

---

*Data Interchange plc*

---

---

# PKI Security

---

Issued: 14 March 2006

Copyright Data Interchange Plc  
Peterborough, England, September 2005.

All rights reserved. No part of this document may be disclosed to third parties or reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of Data Interchange Plc.



# Table of Contents

<b>PKI Security</b> .....	<b>5</b>
Security Objectives .....	5
Symmetric and Asymmetric Ciphers .....	5
<i>Symmetric</i> .....	5
<i>Asymmetric</i> .....	6
PKI Details .....	6
<i>Message Digest</i> .....	6
<i>Digital Signatures</i> .....	7
<i>Sending a message using PKI</i> .....	8
<i>Receiving a message using PKI</i> .....	8
<i>Certificates and Certification</i> .....	8
PKI Security in DI products .....	9



# PKI Security

## Security Objectives

PKI security provides the encryption technologies required by electronic data interchange to meet the following security objectives:

**Authentication:** The process of proving one's identity.

**Confidentiality:** Ensuring that no one can read the message except the intended recipient.

**Integrity:** Assuring the recipient that the received message has not been altered in any way from the original.

**Non-repudiation:** A mechanism to prove that the sender/recipient really sent/received a message.

## Symmetric and Asymmetric Ciphers

### Symmetric

Symmetric Ciphers (secret key) have been used for many years. A simple example of such a cipher is ROT-13, in which the letters of the plaintext are substituted for the letter 13 places ahead in the English alphabet. The encrypted text formed from the initial plaintext is called the ciphertext. To decrypt the ciphertext back into plain text simply requires the application of the same key once again.

Symmetric Keys:

- Encryption key and the decryption key are identical
- One key is very easily derived from the other

Symmetric Key Advantages:

- High encryption speeds

Symmetric Key Disadvantages:

- The success of symmetric key encryption is reliant on both parties in the exchange sharing a secret key prior to the transmission of the actual business documents.
- Therefore a prior secure communication session will be required to exchange this secret key.
- This 'prior' communication session causes a problem in itself if the parties are unknown to each other (i.e. have no previous experience upon which to base any trust)

- Difficulties of scale also occur when any such company or user wishes to communicate securely with multiple different companies or users.

## Asymmetric

Asymmetric ciphers make use of two related yet different keys. The keys are related but sufficiently different that knowing one key does not allow the derivation or computation of the other. The key pair is made up of a private key and public key. Due to the relationship between the keys, the public key can be freely distributed.

By using two different keys, one for encryption and the other for decryption, Asymmetric cryptography overcomes the main disadvantage of Symmetric cryptography. However this comes at a cost, as the algorithms used for Asymmetric cryptography are slow and therefore unsuitable for encrypting large files.

## PKI Details

Public Key Infrastructure security utilises both Symmetric and Asymmetric security to deliver a highly secure security mechanism that removes the disadvantages of each.

PKI achieves each of the security objectives mentioned above.

- The digital signature is used to **Authenticate** the message
- Encryption of the message is used to ensure the **Confidentiality** of the message
- The digital signature is used to ensure the **Integrity** of the message
- The uniqueness of the digital signature prevents the owner of the signature from disowning the signature and thus provides **Non-repudiation**

## Message Digest

The message digest is a digital fingerprint of a message, which is obtained by performing a hash function on the message data. This hashing function is fast and produces a small message digest from the contents of the message.

The message digest algorithms have two very important features:

- the same input always produces the same output but different inputs could never produce the same output
- it is impossible to determine the actual message from the message digest.

The message digest is used to guarantee that the message data is not altered during transit. The message digest is encrypted with the sender's private key to form a digital signature.

## Digital Signatures

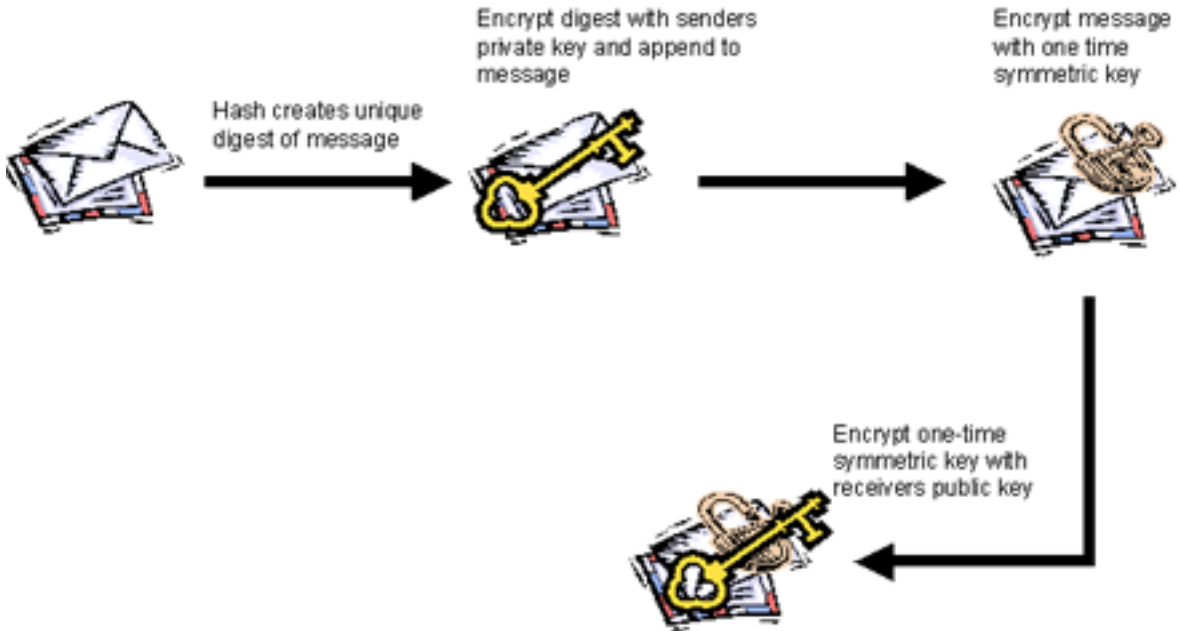
A service enabled by public-key cryptography is that of Digital Signatures. This, as the name suggests, is the equivalent of a handwritten signature; many people can read and verify the signature but only one person can produce the signature.

A digital signature relies on the key pair. The signer, to explicitly link the data to himself, uses the private key to sign the data. The public key can then be published/distributed to all trading partners, allowing them to validate the signature.

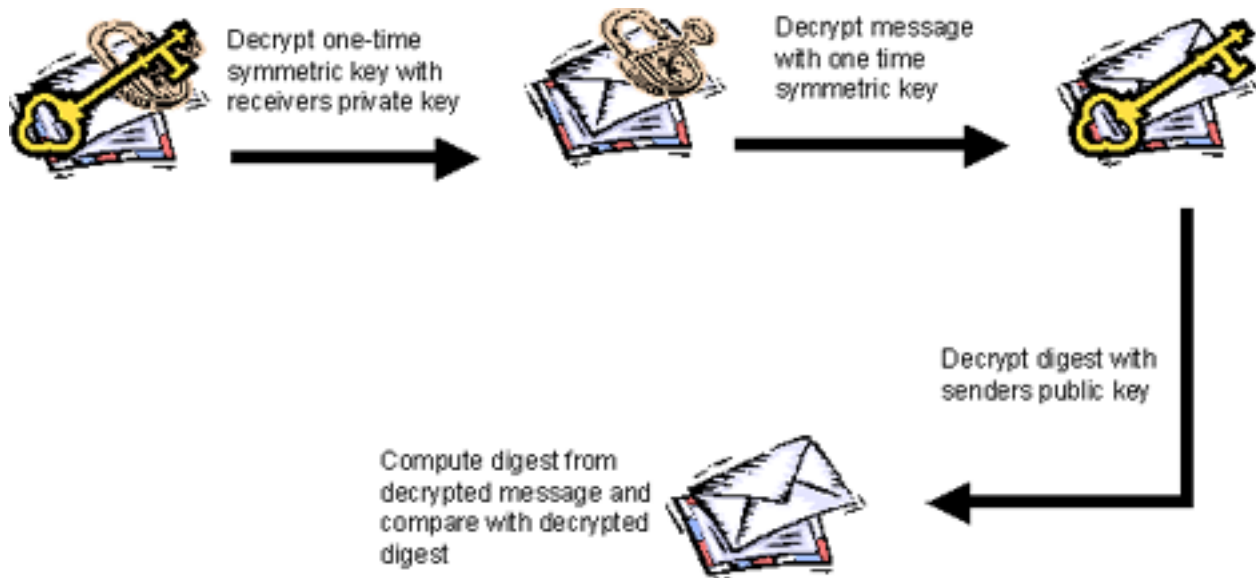
This is impossible to achieve while using a symmetric key system, as the symmetric key would need to be known by both the signer and the receiving party. Once a symmetric key is revealed to a second party, that key can no longer be exclusively linked to one trading partner. This means for future message exchanges, use of this key would no longer provide authentication.

A digital signature should be seen as a private key operation on data, with the resulting value being a signature. The data to be signed may be of any size (a few kb through to a 100mb file), but a private key operation takes a fixed size input and produces a fixed size output. To solve this problem a hash function is used to produce the fixed sized input (the message digest) for the private key operation.

## Sending a message using PKI



## Receiving a message using PKI



## Certificates and Certification

The distribution of the public component, if not undertaken correctly, would defeat the objectives of a PKI. Therefore two mechanisms are required, firstly data integrity to ensure that the contents of the public key (and any other info attributed to it) is not modified without detection.

Secondly a mechanism that binds the public key to the claimed owner is also required.

This is achieved using a public key certificate. There are numerous different types of certificates, but the most common and the one normally referred to as a certificate or digital certificate, is an X.509 public key certificate (RFC 3647).

An X.509 certificate contains the following information:

**X.509 Certificate Structure:**

Version

Serial Number

Signature – the algorithm identifier

Issuer – the distinguished name (DN) of the CA that issued the signature.

Validity – the time window that the certificate should be considered valid.

Subject – The DN of the certificate owner

Subject public key info – the public key and (algorithm identifier)

Issuer Unique ID – rarely used.

**PKI Security in DI products**

The following products support PKI security:

BACS.*IP*