

# 36th RIPE Meeting Budapest 2000

## APNIC Certificate Authority Status Report



# APNIC CA Project

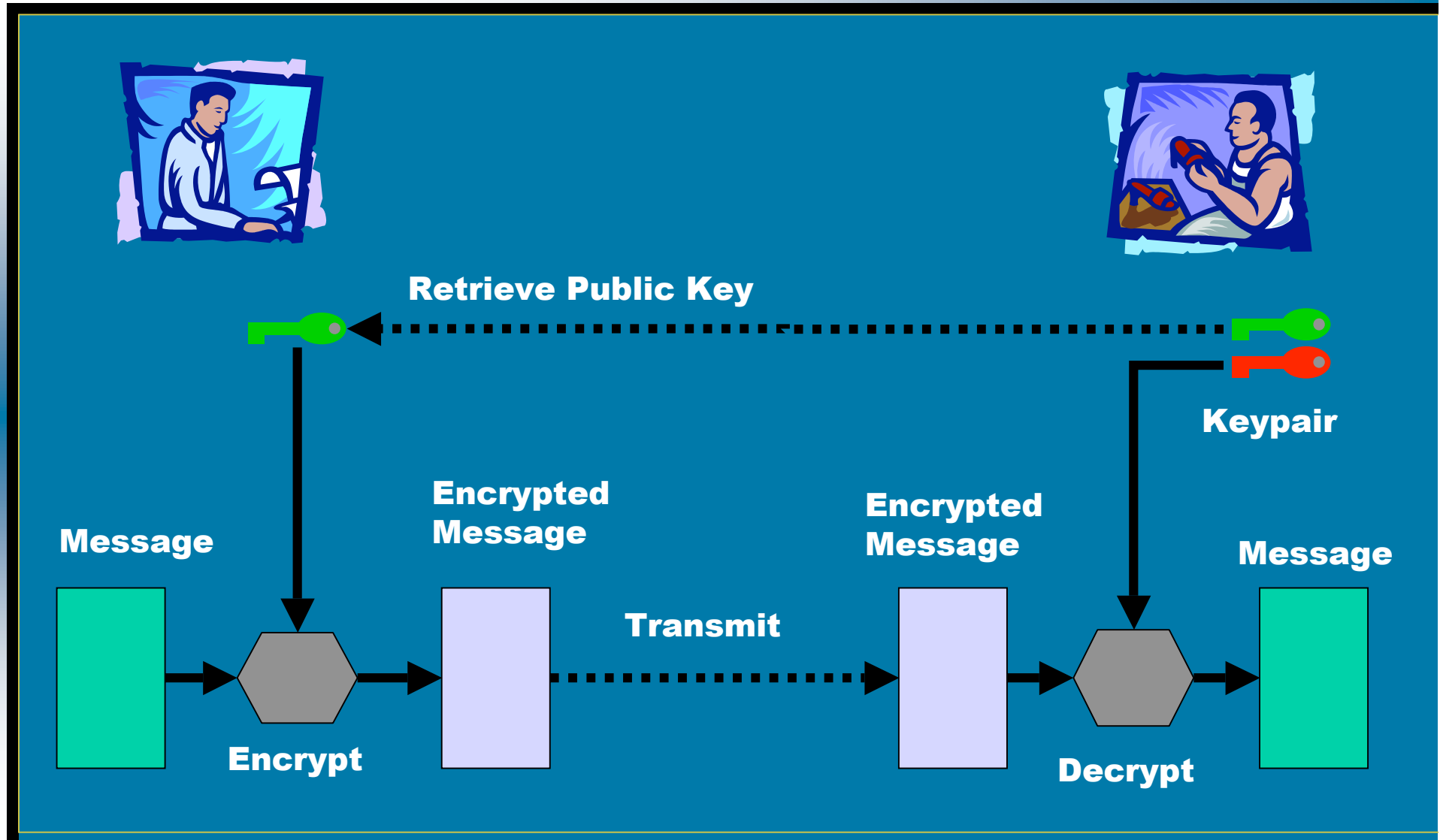
- ◆ Cryptography and PKI Overview
- ◆ APNIC CA project
- ◆ Benefits and costs
- ◆ Project plans
- ◆ Future developments
- ◆ References
  
- ◆ Questions?

# Cryptography - Terms

- ◆ Public key cryptography
  - ◆ Cryptography technique using different keys for encoding and decoding messages
- ◆ Keypair
  - ◆ Private key and public key, generated together, used in public key cryptography
- ◆ Encryption/Decryption
  - ◆ To encode/decode a message using a public or private key

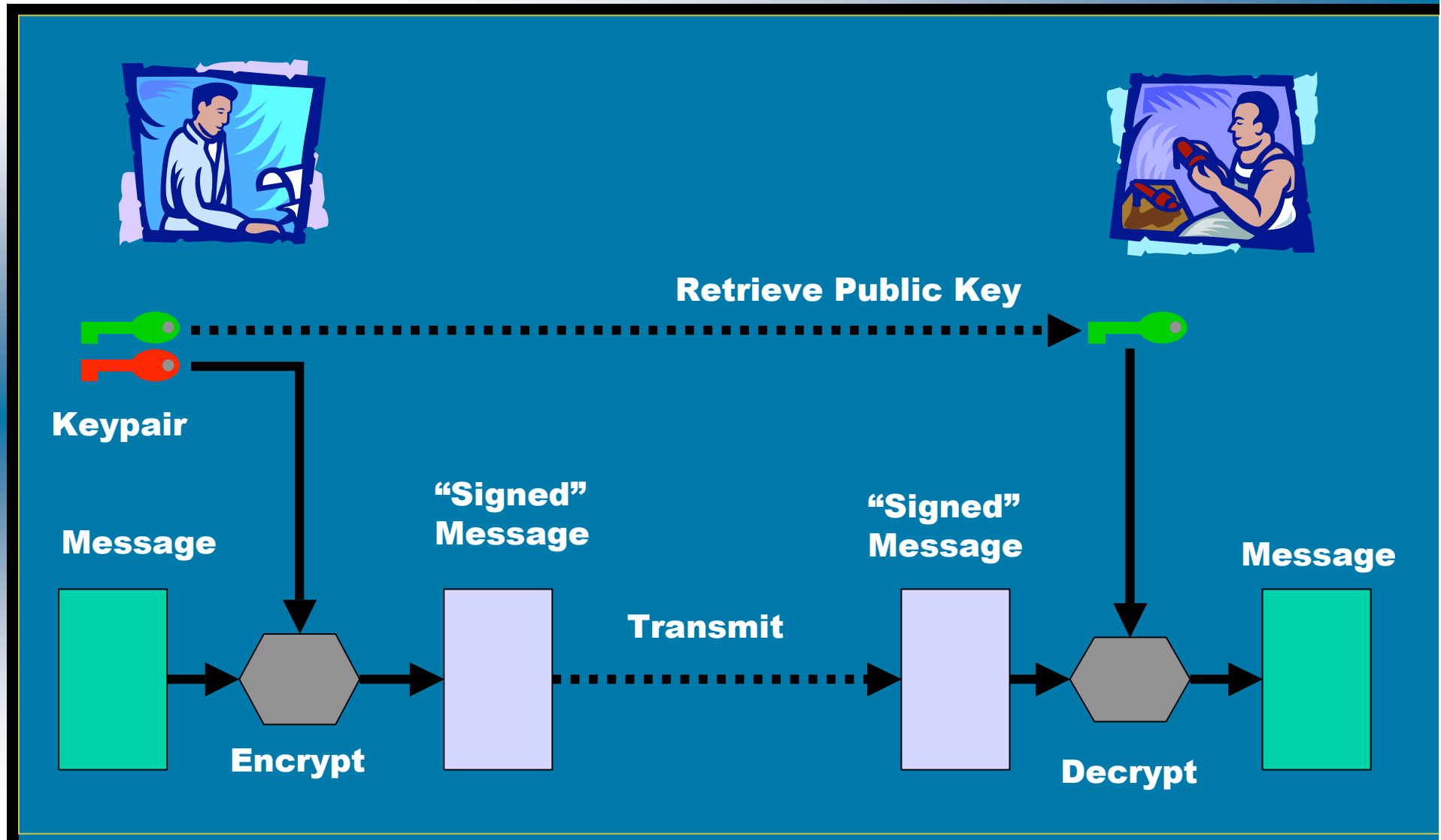
# Public Key Cryptography

- *Encryption*



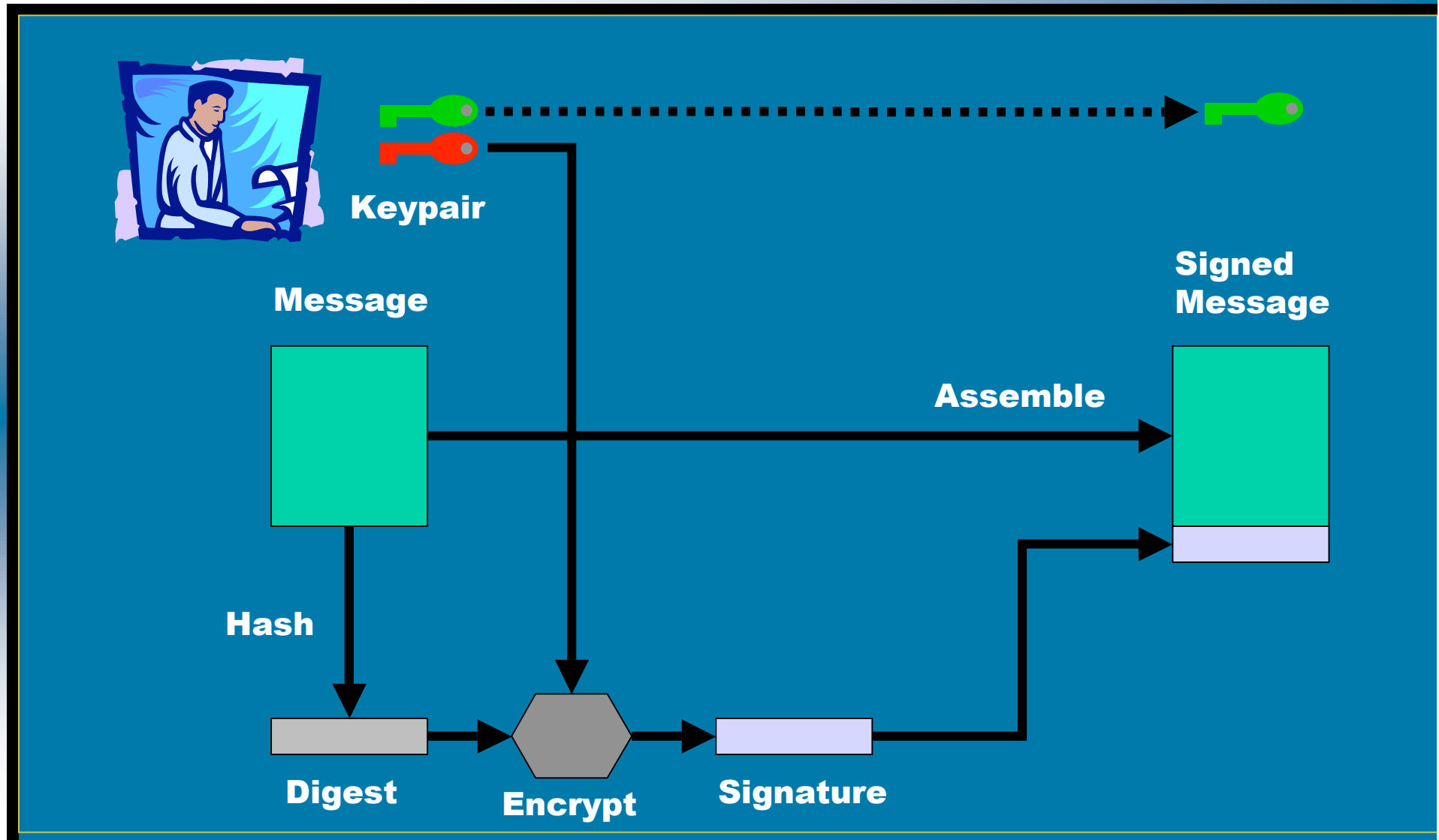
# Public Key Cryptography

- *Encryption*



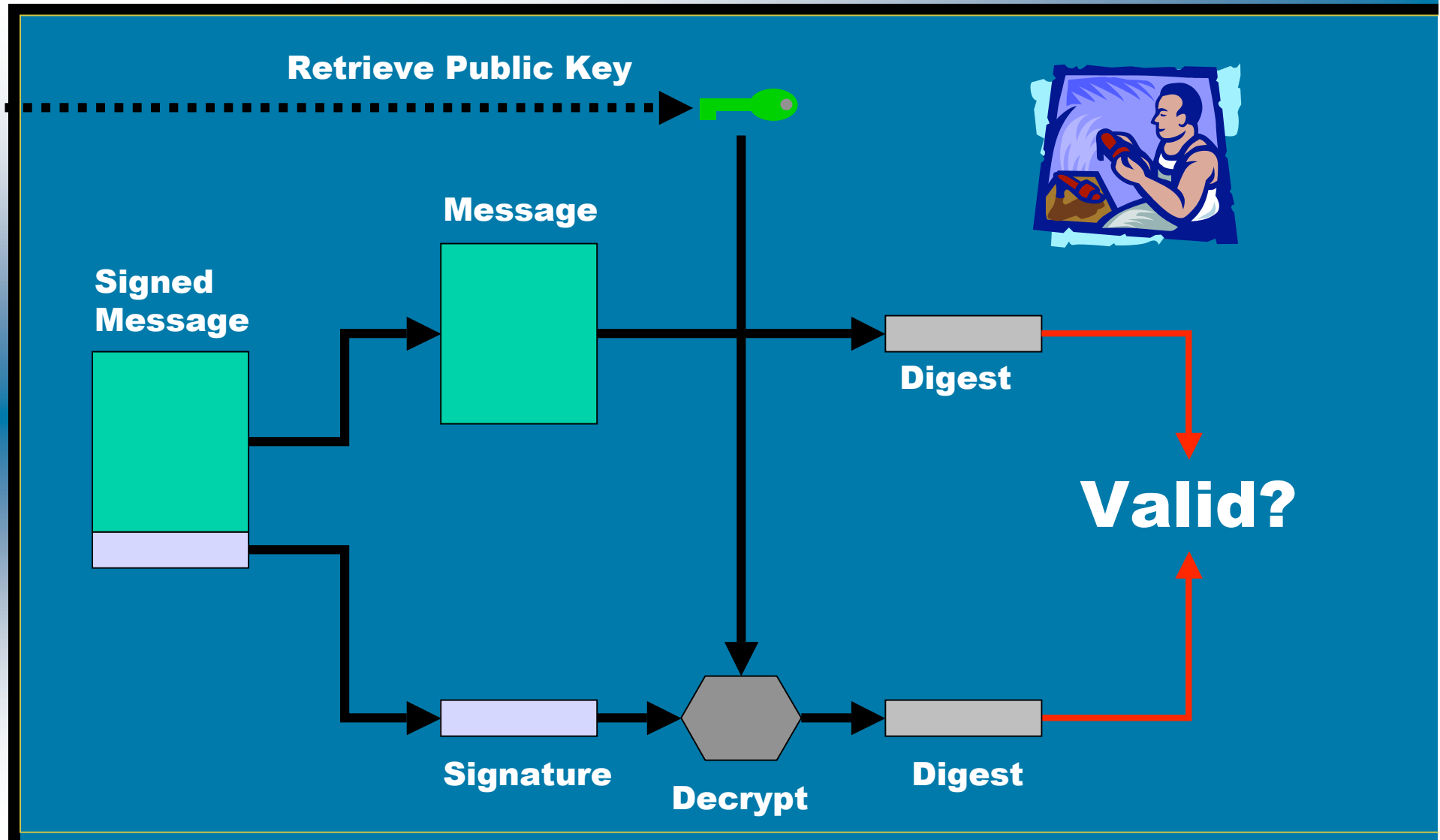
# Public Key Cryptography

- *Digital Signature*



# Public Key Cryptography

- *Digital Signature*



# PKI - Terminology

- ◆ Public Key Infrastructure (PKI)
  - ◆ Administrative structure for support of public key cryptography
- ◆ Public Key Certificate (Digital Certificate)
  - ◆ Document linking a Public Key to an identity, signed by a CA, defined by X.509
- ◆ Certificate Authority (CA)
  - ◆ Trusted authority which issues digital certificates



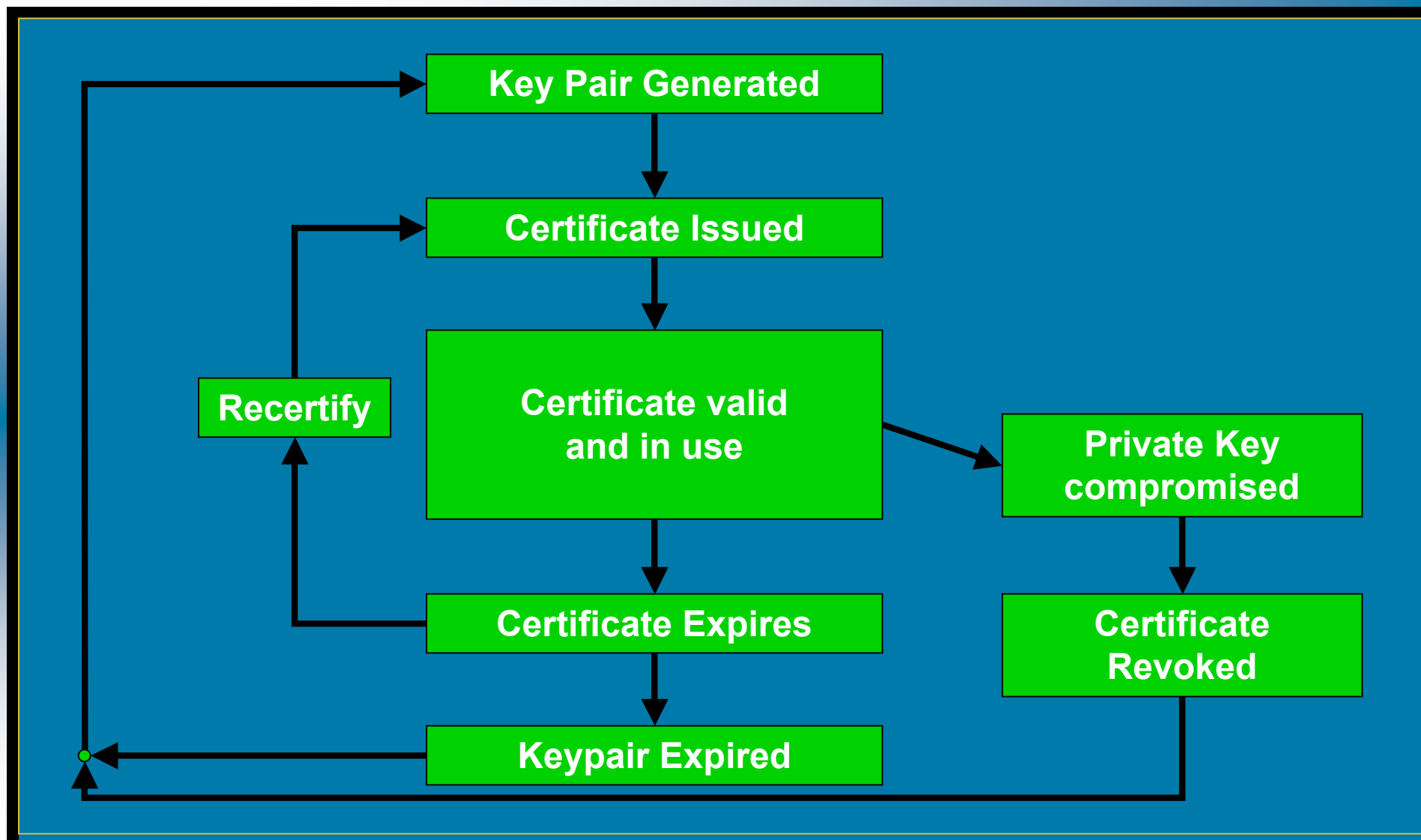
# Digital Certificates

- ◆ A digital certificate contains:
  - ◆ Identity details
    - ◆ eg Personal ID, email address, web site URL
  - ◆ Public key of identity
  - ◆ Issuer (Certification Authority)
  - ◆ Validity period
  - ◆ Attributes
- ◆ The certificate is *signed* by the CA

# Digital Certificate - Example

```
Certificate ::= SEQUENCE {  
    tbsCertificate          TBSCertificate,  
    signatureAlgorithm      AlgorithmIdentifier,  
    signature               BIT STRING  
}  
  
TBSCertificate ::= SEQUENCE {  
    version                 [0] EXPLICIT Version DEFAULT v1,  
    serialNumber            CertificateSerialNumber,  
    signature               AlgorithmIdentifier,  
    issuer                  Name,  
    validity                Validity,  
    subject                 Name,  
    subjectPublicKeyInfo    SubjectPublicKeyInfo,  
    issuerUniqueID          [1] IMPLICIT UniqueIdentifier OPTIONAL,  
    subjectUniqueID         [2] IMPLICIT UniqueIdentifier OPTIONAL,  
    extensions              [3] EXPLICIT Extensions OPTIONAL  
}
```

# Digital Certificate - Lifecycle



# APNIC CA - Why?

- ◆ In response to
  - ◆ Membership concern for greater security
    - ◆ Confidential info exchange with APNIC
    - ◆ Is my database transaction secure?
    - ◆ Whose prefixes do you accept?
  - ◆ Internet community interest in security, PKI, digital certificates
    - ◆ e.g. rps-auth
    - ◆ IETF working group: PKIX



# APNIC CA - Overview

- ◆ Certificate issued to APNIC member
  - ◆ Corresponds to *Membership* of APNIC
  - ◆ Provides uniform mechanism for all security needs, such as:
    - ◆ Encryption and signature of email with APNIC
    - ◆ Authentication of access to APNIC web site
    - ◆ Secure maintainer mechanism for APNIC database
    - ◆ Future authorisation mechanism for Internet resources
    - ◆ Authentication of resource custodianship

# APNIC CA - Benefits/Costs

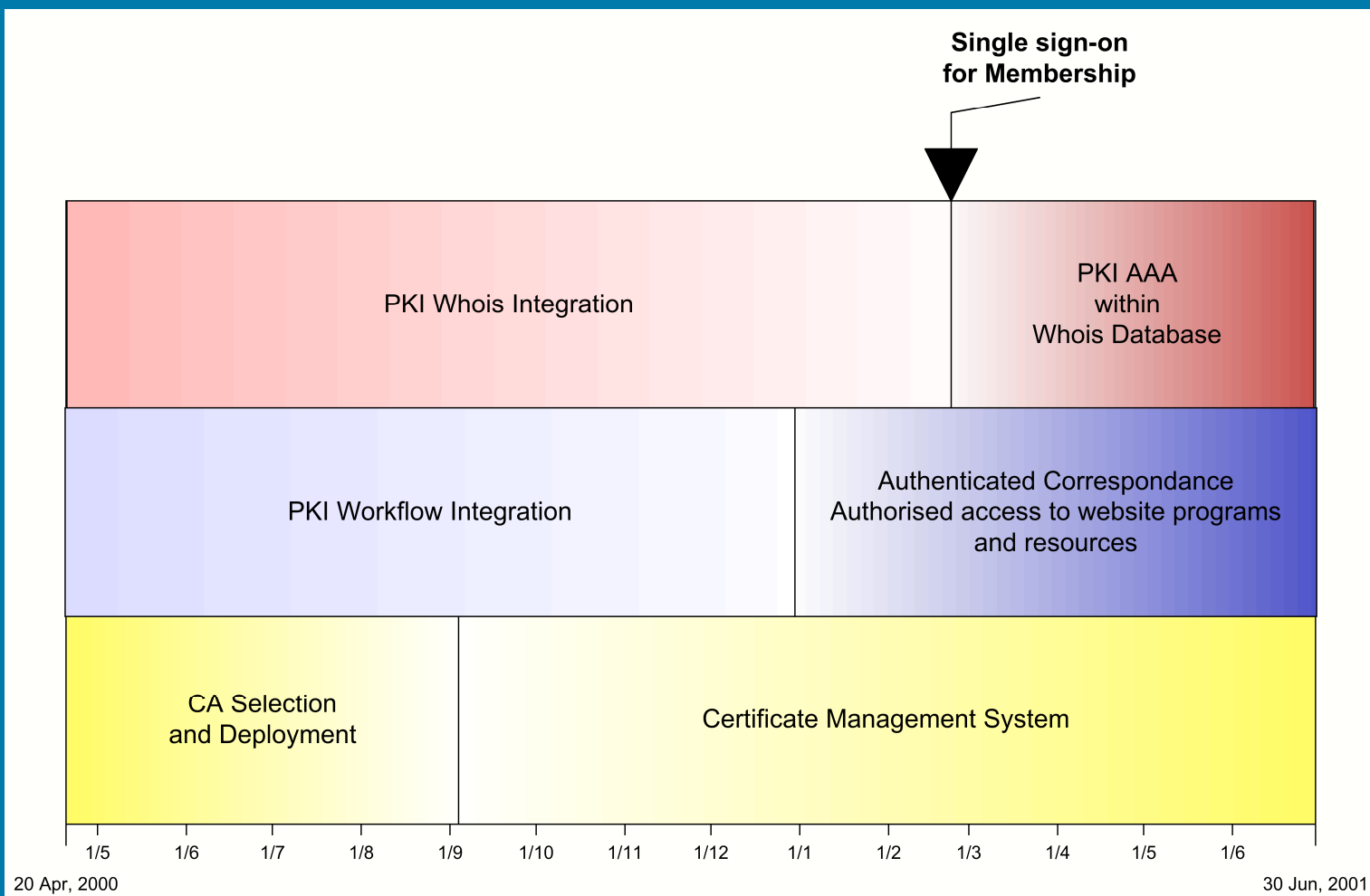
## ◆ Benefits

- ◆ Uniform industry-standard mechanism for “single password” security, authentication and authorisation
- ◆ Strong public key cryptography, end-to-end

## ◆ Costs

- ◆ Server and client software
- ◆ Change to current procedures
- ◆ New policies
- ◆ Establishment: software purchase and/or development

# APNIC CA - Roadmap





# APNIC CA - Timeline

Scoping project	Oct 1999 - Jan 2000
Phase 1	Apr – Nov 2000
Phase 2	Jan – Jun 2001





# APNIC CA – Phase 1 Timeline

Requirements Document	April – May
Programming and Testing	May – Sep
Initial deployment	Sep - Nov

# APNIC CA - Scoping Project

- ◆ October 1999 - January 2000
- ◆ Objectives
  - ◆ Analyse impact of introducing PKI
  - ◆ Provide focus for discussions
  - ◆ Raise awareness of PKI in general
- ◆ Conclusions
  - ◆ Significant benefits for members' security
  - ◆ Growing standards support for PKI
  - ◆ See: <http://www.apnic.net/ca>

# APNIC CA – Phase 1

- ◆ April – November 2000
- ◆ Deliverables
  - ◆ Tender and selection of CA software
  - ◆ Policies for use of APNIC Certificates
  - ◆ Procedures for issuance and revocation of Identity certificates to members
  - ◆ Browser and deployment issues analysis
  - ◆ Issue trial certificates at APNIC Meeting October 2000
  - ◆ Risk Analysis



# APNIC CA – Phase 2

- ◆ January – June 2001
- ◆ Deliverables
  - ◆ Certificates used for website access control
  - ◆ Support for X509 certificates in whois database
  - ◆ Strong encryption for member correspondence
  - ◆ Investigation of use of Attribute Certificates with resource allocation

# APNIC CA - Future

- ◆ Generalised CA function
  - ◆ APNIC Certificates may be used for general purposes
  - ◆ Requires tight policy and quality framework for APNIC certificates to be trusted
- ◆ Hierarchical certification
  - ◆ APNIC Members may use their certificates to certify their own members or customers
  - ◆ May be applicable for ISPs and NIRs

# APNIC CA - Future

- ◆ Public Key Certificates
  - ◆ X.509 certificate linking a Public Key to an identity, issued by CA
- ◆ Attribute Certificates
  - ◆ X.509 certificate linking Attributes to an identity, issued by CA or other authority
  - ◆ Provides *authorisation*, rather than *authentication*, information
  - ◆ Not yet widely deployed or supported
  - ◆ May be extended to carry resource allocation information

# APNIC CA - Future

- ◆ Resource certification
  - ◆ For verification of resource allocations by RIRs
  - ◆ Currently under discussion in IETF PKIX working group
    - draft-clynn-bgp-x509-auth-01.txt
    - “X.509 Extensions for Authorization of IP Addresses AS Numbers, and Routers within an AS”*
  - ◆ APNIC watching developments

# APNIC CA - Consultation

- ◆ Mailing list open after Apricot2000
  - ◆ [pki-wg@lists.apnic.net](mailto:pki-wg@lists.apnic.net)
  - ◆ <http://www.apnic.net/wilma-bin/wilma/pki-wg>
- ◆ Further developments
  - ◆ See: <http://www.apnic.net/ca>



- ◆ IETF PKIX drafts:

draft-ietf-pkix-roadmap-04.txt

*"Internet X.509 Public Key Infrastructure PKIX Roadmap"*

draft-clynn-bgp-x509-auth-01.txt

*"X.509 Extensions for Authorization of IP Addresses AS Numbers, and Routers within an AS"*

draft-ietf-pkix-ac509prof-01.txt

*"An Internet Attribute Certificate Profile for Authorization"*

- ◆ <http://www.ietf.org/html.charters/pkix-charter.html>

# Questions?