

# Digital Certificates

Introduction

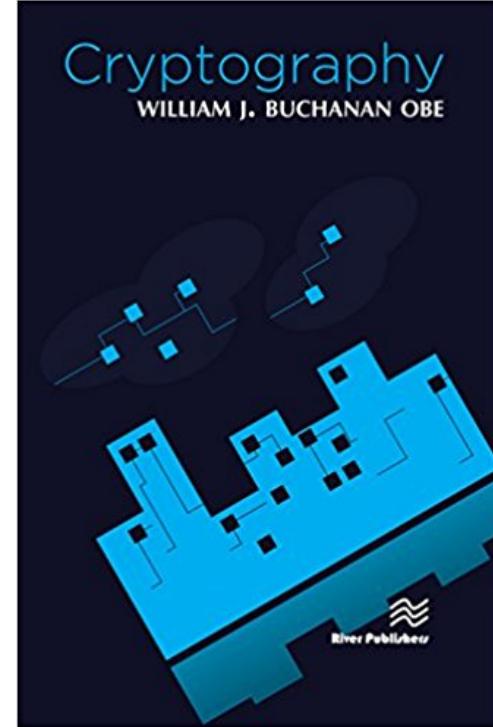
Authentication Methods

PKI

Digital Certificate Passing

**Prof Bill Buchanan OBE**

<http://asecuritysite.com/encryption>  
<http://asecuritysite.com/unit06>



# Digi Introduc Authent PKI Digital C

## Prof E

<http://as>  
<http://as>

No	Date	Subject	Lab
1	17 Jan 2020	Ciphers and Fundamentals <a href="#">Unit</a>	Lab <a href="#">[Link]</a> Demo <a href="#">[Link]</a>
2	24 Jan 2020	Symmetric Key <a href="#">Unit</a>	Lab <a href="#">[Link]</a> Demo <a href="#">[Link]</a>
3	31 Jan 2020	Hashing and MAC <a href="#">Unit</a>	Lab <a href="#">[Link]</a>
4	7 Feb 2020	Asymmetric (Public) Key <a href="#">Unit</a>	Lab <a href="#">[Link]</a>
5	14 Feb 2020	Key Exchange <a href="#">Unit</a>	Lab <a href="#">[Link]</a>
6	21 Feb 2020	Guest lecture	Mini-project/Coursework <a href="#">[Link]</a>
7	28 Feb 2020	Trust and Digital Certificates <a href="#">Unit</a>	Lab <a href="#">[Link]</a>
8	6 Mar 2020	Tunnelling <a href="#">Unit</a>	Lab <a href="#">[Link]</a>
9	13 Mar 2020	Test 1 (Units 1-5) <a href="#">[Study guide]</a>	
10	20 Mar 2020	Blockchain <a href="#">Unit</a>	Lab <a href="#">[Link]</a>
11	27 Mar 2020	Future Cryptography <a href="#">Unit</a>	Lab <a href="#">[Link]</a>
12	3 April 2020	Tokens, Authorization and Docker <a href="#">Unit</a>	Lab <a href="#">[Link]</a>
13	10 April 2020	Trusted Hosts <a href="#">Unit</a>	
Easter Break			
14	Week beginning 27 April 2020 (TBC)	Test 2 (Units 6-10)	
15	Week beginning 4 May 2020 (TBC)	Coursework Hand-in <a href="#">[Draft]</a>	





# Identity on the Internet

Identifies it is trusted  
(Digital Certificate)

Keeps communications  
secure (encryption)

Firefox

P Accept Online Payments And Mobile Pa... +

PayPal, Inc. (US) | https://www.paypal.com/uk/webapps/mpp/home-merchant

You are connected to  
**paypal.com**  
which is run by  
**PayPal, Inc.**  
San Jose  
California, US  
Verified by: VeriSign, Inc.

The connection to this website is secure.

More Information...

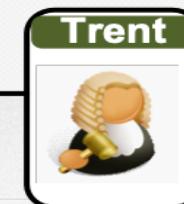
However you do business, PayPal gets you paid.  
Choose your payment solution, you can switch any time.

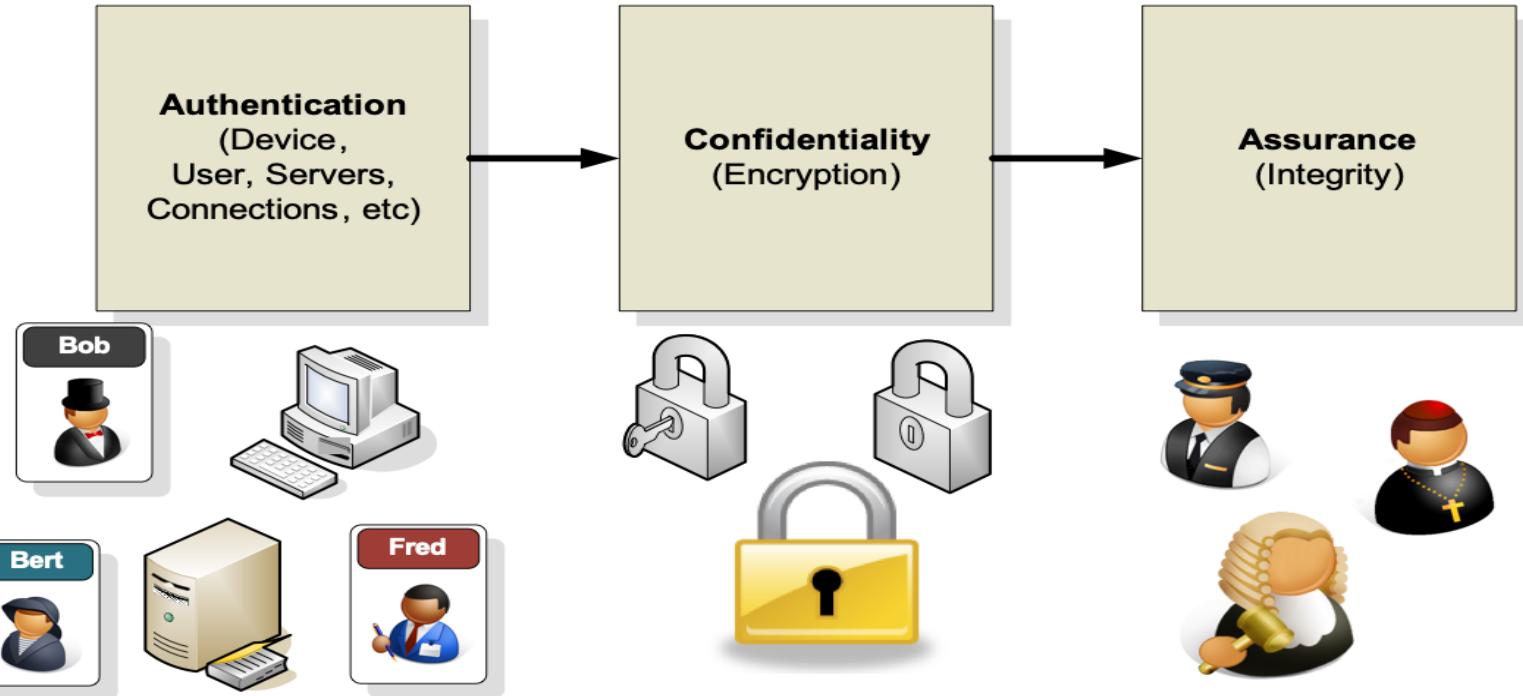
Accept card payments anywhere with PayPal Here™ [Learn More](#)

Eve

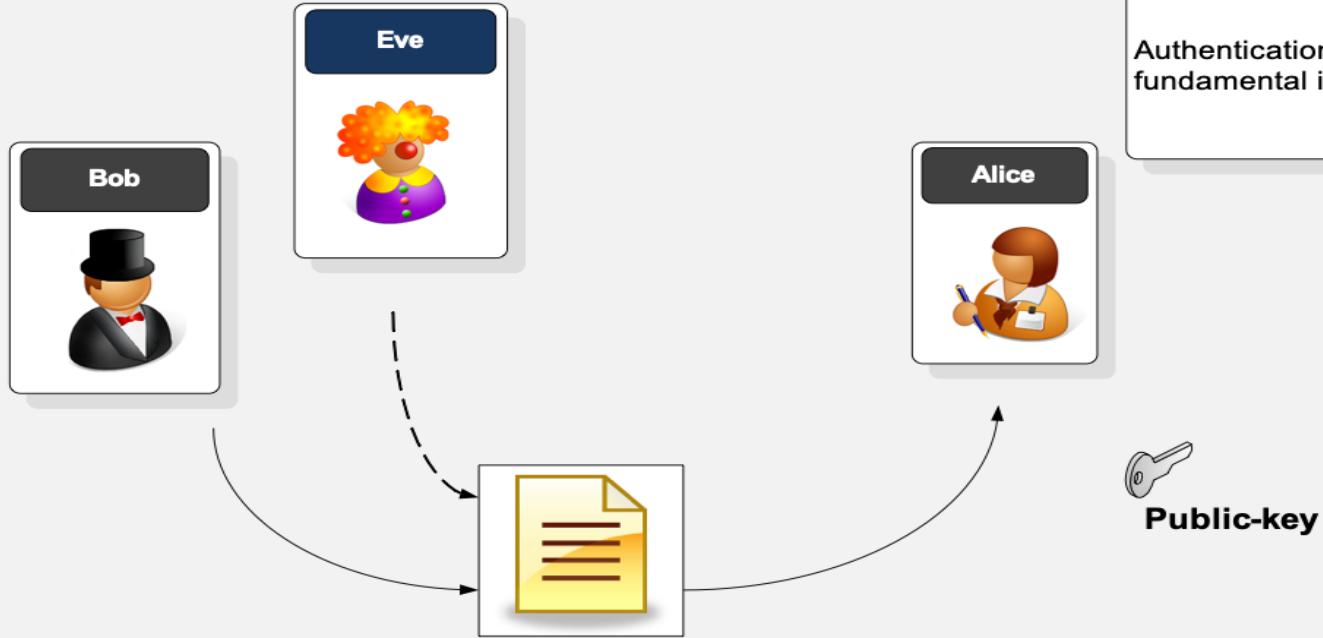


Bob



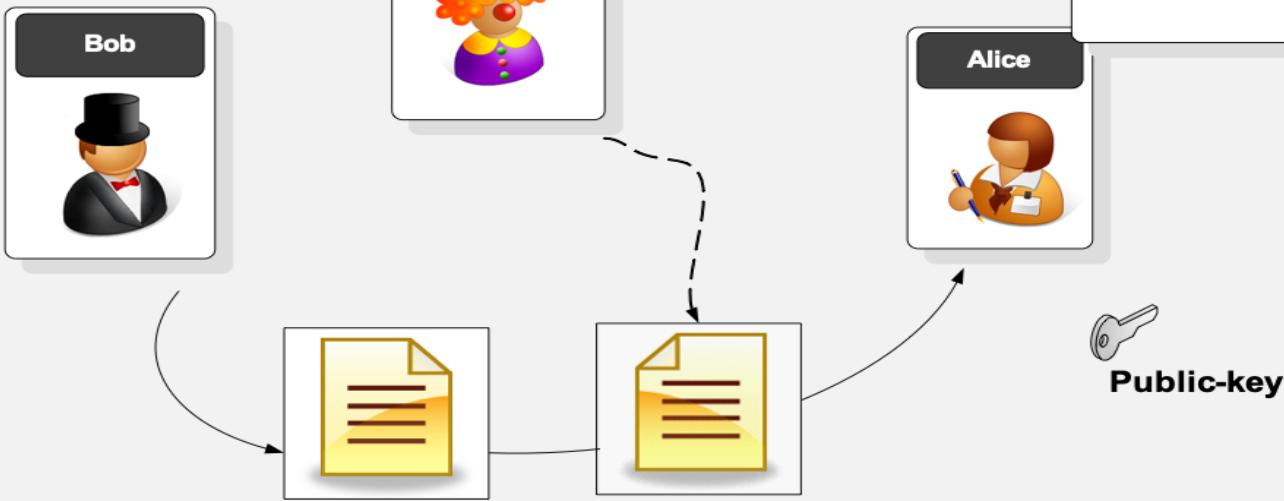


Authentication is a fundamental issue in security.



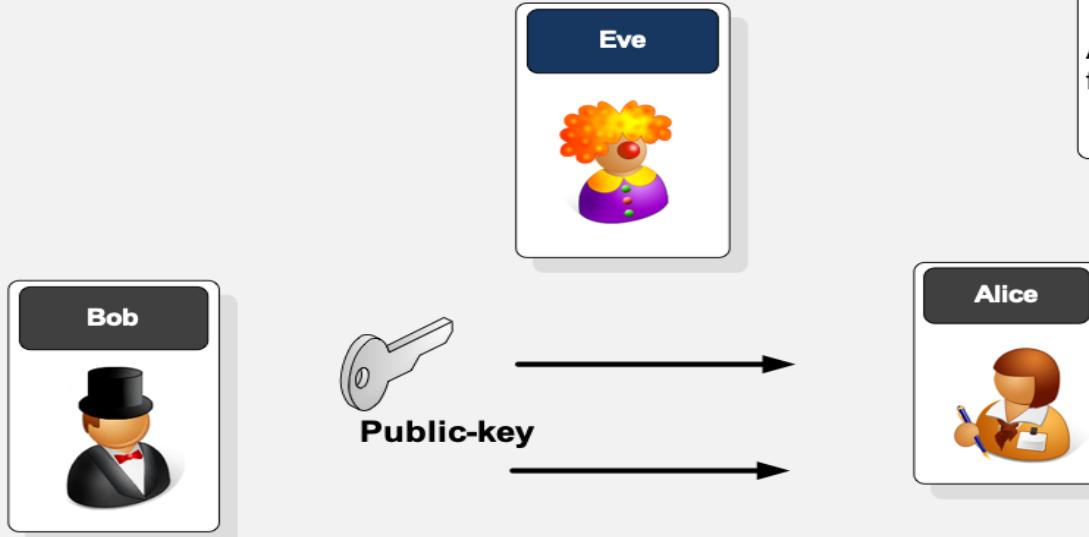
**How do we know that it was really Bob who sent the data , as anyone can get Alice's public key , and thus pretend to be Bob?**

Authentication is a fundamental issue in security.

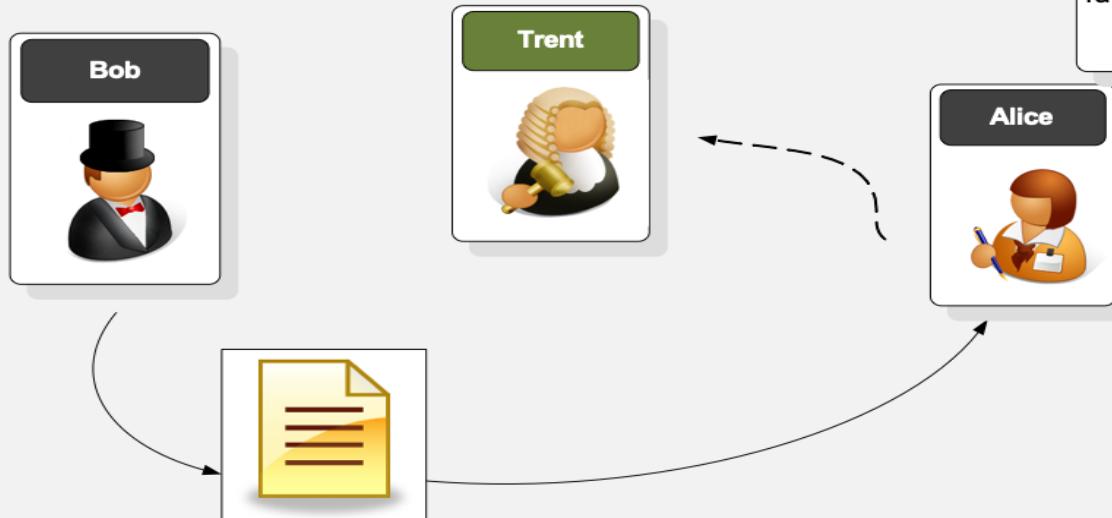


**How can we tell that the message has not been tampered with ?**

Authentication is a fundamental issue in security

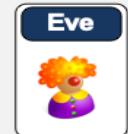


**How does Bob distribute his public key to Alice, without having to post it onto a Web site or for Bob to be on-line when Alice reads the message?**



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

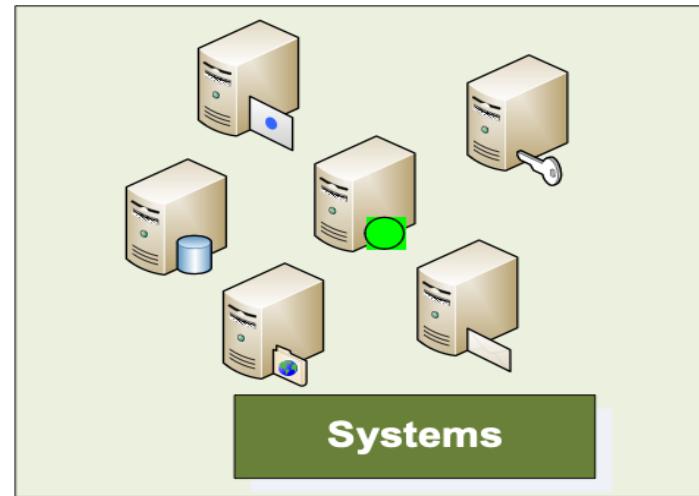
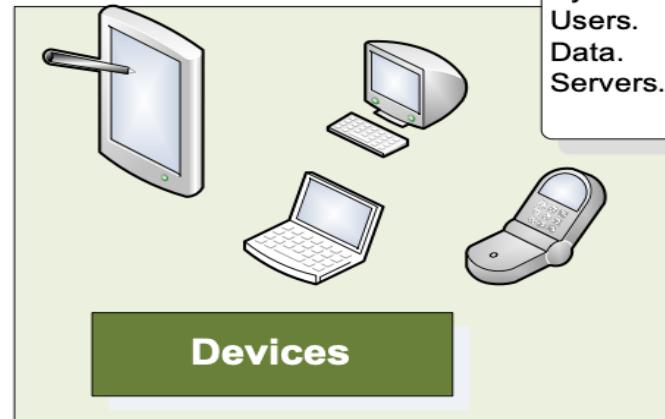
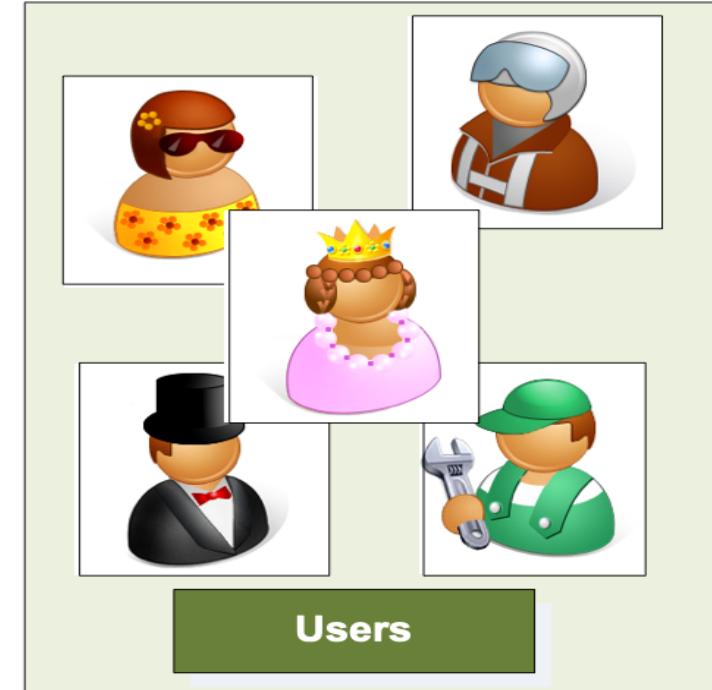
Authentication Methods

**Prof Bill Buchanan OBE**

<http://asecuritysite.com/crypto06>

<http://asecuritysite.com/encryption>





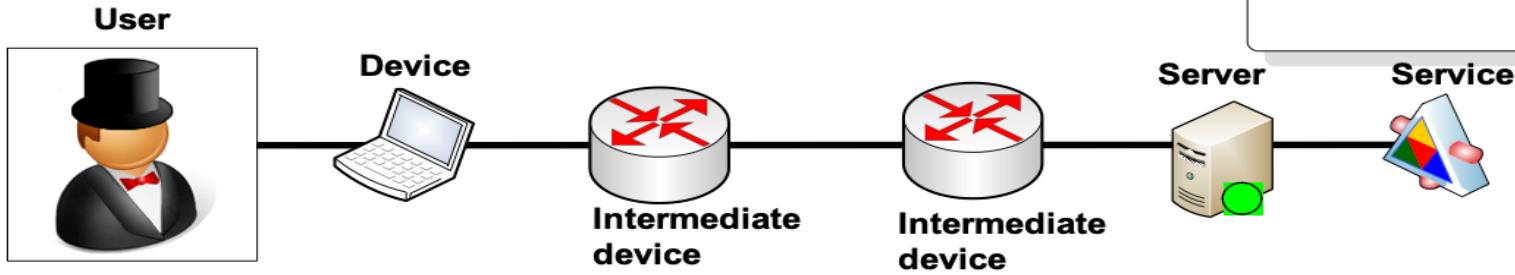
## What to authenticate?

Systems.  
Users.  
Data.  
Servers.

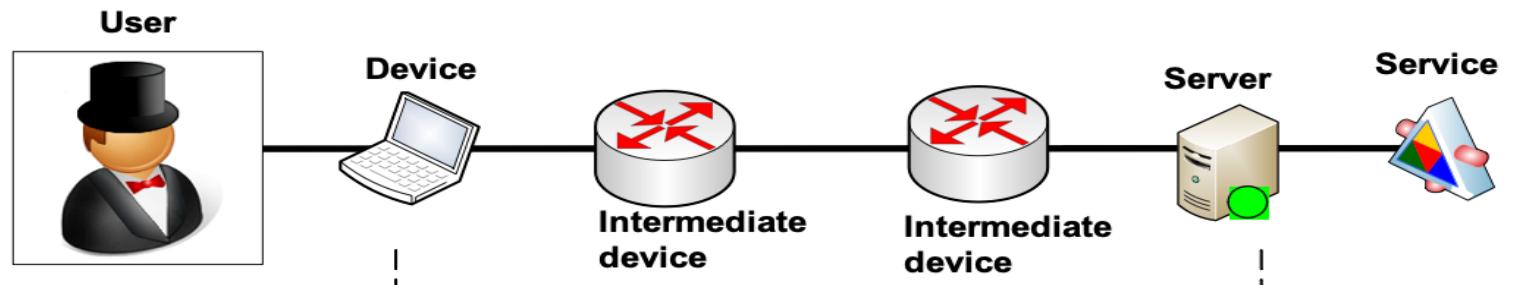
## Where authenticated?

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

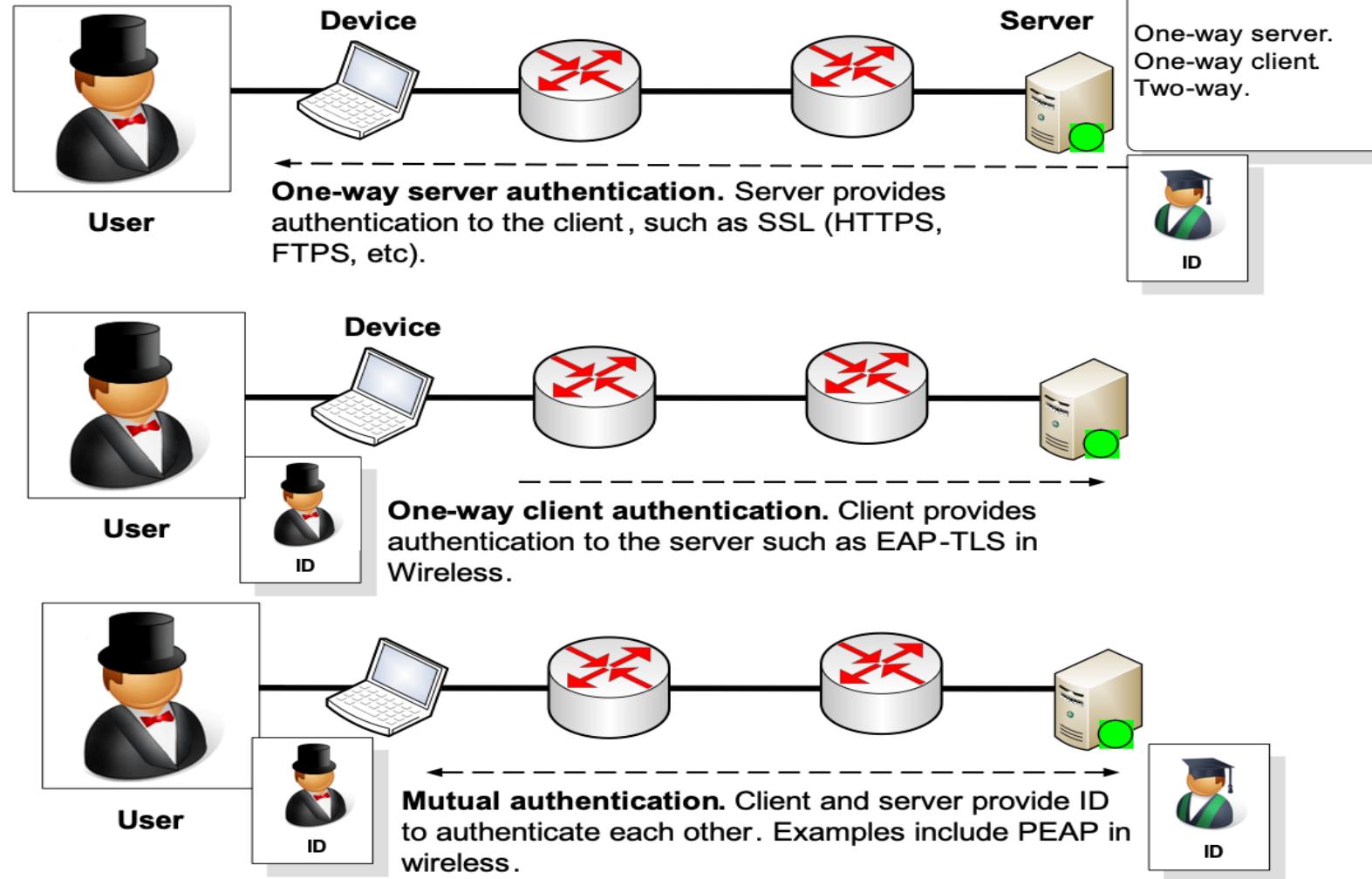
Authentication Methods



End-to-end authentication



Intermediate authentication



## Authentication

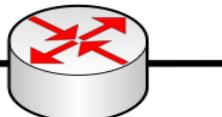
### User



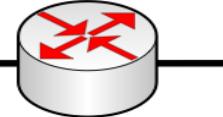
### Device



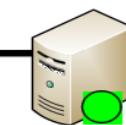
### Intermediate device



### Intermediate device



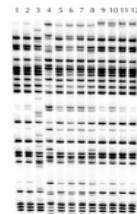
### Server



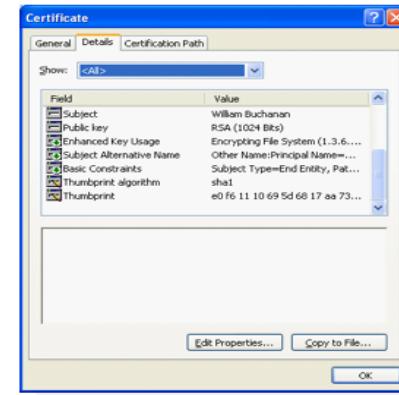
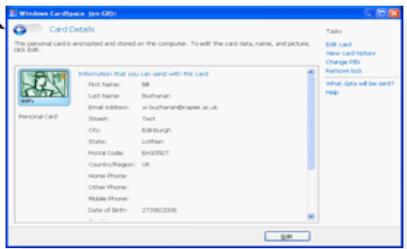
### Service

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

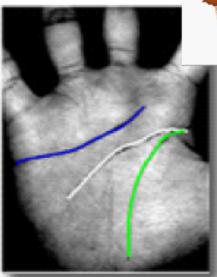


Retina scan



Finger prints

Iris scans



Palm prints

**Something you are**



Username/  
password



Digital certificate



Smart card

Network/physical  
address

**Something you  
have**



Mother's maiden name

**Something you  
know**

# Digital Certificates

Introduction

Authentication Methods

PKI

Digital Certificate Passing

**Prof Bill Buchanan OBE**

<http://asecuritysite.com/crypto06>

<http://asecuritysite.com/encryption>



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?



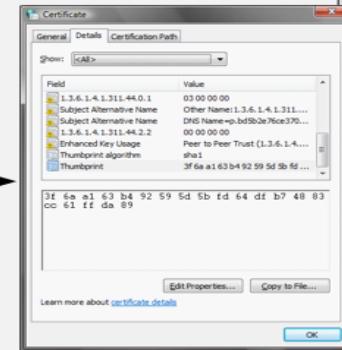
Public-key



## 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 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

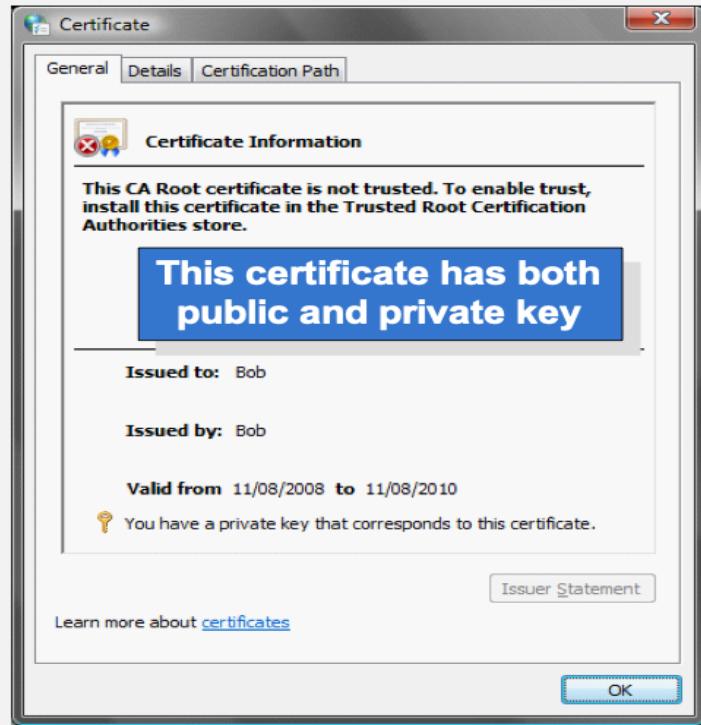
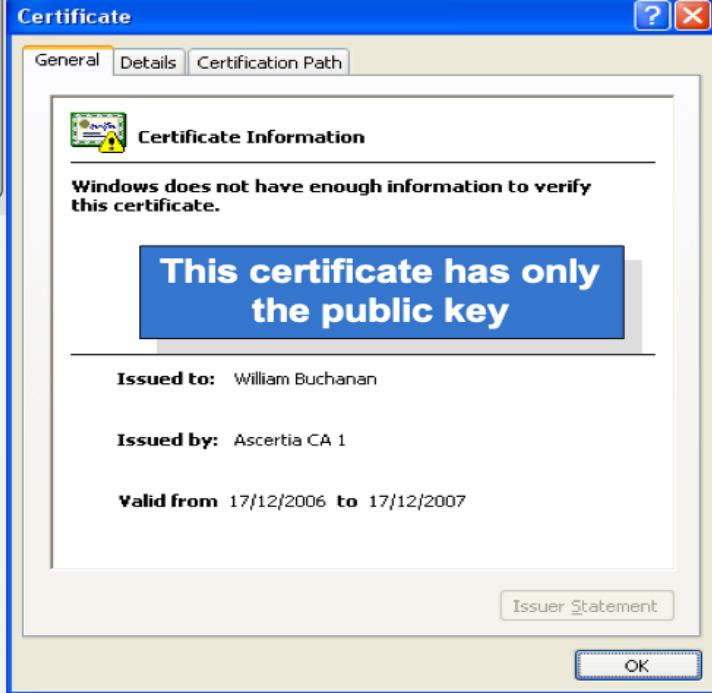
Issuer

Edit Properties...

Copy to File...

OK

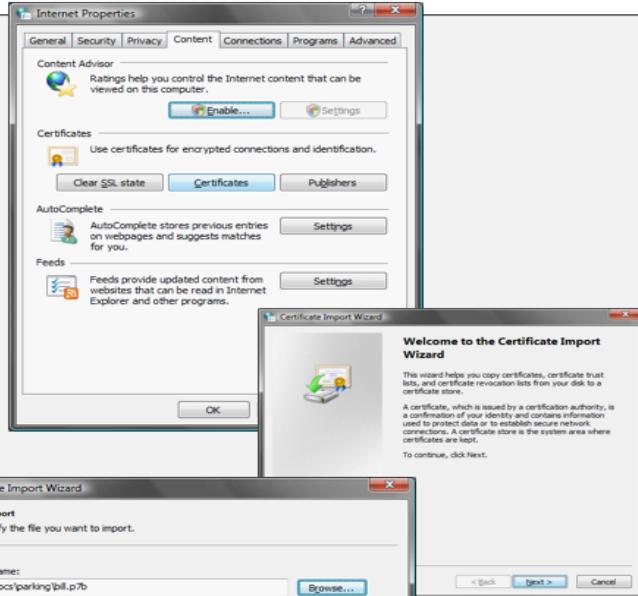
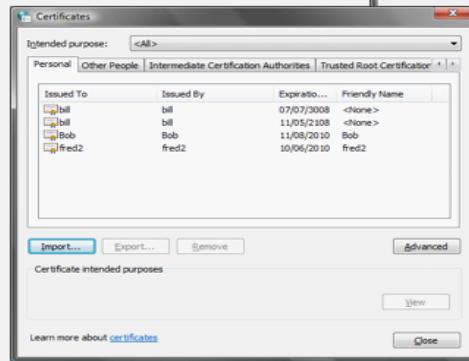
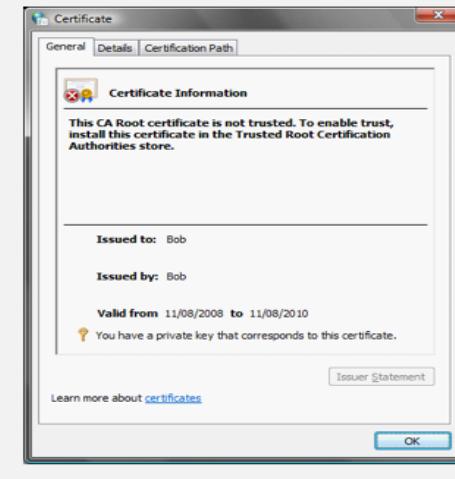
Digital certificate contains a thumbprint to verify it

**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 1UECxMCsvQxtAxBgNVBAMTdpbgxpVw 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 4EFgQUzy/YccJwT5opPHLPIcqkkolkjwwyyvDR 0j
BFwwloAU1P 5Zh0V700k6 CorvRMwB9ifvkBmhP6Q9MDsxC2AjB9NVBAYTAKdCMREW
DwYDQVQKEwhB 2N1cnRpYTEZMBcGA 1UEAxMQXNzjZXJ 0awEgum9vdCBQYIBDTBN
BgNvHR8ERjBEMEkQKA+hjxodhrwo1 8vd3d3LmfjzY2vydG1hlmNbVs 5pbpxbmVD
QS9jcmxzL0FzY2vydglhQ 0ExL3nSYXNzMS 5jcmrwPgYIKWvBQHUQAQEMJAWMC 4G
CCsGAQFBzAChiJodhrwo1 8vb2Nzcc5nbG9iYwx0cnvzdgZpbmr1ci 5j2b2v0mAOG
CSqGSib 3DQEBBQAA0EATOCwGJ 1t50kt1upmpjkM1 8idxMmD5wuhszb1GsMhPxI
H+vXhL9yaOw+Prpz7aJS4/3xxu8vRAnhyu 9yu4qDA==
-----END CERTIFICATE-----
```



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

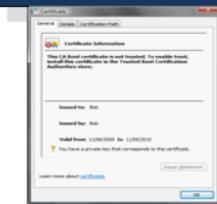


- A. Bob creates the message.
- B. Bob encrypts with Alice's public key and sends Alice the encrypted message
- C. Alice decrypts with her private key
- D. Alice receives the message



Hello

H&\$d .

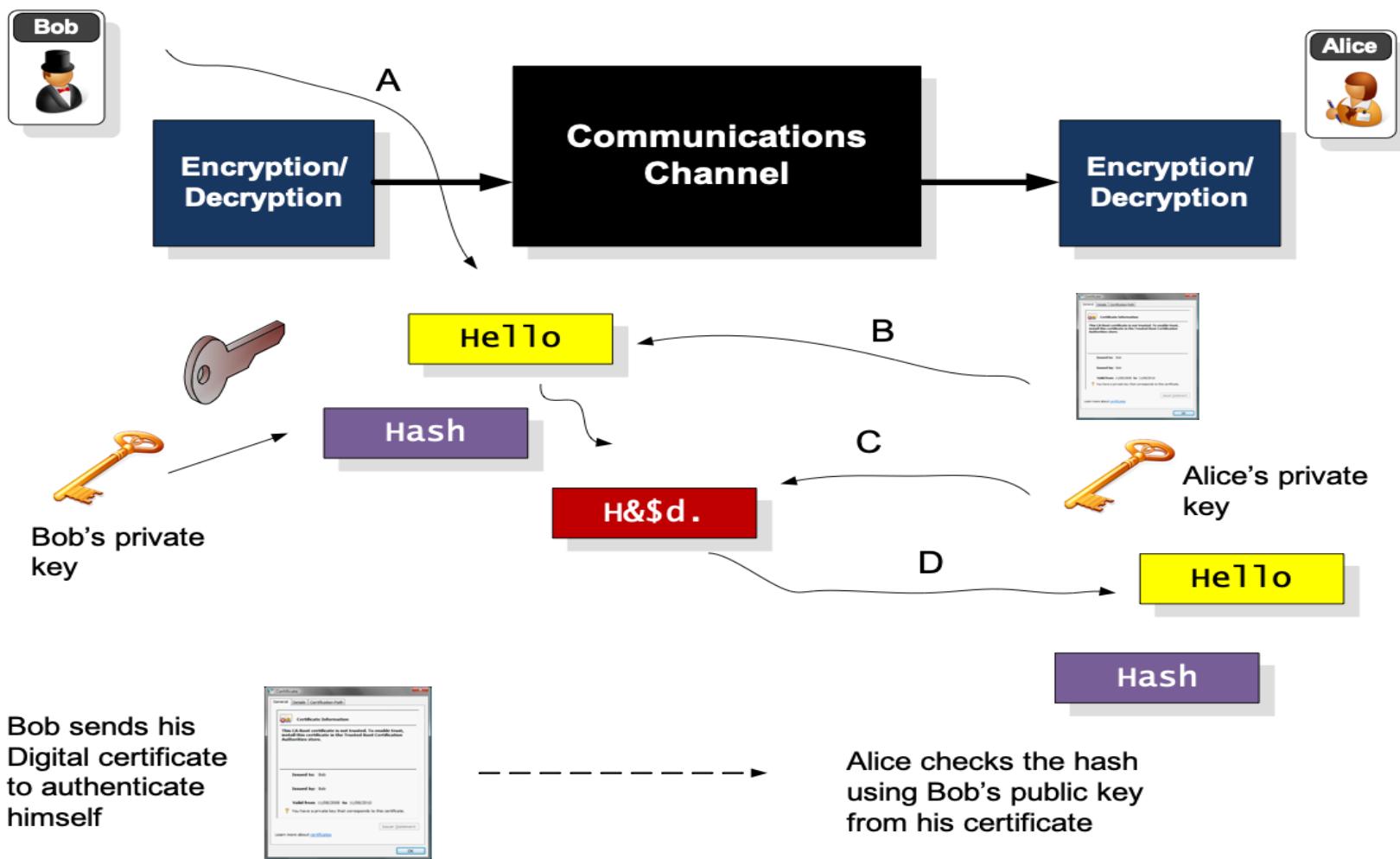


Alice sends her digital certificate with her public key on it



Alice's private key

Hello



Bob sends his Digital certificate to authenticate himself



Alice checks the hash using Bob's public key from his certificate

# Digital Certificates

Introduction

Authentication Methods

PKI

Certificate Creation

Digital Certificate Passing

**Prof Bill Buchanan OBE**

<http://asecuritysite.com/crypto06>

<http://asecuritysite.com/encryption>



asecuritysite.com

Your connection to this site is private.

Permissions

Connection



The identity of this website has been verified by Go Daddy Secure Certificate Authority - G2. No Certificate Transparency information was supplied by the server.

[Certificate information](#)



Your connection to asecuritysite.com is encrypted using an obsolete cipher suite.

The connection uses TLS 1.0.

The connection is encrypted using AES\_128\_CBC, with HMAC-SHA1 for message authentication and RSA as the key exchange mechanism.

[What do these mean?](#)

- Coding. [Coding](#). The
- Challenges. [Challen](#)
- IP. [IP](#). These pages
- Information. [Info](#).
- Fun. [Fun](#). These pac
- Introduction to Se
- SQL Statements. [S](#)
- File and Network
- Cisco Simulators.
- Install on Android
- Wireless. [Wireless](#)

### Certificate

General

Details

Certification Path

#### Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- 2.16.840.1.114413.1.7.23.1

\* Refer to the certification authority's statement for details.

**Issued to:** asecuritysite.com

**Issued by:** Go Daddy Secure Certificate Authority - G2

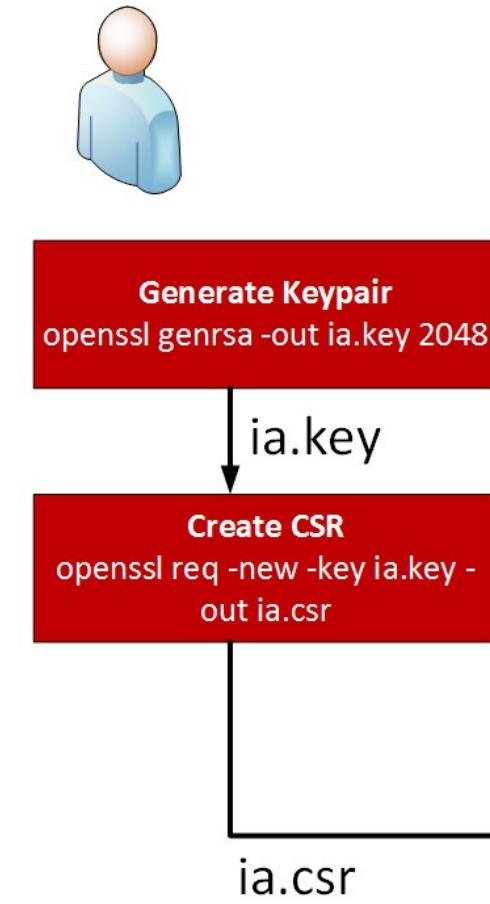
**Valid from** 20- Sep- 15 **to** 20- Sep- 16

[Issuer Statement](#)

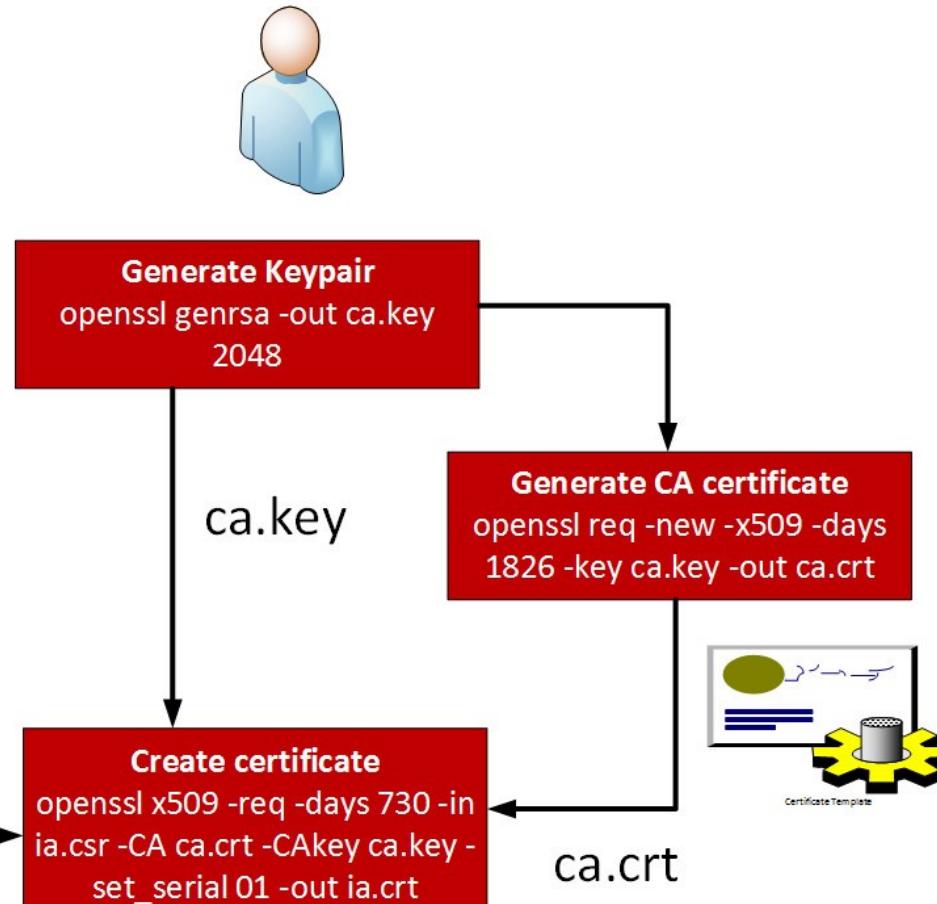
Learn more about [certificates](#)

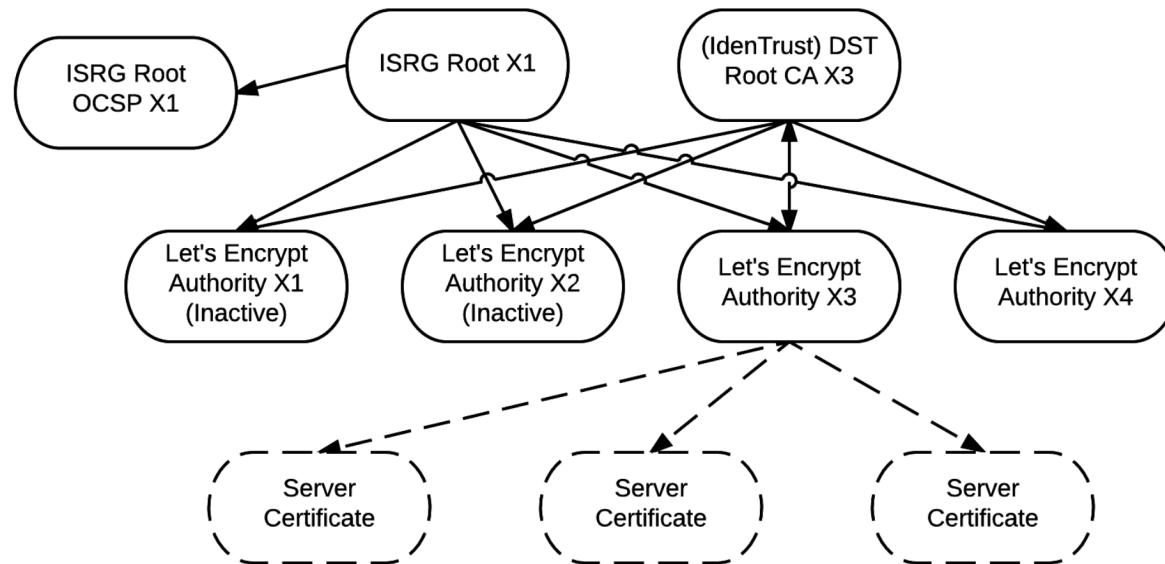
OK

## Organisation



## Root CA





## PEM

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

```
MIIEwTCCA6mgAwIBAgIRA093GGFLfHw0CAAAAAAucZgwDQYJKoZIhvCNQELBQAw
QjELMAkGA1UEBhMCVVMxHjAcBgNVBAoTFUdvb2dsZSBucnVzdCBTZJ2aN1czET
MBEGA1UEAxMKR1RTIENBIDFPMTAeFw0yMDAyMTIxMTQ3NDFaFw0yMDA1MDYxMTQ3
NDFaMGgxCzAJBgNVBAYTA1VTMRMwEQYDVQQIEwpDYWxpZm9ybmlhMRYwFAYDVQQH
Ew1Nb3VudGFpbibWaWV3MRMwEQYDVQQKEwpHb29nbGUgTeXDMRcwFQYDVQQDEw53
d3cuZ29vZ2xLLmNvbTBZMBMGBYqGSM49AgEGCCqGSM49AwEHA0IABCzzLJYFjb8W
TpQxWL0TySDvfEWCKMe7l81CFspT60kn13YILndTM22sUwPycyogKjBSaQZ9Axi
hCeGEAIjkbejjgJVMICUTA0BgNVHQ8BAf8EBAMCB4AwEwYDVR0lBAwwCgYIKwYB
BQUH AwEwDAYDVR0TAQH/BAIwADAdBgNVHQ4EFgQU9Ty3t90o7UW9+Hc6kv/j9511
BBwwHwYDVR0jBBgwFoAUmnH4bhDrz5vsYJ8YkBug630J/SswZAYIKwYBBQUHAQEE
WDBWMCCGCCsGAQUFBzABhtodHRw0i8vb2NzcC5wa2kuZ29vZy9ndHMxbzEwKwYI
KwYBBQUHMAKGH2h0dHA6Ly9wa2kuZ29vZy9nc3IyL0dUUzFPMS5jcnQwGQYDVR0R
BBIwEI0d3d3Lmdvb2dsZS5jb20wIqYDVR0gBBowGDAIBgZngQwBAgIwDAYKKwYB
BAHWeQIFAzAvBgNVHR8EKDAmMCsgIqAghh5odHRw0i8vY3jsLnBraS5nb29nL0dU
UzFPMS5jcmwgEFBgorBgeEAdZ5AgQCBIH2BIHzaPEAdgCyHgXMi6LNiiB0h2b5
K7mKJSBna9r6c0eySVMt74u0XgAAAXA5cNqwAAAЕawBHMEUCIQCojKtz0e8l1JYK
HmKnbt1puqT4AE3peMVAVk/WewGp10IgbvRMbNkwF6i8+jVv3CfTHKvFd8e00+GY
PbXJZb1drKEAdwBep3P531bA57U2SH30SeAyepGaDIShEhKEGHWwgXFFWAAAAXA5
cNrLAAAЕawBIMEYCIQCQSONppELPODh65oFT5ZAGsSQz4FsjNNZedgS7WqzLnQIh
AMAru0QuuoE3RWngfhI6W7n1kxxEmd0vSZTe6+Ql+jVuMA0GCSqGSIB3DQEBCwUA
A4IBAQCDU8CVusGstVk1lAmrtg3DyYhNV1UnKyLk3RrHKumwYz5mC25bWGoLVKvv
pxxBN3zA329/9JZq0mnn0vmPMxjTDvh9sVQ7g4znwha/KJfzL8AZKUDldD90+hD0
tlHtqVqITZPCAI/ANvbHdZiMEEPB8eA+oTiw2ucChqlLsop5Mio8ckg7aXG4/qFc
AIDbvkoFFK44rs4UEpsaqGe9QmjTu07ZCZrFd1m3geq2ARKPHgPoPM6UbDdqg0
TNQo9C0F5Z10k0gV/qshvpT04YzE7TB2U571eYEqNXH48syVx8XSk3P7FjM7FI22
IzbJSEipZJm8DsP10ffFxptoIn+zKoQAxAA==
```

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

## PKCS#7

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

```
MIIE8gYJKoZIhvCNQCoIE4zC0Iw0BBwGgggTFC0Iw0BBwGgggTFC0Iw0BBwGgggTFC0
wTCCA6mgAwIBAgIRA093GGFLfHw0CAAAAAAucZgwDQYJKoZIhvCNQELBQAw
MAKGA1UEBhMCVVMxHjAcBgNVBAoTFUdvb2dsZSBucnVzdCBTZJ2aN1czET
A1UEAxMKR1RTIENBIDFPMTAeFw0yMDAyMTIxMTQ3NDFaFw0yMDA1MDYxMTQ3
MGgxCzAJBgNVBAYTA1VTMRMwEQYDVQQIEwpHb29nbGUgTeXDMRcwFQYDVQQDEw53
b3VudGFpbibWaWV3MRMwEQYDVQQKEwpHb29nbGUgTeXDMRcwFQYDVQQDEw53
Z29vZ2xLLmNvbTBZMBMGBYqGSM49AgEGCCqGSM49AwEHA0IABCzzLJYFjb8W
WL0TySDvfEWCKMe7l81CFspT60kn13YILndTM22sUwPycyogKjBSaQZ9Axi
EAiJkbejjgJVMICUTA0BgNVHQ8BAf8EBAMCB4AwEwYDVR0lBAwwCgYIKwYB
AwEwDAYDVR0TAQH/BAIwADAdBgNVHQ4EFgQU9Ty3t90o7UW9+Hc6kv/j9511
HwYDVR0jBBgwFoAUmnH4bhDrz5vsYJ8YkBug630J/SswZAYIKwYBBQUHAQEE
McC GCCsGAQUFBzABhtodHRw0i8vb2NzcC5wa2kuZ29vZy9ndHMxbzEwKwYI
BQUHMAKGH2h0dHA6Ly9wa2kuZ29vZy9nc3IyL0dUUzFPMS5jcnQwGQYDVR0R
EII0d3d3Lmdvb2dsZS5jb20wIqYDVR0gBBowGDAIBgZngQwBAgIwDAYKKwYB
eQIFAzAvBgNVHR8EKDAmMCsgIqAghh5odHRw0i8vY3jsLnBraS5nb29nL0dU
MS5jcmwgEFBgorBgeEAdZ5AgQCBIH2BIHzaPEAdgCyHgXMi6LNiiB0h2b5
JSBna9r6c0eySVMt74u0XgAAAXA5cNqwAAAЕawBHMEUCIQCojKtz0e8l1JYK
bt1puqT4AE3peMVAVk/WewGp10IgbvRmbNkwF6i8+jVv3CfTHKvFd8e00+GY
Zb1drKEAdwBep3P531bA57U2SH30SeAyepGaDIShEhKEGHWwgXFxFWAAAAXA5
AAAЕawBIMEYCIQCQSONppELPODh65oFT5ZAGsSQz4FsjNNZedgS7WqzLnQIh
u0QuuoE3RWngfhI6W7n1kxxEmd0vSZTe6+Ql+jVuMA0GCSqGSIB3DQEBCwUA
A0CDU8CVusGstVk1lAmrtg3DyYhNV1UnKyLk3RrHKumwYz5mC25bWGoLVKvv
N3zA329/9JZq0mnn0vmPMxjTDvh9sVQ7g4znwha/KJfzL8AZKUDldD90+hD0
qVqITZPCAI/ANvbHdZiMEEPB8eA+oTiw2ucChqlLsop5Mio8ckg7aXG4/qFc
vkoffK44rs4UEpsaqGe9QmjTu07ZCZrFd1m3geq2ARKPHgPoPM6UbDdqg0
9C0F5Z10k0gV/qshvpT04YzE7TB2U571eYEqNXH48syVx8XSk3P7FjM7FI22
SEipZJm8DsP10ffFxptoIn+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
```

## PEM

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

MIIewTCCA6mgAwIBAgIRA093GGFLfHw0CAAAAAAucZgwDQYJKoZIhvCNQELBQA...  
QjELMAkGA1UEBhMCVVMxHjAcBgNVBAoTFUdvb2dsZSBucnVzdCBTZJ2aWNlcET  
MBEGA1UEAxMKR1RTIENBIDFPMTAeFw0yMDAyMTIxMTQ3NDFaFw0yMDA1MDYxMTQ3  
NDFaMGgxCzAJBgNVBAYTA1VTMRMwEQYDVQQIEwpDYWxpZm9ybmlhMRYwFAYDVQQH  
Ew1Nb3VudGFpbibWaWV3MRMwEQYDVQQKEwpHb29nbGUgTEXDMRcwFQYDVQQDEw53  
d3cuZ29vZ2x1LmNvbTBZMBMGBYqGSM49AgEGCCqGSM49AwEHA0IABCzzLJYFjb8W  
Tb0xWL0TvsDvfEWCKMe71816CspT60kn113YT1ndTM22slwPvcycokKiBSa070Axi

- X.509 Certificate (PEM)
- 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.

AIDbvkoFF44rs4UEpsaqGe90qMJjTu07ZCZrFd1m3geq2ARKPHgPoPM6UbDdqg0  
TNQoC0F5Zl0k0gV/qshvpT04YzE7TB2U571eYEqNXH48syVx8XSk3P7FjM7FI22  
IzbJSEipZJm8DsP10ffFXpToIn+zKoQAxAA==  
-----END CERTIFICATE-----

## PKCS#7

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

MIIe8gYJKoZIhvCNQCoIE4zC...  
wTCCA6mgAwIBAgIRA093GGFLfHw0CAAAAAAucZgwDQYJKoZIhvCNQELBQA...  
MAKGA1UEBhMCVVMxHjAcBgNVBAoTFUdvb2dsZSBucnVzdCBTZJ2aWNlcET  
A1UEAxMKR1RTIENBIDFPMTAeFw0yMDAyMTIxMTQ3NDFaFw0yMDA1MDYxMTQ3  
MGgxCzAJBgNVBAYTA1VTMRMwEQYDVQQIEwpDYWxpZm9ybmlhMRYwFAYDVQQH  
b3VudGFpbibWaWV3MRMwEQYDVQQKEwpHb29nbGUgTEXDMRcwFQYDVQQDEw53  
Z29vZ2x1LmNvbTBZMBMGBYqGSM49AgEGCCqGSM49AwEHA0IABCzzLJYFjb8W  
WL0TySDvfEWCKMe7181CFspT60kn113YLndTM22sUwPcyogKjBSa0Z9Ax1  
EAiJkbejjgJVMICUTA0BgNVHQ8BAf8EBAMCB4AwEYDVRO1LBawwCgYIKwYB  
AwEYDVROTAQH/BAIwADAdBgNVHQ4EFgQU9Ty3t90u7UW9+Hc6kvJ9511  
HwYDVR0jBBgwFoAUmNH4bhDrz5vsYJ8YkBug630j/SswZAYIKwYBBQUHAQEE  
McC GCCsGAQUFBzAbhtodHRw0i8vb2Nzc5wa2kuZ29vZy9ndHMxbzEwKwYI  
BQUHMAKGh2h0dHA6Ly9wa2kuZ29vZy9nc3IyL0dUUzFPMS5jcnQwGQYDVRORE  
EII0d3d3Lmdvb2dsZS5jb20wIQYDVR0gB BowGDAIBgZngQwB AgIwDAYKKwYB  
eQIFAzAvBgNVHR8EKDAmMC SgIqAgh50dHRw0i8vY3jsLnBraS5nb29nL0dU  
MS5jcmwggeFBgorBgEEAdZ5AgQCBH2BIHzAPEAdgCyHgXMi6LNi1B0h2b5  
JSBna9r6c0eySvMt74uQXgAAAXA5cNwqAAAEAwBHMEUCIQCojKtz0e81JYK  
bt1puqT4AE3peMVAVk/WewGp10IgbvRmbNkwF6i8-JVv3CfTHKvFd8e00+GY  
Zb1drKEAdwBep3P531bA57U2SH30SeAyepGaDISH E hKEGHWgXFxFWAAAAXA5  
AAA AwBIMEYCIQCQS0NppELP0Dh65oFT5ZAGsSQz4FsjNNZedgS7WqzLnQIh  
u0QuoE3RWngfhI6W7n1kxkEmd0vSZTe6+Ql+jVuMA0GCSqGS1b3DQEBCwUA  
AQCDU8CVusGstV k1lAmrtg3DyYhN1UnKyLk3RrHKumwYz5mC25bWGoLVKvv  
N3zA329/9JZq0mnn0vmpMxjTDvh9sVQ7g4znwha/KJfzL8AZKUdldD90+hD  
qVqITZPCAI/ANvbhdZiMEEPB8eA+oTiw2ucChqlsop5Mio8ckg7aXG4/Qfc  
vkoffK44rs4UEpsaqGe90qMjjTu07ZCZrFd1m3geq2ARKPHgPoPM6UbDdqg0  
9C0F5Zl0k0gV/qshvpT04YzE7TB2U571eYEqNXH48syVx8XSk3P7FjM7FI22  
SEipZJm8DsP10ffFXpToIn+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

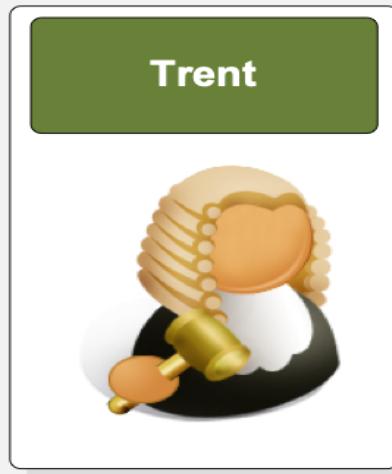
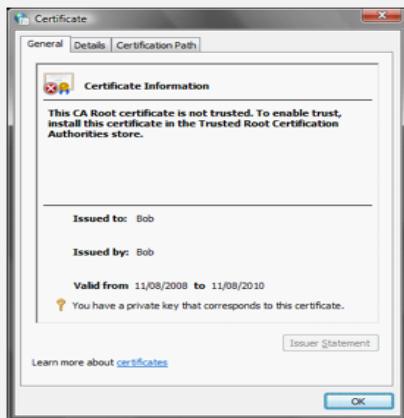
**Prof Bill Buchanan OBE**

<http://asecuritysite.com/crypto06>

<http://asecuritysite.com/encryption>



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



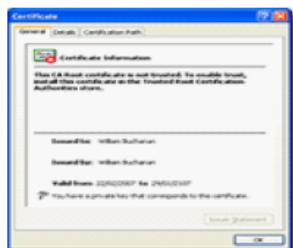
## Digital Certificates

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



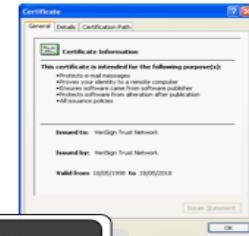
Trusted root certificates are installed as a default on the machine (or installed with the user's permission)

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.



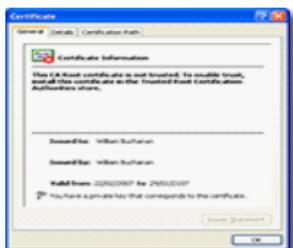
Author: Prof Bill Buchanan



## 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 Kozjegyzo (Class ...)	NetLock Kozjegyzo (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

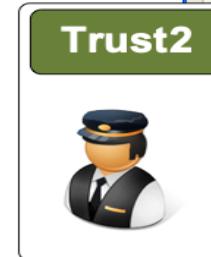
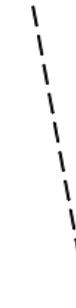
**Certificate Information**

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

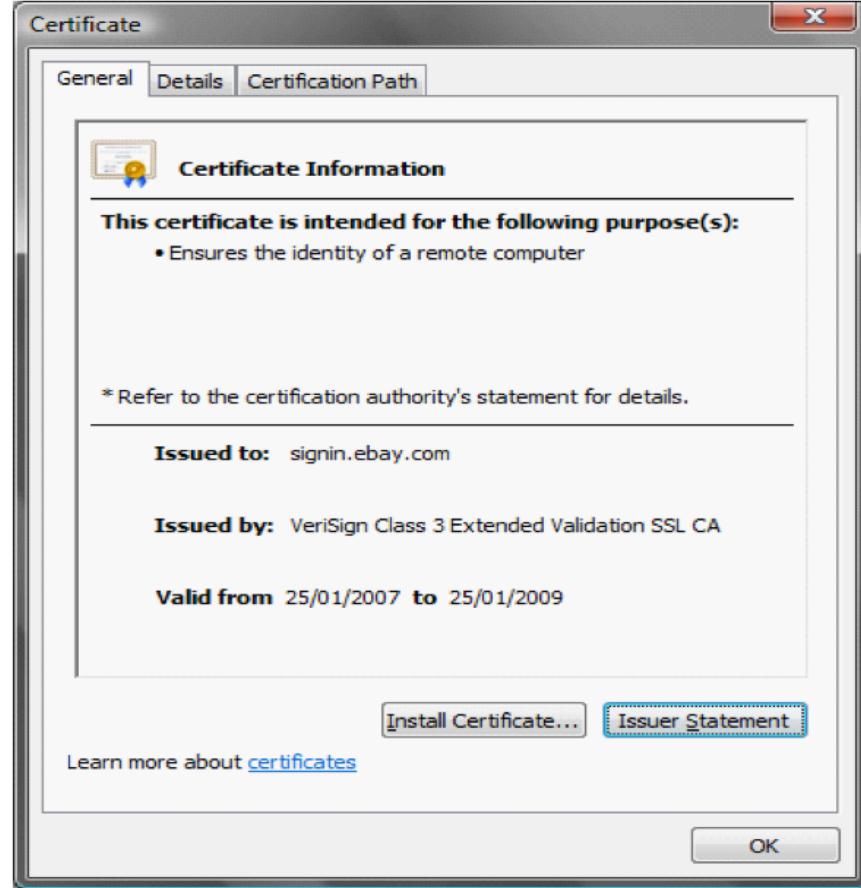


Bob



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.

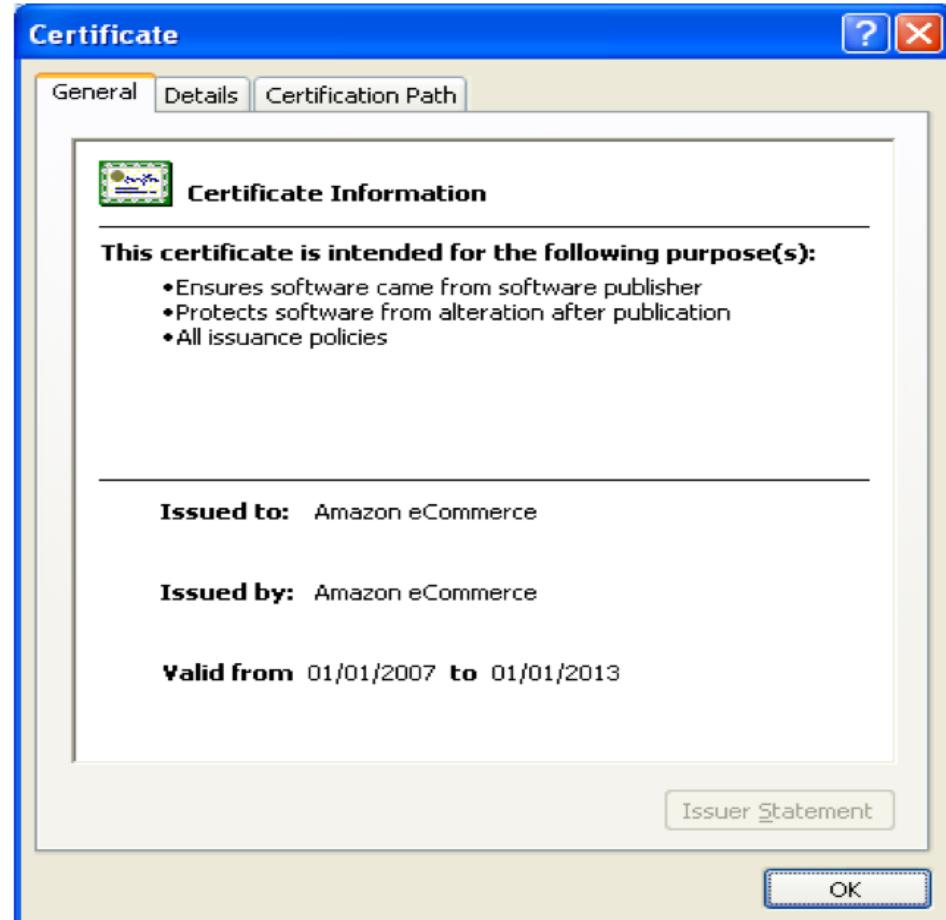
**2. Definitions.**  
"Certificate" or "Digital Certificate" means a message that, at least, states a name or identifier for the Subscriber, contains the Subscriber's public key, identifies the Certificate's serial number, and contains a digital signature of the issuing CA.



# Real!

Author: Prof Bill Buchanan

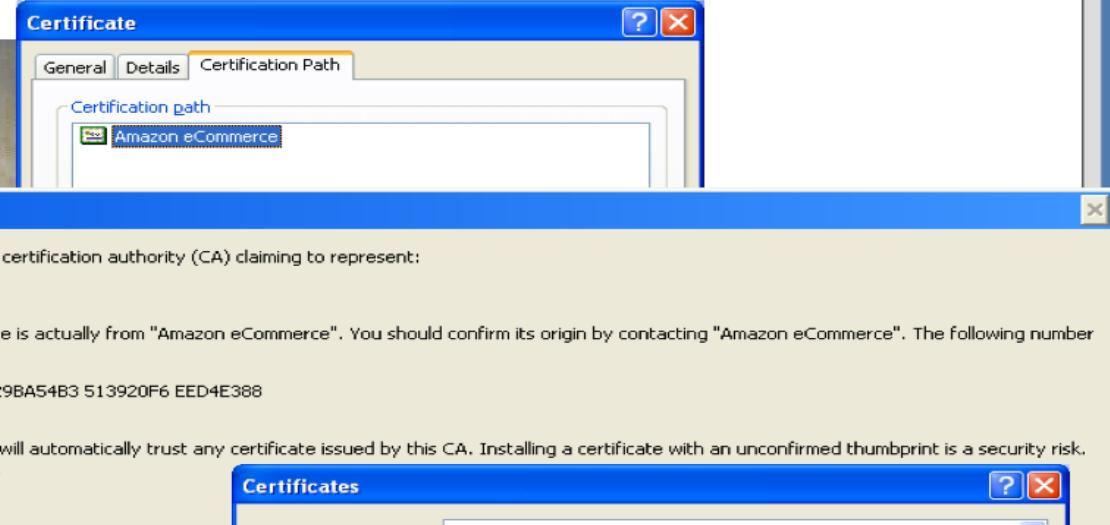
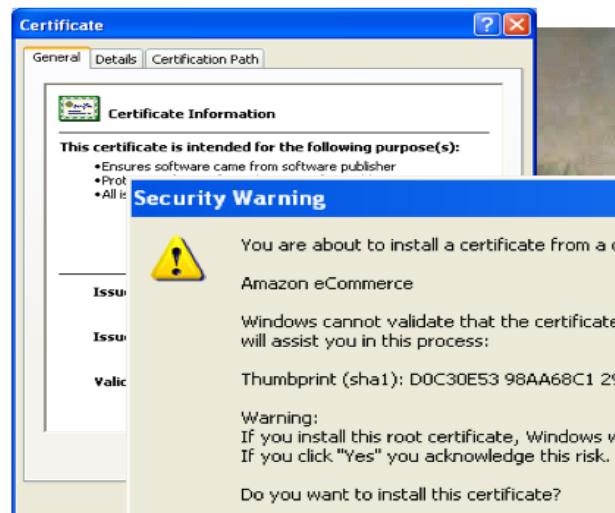
Real or fake?



# Real or fake?

Author: Prof Bill Buchanan

Real or fake?



**Certificates**

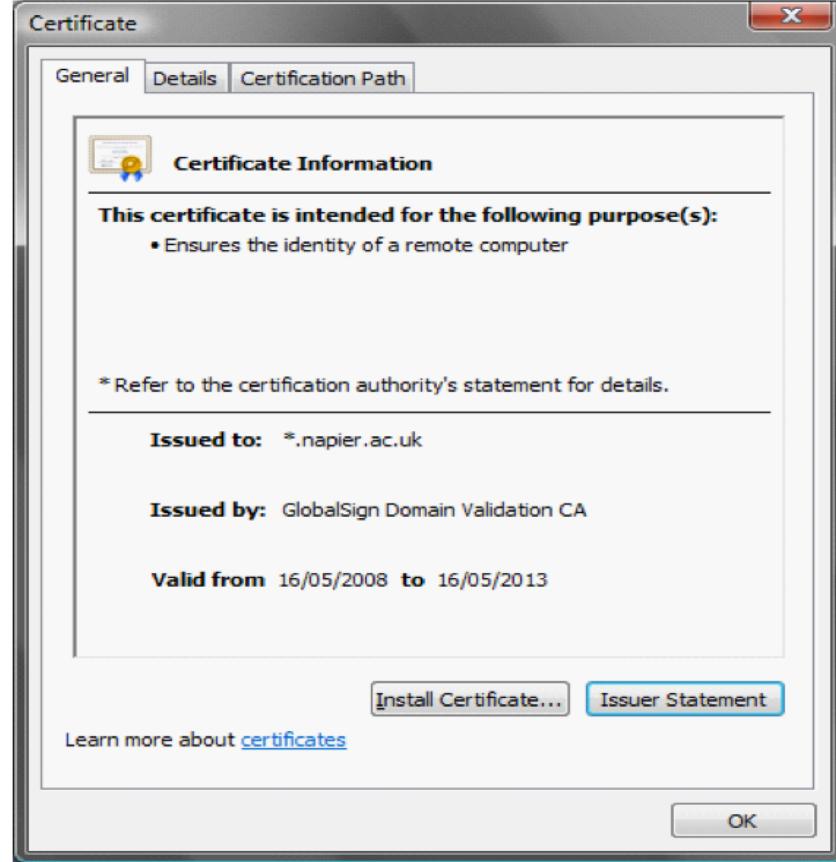
Intended purpose: <All>

Issued To	Issued By	Expiration Date	Friendly Name
ABA ECOM Root CA	ABA.ECOM Root CA	09/07/2009	DST (ABA.ECOM...)
Amazon eCommerce	Amazon eCommerce	01/01/2013	<None>
Autoridad Certifica...	Autoridad Certificador...	28/06/2009	Autoridad Certifi...
Autoridad Certifica...	Autoridad Certificador...	29/06/2009	Autoridad Certifi...
Baltimore EZ by DST	Baltimore EZ by DST	03/07/2009	DST (Baltimore E...
Belgacom E-Trust P...	Belgacom E-Trust Prim...	21/01/2010	Belgacom E-Trus...
C&W HKT SecureN...	C&W HKT SecureNet ...	16/10/2009	CW HKT Secure...
C&W HKT SecureN...	C&W HKT SecureNet ...	16/10/2009	CW HKT Secure...
C&W HKT SecureN...	C&W HKT SecureNet ...	16/10/2010	CW HKT Secure...

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

Certificate intended purposes

Code Signing View Close



# 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**

<http://asecuritysite.com/encryption>

<http://asecuritysite.com/unit06>





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



Eve



Trent



MegaCorp



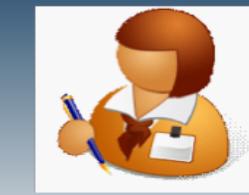
Bob's Private Key



Bob's Public Key



Alice's Public Key



Alice's Private Key



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



Eve



Trent



MegaCorp



Bob's Private Key



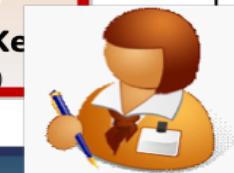
Bob's Public Key



Alice's Public Key



Alice's Public Key



Alice's Private Key



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



MegaCorp





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



Eve



Trent



MegaCorp



Alice's Public Key



Bob's Private Key



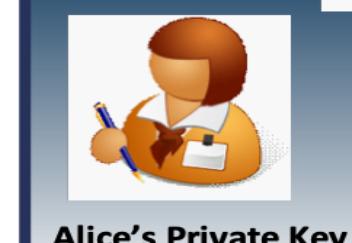
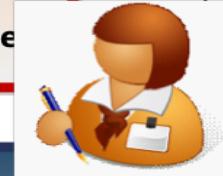
Bob's Public Key

Hello Alice,  
Wish you were  
here!  
- Bob

Bob.



Alice's Public Key



Alice's Private Key



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



Eve



Trent



MegaCorp

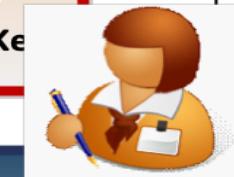


Hello Alice,  
Wish you were  
here!  
- Bob

Bob:



Bob's Private Key





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



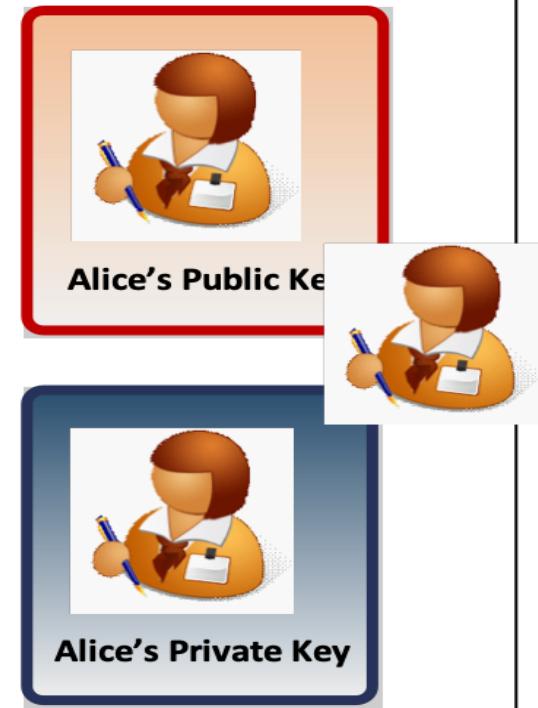
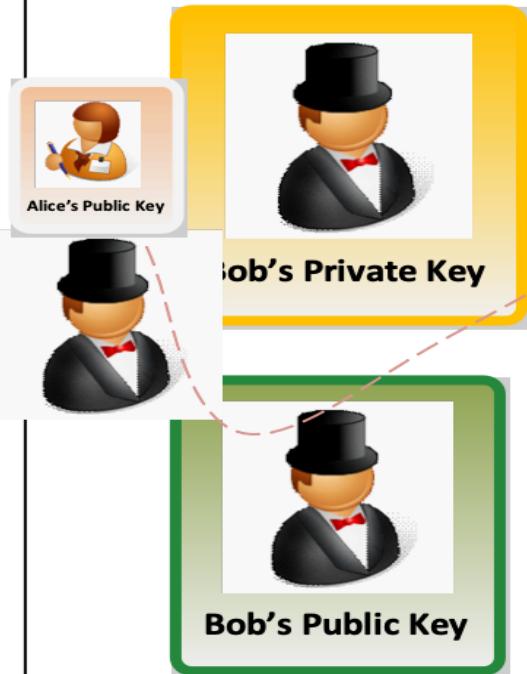
Eve



Trent

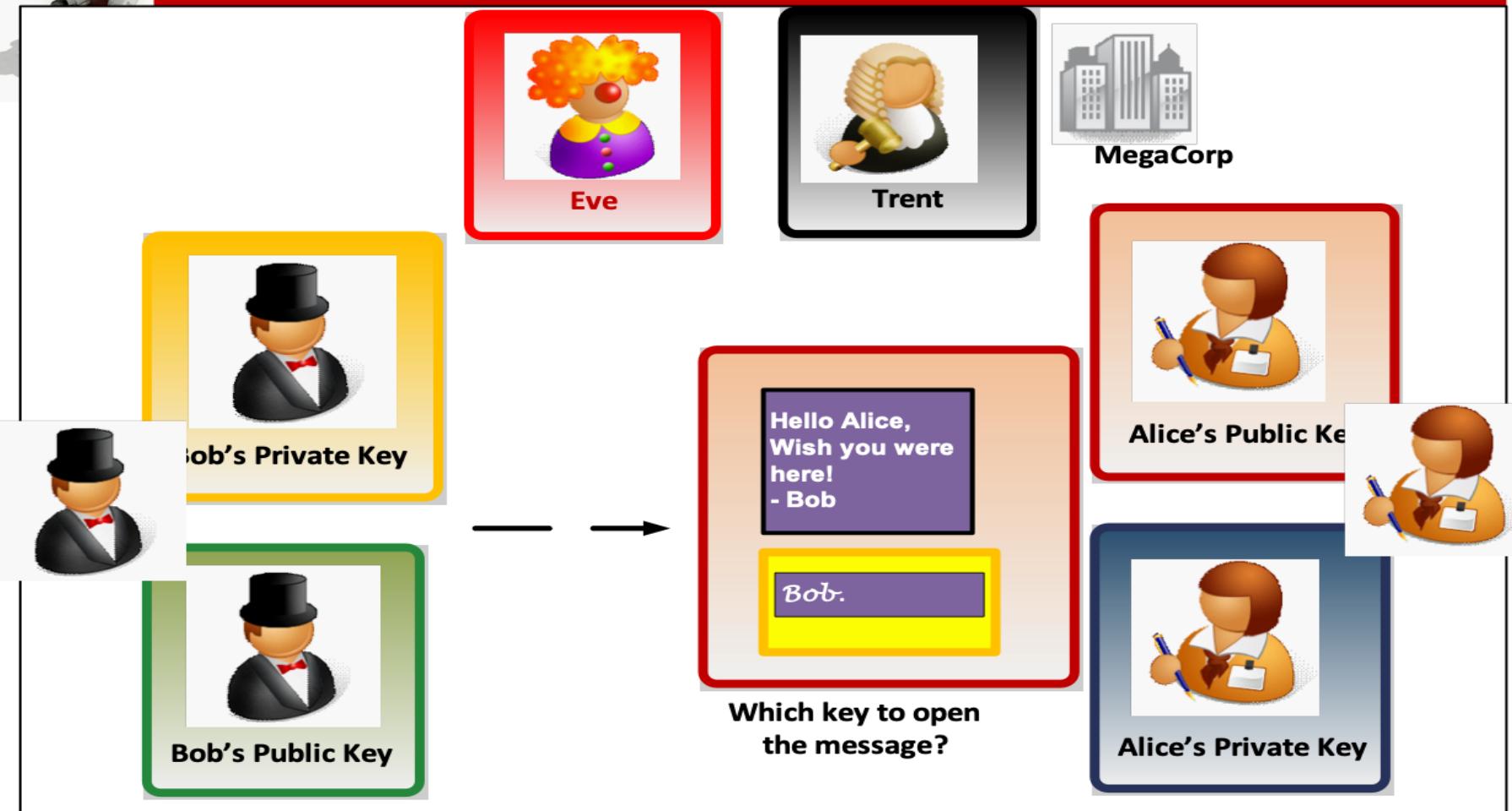


MegaCorp





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





# 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



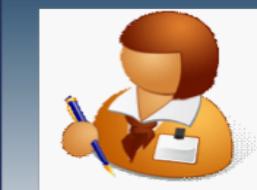
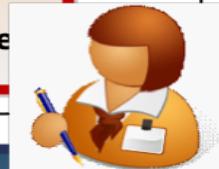
Bob's Private Key



Bob's Public Key



Alice's Public Key



Alice's Private Key

Hello Alice,  
Wish you were  
here!  
- Bob

Bob:

Which key to we  
open the signature  
with?



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

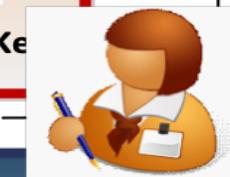


MegaCorp



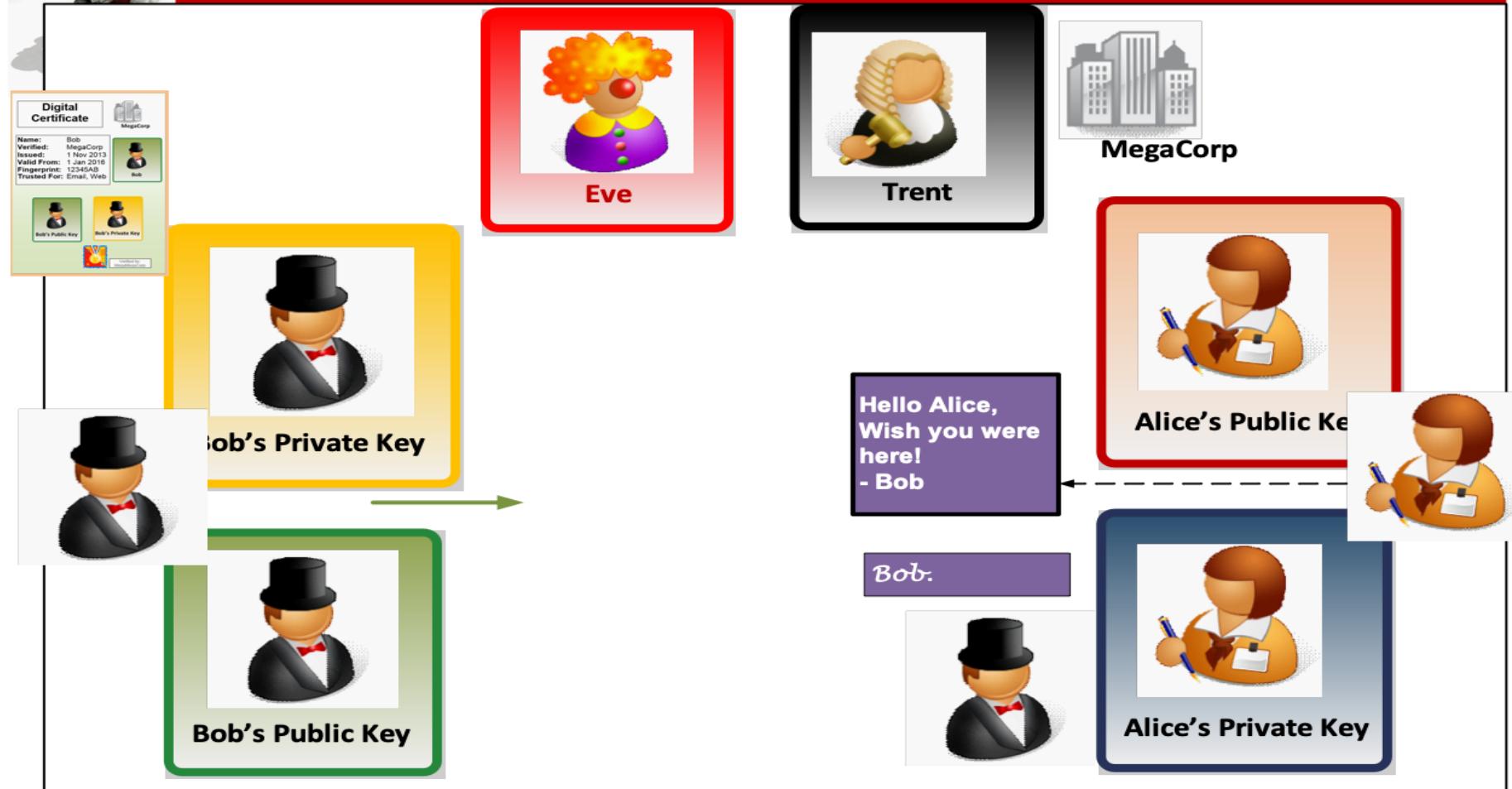
Hello Alice,  
Wish you were  
here!  
- Bob

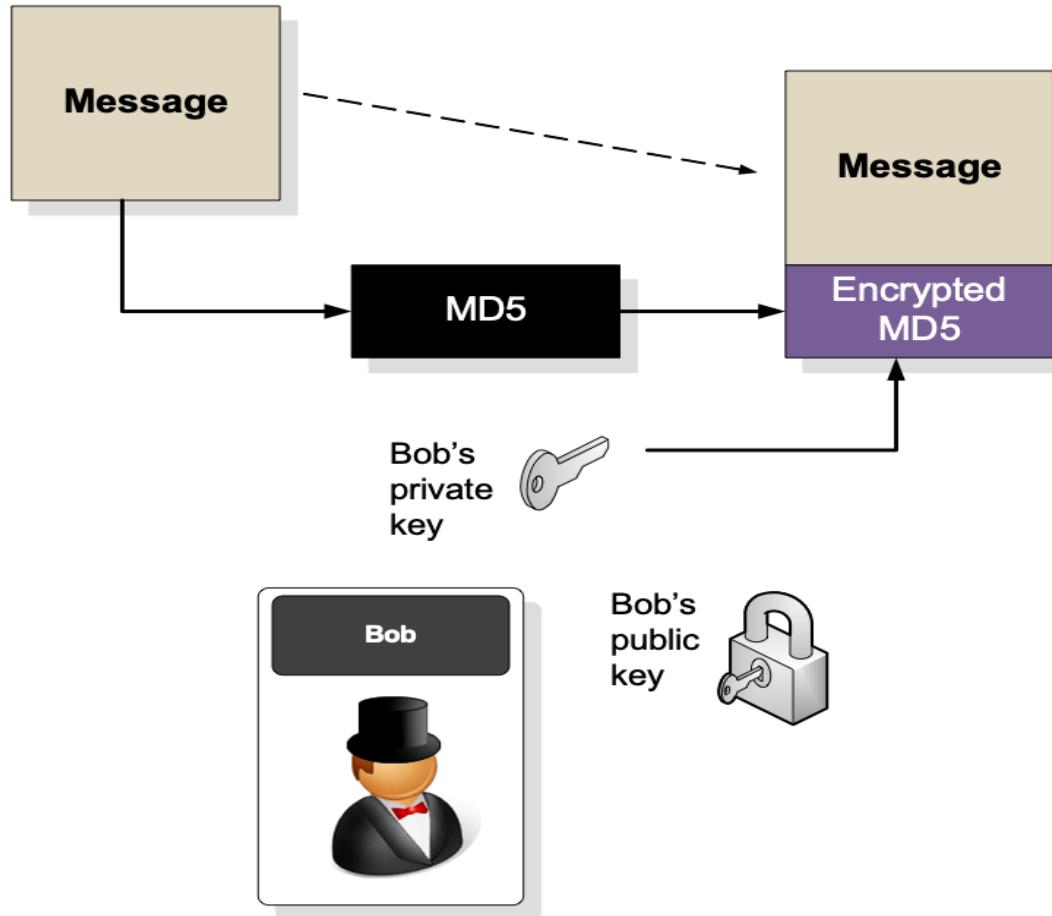
Bob:

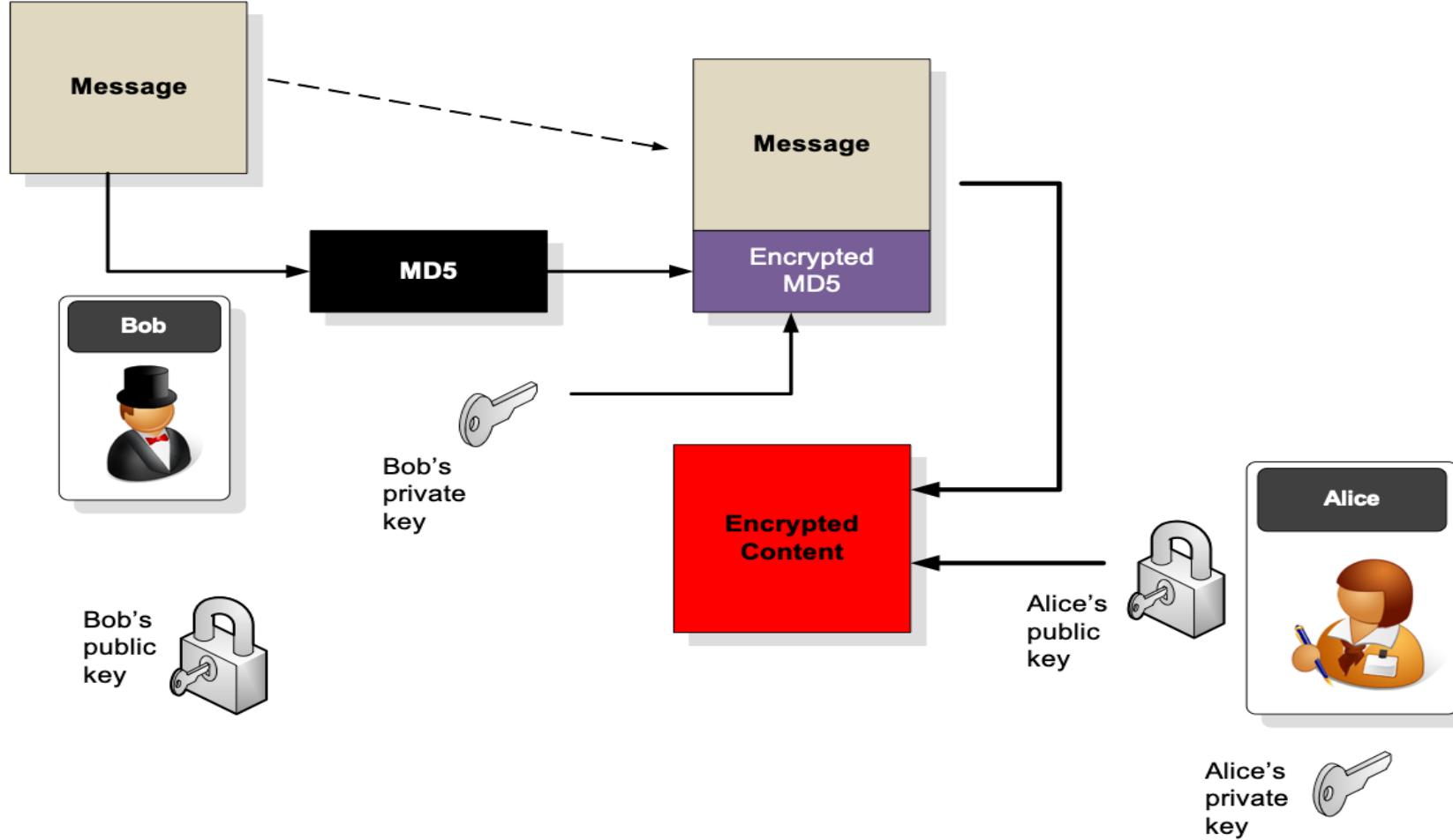




# Public key encryption ... secret ... identity ... trust

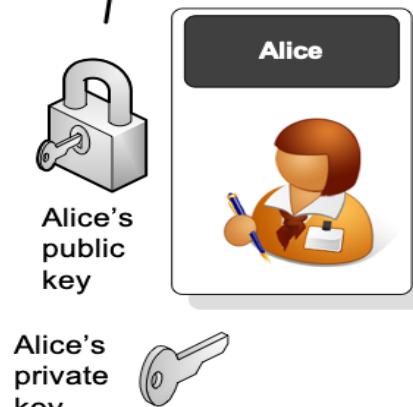
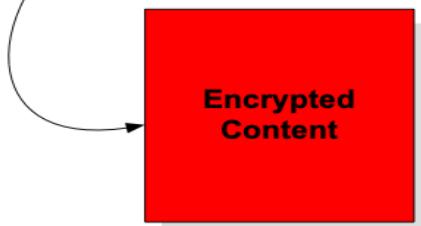
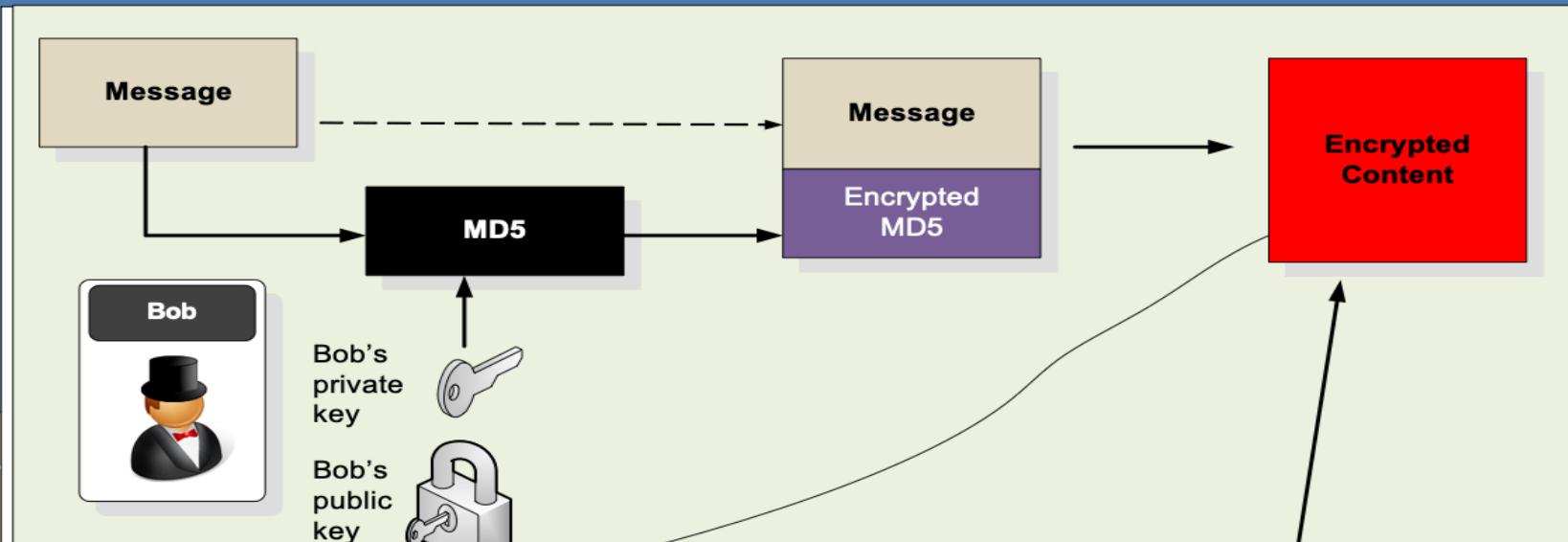






## Authentication

The magic private key

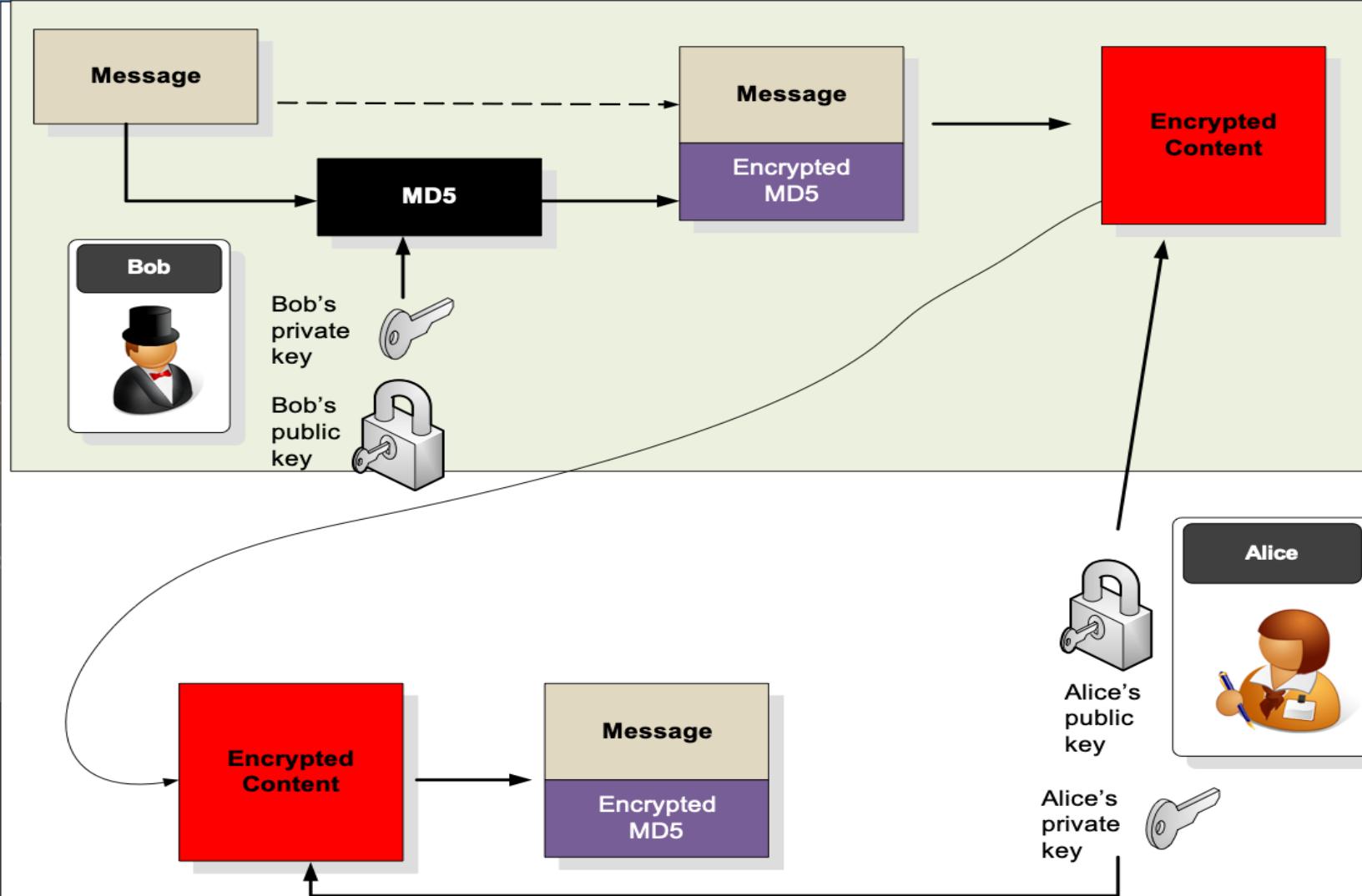


**Bob encrypts the message/hash with Alice's public key**

Author: Prof Bill Buchanan

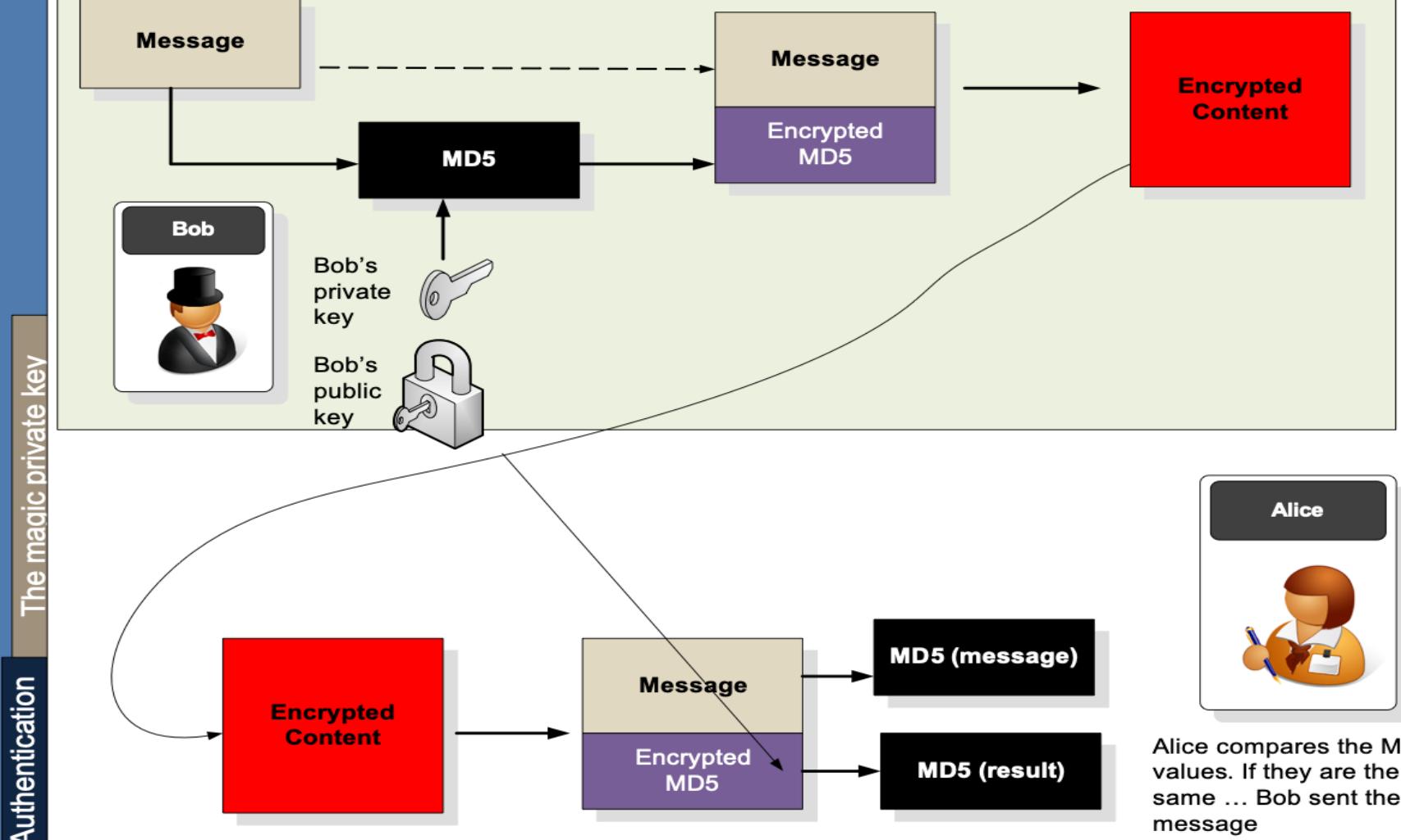
## Authentication

The magic private key



Author: Prof Bill Buchanan

Alice decrypts the message



**Alice decrypts the message**

Author: Prof Bill Buchanan

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

# Digital Certificates

Introduction

Authentication Methods

PKI

Digital Certificate Passing

**Prof Bill Buchanan OBE**

<http://asecuritysite.com/encryption>

<http://asecuritysite.com/unit06>

