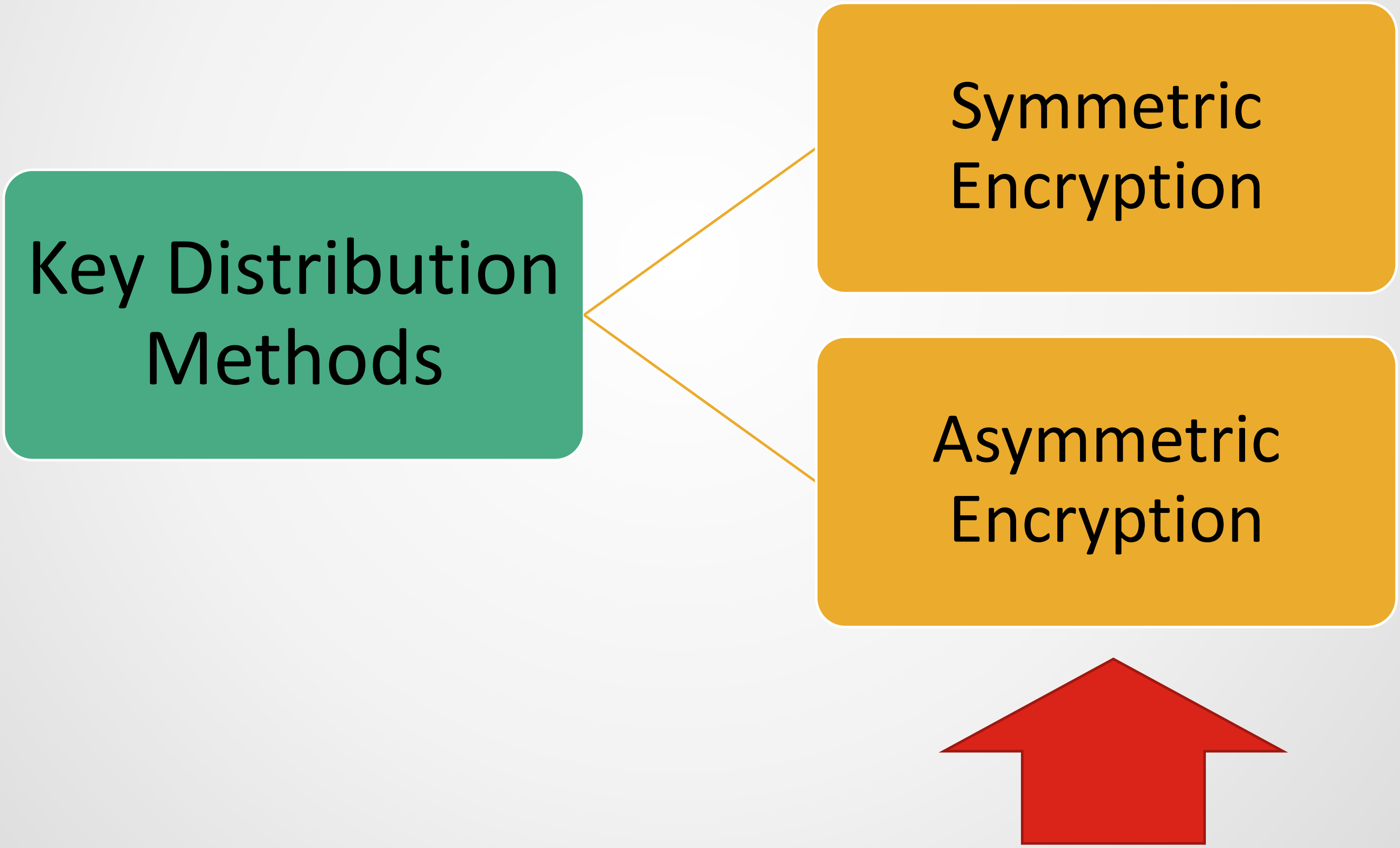
Theory of Blockchain

Session 4:

Asymmetric Cryptography - Part 2

Module 2 – Key Management

Key Distribution Methods

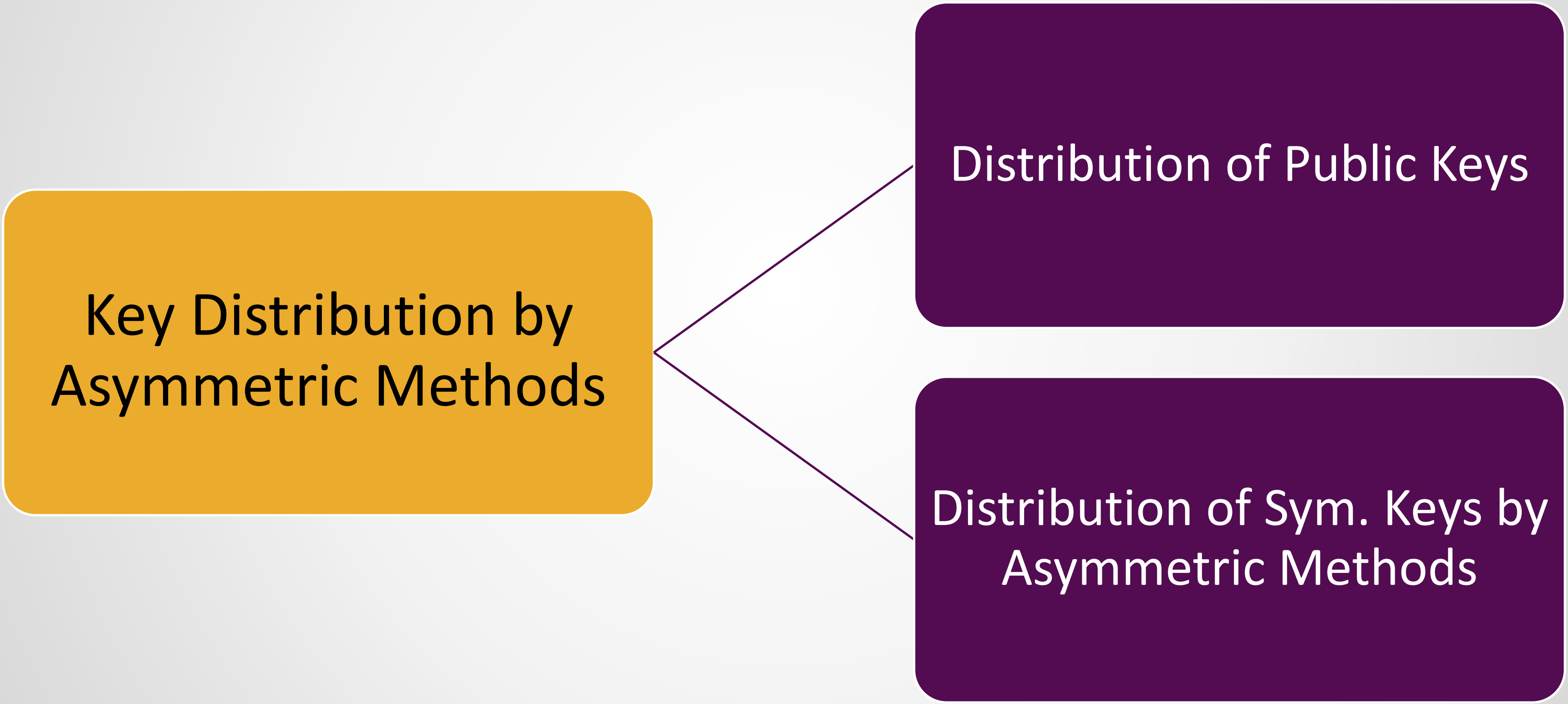


Key Distribution Methods

Symmetric Encryption

Asymmetric Encryption

Key Distribution using Asymmetric Methods



Key Distribution by Asymmetric Methods

Distribution of Public Keys

Distribution of Sym. Keys by Asymmetric Methods

Possible Ways to Distribute Keys

1. A key could be selected by A and physically delivered to B.
2. If A and B have previously shared a key, one party could transmit the new key to the other, using the old key to encrypt the new key.
3. A third party (C) could select the key and physically deliver it to A and B (or C can take A's key and deliver it to B).
4. If a third party like C has keys with both A and B, C , either directly or indirectly can deliver a key over encrypted links to A and B.
5. A trusted third party like C endorses the (public) keys of A and B.
6. A and B use Diffie-Hellman-like protocols.

C= Key Distribution Centre (KDC)
or Trusted Third Party (TTP)

Public Key Certificates

- Anyone can create a pair of public/private keys (e.g. by openssl). But how is the public key associated with the real identity of the key creator/owner?
  - Can we trust the claims about key ownerships over internet links?
    - If there's no authority to endorse the association of a key with the real identity of the owner, anybody can claim to be the owner of the key over internet. Similarly, an attacker can sit over the link and replace the key on the transit with his/her key. Afterwards, the recipient thinks that is the key of the sender and encrypts confidential information with the attacker's key.

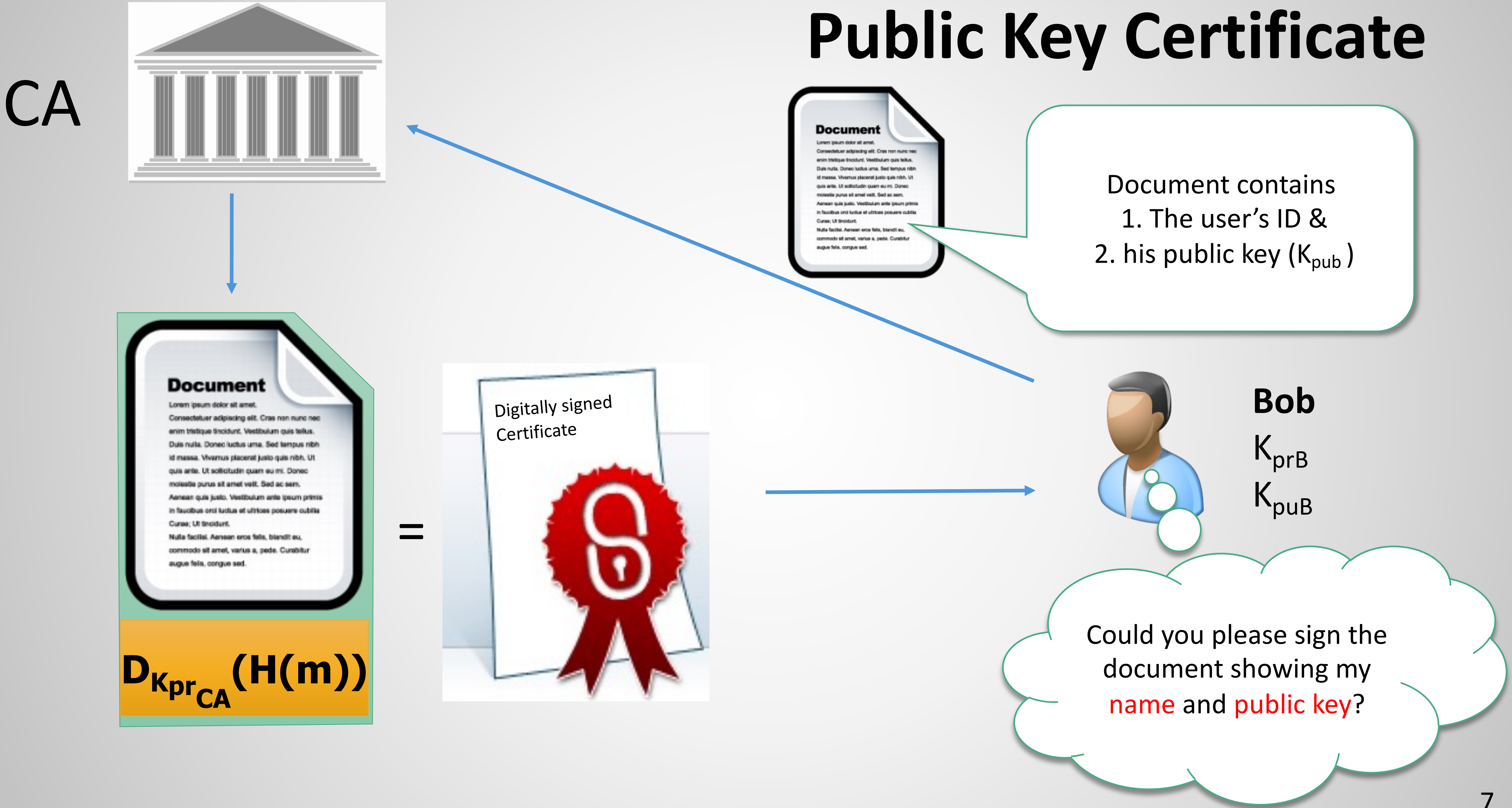
Therefore, we need someone trusted to endorse the ownership of (public) keys. Such a person is called TTP or in practice, Certificate Authority (CA).

Authentication using the Trusted 3rd Party

- Once we securely find the public key of an entity on the net, we can use any of the previous asymmetric algorithms to authenticate it e.g. by sending an encrypted challenge and asking the entity to decrypt it.

- Websites which use https (http over SSL/TLS) are usually authenticated by such asymmetric methods.

Public Key Certificate



CA

Document contains
1. The user's ID &
2. his public key (K_{pub})

Bob
K_{prB}
K_{puB}

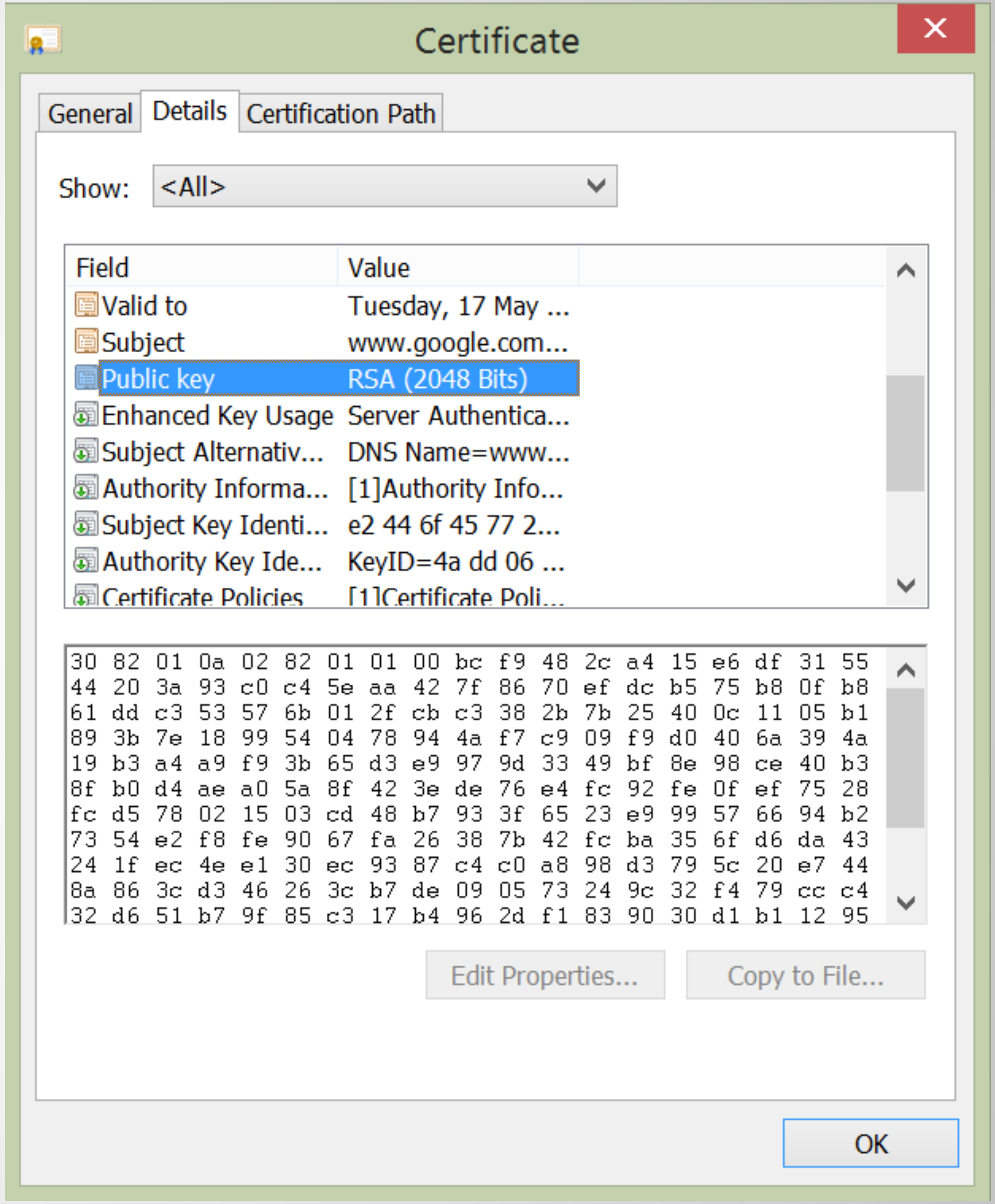
Could you please sign the document showing my name and public key?

$D_{Kpr_{CA}}(H(m))$ =

HTTPS

- In a secure website's case, Bob's name is "www.example.com".

- So the certificate will be issued for www.example.com which contains its public key.



Show: <All>

Field	Value
Valid to	Tuesday, 17 May ...
Subject	www.google.com...
Public key	RSA (2048 Bits)
Enhanced Key Usage	Server Authentica...
Subject Alternativ...	DNS Name=www...
Authority Informa...	[1]Authority Info...
Subject Key Identi...	e2 44 6f 45 77 2...
Authority Key Ide...	KeyID=4a dd 06 ...
Certificate Policies	[1]Certificate Poli...

```
30 82 01 0a 02 82 01 01 00 bc f9 48 2c a4 15 e6 df 31 55
44 20 3a 93 c0 c4 5e aa 42 7f 86 70 ef dc b5 75 b8 0f b8
61 dd c3 53 57 6b 01 2f cb c3 38 2b 7b 25 40 0c 11 05 b1
89 3b 7e 18 99 54 04 78 94 4a f7 c9 09 f9 d0 40 6a 39 4a
19 b3 a4 a9 f9 3b 65 d3 e9 97 9d 33 49 bf 8e 98 ce 40 b3
8f b0 d4 ae a0 5a 8f 42 3e de 76 e4 fc 92 fe 0f ef 75 28
fc d5 78 02 15 03 cd 48 b7 93 3f 65 23 e9 99 57 66 94 b2
73 54 e2 f8 fe 90 67 fa 26 38 7b 42 fc ba 35 6f d6 da 43
24 1f ec 4e e1 30 ec 93 87 c4 c0 a8 98 d3 79 5c 20 e7 44
8a 86 3c d3 46 26 3c b7 de 09 05 73 24 9c 32 f4 79 cc c4
32 d6 51 b7 9f 85 c3 17 b4 96 2d f1 83 90 30 d1 b1 12 95
```

X.509

- X.509 is a widely accepted format for certificates.
  - It is part of ITU X.500 standards which provide a framework for user authentication based on distributed directory services.

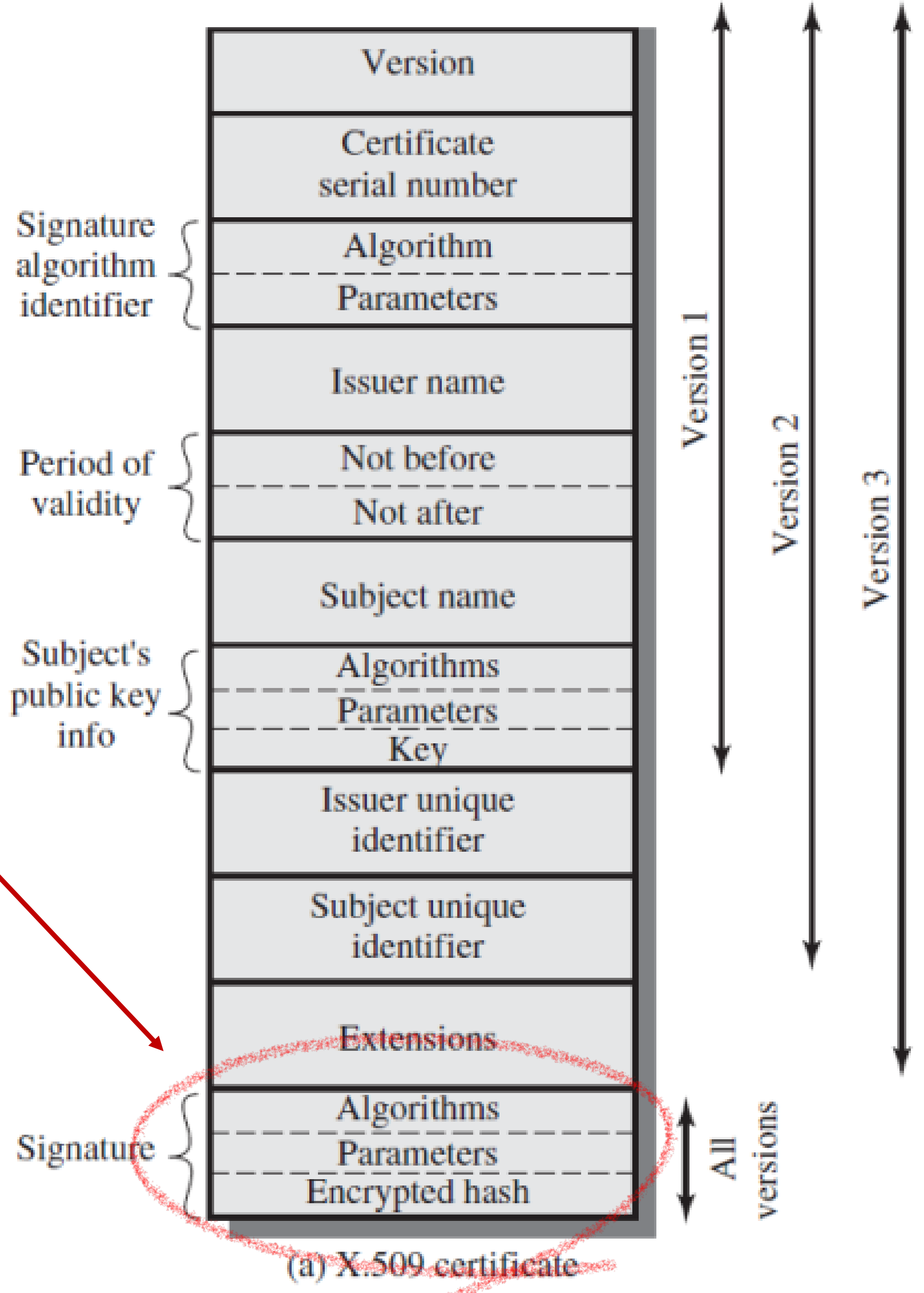
- X.509 is based on hash, asymmetric cryptography and digital signature, but does not mandate a specific protocol or algorithm.

X.509 Certificate Format

- Different versions had different fields.

- But all of them had CA's signature (encrypted hash) at the end.

- In the certificate, the name of the key owner (subject), the public key, and expiry date have been written.

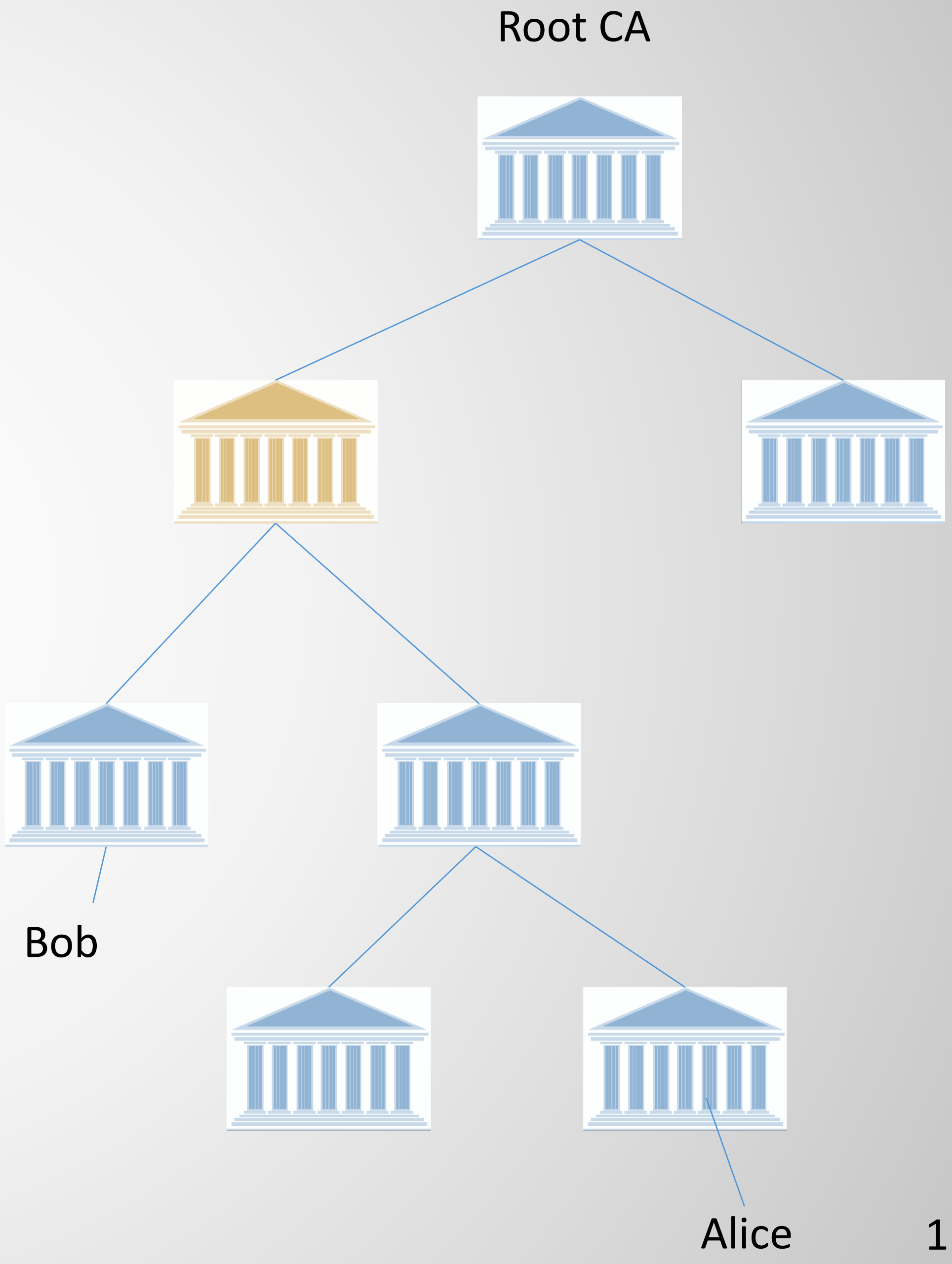


(a) X.509 certificate

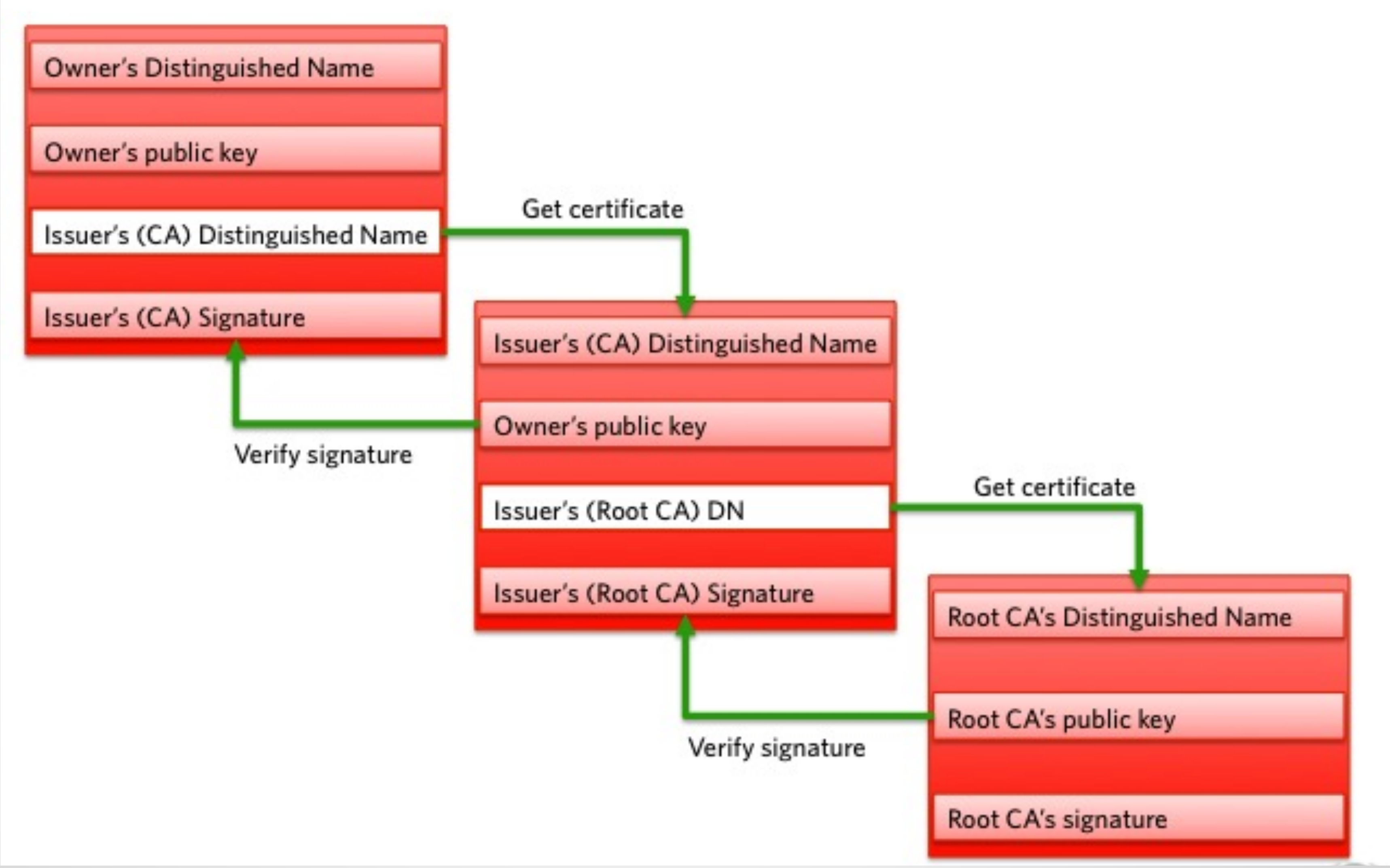
CAs Structure

- In the case of the Internet, CAs are organized in hierarchies. There are some roots, and other CAs are their children or children of children. Every CA signs the public key certificate of its children, including child CA's and normal user's.

- If Alice gives Bob her certificate, Bob sees who has signed it and if he knows its public key to verify the correctness of the signature. If not, he see who has provided certificate for the one who singed Alice's key. This continues until Bob reaches a CA that he knows (i.e. he knows its public key).



Chain of Trust



Owner's Distinguished Name

Owner's public key

Issuer's (CA) Distinguished Name

Issuer's (CA) Signature

Get certificate

Verify signature

Issuer's (CA) Distinguished Name

Owner's public key

Issuer's (Root CA) DN

Issuer's (Root CA) Signature

Get certificate

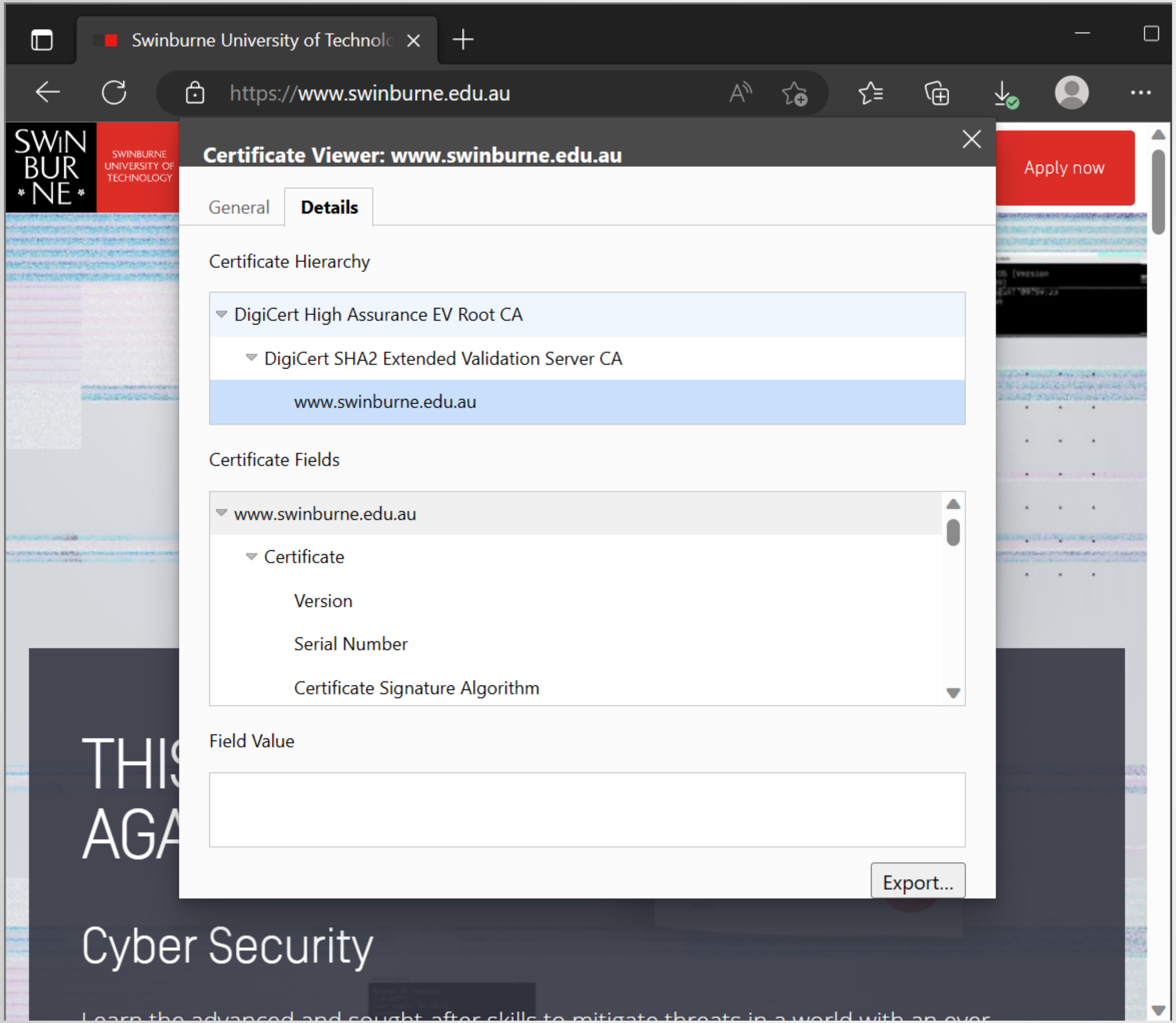
Verify signature

Root CA's Distinguished Name

Root CA's public key

Root CA's signature

Example


Swinburne University of Technolo
https://www.swinburne.edu.au
SWIN BUR NE
SWINBURNE UNIVERSITY OF TECHNOLOGY
Apply now
THIS AGA
Cyber Security
Learn the advanced and sought-after skills to mitigate threats in a world with an ever

Certificate Viewer: www.swinburne.edu.au

General | **Details**

Certificate Hierarchy

- DigiCert High Assurance EV Root CA
  - DigiCert SHA2 Extended Validation Server CA
    - www.swinburne.edu.au

Certificate Fields

- www.swinburne.edu.au
  - Certificate
    - Version
    - Serial Number
    - Certificate Signature Algorithm

Field Value

Export...

Certificate Revocation

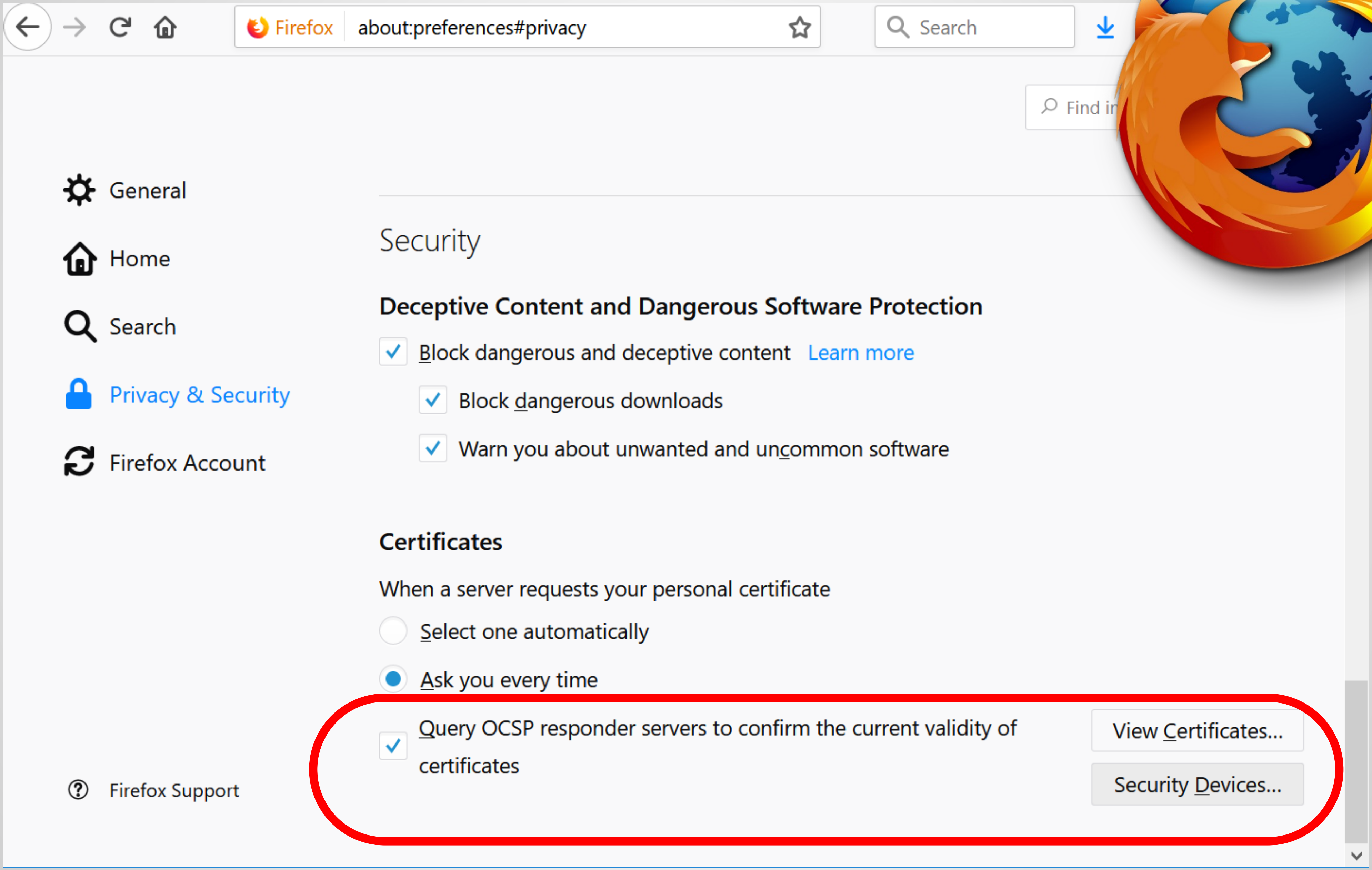
- Private key could be lost, or compromised. In that case, the associated public key certificate must be revoked. Otherwise the person who has obtained the private key can impersonate.

- Each certificate has a serial number. CAs periodically publish a list of serial numbers whose certificates are revoked. Such a list is signed by the issuing CA. The time of next update is also mentioned in the issued list. This list is called CRL (Certificate Revocation List).

OCSP

- The **Online Certificate Status Protocol** (**OCSP**) is also used for obtaining the revocation status of an X.509 certificate. It is described in RFC 6960. It was created as an alternative to CRLs, specifically addressing certain problems associated with using them in a public key infrastructure.

- Messages communicated via OCSP are encoded in ASN.1 and are usually communicated over HTTP. The "request/response" nature of these messages leads to OCSP servers being termed *OCSP responders.*



Security

Deceptive Content and Dangerous Software Protection

☑ Block dangerous and deceptive content Learn more

☑ Block dangerous downloads

☑ Warn you about unwanted and uncommon software

Certificates

When a server requests your personal certificate

○ Select one automatically

● Ask you every time

☑ Query OCSP responder servers to confirm the current validity of certificates

Public Key Infrastructure (PKI)

- RFC 2822 (*Internet Security Glossary*) defines Public-Key Infrastructure (PKI) as the set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates based on asymmetric cryptography.

- The main goal of PKI development was to create a simple yet secure architecture to find authentic public keys over the internet.

Public Key Cryptography in Blockchain

- Sometimes, we do not want to bind user’s identity with his/her public key.
  - This is the case in many blockchains, including Bitcoin.
  - Preserving user anonymity is the main reason behind such a detachment.

- Public key ownerships are proven by digital signatures in blockchains.
  - As we will see, public keys are usually regarded as account numbers.

What Comes Next …

- We learned about public key management and PKI.
- We learned how certificates are generated and verified.
- In the next video, we explain the concept of zero knowledge.

See you in the next video …