Digital Certificates

Nigel Pentland

nigel.pentland@eu.nabgroup.com

nigel@nigelpentland.net

Guide Share Europe, April 2005

National

Digital Certificates

What are Digital Certificates all about?

How can we make use of them?

Examples relating to WebSphere

Some useful tools to assist us along the way

National

The Russian Postal System Puzzle †

- Boris in Moscow
- Natasha in St. Petersburg
- Boris has a ring and wants to get engaged as quickly as possible
- Strong box with a hasp to which a number of padlocks could be attached
- Together they hatched a clever scheme to get the precious jewel from Moscow to St. Petersburg securely – how did they do it?

† Taken from ‘In Code’ by Sarah Flannery

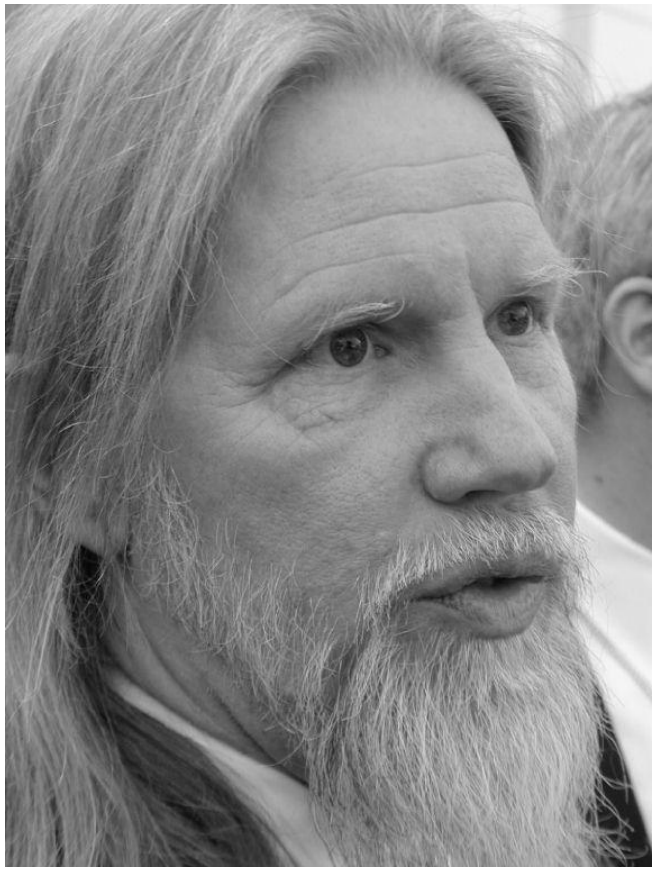
Cryptography

- Symmetric cryptography has been around thousands of years
  hieroglyphs
  Caesar cipher
  The Cipher of Mary Queen of Scots
  Le Chiffre Indéchiffrable
  http://www.simonsingh.com/
  excellent CD-ROM free download…
- Asymmetric is relatively very new !
- Latest development - Secret Sharing (polynomial or hyperplanes)

Coming up with the idea

Concept:

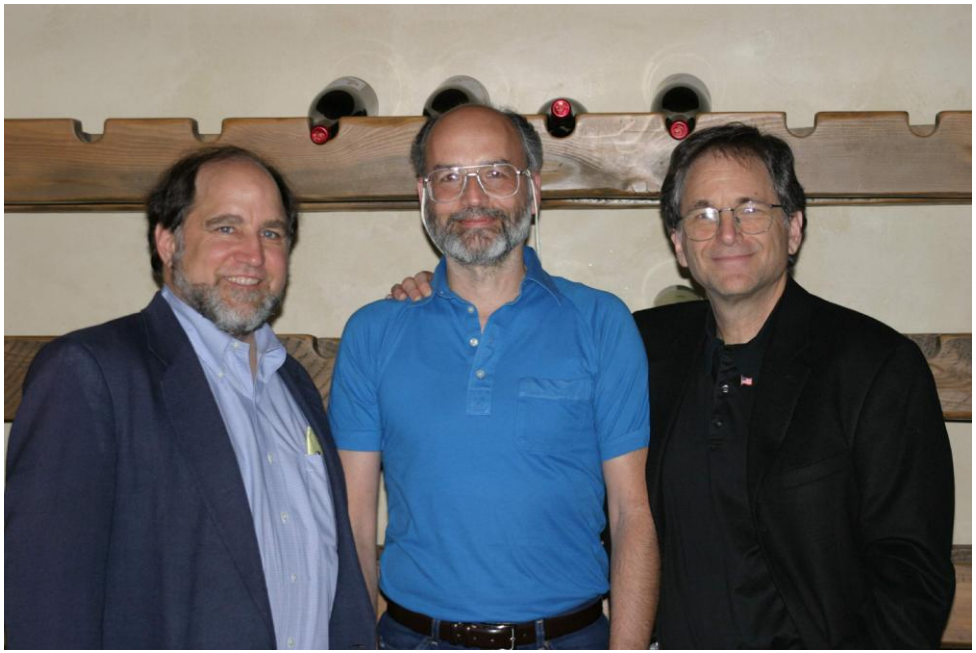
- James Ellis – GCHQ – allegedly – 1970
- Witfield Diffe & Martin Hellman – 1977



Making the idea work

Mathenatical implementation:

- **RSA**
  U.S. Patent: 4,405,829
  Filed: December 14, **1977**
  Issued: September 20, **1983**
- Ron Rivest,
  Adi Shamir,
  Len Adleman
- RSA Patent expired
  21st Sept **2000**



National

Crypto – by Steven Levy

‘Steven Levy’s *Crypto* is the story of the unlikely, not to say downright motley, crew of mathematical and computer revolutionaries who broke NSA’s and GCHQ’s cryptographic monopoly, and in so doing helped to launch the internet revolution … an unparalleled chronicle of a remarkable group of people who have affected all of our lives’

Stephen Budiansky, *Daily Mail*

Jim Bidzos

Asymmetric cryptography

- Works by using pairs of keys with special properties (i.e. a one way trap door function)
- If you encrypt with one then you can only decrypt using partner
- By convention we refer to these as **public** and **private** keys

public certificate

private key

Digital Certificate Standards

- PKCS10 – Certification Request Syntax Standard
- PKCS11 – Cryptographic Token Interface Standard
- PKCS12 – Personal Information Exchange Syntax Standard
- RFC3280 – Internet X.509 Public Key Infrastructure
- ASN.1 – Abstract Syntax Notation 1
  note: this includes Object Identifiers or OIDs (RFC 3061)
  http://asn1.elibel.tm.fr/en/index.htm

RFC3280

```
 …<snip>
KeyUsage ::= BIT STRING {
             digitalSignature        (0),
             nonRepudiation          (1),
             keyEncipherment         (2),
             dataEncipherment        (3),
             keyAgreement            (4),
             keyCertSign             (5),
             cRLSign                 (6),
             encipherOnly            (7),
             decipherOnly            (8) }
  <snip>…
```

De facto Notation

Asymmetric cryptography

Alice & Bob

Ron Rivest

Alice and Bob After Dinner Speech
Given by John Gordon in Zurich 1984
http://www.conceptlabs.co.uk/alicebob.html

Who generates certificates?

- Trusted 3rd party ?
- Internal Certificate Authority (i.e. CA)

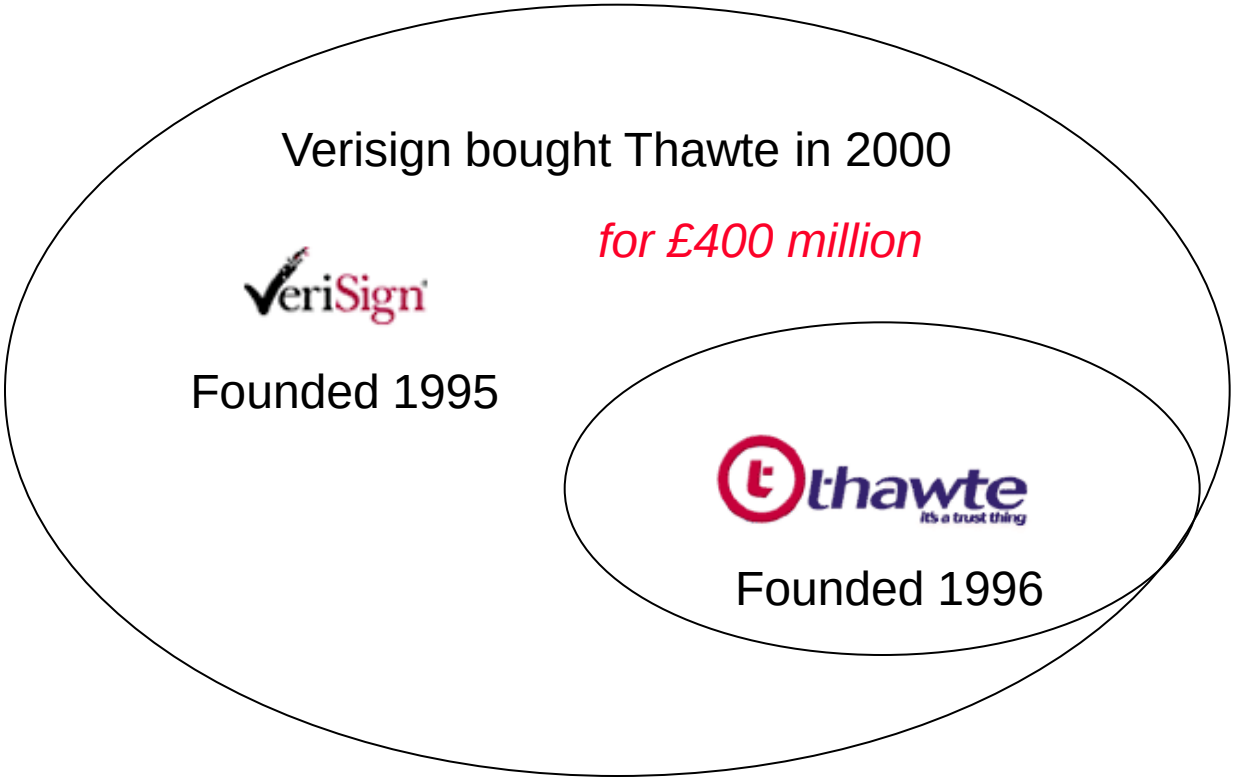
Deciding factors are:

Trust

Cost

National

Trusted 3rd Parties



Plus lots of others too…

National

Soyuz TM-34 – April 2002

paid £13 million to be 2nd space tourist

Soyuz Commander	Yuri Gidzenko	Russia
Flight Engineer	Roberto Vittori	Italy
Tourist	**Mark Shuttleworth**	**South Africa**

Internal Certificate Authority (CA)

- RACF – i.e. RACDCERT command
  ICSF – Integrated Cryptographic Support Facility – beware backup !
- PKI Services – i.e. RACF bolt-on
- GSK Toolkit (aka ikeyman)
  Note: multiple versions !
- OpenSSL

RSA BSAFE®

National

Digital Certificates

What are Digital Certificates all about?

How can we make use of them?

Examples relating to WebSphere

Some useful tools to assist us along the way

National

Encryption and or Authentication

This is done using a **framework** defined by one of the following standards:

- SSL (probably v3) Secure Sockets Layer
- TLS Transport Layer Security

- Cryptographic client server handshake protocol

- **SSL** and **TLS** - Designing and Building Secure Systems by Eric Rescorla

Simple Client Server

- **Server has a certificate**
  typically one issued by a Certificate Authority
- **Client needs to establish trust relationship**
  typically it needs to trust the issuing Certificate Authority
- Unless that is **SGC** is being used – Server Gated Cryptography

Mutual or Client Authentication

- SSL or TLS is used to authenticate both ways
- First the server is authenticated as before
- Then the client is authenticated to the server in the same way
- Exactly how this happens depends on the protocol being used
  - Hence MQ operates differently to WAS using only labels, where WAS also uses Common Name (i.e. URL) defined in the certificate

Digital Certificates

What are Digital Certificates all about?

How can we make use of them?

Examples relating to Websphere

Some useful tools to assist us along the way

National

Example 1- generate a Unix MQ Manager certificate

```
//RACF EXEC PGM=IKJEFT01
//SYSTSPRT DD SYSOUT=A,HOLD=YES
//SYSTSIN DD *
 PROFILE NOPREFIX
 RACDCERT GENCERT +
  ID(USERID) +
  SUBJECTSDN(CN('ibmwebspheremqmanager') +
             OU('Technology') +
              O('National Australia Group Europe') +
              L('Glasgow') +
             SP('Scotland') +
              C('GB')) +
  SIZE(1024) +
  NOTBEFORE(DATE(2004-08-25)) +
  NOTAFTER(DATE(2006-08-25)) +
  WITHLABEL('ibmwebspheremqmanager') +
  SIGNWITH(CERTAUTH LABEL('TEST-MQ-ROOT')) +
  KEYUSAGE(HANDSHAKE,DATAENCRYPT)
/*
```

Example 2 – generate a z/OS MQ Manager certificate

```
//RACF EXEC PGM=IKJEFT01
//SYSTSPRT DD SYSOUT=A,HOLD=YES
//SYSTSIN DD *
 PROFILE NOPREFIX
 RACDCERT GENCERT +
  ID(MQUSERID) +
  SUBJECTSDN(CN('ibmWebSphereMQ1234') +
             OU('Technology') +
              O('National Australia Group Europe') +
              L('Glasgow') +
             SP('Scotland') +
              C('GB')) +
  SIZE(1024) +
  NOTBEFORE(DATE(2004-10-01)) +
  NOTAFTER(DATE(2006-10-01)) +
  WITHLABEL('ibmWebSphereMQ1234') +
  SIGNWITH(CERTAUTH,LABEL('TEST-MQ-ROOT')) +
  KEYUSAGE(HANDSHAKE DATAENCRYPT)
/*
```

Example 3 – generate SSL Server certificate

```
//RACF EXEC PGM=IKJEFT01
//SYSTSPRT DD SYSOUT=A,HOLD=YES
//SYSTSIN DD *
 PROFILE NOPREFIX
 RACDCERT GENCERT +
  ID(USERID) +
  SUBJECTSDN(CN('was.domain.com') +
             OU('Technology') +
              O('National Australia Group Europe') +
              L('Glasgow') +
             SP('Scotland') +
              C('GB')) +
  SIZE(1024) +
  NOTBEFORE(DATE(2004-10-01)) +
  NOTAFTER(DATE(2006-10-01)) +
  WITHLABEL('was label') +
  SIGNWITH(CERTAUTH,LABEL('TEST-ROOT')) +
  KEYUSAGE(HANDSHAKE DATAENCRYPT)
/*
```


National

Example 4 – certificate renewal – step 1

```
//RACF EXEC PGM=IKJEFT01
//SYSTSPRT DD SYSOUT=A,HOLD=YES
//SYSTSIN DD *
 PROFILE NOPREFIX
 RACDCERT ID(USERID) GENREQ(LABEL('TEST')) +
          DSN('USERID.PKCS10.REQ')
/*
```

Example 5 – certificate renewal - step 2

```
//RACF EXEC PGM=IKJEFT01
//SYSTSPRT DD SYSOUT=A,HOLD=YES
//SYSTSIN DD *
 PROFILE NOPREFIX
 RACDCERT GENCERT ('USERID.PKCS10.REQ') +
  ID(USERID) +
  NOTBEFORE(DATE(2004-11-08)) +
  NOTAFTER(DATE(2004-11-15)) +
  WITHLABEL('TEST') +
  SIGNWITH(CERTAUTH LABEL('TEST-ROOT'))
/*
```

Digital Certificates

What are Digital Certificates all about?

How can we make use of them?

Examples relating to WebSphere

Some useful tools to assist us along the way

National

Useful Tools

- base64
- CertMgr
- dumpasn1
- ikeyman
- MMC
- Mozilla
- OpenSSL
- racf.co.uk

base64

```
base64  --  Encode/decode file as base64.  Call:
            base64 [-e / -d] [options] [infile] [outfile]

Options:
            --copyright         Print copyright information
            -d, --decode        Decode base64 encoded file
            -e, --encode        Encode file into base64
            -n, --noerrcheck    Ignore errors when decoding
            -u, --help          Print this message
            --version           Print version number

by John Walker
http://www.fourmilab.ch/
```

CertMgr

- Now part of the Microsoft .NET Framework SDK tools
- Useful both as a GUI and command line tool
- **As a GUI it gives a shortcut way to fire up MS Certificate Manager**
- Command line example that lists certificates for current user

```
certmgr /s my
```

dumpasn1

- Very useful command line tool
- Peter Gutmann - Professional Paranoid
- http://www.cs.auckland.ac.nz/~pgut001/dumpasn1.c
  multi-platform source code
- Works on binary certificate files, namely DER encoded

  DER: Distinguished Encoding Rules for ASN.1, as defined in X.509

ikeyman

- Two main versions, one does kdb (aka CMS) and the other does jks (Cryptographic Message Standard – RFC 3852)
- **kdb** - D:\Program Files\ibm\gsk5\bin\gsk5ikm.exe
  sth – associated password stash file
- **jks** - D:\Program Files\WebSphere\AppServer\bin\ikeyman.bat

MMC

- Microsoft Management Console
- **Certificates** is a standard Snap-In
- Useful for managing certificates in a Windows client, or server
- Enables a **local** administrator to administer all certificates within **local** Windows environment

Mozilla

- Netscape or Firefox are particularly useful
- Excellent error reporting in relation to certificates
- They use dedicated certificate repository, not Windows
- **Netscape** allows the user to enable the **NULL** encryption suites
- for example https://mqmanager:1414/ would give option to display certificate

OpenSSL

- Source - http://www.openssl.org/
- Win32 - http://www.shininglightpro.com/products/Win32OpenSSL.html
- Docs - http://www.mkssoftware.com/docs/man1/openssl.1.asp
- Example command
  openssl s_client -connect mqmanager:1414
- Very, very, powerful utility, unable to do it justice on one slide !
- Try using **openssl s_server** to emulate a server in one window
- And then try **openssl s_client** to emulate a client in another …

racf.co.uk

Beware IRRDBU00 only unloads top level Common Name

- **RACF94** List of Certificates by user and label
- RACF95 List of Certificates (unsorted)
- RACF96 List of Key Rings
- RACF97 List of Mappings
- RACF98 List of Certificate Trusts
- **RACF99** List of Certificates (sorted by expiry date)
- **RACF101** List of Certificates (sorted by month of expiry)

Digital Certificates

The End.

National