

PKI : state of the art and future trends

David Chadwick

d.w.chadwick@truetrust.co.uk

Contents

- Review of X.509 state of the art to date
- What is new in X.509 (2016)
- What is new elsewhere
 - ITU-T
 - ISO
 - IETF
- Conclusion

X.509 to date

- First version in 1988 (v1 certs)
- Second version in 1993 (v2 certs – not used)
- Third version in 1997 (v3 certs – basis of today's PKIs)
- Fourth version in 2001 (X.509 AC infrastructure – basis of OASIS SAML attribute assertions)
- Subsequent versions: 2005, 2009, 2013 mainly bug fixes and minor enhancements
- Next version in 2016/7 has introduced a new trust model for open PKIs

Why a new Trust Model?

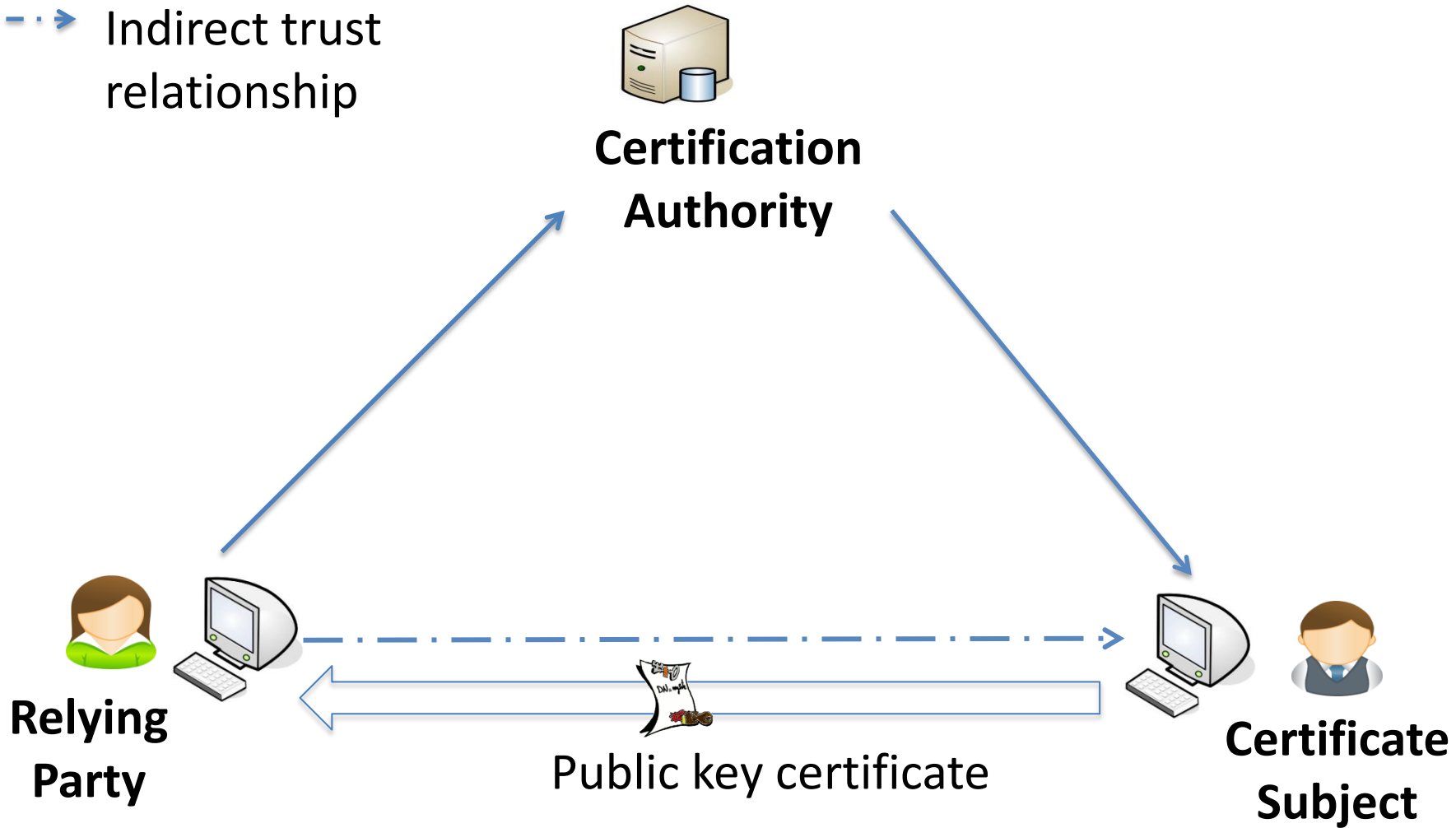
- Original X.509 PKI model assumed everyone would have a certificate from a CA, so that certificate subjects were also relying parties (RPs)
- Three cornered trust model
- Every RP had a relationship with its trust anchor/root of trust
- Cross certification ensured trust in other CAs when RP and subject had different CAs

3 Cornered (Closed) Trust Model

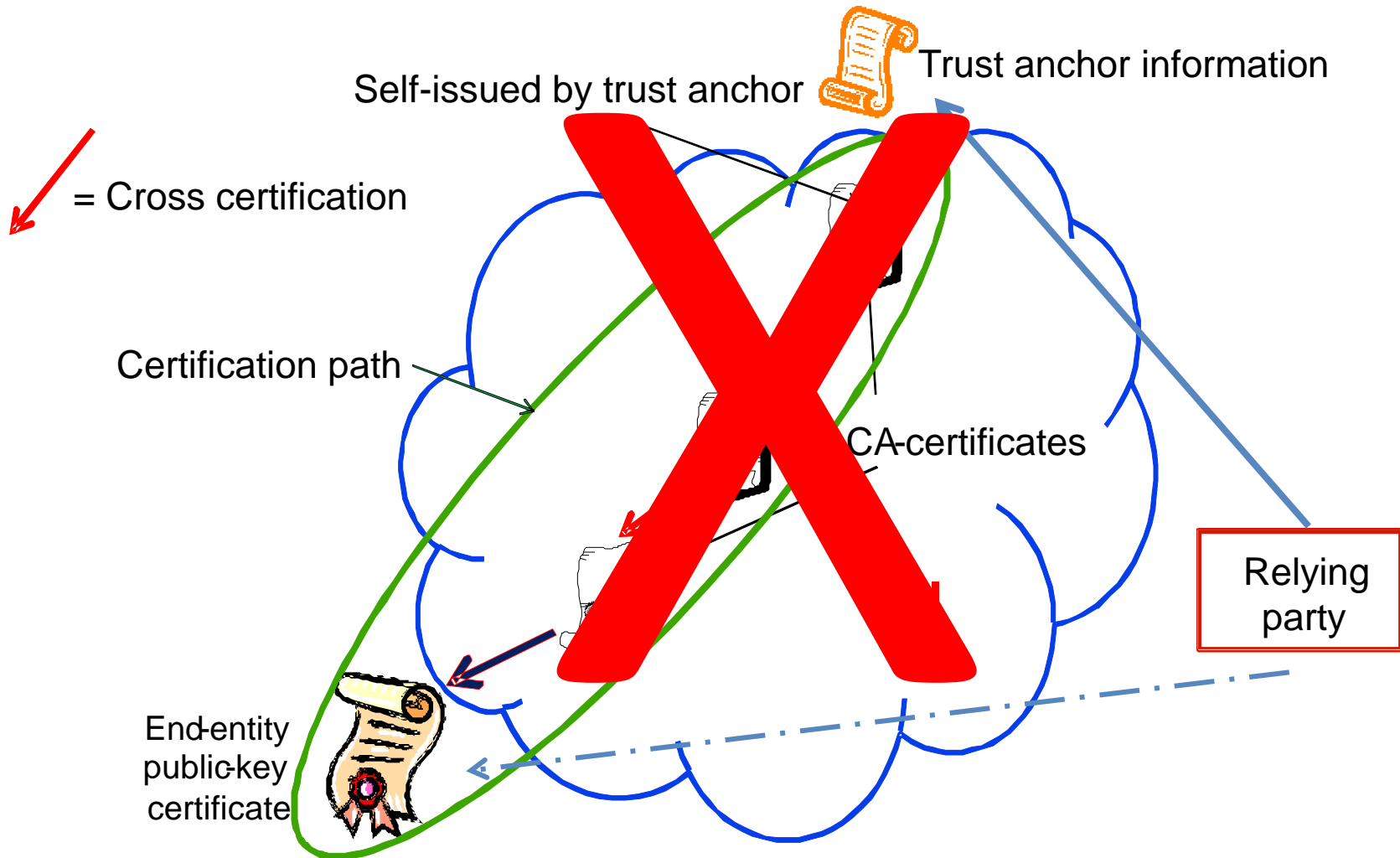
Direct

→ Trust relationship

- - - - - Indirect trust relationship



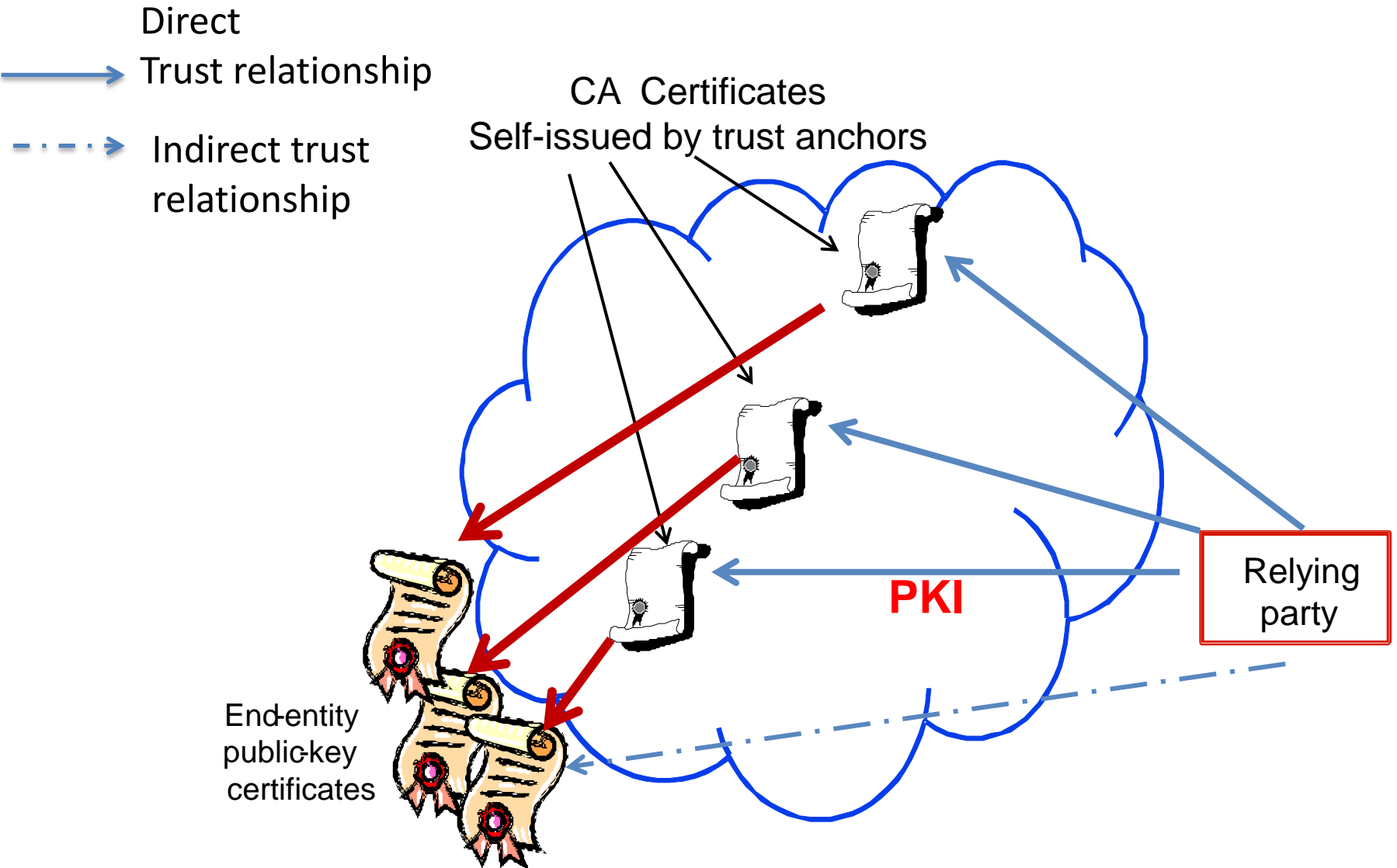
Certification Path



Cross Certification

- Rarely/Never happens in practice
- Trust, legal and liability issues
- Certifying CA needs to trust certified CA
- Certifying CA takes on liabilities when cross certified CA fails to act properly, or is attacked, or makes a mistake etc.
- So lawyers ensured cross certification was not commercially viable

Lots of Trust Anchor CAs



State of Art - Today's PKI

- Technically X.509 PKI works and is ubiquitous
- Most common use of PKI is SSL/TLS for secure communication with millions of web servers
- But most RPs (users) do not have certificates or relationships with any CAs
- Over 600 commercial CAs in existence
 - From many different countries
- How can an RP know if all of these are trustworthy?
 - Reading their CPs/CPSs is not practical
- How can an RP get damages if CA is untrustworthy or careless or is hacked etc.
 - When it has no formal relationship with CA
 - Taking into account cross border legal issues

Many are not Trustworthy!

- In March 2011, Comodo's root CA was hacked and issued 9 SSL certificates for 7 domains including Microsoft, Google, Skype, Yahoo and Mozilla
- In Sept 2011, Diginotar CA went out of business after hackers broke in and issued at least 531 fraudulent certificates
 - It issued certificates for the Dutch Government!
- Malaysian Agricultural Research and Development Institute CA (DigiCert Sdn. Bhd.) had its keys stolen in 2011 which allowed a fake Adode Flash Updater to be created which installed malware on users PCs turning them into spies. This CA's cert is now revoked by browsers

Compelled Certificate Creation Attack

- Government agency compels a national CA to issue a false SSL certificate to it in name of an Org or intermediate CA
- This certificate is then used by law enforcement to launch a MITM attack e.g. via a cyber café or hotel internet connection
- User's browser sees a "genuine" trusted SSL certificate from the site and lock icon is displayed
- Whilst Agency decrypts data using its MITM certificate and re-encrypts it for the genuine web site
- Packet Forensics from Arizona produce a commercial box for this MITM attack

Part of Packet Forensics Marketing Brochure



PACKET FORENSICS

Technical Details

Man-in-the-Middle Capabilities

Intercept any communication within Secure Socket Layer (SSL) or Transport Layer Security (TLS) sessions

All Packet Forensics targeting and policy capabilities can operate within the encrypted tunnel

Operational Configurations

In-line with hardware bypass / failsafe

Import any certificate / public key or generate your own for presentation

Availability

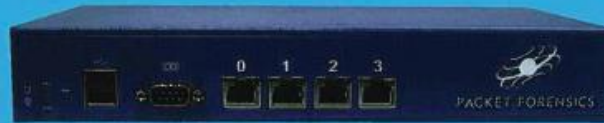
Available in firmware releases after August 31st, 2009 for all Packet Forensics platforms

Available under customization program

Packet Forensics 5-Series are the most flexible tactical surveillance devices in the world of IP networks. Designed for defense and (counter) intelligence applications, they are fully-embedded without moving parts and available in a variety of sizes, shapes and power footprints, all customized for the client. In under five minutes, they can be configured and installed in-line without knowledge of existing network topology. **Capabilities include:** Keyword, RADIUS, DHCP and behavior-based session identification; filtering, modification and injection of packets; compatibility with existing collection systems. With this modular platform, Packet Forensics



creates **mission packages** based on customer requirements. Best of all, they're so cost effective, they're disposable--that means less risk to personnel.



The Internet Cafe




The 5-Series is an ideal solution to the "Internet Cafe Problem." Quick deployment and remote control minimize personnel risk and maximize collection capabilities. Small footprint and minimal power requirements make installation easy.

How do RPs manage?

- Browser manufacturers act as a proxy for all users in validating that a CA is trustworthy
- They SHOULD only add root certificates of trustworthy CAs to their trust stores
- They SHOULD check revocation information before validating a web sites certificates
- They SHOULD check all policy information in certificates such as key usage, policy fields, name constraints etc. when validating certificates
- They SHOULD remove untrustworthy root and subordinate CA certificates from their trust stores
 - Can still find MD5 root certs, used by APTs Flame, Stuxnet etc.
- They SHOULD offer liabilities to users if they get it wrong and the user suffers a loss because of their neglect
- DO THEY?
- Read: 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

What is the alternative?

- Introduce a trusted third party – trust broker – who acts on behalf of RPs in validating certificates
- RP enters into a contractual relationship with TB, who will offer guarantees and compensation if it makes a wrong trust decision about a certificate
- TB will read CPs and CPSs of CAs and determine how trustworthy they are, what their certificates can be used for, and what liabilities they offer
- We have a four cornered trust model
- Rationale and model is presented in
- Ahmad Samer Wazan, Romain Laborde, François Barrere, Abdelmalek Benzekri, David W Chadwick. "PKI interoperability: Still an issue? A solution in the X.509 realm" Proc 8th World conference on Information Security Education, New Zealand July 2013

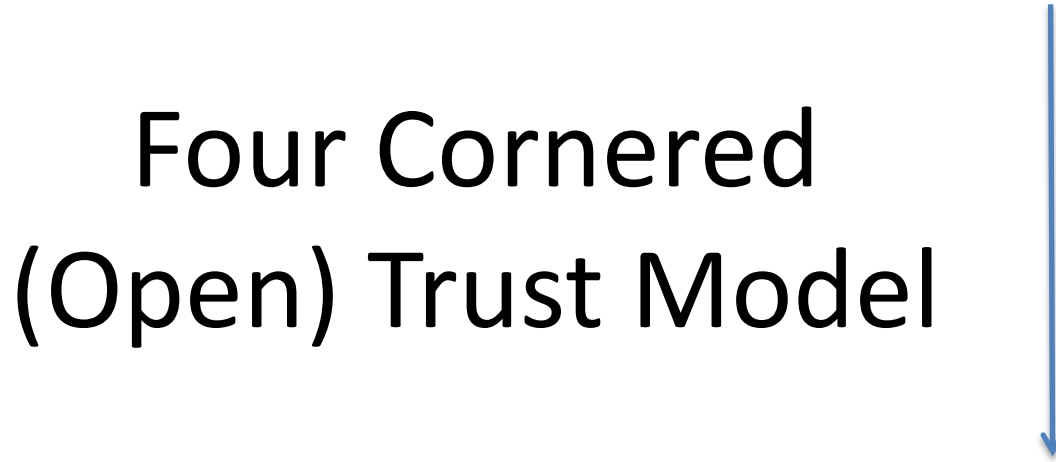
-  Trust Evaluation
-  Direct trust relationship
-  Indirect trust relationship



Trust Broker



Certification Authority



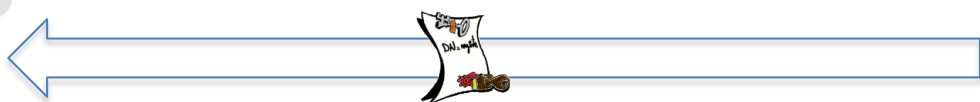
Four Cornered (Open) Trust Model



Relying Party



Certificate Subject



Public key certificate

New X.509 Trust Model Does Not Solve Everything

- Still need standardised protocol(s) for communications between RP and TB
- Support for TBs will need to be built into web browsers either via a plugin or direct manufacturer support
- Needs a profitable business model to ensure that entrepreneurs will offer a TB service
- All of the above is traditionally outside the scope of ITU-T X.509

Other Proposed Changes in X.509 (2016)

- Cleaning up of the text
 - Removing errors and inconsistencies and replacing badly worded descriptions
- Removing non-PKI and PMI material from X.509
 - Move the directory authentication specifications from X.509 to X.511.
 - Move Password Policy specifications from X.509 to X.511
 - Move Password Policy schema definitions from X.509 to X.520
- Cleanly separate PKI and PMI into different sections
 - In Aug 13 issued a defect report on text which said ACs and PKCs could appear in the same CRL
- Removing unused and duplicate ASN.1 data structures
 - certificationPath, forwardCertificationPath and crossCertificate (pkiPath is used instead)

Other X.509 Work

- PKI Profiles for
 - Smart Grids
 - Wireless PKI (WPKI)
 - Cloud Computing
- Cryptographic Message Syntax (CMS)
 - eliminate all obsolete ASN.1 features and make it usable with all ASN.1 standardized encoding rules
- Procedures for establishing and maintaining a PKI
 - For large PKI networks with machine to machine interactions
- Certified Mail Transport and Certified Post Office Protocols
 - The electronic equivalent of registered post

Smart Grids

- Vast numbers of devices connected to electricity grids – possibly more than existing Internet – so PKI scalability issues
- Means many more roots of trust, how will this be handled
- Means millions of cheap devices holding their own private keys and roots of trust, may be built in foreign factories by unvetted workers, so probably easily compromised, thus revocation issues
- CRLs today are consistently larger than first envisaged, so cause bandwidth and latency problems. OCSP also has performance issues
- What is the identity of the certificate subject? Manufacturer of device? Supplier of electricity? Owner of property? Occupant of property? Most not known when key is installed in device, so may need dynamic certification or other means of identifying subject such as an AC
- Who is authorised to request re-certification, or revocation?
- How do we rekey a hardware device whose private key has been compromised?
- How do we protect the privacy of the data subject?

ISO/IEC JTC1/SC27

- New Study Group: Framework for PKI Policy / Practices / Audit
- TOR: To gauge interest in the development of an internationally accepted and standardized approach to the management, operation, assessment, and certification of PKI Trust Service Providers at varying levels of assurance. This includes management, procedural, assurance and technical standards
- Still at very early stage of fleshing out content. Focus seems to be on audit of trust service providers
- Next meeting Incheon, Republic of Korea, 21st – 25th October 2013

IETF (1)

- PKIX Working Group

- Started in 1995 with goal of developing Internet standards to support X.509 PKIs

- Published over 60 RFCs about X.509 including:

- **Protocols** for certificate management, time stamping, online certificate status, use of LDAPv2 & FTP/HTTP, Data Validation and Certification Server, Delegated Path Validation and Delegated Path Discovery, Server based certificate validation, trust anchor management
 - **Profiles** for PKCs and ACs, Qualified certificates
 - **New certificate extensions:** logotype, proxy certs, warranty, permanent ID, attributes supporting authentication in PPP and WLAN, IP addresses and AS identifiers, subject identification method, clearance attribute
 - **Others:** Diffie-Hellman POP Algorithm, SHA 224, DNS Certification Authority Authorization (CAA) Resource Record

IETF (2)

- Certificate Transparency from Google
 - Experimental RFC 6962, June 2013
 - Log servers hold Merkle hash trees (append only logs) of all issued certificates. Any CA can send a cert to a log server and get a signed time stamp in response
 - Monitor servers check on all log servers periodically and will flag any unauthorized or suspicious certificates
 - Auditors (typically running in browsers) can check that any certificate and time stamp they receive appears in the log. If not, the certificate of the SSL site is suspect and should not be trusted
 - Will stop MITM attacks, compelled certificate creation attacks, duplicate certs with stolen keys etc.
 - Sovereign Keys from Electronic Frontier Foundation is a similar idea, using “timeline servers” to hold public keys of web sites

IETF (3)

- HTTP Strict Transport Security (HSTS)
 - RFC 6797, Nov 2012, from Web Security Working Group
 - Allows web sites to say that they are only contactable via HTTPS
 - HTTP Response header contains the sites security policy
 - Browsers remember the policy and will strictly enforce it
 - This stops users “clicking through” browser security warnings of web sites that the browser does not trust
- Public Key Pinning Extension for HTTP
 - Internet draft of Web Security WG
 - HTTP protocol extension allowing web sites to instruct browsers to remember ("pin") the hosts' public keys for a given period of time
 - During this time, browsers will require hosts to present a certificate chain including at least one Public Key that matches one of the pinned ones

IETF (4)

- Web PKI Operations (wpkops) working group
 - improve the consistency of Web security behavior
 - address the problems caused by hundreds of variations of Web PKI currently in use
 - describe how Web PKI "actually" works in browsers and servers in common use today by
 - The trust model on which it is based;
 - The contents and processing of fields and extensions;
 - The processing of the various revocation schemes;
 - How the TLS stack deals with PKI, including varying interpretations and implementation errors, as well as state changes visible to the user.
 - The state changes that are visible to and/or controlled by the user (to help predict the decisions that will be made the users and so determine the effectiveness of the Web PKI).
 - Identification of when Web PKI mechanisms are reused by other applications and implications of that reuse.
 - The working group will not
 - describe how the Web PKI should work
 - examine the certification practices of certificate issuers.
 - investigate applications (such as client authentication, document signing, code signing, and secure email)

Conclusions

- X.509 PKI is now ubiquitous
- The PKI technology is pretty robust and secure
 - providing the algorithms are kept up to date and
 - the implementations are complete and correct
- The trust framework, policies, and procedures are the weakest areas
 - This is where most of the standards work is now focussed, and where most of the successful attacks are
- New application domains are continually being found, with new requirements
 - New/revised/enhanced standards are required for these

Any Questions?