Popis aplikačního programového rozhraní CertIQ 2

MathAn Praha
31.10.2016

Aplikace CertIQ 2 provádí ověření certifikátu oproti periodicky stahovaným seznamům služeb vytvářejících důvěru (*Trusted Lists*) vydávaných členskými státy Evropské unie a Evropského hospodářského prostoru v souladu s nařízením eIDAS a návaznými předpisy a standardy. Tato funkčnost je dostupná běžným uživatelům přes webové rozhraní a zároveň i jako webová služba typu REST. Tento dokument obsahuje popis této webové služby – aplikačního programového informačního systému CertIQ 2.

CertIQ 2 API

Volání služby ověření certifikátu

Služba je dostupná na adrese http://tsl.gov.cz/certiq/services/CertificateValidationService. Alternativně je dostupná i protokolem HTTPS.

Služba poskytuje metodu validateCertificate dostupnou metodou POST. Tělem požadavku POST je certifikát, který má být kontrolován, uvedený v kódování DER. Hlavička požadavku Content-Type musí mít hodnotu application/octet-stream.

Metoda validateCertificate může mít volitelný parametr referenceTime, který se uvádí jako pokračování cesty ve volajícím URL. Jeho hodnota může být specifikace časového okamžiku, ke kterému se má kontrola certifikátu provést. Není-li parametr uveden, provádí se kontrola k současnému okamžiku. Hodnota parametru referenceTime musí být tvaru odpovídajícího specifikaci rozšířeného data a času podle standardu ISO 8601.[1] Například pro kontrolu certifikátu k času 9:25:42 středoevropského letního času dne 1.8.2016 se certifikát zašle službě na adresu http://tsl.gov.cz/certiq/services/CertificateValidationService/validateCertificate/referenceTime/2016-08-01T09:25:42+02:00. Čas musí být vždy uveden kompletní včetně časové zóny. Za sekundami mohou být případně po desetinné tečce uvedeny další číslice zpřesňující časový údaj.

Výsledek práce služby ověření certifikátu

Služba ověření certifikátu vydá odpověď ve formátu XML ve jmenném prostoru urn:cz:isvs:mvcr:schemas:certiq-2.0. XML Schema pro tento jmenný prostor bude zveřejněno na adrese http://tsl.gov.cz/certiq/schemas/certiq-2.0.xsd. Odpověď služby obsahuje následující údaje:

- Datum a čas provedení kontroly certifikátu
- Referenční datum a čas – okamžik, ke kterému se má zjišťovat stav, typ a další údaje služby z příslušného seznamu služeb vytvářejících důvěru
- Seznam služeb vytvářejících důvěru, které odpovídají předloženému

1 https://docs.oracle.com/javase/8/docs/api/java/time/format/DateTimeFormatter.html#ISO_OFFSET_DATE_TIME

certifikátu (tj. služba, která certifikát vydala či jej používá). Tento seznam bude typicky prázdný nebo bude obsahovat jednu službu, avšak v některých případech může být služeb i více. Pro každou odpovídající službu vytvářející důvěru se uvedou následující údaje (ze seznamu služeb vytvářejících důvěru):

- Typ služby
- Jméno služby
- Poskytovatel služby: název, adresa.
- Stav služby k referenčnímu okamžiku včetně časového intervalu platnosti tohoto stavu
- Digitální identita služby (*Service digital identity*)
- Rozšířené informace o službě – uvedeny jsou ty kvalifikátory, jejichž podmínky předložený certifikát splňuje
- Informace o seznamu služeb vytvářejících důvěru, ze kterého jsou čerpány informace

Fakt, zda se jedná o kvalifikovaný certifikát či o certifikát kvalifikovaného poskytovatele služeb vytvářejících důvěru, na základě kterého jsou podepsána či opatřena pečetí elektronická časová razítka, zjistí uživatel webové služby služby z typu služby a jejího stavu.

Případné rozlišení u kvalifikovaného certifikátu (zda jde o kvalifikovaný certifikát pro elektronický podpis, pro elektronickou pečeť nebo pro autentizaci internetových stránek) provede uživatel služby z rozšířených informací o službě vytvářející důvěru.

Příklad volání služby ověření certifikátu z příkazové řádky

Nechť soubor cert.der obsahuje certifikát, který má být kontrolován. Následující volání programu curl[2] tento certifikát předloží k posouzení webové službě CertIQ 2:

```
curl -X POST --data-binary @cert.der --header "Content-Type: application/octet-stream" \
    https://tsl.gov.cz/certiq/services/CertificateValidationService/validateCertificate
```

Příklad pozitivní odpovědi (služba, která vydala nebo používá certifikát, je na některém seznamu služeb vytvářejících důvěru):

```
<?xml version="1.0" encoding="utf-8"?>
<OvereniCertifikatu xmlns="urn:cz:isvs:mvcr:schemas:certiq-2.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="urn:cz:isvs:mvcr:schemas:certiq-2.0 http://tsl.gov.cz/certiq/schemas/certiq-2.0.xsd">
  <DatumCasZahajeni>2016-07-04T06:58:33+02:00</DatumCasZahajeni>
  <DatumCasReferencni>2016-07-01T09:25:00+02:00</DatumCasReferencni>
  <Certifikat>
    <PredmetJmeno>Ing. ROMAN SLAVÍK</PredmetJmeno>
    <ID>2051A32FAEFC114C575E562BFEF97EC251C130B27884A1B18C864D5022345C87</ID>
  </Certifikat>
  <OdpovidajiciSluzby>
    <Sluzba>
```

2 https://curl.haxx.se/

```
    <Typ>http://uri.etsi.org/TrstSvc/Svctype/CA/QC</Typ>
    <Jmeno>(78) I.CA - vydávání kvalifikovaných certifikátů</Jmeno>
    <Poskytovatel>
      <Jmeno>První certifikační autorita, a.s.</Jmeno>
      <Adresa>Podvinný mlýn 2178/6, 19000, Praha 9, CZ</Adresa>
    </Poskytovatel>
    <Stav platnostOd="2016-07-01T02:00:00+02:00">http://uri.etsi.org/TrstSvc/TrustedList/Svcstatus/granted</Stav>
    <ServiceDigitalIdentity xmlns="http://uri.etsi.org/02231/v2#">
      <DigitalId>
<X509Certificate>MIIHpTCCBY2gAwIBAgIEBfXk7jANBgkqhkiG9w0BAQsFADBwMQswCQYDVQQGEwJDWjEtMCsGA1UECgwkUHJ2bsOtIGNlcnRpZmlrYcSNbsOtIGF1dG9yaXRhLCBhLnMuMRkwFwYDVQ
QDDBBJLkNBIFJvb3QgQ0EvUlNBMRcwFQYDVQQFEw5OVFJDWi0yNjQzOTM5NTAeFw0xNjAyMTExMjE3MTFaFw0yNjAyMDgxMjE3MTFaMH8xCzAJBgNVBAYTAkNaMSgwJgYDVQQDDB9JLkNBIFF1YWxpZmlIZCAyI
ENBL1JTQSAwMi8yMDE2MS0wKwYDVQQKDCRQcnZuw60gY2VydGlmaWthxI1uw60gYXV0b3JpdGEsIGEucy4xFzAVBgNVBAUTDk5UUkNaLTI2NDM5Mzk1MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAy
MALHP/YeXEtOEHHJXTrhOrZWZ5SeX3f8phlvUiCIxoJt2yZ4CI2Y26tSuD+Ard7c539buJlzoZnuFs6xswvSVJwpwoKF3pfIZ5DZjyqUhPpDZdEXQyne1U9uo1T9wD1WWKQ/yONzKcawxfH2tr0ourILIjVtB6I99u5uA7fIA/mynGuc
R1C4PC9WbY4MrRV+YkSAzWb88K1wyhVZ0Tq50+jINrL8xCGzRNLSPbMw9lBsWNPfcom2ajPbmIfyaf3uMBGNdNxUjQoiBjC0mYWkrEd95K6S0dkOA8Kgell/3Kyut/kxc1RsLXgIo0DNSQ9F38q2I8KWpmxm2sOAHBR191f
NEwhnfomCi1jjx6nHpIhHR1Vs5KcjL6z8Qr42otM55qtEBhOnM1juPZs5+GYjpHG08e9cATWBC3GLd59hN6uSdZjNSb6LVg0hB194Jb29WpaNj0wzEx98zR1W4NQy+EXSaBfj8bb7UZrxtSoJzF2YMNAPb/oYlRVNuP4tmnUs
W3m6r09j7cltBXCo/YfXDRX0rWNlJ7p+gDRHU1+nPlih6LWgyI/yrhJqGg4dg63YyywvuuoDI0zfjlhBSkqQymNwNelg1mDcEFUVxk8LKzXPXJlFNEt33+qT+CMXlR+IkUC0jOl1SZV3uwcAwgbQWazNljKFpoJjGXc4fwh2A8CAw
EAAaOCAjYwggIyMIHXBgNVHSAEgc8wgcwwgckGBFUdIAAwgcAwgb0GCCsGAQUFBwICMIGwGoGtVGVudG8ga3ZhbGlmaWtvdmFueSBzeXN0ZW1vdnkgY2VydGlmaWthdCBieWwgdnlkYW4gcG9kbGUgemFrb25hIDI
yNy8yMDAwIFNiLiB2IHBsYXRuZW0gem5lbmkvVGhpcyBxdWFsaWZpZWQgc3lzdGVtIGNlcnRpZmljYXRlIHdhcyBpc3N1ZWQgYWNjb3JkaW5nIHRvIEFjdCBOby4gMjI3LzIwMDAgQ29sbC4wEgYDVR0TAQH/BAgwBgEB/
wIBADAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0OBBYEFHSCCJHj2WRocYXW6zHkct+LJrFtMB8GA1UdIwQYMBaAFHa5A0j71RihoTeg7cxogkxSNDYNMIGMBgNVHR8EgYQwgYEwKaAnoCWGI2h0dHA6Ly9xY3JsZH
AxLmljYS5jei9yY2ExNV9yc2EuY3JsMCmgJ6AlhiNodHRwOi8vcWNybGRwMi5pY2EuY3ovcmNhMTVfcnNhLmNlcjAoBggrBgEFBQcwAYYcaHR0cDovL29jc3AuaWNhLmN6L3JjYTE1X3JzYS5jcmwwYwYIKwYBBQUHAQEEVz
BVMCkGCCsGAQUFBzAChh1odHRwOi8vci5pY2EuY3ovcmNhMTVfcnNhLmNlcjAoBggrBgEFBQcwAYYcaHR0cDovL29jc3AuaWNhLmN6L3JjYTE1X3JzYS5jcmwwYwYIKwYBBQUHAQEEVz
PRspgixVwI4TQBW+9uQXPz0Og3C2Qf7FHZwlB93EXz9D4jxQwffA0fugp/eRu6eZ6v55tR7M5Vvl3rlBPFVlDs1+8CWLABLtX61hcXslU1Sdtqi6lGab9pDoBMdvLOky/CLMdQvA01XMEjCUIslT+U6UlCUhGG3Oh/KBqIORdFc
WaseoInsJrBpiAA8+wohMKZGomKSXYIUtuwywZ/GNrkHhJd5nN7auEDnM39uAYINSeQ7pHYFtyb4Xik8jOsk5LaQcgC/yOOcVVcZhmPJFamwA+xBhJY+ynoB7cJyLx2IxiO/7PHSBNsobUaFobfAVNJgoY8X+FYmlcGv5526v
8dHH6FEdyq/0mxeXlFpqLrscfJj4zWNcs8+zmrphCrRgeWrrZkciJ+f6tceW+hdDYtpoHDhpJHnUJRqc2R67x88t55DL9vjcbGNB8CTOthlOUv1UWzmIVO0FOEomUKy7d6cf4g2qbF6Fbq9l3WzkYyxlizNmEAFVDhT2YdK19lWK
8dlabxjIH9KF1yuhIG71NJWM6EVz9058ebJcfPdpTRhNkZd+X84+YeFDsxYtOd8Q+L3CmX2Xzj9GrssN9ewTVeW7acSLa5gcdzAiTUF92rQUfuVwr0zGuvZLnsoLIIsaWrx+pgHcBnL49PVJQV5w4c=
</X509Certificate>
      </DigitalId>
    </ServiceDigitalIdentity>
    <RozsireneInformace>
      <Qualifiers>
        <Qualifier uri="http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/QCQSCDStatusAsInCert" />
      </Qualifiers>
      <AdditionalServiceInformation xmlns="http://uri.etsi.org/02231/v2#">
        <URI xml:lang="en">http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures</URI>
      </AdditionalServiceInformation>
    </RozsireneInformace>
    <DuveryhodnySeznam>
      <Uzemi>CZ</Uzemi>
      <PoradoveCislo>42</PoradoveCislo>
      <DatumCasVydani>2016-07-25T10:20:00+02:00</DatumCasVydani>
      <DatumCasDalsihoVydani>2017-01-10T11:00:00+01:00</DatumCasDalsihoVydani>
      <DatumCasStazeni>2016-11-09T16:05:55.87+01:00</DatumCasStazeni>
    </DuveryhodnySeznam>
  </Sluzba>
 </OdpovidajiciSluzby>
</OvereniCertifikatu>
```

Příklad negativní odpovědi (služba, která vydala nebo používá certifikát, není na žádném seznamu služeb vytvářejících důvěru, tj. element OdpovidajiciSluzby je prázdný):

```
<?xml version="1.0" encoding="utf-8"?>
<OvereniCertifikatu xmlns="urn:cz:isvs:mvcr:schemas:certiq-2.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation="urn:cz:isvs:mvcr:schemas:certiq-2.0 http://tsl.gov.cz/certiq/schemas/certiq-2.0.xsd">
 <DatumCasZahajeni>2016-07-04T06:58:33+02:00</DatumCasZahajeni>
 <DatumCasReferencni>2016-07-01T02:00:00+02:00</DatumCasReferencni>
 <Certifikat>
  <PredmetJmeno>Ing. ROMAN SLAVÍK</PredmetJmeno>
  <ID>2051A32FAEFC114C575E562BFEF97EC251C130B27884A1B18C864D5022345C87</ID>
 </Certifikat>
 <OdpovidajiciSluzby/>
</OvereniCertifikatu>
```

V případě chyby je odpověď prázdná nebo obsahuje kód chyby.