Encryption and Digital Signature Explained

Entrust® is a family of software products for encryption and digital signature on client/server networks with fully automated key management. This document provides a background on how encryption and digital signature work to secure word processing files, e-mail, spreadsheets, and a host of other applications.

History

The art of cryptography has a long history. Julius Caesar used a crude system of encryption when he sent orders to his generals. It involved shifting the letters of the alphabet a predetermined number of characters. In its day, the method Caesar used would have been considered state-of-the-art.

As encryption evolved, more sophisticated mathematical transformations were used. What stayed constant was the need to send the unlocking or decrypting key separately and securely. That, and the relative weakness of the encryption algorithms, have been the major shortcomings up until the last two decades.

Two Things Have Changed in Cryptography

The introduction of high-speed computers allowed the development of more complex and thus stronger encryption algorithms.

The second major advancement was the development of public-key cryptography. The public-key system (which is explained later) solved the problem of making the decryption key (as opposed to the encrypted data) available in a secure fashion.

To better understand how cryptography is used to secure electronic communications, let’s look at a process we are all familiar with.... writing and sending a check.

Securing the Electronic Version

The simplest electronic version of the check can be text, created with a word processor or e-mail package, asking your bank to pay someone a specific sum. However, sending this check over an electronic network creates several security problems:

- Since anyone could intercept and read the file, we need privacy.
- Since someone else could create a similar counterfeit file, we need authentication.
- Since the originator could deny creating the file, we need non-repudiation.
- Since someone could alter the file, we need integrity.

To overcome these issues, Entrust performs a number of steps hidden behind a simple user interface.

Privacy and Encryption

The electronic check can be encrypted using a high-speed mathematical transformation with a key that will be used later to decrypt the document. This is often referred to as a *symmetric key* system because the same key is used at both ends of the process.

As the check is sent over the network, it is unreadable without the key. The next challenge is to deliver the symmetric key in a secure fashion.

Public-Key Cryptography for Delivering Symmetric Keys

The introduction of public-key encryption in the late 1970s solved the problem of delivering the symmetric encryption key to the target destination in a secure manner. With public-key cryptography there are two keys: one is kept private, and the mate is made publicly available. What is encrypted with one can only be decrypted with the other (and vice versa). The innovation is that revealing the public key does not in any way compromise the private key. No other private key can decrypt the data that is encrypted with your public key.

Unfortunately, public-key algorithms are relatively slow, but are ideal for encrypting small amounts of information such as a symmetric key! So the check is encrypted with a fast symmetric key (uniquely generated for this occasion) and then, the symmetric key is encrypted with the receiver’s public key. Now only the private key of the receiver can recover the symmetric key, and thus decrypt the check.

Digital Envelope

Now we have a check that is encrypted and can be read only by the target recipient. We have just created a digital version of the envelope. Unfortunately, someone else could have created the same document using the public key of the recipient, and e-mailed a bogus check. To prevent this, we need the digital equivalent of a signature.

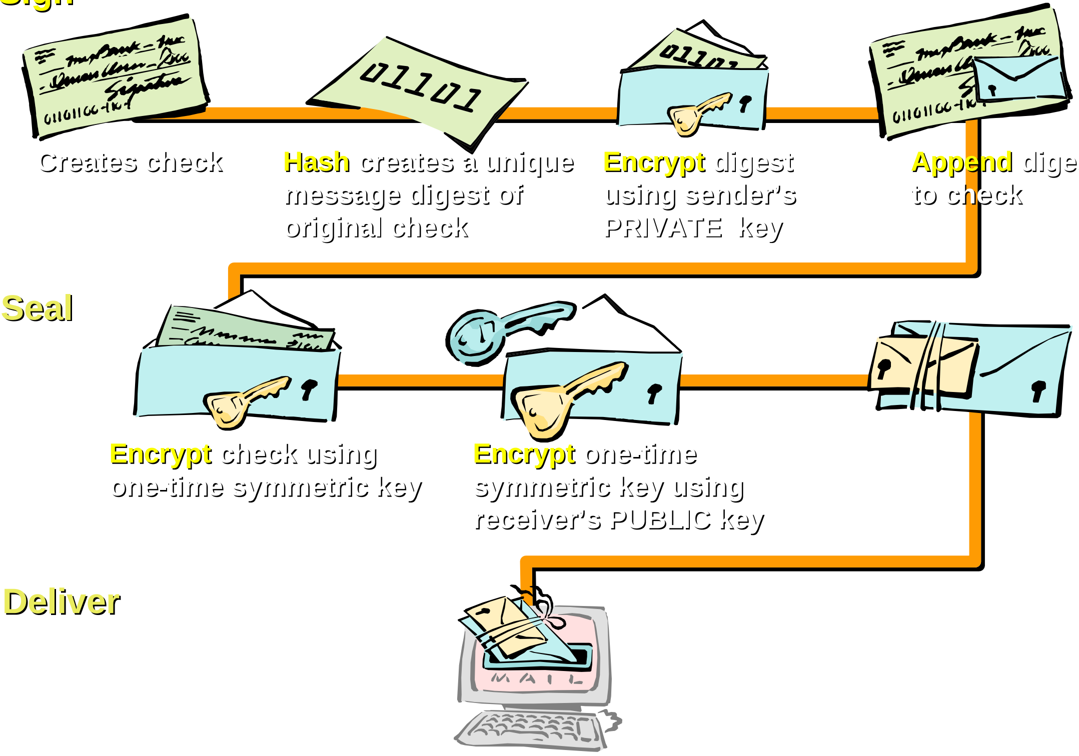
Digital Signature

The same public- and private-key system used for the digital envelope can be used to guarantee the identity of the originator. We simply switch the roles of the public and private keys. Anything encrypted with your private key can be decrypted by anyone else using your public key. It must have come from you because only you have your private key.

The process of digitally signing starts by taking a mathematical summary (called a hash) of the check. If even a single bit of the check changes, the hash code will dramatically change. The next step in creating a digital signature is to encrypt the hash code with your private key. Finally, this encrypted fingerprint is appended to the check.

How is this a signature? Well, the receiver of your check can decrypt the hash code sent by you, using your public key. At the same time, the hash code can be recreated from the received check and compared with the original hash code. If the hash codes match, then the receiver has verified that the check has not been altered. The receiver also knows that only you could have sent the check because no one else has the private key that encrypted the original hash code.

The following illustration describes what Entrust does behind the scenes.



Sign

Creates check

Hash creates a unique message digest of original check

Encrypt digest using sender's PRIVATE key

Append digest to check

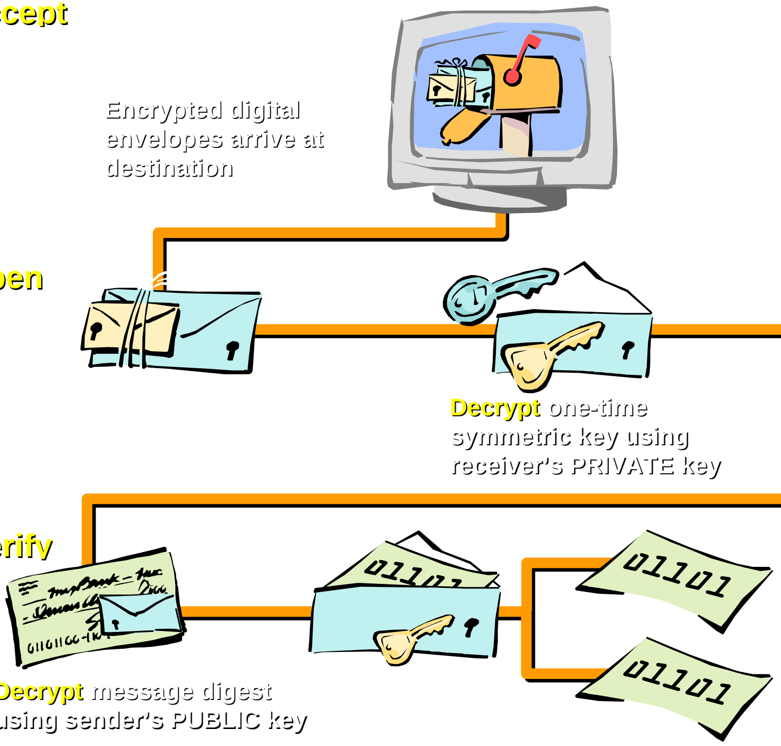
Seal

Encrypt check using one-time symmetric key

Encrypt one-time symmetric key using receiver's PUBLIC key

Deliver

Mail electronic envelopes to receiver



Accept

Encrypted digital envelopes arrive at destination

Open

Decrypt one-time symmetric key using receiver's PRIVATE key

Decrypt check using one-time symmetric key

Verify

Decrypt message digest using sender's PUBLIC key

Rehash creates a new digest from decrypted check for comparison with the original

Digital Certificates

Now we have a system that can encrypt your check, secure the keys, and authenticate the sender. The last piece of the puzzle is to guarantee that the public-key list (used by everyone to verify signatures) has not been tampered with. This would be equivalent to warranting that the signature card you have on file at the bank has not been switched with a forgery.

This is done by having the public directory entries digitally 'signed' by the system administrator. Using the system administrator's public key, anyone can verify that the directory entry is genuine. The signed directory entry is known as a *certificate*.

Entrust

Entrust is a unique and powerful software system that executes the above steps for encryption and digital signature at the click of a button.

Simple and easy to use, Entrust is at the same time fast and secure. It uses the latest in software and cryptographic technology to make security transparent and automatic to the user.

Entrust provides the customer with the following:

- support for enterprises from hundreds to tens of thousands of users and beyond
- applications integration with industry-leading applications
- automatic (and transparent) key management
- an open solution, true to standards
- a choice of cryptographic algorithms
- a high-level Application Programming Interface (API)

For more information on Entrust contact:
1-613-765-5607

or visit our home page at:
http://www.entrust.com

This information is subject to change as Entrust Technologies Limited reserves the right, without notice, to make changes to its products, as progress in engineering or manufacturing methods or circumstances may warrant.

Export restrictions apply to all cryptographic products and licenses may be required.

Printed in Canada.