RIKSGÄLDEN
SWEDISH NATIONAL DEBT OFFICE

Dnr 2014/1651
2017-07-18

Arkivering, kryptering och signering v 3.1

Riksgäldskontoret
ORG.NR.
202100-2635

POSTADRESS POSTAL ADDRESS
SE-103 74 Stockholm
Sweden

BESÖK VISITORS
Norrlandsgatan 15

TELEFON TELEPHONE
NAT. 08 613 52 00
INT. +46 8 613 52 00

TELEFAX
NAT. 08 21 85 53
INT. +46 8 21 85 53

INTERNET
riksgalden@riksgalden.se
www.insattningsgarantin.se

Innehållsförteckning

Inledning

Observera att Riksgälden inte kan ta ansvar för några produkter som nämns i detta dokument. Inte heller kan vi garantera att de exempel som ges är kompletta eller korrekta. De är bara tänkta som en översiktlig hjälp för att komma igång med tekniken. Riksgälden rekommenderar alla institut att noga läsa och förstå dokumentationen till de produkter de väljer att använda sig av.

Arkivering och komprimering

De fyra textfilerna ska arkiveras och komprimeras till ett 7z-arkiv[1]. Filformat för 7z-arkiv finns specificerat i källkoden till 7-zip[3]. MIME-typen för 7z-arkiv är *application/x-7z-compressed*.

Exempel

Skapa de fyra textfilerna enligt filspecifikation i detta dokument.

Skapa ett 7z-arkiv av dessa filer:

```
7za a -t7z -m0=lzma -mx=9 -mfb=64 -md=32m -ms=on till_riksgalden.7z
   fil1.txt fil2.txt fil3.txt fil4.txt
```

Obs! Om Windows-versionen av 7-Zip används heter kommandot 7z istället för 7za. Man kan även skapa ett 7-zip arkiv i GUI-versionen av 7-zip.

Kryptering och signering

Det 7z-arkiv som skapats ska nu krypteras och signeras så att den resulterande filen är en fil i Cryptographic Message Syntax (CMS[2]) -format.

Kryptering och signering kan göras med programvaran OpenSSL[4] eller annan programvara som är kompatibel med specifikationen för CMS.

Godkända krypterings- och hashalgoritmer och nyckellängder måste väljas ur en av Riksgälden given lista som finns nedan i avsnittet ”Krav på kryptografisk teknik”.

De certifikat som ska användas för kryptering och signering levereras av Buypass och beställs från Riksgälden.

- Vid kryptering ska Riksgäldens publika certifikat användas. Riksgälden ansvarar för att publicera det publika certifikatet på https://ig.riksgalden.se. Observera att det inte är webserverns certifikat som ska användas för krypteringen.
- För signering ska det certifikat, som institutet erhållit från Riksgäldens certifikatutgivare Buypass, användas. Som framgår ovan beställs detta certifikat från Riksgälden, se Bilaga 1 ”Beställning av certifikat”. Vid beställning ska beställningsblanketten fyllas i och skickas in.

- Institutet ansvarar för att vid var tidpunkt ha ett giltigt certifikat. Tre månader före utgången av certifikatets giltighetsperiod kan ett nytt certifikat beställas. Buypass meddelar per e-post institutet på de e-postadresser som angavs i ansökan 2 månader innan certifikatet förfaller.
- Krypteringen ska endast ske med av Riksgälden godkända krypteringsalgoritmer och nyckellängder (se avsnittet ”Krav på kryptografisk teknik”).
- Signeringen ska endast ske med hjälp av godkänd hashalgoritm och godkänd krypteringsalgoritm och nyckellängd (se avsnittet ”Krav på kryptografisk teknik”).
- Samtidigt som ett institut beställer sitt certifikat så ska man även till Riksgälden uppge en eller flera, dock maximalt fem, unika IP-adresser. Undantagsvis kan Riksgälden godkänna att en range istället anges. Endast dessa adresser kan användas som avsändare när institutet sedan ska ladda upp informationsfilerna till Riksgälden, se avsnittet ” Uppladdning till Riksgälden”. Om institutet redan tidigare meddelat Riksgälden IP-adresserna behöver detta inte ske vid varje certifikatsbeställning såvida man inte önskar ändra dessa.

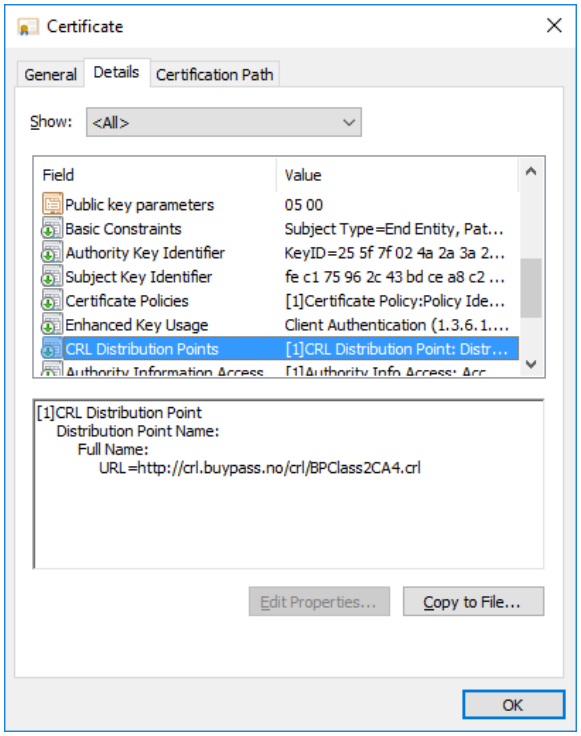
Nedan följer exempel på hur kryptering och signering kan göras med OpenSSL.

Kryptering och signering (OpenSSL)

Börja med att kopiera filerna i IGEncrypt.zip. ”IGEncrypt.pem” är den nyckel ni ska kryptera emot och CA.pem innehåller rootcertifikat och intermediate-CA.

Processen startar med en kontroll av att Riksgäldens cerifikat är giltigt och inte har revokerats. OpenSSL kan arbeta dels med en CA-fil som innehåller alla CA:s och en lista med revokerade certifikat, eller en katalogstruktur. I detta exempel beskrivs tekniken med en CA-fil.

Ladda hem en lista med revokerade certifikat. Detta kan ske genom att man men en webläsare ansluter sig mot den adress som pekas ut i certifikatet. För att få fram rätt URL kan man i Windows öppna certifikatet, välja fliken ”Details”, och läsa fältet ”CRL Distribution Points”.



I vårt exempel är adressen:
http://crl.buypass.no/crl/BPClass2CA4.crl

När CRL:en är nedladdad så måste den konverteras till PEM-format.

```
openssl crl -in BPClass2CA4.crl -inform DER -out LatestCRL.pem
```

LatestCRL.pem ska sedan konkateneras till filen CA.pem. Detta kan ske med en enkel filkopiering.

```
copy CA.pem + LatestCRL.pem CACRL.pem
```

Revokeringskontrollen kan sedan göras genom att köra följande kommando:

```
openssl verify -crl_check -CAfile CACRL.pem IGEncrypt.pem
```

OpenSSL ska ge följande meddelande:

```
IGEncrypt.pem: OK
```

Observera att kontrollen alltid måste göras med en nyligen uppdaterad CRL.

Kryptering av filen sker så här:

```
openssl cms -encrypt -binary -aes256 -in till_riksgalden.7z -out
  till_riksgalden.7z.krypterat -outform der IGEncrypt.pem
```

Signering:

```
openssl cms -sign -binary -md SHA512 -in till_riksgalden.7z.krypterat -
  inform der -out till_riksgalden.7z.krypterat.signerat -outform der -
  nodetach -signer signeringscert.pem
```

Filen ”signeringscert.pem” skapades tidigare om dokumentet ”Beställning-av-certifikat” följts.

Som nämnts ovan får även annan programvara användas för kryptering och signering om institutet kan garantera att programvaran som används följer CMS. Restriktioner gällande krypterings- och hashalgoritm och nyckellängd gäller som vanligt.

Uppladdning till Riksgälden – endast på begäran

Den krypterade filen kan nu skickas till Riksgälden genom att starta en webbläsare och ange adressen https://ig.riksgalden.se. Följ sedan de instruktioner som visas på webbsidan. **Observera att detta endast ska göras på Riksgäldens begäran.**

Notera att uppladdning till Riksgälden endast kan göras från en av de unika IP-adresser som institutet på förhand har angivit till Riksgälden.

Obs! Det är viktigt att uppmärksamma eventuella säkerhetsvarningar då man besöker ig.riksgalden.se. Om webbläsaren varnar för problem med certifikat eller att webbplatsen på annat sätt inte är pålitlig, kontakta Riksgälden.

Tekniska krav på institutets unika IP-adresser

Den eller de IP-adresser som institutet uppger till Riksgäldskontoret ska vara adresser enligt formatet IPv4.

Krav på kryptografisk teknik

1. Kryptering ska ske med krypteringsalgoritmen AES256.
2. Signering ska ske med hashalgoritmen SHA512.
3. Meddelandeformatet ska följa CMS (RFC5652).
4. Anonyma metoder för nyckelutbyte får inte användas.
5. Minsta tillåtna längd på kryptografiska nycklar för asymmetriska algoritmer är 2048 bitar.

6. Väl kända och granskade implementeringar av kryptografiska programvaror ska användas.

7. Det kryptografiska systemet ska ha skydd mot angrepp såsom (i) att någon ställer sig som mellanhand mellan server och klient och på så sätt obehörigen tar del av information (s.k. man-in-the-middle), (ii) repetition, och (iii) fördröjnings attacker.

Viktigt att tänka på angående kryptografi och PKI

Det är mycket viktigt att:

- hantera privata nycklar på rätt sätt.
- verifiera att man verkligen kommunicerar med rätt part.
- förstå vad kryptografi skyddar mot och ej.

Om den privata nyckel man använder på något sätt blir tillgänglig för en angripare så innebär detta kort och gott att all kryptografi baserad på denna nyckel är verkningslös. Data kan avlyssnas och modifieras eller förfalskas enligt en angriparens godtycke. Det är därför av yttersta vikt att man skyddar sin privata nyckel på alla sätt man kan; det absolut bästa, om än inte alltid praktiskt möjligt, är att inte ha den privata nyckeln online någonsin. En sökning på Google med söksträngen

```
http://www.google.com/search?q=%22BEGIN+PGP+PRIVATE+KEY+BLOCK%22+filetype%3Aasc
```

ger 88 unika resultat per 2011-05-04. Detta är alltså personer som gjort sina privata certifikat tillgängliga för alla genom att ha dem på sina webbsiter. Även om man inte delar ut sin privata nyckel på en webbplats så är det viktigt att komma ihåg att den dator man använder kan vara angripen och att även en privat nyckel som inte finns utdelad kan bli kopierad av en angripare. Därför vill vi påpeka igen att det bästa är att inte överhuvudtaget ha den privata nyckeln tillgänglig på en maskin som är online.

Skulle den privata nyckeln bli komprometterad ska certifikatet revokeras. Detta sker lämpligen genom att kontakta Buypass. Revokering kan då genomföras av någon av de personer som angavs på den ursprungliga ansökan. Riksgälden kan också revokera certifikatet för institutets räkning.

Revokering av certifikatet ske på följande adress:

http://www.buypass.com/support/revocation-service-ssl-vid

Referenser

[1] http://www.7-zip.org/7z.html

[2] RFC-5652 - Cryptographic Message Syntax

[3] http://www.7-zip.org/download.html

[4] http://www.openssl.org/docs/apps/cms.html