



Australian Government

Medicare Australia

Demystifying Public Key Infrastructure

Name: PKI and Information

Standards Section

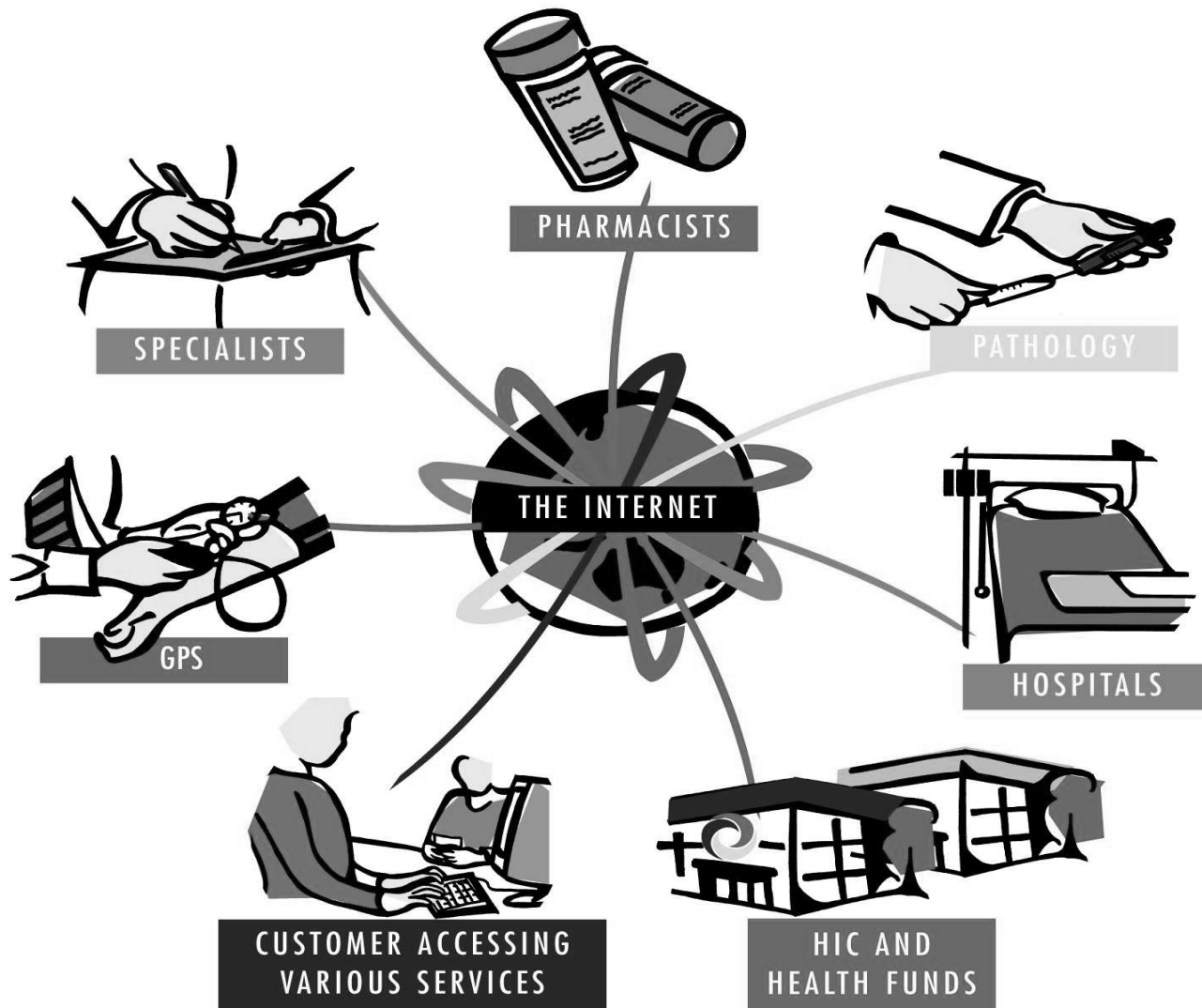
Date: August 2002



Australian Government

Medicare Australia

Connecting the Health Sector



TOMORROW'S HEALTH SECTOR CONNECTIVITY



Why Connect the Health Sector?

To improve health outcomes - but how might this be achieved?

- by improving the decisions made
- by having the right information available to decision-makers when they need it
- via assisting with development and implementation of standards in UN/EDIFACT, HL7 and PKI





National Health Information Management Advisory Council (NHIMAC):

- National strategic plan for using new and emerging technologies for delivering health services that benefit all areas of health sector
- Information services tailored to meet consumer expectations
- Support for clinical care through sharing of information
- Efficiency gains through use of secure electronic data transfer



Critical issues for going forward - online access to information:

- security
- confidentiality
- privacy
- consent

PKI - the building block which provides robust security to address these critical requirements



- Real time allows for greater data accuracy
- Wider range of information products
- Much faster access to information



- Dominant medium
- Inexpensive
- Protocols well established
- Skills available for software development
- Easy to integrate into existing systems



Provide a regulatory framework that:

- recognises the importance of the information economy to the future economic and social prosperity of Australia
- facilitates the use of electronic transactions
- promotes business and community confidence in the use of electronic transactions
- enables business and the community to use electronic communications in their dealings with government
- IT standards for electronic transmission, scanning and storage of Referrals to specialists/consultant physicians and Requests for pathology and diagnostic imaging services



Australian Government

Medicare Australia

General rule - Electronic Transactions Act

General rule- Electronic Transactions Act

Allows e-commerce to be treated the same as paper transactions:

- paper and electronic have the same legal footing
- will not discriminate between technologies
- principled approach to electronic signatures



Australian Government

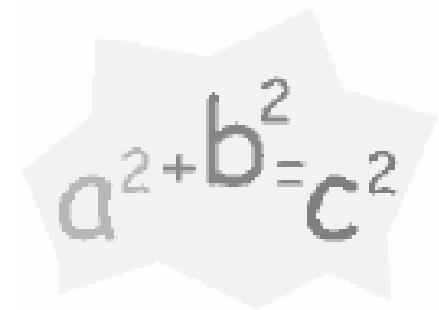
Medicare Australia

Privacy and security



To do business in the electronic world you will need:

- Digital Certificates
- Digital Key pairs
- Digital Signatures





Signing - public and private key pair:

- non-repudiation
- authentication
- integrity

Encrypting - public and private key pair:

- confidentiality
- integrity



Has a history as long as writing itself

Is the science of scrambling messages to ensure secure communications between sender and receiver - as with codes used during wartime

The advent of the Internet has seen cryptography come to the fore for securing messages going over insecure networks

Only those who possess the key (or cipher) can scramble or unscramble messages



Achieved by applying a mathematical algorithm to convert plain text, data or other information to ciphertext

The cipher is the set of rules used to encrypt the plain text, data or other information

Cipher is also known as 'key'

The cipher and the encryption algorithm are the two essential components for secure messaging over a network



Data Encryption Standard - or DES originated at IBM in 1977

Adopted by US Department of Defence

Because of concern about use of DES by 'unfriendly governments' export of this encryption software was prevented by US Government for some years



Australian Government

Medicare Australia

DES Encryption Keys

There are 72,000,000,000,000,000 (ie 72 quadrillion) or more possible encryption keys that can be used

For individual messages the key is chosen at random from amongst this 72 quadrillion plus number of possibilities



DES applies a 56-bit key to each 64-bit block of data

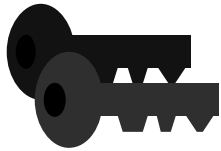
Process can run in several modes and involves '16 rounds' or operation

Although considered strong encryption, many users chose TRIPLE DES

Triple DES applies three keys in succession



To use Public/Private key cryptography,
first you need some keys



A security software package will create a *Private key* and a *Public key* for you. This is known as a keypair. The *Private key* will then be stored on a smartcard.

The *Public key* is mathematically related to the *Private key*, but the *Private key* cannot be calculated using the *Public key*.



Private key

Your *Private Key* is your identity when sending digitally signed messages. It is the equivalent of your handwritten signature.



Public Key

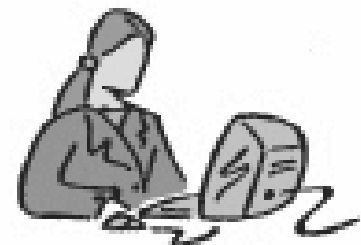
Your *Public Key* is the means by which your digital signature is verified by the recipient.

Both Private and Public keys are simply very long numbers such as

A7 66 CF 34 79 90 EC 65 E4 0D A7 DA 28 BC 2F D6



The Paper World



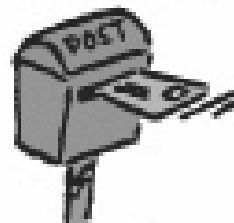
Write



Sign



Close



Send



Open



Verify

ELECTRONIC EQUIVALENT

Write



Digital
Signature



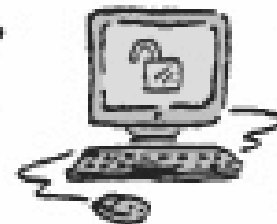
Encrypt



Deliver



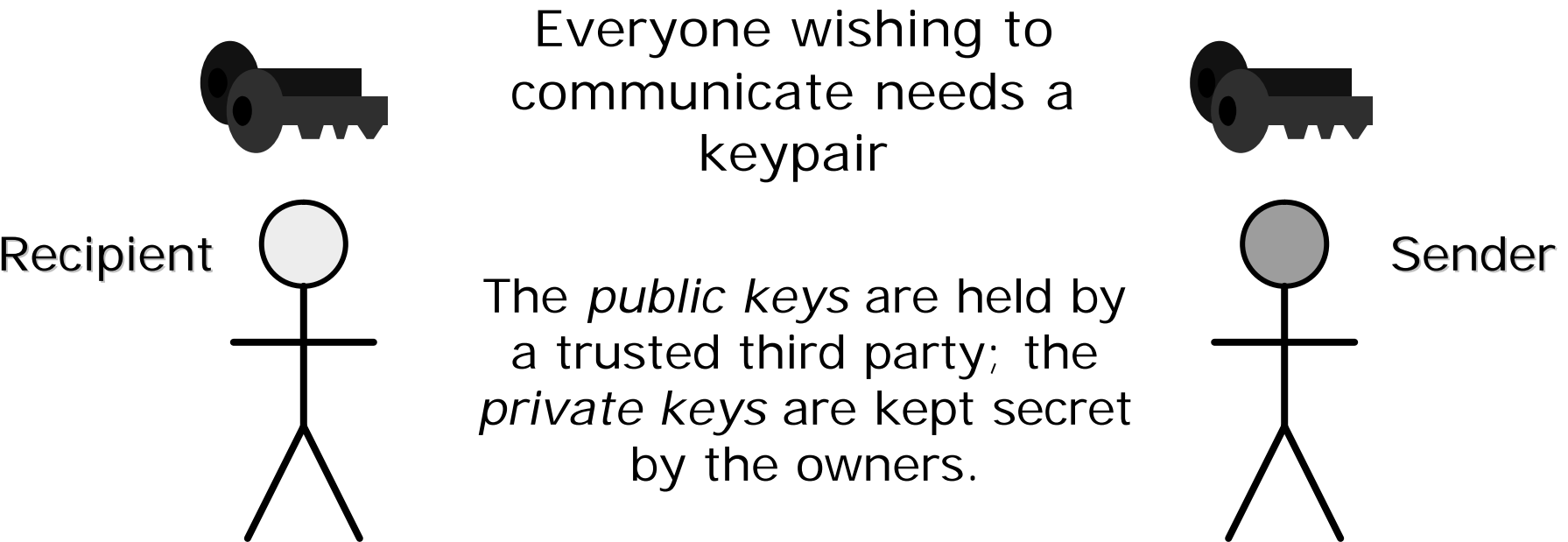
Message
Decrypted



Signature
Verified



The Electronic World



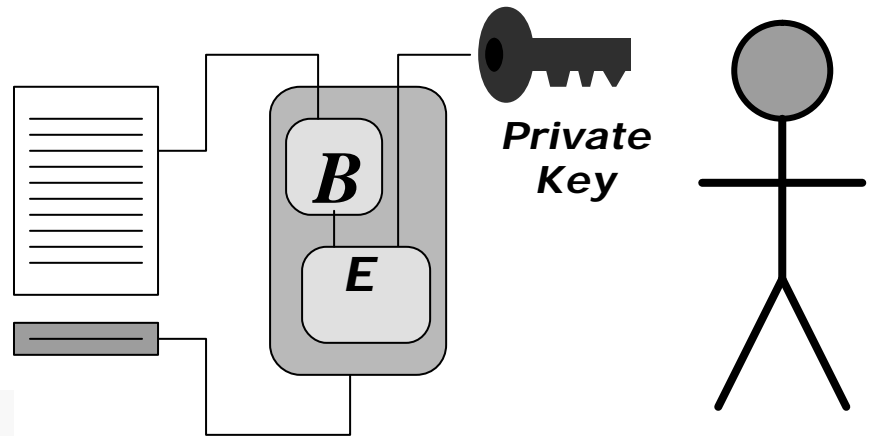
Your *Public* key is made free to anyone who needs it.
Your *Private* key is known only to you.



Using Keys to Sign Messages

First, a special electronic blueprint is taken of the document you are about to sign.

The encoded blueprint is encrypted using your *Private key*.



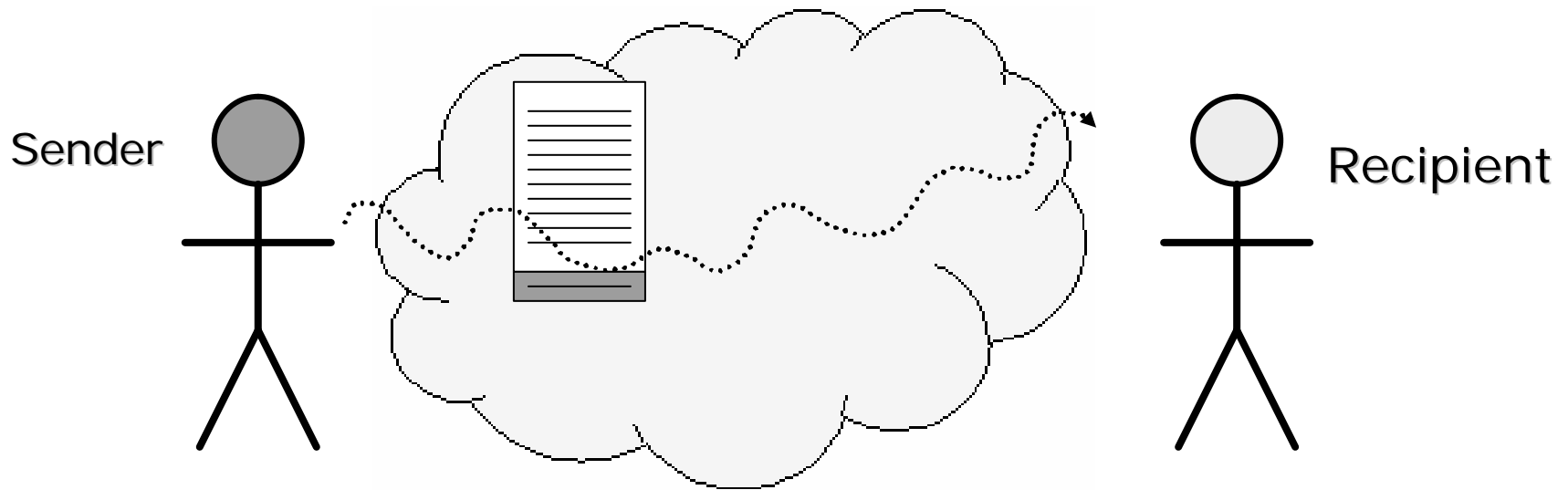
The encrypted blueprint is then appended to the document as the digital signature.



Australian Government

Medicare Australia

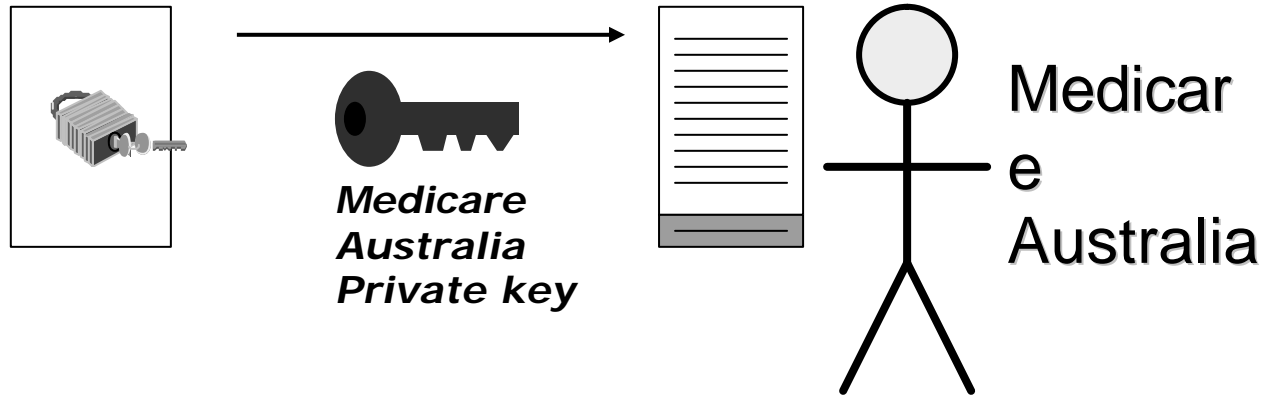
Internet Transaction



The signed message is transmitted to the intended recipient...



Encryption provides confidentiality

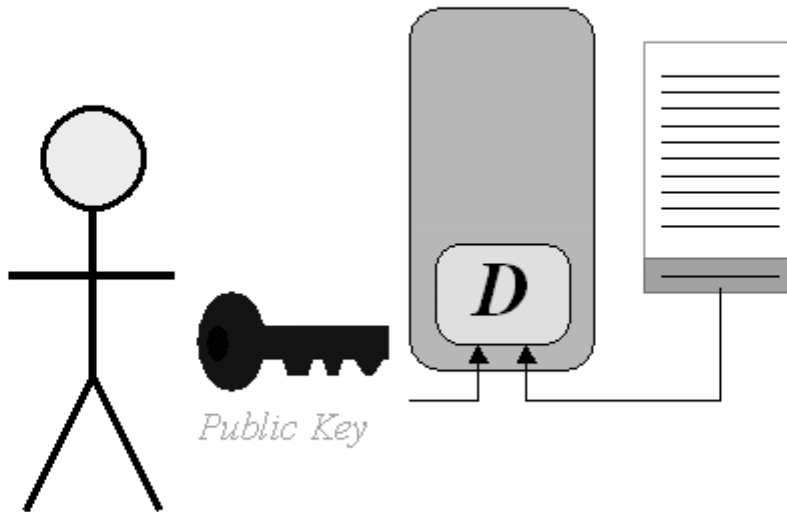


The message, encrypted with the recipient's *Public key*, can only be decrypted with the related *Private key*.

After decryption, the signed message will be available for verification...



Recipient

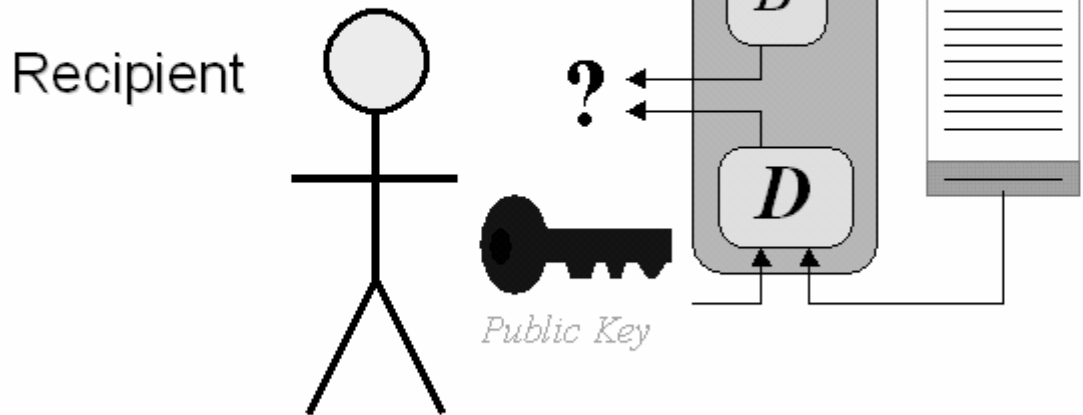


The recipient uses the sender's *Public* key to decrypt the document blueprint.



The two blueprints are then compared to check they are identical.

At the same time, the document information is extracted again, from the original document



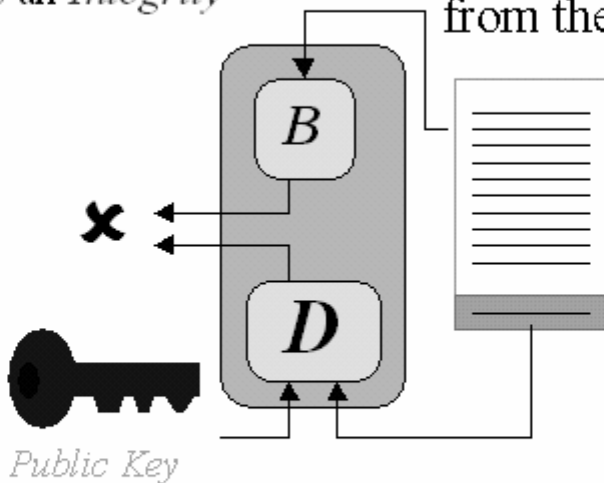
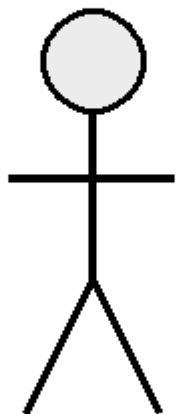
The recipient uses the sender's *Public key* to decrypt the document blueprint.



If the two blueprints are not identical, it means the document may have been altered in transit. This is an *Integrity* check.

At the same time, the document information is extracted again, from the original document

Recipient



Integrity

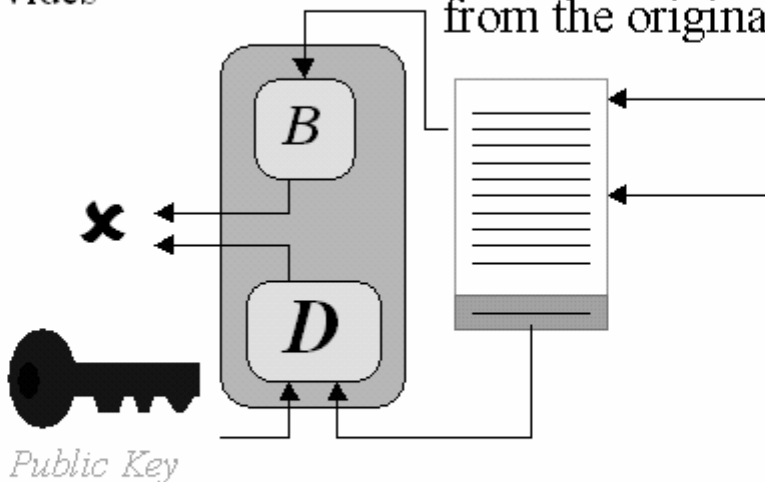
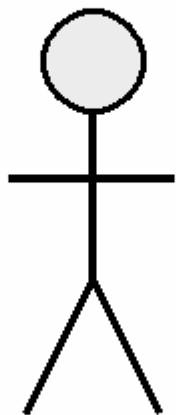
The recipient uses the sender's *Public* key to decrypt the document blueprint.



If someone other than the sender signed the document, the blueprints will not match. This provides *Authenticity*.

At the same time, the document information is extracted again, from the original document

Recipient



Integrity

Authenticity

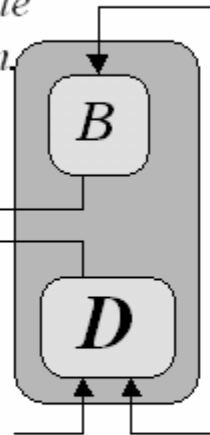
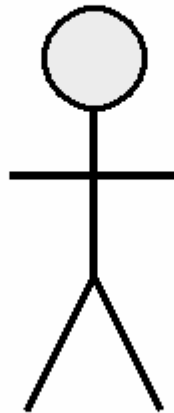
The recipient uses the sender's *Public key* to decrypt the document blueprint.



If the blueprints match, the sender cannot deny having signed it, since only they have access to their *private key*. This provides *Non-Repudiation*.

At the same time, the document information is extracted again, from the original document

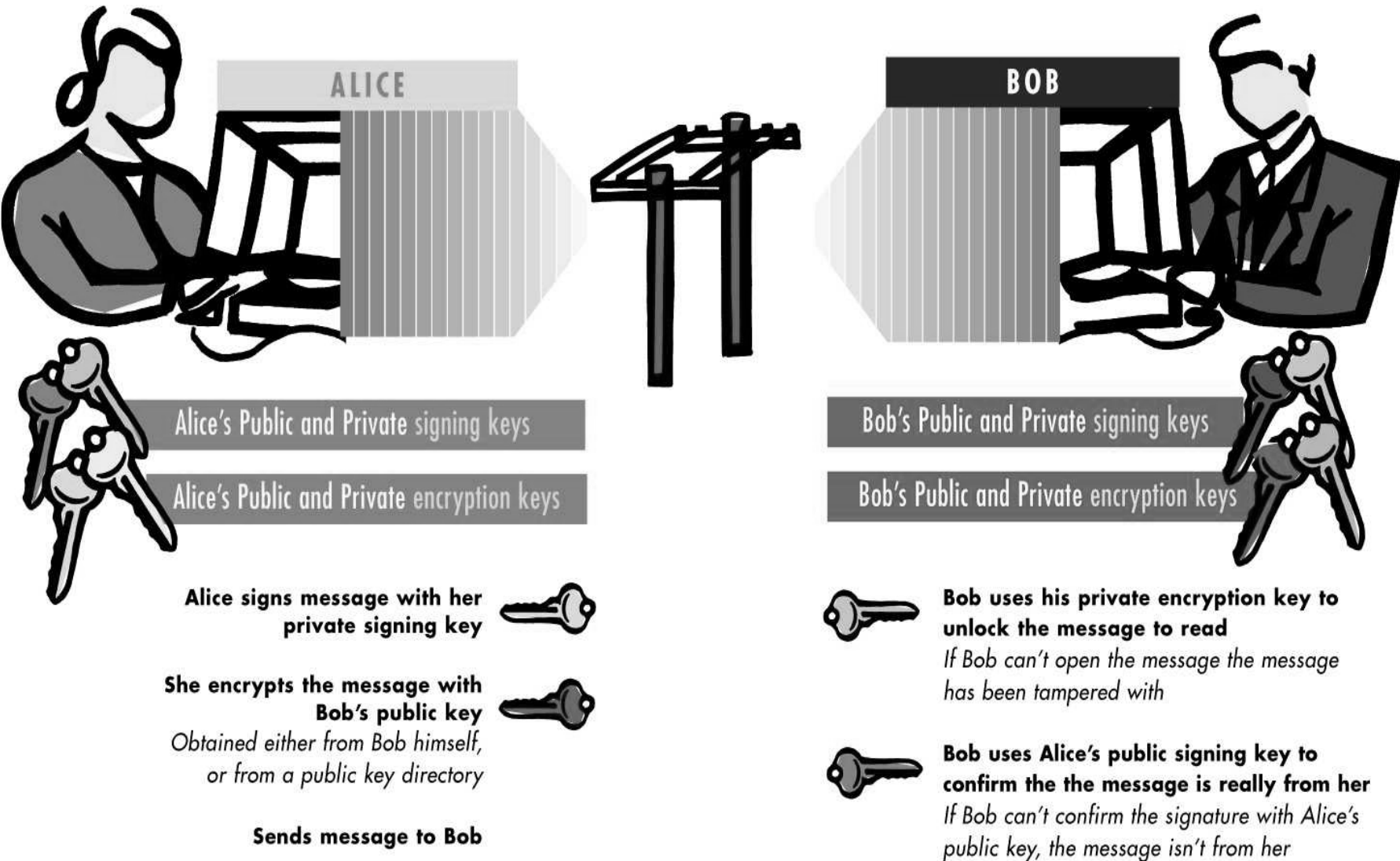
Recipient

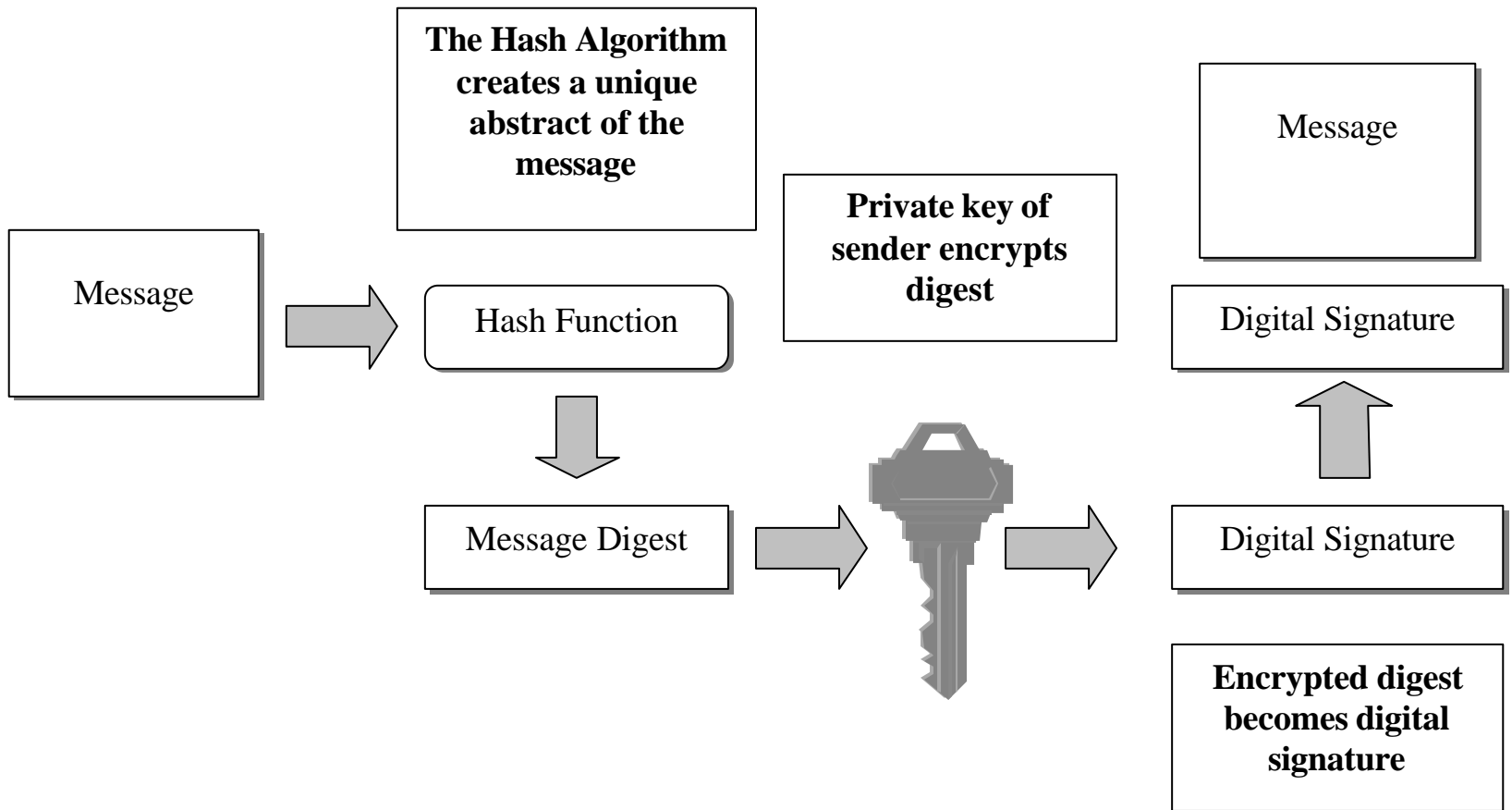


- Integrity*
- Authenticity*
- Non-Repudiation*

The recipient uses the sender's *Public key* to decrypt the document blueprint.

SAFE ELECTRONIC INFORMATION TRANSFER







E-mail:

pki@medicareaustralia.gov.au



References:

www.medicareaustralia.gov.au/pki

www.hesa.gov.au

www.govonline.gov.au (Gatekeeper)



PKI Customer Service Centre

24hours x 7 days

1300 660 035