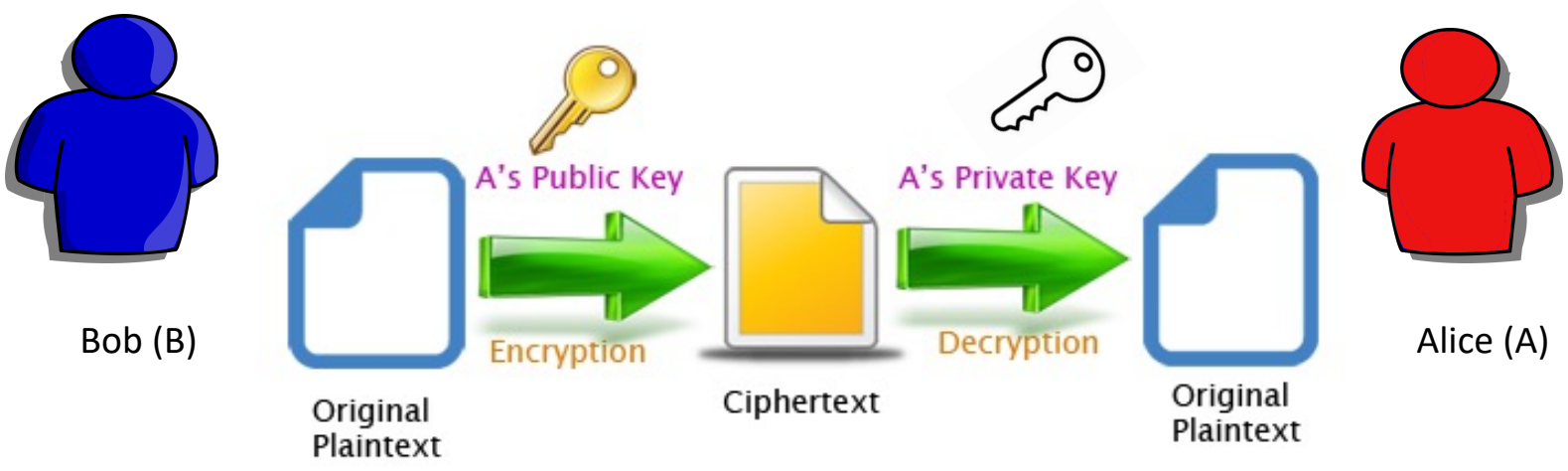
Public-Key Infrastructure



Question

How to confirm the correct public key

Matching Identity with Public Key

- Bind an identity with a key.

Matching Identity with Public Key

- Bind an identity with a key.
- Could we self-sign? Alice signs their own public key with their own signing key.

Matching Identity with Public Key

- Bind an identity with a key.
- Could we self-sign? Alice signs their own public key with their own signing key.
- Problem remains, Adversary could do the same. Question is: How to verify, it is Alice themselves who generated and signed the key.

Matching Identity with Public Key

- Bind an identity with a key.
- Could we self-sign? Alice signs their own public key with their own signing key.
- Problem remains, Adversary could do the same. Question is: How to verify, it is Alice themselves who generated and signed the key.
- Kohnfelder,1978: Use a *certificate*

Certificates

- A statement containing
  - Identity (e.g. University of Birmingham)
  - Public Key
  - Timestamp
  - Other Informations.
- Authentication of Certificate: Signed by a certifying authority (eg.GEANT, Google CA)

Communication using Certificate

- Suppose our browser is Bob and University of Birmingham weberver be Alice.
- Bob obtains Alice's certificate.
- If Bob knows GEANT's (Certifying Authority) public key then verify the signature.
- Now Bob has Alice's Public Key.

Communication using Certificate

- If Bob does not know CA's public key
  - Repeat the process for CA's public key.

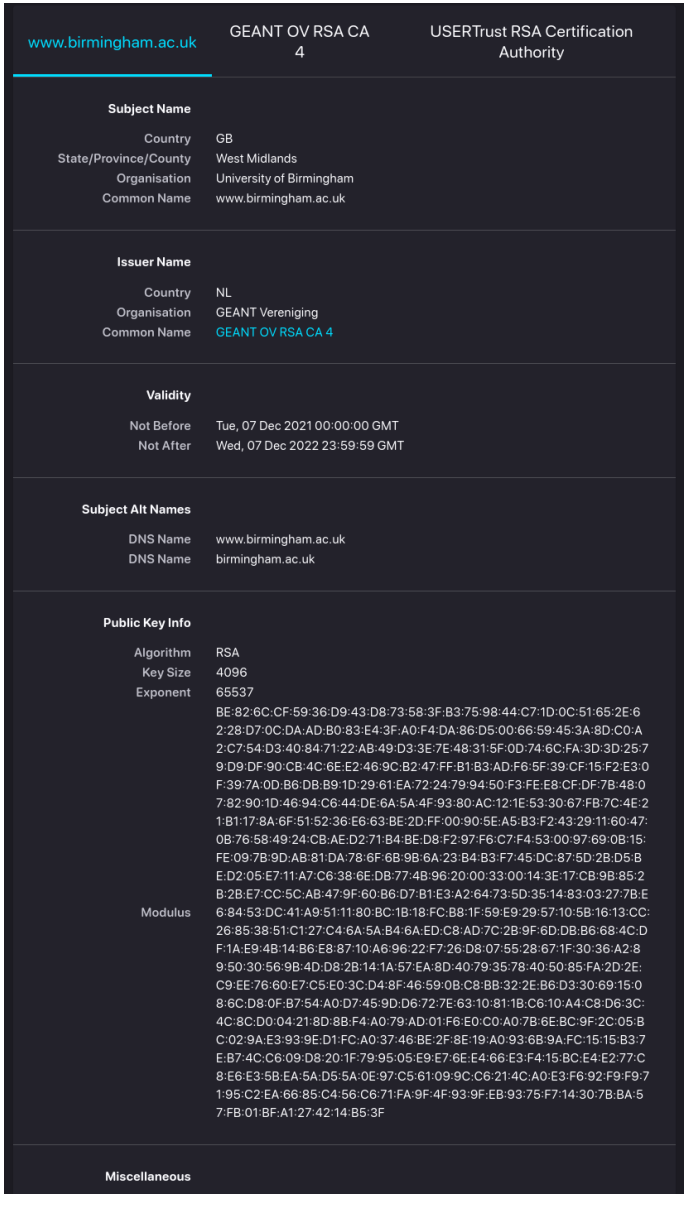
Communication using Certificate

- If Bob does not know CA's public key
  - Repeat the process for CA's public key.
  - How long should we go?

Communication using Certificate

- If Bob does not know CA's public key
  - Repeat the process for CA's public key.
  - How long should we go?
  - Create certificate signature chains (tree like hierarchy) with public key of the root hard coded in browser. (X.509 certificate signature chains)

X.509 certificate



www.birmingham.ac.uk | GEANT OV RSA CA 4 | USERTrust RSA Certification Authority

Subject Name

Country	GB
State/Province/County	West Midlands
Organisation	University of Birmingham
Common Name	www.birmingham.ac.uk

Issuer Name

Country	NL
Organisation	GEANT Vereniging
Common Name	GEANT OV RSA CA 4

Validity

Not Before	Tue, 07 Dec 2021 00:00:00 GMT
Not After	Wed, 07 Dec 2022 23:59:59 GMT

Subject Alt Names

DNS Name	www.birmingham.ac.uk
DNS Name	birmingham.ac.uk

Public Key Info

Algorithm	RSA
Key Size	4096
Exponent	65537
Modulus	BE:82:6C:CF:59:36:D9:43:D8:73:58:3F:B3:75:98:44:C7:1D:0C:51:65:2E:62:28:D7:0C:DA:AD:B0:83:E4:3F:A0:F4:DA:86:D5:00:66:59:45:3A:8D:C0:A2:C7:54:D3:40:84:71:22:AB:49:D3:3E:7E:48:31:5F:0D:74:6C:FA:3D:3D:25:79:D9:DF:90:CB:4C:6E:E2:46:9C:B2:47:FF:B1:B3:AD:F6:5F:39:CF:15:F2:E3:0F:39:7A:0D:B6:DB:B9:1D:29:61:EA:72:24:79:94:50:F3:FE:E8:CF:DF:7B:48:07:82:90:1D:46:94:C6:44:DE:6A:5A:4F:93:80:AC:12:1E:53:30:67:FB:7C:4E:21:B1:17:8A:6F:51:52:36:E6:63:BE:2D:FF:00:90:5E:A5:B3:F2:43:29:11:60:47:0B:76:58:49:24:CB:AE:D2:71:B4:BE:D8:F2:97:F6:C7:F4:53:00:97:69:0B:15:FE:09:7B:9D:AB:81:DA:78:6F:6B:9B:6A:23:B4:B3:F7:45:DC:87:5D:2B:D5:BE:D2:05:E7:11:A7:C6:38:6E:DB:77:4B:96:20:00:33:00:14:3E:17:CB:9B:85:2B:2B:E7:CC:5C:AB:47:9F:60:B6:D7:B1:E3:A2:64:73:5D:35:14:83:03:27:7B:E6:84:53:DC:41:A9:51:11:80:BC:1B:18:FC:B8:1F:59:E9:29:57:10:5B:16:13:CC:26:85:38:51:C1:27:C4:6A:5A:B4:6A:ED:C8:AD:7C:2B:9F:6D:DB:B6:68:4C:DF:1A:E9:4B:14:B6:E8:87:10:A6:96:22:F7:26:D8:07:55:28:67:1F:30:36:A2:89:50:30:56:9B:4D:D8:2B:14:1A:57:EA:8D:40:79:35:78:40:50:85:FA:2D:2E:C9:EE:76:60:E7:C5:E0:3C:D4:8F:46:59:0B:C8:BB:32:2E:B6:D3:30:69:15:08:6C:D8:0F:B7:54:A0:D7:45:9D:D6:72:7E:63:10:81:1B:C6:10:A4:C8:D6:3C:4C:8C:D0:04:21:8D:8B:F4:A0:79:AD:01:F6:E0:C0:A0:7B:6E:BC:9F:2C:05:BC:02:9A:E3:93:9E:D1:FC:A0:37:46:BE:2F:8E:19:A0:93:6B:9A:FC:15:15:B3:7E:B7:4C:C6:09:D8:20:1F:79:95:05:E9:E7:6E:E4:66:E3:F4:15:BC:E4:E2:77:C8:E6:E3:5B:EA:5A:D5:5A:0E:97:C5:61:09:9C:C6:21:4C:A0:E3:F6:92:F9:F9:71:95:C2:EA:66:85:C4:56:C6:71:FA:9F:4F:93:9F:EB:93:75:F7:14:30:7B:BA:57:FB:01:BF:A1:27:42:14:B5:3F

Miscellaneous

Serial Number	4E:BC:E2:46:48:00:43:8E:1B:7E:ED:63:92:0D:76:82
Signature Algorithm	SHA-384 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)

Fingerprints

SHA-256	FB:B0:FC:2A:29:AD:27:1D:3F:B7:94:DA:12:BC:AA:D8:88:94:BA:FC:7A:CC:...
SHA-1	45:D4:37:C7:47:01:6E:B1:BA:C3:1F:29:AF:F2:38:6E:F7:11:4B:58

Basic Constraints

Certificate Authority	No

Key Usages

Purposes	Digital Signature, Key Encipherment

Extended Key Usages

Purposes	Server Authentication, Client Authentication

Subject Key ID

Key ID	EC:FB:41:87:39:7F:DE:6D:79:EF:FD:61:71:AC:6F:F9:90:3F:97:F6

Authority Key ID

Key ID	6F:1D:35:49:10:6C:32:FA:59:A0:9E:BC:8A:E8:1F:95:BE:71:7A:0C

CRL Endpoints

Distribution Point	http://GEANT.crl.sectigo.com/GEANTOVRSACA4.crl

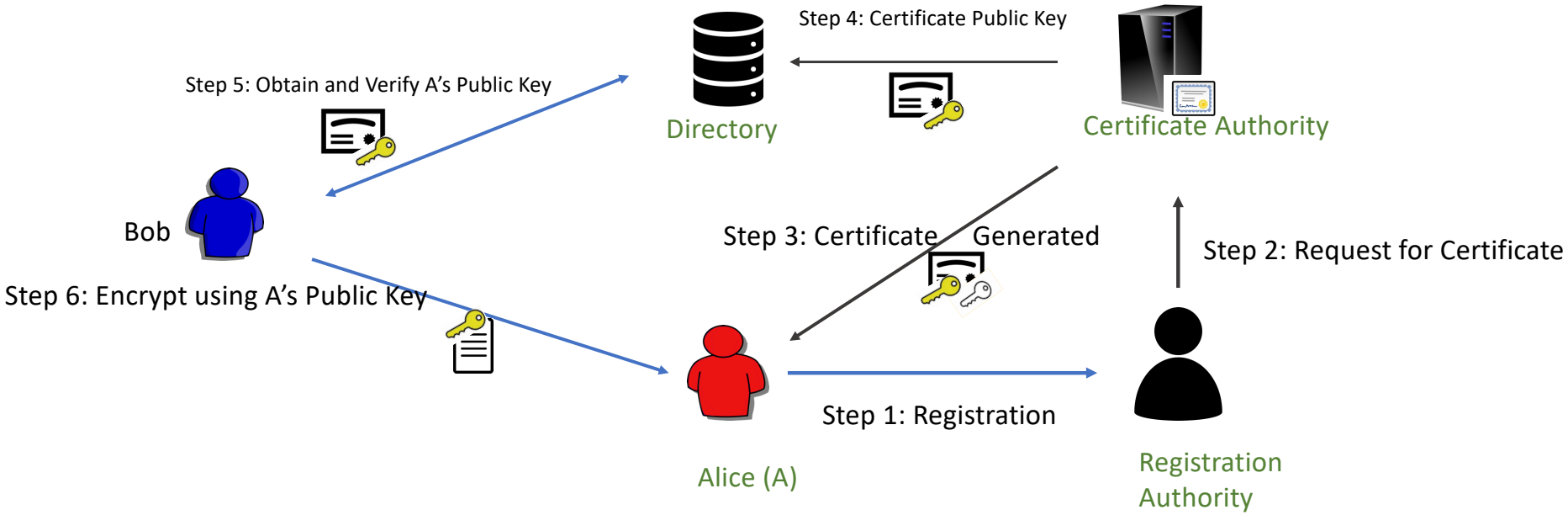
Authority Info (AIA)

Location	http://GEANT.crt.sectigo.com/GEANTOVRSACA4.crt
Method	CA Issuers
Location	http://GEANT.ocsp.sectigo.com
Method	Online Certificate Status Protocol (OCSP)

Certificate Policies

Policy	Statement Identifier (1.3.6.1.4.1)
Value	1.3.6.1.4.1.6449.1.2.2.79
Qualifier	Practices Statement (1.3.6.1.5.5.7.2.1)
Value	https://sectigo.com/CPS
Policy	Certificate Type (2.23.140.1.2.2)
Value	Organization Validation

Public Key Infrastructure



Revoked Certificates

- CA may revoke certificates.
  - Certificate Expiration (Very Common)
  - Compromised Private key
  - User Details changed.

Key Recovery and Key Escrow

- Unaccessible keys can be recovered in principle (from Key Recovery Server).
- Human Entity (Key Recovery Agent); often more than one is required.
- Copies of private key is often kept in a key archival system too.
- Requested by law enforcement with proper court order.