Public Key Infrastructure (PKI)

Key Authentication

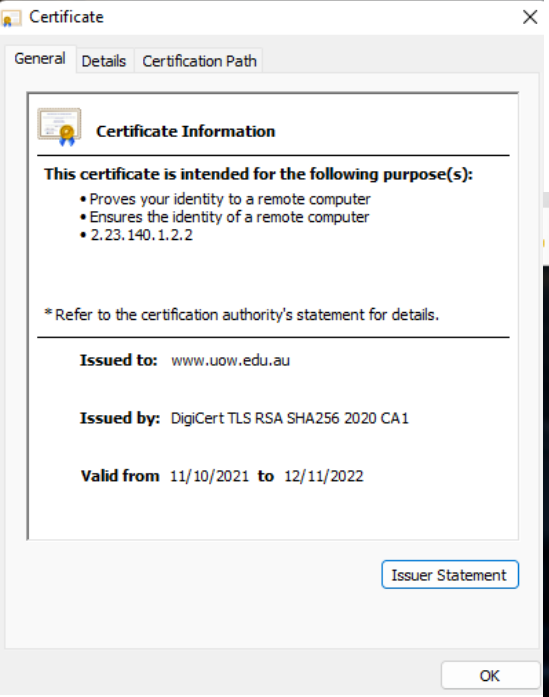
- Public Key Distribution:
  - How do you trust the source of the PK?
  - Potential for attacks
- Certification Authorities (CAs)
  - Keys are signed by the state, the corporation or someone you trust.
- Distribution of Trust
  - Your trust in a key is replaced by trust in a body, the CA

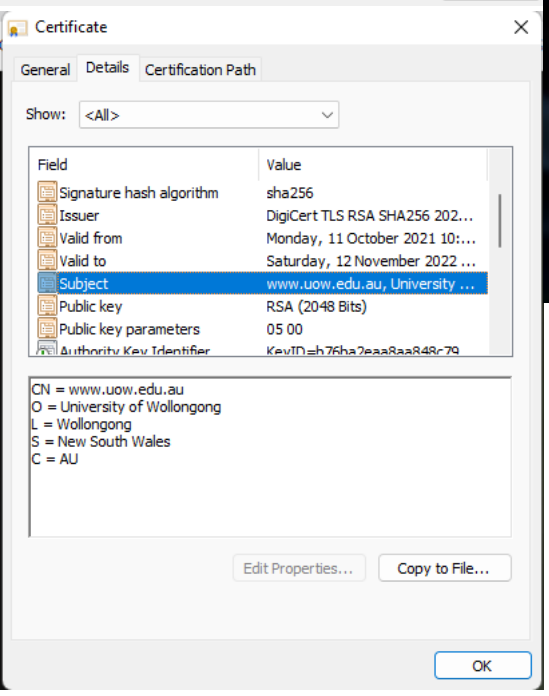
Certification Authorities

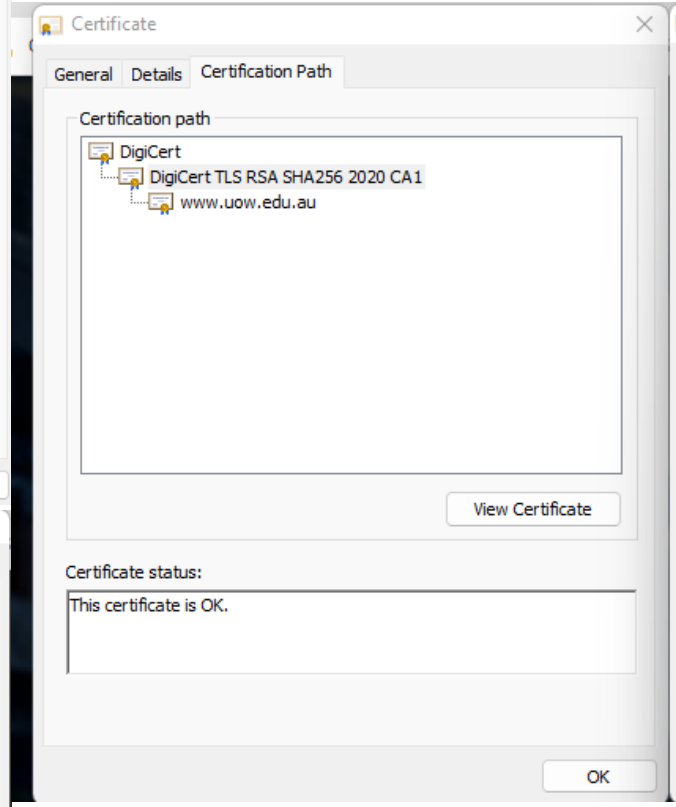
- With all public key schemes (for encryption or signature), we have the problem of distributing PK so the recipient knows it is valid.
- Solution: *All choose a CA and get a copy of the CA's public signature verification key by some trusted means.*
- Note: All users **must** trust the CA

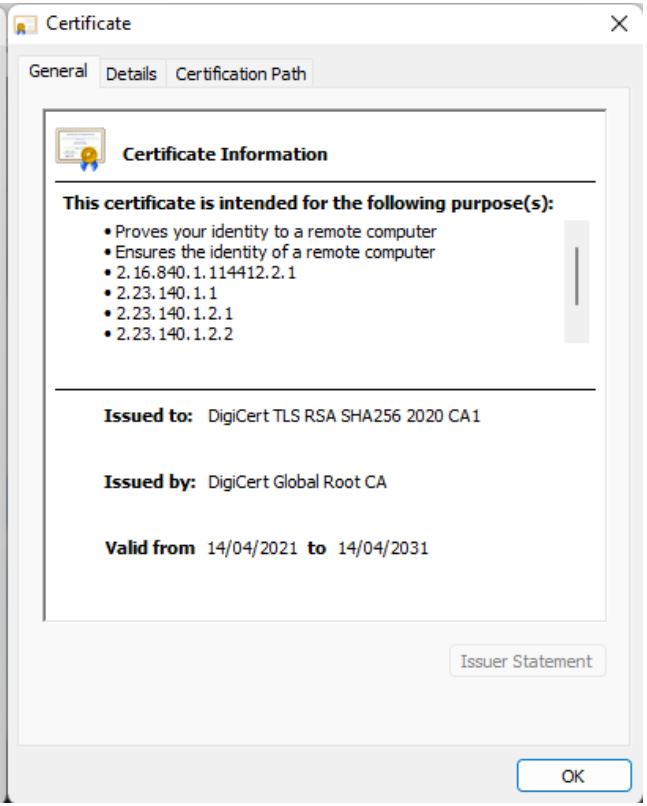
Certificates

- Every user submits their PK to the CA. The CA concatenates: *user name, user PK, expiry date, etc.* and generates a signature on this data string.
- The combination of data string and signature is called a *Public Key Certificate*. This is sent back to user.
- Anyone with CA's PK can verify the users' PK certificate and so obtain a trusted copy of the users' PK.


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Proves your identity to a remote computer
• Ensures the identity of a remote computer
• 2.23.140.1.2.2
* Refer to the certification authority's statement for details.
Issued to: www.uow.edu.au
Issued by: DigiCert TLS RSA SHA256 2020 CA1
Valid from 11/10/2021 to 12/11/2022
Issuer Statement
OK


Certificate
General
Details
Certification Path
Show: <All>
Field
Value
Signature hash algorithm
sha256
Issuer
DigiCert TLS RSA SHA256 202...
Valid from
Monday, 11 October 2021 10:...
Valid to
Saturday, 12 November 2022 ...
Subject
www.uow.edu.au, University ...
Public key
RSA (2048 Bits)
Public key parameters
05 00
CN = www.uow.edu.au
O = University of Wollongong
L = Wollongong
S = New South Wales
C = AU
Edit Properties...
Copy to File...
OK


Certificate
General
Details
Certification Path
Certification path
DigiCert
DigiCert TLS RSA SHA256 2020 CA1
www.uow.edu.au
View Certificate
Certificate status:
This certificate is OK.
OK


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Proves your identity to a remote computer
• Ensures the identity of a remote computer
• 2.16.840.1.114412.2.1
• 2.23.140.1.1
• 2.23.140.1.2.1
• 2.23.140.1.2.2
Issued to: DigiCert TLS RSA SHA256 2020 CA1
Issued by: DigiCert Global Root CA
Valid from 14/04/2021 to 14/04/2031
Issuer Statement
OK

Cross-Certification

- If more than one CA exist, then a user may not have a trusted copy of the CA's PK needed to verify another user's certificate.
- This is solved by *cross-certificate*, I.e. one CA's PK is signed by another CA.
- The user first verifies the appropriate cross-certificate, and then verifies the user certificate itself.

Example

- Alice trusts CA1.
  - She obtains Bob's PK which is signed by the SK of CA2.
  - She obtains CA2's PK which is signed by the SK of CA1.
- Hence, she trusts Bob's PK.

Registration & RA's

- When a user wishes to be issued with a certificate the identity of the user needs to be established.
- This is the role of the registration authority (RA), which can be co-implemented with the CA.
- User must also prove he/she knows the SK corresponding to the PK being certified and that the key was generated "correctly".

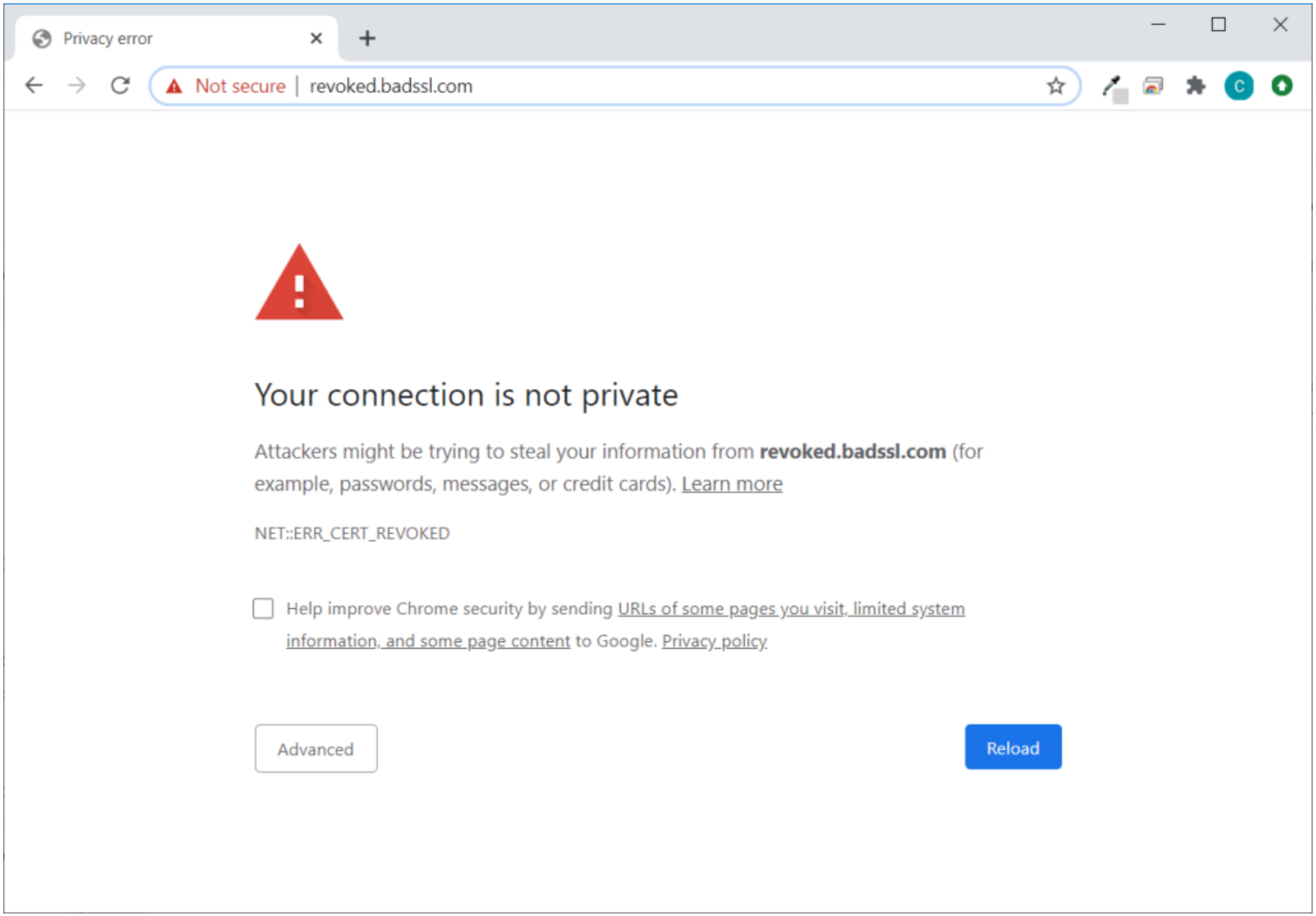
Revocation

- If a user's PK is compromised, i.e. a third party has gained knowledge of the SK then the corresponding PK must be *revoked*.
- The CA must somehow inform all users that the certificate(s) containing this PK is/are no longer valid.
- This is called *certificate revocation*.

Certificate Revocation List (CRL)

- A CRL is a way of telling users about revoked certificates.
- A CRL is a list of the serial numbers of all the certificates revoked by a particular CA, signed by the CA concerned.
- Users must ensure that they have the latest CRL.
- A CRL is a bit like the list of bad credit card numbers which used to be kept next to the tellers in supermarkets.

https://www.entrust.net/customer/crlchecker



https://securityboulevard.com/2020/07/crl-explained-what-is-a-certificate-revocation-list/

What's in a PKI?

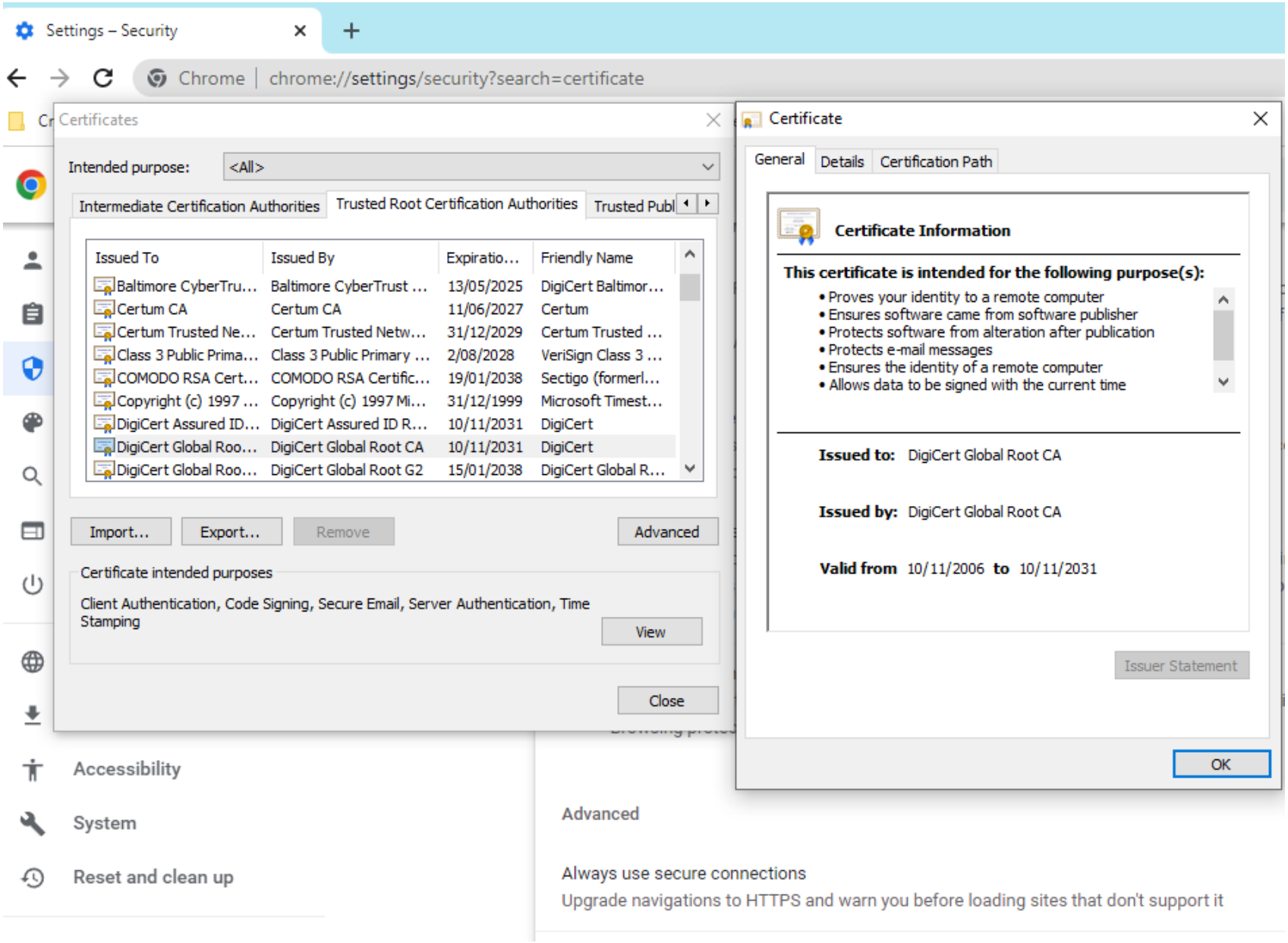
- Public-key cryptography.
- Certification authorities.
- Digital certificates.
- Registration authorities.
- …

More generally, PKI's may contain a combination of personnel, policies, protocols, hardware, software, PK cryptography tools, and services to provide security for communications over an insecure network, such as the Internet. Different PKI's exist for different application domains.

Certificate Access

- PK certificates will typically be stored in repositories and accessed as required.
- Certificate repositories may be separated from the CA which generates them.
- The certificates DO NOT need to be stored securely.

Certificate Repositories in Chrome



Trusted Third Party (TTP)

- CA's and RA's are examples of third parties who users must trust in some way.
- Such entities are generically referred to as trusted third parties (TTP's).
  - TTP's may even know the user secret key in some network systems

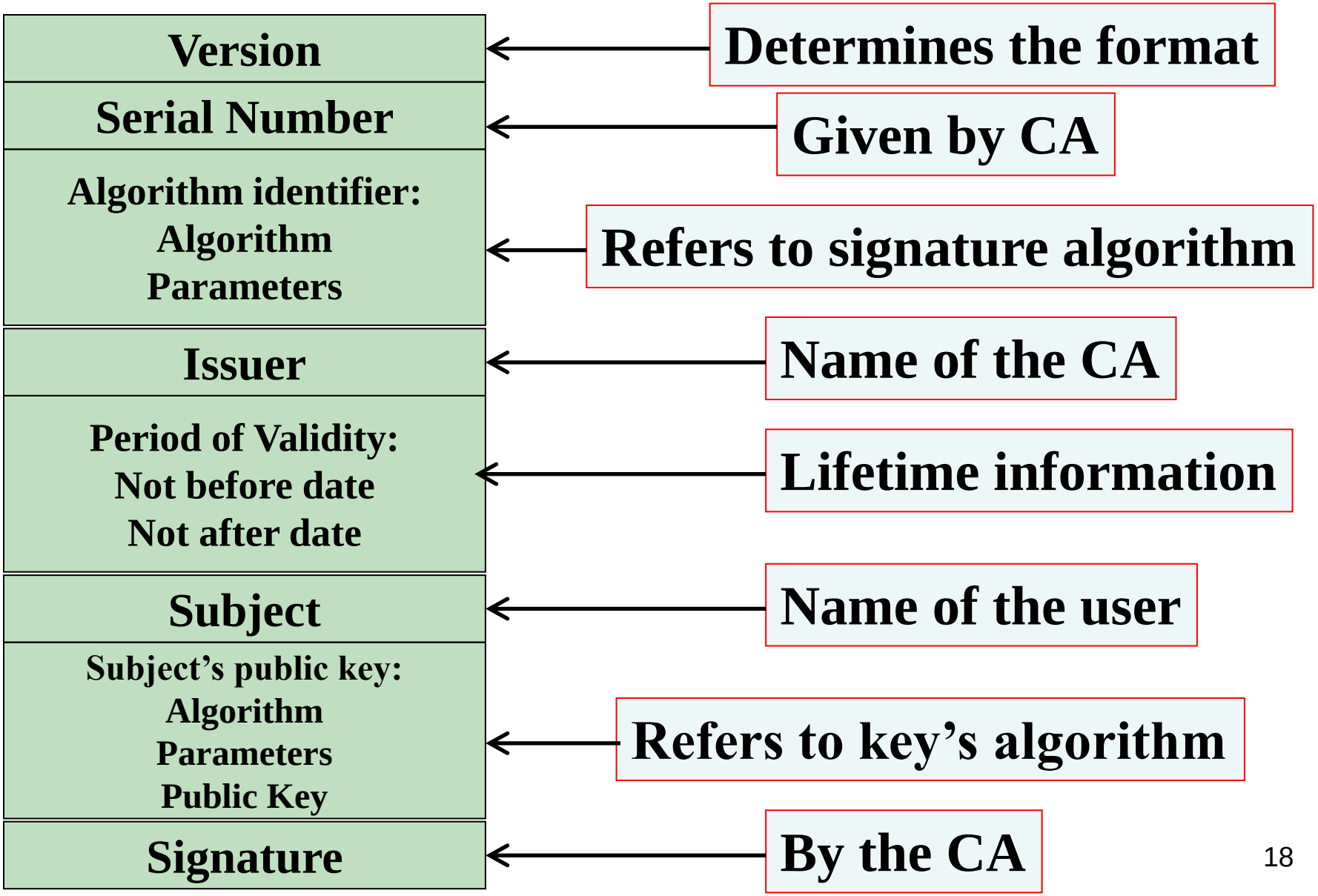
PKI Examples

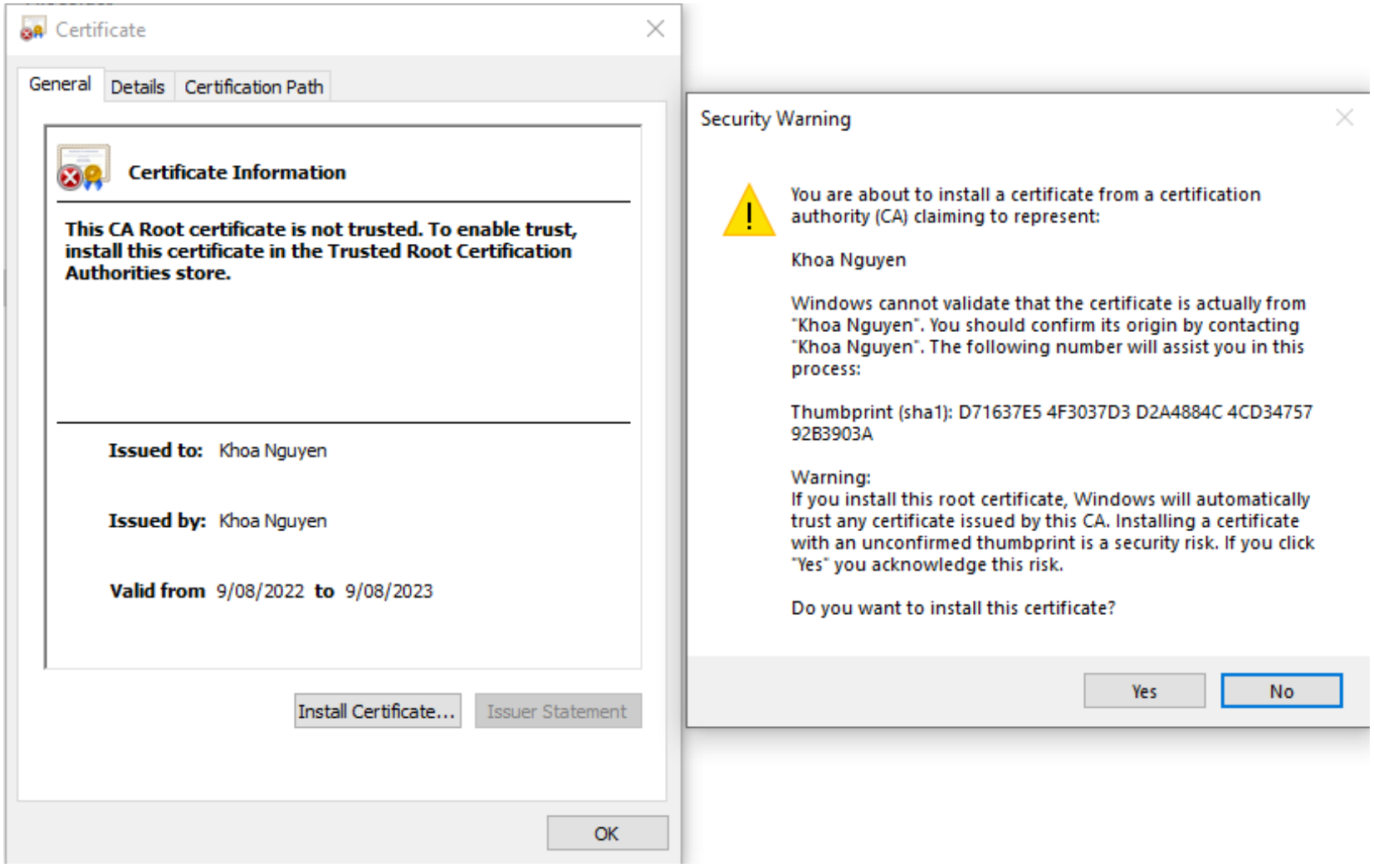
- X.509/PKIX
- PGP (Web of Trust)

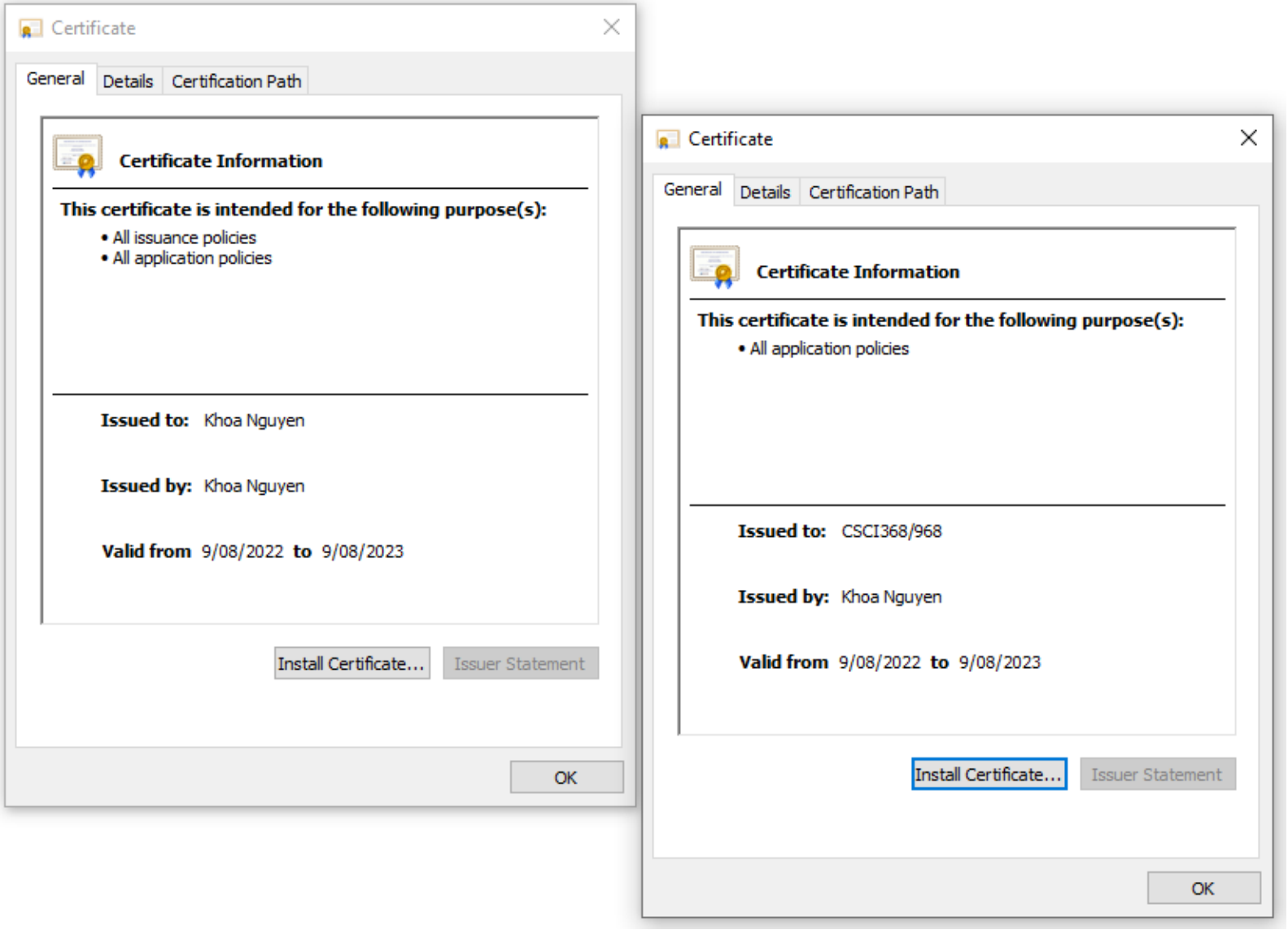
X.509

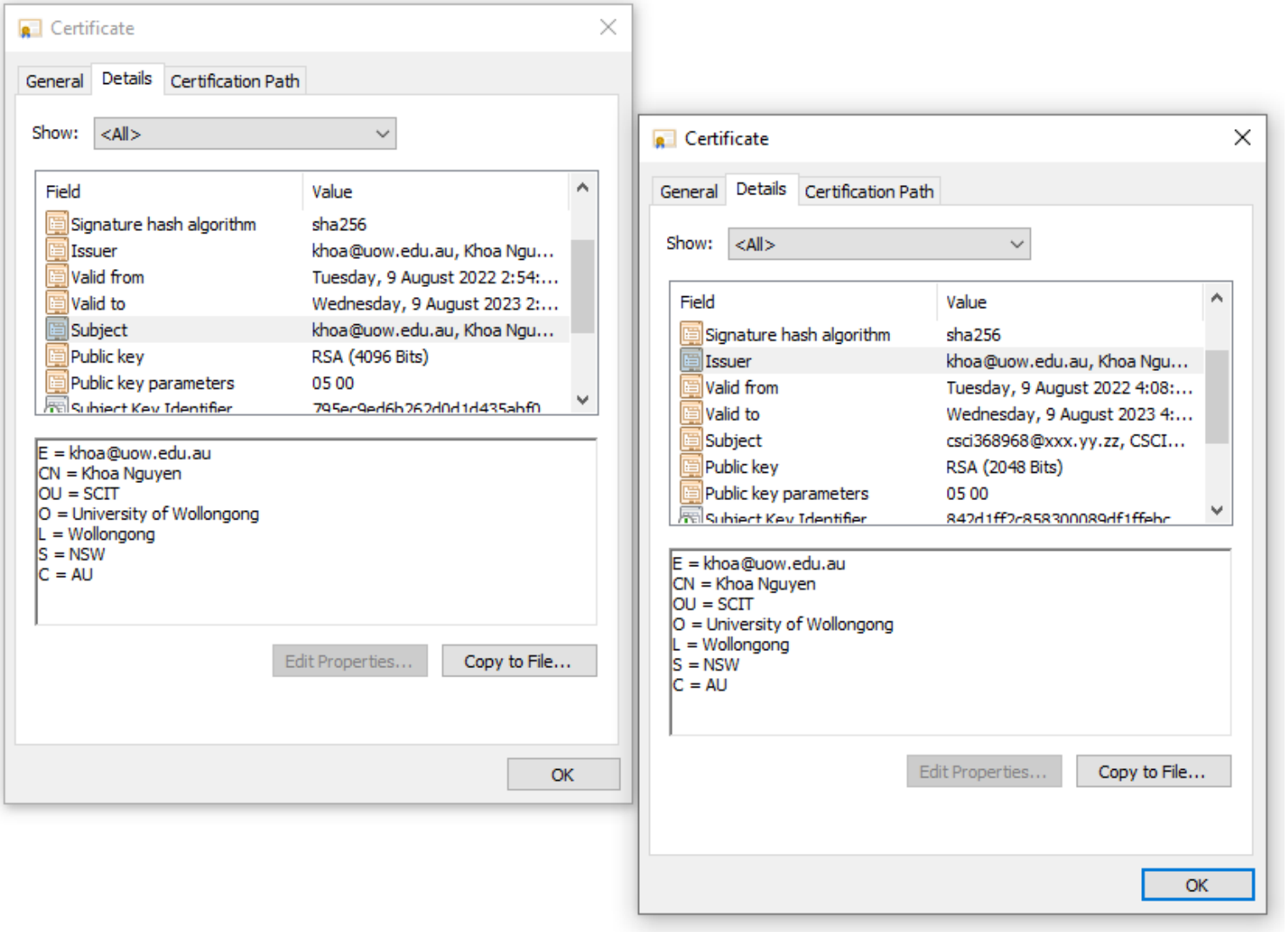
- X.509 defines a structure for PK Certificates.
- A CA assigns a unique name to each user and issues a signed certificate, often name is the URL or email address.
- CA’s are connected in a tree structure. Each CA issues a certificate for those beneath it.

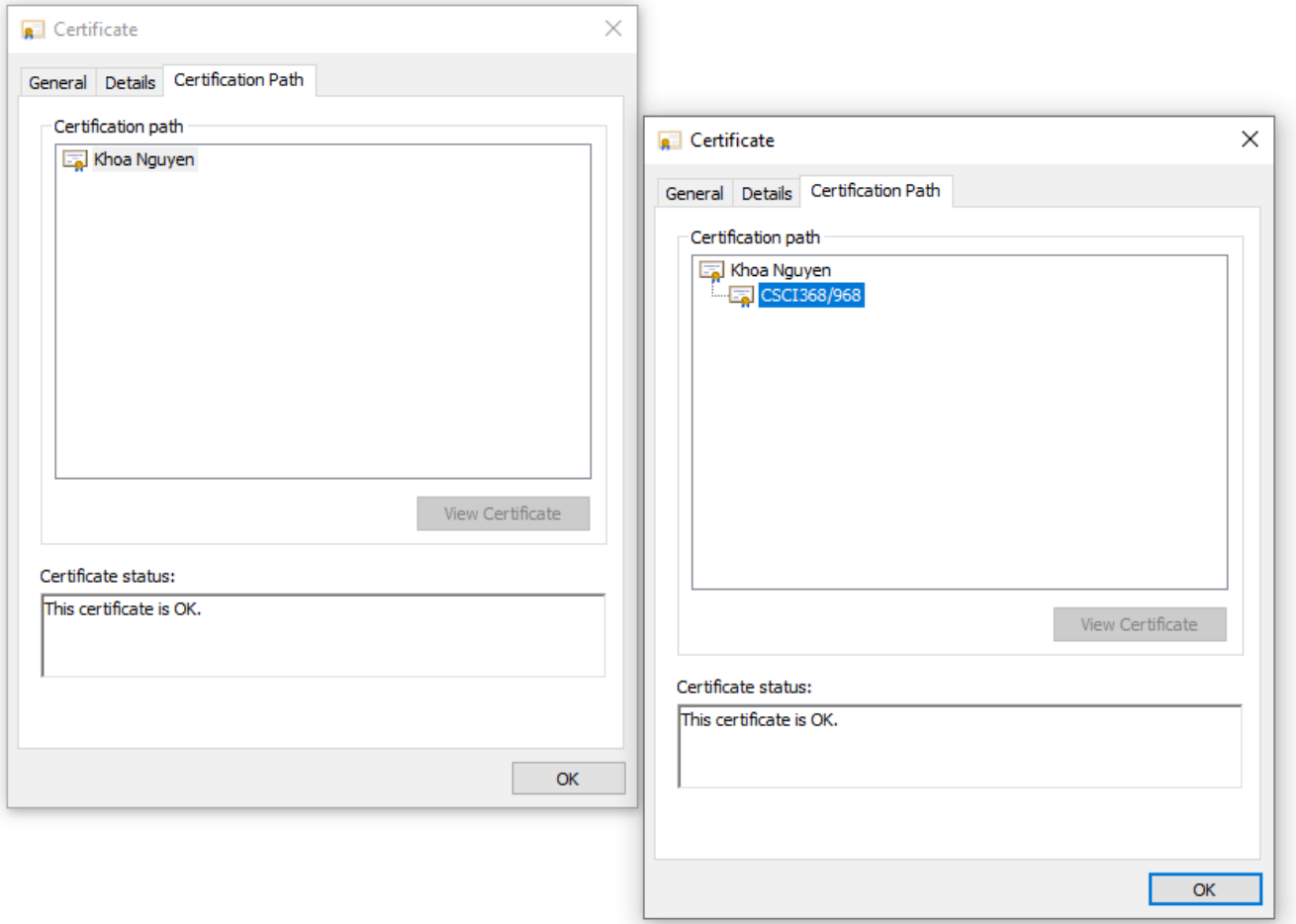
X.509 Certificate Structures




Certificate
General
Details
Certification Path
Certificate Information
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.
Issued to: Khoa Nguyen
Issued by: Khoa Nguyen
Valid from 9/08/2022 to 9/08/2023
Install Certificate...
Issuer Statement
OK
Security Warning
You are about to install a certificate from a certification authority (CA) claiming to represent:
Khoa Nguyen
Windows cannot validate that the certificate is actually from "Khoa Nguyen". You should confirm its origin by contacting "Khoa Nguyen". The following number will assist you in this process:
Thumbprint (sha1): D71637E5 4F3037D3 D2A4884C 4CD34757 92B3903A
Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.
Do you want to install this certificate?
Yes
No


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• All issuance policies
• All application policies
Issued to: Khoa Nguyen
Issued by: Khoa Nguyen
Valid from 9/08/2022 to 9/08/2023
Install Certificate...
Issuer Statement
OK
Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• All application policies
Issued to: CSCI368/968
Issued by: Khoa Nguyen
Valid from 9/08/2022 to 9/08/2023
Install Certificate...
Issuer Statement
OK


Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Signature hash algorithm
sha256
Issuer
khoa@uow.edu.au, Khoa Ngu...
Valid from
Tuesday, 9 August 2022 2:54:...
Valid to
Wednesday, 9 August 2023 2:...
Subject
khoa@uow.edu.au, Khoa Ngu...
Public key
RSA (4096 Bits)
Public key parameters
05 00
E = khoa@uow.edu.au
CN = Khoa Nguyen
OU = SCIT
O = University of Wollongong
L = Wollongong
S = NSW
C = AU
Edit Properties...
Copy to File...
OK
Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Signature hash algorithm
sha256
Issuer
khoa@uow.edu.au, Khoa Ngu...
Valid from
Tuesday, 9 August 2022 4:08:...
Valid to
Wednesday, 9 August 2023 4:...
Subject
csci368968@xxx.yy.zz, CSCI...
Public key
RSA (2048 Bits)
Public key parameters
05 00
E = khoa@uow.edu.au
CN = Khoa Nguyen
OU = SCIT
O = University of Wollongong
L = Wollongong
S = NSW
C = AU
Edit Properties...
Copy to File...
OK


Certificate
General
Details
Certification Path
Certification path
Khoa Nguyen
View Certificate
Certificate status:
This certificate is OK.
OK
Certificate
General
Details
Certification Path
Certification path
Khoa Nguyen
CSCI368/968
View Certificate
Certificate status:
This certificate is OK.
OK

PKI Trust Models

- Monopoly Model
- Oligarchy
- Delegated CA’s
- Anarchy

Monopoly Model

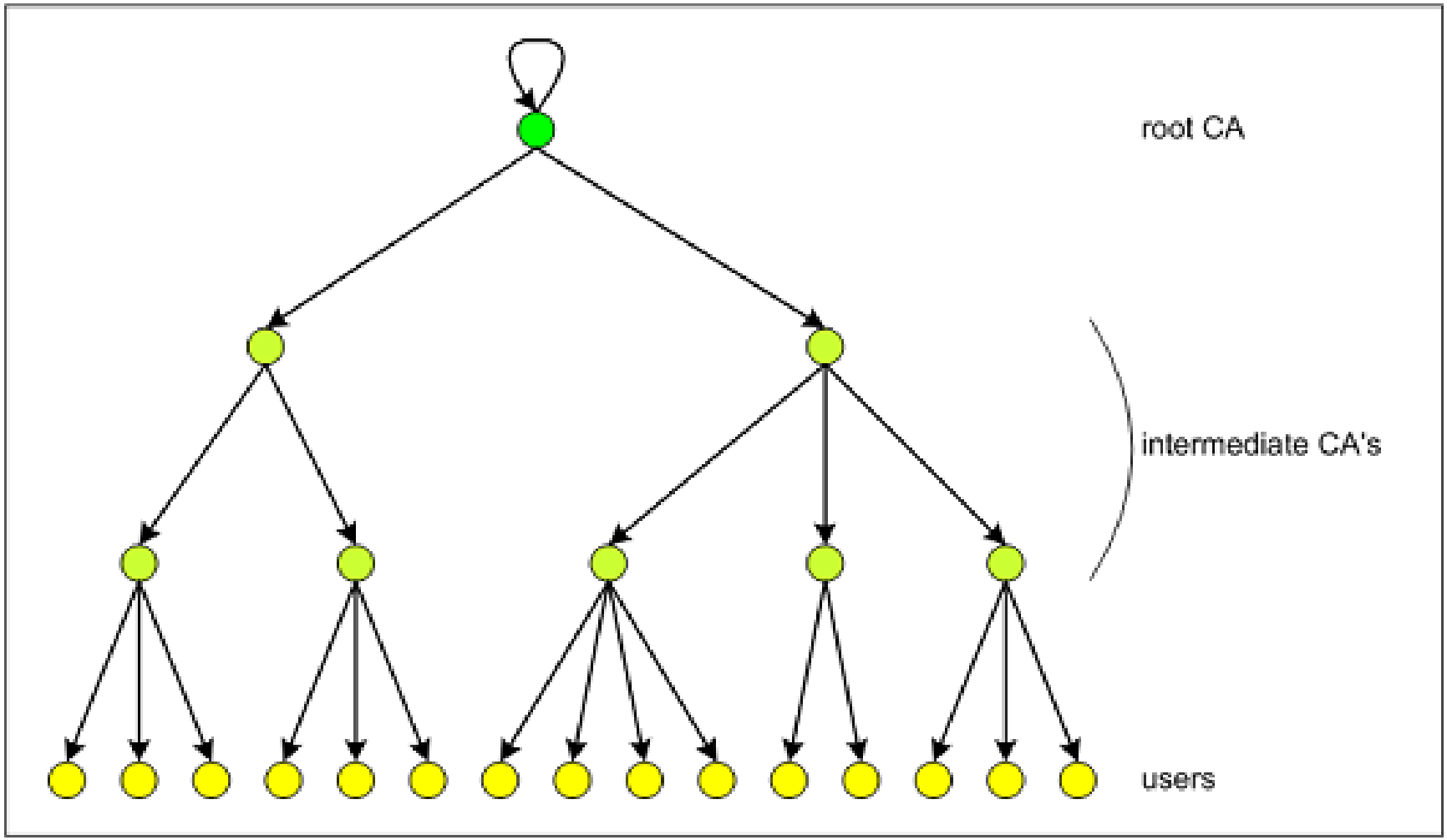
- There is only one universally trusted CA.
- Very hard in practice.

Oligarchy

- Commonly used in browsers.
- Products come configured with many trust anchors, and a certificate issued by any one of them is accepted.

Delegated CA's

- CA can issue certificates to other CA's vouching for their PK's and vouching for their trustworthiness as CA's.
- Users can then obtain certificates from one of the delegated CA's instead of having to go to the *trust anchor* CA.
- There is a *chain of certificate* that is visible to user in this model.


root CA
intermediate CA's
users

Anarchy

- No centralised CA
- Used by PGP.
- Each user is responsible for configuring some trust anchors, eg. PK’s of people he has met and who have handed him a business card with a PGP fingerprint (the message digest of the PK).