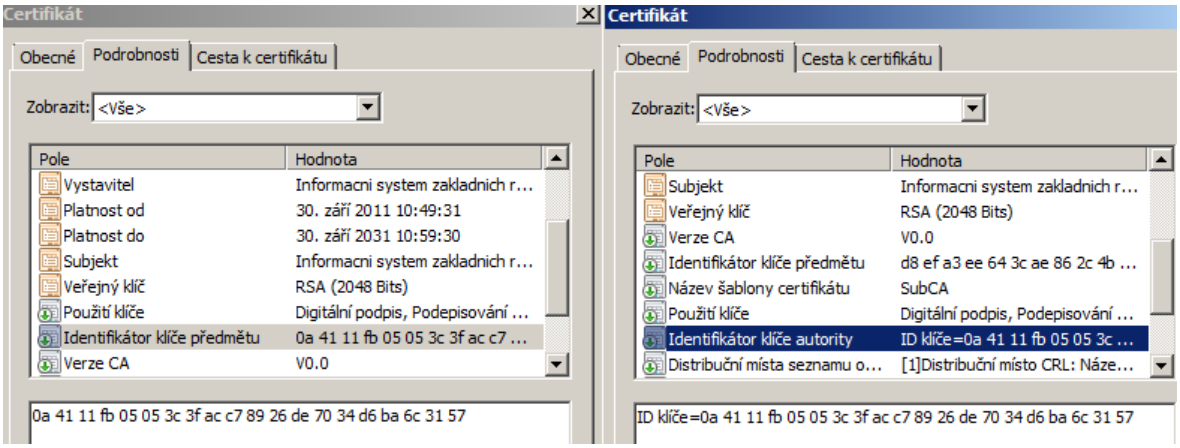


Testovací prostředí základních registrů

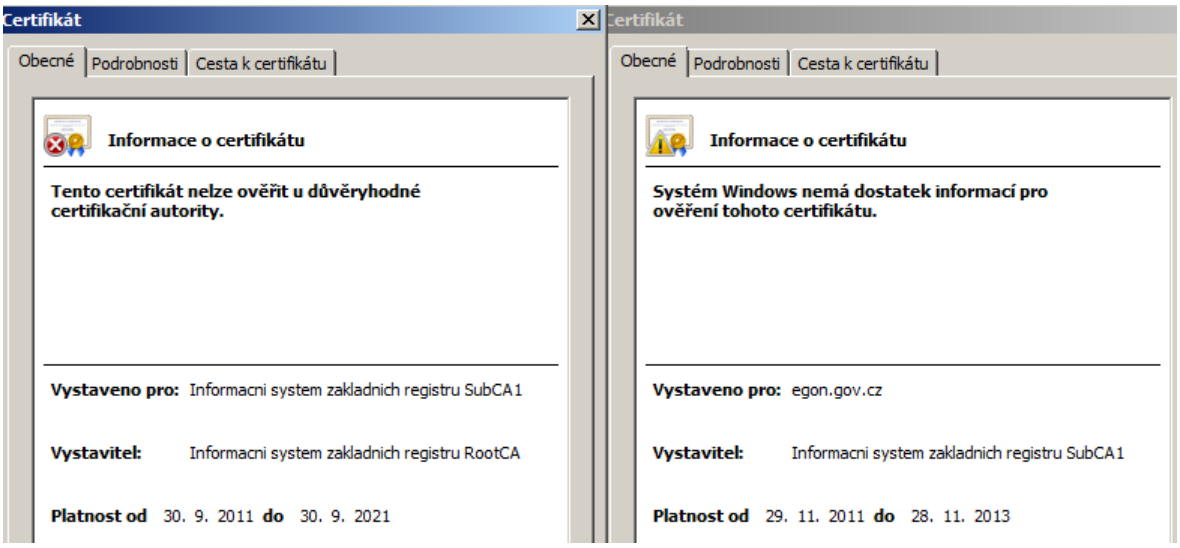
Root CA vydala certifikát pro podřízenou CA:



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



Podřízená CA vydala certifikát pro AIS, respektive ISZR:



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