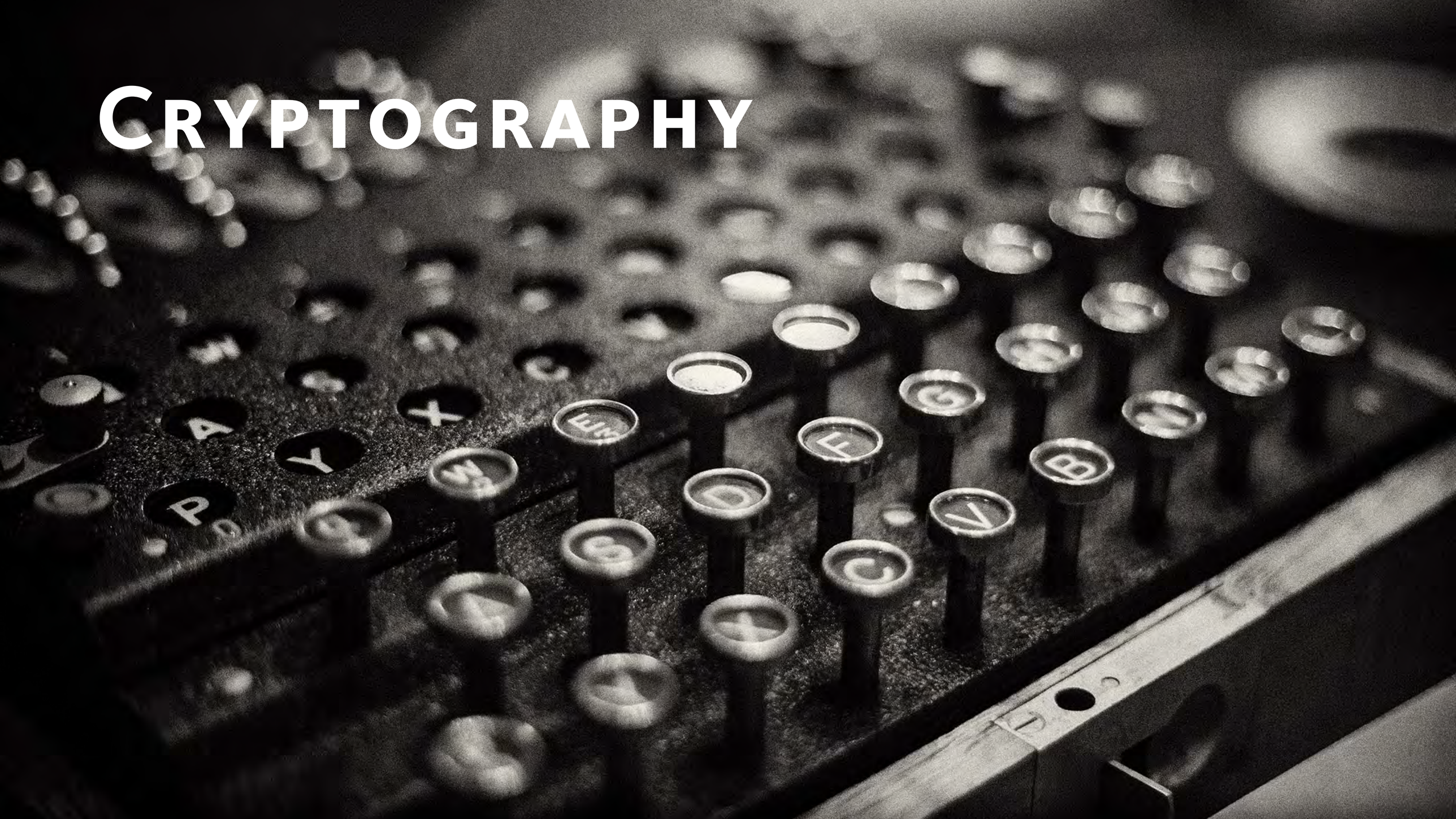

MAC · SYS · ADMIN
GOTHENBURG · 2016 ·


UNIVERSITY OF · OXFORD ·
DOMI NVS ILLV
MINA TIO MEA
UNIVERSITY OF
OXFORD

Certificates

How do they work?

Cryptography



Symmetric Keys

UNIVERSITY OF OXFORD

Bob

Alice

Symmetric Keys

UNIVERSITY OF OXFORD

Bob

Alice

Symmetric Keys

UNIVERSITY OF OXFORD

Bob

E

Symmetric Keys

UNIVERSITY OF OXFORD

Bob

Alice

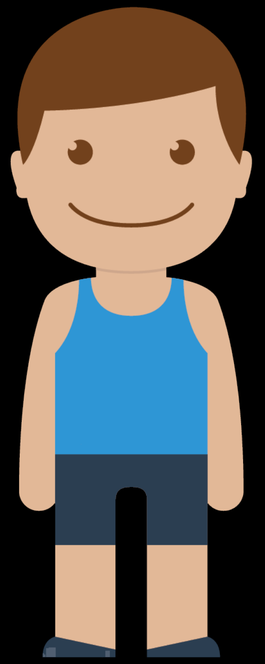
Secure Key Exchange

UNIVERSITY OF OXFORD

- Meet in person for secure key exchange
  - Impractical for many people / large groups
  - Often impossible
- Secure cryptographic key exchange over a public channel
  - Extra complexity and overheads
  - Example: Diffie–Helman key exchange

Public Key Cryptography – Idea

UNIVERSITY OF OXFORD

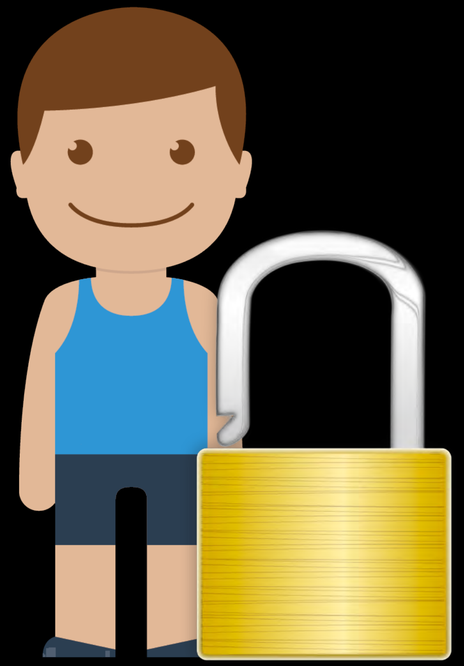


Bob

1.Lock: encryption key
Key: decryption key

Alice

Public Key Cryptography – Idea



Bob

1. Lock: encryption key
   Key: decryption key
2. Encryption key may be shared in public
   as it can only perform a one-way function

Alice

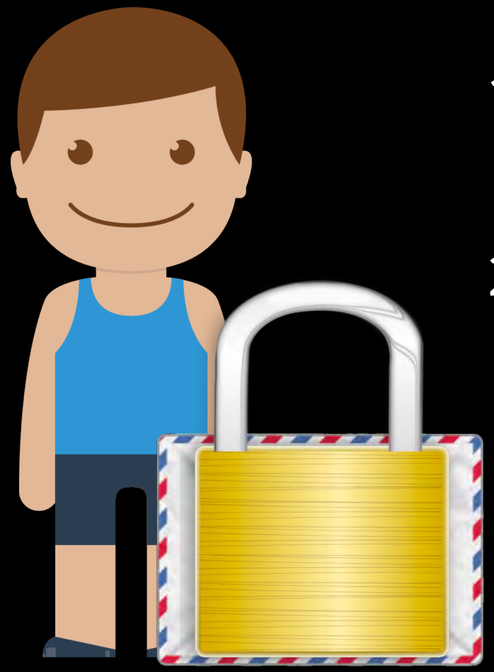
Public Key Cryptography – Idea

Bob

1. Lock: encryption key
   Key: decryption key
2. Encryption key may be shared in public
   as it can only perform a one-way function

Alice

Public Key Cryptography – Idea



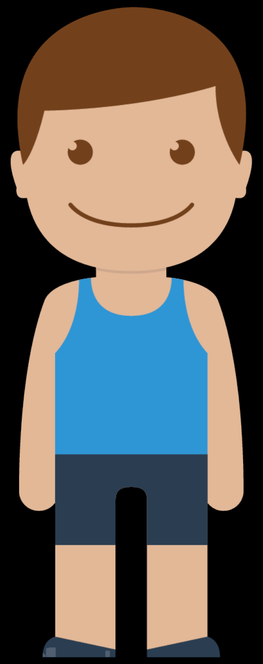
Bob

1. Lock: encryption key
   Key: decryption key
2. Encryption key may be shared in public
   as it can only perform a one-way function

Alice

Public Key Cryptography – Idea

UNIVERSITY OF OXFORD

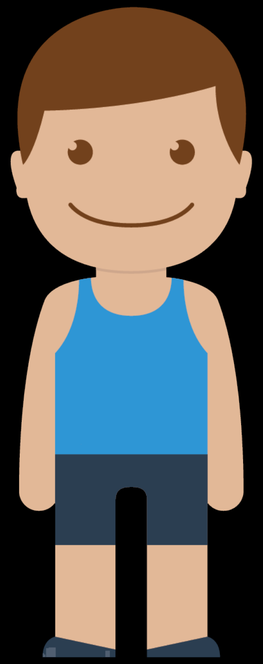


Bob

1. Lock: encryption key
   Key: decryption key
2. Encryption key may be shared in public
   as it can only perform a one-way function

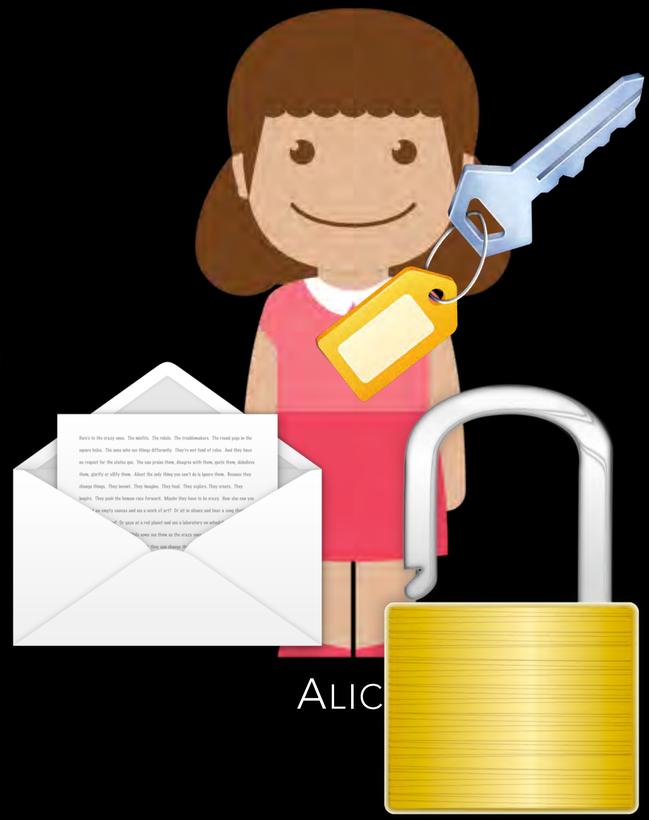
Alice

Public Key Cryptography – Idea



Bob

1. Lock: encryption key
   Key: decryption key
2. Encryption key may be shared in public
   as it can only perform a one-way function
3. Decryption key performs the inverse
   (or undo) operation which was applied
   by the encryption key.



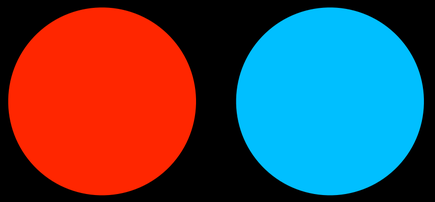
Alic

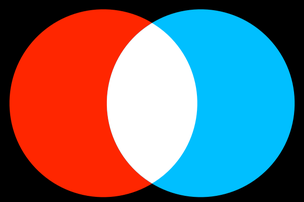
Assumptions

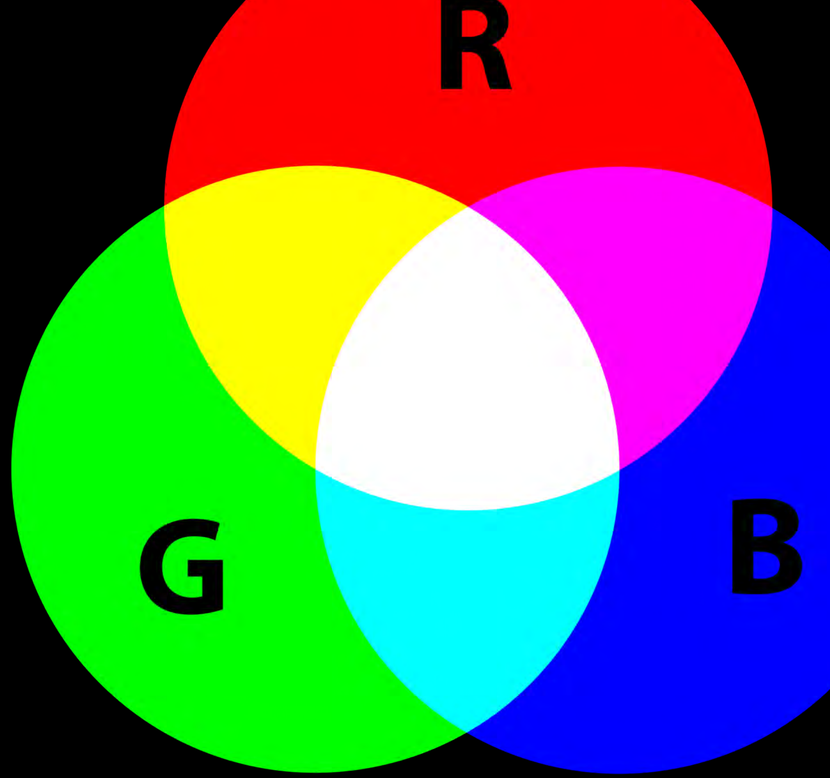
1. The inverse of an additive colour is called complementary colour.

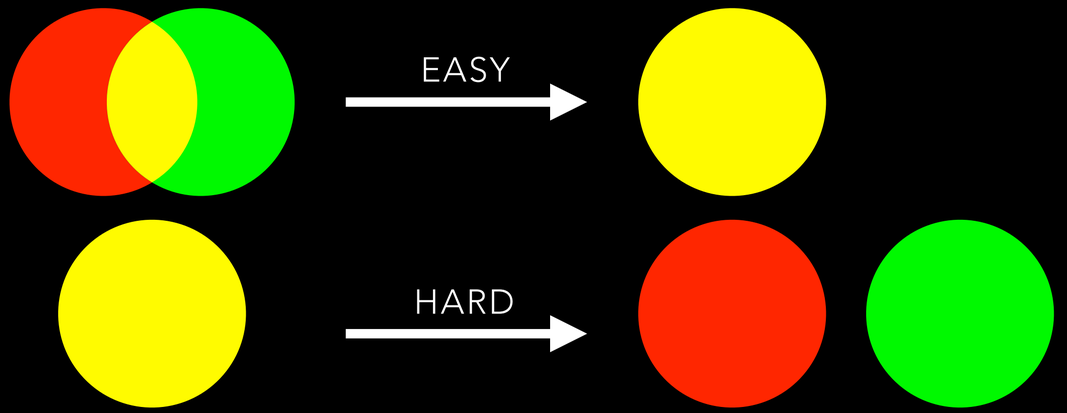
2. Adding the complementary colour to a colour produces white (undoes the effect of the colour)

3. Mixing colours is a one-way function as mixing is fast, but slow to undo.



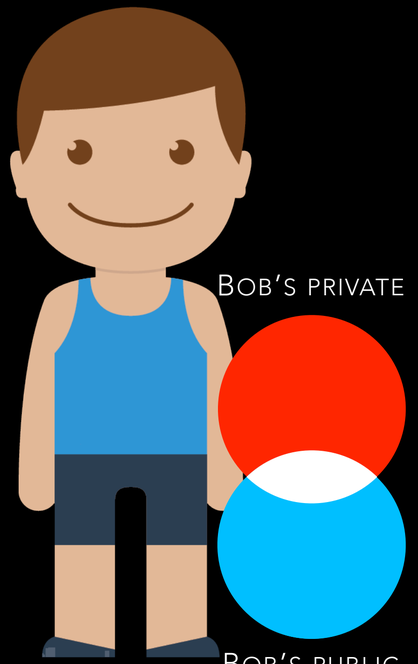


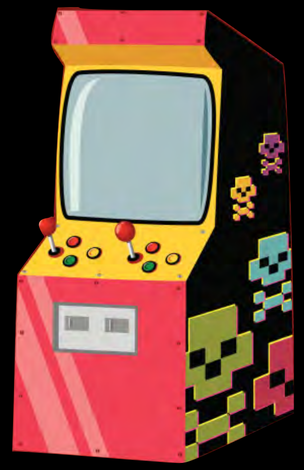




Public Key Cryptography – Encryption

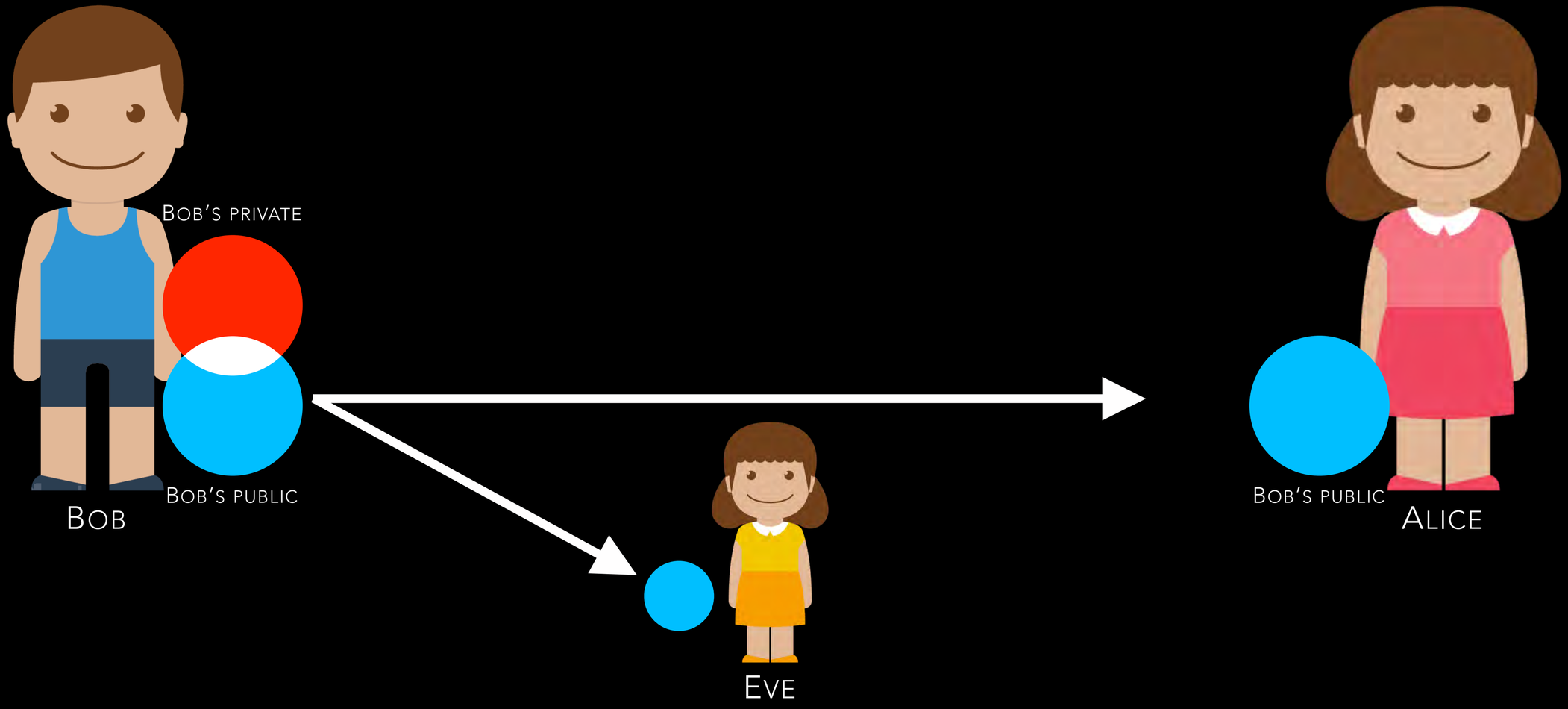
UNIVERSITY OF OXFORD





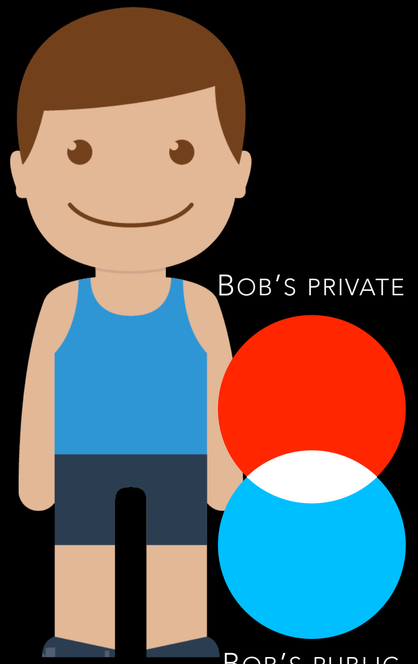
Secret Colour Machine

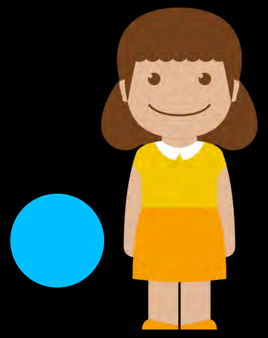
Public Key Cryptography – Encryption

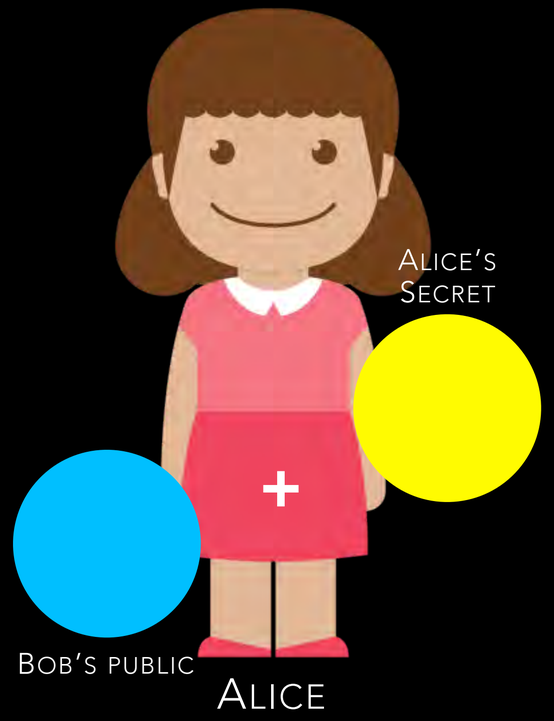


Public Key Cryptography – Encryption

UNIVERSITY OF OXFORD

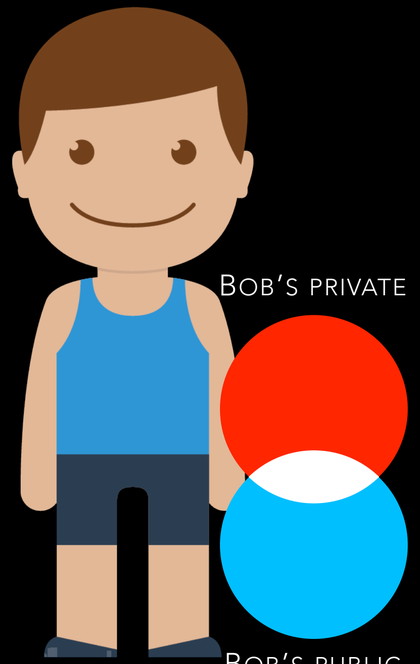


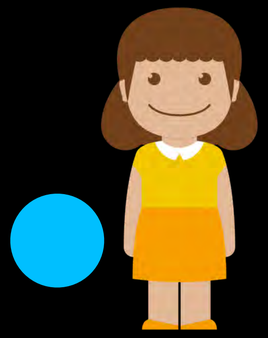


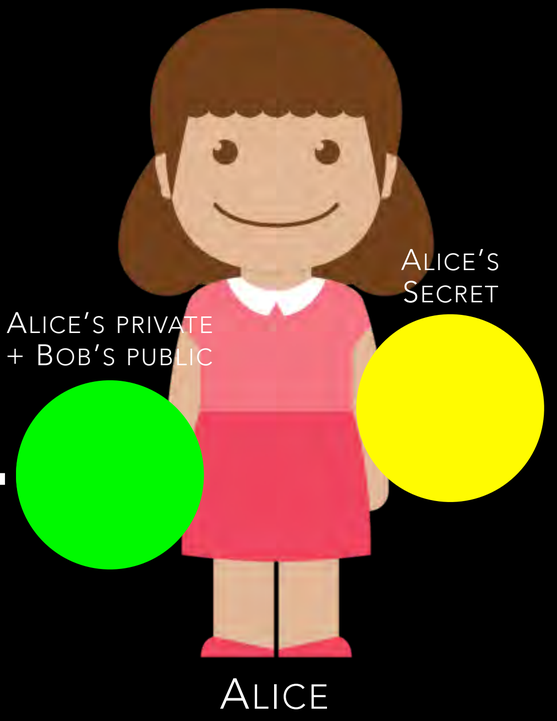


Public Key Cryptography – Encryption

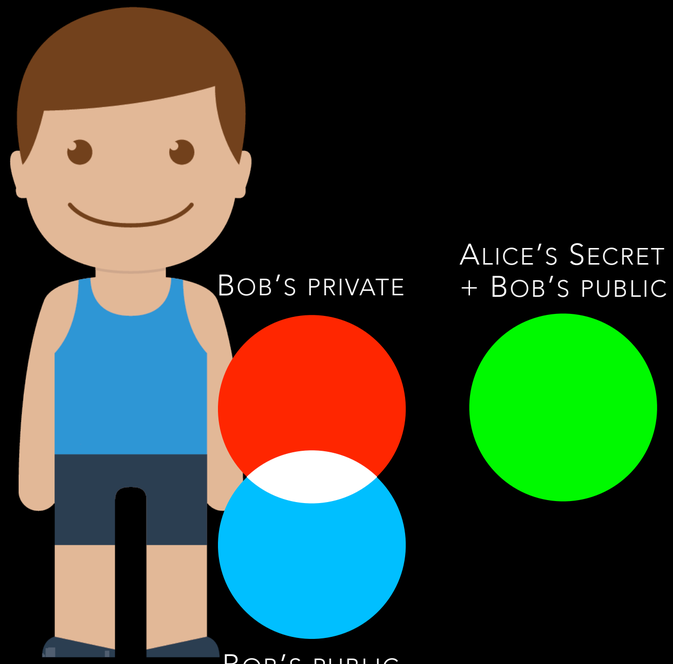
UNIVERSITY OF OXFORD

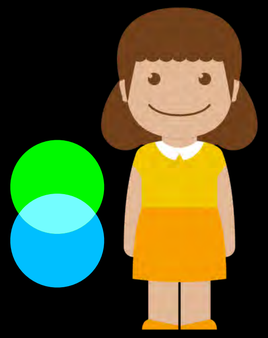


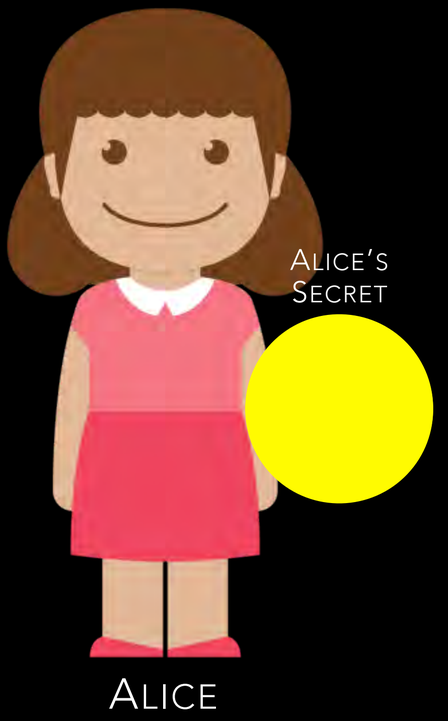




Public Key Cryptography – Encryption

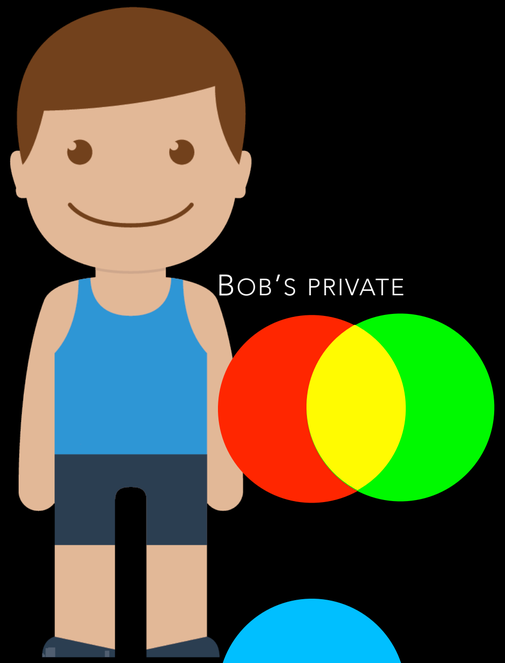






Public Key Cryptography – Encryption

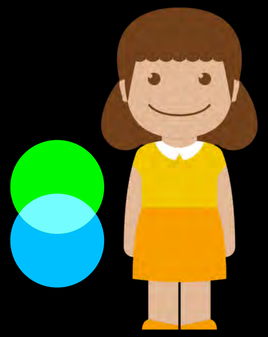
UNIVERSITY OF OXFORD



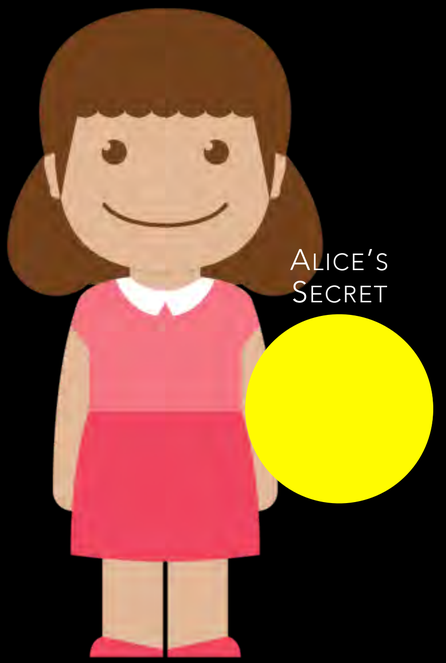
Bob's private

Bob

Bob's public



Eve

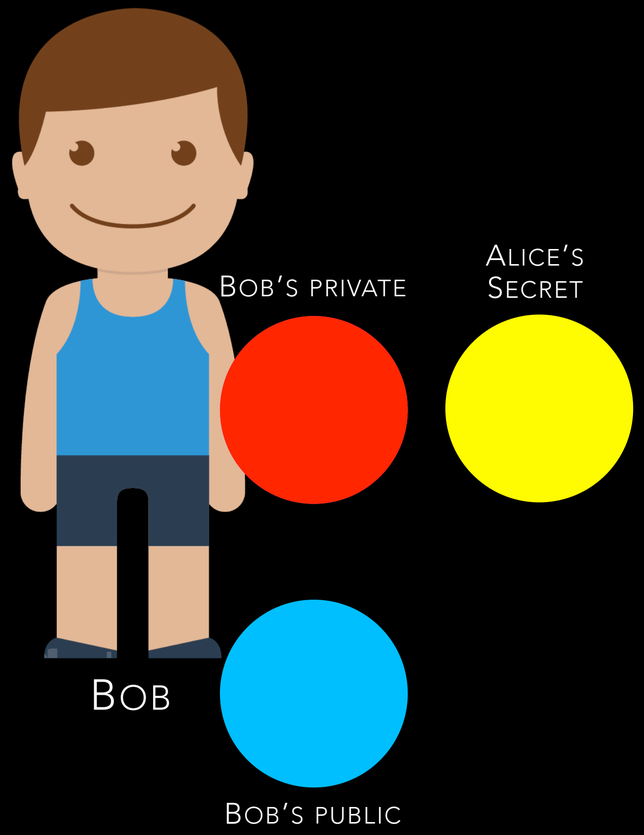


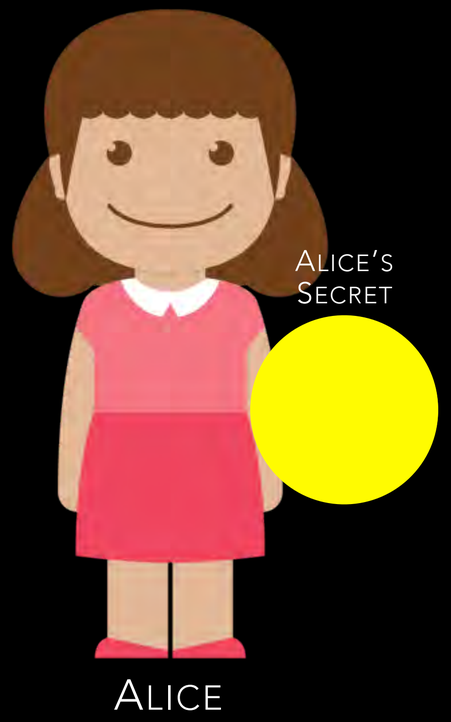
Alice's Secret

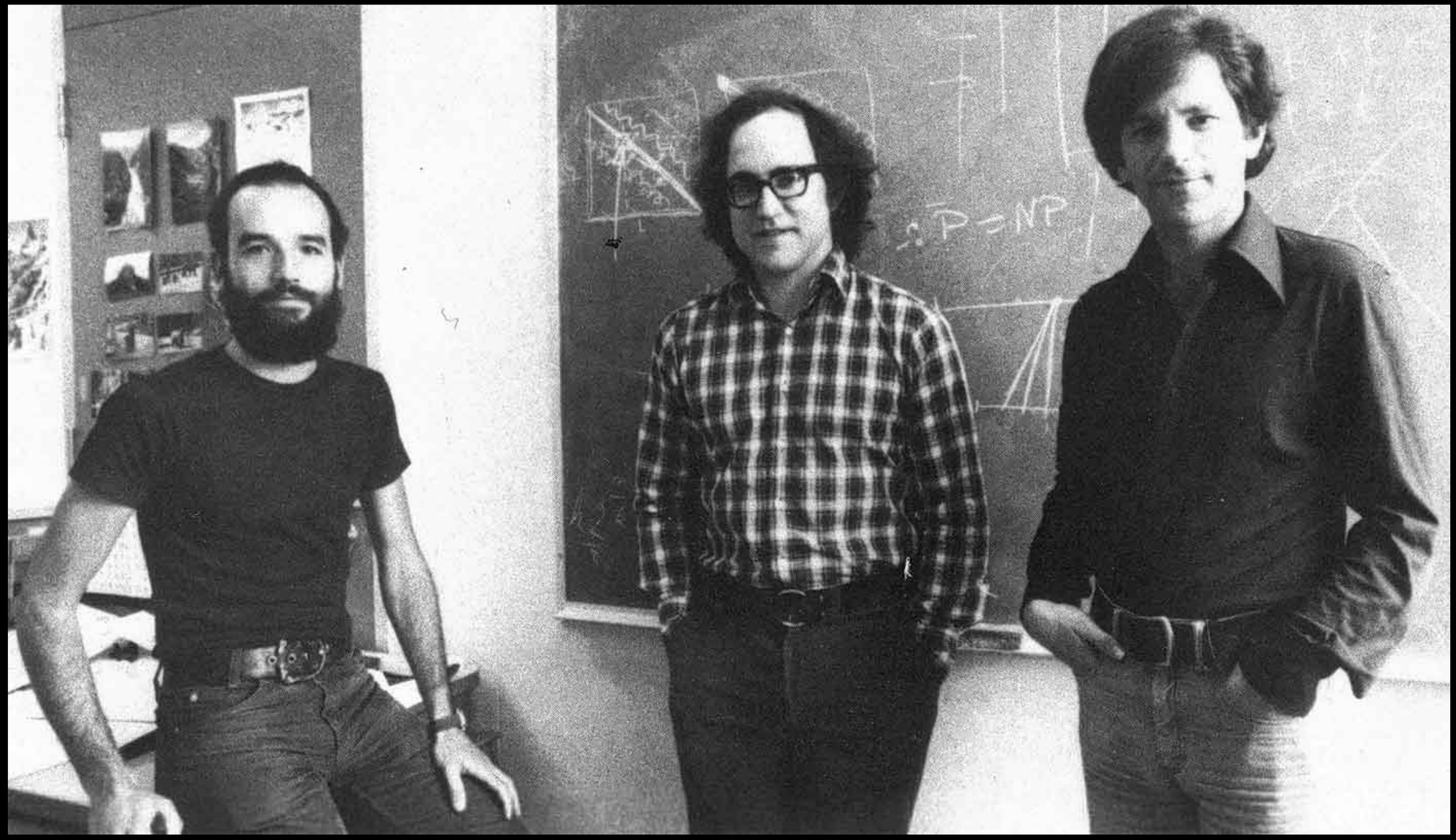
Alice

Public Key Cryptography – Encryption

UNIVERSITY OF OXFORD



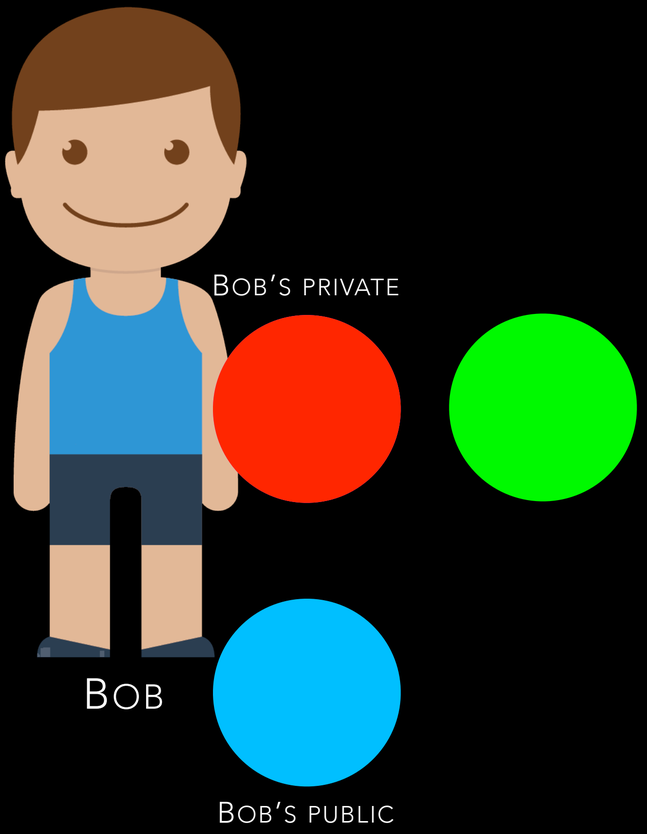




Ron Rivest, Adi Shamir, and Leonard Adleman – the inventors of RSA (1977)

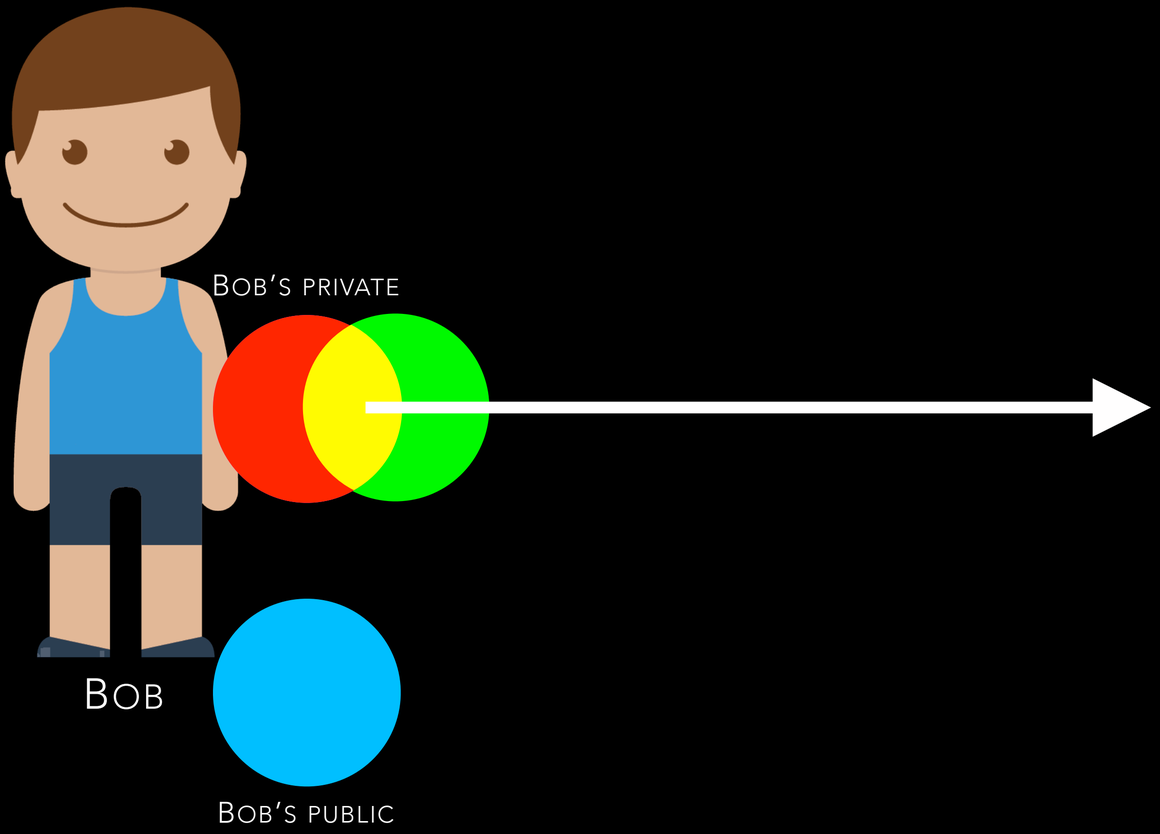
Public Key Cryptography – Signatures

UNIVERSITY OF OXFORD

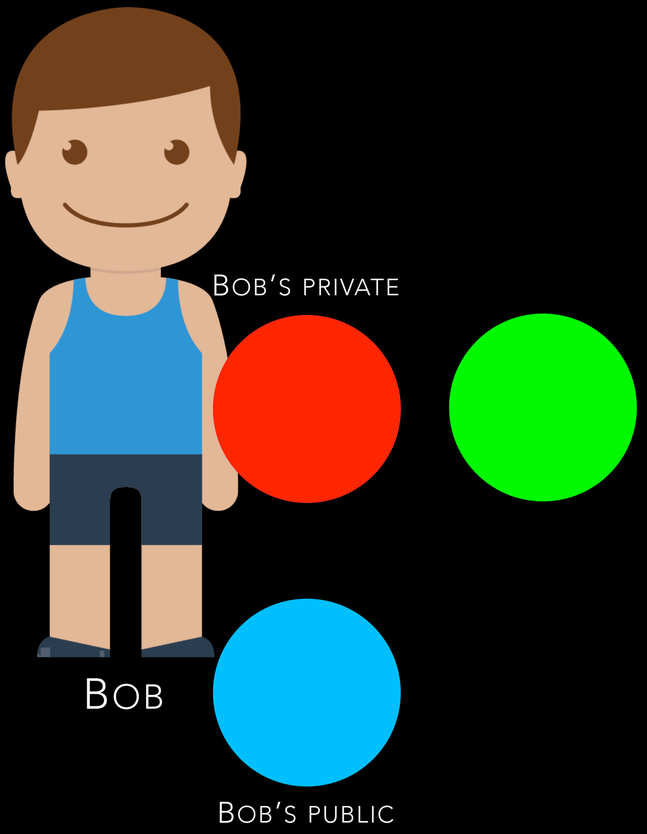


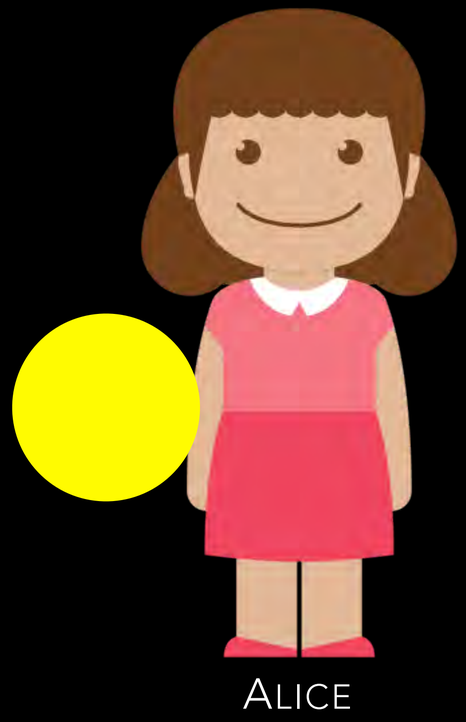
Public Key Cryptography – Signatures

UNIVERSITY OF OXFORD

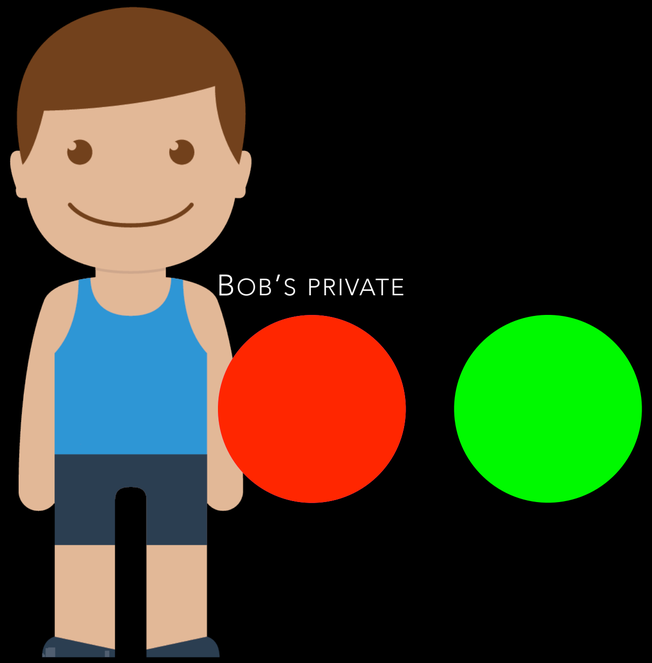


Public Key Cryptography – Signatures

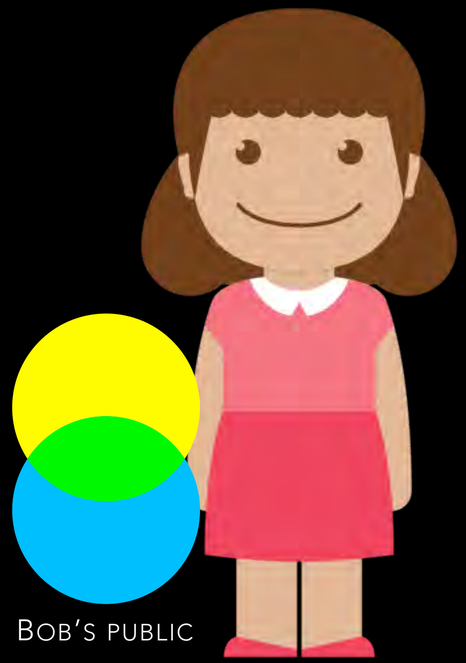




Public Key Cryptography – Signatures

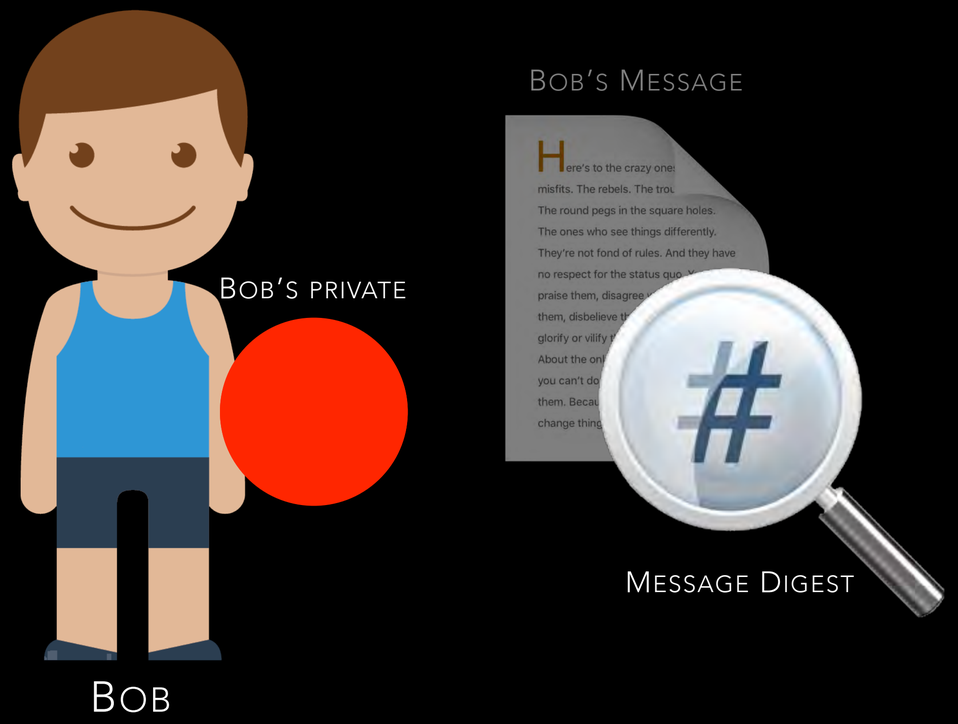


Bob



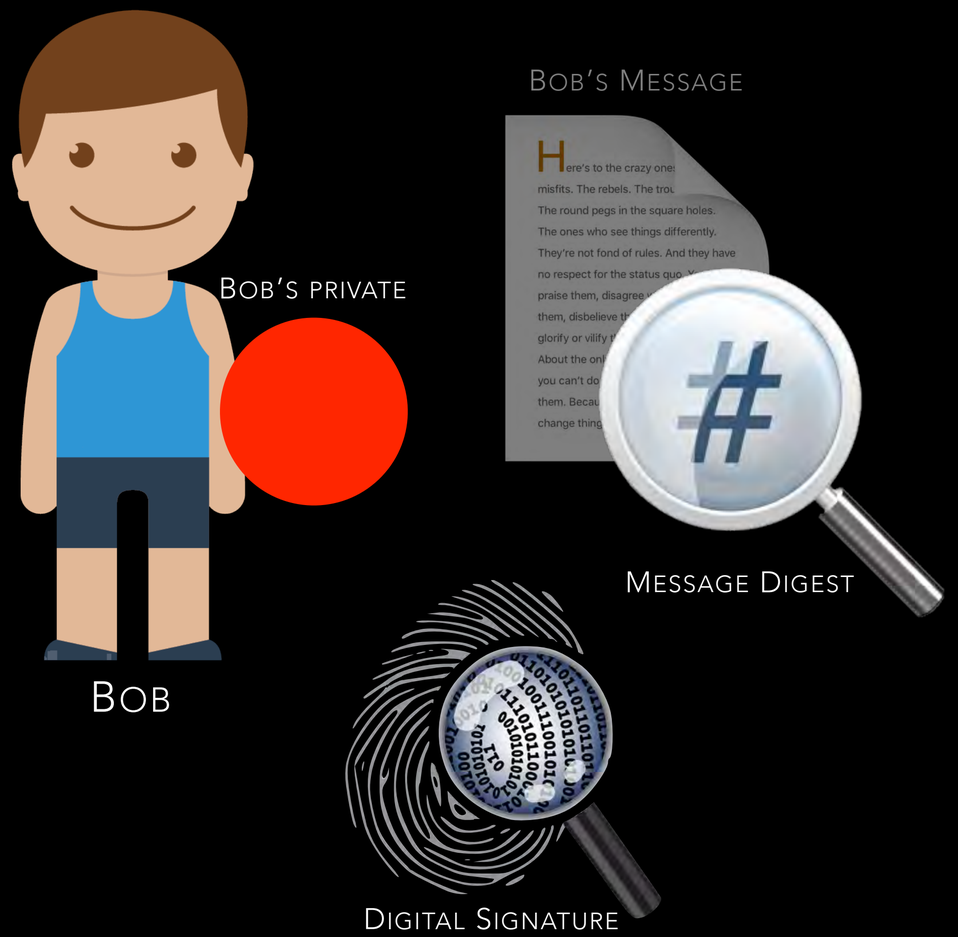
Alice

Public Key Cryptography – Signatures



1. Bob computes the message hash to create the message digest.

Public Key Cryptography – Signatures

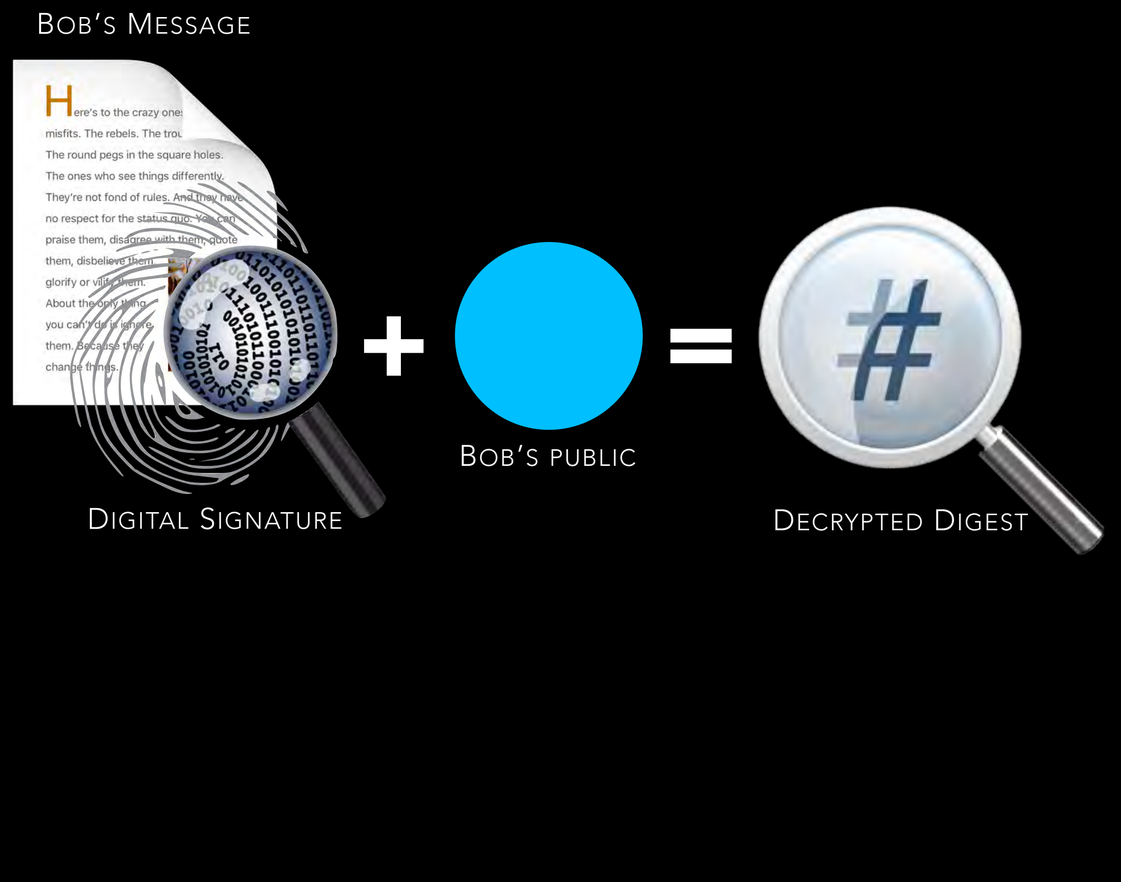


1. Bob computes the message hash to create the message digest.
2. Bob encrypts the message digest with his private key to create a digital signature.

Public Key Cryptography – Signatures

UNIVERSITY OF OXFORD

3. Alice decrypts the digital signature with the Bob's public key to produce the decrypted digest.

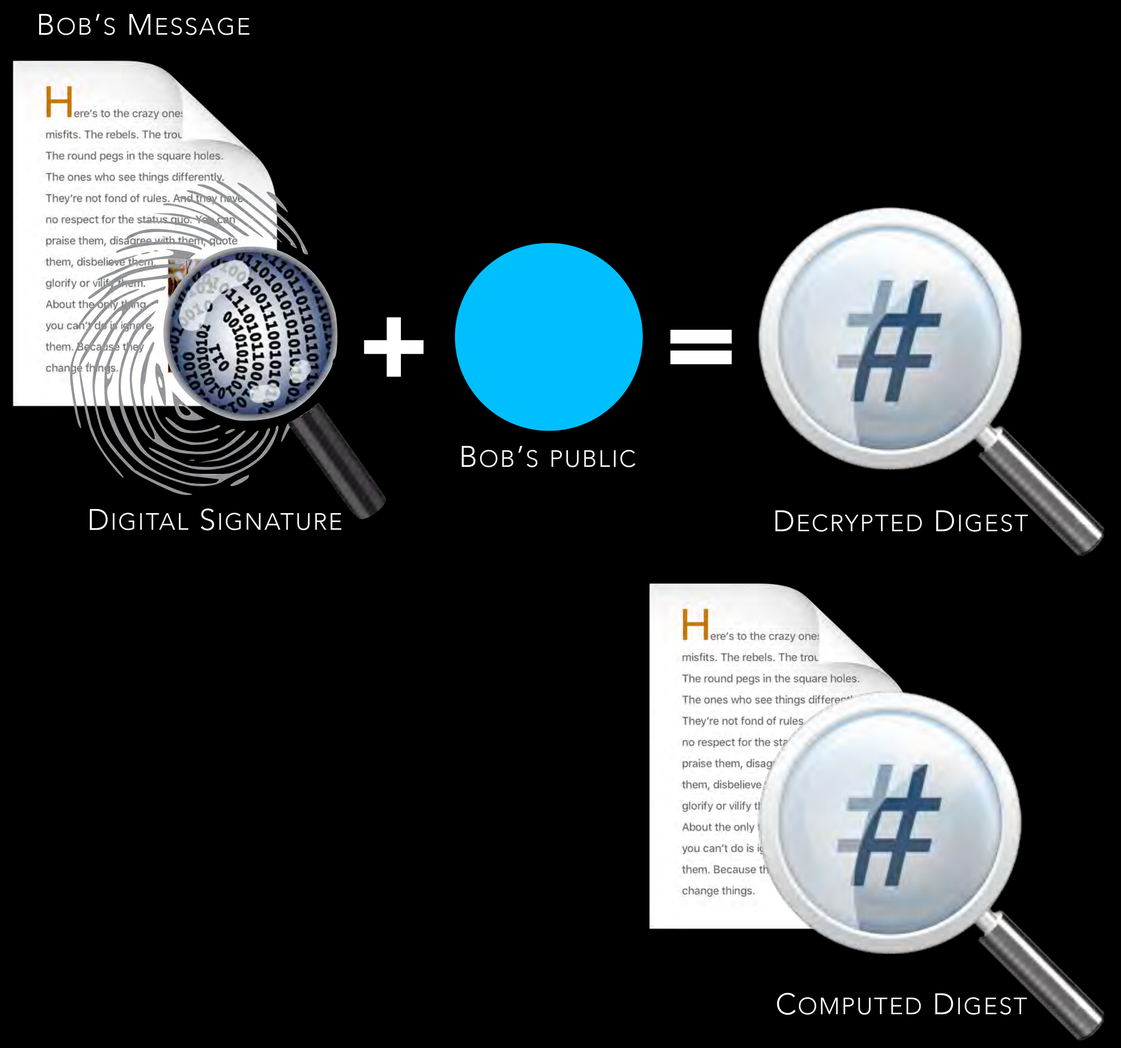


Public Key Cryptography – Signatures

UNIVERSITY OF OXFORD

3. Alice decrypts the digital signature with the Bob's public key to produce the decrypted digest.

4. Alice computes the message hash to produce the computed digest.



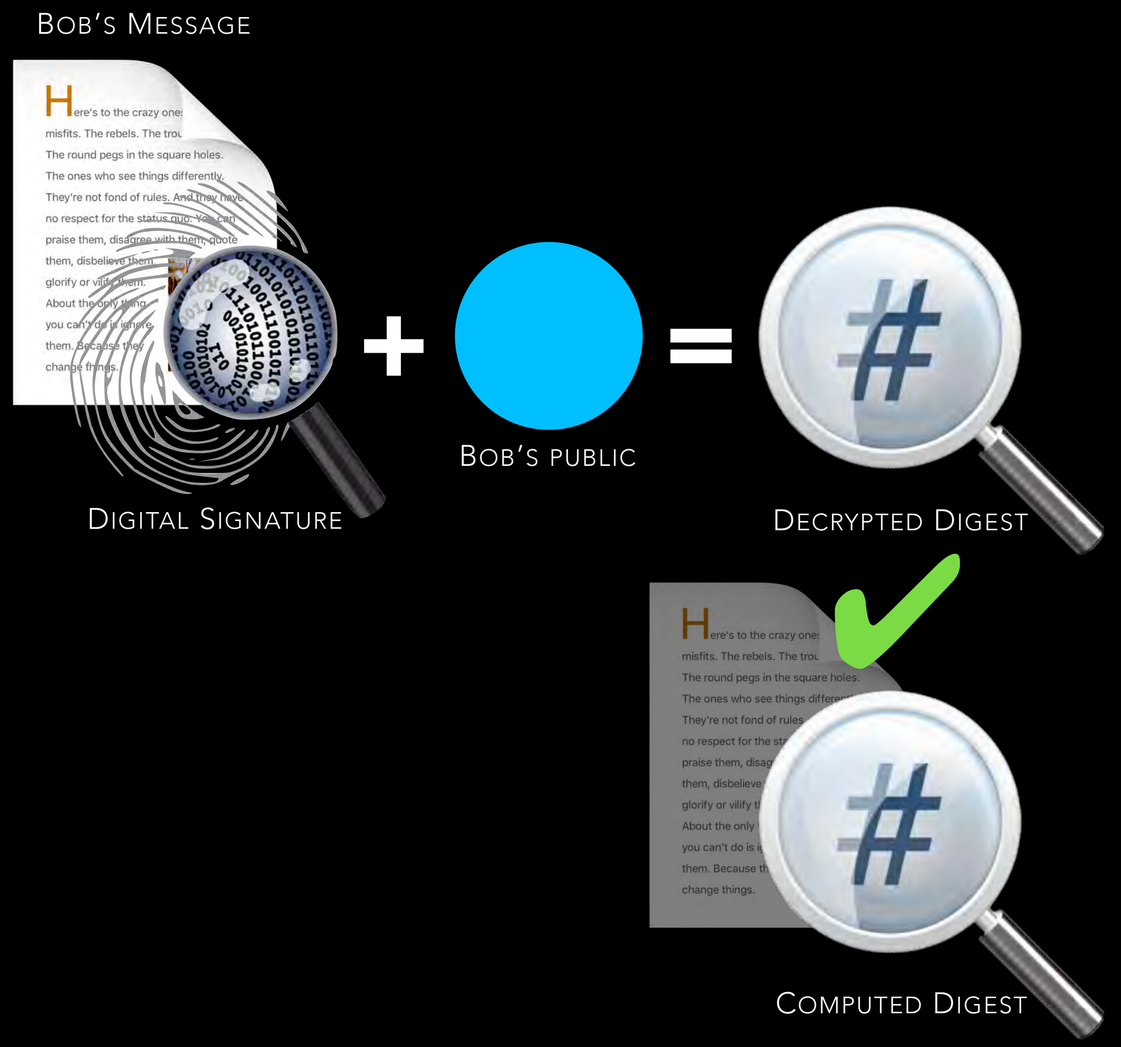
Public Key Cryptography – Signatures

UNIVERSITY OF OXFORD

3. Alice decrypts the digital signature with the Bob's public key to produce the decrypted digest.

4. Alice computes the message hash to produce the computed digest.

5. If the decrypted digest and the computed digest match, the message must have been signed by Bob and has not been modified.



Certificates

What is a Public Key Certificate?

UNIVERSITY OF OXFORD

In cryptography, a **public key certificate** is an **electronic document used to prove ownership of a public key**.

Contents of a Public Key Certificate?

UNIVERSITY OF OXFORD

Information about the certificate holder: name, email address, company name, the owner's public key, etc.

A digital signature from a certification authority: to ensure that the certificate has not been altered and to indicate the identity of the issuer.

Validity period: the certificate is not valid before or after this period.

Structural Information: version, serial number, the message digest algorithm used to create the signature, and so on.

Certificate extensions — attributes that contain additional information such as allowable uses for this certificate.

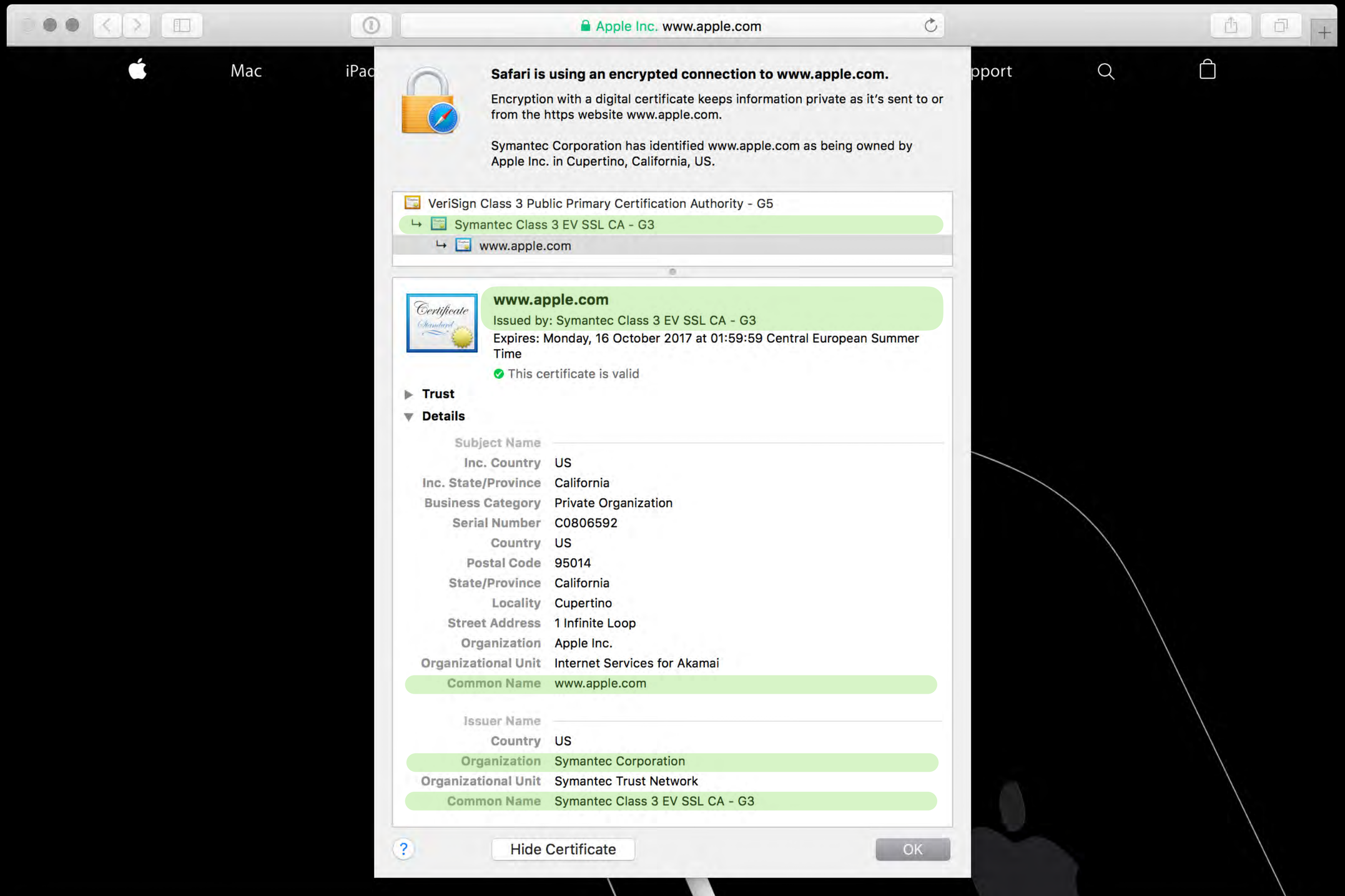
Apple Inc. www.apple.com

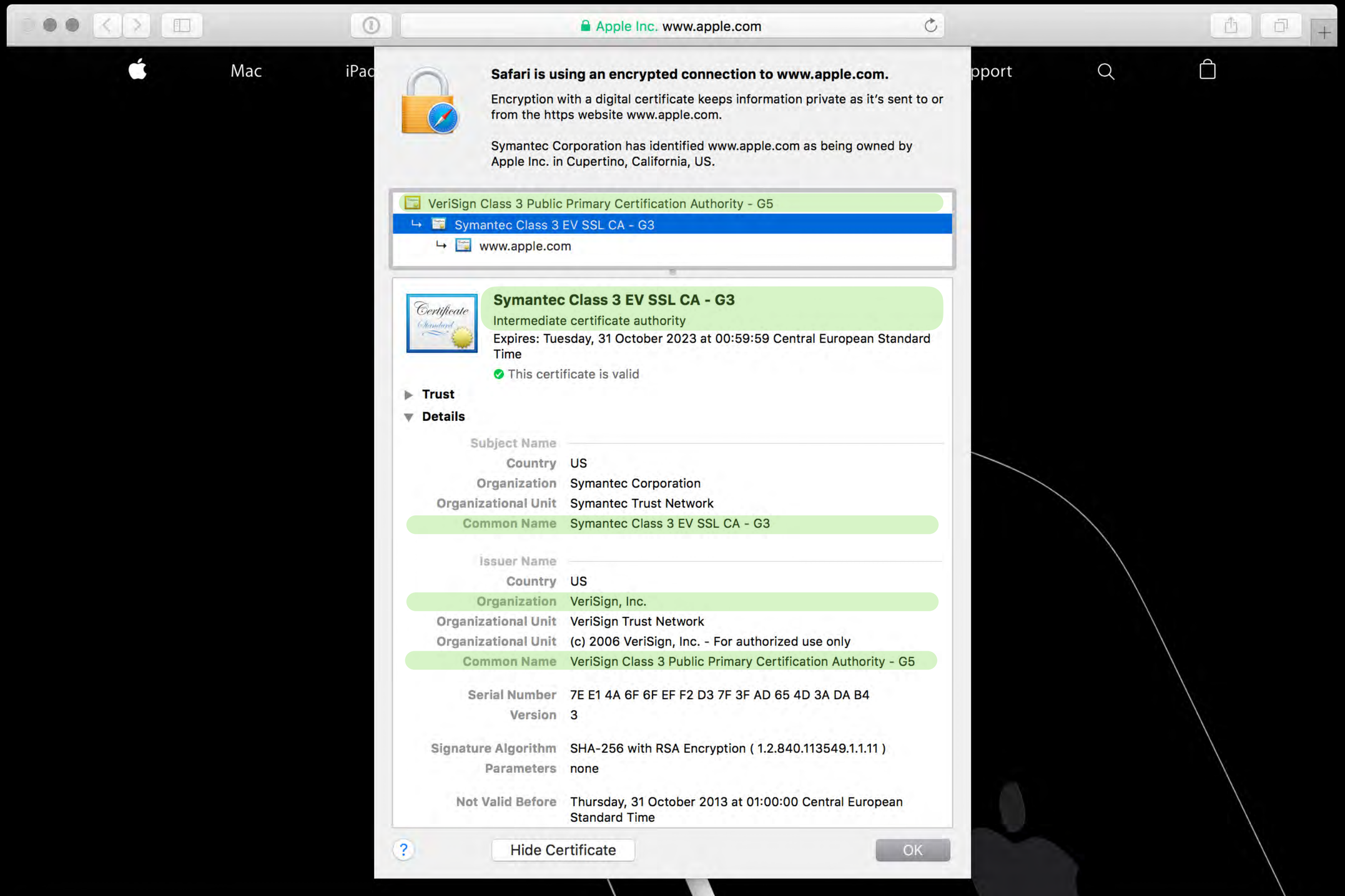
Mac iPad iPhone Watch TV Music Support

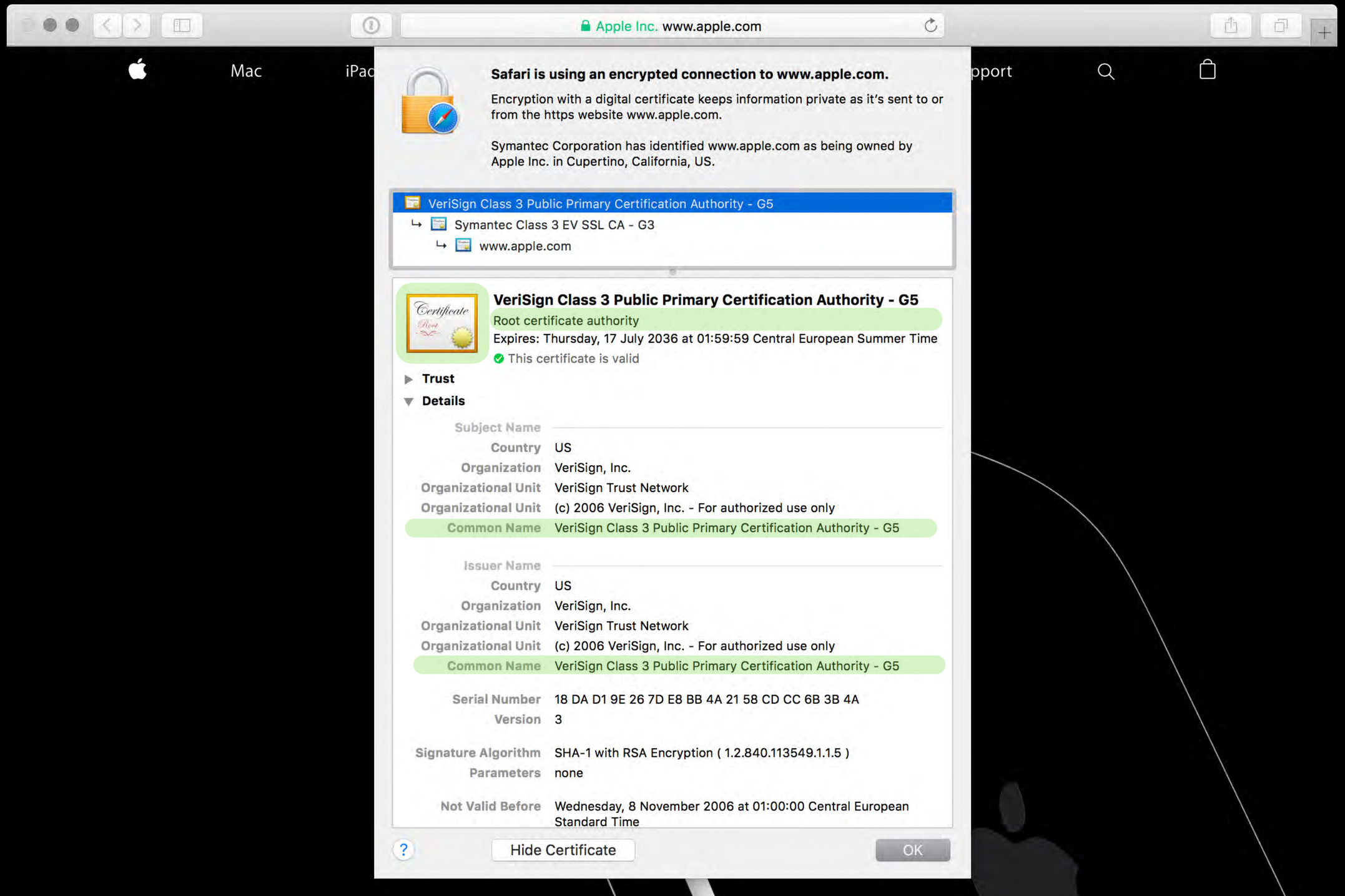
iPhone

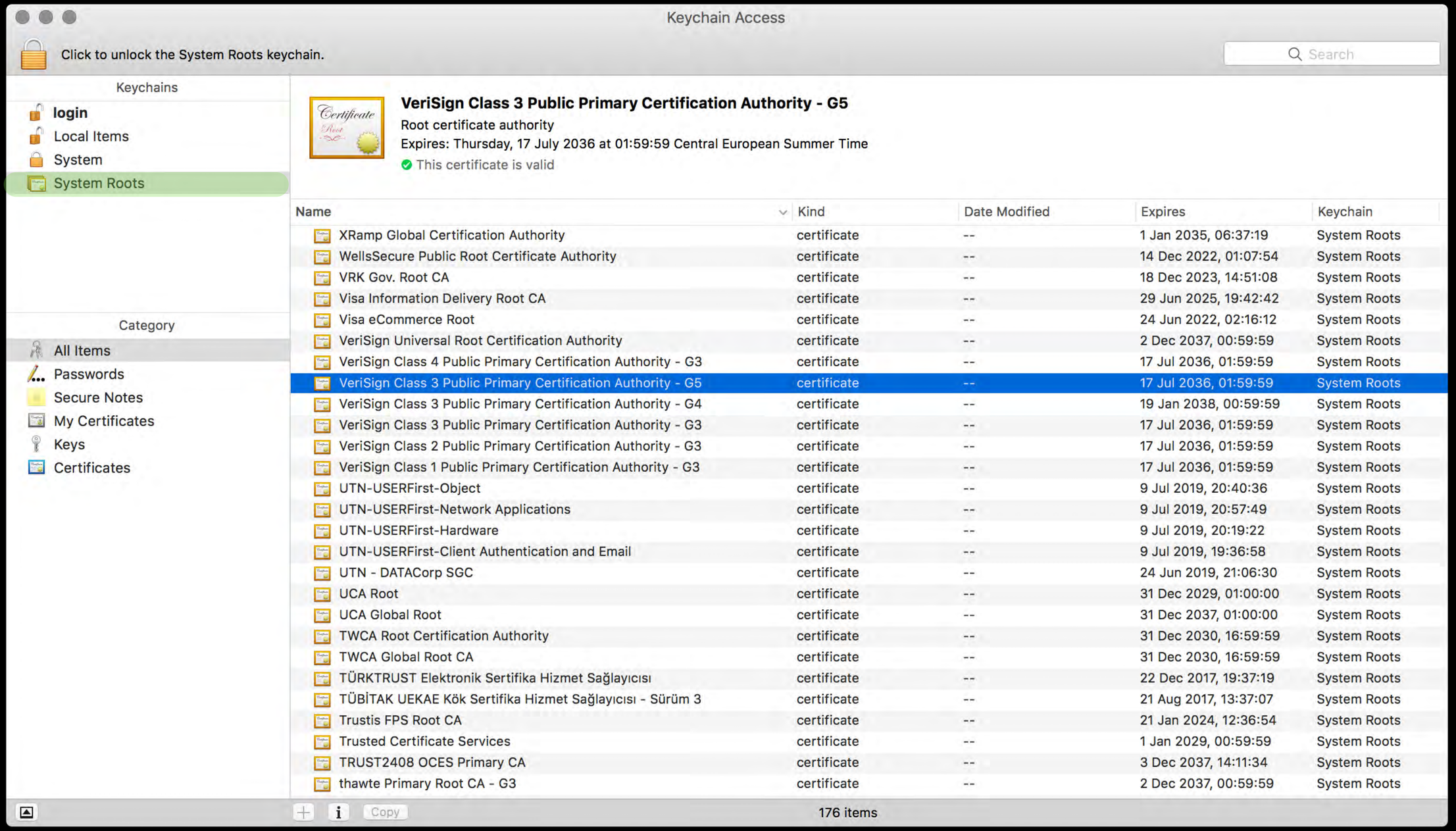
This is 7.


Apple Inc. www.apple.com
Mac
iPad
pport
Safari is using an encrypted connection to www.apple.com.
Encryption with a digital certificate keeps information private as it's sent to or from the https website www.apple.com.
Symantec Corporation has identified www.apple.com as being owned by Apple Inc. in Cupertino, California, US.
VeriSign Class 3 Public Primary Certification Authority - G5
Symantec Class 3 EV SSL CA - G3
www.apple.com
Certificate
Standard
www.apple.com
Issued by: Symantec Class 3 EV SSL CA - G3
Expires: Monday, 16 October 2017 at 01:59:59 Central European Summer Time
This certificate is valid


Apple Inc. www.apple.com
Mac
iPac
pport
Safari is using an encrypted connection to www.apple.com.
Encryption with a digital certificate keeps information private as it's sent to or from the https website www.apple.com.
Symantec Corporation has identified www.apple.com as being owned by Apple Inc. in Cupertino, California, US.
VeriSign Class 3 Public Primary Certification Authority - G5
Symantec Class 3 EV SSL CA - G3
www.apple.com
www.apple.com
Issued by: Symantec Class 3 EV SSL CA - G3
Expires: Monday, 16 October 2017 at 01:59:59 Central European Summer Time
This certificate is valid
Trust
Details
Subject Name
Inc. Country US
Inc. State/Province California
Business Category Private Organization
Serial Number C0806592
Country US
Postal Code 95014
State/Province California
Locality Cupertino
Street Address 1 Infinite Loop
Organization Apple Inc.
Organizational Unit Internet Services for Akamai
Common Name www.apple.com
Issuer Name
Country US
Organization Symantec Corporation
Organizational Unit Symantec Trust Network
Common Name Symantec Class 3 EV SSL CA - G3
Hide Certificate
OK


Apple Inc. www.apple.com
Mac
iPac
pport
Safari is using an encrypted connection to www.apple.com.
Encryption with a digital certificate keeps information private as it's sent to or from the https website www.apple.com.
Symantec Corporation has identified www.apple.com as being owned by Apple Inc. in Cupertino, California, US.
VeriSign Class 3 Public Primary Certification Authority - G5
Symantec Class 3 EV SSL CA - G3
www.apple.com
Symantec Class 3 EV SSL CA - G3
Intermediate certificate authority
Expires: Tuesday, 31 October 2023 at 00:59:59 Central European Standard Time
This certificate is valid
Trust
Details
Subject Name
Country US
Organization Symantec Corporation
Organizational Unit Symantec Trust Network
Common Name Symantec Class 3 EV SSL CA - G3
Issuer Name
Country US
Organization VeriSign, Inc.
Organizational Unit VeriSign Trust Network
Organizational Unit (c) 2006 VeriSign, Inc. - For authorized use only
Common Name VeriSign Class 3 Public Primary Certification Authority - G5
Serial Number 7E E1 4A 6F 6F EF F2 D3 7F 3F AD 65 4D 3A DA B4
Version 3
Signature Algorithm SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters none
Not Valid Before Thursday, 31 October 2013 at 01:00:00 Central European Standard Time
Hide Certificate
OK


Apple Inc. www.apple.com
Mac
iPac
pport
Safari is using an encrypted connection to www.apple.com.
Encryption with a digital certificate keeps information private as it's sent to or from the https website www.apple.com.
Symantec Corporation has identified www.apple.com as being owned by Apple Inc. in Cupertino, California, US.
VeriSign Class 3 Public Primary Certification Authority - G5
Symantec Class 3 EV SSL CA - G3
www.apple.com
VeriSign Class 3 Public Primary Certification Authority - G5
Root certificate authority
Expires: Thursday, 17 July 2036 at 01:59:59 Central European Summer Time
This certificate is valid
Trust
Details
Subject Name
Country US
Organization VeriSign, Inc.
Organizational Unit VeriSign Trust Network
Organizational Unit (c) 2006 VeriSign, Inc. - For authorized use only
Common Name VeriSign Class 3 Public Primary Certification Authority - G5
Issuer Name
Country US
Organization VeriSign, Inc.
Organizational Unit VeriSign Trust Network
Organizational Unit (c) 2006 VeriSign, Inc. - For authorized use only
Common Name VeriSign Class 3 Public Primary Certification Authority - G5
Serial Number 18 DA D1 9E 26 7D E8 BB 4A 21 58 CD CC 6B 3B 4A
Version 3
Signature Algorithm SHA-1 with RSA Encryption (1.2.840.113549.1.1.5)
Parameters none
Not Valid Before Wednesday, 8 November 2006 at 01:00:00 Central European Standard Time
Hide Certificate
OK


Keychain Access
Click to unlock the System Roots keychain.
Search
Keychains
login
Local Items
System
System Roots
Category
All Items
Passwords
Secure Notes
My Certificates
Keys
Certificates
VeriSign Class 3 Public Primary Certification Authority - G5
Root certificate authority
Expires: Thursday, 17 July 2036 at 01:59:59 Central European Summer Time
This certificate is valid
Name
Kind
Date Modified
Expires
Keychain
XRamp Global Certification Authority certificate -- 1 Jan 2035, 06:37:19 System Roots
WellsSecure Public Root Certificate Authority certificate -- 14 Dec 2022, 01:07:54 System Roots
VRK Gov. Root CA certificate -- 18 Dec 2023, 14:51:08 System Roots
Visa Information Delivery Root CA certificate -- 29 Jun 2025, 19:42:42 System Roots
Visa eCommerce Root certificate -- 24 Jun 2022, 02:16:12 System Roots
VeriSign Universal Root Certification Authority certificate -- 2 Dec 2037, 00:59:59 System Roots
VeriSign Class 4 Public Primary Certification Authority - G3 certificate -- 17 Jul 2036, 01:59:59 System Roots
VeriSign Class 3 Public Primary Certification Authority - G5 certificate -- 17 Jul 2036, 01:59:59 System Roots
VeriSign Class 3 Public Primary Certification Authority - G4 certificate -- 19 Jan 2038, 00:59:59 System Roots
VeriSign Class 3 Public Primary Certification Authority - G3 certificate -- 17 Jul 2036, 01:59:59 System Roots
VeriSign Class 2 Public Primary Certification Authority - G3 certificate -- 17 Jul 2036, 01:59:59 System Roots
VeriSign Class 1 Public Primary Certification Authority - G3 certificate -- 17 Jul 2036, 01:59:59 System Roots
UTN-USERFirst-Object certificate -- 9 Jul 2019, 20:40:36 System Roots
UTN-USERFirst-Network Applications certificate -- 9 Jul 2019, 20:57:49 System Roots
UTN-USERFirst-Hardware certificate -- 9 Jul 2019, 20:19:22 System Roots
UTN-USERFirst-Client Authentication and Email certificate -- 9 Jul 2019, 19:36:58 System Roots
UTN - DATACorp SGC certificate -- 24 Jun 2019, 21:06:30 System Roots
UCA Root certificate -- 31 Dec 2029, 01:00:00 System Roots
UCA Global Root certificate -- 31 Dec 2037, 01:00:00 System Roots
TWCA Root Certification Authority certificate -- 31 Dec 2030, 16:59:59 System Roots
TWCA Global Root CA certificate -- 31 Dec 2030, 16:59:59 System Roots
TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı certificate -- 22 Dec 2017, 19:37:19 System Roots
TÜBİTAK UEKAE Kök Sertifika Hizmet Sağlayıcısı - Sürüm 3 certificate -- 21 Aug 2017, 13:37:07 System Roots
Trustis FPS Root CA certificate -- 21 Jan 2024, 12:36:54 System Roots
Trusted Certificate Services certificate -- 1 Jan 2029, 00:59:59 System Roots
TRUST2408 OCES Primary CA certificate -- 3 Dec 2037, 14:11:34 System Roots
thawte Primary Root CA - G3 certificate -- 2 Dec 2037, 00:59:59 System Roots
Copy
176 items

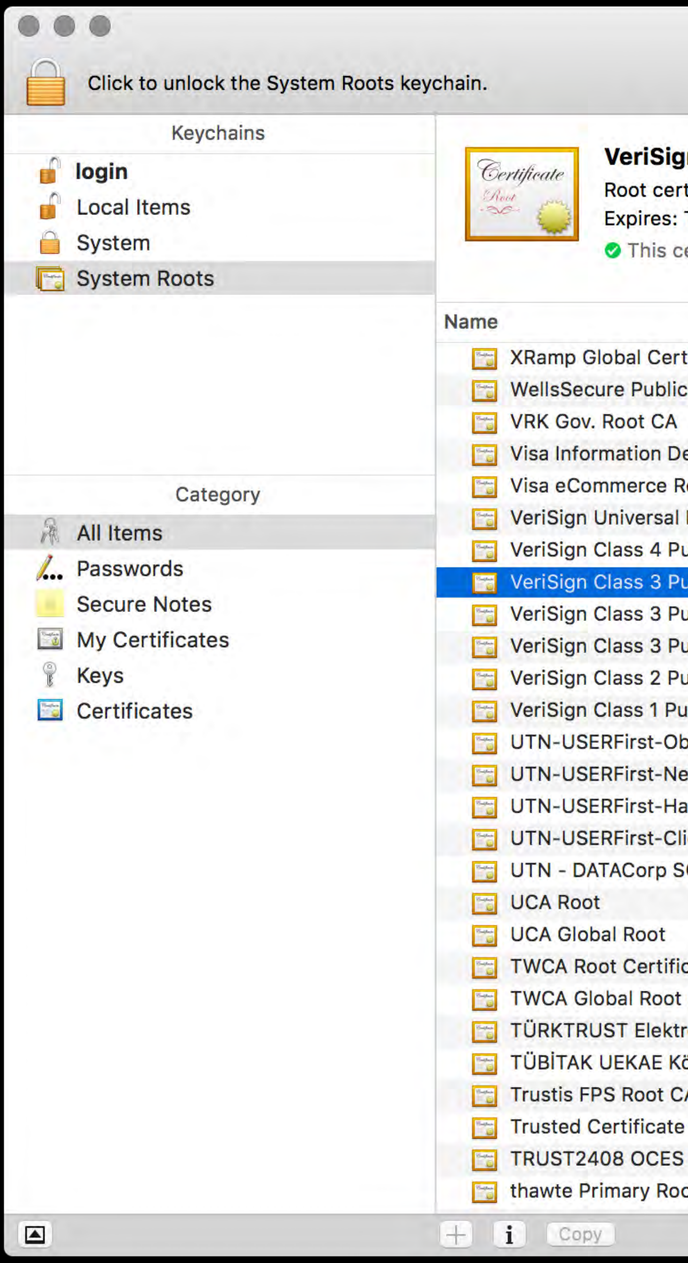
So many Keychains

LOGIN: user specific items, typically login password
/Users/<username>/Library/Keychains/login.keychain

iCLOUD/LOCAL ITEMS: enabled/disabled cloud synced
/Users/<username>/Library/Keychains/<UUID>

SYSTEM: not user specific authentication assets
Only administrative users can make changes to it.
/Library/Keychains/System.keychain

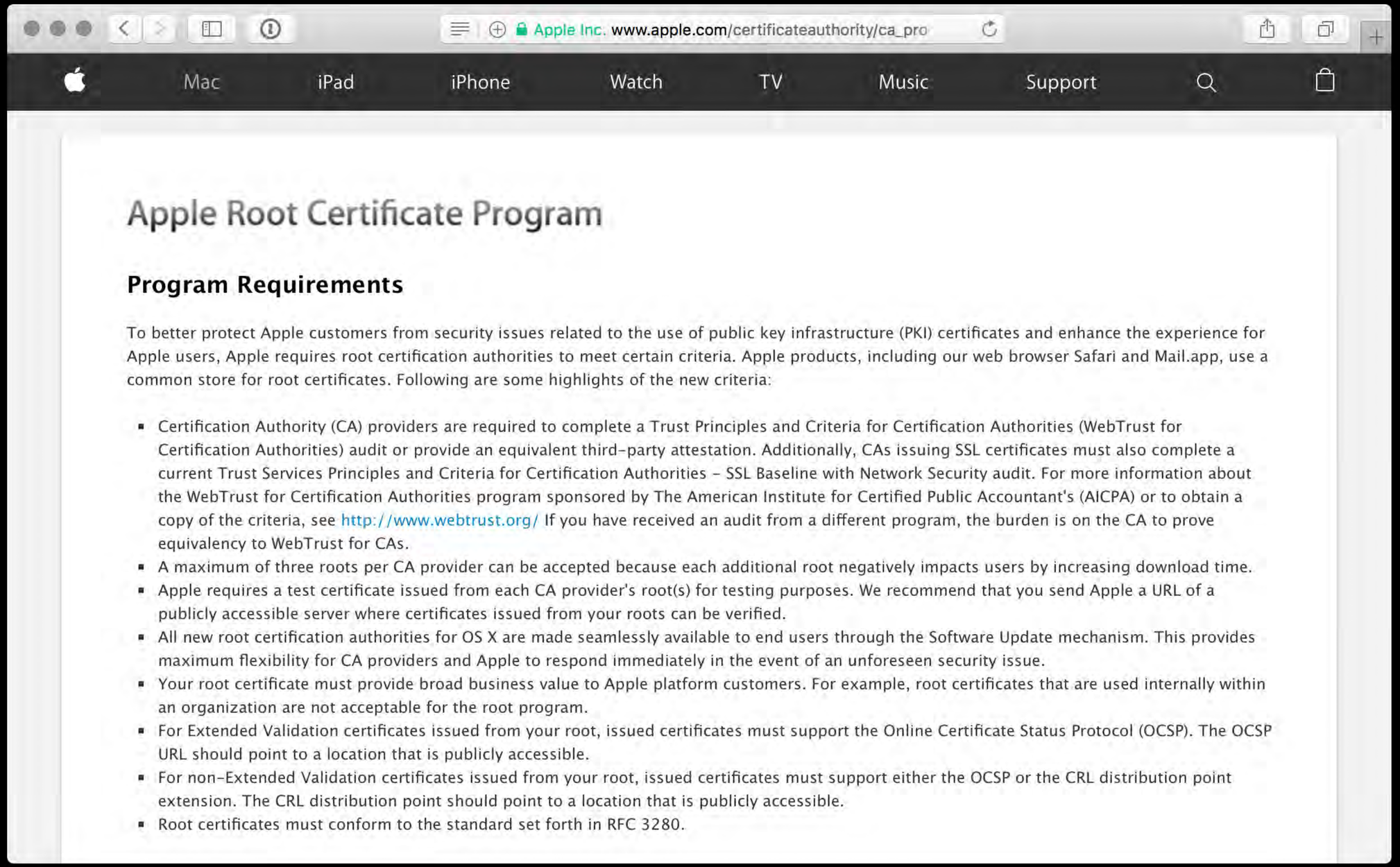
SYSTEM ROOTS: system wide trusted root certificates.
Only administrative users can change trust settings.
/System/Library/Keychains/SystemCACertificates.keychain
See also https://support.apple.com/en-us/HT202858



Root Certificate Stores

BROWSER				
OPERATING SYSTEM	X iOS		ALL	
ROOT CERTIFICATE STORE			mozilla	

Source: https://certsimple.com/blog/control-the-ssl-cas-your-browser-trusts



https://www.apple.com/certificateauthority/ca_program.html

Public Key Infrastructure

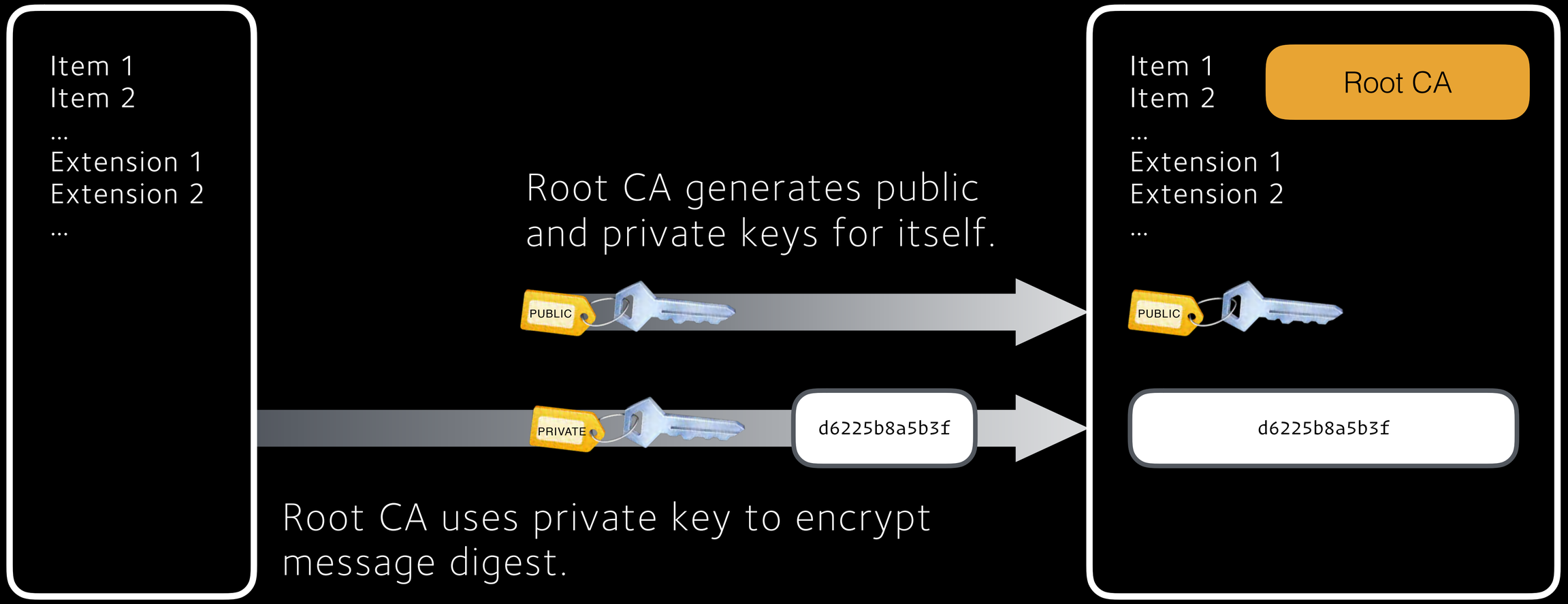
A public key infrastructure typically consists of:

- A **Certificate Authority (CA)** that stores, issues and signs the digital certificates.
- A **Registration Authority (RA)** which verifies the identity of entities requesting their digital certificates to be signed by and stored at the CA.
- A (third-party) **Validation Authority (VA)**.
- A **Central Directory**—i.e., a secure location in which to store and index keys.
- A **Certificate Management System** managing things like the access to stored certificates or the delivery of the certificates to be issued.
- A **Certificate Policy.**

Creating a Root CA

UNIVERSITY OF OXFORD

Root CA assigns certificate attributes for own CA.



Creating an Intermediate CA

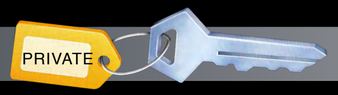
UNIVERSITY OF OXFORD

Root CA assigns certificate attributes

Item 1
Item 2
...
Extension 1
Extension 2
...

Intermediate CA generates public and private key and provides its public key to the Root CA.

Root CA uses private key to encrypt message digest.



421c76d77563

Root CA uses own certificate to sign intermediate certificate.

Item 1
Item 2
...
Extension 1
Extension 2
...

Intermediate CA

421c76d77563

Root CA

Creating an User Certificate

UNIVERSITY OF OXFORD

Intermediate CA assigns
user certificate attributes

Item 1
Item 2
…
Extension 1
Extension 2
…

End user creates public and private key and provides its public key to the intermediate CA.

Intermediate CA uses private key to encrypt message digest.

d77563421c76

Intermediate CA uses own certificate to sign intermediate certificate.

Item 1
Item 2
…
Extension 1
Extension 2
…

User Cert

d77563421c76

Intermediate CA

Certificate Chain

UNIVERSITY OF OXFORD

Item 1
Item 2
...
Extension 1
Extension 2
...

User Cert

d77563421c76

Intermediate CA

Item 1
Item 2
...
Extension 1
Extension 2
...

Intermediate CA

421c76d77563

Root CA

Item 1
Item 2
...
Extension 1
Extension 2
...

Root CA

d6225b8a5b3f

Certificate Revocation Lists


```
$ openssl crl -in apple-ca-root.crl -inform DER -text
Certificate Revocation List (CRL):
        Version 2 (0x1)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: /C=US/O=Apple Inc./OU=Apple Certification Authority/CN=Apple Root CA
        Last Update: Aug 17 02:42:03 2016 GMT
        Next Update: Dec 30 02:42:03 2016 GMT
        CRL extensions:
            X509v3 Authority Key Identifier:
                keyid:2B:D0:69:47:94:76:09:FE:F4:6B:8D:2E:40:A6:F7:47:4D:7F:08:5E

No Revoked Certificates.
    Signature Algorithm: sha1WithRSAEncryption
        af:67:57:57:bd:51:3f:b3:69:aa:02:[…]c9:de:9c:c6
-----BEGIN X509 CRL-----
MIIB0DCBuQIBATANBgkqhkiG9w0BAQUFADBiMQswCQYDVQQGEwJVUzETMBEGA1UE
ChMKQXBwbGUgSW5jLjEmMCQGA1UECxMdQXBwbGUgQ2VydGlmaWNhdGlvbiBBdXRo
[…]/NdyVbvoD94PCz2cvNxlrgc3yowAAfpoULNne/QsDjfJ3pzG
-----END X509 CRL-----
```

Certificate Revocation Lists


```
$ openssl crl -in apple-wwdrca.crl -inform DER -text
Certificate Revocation List (CRL):
  Version 2 (0x1)
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: /C=US/O=Apple Inc./OU=Apple Worldwide Developer Relations/
    CN=Apple Worldwide Developer Relations Certification Authority
  Last Update: Oct  5 02:21:44 2016 GMT
  Next Update: Oct 19 02:21:44 2016 GMT
  CRL extensions:
    X509v3 Authority Key Identifier: keyid:88:27:17:09:A9:B6:18:60:[…]:47:59:C5:52:54:A3:B7
    X509v3 CRL Number: 4576
    X509v3 Issuing Distrubution Point: critical
      0B.@.>.<http://developer.apple.com/certificationauthority/wwdrca.crl

Revoked Certificates:
  Serial Number: 08D53EDF8EE90515
    Revocation Date: Mar  4 00:45:10 2016 GMT
      CRL entry extensions:
      X509v3 CRL Reason Code: Key Compromise
[…]
```

Certificate Revocation Lists


```
$ openssl crl -in apple-wwdrca.crl -inform DER -text | grep "Serial Number:" | wc -l
```

2.454.163

Certificate Revocation Lists

UNIVERSITY OF OXFORD

- A CRL is generated and published periodically, often at a defined interval.
- CRLs usually carry a digital signature associated with the CA by which they are published.
- Part of every good CA Policy
- Should be part of every signing certificate as certificate extension:
  CRL Distribution Points (2.5.29.31)
- Specified in RFC5280
  https://tools.ietf.org/html/rfc5280

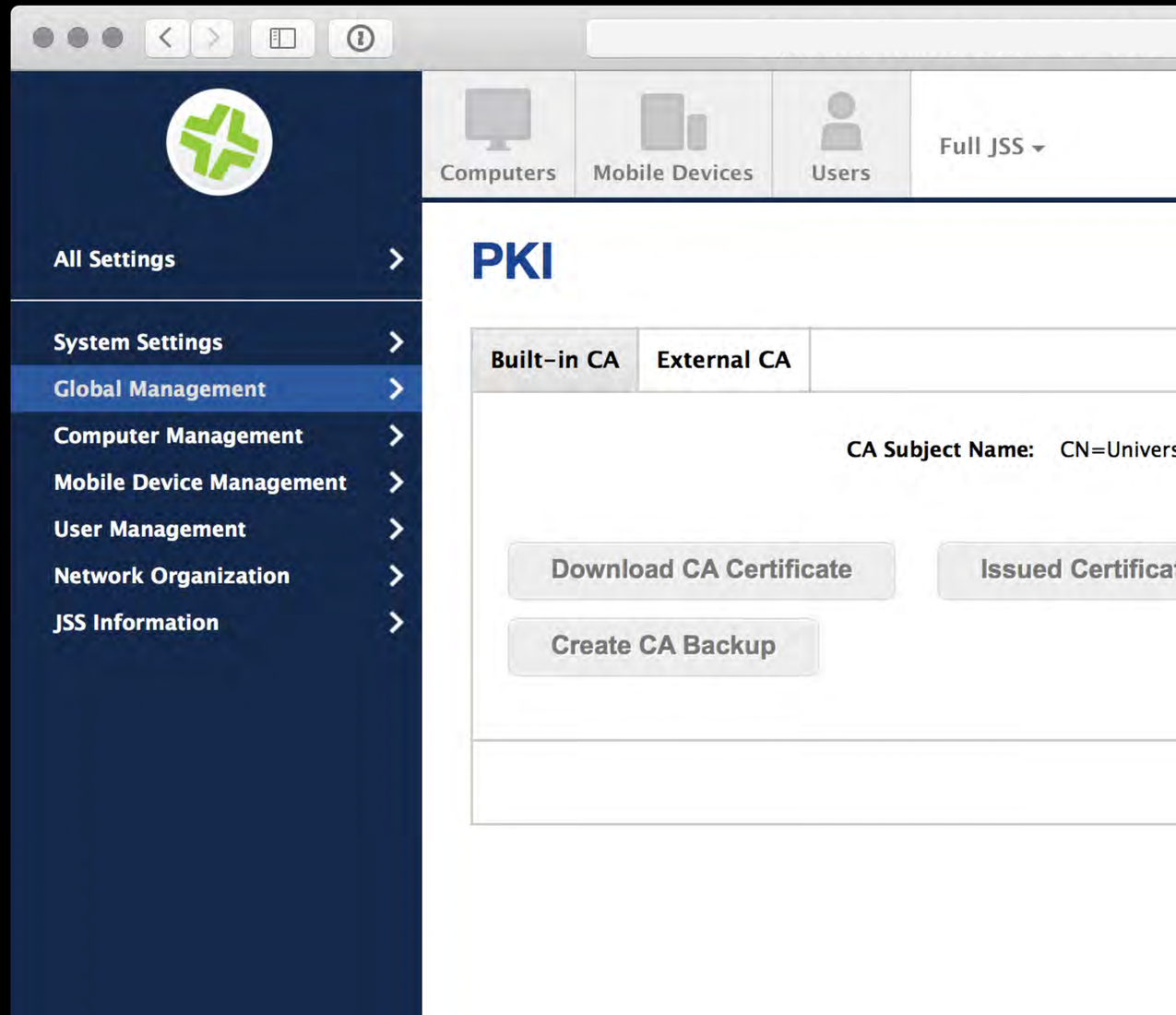
Online Certificate Status Protocol

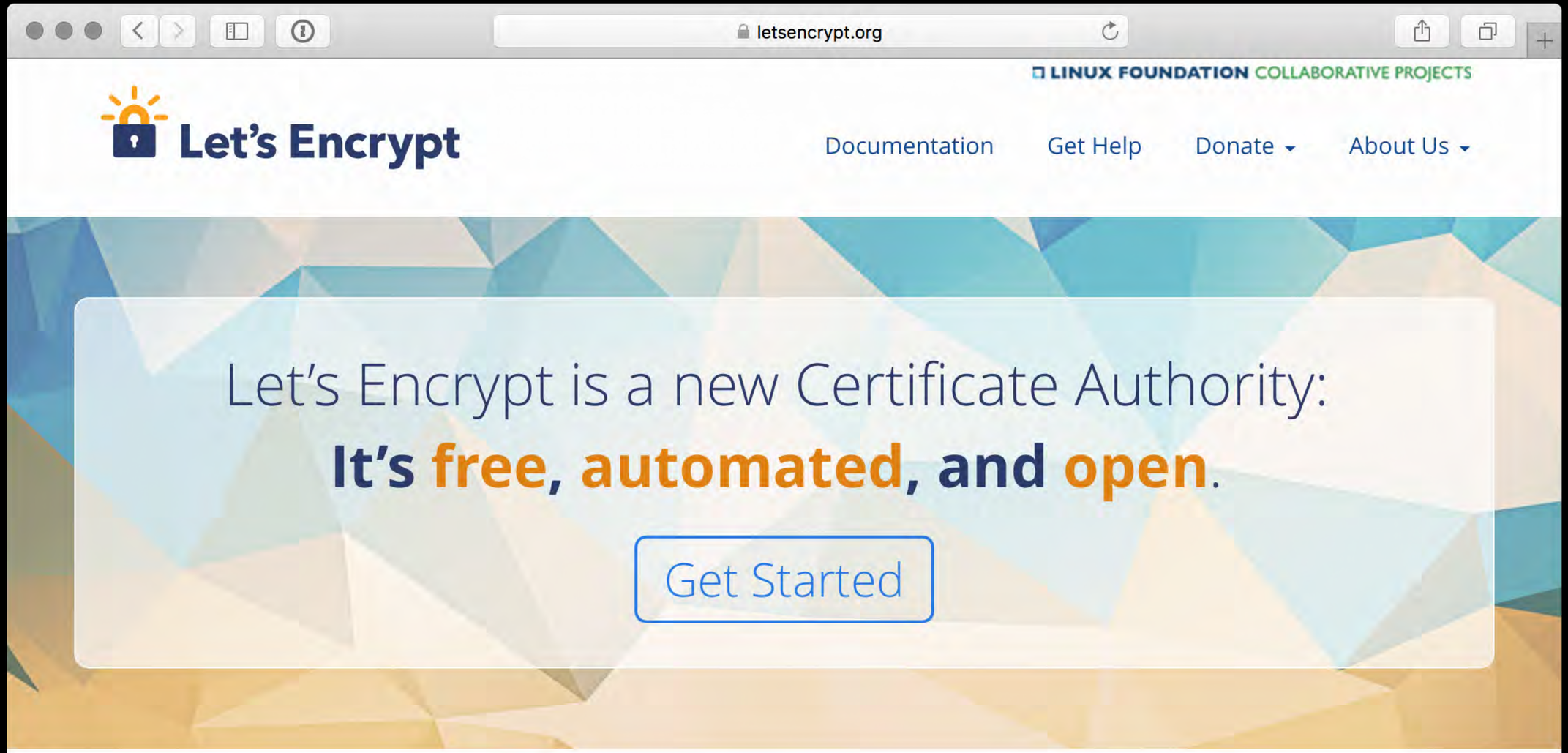
- Messages communicated via OCSP are encoded in ASN.1 over HTTP
- **OCSP servers are often also called OCSP responders** ("request/response" pattern) Signed responses signify that the certificate specified in the request is 'good', 'revoked', or 'unknown'.
- More efficient than CRLs (less bandwidth, client library code, and client resource)
- OCSP discloses to the responder that a particular network host used a particular certificate at a particular time.
- Specified in RFC6960
  https://tools.ietf.org/html/rfc6960

PKI Implementations

UNIVERSITY OF OXFORD

- Microsoft Certification Authority roles
- OpenSSL
- EJBCA
- OpenCA PKI Research Labs
- JAMF Software Server and other MDMs




letsencrypt.org
LINUX FOUNDATION COLLABORATIVE PROJECTS
Let's Encrypt
Documentation
Get Help
Donate
About Us
Let's Encrypt is a new Certificate Authority:
It's free, automated, and open.
Get Started
FROM OUR BLOG
Oct 1, 2016
ISRG Legal Transparency Report, January 2016 - June 2016
The trust of our users is ISRG's most critical asset.
MAJOR SPONSORS
mozilla
Akamai
CISCO
EFF
OVH
chrome
IdenTrust
Internet Society

Products

SSL for the Enterprise

SSL Certificates [Compare All]

- SSL Web Server Certificates with EV
- SSL Web Server Certificates
- SSL 123 Certificates
- SAN/UC Capable Certificates
- Wildcard SSL Certificates
- SSL123 Wildcard

Code Signing Certificates

Thawte Trusted Site Seal

US Home > Products > SSL Certificates

Email Share Print

SSL Certificates

Find the best SSL Certificate for your business

	SSL Web Server with EV	SSL Web Server	SSL123
Issuance Time	Most certificates issued in **1-3 days**	Most certificates issued in **one day**	Most certificates issued in **minutes**
Price: 1 year	Best for: Credit Card Transacting Websites Banks and Financial Institutions $299 BUY NOW RENEW	Best for: Enterprise Applications Business Websites $199 add wildcard + $300 BUY NOW RENEW	Best for: Securing Internal Servers Private Websites $149 add wildcard + $596 BUY NOW RENEW
Browser Display	Your business https://	https://www...	https://www...
Identity validation and customer assurance	Prominent visible assurance to increase trust and boost customer confidence	Visible assurance to customers that your website and domain are tied to your organization.	SSL encryption with padlock icon
Warranty (USD)	$1,500,000	$1,250,000	$500,000
Validity Options	1-2 years	1-3 years	1-3 years

Contact Sales

US Toll-Free:
+1 888 484 2983
US Direct:
+1 520 477 3128
South Africa:
+353 1 793 9142
Germany:
+49 69 3807 89081
France:
+33 1 57 32 42 68
UK:
+44 203 450 5486
Submit Inquiry Online

Symantec Corporation www.symantec.com/ssl-certificates/#overview

Enterprise | Small Business | Norton | Partners | Login to PartnerNet

Symantec

PRODUCTS | SERVICES | SOLUTIONS | SUPPORT CENTER | SECURITY CENTER

Website Security / SSL/TLS Certificates

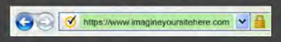
Choose the Right SSL Certificates

Chat unavailable | Support | Account Login

Choose the Right SSL Certificates

Helpful information to find the right SSL Certificates

SSL Certificates with **Visible SSL Protection**



Guard against phishing with green address bar

SSL Certificates with **Strong encryption options**

ECC, DSA and RSA Encryption options available

Wildcard SSL Certificates

Protect multiple subdomains with one certificate

Enterprise Solutions

Complete Website Security

Advantages of Symantec SSL Certificates

Symantec SSL/TLS certificates, formerly by VeriSign, uses industry-leading SSL encryption across all products, with various solutions for website and server security. Extended Validation (EV) SSL certificates will increase customers' confidence and help your website reach its full potential. Our 'Pro' SSL products offer ECC encryption, strong security on a short key length. Wildcard SSL certificate protects multiple subdomains under one SSL certificate. Compare and buy Symantec SSL Certificates here, to make sure your customers are safe from search to browse to buy.

Compare SSL Certificates

	Visible SSL Protection				
Symantec SSL Certificates	**Secure Site with EV**	**Secure Site Pro with EV**	**Secure Site**	**Secure Site Pro**	**Secure Site Wildcard**
Buy Now	BUY NOW	BUY NOW	BUY NOW	BUY NOW	BUY NOW
Renew Now	RENEW	RENEW	RENEW	RENEW	RENEW
Price: 1 year	$995	$1,499	$399	$995	$1999
Green Address Bar	✓	✓			

www.wosign.com/english/index.htm

WoSign® Making the internet more secure and trusted

(+1) 844-8-WOSIGN CHINESE

Live Chat | Partner Programs | Digital Certificate Store

Home | Products | Price | Support | News | About Us | Contact Us | My Account | Partner

Securing the Global Internet

Hi-Tech, Made in CHINA

The world-class reliable PKI system, The world-class best service team

Lists of available trusted root certificates in macOS

The macOS Trust Store contains trusted root certificates that are preinstalled with macOS.

Blocking Trust for WoSign CA Free SSL Certificate G2

Certificate Authority WoSign experienced multiple control failures in their certificate issuance processes for the WoSign CA Free SSL Certificate G2 intermediate CA. Although no WoSign root is in the list of Apple trusted roots, this intermediate CA used cross-signed certificate relationships with StartCom and Comodo to establish trust on Apple products.

In light of these findings, we are taking action to protect users in an upcoming security update. Apple products will no longer trust the WoSign CA Free SSL Certificate G2 intermediate CA.

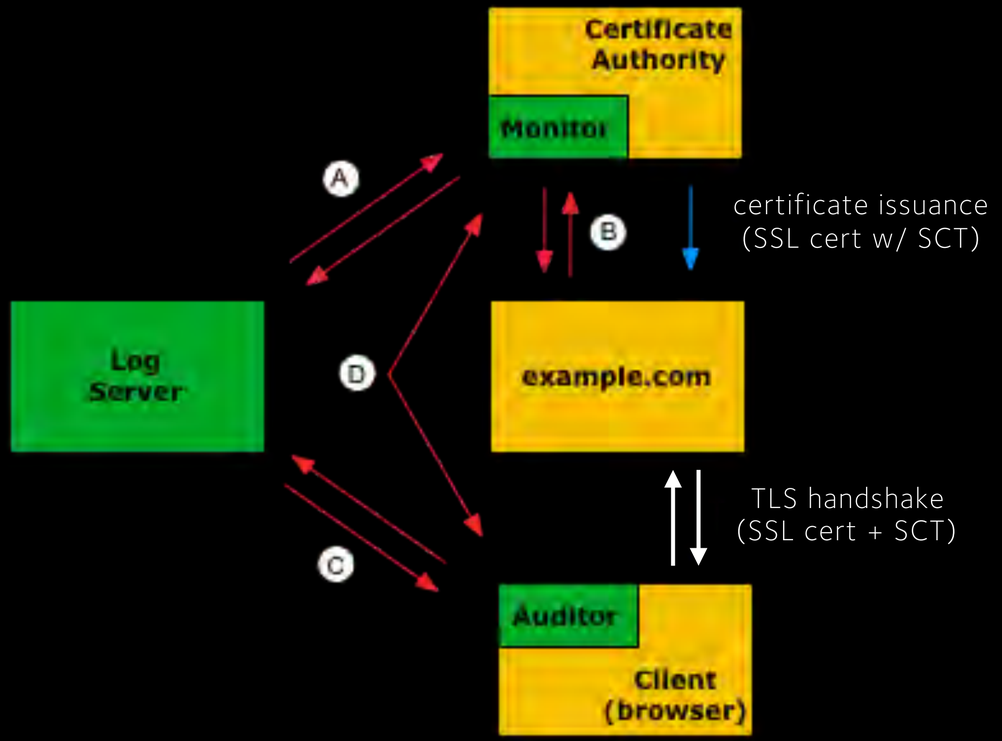
To avoid disruption to existing WoSign certificate holders and to allow their transition to trusted roots, Apple products will trust individual existing certificates issued from this intermediate CA and published to public Certificate Transparency log servers by 2016-09-19. They will continue to be trusted until they expire, are revoked, or are untrusted at Apple's discretion.

As the investigation progresses, we will take further action on WoSign/StartCom trust anchors

Certificate Transparency

UNIVERSITY OF OXFORD

- Open framework for monitoring and auditing of SSL certificates
  - detect SSL certificates that have been mistakenly issued by a CA or maliciously acquired from an otherwise unimpeachable CA
  - identify CAs that have gone rogue and are maliciously issuing certificates
- See https://www.certificate-transparency.org
- Specified in RFC6962
  https://tools.ietf.org/html/rfc6962



A Monitors watch logs for suspicious certs and verify that all logged certs are visible.

B Certificate owners query monitors to verify that nobody has logged illegitimate certs for their domain.

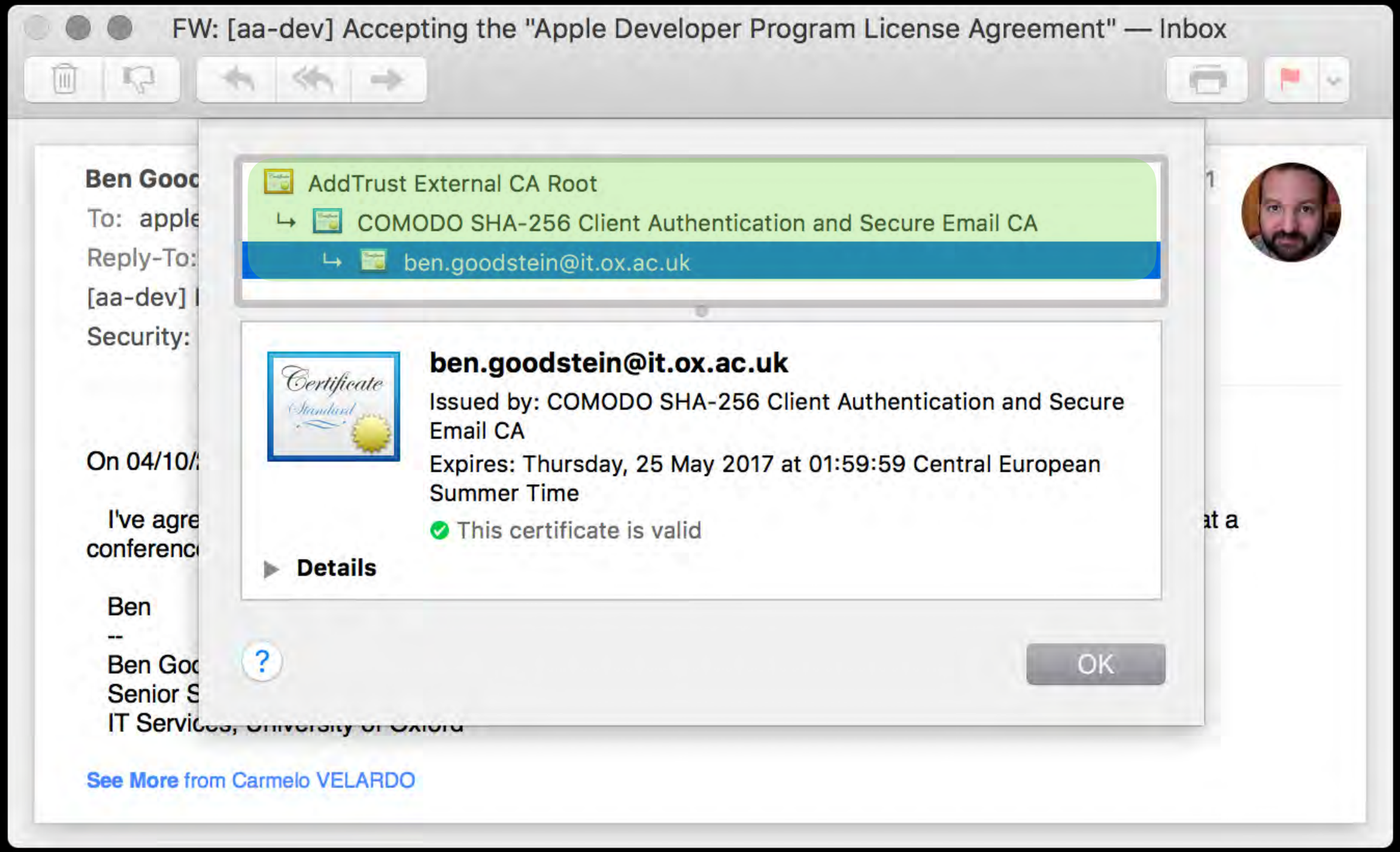
C Auditors verify that logs are behaving properly; they can also verify a particular cert has been logged.

D Monitors and auditors exchange information about logs to help detect forked or branched logs.

```
$ openssl x509 -in apple.pem -noout -text
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      4c:d7:ab:ff:b5:b3:05:6d:d6:23:f3:0a:11:1b:95:f9
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 EV SSL CA - G3
    Validity
      Not Before: Mar 28 00:00:00 2016 GMT
      Not After : Oct 15 23:59:59 2017 GMT
    Subject: 1.3.6.1.4.1.311.60.2.1.3=US/1.3.6.1.4.1.311.60.2.1.2=California/businessCategory=Private
      Organization/serialNumber=C0806592, C=US/postalCode=95014, ST=California, L=Cupertino/
      street=1 Infinite Loop, O=Apple Inc., OU=Internet Services for Akamai, CN=www.apple.com
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (2048 bit)
        Modulus (2048 bit):
          00:e8:8d:83:fe:77:01:0d:8f:e5:28:51:60:c2:02:[…]:3f:2d
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Subject Alternative Name:
        DNS:www.apple.com
      X509v3 Key Usage: critical
        Digital Signature, Key Encipherment
      X509v3 Extended Key Usage:
        TLS Web Server Authentication, TLS Web Client Authentication
```

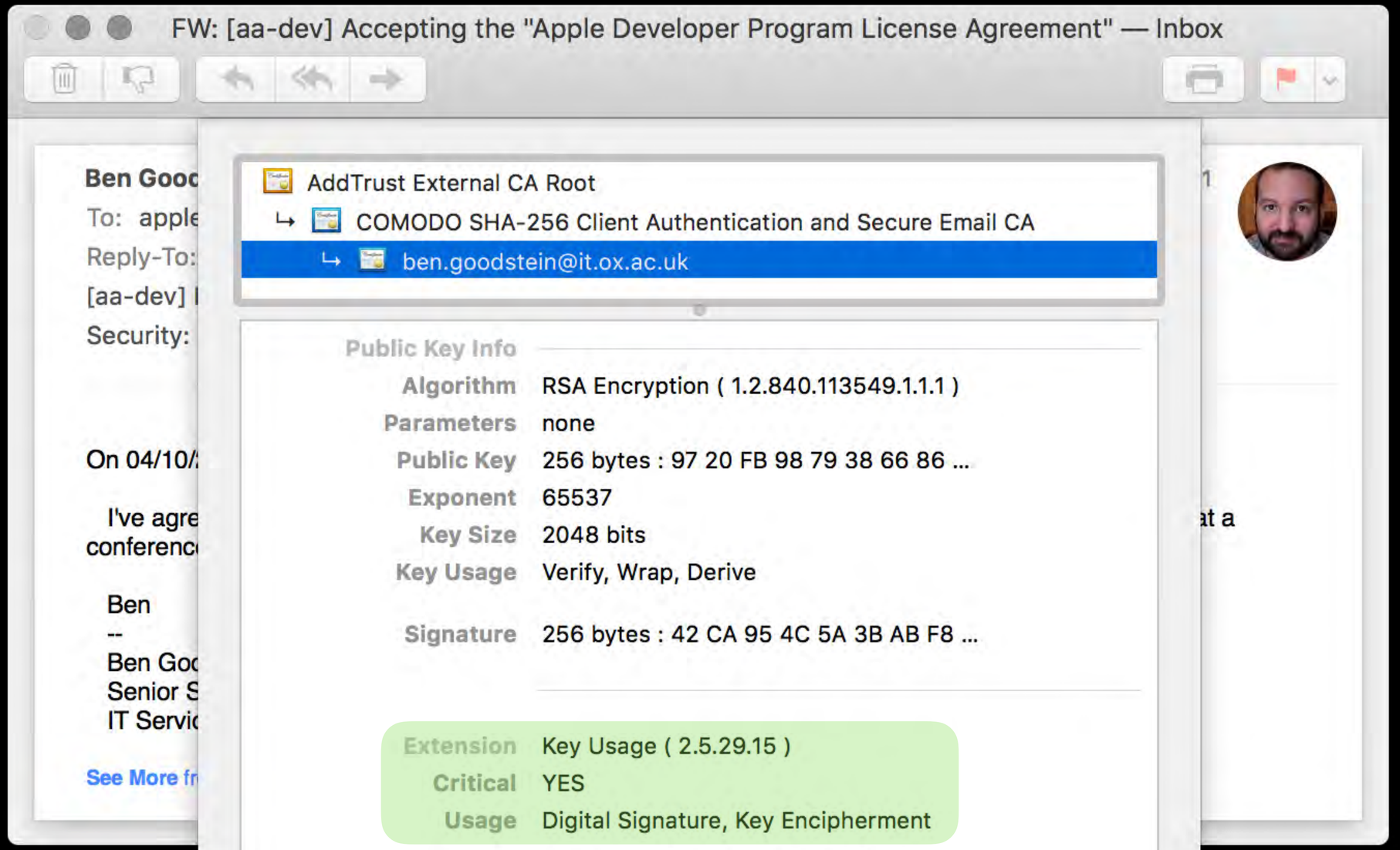
Email Signatures – S/MIME

UNIVERSITY OF OXFORD



Email Signatures – S/MIME

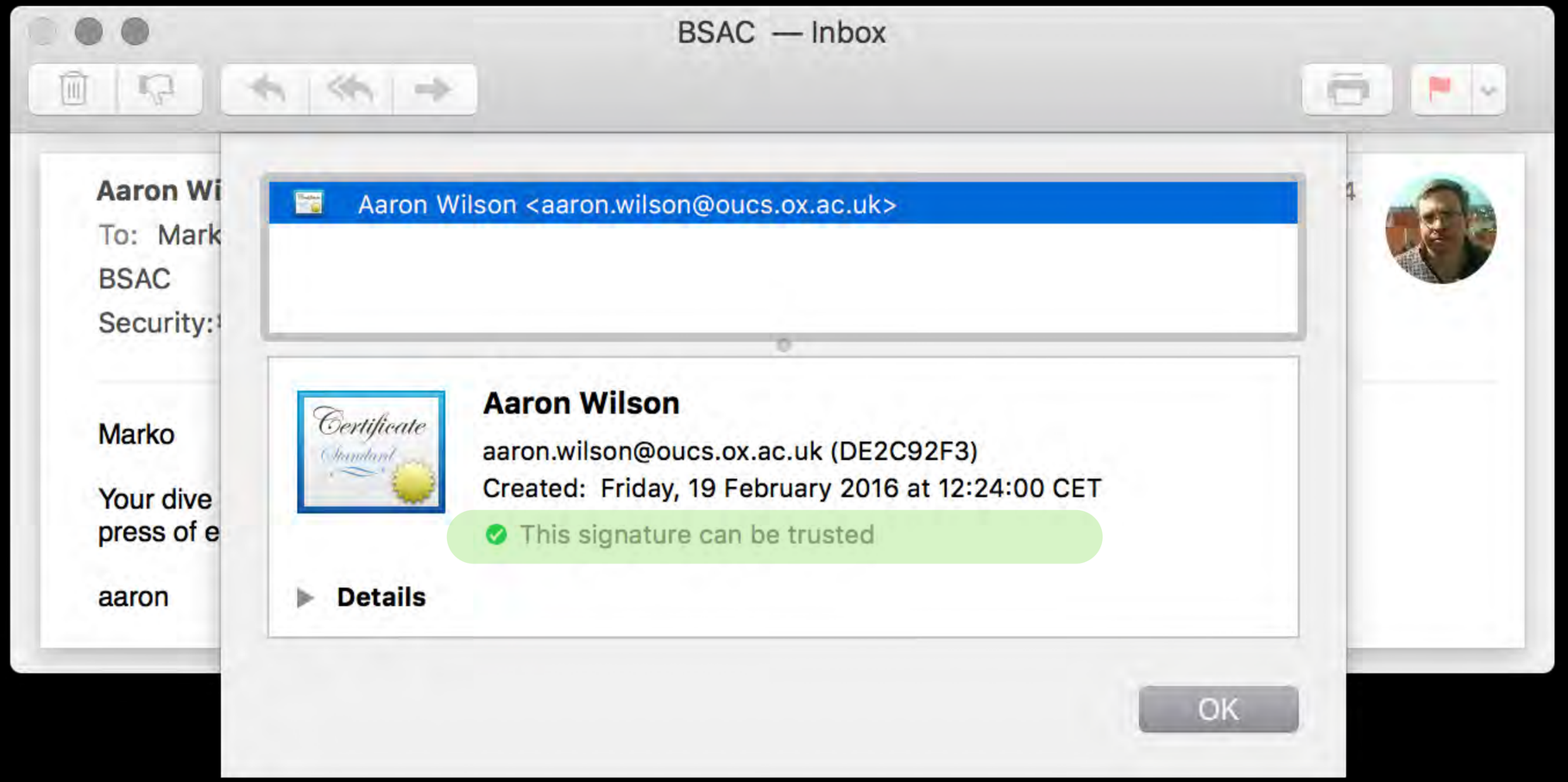
UNIVERSITY OF OXFORD




```
From: Ben Goodstein
To: Apple App Developers <apple-app-developers@maillist.ox.ac.uk>
Subject: [aa-dev] FW: Accepting the "Apple Developer Program License Agreement"
Date: Tue, 4 Oct 2016 13:31:21 +0000 […]
MIME-Version: 1.0

--B_3558439839_905099814
Content-type: text/plain;
  charset="UTF-8"
Content-transfer-encoding: 7bit

On 04/10/2016, 15:29, "Ben Goodstein" <ben.goodstein@it.ox.ac.uk> wrote:
> I've agreed to the updated terms, Marko will probably need to do the app
> transfer, we're both away at a conference so I'll bug him about it later.
>
>  Ben

[…]

--B_3558439839_905099814
Content-Type: application/pkcs7-signature; name="smime.p7s"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7s"

MIIQvwYJKoZIhvcNAQcCoIIQsDCCEKwCAQExDzANBglghkgBZQMEAgEFADALBgkqhkiG9w0B
BwGggg47MIIFSjCCBDKgAwIBAgIRAI7AiGB6QKPklqcDspN3tDcwDQYJKoZIhvcNAQELBQAw
[…] xLmGVKR02enhIZz81iiHa6xZ0+0sJPp/Hg==

--B_3558439839_905099814--
```

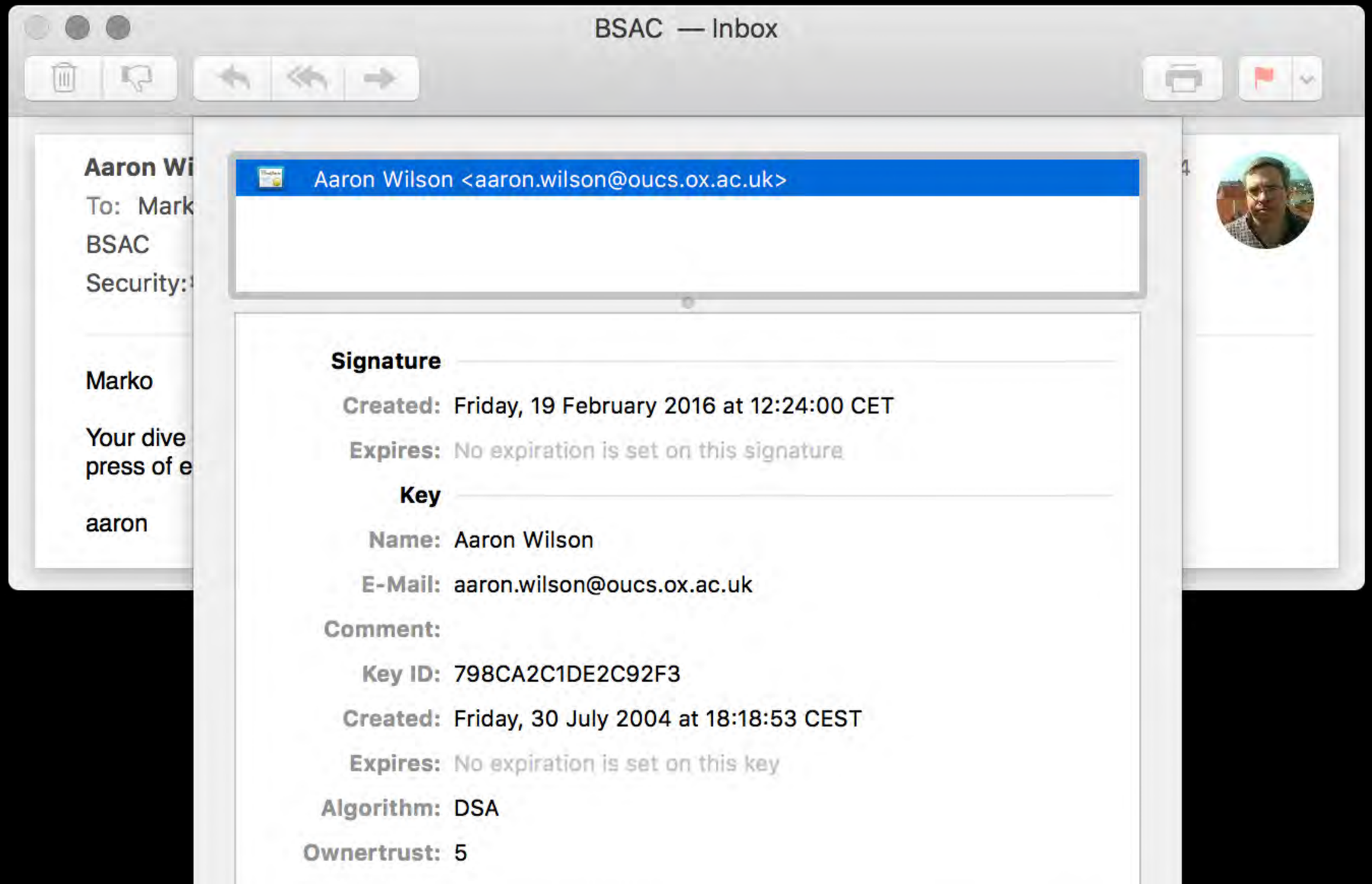
Email Signatures – OpenPGP

UNIVERSITY OF OXFORD



Email Signatures – OpenPGP

UNIVERSITY OF OXFORD



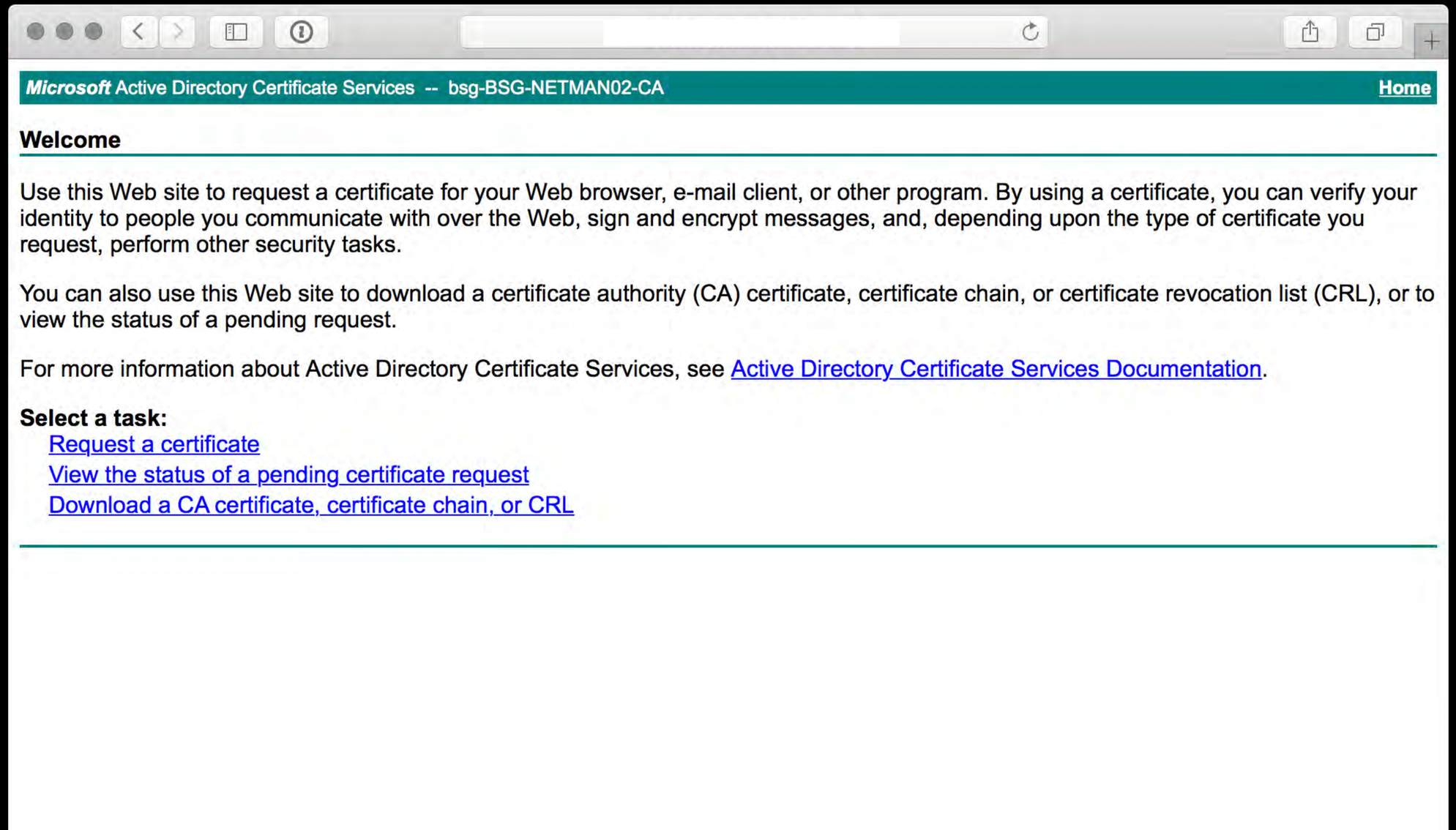
```
From: Aaron Wilson
To: Marko Jung <marko.jung@it.ox.ac.uk>
Date: Fri, 19 Feb 2016 11:24:00 +0000
Subject: BSAC […]
MIME-Version: 1.0

--OROCMA9jn6tkzFBc
Content-Type: text/plain; charset=us-ascii
Content-Disposition: inline

Marko

Your dive packs have arrived; would you like them delivered to Rickty
press of elsewhere ?

aaron

--OROCMA9jn6tkzFBc
Content-Type: application/pgp-signature; name="signature.asc"
Content-Description: Digital signature

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1

iEYEARECAAYFAlbG+1AACgkQeYyiwd4skvNYKQCggwuxTgwalBG/7r/IkxxUnH1j
hBkAn0GSi/9IjD3QgJOtwDUQZcx+gyF7
=HQFH
-----END PGP SIGNATURE-----

--OROCMA9jn6tkzFBc--
```

UNIVERSITY OF OXFORD

https://gpgtools.org/

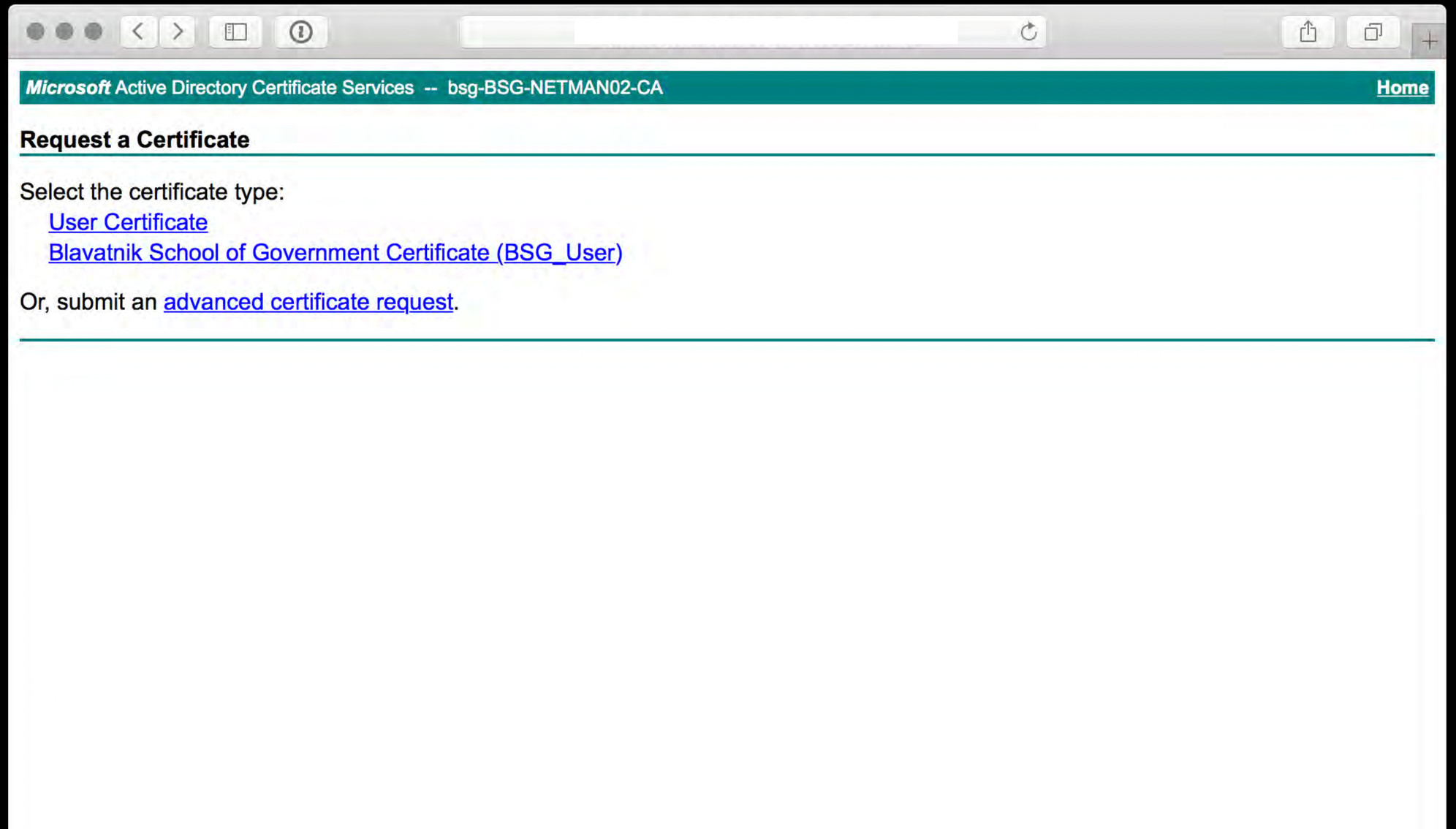
Example: obtaining a Certificate

UNIVERSITY OF OXFORD



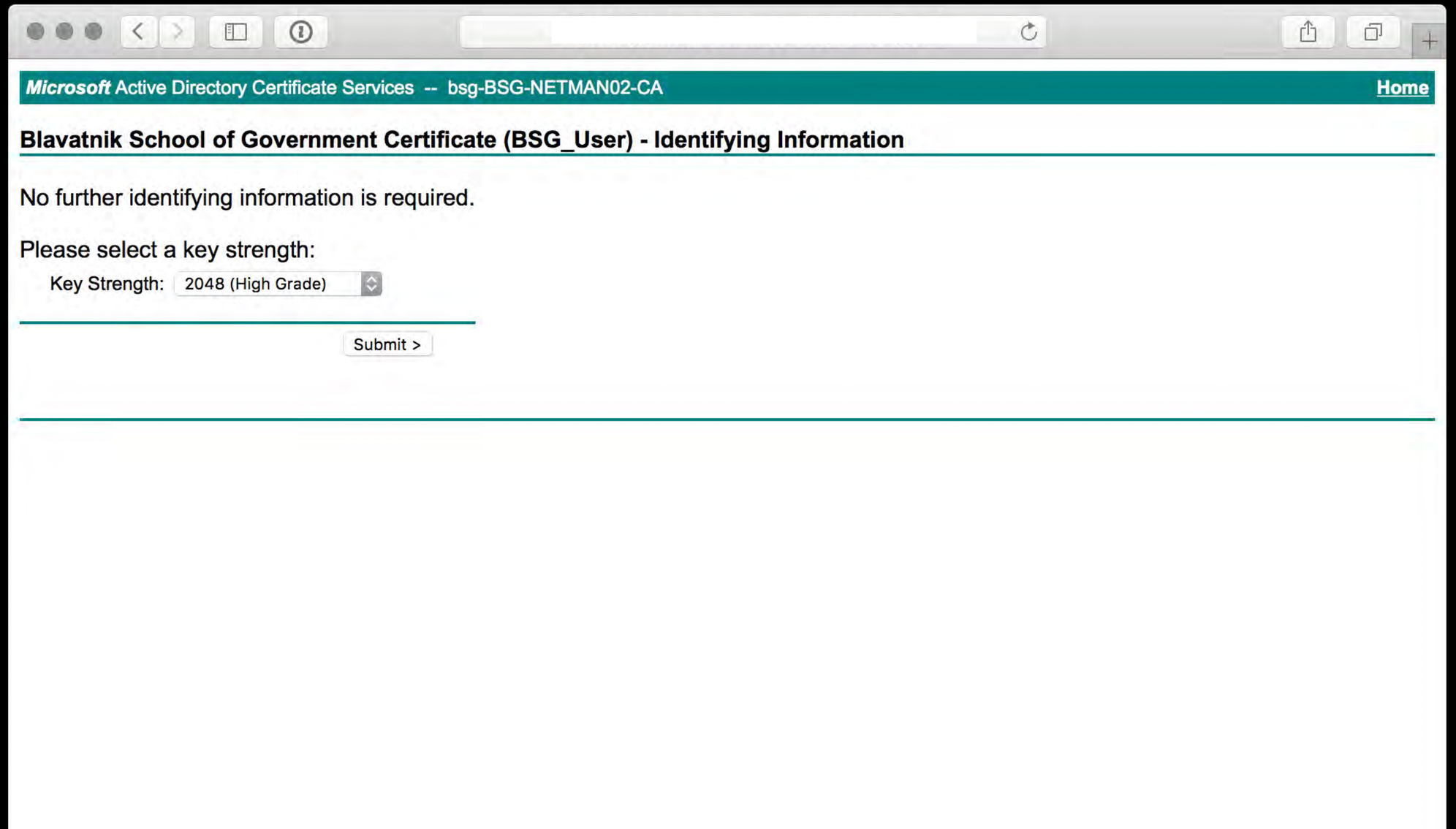
Example: obtaining a Certificate

UNIVERSITY OF OXFORD



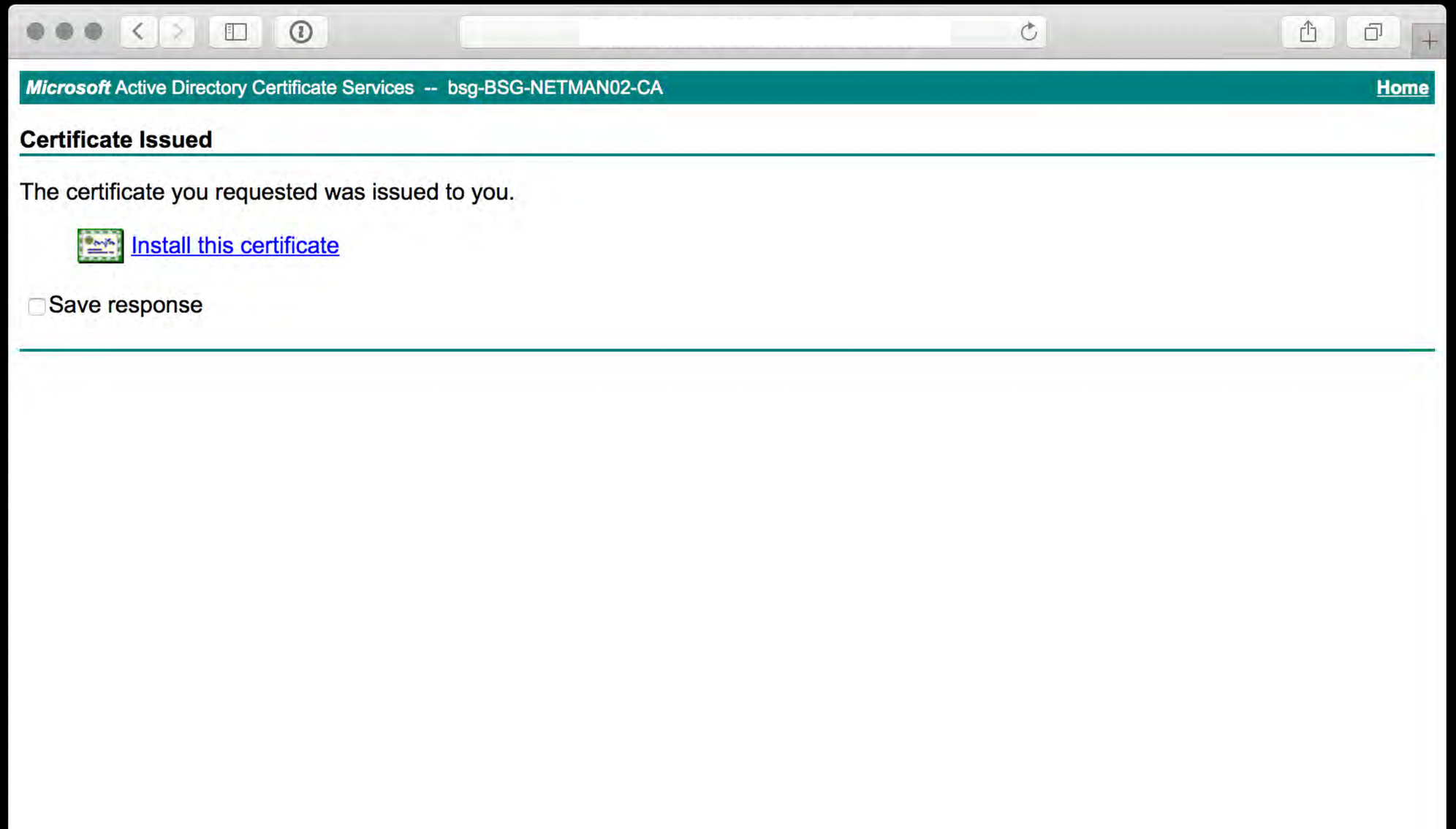
Example: obtaining a Certificate

UNIVERSITY OF OXFORD

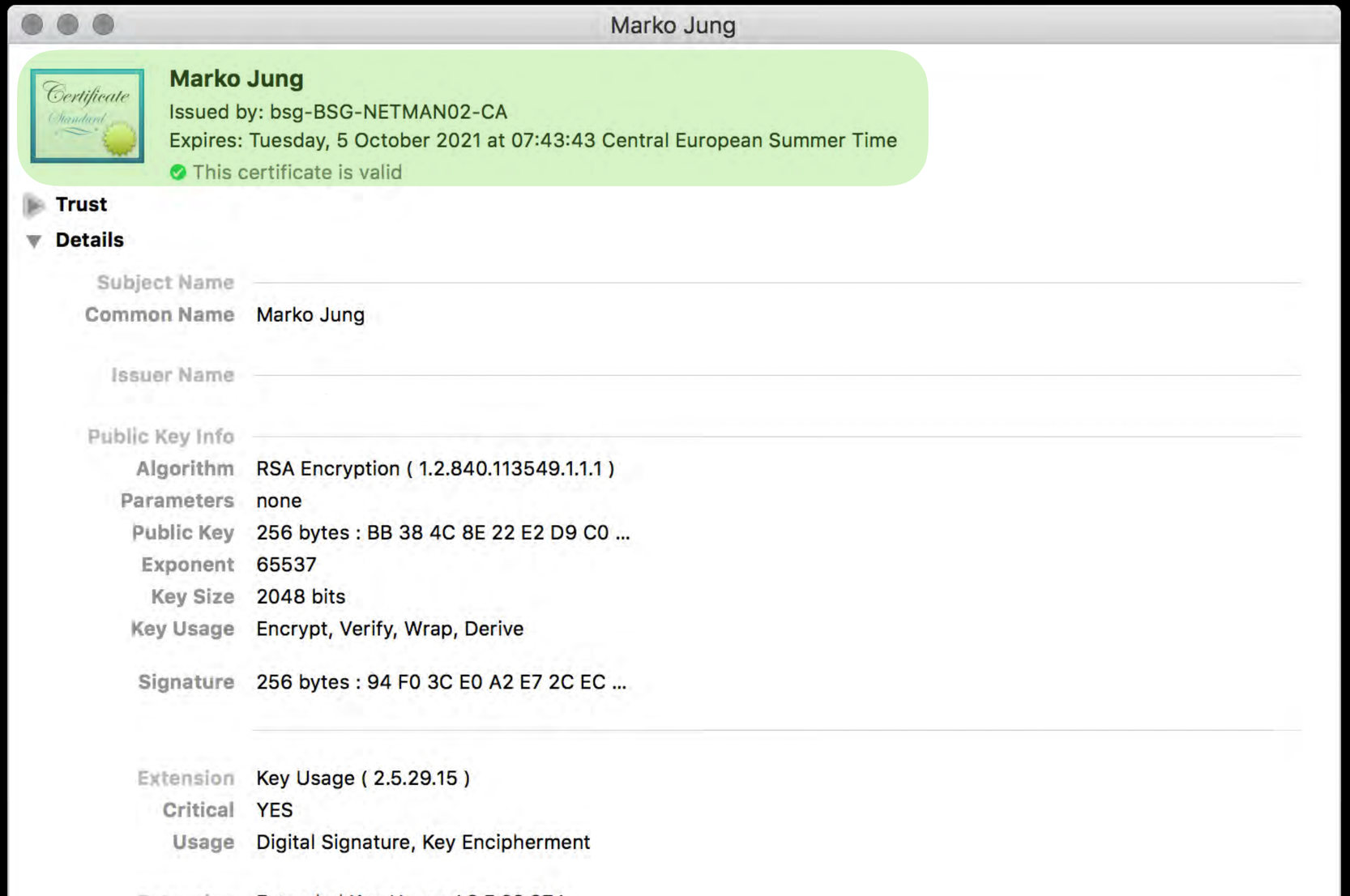


Example: obtaining a Certificate

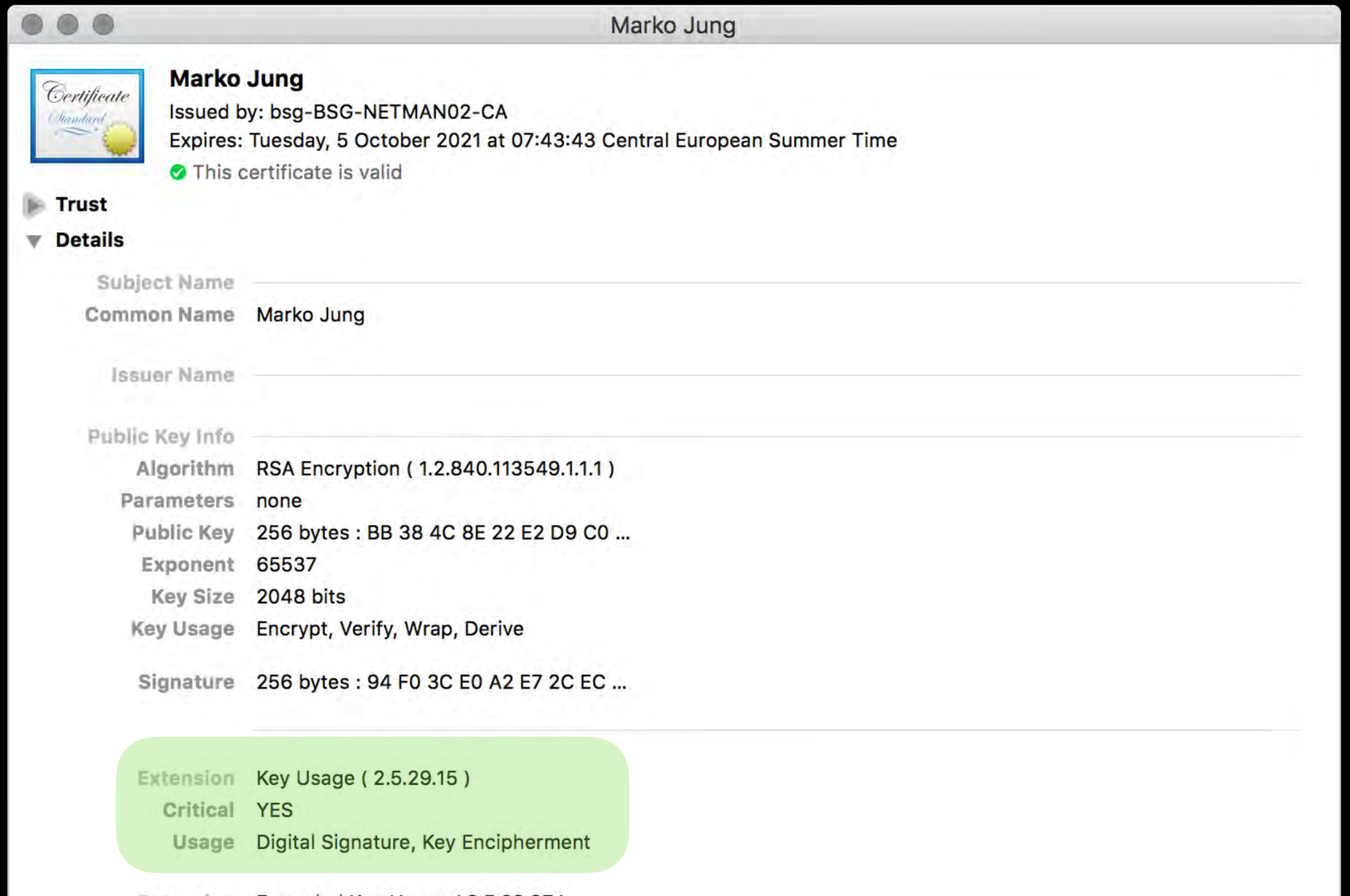
UNIVERSITY OF OXFORD



UNIVERSITY OF OXFORD

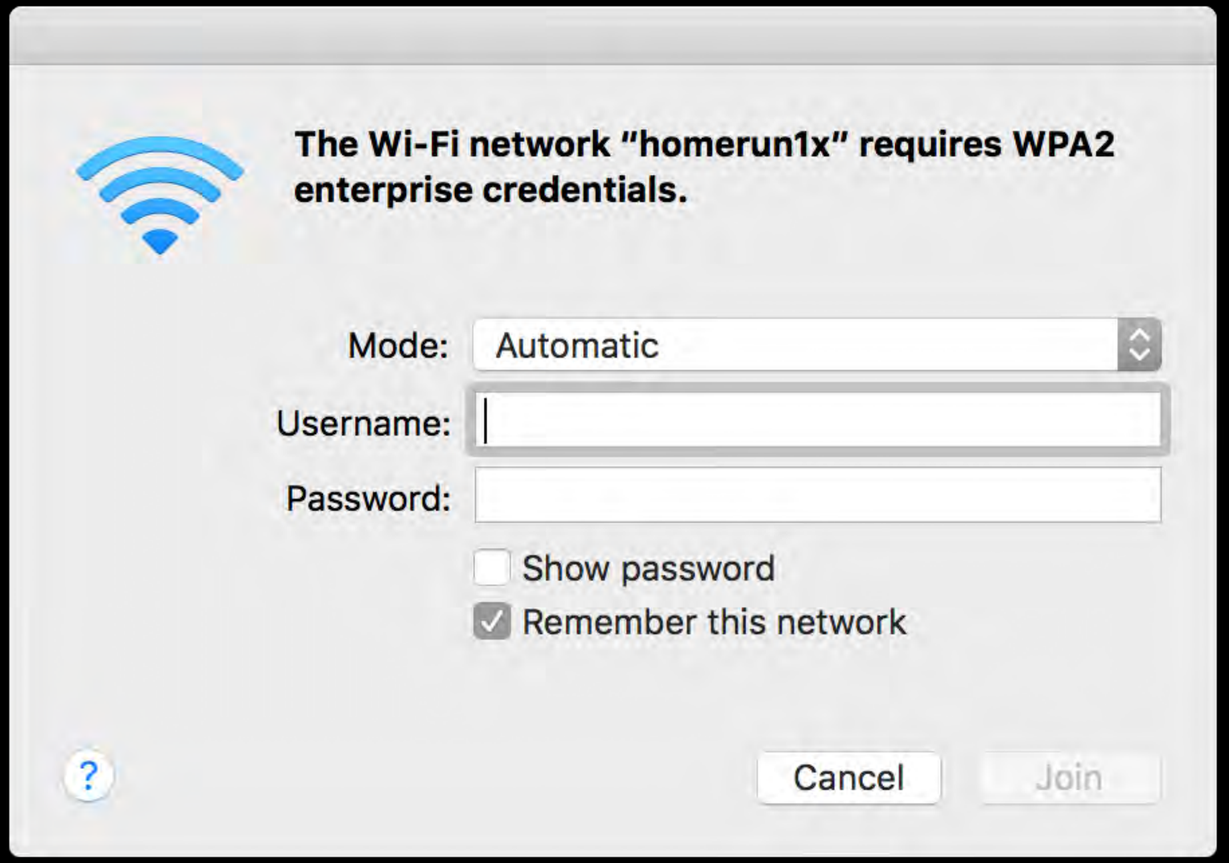


UNIVERSITY OF OXFORD



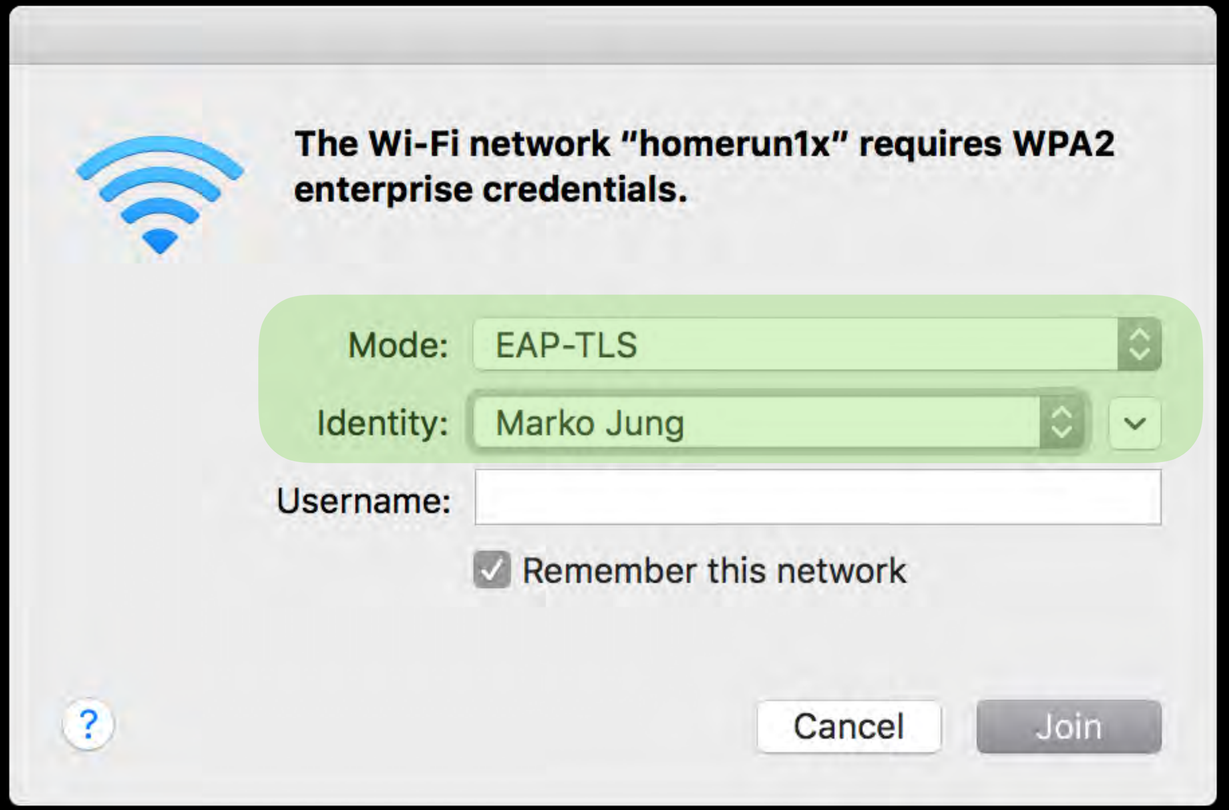
Client Authentication

UNIVERSITY OF OXFORD



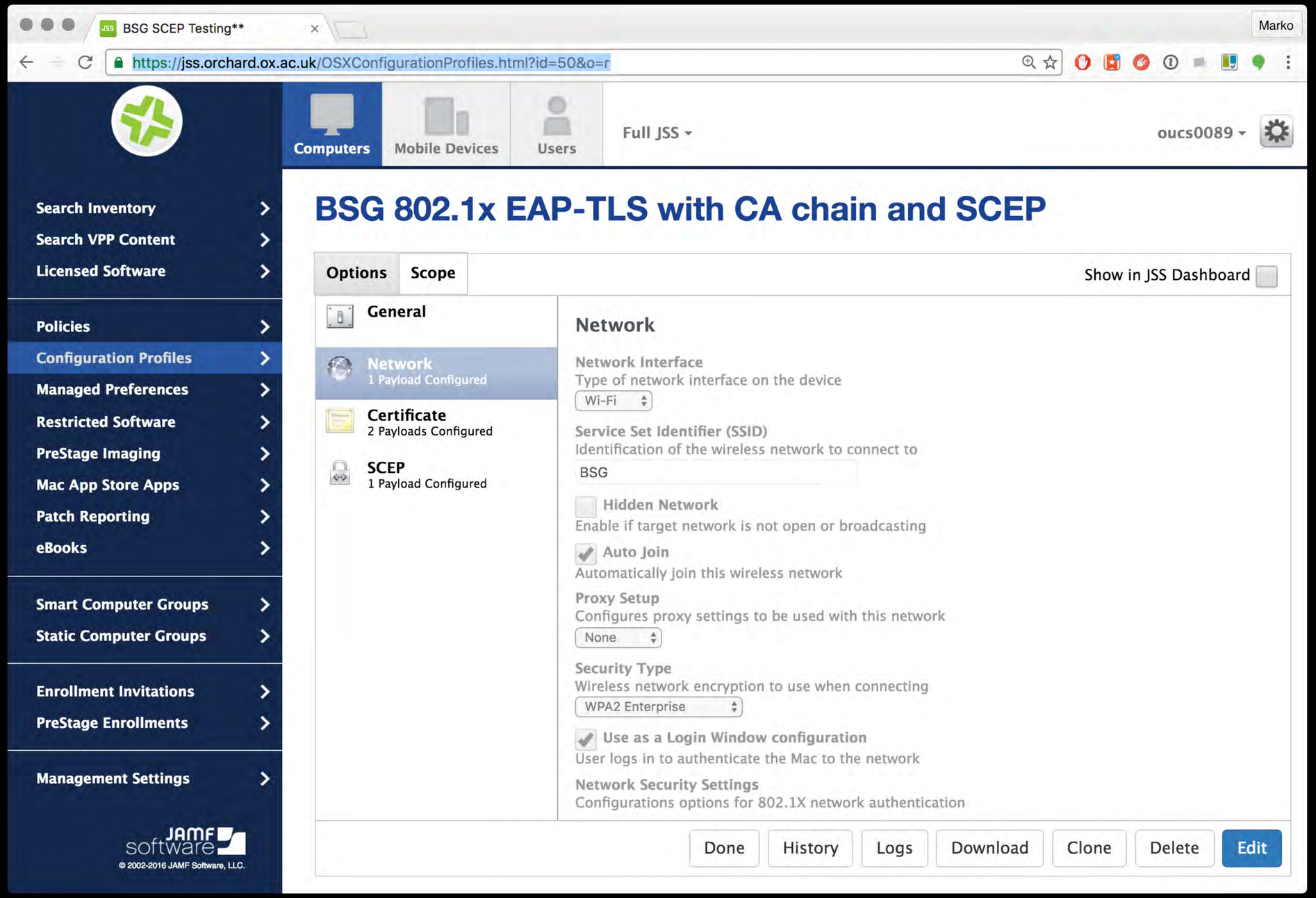
Client Authentication

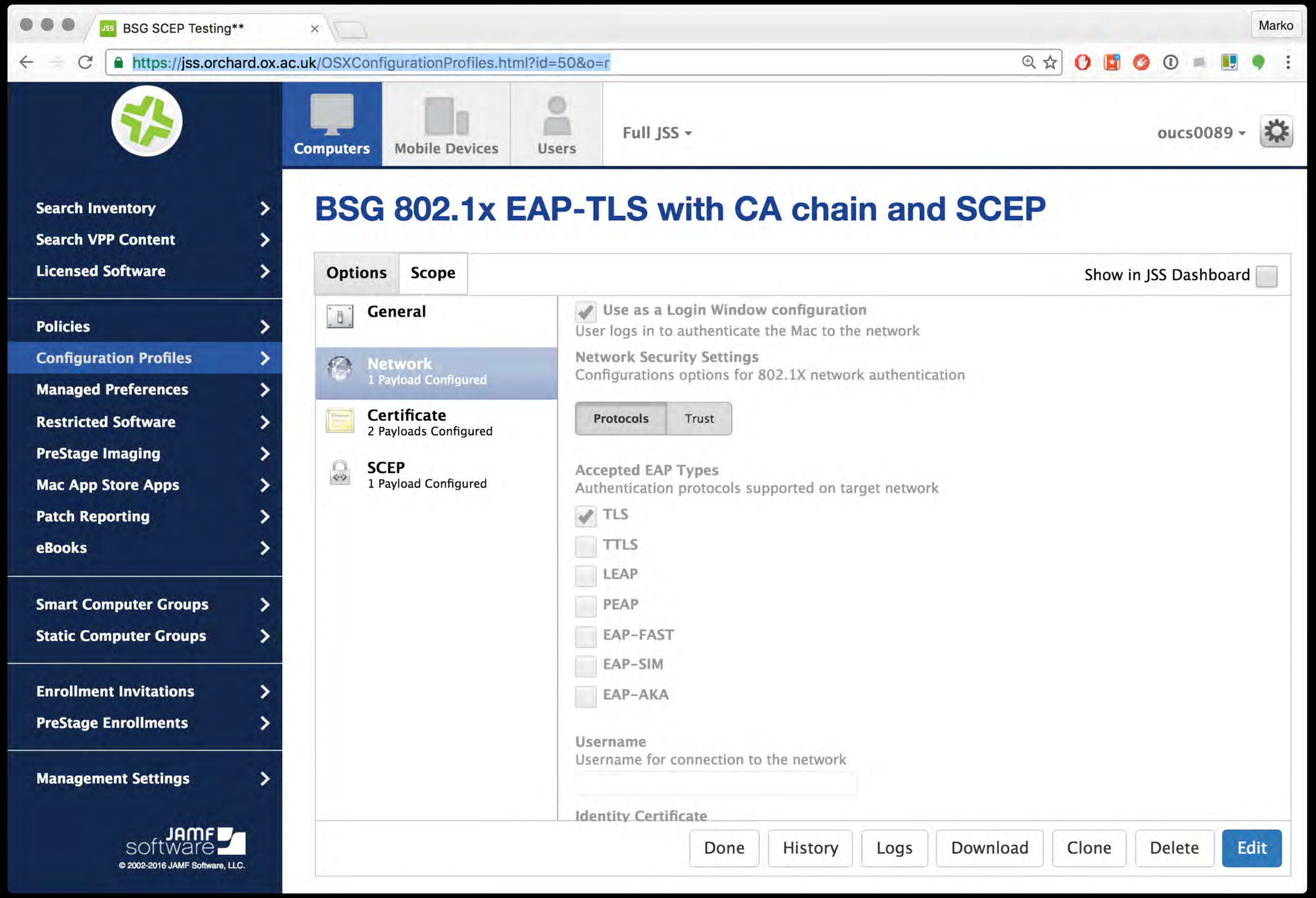
UNIVERSITY OF OXFORD

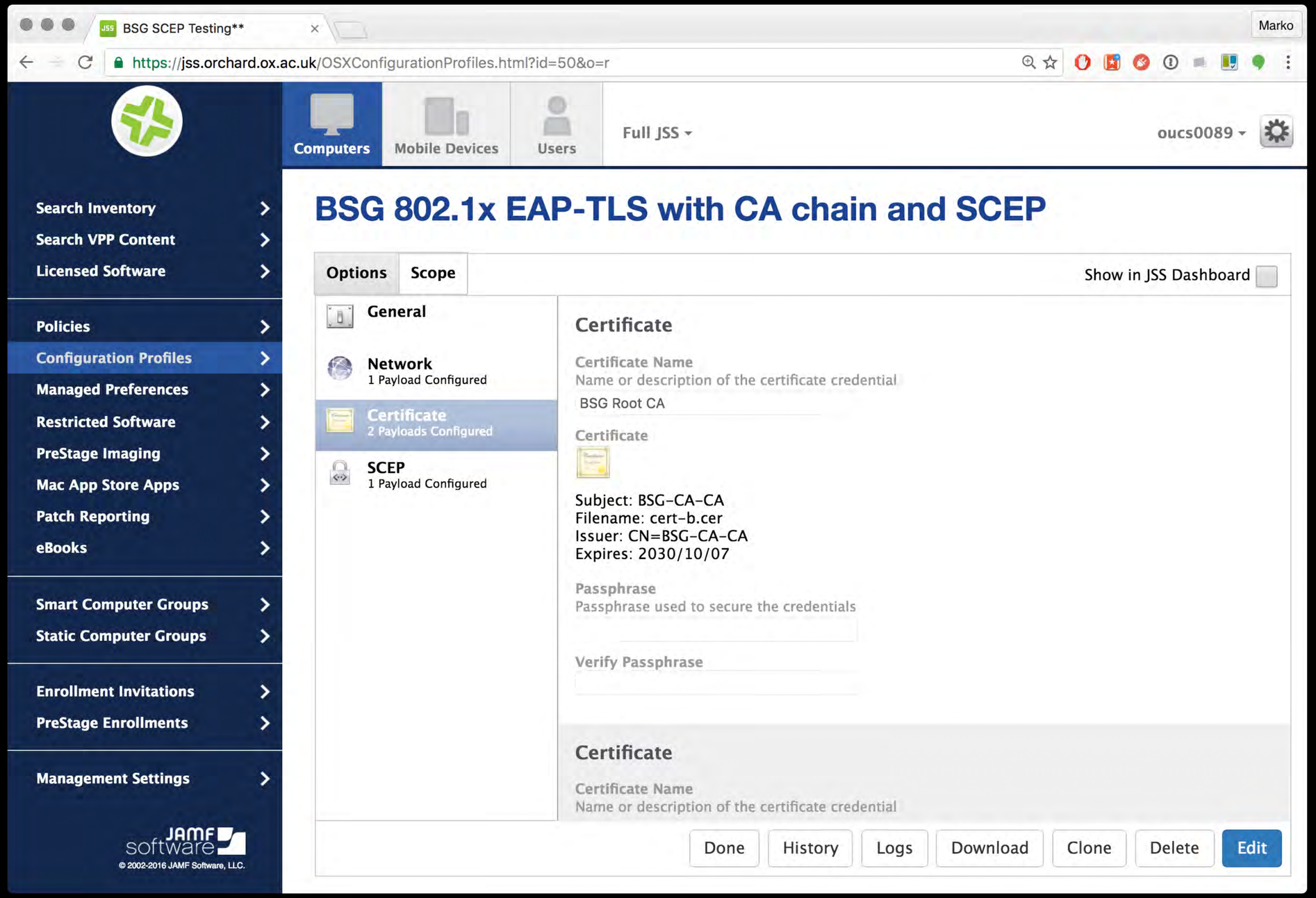


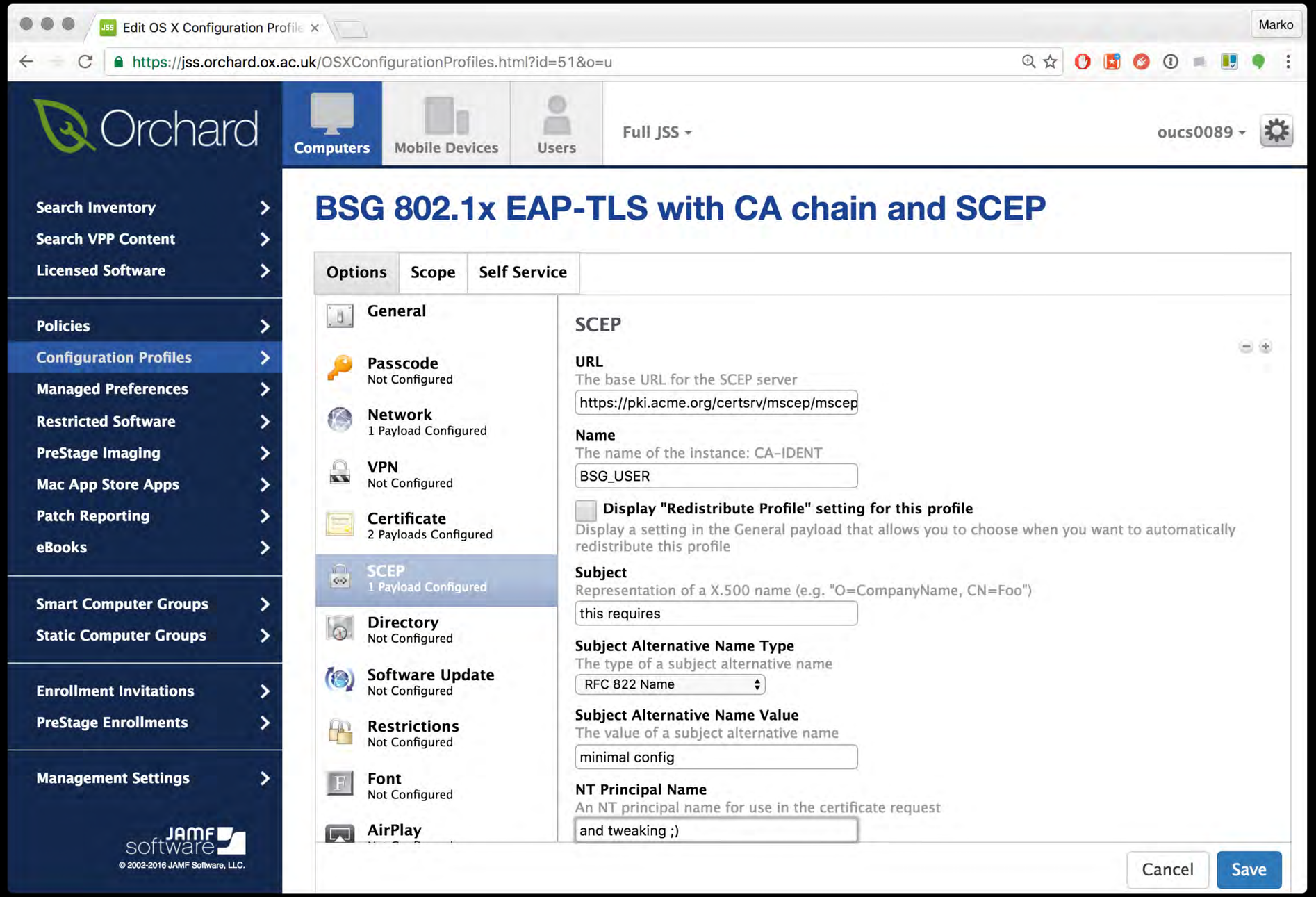

LIKELIHOOD YOU WILL GET CODE WORKING BASED ON HOW YOU'RE SUPPOSED TO INSTALL IT:
VERY LIKELY
APP STORE OR PACKAGE MANAGER
GITHUB LINK
SOURCEFORGE LINK
GEOCITIES/TRIPOD LINK
COPY-AND-PASTE EXAMPLE CODE FROM PAPER'S APPENDIX
ANYTHING THAT "REQUIRES ONLY MINIMAL CONFIGURATION AND TWEAKING"
UNLIKELY


NOT AN EXPERT?
PAY ONE!


BSG SCEP Testing**
Marko
https://jss.orchard.ox.ac.uk/OSXConfigurationProfiles.html?id=50&o=r
Computers
Mobile Devices
Users
Full JSS
oucs0089
Search Inventory
Search VPP Content
Licensed Software
Policies
Configuration Profiles
Managed Preferences
Restricted Software
PreStage Imaging
Mac App Store Apps
Patch Reporting
eBooks
Smart Computer Groups
Static Computer Groups
Enrollment Invitations
PreStage Enrollments
Management Settings
JAMF software
© 2002-2016 JAMF Software, LLC.
BSG 802.1x EAP-TLS with CA chain and SCEP
Options
Scope
Show in JSS Dashboard
General
Network
1 Payload Configured
Certificate
2 Payloads Configured
SCEP
1 Payload Configured
Network
Network Interface
Type of network interface on the device
Wi-Fi
Service Set Identifier (SSID)
Identification of the wireless network to connect to
BSG
Hidden Network
Enable if target network is not open or broadcasting
Auto Join
Automatically join this wireless network
Proxy Setup
Configures proxy settings to be used with this network
None
Security Type
Wireless network encryption to use when connecting
WPA2 Enterprise
Use as a Login Window configuration
User logs in to authenticate the Mac to the network
Network Security Settings
Configurations options for 802.1X network authentication
Done
History
Logs
Download
Clone
Delete
Edit


BSG SCEP Testing**
Marko
https://jss.orchard.ox.ac.uk/OSXConfigurationProfiles.html?id=50&o=r
Computers
Mobile Devices
Users
Full JSS
oucs0089
Search Inventory
Search VPP Content
Licensed Software
Policies
Configuration Profiles
Managed Preferences
Restricted Software
PreStage Imaging
Mac App Store Apps
Patch Reporting
eBooks
Smart Computer Groups
Static Computer Groups
Enrollment Invitations
PreStage Enrollments
Management Settings
JAMF software
© 2002-2016 JAMF Software, LLC.
BSG 802.1x EAP-TLS with CA chain and SCEP
Options
Scope
Show in JSS Dashboard
General
Network
1 Payload Configured
Certificate
2 Payloads Configured
SCEP
1 Payload Configured
Use as a Login Window configuration
User logs in to authenticate the Mac to the network
Network Security Settings
Configurations options for 802.1X network authentication
Protocols
Trust
Accepted EAP Types
Authentication protocols supported on target network
TLS
TTLS
LEAP
PEAP
EAP-FAST
EAP-SIM
EAP-AKA
Username
Username for connection to the network
Identity Certificate
Done
History
Logs
Download
Clone
Delete
Edit


BSG SCEP Testing**
Marko
https://jss.orchard.ox.ac.uk/OSXConfigurationProfiles.html?id=50&o=r
Computers
Mobile Devices
Users
Full JSS
oucs0089
Search Inventory
Search VPP Content
Licensed Software
Policies
Configuration Profiles
Managed Preferences
Restricted Software
PreStage Imaging
Mac App Store Apps
Patch Reporting
eBooks
Smart Computer Groups
Static Computer Groups
Enrollment Invitations
PreStage Enrollments
Management Settings
JAMF software
© 2002-2016 JAMF Software, LLC.
BSG 802.1x EAP-TLS with CA chain and SCEP
Options
Scope
Show in JSS Dashboard
General
Network
1 Payload Configured
Certificate
2 Payloads Configured
SCEP
1 Payload Configured
Certificate
Certificate Name
Name or description of the certificate credential
BSG Root CA
Certificate
Subject: BSG-CA-CA
Filename: cert-b.cer
Issuer: CN=BSG-CA-CA
Expires: 2030/10/07
Passphrase
Passphrase used to secure the credentials
Verify Passphrase
Certificate
Certificate Name
Name or description of the certificate credential
Done
History
Logs
Download
Clone
Delete
Edit


Edit OS X Configuration Profile
Marko
https://jss.orchard.ox.ac.uk/OSXConfigurationProfiles.html?id=51&o=u
Orchard
Computers
Mobile Devices
Users
Full JSS
oucs0089
Search Inventory
Search VPP Content
Licensed Software
Policies
Configuration Profiles
Managed Preferences
Restricted Software
PreStage Imaging
Mac App Store Apps
Patch Reporting
eBooks
Smart Computer Groups
Static Computer Groups
Enrollment Invitations
PreStage Enrollments
Management Settings
JAMF software
© 2002-2016 JAMF Software, LLC.
BSG 802.1x EAP-TLS with CA chain and SCEP
Options
Scope
Self Service
General
Passcode
Not Configured
Network
1 Payload Configured
VPN
Not Configured
Certificate
2 Payloads Configured
SCEP
1 Payload Configured
Directory
Not Configured
Software Update
Not Configured
Restrictions
Not Configured
Font
Not Configured
AirPlay
SCEP
URL
The base URL for the SCEP server
https://pki.acme.org/certsrv/mscep/mscep
Name
The name of the instance: CA-IDENT
BSG_USER
Display "Redistribute Profile" setting for this profile
Display a setting in the General payload that allows you to choose when you want to automatically redistribute this profile
Subject
Representation of a X.500 name (e.g. "O=CompanyName, CN=Foo")
this requires
Subject Alternative Name Type
The type of a subject alternative name
RFC 822 Name
Subject Alternative Name Value
The value of a subject alternative name
minimal config
NT Principal Name
An NT principal name for use in the certificate request
and tweaking ;)
Cancel
Save

Simple Certificate Enrolment Protocol

- Aims to make the issuing of digital certificates as scalable as possible

- Simplistic request/response format over HTTP (preferably with TLS).
  Responses are returned as standard HTTP content, with a Content-Type, e.g.

  `application/x-x509-ca-cert`
  in response to the GetCACert operation, DER-encoderd X.509 CA cert)

- Features:
  - Initial Enrolment
  - Renewal (including client key rollover)
  - CA and Client Certificate retrieval
  - CA key and certificate rollover

See also http://www.ietf.org/proceedings/69/slides/pkix-3.pdf

Further Reading

Bruce Schneier: Applied Cryptography,

John Wiley & Sons; 2nd revised edition (16 Nov. 1995)

Apple Developer Library: Cryptography Concepts In Depth

https://developer.apple.com/library/content/documentation/Security/Conceptual/cryptoservices/CryptographyConcepts/CryptographyConcepts.html

Apple Technical White Paper: 802.1X Authentication

http://training.apple.com/pdf/WP_8021X_Authentication.pdf

Thank You!


https://github.com/mjung/publications

Marko Jung


m@mju.ng


@mjung


fb.com/markohjung

http://mju.ng/give