E-LOCK

Certificate Validation

Table of Contents

1 INTRODUCTION

Digital Certificates help in identifying and establishing the credentials of individuals participating in on-line communication or transactions. Individuals are proofed and then issued certificates that can be used in online transactions. These certificates vouch for the owner's identity and/or association with a particular organization and endorse his/her authority to participate in specific transactions. Certificates are issued and managed by trusted third parties known as Certificate Authorities (CAs) or can be issued and managed internally within an organization. Certificate Authorities are also responsible for checking and reporting on the status of revoked or cancelled certificates. At the time of issue, certificates are given a fixed life span and expire at the end of this set period.

1.1 NEED FOR REVOCATION

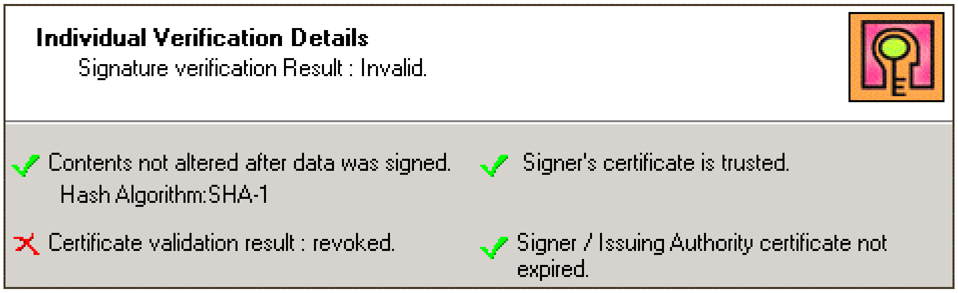
There are several reasons for why a certificate might need to be revoked much before the due expiry date such as in the case of a change in job status, termination of employment or suspected private key compromise. For instance when individuals in positions of authority change organizations or for some reason are no longer associated with a particular organization, their authority and subsequently their digital certificates, which represent this authority need to be revoked.

Under certain circumstances, a user may personally initiate revocation of his/her own certificate (for eg due to suspected compromise of the corresponding private key). Timely certificate revocation ensures that the certificate will not be used either accidentally or deliberately for unauthorized participation in transactions.

1.2 DIGITAL CERTIFICATES AND E-LOCK PROSIGNER

E-Lock ProSigner allows users to use digital certificates to sign files of any format. ProSigner integrates into MS Word, Excel, Adobe Acrobat and Windows Explorer. You can use any x.509 certificate issued by a Certificate Authority such as VeriSign or a certificate issued by your organization (through a PKI Server).

ProSigner not only allows you to sign using certificates, but provides value additions to the use of these certificates. It enables users to check to the validity of certificates before they are used to sign, and also enables recipients of signed documents to check the status of the certificate that the document was signed with. The signing certificate (i.e. the certificate that vouches for the identity of the person that signs the document) is one of the most important variables in the signing process as it is the application of a certificate to data that creates the digital signature; it is therefore very essential to check the validity of the certificate, as an invalid certificate would amount to an invalid signature or transaction.



Individual Verification Details
Signature verification Result : Invalid.

✓ Contents not altered after data was signed.
Hash Algorithm:SHA-1

✓ Signer's certificate is trusted.

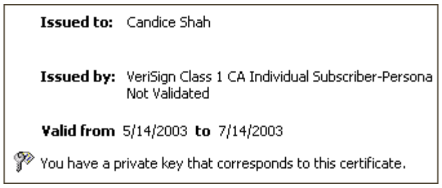
✗ Certificate validation result : revoked.

✓ Signer / Issuing Authority certificate not expired.

2 VALIDATION

Certificate validation fundamentally deals with assessing the legitimacy of a given certificate. It includes:

- Verification of the certificate's integrity including the revocation status
- Assurance that the certificate was issued by a trusted CA
- The validity period of the certificate is appropriate (that is, the time of use is between the Not Before and Not After dates/times as specified within the certificate)
- The certificate is being used in compliance with any intended usage and/or policy restrictions



Issued to: Candice Shah

Issued by: VeriSign Class 1 CA Individual Subscriber-Persona Not Validated

Valid from 5/14/2003 **to** 7/14/2003

You have a private key that corresponds to this certificate.

3 REVOCATION CHECKING

Certificate Revocation checking can be done through the following mechanisms:

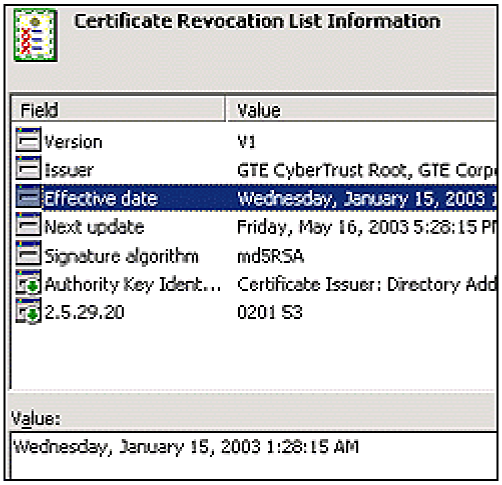
1. Certificate Revocation Lists
2. Online Certificate Status Protocol
3. CAM

ProSigner supports all these validation mechanisms.

4 CERTIFICATE REVOCATION LISTS - CRLS

Certificate Authorities publish certificate revocation lists (CRLs), which as the name suggests are lists of revoked or cancelled certificates. These CRLs are published at regular intervals and contain periodic updates to the status of certificates.

Through certificate revocation, the CA notifies users that a particular certificate is no longer valid. Whenever a user or an application attempts to validate a certificate, it checks the certificate revocation list for certificate information and status.



Certificate Revocation List Information

Field	Value
Version	V1
Issuer	GTE CyberTrust Root, GTE Corp
Effective date	Wednesday, January 15, 2003 1
Next update	Friday, May 16, 2003 5:28:15 P
Signature algorithm	md5RSA
Authority Key Ident...	Certificate Issuer: Directory Add
2.5.29.20	0201 53

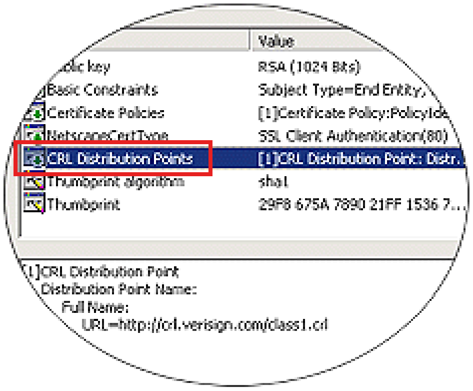
Value:

Wednesday, January 15, 2003 1:28:15 AM

4.1 CRL DISTRIBUTION POINTS

Certificates optionally contain a field called the “CRL Distribution Point” with information on the location of the CRL on the CA or the Directory where the CA publishes the certificates and CRLs. When an attempt is made to validate a certificate, this “CRL Distribution Point” field is referenced to locate the CRL. There are three methods by which ProSigner refers to CRLs for revocation checking:

- If a CRL is already installed with help of the “Install CRL” utility available with ProSigner
- If the signed document has a policy attached, which contains a validation rule that provides the URL to the CRL file.
- If the CRLDP is stamped on the certificate being verified with a valid URL pointing to the CRL file



	Value
blic key	RSA (1024 Bits)
Basic Constraints	Subject Type=End Entity,
Certificate Policies	[1]Certificate Policy:PolicyIde
NetscapeCertType	SSL Client Authentication(80)
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Thumbprint algorithm	sha1
Thumbprint	29F8 675A 7890 21FF 1536 7...

```
[1]CRL Distribution Point
  Distribution Point Name:
    Full Name:
      URL=http://crl.verisign.com/class1.crl
```

4.2 MULTIPLE CRLDP

Sometimes Certificate issuers stamp the CRLDP with multiple CRL distribution points. This is to overcome any difficulty in connecting to a particular URL. ProSigner sequentially checks all CRLDPs. If the first connection fails, it falls back on the next CRLDP and so on.

5 OCSP (ONLINE CERTIFICATE STATUS PROTOCOL)

Certificate Authorities typically issue a large number of certificates and might also revoke certificates in large numbers over a period of time. Correspondingly, the size of the CRL file will also increase, and it might in due course, grow to an unacceptable size. In such a situation, the retrieval of a large CRL will take a considerable amount of time and will in effect, delay the validation process itself.

The other issue at hand is that of high-value transactions. Business processes that are primarily transaction-oriented require instant checking of a certificate's status. Any lapse that might occur in case of a not sufficiently fresh CRL, which fails to reflect the most current status of a certificate, would directly impact business trust and might result in loss of revenue and other such complications.

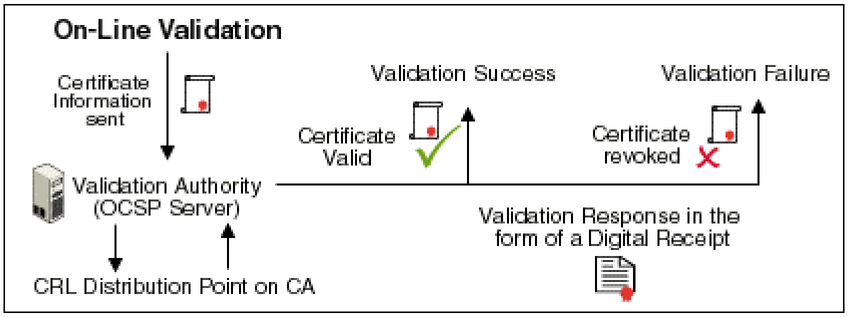
Such delays and hindrances would be inherent in all CRL based mechanisms. To counter this, the Internet Engineering Task Force developed the Online Certificate Status Protocol (OCSP) standard. Through OCSP, any user or application can establish a connection with an OCSP Responder to obtain a current online report of a certificate's status. An OCSP Responder is a server application, which maintains and stores up-to-date certificate revocation information and can have connections to several Certificate Issuing PKI Servers.

5.1 OCSP RESPONDER

Whenever an application wishes to obtain the status of a certificate, it makes a request to the OCSP Responder - which in turn replies whether a certificate is valid, revoked or of unknown status. All OCSP responses are digitally signed either by the CA who issued certificate in question, or by a responder designated by the CA. A Certificate Issuer explicitly delegates OCSP signing authority by issuing a certificate containing a unique value for extended Key Usage in the OCSP signer's certificate. This specially marked certificate issued by the CA to the responder is indicative of the responder's authority to issue responses for that CA.

Since an authorized OCSP responder provides revocation status information for one or more CAs, it is important that OCSP clients – applications that make requests for certificate status information - trust the OCSP responder. This may be one in one the following ways

- A CA may specify that an OCSP Client trust a responder for the lifetime of the responder's certificate.
- Alternately, the CA can specify how a responder's certificate may be checked for revocation. This can be specified in the CRL Distribution Point.


On-Line Validation
Certificate Information sent
Validation Success
Validation Failure
Certificate Valid
Certificate revoked
Validation Authority (OCSP Server)
Validation Response in the form of a Digital Receipt
CRL Distribution Point on CA

5.2 OCSP – BUSINESS PERSPECTIVE

Through OCSP, immediate notification of a certificate's revocation is available to users. It provides e-businesses with a faster and more reliable method of revocation checking than the traditional method of downloading and processing CRLs. It affords business transactions a higher level of trust and eliminates the potential for security breaches and uninformed business decisions. Another advantage is that through OCSP a response is generated and sent to the application. Applications can then opt to save this response and attach it to the document or the transaction being validated.

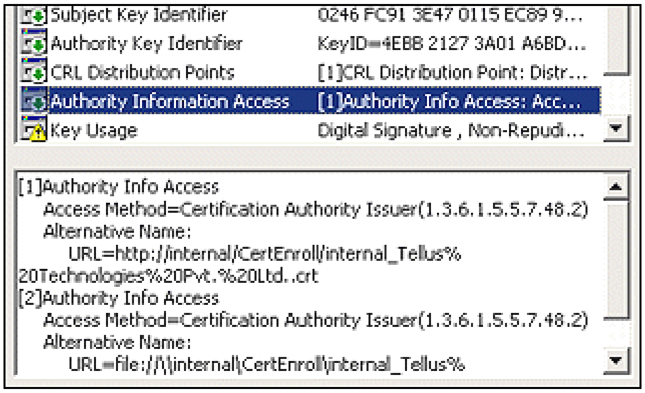
Using the Online Certificate Status Protocol, an organization can link multiple responders. If a certificate status request is made to a responder, who does not have the information, the responder can obtain the information from another responder. Creating such a network of responders provides users and trading partners a high degree of flexibility to validate certificates and conduct business over the net.

5.3 APPLICATION SUPPORT FOR OCSP

Digital Signature products need to support OCSP to validate certificates; applications also need the location of the Validation Authority to query the certificate validity. This can be achieved by one of two methods.

The first method is for the application to support some sort of policy, which will allow for defining the path (URL or LDAP) for the Validation Authority.

The second method is for a CA to define the path (URL only) in the AIA (Authority Information Access) extension within the certificate. The applications then look at this path and perform their query.



Subject Key Identifier	0246 FC91 3E47 0115 EC89 9...
Authority Key Identifier	KeyID=4EBB 2127 3A01 A6BD...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Key Usage	Digital Signature , Non-Repudi...

```
[1]Authority Info Access
     Access Method=Certification Authority Issuer(1.3.6.1.5.5.7.48.2)
     Alternative Name:
          URL=http://internal/CertEnroll/internal_Tellus%
20Technologies%20Pvt.%20Ltd..crt
[2]Authority Info Access
     Access Method=Certification Authority Issuer(1.3.6.1.5.5.7.48.2)
     Alternative Name:
          URL=file://\\internal\CertEnroll\internal_Tellus%
```

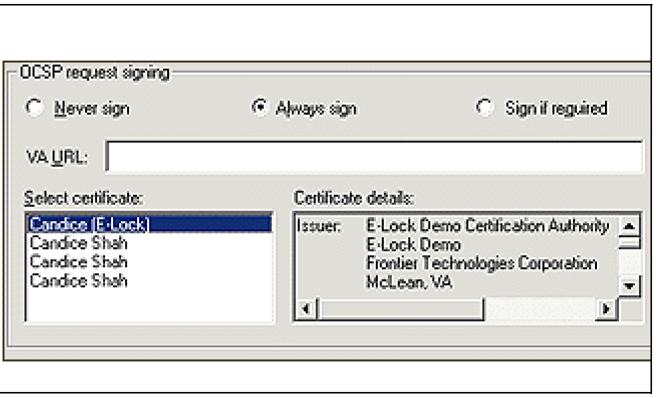
There are two methods by which ProSigner performs OCSP validation:

- If the certificate being verified is stamped with a valid URL to the OCSP responder
- If the document being verified has a policy attached which explicitly refers to a valid OCSP responder.

5.4 SIGNED OCSP REQUESTS

Recently, Validation Authorities have started responding to only signed requests for OCSP validation. The reason for this could be to ensure that only valid requests to the OCSP responder are entertained. The other reason is to track those performing validation and charge them for the service.

ProSigner allows for sending signed requests to the OCSP responder. From the configuration manager you define whether to send signed or unsigned requests and accordingly the certificate with which the OCSP request should be signed.



OCSP request signing

○ Never sign ● Always sign ○ Sign if required

VA URL:

Select certificate:

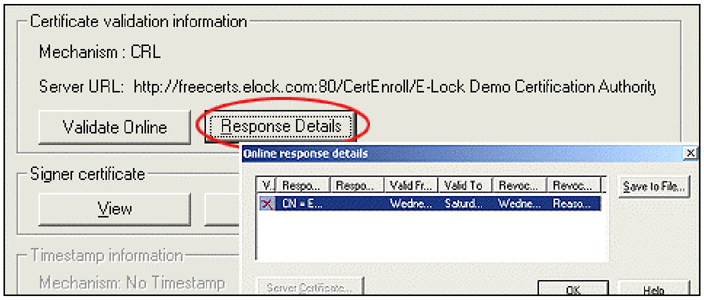
Candice (E-Lock)
Candice Shah
Candice Shah
Candice Shah

Certificate details:

Issuer: E-Lock Demo Certification Authority
E-Lock Demo
Frontier Technologies Corporation
McLean, VA

5.5 STORING VALIDATION RESPONSES

The OCSP protocol provides the added advantage of sending validation information in a specific formatted response, which can be stored and attached to documents or transactions. The response travels with the document or transaction throughout its lifecycle, thus provides a good method of audit in case of disputes. The response can be viewed at a later date to prove the validity of the certificate both at the signing time and at the time of verification of the document or transaction.



Certificate validation information

Mechanism : CRL

Server URL: http://freecerts.elock.com:80/CertEnroll/E-Lock Demo Certification Authority

Signer certificate

Timestamp information

Mechanism: No Timestamp

Online response details

V..	Respo...	Respo...	Valid Fr...	Valid To	Revoc...	Revoc...
☒	CN = E...		Wedne...	Saturd...	Wedne...	Reaso...

6 VALIDATION PARAMETERS

6.1 PROTOCOL SUPPORT FOR VALIDATION

Currently ProSigner supports two protocols for validation for either CRL or for OCSP

- HTTP
- HTTPS
- LDAP
- LDAPS

6.2 PROXY SUPPORT FOR VALIDATION

Many organizations are behind firewalls and use a proxy server to connect to the Internet. This prevents applications from connecting to the Internet without having a specific facility to understand that a Proxy Server is present. Since Validation requires connecting to the Internet, ProSigner provides the facility to specify the URL for the proxy and the validation will then take place accordingly.

6.3 VALIDATION PREFERENCE

Sometimes Issuing Certificate Authorities stamp a certificate with both a valid URL for fetching a CRL and valid URL to an OCSP responder in the AIA extension of the certificate. In such a case, ProSigner will always try to connect to the OCSP responder for a validation response.

6.4 VALIDATION FALLBACK

ProSigner will fallback on CRLDP validation from OCSP validation if:

- The OCSP responder URL stamping is incorrect
- ProSigner cannot connect to the OCSP server
- The OCSP responder asks for a signed request and the configuration manager is set to never send signed requests

The fallback will only occur if the certificate is stamped with a valid CRLDP.

6.5 OFFLINE/ONLINE VALIDATION

To optimize the validation process, ProSigner provides for offline verification. This means that ProSigner will not connect to intranets or the Internet for validation.

The first time a document is verified, ProSigner fetches the CRL or the OCSP response from the Internet. If the CRL is fetched, then it stores and caches it locally. For an OCSP response it staples the response to the document itself.

During offline verification, ProSigner searches for the CRL in the local cache and if found, it provides the result from there itself. For OCSP it checks the previous OCSP response and displays the result.

6.6 CHAIN VALIDATION / END ENTITY VALIDATION ONLY

The certificate with which a document is signed is termed as the End Entity certificate – which in many cases may be issued by an intermediate Certifying Authority. Some organizations require that the whole chain right till the Root Certificate should be validated. This provides more authenticity to the validation.

But sometimes, the intermediate certificates may not have any stamping for either CRL or OCSP validation. In such cases it is preferable to validate only the end entity certificate so that the verification result does not show as unknown.

When the user has opted to validate the whole chain (the default setting), each certificate till the root certificate is validated individually. So it is possible that the revocation methods may be different for different levels of certificates. ProSigner handles this transparently for the user.

6.7 BASIC CONSTRAINTS

By RFC standards, all intermediate certificates and supposed to be with a stamp basic constraint extension. This is to distinguish them as intermediate certifying authority certificate as opposed to an end entity certificate. If this extension is not stamped then further chain building for trust to the root certificate is not achieved. Some organizations especially Government institutes require that this extension be checked during establishing trust.

But in an actual deployment scenario, intermediate certificates may not be stamped correctly. This will prevent any trust chain building that the validation result will always fail. To overcome this, ProSigner provides a feature to disable this checking and go ahead with trust building.

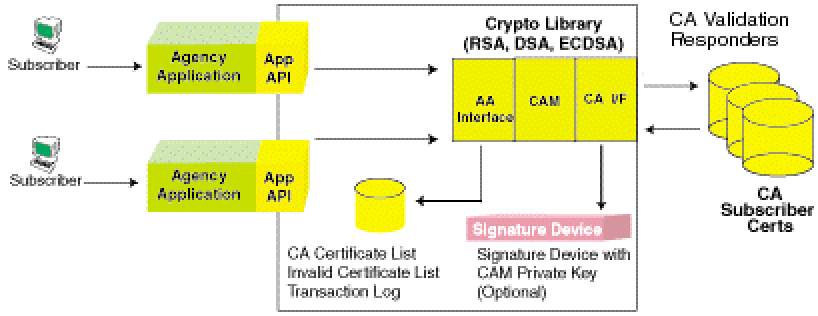
7 CERTIFICATE ARBITRATOR MODULE (CAM)

The Certificate Arbitrator Module (CAM) was originally developed for the “Access Certificates for Electronic Services” (ACES) PKI initiative of the Federal Government’s General Services Administration (GSA). CAM is a “middleware” software server that provides real-time certificate validation, centralized trust management, auditing, and interoperability between different vendor's validation protocols.

Under ACES, CA service contracts were to be awarded to multiple vendors. This created the need for a vendor-neutral validation interoperability tool. CAM was created to provide real-time validation and trust management (trust list checking) as a TCP/IP service. CAM acts as a go-between for “Agency Applications” and the CAs or the Validation responders. The Agency Applications communicate with CAM using a protocol known as “AA-CAM” or just CAM. CAM, in turn, communicates with CAs using an outbound protocol. In a typical deployment, the CAM server resides in the local domain of the relying parties.

The CAM server maintains a trust-list database whose entries include validation instructions. This consists of the network address and protocol type for each CA’s on-line validation service, or may give instructions to look inside the certificate for that information for CAs that populate it.

CAM’s outbound validation mechanisms include a simple CAM proprietary protocol, which is not commonly used, and the “online certificate status protocol” (OCSP). CAM does not internally support validation via certificate revocation lists (CRLs), but can link to DAVE, which does.



CAM validation does not have any specific stamping in the certificate for determining the location of the CAM server. The responsibility falls on the verifying application. Prosigner provides this facility.

7.1 CAM THROUGH PROSIGNER

The Configuration manager has a setting in the validation tab to set the URL, the PORT number and the Application Identifier for the CAM server. Once this is set in the configuration manager, all the validation on that machine for that user will happen with CAM. If a user wants only ACES certificates to be validated with CAM then the user can set this in the configuration manager.

8 TIME REFERENCE FOR CERTIFICATE VALIDATION

One important property in the context of non-repudiation is that a signature, having been found once to be valid, shall continue to be so, for the same data, months or years later. To do so, it is important to establish that the certificate used at the time of signing was a valid certificate. So, even if the certificate may have expired or been revoked at a later date, the validation status of the certificate at the time of signing provides for true non-repudiation. In other words, it is necessary to ascertain the validity of a certificate at the time of signing rather than its current validity. The current validity of a certificate may not be of any real business value or significance.

For instance, let us consider the case of an authorized signatory of a company who uses a valid corporate digital certificate to endorse a transaction. If this individual is no longer associated with the organization in question say three months later, any verification of his certificate will fail.

This will happen since the verification process will consider the current status of his certificate, which would have been revoked or cancelled as a result of his being no longer involved with the organization. However, this does not imply that his participation in the transaction was unauthorized or invalid since his certificate was probably valid at the time of singing. Therefore, it is only necessary to verify that his certificate was valid when it was used to sign the transaction and not in the present context.

9 CONCLUSION

The passage of the E-sign bill has given a major push for conducting business on-line. But the law is just a facilitator. Organizations have to look into the various technologies that can make use of this law and implement them within their business processes. One of the most important factors would be establishing business trust with the help of e-signatures. Digital Signature Technology is a clear winner from this perspective. The ability not only to verify the document contents but also the signer certificate provides a much higher level of business trust and non-repudiation. It is important that the organizations look into digital signature applications, which allow for these features within them so as to provide for an overall secure e-business solution.