PKI, Past, Present and Future

David Chadwick

Contents

- PKI Past
- PKI Present
- PKI Future

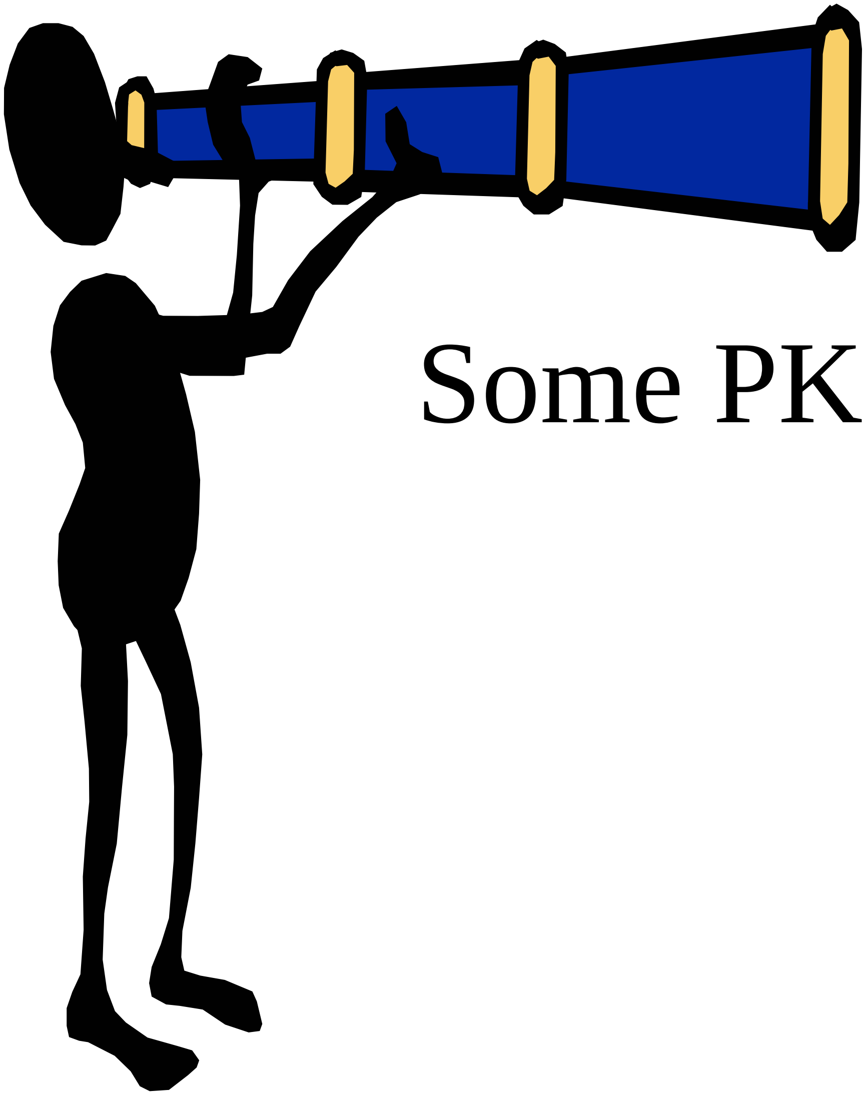
My CPS

Remove liability from yourself

Note Well

- The contents of this presentation cannot in anyway be construed as representing the views of the author or of his employer or of the Queen of England, and if anything, was encouraged by the conference organisers and the audience

Transfer liability to subjects and relying parties



Some PKI History

X.509 – the Basics

- In 1988 the first version of X.509 was issued
- Very simple in concept
- A certificate binds a **globally unique X.500 distinguished name** to a public key
- So there are just Two Basic Concepts for a CA
- Name Validation
- Key Management

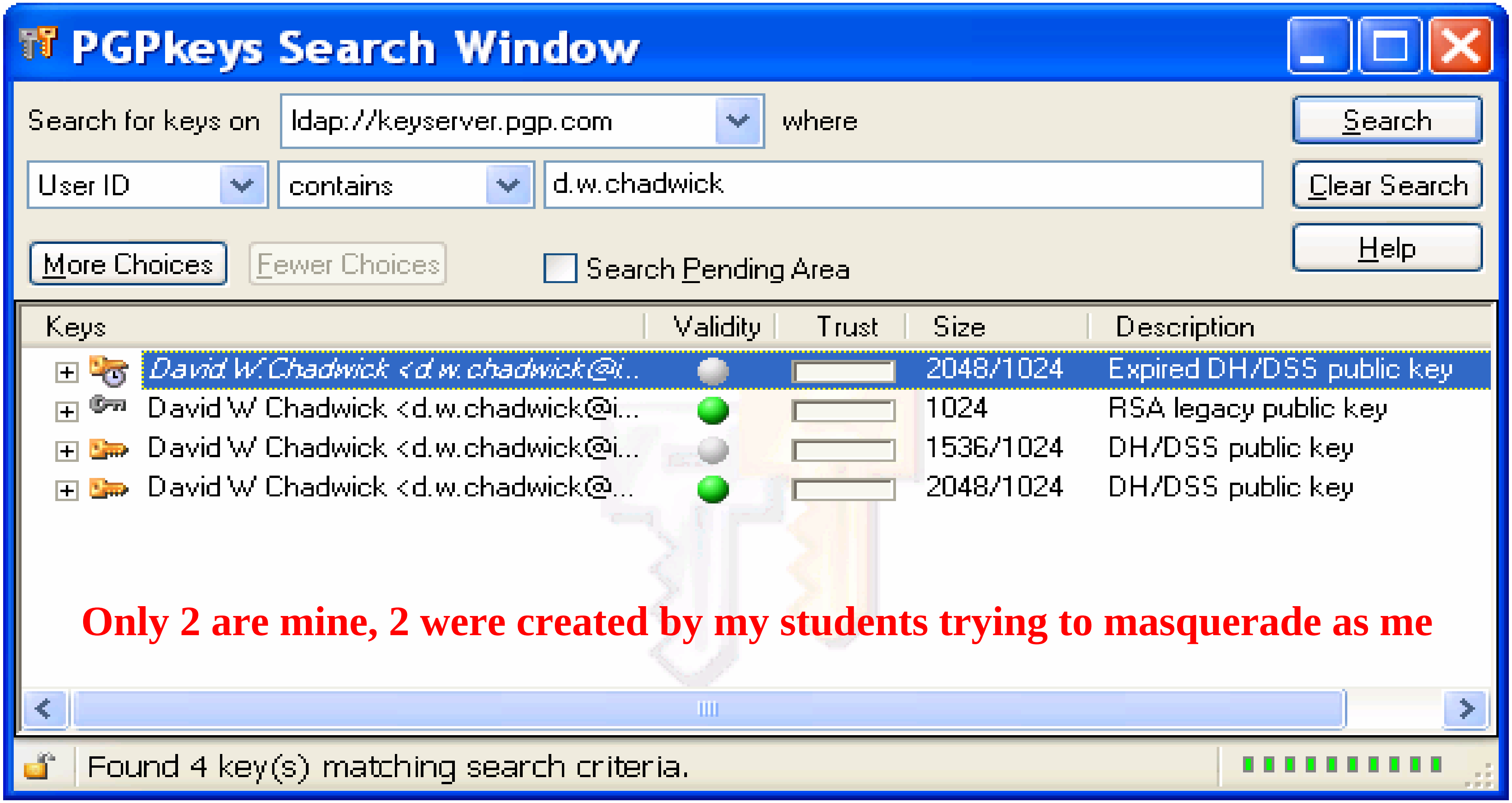
More Basics

- X.509 (88) only envisaged a user needing a single key pair at any one time. This could be used to sign/encrypt everything
  - Pragmatics of losing a signing key and a decryption key soon led to a rethink on key pairs
  - But some systems are still happy with single key pairs
- Globally Unique Names would be allocated by Naming Authorities starting from ISO 9594 which defines country codes based on ISO 3166 *Codes for the representation of names of countries*
- Each country then creates its own naming authority or authorities

Why do we need Global Names/IDs ?

- To make sure that allocated names are globally unique. Local names by definition are not.
- Cant we simply use the key ID ?
- Yes, but names outlive keys (usually!), and key IDs are not exactly user friendly (have you ever tried using SPKI?). How do we link a key ID to its owner e.g. a real person?
- The purpose of a CA should be to authenticate an **existing** name (not to allocate it or register it) and then bind it to the current temporary public key. Then people who already know the name, automatically know whose key it is.
- Look what happens when we allow anyone to act as a CA and to allocate any names they choose

PGP Key Search for d.w.chadwick



Search for keys on ldap://keyserver.pgp.com where

User ID contains d.w.chadwick

☐ Search Pending Area

Keys	Validity	Trust	Size	Description
David W Chadwick <d.w.chadwick@i...	○		2048/1024	Expired DH/DSS public key
David W Chadwick <d.w.chadwick@i...	●		1024	RSA legacy public key
David W Chadwick <d.w.chadwick@i...	○		1536/1024	DH/DSS public key
David W Chadwick <d.w.chadwick@...	●		2048/1024	DH/DSS public key

Only 2 are mine, 2 were created by my students trying to masquerade as me

Found 4 key(s) matching search criteria.

Cop Out

- Most CAs, probably because they were directed by their lawyers, chose not to use pre-existing globally unique names for their subjects, but rather to allocate local names themselves, often based on their own name
- This is probably part of removing all liability from the CA, so that it cant be sued
- Interestingly, Verisign Class 1 certs do use globally unique names (email addresses) and do verify them during the registration process (but more about that later)

Use of Global Names

- But doesn’t the use of global names lead to Identity theft?

Identity Theft

- Protection of identity should NOT be based on having secret identities
  - This is secrecy by obscurity, which is a BAD thing
  - How can George Bush keep his identity secret?
- Identity protection should be based on having strong credentials that are very hard to steal e.g.
  - Really secret secrets (and not my mother's maiden name)
  - Not biometrics (which are public) but rather the live capture of biometrics
  - Hardware tokens rather than software tokens
- And if someone steals my credentials I should easily know about it
  - Like loss or theft of my mobile phone or my credit card

Global Naming in Practice

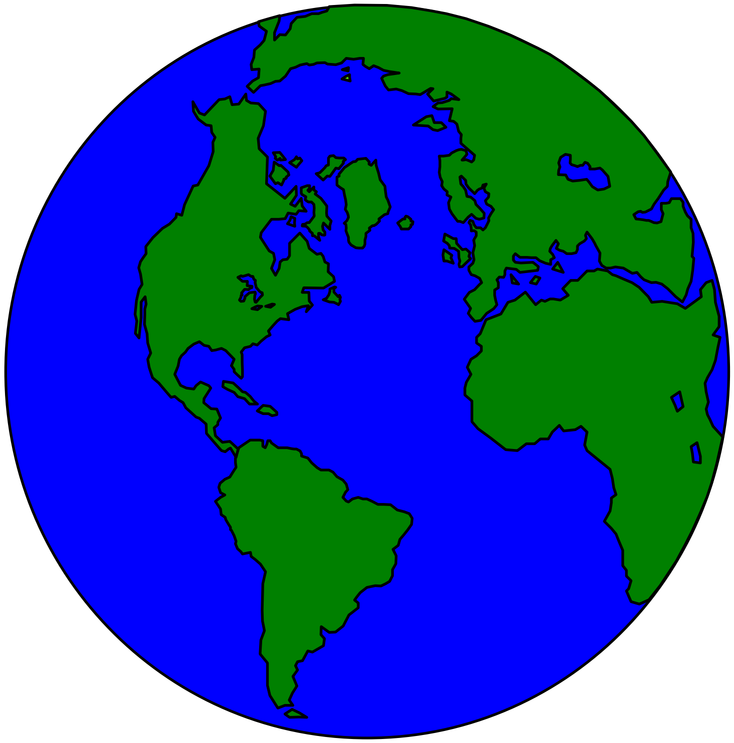
- This worked well in some cases e.g. the UK
  - BSI created British Standard BS 7453 Part 1. Procedures for UK Registration for Open System Standards Part 1: Procedures for the UK Name Registration Authority
  - Gave procedures for registering OIDs, X.500 DNs and X.400 O/R names
  - Allowed all UK public and limited companies to use their existing registered company names and numbers to provide default X.500 DNs and OIDs without needing to re-register or pay any additional fees
  - OIDs are 1.2.826.0.*n* and DNs c=gb,o=*registered name* Ltd
  - All UK universities registered their preferred X.500 DNs with BS 7453 at a cost of £150 each
- IANA set up a global OID register for anyone via its web stie http://www.iana.org/cgi-bin/enterprise.pl

It should have worked well in all cases

- Because every country already has several unique national naming and numbering schemes
  - E.g. National insurance numbers, national company names, national ID cards, national health numbers, national driving licenses etc. etc.
- Because the Internet already has a global naming scheme (called the DNS)
- Because various international schemes also already exist
  - E.g. IATA, DUNS, BICC

But there were Problems

- The US (as always ---
- Naming International Organisations
  - ISO refused to set up a naming register for them
  - All ISO had to do was edit IS 6532 (Structure for the Identification of Organisations)
  - But who would pay to run the service?
- Who would operate a global directory service in which to locate certificates and CRLs ?



Examples of previous Standards problems with the US

- Overheard at one ISO meeting “Why don’t you guys use standard paper sizes like we do in the US”
  - have they never heard of A4?
- Why don’t you guys use standard mobile phone frequencies like we do
  - have they never heard of GSM?
- Why cant everyone use ASCII standard characters to write their names like we in the US do
  - have they never heard of accents and different character sets like Greek, Cyrillic, Arabic, Chinese, Kanji??

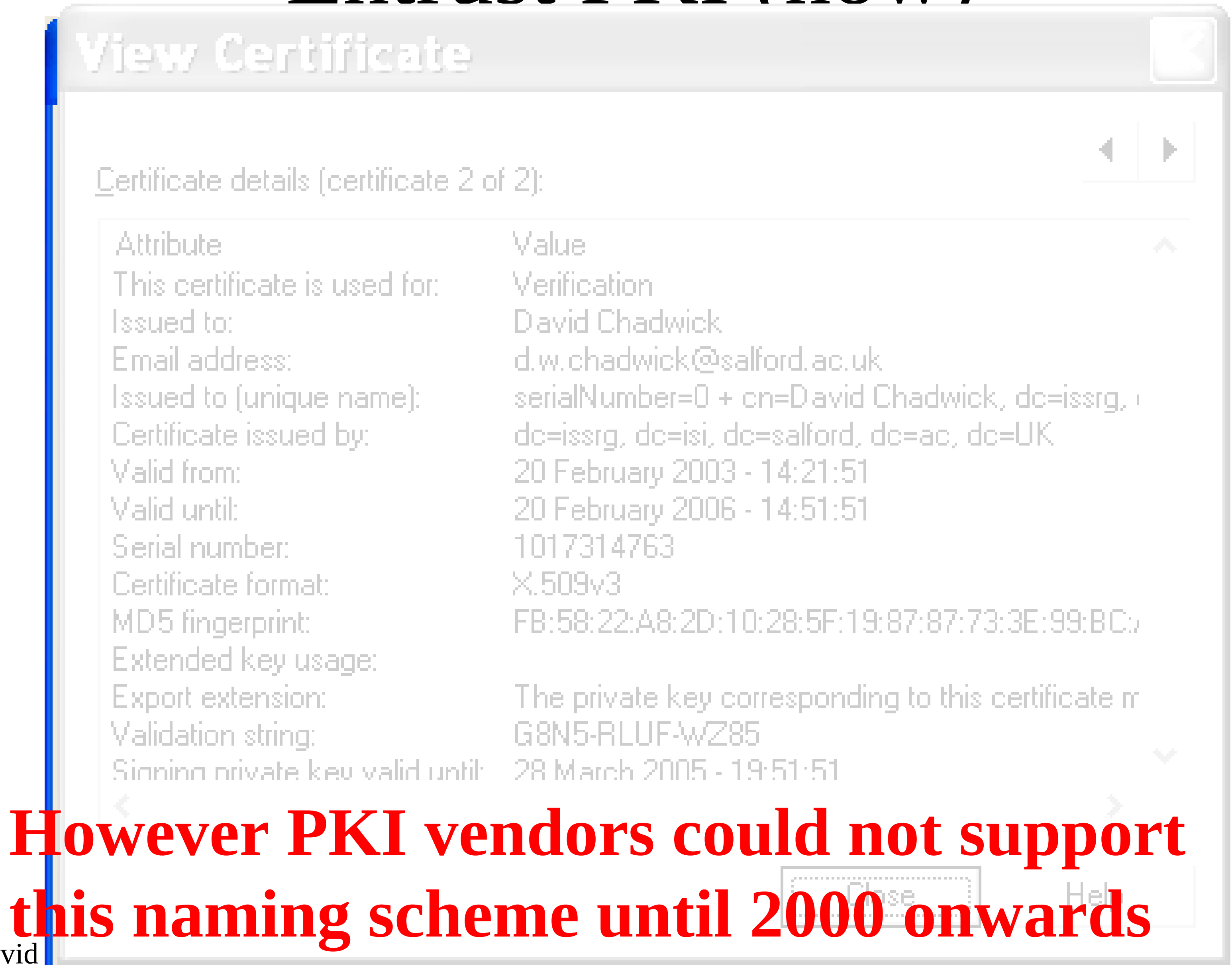
US Naming

- ANSI coerced all commercial organisations to register at the state level, creating names such as:
  - C=US, St=Maryland, O=IBM,etc.
- By charging $2,500 for national registration
- But the various US states never bothered to create naming authorities, so organisations found it impossible to get globally unique distinguished names for a fair price
- Consequence. Everyone set up their directory names with a root local name of O=My Company Name
  - This was even RECOMMENDED by Netscape

Global Naming Easily Solved

- Global naming is not difficult, otherwise how would email work?
- One Solution. Leverage the DNS, and create X.500 DNs for certs using the DC attribute type defined in RFC 2247 plus CommonName for the last component
  - E.g. fred@mx.com →cn=fred,dc=mx,dc=com
  - Incidentally, RFC 2247 was published in Jan 1998
- Or use person's full name for CN, and where multiple entities exist with the same name use the Serial Number attribute to differentiate
  - E.g. CN=David Chadwick + Serial Number=1234, dc=salford, dc=ac, dc=uk
  - X.520 was specifically edited to allow for this
- Alternatively, use existing social security numbers, health numbers etc. prefixed by an ISO 3166 country code

This is how we have set up our Entrust PKI (now)



Certificate details (certificate 2 of 2):

Attribute	Value
This certificate is used for:	Verification
Issued to:	David Chadwick
Email address:	d.w.chadwick@salford.ac.uk
Issued to (unique name):	serialNumber=0 + cn=David Chadwick, dc=issrg,
Certificate issued by:	dc=issrg, dc=isi, dc=salford, dc=ac, dc=UK
Valid from:	20 February 2003 - 14:21:51
Valid until:	20 February 2006 - 14:51:51
Serial number:	1017314763
Certificate format:	X.509v3
MD5 fingerprint:	FB:58:22:A8:2D:10:28:5F:19:87:87:73:3E:99:BC:
Extended key usage:	
Export extension:	The private key corresponding to this certificate m
Validation string:	G8N5-RLUF-WZ85
Signing private key valid until:	28 March 2005 - 19:51:51

However PKI vendors could not support this naming scheme until 2000 onwards

Spurious Arguments

- Arguments about how to name nomads, people in blocks of flats or in prisons, on ships etc. are spurious and irrelevant to PKI
- Are we saying we cannot email these people today? Or that they cannot obtain passports, social security numbers etc.
  - Well perhaps yes for people in prison!
- But in general they already have globally unique names (possibly several)
- The important thing for the CA is to **authenticate** the name they already have, **not to allocate it**

A Less Flexible Alternative

- Use the hash of the public key as a globally unique name. Use CN or define a new attribute type for this (say KID) and a rule for creating base64 strings from the hash
- Create DNs of the form
  - KID=34A52F9EB28C… or
  - CN=<KID> 34A52F9EB28C…</KID>[1]
- This solves the certificate chain validation problem, but because it directly links the person's ID to the key, it lacks flexibility in key rollover, and is difficult to identify who the key owner is

[1] Suggested by Frank Siebenlist

PARADISE – a Global X.500 Directory Service

- The EC COSINE funded PARADISE project ran a global X.500 directory service from 1990 to 94
- Funded by DANTE and others until November 1999
- Based on ESPRIT funded Quipu X.500 code developed by UCL between 1985-88
- In its heyday (94-96) Paradise had nearly 2 million entries from over a 1000 organisations connected together by over 600 DSAs
- Note that LDAP servers today still cannot provide an equivalent service, which is why US DoD and others still use X.500 servers to support PKIs

But there were Problems in Paradise

- No one (outside the US) knew which US State directory to look in for organisation entries
- Similarly, US folk typically didn’t know which countries European organisations were in.
  - Is Stella Artois from Belgium, the Netherlands or France?
- So users did not know where to start their directory searches to find remote certificates and CRLs
- The result was inefficient **global** searching of Paradise and poor performance
  - Plus poor admin tools etc. etc. typical from university provided software
- Eventually Paradise had to be switched off because Quipu was not Y2K compliant. Now been replaced by LDAP

LDAP

- ***So far, LDAP has not done a great job of supporting PKI requirements*** Stephen Kent, PKIX Chair

- Some things LDAP can't do
- Can't search for specific certificates or CRLs based on their contents
- Can't retrieve a single CRL or cert from a multi-valued attribute
- Can't always store using V2 userCertificate and retrieve using V3 userCertificate;binary
- In general companies don't make their LDAP information publicly available so can't look up certs or CRLs anyway

Full description in: D.W.Chadwick. "Deficiencies in LDAP when used to support a Public Key Infrastructure", Communications of the ACM, March 2003/Vol 46, No. 3 pp. 99-104.

PKI use of LDAP DNs

- ***So far, PKI has not done a great job of supporting LDAP/X.500 distinguished names***

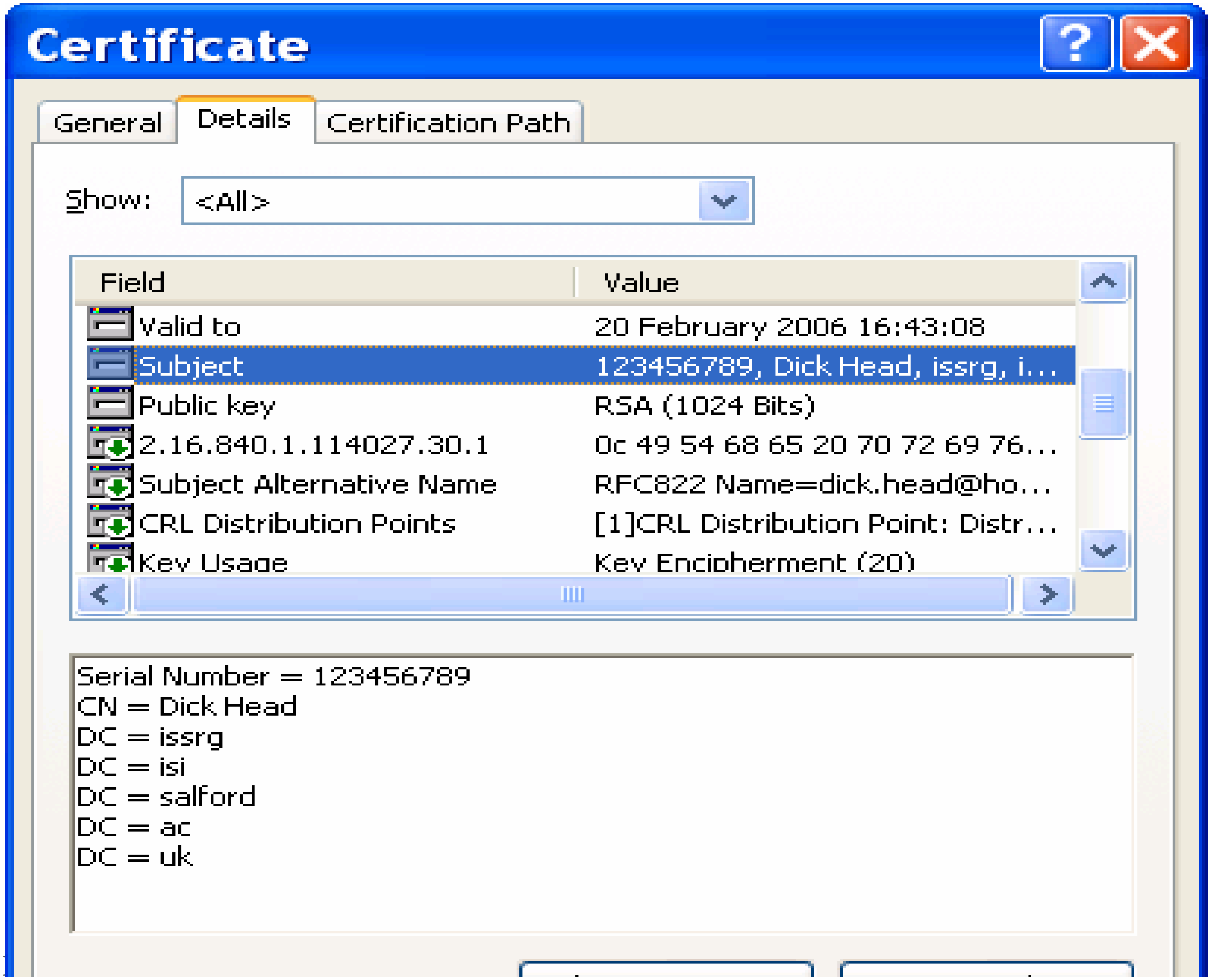
  David Chadwick, 1st EuroPKI W/shop

- PKI vendors and implementers don’t know the meaning of ASN.1 SEQUENCE and cannot differentiate between a SET and a SEQUENCE in an X.500 DN
  - Distinguished naming is more or less random with arbitrary grouping of AVAs, and the ordering and number of RDNs
    - » Peter Gutmann, 2004 PKI Worshop
  - ***“I don't treat a DN as a SET or SEQUENCE but as a "string". That is how e-business do it.”*** A Very Vocal Voice on the PKIX list (name withheld so as to not cause too much

CAs and DNs

- Some DNs may be encoded backwards which is a result of the unfortunate LDAP RFC 1779 string representation
- *“One European national CA encodes DNs backwards and forwards at random. Other CAs are more consistent in getting DNs backwards”* Peter Gutmann, NIST PKI W/shop 2004
- I don’t think any PKI software supports X.500/LDAP DN matching rules. They usually do a simple binary string compare.
- Microsoft doesn’t even allow multi-AVAs in RDNs in Active Directory and IE shows them as separate RDNs

A multi-AVA RDN displayed in IE6



Field	Value
Valid to	20 February 2006 16:43:08
Subject	123456789, Dick Head, issrg, i...
Public key	RSA (1024 Bits)
2.16.840.1.114027.30.1	0c 49 54 68 65 20 70 72 69 76...
Subject Alternative Name	RFC822 Name=dick.head@ho...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Key Usage	Key Encipherment (20)

Serial Number = 123456789
CN = Dick Head
DC = issrg
DC = isi
DC = salford
DC = ac
DC = uk

Accessing Directories

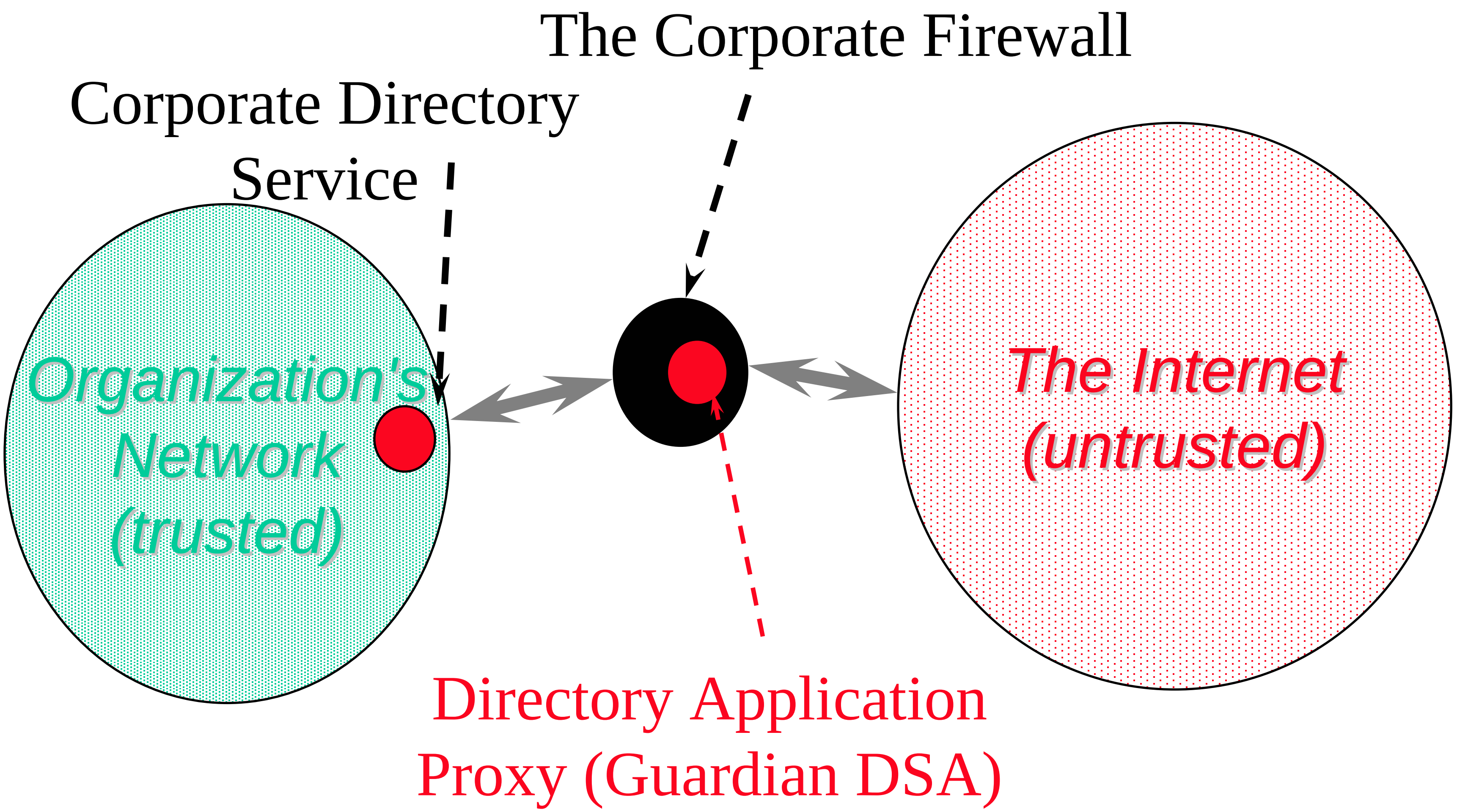
- Most organisations don’t allow public access to their directories to obtain certs and CRLs
- Solution
  - Use a web gateway
  - Use an LDAP/X.500 firewall

Web Access

- Free Http/LDAP gateways can be obtained from the Internet. E.g.
  - Web500gw written by Frank.Richter@hrz.tu-chemnitz.de
  - Download free from http://web500gw.sourceforge.net/
  - Web2LDAP gateway written by Michael Ströder michael@stroeder.com
  - Free download from http://www.web2ldap.de/download.html
- Benefits
  - Strictly limit the types of operations e.g. no modifications, adds or deletes
  - Strictly limit the attributes that can be returned
  - Strictly limit the DIT subtree that can be searched
  - Opens up your firewall nicely

LDAP/X.500 Firewalls

- Guardian DSA from Salford University


The Corporate Firewall
Corporate Directory Service
Organization's Network (trusted)
The Internet (untrusted)
Directory Application Proxy (Guardian DSA)

Guardian DSA functionality

- Configurable incoming and outgoing filters to
  - Prevent access to sensitive information
  - Prevent overwriting of important information
  - Prevent accidental release of confidential information
  - Prevent access to external information
  - Check credentials and discard or replace untrustworthy ones
  - Block all Modification operations
  - Remove confidential attributes, names, referrals, cross references, signatures etc.

  Full details in: Chadwick, D.W., Young, A.J. "Enabling The Internet White Pages Service - The Directory Guardian", presented at The Internet Society 1998 Symposium on Network and Distributed Systems Security (NDSS 98), March 10-12, San Diego, California
- Similar system was made into a commercial product by Nexor – the Directory Guardian

The EC PASSWORD Project

- The EC PASSWORD project (1992-94) built X.509 clients and servers, but found
- It took 11 secs on a 386 to create a digital signature
- SMTP worked better than X.400 for transferring secure Email
  - This was because X.400 stored the security information on the message envelope, rather than inside it, therefore MTAs that did not understand this bounced the message, whereas SMTP servers relayed them OK
- Users could not only sign documents, but could also sign their own certificates and introduce their friends into the PKI
- This led to the basicConstraints extension being introduced into the 1997 X.509 standard
  - basicConstraints says whether a cert is an end user cert (default) or a CA cert, and if a CA cert, also the max number of CA certs that may follow this one in the path

PKI Hype

- 1997 was the year of PKI

- So was 1998

- During the late 90s every year was the year of PKI

PKI Reality

- During the late 90s a national organisation set up a national PKI service in the UK and reported several hundred bugs to their PKI software vendor
  - The PKI service went bust in 2002
- Different software releases were incompatible with earlier releases
  - Meant that sometimes you had to re-issue all your certs and start again
- User interfaces were difficult (an understatement!)
- Administrative interfaces and error diagnostic messages were gooble de gook or misleading
- Etc. etc. Its all history now.

Commercial Consequences of the PKI Hype

- Many PKI companies started in the late 90s
- They flourished on the dotcom boom
- But there was something fundamentally wrong with the market
- Companies like Entrust and Baltimore had P/E ratios in their thousands or even infinity (if loss making)
- A company with a P/E ratio of 1000 on doubling its earnings every year would take 6 years to reduce it to 15
  - That’s a long term huge financial risk to take
- In 1999 Entrust and RSA had the same share price whilst RSA had 10 times the earnings of Entrust
  - Message. Sell you Entrust shares and buy RSA ones quick!
- Eventually this led to many PKI company failures

X.509 Standard's Cock Ups

- Changing the semantics of X.509 elements and not changing their OIDs. Examples
- The first (88) and second (93) versions of CRLs were different but used the same attribute OID
  - Got away with it because no-one had implemented 88 CRLs
- The '97 definition of skipCerts in the policyConstraints extension had its semantics changed in 2001, but the OID of the extension remains the same
  - Caused confusion because some companies had implemented the 97 semantics and then had to change it

Too Many Almost Duplicate or Conflicting Extensions

- CRL number (supposed to be unique) and CRL stream identifier (identifies context in which CRL number is unique)
- Freshest CRL and Distribution Point extensions in certificates both point to where the latest CRLs can be found
- CRL Scope and Issuing Distribution Point both describe the contents of a CRL
- *"Because of the potential for conflicting information a CRL shall not contain both the **deltaCRLIndicator** extension and a **crlScope** extension with the **baseRevocationInfo** component"* X.509 (2001)

The Non-Repudiation Bit

- *Never in the field of human intellect has so much time and effort been spent by so many on so little*

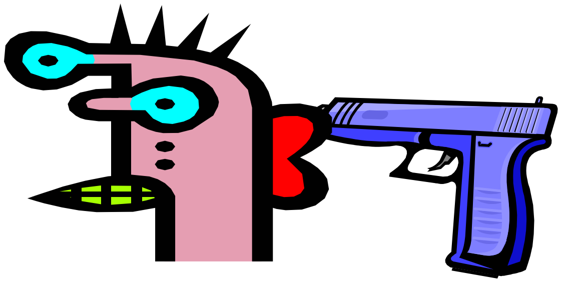
  David "Winston" Chadwick

- This one bit has caused more hot air, more defect resolution time, more paper descriptions, counter descriptions, re-wording and re-re-rewording than any other part of X.509
- So what's all the fuss about?

Repudiation

- Repudiation is a legal issue. It is up to a judge to determine if a signatory intended to digitally sign a document or not. The setting of the “non-repudiation” bit cannot prove the legal validity of a digital signature
- Anyone is entitled to repudiate an action at a later date. A judge determines their intentions
- So even if I digitally sign a message using my smart card, PIN and biometric and the NR bit is set in the corresponding certificate, I can still repudiate my action later on

After all – SOMEONE MIGHT HAVE HAD A GUN TO MY HEAD



PKI Today

Content Commitment (March 04 text)

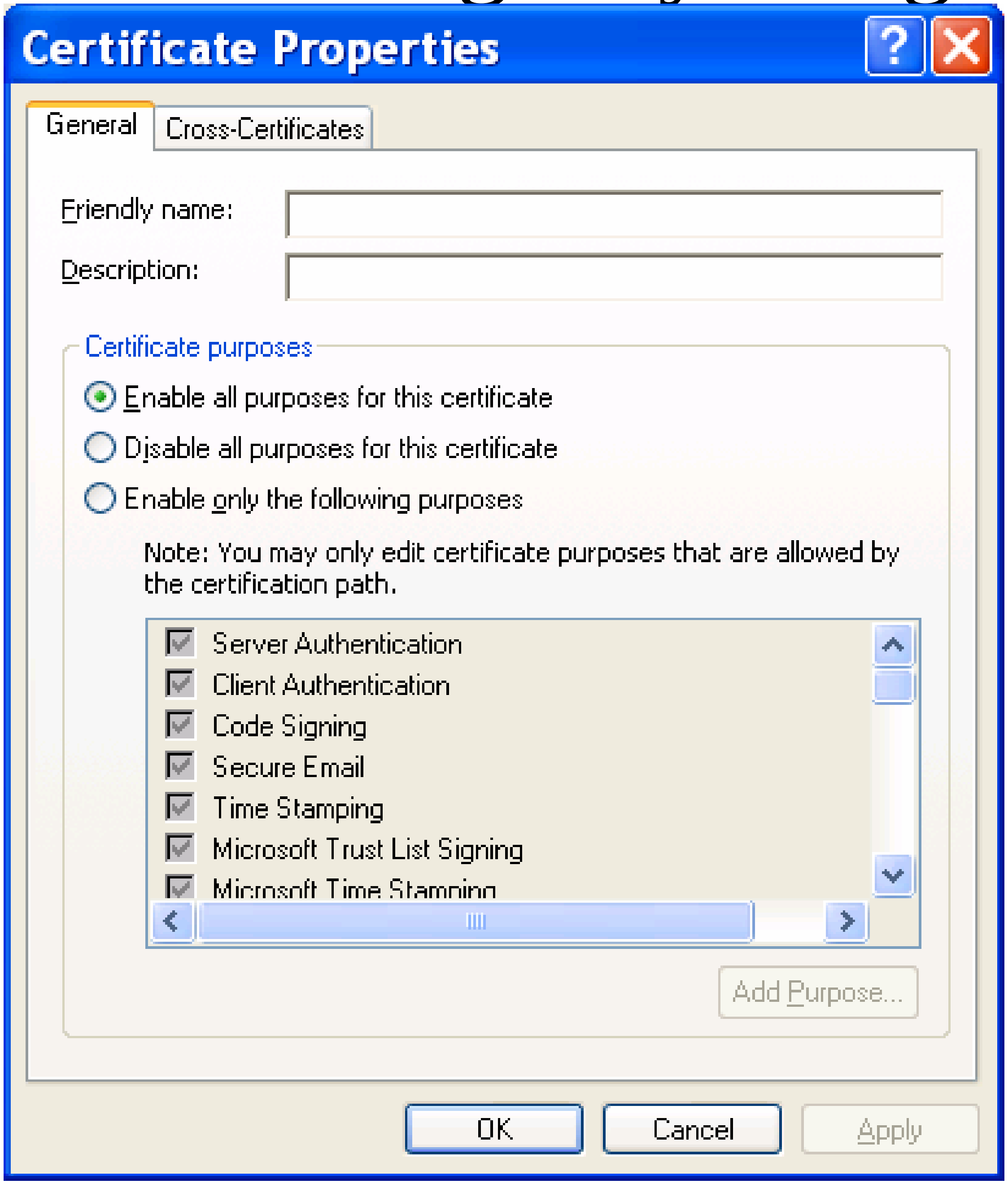
- So the bit is now named Content Commitment
  - “Any participant in an event may subsequently decide to repudiate anything that participant digitally signed in that event. For example, one can dispute one’s participation in a key establishment or being the originator of a signed email message as easily as one can dispute one’s signing a document with the intent to be bound to the content of that document.”
  - “**contentCommitment**: for verifying digital signatures which are intended to signal that the signer is committing to the content being signed. The type of commitment the certificate can be used to support may be further constrained by the CA, e.g. through a certificate policy. The precise type of commitment of the signer e.g. "reviewed and approved" or "with the intent to be bound", may be signalled by the content being signed, e.g. the signed document itself or some additional signed information.”

And More…

  – “Setting a specific value of **KeyUsage** in a certificate does not in itself signal for an instance of communication that the communicating parties are acting in accordance with this setting, e.g. when signing a document. Definition of methods by which parties may signal their intent for a specific instance of communication (e.g. commitment to content for that specific instance) is outside the scope of this Directory Specification, but it is anticipated that multiple methods will exist. Although not recommended, it is possible to use the content of the certificate, e.g. certificate policy, to signal the intent of the signing. However, since that signal was made when the certificate was issued by the CA, such use may not meet the requirement that declaring the intent is made at the time of signing by the signer.”

- So is there any value left in the key usage extension ??
- Apparently not, since the user can over-ride this in IE6

Over-riding Key Usage



Friendly name:

Description:

Certificate purposes

● Enable all purposes for this certificate

○ Disable all purposes for this certificate

○ Enable only the following purposes

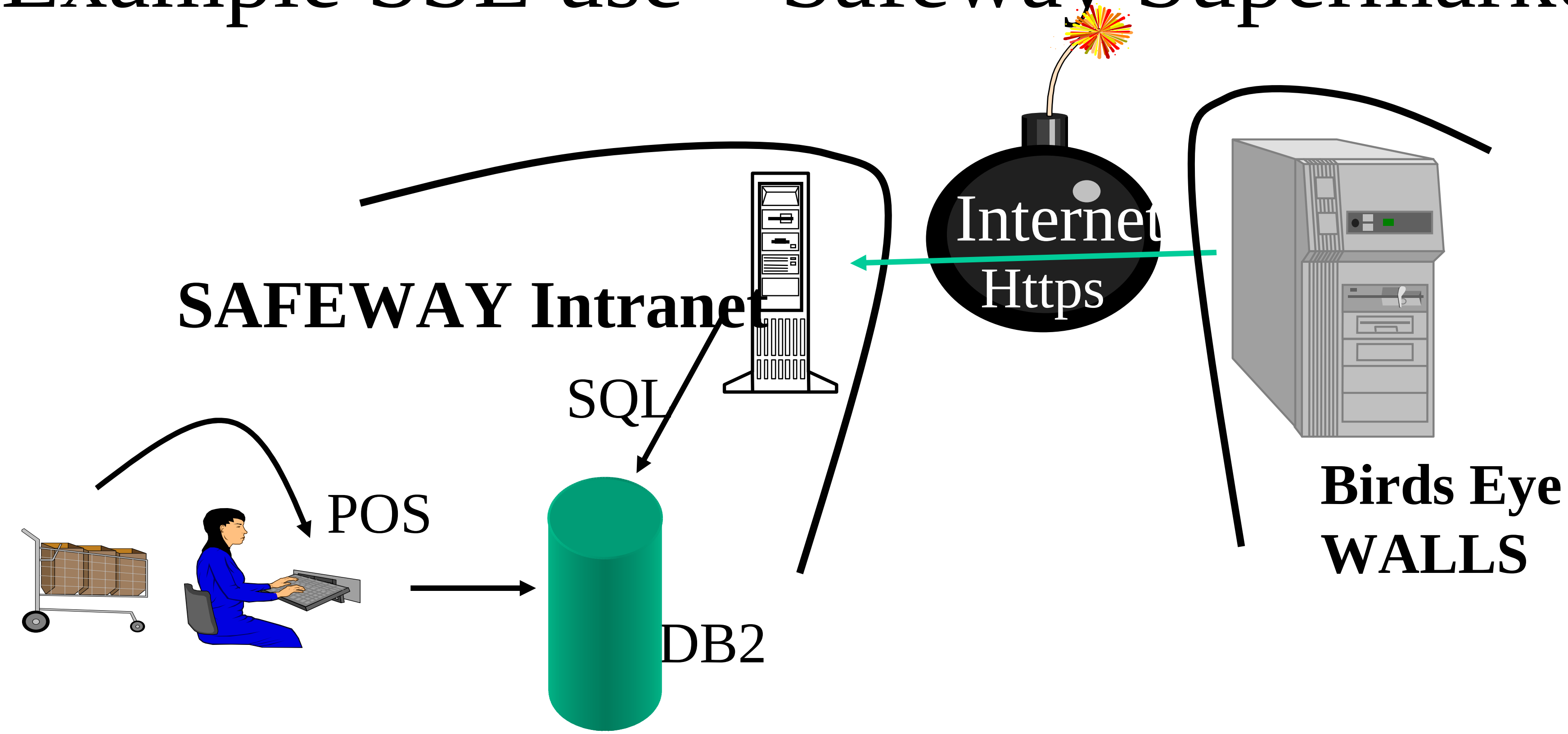
Note: You may only edit certificate purposes that are allowed by the certification path.

☑ Server Authentication
☑ Client Authentication
☑ Code Signing
☑ Secure Email
☑ Time Stamping
☑ Microsoft Trust List Signing
☑ Microsoft Time Stamping

Current uses of PKI today

- Who is using PKI today? Many and varied
- All SSL servers use a PKI (of sorts)
- All web browsers support PKI (of sorts)
- In several countries e.g. Spain and UK, you can fill in tax returns to the Inland Revenue using PKI certs
- In US, the DOD is enforcing a requirement that all contractors participate in the Interim External CA program.
  - IECA requires DOD contractors (approx 350,000 of them) to have one-year encrypted digital certificates to ensure the security of vendor communications with the department e.g. when submitting electronic invoices
  - Published March 04 at http://www.gcn.com/23_6/news/25310-1.html
- Many commercial banks are using PKI for Internet banking
- Scientific Grid community requires use of PKI
- Several countries have incorporated PKI key pairs into their national ID cards e.g. Finland, Sweden, Italy, Belgium

Example SSL use – Safeway Supermarket

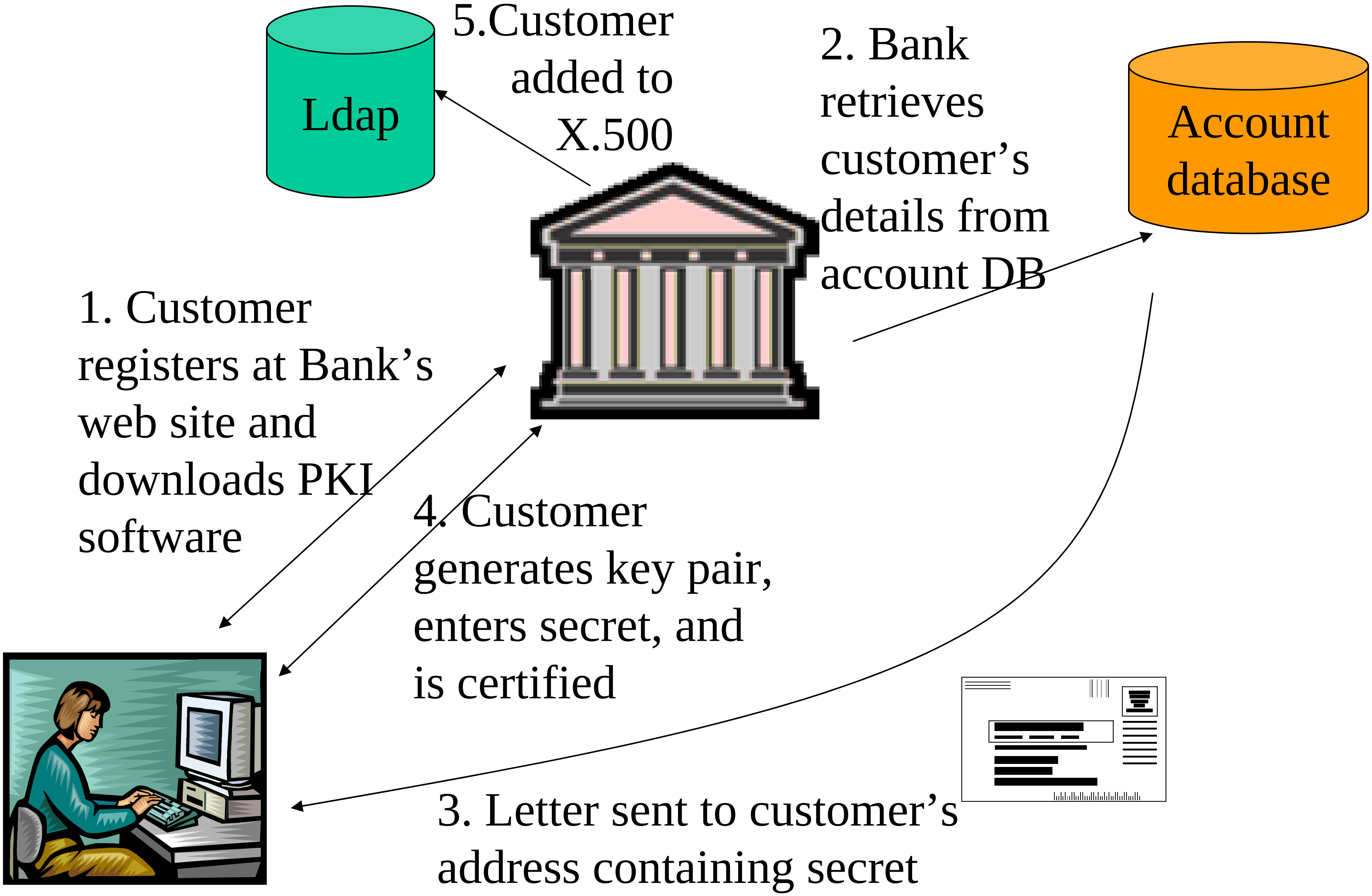


- Safeway shares real time information with Walls about stock levels, shelf space and sales forecasts
- Walls uses this to decide when to deliver
- Lead times reduced from 45 hours to 10 hours, service levels increased from 90% to 95%

Bank use of PKI – Some examples

- Scotiabank, Canada was the first to use PKI, using Entrust. Launched in 1997
- Identrus, the organisation originally formed in 1988 by 9 banks, now has > 60 financial institutions as participants
- And not forgetting its rival Betrusted, formed by PWC in 1999, and now owned by BankOne of America
- The Danish Savings Banks Data Center uses mobile phones and a central key store to provide user roaming
  - Over 50 Danish banks participate in this

Scotiabank, Canada



1. Customer registers at Bank’s web site and downloads PKI software

2. Bank retrieves customer’s details from account DB

3. Letter sent to customer’s address containing secret

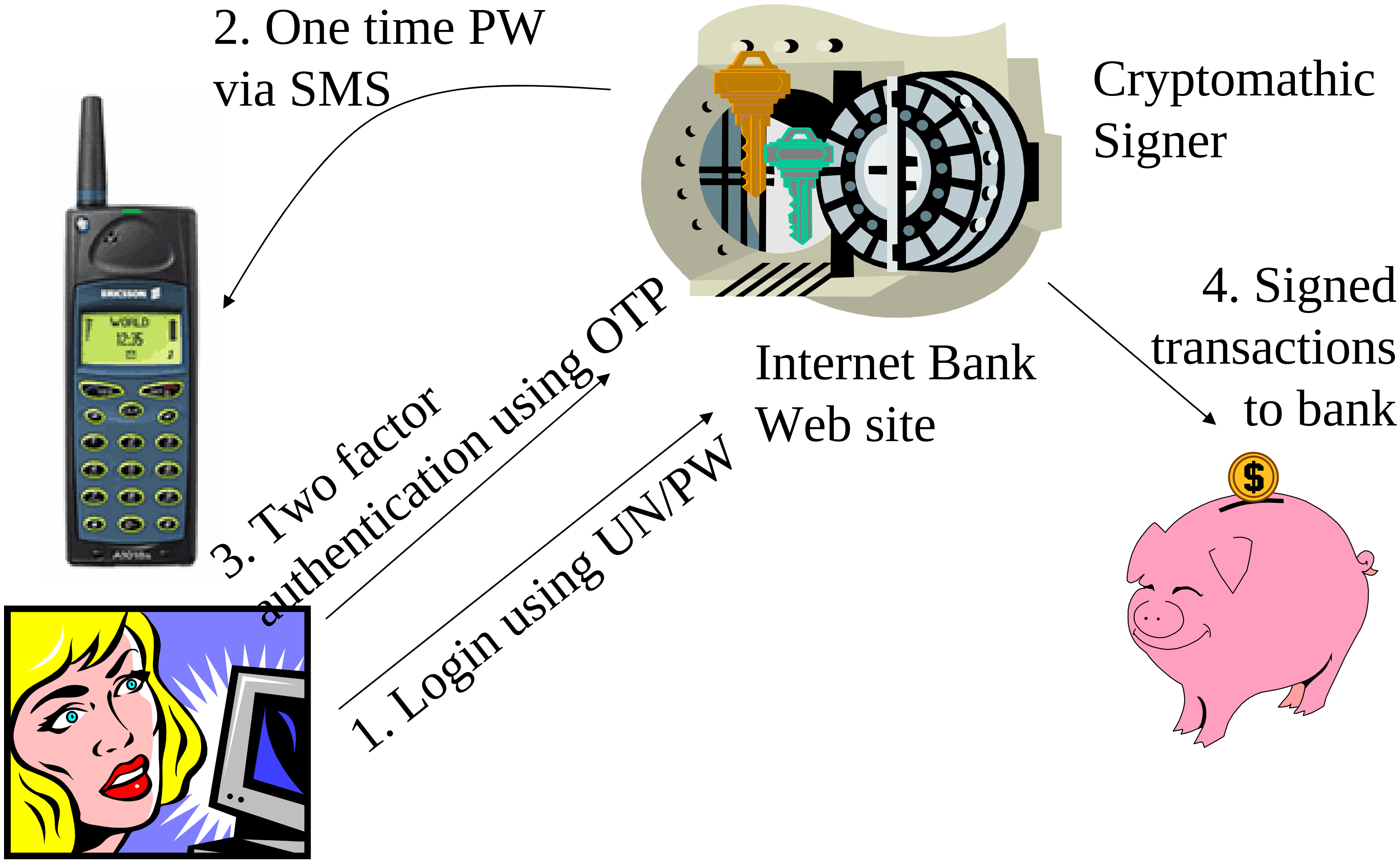
4. Customer generates key pair, enters secret, and is certified

5.Customer added to X.500

Scotiabank, Canada

- Users must already be registered account holders with bank
- Every user is given a unique ID and DN of the form {O=Scotiabank, UID=123456789}
  - Note the local naming, but certificate was only intended to be used in this domain
- User’s X.500 DIT entry held X.509 public key certificate, account information and attribute certificates which authorised particular banking services
- In 2004 converted to Betrusted certificates

Café Bank, Denmark



2. One time PW
via SMS

Cryptomathic
Signer

3. Two factor
authentication using OTP

1. Login using UN/PW

Internet Bank
Web site

4. Signed
transactions
to bank

Grid use of PKI

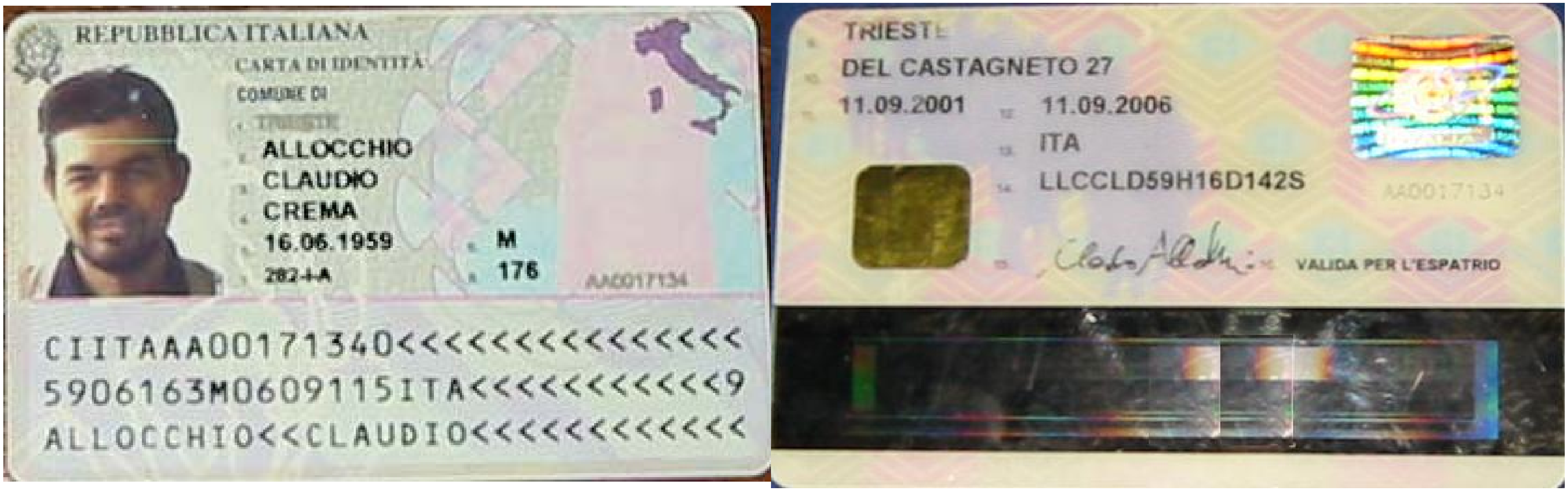
- Grid users authenticate with dig sigs and X.509 certificates
- They want to spawn jobs to run on various computers throughout the Grid
- The idea is to have the job create its own key pair, then the user signs the job's certificate so that the job can be a proxy for the user
- But certificate validation did not work because of the basicConstraints extension which stops users issuing certs
  - Remember the experiences of the PASSWORD project??
- The result – a new *proxy* extension added to over-ride basicConstraints, effectively allowing the user to act as a CA!

UK Grid Registration Procedures

- Registration requires face to face authentication to provide medium assurance certificates
- This means the user physically comes to the RA with a photo ID card (usually their university ID card)
- But this is an expensive and time consuming process
- We have suggested that universities could use their student registration database to do bulk registration for medium assurance certificates
- This has been rejected on the basis that a photo ID is currently required for face to face authentication
- But the photo ID card that is usually used is the one generated from the student registration database!!!

National ID cards and PKIs

- Italy was one of the first countries, in 2001



REPUBBLICA ITALIANA

CARTA DI IDENTITÀ

COMUNE DI

TRIESTE

ALLOCCHIO

CLAUDIO

CREMA

16.06.1959 M

282+A 176

AA0017134

```
CIITAAA00171340<<<<<<<<<<<<<<<
5906163M0609115ITA<<<<<<<<<<<9
ALLOCCHIO<<CLAUDIO<<<<<<<<<<<<
```

TRIESTE

DEL CASTAGNETO 27

11.09.2001 11.09.2006

ITA

LLCCLD59H16D142S

AA0017134

Claudio Allocchio

VALIDA PER L'ESPATRIO

- It uses the name and social security number to identify the owner

But - Some have Really Lost the Plot

- EC with its qualified certificates and piles of standards (equivalent of gold pen to sign a letter)
- Web browsers by adding 100+ trusted root CAs to our browsers
- PKIX (and X.509) with its myriad of certificate extensions and standards
- CA providers with their subject distinguished names e.g.
  - E = d.w.chadwick@salford.ac.uk, CN = David Chadwick, OU = Digital ID Class 1 - Microsoft Full Service, OU = Persona Not Validated, OU = www.verisign.com/repository/RPA Incorp. by Ref.,LIAB.LTD(c)98, OU = VeriSign Trust Network, O = VeriSign, Inc.
  - CN = Microsoft Internet Authority

EESSI Standards

- CWA 14167-1 (2001): "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements".
- CWA 14167-2 (2002): "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2 Cryptographic Module for CSP Signing Operations – Protection Profile (MCSO-PP)".
- CWA 14169 (2002): "Secure Signature-Creation Devices, version 'EAL 4+'".
- CWA 14170 (2001): "Security Requirements for Signature Creation Systems".
- CWA 14171 (2001): "Procedures for Electronic Signature Verification".
- CWA 14172-1 (2001): "EESSI Conformity Assessment Guidance - Part:1: General".

EESSI Standards (cont)

- CWA 14172-2 (2001): "EESSI Conformity Assessment Guidance - Part 2: Certification Authority services and processes".
- CWA 14172-3 (2001): "EESSI Conformity Assessment Guidance - Part 3: Trustworthy systems managing certificates for electronic signatures".
- CWA 14172-4 (2001): "EESSI Conformity Assessment Guidance - Part 4: Signature Creation Applications and Procedures for Electronic Signature Verification".
- CWA 14172-5 (2001): "EESSI Conformity Assessment Guidance - Part 5: Secure signature creation devices".
- CWA 14355 (2002): "Guidelines for the implementation of Secure Signature-Creation Devices".
- ETSI SR 002 176: "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures".

EESSI Standards (cont)

- ETSI TS 101 456: "Policy requirements for certification authorities issuing qualified certificates".
- ETSI TS 101 733: "Electronic Signatures and Infrastructures (ESI); Electronic Signature Formats".
- ETSI TS 101 862: "Qualified certificate profile".
- ETSI TS 101 903: "XML Advanced Electronic Signatures (XAdES)".
- ETSI TR 102 038: "TC Security - Electronic Signatures and Infrastructures (ESI); XML format for signature policies".
- ETSI TR 102 041: "Signature Policies Report".
- ETSI TR 102 045: "Electronic Signatures and Infrastructures (ESI); Signature policy for extended business model".
- AND this is not a complete list

PKIX IDs and RFCs

- Housley, R., Ford, W., Polk, W., and Solo, D., "Internet X.509 Public Key Infrastructure Certificate and CRL Profile," RFC 3280, April 2002
- Adams, C., Farrell, S., "Internet X.509 Public Key Infrastructure Certificate Management Protocols,"
- Myers, M., Adams, C., Solo, D., and Kemp D. "Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF),“
- Chokhani, S., Ford, W., Sabett, R., Merrill, C., and Wu, S., "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework,"
- Myers, M., Liu, X., Fox, B., and Weinstein, J., "Certificate Management Messages over CMS,“
- Farrell, S., and Housley, R., "An Internet Attribute Certificate Profile for Authorization," RFC 3281, April 2002.
- Yee, P., "Attribute Certificate Request Message Format,"
- Yee, P., "Attribute Certificate Management Messages over CMS,"

PKIX IDs and RFCs (cont)

- Chadwick, D., Legg, S., "Internet X.509 Public Key Infrastructure Additional LDAP Schema for PKIs and PMIs,"
- Myers, M., Liu, X., Schaad, J., and Weinstein, J., "Certificate Management Messages over CMS," (RFC 2797), April 2000.
- Adams, C., Farrell, S., "Internet X.509 Public Key Infrastructure Certificate Management Protocols," RFC 2510, March 1999.
- R. Housley, "Cryptographic Message Syntax," RFC 2630, July 1999.
- Myers, M., Adams, C., Solo, D., and Kemp, D., "Internet X.509 Certificate Request Message Format," RFC 2511, March 1999.
- Prafullchandra, H., and Schaad, J., "Diffie-Hellman Proof-of-Possession Algorithms," RFC 2875, July 2000 1999.
- Myers, M., Adams, C., Farrell, S., "Delegated Path Discovery with OCSP".
- Myers, M., Adams, C., Farrell, S., "Delegated Path Validation".
- Pinaks, D., Housley, R., "Delegated Path Validation and Delegated Path Discovery Protocol Requirements (DPV&DPD-REQ),"

PKIX IDs and RFCs (cont)

- Adams, C., Sylvester, P., Zolotarev, M., Zuccherato, R., "Internet X.509 Public Key Infrastructure Data Certification Server Protocols", RFC 3029, February 2001.
- Housley, R., and Hoffman, P., "Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP," RFC 2585, July 1998.
- Lynn, C., Kent, S., Seo, K., "X.509 Extensions for IP Addresses and AS Identifiers,"
- Housley, R., and Polk, W., "Internet X.509 Public Key Infrastructure Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates," RFC 2528, March 1999.
- Farrell, S., Chadwick, C.W., "Limited Attribute Certificate Acquisition Protocol".
- Santesson, S. Housley, R., Freeman, T., "X.509 Internet Public Key Infrastructure Logotypes in X.509 Certificates,"

PKIX IDs and RFCs (cont)

- Myers, M., Ankney, R., Adams, C., "Online Certificate Status Protocol, version 2,"
- Pinka, D., Gindin, T., "Internet X.509 Public Key Infrastructure Permanent Identifier,"
- Boeyen, S., Howes, T., and Richard, P., "Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2," RFC 2559, April 1999.
- Chadwick, D.W., "Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv3,“
- Chokhani, S., and Ford, W., "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework," RFC 2527, March 1999.
- Santesson, S., Polk, W., Barzin, P., and Nystrom, M., "Internet X.509 Public Key Infrastructure Qualified Certificates," RFC 3039, January 2001.
- Boeyen, S., Hallam-Baker, P., "Internet X.509 Public Key Infrastructure Repository Locator Service,“

PKIX IDs and RFCs (cont)

- Bassham, L., Housley, R., Polk, W., "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRL Profile,“
- Boeyen, S., Howes, T., and Richard, P., "Internet X.509 Public Key Infrastructure LDAPv2 Schema," RFC 2587, June 1999.
- Malpani, A., Hoffman, P., Housley, R., and Freeman, T., "Simple Certificate Validation Protocol (SCVP),"
- Schaad, J., " CMC Extensions: Server Side Key Generation and Key Archival,"
- Singer, A., and Whyte, W., "Supplemental Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRL Profile,"
- Gindin, T., "Internet X.509 Public Key Infrastructure Technical Requirements for a non-Repudiation Service," December 2000.
- Schaad, J. Myers, M., Liu, X., Weinstein, J., "CMC Transport,"
- Kapoor , A., Tschalaer, R., "Transport Protocols for CMP,"

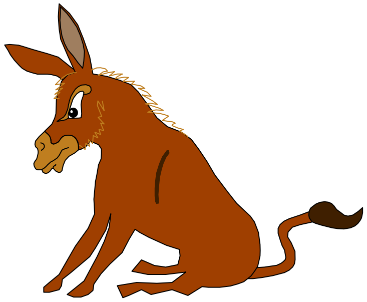
PKIX IDs and RFCs (cont)

- Myers, M., Ankney, R., Malpani, A., Galperin, S., and Adams, C., "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP," RFC 2560, June 1999.
- Adams, C., Cain, P., Pinkas, D., and Zuccherato, R., "Internet X.509 Public Key Infrastructure Time Stamp Protocols", RFC 3161, August 2001
  - I trust Company X enough to do $20million of business with them, but I do not trust them enough to be able to tell the time
- Linsenbardt, D., Pontius, S., "Warranty Certificate Extension,"
- And I have missed some of the latest ones ☺

Whatever happened to KISS ?

- Keep It Simple Stupid
  - As Ravi Sandhu says “security that is too complex wont be implemented or will be implemented wrongly”
  - X.509 and its myriad of extensions is now far too complex for most people to understand and implement correctly
  - Even national reps to X.509 meetings are no longer familiar with all the contents of the standard
- The result
  - Most extensions have not been implemented or implemented properly
- Whatever happened to KISS?

Kiss My Ass ?



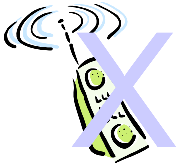
One thing X.509 did get right

- Compact binary encodings using ASN.1
- The alternative XML encodings are verbose, have poor performance, and often cant be read by humans anyway
- Research by UoS shows that using ASN.1 BER for signed certificate type constructs performs an order of a magnitude better than using XML signatures
  - Mundy, D. and Chadwick, D.W., "An XML Alternative for Performance and Security: ASN.1", IEEE IT Professional, Vol 6., No.1, Jan 2004, pp30-36
- Sun have also published a paper with similar findings
  - P. Sandoz, S. Pericas-Geertsen, K. Kawaguchi, M. Hadley, and E. Pelegri-Llopart. “Fast Web Services”, Aug 2003, Available from: http://java.sun.com/developer/technicalArticles/WebServices/fastWS/
- W3C now has the XML Binary Characterization Working Group

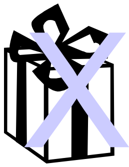
ASN.1 Success Stories

- Without ASN.1-defined messages:
  - The lights go out!

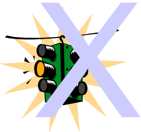
  - Mobile phones don’t work!



  - Parcels get lost!



  - Traffic lights fail!



  - Aircraft fall from the sky!

  - Your impending marriage suffers as Net Meeting fails!

Thanks to Prof John Larmouth for the above list

Who says binary encodings cant work?

```
ÐÏ   à¡±   á              >    þÿ                        !           #       þÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿìÁ
ð   ¿                      bjbjUqUq                          &    7     7
ÿÿ        ÿÿ        ÿÿ            l    B      B    B      B      B      B
B           V       p       p       p       p        |        V      Ÿ    ¶   ”
”      ”      ”      ”      ”      ”      ”

        $   U        u    Ž   D                  B      ”                ”
”      ”      ”      D        ´      B      B      ”           ”      Y        ´
´      ´      ”      B      ”      B      ”                  ´
”             ´    j  ´                  B      B
       ”      ˆ      Ð, 1Ê/Ä   V        p     ª                     o
0   Ÿ                  ´                  ´      V      V      B
B      B      B        Ù   A very simple word doc
```

Conclusion

- It’s the wide availability of tools that matter, not the encoding format
- If a comprehensive set of Open Source ASN.1 tools had been made available 15 years ago it would have been the encoding format of choice today

Who says XML is readable?

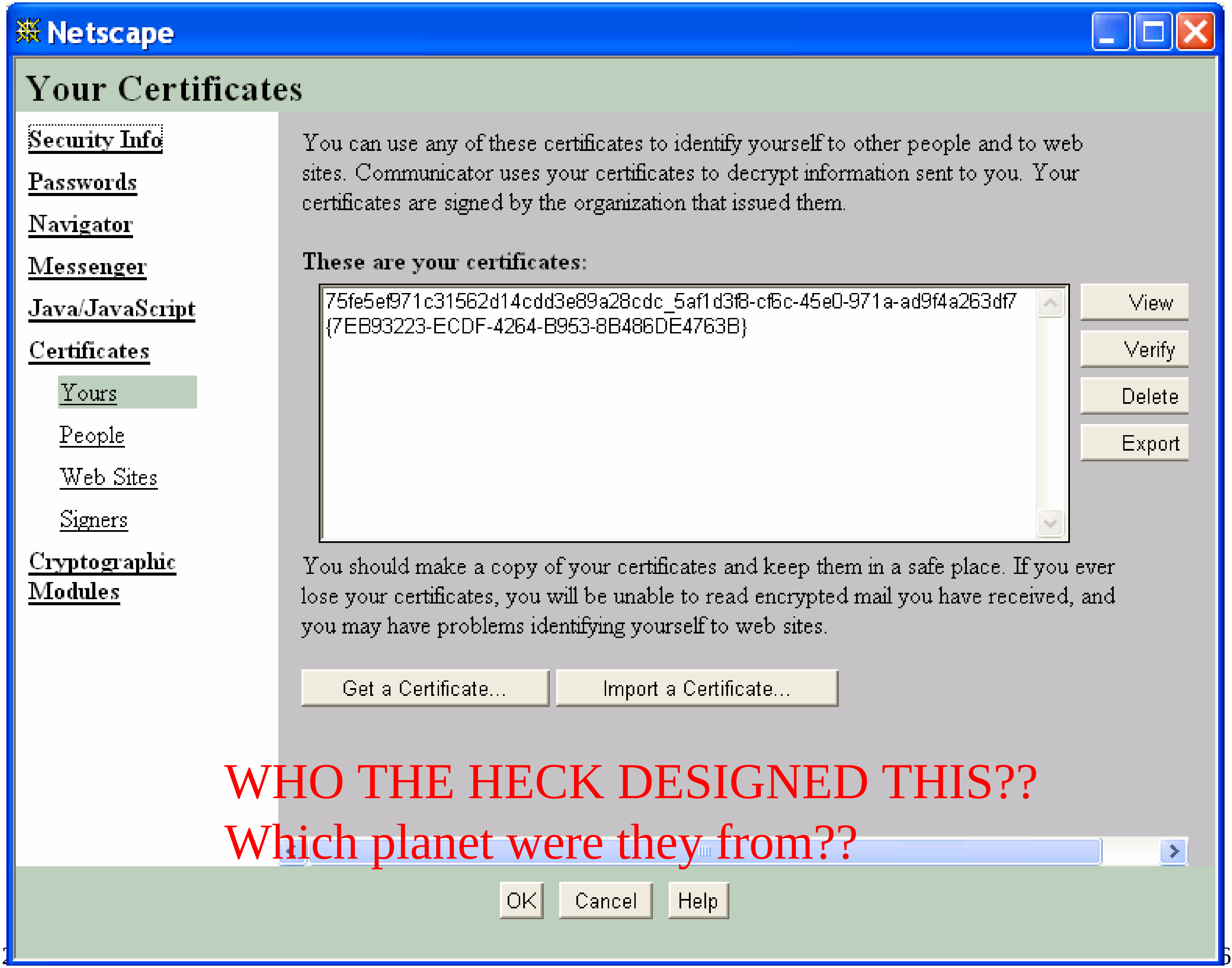
```
<?xml version="1.0" encoding="GB2312" ?>
    <备注>
      <抵>北京</抵>
      <始>伦敦</始>
      <题目>提示信息</题目>
        <题目内容>出发前请提醒我！</题目内容>
    </备注>
```

One thing SPKI got right

- Attaching local names to public keys/certificates
- Netscape did not quite get it right, as the next screen shows

One thing SPKI got wrong

- Passing the local name around to other users
- The local name should stay local and a global name/ID should accompany the public key



Your Certificates

You can use any of these certificates to identify yourself to other people and to web sites. Communicator uses your certificates to decrypt information sent to you. Your certificates are signed by the organization that issued them.

These are your certificates:

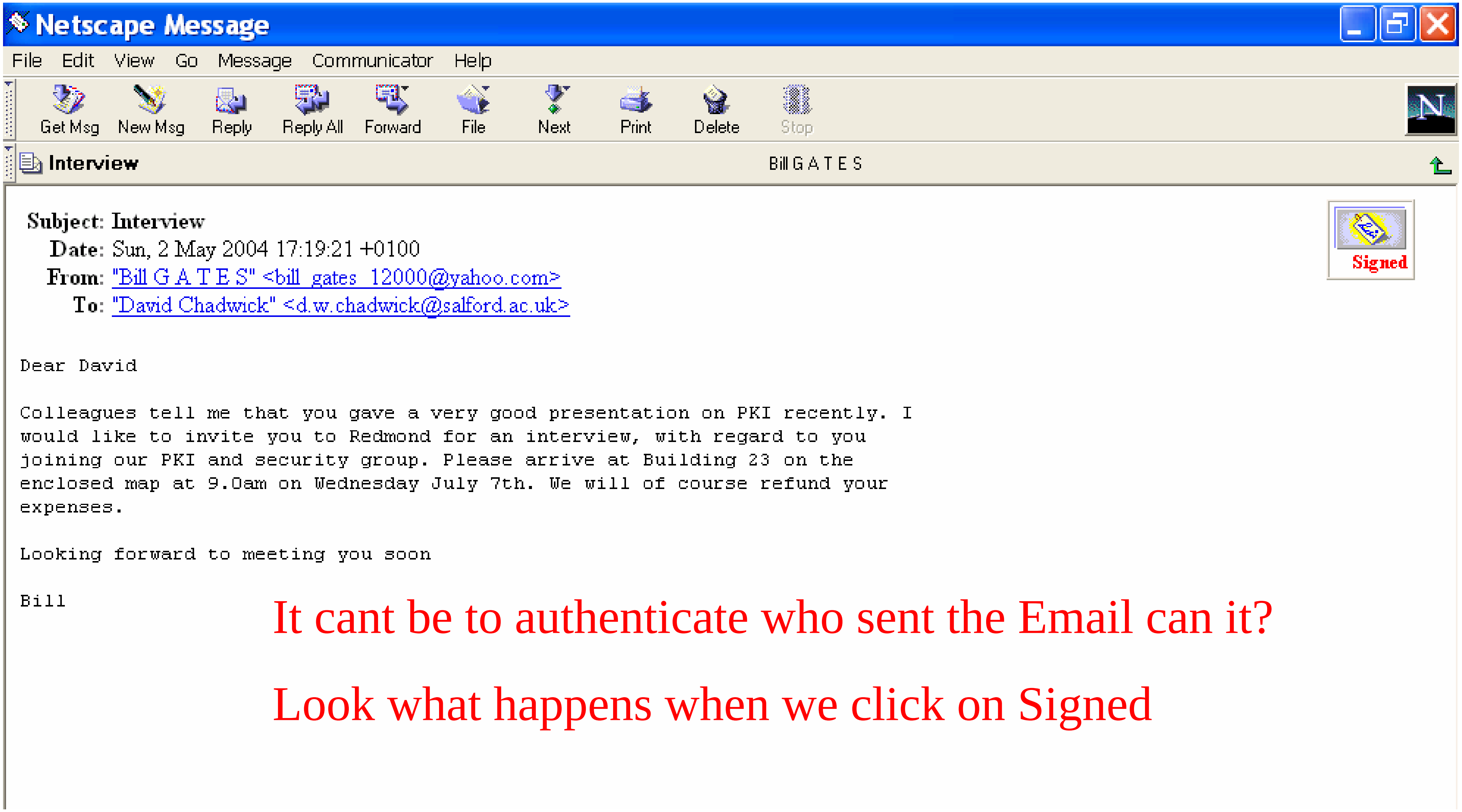
```
75fe5ef971c31562d14cdd3e89a28cdc_5af1d3f8-cf6c-45e0-971a-ad9f4a263df7
{7EB93223-ECDF-4264-B953-8B486DE4763B}
```

You should make a copy of your certificates and keep them in a safe place. If you ever lose your certificates, you will be unable to read encrypted mail you have received, and you may have problems identifying yourself to web sites.

WHO THE HECK DESIGNED THIS??

Which planet were they from??

So What is the Point of a digital signature and a PKI Anyway?

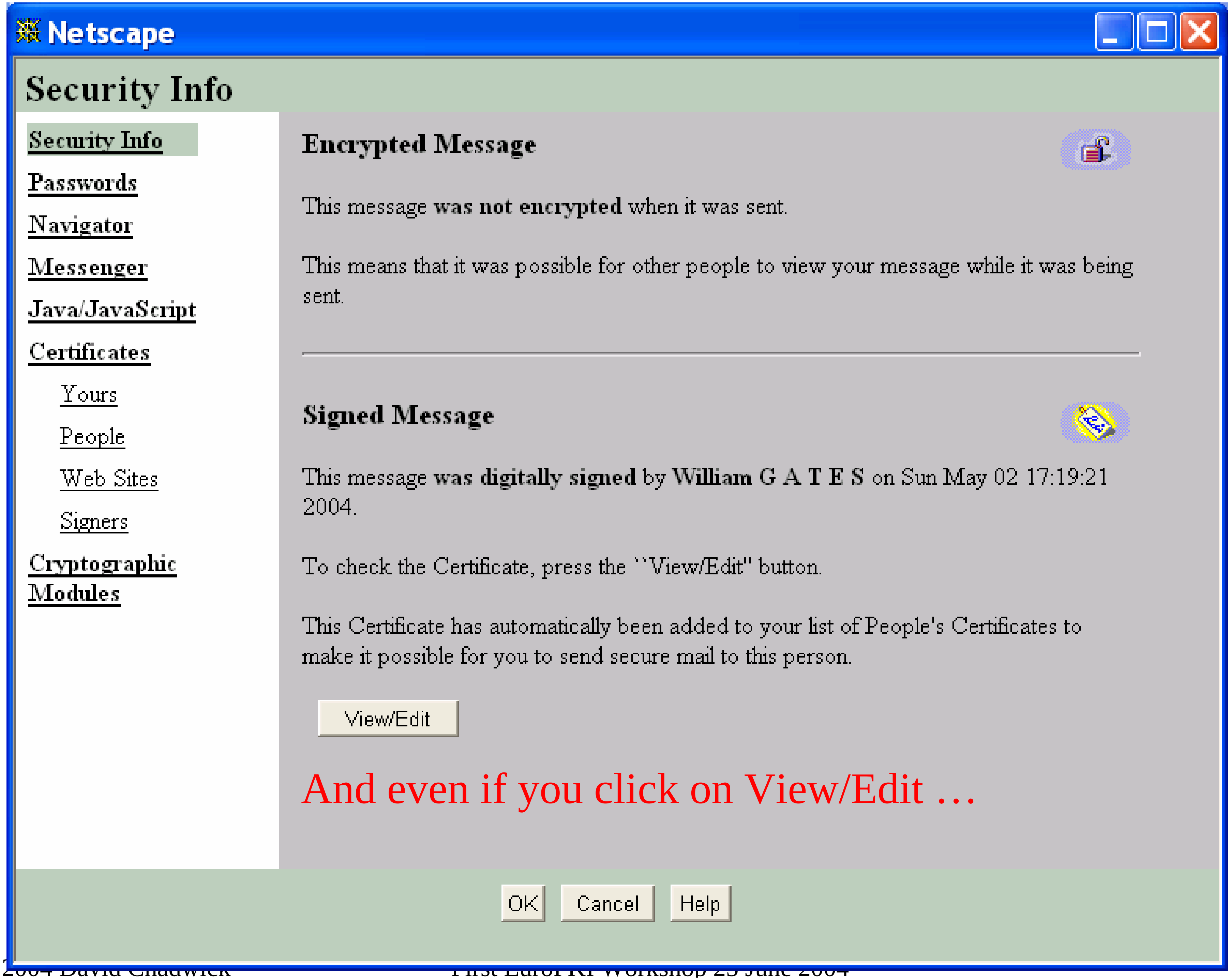


Subject: Interview
Date: Sun, 2 May 2004 17:19:21 +0100
From: "Bill G A T E S" <bill_gates_12000@yahoo.com>
To: "David Chadwick" <d.w.chadwick@salford.ac.uk>

```
Dear David

Colleagues tell me that you gave a very good presentation on PKI recently. I
would like to invite you to Redmond for an interview, with regard to you
joining our PKI and security group. Please arrive at Building 23 on the
enclosed map at 9.0am on Wednesday July 7th. We will of course refund your
expenses.

Looking forward to meeting you soon

Bill
```

It cant be to authenticate who sent the Email can it?

Look what happens when we click on Signed



Security Info

Encrypted Message

This message **was not encrypted** when it was sent.

This means that it was possible for other people to view your message while it was being sent.

Signed Message

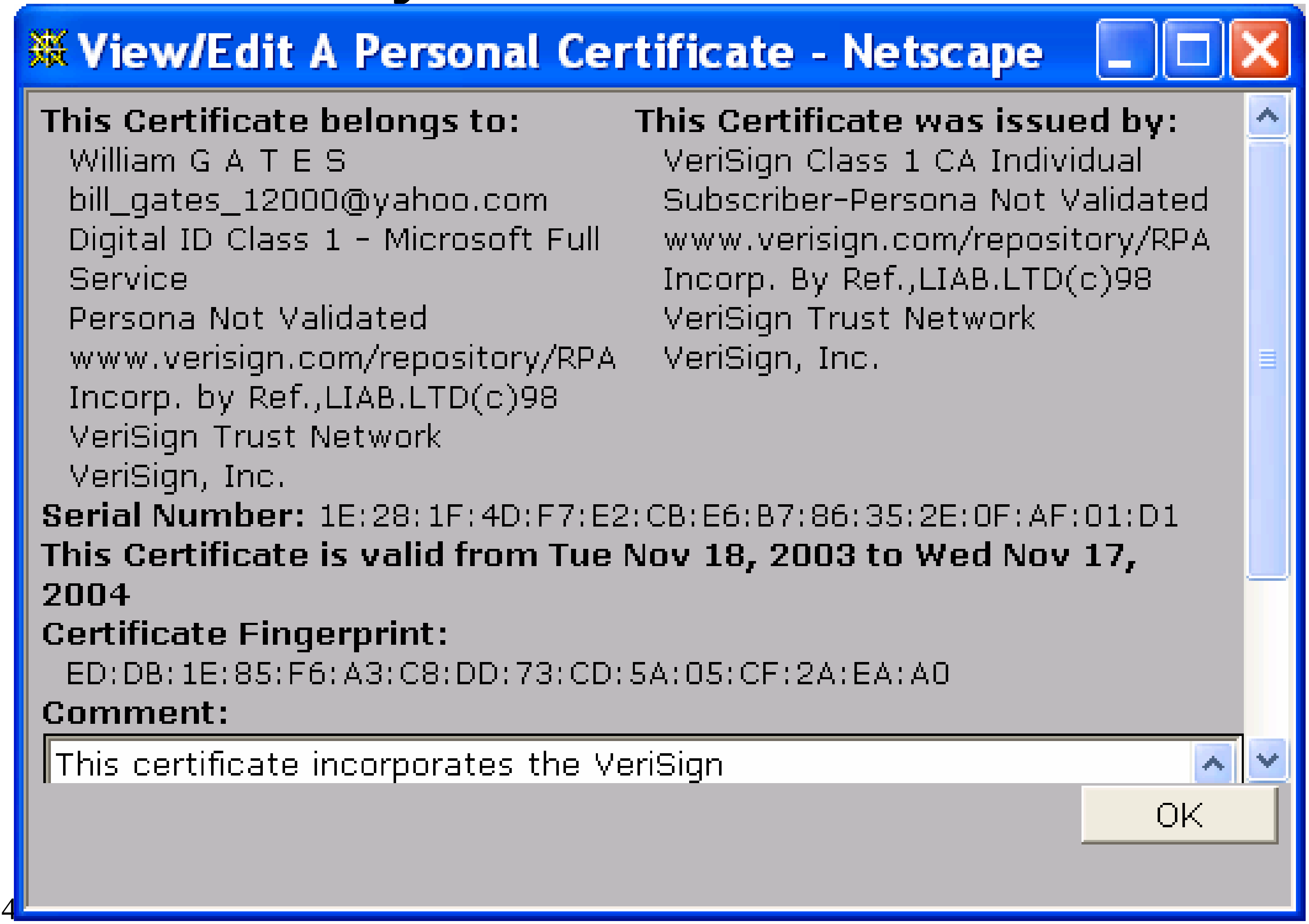
This message **was digitally signed** by **William G A T E S** on Sun May 02 17:19:21 2004.

To check the Certificate, press the ``View/Edit'' button.

This Certificate has automatically been added to your list of People's Certificates to make it possible for you to send secure mail to this person.

And even if you click on View/Edit …

You have to look real hard to see it was a Persona Not Validated certificate– Why make it so obtuse??



View/Edit A Personal Certificate - Netscape

This Certificate belongs to:

William G A T E S
bill_gates_12000@yahoo.com
Digital ID Class 1 - Microsoft Full Service
Persona Not Validated
www.verisign.com/repository/RPA Incorp. by Ref.,LIAB.LTD(c)98
VeriSign Trust Network
VeriSign, Inc.

This Certificate was issued by:

VeriSign Class 1 CA Individual Subscriber-Persona Not Validated
www.verisign.com/repository/RPA Incorp. By Ref.,LIAB.LTD(c)98
VeriSign Trust Network
VeriSign, Inc.

Serial Number: 1E:28:1F:4D:F7:E2:CB:E6:B7:86:35:2E:0F:AF:01:D1

This Certificate is valid from Tue Nov 18, 2003 to Wed Nov 17, 2004

Certificate Fingerprint:

ED:DB:1E:85:F6:A3:C8:DD:73:CD:5A:05:CF:2A:EA:A0

Comment:

This certificate incorporates the VeriSign

What Should Verisign Have Done?

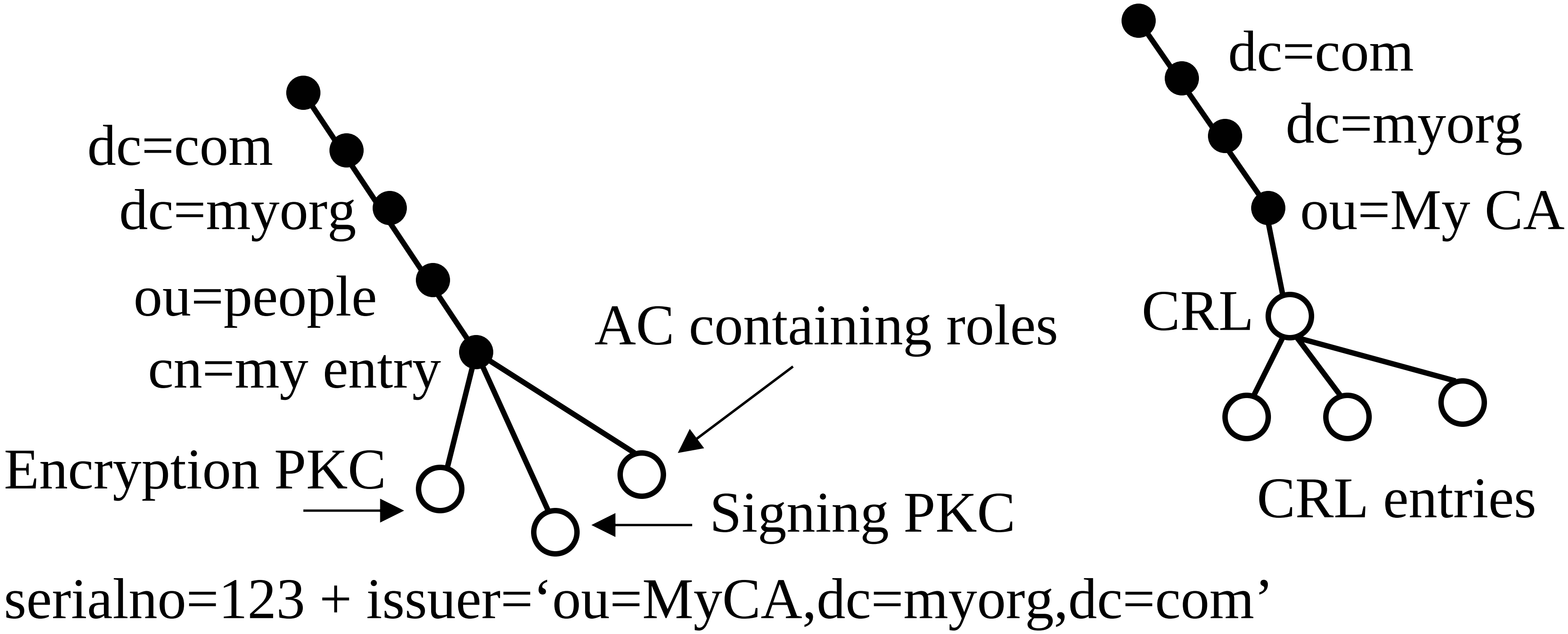
- NOT allowed the user to insert any name in the Common Name field
- Verisign do validate the globally unique email address, so… EITHER
- Put the validated Email address in the Common Name field (using DC naming as well if desired) OR
- Put “Anonymous User” or “Name Not Validated” or something similar in the Common Name field and put the Email address in the Subject Alt Name extension
- But THEY SHOULD NOT have allowed the user to put anything they wanted in the Common Name field

Returning to the LDAP problems

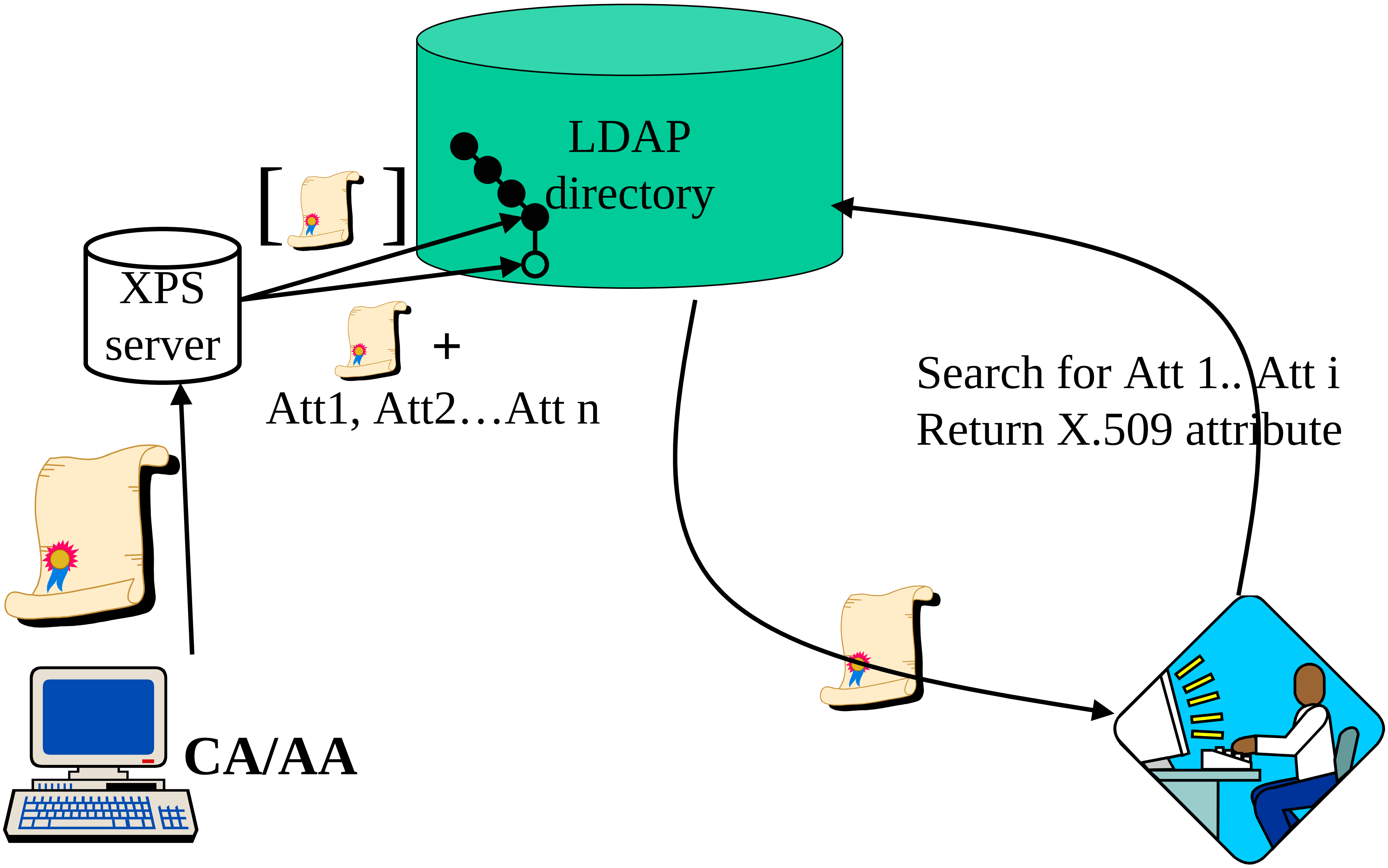
- Can’t search for specific certificates or CRLs based on their contents
- Can’t retrieve a single CRL or cert from a multi-valued attribute
  - Solution XPS – the X.509 attribute Parsing Server
  - Sits in front of (or part of) the LDAP server. Parses X.509 attributes (CRLs, PKCs and ACs) and creates a separate entry for each one, with each field a separate attribute
  - Implements current PKIX Internet Drafts
- Can’t find the right LDAP server to Search – many solutions but few implemented ! E.g.
  - For DC based DNs, perform a DNS look up of well known alias i.e. ldap.domain.name or use DNS SRV records, which bind host name/port to service
  - Use IAI PKIX extension

The XPS DIT Structure

- PKCs and ACs are held in child entries
- CRLs are held in child subtrees

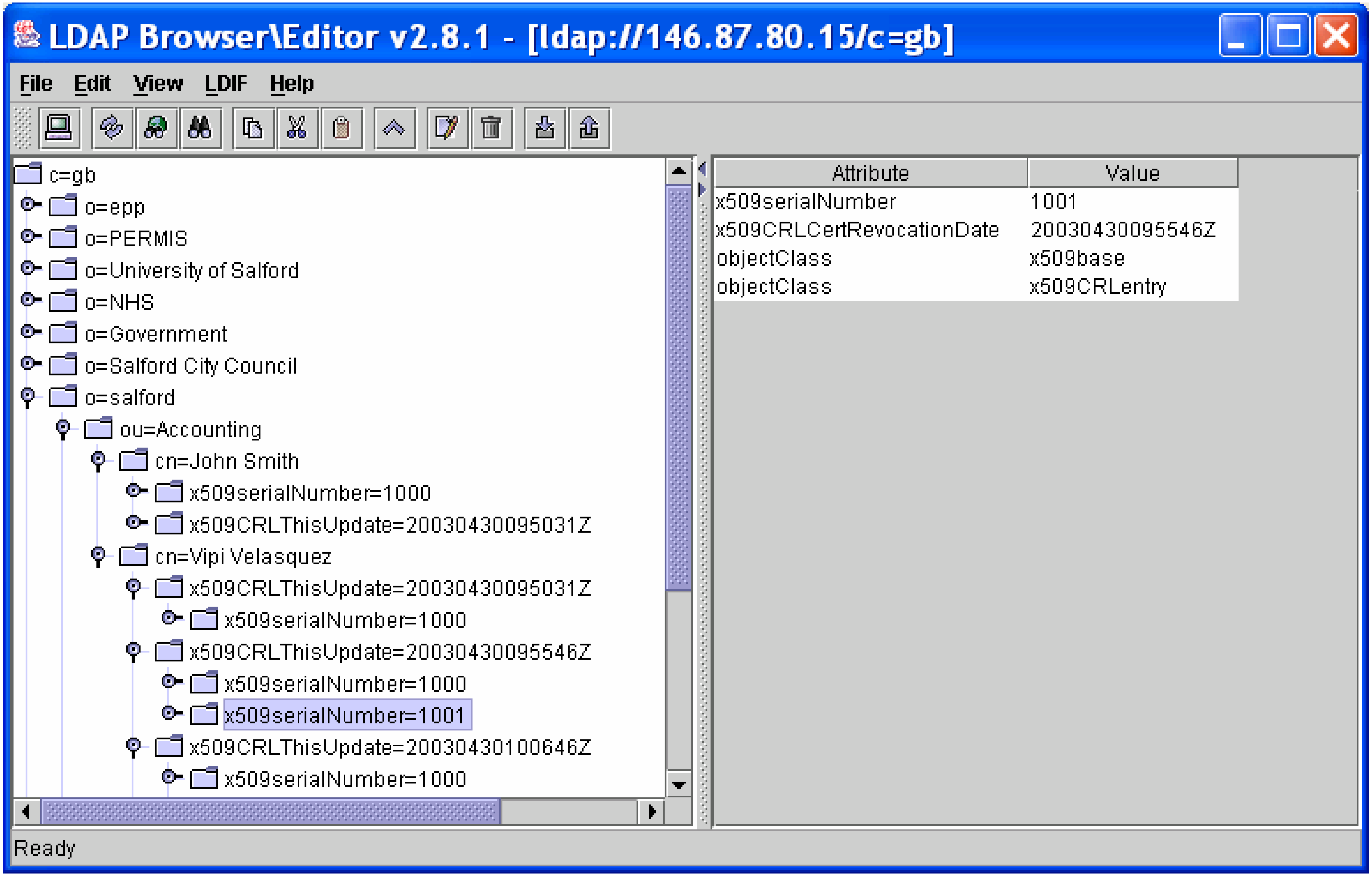


XPS



LDAP
directory
[ ]
XPS
server
+
Att1, Att2…Att n
Search for Att 1.. Att i
Return X.509 attribute
CA/AA

LDAP Client view of XPS



```
c=gb
  o=epp
  o=PERMIS
  o=University of Salford
  o=NHS
  o=Government
  o=Salford City Council
  o=salford
    ou=Accounting
      cn=John Smith
        x509serialNumber=1000
        x509CRLThisUpdate=20030430095031Z
      cn=Vipi Velasquez
        x509CRLThisUpdate=20030430095031Z
          x509serialNumber=1000
        x509CRLThisUpdate=20030430095546Z
          x509serialNumber=1000
          x509serialNumber=1001
        x509CRLThisUpdate=20030430100646Z
          x509serialNumber=1000
```

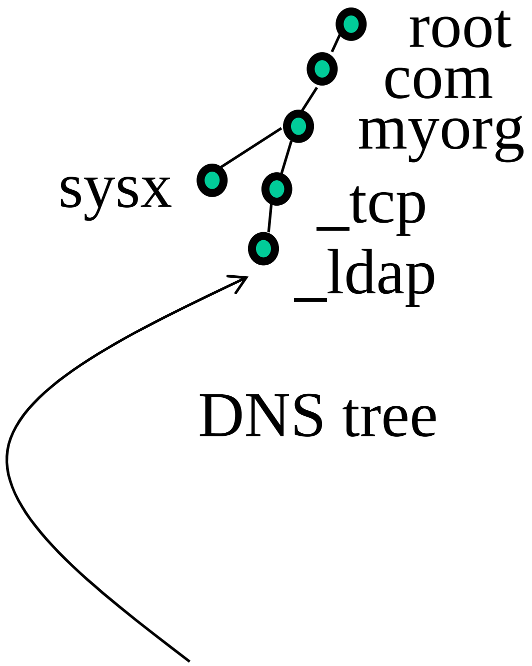
Attribute	Value
x509serialNumber	1001
x509CRLCertRevocationDate	20030430095546Z
objectClass	x509base
objectClass	x509CRLentry

Finding the right LDAP server

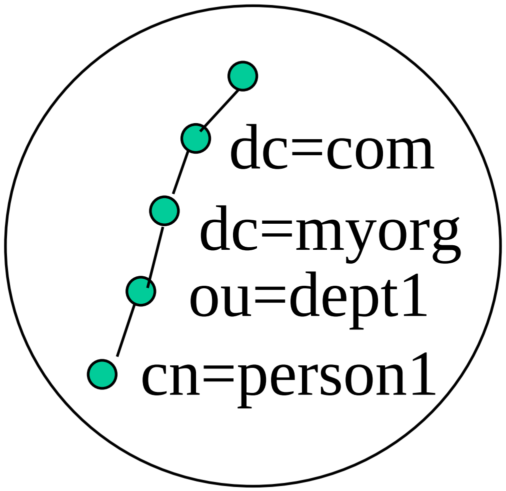
- Use the AIA extension defined by PKIX
  - But need to have one cert to find next in chain
  - Note that AIA works for http, ftp as well as ldap
- If using DC based naming, convert user's DN into a domain name
  - start at RHS and stop at first non-DC RDN e.g. cn=david chadwick, ou=sales, dc=jtm, dc=com becomes jtm.com
  - Then lookup WKS RR or SRV RR in DNS
  - But need to know DN of certificate subject
- If not using DC based naming much harder
  - Pre-configure LDAP clients (Entrust solution) with details of LDAP server
  - Have an LDAP knowledge server that returns referrals

Example Use of SRV Records

- E.g. I want the certificate for cn=person1, ou=dept1, dc=myorg, dc=com
- This maps to DNS name myorg.com



DNS tree



LDAP server running in sysx.myorg.com

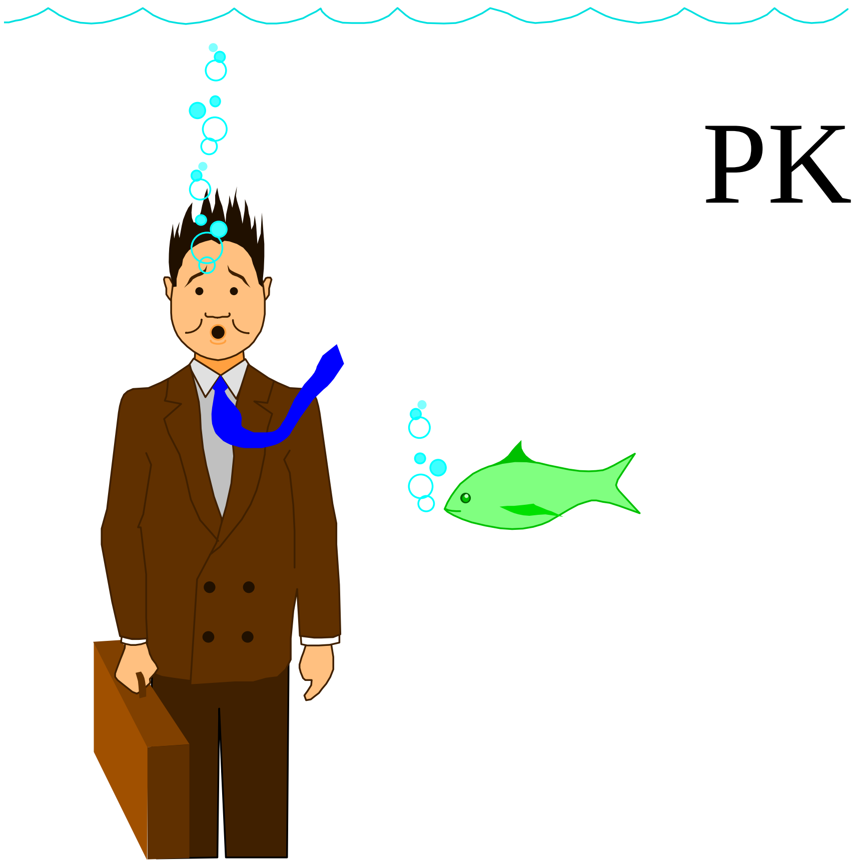
IN SRV 86400 0 0 389 sysx.myorg.com

Finding the right Certificate/CRL

- Because of all the problems with LDAP, Peter Gutmann suggests using the Web as the public repository as follows:
- Simple solution
  - Stick a base64-encoded certificate on your home page
  - Add a standardised string for search engines, e.g. certificate joe@foo.com
  - Search Google, cut & paste
- Proper solution
  - Use HTTP to fetch keys from a backend database
  - GET *uri?attrib=value* e.g. GET /search-cgi?email=joe@foo.com
  - Define a whole set of attributes
  - This would work nicely with an XPS backend!!

Confusion between Authentication and Authorisation

- PKI was always intended as an authentication infrastructure
- But people try to use it as an authorisation infrastructure, which is shown in such statements as
- “the "all-or-nothing" trust policy implicit in PKI for SSL and browsers is less than helpful”
- “It doesn't make sense for applications to rely on the 100-odd certs of often-dubious provenance trusted by most browsers. Instead there should be application-specific roots matched to the policies and needs of the application”
- But if a user’s signed request was only used to authenticate the user/signing key and in addition the user had to have an authorisation certificate to gain access (which could be tied to their public key or name) then the root cert problem disappears.



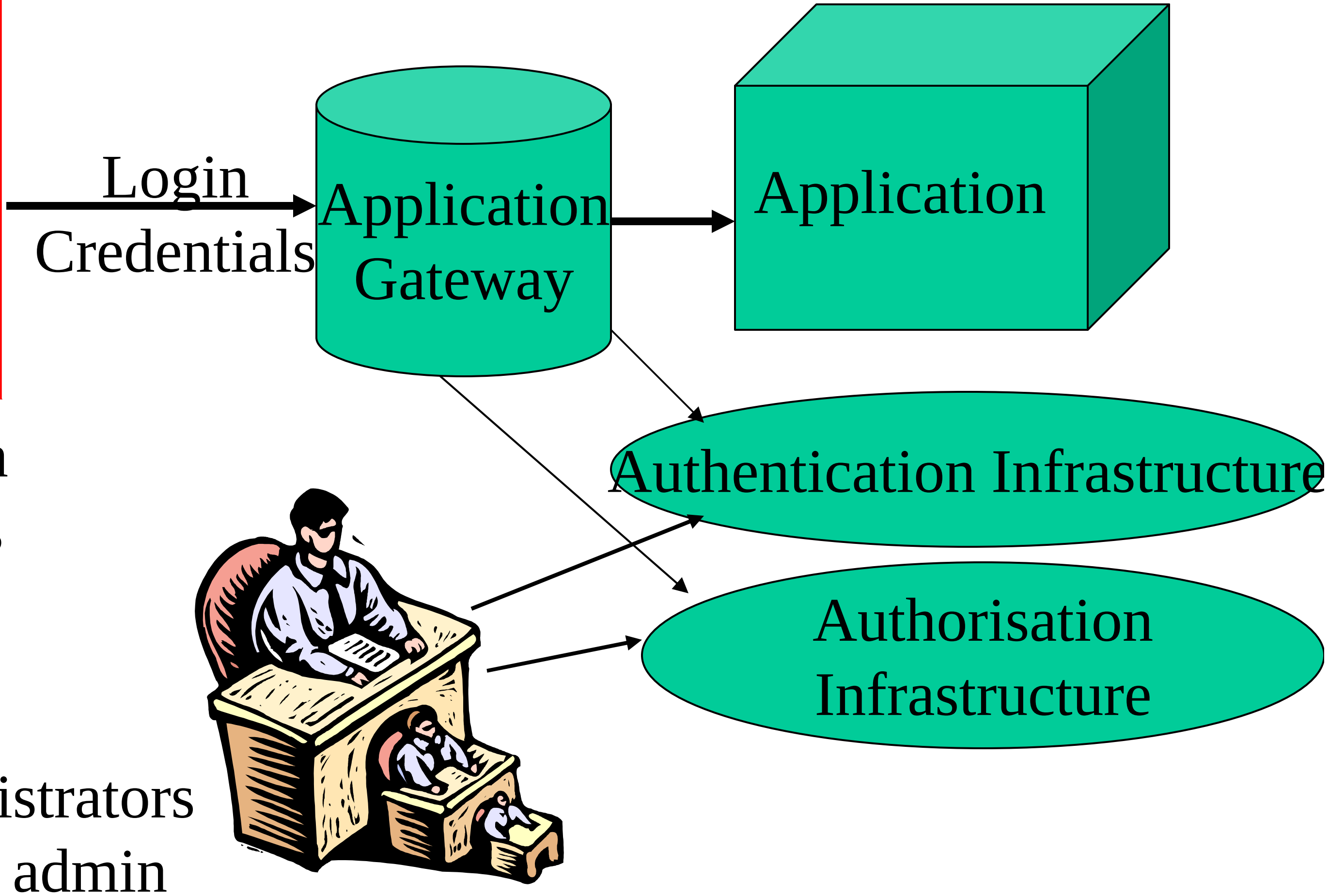
PKI Future

Some things to Aim for

- Single Sign On
  - – We might be getting there with Shibboleth and Liberty Alliance
- Separate authentication and authorisation into two infrastructures – PKI and PMI (Privilege Management Infrastructure) e.g. as in X.509 2001, and remove authorisation from the user
- Automate the handling of Trust in the PKI to a Trust Management Infrastructure
- Make PKI user friendly and ubiquitous

Separate Authn & Authz Infrastructures

- Authentication and Authorisation are External to the Application
- Authorisation is external to the user



Login Credentials

Application Gateway

Application

Authentication Infrastructure

Authorisation Infrastructure

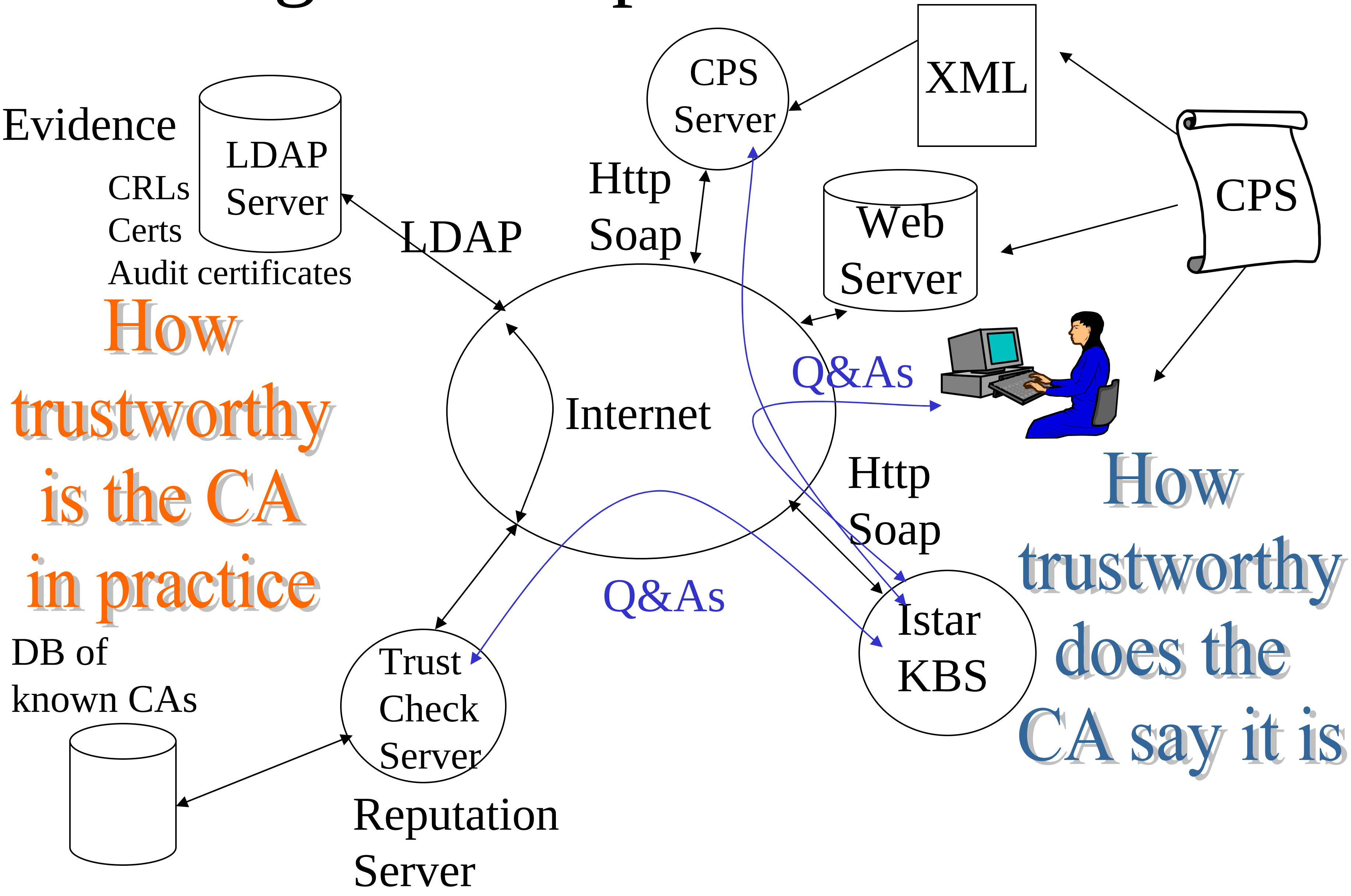
One password or pin
to access credentials
Happy Users!

Fewer Administrators
Lower cost of admin
Overall Security Policy

Have a Trust Management Infrastructure

- Have a trust management infrastructure that can compute trustworthiness of entities - PKI roots and end users
- Reputation systems for end user trust are already in existence e.g. e Bay
- Research system has already been produced for calculating the trustworthiness of PKI roots – e.g. the Intelligent Computation of Trust project at UoS

Intelligent Computation of Trust



Evidence

CRLs
Certs
Audit certificates

LDAP
Server

LDAP

CPS
Server

Http
Soap

XML

CPS

Web
Server

Internet

Q&As

How trustworthy is the CA in practice

Http
Soap

Q&As

DB of
known CAs

Trust
Check
Server

Reputation
Server

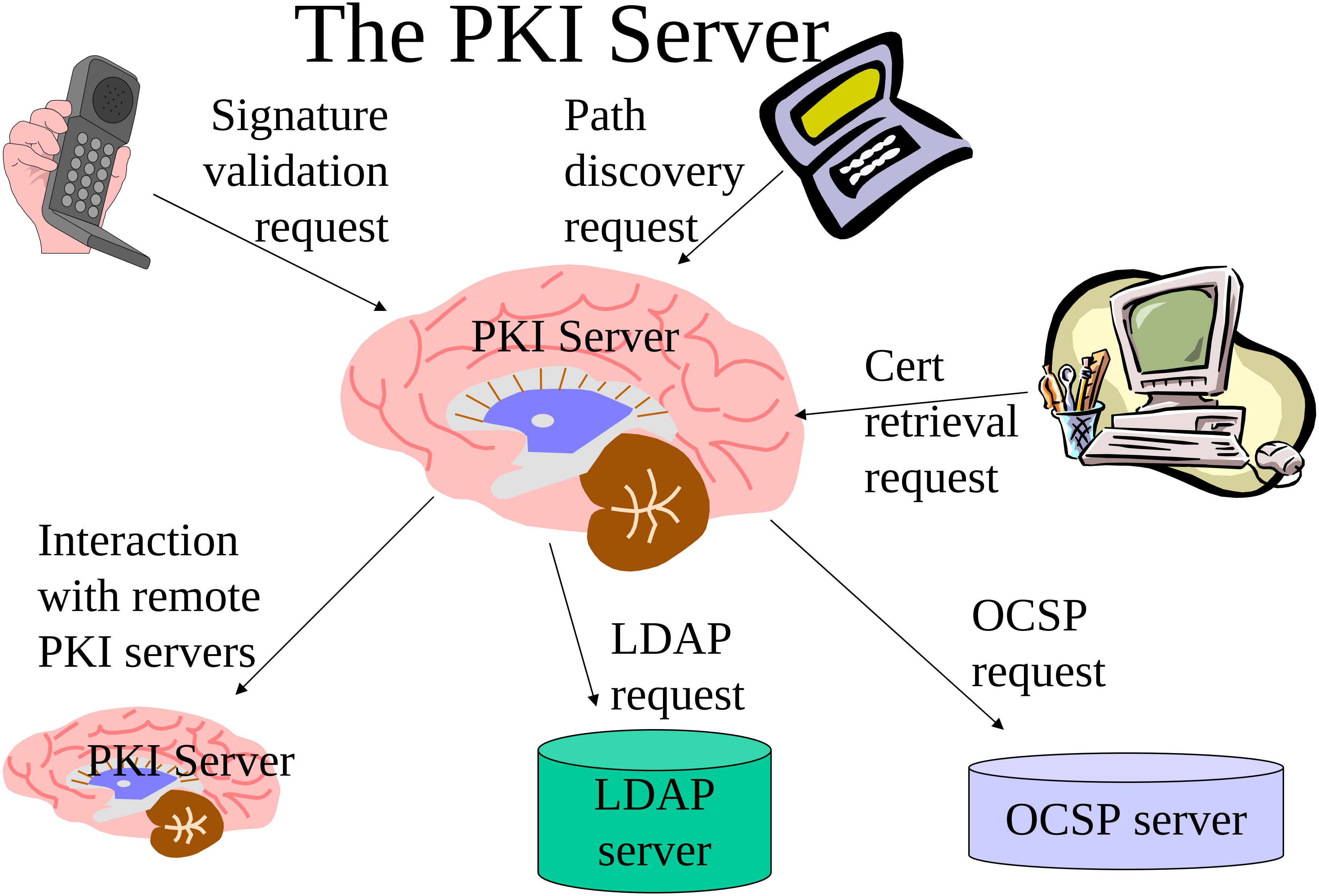
Istar
KBS

How trustworthy does the CA say it is

Link Authorisation Infrastructure to Trust Management Infrastructure

- Tie the authorisation decision making process into the trustworthiness of the user and the PKI root E.g.
  - User can read resource ***X*** if Authentication Level > 1 and CA's trust quotient > 0.3 and user's reputation > 0.6
  - User can write to resource ***X*** if Authentication Level > 2 and CA's trust quotient > 0.5 and user's reputation > 0.9
- NIST already have a Draft Recommendation for Electronic Authentication
  - Special Publication 800-63, Jan 2004, defines 4 levels of authentication
- We now have a couple of project to implement this into our PERMIS authorisation infrastructure

Making it simple for the user – The PKI Server



Signature validation request

Path discovery request

PKI Server

Cert retrieval request

Interaction with remote PKI servers

LDAP request

OCSP request

PKI Server

LDAP server

OCSP server

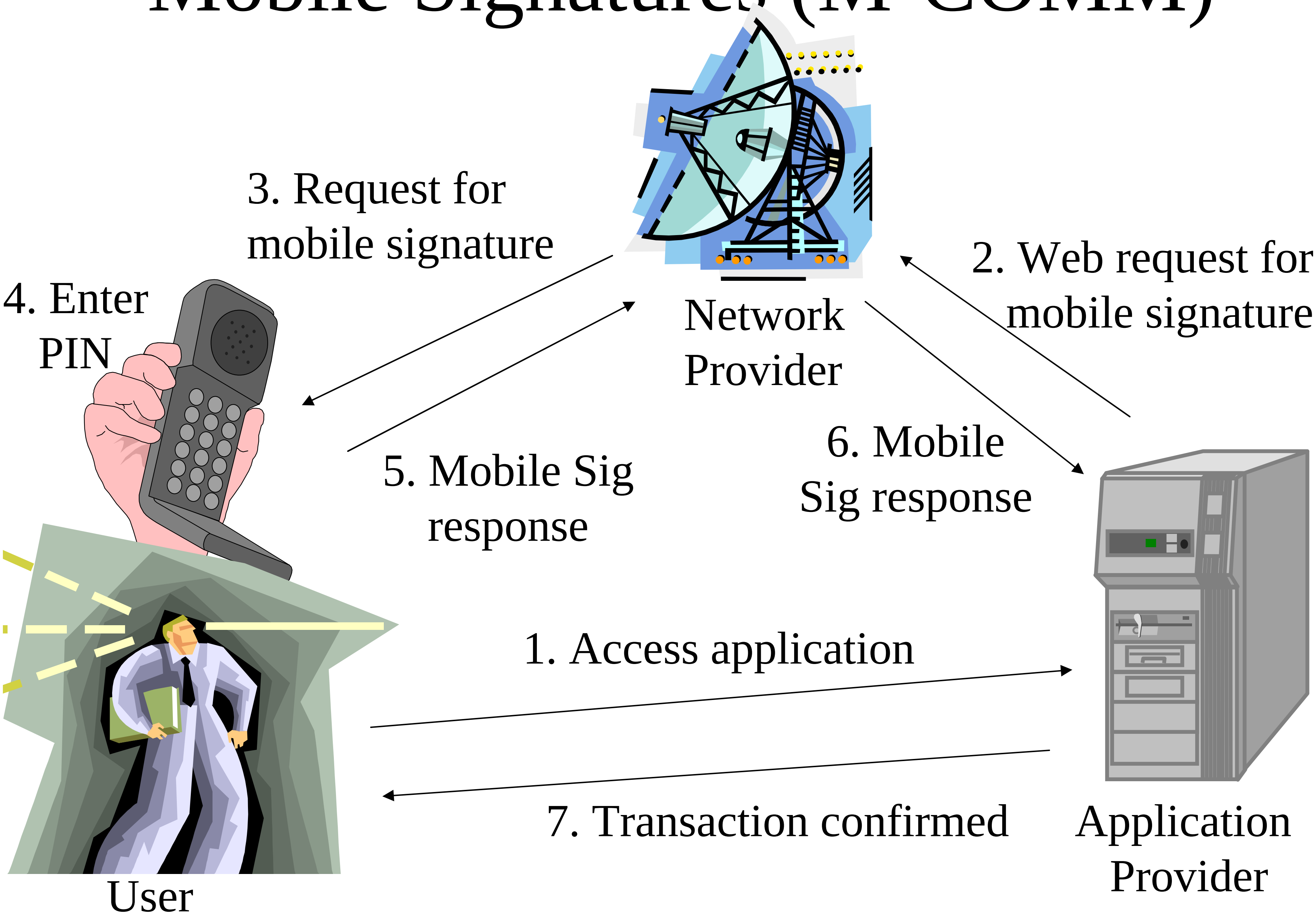
The PKI Server

- Developed by Fraunhoffer Institute in Germany
- PKI server is responsible for
  - Management of root certs and CRLs
  - Management of security policies
  - Trust path construction and validation
  - Talking various protocols e.g. OCSP, LDAP, SCVP
- PKI Server is driven by validation and signature policies
  - Persistent ones defined by the management
  - Temporary ones defined by clients
- PKI client can simply ask for
  - Signature and/or certificate validation
  - Trust path construction and/or validation
- PKI client simply has to trust the certificate of the PKI server and hence the signed responses
  - Revocation of PKI server certificate is not defined

Use of Hardware Tokens

- Keyboard sniffers are a problem when you have a software encrypted private key
  - Capture the encrypted private key file and the password
- Hardware token to hold key pair can solve this
- Smart cards – possibly
- National ID cards – more likely
- Mobile Phones – certain to be the winner
  - Provide mobility
  - Ubiquitous, 800 Million users with up to 80% coverage in some countries
  - One third are lost or stolen each year, nearly one half are replaced each year, so capability is being rolled out today

Mobile Signatures (M-COMM)



Network Provider

User

Application Provider

1. Access application

2. Web request for mobile signature

3. Request for mobile signature

4. Enter PIN

5. Mobile Sig response

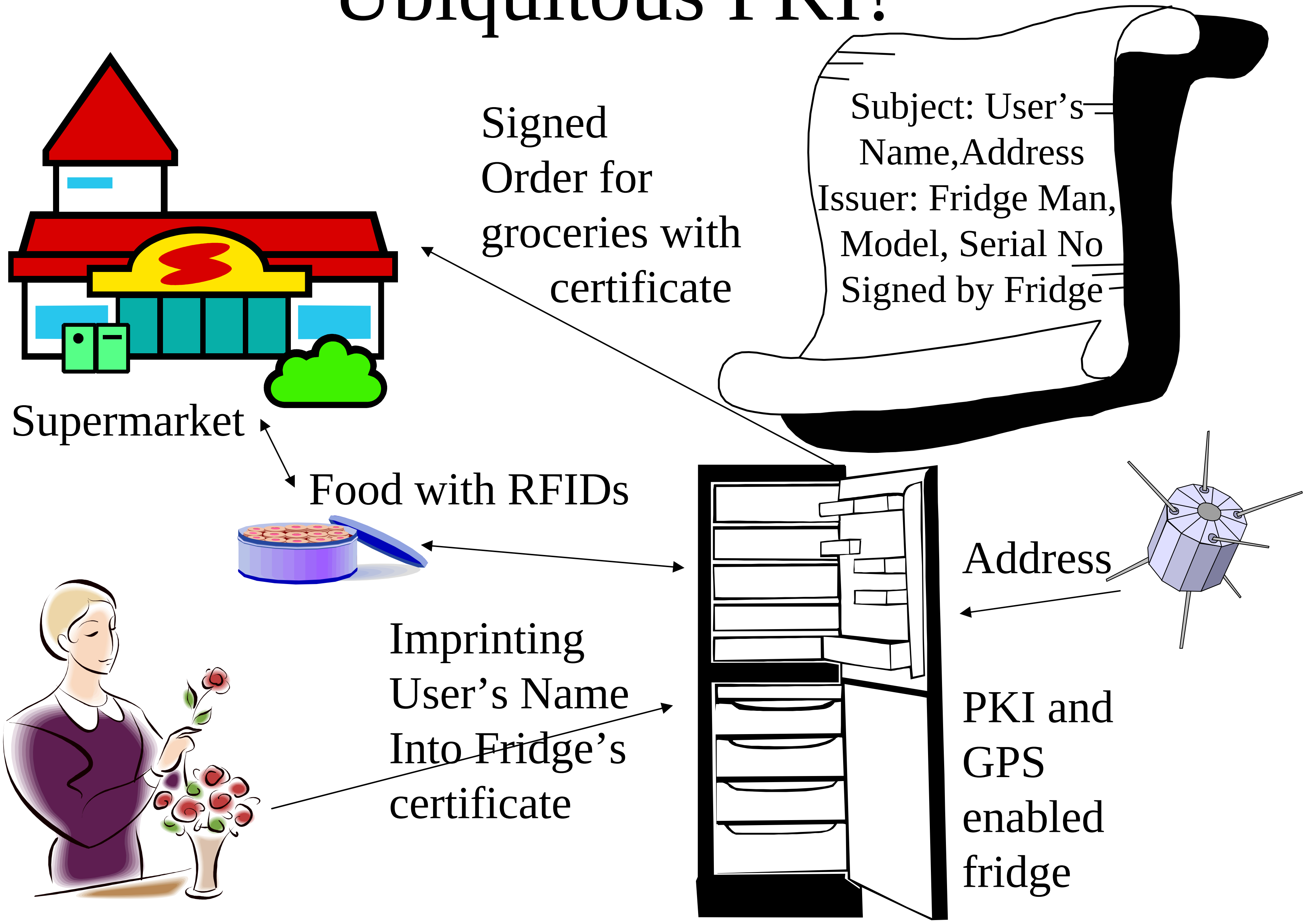
6. Mobile Sig response

7. Transaction confirmed

Features of M-COMM Standard

- Can be used for face to face and citizen not present transactions
- Signature is provided by SIM or UICC smartcards
- User is shown what they are signing and confirms it by entering a Signing PIN
- Can be used to support EC qualified signatures
- Provided as a web service to application providers
- Defined in ETSI TR/TS 102 203/4/6/7

Ubiquitous PKI?



Signed
Order for
groceries with
certificate

Subject: User’s
Name,Address
Issuer: Fridge Man,
Model, Serial No
Signed by Fridge

Supermarket

Food with RFIDs

Address

Imprinting
User’s Name
Into Fridge’s
certificate

PKI and
GPS
enabled
fridge

So What is the Future of PKI?

The Future is Bright

The Future is PMI !

The Future is Trust Management !

The Future is Mobile Phone use of PKI !

Thankyou !

- Any questions ??
??
??
??
??
??
??
??
??