



Concept of Electronic Approvals

E-Lock Technologies

Contact

info@elock.com

Table of Contents

<u>1</u>	<u>INTRODUCTION</u>	<u>3</u>
<u>2</u>	<u>WHAT ARE ELECTRONIC APPROVALS?</u>	<u>3</u>
<u>3</u>	<u>HOW DO INDIVIDUALS IDENTIFY THEMSELVES IN THE ELECTRONIC WORLD?</u>	<u>3</u>
<u>4</u>	<u>WHAT IS THE TECHNOLOGY BEHIND DIGITAL CERTIFICATES?</u>	<u>3</u>
<u>5</u>	<u>WHERE DO I STORE MY DIGITAL CERTIFICATE?</u>	<u>4</u>
5.1	IN THE SECURITY FRAMEWORK ON YOUR COMPUTER (VISIBLE THROUGH YOUR BROWSER)	4
5.2	IN A FILE	4
5.3	ON A SMART CARD	4
<u>6</u>	<u>HOW DO YOU USE DIGITAL CERTIFICATES TO SIGN DOCUMENTS?</u>	<u>5</u>
<u>7</u>	<u>WHAT DOES DIGITAL SIGNING AND VERIFICATION OF A DOCUMENT INVOLVE?</u>	<u>5</u>
<u>8</u>	<u>WHAT IS THE DIFFERENCE BETWEEN SIGNING AND ENCRYPTING DOCUMENTS?</u>	<u>6</u>
<u>9</u>	<u>WHAT MAKES FOR A GOOD ELECTRONIC SIGNATURE SOLUTION?</u>	<u>6</u>

1 INTRODUCTION

This document explains the concept of electronic approvals and what is involved. It goes in-depth to explain all the elements and helps you understand how an electronic signature solution works.

2 WHAT ARE ELECTRONIC APPROVALS?

Electronic approvals refer to taking the approval and signing process online enabling individuals, organizations and governments to quickly authorize and sign and approve documents and transactions. Electronic Approvals represent considerable time and cost savings over traditional paper intensive methods.

More importantly, electronic approvals have now acquired legal status and carry the same weight as paper based documents. Several countries across the world have passed electronic signature legislation, laying down the terms and conditions for legally binding electronic transactions.

3 HOW DO INDIVIDUALS IDENTIFY THEMSELVES IN THE ELECTRONIC WORLD?


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 (CA's).

4 WHAT IS THE TECHNOLOGY BEHIND DIGITAL CERTIFICATES?

The underlying technology to digital certificates is called PKI or Public Key Infrastructure. This technology is based on cryptography and it utilizes what is known as a "key pair" - a public key and a private key. These are nothing but 2 pieces of mathematically related information. Both these together comprise the digital certificate.

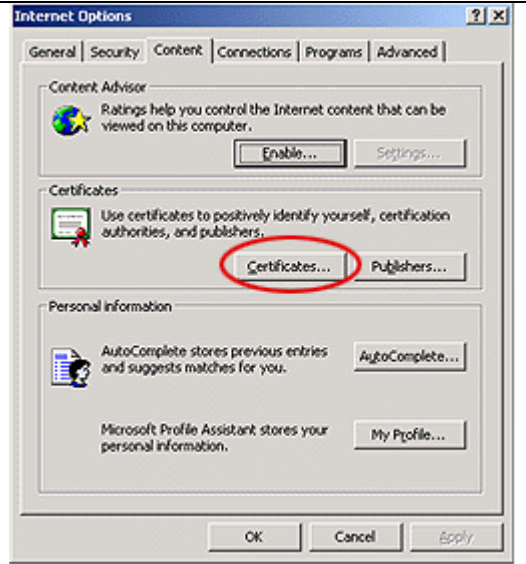

The private key is always under the sole control of the owner and the public key can be distributed to other users. The private key cannot be compromised through knowledge of the associated public key.

Each key in the key pair performs the inverse function of the other. What one key does, only the other can undo. The private key is used for signing and decrypting a message or a document while the public key is used to verify or encrypt. All this is transparent to the user.

 <p>The screenshot shows a 'Certificate' dialog box with three tabs: 'General', 'Details', and 'Certification Path'. The 'General' tab is selected, displaying 'Certificate Information'. It states: 'This certificate is intended to: •Proves your identity to a remote computer'. Below this, it lists: 'Issued to: Candice (E-Lock)', 'Issued by: Tellus Technologies Pvt. Ltd.', and 'Valid from 3/26/2003 to 3/26/2004'. A note at the bottom says: 'You have a private key that corresponds to this certificate.' There are 'Issue Statement...' and 'OK' buttons at the bottom.</p>	<p>This is what a digital certificate looks like. It contains information on:</p> <ul style="list-style-type: none"> • The person it is issued to • The Issuer • The validity period
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

5 WHERE DO I STORE MY DIGITAL CERTIFICATE?

You can opt to store your certificate in one or all of the following ways:

<p>5.1 IN THE SECURITY FRAMEWORK ON YOUR COMPUTER (VISIBLE THROUGH YOUR BROWSER)</p> <p>If you open Internet Explorer and go to Tools→Internet Options→ Content Tab you will see a section called Certificates. This corresponds to the security framework, which is present on your computer by default. This is the most common place to store certificates.</p> <p>If you click the certificate button, you will see some certificates that are already present on your computer. This is divided into an area for your own personal certificates, other people's certificates and CA root certificates.</p>	 <p>The screenshot shows the 'Internet Options' dialog box with the 'Content' tab selected. Under the 'Certificates' section, the text reads: 'Use certificates to positively identify yourself, certification authorities, and publishers.' Below this text, there are two buttons: 'Certificates...' and 'Publishers...'. The 'Certificates...' button is circled in red.</p>
<p>5.2 IN A FILE</p> <p>You can opt to store your certificate to a file. It will have one of the following extensions: pfx or p12.</p>	 <p>The image shows a file icon with a yellow background and a magnifying glass over it. Below the icon, the text 'BILL' is displayed.</p>
<p>5.3 ON A SMART CARD</p> <p>This is the most secure way to store your certificate. It is also convenient for users that are mobile; this provides a way for them to carry their certificate with them wherever they go.</p>	

6 HOW DO YOU USE DIGITAL CERTIFICATES TO SIGN DOCUMENTS?

Once you acquire a digital certificate, Digital Signature applications enable you utilize that certificate to sign documents electronically. Since a digital certificate vouches for your electronic identity, the application of that certificate to any data (documents or transactions) establishes a user's connection to a document.

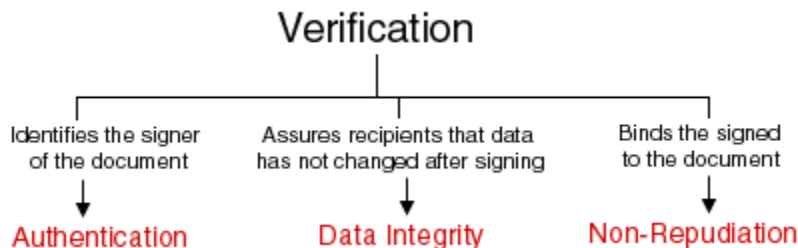
7 WHAT DOES DIGITAL SIGNING AND VERIFICATION OF A DOCUMENT INVOLVE?

When you digitally sign a document, you're actually binding your digital certificate (and thus your identify) to the contents of the document.

When you sign (using your certificate), an algorithm is used to create a hash of the application of your certificate to the document. This hash is then internally encrypted (not to be confused with encrypting a document) using the private key component of your certificate. This encrypted hash is the actual "digital signature". The public key component of the certificate and the hash created travels transparently with the signed document.

This signed document can then be routed to the recipient. When the Recipient attempts to verify the signed document, the public key that travels along with the signed document is first used to decrypt the digital signature; the hash is retrieved on doing this. Another hash is created on the recipients end, and this hash is compared with the older hash. If both match, then the verification is deemed successful.

When Verification is successful, it means that No changes have been made to the document after signing. It also identifies the signer of the document to the recipient (through the digital certificate). The recipient can therefore be certain of who the document came from.



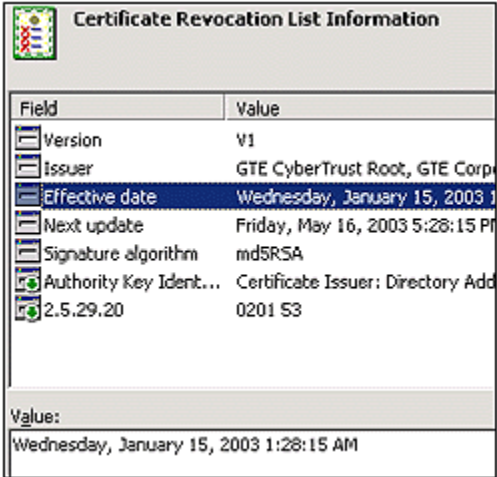
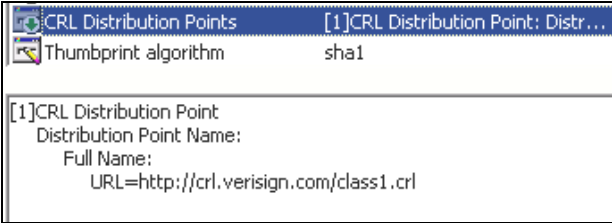
8 HOW DO I CHECK IF A DOCUMENT HAS BEEN SIGNED USING A VALID CERTIFICATE?

At the time of issue, certificates are given a fixed life span and expire at the end of this set period. 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.

It is important that your electronic signature solution is capable of checking the status of certificates that have been used to sign documents. Certificate Authorities periodically publish lists of revoked certificates called Certificate Revocation Lists (CRLs). The CRL location for a particular Certificate Authority is typically mentioned in the details of any certificate issued by that CA – and the location is called a CRLDP (Certificate Revocation List Distribution Point)

A Certificate Revocation List	The CRLDP as specified in a certificate																
 <p>Certificate Revocation List Information</p> <table border="1"> <thead> <tr> <th>Field</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>Version</td> <td>V1</td> </tr> <tr> <td>Issuer</td> <td>GTE CyberTrust Root, GTE Corp</td> </tr> <tr> <td>Effective date</td> <td>Wednesday, January 15, 2003 1:28:15 AM</td> </tr> <tr> <td>Next update</td> <td>Friday, May 16, 2003 5:28:15 PM</td> </tr> <tr> <td>Signature algorithm</td> <td>md5RSA</td> </tr> <tr> <td>Authority Key Ident...</td> <td>Certificate Issuer: Directory Add...</td> </tr> <tr> <td>2.5.29.20</td> <td>0201 53</td> </tr> </tbody> </table> <p>Value: Wednesday, January 15, 2003 1:28:15 AM</p>	Field	Value	Version	V1	Issuer	GTE CyberTrust Root, GTE Corp	Effective date	Wednesday, January 15, 2003 1:28:15 AM	Next update	Friday, May 16, 2003 5:28:15 PM	Signature algorithm	md5RSA	Authority Key Ident...	Certificate Issuer: Directory Add...	2.5.29.20	0201 53	 <p>CRL Distribution Points [1]CRL Distribution Point: Distr...</p> <p>Thumbprint algorithm sha1</p> <p>[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.verisign.com/class1.crl</p>
Field	Value																
Version	V1																
Issuer	GTE CyberTrust Root, GTE Corp																
Effective date	Wednesday, January 15, 2003 1:28:15 AM																
Next update	Friday, May 16, 2003 5:28:15 PM																
Signature algorithm	md5RSA																
Authority Key Ident...	Certificate Issuer: Directory Add...																
2.5.29.20	0201 53																

9 WHAT IS THE DIFFERENCE BETWEEN SIGNING AND ENCRYPTING DOCUMENTS?

The major difference between signing and encrypting documents is that when you sign a document you are certifying the contents and when you encrypt it you are blocking the content from all except the intended recipient(s). A signed document is visible by all but an encrypted document is only visible to the person(s) that have the authority to decrypt it.

In most cases you would need to just sign the document, however if the content is of high-value or confidential, you may want to encrypt it so only the intended persons can view it.

10 WHAT MAKES FOR A GOOD ELECTRONIC SIGNATURE SOLUTION?

A good solution is one that combines ease of use with strong security that's transparent to the user. It's important that users be able migrate to the new electronic system with a minimal learning curve. As such, the electronic signature solution should be intuitive to use, and easily scaleable to meet future needs. The signature solution should work with any Digital Certificate issued by a recognized Certificate Authority (x.509 is the certificate format standard). This ensures PKI independence. It should also interoperate with smart cards and signature capture devices, as these elements combine to offer users a complete solution.

It helps if user functions are wizard based for ease of use to even first time users and if settings for common operations can be preset and automated. It's also a good idea if the

solution allows for security policies so you can control and define how security is used complied with in your organization.

Lastly, a good signature solution should comply with at least the key conditions laid down in the digital signature legislation of your country (if applicable).
