HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Metode povlačenja digitalnih certifikata

CCERT-PUBDOC-2005-03-115

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Infrastruktura javnih ključeva, odnosno PKI (eng. *public key infrastructure*) predstavlja tehnologiju koja omogućava autentikaciju, korištenje digitalnih potpisa, osiguranje tajnosti i neporecivosti na globalnoj razini. Temelj tehnologije predstavlja ISO/IEC CCITT/ITU-T X.509 standard iz 1994. godine (postoji i ranija inačica iz 1988.), odnosno njegov Internet profil definiran u RFC dokumentu 3280 (http://www.ietf.org/rfc/rfc3280.txt).

PKI infrastruktura sama po sebi nema posebnu vrijednost ili korist za neku organizaciju. Pravu vrijednost i fleksibilnost PKI infrastrukture osiguravaju servisi i aplikacije koji za identifikaciju, autentikaciju, digitalne potpise te osiguranje neporecivosti i tajnosti koriste PKI infrastrukturu, odnosno digitalne certifikate. Na globalnoj razini, PKI se danas najčešće koristi za (uglavnom poslužiteljsku) autentikaciju za sigurnu (HTTPS) Web komunikaciju i digitalne potpise odnosno šifriranje e-mail poruka (slično kao i PGP). Postoji još dosta servisa i aplikacija koje koriste mogućnosti PKI infrastrukture, ali njihova uporaba nije globalna, već je ograničena na pojedina okruženja (korporativna ili najčešće bankarska).

Općenito gledajući, u današnjem svijetu PKI se koristi osjetno manje nego što se to predviđalo pred 5 ili 10 godina, kada se smatralo da će PKI izrasti u globalnu infrastrukturu. Bez obzira na to, zbog svoje fleksibilnosti i mogućnosti koje pruža, primjena PKI ipak je sve češća i češća.

U dokumentu će ukratko biti opisana sama PKI infrastruktura i osnovni elementi koji je sačinjavaju, a zatim će detaljno biti opisani postupci kojima se izvanredno ukida valjanost digitalnih certifikata, pošto je to jedan od elemenata PKI koji često izaziva najviše problema u konkretnim implementacijama, a ponekad čak i ograničava mogućnosti uporabe. Izvanredno ukidanje valjanosti digitalnih certifikata, odnosno njihovo povlačenje ili revokacija (eng. *revocation*) može se provoditi na nekoliko načina, od kojih svaki ima svoje prednosti i nedostatke koji će biti također opisani u dokumentu. Na kraju dokumenta biti će spomenuti i prijedlozi nekih rješenja koja bi mogla unaprijediti postojeće metode povlačenja digitalnih certifikata.

2. PKI infrastruktura

2.1. Digitalni certifikat

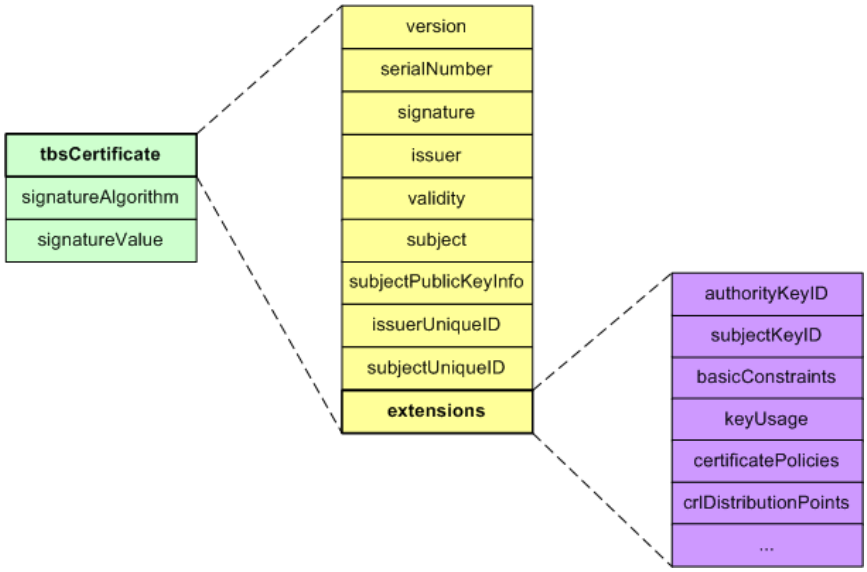
Koncept digitalnog certifikata omogućuje utvrđivanje povezanosti tajnog ključa kojeg posjeduje određeni entitet (osoba, aplikacija) i pripadajućeg mu javnog ključa. Digitalni certifikat predstavlja strukturu u kojoj je pohranjen identitet entiteta zajedno s javnim ključem, a cijela struktura digitalno je potpisana od treće strane koja predstavlja autoritet od povjerenja. Digitalni certifikat kao takav izdaje se na određeno vrijeme, a njegova valjanost može biti ukinuta i prije vremenskog roka na koji je digitalni certifikat inicijalno izdan.

Digitalni certifikat se može distribuirati korištenjem nesigurnih komunikacijskih kanala i pohranjivati na nesigurnim lokacijama, a svaki entitet može provjeriti njegovu valjanost provjerom digitalnog potpisa, uz uvjet da postoji direktno povjerenje ili lanac povjerenja do autoriteta koji je ovjerio odgovarajući digitalni certifikat.

Format digitalnog certifikata definira X.509 standard, odnosno njegova v3 inačica, koja je preuzeta i u RFC dokumentima 2459 i 3280 – "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

Digitalni certifikat enkodira se korištenjem ASN.1 (eng. *abstract syntax notation*) DER (eng. *distinguished encoding rules*) pravila.

Slika 1 grafički prikazuje `Certificate` strukturu koja definira X.509 v3 digitalni certifikat.



Slika 1: Grafički prikaz certificate strukture digitalnog certifikata

`Certificate` struktura predstavlja niz od 3 obvezna polja:

- `tbsCeritficate` predstavlja niz koji sadrži ime entiteta kojem se izdaje digitalni certifikat i ime izdavača (CA), pripadajući javni ključ entiteta, period valjanosti i druge informacije,
- `signatureAlgorithm` predstavlja polje koje sadrži identifikator algoritma koji se izdavač digitalnog certifikata koristio za njegovo digitalno potpisivanje (npr. RSA-MD2, RSA-MD5, RSA-SHA-1, DSA-SHA-1),
- `signatureValue` polje sadrži digitalni potpis izračunat nad ASN.1 DER enkodiranom `tbsCertificate` strukturom korištenjem algoritma čiji identifikator je naveden u `signatureAlgorithm` polju; digitalni potpis također je ASN.1 enkodiran kao niz bitova (eng. *bit string*).

`tbsCertificate` struktura sastoji se od informacija koje identificiraju entitet kojem se izdaje digitalni certifikat i izdavača digitalnog certifikata. Struktura mora sadržavati ime izdavača digitalnog

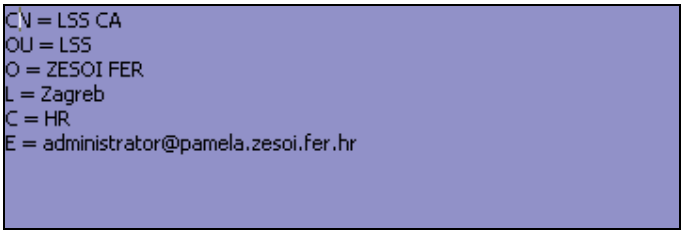
certifikata, ime entiteta i njegov javni ključ, period valjanosti, inačicu, te opcionalne ekstenzije. Opis polja `tbsCertificate` strukture slijedi u nastavku.

`Version` – označava inačicu enkodiranog certifikata. Ovo polje u načelu sadrži oznaku v3 inačice certifikata (u tim slučaju obvezno se koriste i ekstenzije), osim ako se ne koriste inačice v2 i v1.

`Serial number` – predstavlja cjelobrojnu vrijednost koju svaki CA dodjeljuje pojedinom digitalnom certifikatu. Ova vrijednost mora biti jedinstvena za svaki digitalni certifikat ovjeren i izdan od strane pojedinog CA.

`Signature` – ovo polje sadrži identifikator algoritma koji je CA koristio za digitalno potpisivanje certifikata. Vrijednost ovog polja mora biti identična vrijednosti u polju `signatureAlgorithm`.

`Issuer` – ovo polje identificira entitet koji je objavio i digitalno potpisao certifikat. Ime identiteta mora biti oblika X.501 `Name` i mora sadržavati X.500 DN (eng. *distinguished name*). X.501 Name struktura predstavlja niz RDN (eng. *relative distinguished name*) polja. Neka od uobičajenih RDN polja, osim DN su CN (eng. *common name*), OU (eng. *organisational unit*), O (eng. *organisation*), C (eng. *country*) i sl. (*Slika 2*).



Slika 2: Primjer issuer polja digitalnog certifikata

`Validity` – ovo polje predstavlja period valjanosti, odnosno vremenski interval u kojem CA garantira za održavanje (valjanost, povlačenje) digitalnog certifikata. Polje je definirano kao niz dva datuma; prvi predstavlja početak valjanosti digitalnog certifikata, a drugi označava datum prestanka valjanosti digitalnog certifikata (enkodirano kao `UTCTime` za datume do 2049. ili `GeneralizedTime` za datume u 2050. i kasnije).

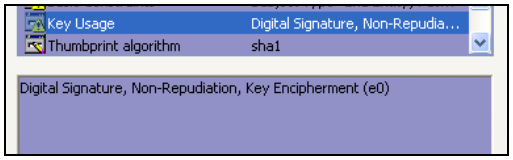
`Subject` – ovo polje identificira enitet koji je povezan s javnim ključem pohranjenim u digitalnom certifikatu (`subject public key info` polju). Ime (oblika X.501 `Name`) entiteta može biti sadržano u ovom isto kao i u `subjectAltName` ekstenziji. Ako je nositelj certifikata CA, ovo polje ne smije biti prazno.

`Subject public key info` – u ovom polju sadržan je javni ključ i identifikator kriptografskog algoritma (RSA, DSA, Diffie-Hellman) za koji se ključ koristi.

`Unique Identifier` (`subject`, `issuer`) – ova dva polja koriste se kod v2 i v3 digitalnih certifikata da bi se omogućilo ponovno izdavanje digitalnih certifikata ili izdavanje više digitalnih certifikata za razne namjene istom entitetu. Svaki certifikat izdan od strane pojedinog CA mora biti jedinstven.

`Extensions` – ovo polje koristi se kod v3 digitalnih certifikata i predstavlja niz od jedne ili više ekstenzija. Ekstenzije mogu biti kritične i nekritične. Ukoliko sustav ne prepoznaje neku od kritičnih ekstenzija digitalnog certifikata on ga mora odbaciti kao nevaljanog. Sljedeće ekstenzije moraju biti podržane od strane CA:

- `Key identifiers` (`authority`, `subject`) – jedinstveni identifikatori javnog ključa; obično se generiraju na temelju *hash* vrijednosti javnog ključa korištenog za digitalno potpisivanje certifikata (`authority`) ili navedenog u polju `subjectPublicKey` (`subject`),
- `Basic constraints` – ova ekstenzija identificira da li se radi o digitalnom certifikatu samog CA i koliko je duboka putanja certifikacije,
- `Key usage` () – ova ekstenzija definira svrhu za koju je digitalni certifikat namijenjen (npr. šifriranje, digitalno potpisivanje itd.),



Slika 3: Primjer korištenja key usage ekstenzije

– `Certificate policies` – ova ekstenzija sadrži niz od jedne ili više informacija o politici izdavanja digitalnih certifikata u OID (eng. *object identifier*) obliku.

Slika 4: Primjer certificate policies ekstenzije

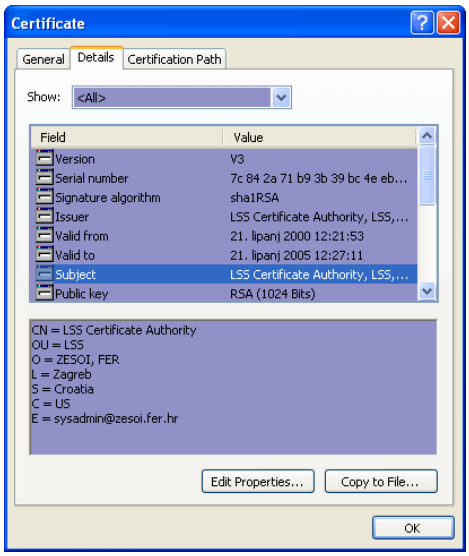
Osim ovih ekstenzija, klijentski sustavi moraju podržavati još i neke dodatne. Među njima je i ekstenzija `CRL Distribution Points` (*Slika 5*) koja služi za identifikaciju mjesta objave CRL liste. Ova ekstenzija nije obvezna, no njena uporaba je preporučena.

Slika 5: Primjer CRL distribution points ekstenzije

Slika 6 prikazuje osnovne informacije o digitalnom certifikatu (svrhu u koju je izdan digitalni certifikat, kome je izdan, te vremenski period njegove valjanosti).

Slika 6: Tipičan izgled digitalnog certifikata

Također, moguće je vidjeti i sve detalje iz digitalnog certifikata, odnosno njegova polja (Slika 7).



Slika 8: Detaljni pregled digitalnog certifikata

2.2. Ostali elementi PKI infrastrukture

Kompletna PKI infrastruktura (*Slika 9*) sastoji se od 6 osnovnih elemenata, iako se u nekim implementacijama pojavljuju i neki dodatni elementi.

Autoritet (eng. *authority*). Certifikacijski autoritet, odnosno CA (eng. *certificate authority*) predstavlja entitet od povjerenja u PKI infrastrukturi. Razina povjerenja ovisi o samom CA i može biti potpuna ili djelomična unutar PKI infrastrukture. CA izdaje X.509 digitalne certifikate koji povezuju pripadajući javni ključ s podacima u digitalnom certifikatu.

Proces izdavanja digitalnih certifikata. Proces izdavanja digitalnih certifikata može uključivati registracijski autoritet, RA (eng. r*egistration authority*, *request authority*) zadužen za registraciju i eventualnu verifikaciju identiteta korisnika. Iako je korištenje RA i verifikacija identiteta korisnika tradicionalno najprihvatljiviji način izdavanja digitalnih certifikata, X.509 standard dozvoljava korištenje anonimnih ili pseudonimskih digitalnih certifikata. Neovisno da li se koristi RA, CA je zadužen za izdavanje digitalnih certifikata koji se nakon toga mogu slobodno razmjenjivati ili objavljivati u odgovarajućim repozitorijima. Uobičajeno se kao repozitoriji certifikata koriste X.500, odnosno LDAP direktoriji, iako je moguće korištenje i alternativnih načina (npr. Web poslužitelja).

Istek valjanosti (terminacija) digitalnih certifikata. Istek valjanosti digitalnih certifikata događa se normalno, u skladu s vremenski periodom valjanosti digitalnog certifikata, koji je sastavni dio svakog digitalnog certifikata. Također, moguće je i ukidanje valjanosti digitalnih certifikata, odnosno njihovo povlačenje, ukoliko je na bilo koji način došlo do kompromitacije korisnika ili samog digitalnog certifikata. U ovom trenutku postoje dva načina povlačenja digitalnih certifikata:

a) objavom informacije o povlačenju na CRL (eng. *certificate revocation list*) revokacijskoj listi i
b) dobivanjem informacija o povučenim digitalnim certifikatima korištenjem OCSP (eng. *online certificate status protocol*) protokola.

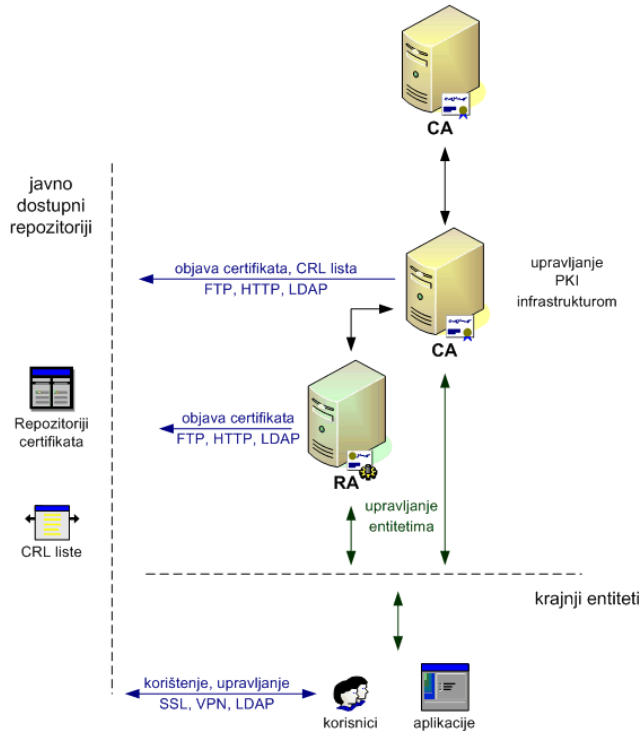
Obje ove metode imaju svoje prednosti i nedostatke koji će detaljno biti pojašnjeni u nastavku dokumenta.

Upravljanje točkama povjerenja (eng. *anchor management*). Standard, kroz proces registracije, definira načine dolaska do točaka povjerenja. Ovisno o implementaciji, klijent može imati više točaka povjerenja, odnosno može im vjerovati.

Upravljanje privatnim ključevima. Standard omogućava obnovu digitalnih certifikata prije njihovog isteka valjanosti. Također, postoji i mogućnost *backup*-a tajnih ključeva.

Provjera valjanosti (eng. *binding validation*). Klijenti za provjeru valjanosti koriste točke povjerenja, odnosno hijerarhiju digitalnih uvjerenja. Provjera valjanosti digitalnih certifikata izdanih

od strane drugih CA može se postići međusobnom certifikacijom (eng. *cross-certification*) CA ili dohvaćanjem digitalnih certifikata odgovarajućih CA prema potrebi.



Slika 9: PKI infrastruktura

3. CRL liste

Objava CRL lista je uobičajeni način za povlačenje digitalnih certifikata. Mehanizam CRL lista (X.509 v2) opisan je u RFC dokumentima 2459 i 3280 – "Internet X.509 Public Key Infrastructure Certificate and CRL Profile". Sama CRL lista je obična datoteka s nizom serijskih brojeva, jedinstvenih za svaki digitalni certifikat, koji označavaju povučene digitalne certifikate. CRL listu objavljuje odgovarajući CA u predefiniranim vremenskim intervalima. Većina komercijalnih PKI rješenja omogućava i ručnu objavu CRL lista.

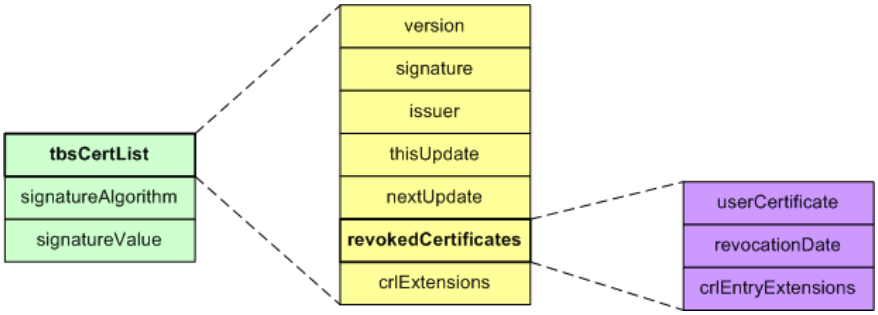
Tako objavljene CRL liste klijentske aplikacije trebale bi dohvaćati nekim od postojećih komunikacijskih protokola kao što su npr. FTP ili HTTP, ili iz LDAP direktorija CA koji je potpisao digitalni certifikat. U praksi se pokazuje da velik broj aplikacija uopće ne dohvaća CRL liste, niti radi provjeru da li je certifikat povučen.

PKI infrastruktura koja za povlačenje certifikata koristi CRL liste ima jedan veliki nedostatak, a to je da takva infrastruktura nije pogodna za transakcije u stvarnom vremenu, odnosno *online* transakcije, pošto period objavljivanja CRL lista od svakih nekoliko dana ili 24 sata ne zadovoljava sigurnosne zahtjeve. Čak i smanjenje tog perioda na 60 minuta ostavlja dovoljno velik vremenski prozor u kojem bi potencijalni zlonamjerni korisnik mogao kompromitirati npr. *online* bankarsku transakciju.

Drugi potencijalni nedostatak je veličina CRL datoteka, pošto neprestanom objavom novih serijskih brojeva povučenih digitalnih certifikata CRL datoteke mogu poprilično narasti. U praksi, obzirom da globalna PKI infrastruktura još nije zaživjela, a postojeće PKI implementacije su relativno male veličine, ovaj nedostatak još nije došao do izražaja.

S druge strane, dobra strana CRL lista jest mogućnost njihovog *offline* korištenja.

Slika 10 grafički prikazuje `CertificateList` strukturu CRL liste koja se u pravilu pohranjuju u ASN.1 DER enkodiranom obliku, a na temelju ASN.1 DER enkodinga izračunava se i digitalni potpis cijele CRL liste.



Slika 10: Grafički prikaz CertificateList strukture CRL liste

`CertificateList` struktura predstavlja niz od tri obvezna polja:

- `tbsCertList` predstavlja niz koji sadrži ime izdavača, datum izdavanja, datum izdavanja iduće CRL liste, popis povučenih certifikata i opcionalne CRL ekstenzije,
- `signatureAlgorithm` je polje koje sadrži identifikator algoritma koji je CA koristio za digitalno potpisivanje liste,
- `signatureValue` polje sadrži digitalni potpis izračunat nad ASN.1 DER enkodiranom `tbsCertList` strukturom korištenjem algoritma čiji je identifikator naveden u `signatureAlgorithm` polju; digitalni potpis također je ASN.1 enkodiran kao niz bitova.

`tbsCertList` se sastoji od niza obveznih i opcionalnih polja. Obvezna polja identificiraju izdavača CRL liste (CA), algoritam koji je korišten za digitalno potpisivanje CRL liste, datum i vrijeme objave CRL liste, te datum i vrijeme sljedeće objave CRL liste. Opcionalna polja odnose se na listu povučenih digitalnih certifikata i CRL ekstenzije. U nastavku slijedi popis svih polja.

`Version` (opcionalno) – opisuje inačicu CRL liste. Kada se koriste ekstenzije ovo polje je obvezno i mora specificirati vrijednost 2 (v2).

`Signature` – sadrži identifikator algoritma koji se koristi za digitalno potpisivanje CRL liste. Vrijednost ovog polja mora biti identična kao i u polju `signatureAlgorithm` u `CertificateList` strukturi.

`Issuer Name` – ovo polje identificira entitet koji je objavio i digitalno potpisao CRL listu. Ime identiteta mora biti oblika X.501 `Name` i mora sadržavati X.500 DN.

`This Update` – ovo polje označava datum i vrijeme objave trenutne CRL liste, a može biti enkodirano kao `UTCTime` ili `GeneralizedTime`.

`Next Update` – ovo polje označava datum i vrijeme objave nove CRL liste. Nova CRL lista može se objaviti i prije tog vremena, no nikako nakon toga.

`Revoked Certificates` – ovo polje sastoji se od popisa povučenih digitalnih certifikata koji su jednoznačno označeni svojim serijskim brojevima. Uz serijski broj povučenog certifikata mora također biti naznačen datum i vrijeme povlačenja. Ostale opcionalne informacije mogu biti naznačene u `crlEntryExtensions` polju. Npr. u tom polju može biti naveden i razlog povlačenja digitalnog certifikata. Razlozi za povlačenje mogu biti:

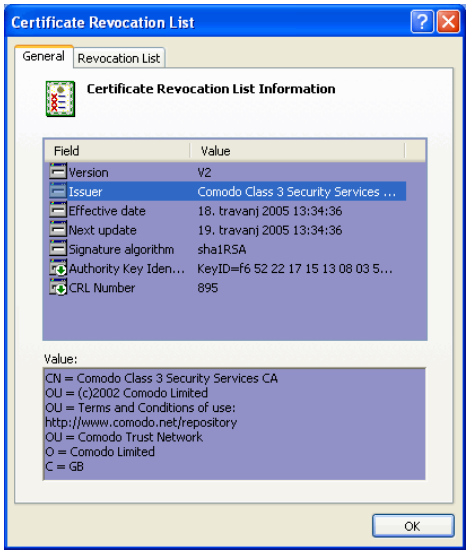
- nespecificirani (eng. *unspecified*),
- kompromitacija ključa (eng. *keycompromise*),
- kompromitacija CA (eng. *CA compromise*),
- promjena povezanosti (eng. *affiliation changed*),
- zamjena (eng. *superseded*),
- prestanak rada (eng. *cessation of operation*),
- privremeno povlačenje (eng. *certificate hold*) i
- brisanje s CRL liste (eng. *remove from CRL*), što može biti uzrokovano ponovnim vraćanjem valjanosti digitalnom certifikatu u slučaju privremenog povlačenja ili npr. prestanak valjanosti digitalnog certifikata (vremena u kojem je digitalni certifikat valjan).

`CRL Extensions` polje omogućava dodavanje dodatnih atributa CRL listama:

- `Authority Key Identifier` osigurava način identifikacije javnog ključa koji odgovara privatnom ključu kojim je digitalno potpisana CRL lista; ovo polje je važno u slučajevima kada određeni CA posjeduje više parova ključeva za digitalno potpisivanje,

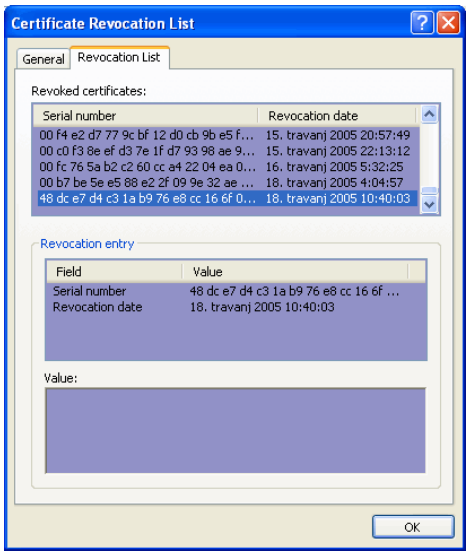
- `Issuer Alternative Name` omogućava dodatno identificiranje entiteta koji je objavio CRL listu (npr. e-mail adresa, DNS ime, IP adresa i sl.),
- `CRL Number` inkrementalno se povećava svakom novom objavom CRL liste te na taj način može pojednostavniti praćenje zastarijevanja pojedine CRL liste,
- `Delta CRL indicator` označava korištenje diferencijalne objave CRL lista (poglavlje 3.1).

Slika 11 prikazuje tipičnu CRL listu. Na slici se može uočiti X.501 imenovanje unutar `Issuer Name` polja, a također se može uočiti korištenje CRL ekstenzija `Issuer Alternative Name` i `CRL Number`.



Slika 11: Primjer CRL liste

CRL lista u primjeru također sadrži određeni broj povučenih digitalnih certifikata. Na slici (*Slika 12*) moguće je uočiti obvezna polja (serijski broj, datum i vrijeme povlačenja), dok se opcionalne informacije vezane uz povučene digitalne certifikate kod ove CRL liste ne koriste.



Slika 12: Popis povučenih digitalnih certifikata na CRL listi

3.1. Delta CRL

RFC 2459 opisuje također i delta CRL mehanizam. Pri tom se koristi diferencijalna metoda koja, općenito gledajući, smanjuje veličinu CRL lista koje klijentska aplikacija mora dohvaćati i skraćuje

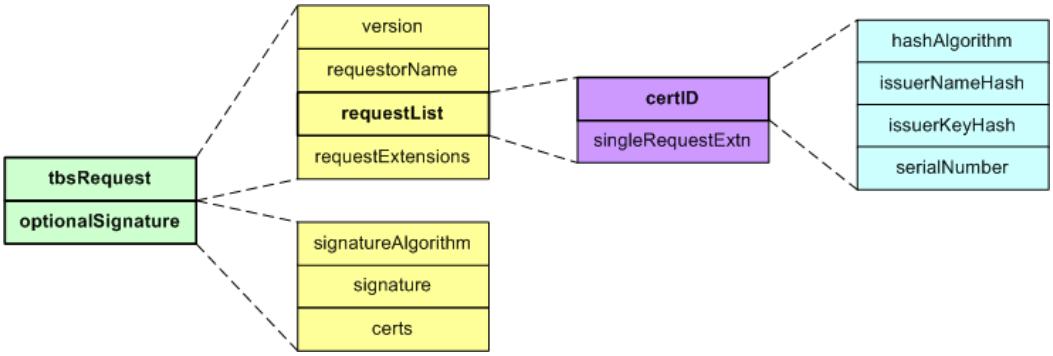
vrijeme potrebno za obradu kod aplikacija koje povučene digitalne certifikate pohranjuju lokalno, u obliku koji nije CRL lista.
Kod korištenja delta CRL, CA i dalje mora objavljivati kompletnu CRL listu. Delta CRL sadrži samo promjene između osnovne (eng. *base*) CRL i trenutne (eng. *current*) CRL koja se objavljuje istovremeno s delta CRL.
Delta CRL lista u `crlExtenstions` polju mora imati `deltaCRLIndicator` polje koje pak sadrži `BaseCRLNumber` polje u kojem je sadržana vrijednost osnovne CRL liste u odnosu na koju se objavljuje delta CRL. Kako je rečeno, uz delta CRL listu mora biti objavljena i trenutna kompletna CRL lista, s time da delta CRL i kompletna CRL lista moraju imati istu vrijednost polja `CRLNumber`.

4. OCSP

OCSP (eng. *online certificate status protocol*) je protokol koji je razvijen iz potrebe da se zaobiđu nedostaci vezani uz CRL liste. To se posebno odnosi na obavljanje transakcija u stvarnom vremenu, za koje PKI infrastruktura s CRL listama nije zadovoljavajuće rješenje.
OCSP u PKI infrastrukturu dodaje još jedan entitet – VA (eng. *validation authority*), odnosno tzv. OCSP responder koji je odgovoran za provjeru valjanosti digitalnog certifikata.
Pritom CA mora slati revokacijske podatke OCSP responderu. Slanje revokacijskih podataka može biti direktno ili se mogu koristiti CRL liste (moguće je *push* i *pull* slanje CRL lista). U bilo kojem slučaju, OCSP responder mora vjerovati CA-u koji objavljuje revokacijske podatke.
Isto tako klijent ili aplikacija moraju vjerovati OCSP responderu. U ovom slučaju klijent (aplikacija) ne provjerava valjanost certifikata direktnom provjerom CRL lista, već šalje upit OCSP responderu. OCSP responder na upit odgovara s jednim od tri moguća stanja: "dobar" (eng. *good*), "povučen" (eng. *revoked*) ili "nepoznat" (eng. *unknown*). Valja istaknuti da odgovor "dobar" ne znači da je digitalni certifikat valjan, već samo da nije bio povučen u trenutku slanja upita.
Isto kao i kod CRL lista, kod OCSP-a postoje određeni nedostaci. Kao prvo, korištenjem OCSP-a gubi se mogućnost *offline* provjere valjanosti digitalnih certifikata. Isto tako, OCSP responderi potencijalno postaju uska grla u komunikaciji. Konačno, iako zamišljen da osigurava provjeru valjanosti digitalnih certifikata u stvarnom vremenu, u praksi OCSP nije idealan, pošto je i dalje osjetljiv na kašnjenje između trenutka povlačenja digitalnog certifikata i objave te povlačenja. To nije implementacijski nedostatak OCSP-a, ali bez obzira na to problem postoji.

4.1. OSCP zahtjev

Slika 13 prikazuje sadržaj `OCSPRequest` zahtjeva. OCSP zahtjev formatiran je korištenjem ASN.1 notacije, a sam oblik zahtjeva ovisi o komunikacijskom protokolu koji se koristi (HTTP, LDAP, SMTP itd.).



Slika 13: Sadržaj OCSP zahtjeva

`OCSPRequest` struktura sastoji se od dva polja:
- `tbsRequest` – sadrži informacije o inačici protokola i zahtjev(e) za verifikacijom digitalnog certifikata i
- `optionalSignature` (opcionalno) – zadrži opcionalni digitalni potpis zahtjeva.

`tbsRequest` struktura sastoji se od sljedećih polja:
- `version` – označava inačicu OCSP protokola (v1),
- `requestorName` (opcionalno) – ime entiteta koji podnosi zahtjev, ovo polje je obvezno samo ako je OCSP zahtjev digitalno potpisan,
- `requestList` –sadrži popis zahtjeva za verifikacijom digitalnih certifikata, a sastoji se od sljedećih polja:
    - `CertID` – polje koje se sastoji od četiri polja koja jednoznačno određuju digitalni certifikat:
        - `hashAlgorithm` – sadrži identifikator algoritma koji se koristi za računanje *hash* vrijednosti u zahtjevu,
        - `issuerNameHash` – sadrži *hash* vrijednost ASN.1 DER enkodiranog `issuerName` polja digitalnog certifikata koji se verificira,
        - `issuerKeyHash` – sadrži *hash* vrijednost ASN.1 DER enkodiranog javnog ključa izdavača digitalnog certifikata koji se verificira,
        - `serialNumber` – sadrži jedinstveni serijski broj digitalnog certifikata,
    - `singleRequestExtensions` (opcionalno) – sadrži opcionalne ekstenzije vezane uz pojedini zahtjev
- `requestExtensions` (opcionalno) – sadrži opcionalne ekstenzije

Opcionalna `optionalSignature` struktura sastoji se od sljedećih polja:
- `signatureAlgorithm` – identifikator algoritma koji se koristi za digitalni potpis,
- `signature` – digitalni potpis ASN1 enkodirane `tbsRequest` strukture OCSP zahtjeva,
- `certs` (opcionalno) – sadrži popis certifikata koji OCSP responderu mogu omogućiti provjeru digitalnog potpisa entiteta koji je poslao zahtjev.

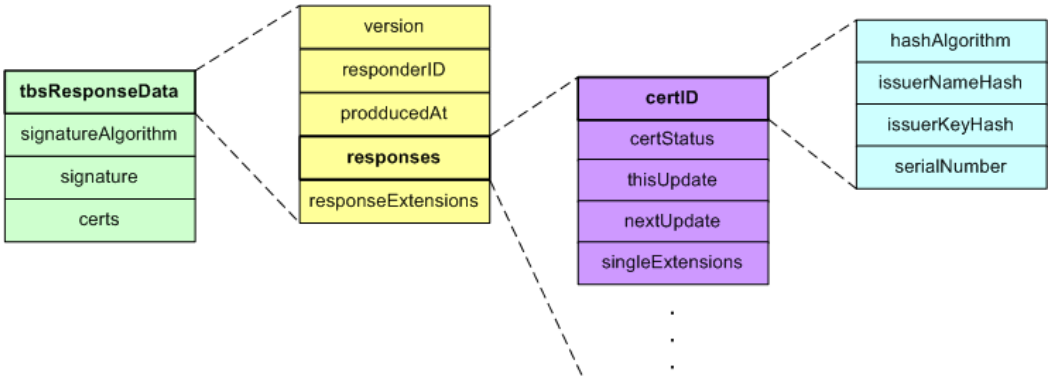
4.2. OCSP odgovor

Isto kao i kod OCSP zahtjeva, oblik OCSP odgovora ovisi o komunikacijskom protokolu koji se koristi, a sam OCSP zahtjev oblikovan je u ASN.1 enkodiranu strukturu.
OCSPResponse struktura sastoji se od dva osnovna polja:
- `responseStatus` i
- `responseBytes`.

`responseStatus` polje označava status OCSP odgovora, a ukoliko je status pogreška, `responseBytes` polje se ne postavlja. `responseStatus` može poprimiti sljedeće vrijednosti:
- *successful* – odgovor je uspješan i postavljeno je `responseBytes` polje,
- *malformedRequest* – pogrešno oblikovan zahtjev,
- *internalError* – interna pogreška kod izdavača,
- *tryLater* – zahtjev je potrebno ponoviti kasnije,
- *sigRequired* – OCSP responder zahtijeva digitalni potpis OCSP zahtjeva,
- *unauthorized* – OCSP zahtjev je neovlašten.

Ukoliko je postavljeno `responseBytes` polje je struktura koja se sastoji od polja
- `responseType` i
- `response`.

Obični (eng. *basic*) OCSP responder će generirati OCSP odgovor tipa `BasicOCSPResponse`. *Slika 14* prikazuje sadržaj `BasicOCSPResponse` strukture.



Slika 14: Sadržaj BasicOCSPResponse strukture

Struktura sastoji se od sljedećih polja:

- `tbsResponseData` – struktura koja sadrži oznaku OCSP respondera, inačicu protokola, vrijeme odgovora, OCSP odgovore i eventualne ekstenzije.
- `signatureAlgorithm` – identifikator algoritma koji se koristi za digitalni potpis,
- `signature` – digitalni potpis ASN1 enkodirane `tbsRequest` strukture OCSP zahtjeva,
- `certs` (opcionalno) – sadrži popis certifikata koji OCSP responderu mogu omogućiti provjeru digitalnog potpisa entiteta koji je poslao zahtjev (ključ OCSP respondera ne mora biti identičan ključu CA koji je izdao digitalni certifikat, no u tom slučaju CA mora dodijeliti odgovarajući digitalni certifikat OCSP responderu, a `extendedKeyUsage` polje tog certifikata mora sadržavati `OCSPsigning` funkcionalnost).

tbsResponseData struktura sastoji se od sljedećih polja:

- `version` – inačica protokola (v1),
- `responderID` – identifikator respondera, može biti ime ili SHA-1 *hash* vrijednost javnog ključa respondera,
- `producedAt` – datum i vrijeme generiranja OCSP odgovora,
- `responses` – niz OCSP odgovora,
- `responseExtensions` (opcionalno).

Struktura `responses` sastoji se od niza pojedinačnih OCSP odgovora definiranih `Single response` strukturom na sljedeći način:

- `certID` – struktura koja na jednoznačan način označava digitalni certifikat, oblik strukutre je identičan kao i kod OCSP zahtjeva,
- `certStatus` – označava status digitalnog certifikata; status može biti dobar (*good*), povučen (*revoked*) ili nepoznat (*unknown*).
- `thisUpdate` – označava vrijeme u koje je digitalni certifikat imao određeni status (odgovara polju `thisUpdate` kod CRL lista); ukoliko je ovo vrijeme kasnije nego kod entiteta koji je tražio verifikaciju digitalnog certifikata OCSP odgovor se može smatrati nepouzdanim,
- `nextUpdate` (opcionalno) – identično `nextUpdate` polju kod CRL lista; ukoliko je ovo vrijeme ranije nego kod entiteta koji je tražio verifikaciju digitalnog certifikata OCSP odgovor se može smatrati nepouzdanim,
- `singleExtensions` (opcionalno).

Valja istaknuti da aplikacije, odnosno sustavi koji koriste OCSP verifikaciju digitalnih certifikata moraju podržavati provjeru `extendedKeyUsage` polja certifikata OCSP respondera, te odbaciti OCSP odgovor ukoliko digitalni certifikat kojim je potpisan on ne ispunjava barem jedan od sljedećih odgovora:

- digitalni certifikat je certifikat CA koji je objavio certifikat čija verifikacija se traži u zahtjevu,
- sadrži vrijednost `OCSPsigning` u `extendedKeyUsage` polju i izdan je od strane CA koji je objavio certifikat čija verifikacija se traži u zahtjevu,
- odgovara lokalnoj konfiguraciji OCSP autoriteta za certifikat čija verifikacija se traži u zahtjevu.

Također, CA treba specificirati na koji način OCSP klijent može provjeriti status digitalnog certifikata OCSP respondera što može napraviti npr. definiranjem CRL distribucijskih točaka u certifikatu OCSP

respondera. Također, CA može postavljanjem odgovarajuće ekstenzije u certifikat OCSP-a klijentu sugerirati da je certifikat valjan sve do isteka njegove vremenske valjanosti (nije sigurna metoda). Ukoliko CA ne specificira način provjere digitalnog certifikata OCSP respondera, OCSP klijent može prihvatiti ili odbaciti taj certifikat ovisno o lokalnoj sigurnosnoj politici.

5. Druge metode povlačenja digitalnih certifikata

5.1. SCVP

SCVP (eng. *simple certificate verification protocol*) protokol je još uvijek na razini prijedloga, a temelji se na uspostavi infrastrukture koja u sebi sadrži OCSP i druge servise. Protokol je zamišljen u obliku zahtjeva i odgovora, a primarni transportni protokol trebao bi biti HTTP.
Za razliku od OCSP-a, kod kojeg OCSP responder odgovara samo da li je određeni certifikat u tom trenutku bio povučen ili ne, SCVP poslužitelj kojem klijent vjeruje radio bi kompletnu provjeru digitalnog certifikata za klijenta.

5.2. Pohrana CRL u DNS sustavu

RFC dokument 2538 "Storing Certificates in the Domain Name System (DNS)" specificira uporabu DNS sustava za pohranu digitalnih certifikata i CRL lista. Da bi se DNS sustav mogao koristiti za tu namjenu potrebno je definirati odgovarajuće DNS RR (eng. *resource records*) zapise.

6. Zaključak

Postojeće metode povlačenja digitalnih certifikata imaju određene nedostatke. Postoje određeni prijedlozi protokola i metoda koje bi ispravile te nedostatke, no zasad nemaju realnu vrijednost.
Nedostaci postojećih metoda, CRL lista, a u manjoj mjeri i OCSP protokola u praksi ipak nisu toliko značajni, obzirom da je korištenje PKI infrastrukture uglavnom lokalnog karaktera. Ukoliko jednog dana ipak zaživi globalna PKI infrastruktura, ti nedostaci će postati ozbiljan problem koji će svakako trebati riješiti. No obzirom da današnji trendovi, suprotno predviđanjima iz 90-ih godina prošlog stoljeća, ipak ne sugeriraju revolucionarni uspon globalne PKI infrastrukture, postojeće metode povlačenja digitalnih certifikata se u idućim godinama mogu smatrati zadovoljavajućima.

7. Reference

[1] RFC 2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, http://www.ietf.org/rfc/rfc2459.txt,
[2] RFC 3280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, http://www.ietf.org/rfc/rfc3280.txt,
[3] RFC 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, http://www.ietf.org/rfc/rfc2560.txt,
[4] RFC 2538, Storing Certificates in the Domain Name System (DNS), http://www.ietf.org/rfc/rfc2538,
[5] Certificate Revocation: When Not To Trust,
http://networkcomputing.com/1112/1112ws1.html?ls=NCJS_1112bt,
[6] The Certificate Revocation Framework, O. Kessler, Open Systems AG, http://www.open.ch,
[7] PKI: Ten Years Later, Carlisle Adams and Mike Just,