Digital Certificates

Introduction
Authentication Methods
Public Key Infrastructures
Digital Certificate Passing
Digital Signatures

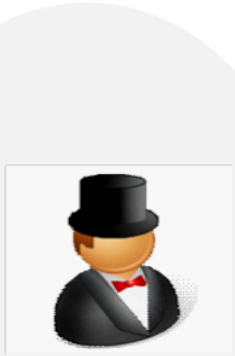
Prof Bill Buchanan OBE

https://asecuritysite.com/digitalcert/

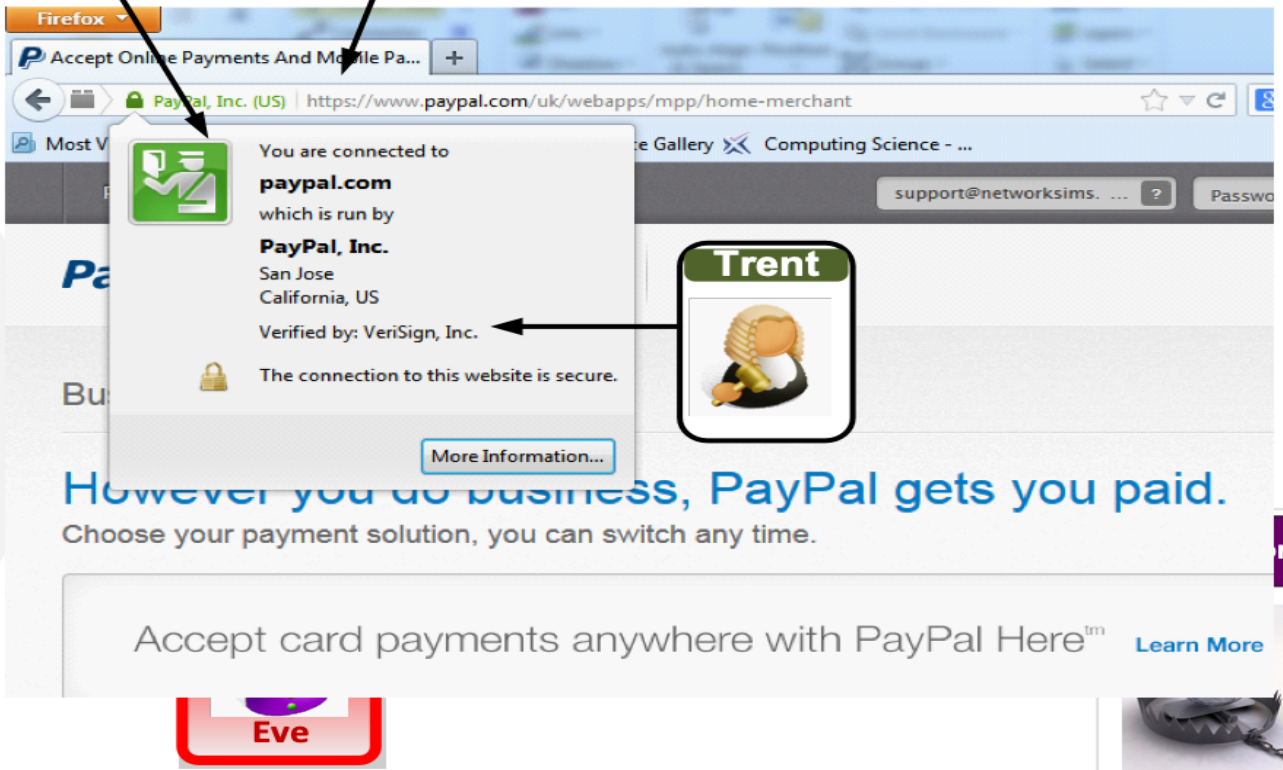
Identity on the Internet

Identifies it is trusted (Digital Certificate)

Keeps communications secure (encryption)



Bob



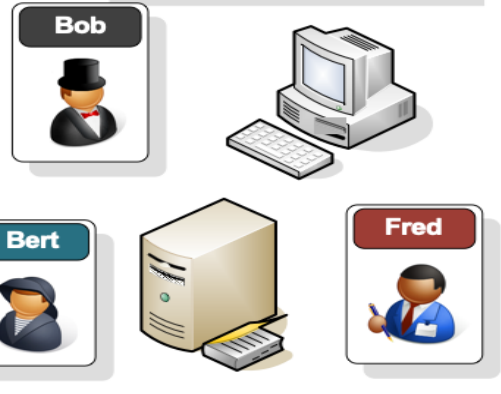
Fundamental principles

Authentication.
Confidence/Assurance.
Privacy/Confidentiality.

Authentication
(Device,
User, Servers,
Connections, etc)

Confidentiality
(Encryption)

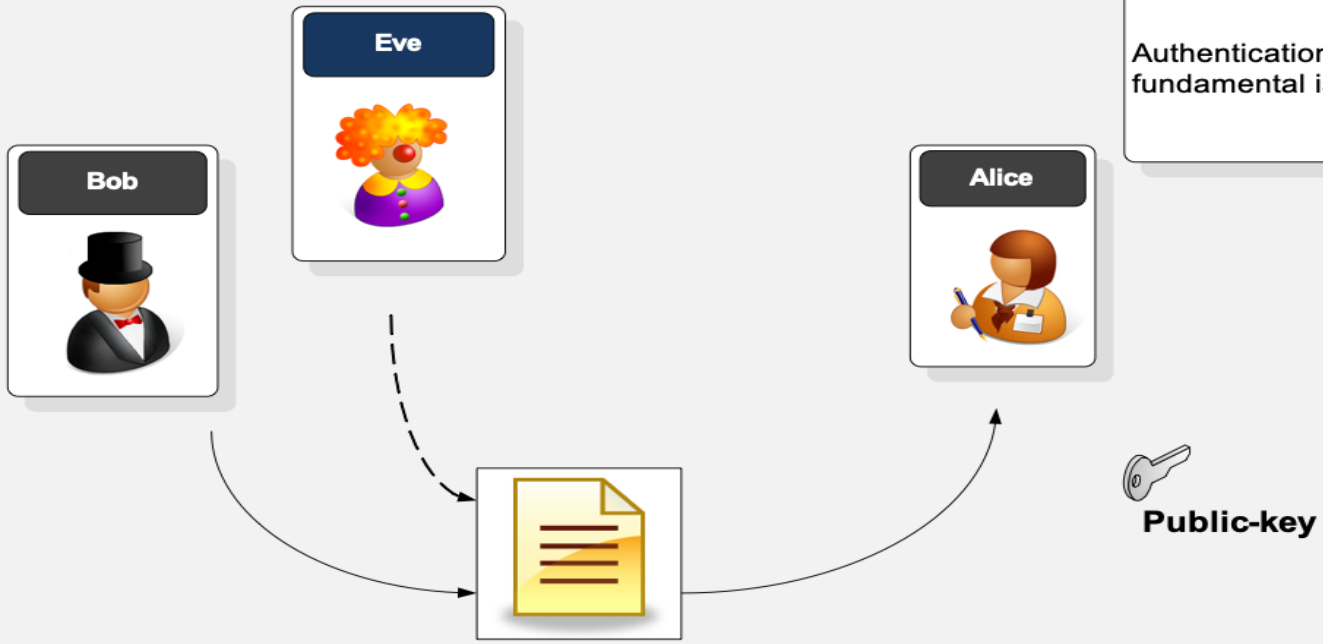
Assurance
(Integrity)



Author: Prof Bill Buchanan

Authentication

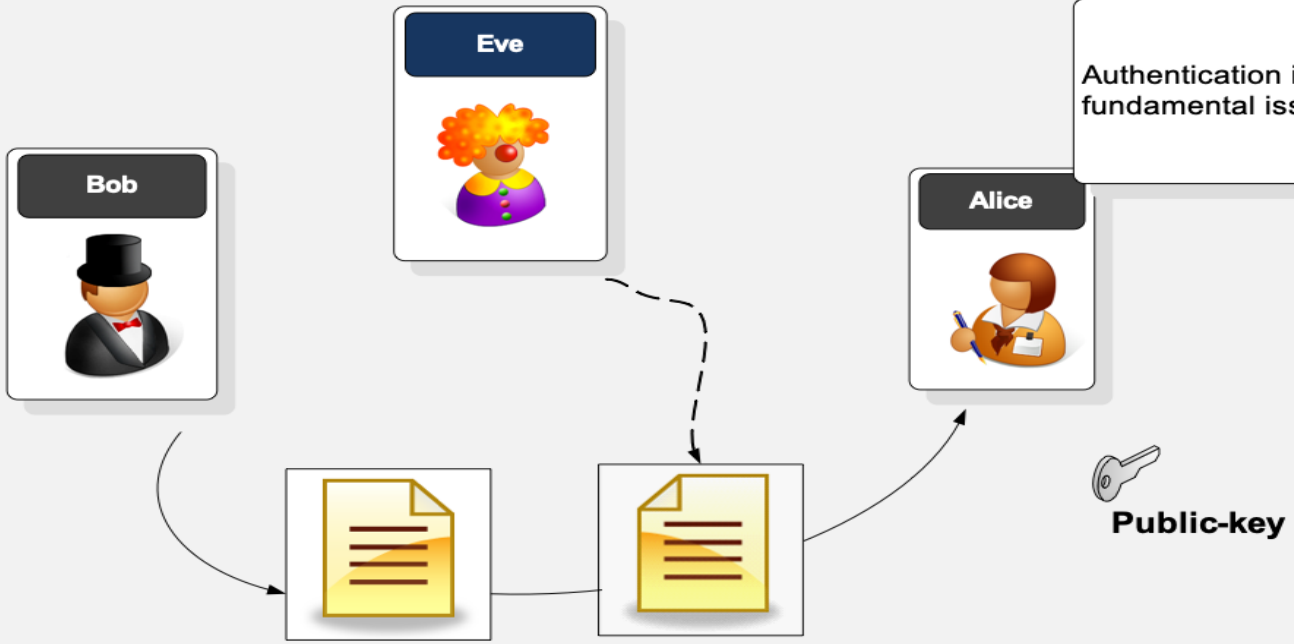
Authentication is a fundamental issue in security.



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

Authentication is a fundamental issue in security.

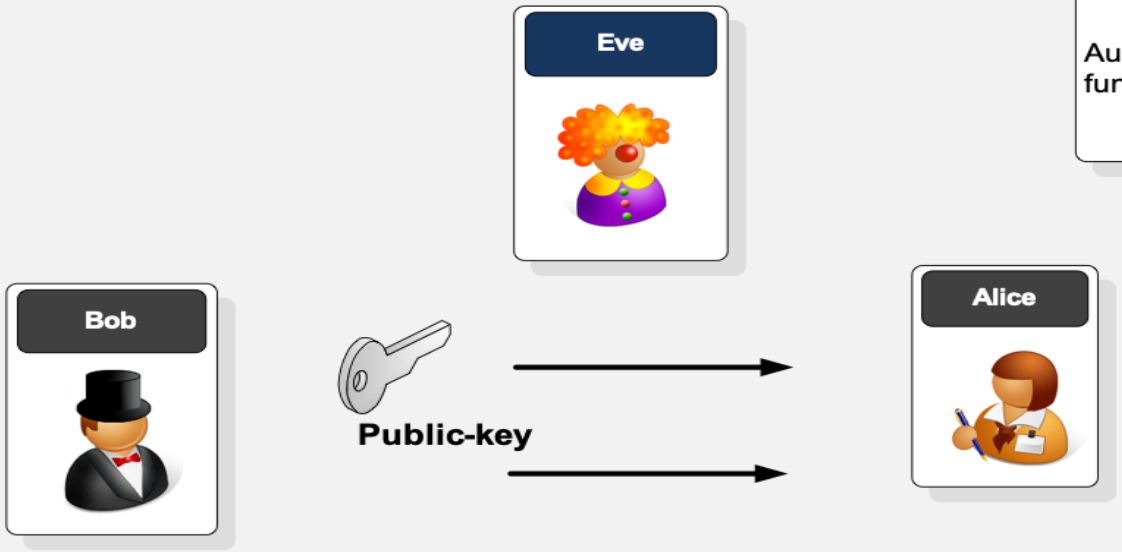


How can we tell that the message has not been tampered with ?

Author: Prof Bill Buchanan

Authentication

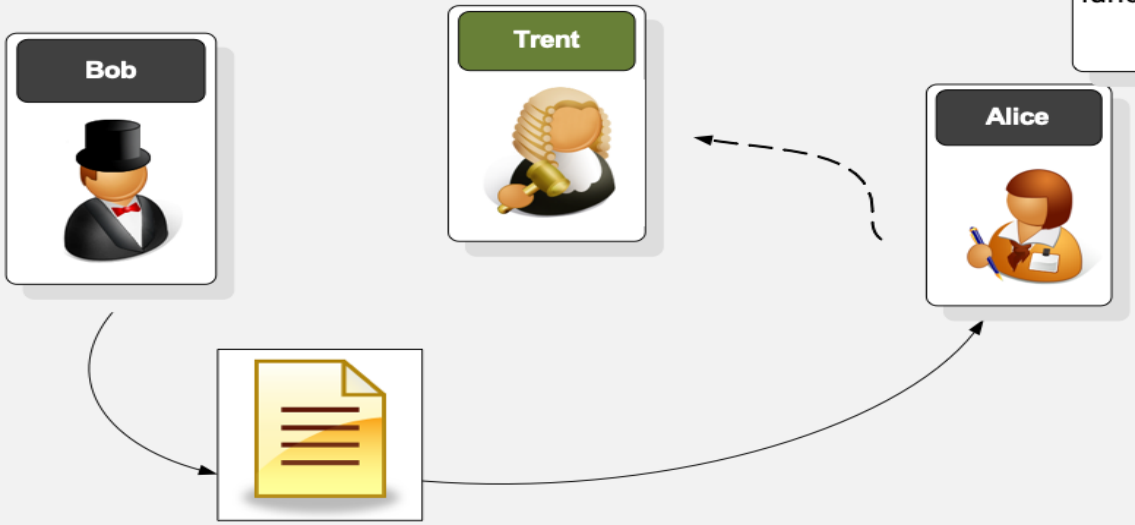
Authentication is a fundamental issue in security.



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

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.

Author: Prof Bill Buchanan

Unit 6: Digital Certificates

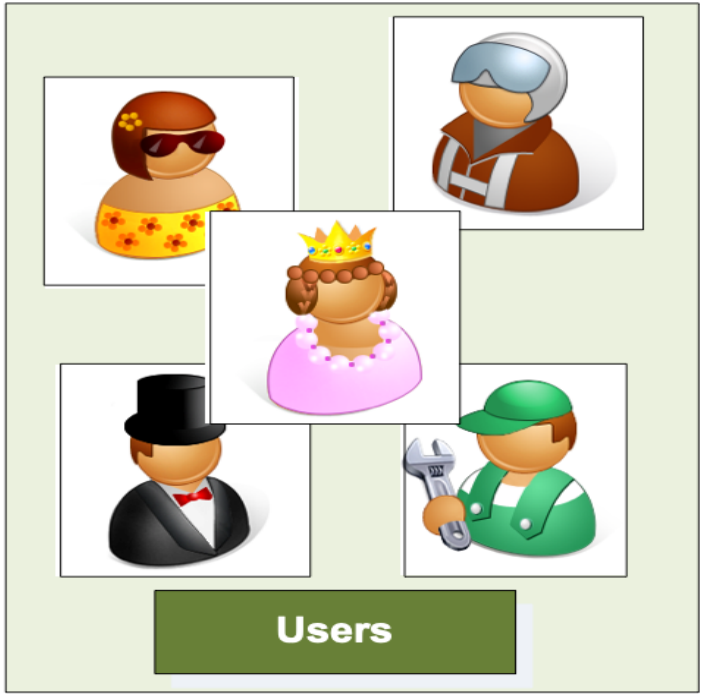
Introduction
Authentication Methods

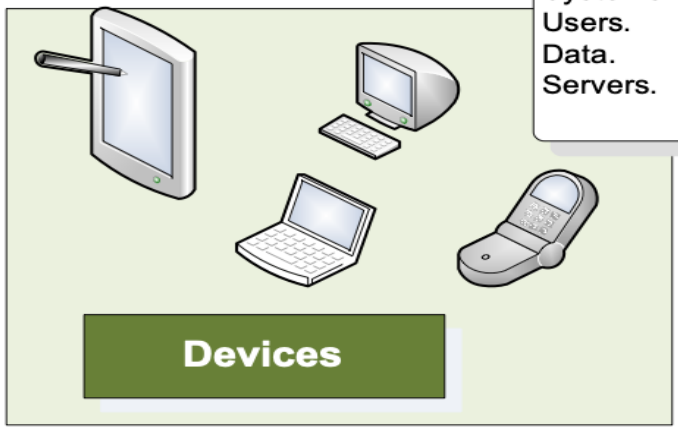
Prof Bill Buchanan OBE

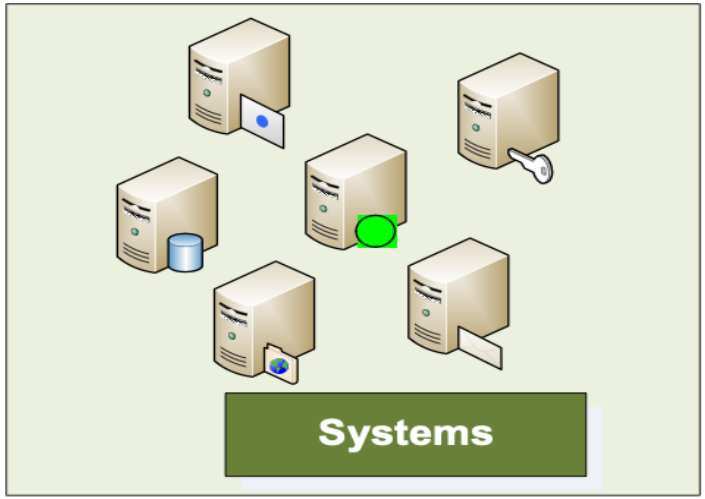
https://asecuritysite.com/digitalcert/

What to authenticate?

Systems.
Users.
Data.
Servers.



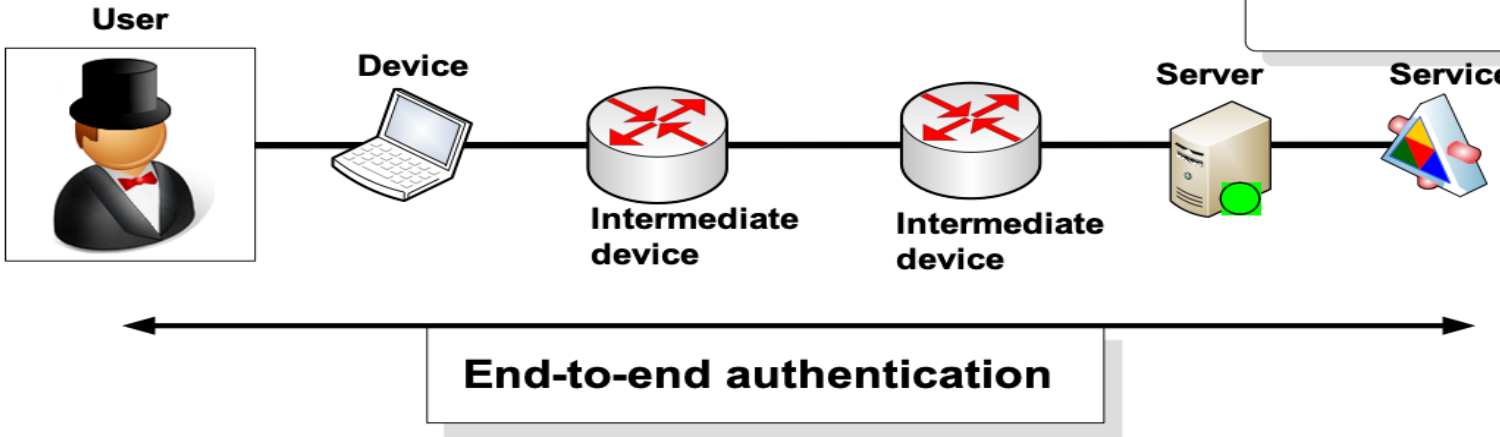


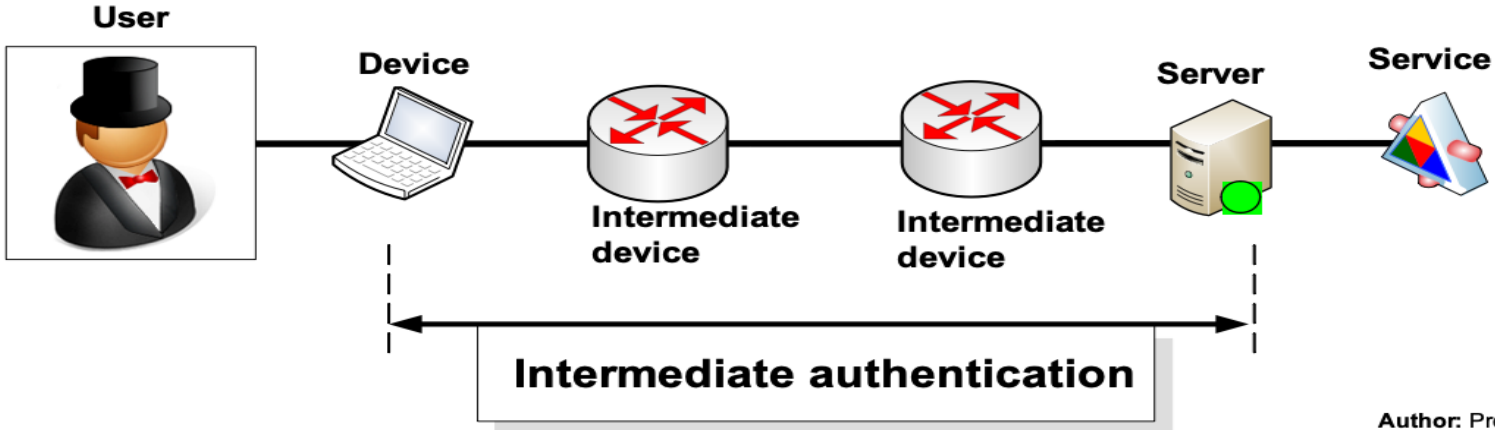


Author: Prof Bill Buchanan

Where authenticated?

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





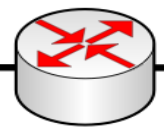
Author: Prof Bill Buchanan

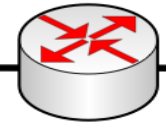
Authentication type

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

User

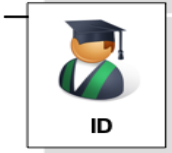
Device





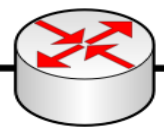
Server

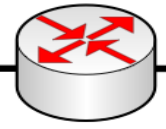
One-way server authentication. Server provides authentication to the client, such as SSL (HTTPS, FTPS, etc).

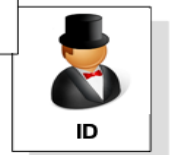


User

Device

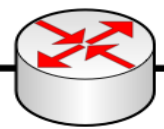


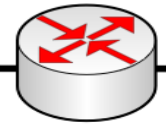




One-way client authentication. Client provides authentication to the server such as EAP-TLS in Wireless.

User





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

Author: Prof Bill Buchanan

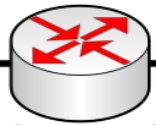
Authentication

Authentication type

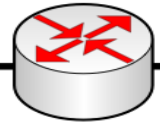
One-way server.
One-way client.
Two-way.

User

Device



Intermediate device



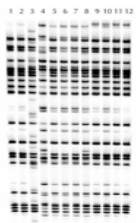
Intermediate device

Server

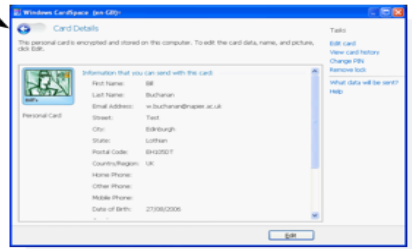
Service

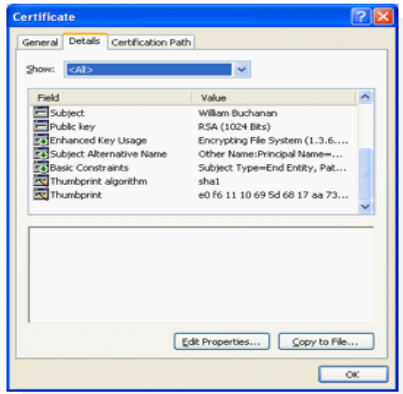
Methods

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



Device name
Digital Certificate
Pass phrase
MAC address
Encryption key





Author: Prof Bill Buchanan

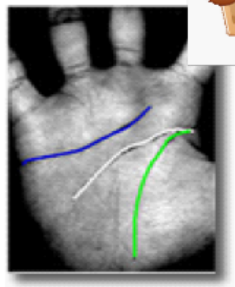
Authentication methods

Something you have
Something you know
Something you are

Authentication Methods

Iris scans

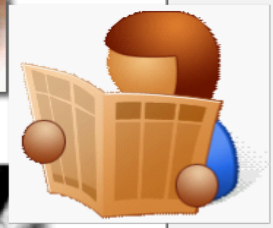
Retina scan

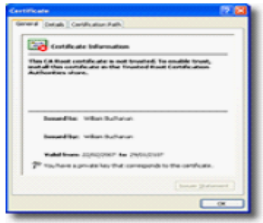


Palm prints

Finger prints

Something you are



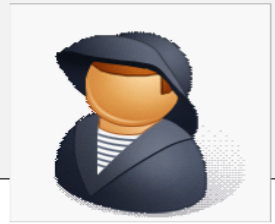


Digital certificate

Network/physical address

Smart card

Something you have



Username/ password

Mother's maiden name

Something you know

Author: Prof Bill Buchanan

Digital Certificates

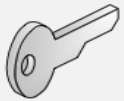
Introduction
Authentication Methods
PKI
Digital Certificate Passing

Prof Bill Buchanan OBE

https://asecuritysite.com/digitalcert/

Digital Certificates

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

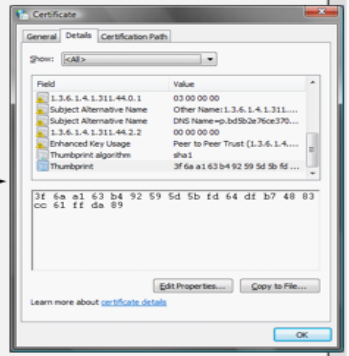


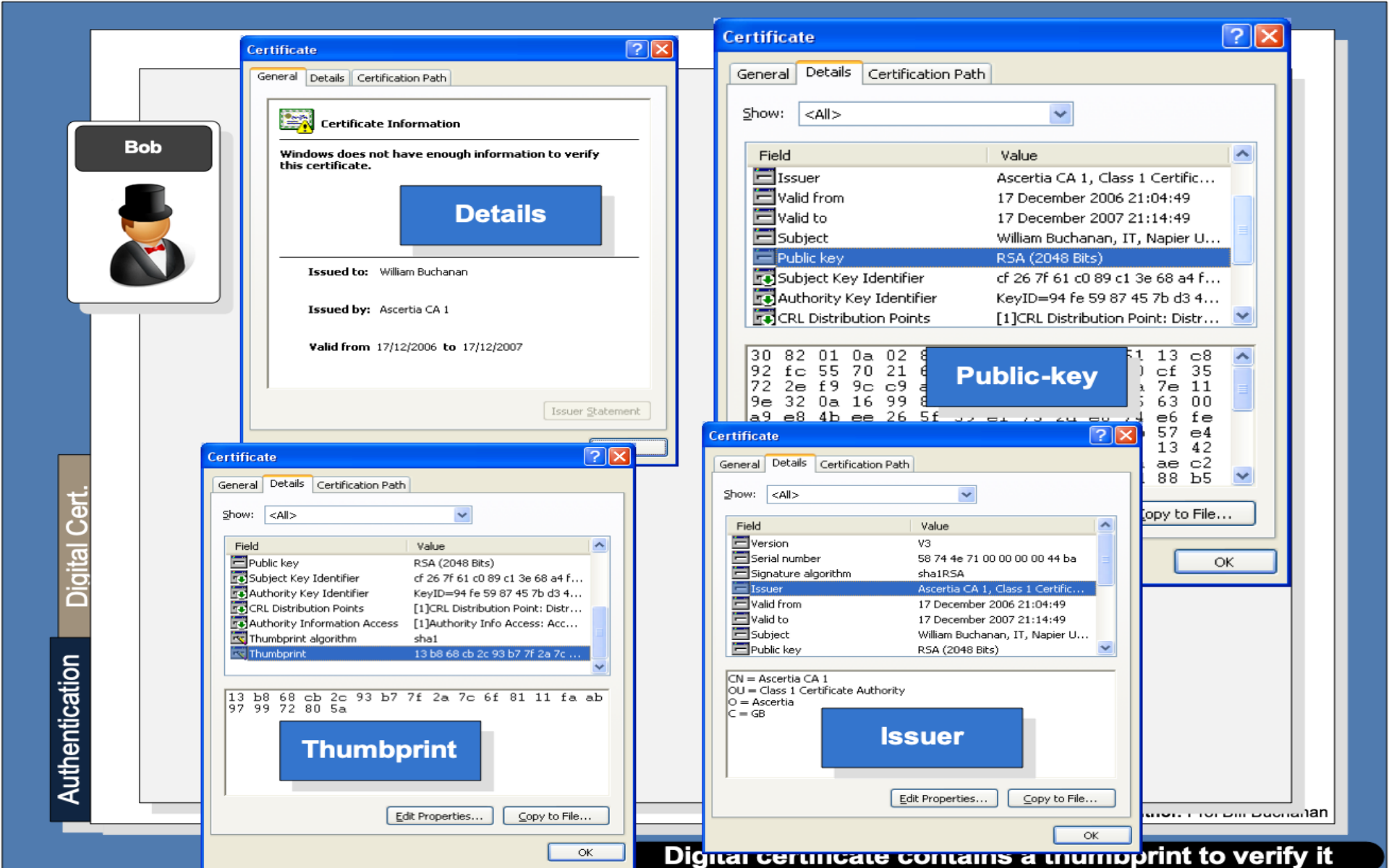
Public-key

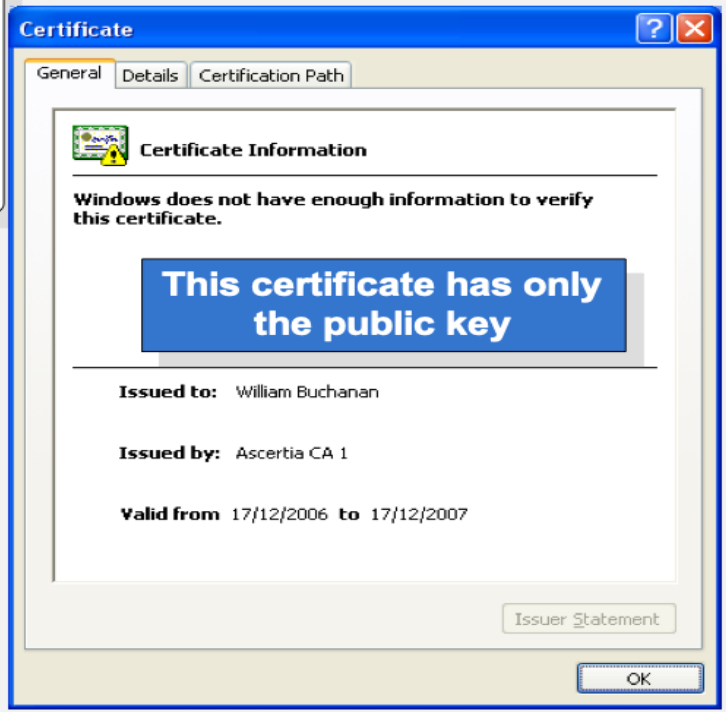
One method is the digital certificate which can carry the public key (and also the private key, if nesc.)

Now that we need the public key to either encrypt data for a receipiant, 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?




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
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...
30 82 01 0a 02
92 fc 55 70 21
72 2e f9 9c c9
9e 32 0a 16 99
a9 e8 4b ee 26 5f
Public-key
Copy to File...
OK
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 ...
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
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 Cert.
Authentication
Digital certificate contains a thumbprint to verify it



Digital certificates should only be distributed with the public key

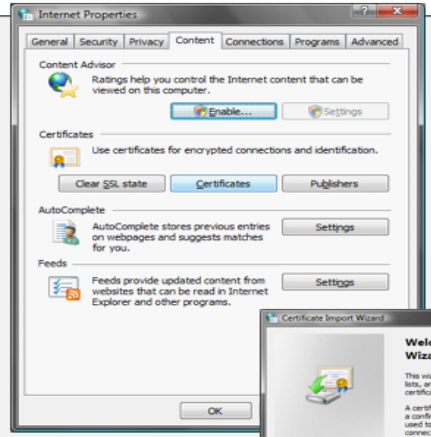
Digital Cert.

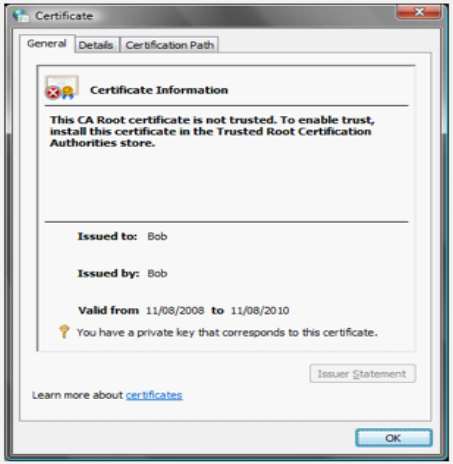
Authentication

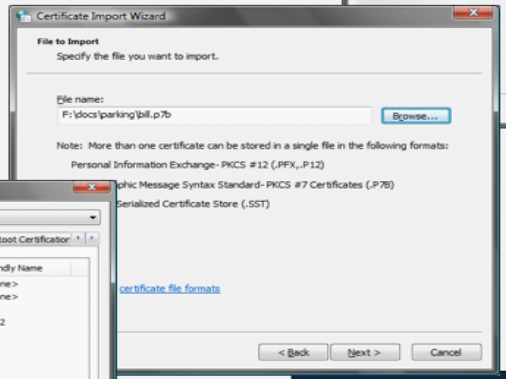
P7b format

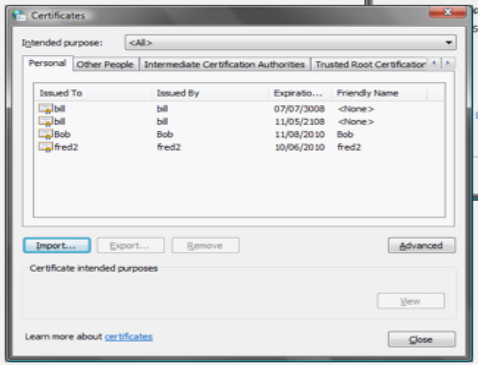
Bob

```
-----BEGIN CERTIFICATE-----
MIID2zCCA4WgAwIBAgIKWHROcQAAAABEujANBgkqhkiG 9w0BAQUFADBgMQswCQYD
VQQGEwJHQjERMA 8GA1UEChMIQXNjZXJ OaWExJjAkBgNVBAsTHUNsYXNzIDEgQ 2Vy
dGlmaWNhdGUgQXV OaG9yaXR 5MRYwFAYDVQQDEw 1Bc2NlcnRpYSBDQSAxMB 4XDTA2
MTIxNzIxMDQ 0OVoXDTA 3MTIxNzIxMTQ 0OVowgZ 8xJjAkBgkqhkiG 9w0BCQEWF 3cu
YnVjaGFuYW 5AbmFwaWVyLmFjLnVrMQswCQYDVQQGEwJVSzEQMA 4GA1UECBMHTG 90
aGlhbjESMBAGA 1UEBxMJRWRpbmJ 1cmdoMRowGAYDVQQKExFOYXBpZXIgVW 5pdmVy
c2l0eTELMAkGA 1UECxMCSVQxGTAXBgNVBAMTEFdpbGxpYW 0gQnVjaGFuYW 4wggEi
MA0GCSqGSIb 3DQEBAQUAA 4IBDwAwggEKAoIBAQCvCFETyJL 8VXAhbEMRzQI 0gM81
ci75nMmsOamjZcb 6fhGeMgoWmYcoscmQkrVjAKnoS +4mXznhcy3md0b+sZbwOVaX
M5FOxhSrV +Q86hsK 8cDc+1sqyJ 8TQtufuDNs ONfNY 6tR6q7CgGqQ 8/VjSxNqzK 39
iLUF1ahhyCet /ab6O/qWzL 4iVsz2nmL 4dyAuyilhLPlVbppHGdE 6sDQXWYd0CpfV
ZN7pauD 5fqBESfO 6bUkCieI47AzRMQj 3kHuDt 7MexVW 7aoX+nXLP4wn7IamaxasF
QvhdOKyCZhYs 82JQDGatXRCqkklztmZW 5i6GkPsE 7xVuX 265WJQ 5afhp2hYlAgMB
AAGjggEXMIIBEzAdBgNVHQ 4EFgQUzyZ /YcCJwT 5opPHLPlcQKkOlkJwwYWYDVR 0j
BFwwWoAUlP 5Zh0V700k6CorvRMWB 9ifVkBmhP 6Q9MDsxCzAJBgNVBAYTAkdCMREw
DwYDVQQKEwhBc 2NlcnRpYTEZMBcGA 1UEAxMQQXNjZXJ OaWEgUm9vdCBDQYIBDTBN
BgNVHR 8ERjBEMEKgQKA +hjxodHRwOi 8vd3d3LmFzY 2VydGlhLmNvbS 9PbmxpbmVD
QS9jcmxzL 0FzY 2VydGlhQ 0ExL 2NsYXNzMS 5jcmwwPgYIKwYBBQUHAQEEMjAwMC 4G
CCsGAQUFBzAChiJodHRwOi 8vb2NzcC 5nbG9iYWx 0cnVzdGZpbmRlci 5jb20vMA0G
CSqGSIb 3DQEBBQUAA 0EATOCwGJ 1tS0kTlupmpjkMl 8IdxMmD 5WuhszjBlGsMhPxI
H+vXhL 9yaOw+Prpzy 7ajS4/3xXU 8vRANhyU 9yU4qDA==
-----END CERTIFICATE-----
```









The main certificate formats include:

- P7b. Text format
- PFX/P12. Binary.
- SST. Binary.

Digital certificates should only be distributed with the public key

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

A

Encryption

Communications Channel

Decryption

Alice sends her digital certificate with her public key on it

Hello

B

C

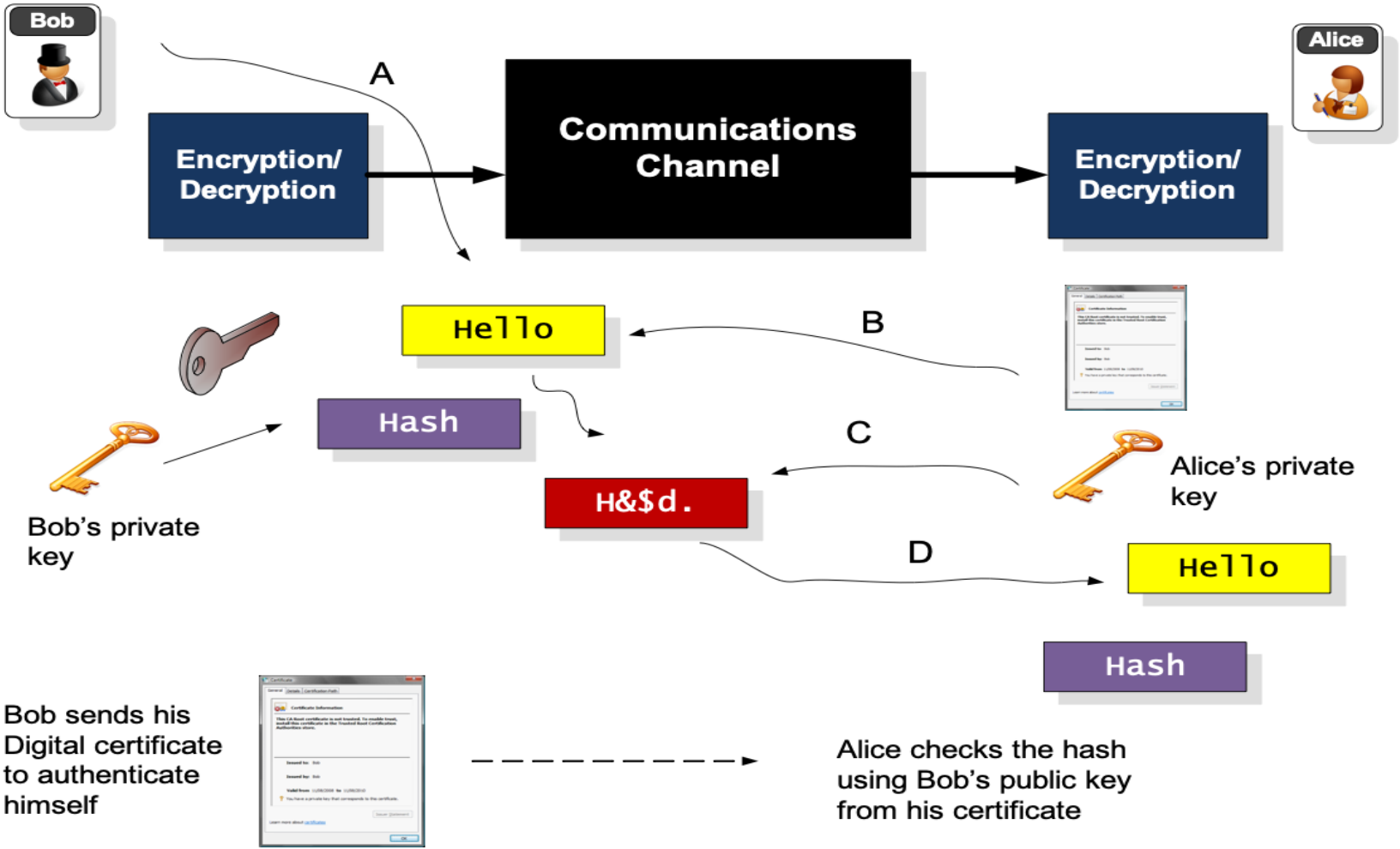
H&$d.

Alice's private key

D

Hello

Author: Prof Bill Buchanan



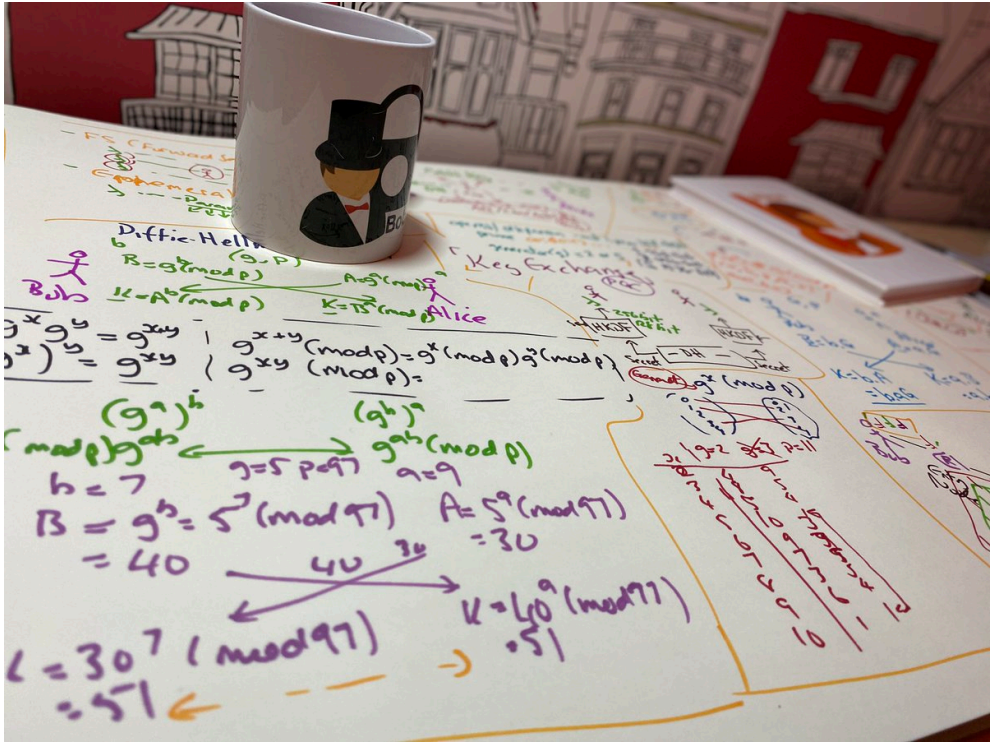
Author: Prof Bill Buchanan

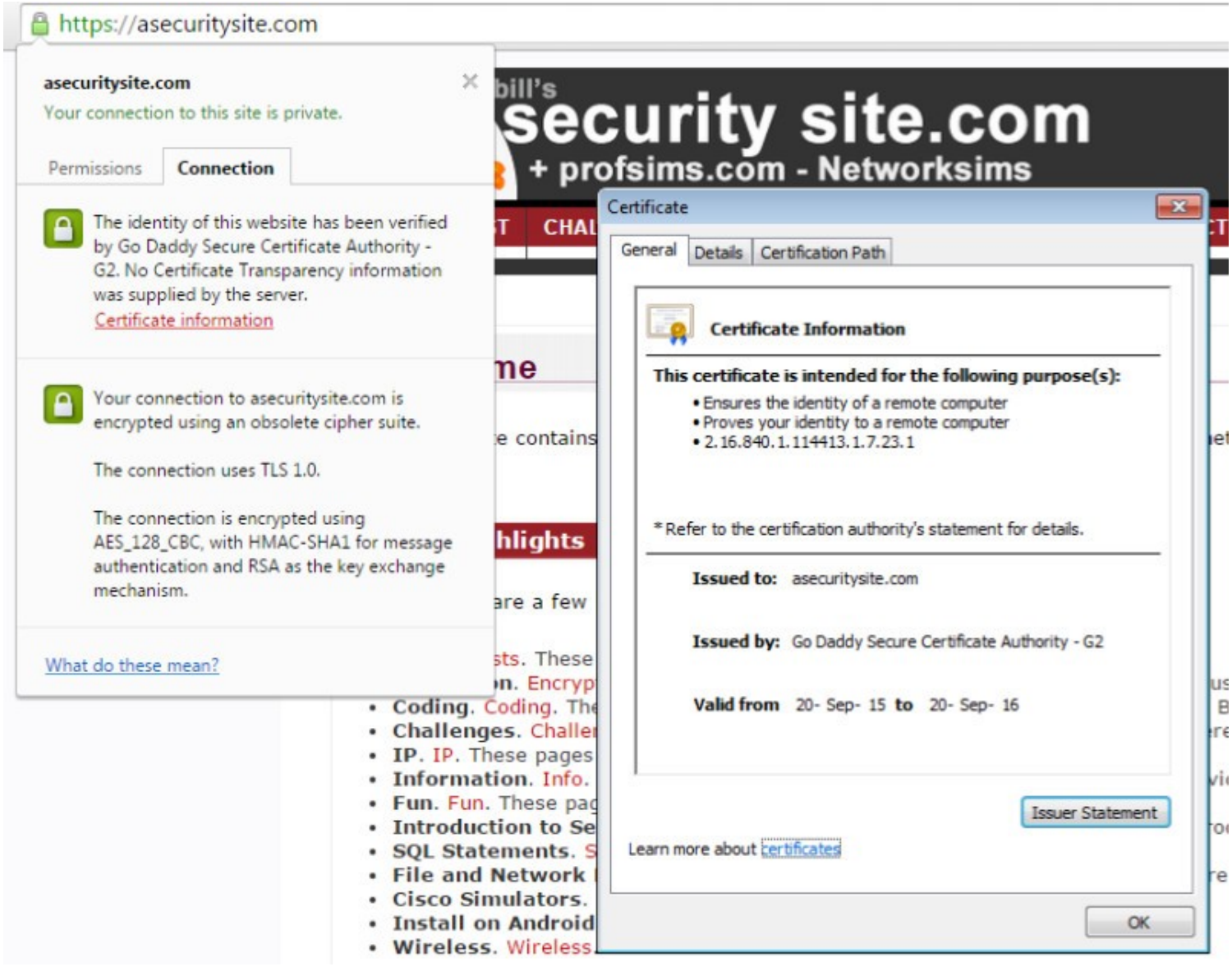
Digital Certificates

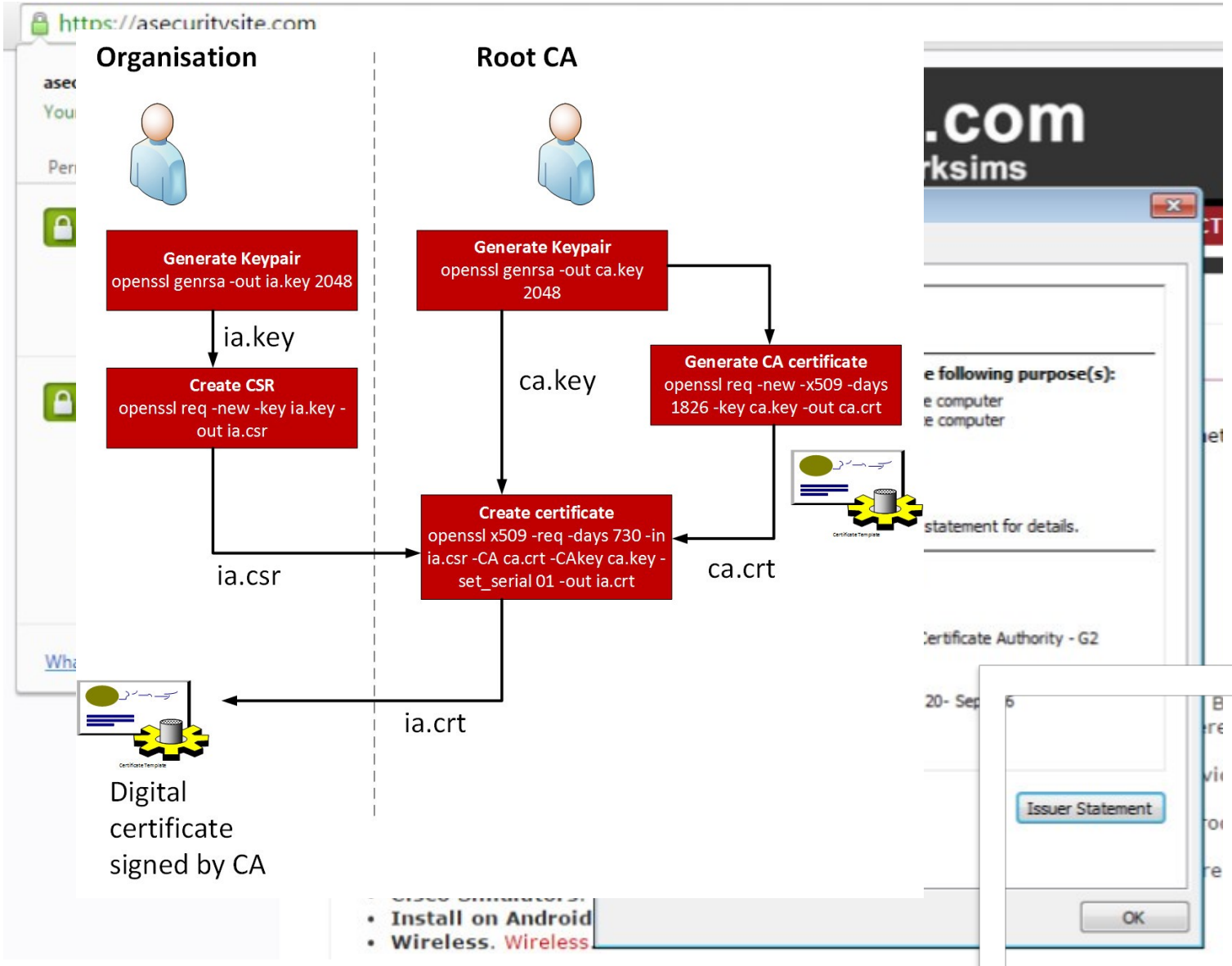
Introduction
Authentication Methods
PKI
Certificate Creation
Digital Certificate Passing

Prof Bill Buchanan OBE

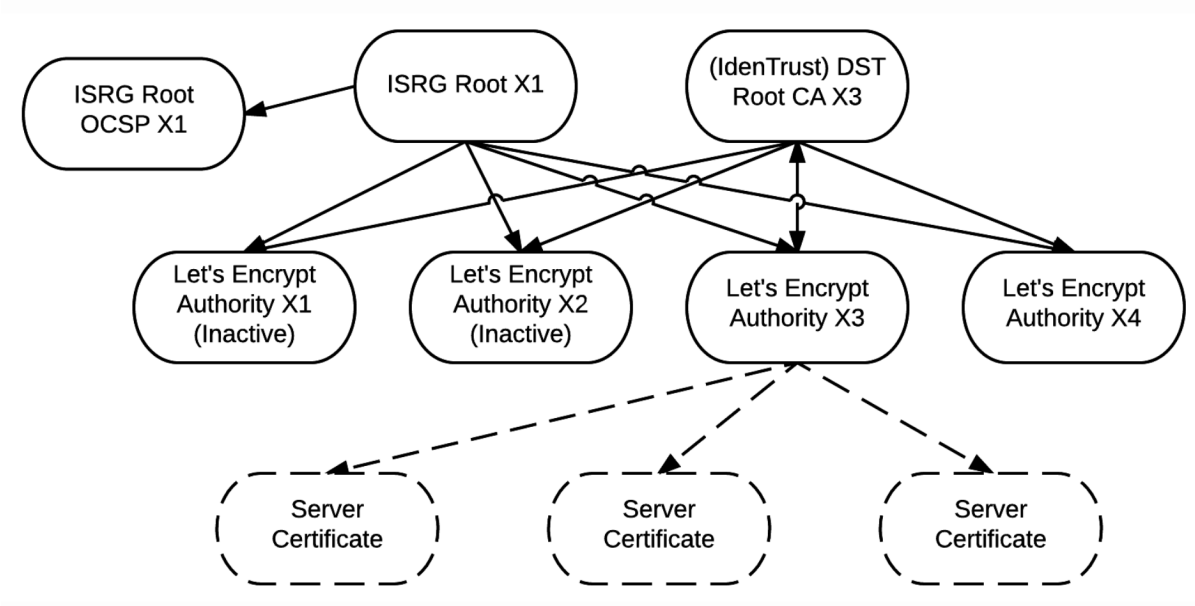
https://asecuritysite.com/digitalcert/




https://asecuritysite.com
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?
bill's
security site.com
+ profsims.com - Networksims
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


https://asecuritysite.com
Organisation
Root CA
Generate Keypair
openssl genrsa -out ia.key 2048
ia.key
Create CSR
openssl req -new -key ia.key -out ia.csr
ia.csr
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
ca.crt
Create certificate
openssl x509 -req -days 730 -in ia.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out ia.crt
ia.crt
Digital certificate signed by CA
Issuer Statement
OK


SECURE THE WEB
Let's Encrypt


ISRG Root OCSP X1
ISRG Root X1
(IdenTrust) DST Root CA X3
Let's Encrypt Authority X1 (Inactive)
Let's Encrypt Authority X2 (Inactive)
Let's Encrypt Authority X3
Let's Encrypt Authority X4
Server Certificate
Server Certificate
Server Certificate

PEM

```
-----BEGIN CERTIFICATE-----
MIIEwTCCA6mgAwIBAgIRAO93GGFLfHwOCAAAAAAucZgwDQYJKoZIhvcNAQELBQAw
QjELMAkGA1UEBhMCVVMxHjAcBgNVBAoTFUdvb2dsZSBUcnVzdCBTZXJ2aWNlczET
MBEGA1UEAxMKR1RTIENBIDFPMTAeFw0yMDAyMTIxMTQ3NDFaFw0yMDA1MDYxMTQ3
NDFaMGgxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlhMRYwFAYDVQQH
Ew1Nb3VudGFpbiBWaWV3MRMwEQYDVQQKEwpHb29nbGUgTExDMRcwFQYDVQQDEw53
d3cuZ29vZ2xlLmNvbTBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABCzzLJYFJb8W
TpQxWL0TySDvfEWCkMe7l81CFspT60knl13YILNdTM22sUwPycyogKjBSaQZ9Axi
hCeGEAiJkbejggJVMIICUTAOBgNVHQ8BAf8EBAMCB4AwEwYDVR0lBAwwCgYIKwYB
BQUHAwEwDAYDVR0TAQH/BAIwADAdBgNVHQ4EFgQU9Ty3t90o7UW9+Hc6kv/j9511
BBwwHwYDVR0jBBgwFoAUmNH4bhDrz5vsYJ8YkBug630J/SswZAYIKwYBBQUHAQEE
WDBWMCcGCCsGAQUFBzABhhtodHRwOi8vb2NzcC5wa2kuZ29vZy9ndHMxbzEwKwYI
KwYBBQUHMAKGH2h0dHA6Ly9wa2kuZ29vZy9nc3IyL0dUUzFPMS5jcnQwGQYDVR0R
BBIwEIIOd3d3Lmdvb2dsZS5jb20wIQYDVR0gBBowGDAIBgZngQwBAgIwDAYKKwYB
BAHWeQIFAzAvBgNVHR8EKDAmMCSgIqAghh5odHRwOi8vY3JsLnBraS5nb29nL0dU
UzFPMS5jcmwwggEFBgorBgEEAdZ5AgQCBIH2BIHzAPEAdgCyHgXMi6LNiiBOh2b5
K7mKJSBna9r6cOeySVMt74uQXgAAAXA5cNqwAAAEAwBHMEUCIQCojKtzOe8l1JYK
HmKnbt1puqT4AE3peMVAVk/WeWGp1QIgBvRMbNkwF6i8+JVv3CfTHKvFd8e00+GY
PbXJZb1drKEAdwBep3P531bA57U2SH3QSeAyepGaDIShEhKEGHWWgXFFWAAAAXA5
cNrLAAAEAwBIMEYCIQCQSONppELPODh65oFT5ZAGsSQz4FsjNNZedgS7WqzLnQIh
AMAru0QUuoE3RWngfhI6W7n1kxkEmd0vSZTe6+Ql+JVuMA0GCSqGSIb3DQEBCwUA
A4IBAQCDU8CVusGstVk1lAmrtg3DyYhNV1UnKyLk3RrHKumwYz5mC25bWGoLVKvv
pwxBN3zA329/9JZq0mnn0vmPMxjTDvh9sVQ7g4znwha/KJfzL8AZKUdldD9O+hDO
tlHtqVqITZPCAI/ANvbHdZiMEePB8eA+oTiw2ucChqLlsop5Mio8ckg7aXG4/QfC
AIDbvkoffK44rs4UEpsaqGe9QqMJjTuO7ZCZrFd1m3geq2ARKPHgPoPM6UbDdqg0
TNQo9C0F5ZlOkOgV/qshvpTO4YzE7TB2U571eYEqNXH48syVx8XSk3P7FjM7FIZ2
IzbJSEipZJm8DsP10fFXpToIn+zK
-----END CERTIFICATE-----
```

PKCS#7

```
-----BEGIN PKCS7-----
MIIE8gYJKoZIhvcNAQcCoIIE4zCCBN8CAQExADALBgkqhkiG9w0BBwGgggTF
wTCCA6mgAwIBAgIRAO93GGFLfHwOCAAAAAAucZgwDQYJKoZIhvcNAQELBQAw
MAkGA1UEBhMCVVMxHjAcBgNVBAoTFUdvb2dsZSBUcnVzdCBTZXJ2aWNlczET
A1UEAxMKR1RTIENBIDFPMTAeFw0yMDAyMTIxMTQ3NDFaFw0yMDA1MDYxMTQ3
MGgxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlhMRYwFAYDVQQH
b3VudGFpbiBWaWV3MRMwEQYDVQQKEwpHb29nbGUgTExDMRcwFQYDVQQDEw53
Z29vZ2xlLmNvbTBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABCzzLJYFJb8W
WL0TySDvfEWCkMe7l81CFspT60knl13YILNdTM22sUwPycyogKjBSaQZ9Axi
EAiJkbejggJVMIICUTAOBgNVHQ8BAf8EBAMCB4AwEwYDVR0lBAwwCgYIKwYB
AwEwDAYDVR0TAQH/BAIwADAdBgNVHQ4EFgQU9Ty3t90o7UW9+Hc6kv/j9511
HwYDVR0jBBgwFoAUmNH4bhDrz5vsYJ8YkBug630J/SswZAYIKwYBBQUHAQEE
MCcGCCsGAQUFBzABhhtodHRwOi8vb2NzcC5wa2kuZ29vZy9ndHMxbzEwKwYI
BQUHMAKGH2h0dHA6Ly9wa2kuZ29vZy9nc3IyL0dUUzFPMS5jcnQwGQYDVR0R
EIIOd3d3Lmdvb2dsZS5jb20wIQYDVR0gBBowGDAIBgZngQwBAgIwDAYKKwYB
eQIFAzAvBgNVHR8EKDAmMCSgIqAghh5odHRwOi8vY3JsLnBraS5nb29nL0dU
MS5jcmwwggEFBgorBgEEAdZ5AgQCBIH2BIHzAPEAdgCyHgXMi6LNiiBOh2b5
JSBna9r6cOeySVMt74uQXgAAAXA5cNqwAAAEAwBHMEUCIQCojKtzOe8l1JYK
bt1puqT4AE3peMVAVk/WeWGp1QIgBvRMbNkwF6i8+JVv3CfTHKvFd8e00+GY
Zb1drKEAdwBep3P531bA57U2SH3QSeAyepGaDIShEhKEGHWWgXFFWAAAAXA5
AAAEAwBIMEYCIQCQSONppELPODh65oFT5ZAGsSQz4FsjNNZedgS7WqzLnQIh
u0QUuoE3RWngfhI6W7n1kxkEmd0vSZTe6+Ql+JVuMA0GCSqGSIb3DQEBCwUA
AQCDU8CVusGstVk1lAmrtg3DyYhNV1UnKyLk3RrHKumwYz5mC25bWGoLVKvv
N3zA329/9JZq0mnn0vmPMxjTDvh9sVQ7g4znwha/KJfzL8AZKUdldD9O+hDO
qVqITZPCAI/ANvbHdZiMEePB8eA+oTiw2ucChqLlsop5Mio8ckg7aXG4/QfC
vkoffK44rs4UEpsaqGe9QqMJjTuO7ZCZrFd1m3geq2ARKPHgPoPM6UbDdqg0
9C0F5ZlOkOgV/qshvpTO4YzE7TB2U571eYEqNXH48syVx8XSk3P7FjM7FIZ2
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
```

PEM

```
-----BEGIN CERTIFICATE-----
MIIEwTCCA6mgAwIBAgIRAO93GGFLfHwOCAAAAAAucZgwDQYJKoZIhvcNAQELBQAw
QjELMAkGA1UEBhMCVVMxHjAcBgNVBAoTFUdvb2dsZSBUcnVzdCBTZXJ2aWNlczET
MBEGA1UEAxMKR1RTIENBIDFPMTAeFw0yMDAyMTIxMTQ3NDFaFw0yMDA1MDYxMTQ3
NDFaMGgxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlhMRYwFAYDVQQH
Ew1Nb3VudGFpbiBWaWV3MRMwEQYDVQQKEwpHb29nbGUgTExDMRcwFQYDVQQDEw53
d3cuZ29vZ2xlLmNvbTBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABCzzLJYFJb8W
TnQ8WL0TySDvfEWCkMe7l81CFspT60knl13YILNdTM22sUwPycyogKjBSaQZ9Axi
AIDbvkoffK44rs4UEpsaqGe9QqMJjTuO7ZCZrFd1m3geq2ARKPHgPoPM6UbDdqgO
TNQo9C0F5ZlOkOgV/qshvpTO4YzE7TB2U571eYEqNXH48syVx8XSk3P7FjM7FIZ2
IzbJSEipZJm8DsP10fFXpToIn+zK
-----END CERTIFICATE-----
```

- 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.

PKCS#7

```
-----BEGIN PKCS7-----
MIIE8gYJKoZIhvcNAQcCoIIE4zCCBN8CAQExADALBgkqhkiG9w0BBwGgggTF
wTCCA6mgAwIBAgIRAO93GGFLfHwOCAAAAAAucZgwDQYJKoZIhvcNAQELBQAw
MAkGA1UEBhMCVVMxHjAcBgNVBAoTFUdvb2dsZSBUcnVzdCBTZXJ2aWNlczET
A1UEAxMKR1RTIENBIDFPMTAeFw0yMDAyMTIxMTQ3NDFaFw0yMDA1MDYxMTQ3
MGgxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlhMRYwFAYDVQQH
b3VudGFpbiBWaWV3MRMwEQYDVQQKEwpHb29nbGUgTExDMRcwFQYDVQQDEw53
Z29vZ2xlLmNvbTBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABCzzLJYFJb8W
WL0TySDvfEWCkMe7l81CFspT60knl13YILNdTM22sUwPycyogKjBSaQZ9Axi
EAiJkbejggJVMIICUTAOBgNVHQ8BAf8EBAMCB4AwEwYDVR0lBAwwCgYIKwYB
AwEwDAYDVR0TAQH/BAIwADAdBgNVHQ4EFgQU9Ty3t90o7UW9+Hc6kv/j9511
HwYDVR0jBBgwFoAUmNH4bhDrz5vsYJ8YkBug630J/SswZAYIKwYBBQUHAQEE
MCcGCCsGAQUFBzABhhtodHRwOi8vb2NzcC5wa2kuZ29vZy9ndHMxbzEwKwYI
BQUHMAKGH2h0dHA6Ly9wa2kuZ29vZy9nc3IyL0dUUzFPMS5jcnQwGQYDVR0R
EIIOd3d3Lmdvb2dsZS5jb20wIQYDVR0gBBowGDAIBgZngQwBAgIwDAYKKwYB
eQIFAzAvBgNVHR8EKDAmMCSgIqAghh5odHRwOi8vY3JsLnBraS5nb29nL0dU
MS5jcmwwggEFBgorBgEEAdZ5AgQCBIH2BIHzAPEAdgCyHgXMi6LNiiBOh2b5
JSBna9r6cOeySVMt74uQXgAAAXA5cNqwAAAEAwBHMEUCIQCojKtzOe8l1JYK
bt1puqT4AE3peMVAVk/WeWGp1QIgBvRMbNkwF6i8+JVv3CfTHKvFd8e00+GY
Zb1drKEAdwBep3P531bA57U2SH3QSeAyepGaDIShEhKEGHWWgXFFWAAAAXA5
AAAEAwBIMEYCIQCQSONppELPODh65oFT5ZAGsSQz4FsjNNZedgS7WqzLnQIh
u0QUuoE3RWngfhI6W7n1kxkEmd0vSZTe6+Ql+JVuMA0GCSqGSIb3DQEBCwUA
AQCDU8CVusGstVk1lAmrtg3DyYhNV1UnKyLk3RrHKumwYz5mC25bWGoLVKvv
N3zA329/9JZq0mnn0vmPMxjTDvh9sVQ7g4znwha/KJfzL8AZKUdldD9O+hDO
qVqITZPCAI/ANvbHdZiMEePB8eA+oTiw2ucChqLlsop5Mio8ckg7aXG4/QfC
vkoffK44rs4UEpsaqGe9QqMJjTuO7ZCZrFd1m3geq2ARKPHgPoPM6UbDdqgO
9C0F5ZlOkOgV/qshvpTO4YzE7TB2U571eYEqNXH48syVx8XSk3P7FjM7FIZ2
SEipZJm8DsP10fFXpToIn+zKoQAxAA==
-----END PKCS7-----
```

Base64

openssl x509 -outform der -in www-google-com.pem -out google.crt

openssl pkcs12 -export -in server.pem -out keystore.pkcs12

Binary

DER

CER

Digital Certificates

Introduction
Authentication Methods
PKI
Digital Certificate Passing

Prof Bill Buchanan OBE

https://asecuritysite.com/digitalcert/

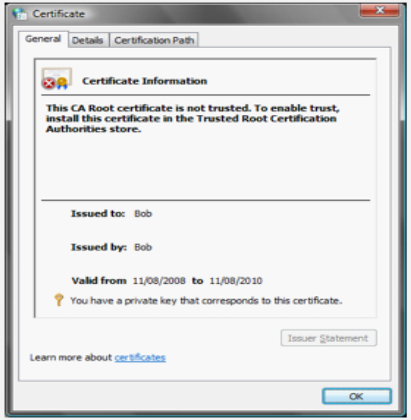
Digital Certificates

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

Eve

Bob

Alice



Trent

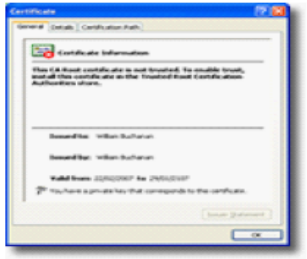
Who do we trust to get Bob's certificate … we can't trust Bob, as he may be Eve… meet Trent.

Who can we trust to get the digital certificate from ?

Trusted Root CA

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

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



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

Trusted root certificate

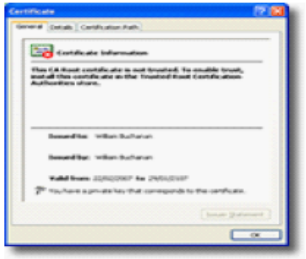
Alice checks the signature of the certificate to validate Bob. Both Alice and Bob trust the CA (Trent) as a third party.

Author: Prof Bill Buchanan

Trusted Root CA

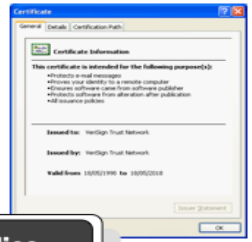
Certificate Authority (CA)
- Able to grant certificates
Examples; Verisign, Entrust, Microsoft Trust.

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



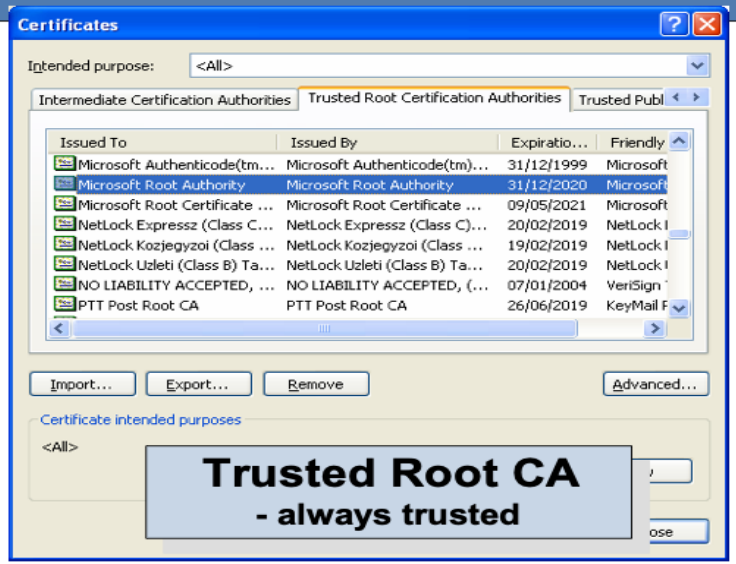
Trusted root certificates are installed as a default on the machine (or installed with the user's permission)

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.

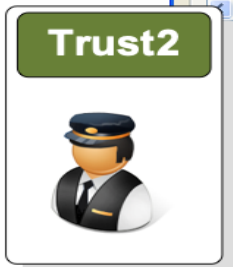
Author: Prof Bill Buchanan

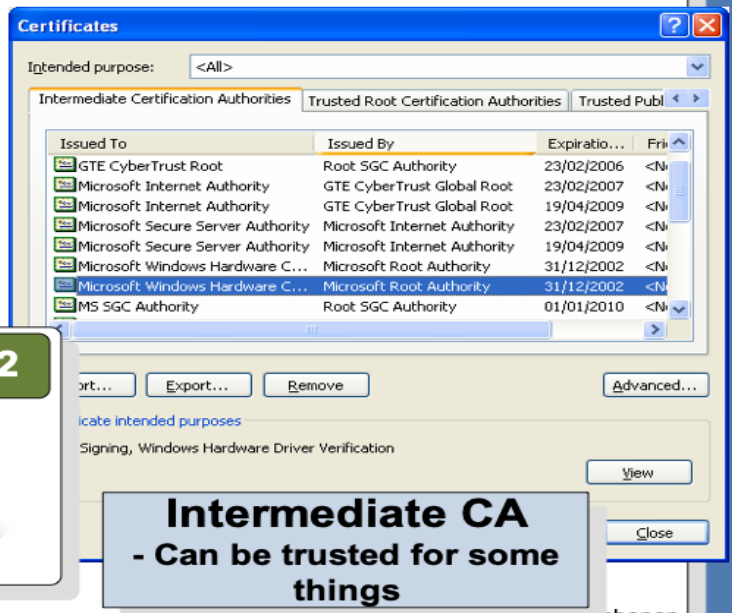


Trusted Root CA

Certificate purposes:

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



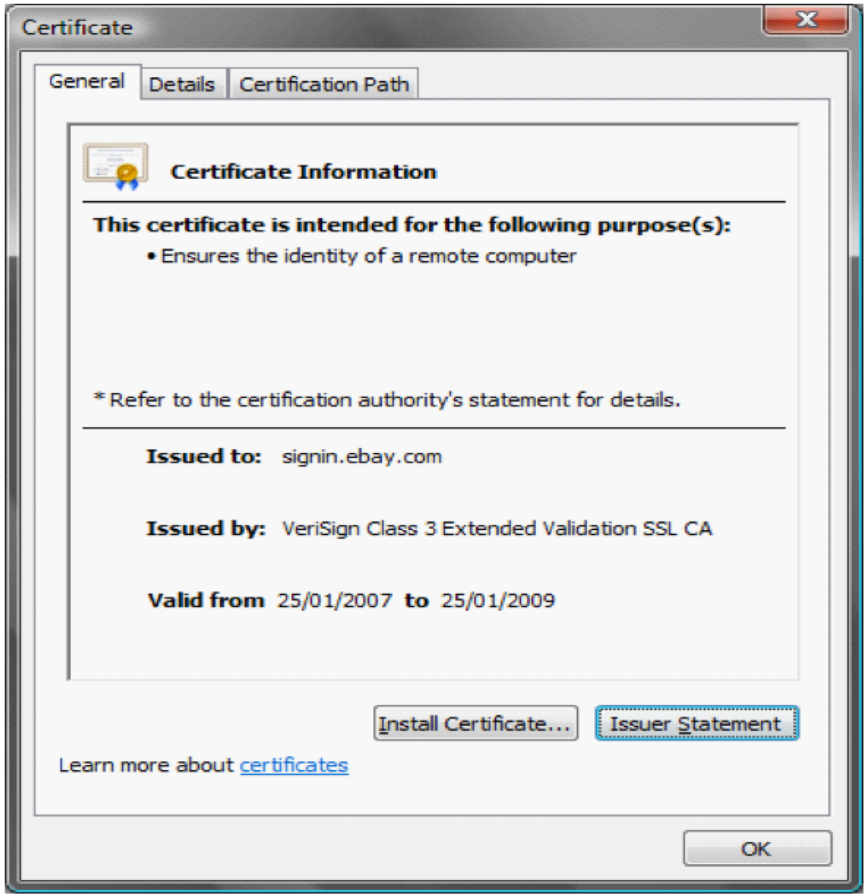


The two main problems with digital certificates are:

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

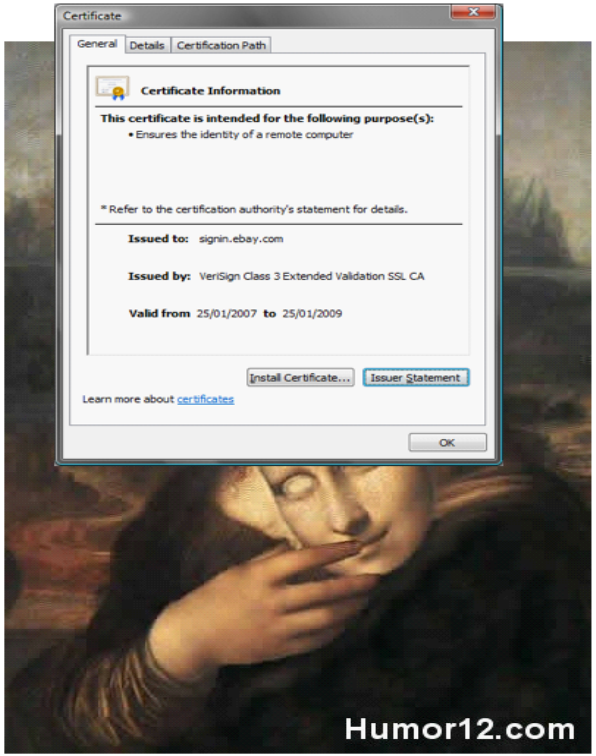
So let's look at a few … are they real or fake?

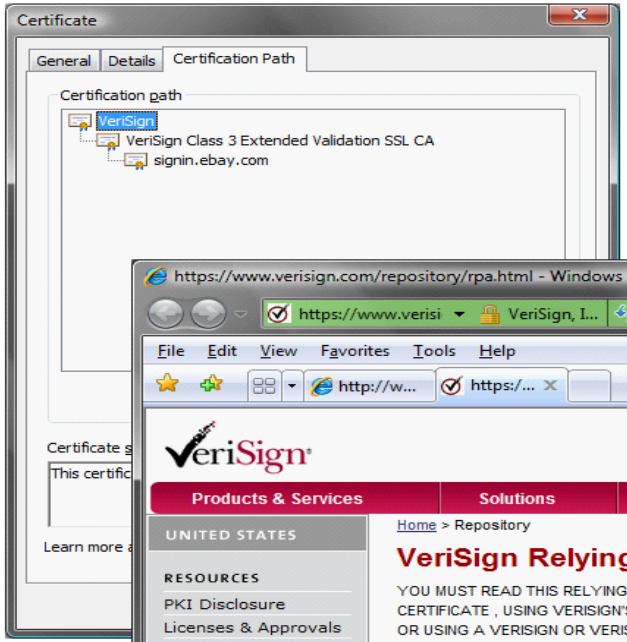
Author: Prof Bill Buchanan



Real or fake?

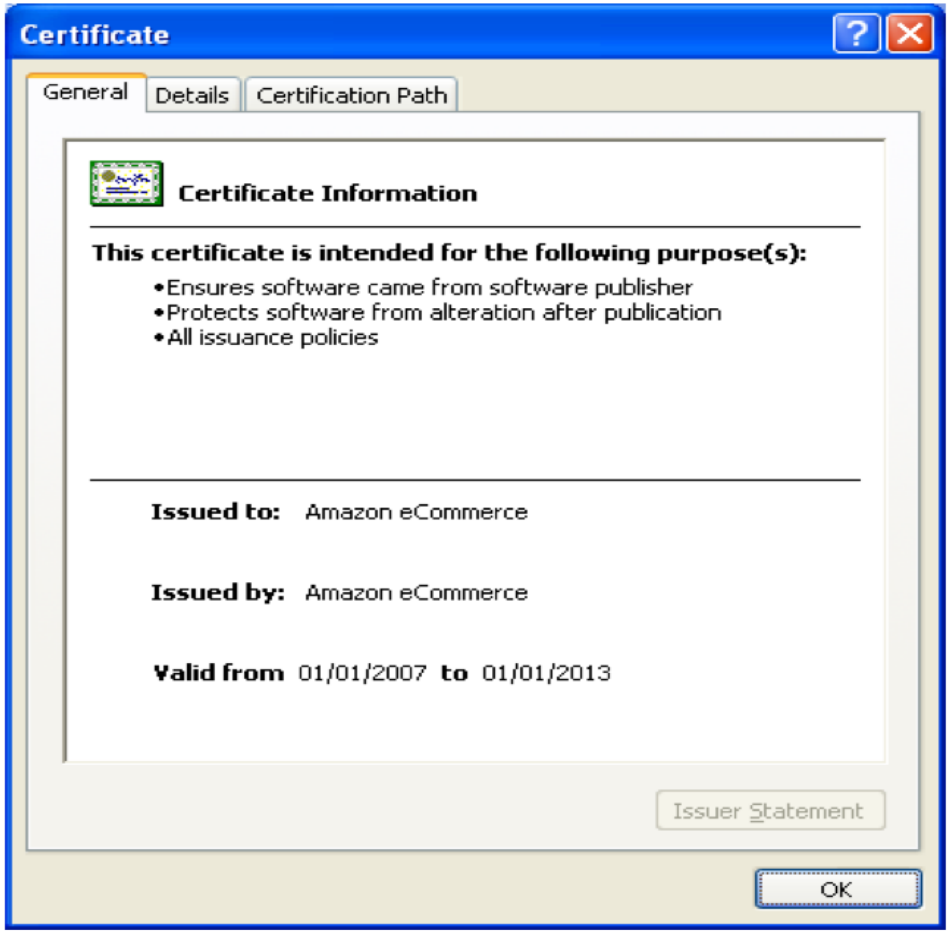
Author: Prof Bill Buchanan





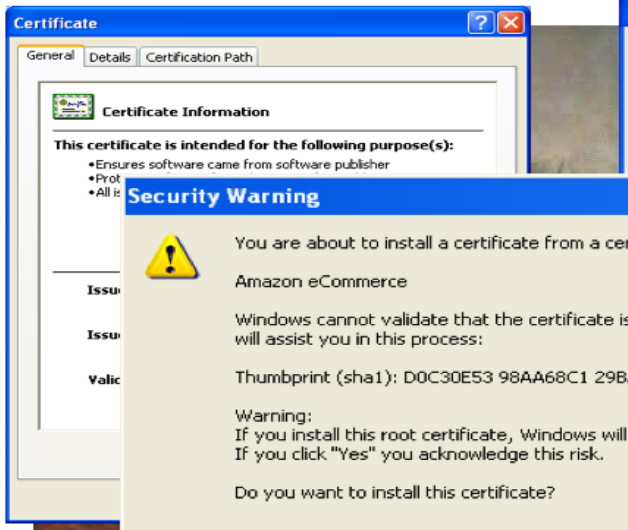
Real!

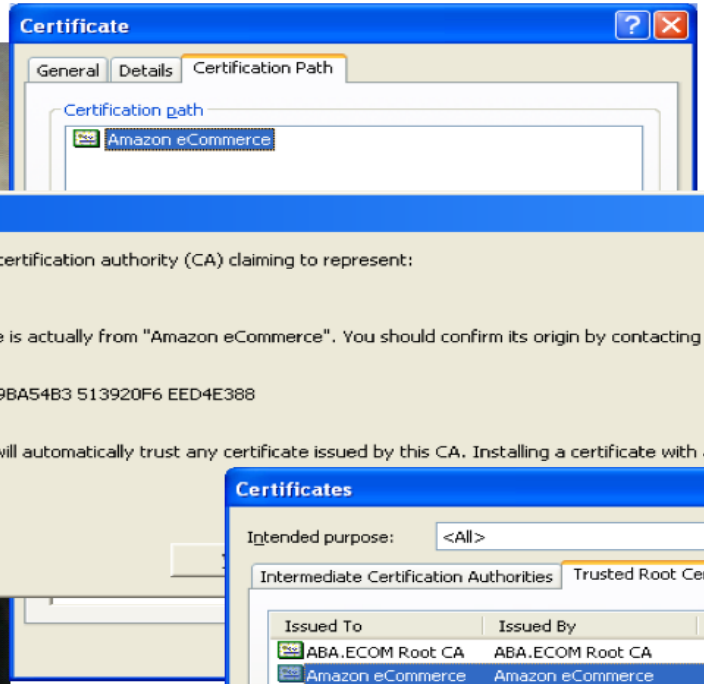
Author: Prof Bill Buchanan



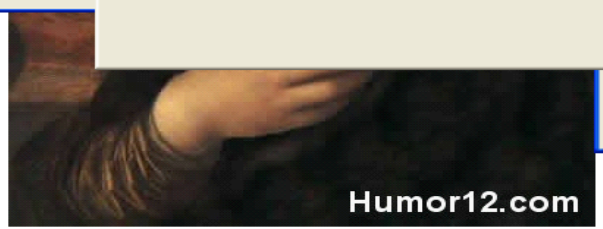
Real or fake?

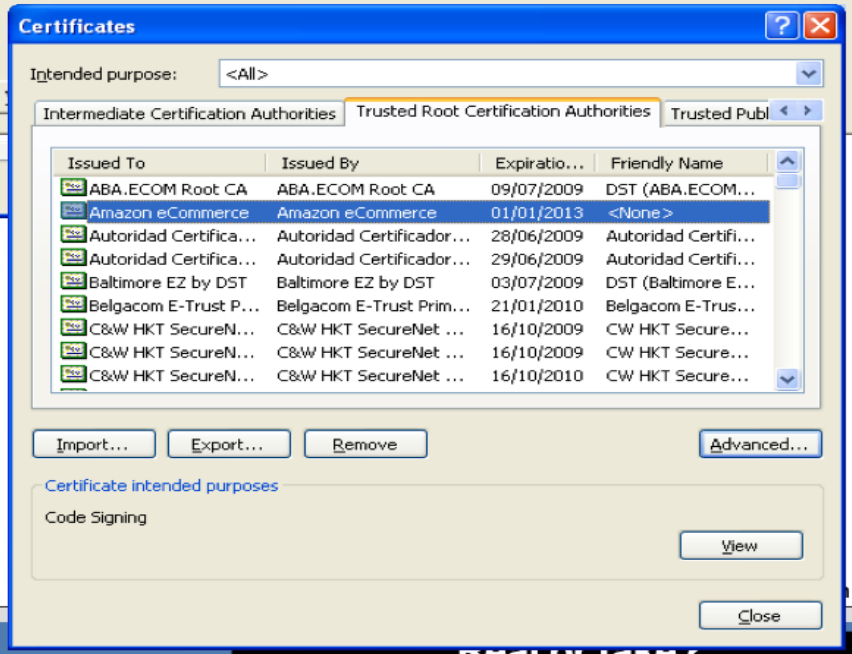
Author: Prof Bill Buchanan


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
•Ensures software came from software publisher


Certificate
General
Details
Certification Path
Certification path
Amazon eCommerce

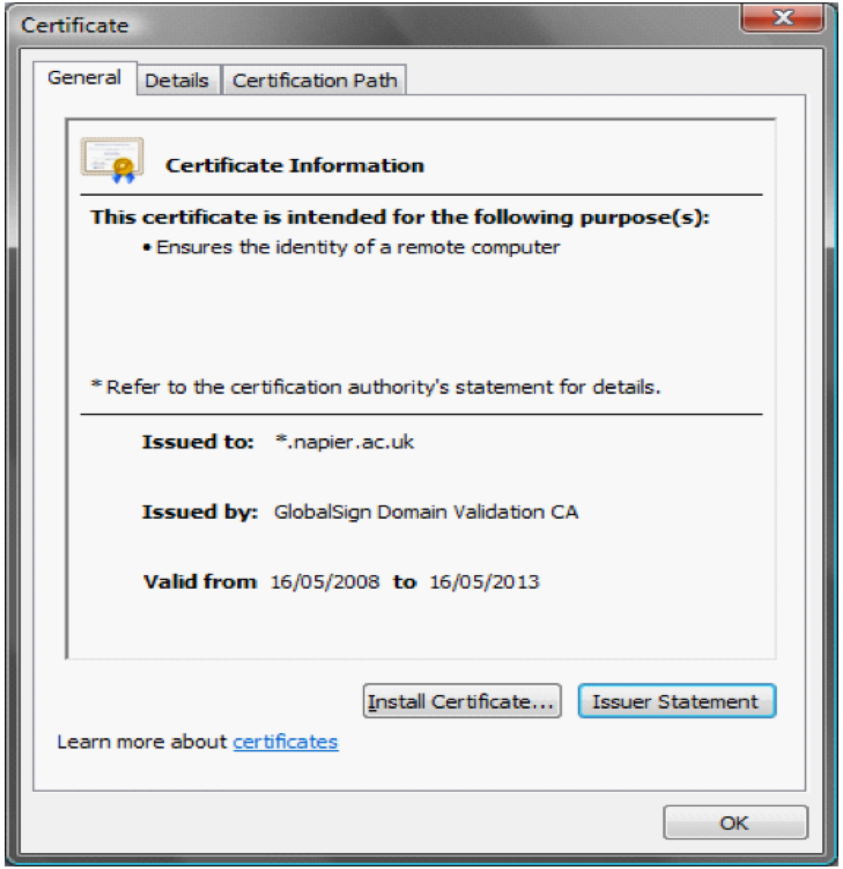
Security Warning
You are about to install a certificate from a certification authority (CA) claiming to represent:
Amazon eCommerce
Windows cannot validate that the certificate is actually from "Amazon eCommerce". You should confirm its origin by contacting "Amazon eCommerce". The following number will assist you in this process:
Thumbprint (sha1): D0C30E53 98AA68C1 29BA54B3 513920F6 EED4E388
Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.
Do you want to install this certificate?


Humor12.com


Certificates
Intended purpose:
<All>
Intermediate Certification Authorities
Trusted Root Certification Authorities
Trusted Publ
Issued To
Issued By
Expiratio...
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

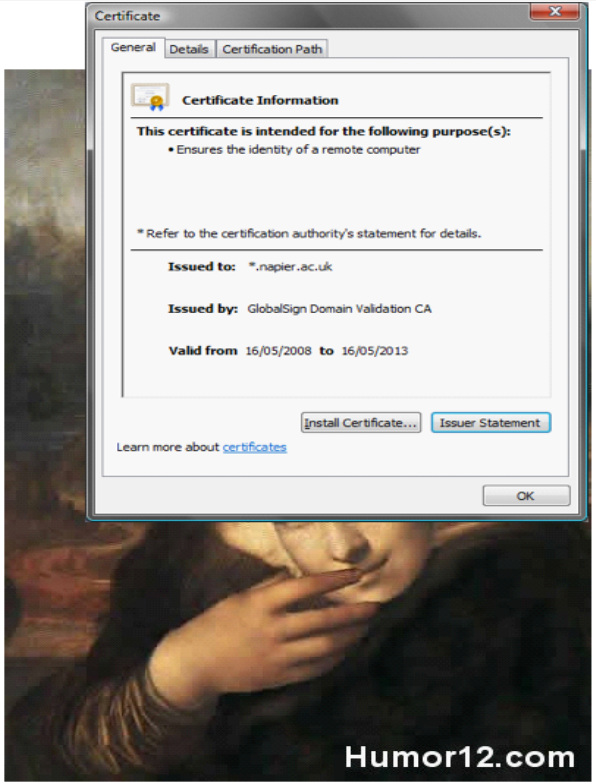

Eve

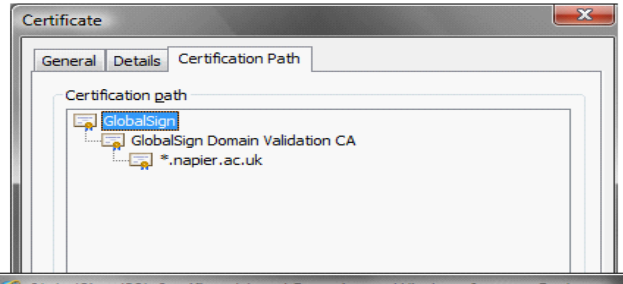
Fake!



Real or fake?

Author: Prof Bill Buchanan





Real

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

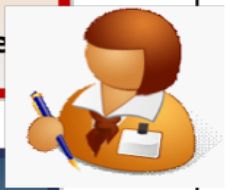
Trent

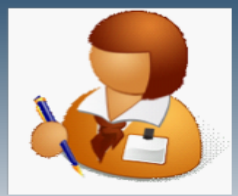
MegaCorp

ob's Private Key

Bob's Public Key

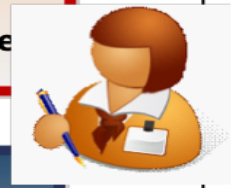
Alice's Public Ke

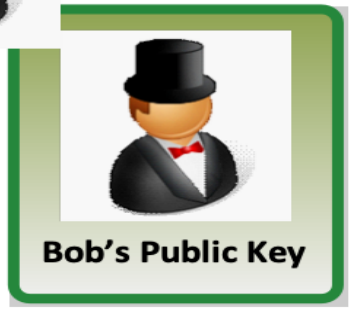




Alice's Private Key

Public key encryption … secret … identity … trust





Public key encryption … secret … identity … trust

Eve

Trent

MegaCorp

Bob's Private Key

Digital Certificate

MegaCorp

Name: Alice
Verified: MegaCorp
Issued: 1 Dec 2013
Valid Until: 1 Jan 2015
Fingerprint: XYZABCD
Trusted For: Email, Web

Alice

Alice's Public Key

Alice's Public Ke

Bob's Public Key

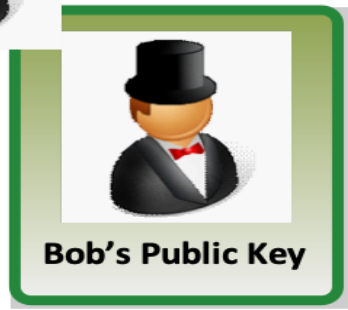
Alice's Public Key

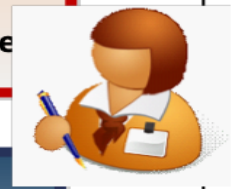
Alice's Private Key

Public key encryption … secret … identity … trust

Hello Alice,
Wish you were here!
- Bob

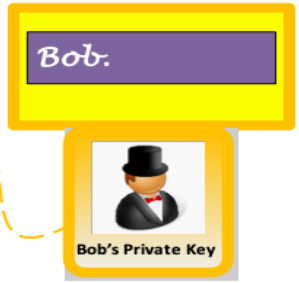
Bob.

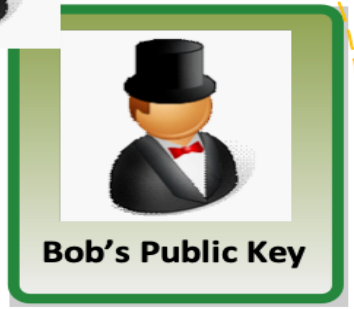


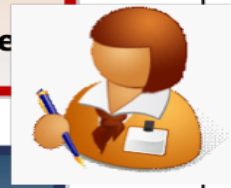


Public key encryption … secret … identity … trust

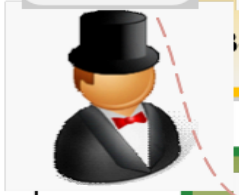
Hello Alice,
Wish you were here!
- Bob

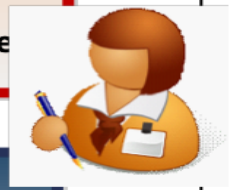


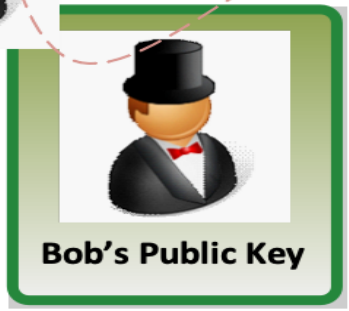




Public key encryption … secret … identity … trust







Public key encryption … secret … identity … trust

Eve

Trent

MegaCorp

ob's Private Key

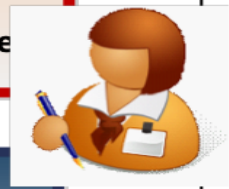
Bob's Public Key

Hello Alice,
Wish you were here!
- Bob

Bob.

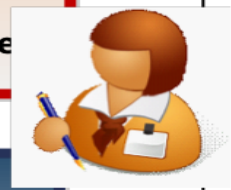
Which key to open the message?

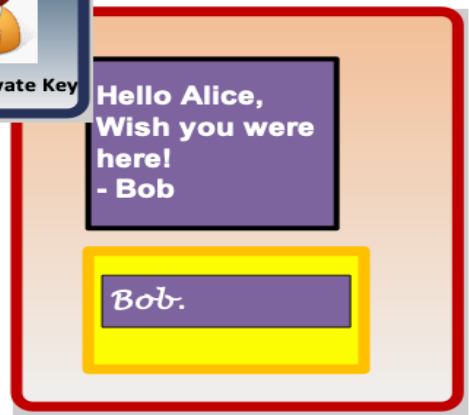
Alice's Public Ke



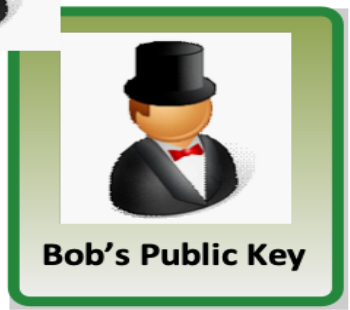
Alice's Private Key

Public key encryption … secret … identity … trust

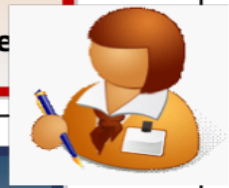




Which key to open the message?

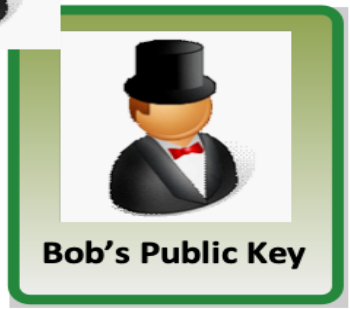


Public key encryption … secret … identity … trust

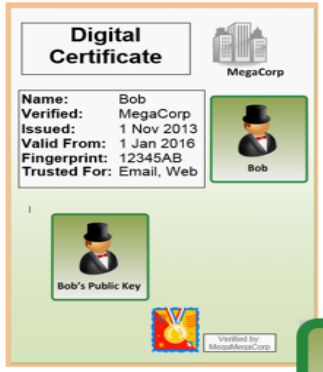


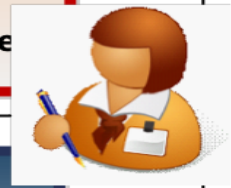
Hello Alice,
Wish you were here!
- Bob

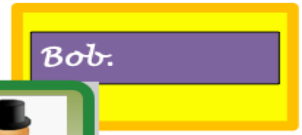
Which key to we open the signature with?

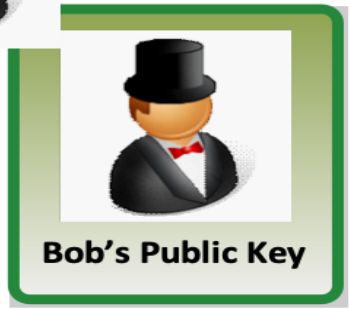


Public key encryption … secret … identity … trust

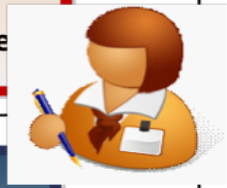




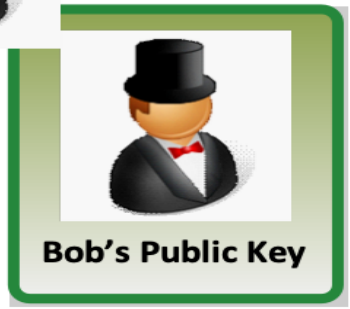




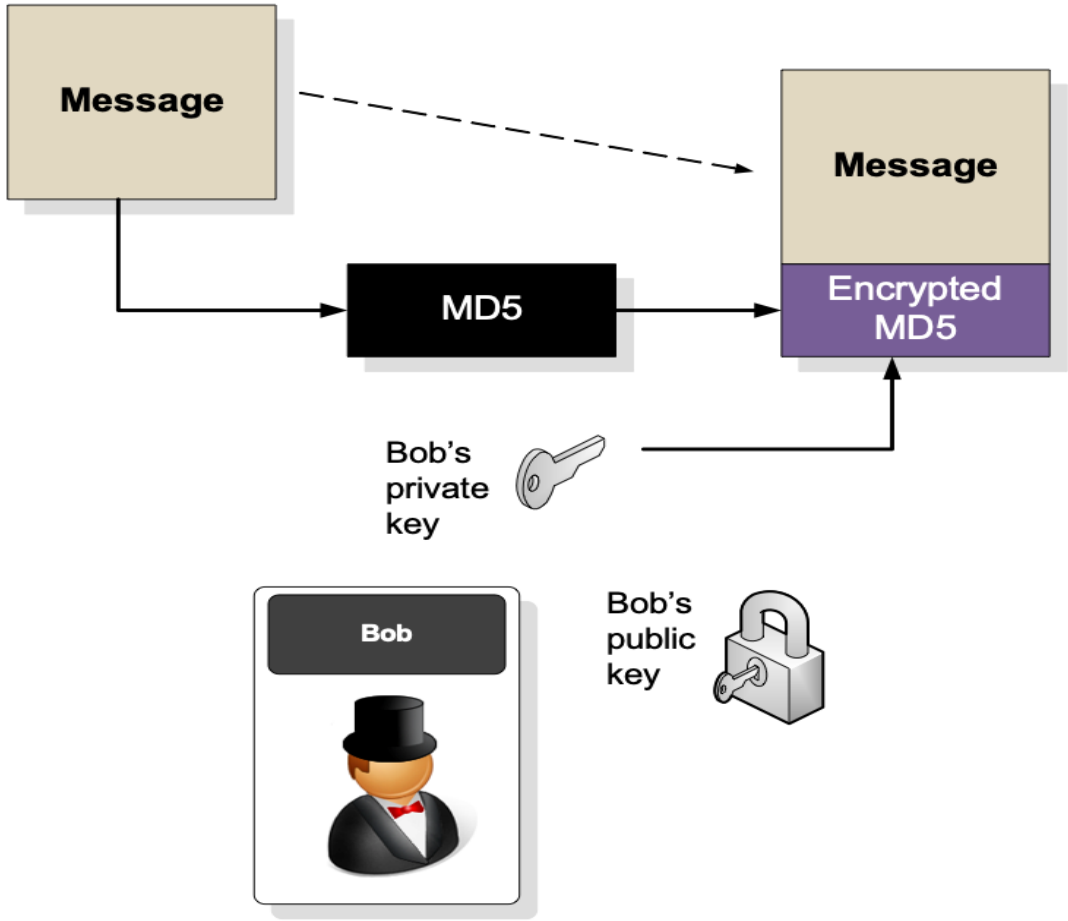
Public key encryption … secret … identity … trust



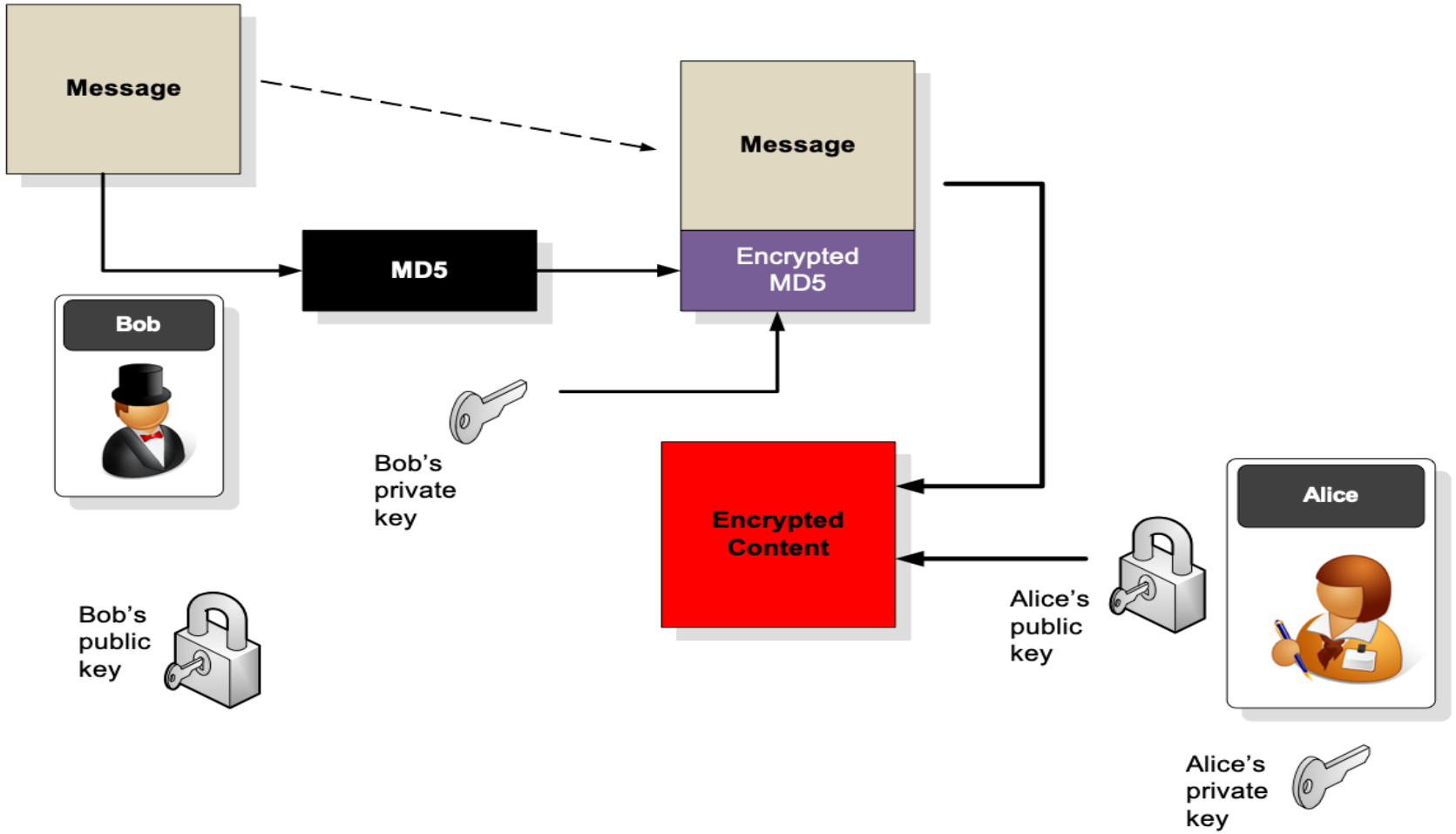
Hello Alice,
Wish you were here!
- Bob



Bob.

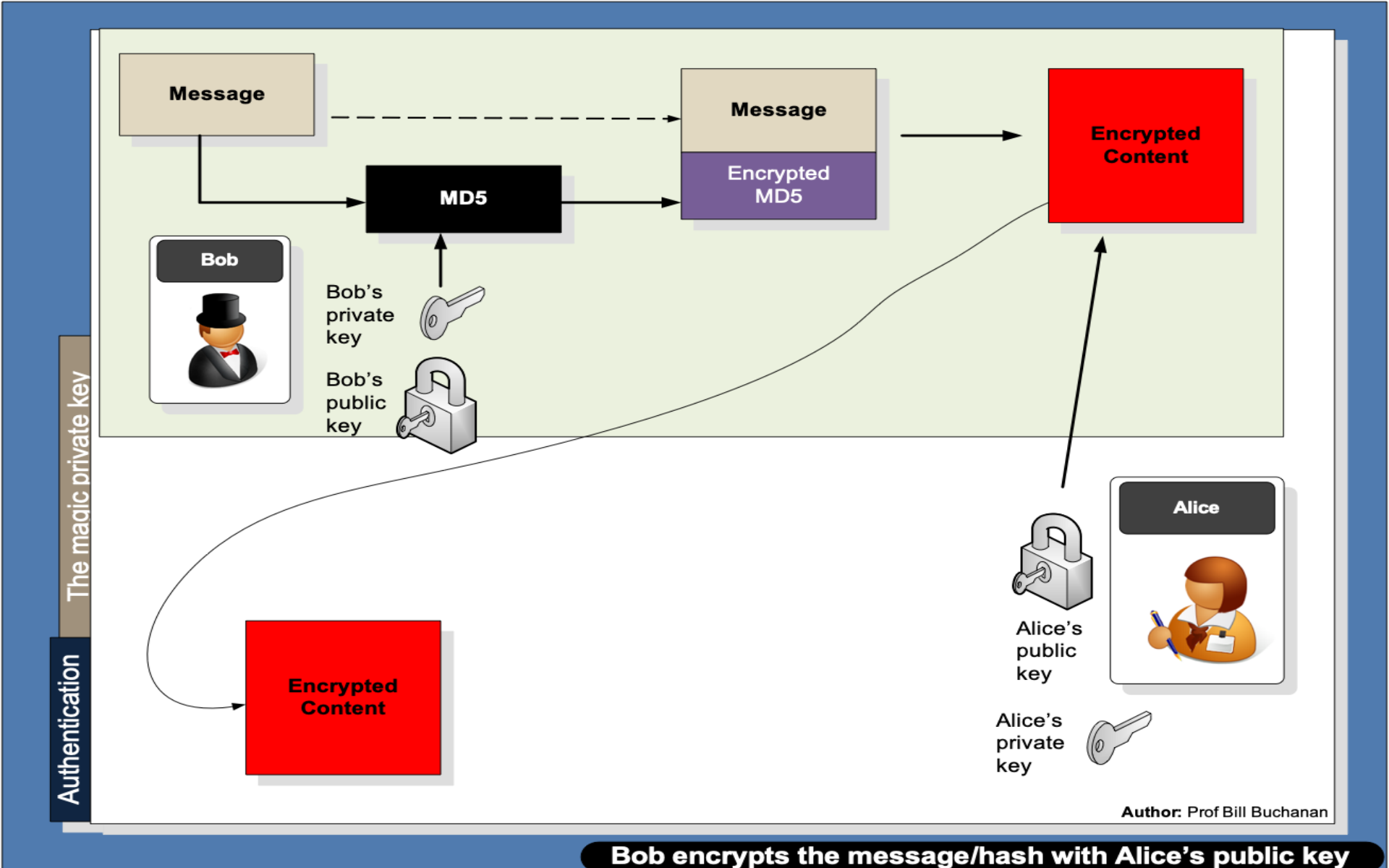


Author: Prof Bill Buchanan

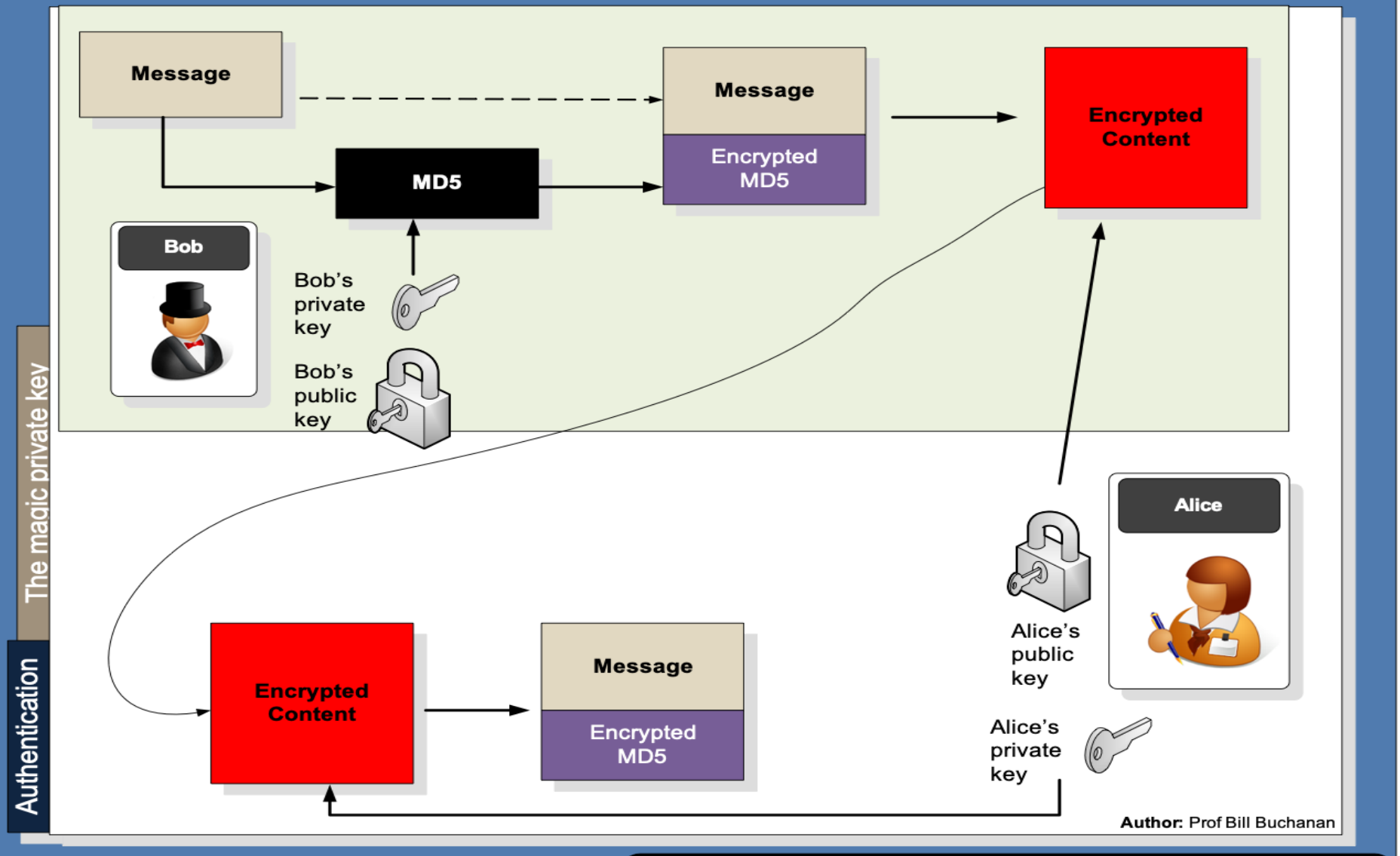


Author: Prof Bill Buchanan

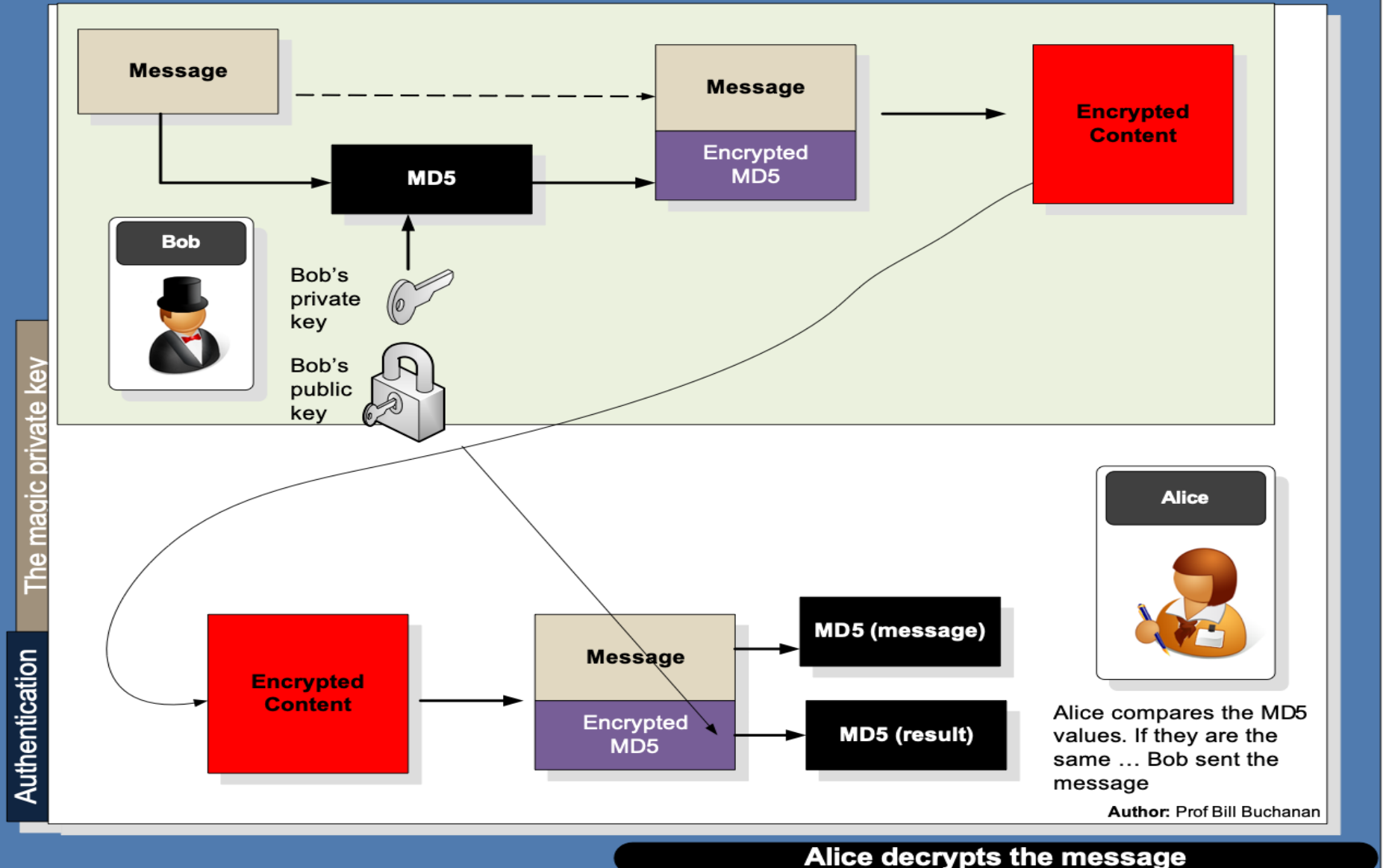
Bob encrypts the message/hash with Alice's public key



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



Alice decrypts the message

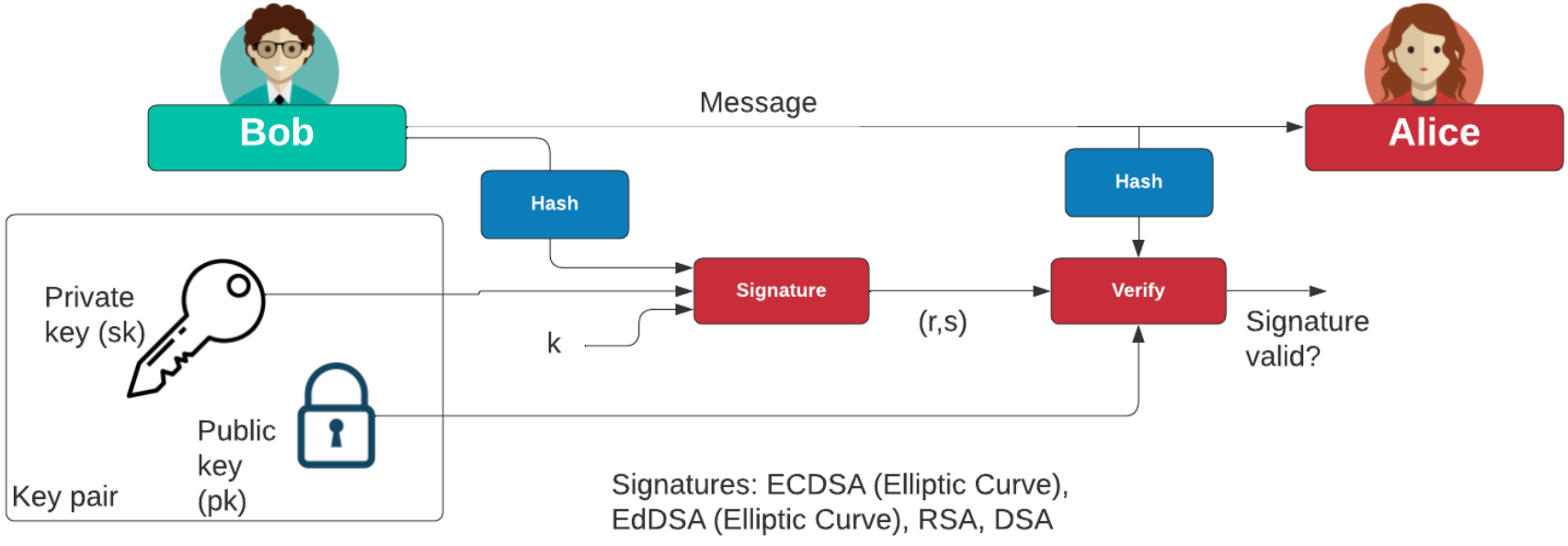

Message
Message
Encrypted MD5
Encrypted Content
MD5
Bob
Bob's private key
Bob's public key
The magic private key
Authentication
Alice
Encrypted Content
Message
Encrypted MD5
MD5 (message)
MD5 (result)
Alice compares the MD5 values. If they are the same … Bob sent the message
Author: Prof Bill Buchanan
Alice decrypts the message

Chapter 6: Digital Certificates

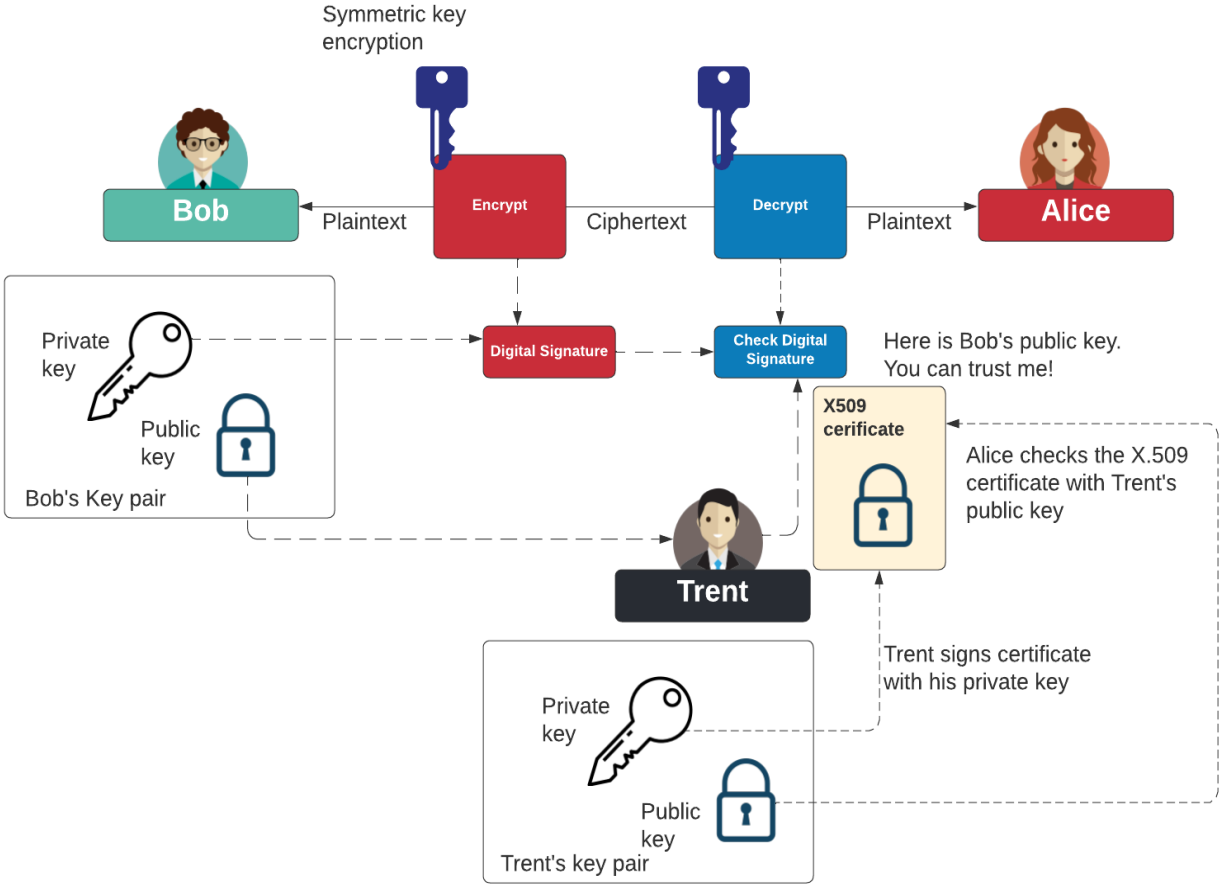
Introduction
Authentication Methods
PKI
Digital Certificate Passing

Prof Bill Buchanan OBE
https://asecuritysite.com/digitalcert/

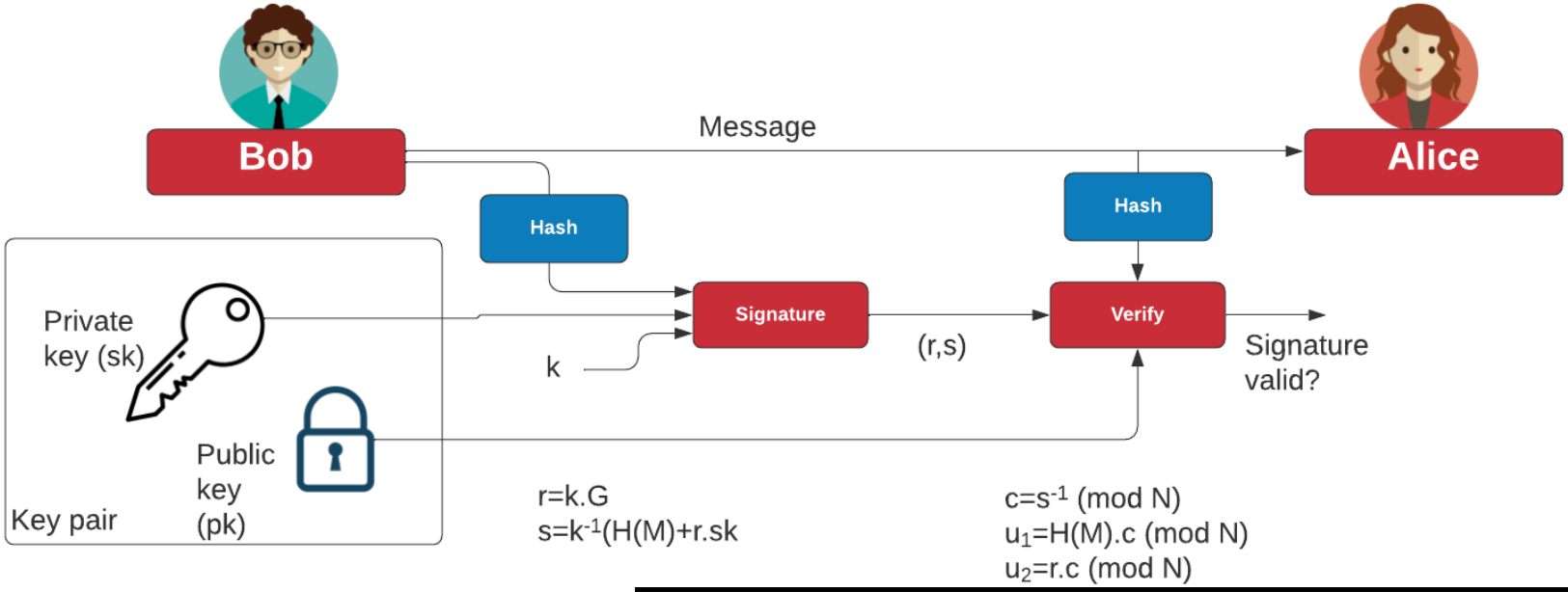
Overview


Bob
Message
Alice
Hash
Hash
Private
key (sk)
Signature
Verify
k
(r,s)
Signature
valid?
Public
key
(pk)
Key pair
Signatures: ECDSA (Elliptic Curve),
EdDSA (Elliptic Curve), RSA, DSA

Trent

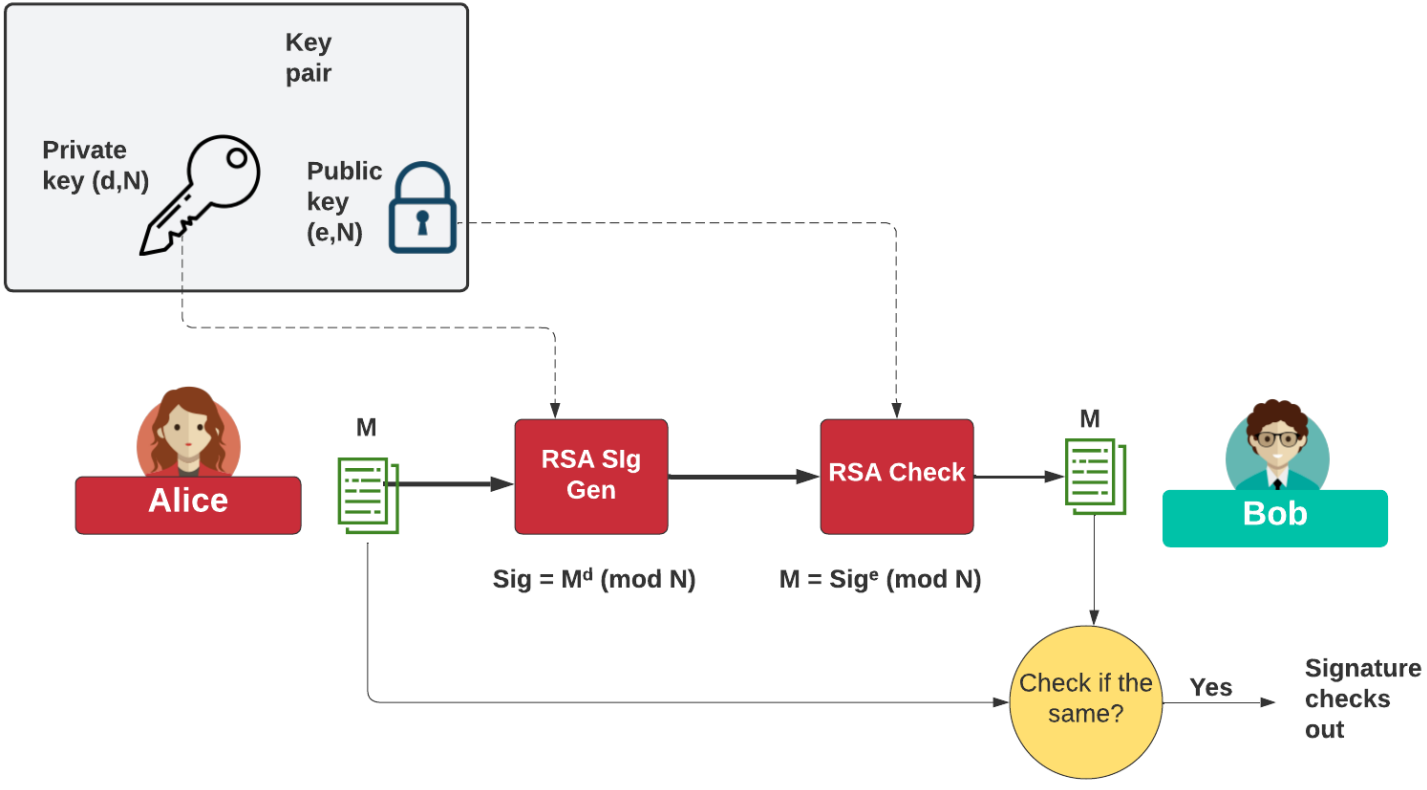

Symmetric key encryption
Bob
Plaintext
Encrypt
Ciphertext
Decrypt
Plaintext
Alice
Private key
Public key
Bob's Key pair
Digital Signature
Check Digital Signature
Here is Bob's public key. You can trust me!
X509 cerificate
Alice checks the X.509 certificate with Trent's public key
Trent
Trent signs certificate with his private key
Private key
Public key
Trent's key pair

ECDSA

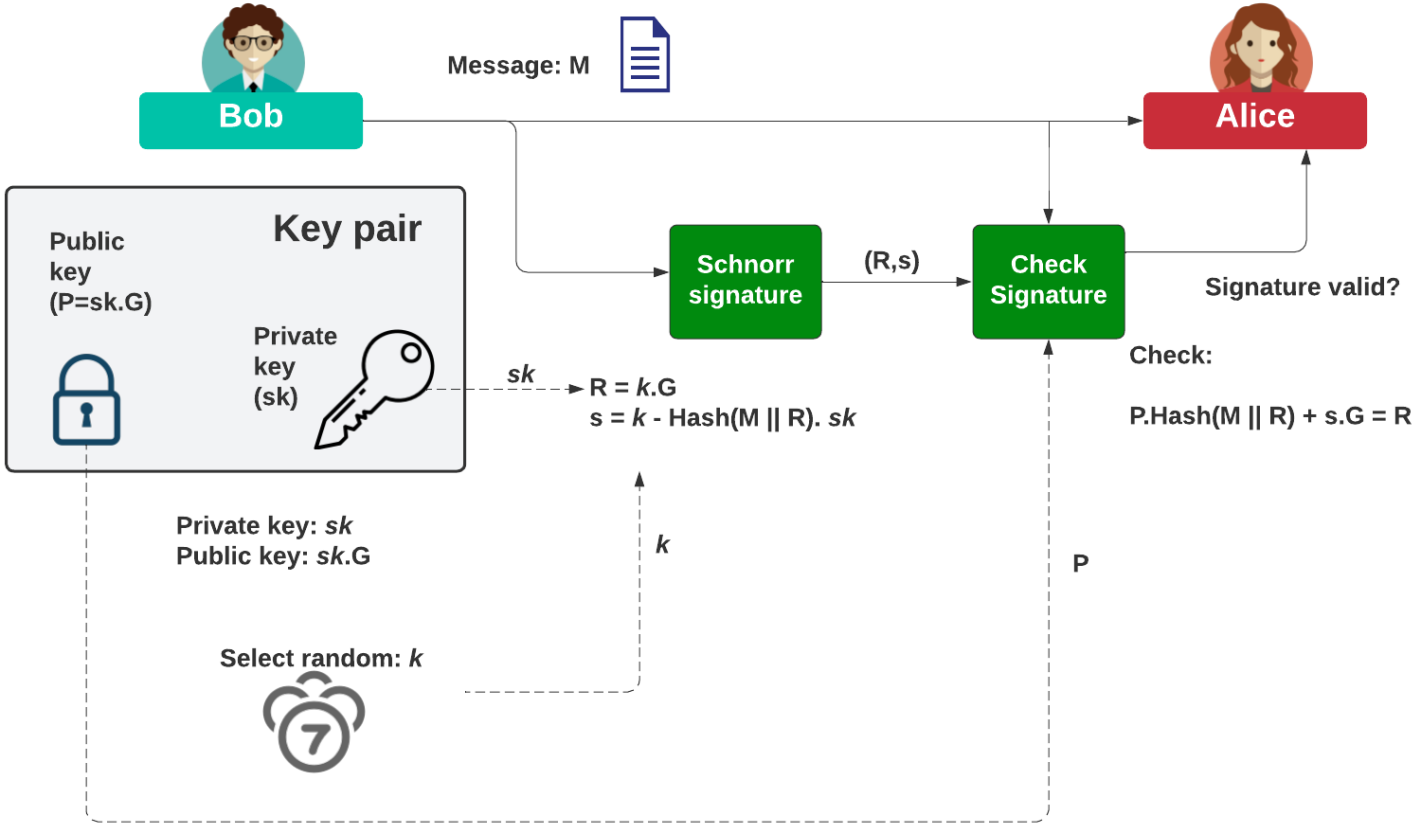



```
Msg: Hello

Alice's private key=91410319197544581782194931321068666964077231613962372395224337286787851207623
Alice's public key=(107007219618086620558122760490508950019883614381385070624798268553636785085033,
50295619771883464285297058390425887963371353465625215351103778057382666752225)
k= 267011473021485390626792993924802270324838695218050221984055234315847884479 63

r=98607808147774449203575356285408019661538158474047478294689777633119075968396
s=99068437226471908177637999380627689653261729073056918331666171421799362411402

Result r=98607808147774449203575356285408019661538158474047478294689777633119075968396
Signature matches!
```

RSA Signatures



Schnorr Signatures – used with EdDSA



Digital Certificates

Introduction
Authentication Methods
PKI
Digital Certificate Passing

Prof Bill Buchanan OBE
https://asecuritysite.com/digitalcert/