Federated Identity Management

David W Chadwick

Contents

- Introduction to FIM and Background Technologies and Issues
- FIM Technologies and Systems
- Some Latest FIM Research

Introduction to FIM

David W Chadwick

Some Definitions

- Identity
  - A whole set of attributes that in combination uniquely characterise a person in a given context
    - hair colour, sound of their voice, height, name, qualifications, past actions, reputation etc
- Identification
  - The process of linking a requestor to an identity
- Authentication
  - Proving that the requestor has the right to the claimed identity
- Authorisation
  - Determining what the requestor is entitled to do

The Missing Link

Tying the requestor to an actual physical person

"On the Internet, nobody knows you're a dog."

Some More Definitions

- Attribute – a property, quality or characteristic of an entity
- Identifier – a string used to uniquely identify an entity in a domain. Often used as login id or primary key in a database. A special type of attribute since it is usually the only one *on its own* that can uniquely identify an entity in a domain.
  - X.500/LDAP DNs, IP addresses, DNS names, URIs, key IDs, login IDs, 128 bit random numbers are all identifiers.
- Attribute Assertion – a statement made by an authority that an entity has a particular attribute. An authority can be the entity itself or a (trusted) third party.
- Attribute Certificate/Authorisation Credential – a cryptographically protected (usually digitally signed) attribute assertion that can be authenticated and validated
- Attribute Authority (AA) – an authoritative source for asserting attributes about entities
- Service Provider/Relying Party – an entity that provides a service to clients
- Identity Provider – an entity that provides an authentication service, and is usually an AA for a set of identity attributes of its users

Federated Identity Management

- From the RSA Web Site
- “A federated identity is a *single user identity* that can be used to access a group of web sites bound by the ties of federation. Without federated identity, users are forced to manage different credentials for every site they use. This *collection of IDs and passwords* becomes difficult to manage and control over time, offering inroads for identity theft.”
- “Federated identity management builds on a trust relationship established between an organization and a person. A federated identity makes it possible for the end user to use one trust relationship to access information with another, related company without establishing new credentials.”

Federated Identity Management

- From the RSA Web Site
- "A federated identity is a *single user identity* that can be used across multiple networked systems that are federation. Without federated identity, users are forced to *collection of IDs and passwords* becomes difficult to manage and control over time, offering inroads for identity theft."
- "Federated identity management builds on a trust relationship established between an organization and a person. A federated identity makes it possible for the end user to use one trust relationship to access information with another, related company without establishing new credentials."

Confusing identity with identifiers and authentication with authorisation

So What is Federated Identity Management ?

- A group of organisations that set up trust relationships which allow them to send assertions about users identities between themselves, in order to grant users access to their resources
- A user can use his credentials (authn and authz) from one or more identity providers to gain access to other sites (service providers) within the federation
- The authenticating IdP will usually provide the user with Single Sign On, but this may be transparent to the SP
- FIM systems typically require the following: data repositories, communications systems, provisioning systems, access management systems, cryptographic systems, trusted third parties and legal agreements

Background Technologies and Issues

David W Chadwick

Contents

- Trust
- PKI and SSL/TLS
- PMI
- SAML assertions, X.509 ACs
- Levels Of Assurance
- SOAP, Web Services
- XML Signatures and Encryption
- Data protection legislation
- Kim Cameron's 7 Laws of Identity

What is Trust?

- Trust is a highly complex and multi-dimensional phenomenon. Highly subjective.
- Depends upon experience
  - the more you have found someone to be trustworthy, the more you are likely to trust them
- Social context
  - You are likely to be more trusting in a church than in Harlem
- Human psyche
  - Some people have a higher propensity to trust than others
- Legal context
  - Likely to be more trusting where there is strong legal protection against fraud

Trust - Some Definitions

- Trust - Firm reliance on the integrity, ability, or character of a person or thing [1]
- Trust - Firm belief in the reliability, truth, ability, or strength of someone or something [2]
- Trusting Intention: The willingness to depend on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible [3]

- [1] Dictionary.com
- [2] Oxford English Dictionary
- [3] McKnight and Chervany 1996. See http://misrc.umn.edu/wpaper/wp96-04.htm

Trust and Business

- Research has found that societies with a high level of trust (Japan, US, Germany) developed efficient large organisations, whereas societies without (France, Italy, China, Taiwan) developed business around families [1]
- Research also found that societies with a higher level of trust tended to be economically more advanced than those where there is little trust [2]
- Trust represents the amount of social capital in a community [1]
- Trust reduces the costs of doing business [2]
- Trust is essential and indispensable to businesses

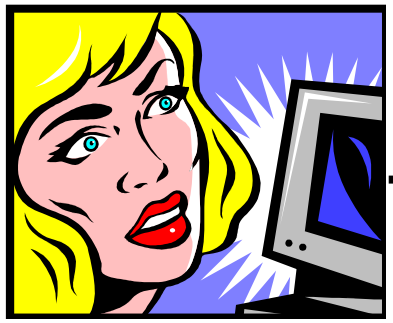
- [1] Social Capital and the Global Economy: A Redrawn Map of the World by Francis Fukuyama From *Foreign Affairs*, September/October 1995. See http://www.foreignaffairs.org/19950901faessay5067/francis-fukuyama/social-capital-and-the-global-economy-a-redrawn-map-of-the-world.html
- [2] **Trust and Growth** by PAUL J. ZAK Claremont Graduate University - Center for Neuroeconomics Studies and STEPHEN KNACK World Bank - Development Economics Research Group (DECRG) September 18, 1998. Available from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=136961

Trust Decision and Trustworthiness

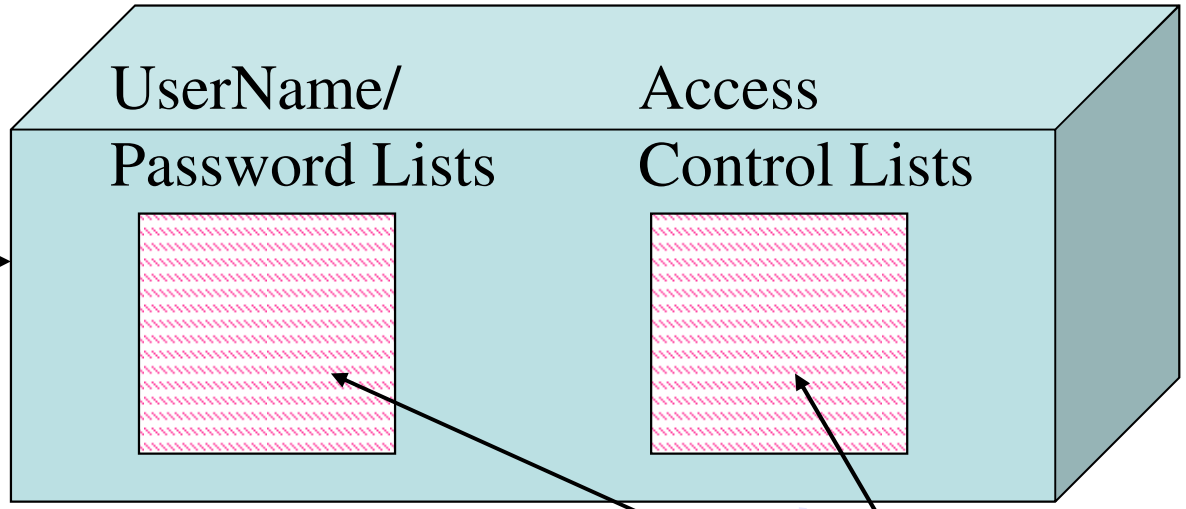
- Trust decisions are binary decisions – you either trust someone to do something or you do not trust them
- BUT Trustworthiness is a variable metric
- If Trustworthiness > some threshold Then the Trust Decision is to Trust
- If Trustworthiness < some threshold Then the Trust Decision is Not to Trust
- PKIs/PMIs are binary systems. A Certificate is either trustworthy or not trustworthy
- Reputation systems use a variable metric so as to get a better measure of trustworthiness
- PREDICTION. Today's FIMs are based on PKIs/PMIs and binary decisions, but tomorrow's FIMs will be based on reputation systems, LOAs and variable metrics

Traditional Applications

- Authentication and Authorisation are Internal to the Application
- Typically based on weak passwords



Multiple passwords
Multiple usernames
Confusion!!



Multiple Administrators
High cost of administration
No overall Security Policy

- Costly, difficult to scale to Internet proportions
- But no Trust required in external entities

Enter Authentication Infrastructure

e.g. PKI, OpenID, Shibboleth etc

- Authentication is External to the Application

Login Credentials

Application Gateway

Access Control Lists

Authentication Infrastructure

One password or pin to access credentials

Happy Users!

Multiple Administrators
High cost of administration
No overall Security Policy

- **Less cost, but now you need to Trust the external authn infrastructure**

Enter Privilege Management Infrastructure

- Authentication and Authorisation are External to the Application

Login Credentials

Application Gateway

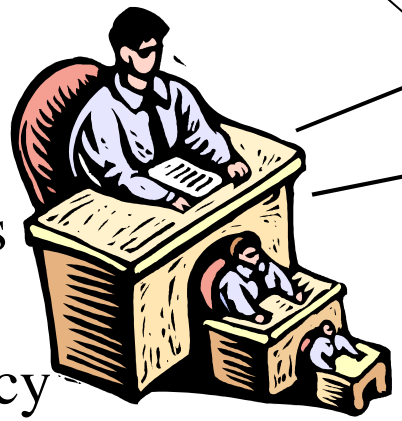
Application

Authentication Infrastructure

Authorisation Infrastructure

One password or pin to access credentials

Happy Users!



Fewer Administrators
Lower cost of admin
Overall Security Policy

- Least cost, but amount of Trust you need is highest

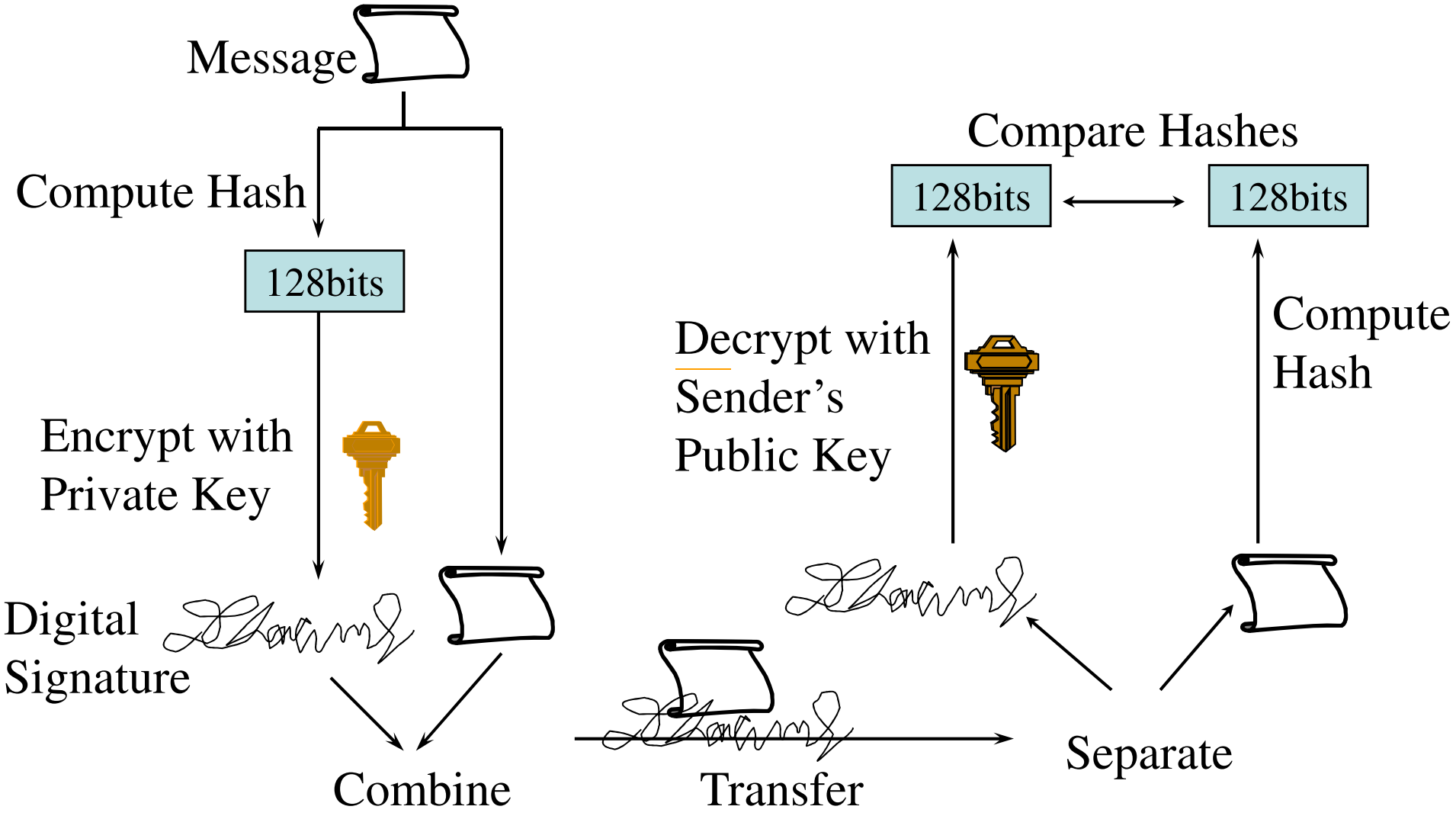
Public Key Infrastructures

- Built upon
- Asymmetric Encryption
- Digital Signatures
- Trust
- (Hierarchies of) Certification Authorities and Bridge CAs

Asymmetric Encryption

- Two keys - one encrypts, the other decrypts (Different from symmetric encryption which uses only one key)
- When encryption key is kept private, and decryption key is made public, basis for authentication
- When decryption key is kept private, and encryption key is made public, basis for confidentiality
- But algorithms are slower than symmetric ones

Digital Signature



TRUST in the Signature

- However…..
- We can only trust that the message came from the sender, if…….
- Only the sender can access the private key
  - If someone else can use my private key then they can masquerade as me
- The receiver has the correct public key for the sender
  - How do you know that it is actually my public key that you have? If it actually belongs to someone else, they can masquerade as me

Public Key Distribution

- How do we know that this public key REALLY belongs to that remote user?
- Potential for masquerade (key substitution)
- Have to secure them prior to network distribution
  - Digitally sign the key and owner's identity into a public key certificate
- Three ways to distribute public keys (certificates)
  - Personally exchange public keys (as in PGP)
  - Get a public key from someone you trust (e.g. a PGP trusted introducer)
  - Get a certified key (certificate) from a public repository (as in PGP and X.509)
- The key certifier is called a Certification Authority (CA)

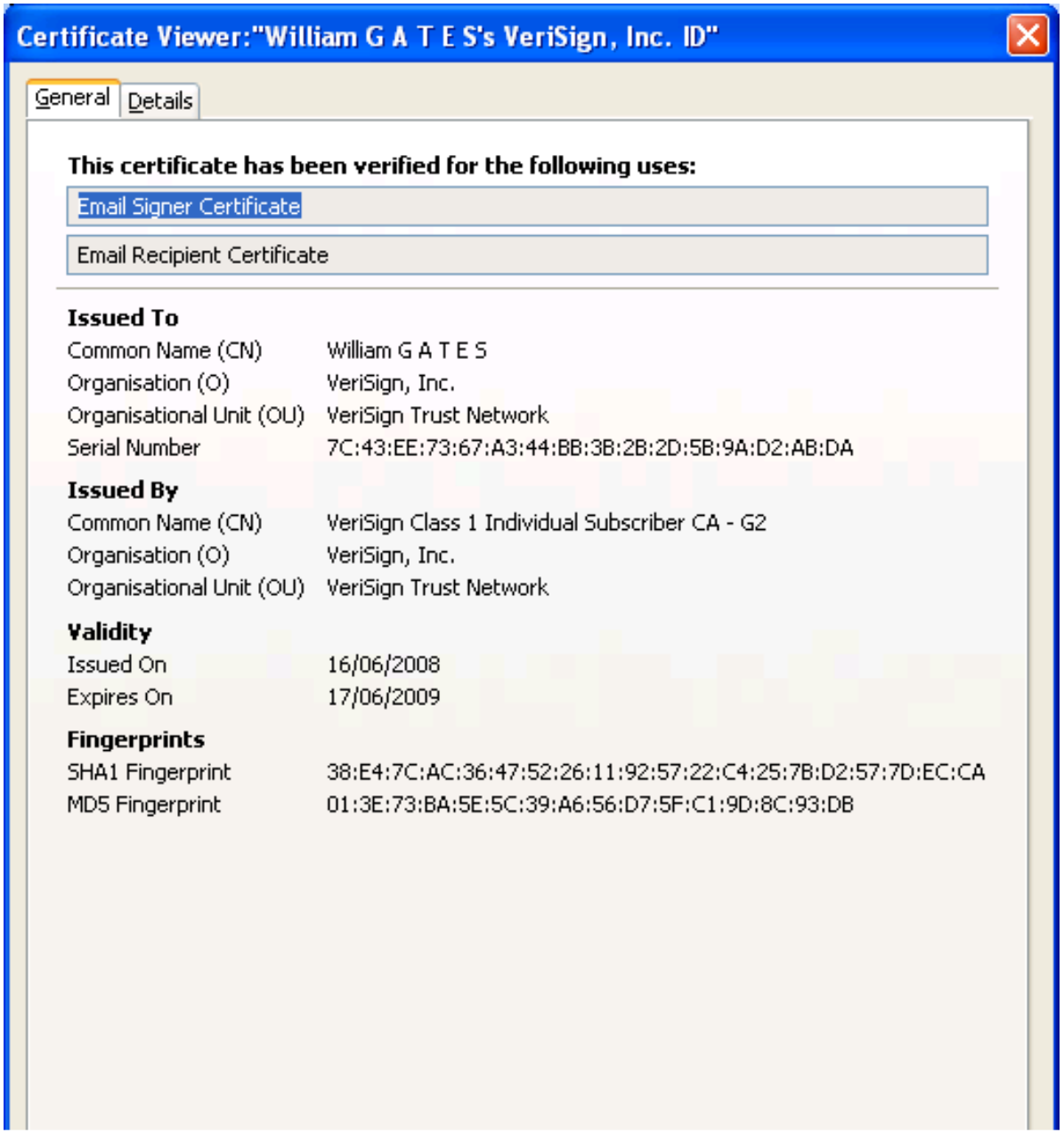
Public Key Certificates (PKCs)

- Secure way of distributing public keys
- Signed by private key of issuer - called a Certification Authority (CA)
- With public key of CA, can check validity of certificate
- X.509 Certificate contains
  - distinguished name of user (plus other optional name forms)
  - public key of user
  - distinguished name of CA
  - validity time
  - Algorithm information
  - Optional policy extensions concerning use of certificate

Distribution of Root CA Public Keys

- Have to be distributed out of band in a trustworthy manner
- Usually distributed as Self Signed PKCs
  - The private key owner signs its own public key
  - Issuer and Subject are the same
- Provides tamper resistance
- But WORTHLESS in themselves for building TRUST
- Therefore must be obtained in a trustworthy manner and be kept securely
- Your web browsers contain dozens of root CA public keys
- But this still does not help, since you still have to know/recognise the name of the subject in their PKC, and trust the CA to have checked that it is the correct name for the physical entity

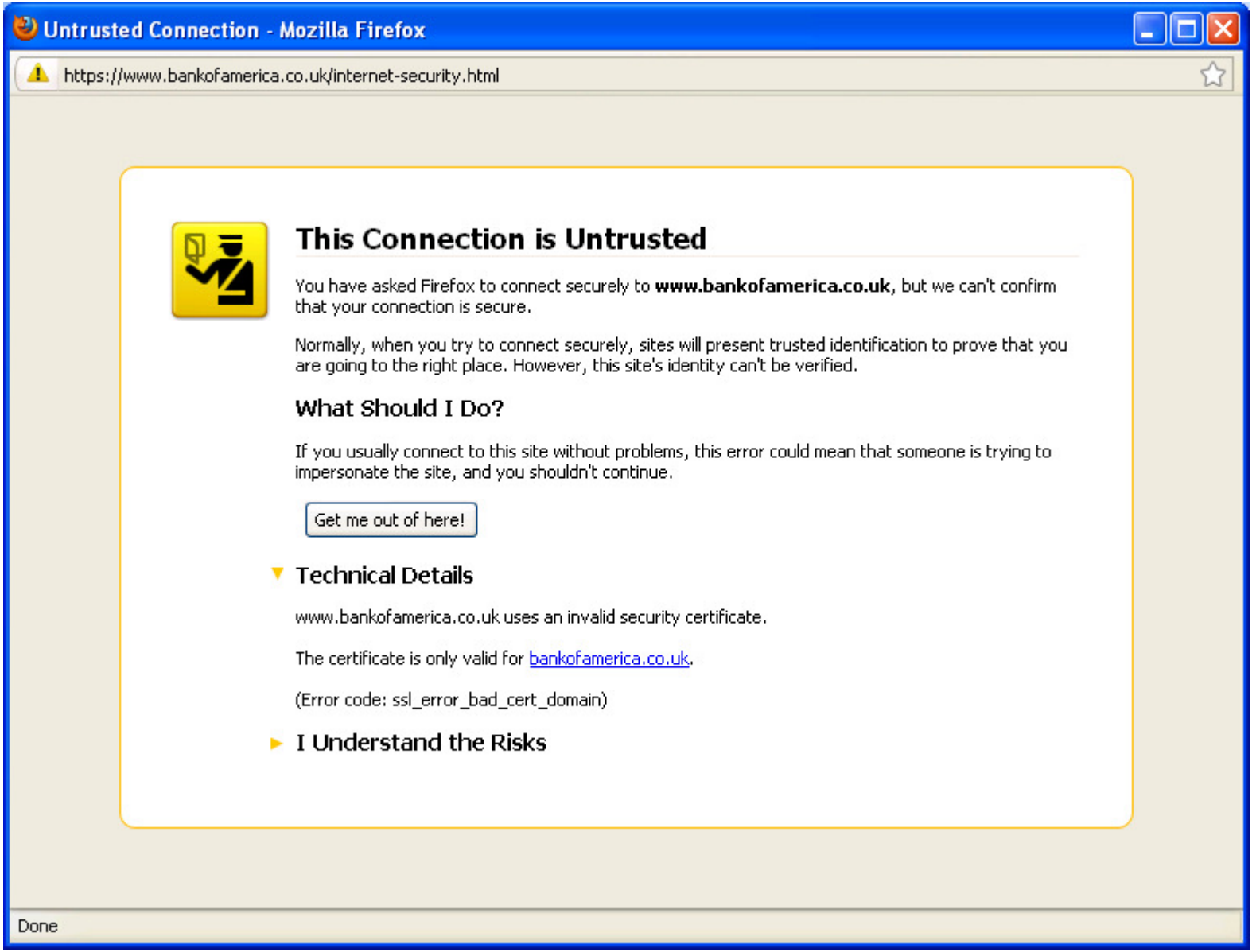
Is this CA trustworthy?



If CAs are NOT Trustworthy

- Why not dispense with CAs altogether and simply distribute public keys in an ad-hoc manner?
  - Some FIM systems do this
  - Some FIM systems even dispense with public keys and use symmetric encryption instead
- OK for small scale FIM between servers, but not for user facing servers, as this introduces the following usability problem

Web site with unknown/untrusted CA



PKI Usability Problems

- Users don't understand key pairs and certificates (e.g. will send p12 files to other people)
- Browser suppliers don't implement PKI properly e.g. see
- Ahmad Samer Wazan, Romain Laborde, David W Chadwick, François Barrere, AbdelMalek Benzekri. "Which web browsers process SSL certificates in a standardized way?" 24th IFIP International Security Conference, Cyprus, May 18-20th, 2009
- Browser suppliers don't provide user friendly or standard interfaces to view or manage certificates
  - E.g. keys and certificates are held in different places by different browsers (e.g. windows registry or internal) and use different names for the same key pair
- Recognising the SSL site is the genuine site
  - E.g. Z1ON Bank and ZION Bank

SSL/TLS in brief (1)

- SSL provides data integrity and an encrypted channel for the Web (https://) plus optional user authentication
- A Web server usually gets an X.509 public key certificate from a CA
- A copy of the root CA's self signed certificate is built into Web browsers
- A Web browser contacts a Web server (https://) and the server returns its certificate so that the client can authenticate it
- A random secret is generated by the browser and transferred to the server, encrypting it using the server's public key from the certificate
- Now both client and server can use the secret to provide a confidential channel with data integrity

SSL/TLS in Brief (2)

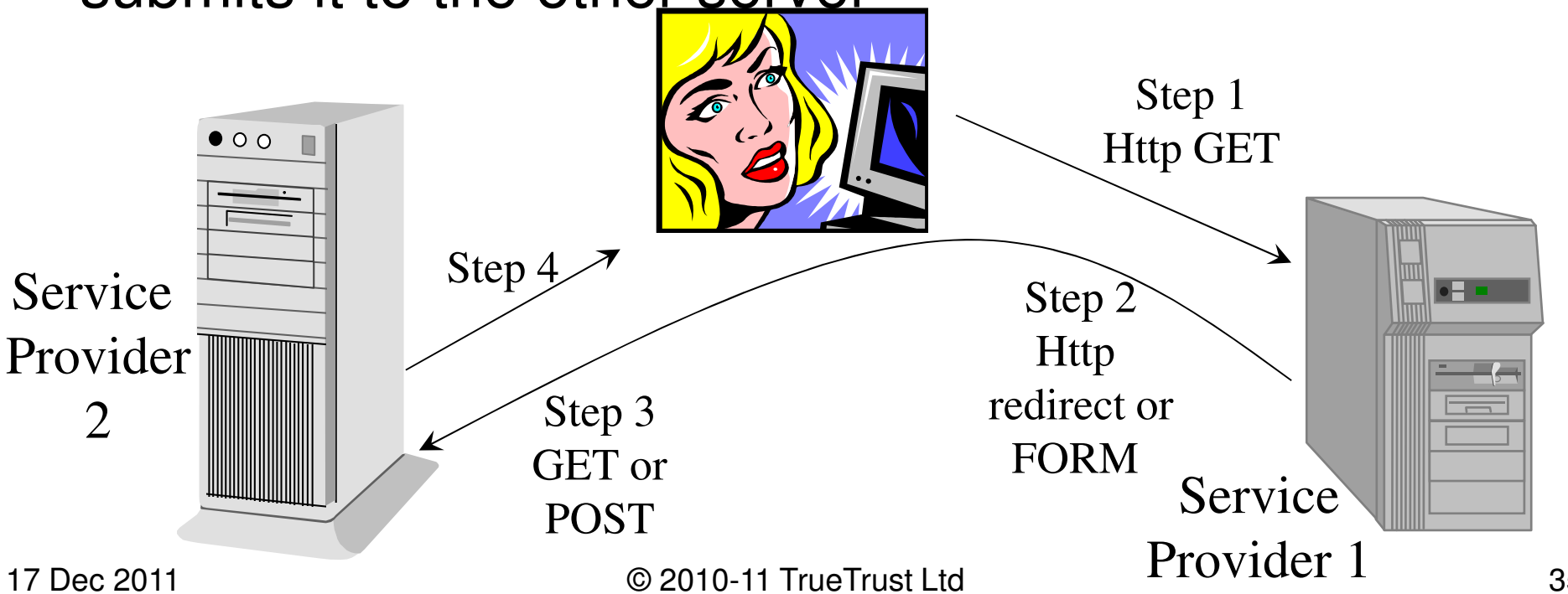
- Some Web sites dispense with CA issued certificates and mint their own
- The user then gets a warning message that the site is untrusted and they have to accept the certificate
  - Most users simply click Yes whenever they are asked anything
- TLS is the Internet standard version of SSL but they are incompatible
  - SSL mandated RSA which was patented whereas TLS mandates DSA and Diffie Hellman
  - Message authentication codes in TLS are performed using the HMAC algorithm whereas SSL has its own keyed MAC algorithm
- SSL/TLS only provide point to point security and not end to end

What is SOAP?

- SOAP (the Simple Object Access Protocol) is an XML-based messaging protocol
- SOAP defines a set of rules for structuring messages that can be used for simple one-way messaging, Remote Procedure Calls (RPCs) and request-response type dialogues
- Used to integrate new and legacy applications into an Internet/Web services environment. Clients and servers communicate using SOAP
- SOAP protocol specification comprises three parts
  - Contents of SOAP messages
  - SOAP encoding rules (says how data types and values are passed)
  - SOAP RPC mechanism (defines a way of invoking procedures on remote servers and returning the outputs)
- One SOAP binding specifies how to carry SOAP between client and server via a browser using http Form-POST and GET

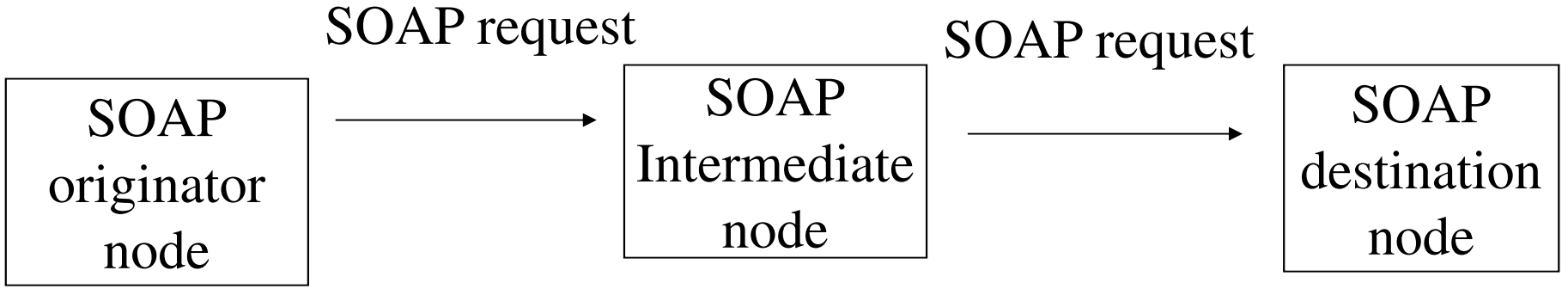
HTTP Redirect and Form-POST

- Http Redirect (status code 3xx) – allows one web server to pass information to another server via the browser, as info in a URL
- Http Form-POST – one server builds a form with an action to POST it to another server, delivers the form to the browser in the message body, which then submits it to the other server



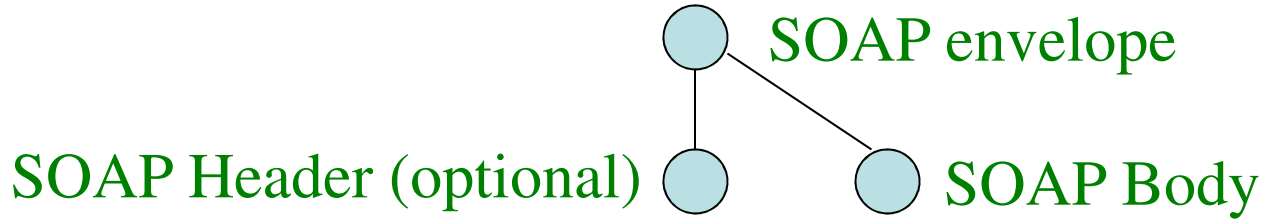
SOAP Distributed System Model

- SOAP messages can optionally be passed via intermediate nodes, which can each process the message before passing it onto the next node
- SOAP Header tells intermediate node what is expected of it
- Different nodes can use different underlying protocols to pass the SOAP messages between themselves



SOAP Messages

- A SOAP Message is an XML document comprising three parts
- A SOAP outer envelope, an optional SOAP header, and a SOAP body

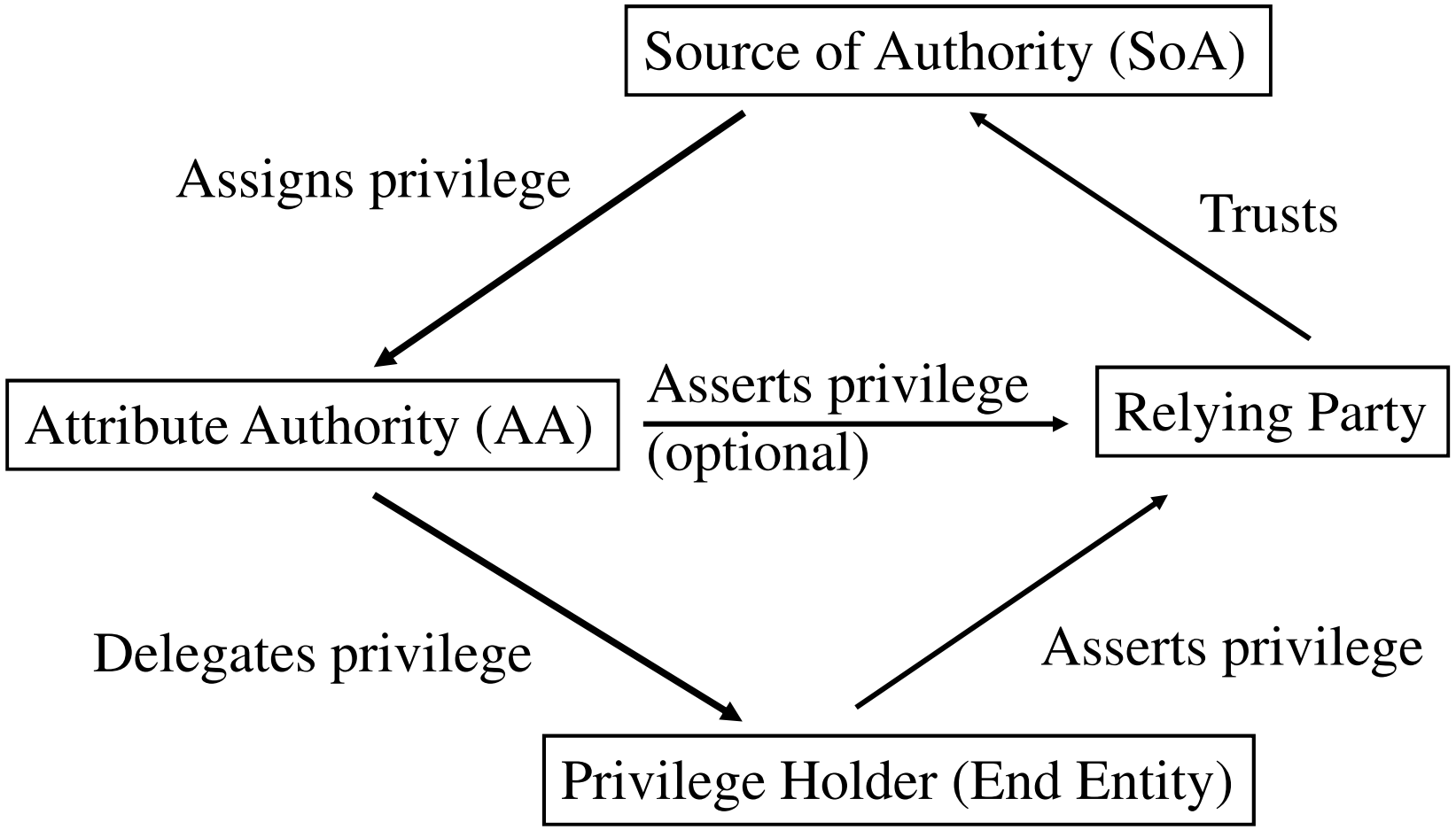


- Envelope
  - Contains namespace declarations and encoding mechanism
- Header (optional)
  - Has actor attribute to say which application/node must process it
  - Has mustUnderstand attribute (boolean) to direct the actor
  - Has application specific control data for the intermediate nodes
- Body
  - Contains application specific data to be processed by the final destination node
- But SOAP does not define any security mechanisms
  - Use XML signatures and XML encryption to protect SOAP messages as directed by WS-* standards

Privilege Management Infrastructures

- Built upon
- Sources of Authority who assign attributes to users and issue them as attribute assertions or attribute certificates (authorisation credentials)
  - Usually based on asymmetric encryption and digital signatures
- Relying Parties who trust the SOAs, validate their attribute assertions/ certificates and give users access to their resources based on these attributes

PMI Entities



Authentic vs. Valid Credentials

- Authentic credentials are ones that have not been tampered with and are received exactly as issued by the issuing authority
- Valid credentials are ones that are trusted for use by the target resource site
  - Example 1: Monopoly money is authentic if obtained from the Monopoly game pack. It was issued by the makers of the game of Monopoly. Monopoly money is valid for buying houses on Mayfair in the game of Monopoly, but it is not valid for buying groceries in Tesco's or LIDL.
  - Example 2: My Amex card is authentic. I can use it to buy groceries in Tesco, so it is valid there, but I cannot use it to pay motorway tolls in France. It is not valid there, but it is still authentic.

What are X.509 Attribute Certificates and SAML Attribute Assertions?

- Data structures for holding any arbitrary attribute assertion about a holder
- They must contain
  - The holder
  - The issuer
  - The validity time of the assertion
  - The attributes
  - The digital signature of the issuer (unless a trusted channel is used)
- They may contain
  - Policy information of the issuer e.g. which targets they are valid for, whether they can be delegated etc.
  - Digital signature of the issuer
  - Any arbitrary extensions

Security Assertions Markup Language (SAML)

- Industry standard specified by OASIS
- Allows security assertions to be encoded in XML
- Authentication assertion states how the subject was authenticated
- Attribute assertion states which attributes have been assigned to the subject
- Authorisation decision assertion states which access to which targets has been granted or denied to the subject (deprecated in v2.0 in place of XACML decisions)
- Three versions, v1, v1.1 and v2.0

SAML Assertion Contents

- The assertion
- name of the issuer of the assertion
- the date and time the assertion was issued
- an assertion ID (for ease of subsequent reference)
- the version of SAML the assertion conforms to
- some optional conditions (that must be obeyed by the assertion user if they are present)
- some optional advice (that can be ignored by the assertion user)
- Optionally, the digital signature of the issuer

What are the differences?

- **X.509 ACs**
- Binary encoding using BER
- Signature is mandatory
- No protocol specified but can be sent by many protocols (LDAP, email, S/MIME etc.)
- Supports XML attributes in ACs
- Has a fully specified trust model linked to X.509 PKIs
- Has a revocation mechanism
- ACs can be short lived or long lived
- Supports delegation of ACs

- **SAML Attribute Assertions**
- XML Text encoding
- XML Signature is optional
- SAML defines a standard protocol for transfer
- Supports X.509 ACs as attributes in SAML assertions after base64 encoding
- Possibly could use X.509 PKIs
- Has no revocation mechanism (uses short lived assertions only)
- SAMLv1 does not support delegation but SAMLv2 does
- Supports encrypted info

Advantages of SAML over X.509 ACs

- SAML maps better to current web services
  - URIs/URLs and HTTP re-direct in particular
- SAML maps better to legacy authentication schemes because the assertions can include any type of authentication ID and indicate the authn mechanism
- Much better industry support
  - Defined by OASIS along with XACML
- Much better academic support
  - SAML used by Shibboleth, and Shib is being rolled out throughout Europe and USA
  - But all for short lived assertions

Disadvantages of SAML vs X.509 ACs

- No revocation mechanism
- Currently the performance of XML signatures is poor
- Size of XML assertions is large (compared to ASN.1 BER encoding of ACs)
- Today most applications use SSL to protect the transfer of messages, so they are using ASN.1 BER already. Mobile phones also use X.509 public key certs and have the ASN.1 machinery, so XML processing and encoding is another large overhead. But ASN.1 is also difficult to use, so…

JSON

- A lightweight data-interchange format
- Based on a subset of the JavaScript Programming Language, Standard ECMA-262 3rd Edition - December 1999
- Text format for carrying
  - A collection of unordered name/value pairs (i.e. an object) and
  - An ordered list of values (i.e. an array)
- An object begins with { ends with } each name is followed by : and the name/value pairs are separated by a comma
  - E.g. {“firstName”:“David”, “surname”: “Chadwick”, “age”:21}
- An array begins with [and ends with] and values are separated by commas
  - E.g. [Monday, Tuesday, Wednesday]
- The format is recursive in that a value can be a string, a number, a boolean (true or false), an object or an array, or null
- Being used in some of the latest FIM technologies such as OAuth 2, to transfer identity information

JSON Example

```
{"menu":
  { "id": "file",  "value": "File“,  "popup":
      {  "menuitem": [
         {"value": "New", "onclick": "CreateNewDoc()"},
         {"value": "Open", "onclick": "OpenDoc()"},
         {"value": "Close", "onclick": "CloseDoc()"}
                        ] } }}
```

The same text in XML

```
<menu id="file" value="File">
  <popup>
    <menuitem value="New“ onclick="CreateNewDoc()" />
    <menuitem value="Open" onclick="OpenDoc()" />
    <menuitem value="Close" onclick="CloseDoc()" />
  </popup>
</menu>
```

From http://www.json.org/example.html

SAML Request/Response Protocol

- SAML assertions can be Requested and returned in SAML Responses
- SAML Request/Response Protocol can be mapped onto any underlying protocol. Http and SOAP is standardised
- SAML authentication request asks “What assertions containing authentication statements are available for this subject?”
- SAML attribute query asks “Can you return the requested attributes for this subject?”
- SAML authorisation decision query asks “Should these actions on this resource be allowed for this subject, given this evidence?”

SAML Request Contains

- the SAML query
- a unique request ID
- the date and time the request was issued
- the type of assertion responses the requestor would like to be returned to the query (called Respond With parameters) – removed in v2.0
- the digital signature of the requestor (optional)
- the version of SAML this message conforms to

SAML Response Contains

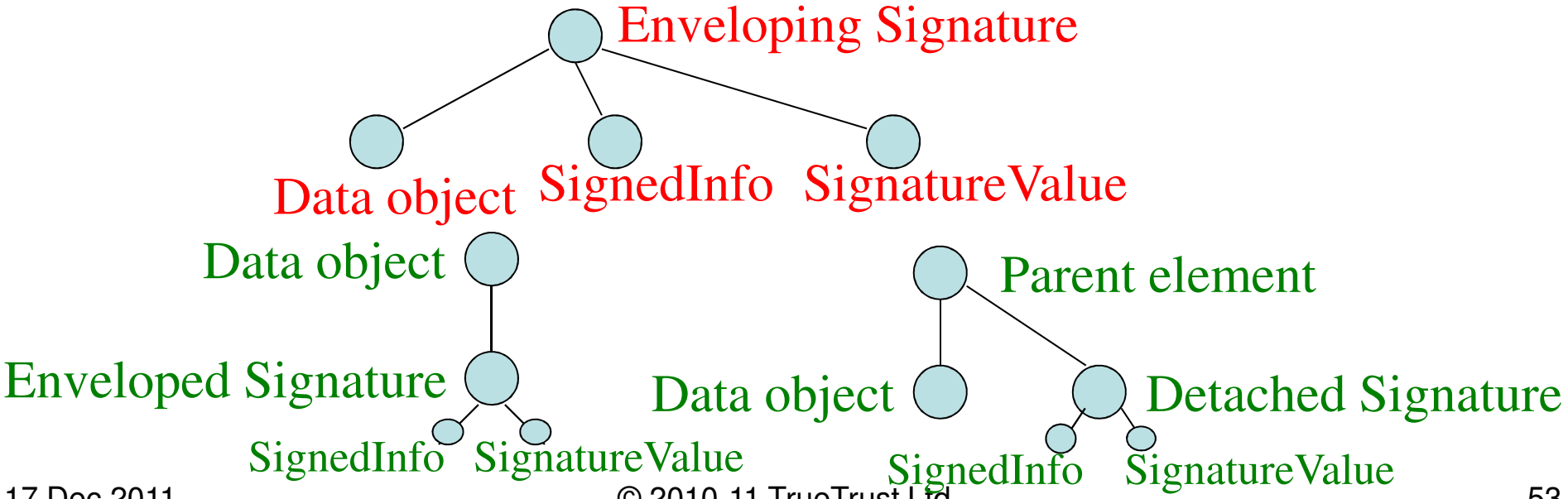
- zero or more SAML assertions
- a status code (indicating if the request was successful or not)
- the unique ID of the original request
- a unique ID for this response (optional)
- the time the response was issued (optional)
- the intended recipient of the response (optional)
- the digital signature of the responder (optional)
- the version of SAML this message conforms to

Some SAML Limitations

- Cannot dynamically (only statically) combine an authentication request and an attribute request to ask for a specific set of attributes
  - E.g. authenticate this user and return his qualifications and credit rating
  - Have to have predefined metadata that says which attribute types are wanted (i.e. static)
- Open to phishing attacks when a bad SP directs a user to a false IdP which tricks the user into releasing their un/pw

XML Signatures

- Provide integrity and message authentication and/or signer authentication of the contents of an XML document, or of external documents (via URL refs)
- XML Signature can be
  - Detached – the signed data is a sibling or external
  - Enveloping – the data is within the signature element
  - Enveloped – the signature is within the data element



XML Encryption

- Used to encrypt (all or parts of) XML documents and external objects
- An Encrypted data object contains
  - Information about what has been encrypted
  - Information about the encryption algorithm used
  - Information about the encryption key used
  - The encrypted information (or a pointer to it)
  - Additional information about the generation of the encrypted data
- The encrypted data object can be either
  - Application data, or
  - An encryption key

Level of Assurance (in Authentication)

- William E. Burr, Donna F. Dodson, Ray A. Perlner, W. Timothy Polk, Sarbari Gupta, Emad A. Nabbus. “Electronic Authentication Guideline”, NIST Special Publication NIST Special Publication 800-63-1, Feb 2008 (revised draft July 2011)
- Level 1: Little or no confidence in the asserted identity’s validity
- Level 2: Some confidence in the asserted identity’s validity
- Level 3: High confidence in the asserted identity’s validity
- Level 4: Very high confidence in the asserted identity’s validity

- Based on token possessed by user, registration and identification mechanisms used, and authentication protocols and assertions

LoA Tokens and Registration

- Type of token used to prove identity
  - Password Tokens. LoA 1-2
  - One-Time Password Hardware Device Tokens. LoA 1-3
  - Soft Tokens. Cryptographic key is stored in software. LoA 1-3
  - Hard Tokens. Cryptographic key is stored in hardware. LoA 1-4
  - LoA 3-4 requires two factor token
- Registration and Identity Proofing
  - Binding a real life person to the claimed identity and token
  - Level 1 allows anonymous authn, remote registration and name to be provided by claimant
  - Level 2. Requires government issued photo ID containing address or nationality, and if remote application a financial document as well. RA validates all details. Pseudonym may be used for identity instead of meaningful name
  - Level 3. Same as level 2 except pseudonyms not allowed to be registered.
  - Level 4. Must turn up in person with 2 documents one of which must be a government issued photo ID

LoA Mechanisms

Remote Authentication Mechanism

Authentication protocol must prevent replay, MITM, eavesdropping, impersonation etc.

Level 1. No plaintext passwords transferred or stored. Probability of correctly guessing password < 1 in 1024 over lifetime of password. This can be achieved e.g.

8 char U/L case PW, no dictionary words, change every year, less than 5 guesses per minute are possible over lifetime

Level 2. As level 1 plus session cannot last longer than 12 hours and probability of guessing < 1 in 16,384 over life of password. This can be achieved e.g.

9 U/L/N/S char PW, change every year, < 10 guesses per hour

Level 3. Based on PoP of key. If OTP > 1 million values. Session < 2hours.

Level 4. Same as 3 except hardware based crypto key must be used in protocol such as TLS.

Assertion Mechanism

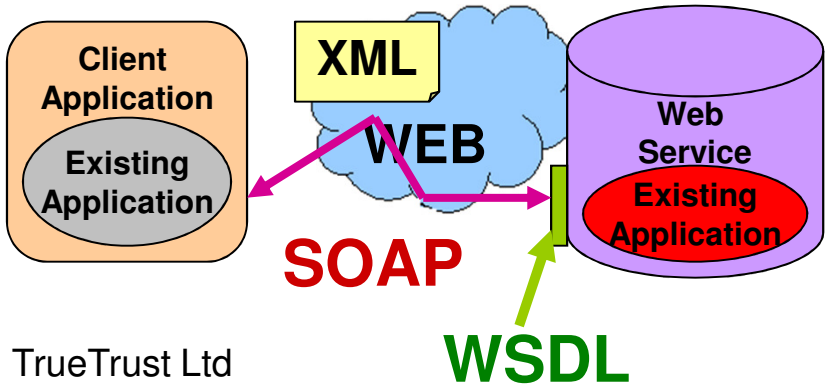
Assertion issued by authenticating entity must be cryptographically protected when transferred to relying party

Limitations of NIST LOA

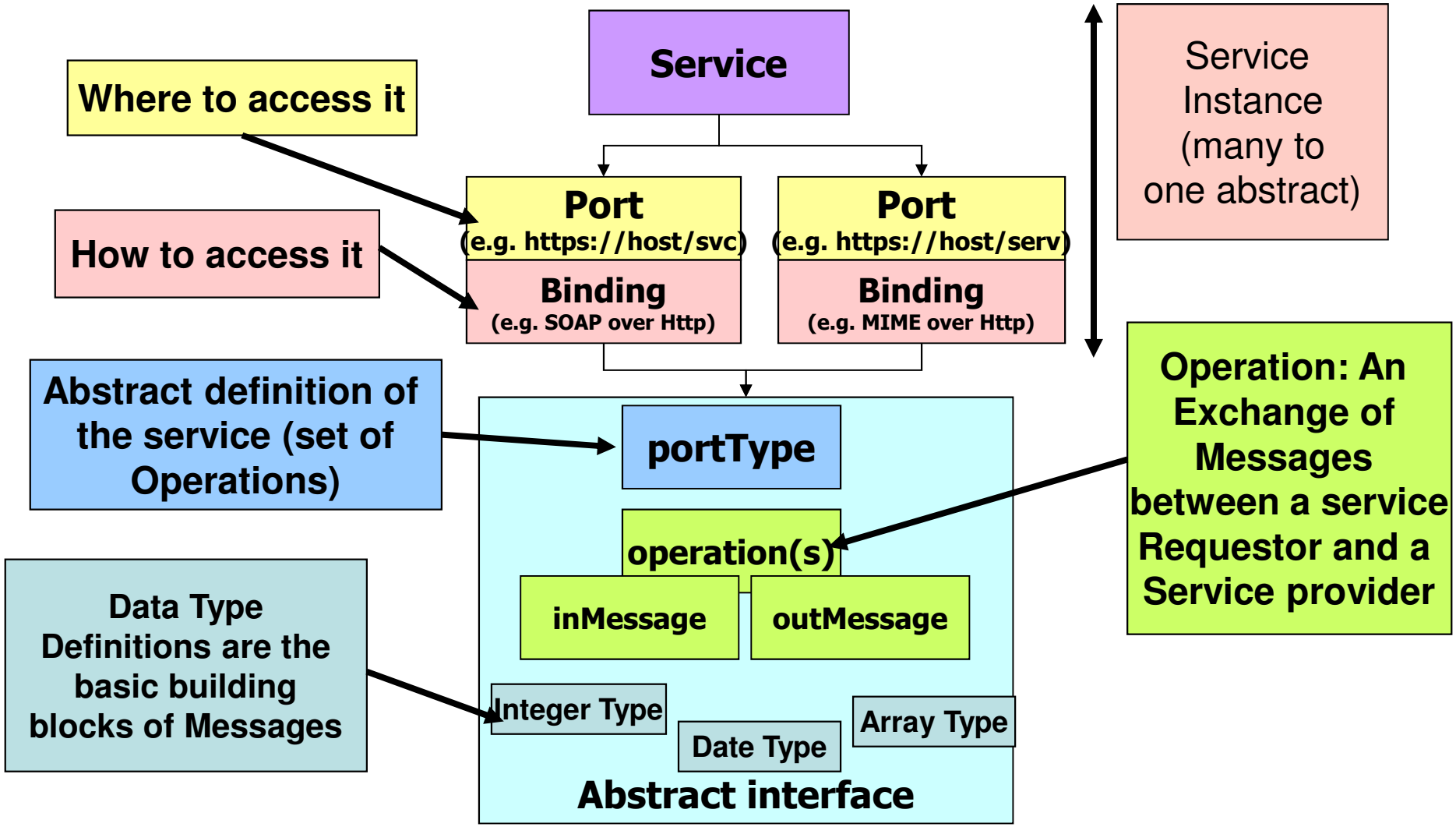
- Only defined for authentication and not for authorisation, so only one LOA per session
  - Need LOA per attribute assertion
- Registration and Authentication mechanism are grouped into the same LOA
  - Need to separate and have Registration LOA and Session LOA
  - Both can change independently

Web Services

- A web service is a software system designed to support interoperable machine-to-machine interaction over a network
- Its interface is described in a machine-processable format (web services description language WSDL)
- Other systems interact with the web service in a manner prescribed by its description using SOAP-messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards
- Web service (WS) standards are provided for security, which build on SOAP and XML security



Web Services Description Language (WSDL)



Privacy Legislation and Guidelines

- OECD Privacy Guidelines, 1980
- EC Directive 95-46, 1995, on processing and movement of personal data
- US Health Insurance Portability and Accountability Act (HIPAA), 1996, of which the Privacy Rule took effect in 2003
- US Gramm-Leach-Biley Act 1999 – infamous for repealing part of the 1933 Glass-Steagall Act (thereby allowing casino banks and high street banks to merge) did however require financial institutions to ensure the security and confidentiality of their clients' personal information
- US Sarbanes-Oxley Act 2002, requires all US public companies to report annually on their financial controls. This will include identity information when related to such things as separation of duties, access to financial systems etc.
- All the above indicate the need for identity management policies and practices to be well documented, maintained and audited

OECD Privacy Guidelines and EC Directive 95-46

- Collection Limitation Principle
  - There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
  - Covered in Articles 6a and 7a of EC Directive 95-46
- Data Quality Principle
  - Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date
  - Covered in Article 6d of EC Directive 95-46
- Purpose Specification Principle
  - The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose
  - Covered in Article 6b of EC Directive 95-46
- Use Limitation Principle
  - Personal data should not be disclosed, made available or otherwise used for purposes other than those specified above except: a) with the consent of the data subject; or b) by the authority of law
  - Covered in Article 6b of EC Directive 95-46

OECD Guidelines (cont)

- Security Safeguards Principle
  - Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data
  - This is enshrined in Articles 4 and 5 of EC Directive 2002-58
- Openness Principle
  - There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller
  - Covered in Article 10 of EC Directive 95-46
- Individual Participation Principle
  - An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
  - Covered in Article 10 of EC Directive 95-46
- Accountability Principle
  - A data controller should be accountable for complying with measures which give effect to the principles stated above.
  - Covered in EC Directive

What is Personal Data?

- any information
  - subjective and objective e.g. voice recordings from telephone banking. Information does not even need to be true. Opinions are included within the scope of the act.
- relating to
  - directly or indirectly about a person. Objects related to a person are included e.g. the value of someone's house when the address of the house is also given
- an identified or identifiable
  - unique identifier or set of attributes that allow a person to be singled out. Includes dynamic IP address assigned to someone
- natural person
  - living people only, usually excludes dead people and unborn children. So it excludes information about web services and businesses (legal persons)

Kim Cameron's 7 Laws of Identity

1. **User Control and Consent**
   - *Technical identity systems must only reveal information identifying a user with the user's consent.*
   - Related to Collection Limitation principle
2. **Minimal Disclosure for a Constrained Use**
   - *The solution which discloses the least amount of identifying information and best limits its use is the most stable long term solution.*
   - Related to Collection Limitation principle
3. **Justifiable Parties**
   - *Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.*
   - Related to Purpose Specification principle
4. **Directed Identity**
   - *A universal identity system must support both "omni-directional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.*

Kim Cameron's 7 Laws of Identity

5. **Pluralism of Operators and Technologies**
   - *A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.*
6. **Human Integration**
   - *The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.*
7. **Consistent Experience Across Contexts**
   - *The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies*.

To be Private or Not to be Private - That is Question

- Scott McNealy said in 1999 "You have zero privacy anyway. Get over it.“
- Was he right?
- Do users care about their privacy?
- Some believe we should do all we can to preserve users’ privacy, hence technologies such as Anonymous Credentials and Liberty Alliance Identity Mapping (see later)
- Others believe the battle is already lost so all we can do is have accountability and audit
- What do you think?