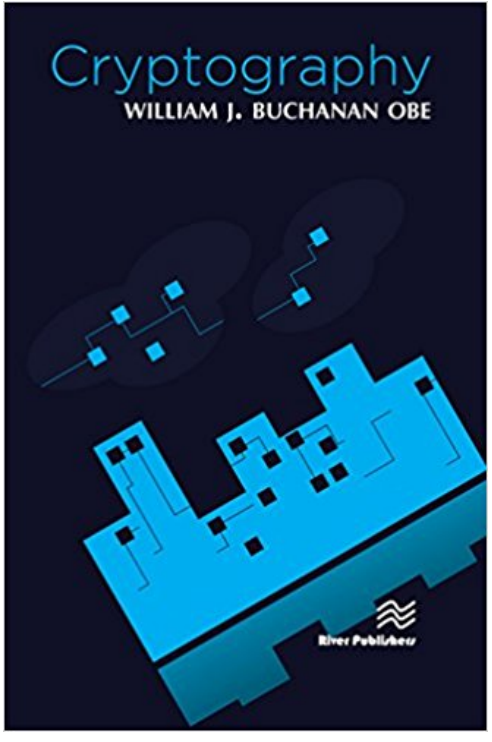
Chapter 6: Digital Certificates

Introduction
Authentication Methods
PKI
Digital Certificate Passing



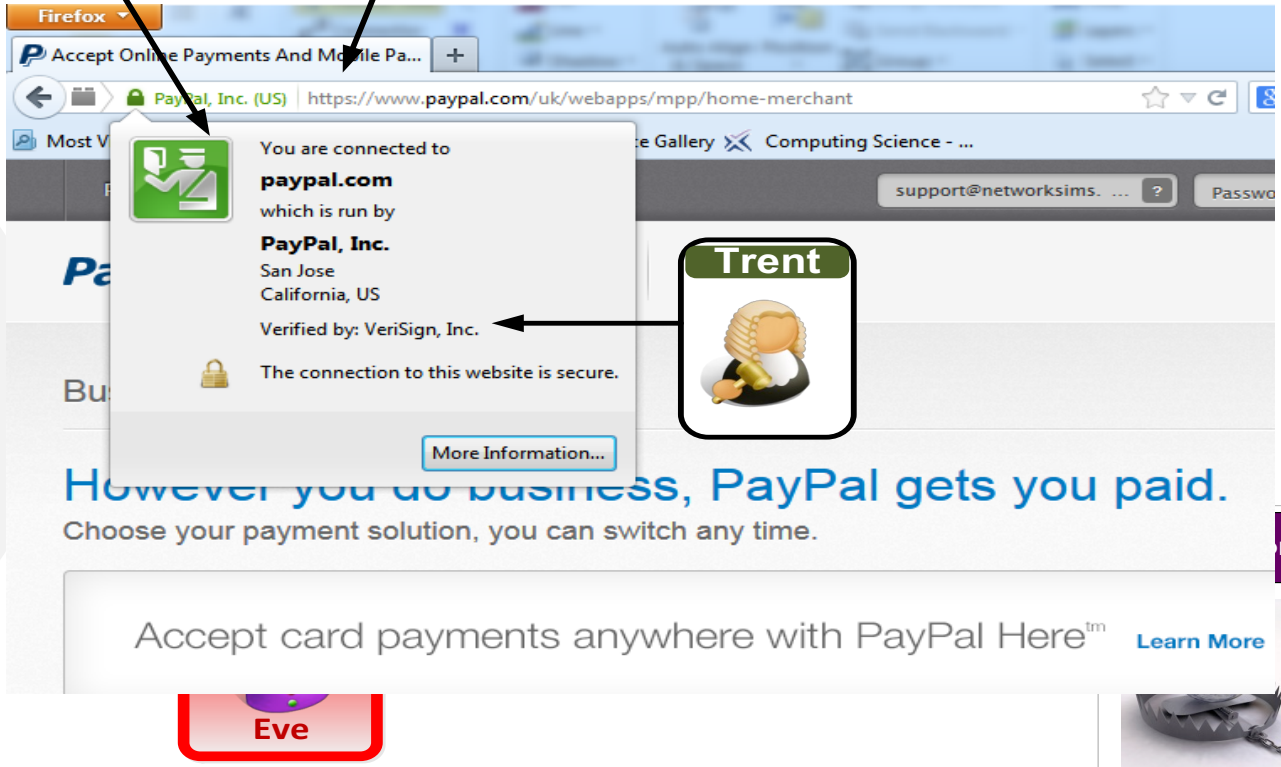
Prof Bill Buchanan OBE

http://asecuritysite.com/crypto06
http://asecuritysite.com/encryption

Identity on the Internet

Identifies it is trusted
(Digital Certificate)

Keeps communications
secure (encryption)



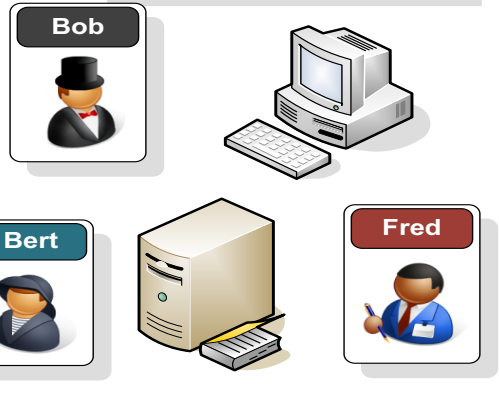
Fundamental principles

Authentication.
Confidence/Assurance.
Privacy/Confidentiality.

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

Confidentiality
(Encryption)

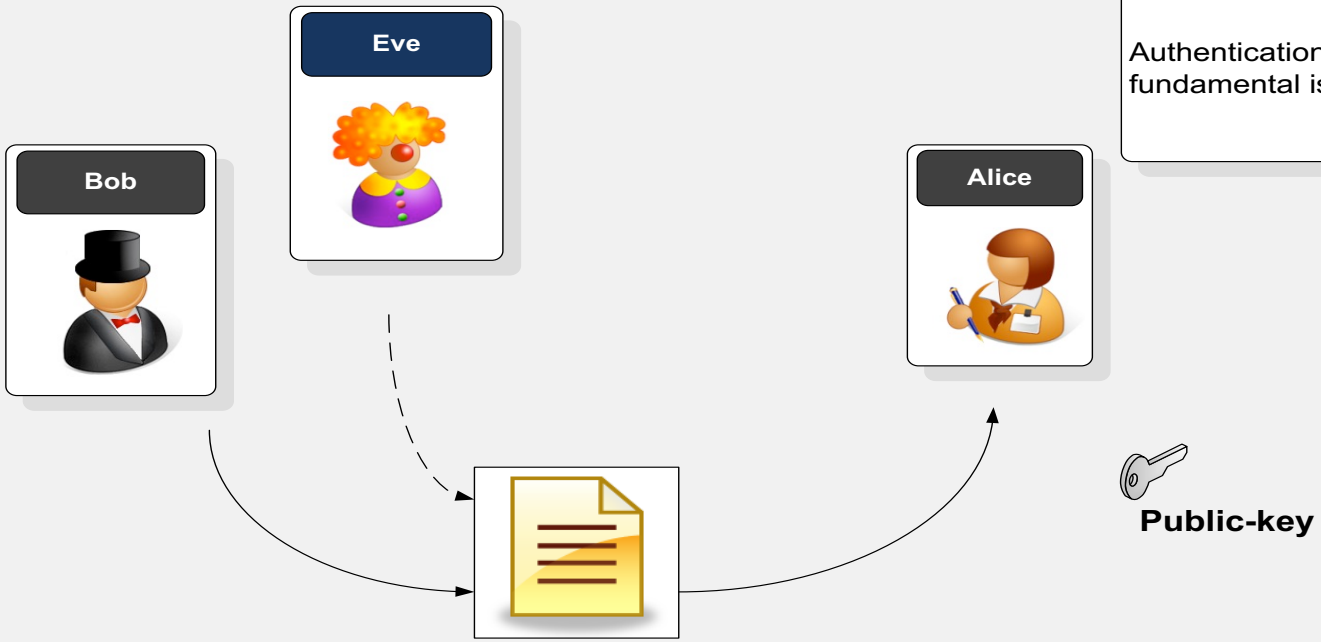
Assurance
(Integrity)



Author: Prof Bill Buchanan

Authentication

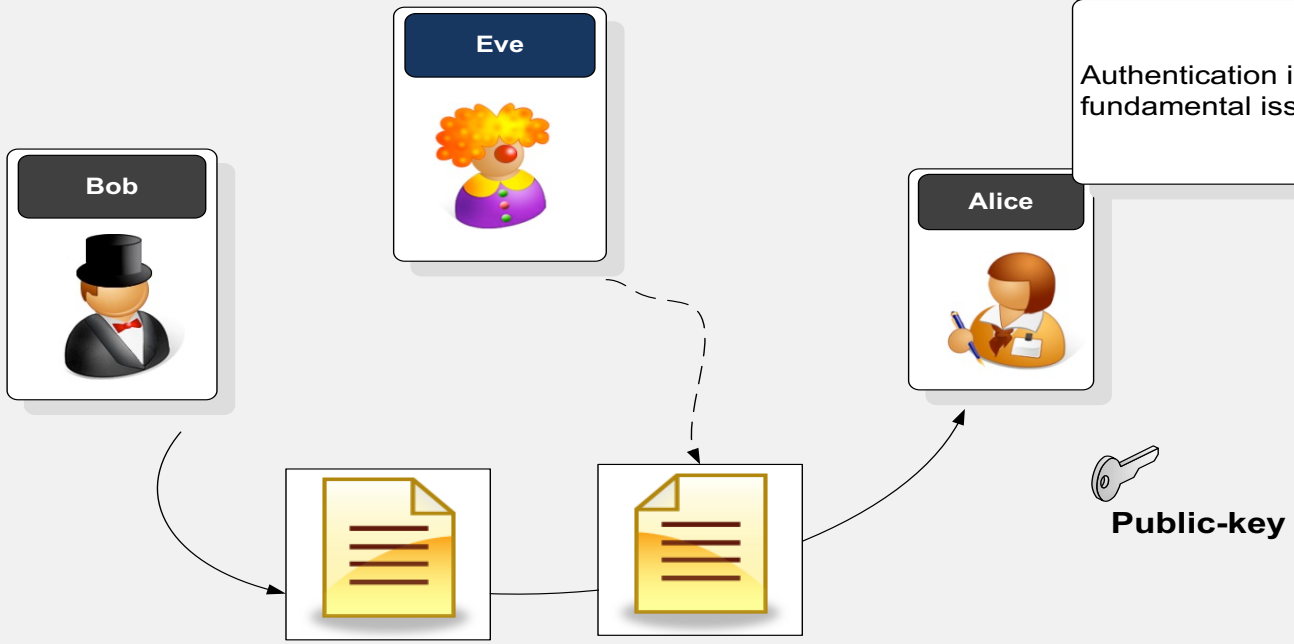
Authentication is a fundamental issue in security.



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.

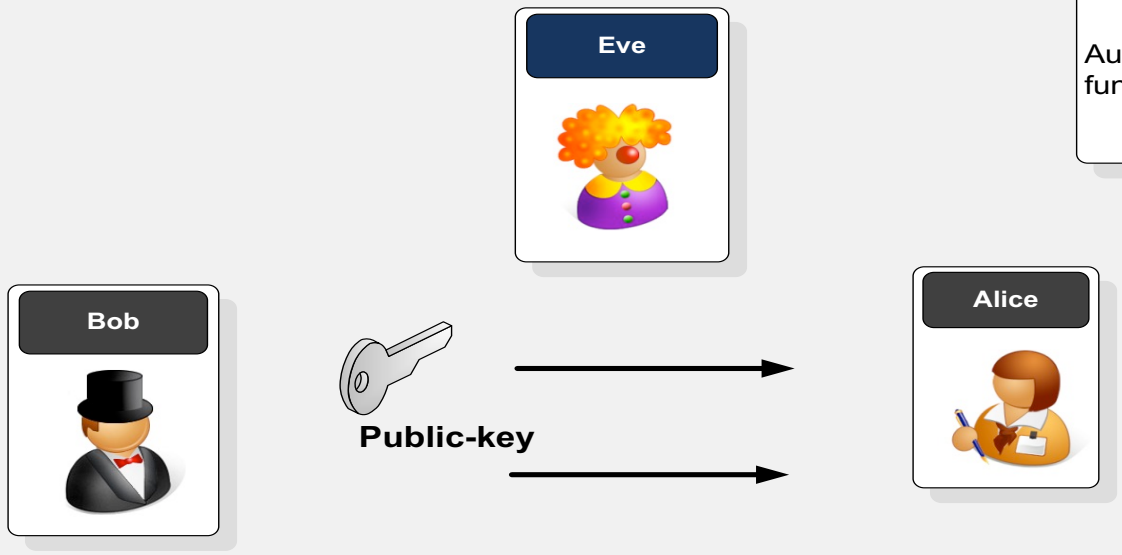


How can we tell that the message has not been tampered with?

Author: Prof Bill Buchanan

Authentication

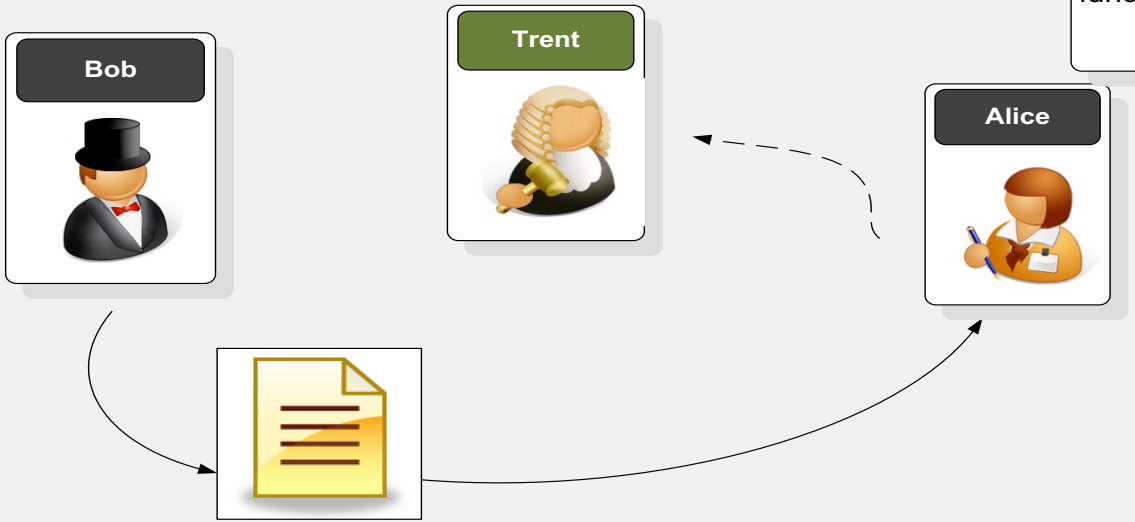
Authentication is a fundamental issue in security.



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.

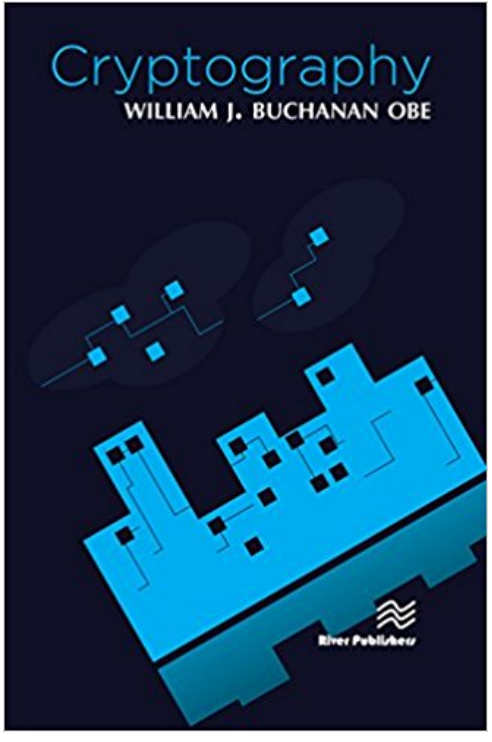
Author: Prof Bill Buchanan

Chapter 6: Digital Certificates

Introduction
Authentication Methods

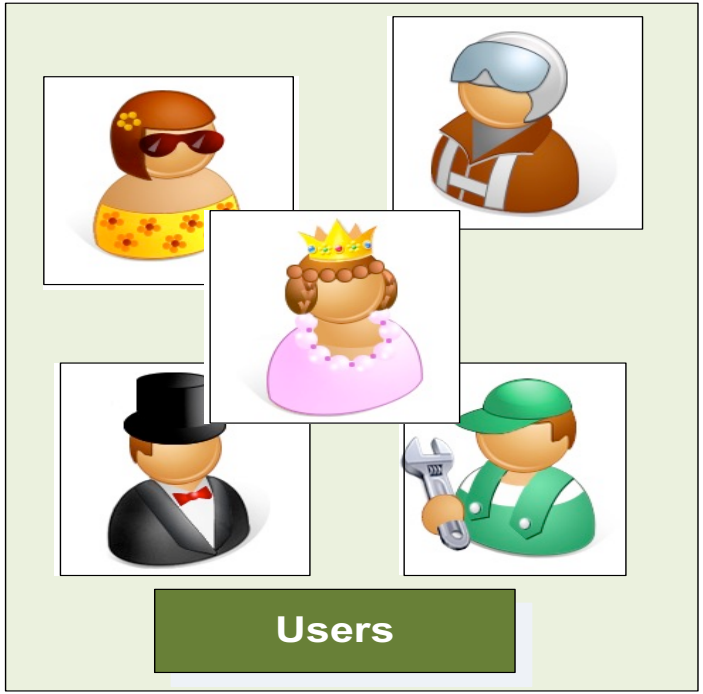
Prof Bill Buchanan OBE

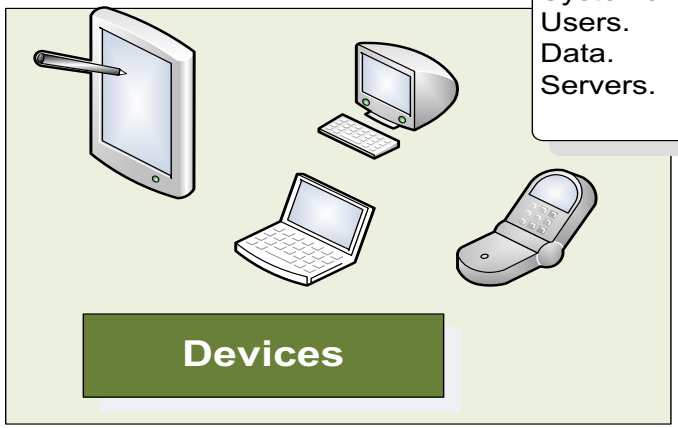
http://asecuritysite.com/crypto06
http://asecuritysite.com/encryption

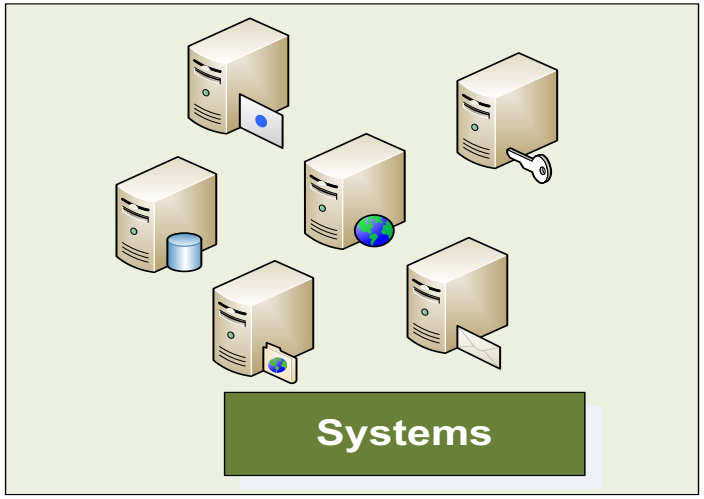


What to authenticate?

Systems.
Users.
Data.
Servers.



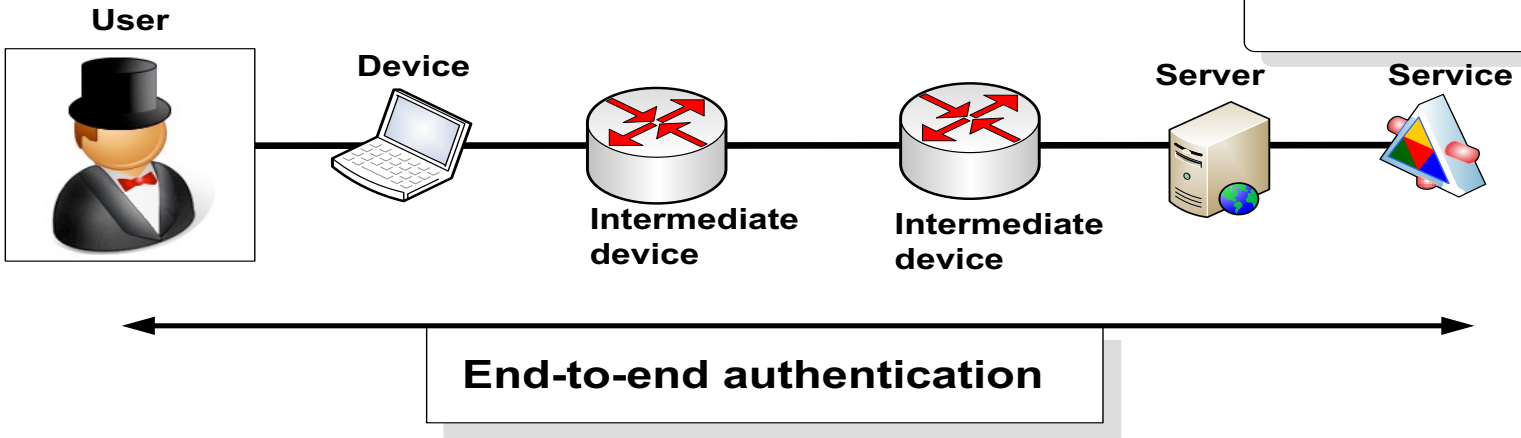


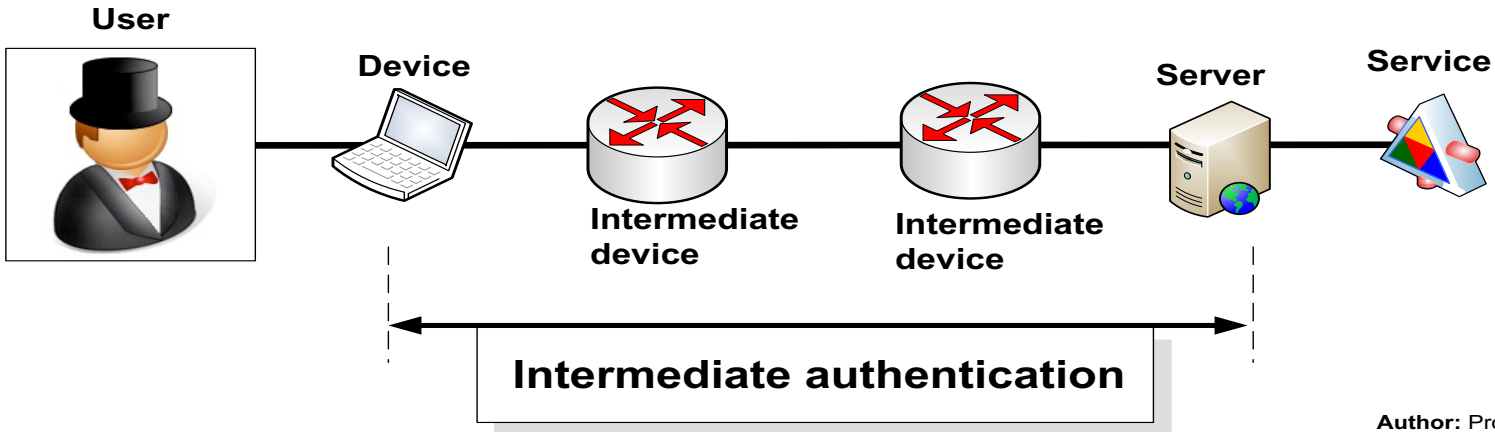


Author: Prof Bill Buchanan

Where authenticated?

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

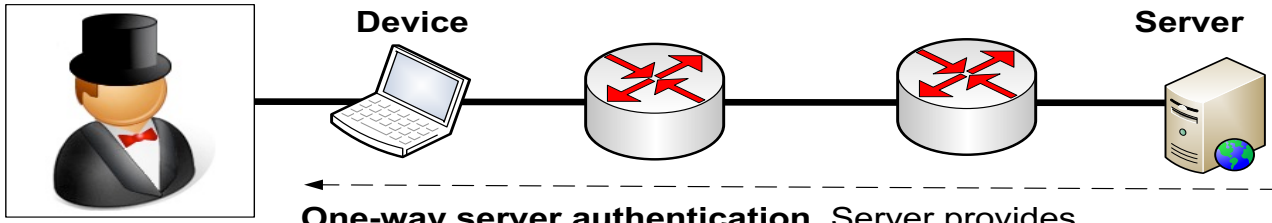




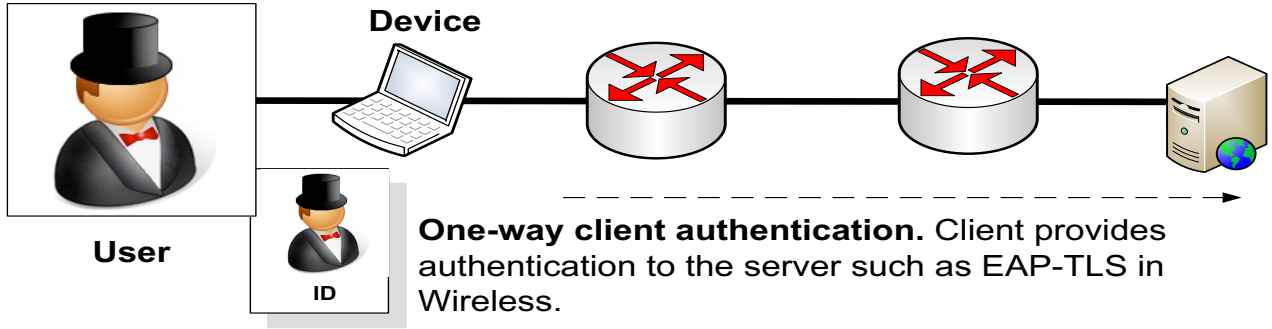
Author: Prof Bill Buchanan

Authentication type

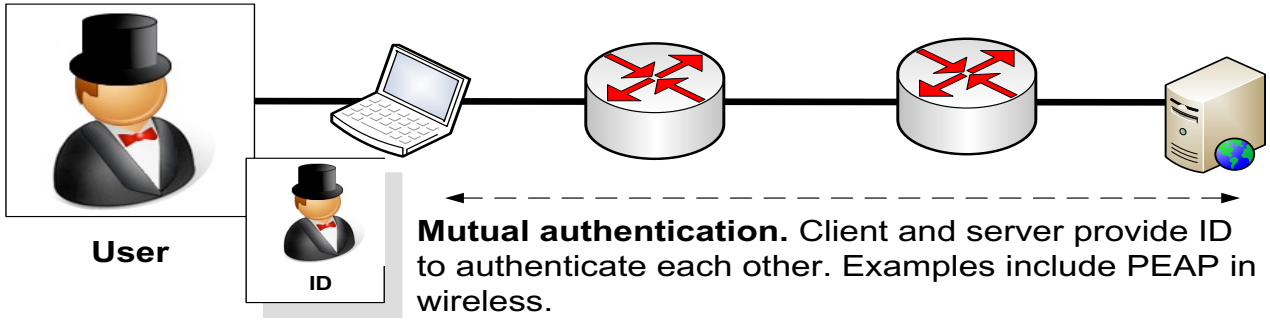
One-way server.
One-way client.
Two-way.



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



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



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

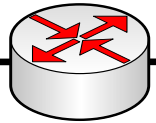
Author: Prof Bill Buchanan

Authentication type

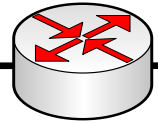
One-way server.
One-way client.
Two-way.

User

Device

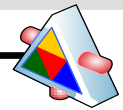


Intermediate device



Intermediate device

Server



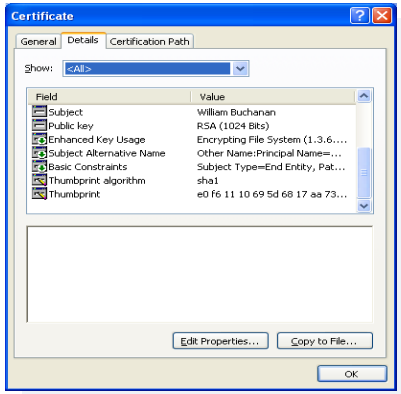
Service

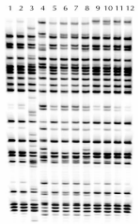
Methods

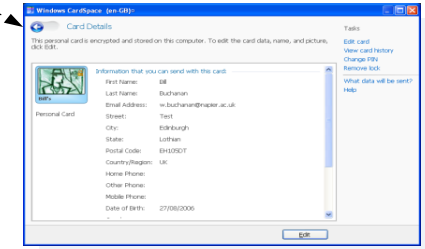
Authentication

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

Device name
Digital Certificate
Pass phrase
MAC address
Encryption key







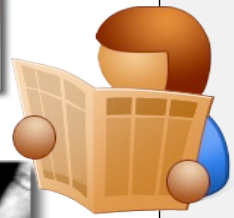
Author: Prof Bill Buchanan

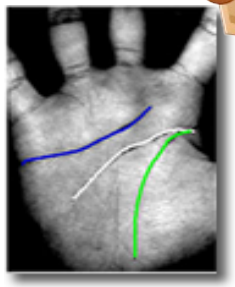
Authentication methods

Something you have
Something you know
Something you are

Iris scans

Retina scan

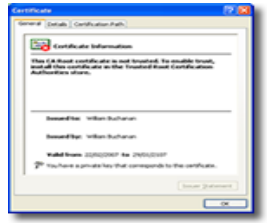




Palm prints

Finger prints

Something you are



Digital certificate

Network/physical address

Smart card

Something you have

Username/ password

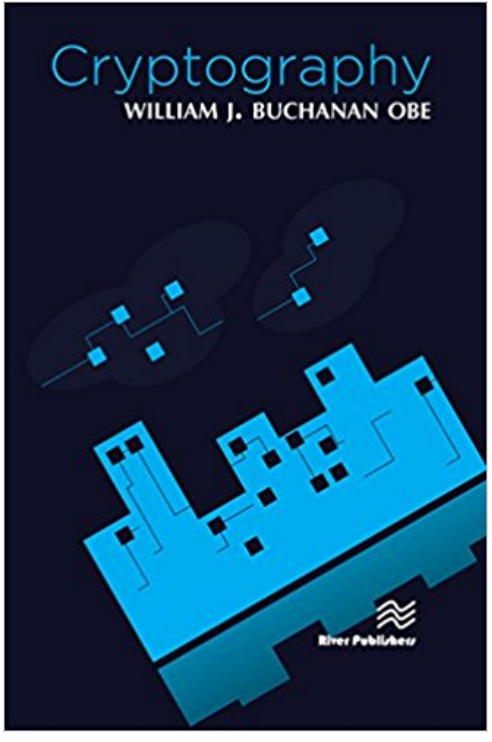
Mother's maiden name

Something you know

Author: Prof Bill Buchanan

Chapter 6: Digital Certificates

Introduction
Authentication Methods
PKI
Digital Certificate Passing

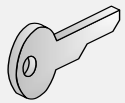


Prof Bill Buchanan OBE

http://asecuritysite.com/crypto06
http://asecuritysite.com/encryption

Digital Certificates

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

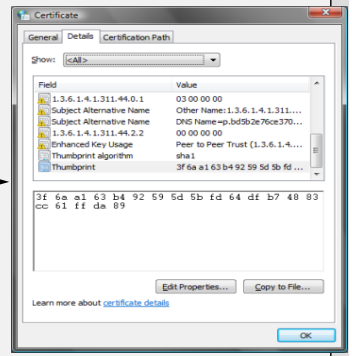


Public-key

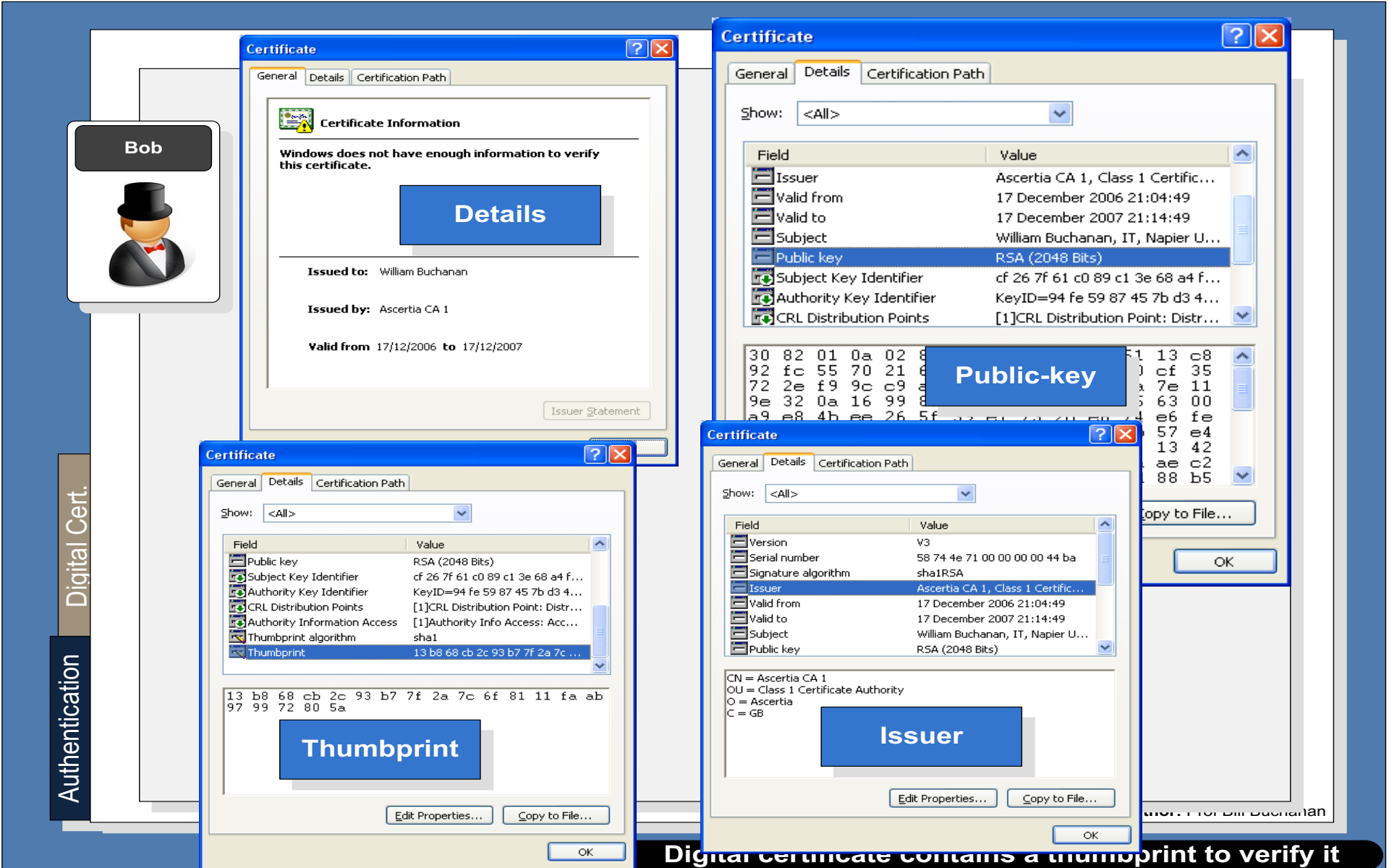
One method is the digital certificate which can carry the public key (and also the private key, if nesc.)

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

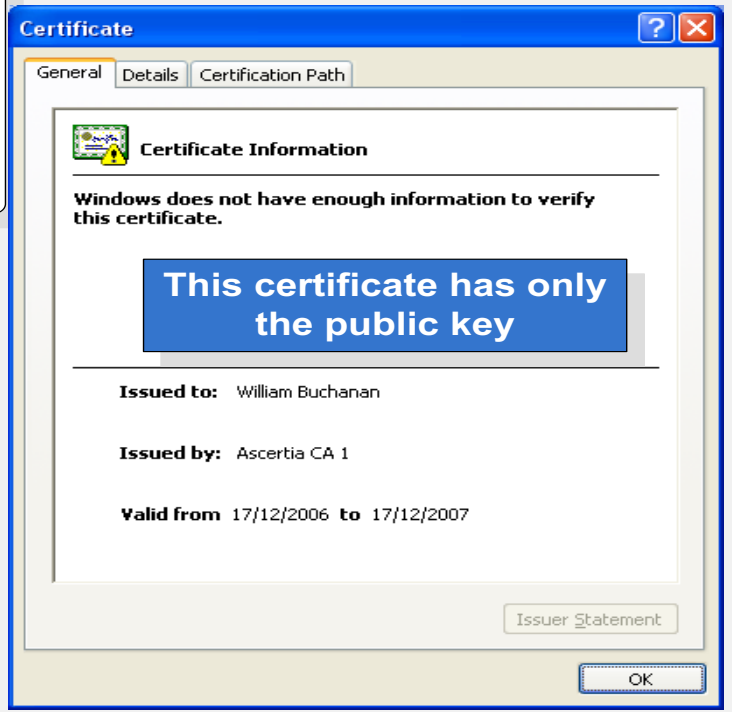
How does Bob distribute his public key to Alice, without having to post it onto a Web site or for Bob to be on-line when Alice reads the message?



How to store the private key and pass the public key?


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...
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

Bob



Digital certificates should only be distributed with the public key

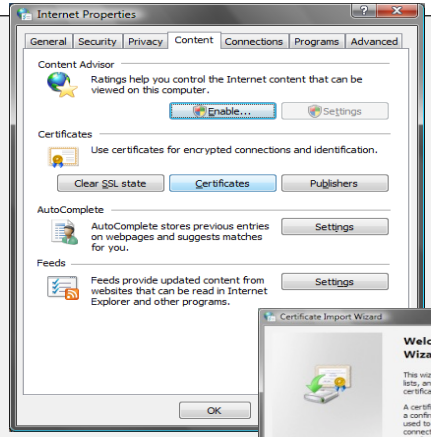
Digital Cert.

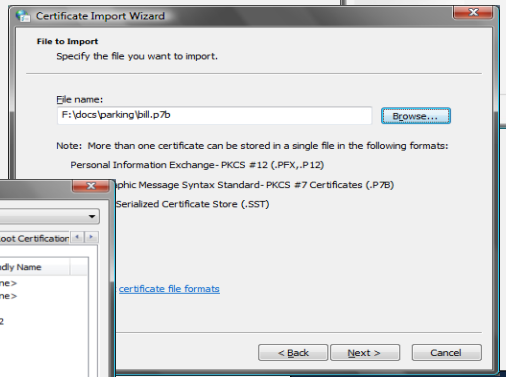
Authentication

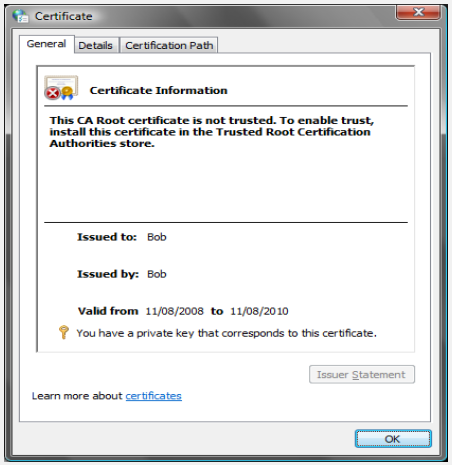
P7b format

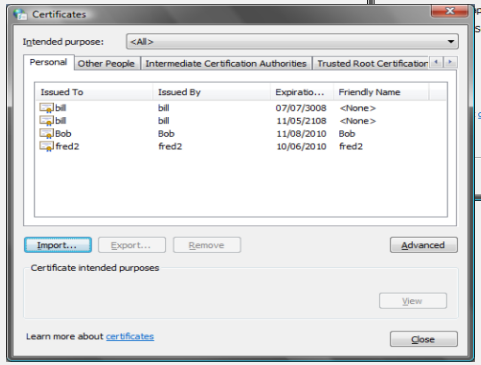
Bob

```
-----BEGIN CERTIFICATE-----
MIID2zCCA4wgAwIBAgIKWHROcQAAAABEujANBgkqhkiG9w0BAQUFADBgMQswCQYD
VQQGEwJHQjERMA8GA1UEChMIQXNjZXJ0aWExJjAkBgNVBAsTHUNsYXNzIDEgQ2Vy
dGlmaWNhdGUgQXV0aG9yaXR5MRYwFAYDVQQDEw1Bc2NlcnRpYSBDQSAxMB4XDTA2
MTIxNzIxMDQ0OVoXDTA3MTIxNzIxMTQ0OVowgZ8xJjAkBgkqhkiG9w0BCQEWF3cu
YnVjaGFuYW5AbmFwaWVyLmFjLnVrMQswCQYDVQQGEwJVSzEQMA4GA1UECBMHTG90
aGlhbjESMBAGA1UEBxMJRWRpbmJ1cmdoMRowGAYDVQQKExFOYXBpZXIgVW5pdmVy
c2l0eTELMAkGA1UECxMCSVQxGTAXBgNVBAMTEFdpbGxpYW0gQnVjaGFuYW4wggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCvCFETyJL8VXAhbEMRzQI0gM81
ci75nMmsOamjZcb6fhGeMgoWmYcoscmQkrVjAKnoS+4mXznhcy3mdOb+sZbwOVaX
M5FOxhSrV+Q86hsK8cDc+1sqyJ8TQtufuDNs0NfNY6tR6q7CgGqQ8/VjSxNqzK39
iLUF1ahhyCet/ab6O/qWzL4iVsz2nmL4dyAuyilhLPlVbppHGdE6sDQXWYd0CpfV
ZN7pauD5fqBESfO6bukCieI47AzRMQj3kHuDt7MexVW7aoX+nXLP4wn7IamaxasF
QvhdOKyCZhYs82JQDGatXRCqkklztmZW5i6GkPsE7XvuX265WJQ5afhp2hYlAgMB
AAGjggEXMIIBEzAdBgNVHQ4EFgQUzyZ/YcCJwT5opPHLPlcQKkOlkJwwYwYDVR0j
BFwwWoAUlP5Zh0V7O0k6CorvRMWB9ifVkBmhP6Q9MDsxCzAJBgNVBAYTAkdCMREw
DwYDVQQKEwhBc2NlcnRpYTEZMBcGA1UEAxMQQXNjZXJ0aWEgUm9vdCBDQYIBDTBN
BgNVHR8ERjBEMEKgQKA+hjxodHRwOi8vd3d3LmFzY2VydGlhLmNvbS9PbmxpbmVD
QS9jcmxzLOFzY2VydGlhQOExL2NsYXNzMS5jcmwwPgYIKwYBBQUHAQEEMjAwMC4G
CCsGAQUFBzAChiJodHRwOi8vb2NzcC5nbG9iYWxOcnVzdGzpbmRlci5jb20vMA0G
CSqGSIb3DQEBBQUAA0EATOCwGJ1tS0kTlupmpjkMl8IdxMmD5WuhszjBlGsMhPxI
H+vXhL9yaOw+Prpzy7ajS4/3xXU8vRANhyU9yU4qDA==
-----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

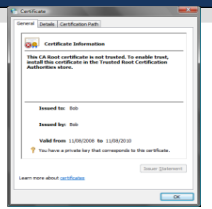
A. Bob creates the message.
B. Bob encrypts with Alice's public key and sends Alice the encrypted message
C. Alice decrypts with her private key
D. Alice receives the message

A

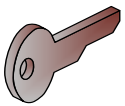
Encryption

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

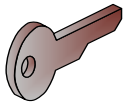
Author: Prof Bill Buchanan

A

Encryption/ Decryption

Communications Channel

Encryption/ Decryption



Hello

B

Hash

C

Alice's private key

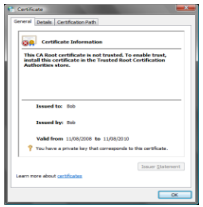
Bob's private key

H&$d.

D

Hello

Hash



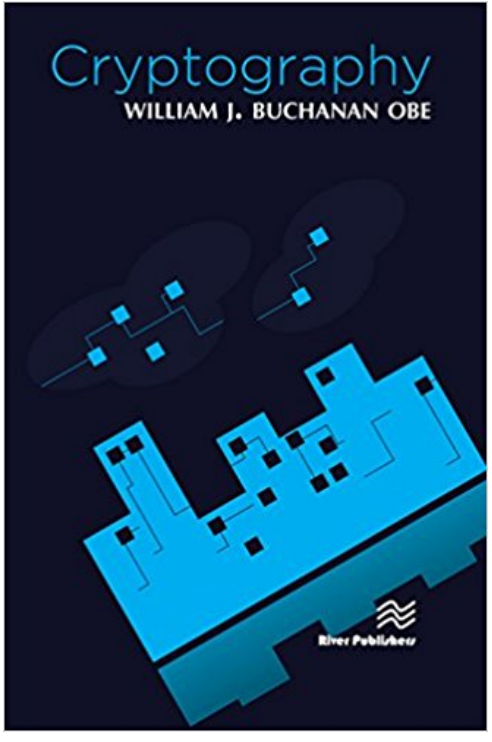
Bob sends his Digital certificate to authenticate himself

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

Author: Prof Bill Buchanan

Chapter 6: Digital Certificates

Introduction
Authentication Methods
PKI
Digital Certificate Passing

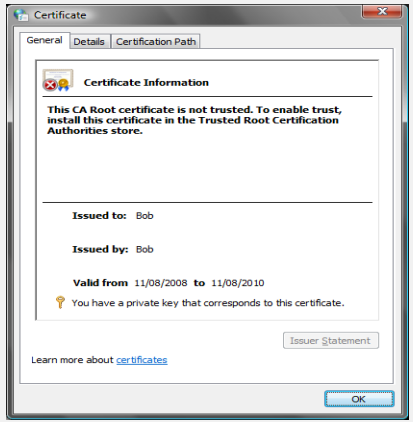


Prof Bill Buchanan OBE

http://asecuritysite.com/crypto06
http://asecuritysite.com/encryption

Digital Certificates

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



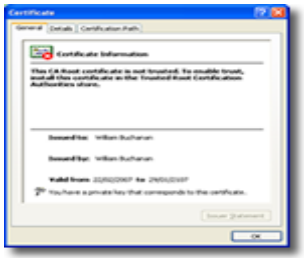
Who do we trust to get Bob's certificate … we can't trust Bob, as he may be Eve… meet Trent.

Who can we trust to get the digital certificate from?

Trusted Root CA

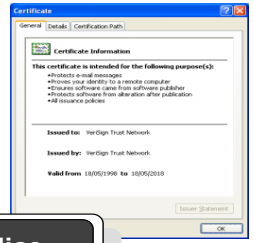
Certificate Authority (CA)
- Able to grant certificates
Examples; Verisign, Entrust, Microsoft Trust.

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



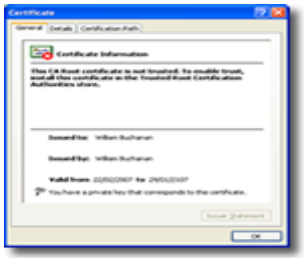
Alice checks the signature of the certificate to validate Bob. Both Alice and Bob trust the CA (Trent) as a third party.

Author: Prof Bill Buchanan

Trusted Root CA

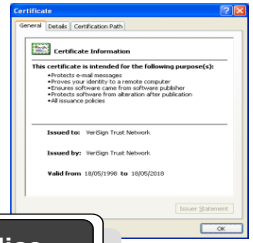
Certificate Authority (CA)
- Able to grant certificates
Examples; Verisign, Entrust, Microsoft Trust.

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



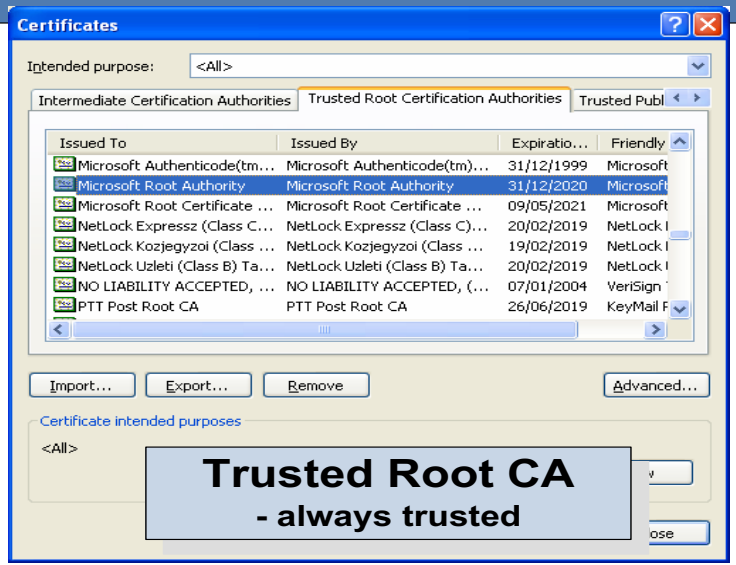
Trusted root certificates are installed as a default on the machine (or installed with the user's permission)

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.

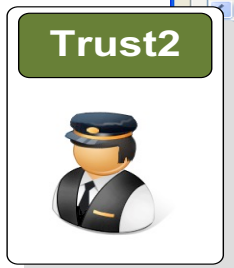
Author: Prof Bill Buchanan

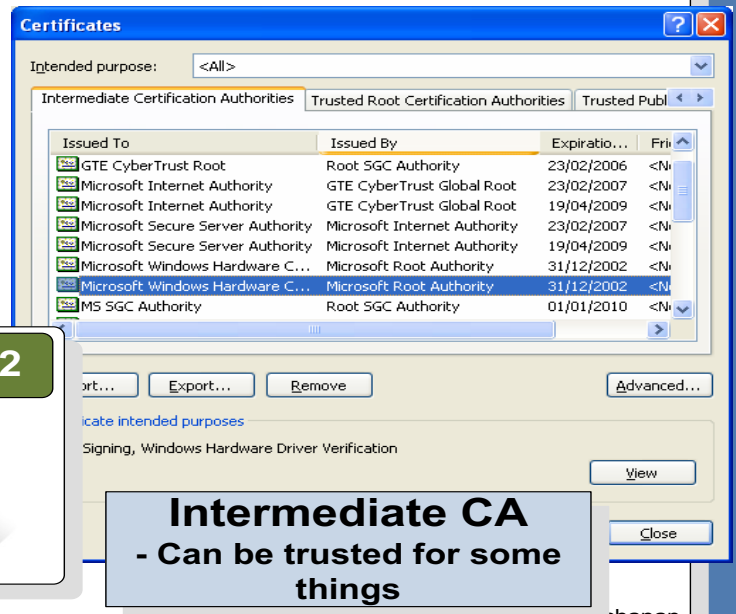


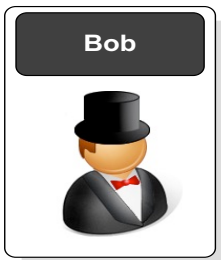
Trusted Root CA

Certificate purposes:

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





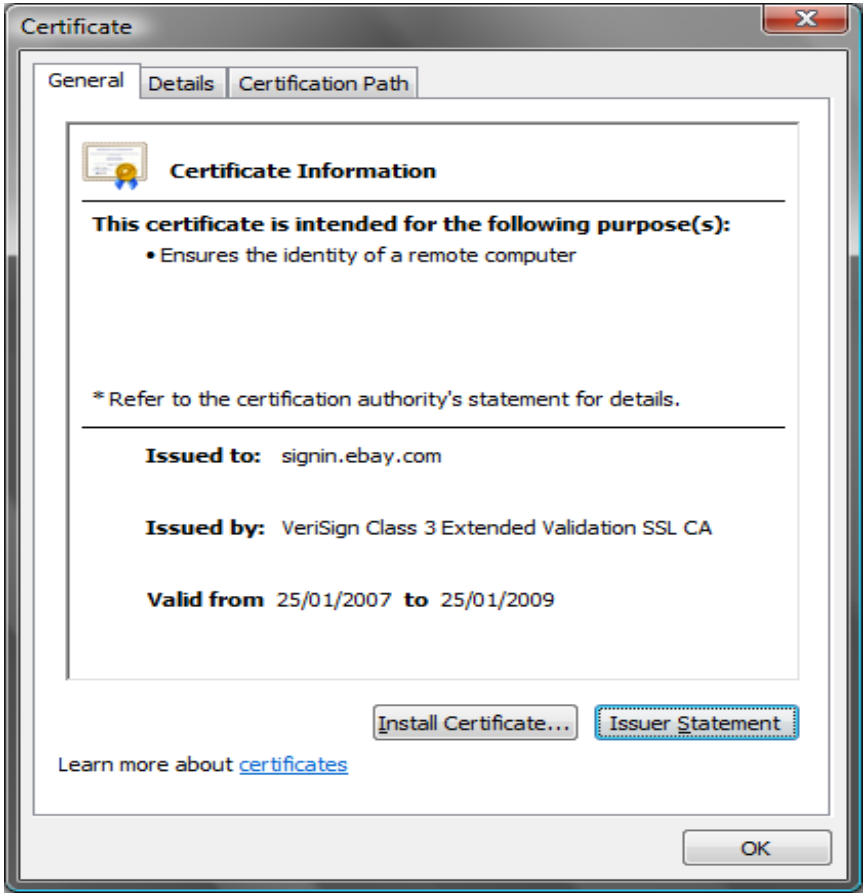


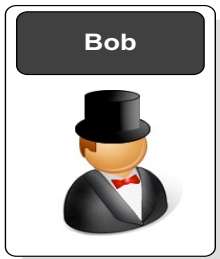
The two main problems with digital certificates are:

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

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

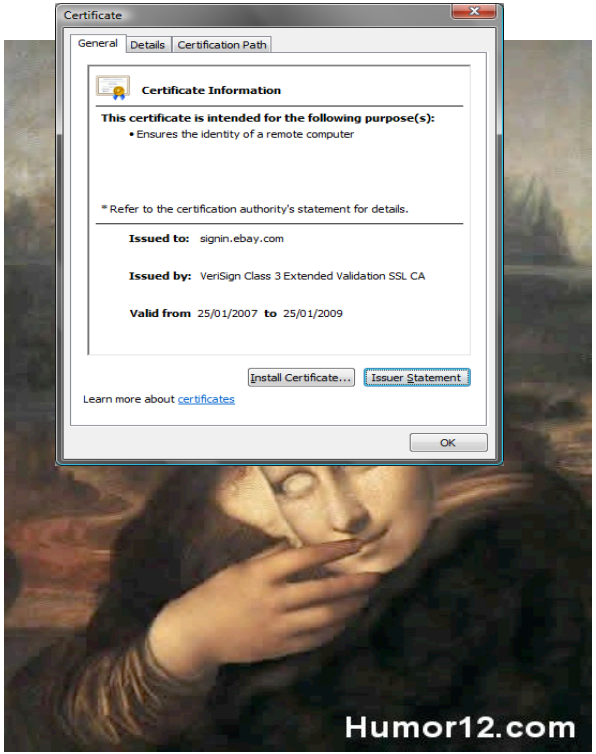
Author: Prof Bill Buchanan

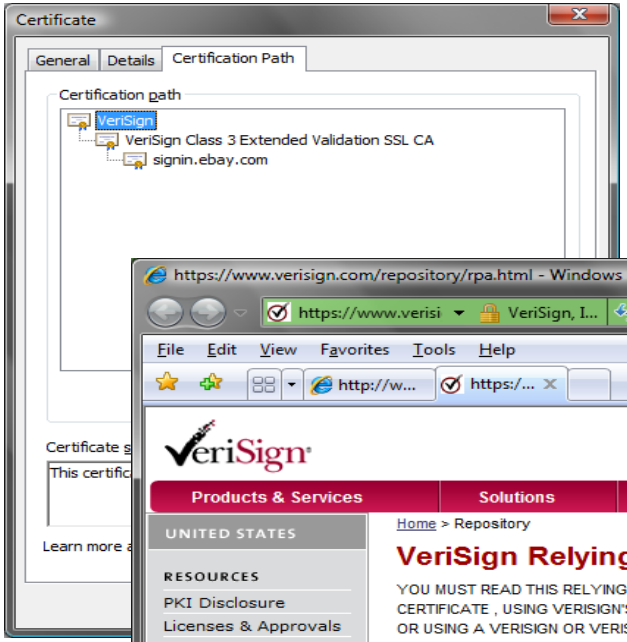




Real or fake?

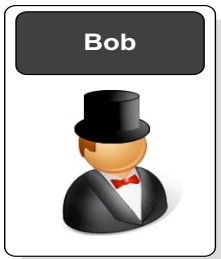
Author: Prof Bill Buchanan

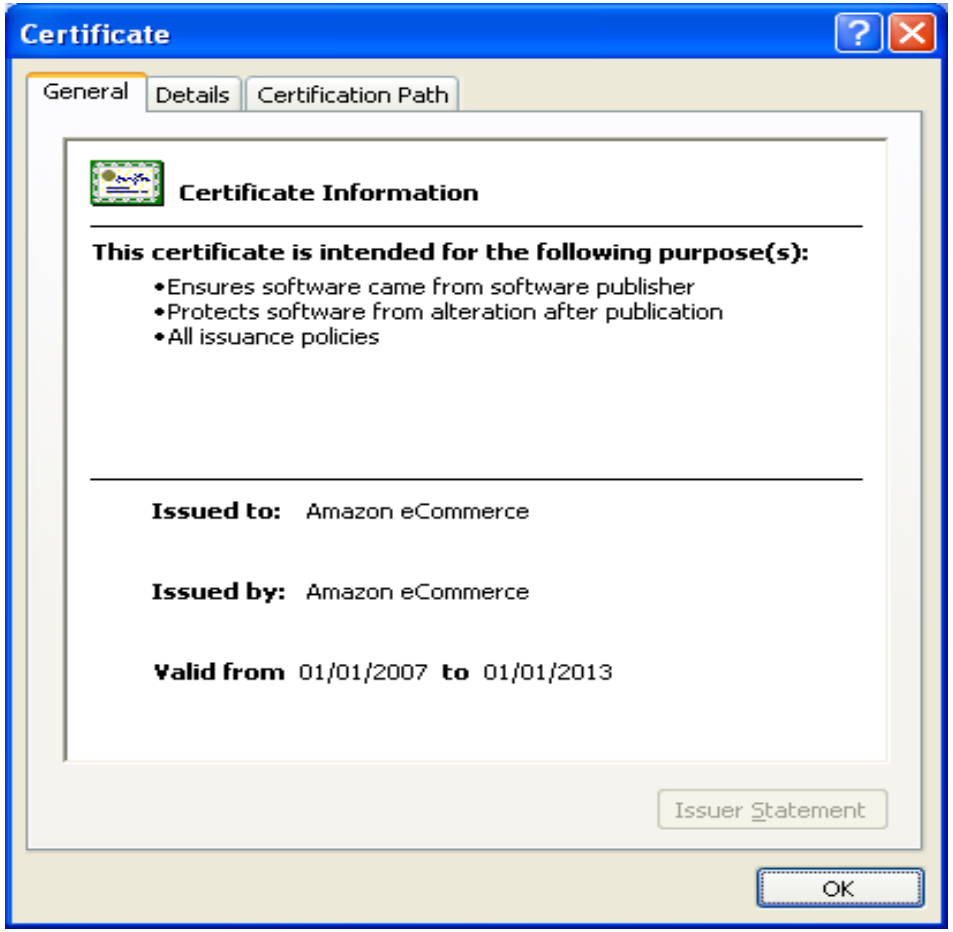




Real!

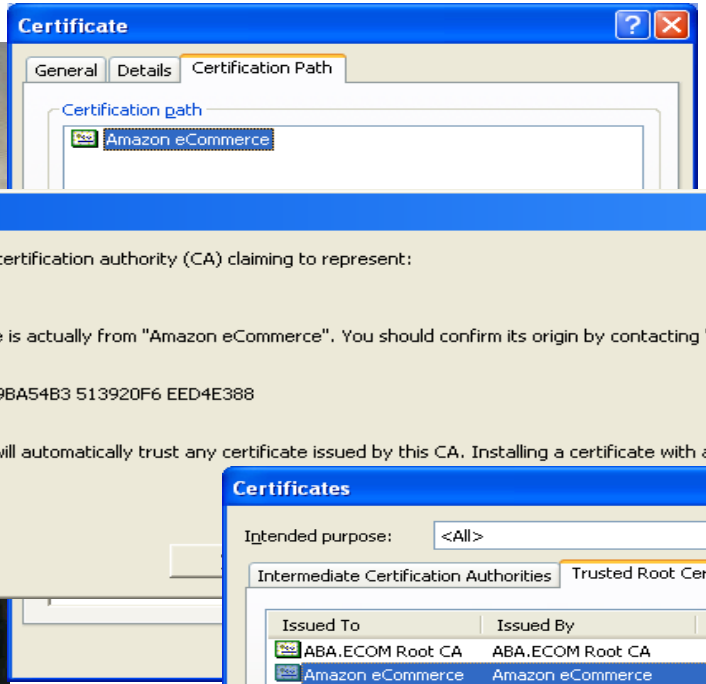
Author: Prof Bill Buchanan

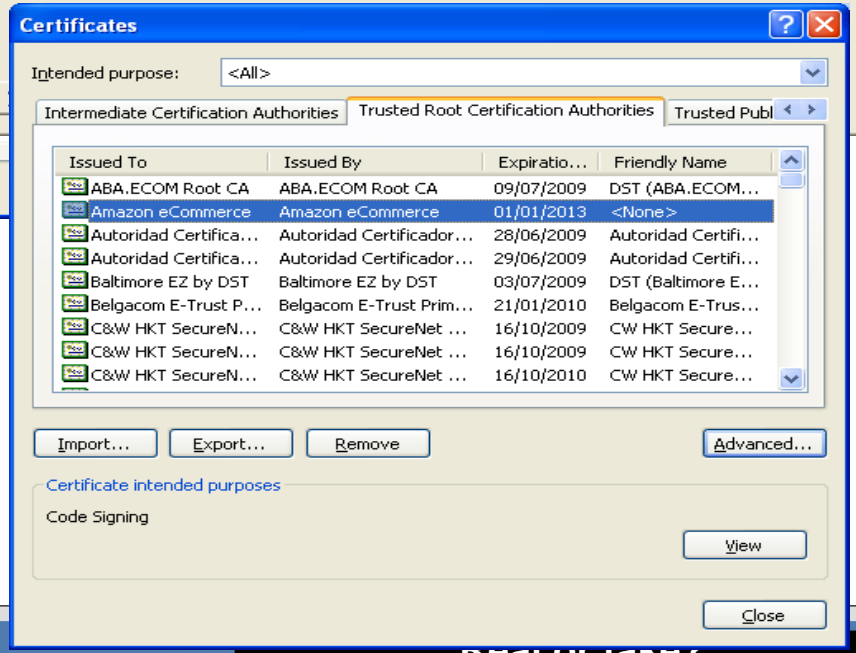




Real or fake?

Author: Prof Bill Buchanan



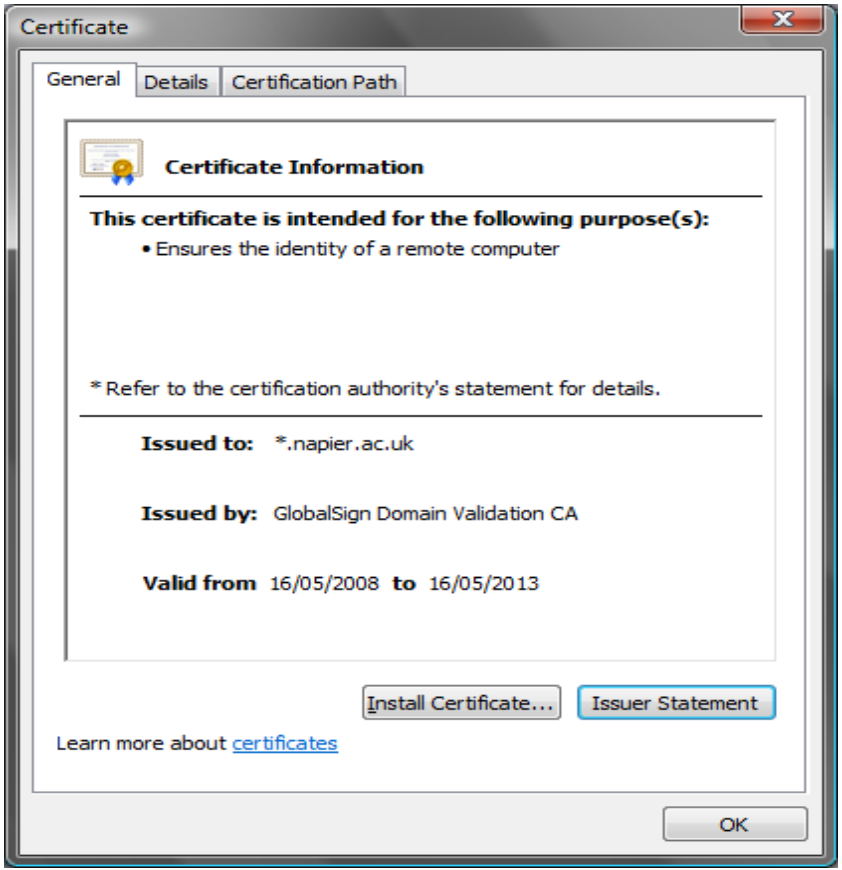


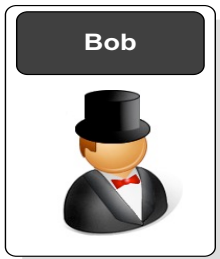
Fake!

PKI

Authentication

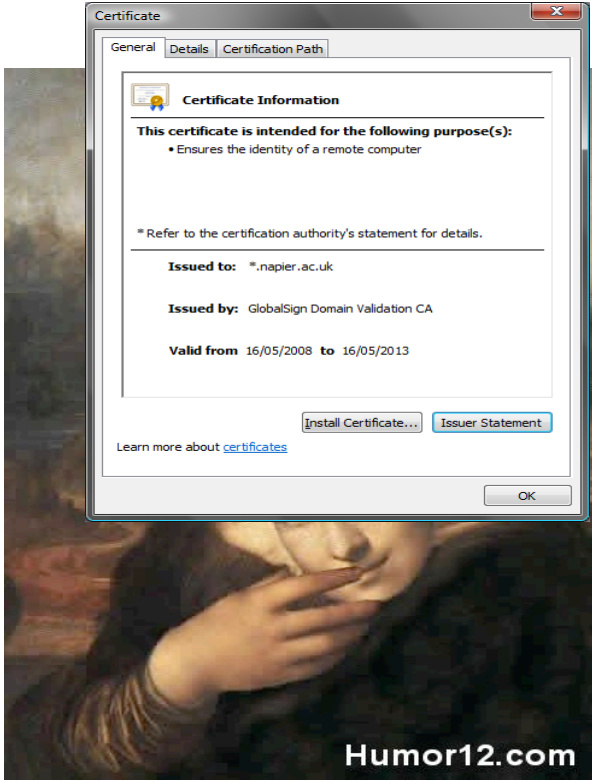
Real or Fake?

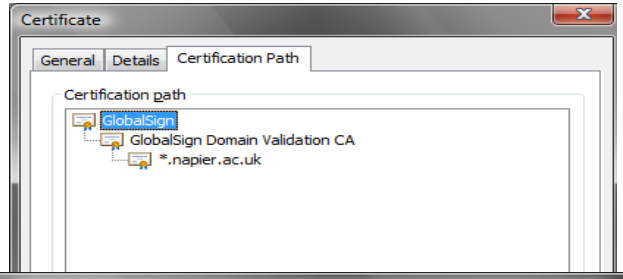




Real or fake?

Author: Prof Bill Buchanan



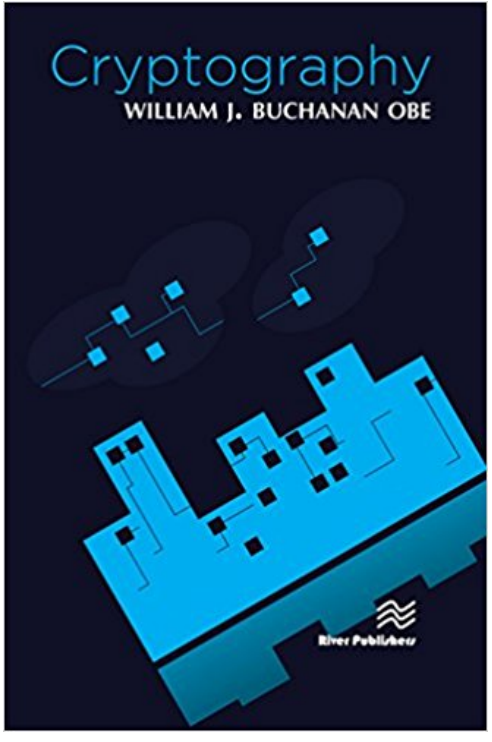


Real

Author: Prof Bill Buchanan

Chapter 6: Digital Certificates

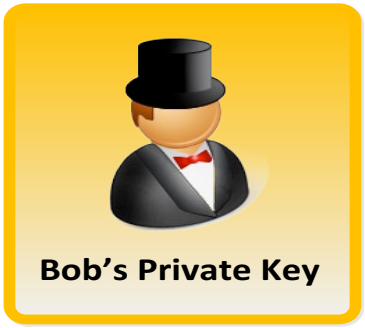
Introduction
Authentication Methods
PKI
Digital Certificate Passing

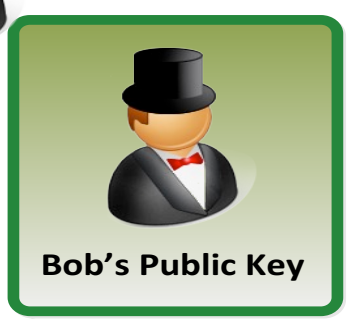


Prof Bill Buchanan OBE

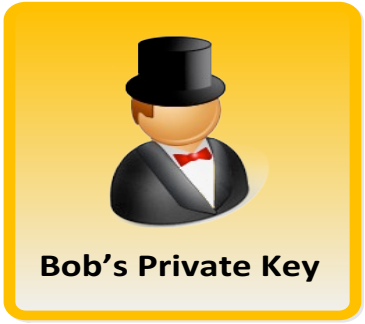
http://asecuritysite.com/crypto06
http://asecuritysite.com/encryption

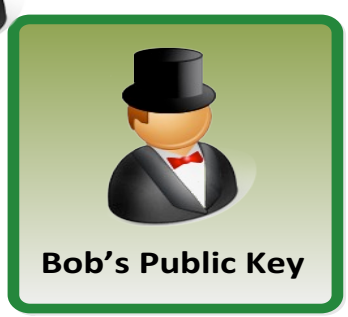
Public key encryption … secret … identity … trust





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

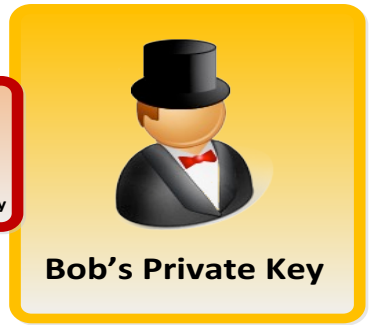
Alice's Public Key

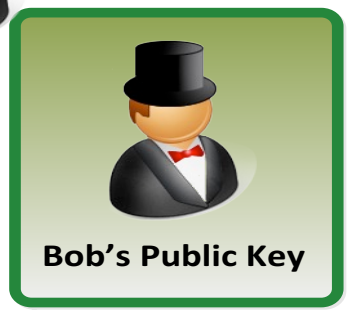
Bob's Public Key

Alice's Public Key

Alice's Private Key

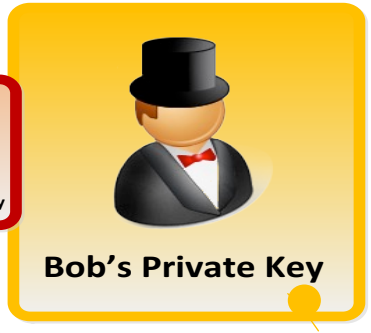
Public key encryption … secret … identity … trust



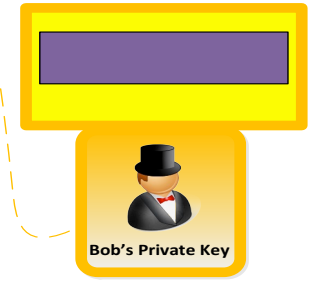


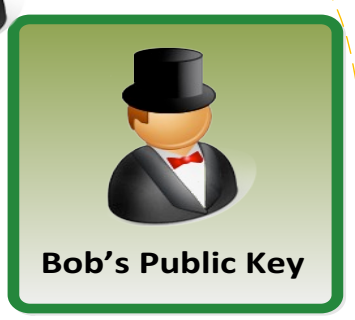
Hello Alice,
Wish you were here!
- Bob

Public key encryption … secret … identity … trust

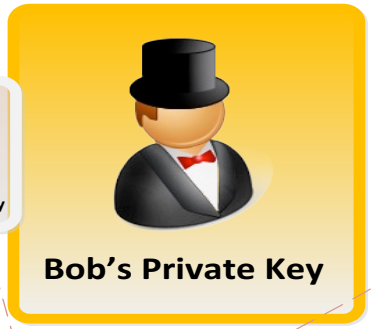


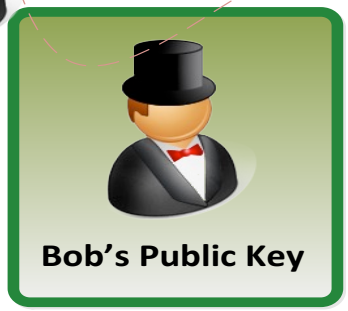
Hello Alice,
Wish you were here!
- Bob



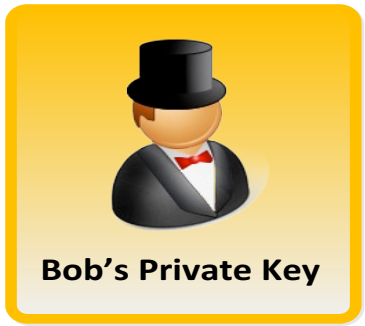


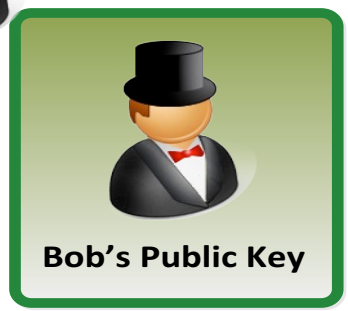
Public key encryption … secret … identity … trust





Public key encryption … secret … identity … trust





Which key to open the message?

Public key encryption … secret … identity … trust

Eve

Trent

MegaCorp

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 Private Key

Alice's Public Key

Verified by MegaMegaCorp

Bob's Private Key

Alice's Private Key

Hello Alice,
Wish you were here!
- Bob

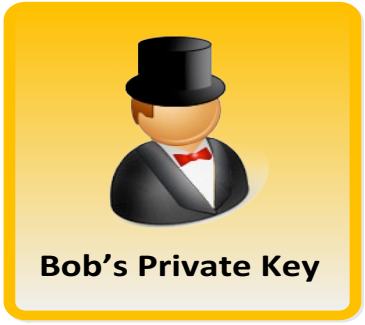
Alice's Public Key

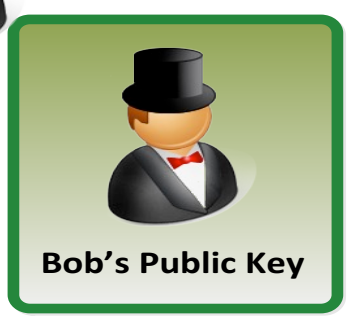
Bob's Public Key

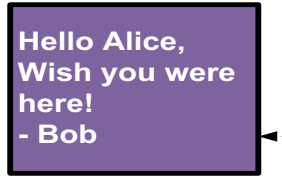
Which key to open the message?

Alice's Private Key

Public key encryption … secret … identity … trust

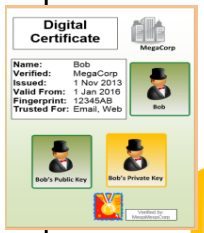


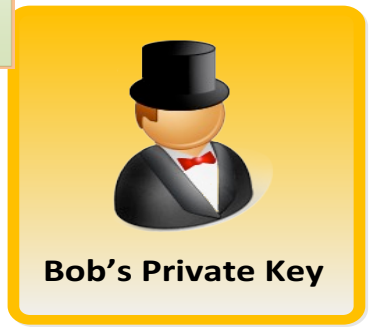


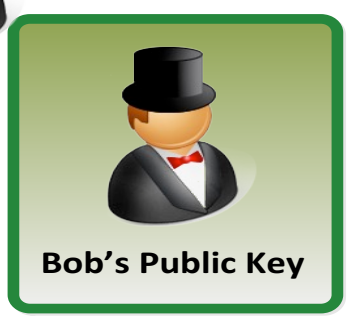


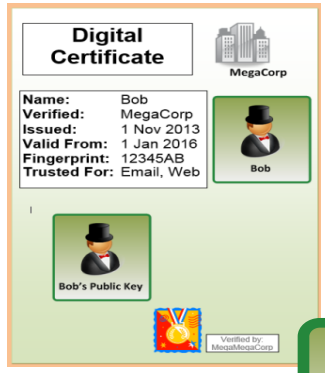
Which key to we open the signature with?

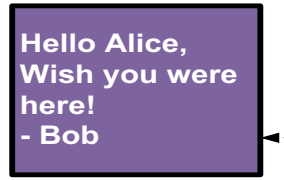
Public key encryption … secret … identity … trust



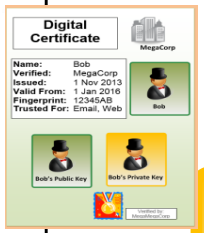


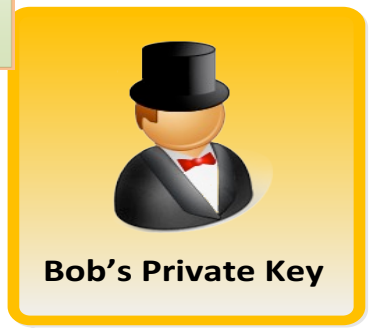


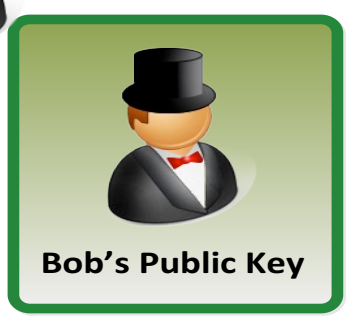


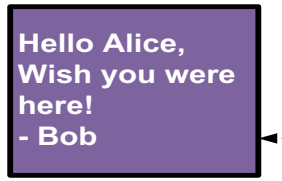


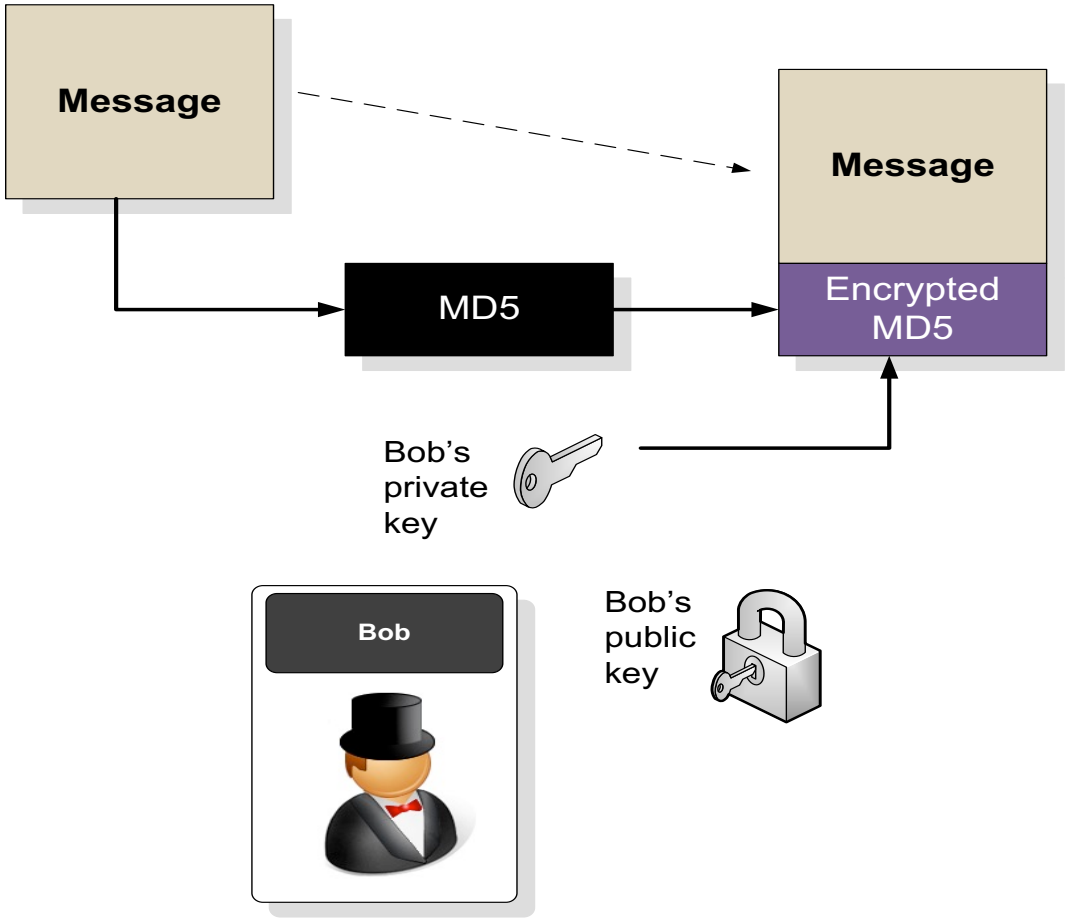
Public key encryption … secret … identity … trust



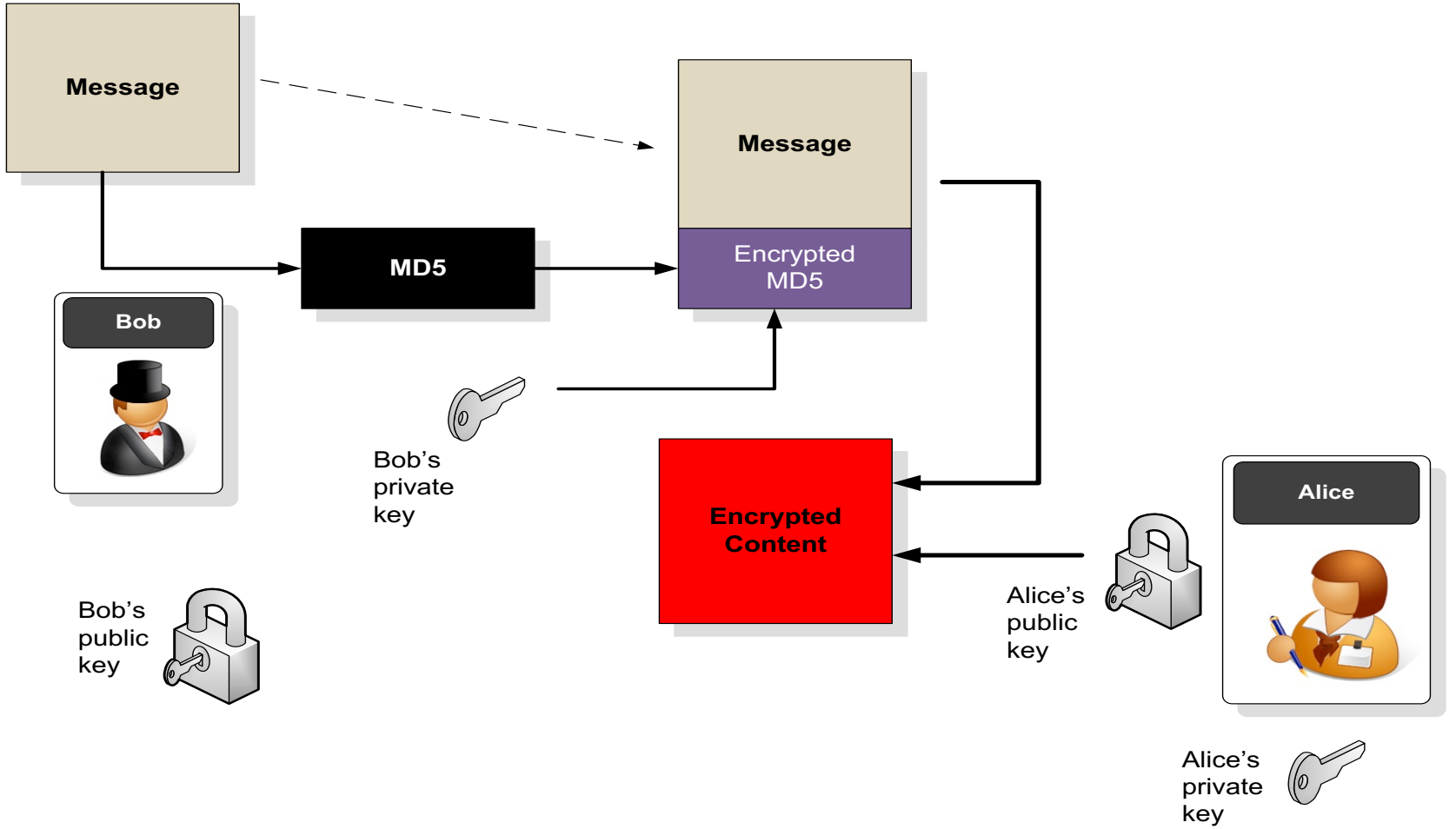






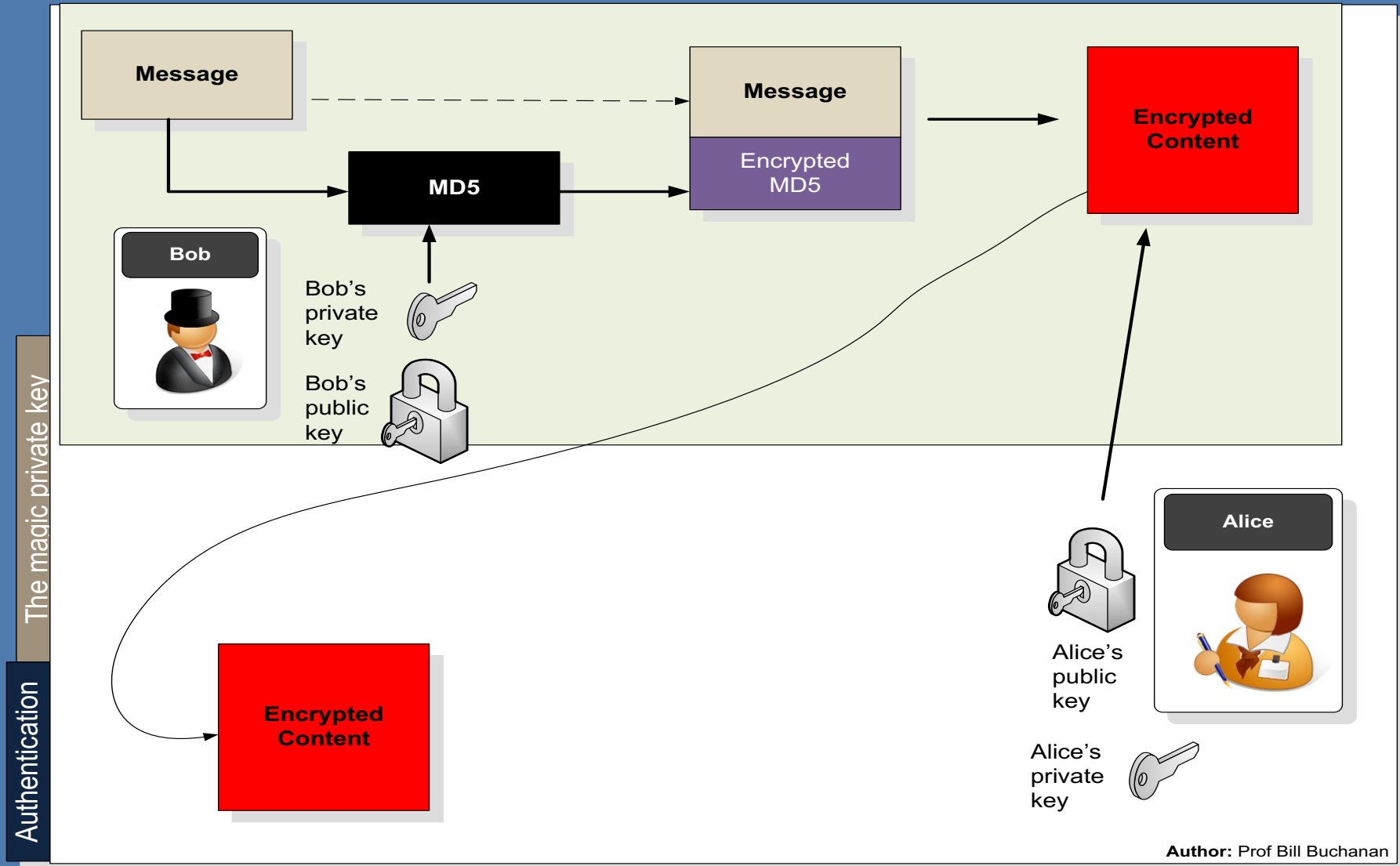


Author: Prof Bill Buchanan

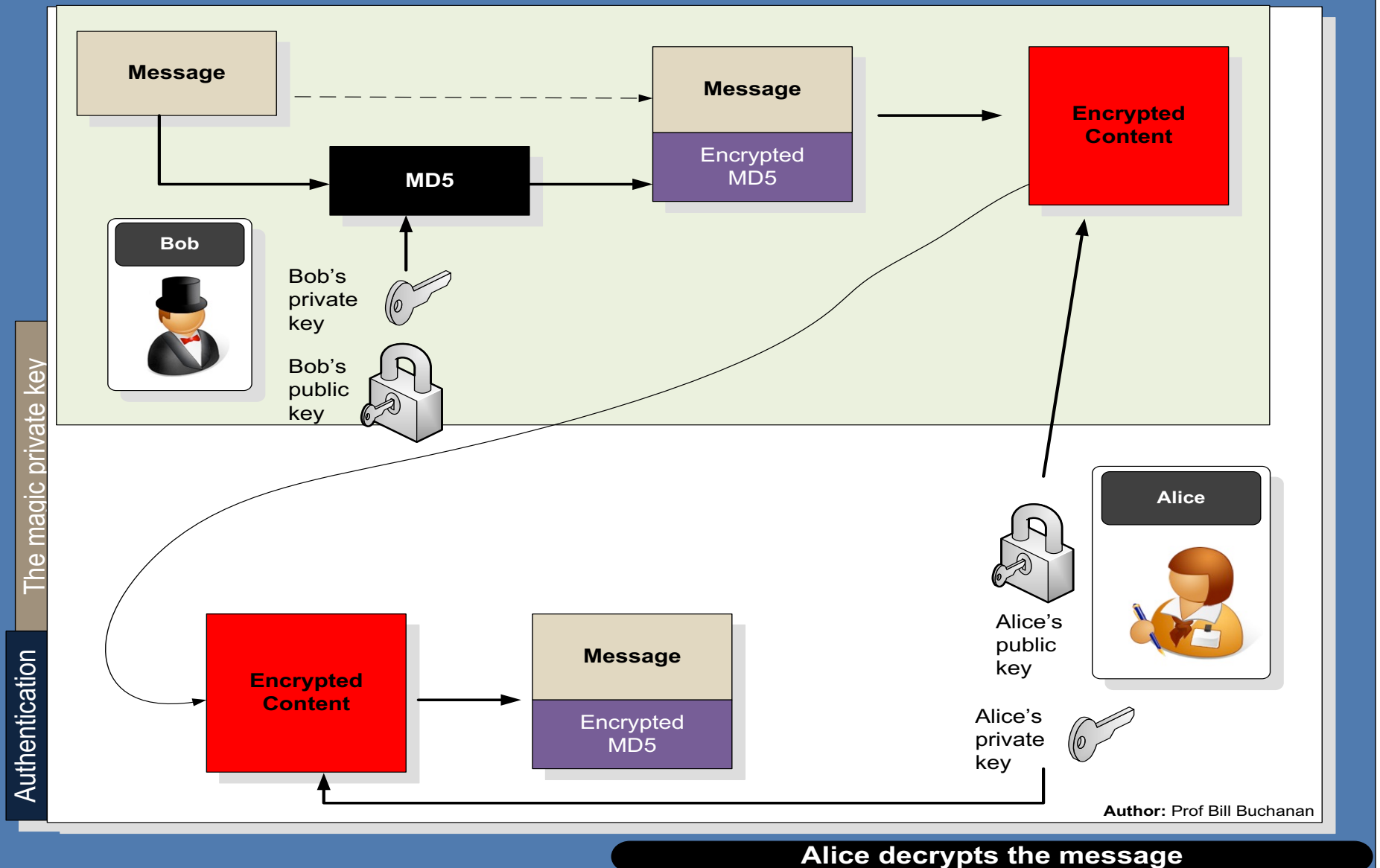


Author: Prof Bill Buchanan

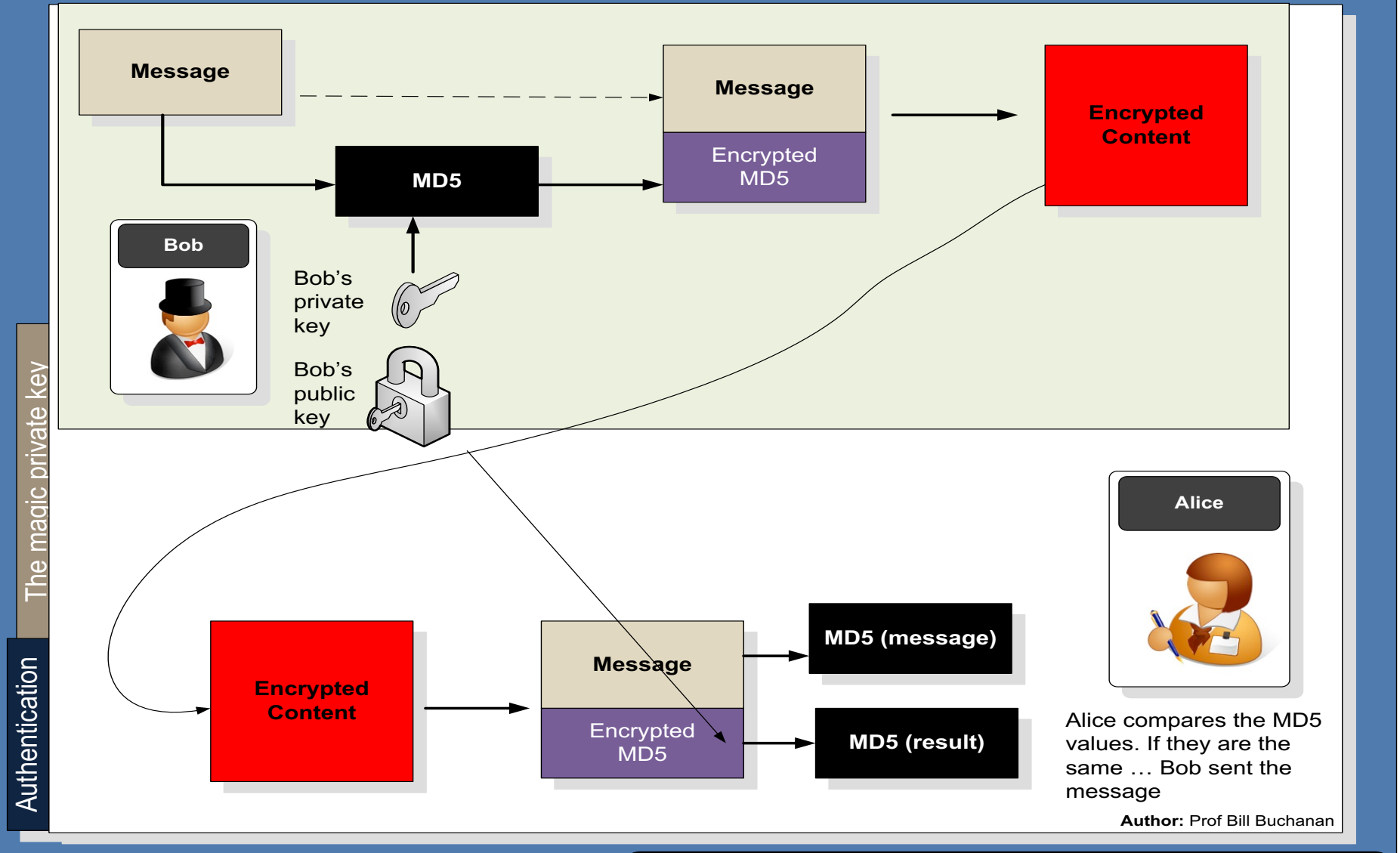
Bob encrypts the message/hash with Alice's public key



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



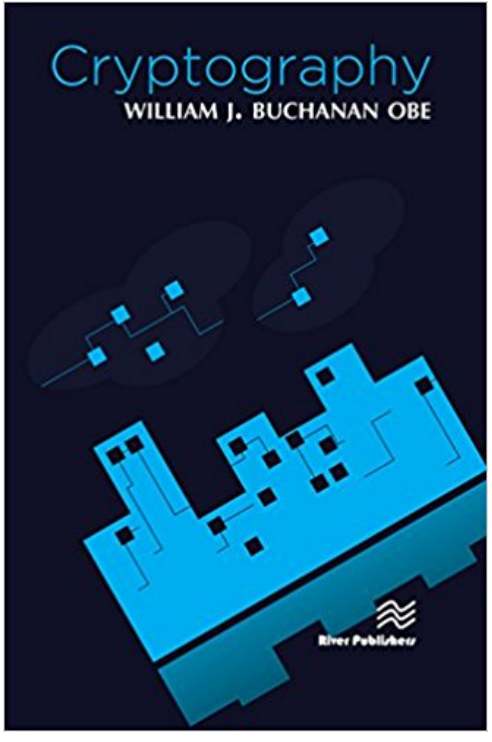
Alice decrypts the message



Alice decrypts the message

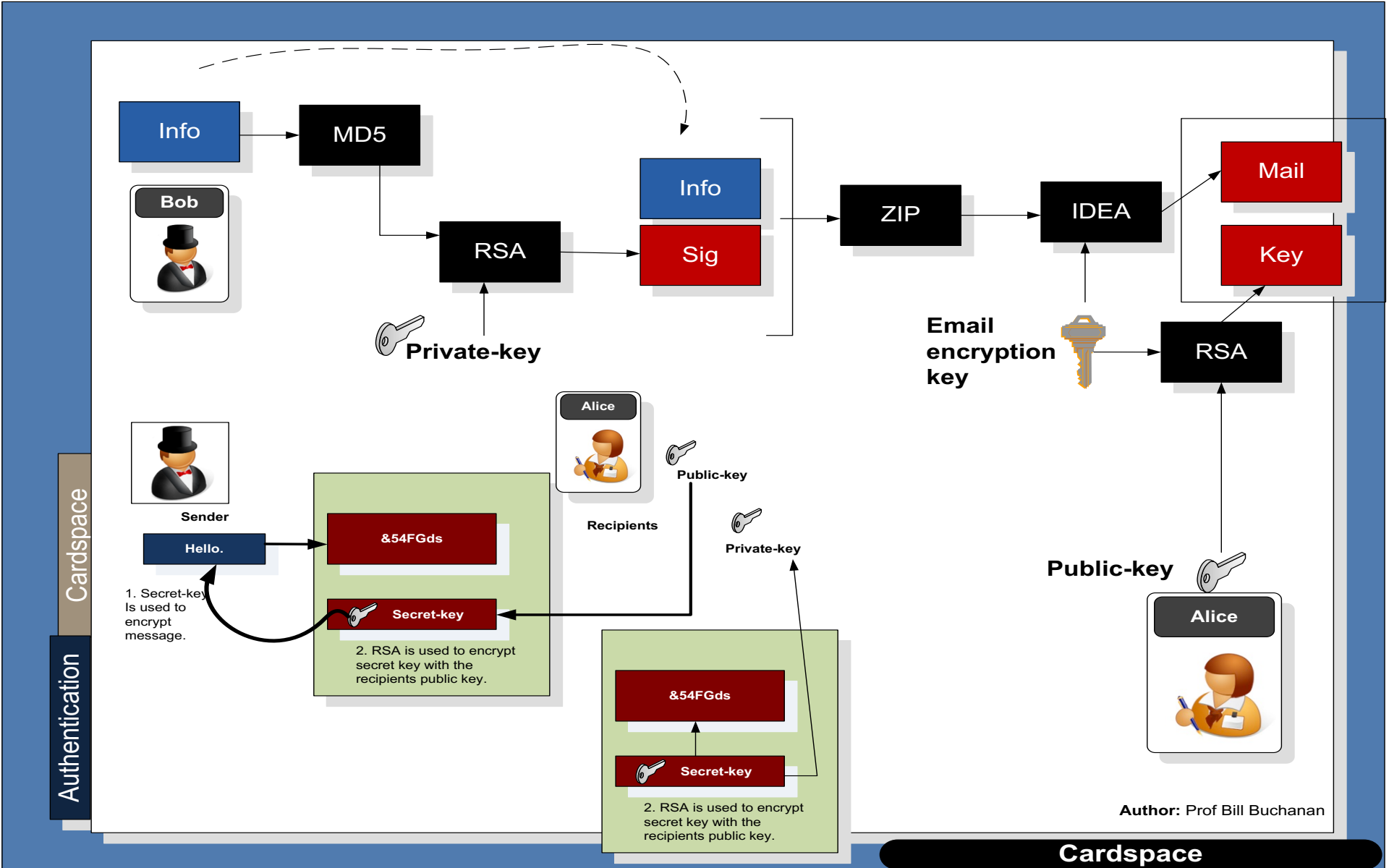
Chapter 6: Digital Certificates

Introduction
Authentication Methods
PKI
Digital Certificate Passing



Prof Bill Buchanan OBE

http://asecuritysite.com/crypto06
http://asecuritysite.com/encryption


Info
MD5
Bob
RSA
Private-key
Info
Sig
ZIP
IDEA
Mail
Key
Email encryption key
RSA
Public-key
Alice
Sender
Hello.
1. Secret-key Is used to encrypt message.
&54FGds
Secret-key
2. RSA is used to encrypt secret key with the recipients public key.
Alice
Recipients
Public-key
Private-key
&54FGds
Secret-key
2. RSA is used to encrypt secret key with the recipients public key.
Public-key
Alice
Author: Prof Bill Buchanan
Cardspace
Authentication
Cardspace