University of BRISTOL

Systems Security

COMSM1500

bristol.ac.uk

University of BRISTOL

Public Key Infrastructure

bristol.ac.uk

Concepts

- Public Key Infrastructure (PKI)
- Public and private key pair
- Digital certificates
- Digital signature
- Certificate Authorities (CA)
- Transport Layer Security (TLS) protocol
- Certificate chains
- Certificate expiration
- Registration Authority
- Certificate Revocation Lists (CRL)

Public Key Infrastructure (PKI)

- It is a framework, not a specific technology or implementation
- Purpose to manage digital certificate
  - Roles
  - Policies
  - Procedures
- Handle lifecycle of certificates
  - Create
  - Distribute
  - Verify
  - Revoke

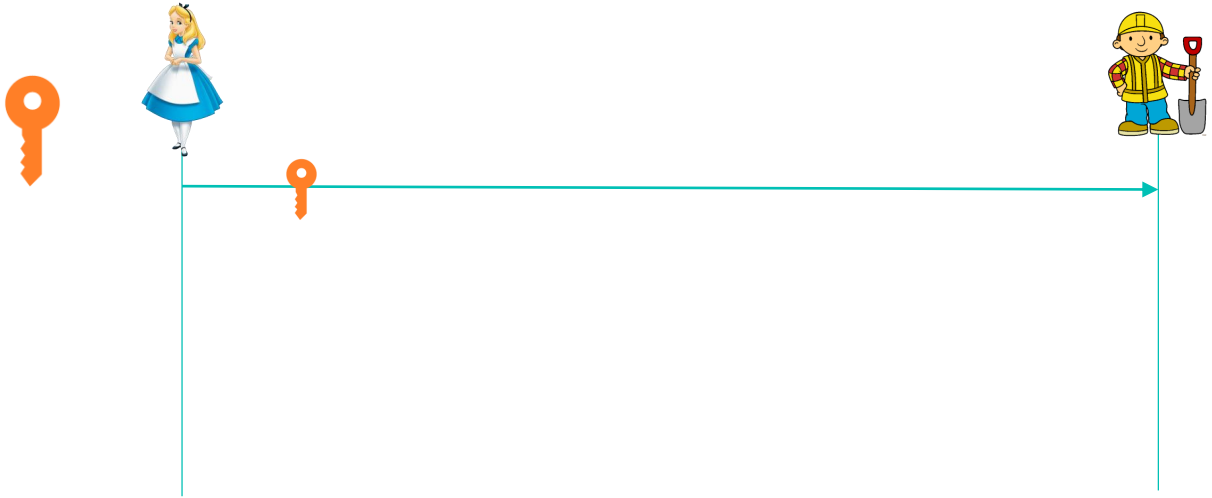
University of BRISTOL

Why PKI?

bristol.ac.uk

Symmetric encryption

Symmetric encryption

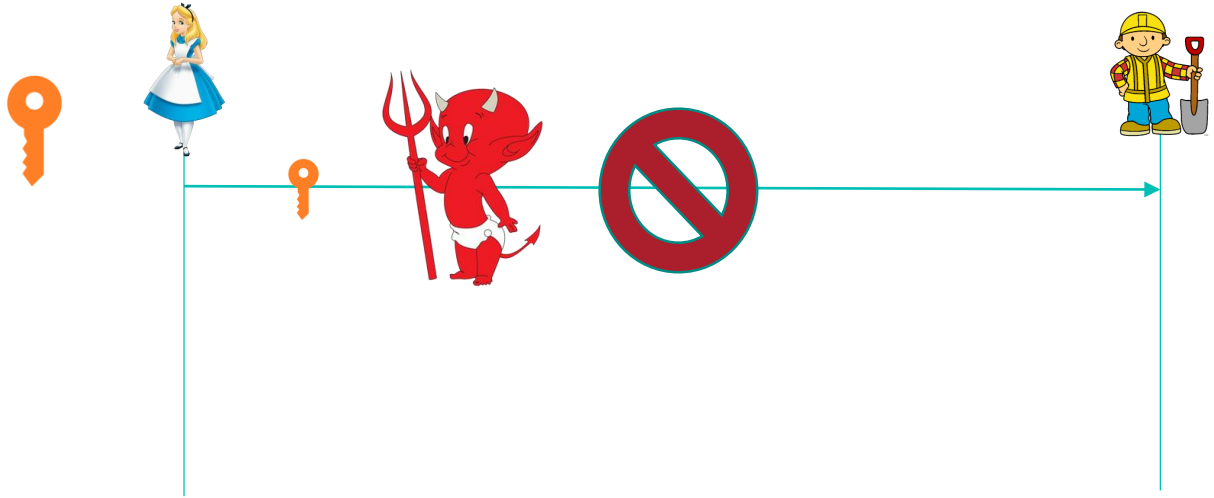


University of BRISTOL

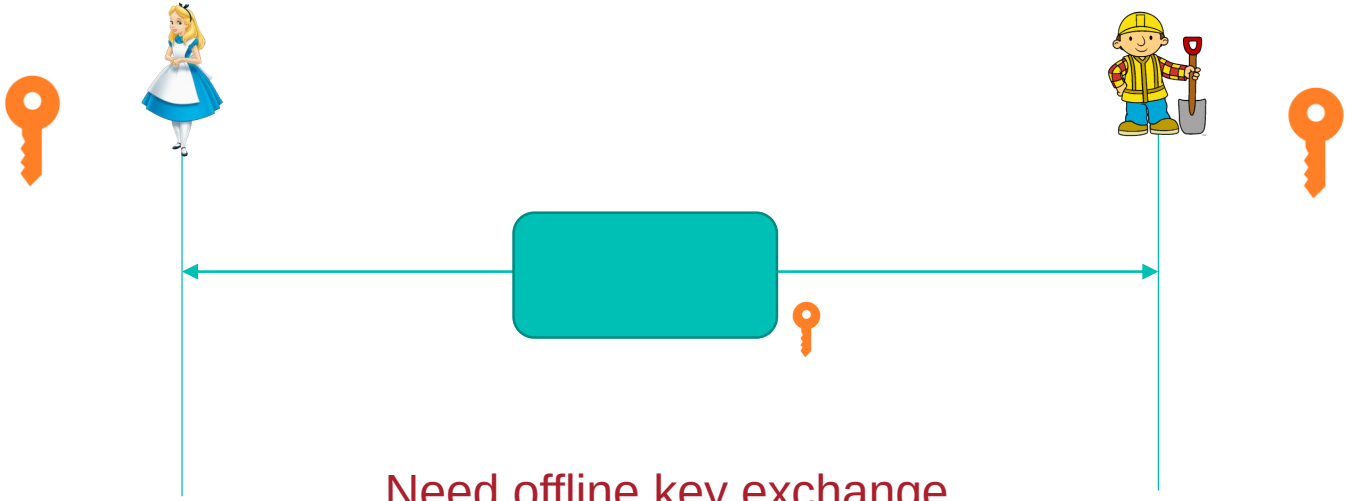
Problem?

bristol.ac.uk

Problem?



Solution?



Need offline key exchange

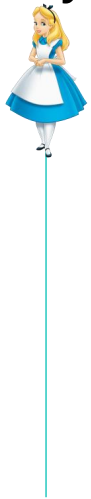
University of BRISTOL

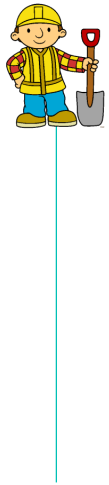
Would asymmetric encryption solve the problem?

bristol.ac.uk

Public/Private key pair

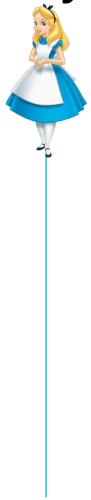
- Asymmetric encryption

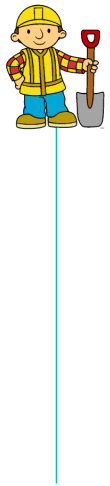




Public/Private key pair

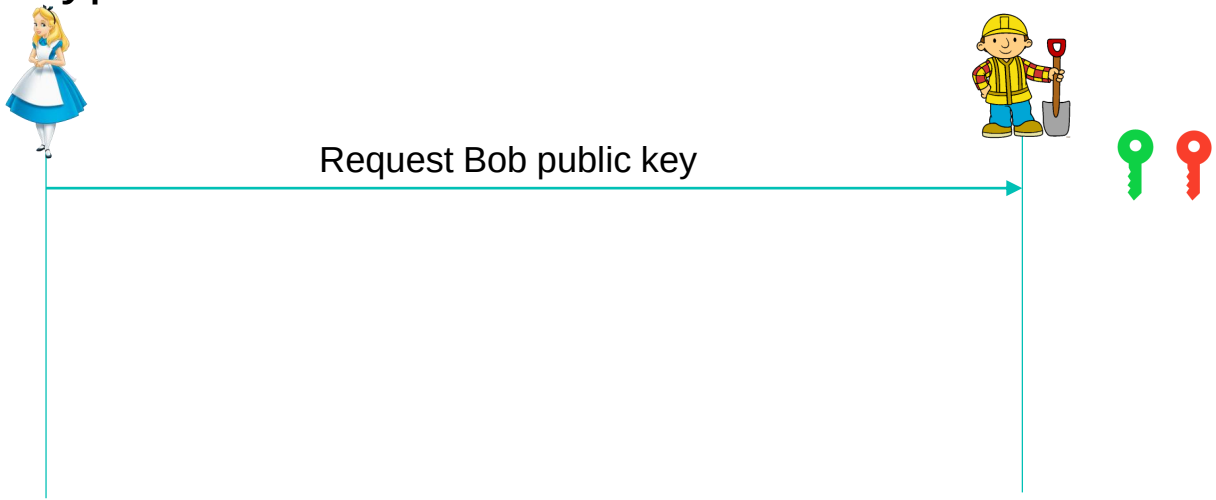
- Asymmetric encryption





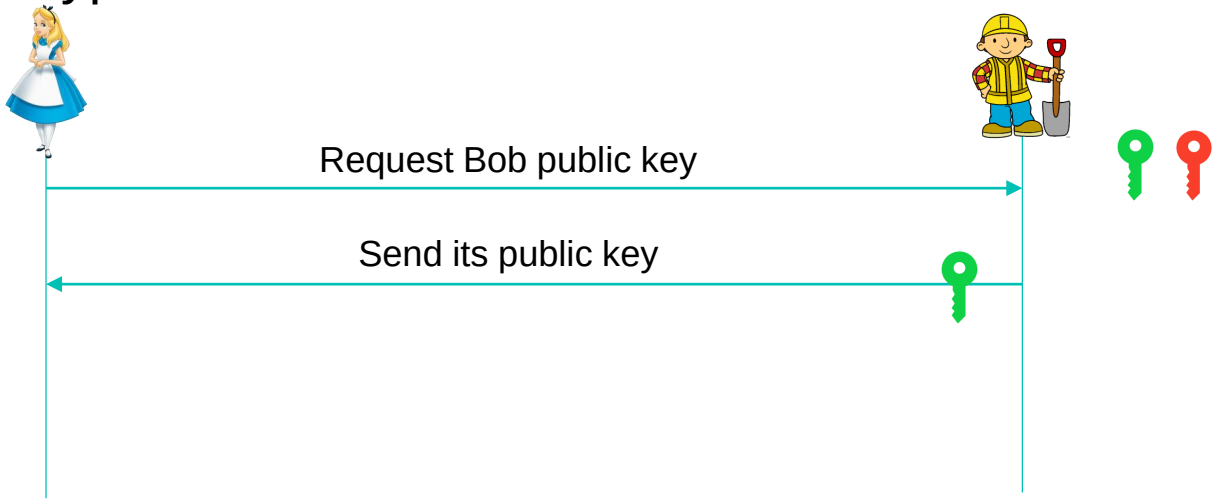
Public/Private key pair

- Asymmetric encryption



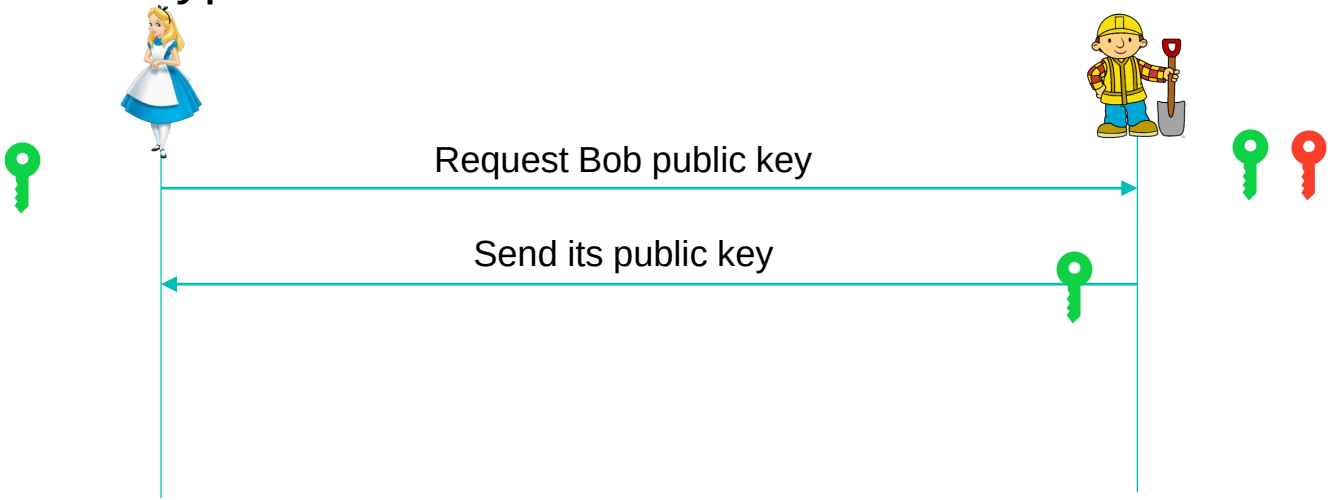
Public/Private key pair

- Asymmetric encryption



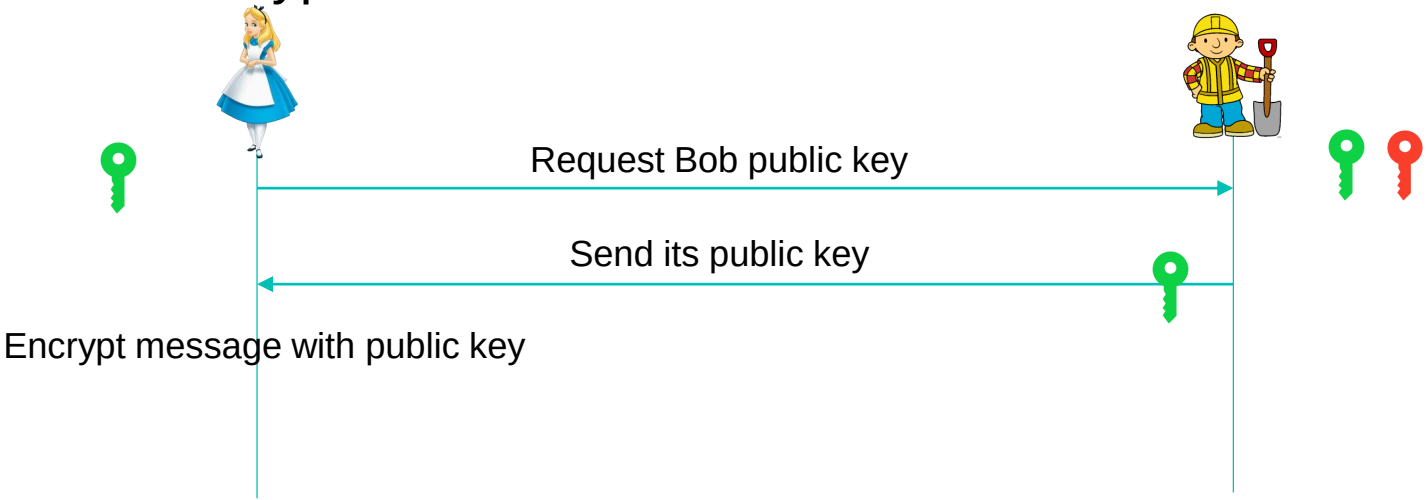
Public/Private key pair

- Asymmetric encryption



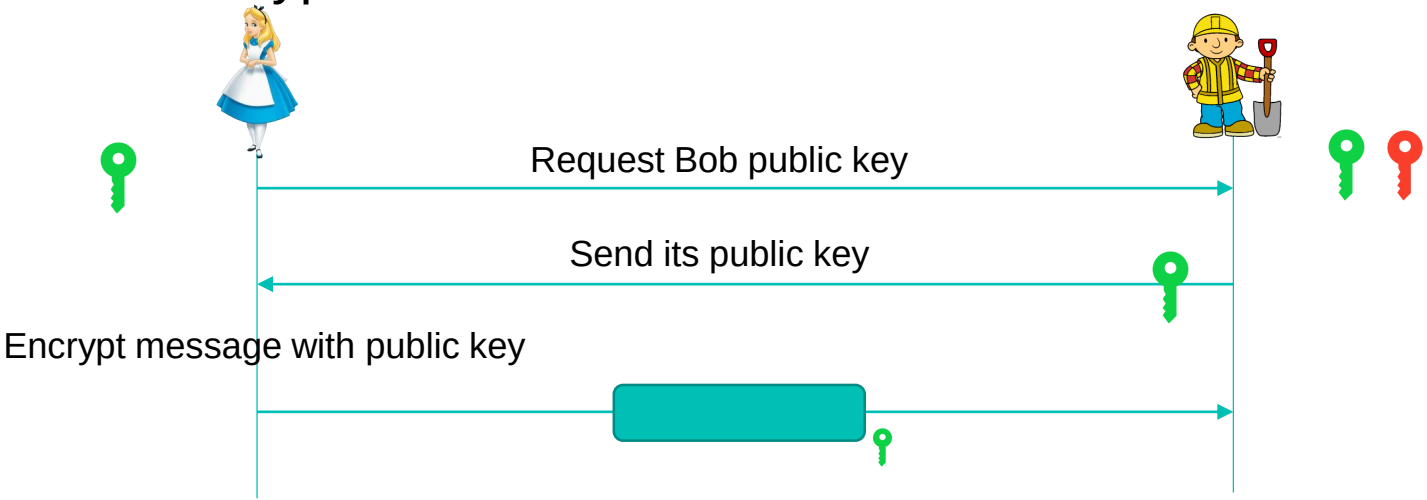
Public/Private key pair

- Asymmetric encryption



Public/Private key pair

- Asymmetric encryption



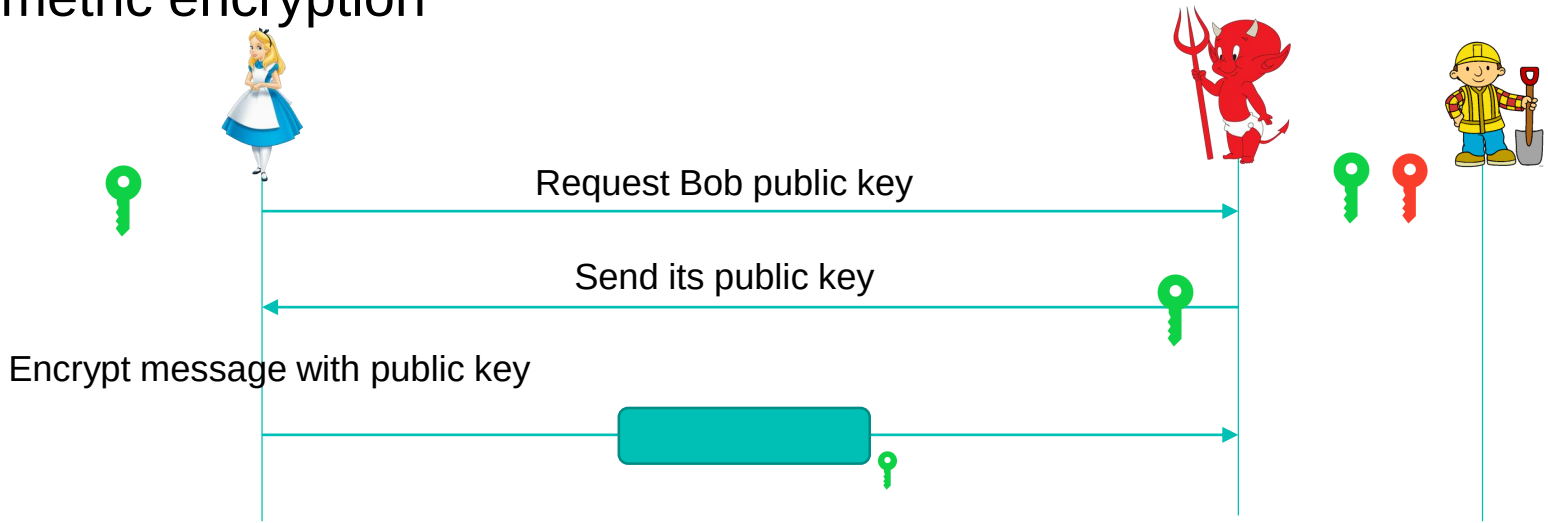
University of BRISTOL

Problem?

bristol.ac.uk

Problem?

- Asymmetric encryption



University of BRISTOL

Solution?

bristol.ac.uk

University of BRISTOL

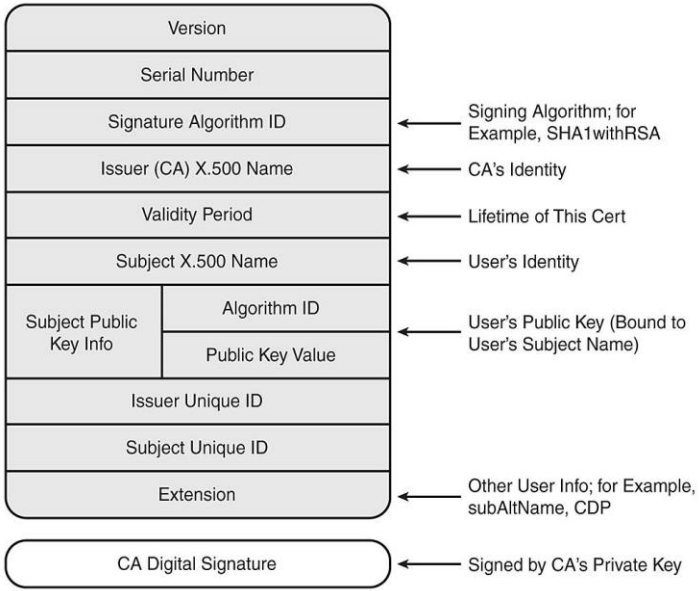
Solution?

Authentication and Certificate

bristol.ac.uk

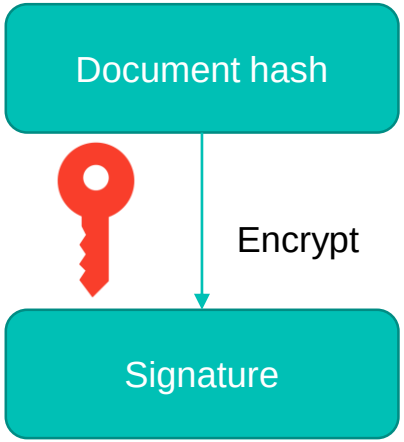
Digital Certificate (X509)

- Help with authentication
- Bind an identity with a public key
- Issued by a Certificate Authority
  - Someone you trust
  - Certify this key belong to Bob!

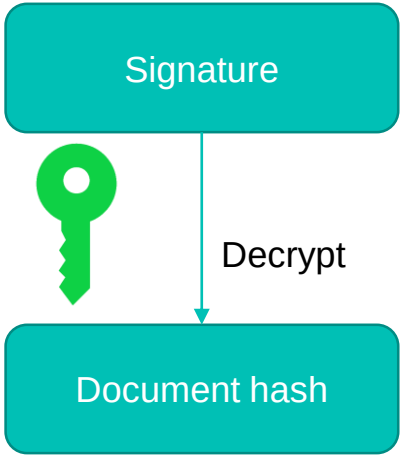


Refresher: digital signature

- Sign



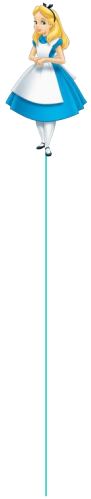
- Verify

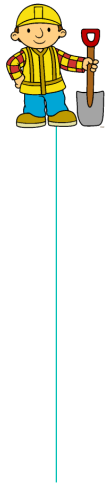


Certificate Authority (CA)

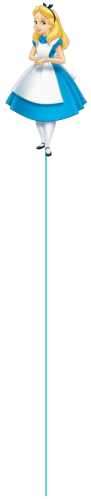
- Responsible for issuing and signing certificate
- Often a “trusted” third party
  - Digicert
  - Verisign
- Companies or organization can have their own CAs

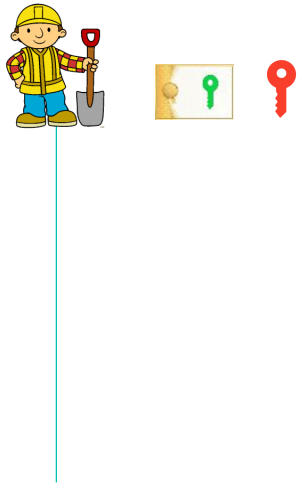
Usage example: TLS (almost)





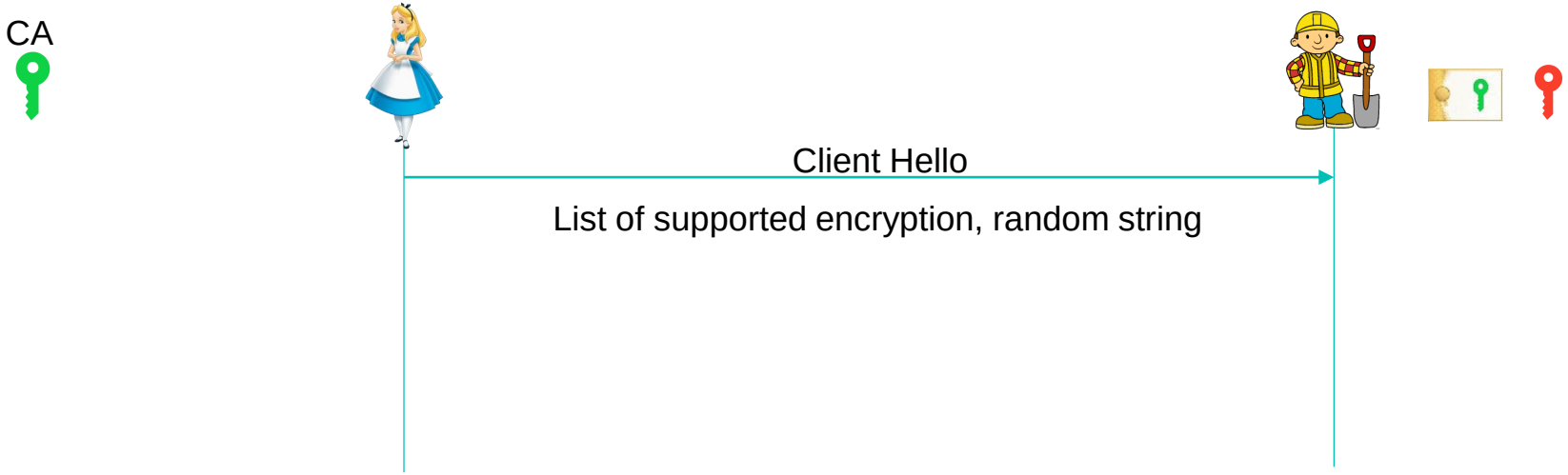
Usage example: TLS (almost)



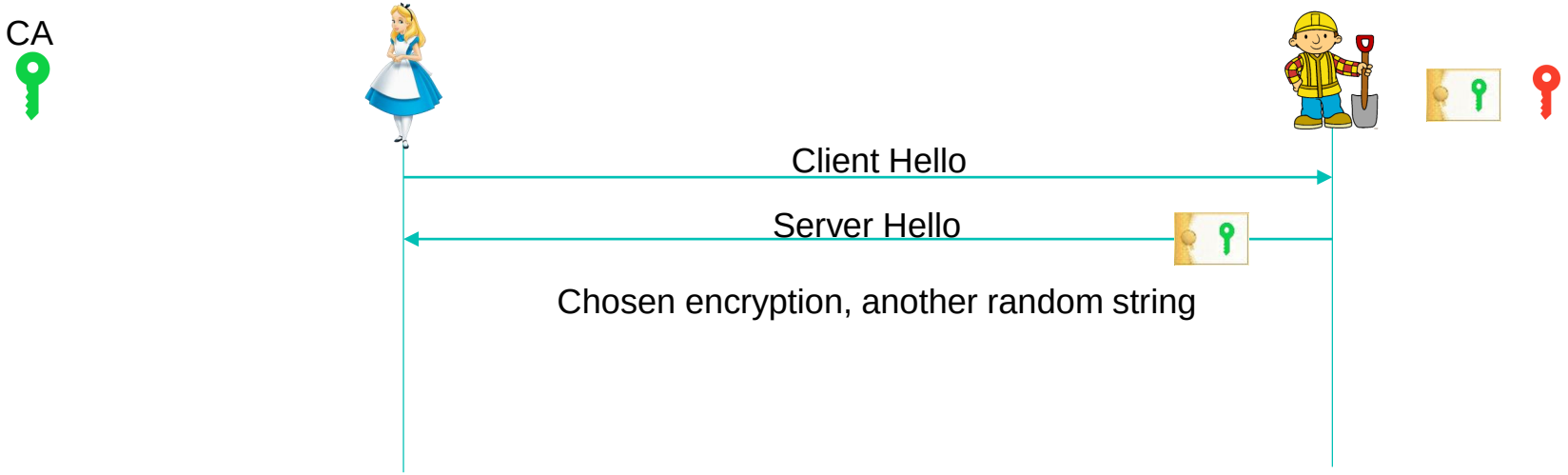


Usage example: TLS (almost)

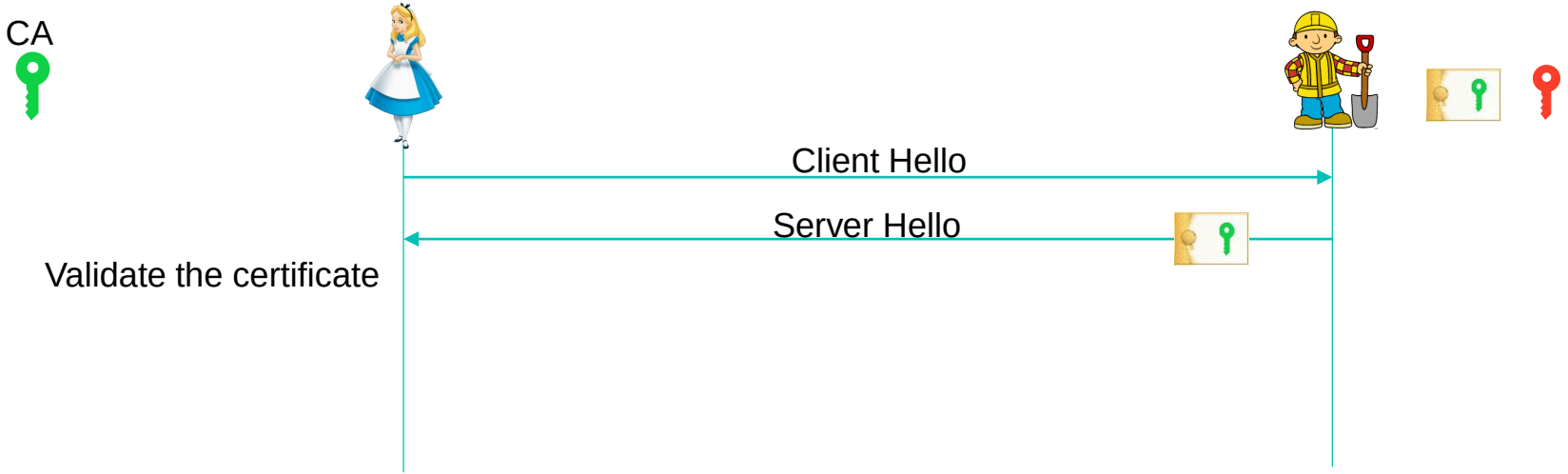
Usage example: TLS



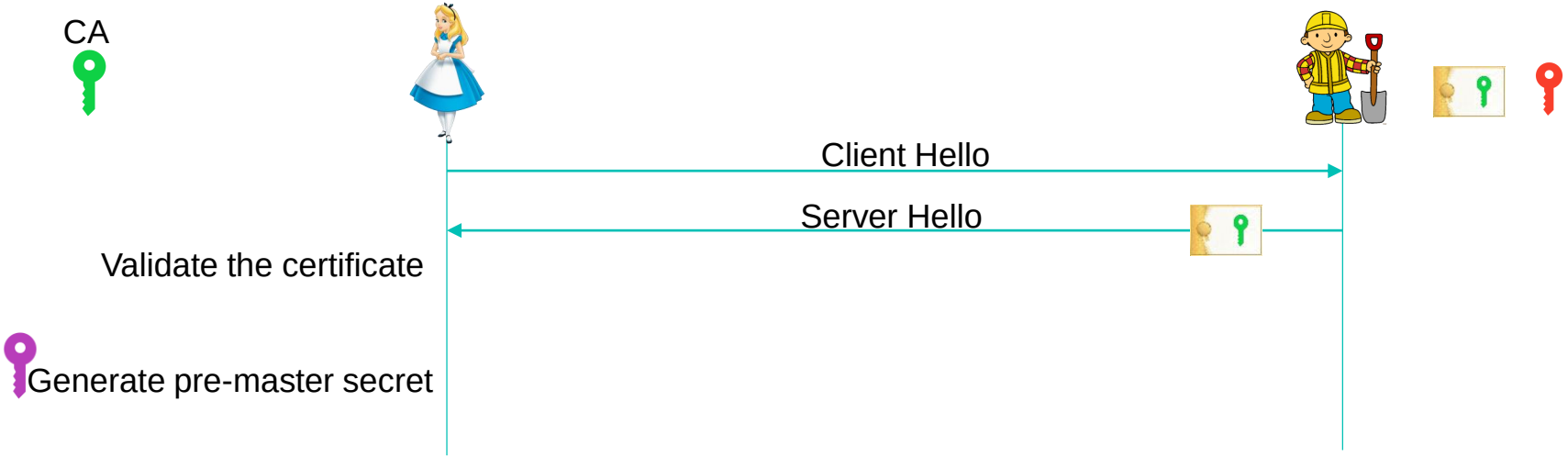
Usage example: TLS (almost)



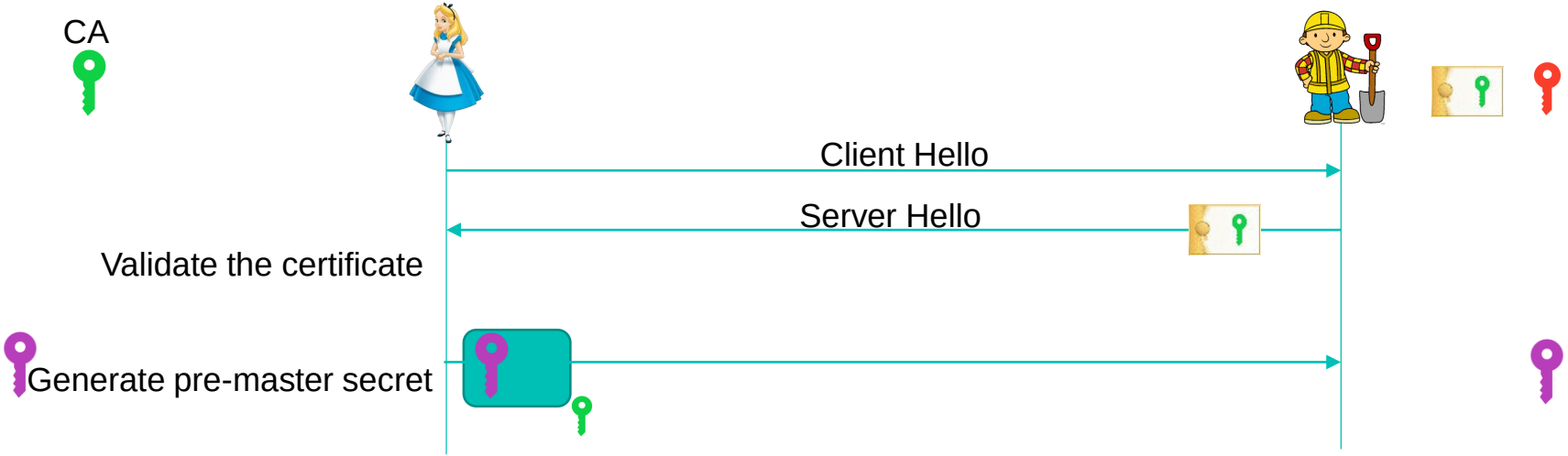
Usage example: TLS (almost)



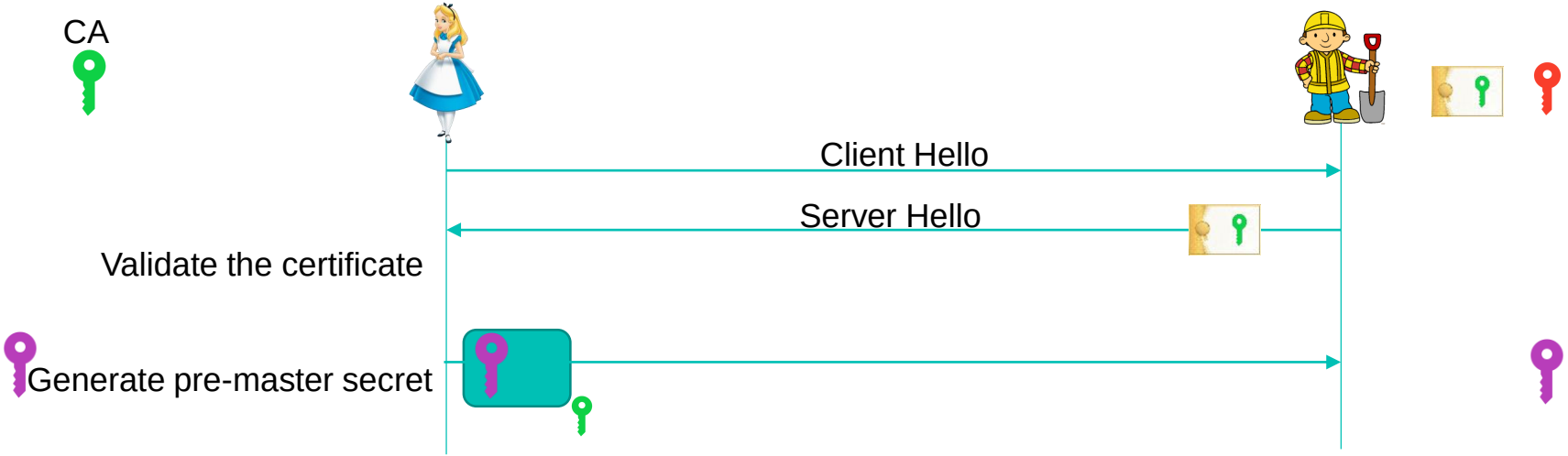
Usage example: TLS (almost)



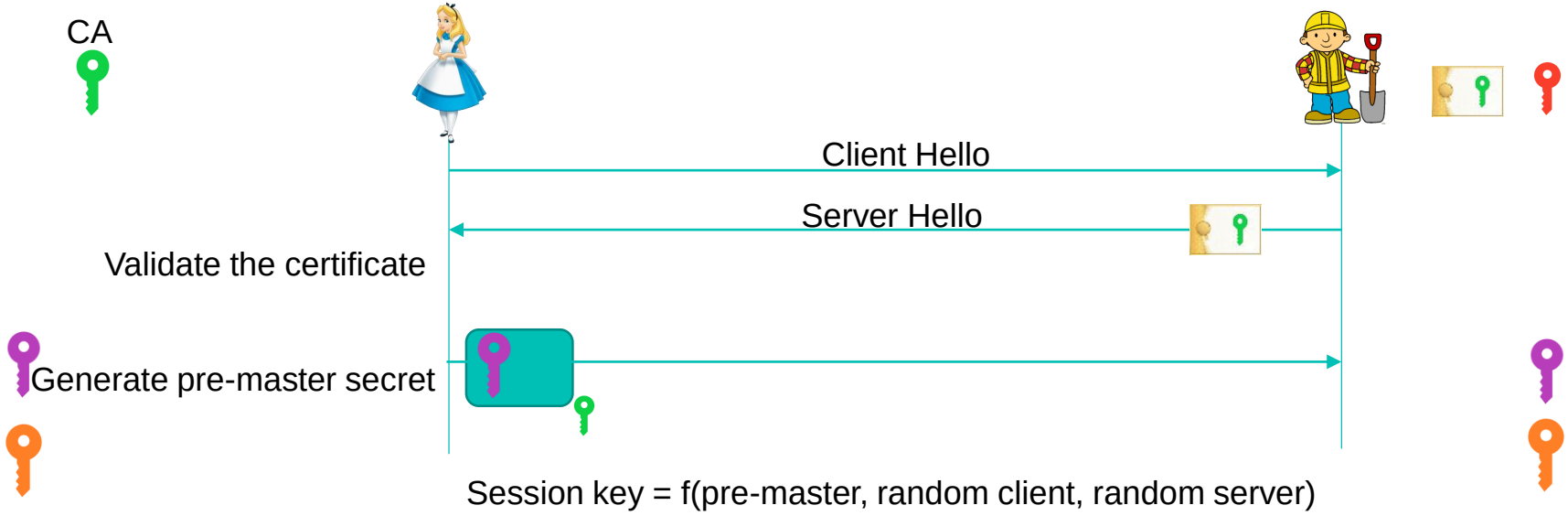
Usage example: TLS (almost)



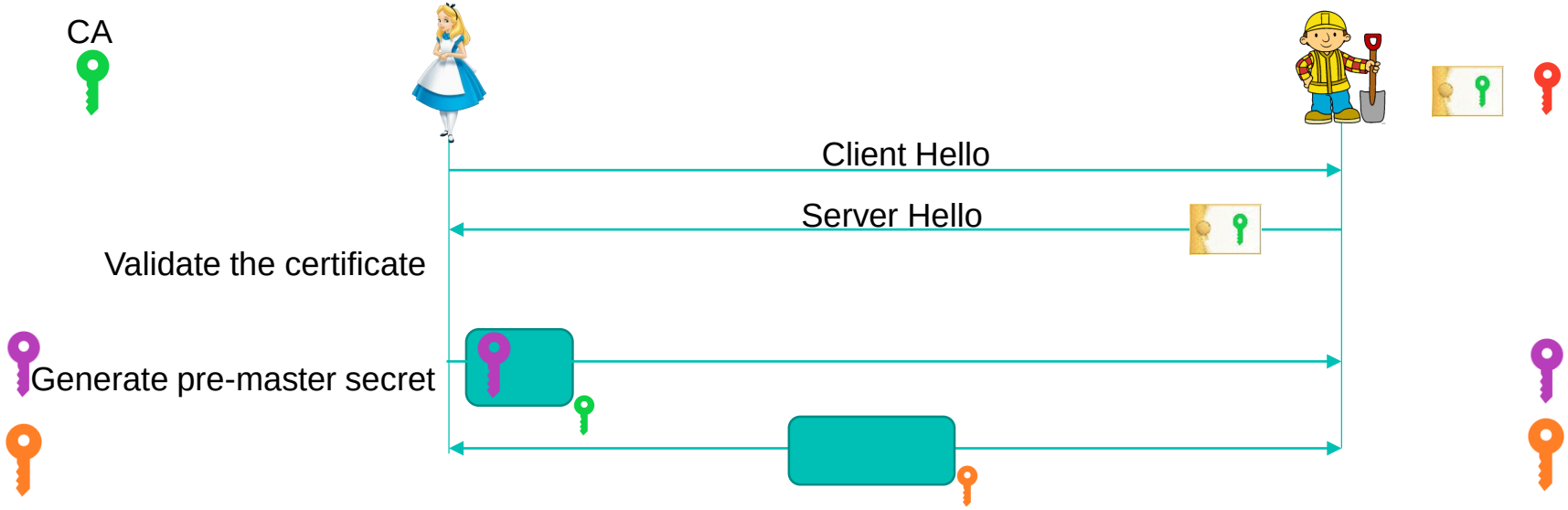
Usage example: TLS (almost)



Usage example: TLS (almost)



Usage example: TLS (almost)



Session established, can exchange message with session key

Usage example: TLS (almost)

- Handshake protocol
  - Authenticate one or both sides (we have seen one side authentication)
  - Negotiate algorithms and parameters
  - Establish a session key (protected via asymmetric cryptography)
- Record protocol
  - Exchange individual message
  - Protected under symmetric key
- Very commong design (SSH, IPsec etc…)

Usage example: TLS (almost)

Homework/potential exam question:
Mutual authentication

- Handshake protocol
  - Authenticate one or both sides (we have seen one side authentication)
  - Negotiate algorithms and parameters
  - Establish a session key (protected via asymmetric cryptography)
- Record protocol
  - Exchange individual message
  - Protected under symmetric key
- Very common design (SSH, IPsec etc…)

RFC 8446

University of BRISTOL

Question

Why the random values?

bristol.ac.uk

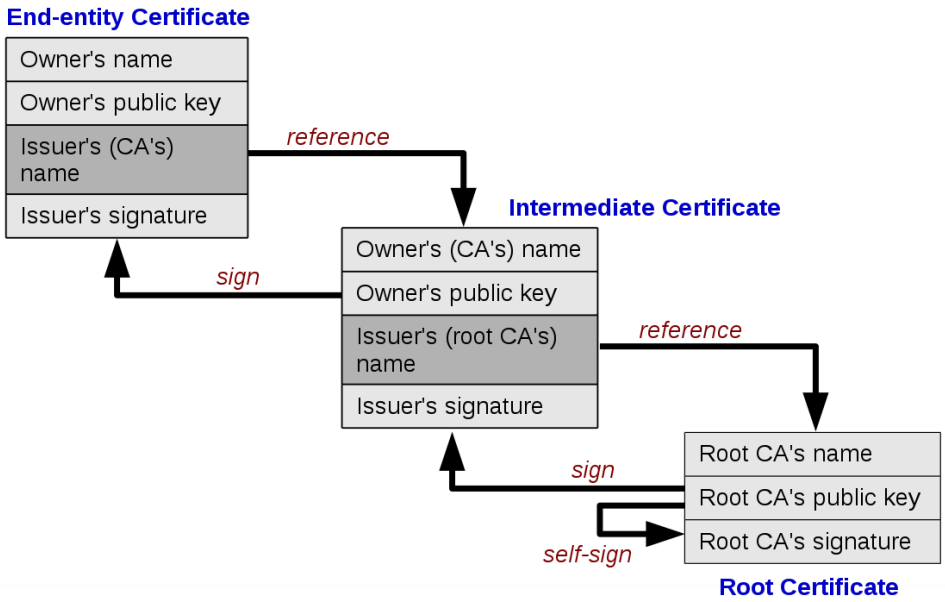
University of BRISTOL

Answer

To avoid replay attack

bristol.ac.uk

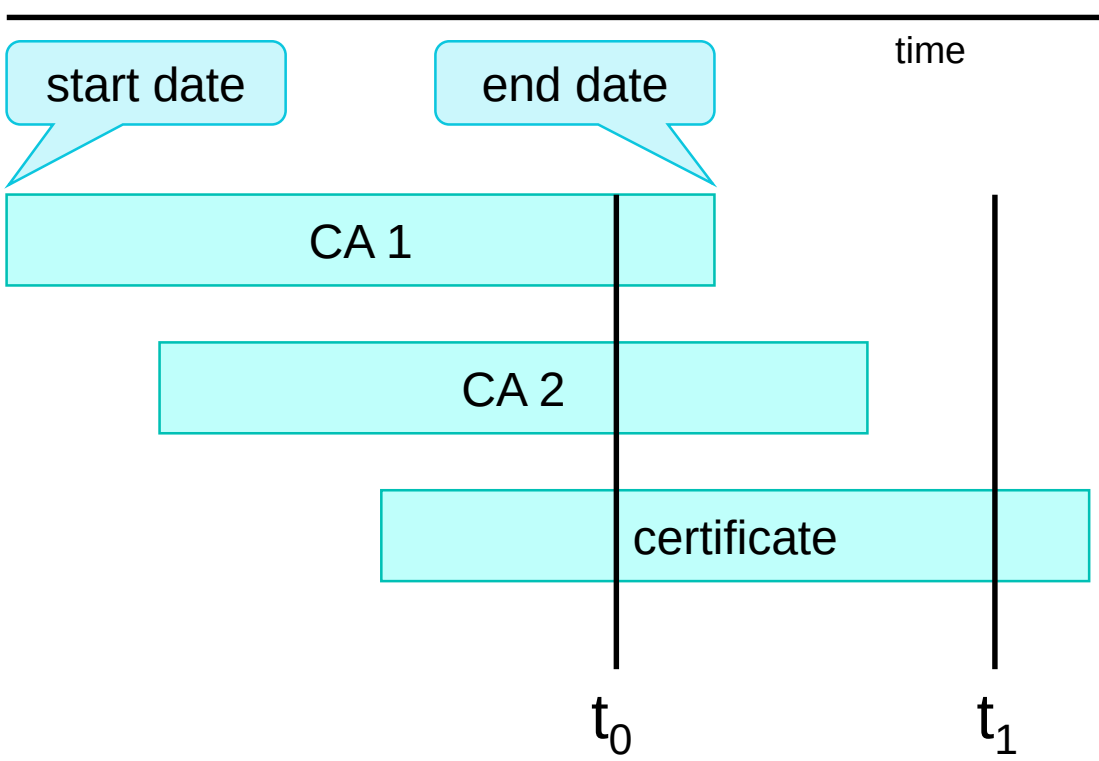
Certificate chains



Certificate chains

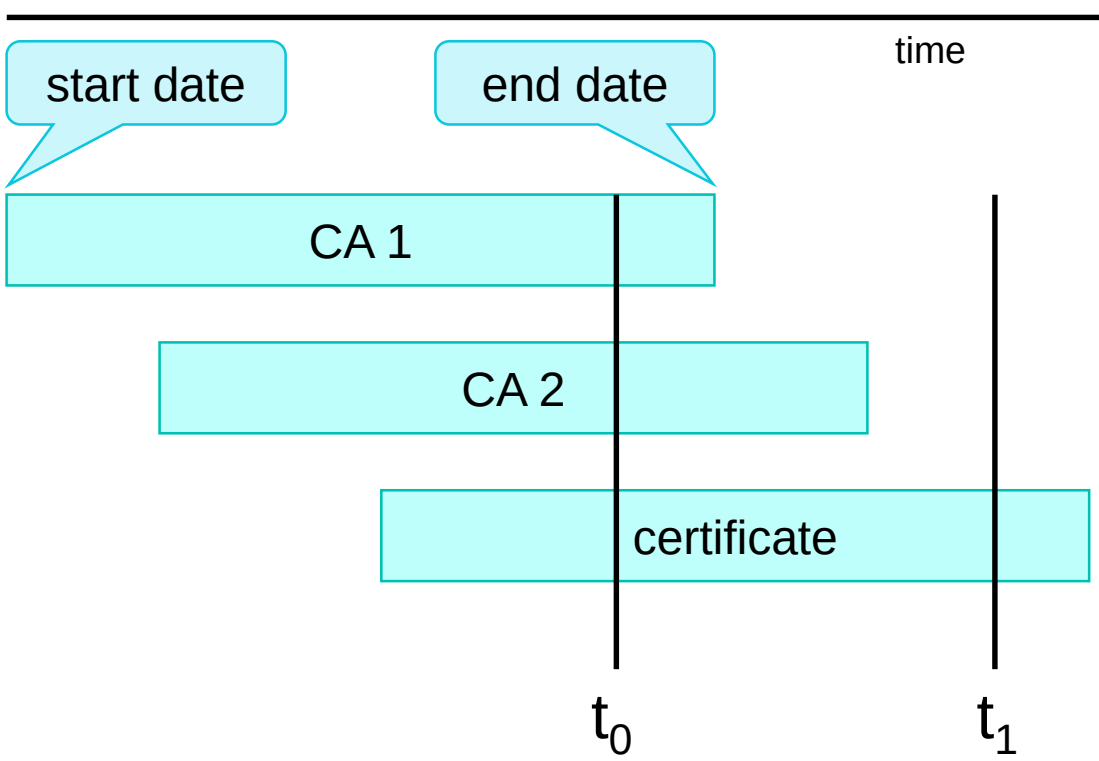
- Constraining delegation
- TLS v3 certificate
  - `nameConstraints=critical;.bristol.ac.uk`
  - Can only issue derived certificate to subdomain of `.bristol.ac.uk`
- If not implemented could create certificate for domain you do not own
- Specified in RFC 5280

Certificate expiration: shell and chains model



- This is a policy decision
- Shell model: certificate is invalid if any certificate in the chain as expired
- Chain model: certificate is valid as long as the certificate itself have not expired, and the parent certificate was valid when the child was signed.
- Is the certificate valid at t0? t1?

Certificate expiration: shell and chains model



- This is a policy decision
- Shell model: certificate is invalid if any certificate in the chain as expired
- Chain model: certificate is valid as long as the certificate itself have not expired, and the parent certificate was valid when the child was signed.
- Is the certificate valid at t0? t1?
  - t0: valid in both case
  - t1: only valid in chain model

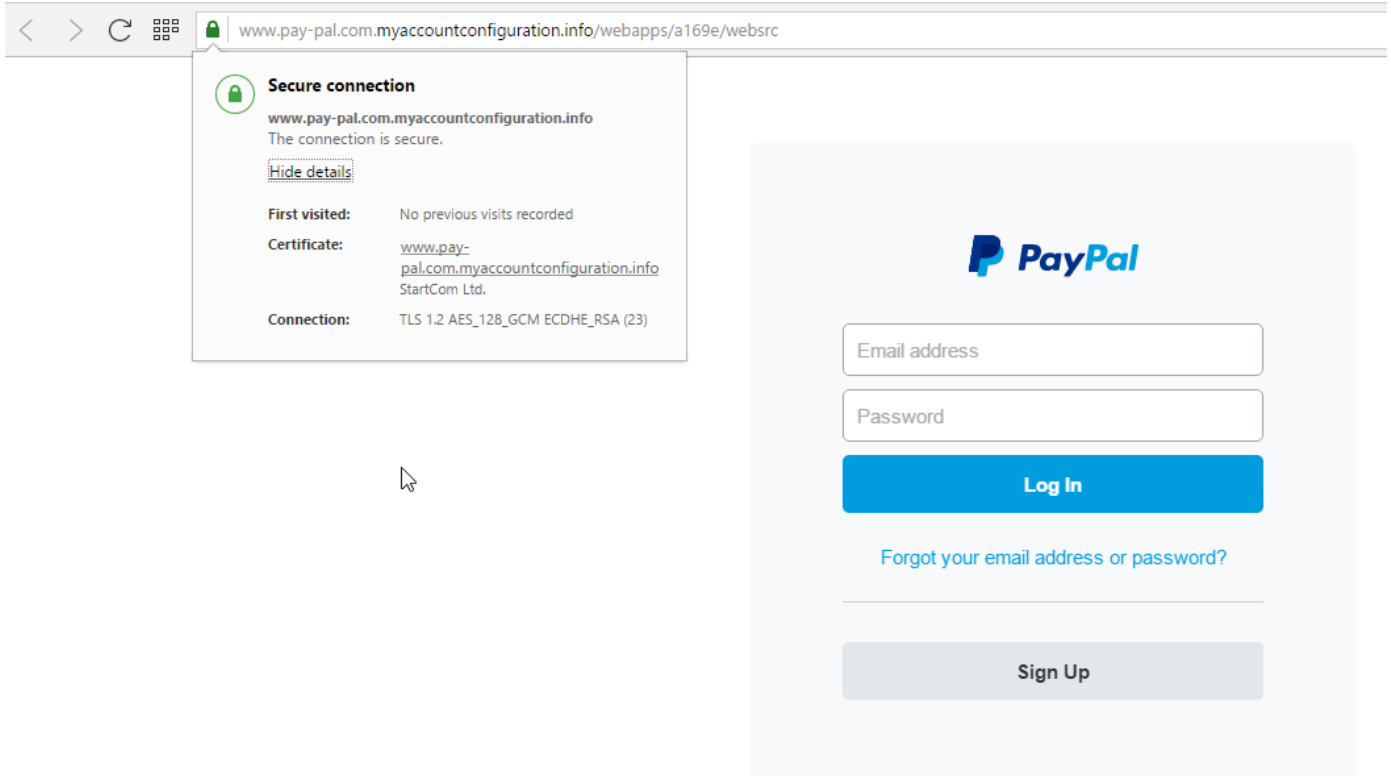
Registration Authority

- The front end entity you interact with to obtain a certificate
- You provide the RA with information
  - e.g. physical presence
- The RA verify your identity
  - e.g. check your passport
- Confirm your identity to the CA and send your public key to be signed
  - Best to generate your own private/key pair
  - Best to limit movement of private key
- Does not sign the certificate

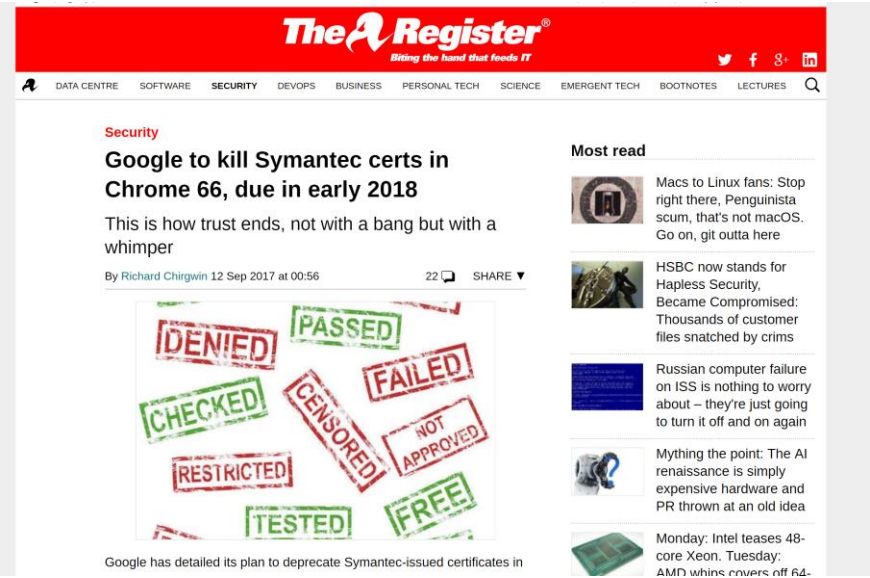
Certificate Revocation List

- The CA publishes and maintain a list of certificates that cannot be used anymore
  - Mean to obtain the list can be in the root certificate
- Reason certificate are revoked (this is permanent)
  - Compromised private key
  - Human resources reason
  - Company change name, physical address, DNS etc…
  - Any other reason you can come up with before expiration
- Certificate owner/administrator can request the certificate to be revoked
- CA may revoke certificates (e.g. malicious website etc.)
- Browsers may stop to include root certificate of untrustworthy CA
  - e.g. give signed certificate to dodgy party
  - Fail to revoke them when notified

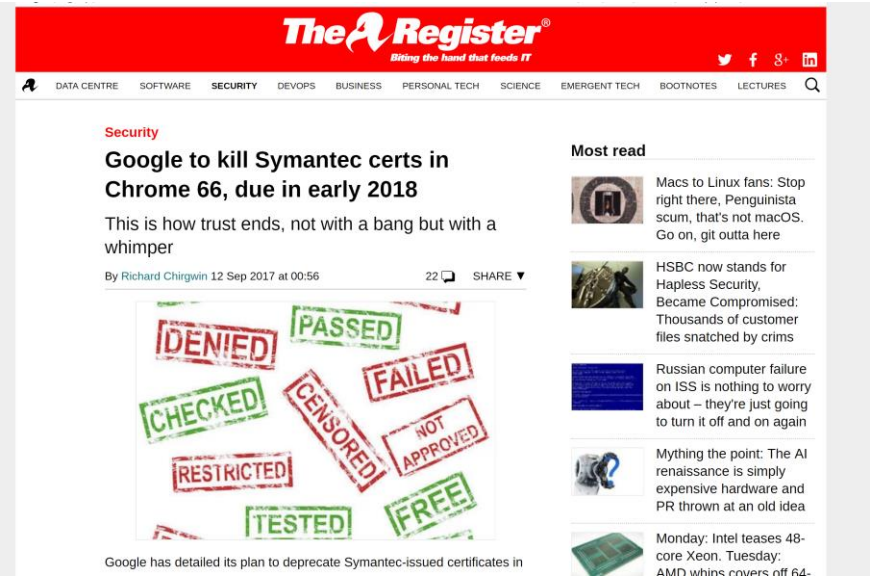
A legitimate fake site (from Lecture 2!)



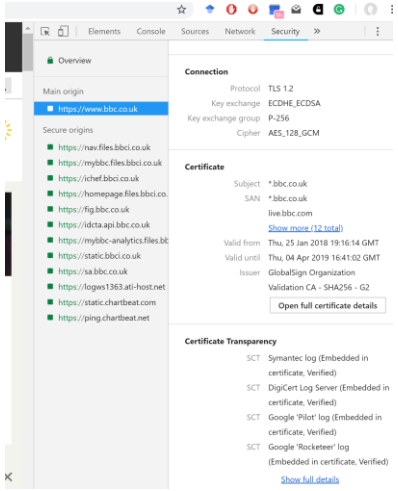
Certificate Revocation List



Certificate Revocation List

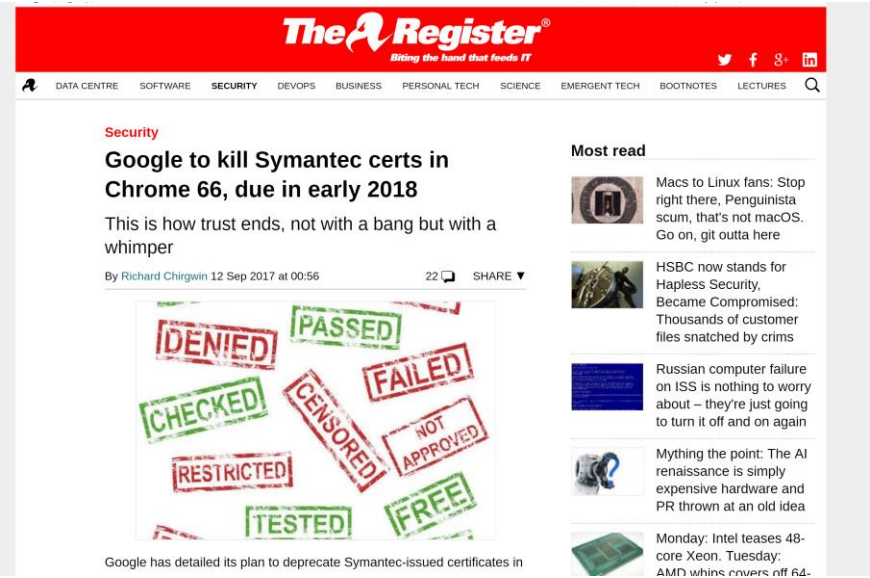


- Read more:
  - https://www.certificate-transparency.org/
  - Check it out on chrome

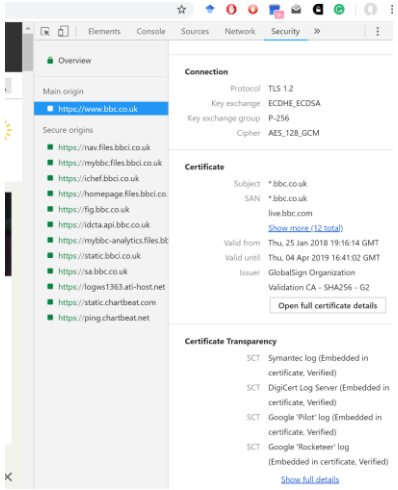


Certificate Revocation List

Homework/potential exam question:
Explain Google's Certificate Transparency



- Read more:
  - https://www.certificate-transparency.org/
  - Check it out on chrome



Key Escrow

- Controversial in many country
- Optional (more secure without it)
- Third party that held private key
- Can disclose this key under certain circumstances
  - e.g. to law enforcement agency with a proper warrant
- Alternative key disclosure law
  - Problematic in some jurisdiction due to self-incrimination (e.g. US 5th)
  - In UK that's fine first case in 2007 against animal right activists

Key Terms

Term	Definition
Public Key Infrastructure	Framework that associates a public key to a verified identity
Public key	Element of the key pair shared with the public. Used for encryption or signature verification.
Private key	Element of the key pair that is secret. Should only be known by the owner. Used for decryption or to generate signature.
Certificate Authority	A CA is responsible for issuing and revoking digital certificates
Digital certificate	An electronic document used to prove the ownership of a public key

Key Terms

Term	Definition
Registration Authority	Verify the identity of the prospective key owner and send it to the CA for signature.
Certificate Revocation List	A list of certificates that are no longer valid. The list is publicly available and maintained by a certificate authority.

Concepts

- Public Key Infrastructure (PKI)
- Public and private key pair
- Digital certificates
- Digital signature
- Certificate Authorities (CA)
- Transport Layer Security (TLS) protocol
- Certificate chains
- Certificate expiration
- Registration Authority
- Certificate Revocation Lists (CRL)

Concepts

- Public Key Infrastructure (PKI)
  - A framework to manage, share and verify public key
  - Used by many technology, not a particular implementation
- Public and private key pair
- Digital certificates
- Digital signature
- Certificate Authorities (CA)
- Transport Layer Security (TLS) protocol
- Certificate chains
- Certificate expiration
- Registration Authority
- Certificate Revocation Lists (CRL)

Concepts

- Public Key Infrastructure (PKI)
- Public and private key pair
  - Mathematically related
  - Decrypt message encrypted by the other member of the pair
  - Asymmetric cryptography
- Digital certificates
- Digital signature
- Certificate Authorities (CA)
- Transport Layer Security (TLS) protocol
- Certificate chains
- Certificate expiration
- Registration Authority
- Certificate Revocation Lists (CRL)

Concepts

- Public Key Infrastructure (PKI)
- Public and private key pair
- Digital certificates
  - Electronic document binding a public key to an identity
- Digital signature
- Certificate Authorities (CA)
- Transport Layer Security (TLS) protocol
- Certificate chains
- Certificate expiration
- Registration Authority
- Certificate Revocation Lists (CRL)

Concepts

- Public Key Infrastructure (PKI)
- Public and private key pair
- Digital certificates
- Digital signature
  - Hash of a document encrypted with a private key
  - Can be verified with a public key
  - Used for authenticate the document (can also be used for integrity or non-repudiation in other contexts)
- Certificate Authorities (CA)
- Transport Layer Security (TLS) protocol
- Certificate chains
- Certificate expiration
- Registration Authority
- Certificate Revocation Lists (CRL)

Concepts

- Public Key Infrastructure (PKI)
- Public and private key pair
- Digital certificates
- Digital signature
- Certificate Authorities (CA)
  - The most important part of PKI
  - Responsible for the management of certificates
- Transport Layer Security (TLS) protocol
- Certificate chains
- Certificate expiration
- Registration Authority
- Certificate Revocation Lists (CRL)

Concepts

- Public Key Infrastructure (PKI)
- Public and private key pair
- Digital certificates
- Digital signature
- Certificate Authorities (CA)
- Transport Layer Security (TLS) protocol
  - Used for example in HTTPS to authenticate servers
  - One example usage of PKI and certificates
- Certificate chains
- Certificate expiration
- Registration Authority
- Certificate Revocation Lists (CRL)

Concepts

- Public Key Infrastructure (PKI)
- Public and private key pair
- Digital certificates
- Digital signature
- Certificate Authorities (CA)
- Transport Layer Security (TLS) protocol
- Certificate chains
  - You can create sub-certificates, for example to delegate authority
  - Need to validate the entire chain
  - Can restrict delegation capability
- Certificate expiration
- Registration Authority
- Certificate Revocation Lists (CRL)

Concepts

- Public Key Infrastructure (PKI)
- Public and private key pair
- Digital certificates
- Digital signature
- Certificate Authorities (CA)
- Transport Layer Security (TLS) protocol
- Certificate chains
- Certificate expiration
  - There is different methods to verify the expiration of a certificate chain (shell or chain model)
  - This is a matter of policy
- Registration Authority
- Certificate Revocation Lists (CRL)

Concepts

- Public Key Infrastructure (PKI)
- Public and private key pair
- Digital certificates
- Digital signature
- Certificate Authorities (CA)
- Transport Layer Security (TLS) protocol
- Certificate chains
- Certificate expiration
- Registration Authority
  - Organisation/individual responsible for verifying and validating individual identity
  - Send public key to generate the certificate to be signed by the CA
- Certificate Revocation Lists (CRL)

Concepts

- Public Key Infrastructure (PKI)
- Public and private key pair
- Digital certificates
- Digital signature
- Certificate Authorities (CA)
- Transport Layer Security (TLS) protocol
- Certificate chains
- Certificate expiration
- Registration Authority
- Certificate Revocation Lists (CRL)
  - A list of certificate that are no longer valid for various reasons (e.g. secret key was stolen)
  - Maintained by the CA

Concepts

- Public Key Infrastructure (PKI)
- Public and private key pair
- Digital certificates
- Digital signature
- Certificate Authorities (CA)
- Transport Layer Security (TLS) protocol
- Certificate chains
- Certificate expiration
- Registration Authority
- Certificate Revocation Lists (CRL)

University of BRISTOL

Thank you, questions?

Office MVB 3.26

bristol.ac.uk