ISDS

Instrukce pro vývojáře aplikací třetích stran

Nové SSL certifikáty s SHA-256

Aktualizovaná a doplněná verze ze dne 4.8.2015, která nahrazuje verzi 1.1 ze dne 28.7.2015

Instrukce pro vývojáře aplikací třetích stran

Autor	Martin Šlancar
Datum	4.8.2015
Quality Assurance	
Verze	1.4
Distribuce/Utajení	Informace určené pro veřejnost

Stručné shrnutí v bodech

- V ISDS budou nasazeny nové SSL certifikáty s SHA-256 (přesněji: certifikáty s hashovací funkcí SHA-256 v podpisu certifikátu). Nový certifikát již byl nasazen v prostředí veřejného testu ISDS, v produkčním prostředí ISDS bude nový certifikát nasazen dne **12.9.2015**.
- **Důležitá změna oproti předchozí verzi dokumentu:**
  Aby se předešlo penalizaci ISDS některými webovými prohlížeči z důvodu používání SHA-1, byla ve veřejném testovacím prostředí ISDS provedena korekce řetězce certifikátů, zasílaného serverem ISDS. Informace k zasílanému řetězci certifikátů se nacházejí na straně 2. Tato změna si může dále vynutit přidání nového kořenového certifikátu do „truststoru“ aplikací; více viz další odrážka níže, nebo strana 5.
- Vývojáři aplikací třetích stran musí své aplikace upravit tak, aby podporovaly hashovací funkce SHA-2 při ověřování platnosti certifikátu. Pokud aplikace k tomuto účelu využívá funkce operačního systému, musí vývojář své zákazníky informovat, že musí aplikaci používat na operačním systému, který podporuje SHA-2.
  Relevantní odkazy:
  https://casecurity.org/resources/
  http://blogs.technet.com/b/pki/archive/2010/09/30/sha2-and-windows.aspx
- Vývojáři musí přidat do „trustoru“ svých aplikací certifikát nové kořenové CA „GeoTrust Primary Certification Authority – G3“.
  Relevantní odkazy:
  https://www.geotrust.com/resources/root-certificates/index.html („Root 5“)
- **Důležitá změna oproti předchozí verzi dokumentu:**
  Dále je potřeba do „truststoru“ vašich aplikací přidat kořenový certifikát „GeoTrust Primary Certification Authority“, pokud zde již není umístěn.
  Relevantní odkazy:
  https://www.geotrust.com/resources/root-certificates/index.html („Root 3“)
- Pokud aplikace třetí strany vyžaduje ve svém „truststoru“ přítomnost certifikátů podřízených (intermediate) CA, musí vývojář dané aplikace umístit do „truststoru“ aplikace dva certifikáty nových podřízených CA – „GeoTrust EV SSL CA - G4“ a „GeoTrust Extended Validation SHA256 SSL CA“.
  Relevantní odkazy:
  https://knowledge.geotrust.com/support/knowledge-base/index?page=content&actp=CROSSLINK&id=SO24866
  https://knowledge.geotrust.com/support/knowledge-base/index?page=content&actp=CROSSLINK&id=SO24887
- Ověření kompatibility vaší aplikace s autoritou „GeoTrust EV SSL CA - G4“ provedete v prostředí veřejného testu ISDS. Ověření kompatibility vaší aplikace s autoritou „GeoTrust Extended Validation SHA256 SSL CA“ provedete v omezené míře na zkušební webové stránce „ssltest21“ poskytované autoritou GeoTrust.
  Relevantní odkazy:
  https://www.czebox.cz
  https://ssltest21.bbtest.net/

Popis plánované změny

V prostředí ISDS bude provedena výměna SSL certifikátů.
Stávající stav: V produkčním prostředí ISDS (www.mojedatovaschranka.cz) se nyní používají certifikáty vydané autoritou GeoTrust, v jejichž podpisu je použita hashovací funkce SHA-1. Ve veřejném testovacím prostředí ISDS (www.czebox.cz) je v tuto chvíli již nasazen nový certifikát založený na SHA-256.
Důležitá změna oproti předchozí verzi dokumentu: Ve veřejném testovacím prostředí byla provedena korekce řetězce certifikátů, který vrací server ISDS. Další informace jsou uvedeny níže.
Budoucí stav: Dne **12.9.2015** bude nasazen SSL certifikát založený na SHA-256 také v produkčním prostředí ISDS (www.mojedatovaschranka.cz). Certifikát vydá nová podřízená (intermediate) certifikační autorita a je pravděpodobné, že dojde také ke změně certifikátu kořenové CA. Na straně ISDS bude z tohoto důvodu aktualizován řetězec certifikátů (certificate chain), který se klientovi vrací spolu s SSL certifikátem v rámci iniciace SSL spojení, aby obsahoval správné certifikáty autorit.

Nejednoznačná autorita pro vydání certifikátu pro produkční prostředí ISDS

V tomto okamžiku nemůžeme jednoznačně určit, která certifikační autorita GeoTrust vydá certifikát pro produkční prostředí ISDS. V úvahu přicházejí tyto varianty:

1. **GeoTrust EV SSL CA - G4** – podřízená CA s podpisem založeným na SHA-256, kterou vydala kořenová CA založená na SHA-1. Tato autorita vydala certifikát určený pro veřejné testovací prostředí ISDS.
2. **GeoTrust Extended Validation SHA256 SSL CA** – podřízená CA s podpisem založeným na SHA-256, kterou vydala nová kořenová CA založená na SHA-256.

Tento dokument byl připraven před vydáním SSL certifikátu pro produkční prostředí ISDS, proto v tuto chvíli není známo, která z těchto dvou autorit vydá koncový SSL certifikát. Tyto instrukce pro vývojáře jsou proto koncipovány tak, aby aplikace byly připraveny na obě možné varianty.

Nový řetězec certifikátů, který bude vracet server ISDS

Veřejné testovací prostředí ISDS

Následující tabulka popisuje server ISDS ve veřejném testovacím prostředí ISDS.
V tabulce se nachází řetězec certifikátů, který server vracel v době nasazení SHA-1 certifikátu, a řetězec certifikátů, který vrací nyní po nasazení SHA-256 certifikátu.

Důležitá změna oproti předchozí verzi dokumentu: Aby se předešlo penalizaci ISDS některými webovými prohlížeči z důvodu používání SHA-1, byla ve veřejném testovacím prostředí ISDS provedena korekce řetězce certifikátů. Pravý sloupec tabulky uvádí v současnosti používaný (korigovaný) řetězec certifikátů.

#	Původní řetězec certifikátů	Nový řetězec certifikátů
1	Subject: GeoTrust Extended Validation SSL CA - G2 Issued by: GeoTrust Primary Certification Authority SHA-1 fingerprint certifikátu: C4 FA 37 41 B7 A7 F1 F6 C2 3D 24 F4 20 9F 5A 49 CD 5E 55 C6	Subject: GeoTrust EV SSL CA - G4 Issued by: GeoTrust Primary Certification Authority SHA-1 fingerprint certifikátu: 30 56 B3 43 48 5B 9D 55 F3 E2 B1 77 A8 95 BB 04 63 EE 3E FD SHA-256 fingerprint certifikátu: 95 B0 9D 02 12 2F A8 AE 62 35 78 0F 6E A6 50 3E 76 7A C0 21 A0 87 4F E8 31 CE 80 3A 50 EA 8F D7

#	Původní řetězec certifikátů	Nový řetězec certifikátů
2	Subject: GeoTrust Primary Certification Authority Issued by: Equifax Secure Certificate Authority SHA-1 fingerprint certifikátu: 68 90 ED 2B 2C 11 10 72 91 2E D6 25 54 59 AD 0D B7 6F 3A D1	Subject: GeoTrust Primary Certification Authority Issued by: GeoTrust Primary Certification Authority SHA-1 fingerprint certifikátu: 32 3C 11 8E 1B F7 B8 B6 52 54 E2 E2 10 0D D6 02 90 37 F0 96 SHA-256 fingerprint certifikátu: 37 D5 10 06 C5 12 EA AB 62 64 21 F1 EC 8C 92 01 3F C5 F8 2A E9 8E E5 33 EB 46 19 B8 DE B4 D0 6C
3	Subject: Equifax Secure Certificate Authority Issued by: Equifax Secure Certificate Authority SHA-1 fingerprint certifikátu: D2 32 09 AD 23 D3 14 23 21 74 E4 0D 7F 9D 62 13 97 86 63 3A	

Poznámka: Některé aplikace mohou zobrazovat pro ověření správnosti certifikátu fingerprint založený na hashovací funkci SHA-1. V tabulce je proto uveden fingerprint certifikátů založený na SHA-1 a SHA-256.

Produkční prostředí ISDS

Následující tabulka popisuje server ISDS v produkčním prostředí ISDS.
Pokud bude certifikát pro produkční prostředí ISDS vydán autoritou „**GeoTrust EV SSL CA - G4**“, bude server ISDS posílat následující řetězec certifikátů.

Důležitá změna oproti předchozí verzi dokumentu: Byla provedena korekce v novém řetězci certifikátů na pravé straně tabulky.

#	Původní řetězec certifikátů	Nový řetězec certifikátů
1	Subject: GeoTrust Extended Validation SSL CA - G2 Issued by: GeoTrust Primary Certification Authority SHA-1 fingerprint certifikátu: C4 FA 37 41 B7 A7 F1 F6 C2 3D 24 F4 20 9F 5A 49 CD 5E 55 C6	Subject: GeoTrust EV SSL CA - G4 Issued by: GeoTrust Primary Certification Authority SHA-1 fingerprint certifikátu: 30 56 B3 43 48 5B 9D 55 F3 E2 B1 77 A8 95 BB 04 63 EE 3E FD SHA-256 fingerprint certifikátu: 95 B0 9D 02 12 2F A8 AE 62 35 78 0F 6E A6 50 3E 76 7A C0 21 A0 87 4F E8 31 CE 80 3A 50 EA 8F D7
2	Subject: GeoTrust Primary Certification Authority Issued by: Equifax Secure Certificate Authority SHA-1 fingerprint certifikátu: 68 90 ED 2B 2C 11 10 72 91 2E D6 25 54 59 AD 0D B7 6F 3A D1	Subject: GeoTrust Primary Certification Authority Issued by: GeoTrust Primary Certification Authority SHA-1 fingerprint certifikátu: 32 3C 11 8E 1B F7 B8 B6 52 54 E2 E2 10 0D D6 02 90 37 F0 96 SHA-256 fingerprint certifikátu: 37 D5 10 06 C5 12 EA AB 62 64 21 F1 EC 8C 92 01 3F C5 F8 2A E9 8E E5 33 EB 46 19 B8 DE B4 D0 6C
3	Subject: Equifax Secure Certificate Authority Issued by: Equifax Secure Certificate Authority SHA-1 fingerprint certifikátu: D2 32 09 AD 23 D3 14 23 21 74 E4 0D 7F 9D 62 13 97 86 63 3A	

Tato tabulka je totožná s tabulkou pro veřejné testovací prostředí ISDS, uvedenou výše.
Poznámka: Některé aplikace mohou zobrazovat pro ověření správnosti certifikátu fingerprint založený na hashovací funkci SHA-1. V tabulce je proto uveden fingerprint certifikátů založený na SHA-1 a SHA-256.

Pokud bude certifikát pro produkční prostředí ISDS vydán autoritou „**GeoTrust Extended Validation SHA256 SSL CA**“, bude server ISDS posílat následující řetězec certifikátů. Dojde ke kompletní změně posílaného řetězce certifikátů!

#	Původní řetězec certifikátů	Nový řetězec certifikátů
1	Subject: GeoTrust Extended Validation SSL CA - G2 Issued by: GeoTrust Primary Certification Authority SHA-1 fingerprint certifikátu: C4 FA 37 41 B7 A7 F1 F6 C2 3D 24 F4 20 9F 5A 49 CD 5E 55 C6	Subject: GeoTrust Extended Validation SHA256 SSL CA Issued by: GeoTrust Primary Certification Authority - G3 SHA-1 fingerprint certifikátu: E2 8A 01 56 B0 3C 75 E0 5F 81 97 96 FF E9 F9 8B BA B6 F1 E3 SHA-256 fingerprint certifikátu: BC 9E 22 3C C4 22 75 CC 03 41 90 DF 2D 01 79 B5 5B 73 2D 5A C5 31 13 7A 7B 52 2D CF E0 4A 05 92
2	Subject: GeoTrust Primary Certification Authority Issued by: Equifax Secure Certificate Authority SHA-1 fingerprint certifikátu: 68 90 ED 2B 2C 11 10 72 91 2E D6 25 54 59 AD 0D B7 6F 3A D1	Subject: GeoTrust Primary Certification Authority - G3 Issued by: GeoTrust Primary Certification Authority - G3 SHA-1 fingerprint certifikátu: 03 9E ED B8 0B E7 A0 3C 69 53 89 3B 20 D2 D9 32 3A 4C 2A FD SHA-256 fingerprint certifikátu: B4 78 B8 12 25 0D F8 78 63 5C 2A A7 EC 7D 15 5E AA 62 5E E8 29 16 E2 CD 29 43 61 88 6C D1 FB D4
3	Subject: Equifax Secure Certificate Authority Issued by: Equifax Secure Certificate Authority SHA-1 fingerprint certifikátu: D2 32 09 AD 23 D3 14 23 21 74 E4 0D 7F 9D 62 13 97 86 63 3A	

Poznámka: Některé aplikace mohou zobrazovat pro ověření správnosti certifikátu fingerprint založený na hashovací funkci SHA-1. V tabulce je proto uveden fingerprint certifikátů založený na SHA-1 a SHA-256.

Jak bylo řečeno již dříve, nyní nejsme schopni říci, jaká autorita nakonec SSL certifikát pro produkční prostředí vydá. Nemůžeme tedy ani garantovat, který ze dvou uvedených řetězců certifikátů bude nakonec vracen serverem SSL.
Pokud se však budete řídit pokyny uvedenými v dalších kapitolách tohoto dokumentu, budete připraveni na obě varianty.

Dopady na vývojáře aplikací třetích stran napojujících se na ISDS

U aplikací třetích stran, které se napojují na ISDS, je zapotřebí provést následující činnosti:

1. Zajistit podporu hashovacích funkcí SHA-2 v softwaru.
2. Zařazení nových certifikačních autorit do „truststoru“ aplikace.

Zajištění podpory hashovacích funkcí SHA-2 v softwaru

Ujistěte se, že váš software podporuje hashovací funkce SHA-2 (SHA-256, SHA-384, SHA-512) v rámci ověřování platnosti certifikátů. Podle potřeby musíte tuto funkcionalitu do svých softwarových produktů doplnit.
Podle zjištěných informací jsou hashovací funkce SHA-2 podporovány v těchto verzích vývojových prostředí a aplikačních knihoven:

- Java – verze 1.4.2 a vyšší
- .NET Framework – verze 1.1 a vyšší
- OpenSSL – verze 0.9.8o a vyšší
- PHP – verze 5.3.2 a vyšší
- Mozilla NSS – verze 3.8 a vyšší

Pokud daná aplikace využívá k ověřování platnosti certifikátů kryptografické funkce operačního systému, musíte informovat své zákazníky, že je nezbytné používat váš softwarový produkt na takovém operačním systému, který podporuje SHA-2.
Na adrese „https://casecurity.org/resources/“ lze stáhnout dokument „SHA-256 Support List“, který obsahuje přehled operačních systémů, webových prohlížečů a serverů podporujících SHA-256.
Podpora SHA-2 konkrétně v operačních systémech Windows je podrobně popsána na této webové stránce: http://blogs.technet.com/b/pki/archive/2010/09/30/sha2-and-windows.aspx.

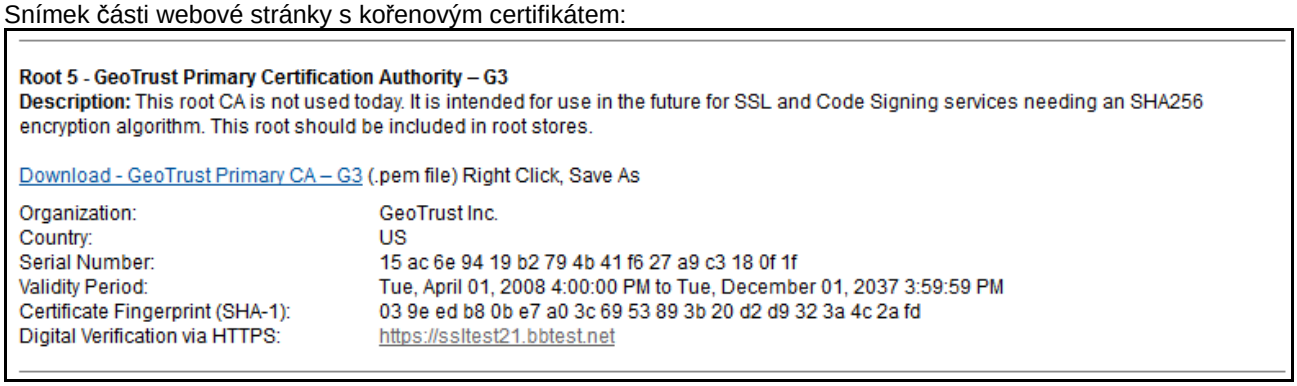
Zařazení nových certifikačních autorit do „truststoru“ aplikace

Některé aplikace mohou zobrazovat pro ověření správnosti certifikátu fingerprint založený na hashovací funkci SHA-1. Proto je dále v textu uveden fingerprint certifikátů založený na SHA-1 a SHA-256.

Certifikát kořenové CA
Do „truststoru“ vaší aplikace přidejte certifikát nové kořenové CA „**GeoTrust Primary Certification Authority – G3**“, který lze stáhnout na následující stránce jako „Root 5“:
https://www.geotrust.com/resources/root-certificates/index.html

Fingerprinty certifikátu:
- SHA-1: 03 9e ed b8 0b e7 a0 3c 69 53 89 3b 20 d2 d9 32 3a 4c 2a fd
- SHA-256: b4 78 b8 12 25 0d f8 78 63 5c 2a a7 ec 7d 15 5e aa 62 5e e8 29 16 e2 cd 29 43 61 88 6c d1 fb d4

Snímek části webové stránky s kořenovým certifikátem:



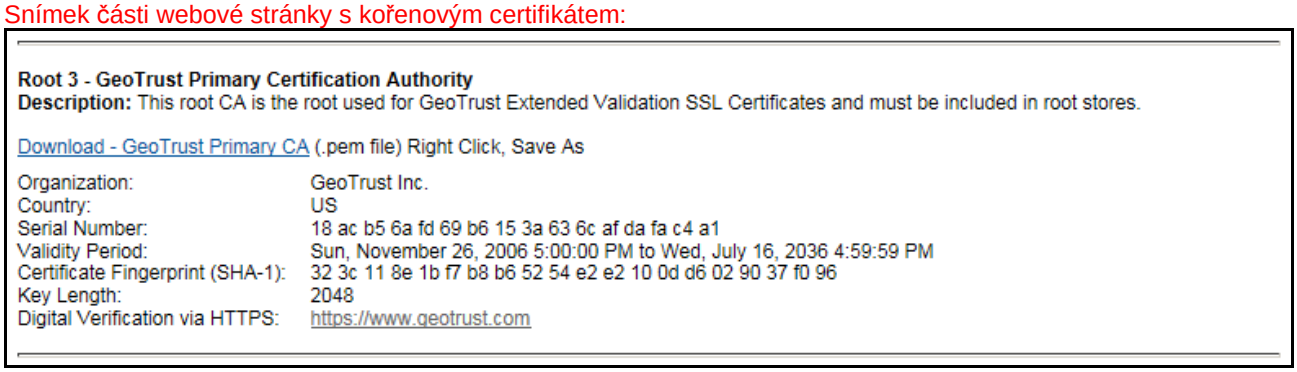
Root 5 - GeoTrust Primary Certification Authority – G3
Description: This root CA is not used today. It is intended for use in the future for SSL and Code Signing services needing an SHA256 encryption algorithm. This root should be included in root stores.

Download - GeoTrust Primary CA – G3 (.pem file) Right Click, Save As

Organization:	GeoTrust Inc.
Country:	US
Serial Number:	15 ac 6e 94 19 b2 79 4b 41 f6 27 a9 c3 18 0f 1f
Validity Period:	Tue, April 01, 2008 4:00:00 PM to Tue, December 01, 2037 3:59:59 PM
Certificate Fingerprint (SHA-1):	03 9e ed b8 0b e7 a0 3c 69 53 89 3b 20 d2 d9 32 3a 4c 2a fd
Digital Verification via HTTPS:	https://ssltest21.bbtest.net

Důležitá změna oproti předchozí verzi dokumentu:
Do „truststoru“ vaší aplikace musíte rovněž přidat certifikát kořenové CA „**GeoTrust Primary Certification Authority**“, pokud tam již není umístěn. Certifikát této autority lze stáhnout jako „Root 3“ ze stránky:
https://www.geotrust.com/resources/root-certificates/index.html
Fingerprinty certifikátu:
- SHA-1: 32 3c 11 8e 1b f7 b8 b6 52 54 e2 e2 10 0d d6 02 90 37 f0 96
- SHA-256: 37 d5 10 06 c5 12 ea ab 62 64 21 f1 ec 8c 92 01 3f c5 f8 2a e9 8e e5 33 eb 46 19 b8 de b4 d0 6c

Snímek části webové stránky s kořenovým certifikátem:



Root 3 - GeoTrust Primary Certification Authority
Description: This root CA is the root used for GeoTrust Extended Validation SSL Certificates and must be included in root stores.

Download - GeoTrust Primary CA (.pem file) Right Click, Save As

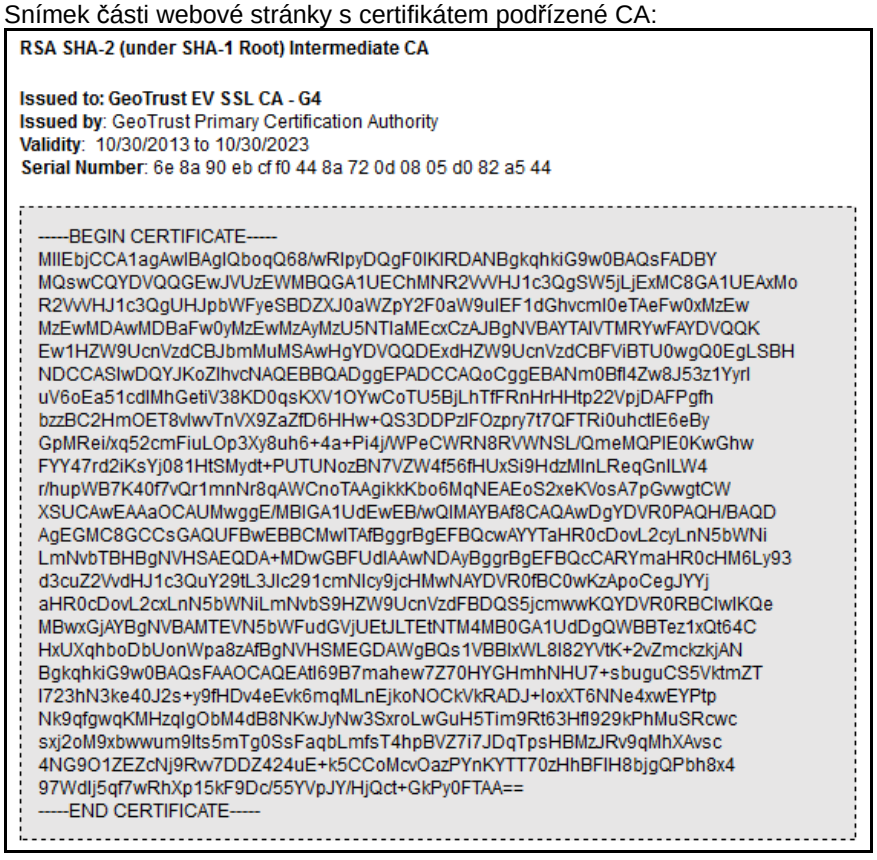
Organization:	GeoTrust Inc.
Country:	US
Serial Number:	18 ac b5 6a fd 69 b6 15 3a 63 6c af da fa c4 a1
Validity Period:	Sun, November 26, 2006 5:00:00 PM to Wed, July 16, 2036 4:59:59 PM
Certificate Fingerprint (SHA-1):	32 3c 11 8e 1b f7 b8 b6 52 54 e2 e2 10 0d d6 02 90 37 f0 96
Key Length:	2048
Digital Verification via HTTPS:	https://www.geotrust.com

Certifikáty podřízených CA

Podřízená certifikační autorita bude obsažena v řetězci certifikátů, který bude vracet server ISDS. Klientské aplikace si obvykle certifikáty podřízených autorit přebírají z tohoto řetězce certifikátů. Za normálních okolností tedy není nutné umisťovat certifikáty podřízených CA do „truststoru“ vaší aplikace.
Pokud je však vaše aplikace navržena tak, že certifikát podřízené CA je v „truststoru“ vyžadován, je zapotřebí do „truststoru“ přidat dva certifikáty podřízených CA:
GeoTrust EV SSL CA - G4 – k dispozici na stránce https://knowledge.geotrust.com/support/knowledge-base/index?page=content&actp=CROSSLINK&id=SO24866
Fingerprinty certifikátu:

- SHA-1: 30 56 b3 43 48 5b 9d 55 f3 e2 b1 77 a8 95 bb 04 63 ee 3e fd
- SHA-256: 95 b0 9d 02 12 2f a8 ae 62 35 78 0f 6e a6 50 3e 76 7a c0 21 a0 87 4f e8 31 ce 80 3a 50 ea 8f d7

Snímek části webové stránky s certifikátem podřízené CA:



RSA SHA-2 (under SHA-1 Root) Intermediate CA

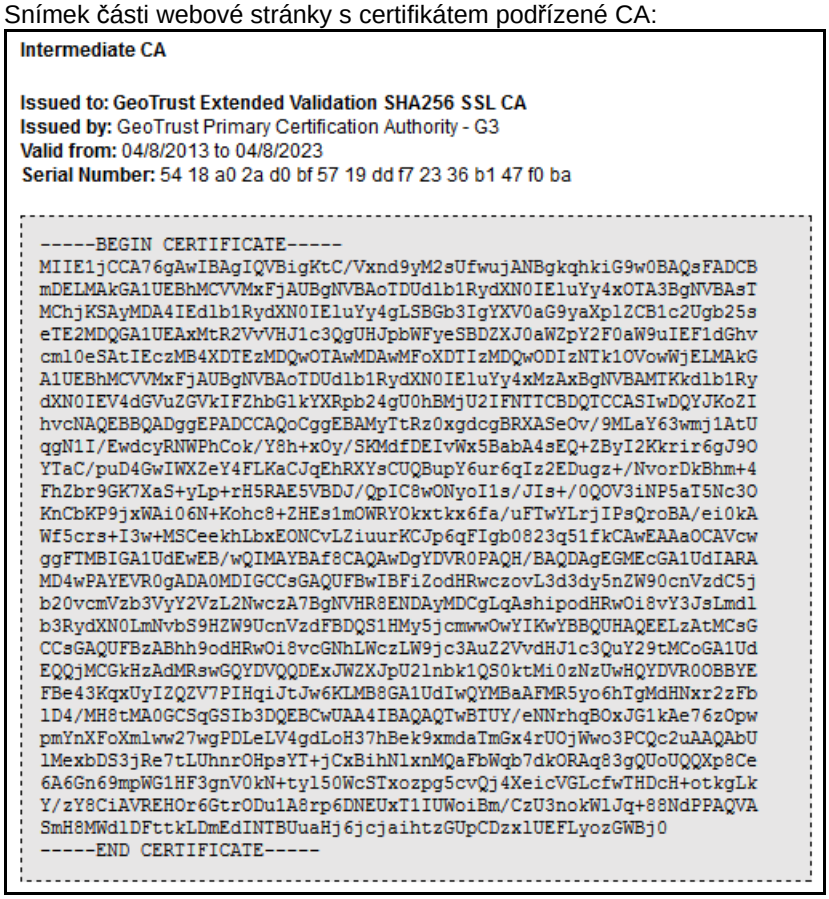
Issued to: GeoTrust EV SSL CA - G4
Issued by: GeoTrust Primary Certification Authority
Validity: 10/30/2013 to 10/30/2023
Serial Number: 6e 8a 90 eb cf f0 44 8a 72 0d 08 05 d0 82 a5 44

-----BEGIN CERTIFICATE-----
MIIEbjCCA1agAwIBAgIQboqQ68/wRIpyDQgF0IKIRDANBgkqhkiG9w0BAQsFADBY
MQswCQYDVQQGEwJVUzEWMBQGA1UEChMNR2VvVHJ1c3QgSW5jLjExMC8GA1UEAxMo
R2VvVHJ1c3QgUHJpbWFyeSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAeFw0xMzEw
MzEwMDAwMDBaFw0yMzEwMzAyMzU5NTlaMEcxCzAJBgNVBAYTAlVTMRYwFAYDVQQK
Ew1HZW9UcnVzdCBJbmMuMSAwHgYDVQQDExdHZW9UcnVzdCBFViBTU0wgQ0EgLSBH
NDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANm0Bfl4Zw8J53z1Yyrl
uV6oEa51cdlMhGetiV38KD0qsKXV1OYwCoTU5BjLhTfFRnHrHHtp22VpjDAFPgfh
bzzBC2HmOET8vlwvTnVX9ZaZfD6HHw+QS3DDPzlFOzpry7t7QFTRi0uhctlE6eBy
GpMRei/xq52cmFiuLOp3Xy8uh6+4a+Pi4j/WPeCWRN8RVWNSL/QmeMQPlE0KwGhw
FYY47rd2iKsYj081HtSMydt+PUTUNozBN7VZW4f56fHUxSi9HdzMlnLReqGnILW4
r/hupWB7K40f7vQr1mnNr8qAWCnoTAAgikkKbo6MqNEAEoS2xeKVosA7pGvwgtCW
XSUCAwEAAaOCAUMwggE/MBIGA1UdEwEB/wQIMAYBAf8CAQAwDgYDVR0PAQH/BAQD
AgEGMC8GCCsGAQUFBwEBBCMwITAfBggrBgEFBQcwAYYTaHR0cDovL2cyLnN5bWNi
LmNvbTBHBgNVHSAEQDA+MDwGBFUdIAAwNDAyBggrBgEFBQcCARYmaHR0cHM6Ly93
d3cuZ2VvdHJ1c3QuY29tL3Jlc291cmNlcy9jcHMwNAYDVR0fBC0wKzApoCegJYYj
aHR0cDovL2cxLnN5bWNiLmNvbS9HZW9UcnVzdFBDQS5jcmwwKQYDVR0RBCIwIKQe
MBwxGjAYBgNVBAMTEVN5bWFudGVjUEtJLTEtNTM4MB0GA1UdDgQWBBTez1xQt64C
HxUXqhboDbUonWpa8zAfBgNVHSMEGDAWgBQs1VBBlxWL8I82YVtK+2vZmckzkjAN
BgkqhkiG9w0BAQsFAAOCAQEAtl69B7mahew7Z70HYGHmhNHU7+sbuguCS5VktmZT
l723hN3ke40J2s+y9fHDv4eEvk6mqMLnEjkoNOCkVkRADJ+loxXT6NNe4xwEYPtp
Nk9qfgwqKMHzqIgObM4dB8NKwJyNw3SxroLwGuH5Tim9Rt63Hfl929kPhMuSRcwc
sxj2oM9xbwwum9lts5mTg0SsFaqbLmfsT4hpBVZ7i7JDqTpsHBMzJRv9qMhXAvsc
4NG9O1ZEZcNj9Rw7DDZ424uE+k5CCoMcvOazPYnKYTT70zHhBFIH8bjgQPbh8x4
97WdIj5qf7wRhXp15kF9Dc/55YVpJY/HjQct+GkPy0FTAA==
-----END CERTIFICATE-----

GeoTrust Extended Validation SHA256 SSL CA – k dispozici na stránce
https://knowledge.geotrust.com/support/knowledge-base/index?page=content&actp=CROSSLINK&id=SO24887
Fingerprinty certifikátu:

- SHA-1: e2 8a 01 56 b0 3c 75 e0 5f 81 97 96 ff e9 f9 8b ba b6 f1 e3
- SHA-256: bc 9e 22 3c c4 22 75 cc 03 41 90 df 2d 01 79 b5 5b 73 2d 5a c5 31 13 7a 7b 52 2d cf e0 4a 05 92

Snímek části webové stránky s certifikátem podřízené CA:



Intermediate CA

Issued to: GeoTrust Extended Validation SHA256 SSL CA
Issued by: GeoTrust Primary Certification Authority - G3
Valid from: 04/8/2013 to 04/8/2023
Serial Number: 54 18 a0 2a d0 bf 57 19 dd f7 23 36 b1 47 f0 ba

```
-----BEGIN CERTIFICATE-----
MIIE1jCCA76gAwIBAgIQVBigKtC/Vxnd9yM2sUfwujANBgkqhkiG9w0BAQsFADCB
mDELMAkGA1UEBhMCVVMxFjAUBgNVBAoTDUdlb1RydXN0IEluYy4xOTA3BgNVBAsT
MChjKSAyMDA4IEdlb1RydXN0IEluYy4gLSBGb3IgYXV0aG9yaXplZCB1c2Ugb25s
eTE2MDQGA1UEAxMtR2VvVHJ1c3QgUHJpbWFyeSBDZXJ0aWZpY2F0aW9uIEF1dGhv
cml0eSAtIEczMB4XDTEzMDQwOTAwMDAwMFoXDTIzMDQwODIzNTk1OVowWjELMAkG
A1UEBhMCVVMxFjAUBgNVBAoTDUdlb1RydXN0IEluYy4xMzAxBgNVBAMTKkdlb1Ry
dXN0IEV4dGVuZGVkIFZhbGlkYXRpb24gU0hBMjU2IFNTTCBDQTCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBAMyTtRz0xgdcgBRXASeOv/9MLaY63wmj1AtU
qgN1I/EwdcyRNWPhCok/Y8h+xOy/SKMdfDEIvWx5BabA4sEQ+ZByI2Kkrir6gJ9O
YTaC/puD4GwIWXZeY4FLKaCJqEhRXYsCUQBupY6ur6qIz2EDugz+/NvorDkBhm+4
FhZbr9GK7XaS+yLp+rH5RAE5VBDJ/QpIC8wONyoI1s/JIs+/0QOV3iNP5aT5Nc3O
KnCbKP9jxWAi06N+Kohc8+ZHEs1mOWRYOkxtkx6fa/uFTwYLrjIPsQroBA/ei0kA
Wf5crs+I3w+MSCeekhLbxEONCvLZiuurKCJp6qFIgb0823q51fkCAwEAAaOCAVcw
ggFTMBIGA1UdEwEB/wQIMAYBAf8CAQAwDgYDVR0PAQH/BAQDAgEGMEcGA1UdIARA
MD4wPAYEVR0gADA0MDIGCCsGAQUFBwIBFiZodHRwczovL3d3dy5nZW90cnVzdC5j
b20vcmVzb3VyY2VzL2NwczA7BgNVHR8ENDAyMDCgLqAshipodHRwOi8vY3JsLmdl
b3RydXN0LmNvbS9HZW9UcnVzdFBDQS1HMy5jcmwwOwYIKwYBBQUHAQEELzAtMCsG
CCsGAQUFBzABhh9odHRwOi8vcGNhLWczLW9jc3AuZ2VvdHJ1c3QuY29tMCoGA1Ud
EQQjMCGkHzAdMRswGQYDVQQDExJWZXJpU2lnbk1QS0ktMi0zNzUwHQYDVR0OBBYE
FBe43KqxUyIZQZV7PIHqiJtJw6KLMB8GA1UdIwQYMBaAFMR5yo6hTgMdHNxr2zFb
lD4/MH8tMA0GCSqGSIb3DQEBCwUAA4IBAQAQTwBTUY/eNNrhqBOxJG1kAe76zOpw
pmYnXFoXmlww27wgPDLeLV4gdLoH37hBek9xmdaTmGx4rUOjWwo3PCQc2uAAQAbU
lMexbDS3jRe7tLUhnrOHpsYT+jCxBihNlxnMQaFbWqb7dkORAq83gQUoUQQXp8Ce
6A6Gn69mpWG1HF3gnV0kN+tyl50WcSTxozpg5cvQj4XeicVGLcfwTHDcH+otkgLk
Y/zY8CiAVREHOr6GtrODu1A8rp6DNEUxT1IUWoiBm/CzU3nokWlJq+88NdPPAQVA
SmH8MWdlDFttkLDmEdINTBUuaHj6jcjaihtzGUpCDzxlUEFLyozGWBj0
-----END CERTIFICATE-----
```

Jak ověřit funkčnost/kompatibilitu vaší aplikace s SHA-256 certifikáty?

Kompatibilitu vaší aplikace s certifikační autoritou „**GeoTrust EV SSL CA - G4**“ si ověříte na veřejném testovacím prostředí ISDS. Adresa webových služeb veřejného testovacího prostředí ISDS je uvedena v příloze č. 2 provozního řádu ISDS. O přístup k veřejnému testu ISDS (zřízení testovacích datových schránek) musí vývojář požádat Ministerstvo vnitra. Žádost se vytváří pomocí formuláře, který lze stáhnout ze stránky:
https://www.datoveschranky.info/o-datovych-schrankach/vyzkousejte-si-datovou-schranku
Kompatibilitu vaší aplikace s certifikační autoritou „**GeoTrust Extended Validation SHA256 SSL CA**“ si ověříte jen částečně tak, že se vaší aplikací pokusíte navázat SSL spojení se zkušební webovou stránkou SSLTEST21, kterou provozuje autorita GeoTrust: https://ssltest21.bbtest.net/
Tato zkušební stránka pochopitelně nedisponuje funkcemi ISDS.
Silně doporučujeme provést ve vaší aplikaci oba výše uvedené testy. Jedině tak budete mít jistotu, že je vaše aplikace připravena na obě certifikační autority GeoTrust.