

Themes in current PKI's trust frameworks and its future

David W Chadwick
University of Kent

Contents

- What is Trust?
- X.509 and PKIX today
- Proposed X.509 Trust Broker
- Evaluating the Trustworthiness of a CA
- Other ISO and IETF work on trust in PKI
- Authentication or Authorisation?

True or False?

- I trust you therefore I will sign a contract with you
- I don't trust you, but I will lend you 100 yen
- Trust Management \equiv Risk Management

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>

What is Trust?

- Trust = Residual Risk
- If there is no risk, no chance of loss, then no trust is needed e.g. Internet e-commerce with credit cards
- Contracts, penalty clauses, rule of law, courts, institutions, standards etc. are all there not to increase trust in doing business but to reduce the risk to an acceptable level and hence reduce the level of trust that we need in order to do business

What is a Trust Framework ?

- A trust framework is a certification program that enables a party who accepts a digital identity credential (called the relying party) to trust the identity, security, and privacy policies of the party who issues the credential (called the identity service provider) and vice versa
 - The Open Identity Exchange (OIX)
- The purpose of a trust framework is to reduce the residual risk to the trustor

X.509 PKI Trust Framework

- A framework for obtaining and trusting a public key of an entity in order to encrypt information to be decrypted by that entity, or in order to verify the digital signature of that entity
 - But who is the entity?
- public-key certificate (PKC): The public key of a user, *together with some other information*, rendered unforgeable by digital signature with the private key of the certification authority which issued it
 - So maybe this other information will tell me who the entity is?
- A certification authority produces the certificate of a user by signing a collection of information, including *the user's distinguished name* and public key
 - So it is the X.500 distinguished name that will identify the entity
 - Herein lies a major problem. Few people use or know about X.500 distinguished names. So they are being asked to trust in something they know nothing about!

What is a PKI Certification Authority?

- From X.509
- certification authority (CA): An authority trusted by one or more users to create and assign public-key certificates (to entities)
- So we must trust the CA to assign the correct X.500 distinguished name (and possibly other information) to the entity
- This is the primary role of a CA

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 is this needed?

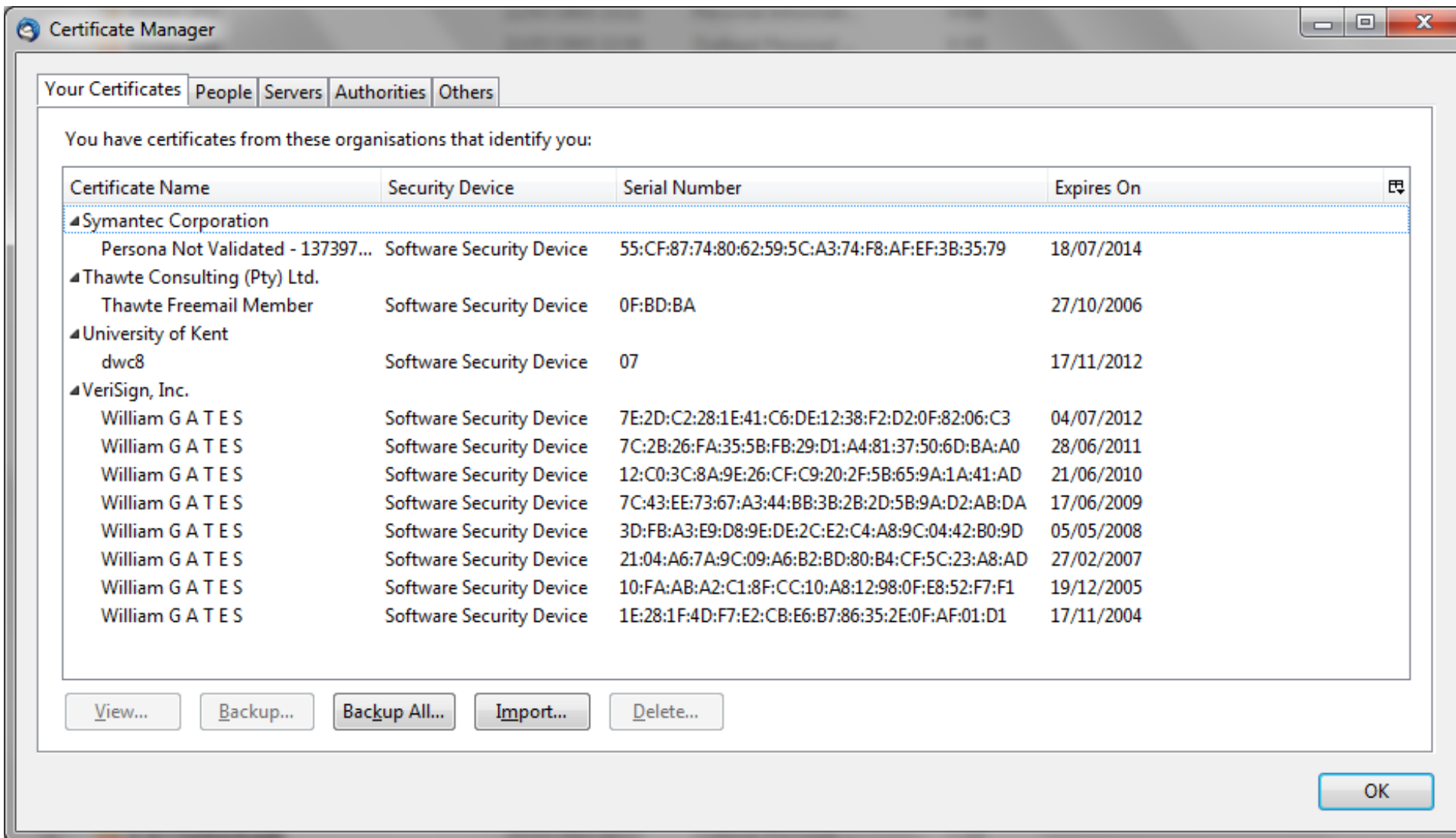
X.509 was lacking, so enter IETF PKIX

- X.509 does not provide operational protocols for CAs and subjects
 - PKIX has provided 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 etc.
- X.509 does not provide any guidance for how CAs should operate
 - PKIX has provided RFC 3647 Certificate Policy and Certification Practices Framework
- X.509 does not provide a real time revocation procedure
 - PKIX has provided OCSP

PKIX is still lacking

- There are no metrics or automated methods for measuring the trustworthiness of a CA. CPs and CPSs are qualitative documents meant for human consumption
- The scale of the Internet PKI is now too big to manage
 - E.g. CAs can perform no subject identity verification and still be trusted on the Internet
 - CAs and subject certificates can be compromised and no-one knows for some time
 - CRLs can get too big and too time consuming to process
- Users (relying parties) have no means of obtaining compensation if they use revoked/fraudulent/untrustworthy etc. certificates

My Bill Gates PKCs



A Message From Bill Gates?

The screenshot shows the Mozilla Thunderbird email client interface. The main window displays an email from Bill Gates (bill_gates_12000@yahoo.com) with the subject 'Job Offer' and recipient d.w.chadwick@truetrust.co.uk. The message content reads: 'Hi David', 'this is Bill Gates here. Would you like a job as PKI security architect within Microsoft? If so, please give me a call', 'yours', and 'Bill'. A 'Message Security' dialog box is overlaid on the right, indicating the message is signed by William G A T E S (bill_gates_12000@yahoo.com) with a VeriSign Class 1 Individual Subscriber CA - G2 certificate. It also states the message is not encrypted. The Windows taskbar at the bottom shows the start button, several open applications, and the system tray with the date and time (Monday, 01/11/20).

Job Offer - Inbox - Local Folders - Mozilla Thunderbird

File Edit View Go Message Tools Help

Get Mail Write Address Book Next Delete Reply Reply All Forward Forwards Back Tag

Search all messages... <Ctrl+K>

Inbox - Lo... Regarding ... Your Indivi... Security co... [TAS3ALL] ... Re: 20101... Re: Securit... Re: WP6 B... CROSSRO... 20101028 ... JISC Six m... [TAS3ALL] ...

from Bill Gates <bill_gates_12000@yahoo.com> ☆
subject Job Offer
to d.w.chadwick@truetrust.co.uk <d.w.chadwick@truetrust.co.uk> ☆

Hi David

this is Bill Gates here. Would you like a job as PKI security architect within Microsoft? If so, please give me a call

yours

Bill

Message Security

Message Is Signed
This message includes a valid digital signature. The message has not been altered since it was sent.

Signed by: William G A T E S
Email address: bill_gates_12000@yahoo.com
Certificate issued by: VeriSign Class 1 Individual Subscriber CA - G2

[View Signature Certificate](#)

Message Not Encrypted
This message was not encrypted before it was sent. Information sent over the Internet without encryption can be seen by other people while in transit.

OK

Unread: 2 Total: 24

start C:\Teaching\... e-ticket_724... Supporting R... ROWLBAC - ... PPU_Securit... Untitled - No... IdFramewor... SemanticSer...

Reverse eng... WP1 Contrib... SWIFT and ... Job Offer - I... six_mnth_pr... PKI - the sol... Trust in Digit...

15:30 Monday 01/11/20

Why a new X.509 Trust Model?

- Original X.509 PKI model assumed everyone would have a certificate (and X.509 DN) from a CA, so that certificate subjects were also relying parties (RPs)
- So everyone would have a DN and know them
- 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

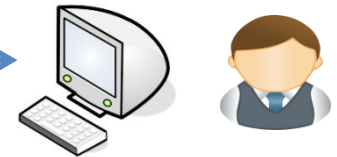
⋯ Indirect trust relationship



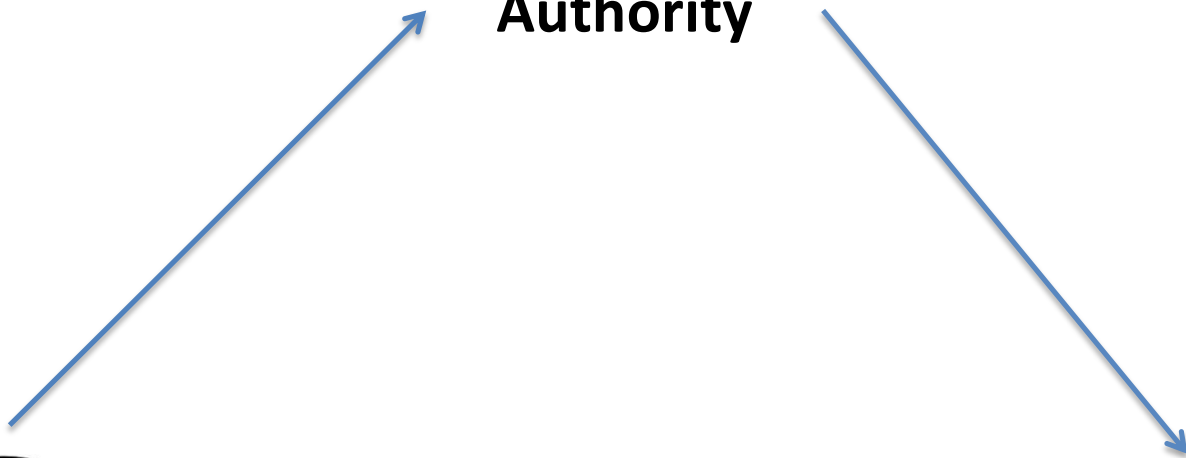
Certification Authority



Relying Party

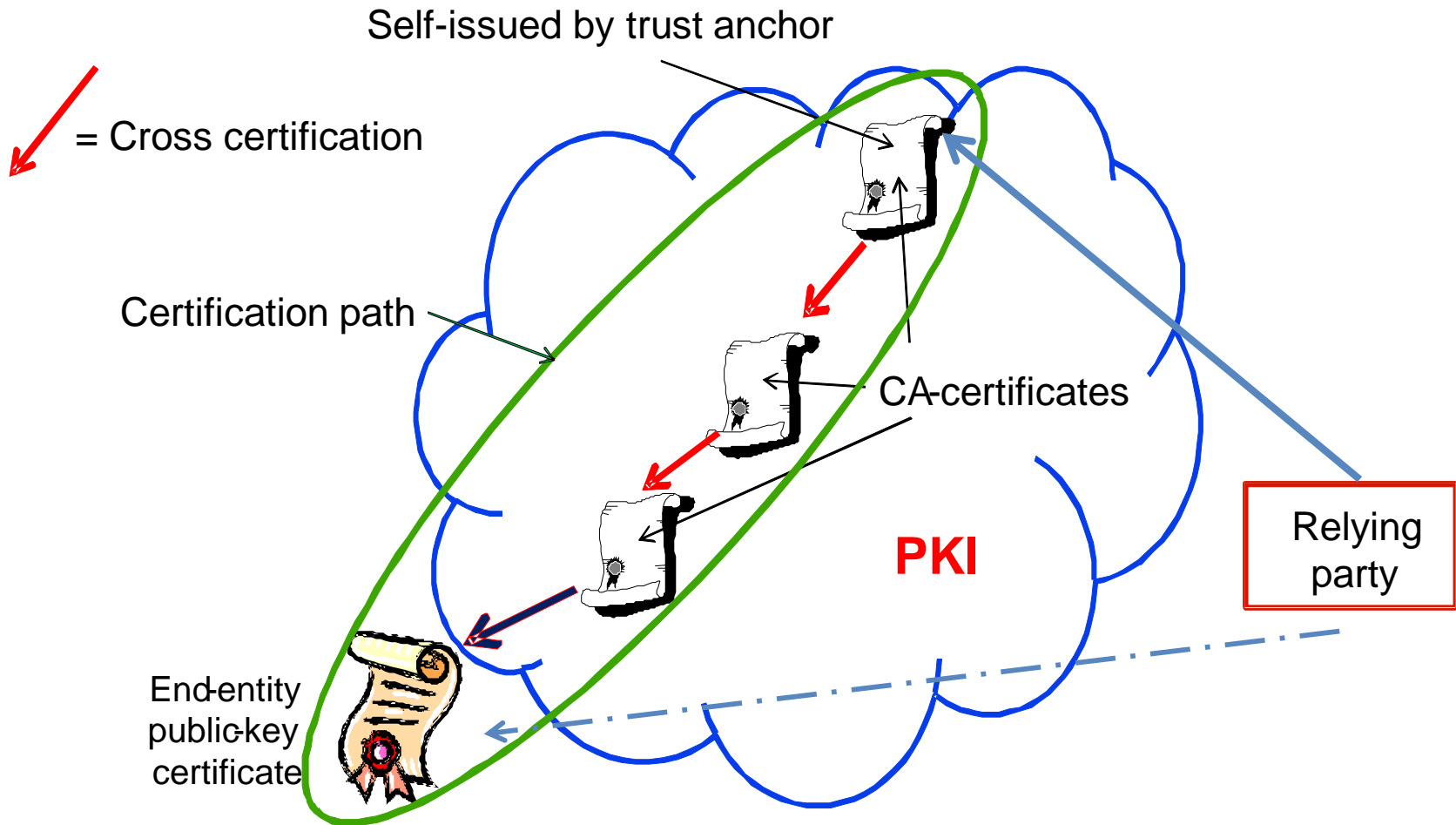


Certificate Subject

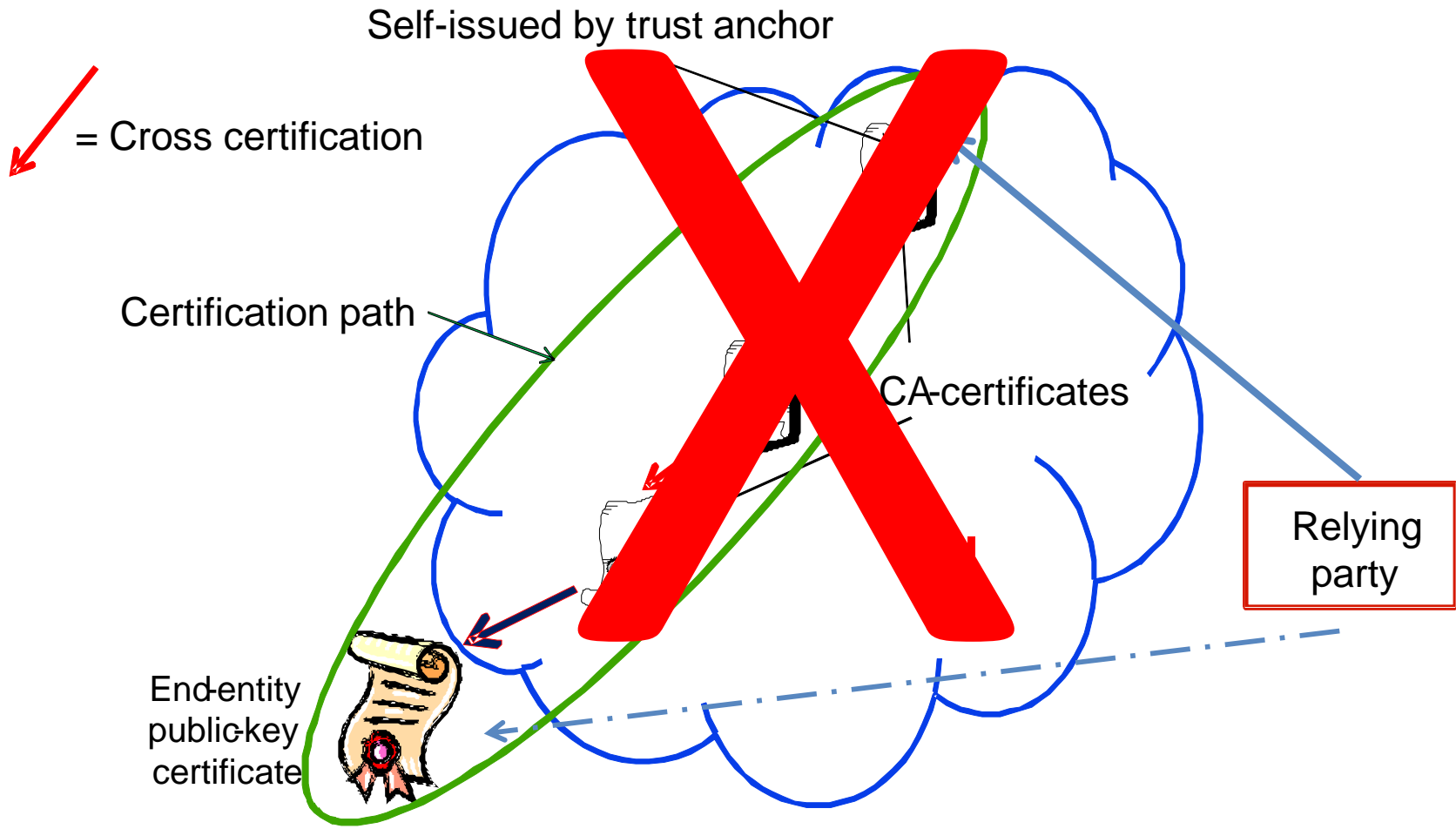


Public key certificate

Certification Path



Certification Path



Cross Certification

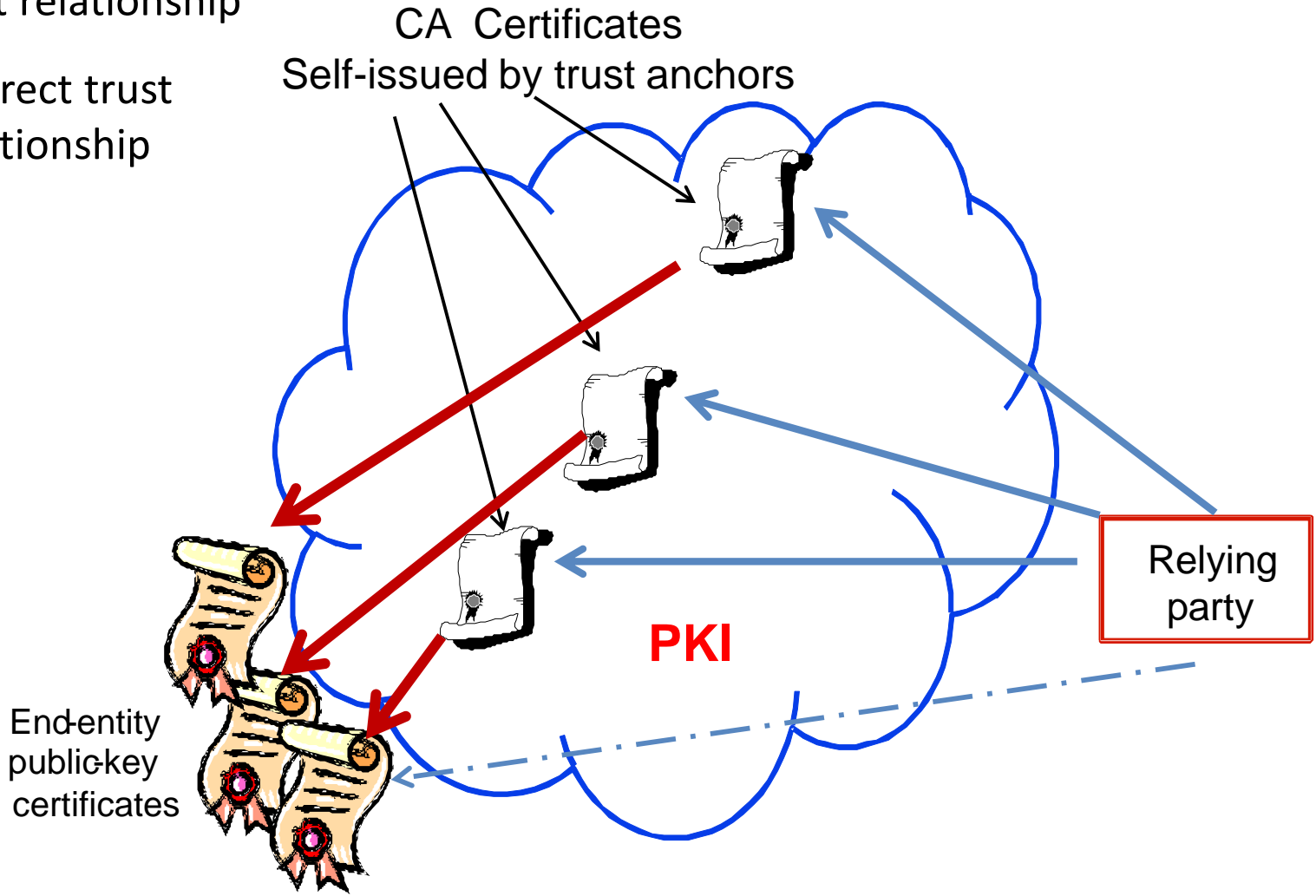
- Rarely/Never happens in practice
- Trust, legal and liability issues
- Certifying CA needs to trust certified CA
- Certifying CA takes on liabilities of cross certified CA, so when the latter fails to act properly, or is attacked, or makes a mistake etc. certifying CA can incur losses
- So lawyers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

Led to Lots of Trust Anchor CAs

Direct

→ Trust relationship

- - - Indirect trust relationship



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 the CA
 - Taking into account cross border legal issues

Some CAs are not Trustworthy!

- In March 2011, one of Comodo's regional affiliate RAs 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
- And these are only some of the latest incidences, there are many more

Compelled Certificate Creation Attack

- Government agency compels a national CA to issue a false TSL 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.

MITM Attack in Japan

GENUINE KENT POP3 CERTIFICATE

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

77:eb:7b:b5:09:24:8c:48:58:a4:4f:96:d1:dd:0d:e0

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=NL, O=TERENA, CN=TERENA SSL CA

Validity

Not Before: Apr 19 00:00:00 2013 GMT

Not After : Apr 18 23:59:59 2016 GMT

Subject: OU=Domain Control Validated,
CN=csmail.ukc.ac.uk

MITM KENT POP3 CERTIFICATE

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

57:5f:7e:cd:26:24:8c:48:58:a4:4f:96:d1:dd:0d:e0

Signature Algorithm: sha1WithRSAEncryption

**Issuer: C=US, ST=California, L=Sunnyvale,
O=Fortinet, OU=Certificate Authority,
CN=FortiGate
CA/emailAddress=support@fortinet.com**

Validity

Not Before: Apr 19 00:00:00 2013 GMT

Not After : Apr 18 23:59:59 2016 GMT

Subject: OU=Domain Control Validated,
CN=csmail.ukc.ac.uk

Who was responsible?

- Could be the hotel or some other gateway using a Fortinet firewall (Fortigate)
 - if it produces PKCs on demand to masquerade as remote SMTP and POP3 servers
- But I will never know for sure

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

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

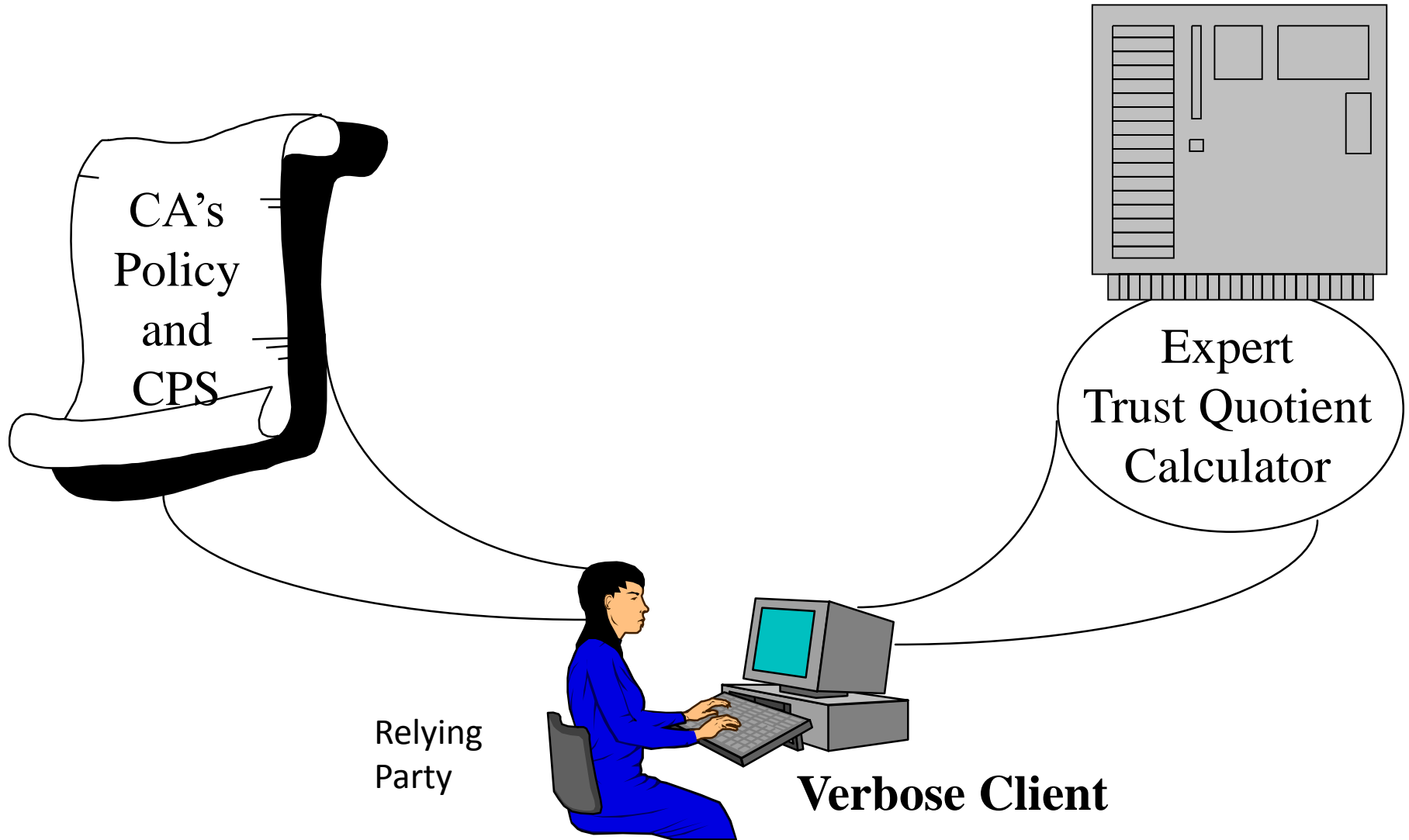
New X.509 Trust Model Does Not Solve Everything

- 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

Evaluating the Trustworthiness of a CA

- Intelligent Computation of Trust project
 - Ran from Jan 1998 to Dec 2000 in the UK
- Built an expert system for computing the Trust Quotient of a CA based on its CP/CPS
 - Interviewed 15 world experts (inc. Chokhani, Ford, Kent etc.) to extract knowledge for the KBS
- Relying Party (or Trust Broker) can answer questions posed by the KBS from reading the CA's CP/CPS

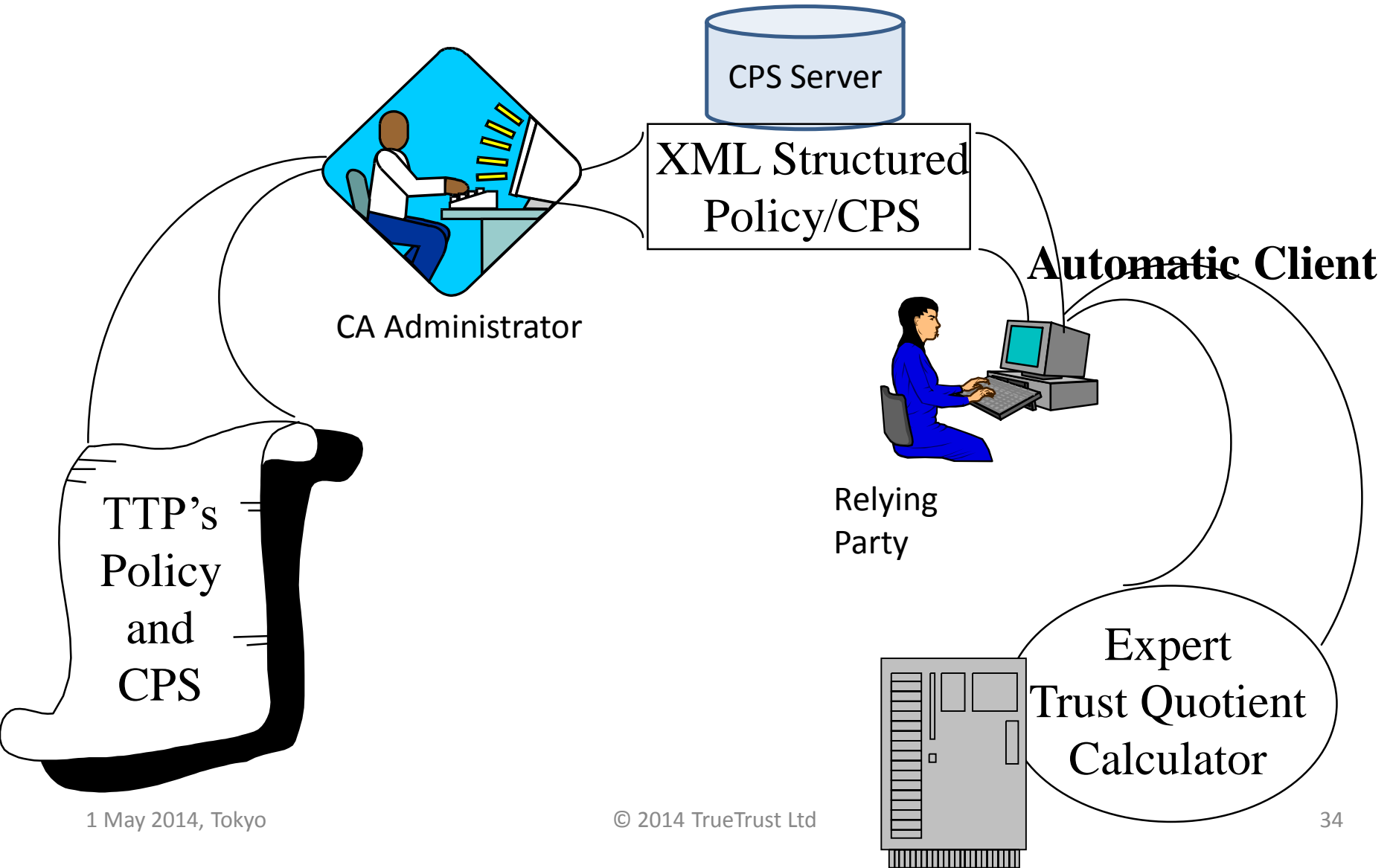
Mode of Operation - Method 1



Automated System

- Original system was time consuming, perhaps error prone, so
- Convert CA/CPS into XML so that it is machine readable and store in a CPS server
- Then a parser can extract the information to automatically answer the questions posed by the KBS

Mode of Operation - Method 2



Still Not Good Enough

- This only computes how trustworthy the CA *says* it is
- Not what it actually does in practise
- So we defined an Audit Certificate (in XML) to be published by the CA's auditor
- And proposed a Trust Check Server that would
 - fetch CRLs of CA to check frequency of issuing
 - fetch Audit Certificate to check conformance to CP/CPS
 - Compute a revised Trust Quotient based on actuality

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 Defects Published in 2014

- Problems with the issuing distribution point extension due to different syntaxes in different versions of the standard (DR 398)
- Unclear specification of the version component of certificate list and what version is it, if it is missing (DR 397)
- Insufficient description of trust anchor, need to align with PKIX (DR 394)
- Unclear text for the expiredCertsOnCRL X.509 extension (DR 393)
- Certificate types and revocation lists. Major edits required to clarify when standard is talking about revocation of ACs, PKCs or both (DR 391)
- A full list of X.500 defects can be found here
<http://x500standard.com/index.php?n=lg.DefectReports>

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

ISO/IEC JTC1/SC27

- New Study Group: Framework for PKI Policy / Practices / Audit started in April 2013.
- 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
- Focus initially was on audit of PKI trust service providers
- Had meetings in Incheon, Korea, 24th October 2013, and Hong Kong, 7-8th April 2014, plus 7 WebEx meetings
- Input from United States (Co-Convenor), France (Co-Convenor), United Kingdom, Luxembourg, Spain, Italy, Germany, South Korea and ETSI

Outcomes of ISO PKI Study Group

- Final report has agreed to start the revision of TR14516/X.842 (2002) “Guidelines for the use and management of Trusted Third Party Services”
 - This provides guidance for the use and management of TTP services: to define the basic duties and services provided, their description and their purpose, and the roles and liabilities of the TTPs and their users.
 - Covers multiple TTPs: time stamping, non-repudiation, key management, certificate management, and electronic notary services
- Has two significant defects which need correction:
 - 1. Certain key CA components are not addressed including CA Key Generation and Certification Practice Statements
 - 2. Makes numerous references to TR 13335 “Guidelines for the management of IT security” which has been withdrawn and superseded by the ISO/IEC 2700x series
- Proposal is to turn it into a multiple part recommendation
 - TR14516-1: Overview and concepts of TSPs
 - TR14516-2: TSP-PKI Guidelines for the information security of the TSP
 - TR14516-3: TSP-PKI Guidelines for the provision of PKI services

Trust Work in IETF

- Certificate Transparency - RFC 6962
- HTTP Strict Transport Security (HSTS) – RFC 6797
- Public Key Pinning Extension for HTTP
- Web PKI Operations (wpkops) working group

Certificate Transparency from Google

- Experimental RFC 6962, June 2013
- Log servers hold signed Merkle hash trees (append only logs) of all issued certificates. Any CA can send a certificate to a log server and get a signed time stamp in response. This time stamp must accompany the certificate in the TLS handshake
- 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 Web Security Working Group

- HTTP Strict Transport Security (HSTS)
 - RFC 6797, Nov 2012
 - 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 e.g. if user is redirected to a masquerading web site that could capture the user’s cookie and then impersonate the user
- 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
 - Hosts can instruct browsers to include sub-domains as well in their policy

Web PKI Operations (WPKOPS) working group

- Improve the consistency of Web security behaviour
- 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)

WPKOPS – Progress to Date

- 4 Internet Drafts Published
 - Trust model - draft-ietf-wpkops-trustmodels-00
 - Browser processing - draft-wilson-wpkops-browser-processing-00
 - Revocation - draft-hallambaker-pkixstatus-01
 - TLS stack - draft-agl-wpkops-tlsstack-00
- Questionnaire for PKI providers distributed 3 months ago
 - 2 of 7 browser suppliers have responded (Mozilla and Comodo), 2 have promised to do so (MS and Google)
 - 1 of 15 server providers have responded (CloudFlare), 1 promised (MS) and 2 refusals (Oracle and OpenSSL)
 - 20 of 67 OCSP providers have responded
 - Its going to be difficult to document the current state of PKI on the Internet today if responses are not forthcoming

Some Interesting Results

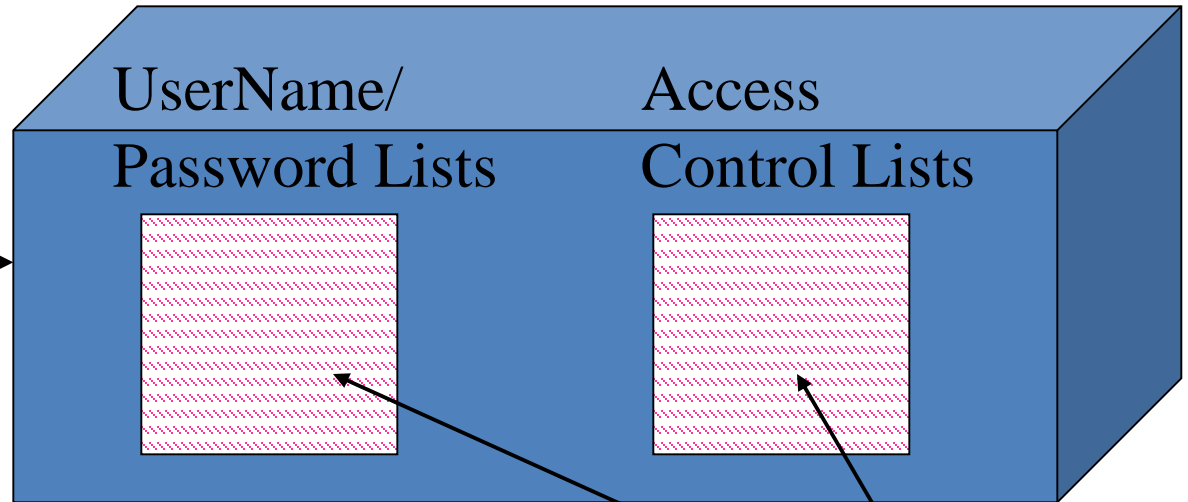
- Firefox currently has very limited support for CRLs and soon will have none
- Chrome generally does not check CRLs or fetch OCSP responses but uses CRLSets pushed as a software update to the browser
 - CRLSets are a Google invention that regularly collect a full set of “important” CRLs from all sources and then push them periodically to their browsers

A Final Thought for the Future - Authentication or Authorisation?

- *Most services don't want to know who you are, they want to know what you are authorised to do*
- Authentication is only the first step in access control. Determining if the user is authorised is the ultimate goal

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

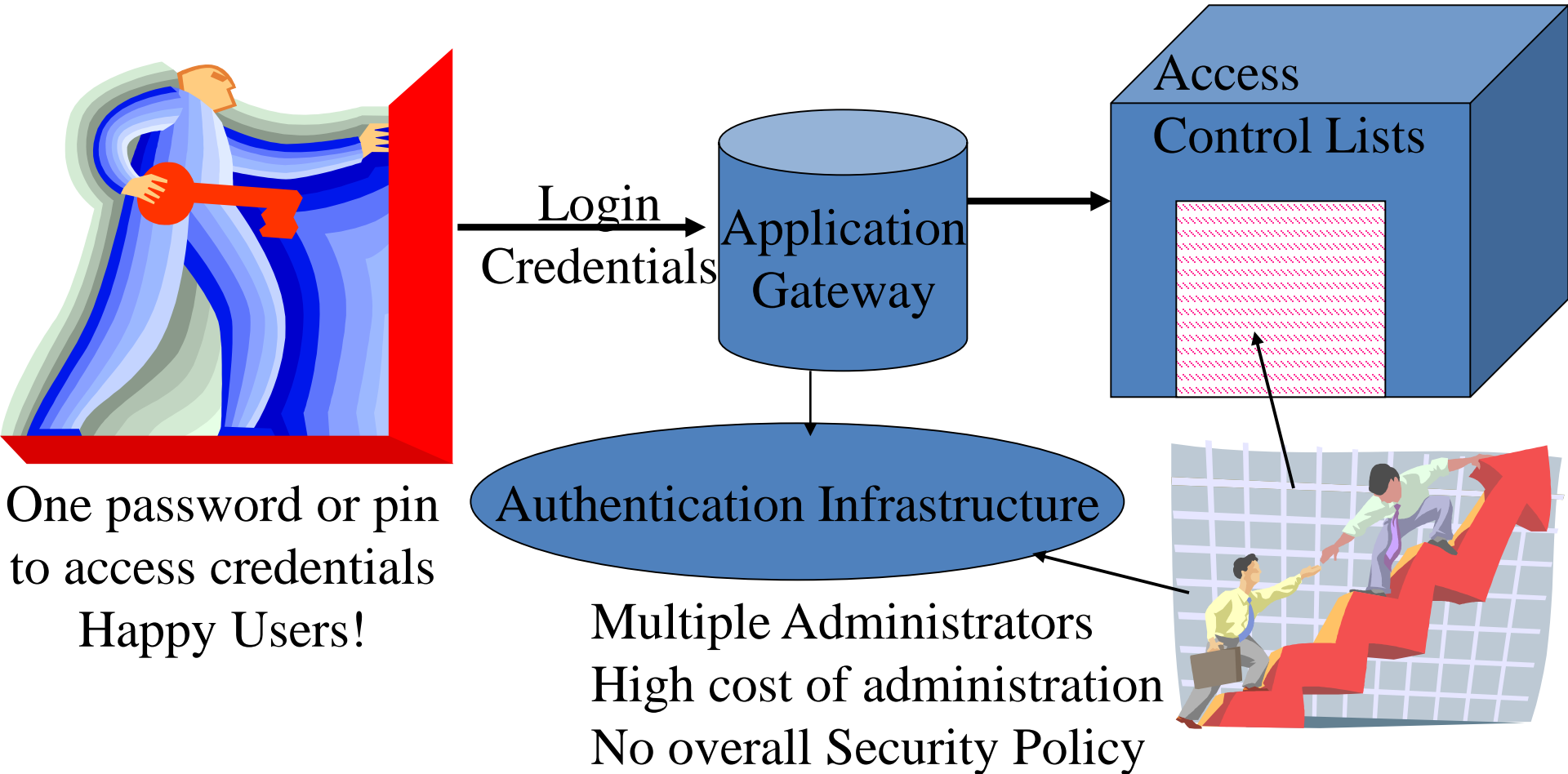


- Costly, difficult to scale to Internet proportions
- But no Trust required in external entities

Enter Authentication Infrastructure

e.g. PKI, OpenID, Shibboleth etc

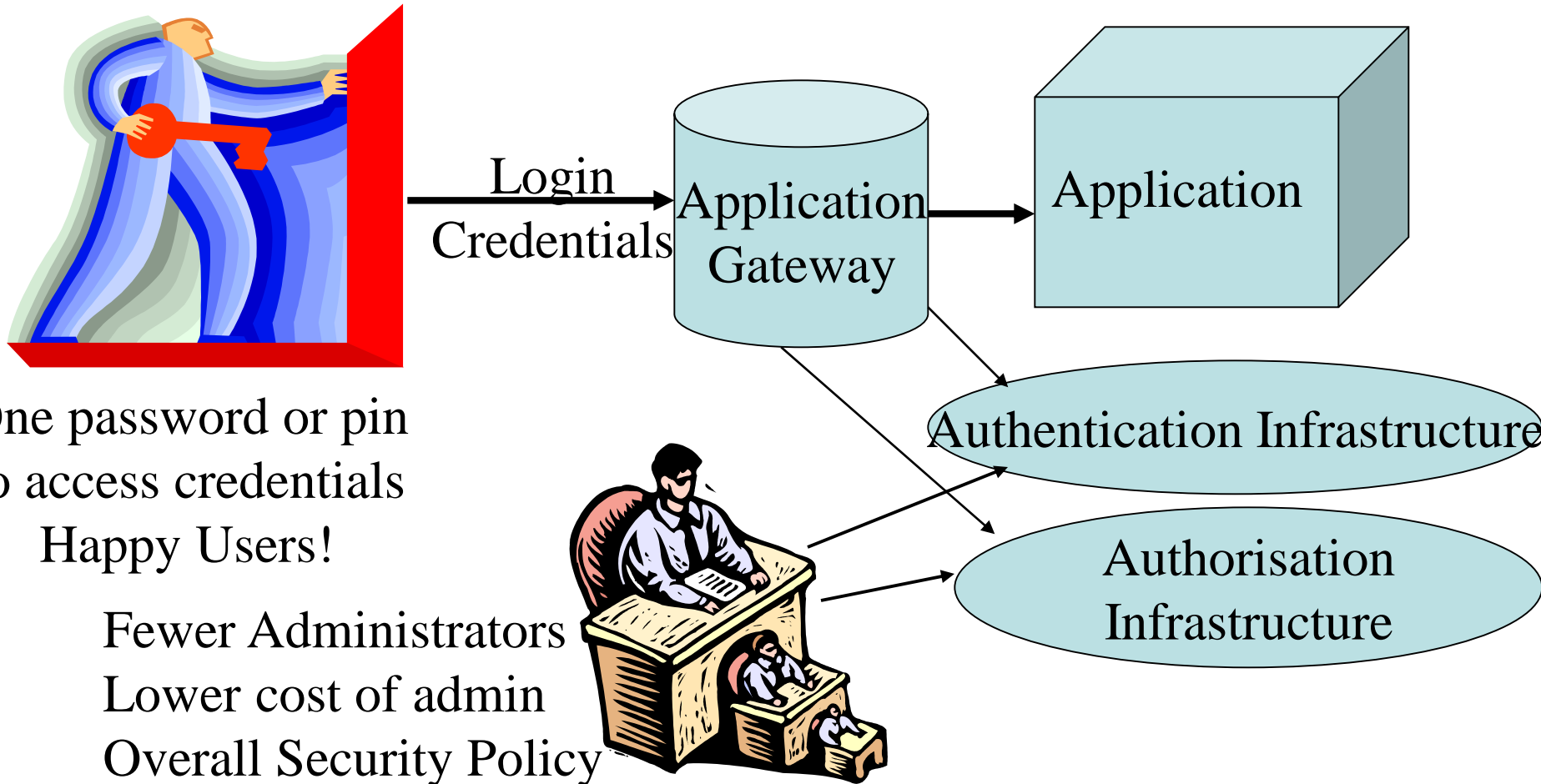
- Authentication is External to the Application



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

Enter Privilege Management Infrastructure

- Authentication and Authorisation are External to the Application



One password or pin
to access credentials

Happy Users!

Fewer Administrators
Lower cost of admin
Overall Security Policy

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

Authorisation Trust Frameworks

- Even more complex than PKI and authentication trust frameworks
- Plenty of work to keep us going for decades to come!

Any Questions

