

Press release

Certification Validation

09/2001

Certificate Validation

To use up-to-date methods of asymmetric cryptography and PKI-technologies users must be provided with a secret key and a public key, which is - in most cases - contained within a certificate issued by some trustcenter. With these methods one can establish authentication and confidentiality and with a little bit of additional effort even authorization. Today these methods are used in widespread fields. Authentication of electronically distributed software and websites is secured using digital signatures, and even more complex E-Business is powered by these technologies (for example within the identrus system). More and more E-Mails are signed and encrypted using asymmetric cryptography like nearly every electronic transaction in whatever system you look at. Asymmetric cryptography is regarded as mathematically secure and - if used properly - as technically secure.

But what about more organisational risks? A private key may be lost or - even worse - stolen. A person may choose to leave the organisation that provides trustcenter services, or even worse - sneaked into such an organization. There are a lot of possibilities of disturbing the trust in asymmetric cryptography, PKI and trustcenters - other than just plain mathematical or technical issues. In March 2001 some unknown person received two Verisign-certificates for the name of "Microsoft Corp." by using a fake name. These certificates can be used to sign software that is then highly trusted in 90% of all PC's in the world. [TODO:other example].

If someone stole a private key and you send a confidential message to the person, whose private key was stolen, this message is not confidential anymore. Meaning, that before you encrypt a message using the recipients certificate, you should check if this certificate is valid. On the other hand, if you receive a digitally signed message from a person whose private key was stolen, the authentication of the sender of this message is not secured. Meaning, that before you trust the authentication of a message from anybody using his certificate, you should check, if this certificate is valid. As the examples given above demonstrate, the risk of trusting invalid certificates cannot be left without a solution. This means before every cryptographic operation the validity of the all used certificates has to be validated.

Certificate Revocation Lists

As this problem is well known for a long time, the concept of Certificate Revocation Lists (CRL) was proposed. This list is issued (and digitally signed) by a trustcenter and contains all revoked (= invalid) certificates. As this list is subject to change, newer lists get issued from time to time. To allow caching of a CRL at the users location, every CRL contains information of its period of validity. That means a CRL can be issued every 5 minutes and have a period of validity of somewhat like an hour. As one can imagine this caching is directly linked to the risk that a PKI takes - the longer a client is allowed to use an old CRL, the higher is the risk of using a revoked certificate.

...

Further information:

SyTrust S.A.

12, route du vin
6794 Grevenmacher
Luxembourg
Fon: +352.267469.0
Fax: +352.267469.20

Ludwigstrasse 55
85399 Hallbergmoos
Germany
Fon: +49(0) 811.959440-0
Fax: +49(0) 811.9594-420

info@sytrust.com

www.sytrust.com

To allow clients access to the most current CRL most trustcenters make them available using LDAP or HTTP. But this distribution imposes the problem of network traffic. For example the CRL for Class 3 Verisign international server certificates is around 0,5 MB in size. So every client trusting a Verisign server certificate should download this CRL. Given that more than 500.000 websites use VeriSign certificates, this means that every user of one of these sites has to download this CRL. This is not only a significant delay in accessing these websites for the user but also generates a VERY high network traffic. The solution to this maybe to allow caching of these CRLs for a longer time, but as mentioned before this imposes a higher risk of using revoked certificates.

There are a few proposals to repair these problems within the idea of a CRL, for example the usage of delta CRLs containing only the different list entries in comparison to the last CRL. But none of these proposals are an elegant solution to repair the problems described above.

Online Certificate Status Check

To solve the problems of Certificate Validation in an efficient manner the PKIX working group of the IETF proposed a Online Certificate Status Protocol (OCSP) in June 1999 (RFC 2560). This protocol allows a client to request information regarding the validity of one or more certificates which will be answered (and digitally signed) by a so called responder. This method to do certificate validation implicates two major improvements. The first and foremost is an efficient risk management as an OCSP-responder is able to provide timely status information to the user. The second improvement of the protocol lesson is the network traffic signficancy, as users do not receive a huge list, needing only a few entries but only get the information they need. To ensure a maximum compatibility with the various networks, HTTP is used to transport the request and the response between a client and the OCSP-responder.

Most e-Commerce systems developed a lot of interest in this technology. This is not only because OCSP provides real-time validation and therefore allows them to setup an effective risk management, but also because of billing issues. To receive a timely return of investment these e-Commerce systems have to bill for their trustcenter-services. This can be done the old way by selling the certificates but these costs hit the users of the systems, meaning it hits the "buyers" (speak: the end-users) of a traditional e-Commerce system. To bill the "sellers" of such a system the number of transactions done by a given merchant has to be counted. The only communication that takes place between seller and trustcenter for every transaction is the OCSP-request. This brought up the idea of billing the "seller" for every OCSP-Request that is made.

With interest a lot requests for additional functionality came up. Protocols such as "Simple Certificate Validation Protocol" SCVP and OCSP Version 2 are discussed within the standardization bodies implementing the same idea of an online certificate validation.

Using OCSP

Validation of a certain certificate brings up the question to what responder the request should be directed to. There are two different possibilities. A company may want to have a central OCSP-responder for all certificates from different trustcenter's. With this responder the company can enforce a central security policy, what trustcenter should be confided in. The second possibility is to use a certain extension in the certificate, which contains the information which OCSP-responder know about this certificate (AIA = Authority Information Access).

As most programs do not support AIA extensions, the problem of automatic search for the correct OCSP-Responders is more difficult than it seems to be. To solve this problem a website named "www.openvalidation.org" was set up. This website not only contains the addresses of most OCSP-responders, but also operates an OCSP-responder itself. Every OCSP-request sent to "ocsp.openvalidation.org" will be directed to the correct OCSP-responder transparently. This site also features a lot of background information regarding online validation.

Finding software which supports OCSP is the more difficult task. As the protocol is rather new, the process of implementing it into client software is not completed yet. Some clients feature OCSP functionality right now, nearly all have it on their roadmap. Most crypto-toolkits can do online certificate validation using OCSP and the opensource community integrated a client into the newest version of their crypto library "OpenSSL".

More than Certificate Validation?

Summarizing one can say, an OCSP-Responder delivers an answer to the question "Is this specific certificate revoked or not?". But most users have a more complicated problem. Their question is more "Can I trust this certificate?".

In a normal trustcenter structure a user only trusts a few so called "root-certificates" of certain trustcenters. With this all certificates are automatically issued by a trusted root. And all other certificates issued by one of these certificates, too. That means, to trust a certificate, a user not only has to check the validity of this certificate, but also has to check, if it is possible to construct a chain of certificates and issuers up to a trusted root certificate. This process is called "certificate chain detection" or "certificate path discovery". Additionally each certificate in this chain has to be validated. The before mentioned question of "Can I trust this certificate?" boils down to "Can I find a chain of Certificates?" and "Can I positively validate every certificate in this chain?".

Therefore two new OCSP-add-ons are currently discussed within the community: "delegated path discovery" tries to answer exactly the first question. With a certain OCSP-extension the responder shall additionally deliver a certificate chain up to a trusted root. "Delegated path validation" tries to answer both questions, meaning that every certificate within the chain is validated as well.

Also the question "Can I trust this data?" maybe answered by some responder in the future. That would imply the above mentioned validation processes but may also implicate the digital equivalent of some notary services. More than that, some e-Commerce systems may come up with the idea of selling additional guarantees with an OCSP-request like payment guarantees or transport insurances.

Products and technology

Given the points mentioned above a some properties are crucial for an OCSP-Responder:

- ✓ high availability and stability: if the responder does not answer, no trusted cryptographic operation can take place. Support of hardware high availability, for the best case built-in software high availability and a robust programming and operating system platform are an absolute requirement.
- ✓ performance: every cryptographic operation has to wait for the OCSP-Responder to answer. Scalability, load sharing support, support of hardware crypto-modules (HSM's) and fast response times are the second import issue when rolling out an OCSP-Responder

Validation confidential is one of them. Another one is the support of Chaining, Proxying and Hiding:

- ✓ Chaining means sending an OCSP-request to another one as it was sent from the user. The other responder receives an exact copy of the users request.
- ✓ Proxying constructs a new OCSP-request with the data of the user's request and sends it. The other responder receives a new request origination from the responder itself. The user request becomes "anonymized".
- ✓ Hiding does not send back the response as sent by the other responder unchanged, but constructs and signs its own new response for the user. Therefore the other responder is hidden for the user.

As shown before, this technology is moving forward fast. So extensibility, the possibility to customize a responder to the specific needs of a PKI and the development speed in picking up new standards and trends should be an argument, too.

There are a bunch of OCSP-Responders on the market right now, having rather different architectures. Some are integrated into crypto suites and other programs like directories, some are coming with their own webserver others make use of existing webserver technology. For example SyTrust's CertControl is implemented using the Apache webserver and makes use of the stability, speed, extensibility and portability of the worlds most used webserver. As OCSP-Responders will evolve into one of the key-components of every PKI, a careful choice should be made.

Summary

The often neglected task of certificate validation is one of the most complex, but most crucial processes in the PKI and e-Commerce world. Meanwhile it shows, the old CRL concept is not the right solution for this problem. Online status validation protocols like OCSP address the need of an e-commerce world a great deal better. Choosing the right product and customizing it to your needs improves risk managements and therefore pays off fast.