

# Digital Certificates

Introduction

Authentication Methods

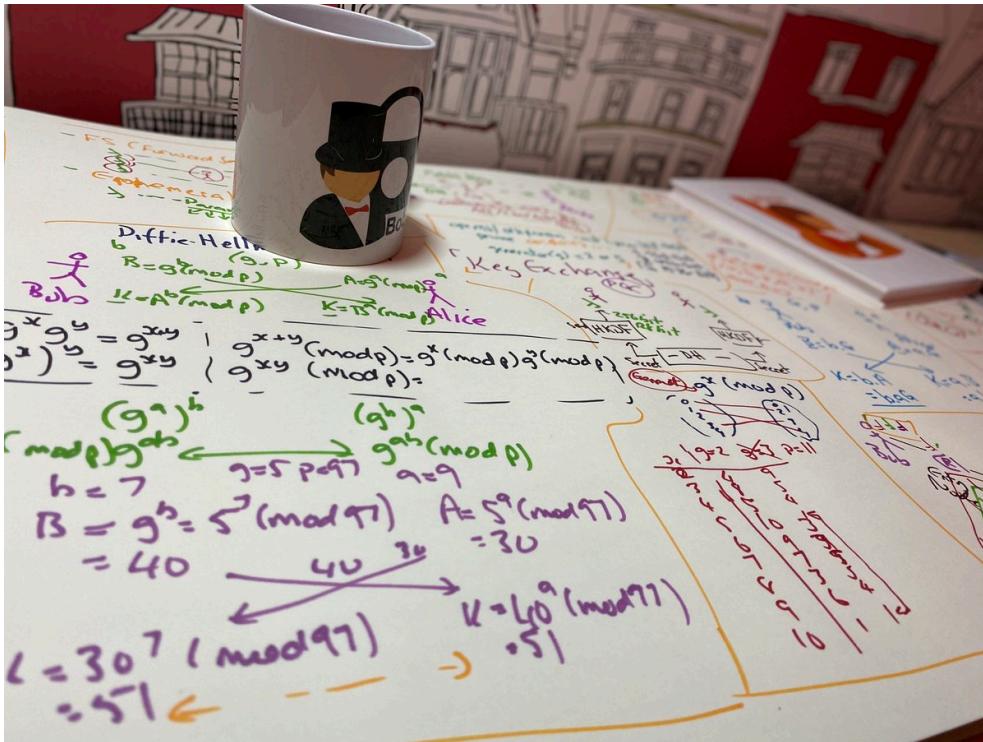
Public Key Infrastructures

Digital Certificate Passing

Digital Signatures

**Prof Bill Buchanan OBE**

<https://asecuritysite.com/digitalcert/>





# Identity on the Internet

Identifies it is trusted  
(Digital Certificate)

Keeps communications  
secure (encryption)

A screenshot of a Firefox browser window displaying a secure connection to [paypal.com](https://www.paypal.com/uk/webapps/mpp/home-merchant). The address bar shows a lock icon and the URL `https://www.paypal.com/uk/webapps/mpp/home-merchant`. A callout box from a character named Bob points to the digital certificate information in the status bar, which reads: "You are connected to **paypal.com** which is run by **PayPal, Inc.** San Jose California, US Verified by: VeriSign, Inc." Another callout box from a character named Trent points to the padlock icon in the status bar, indicating a secure connection. The main content area of the browser shows a promotional message: "However you do business, PayPal gets you paid. Choose your payment solution, you can switch any time." Below this, there is a button for "Accept card payments anywhere with PayPal Here™" and a link to "Learn More".

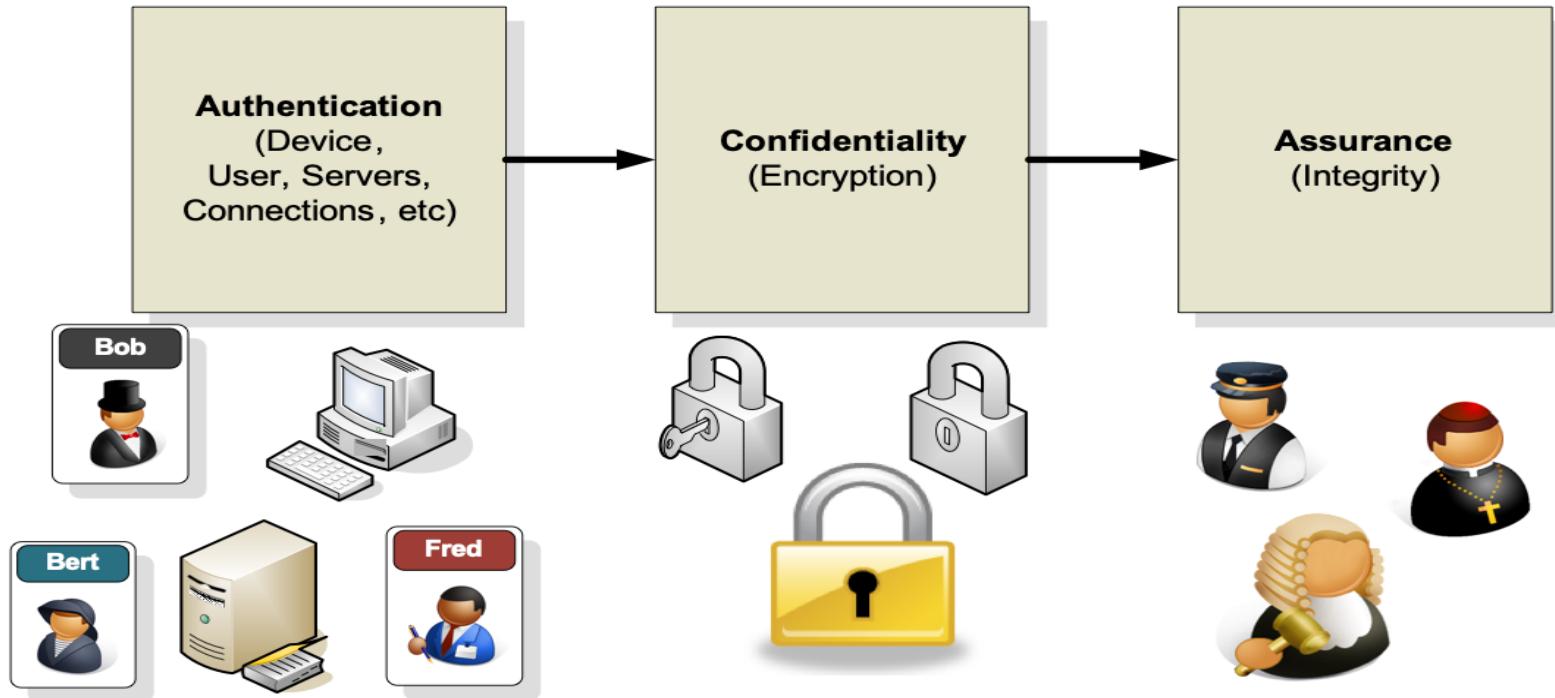
Bob

Eve

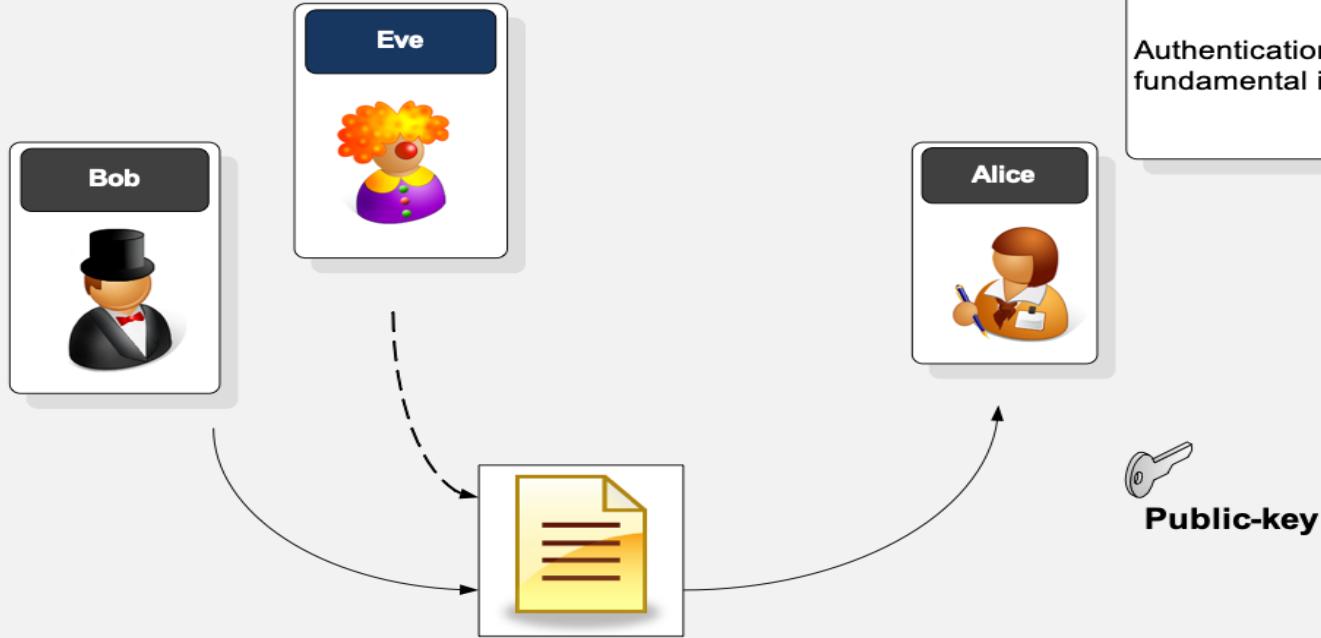
Learn More

## Fundamental principles

Authentication.  
Confidence/Assurance.  
Privacy/Confidentiality.

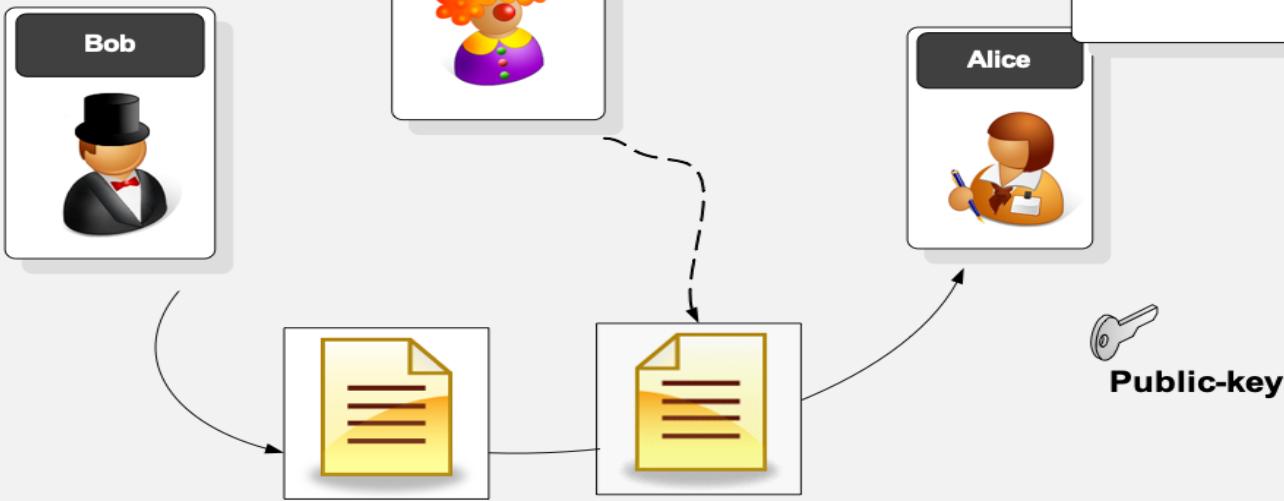


Authentication is a fundamental issue in security.



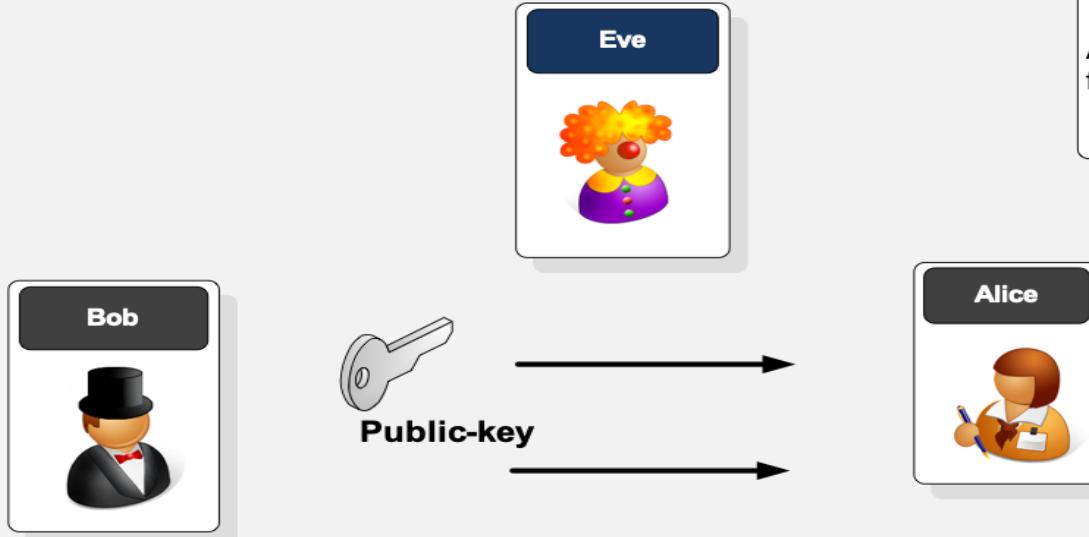
**How do we know that it was really Bob who sent the data , as anyone can get Alice's public key , and thus pretend to be Bob?**

Authentication is a fundamental issue in security.

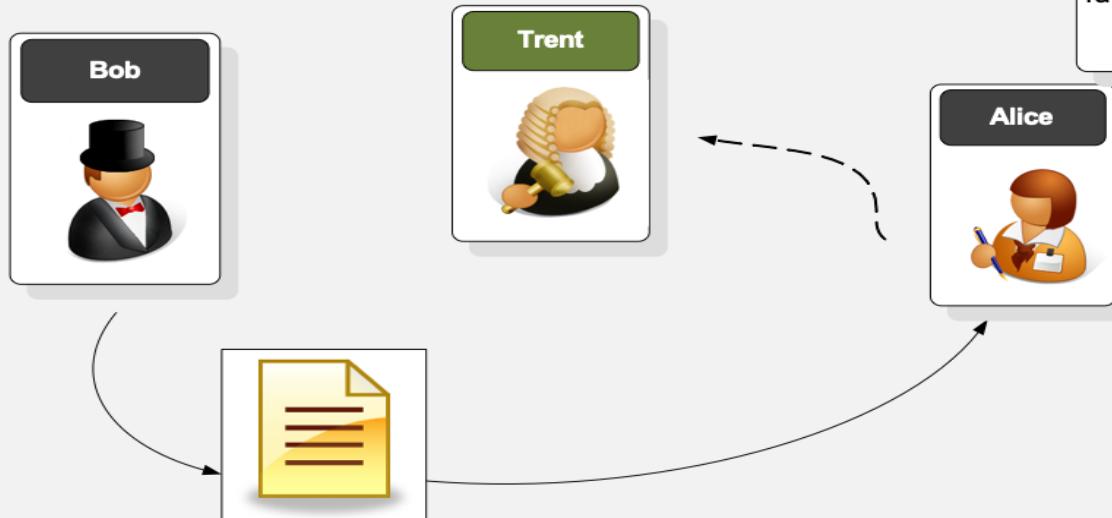


**How can we tell that the message has not been tampered with ?**

Authentication is a fundamental issue in security

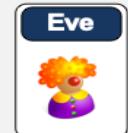


**How does Bob distribute his public key to Alice, without having to post it onto a Web site or for Bob to be on-line when Alice reads the message?**



Authentication is a fundamental issue in security.

**Who can we *really* trust to properly authenticate Bob? Obviously we can't trust Bob to authenticate that he really is Bob.**



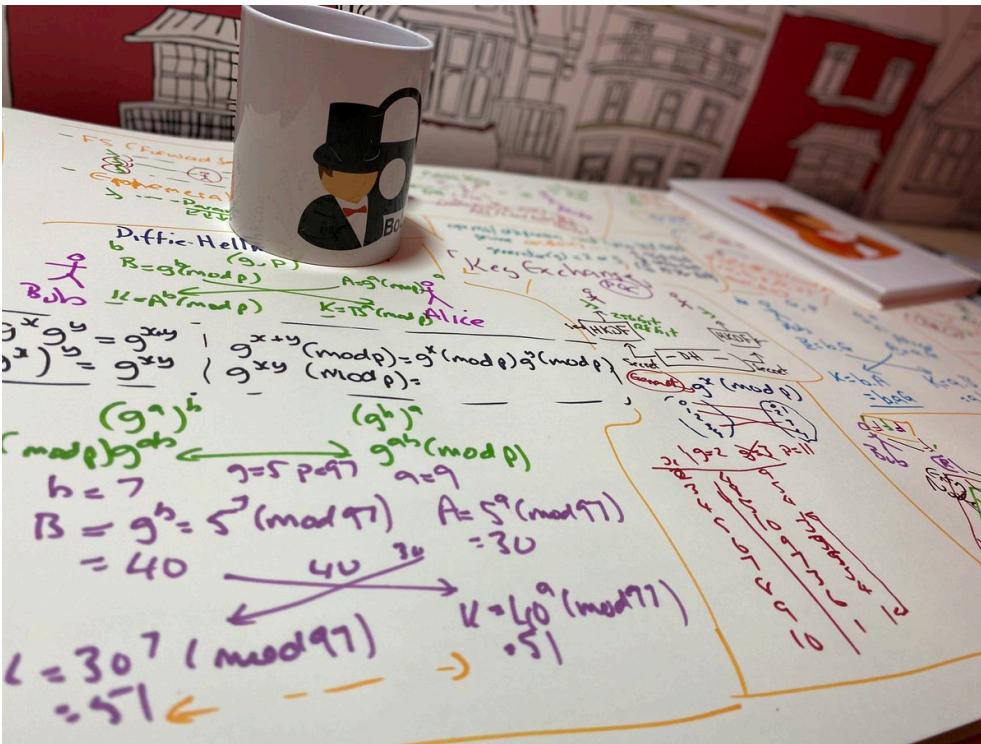
# Unit 6: Digital Certificates

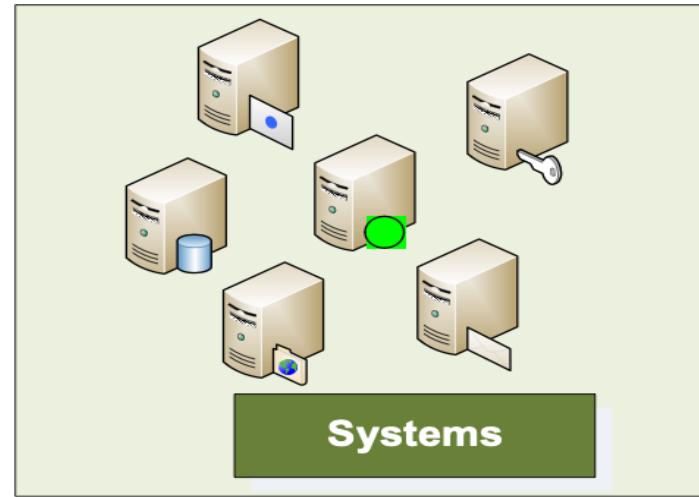
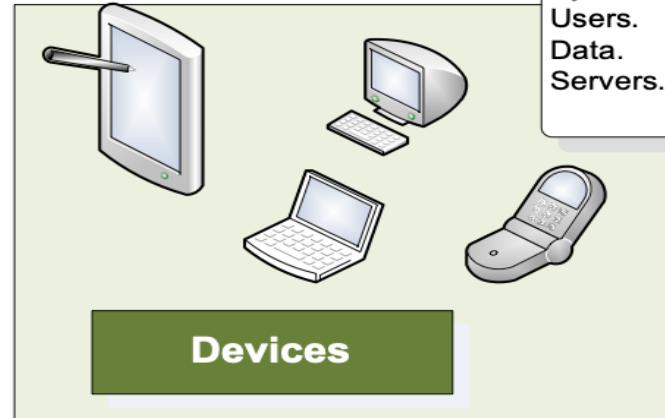
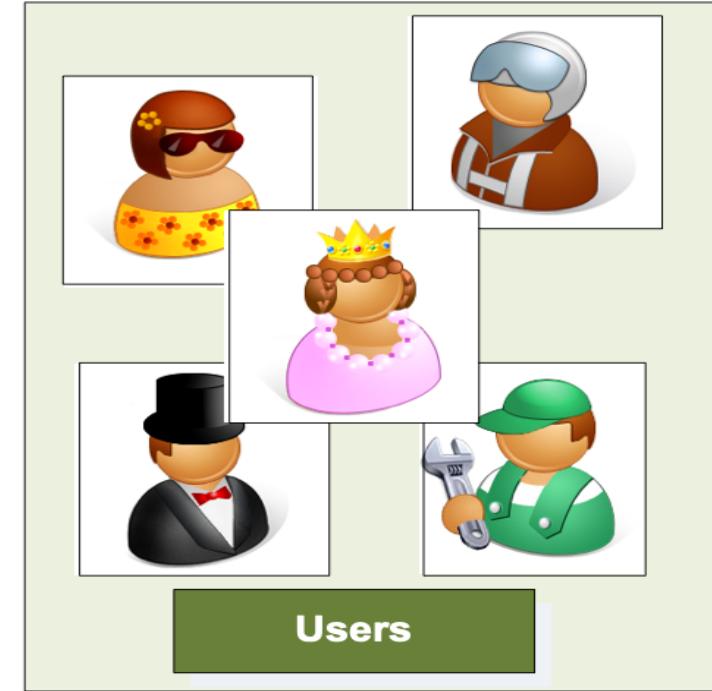
Introduction

Authentication Methods

**Prof Bill Buchanan OBE**

<https://asecuritysite.com/digitalcert/>





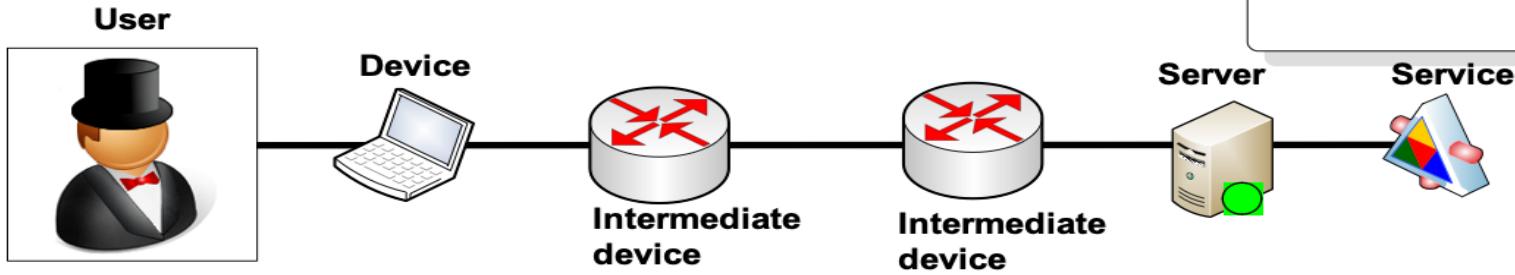
What to authenticate?

Systems.  
Users.  
Data.  
Servers.

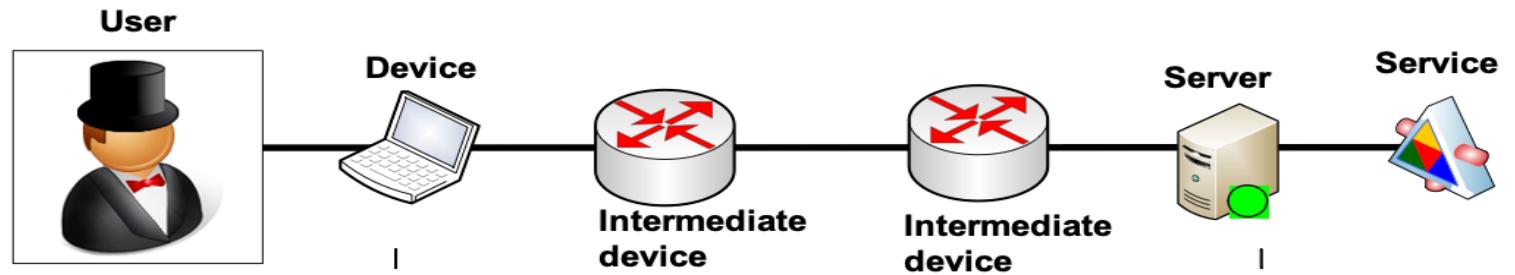
## Where authenticated?

End-to-end. User to service.  
Intermediate. Part of the authentication process.

Authentication Methods



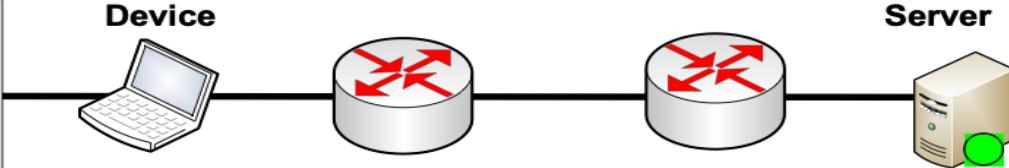
End-to-end authentication



Intermediate authentication



User



**One-way server authentication.** Server provides authentication to the client, such as SSL (HTTPS, FTPS, etc).

## Authentication type

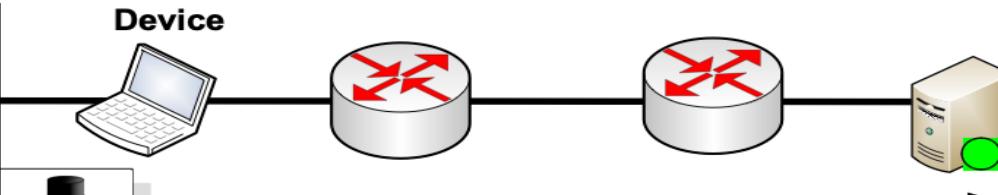
One-way server.  
One-way client.  
Two-way.



ID



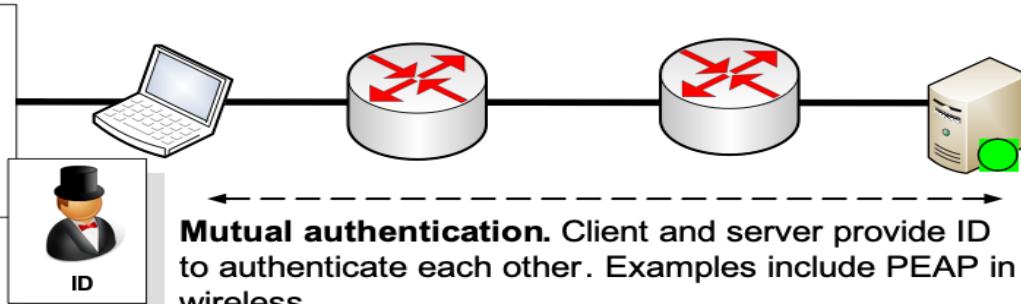
User



**One-way client authentication.** Client provides authentication to the server such as EAP-TLS in Wireless.



User



**Mutual authentication.** Client and server provide ID to authenticate each other. Examples include PEAP in wireless.



ID

## Authentication

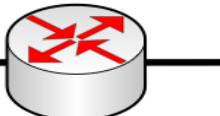
### User



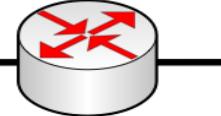
### Device



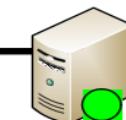
### Intermediate device



### Intermediate device



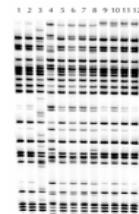
### Server



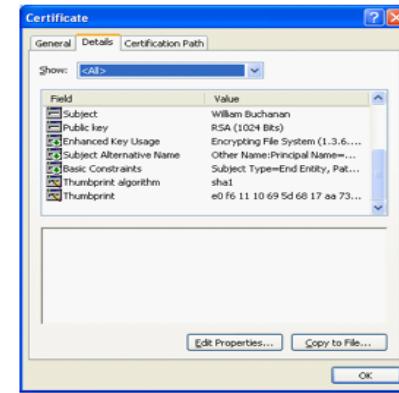
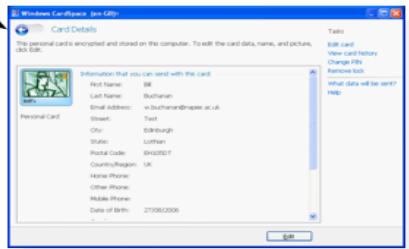
### Service

One-way server.  
One-way client  
Two-way.

**Username/password**  
**Digital Certificate**  
**Token Card**  
**Soft Tokens**  
**Session key**  
**Pass phrase**  
**Biometrics**



**Device name**  
**Digital Certificate**  
**Pass phrase**  
**MAC address**  
**Encryption key**



## Authentication methods

Something you have  
Something you know  
Something you are

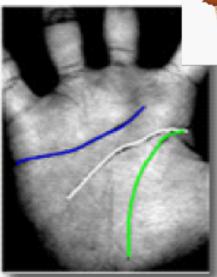


Retina scan



Finger prints

Iris scans



Palm prints

**Something you are**



Username/  
password



Mother's maiden name



Digital certificate



Smart card

Network/physical  
address

**Something you  
have**

**Something you  
know**

# Digital Certificates

Introduction

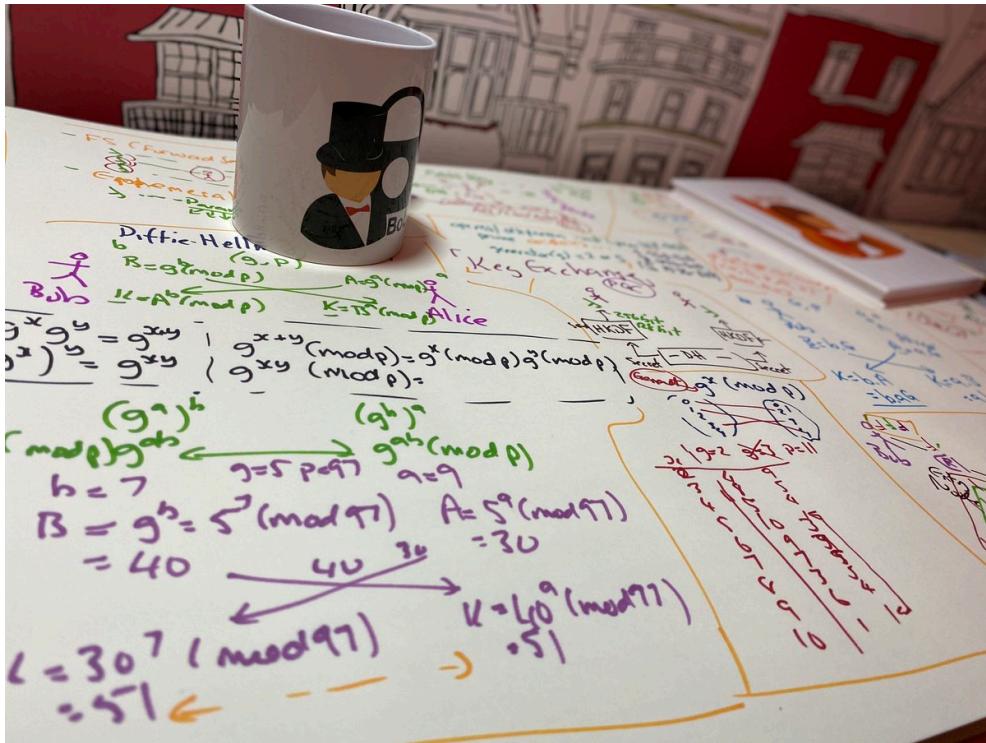
Authentication Methods

PKI

Digital Certificate Passing

**Prof Bill Buchanan OBE**

<https://asecuritysite.com/digitalcert/>



Now that we need the public key to either encrypt data for a recipient, or to authenticate a sender...

How does Bob distribute his public key to Alice , without having to post it onto a Web site or for Bob to be on -line when Alice reads the message?



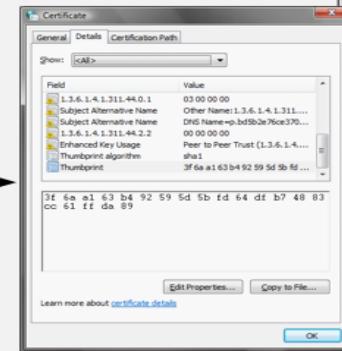
Public-key



## Digital Certificates

Digital certificates are a soft token of authentication, and require a trust mechanism

One method is the digital certificate which can carry the public key (and also the private key, if nesc.)



## Authentication

## Digital Cert.

Bob



**Certificate**

General Details Certification Path

**Certificate Information**

Windows does not have enough information to verify this certificate.

**Details**

**Issued to:** William Buchanan

**Issued by:** Ascertia CA 1

**Valid from:** 17/12/2006 to 17/12/2007

**Issuer Statement**

**Certificate**

General Details Certification Path

Show: <All>

Field	Value
Public key	RSA (2048 Bits)
Subject Key Identifier	cf 26 7f 61 c0 89 c1 3e 68 a4 f...
Authority Key Identifier	KeyID=94 fe 59 87 45 7b d3 4...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Thumbprint algorithm	sha1
Thumbprint	13 b8 68 cb 2c 93 b7 7f 2a 7c 6f 81 11 fa ab 97 99 72 80 5a

**Thumbprint**

Edit Properties... Copy to File... OK

**Certificate**

General Details Certification Path

Show: <All>

Field	Value
Issuer	Ascertia CA 1, Class 1 Certific...
Valid from	17 December 2006 21:04:49
Valid to	17 December 2007 21:14:49
Subject	William Buchanan, IT, Napier U...
Public key	RSA (2048 Bits)
Subject Key Identifier	cf 26 7f 61 c0 89 c1 3e 68 a4 f...
Authority Key Identifier	KeyID=94 fe 59 87 45 7b d3 4...
CRL Distribution Points	[1]CRL Distribution Point: Distr...

**Public-key**

**Certificate**

General Details Certification Path

Show: <All>

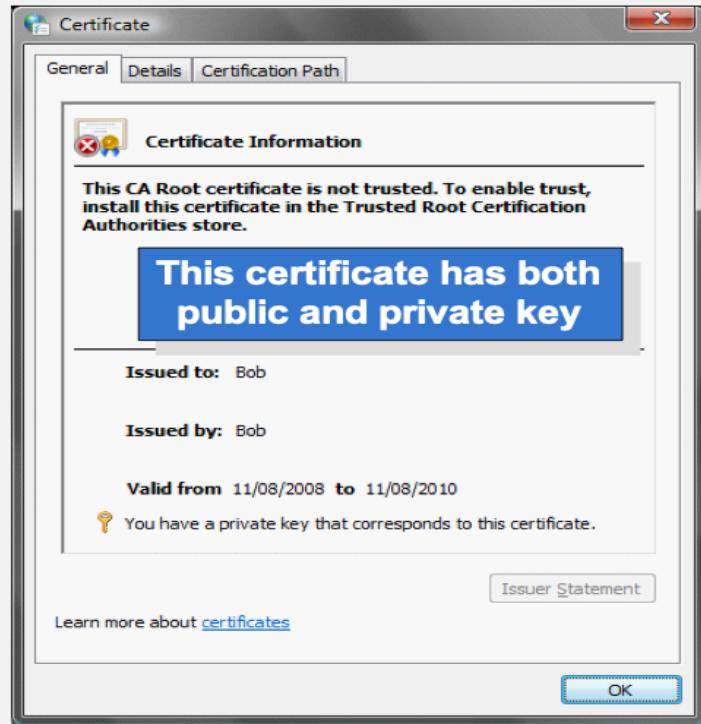
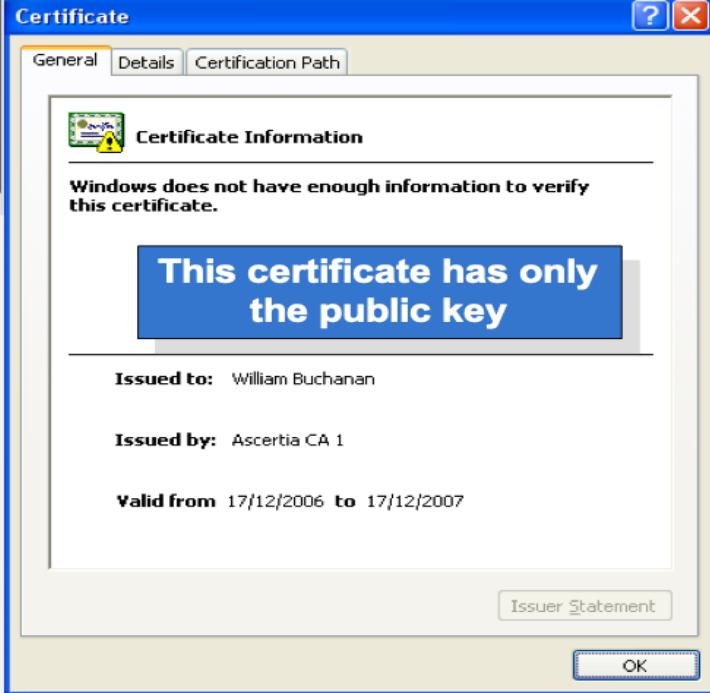
Field	Value
Version	V3
Serial number	58 74 4e 71 00 00 00 00 44 ba
Signature algorithm	sha1RSA
Issuer	Ascertia CA 1, Class 1 Certific...
Valid from	17 December 2006 21:04:49
Valid to	17 December 2007 21:14:49
Subject	William Buchanan, IT, Napier U...
Public key	RSA (2048 Bits)

CN = Ascertia CA 1  
OU = Class 1 Certificate Authority  
O = Ascertia  
C = GB

**Issuer**

Edit Properties... Copy to File... OK

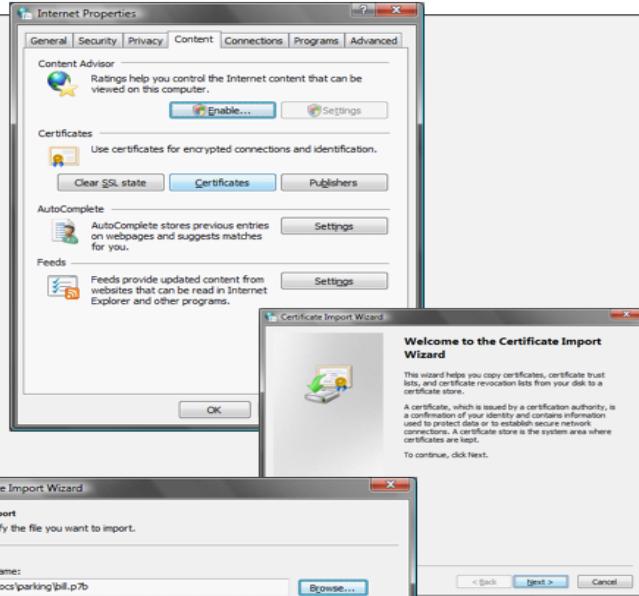
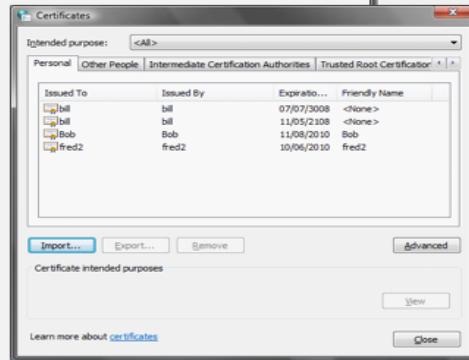
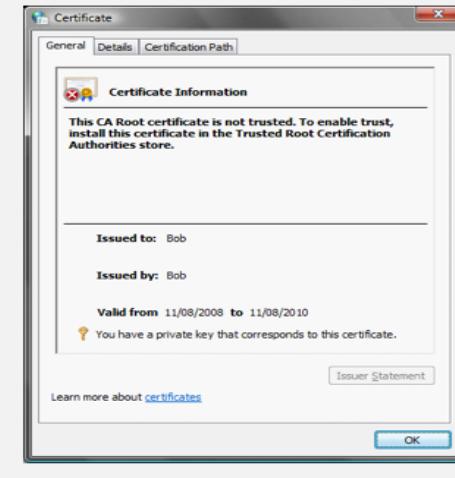
Digital certificate contains a thumbprint to verify it

**Bob**

**Bob**

## P7b format

```
-----BEGIN CERTIFICATE-----
MIIDZCCA4wgAwIBAgIKWHR0cQAAAABeujANBgkqhkiG 9w0BAQUFADBgMQSwCQYD
VQQGEWJHqjERMA 8GA1UEChMIQXnjZXJ 0awExJjAkBgNvBAS THUnsYXKnZIDEgQ_2Vv
dglmawNhgdUgox 0 ag9yaXR 5MRWfAYDVQDew 1bc2n1cnRpYSBDQSAxMB 4XDTA2
MTIxNzIxMDQ 0 0voxDTA3MTIxNzIxMTQ 0 0VowgZ 8xJjAkBgkqhkiG 9w0BCQEWf3cu
YnvjagFuYw 5AbmFwawVylMfjLnVmRQSwCQYDVQGEWJSZEOMA 4GA1UECBMHTG 90
ag1hbjEsmBAGA 1UEBxMjRWrbmJ 1cmdoMrRowGAYDVQKExFOYKbpZXigVw 5pdmy
c210etELMAKGA 1UECxMCsvQxtAxBgNVBAMTefdpbgxpVw 0 qgnVjaGFuYw 4wgEi
MA0GCSqGSIb3DQEBAQAA4IBDwAwggEKAoIBAQCVCFETyJL 8VxAhEMRzQI0gM81
ci75nmMsomajzcB 6fhGmGowmYcoscmQkrVjAknoS +4mxzhny3mdob+szbwVaX
M5FoXhsrV+Q86hsk8Cdc+lsqy38TQtufuDns 0tR6q7CgGqQ8/VjsXnqzK 39
iLUF1ahycet/ab60/gwzL4ivSz2nml4dyauyt1hLP1VbpbHGde 6sDQXWyd0cpfv
ZN7paud5fqBESf06bukcieI47AzRMQj 3kHuDt7MexVw7aoX+nXLP4wn7iamaxasF
QvhdoKyczHs 82JQDGatXRCqkk1ztmz 5i6GKpse7XvuX265Wjq5fhp2hY1AgMB
AAGjggEXMIEBEZAdgNVHQ 4EFgQoUzY/YccJwT5opPHLPIcqkkolkjwwyyvDR 0j
BFwwloAUtP 5Zh0V700k6 CorvRMwB9ifvkBmhP6Q9MDsxC2AjB9NVBAYTAKdCMREW
DwYDQVQKEwhB 2N1cnRpYTEZMBcGA 1UEAxMQXNzjZXJ 0awEgum9vdCBQYIBDTBN
BgNvHR8ERjBEMEkQKA+hjxodhrwo1 8vd3d3LmfjzY2vydG1hlmNbVs 5pbpxbmVD
QS9jcmxzL0FzY2vydglhQ 0ExL3nSYXNzMS 5jcmrwPgYIKWvBQHUQAQEMJAWMC 4G
CCsGAAQFBzAChiJodhrwo1 8vb2Nzcc5nbG9iYwx0cnvzdgZpbmr1ci 5j2b2v0mAOG
CSqGSiB 3DQEBBQAA0EATOCwGJ 1t50kt1upmpjkM1 8idxMmD5wuhszjB1GsMhPxI
H+vXhL9yaOw+Prpz7aJS4/3xxu8vRAnhyu 9yu4qDA==
-----END CERTIFICATE-----
```



- The main certificate formats include:**
- P7b. Text format
  - PFX/P12. Binary.
  - SST. Binary.

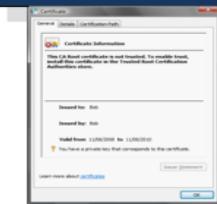


- A. Bob creates the message.
- B. Bob encrypts with Alice's public key and sends Alice the encrypted message
- C. Alice decrypts with her private key
- D. Alice receives the message



Hello

H&\$d .

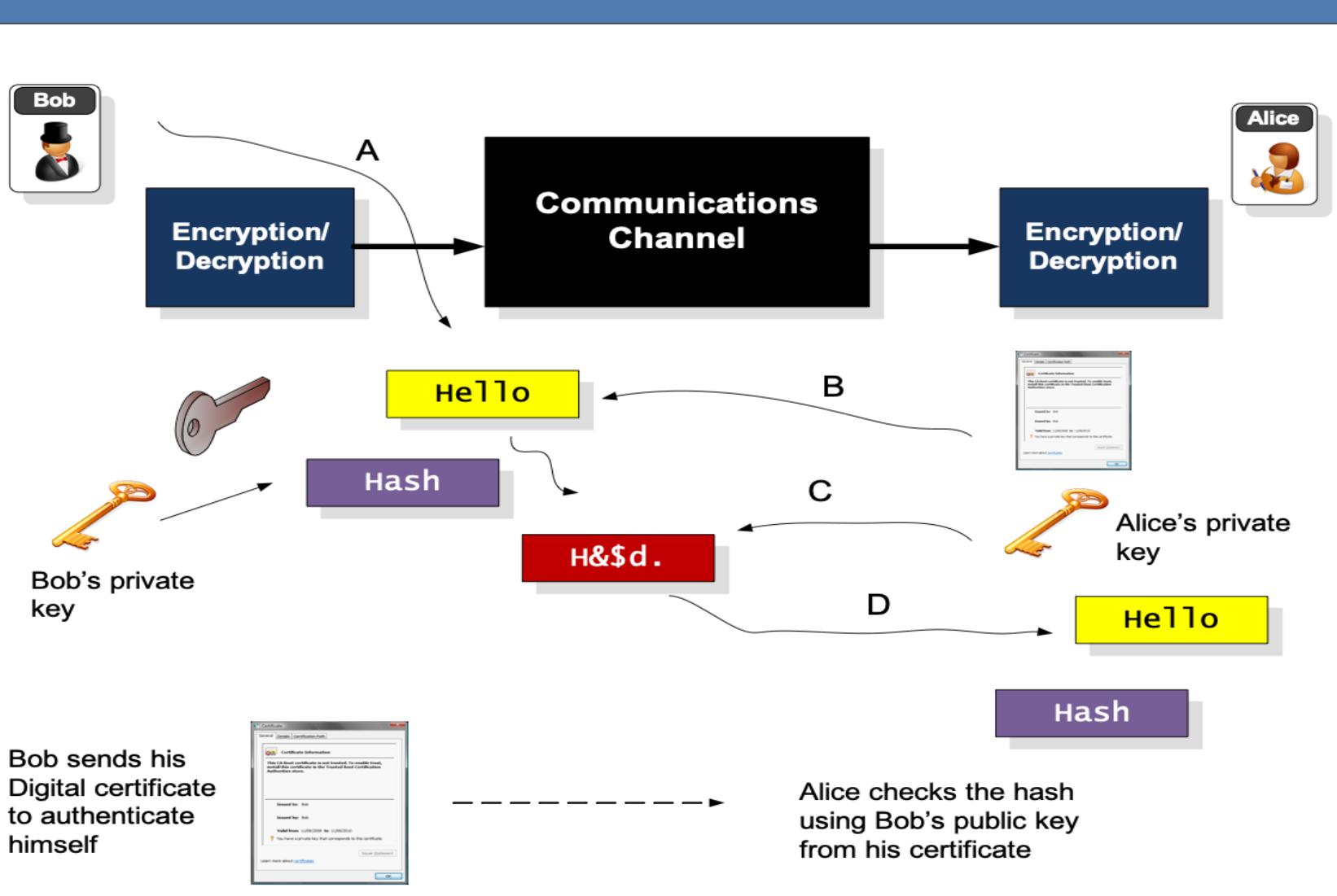


Alice sends her digital certificate with her public key on it



Alice's private key

Hello



# Digital Certificates

Introduction

Authentication Methods

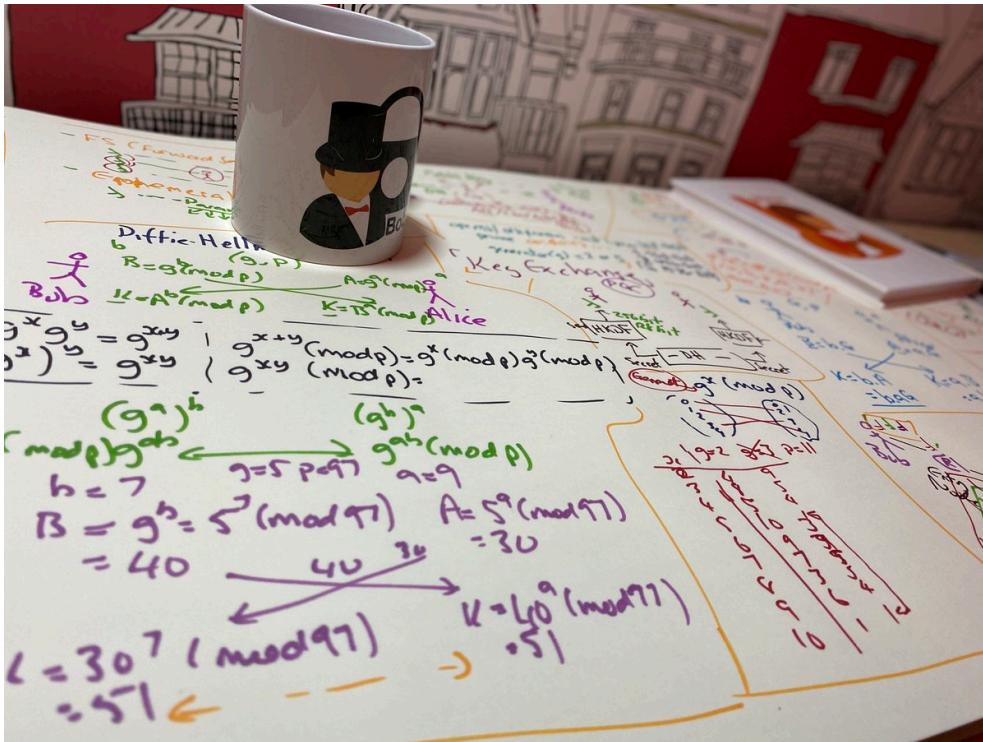
PKI

Certificate Creation

Digital Certificate Passing

**Prof Bill Buchanan OBE**

<https://asecuritysite.com/digitalcert/>



## Organisation

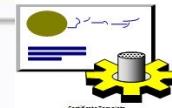


Generate Keypair  
openssl genrsa -out ia.key 2048

ia.key

Create CSR  
openssl req -new -key ia.key -out ia.csr

ia.csr



Digital certificate signed by CA

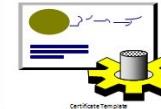
## Root CA



Generate Keypair  
openssl genrsa -out ca.key 2048

ca.key

Generate CA certificate  
openssl req -new -x509 -days 1826 -key ca.key -out ca.crt



Create certificate  
openssl x509 -req -days 730 -in ia.csr -CA ca.crt -CAkey ca.key -set\_serial 01 -out ia.crt

ca.crt

ia.crt

.com  
arksims

e following purpose(s):

e computer  
e computer

statement for details.

Certificate Authority - G2

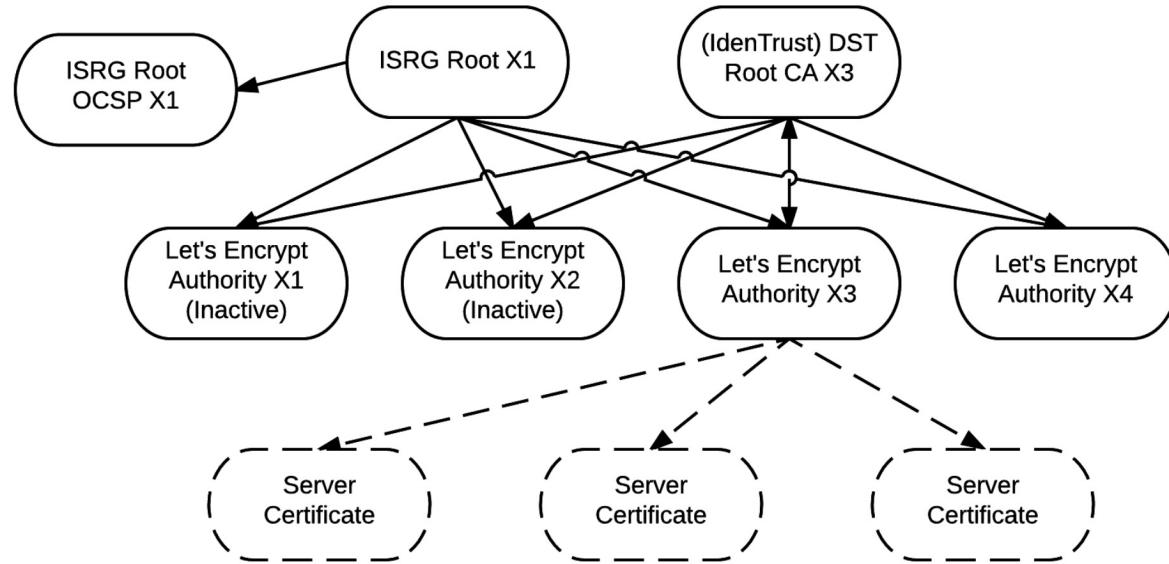
20- Sep

6

Issuer Statement

OK

- Install on Android
- Wireless. Wireless



-----BEGIN CERTIFICATE-----

PEM

MIIEwTCCA6mgAwIBAgIRA093GGFLf...  
 QjELMAkGA1UEBhMCVVMxHjAcBgNVBAoTFUdvb2dsZSBucnVzdCBTZJ2aWn1czET  
 MBEGA1UEAxMKR1RTIENBIDFPMTAeFw0yMDAyMTIxMTQ3NDFaFw0yMDA1MDYxMTQ3  
 NDfaMGgxCzAJBgNVBAYTA1VTMRMwEQYDVQQIEwpDYWxpZm9ybmlhMRYwFAYDVQHQH  
 Ew1Nb3VudGFpbIBWaWV3MRMwEQYDVQQKEwpHb29nbGUgTExDMRcwFQYDVQQDEw53  
 d3cuZ29vZ2x1LmNvbTBZMBMGBYqGSM49AgEGCCqGSM49AwEHA0IABCzzLJYFJb8W  
 TpQxWL01vSDvEWCKed7181CFspT60kn13YILNdTM22sUwPcyogKjBSaQZ9Axi

- X.509 Certificate (DER)
- X.509 Certificate (PKCS#7)

PKCS#1 v2 - Padding for Public Key

PKCS #7 v1.5 - Cryptography Message Syntax

PKCS 10 v1.7 - Certificate Request Standard.

t1HtqVqITZPCAI/ANvbHdZiMEePB8eA+oTiw2ucChqLlsop5Mio8ckg7aXG4/QfC  
 AIDbvkoFFK44rs4UEpsaqGe90qmMjjTu07ZCzrFd1m3geq2ARKPHgPoPM6UbDdqg0  
 TNQo9C0F5Zl0k0gV/qshvpT04YzE7TB2U571eYEeqNXH48syVx8XSk3P7FjM7FIZ2  
 IzbJSEipZJm8DsP10fFXpToIn+zK

-----END CERTIFICATE-----

PKCS#7

-----BEGIN PKCS7-----

MIIE8gYJKoZIhvCNQCoIIIE4zC...  
 wTCCA6mgAwIBAgIRA093GGFLfHw0CAAAAAAcZgwDQYJKoZIhvCNQELBQA...  
 MAKGA1UEBhMCVVMxHjAcBgNVBAoTFUdvb2dsZSBucnVzdCBTZJ2aWn1czET  
 A1UEAxMKR1RTIENBIDFPMTAeFw0yMDAyMTIxMTQ3NDFaFw0yMDA1MDYxMTQ3  
 MGgxCzAJBgNVBAYTA1VTMRMwEQYDVQQIEwpDYWxpZm9ybmlhMRYwFAYDVQHQH  
 b3VudGFpbIBWaWV3MRMwEQYDVQQKEwpHb29nbGUgTExDMRcwFQYDVQQDEw53  
 Z29vZ2x1LmNvbTBZMBMGBYqGSM49AgEGCCqGSM49AwEHA0IABCzzLJYFJb8W  
 WL0TySDvEWCKed7181CFspT60kn13YILNdTM22sUwPcyogKjBSaQZ9Axi  
 EAiJkbejjgJMIICUTAOBgNHQ8BaF8EBAMCB4AwEwDVR01LBawwCgYIKwYE  
 AwEwDAYDVR0TAQH/BAiWADAdBgNVHQ4EFgQU9Ty3t9007UW9+Hc6kv/j9511  
 HwYDVR0jBBgwFoAUmNH4bhDrz5vsYJ8YKBUG630J/SswZAYIKwYBBQUHAQE  
 MCcGCCsGAQUFBzABhtodHRw0i8vb2Nzc5wa2kuZ29vZy9ndHmxzbEwKwYI  
 BQUHMAKGH2h0dHAGLy9wa2kuZ29vZy9nc3IyL0dUzFPMS5jcncQwGQYDVR0  
 EII0d3d3Lmdvb2dsZs5jb20wIQYDVR0gBBowGDAIBgZngQwBAgIwDAYKkwYE  
 eQIFAzAvBgNVHR8EKDAmMCsgIqAghh5odHRw0i8vY3JsLnBras5nb29nL0d  
 MS5jcmwggEFBgorBgEEAdZ5AgQCBH2BIHzAPEAdgCyHgXMi6LNiiB0h2b5  
 JSBna9r6c0eySvt74uQXgAAAXA5cNqwAAAEAwBHMEUCIQCojKtz0e8l1JYK  
 bt1puqt4AE3peMVAVk/WewGp1QIgBvRmbNkwF6i8+JVv3CfTHKvFd8e00+G  
 Zb1drKEAdwBep3P531bA57U2SH3QSeAyeGaDIShEhKEGHwWgXFFWAAAAXA5  
 AAAEAwBIMEYCIQCOS0NppELPOdH65oFT5ZAGsSQz4FsJNNZedgS7WqzLnQI  
 u0QuuoE3RWngfhI6W7n1kxxEmd0vSZTe6+0l+JVuMA0GCSqGSIB3DQEBCwUA  
 AQCDU8CVusGstVkk1Amrtg3DyYhNV1UnKyLk3RrHKumwYz5mC25bWGoLVKv  
 N3za329/9JZq0mn0vpmPxjTDvh9sVQ7g4znwha/KJfzL8AZKudldD90+hD0  
 qVqITZPCAI/ANvbHdZiMEePB8eA+oTiw2ucChqLlsop5Mio8ckg7aXG4/QfC  
 vkoffK44rs4UEpsaqGe90qmMjjTu07ZCzrFd1m3geq2ARKPHgPoPM6UbDdqg0  
 9C0F5Zl0k0gV/qshvpT04YzE7TB2U571eYEeqNXH48syVx8XSk3P7FjM7FIZ2  
 SEipZJm8DsP10fFXpToIn+zKoQAxAA==  
 -----END PKCS7-----

Base64

Binary

DER  
CER

```
openssl x509 -outform der -in www-google-com.pem -out google.crt
openssl pkcs12 -export -in server.pem -out keystore.pkcs12
```

# Digital Certificates

Introduction

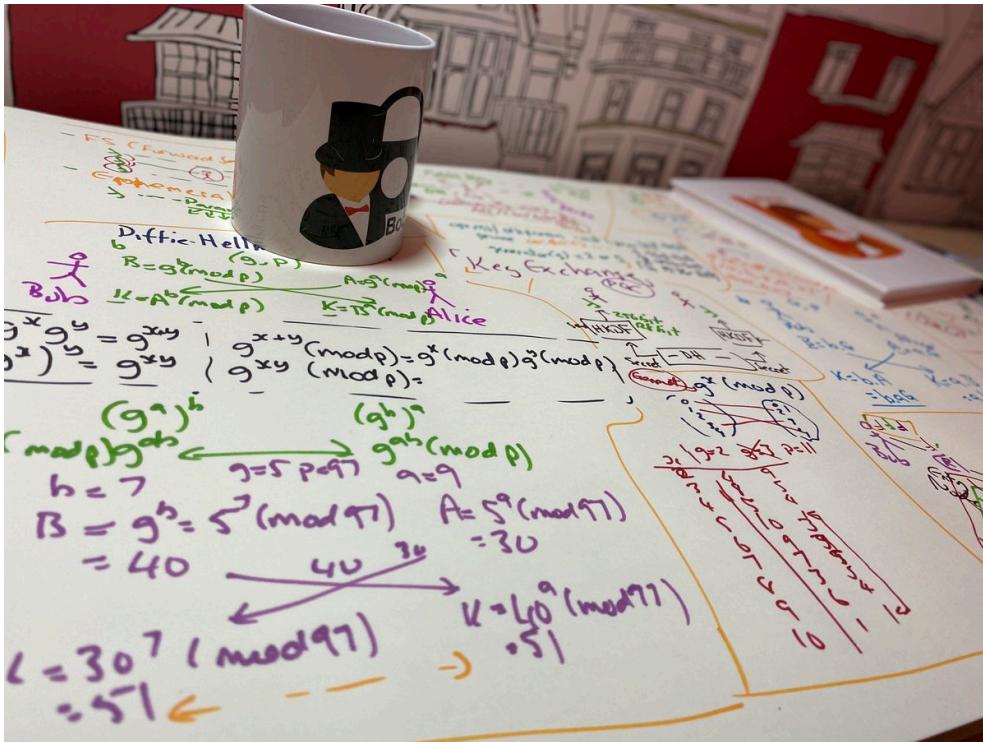
Authentication Methods

PKI

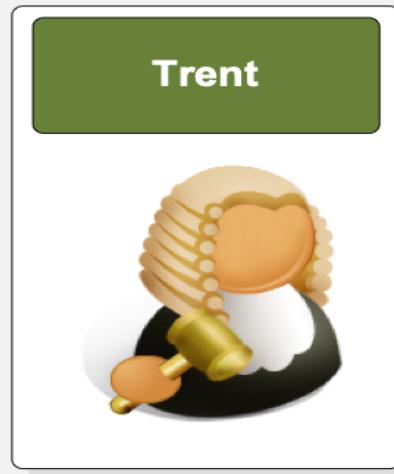
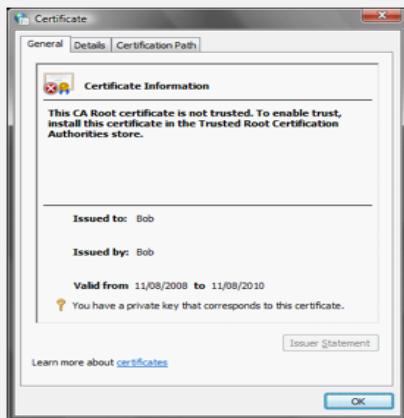
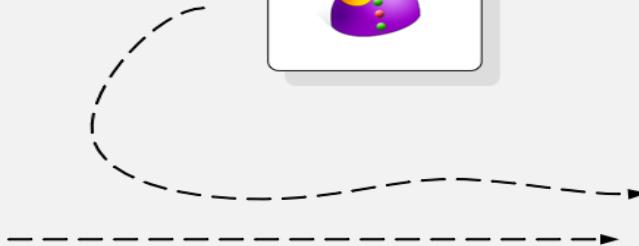
Digital Certificate Passing

**Prof Bill Buchanan OBE**

<https://asecuritysite.com/digitalcert/>



**Who do we trust to get Bob's certificate ... we can't trust Bob, as he may be Eve... meet Trent.**



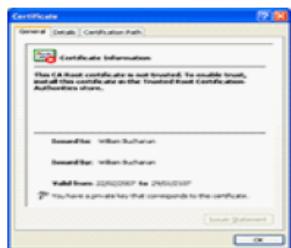
## Digital Certificates

Digital certificates are a soft token of authentication, and require a trust mechanism

## Trusted Root CA



The Trusted Root CE (Trent) checks Bob's identity and creates a certificate which he signs



Certificate Authority (CA)  
- Able to grant certificates  
Examples; Verisign, Entrust, Microsoft Trust.

Trent



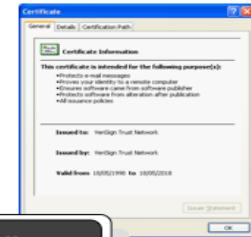
Trusted root certificates are installed as a default on the machine (or installed with the user's permission)

Trusted root certificate

Alice checks the signature of the certificate to validate Bob. Both Alice and Bob trust the CA (Trent) as a third party.



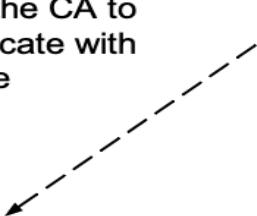
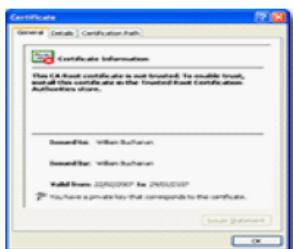
Author: Prof Bill Buchanan



## Trusted Root CA



Eve tricks the CA to get a certificate with Bob's name



Certificate Authority (CA)  
- Able to grant certificates  
Examples; Verisign, Entrust, Microsoft Trust.

Trent



Trusted root certificates are installed as a default on the machine (or installed with the user's permission)

Trusted root certificate



Alice checks the signature of the certificate to validate Bob. Both Alice and Bob trust the CA (Trent) as a third party.

Author: Prof Bill Buchanan

**Certificates**

Intended purpose: <All>

Intermediate Certification Authorities Trusted Root Certification Authorities Trusted Publ

Issued To	Issued By	Expiration...	Friendly...
Microsoft Authenticode(tm)...	Microsoft Authenticode(tm)...	31/12/1999	Microsoft
Microsoft Root Authority	Microsoft Root Authority	31/12/2020	Microsoft
Microsoft Root Certificate ...	Microsoft Root Certificate ...	09/05/2021	Microsoft
NetLock Expressz (Class C...)	NetLock Expressz (Class C...)	20/02/2019	NetLock I
NetLock Kozjegyzoj (Class ...)	NetLock Kozjegyzoj (Class ...)	19/02/2019	NetLock I
NetLock Uzleti (Class B) Ta...	NetLock Uzleti (Class B) Ta...	20/02/2019	NetLock I
NO LIABILITY ACCEPTED, ...	NO LIABILITY ACCEPTED, (...)	07/01/2004	VeriSign
PTT Post Root CA	PTT Post Root CA	26/06/2019	KeyMail F

Import... Export... Remove Advanced...

Certificate intended purposes <All>

**Trusted Root CA**  
- always trusted

## Trusted Root CA



### Certificate purposes:

- Secure email.
- Server authentication.
- Code signing.
- Driver authentication.
- Time stamping.
- Client authentication.
- IP tunnelling.
- EFS (Encrypted File System).

**Certificate**

General Details Certification Path

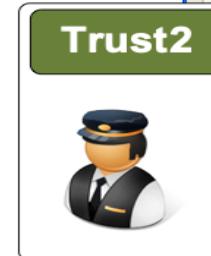
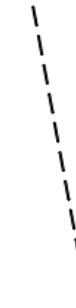
**Certificate Information**

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

**Self signed**  
- Can never be trusted

Issued to: William Buchanan  
Issued by: William Buchanan  
Valid from 22/02/2007 to 29/01/2107  
You have a private key that corresponds to this certificate.

Issuer Statement OK



**Certificates**

Intended purpose: <All>

Intermediate Certification Authorities Trusted Root Certification Authorities Trusted Publ

Issued To	Issued By	Expiration...	Friendly...
GTE CyberTrust Root	Root SGC Authority	23/02/2006	<N>
Microsoft Internet Authority	GTE CyberTrust Global Root	23/02/2007	<N>
Microsoft Internet Authority	GTE CyberTrust Global Root	19/04/2009	<N>
Microsoft Secure Server Authority	Microsoft Internet Authority	23/02/2007	<N>
Microsoft Secure Server Authority	Microsoft Internet Authority	19/04/2009	<N>
Microsoft Windows Hardware C...	Microsoft Root Authority	31/12/2002	<N>
Microsoft Windows Hardware C...	Microsoft Root Authority	31/12/2002	<N>
MS SGC Authority	Root SGC Authority	01/01/2010	<N>

Import... Export... Remove Advanced...

Certificate intended purposes

Signing, Windows Hardware Driver Verification

**Intermediate CA**  
- Can be trusted for some things

Levels of trust



The two main problems with digital certificates are:

- Lack of understanding of how they work.
- They can be spoofed.

So let's look at a few ... are they real or fake?



Humor12.com

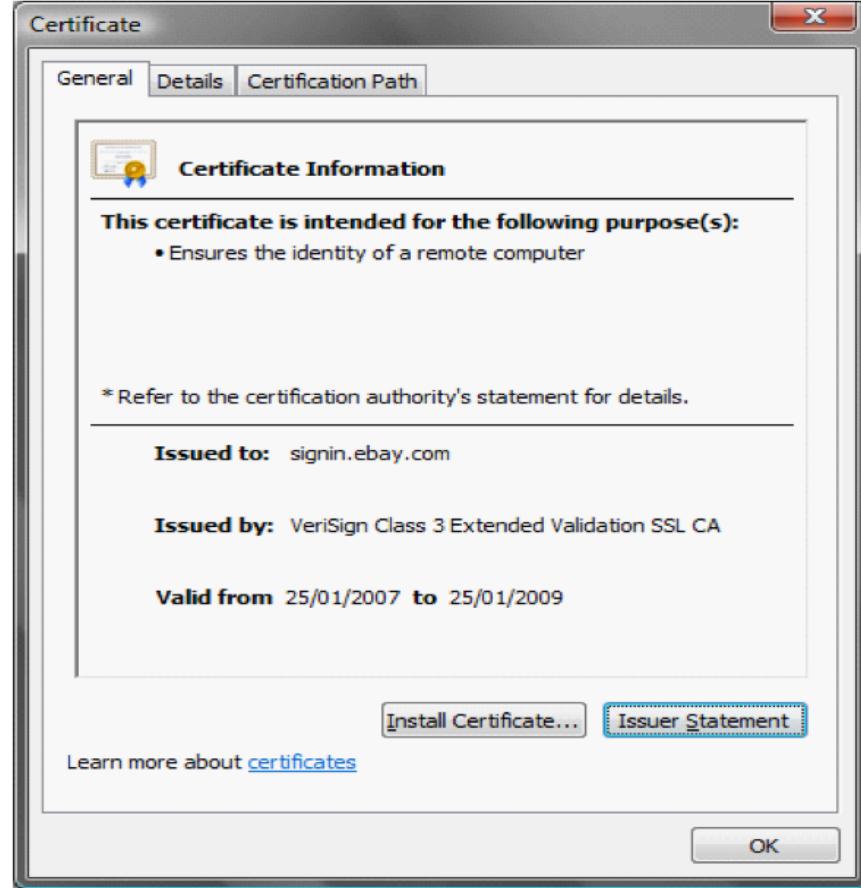


Bob



Eve

# Real or fake?



Author: Prof Bill Buchanan

Real or fake?



Certificate

General Details Certification Path

Certification path

VeriSign  
VeriSign Class 3 Extended Validation SSL CA  
signin.ebay.com

https://www.verisign.com/repository/rpa.html - Windows Internet Explorer

File Edit View Favorites Tools Help

Products & Services Solutions Support About VeriSign

UNITED STATES

RESOURCES

PKI Disclosure  
Licenses & Approvals  
E-Sign  
Publications

Home > Repository

## VeriSign Relying Party Agreement

YOU MUST READ THIS RELYING PARTY AGREEMENT ("AGREEMENT") BEFORE VALIDATING A CERTIFICATE, USING VERISIGN'S ONLINE CERTIFICATE STATUS PROTOCOL ("OCSP") OR USING A VERISIGN OR VERISIGN AFFILIATE DATABASE OF CERTIFICATE REVOCATION LIST ("CRL"). IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT SUBMIT A QUERY AND DO NOT ACCESS, OR RELY ON ANY VERISIGN INFORMATION. IN CONSIDERATION OF YOUR AGREEMENT, YOU ARE ENTITLED TO USE VERISIGN INFORMATION AS SET FORTH HEREIN.

**1. Term of Agreement.** This Agreement becomes effective when you submit a query to validate a Certificate, or rely on any VeriSign Information in the manner set forth in the preamble and shall be applicable for as long as you use and/or rely on such VeriSign Information.

**2. Definitions.**  
"Certificate" or "Digital Certificate" means a message that, at least, states a name or identifier for the Subscriber, contains the Subscriber's public key, identifies the Certificate's serial number, and contains a digital signature of the issuing CA.

Done

Internet | Protected Mode: Off

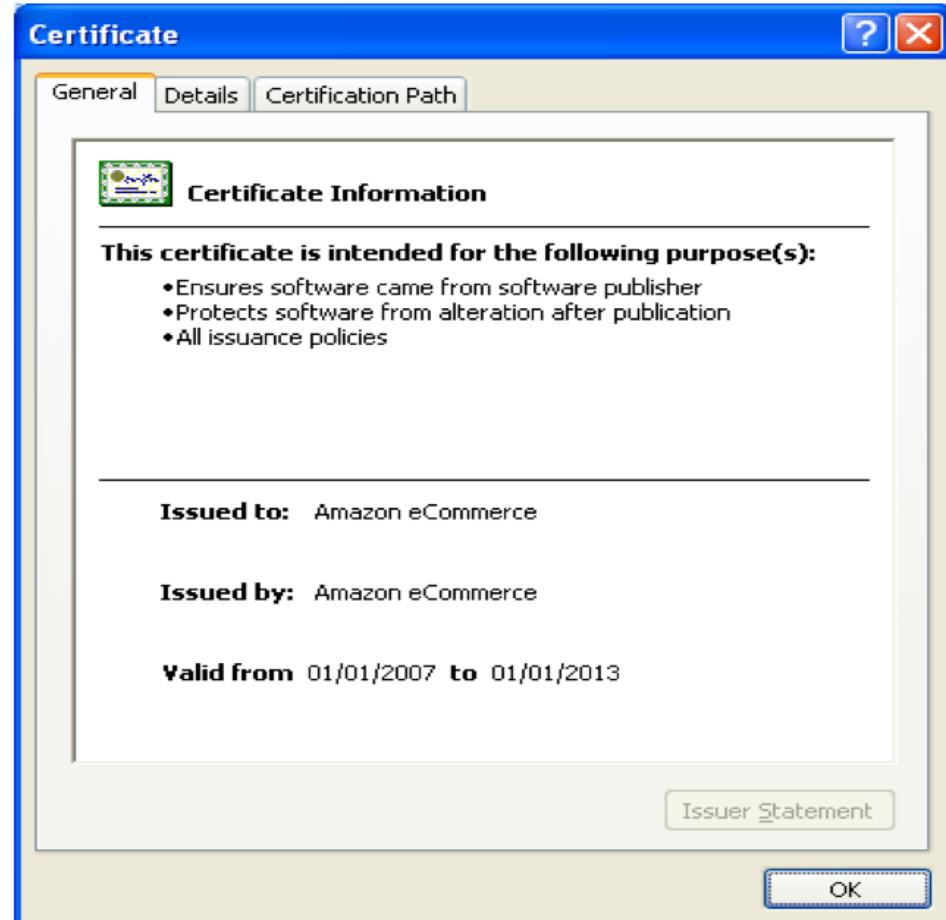
100%



# Real!

Author: Prof Bill Buchanan

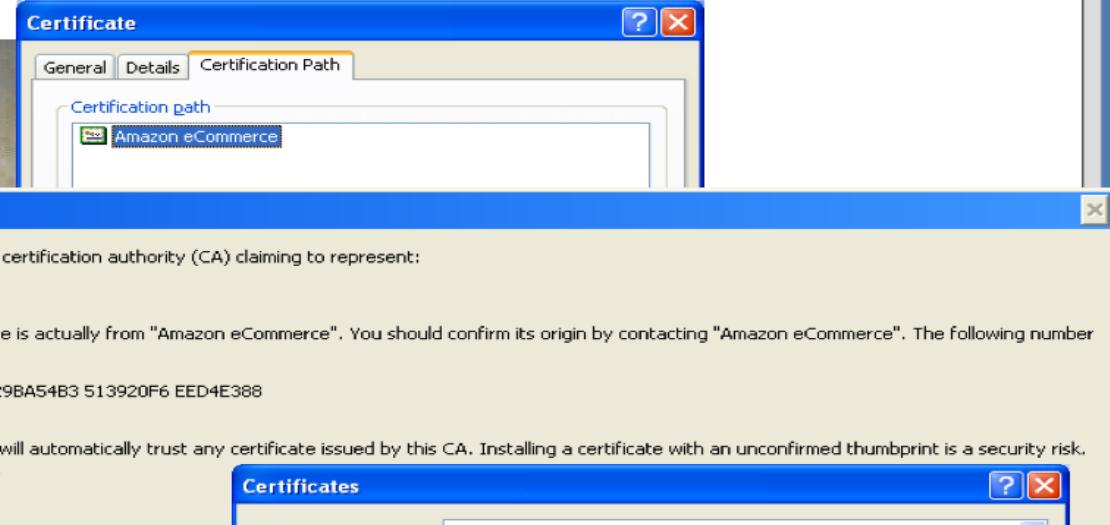
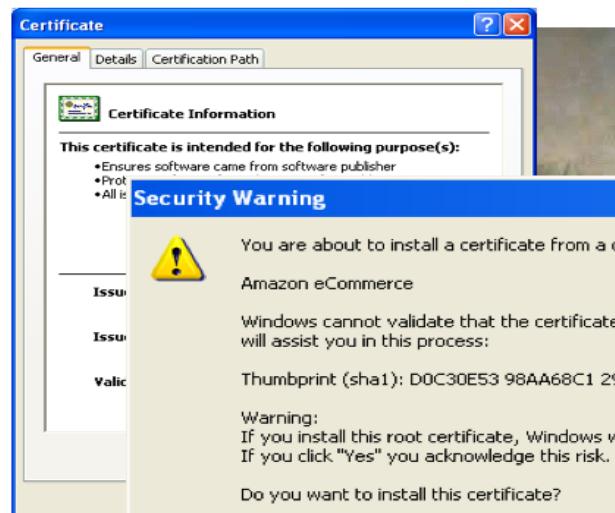
Real or fake?

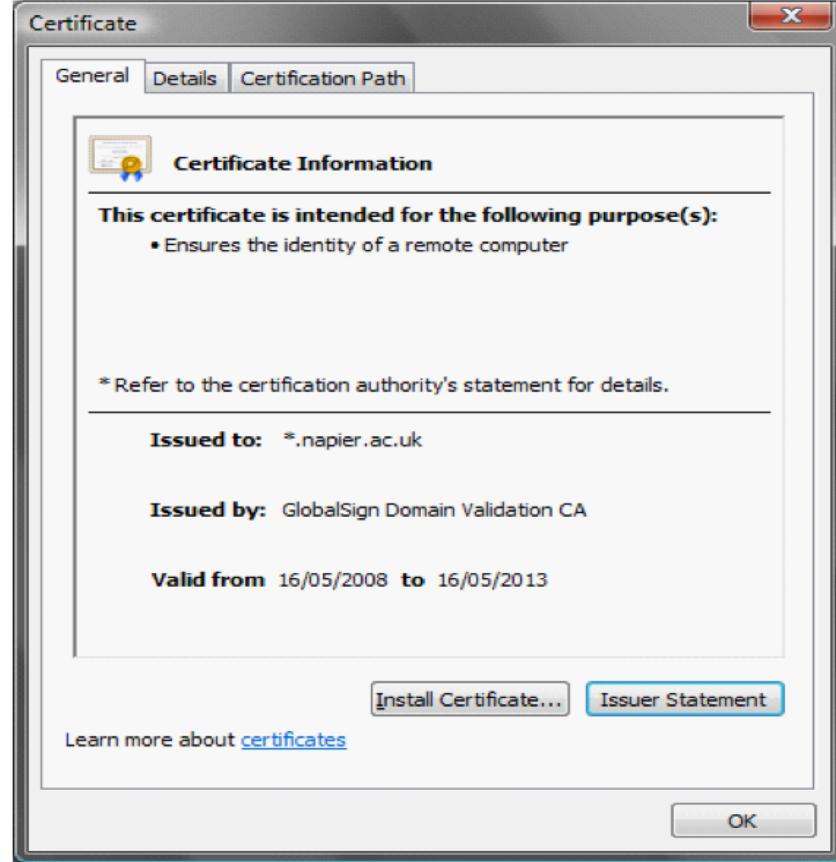


# Real or fake?

Author: Prof Bill Buchanan

Real or fake?





# Real or fake?

Author: Prof Bill Buchanan

Real or fake?



# Real



Certificate

General Details Certification Path

Certification path

- GlobalSign
- GlobalSign Domain Validation CA
- \*.napier.ac.uk

GlobalSign (SSL Certificate) Legal Repository - Windows Internet Explorer

File Edit View Favorites Tools Help

GlobalSign (SSL Certificate) Legal Repository

Contact Us

GlobalSign™  
GMO Internet Group

HOME Products Solutions Partners About GlobalSign

You are here: United States Home > Repository > Legal Documents

About GlobalSign

- Company Profile
- Company History
- Management Team
- Press Center
- Repository**
- Content Library
- International
- Contact Us

**Repository of Legal Documents & Root Certificates**

GlobalSign Root Certificates  
All Root & Intermediate CA Certificates

GlobalSign Certification Practice Statement (CPS)  
Current version - v6.1 - June 08  
Previous version - v6.0 - December 07

GlobalSign Certification Practice Statement (CPS) for  
Adobe Certified Document Services (CDS)

Waiting 100% Internet | Protected Mode: Off Author: Prof Bill Buchanan

# Chapter 6: Digital Certificates

Introduction

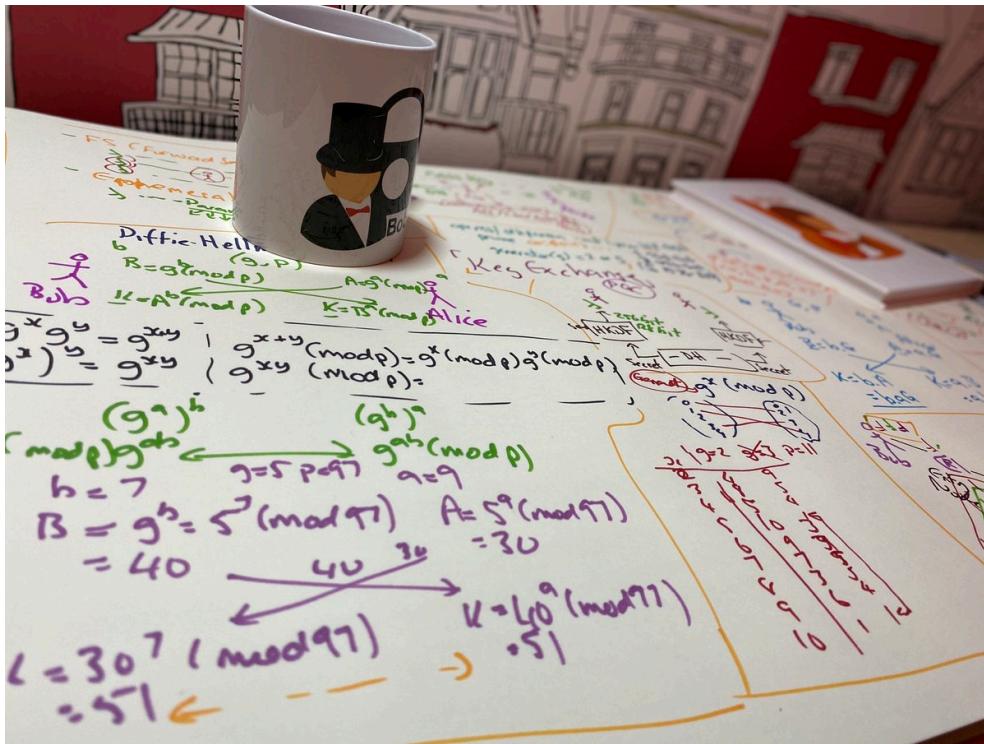
Authentication Methods

PKI

Digital Certificate Passing

**Prof Bill Buchanan OBE**

<https://asecuritysite.com/digitalcert/>





## Public key encryption ... secret ... identity ... trust



Eve



Trent



MegaCorp



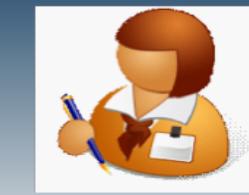
Bob's Private Key



Bob's Public Key



Alice's Public Key



Alice's Private Key



## Public key encryption ... secret ... identity ... trust



Eve



Trent

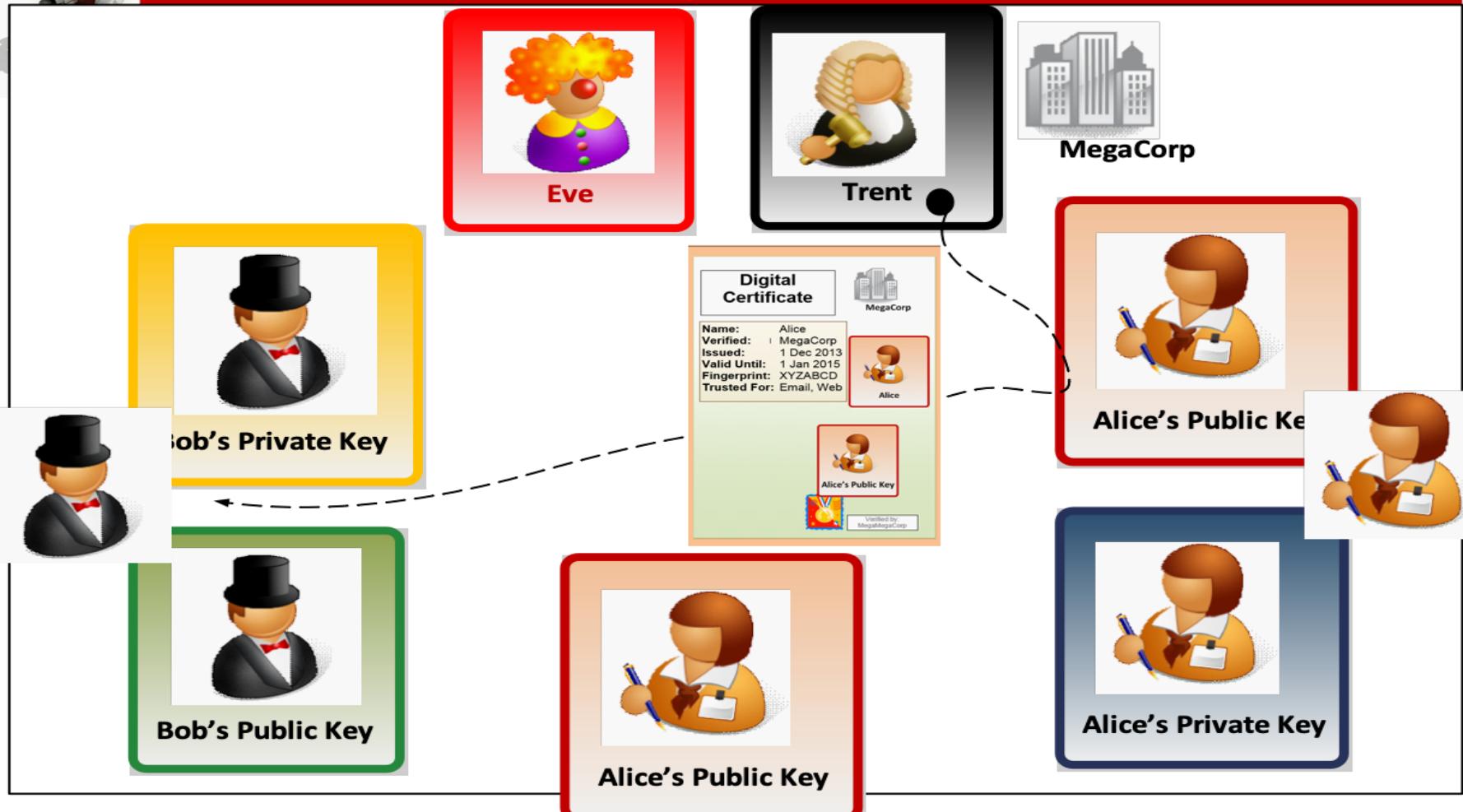


MegaCorp





# Public key encryption ... secret ... identity ... trust





## Public key encryption ... secret ... identity ... trust



Eve



Trent



MegaCorp



Alice's Public Key



Bob's Private Key



Hello Alice,  
Wish you were  
here!  
- Bob

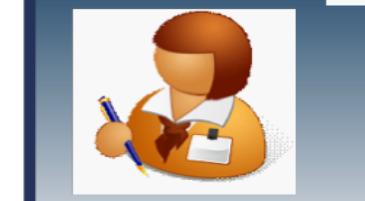
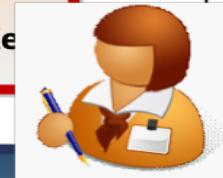
Bob.



Bob's Public Key



Alice's Public Key



Alice's Private Key



# Public key encryption ... secret ... identity ... trust



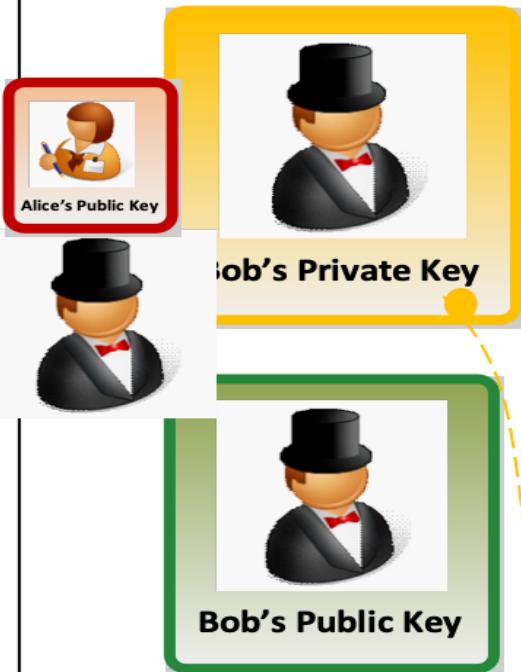
Eve



Trent



MegaCorp

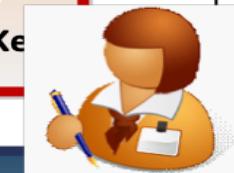


Hello Alice,  
Wish you were  
here!  
- Bob

Bob:



Bob's Private Key





# Public key encryption ... secret ... identity ... trust



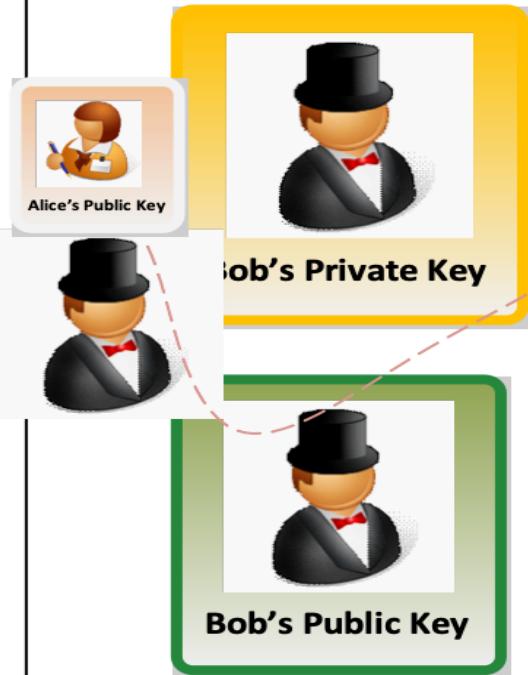
Eve



Trent



MegaCorp





## Public key encryption ... secret ... identity ... trust



Eve



Trent



MegaCorp



Bob's Private Key



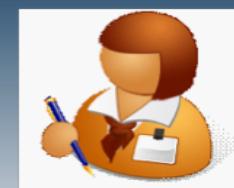
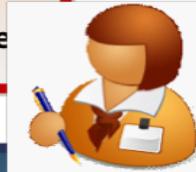
Bob's Public Key

Hello Alice,  
Wish you were  
here!  
- Bob

Bob.



Alice's Public Key



Alice's Private Key



Which key to open  
the message?



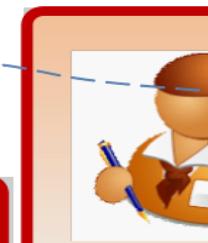
# Public key encryption ... secret ... identity ... trust



Hello Alice,  
Wish you were  
here!  
- Bob

Bob.

Which key to open  
the message?





## Public key encryption ... secret ... identity ... trust



Eve



Trent



MegaCorp



Bob's Private Key



Bob's Public Key

Hello Alice,  
Wish you were  
here!  
- Bob

Bob:

Which key to we  
open the signature  
with?



Alice's Public Key



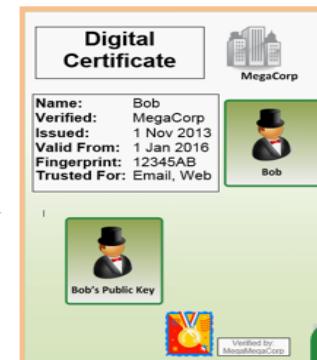
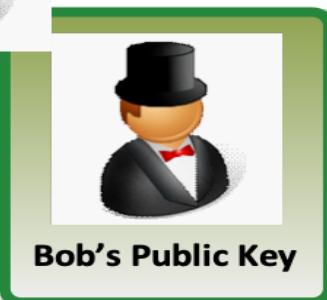
Alice's Private Key



# Public key encryption ... secret ... identity ... trust



MegaCorp



Hello Alice,  
Wish you were  
here!  
- Bob

Bob:





# Public key encryption ... secret ... identity ... trust



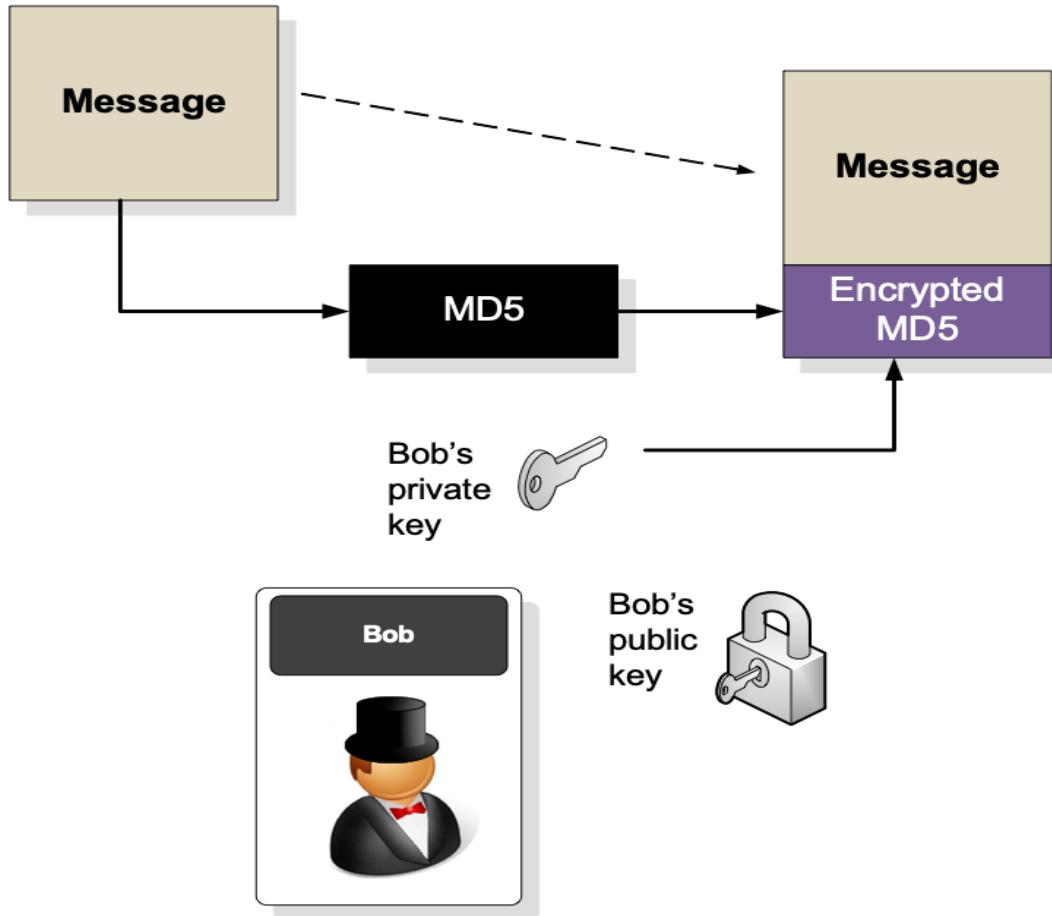
MegaCorp

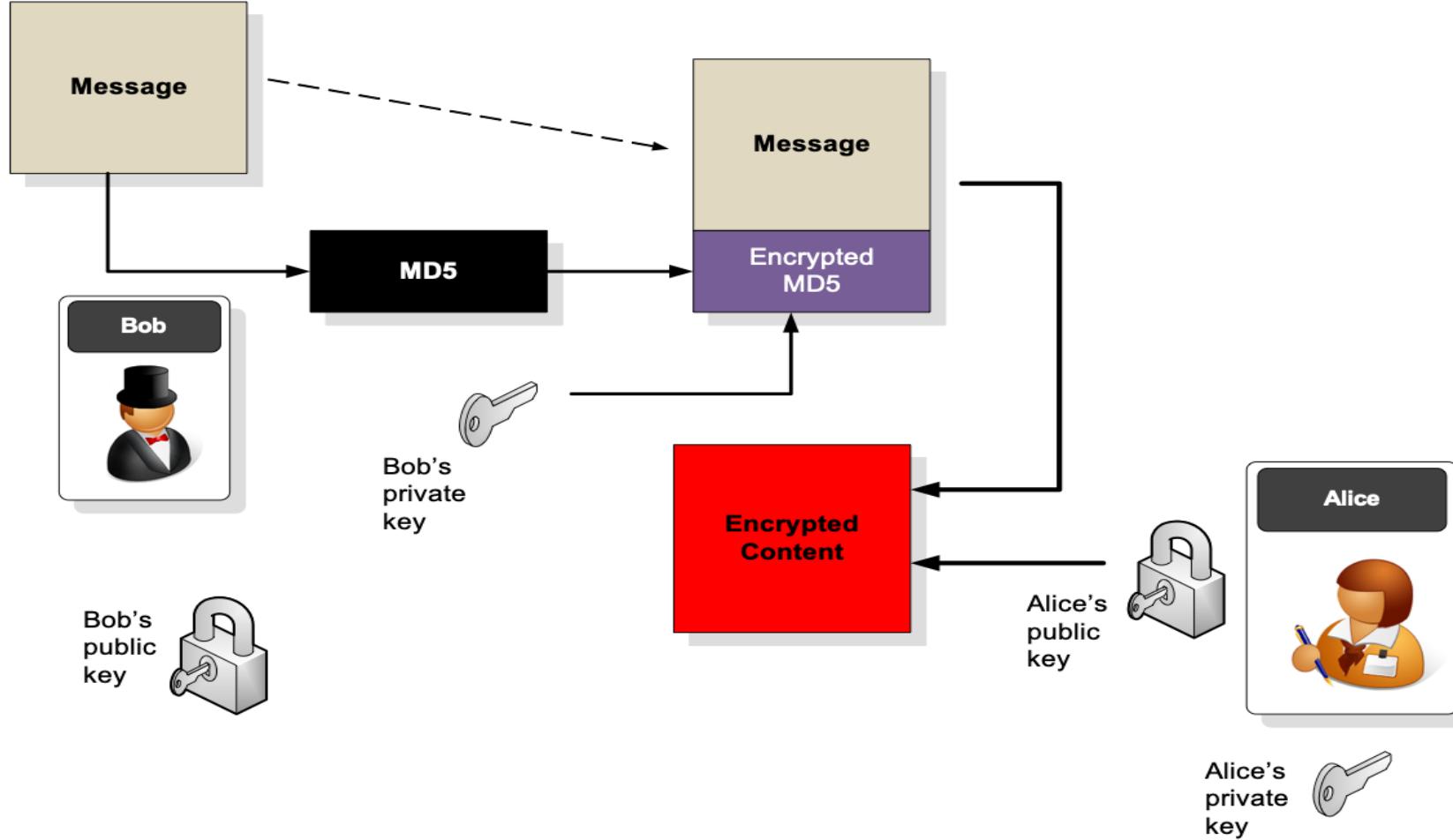


Hello Alice,  
Wish you were  
here!  
- Bob

Bob:

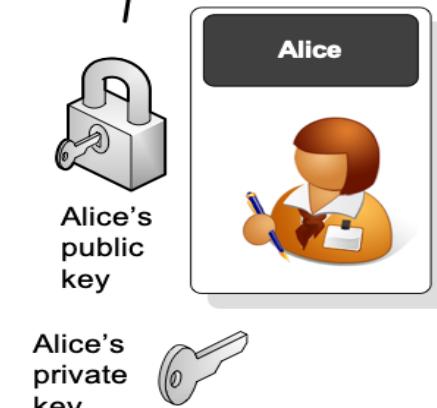
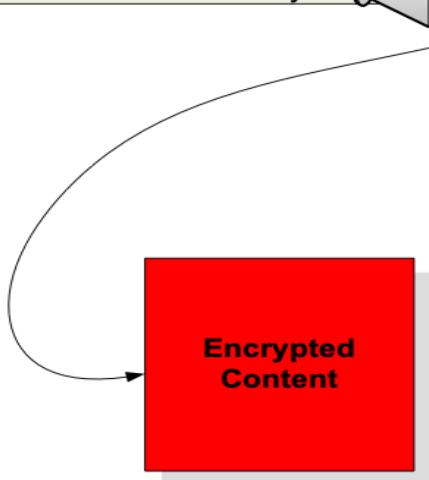
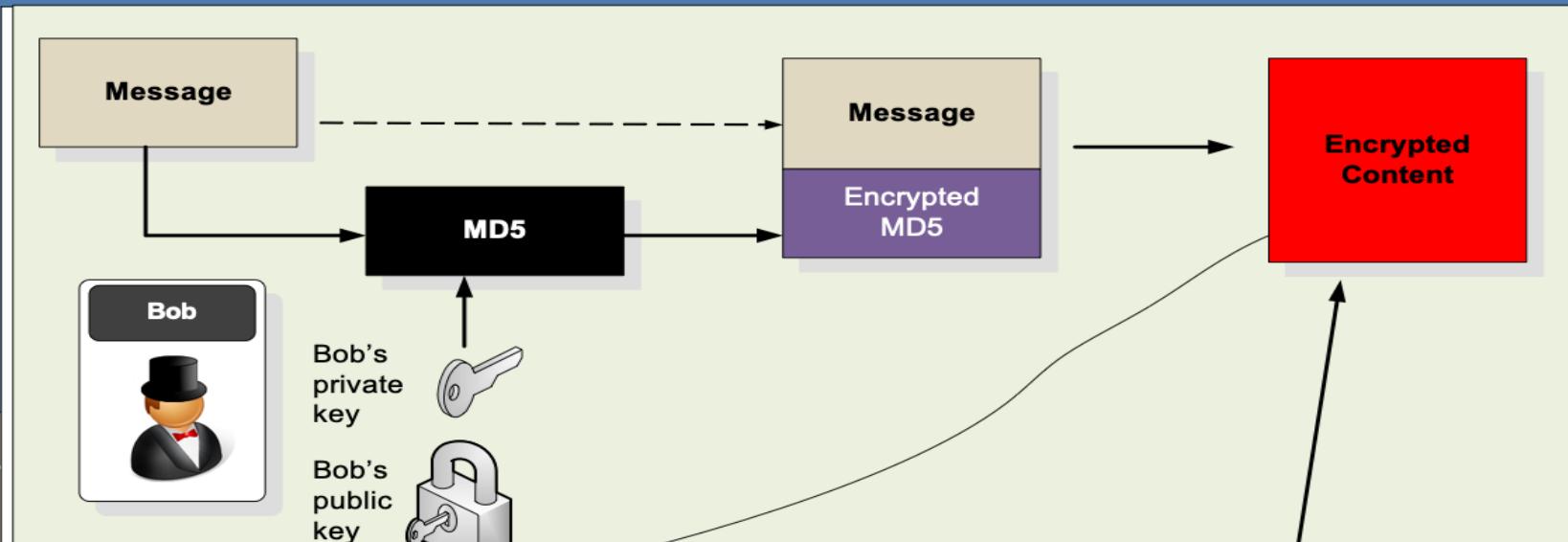






## Authentication

The magic private key

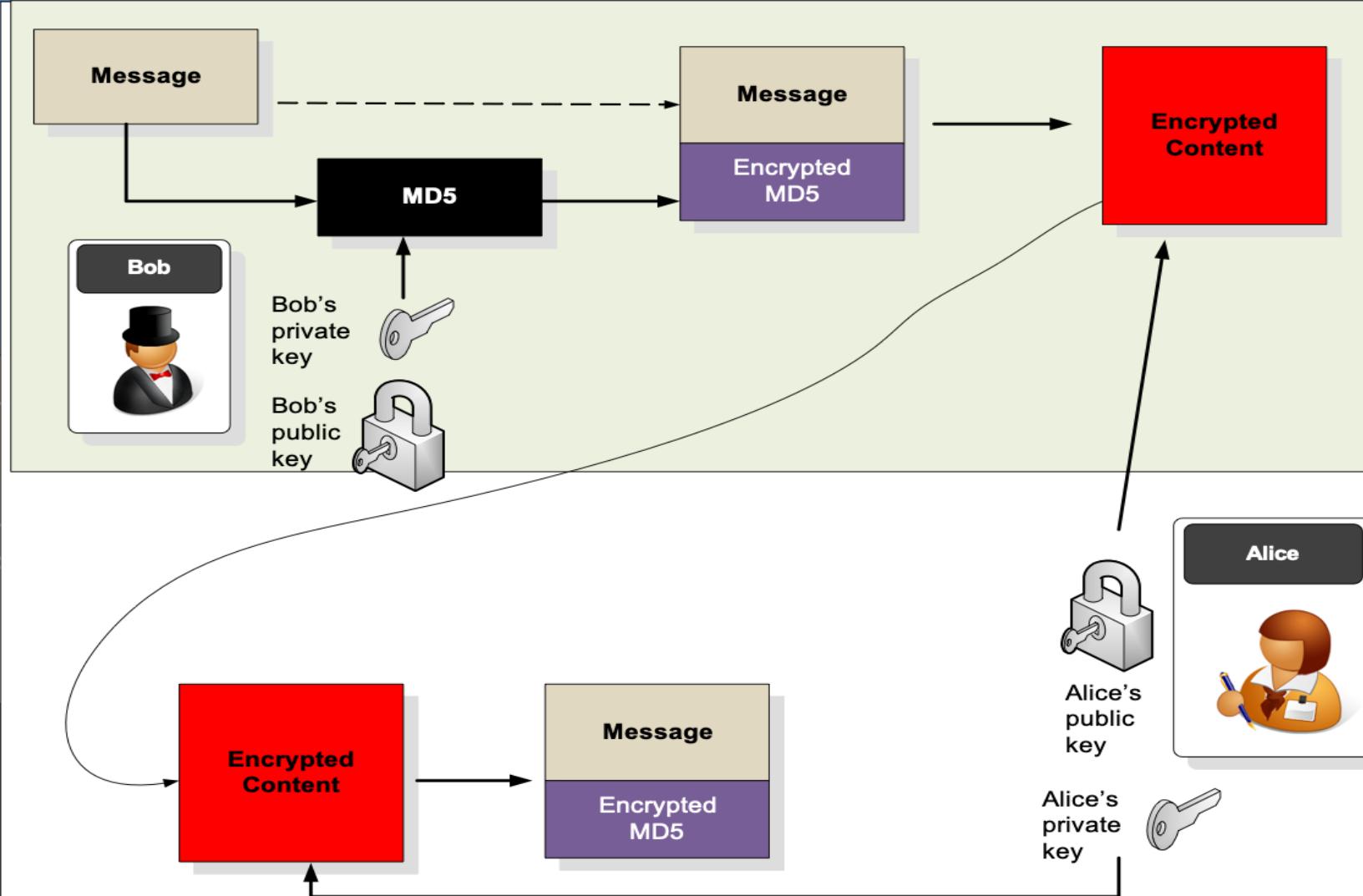


Author: Prof Bill Buchanan

**Bob encrypts the message/hash with Alice's public key**

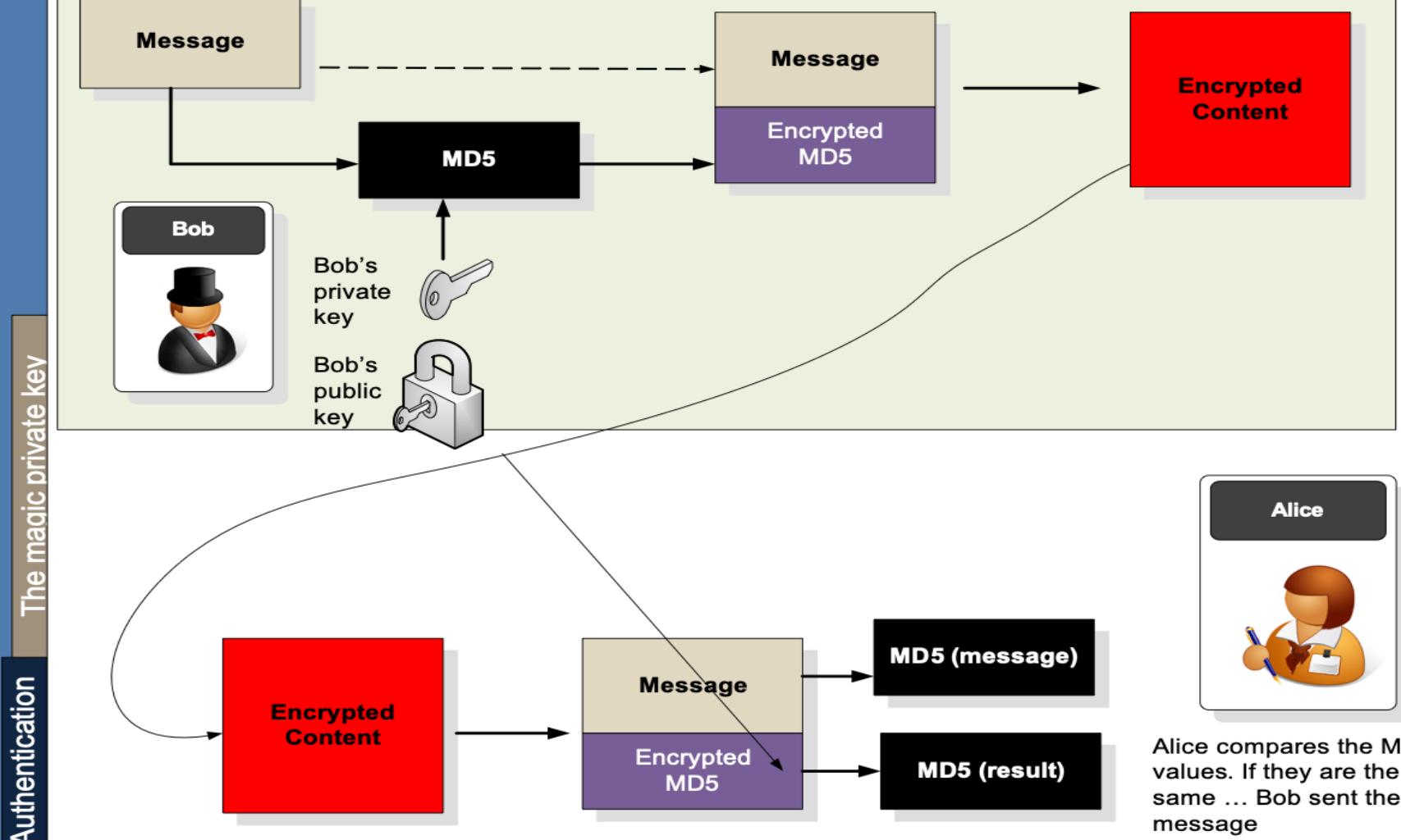
## Authentication

The magic private key



Author: Prof Bill Buchanan

Alice decrypts the message



Authenticator

The magic private key

Alice compares the MD5 values. If they are the same ... Bob sent the message

Author: Prof Bill Buchanan

Alice decrypts the message

# Chapter 6: Digital Certificates

Introduction

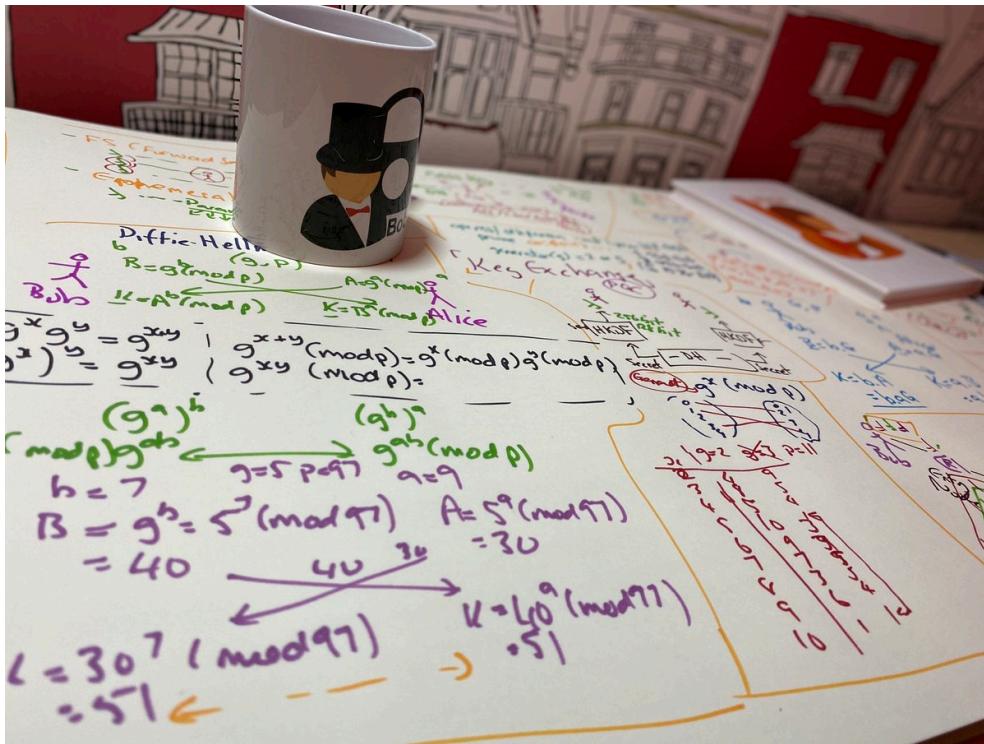
Authentication Methods

PKI

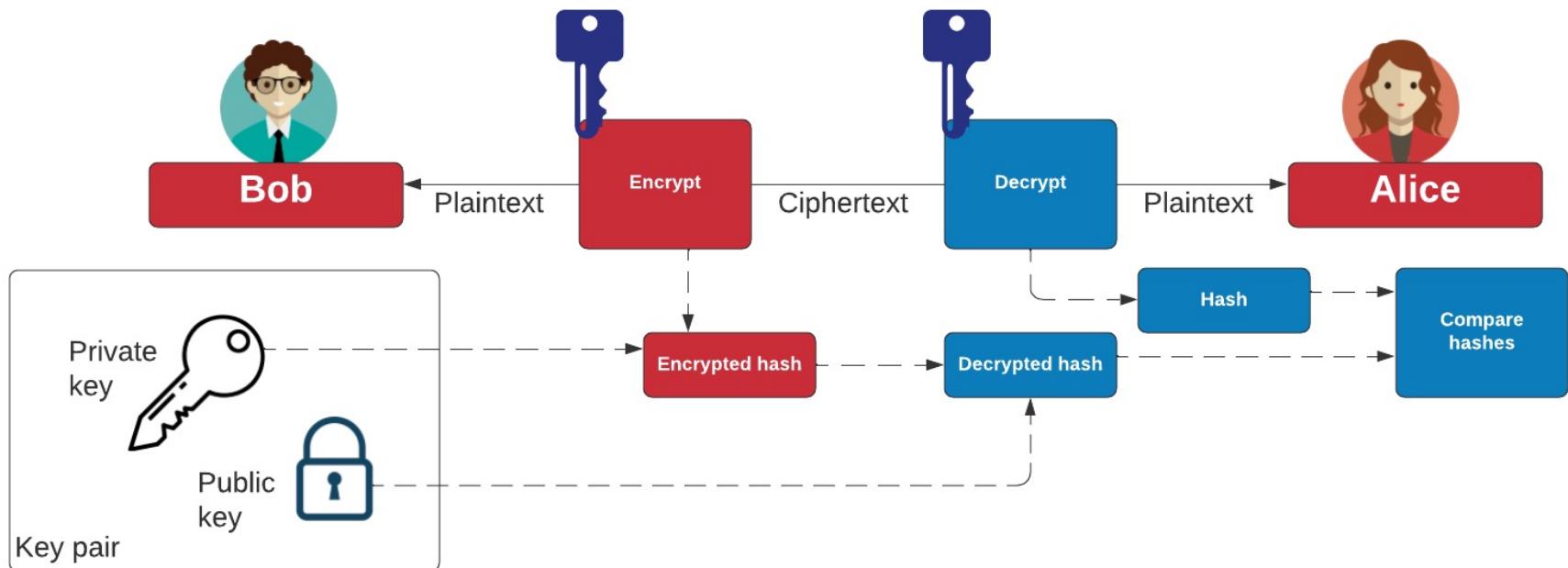
Digital Certificate Passing

**Prof Bill Buchanan OBE**

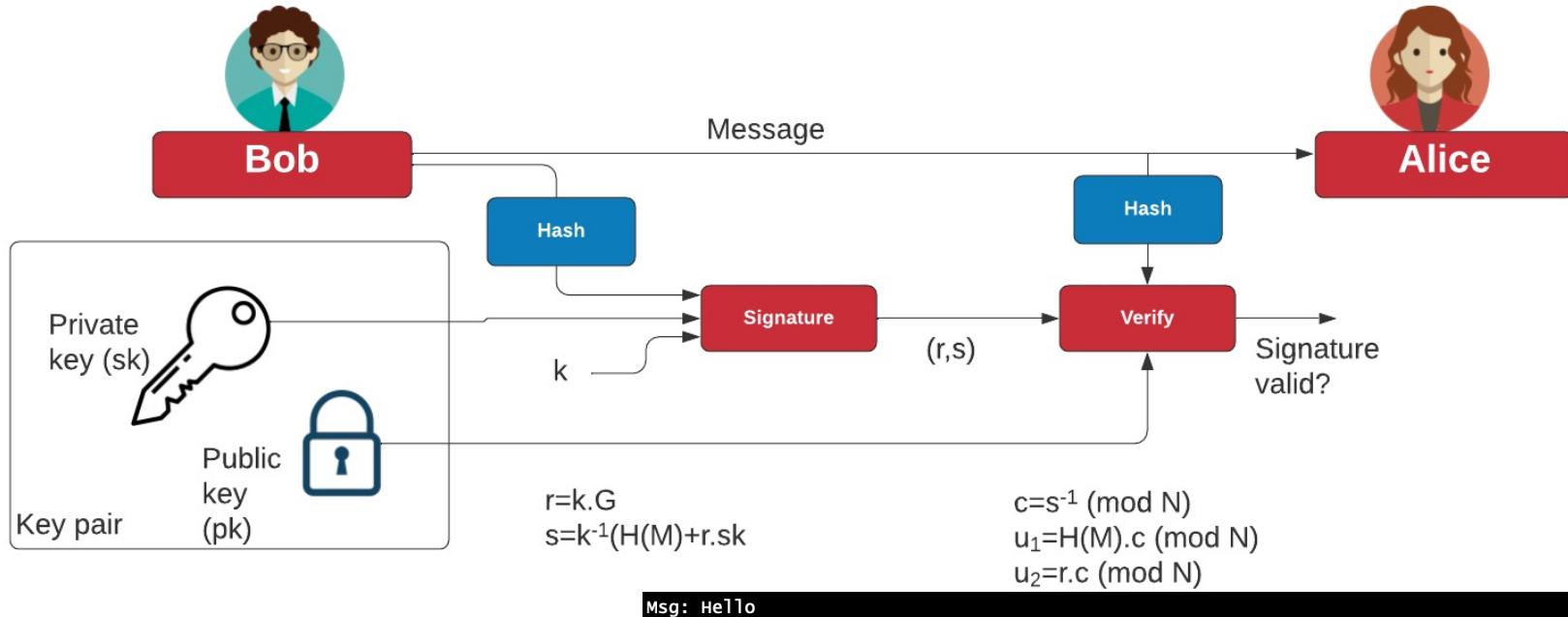
<https://asecuritysite.com/digitalcert/>



# Overview



# ECDSA



Msg: Hello

Alice's private key=91410319197544581782194931321068666964077231613962372395224337286787851207623  
Alice's public key=(107007219618086620558122760490508950019883614381385070624798268553636785085033,  
50295619771883464285297058390425887963371353465625215351103778057382666752225)  
k= 26701147302148539062679299392480227032483869521805022198405523431584788447963

r=9860780814777449203575356285408019661538158474047478294689777633119075968396  
s=99068437226471908177637999380627689653261729073056918331666171421799362411402

Result r=9860780814777449203575356285408019661538158474047478294689777633119075968396  
Signature matches!

# Digital Certificates

Introduction

Authentication Methods

PKI

Digital Certificate Passing

**Prof Bill Buchanan OBE**

<https://asecuritysite.com/digitalcert/>

