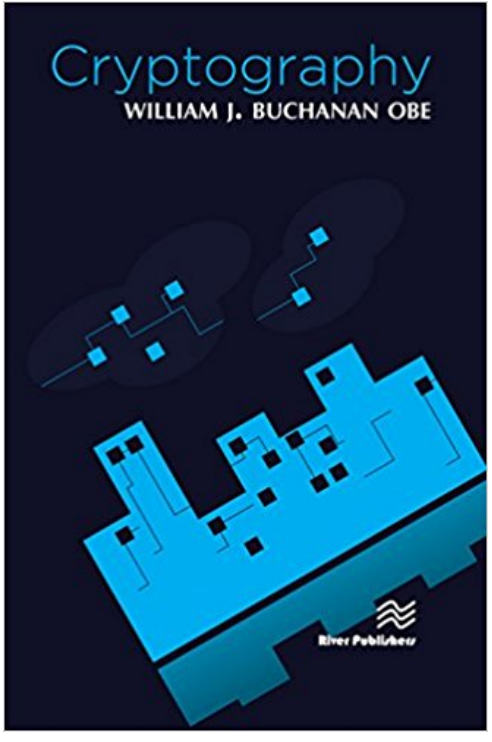
Chapter 6: Digital Certificates

Introduction
Authentication Methods
PKI
Digital Certificate Passing

Prof Bill Buchanan OBE

http://asecuritysite.com/esecurity/unit06

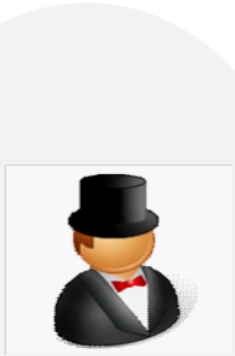
http://asecuritysite.com/encryption



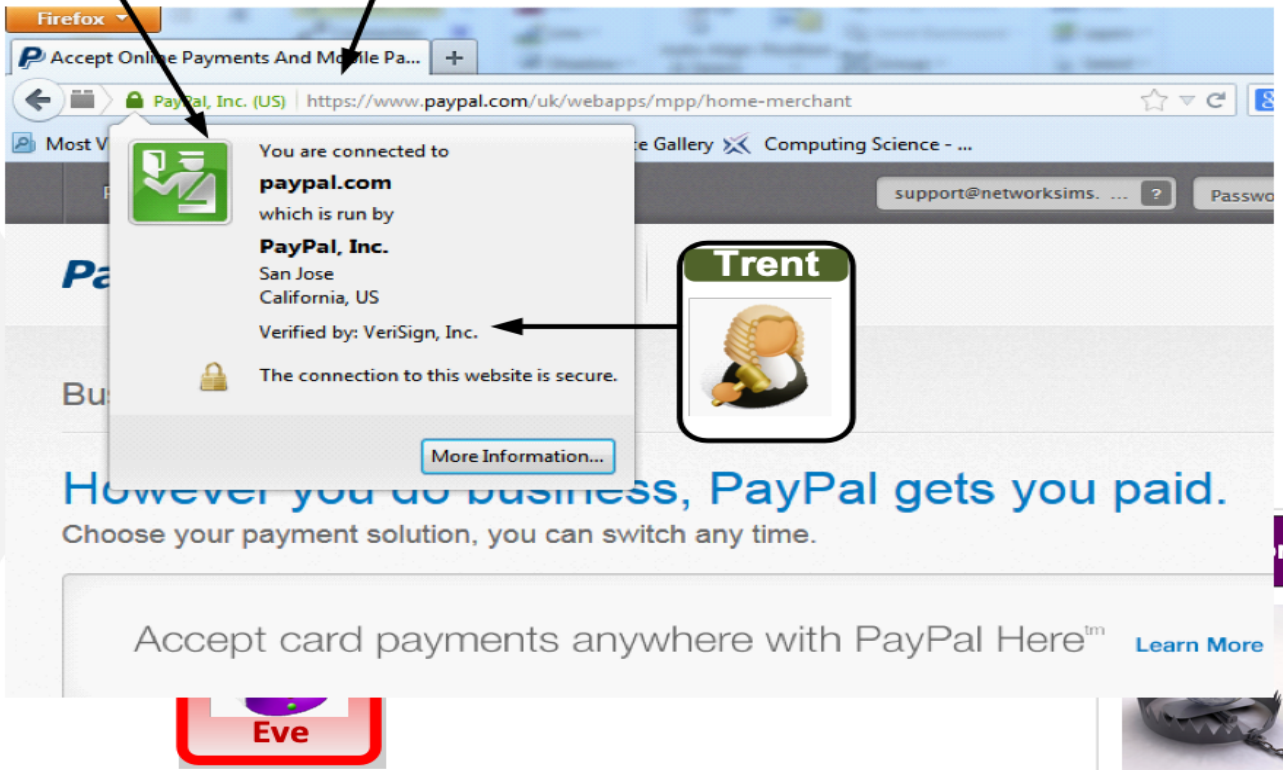
Identity on the Internet

Identifies it is trusted (Digital Certificate)

Keeps communications secure (encryption)



Bob



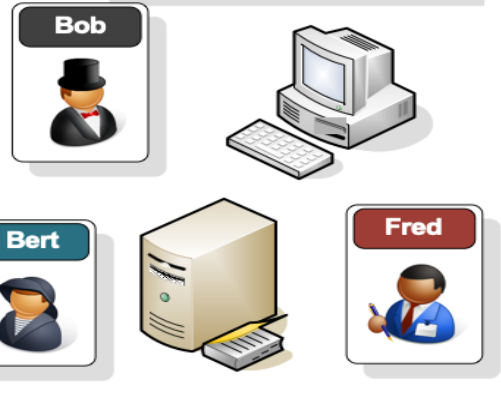
Fundamental principles

Authentication.
Confidence/Assurance.
Privacy/Confidentiality.

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

Confidentiality
(Encryption)

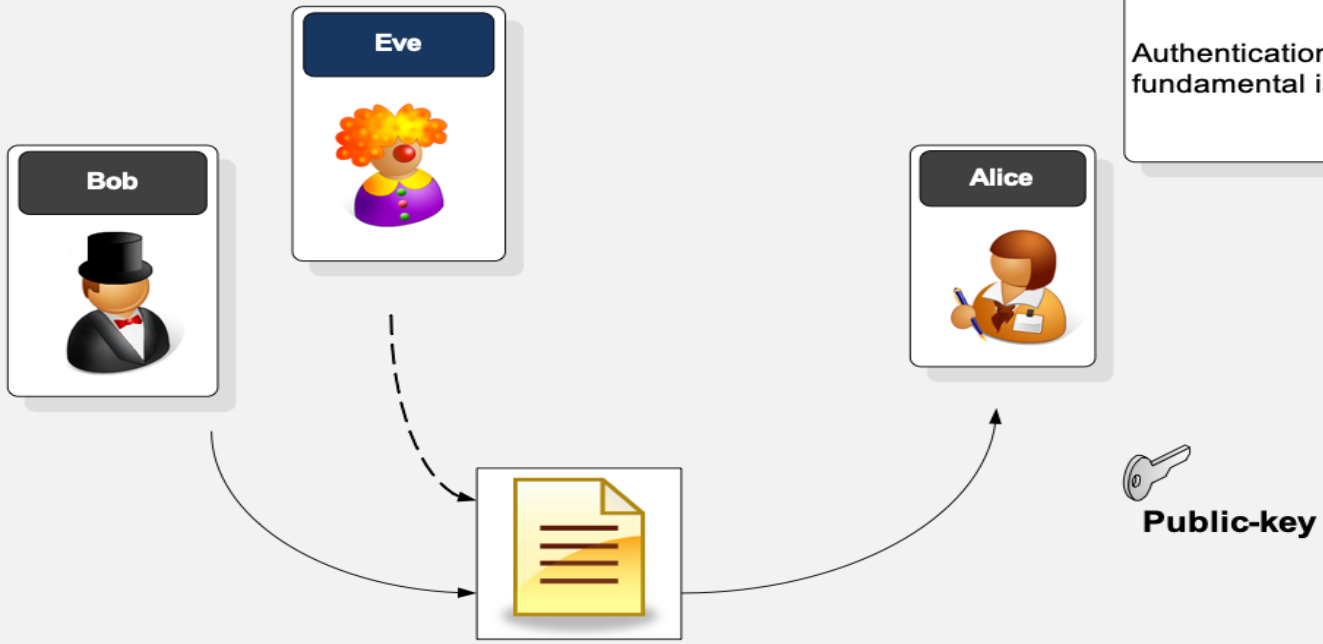
Assurance
(Integrity)



Author: Prof Bill Buchanan

Authentication

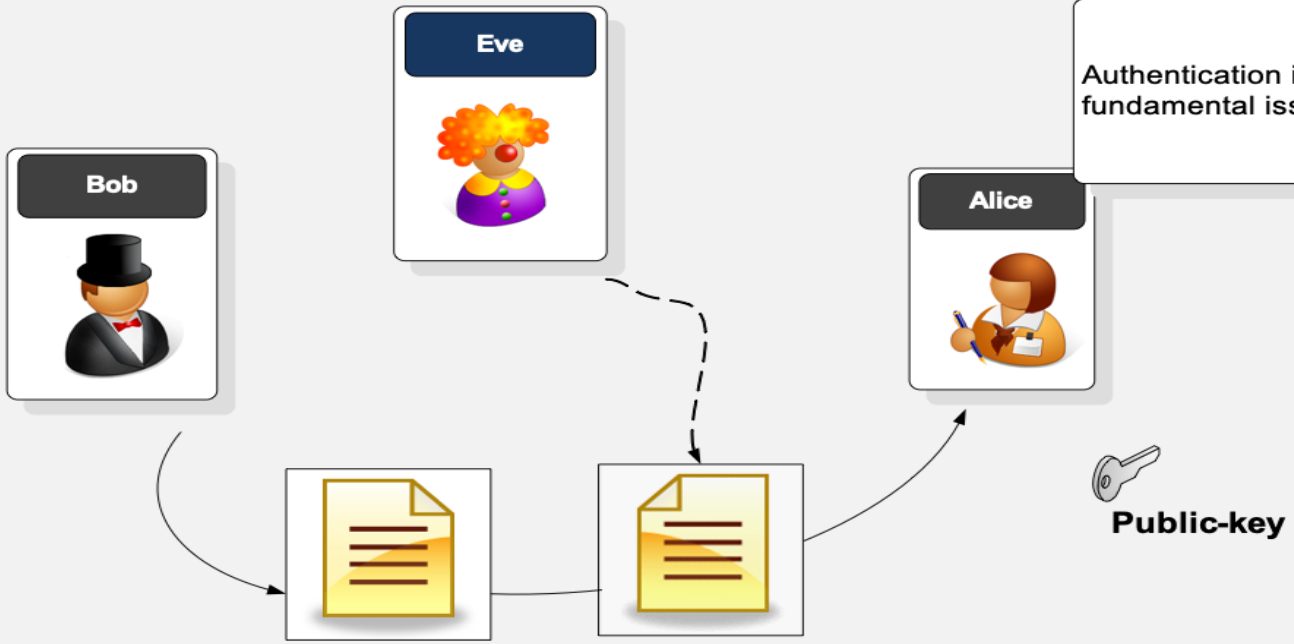
Authentication is a fundamental issue in security.



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.

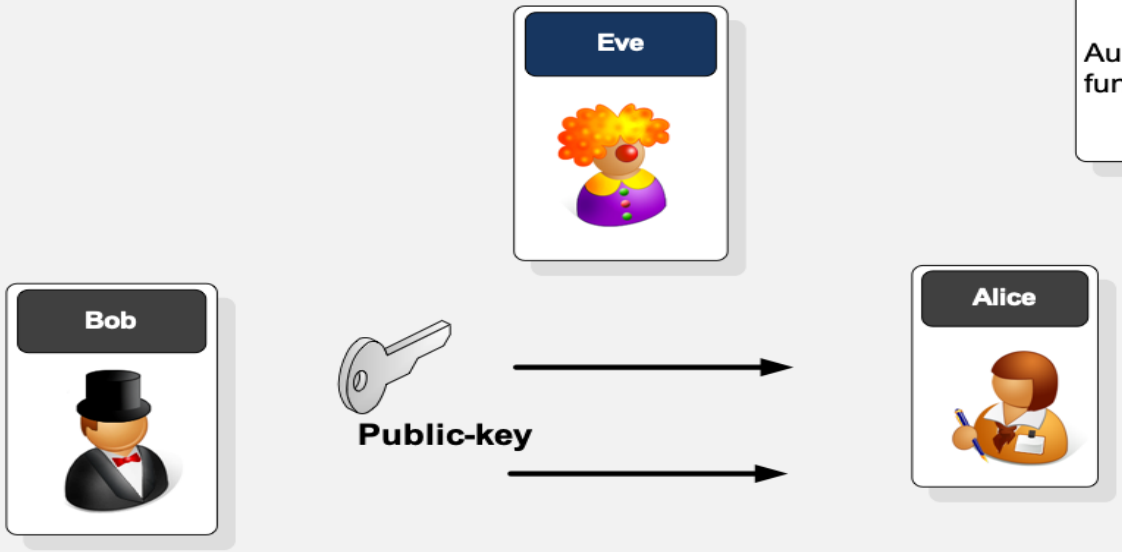


How can we tell that the message has not been tampered with ?

Author: Prof Bill Buchanan

Authentication

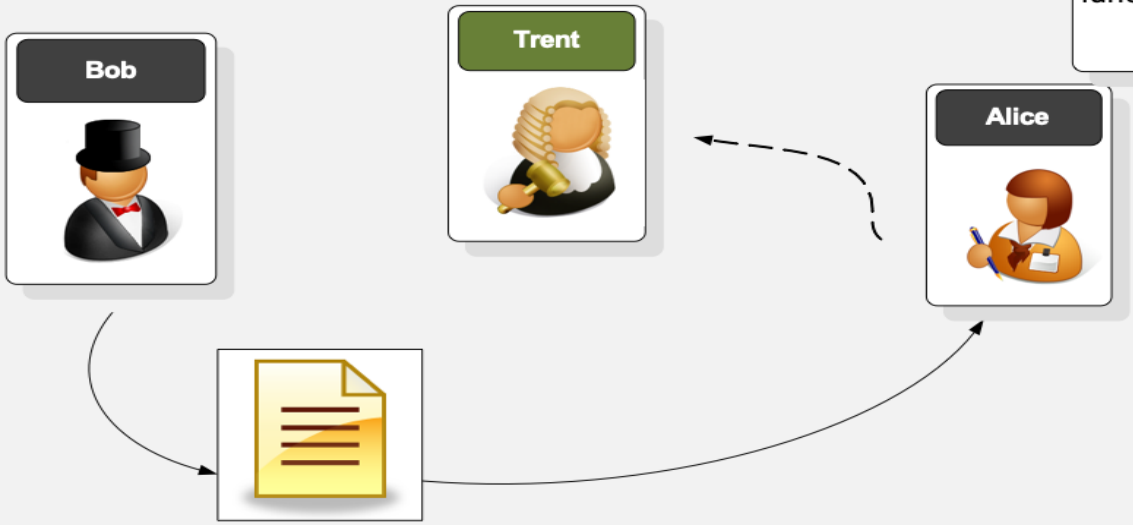
Authentication is a fundamental issue in security.



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

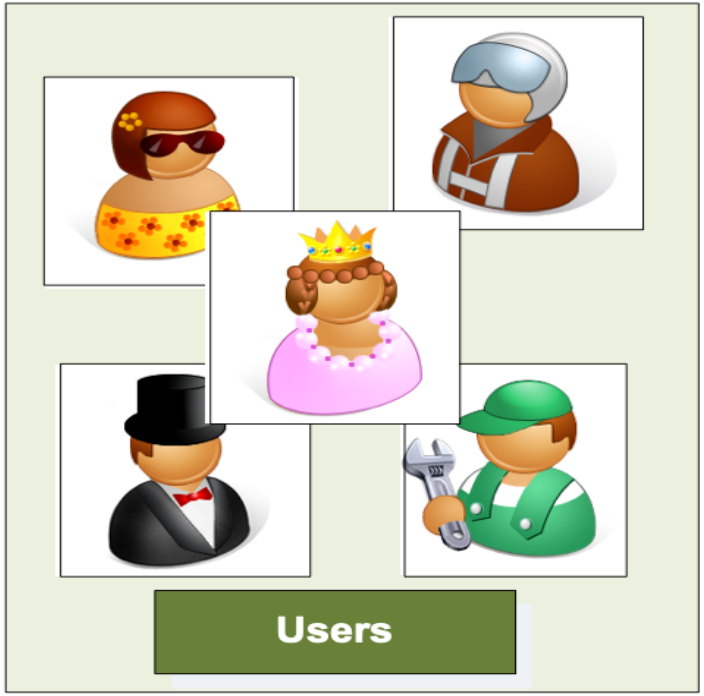
Chapter 6: Digital Certificates

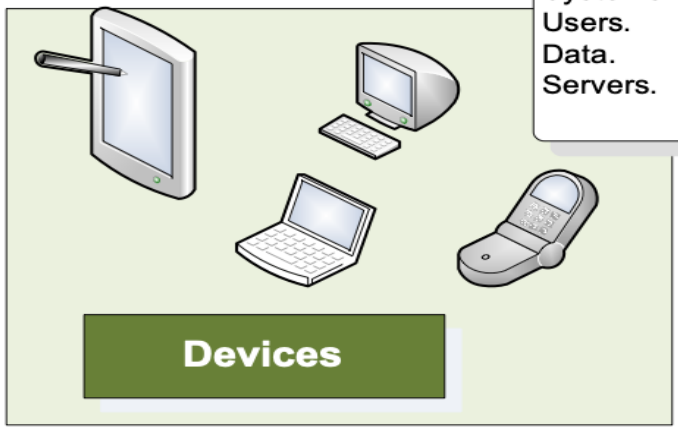
Introduction
Authentication Methods

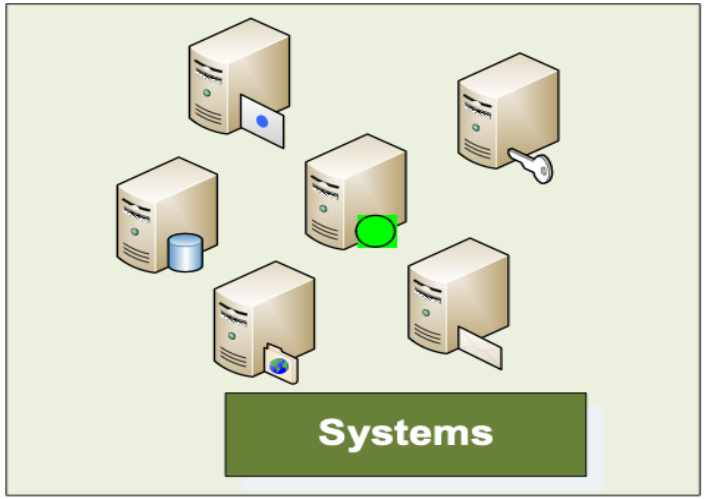
Prof Bill Buchanan OBE
http://asecuritysite.com/crypto06

What to authenticate?

Systems.
Users.
Data.
Servers.



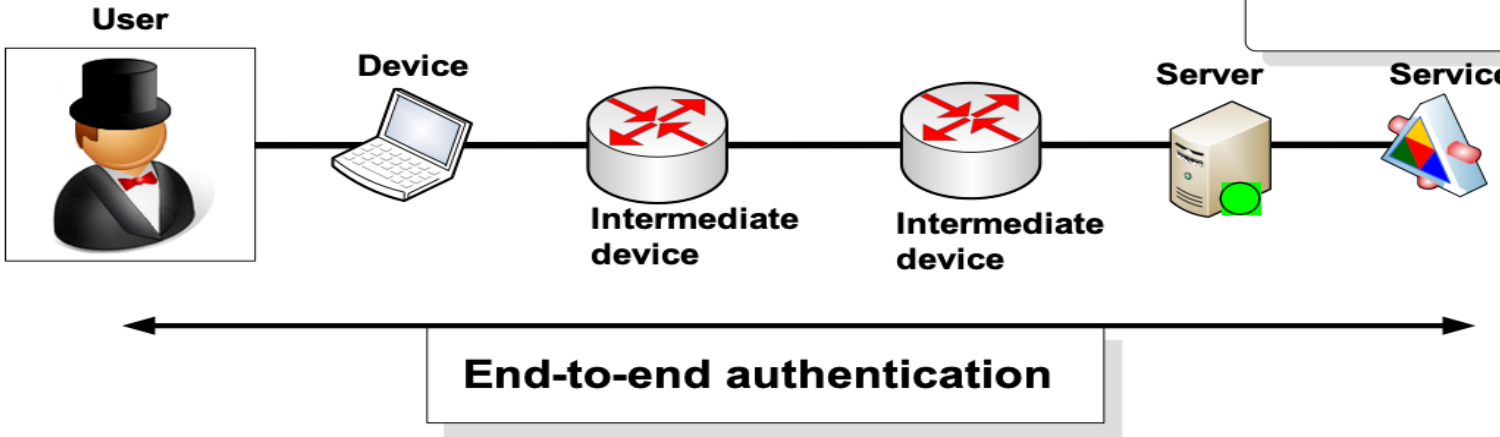


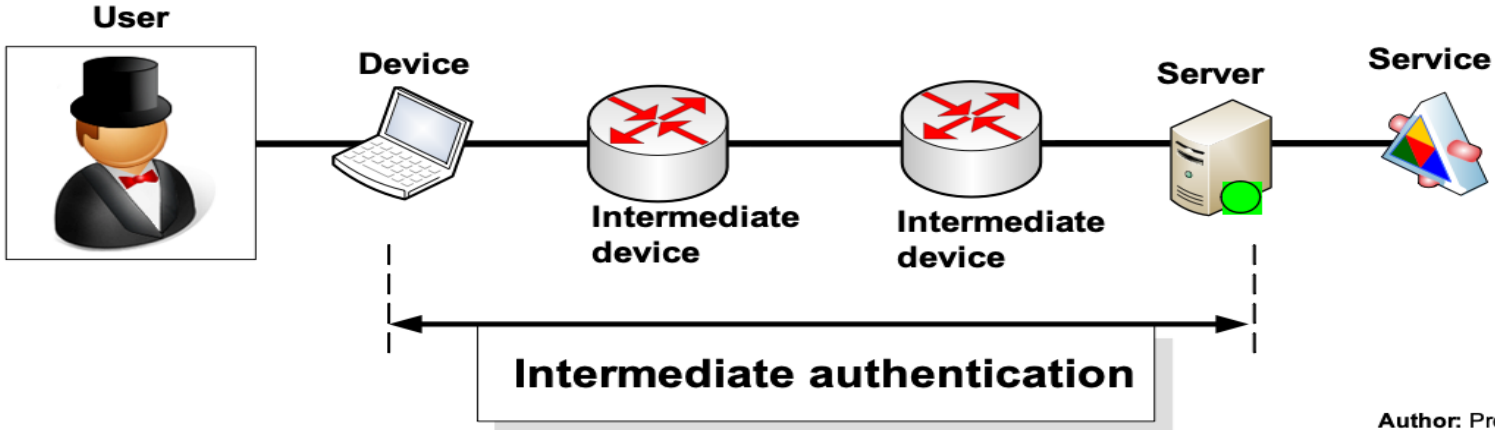


Author: Prof Bill Buchanan

Where authenticated?

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





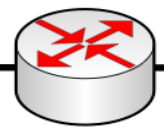
Author: Prof Bill Buchanan

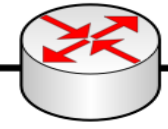
Authentication type

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

User

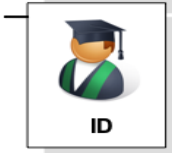
Device





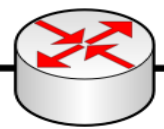
Server

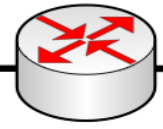
One-way server authentication. Server provides authentication to the client, such as SSL (HTTPS, FTPS, etc).

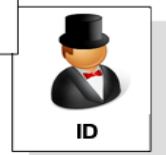


User

Device

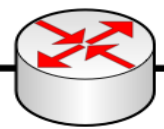


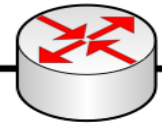




One-way client authentication. Client provides authentication to the server such as EAP-TLS in Wireless.

User





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

Author: Prof Bill Buchanan

Authentication

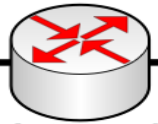
Authentication type

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

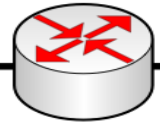
User

Device

Intermediate device



Intermediate device

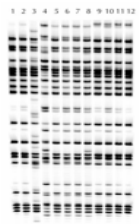


Server

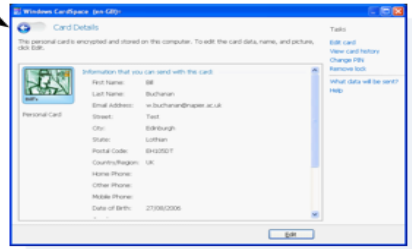
Service

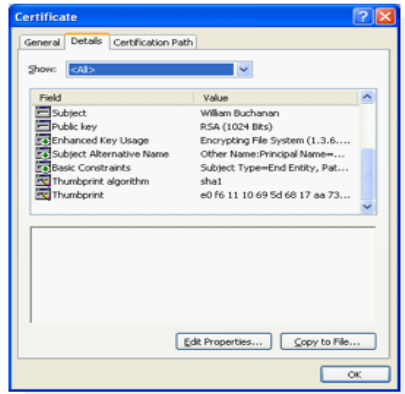
Methods

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



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





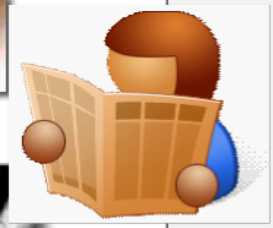
Author: Prof Bill Buchanan

Authentication methods

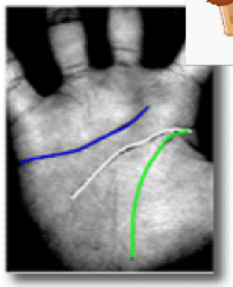
Something you have
Something you know
Something you are

Authentication Methods

Iris scans



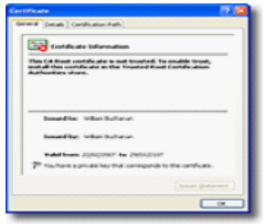
Retina scan



Palm prints

Finger prints

Something you are

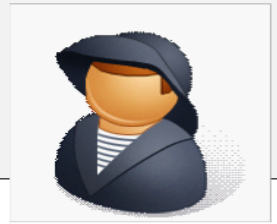


Digital certificate

Network/physical address

Smart card

Something you have



Username/ password

Mother's maiden name

Something you know

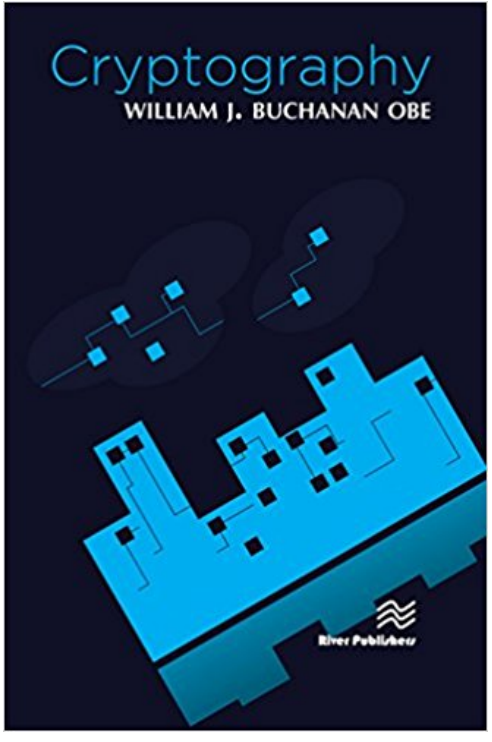
Author: Prof Bill Buchanan

Chapter 6: Digital Certificates

Introduction
Authentication Methods
PKI
Digital Certificate Passing

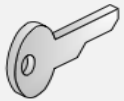
Prof Bill Buchanan OBE

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



Digital Certificates

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

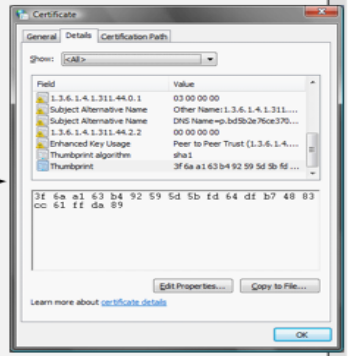


Public-key

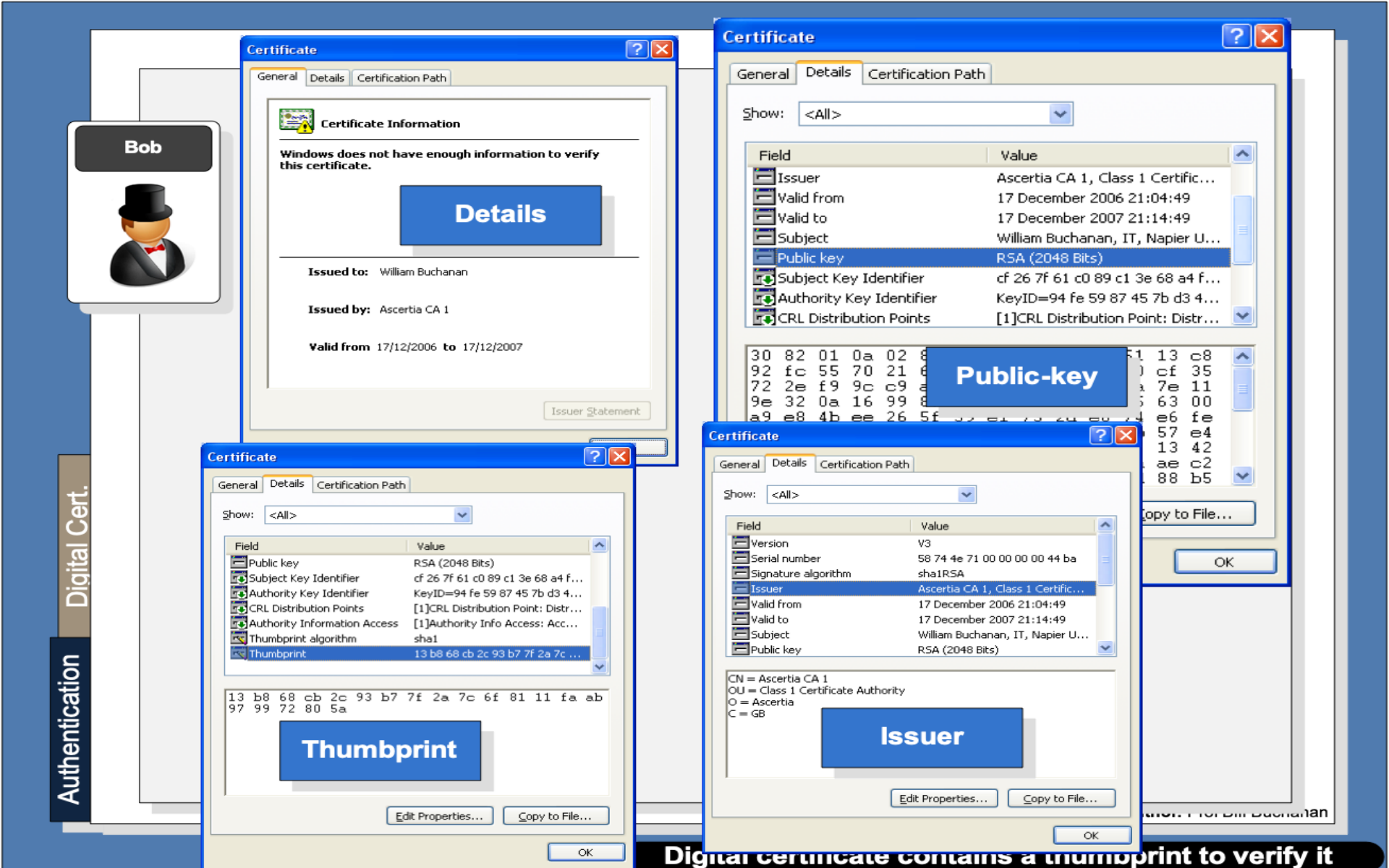
One method is the digital certificate which can carry the public key (and also the private key, if nesc.)

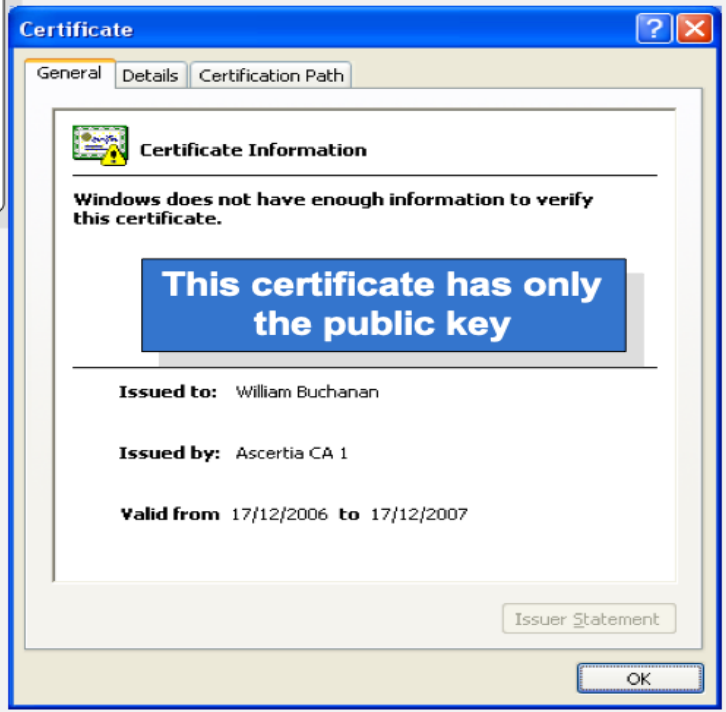
Now that we need the public key to either encrypt data for a receipiant, or to authenticate a sender...

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...
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

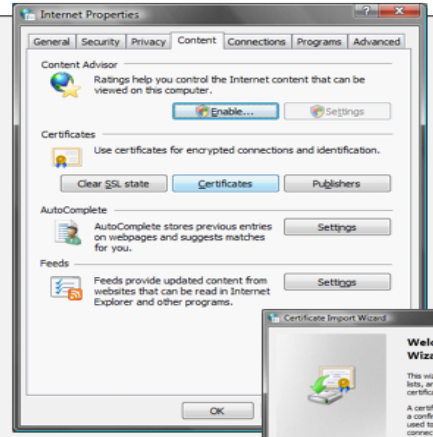
Digital Cert.

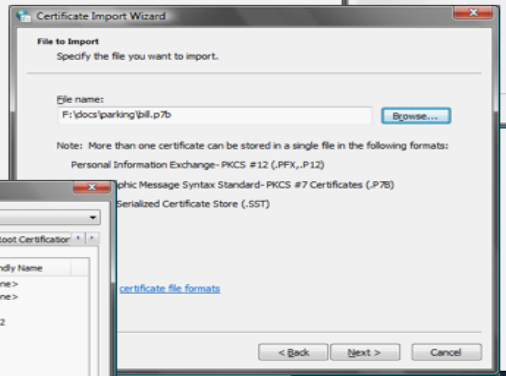
Authentication

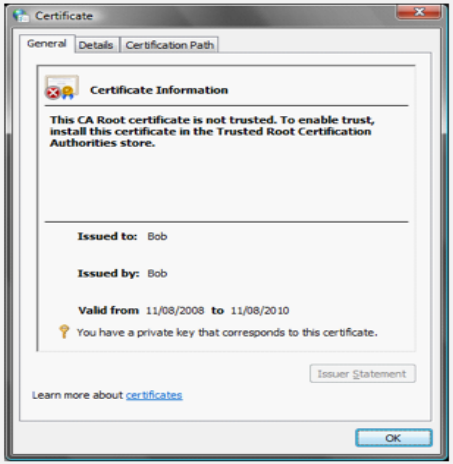
P7b format

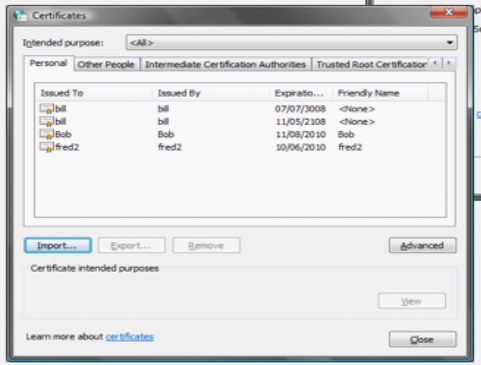
Bob

```
-----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 4iVsz 2nmL 4dyAuyilhLPlVbppHGdE 6sDQXWYd0CpfV
ZN7pauD 5fqBESfO 6bUkCieI 47AzRMQj 3kHuDt 7MexVW 7aoX+nXLP 4wn7IamaxasF
QvhdOKyCZhYs 82JQDGatXRCqkklztmZW 5i6GkPsE 7xVuX 265WJQ 5afhp 2hYlAgMB
AAGjggEXMIIBEzAdBgNVHQ 4EFgQUzyZ /YcCJwT 5opPHLPlcQKkOlkJwwYWYDVR 0j
BFwwWoAUlP 5Zh0V700k 6CorvRMWB 9ifVkBmhP 6Q9MDsxCzAJBgNVBAYTAkdCMREw
DwYDVQQKEwhBc 2NlcnRpYTEZMBcGA 1UEAxMQQXNjZXJ OaWEgUm 9vdCBDQYIBDTBN
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

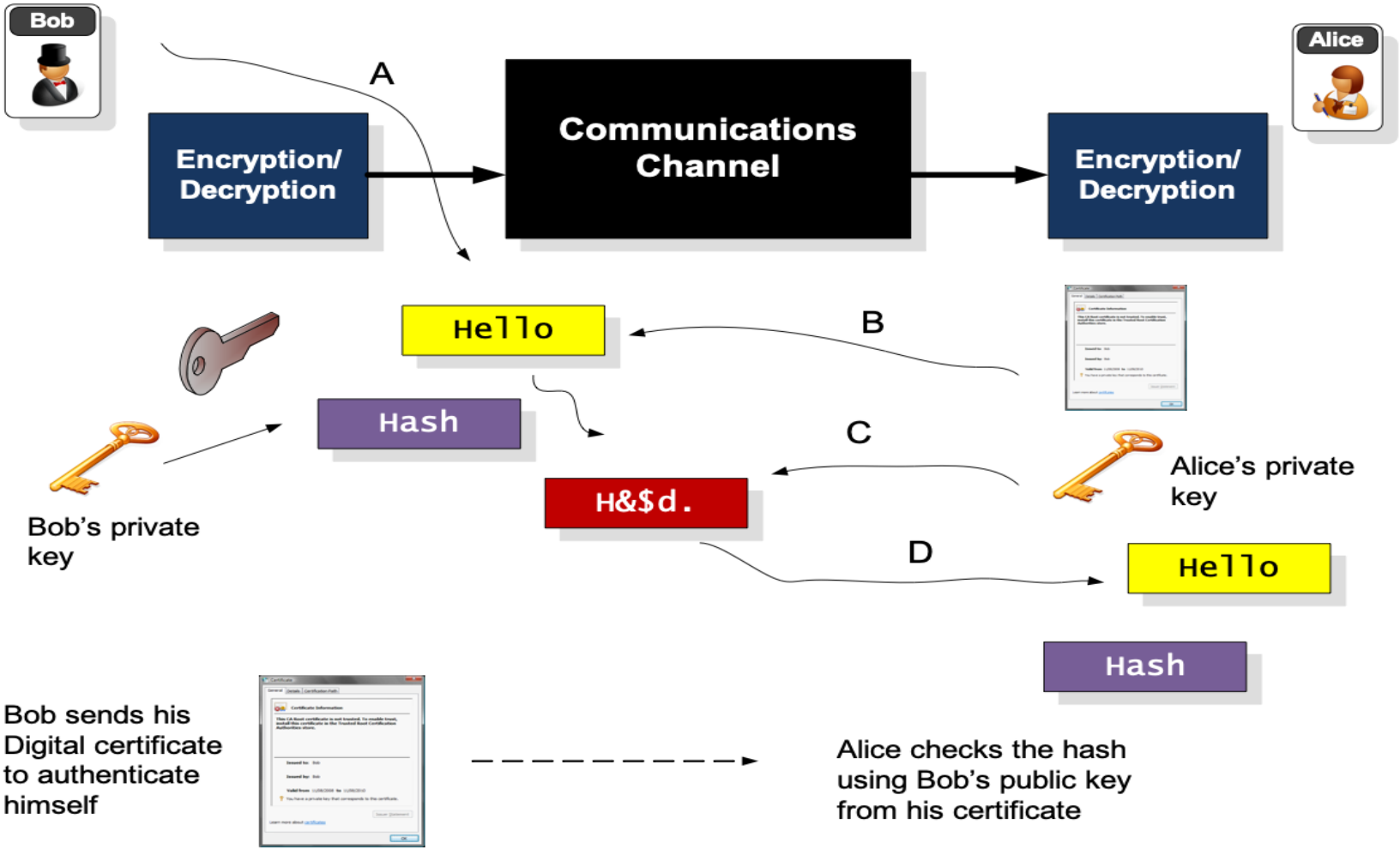
H&$d.

Alice's private key

D

Hello

Author: Prof Bill Buchanan



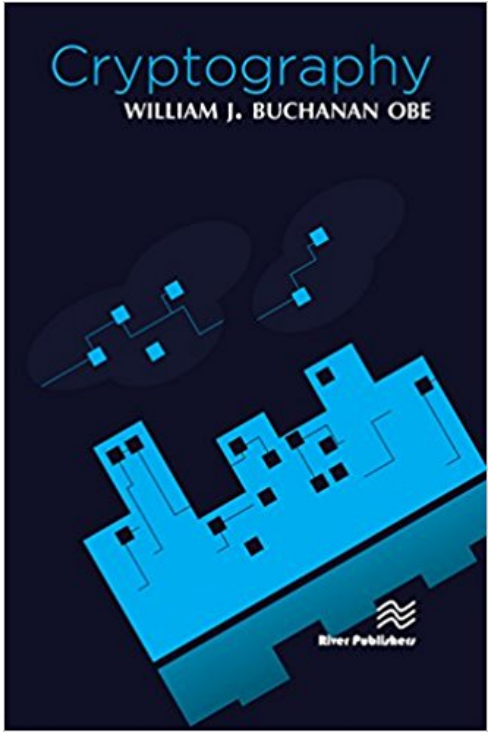
Author: Prof Bill Buchanan

Chapter 6: Digital Certificates

Introduction
Authentication Methods
PKI
Digital Certificate Passing

Prof Bill Buchanan OBE

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



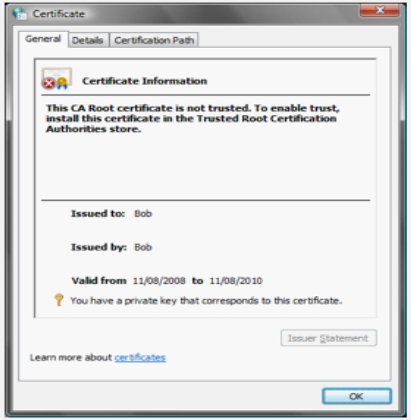
Digital Certificates

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

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.

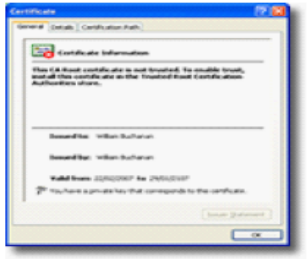
Author: Prof Bill Buchanan

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

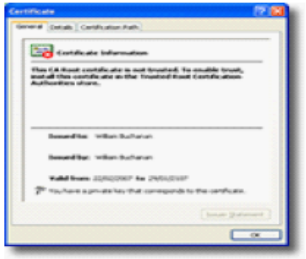
Alice checks the signature of the certificate to validate Bob. Both Alice and Bob trust the CA (Trent) as a third party.

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

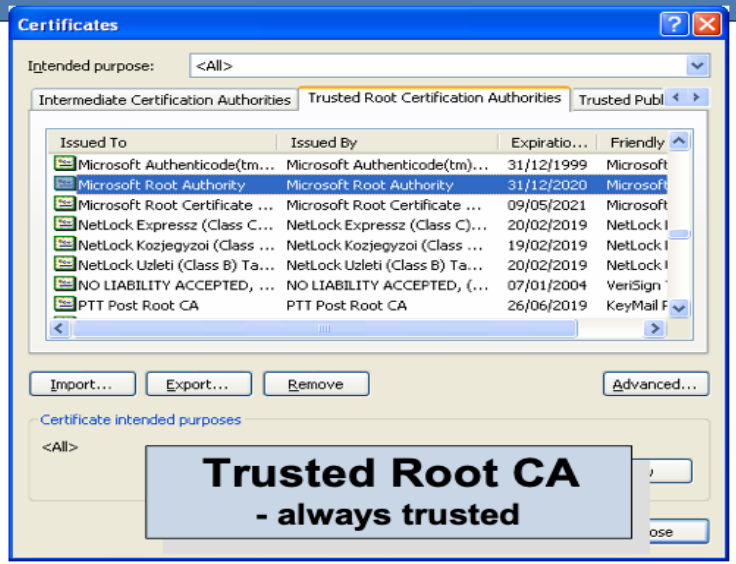


Trusted root certificates are installed as a default on the machine (or installed with the user's permission)

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.

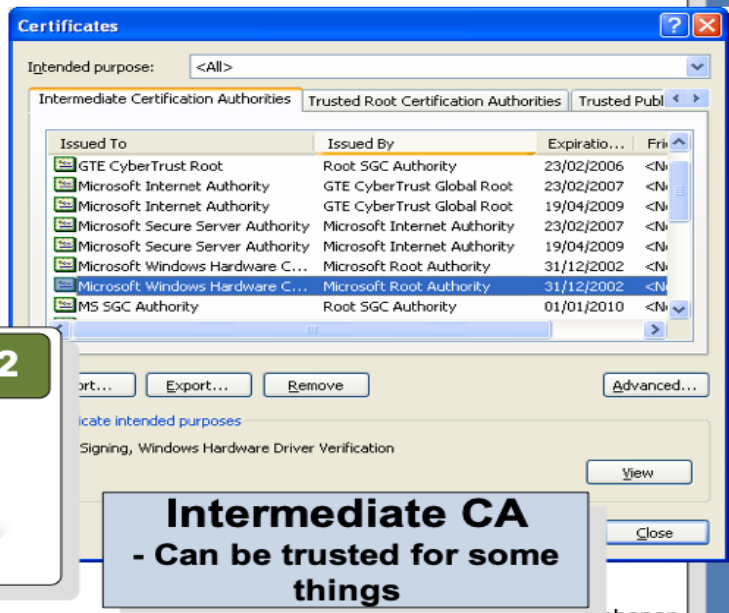
Author: Prof Bill Buchanan



Trusted Root CA

Certificate purposes:

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

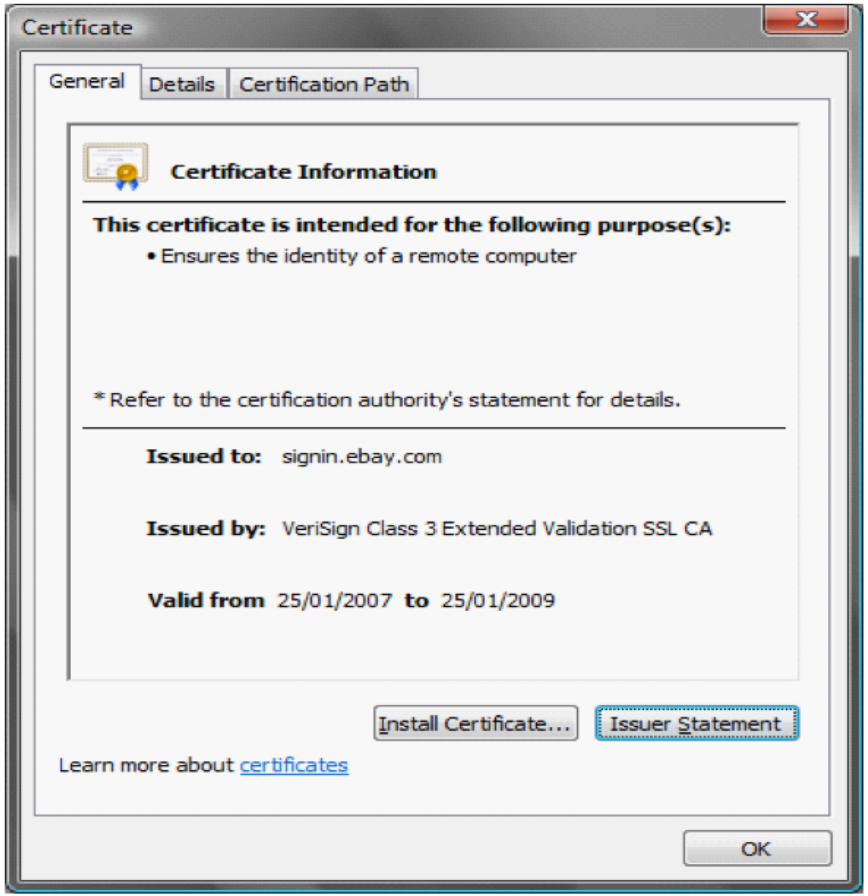


The two main problems with digital certificates are:

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

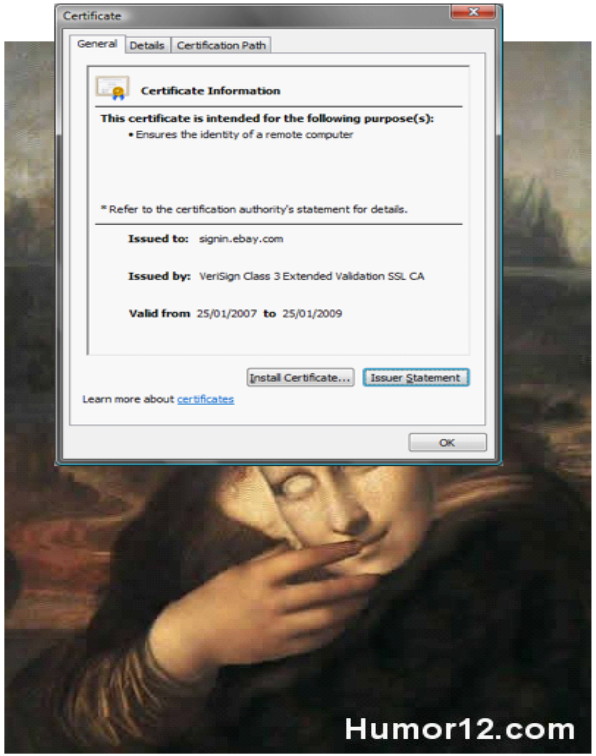
So let's look at a few … are they real or fake?

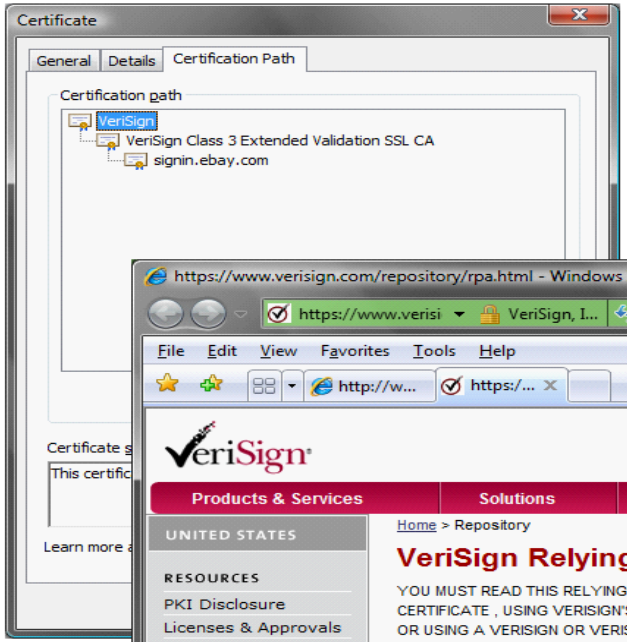
Author: Prof Bill Buchanan



Real or fake?

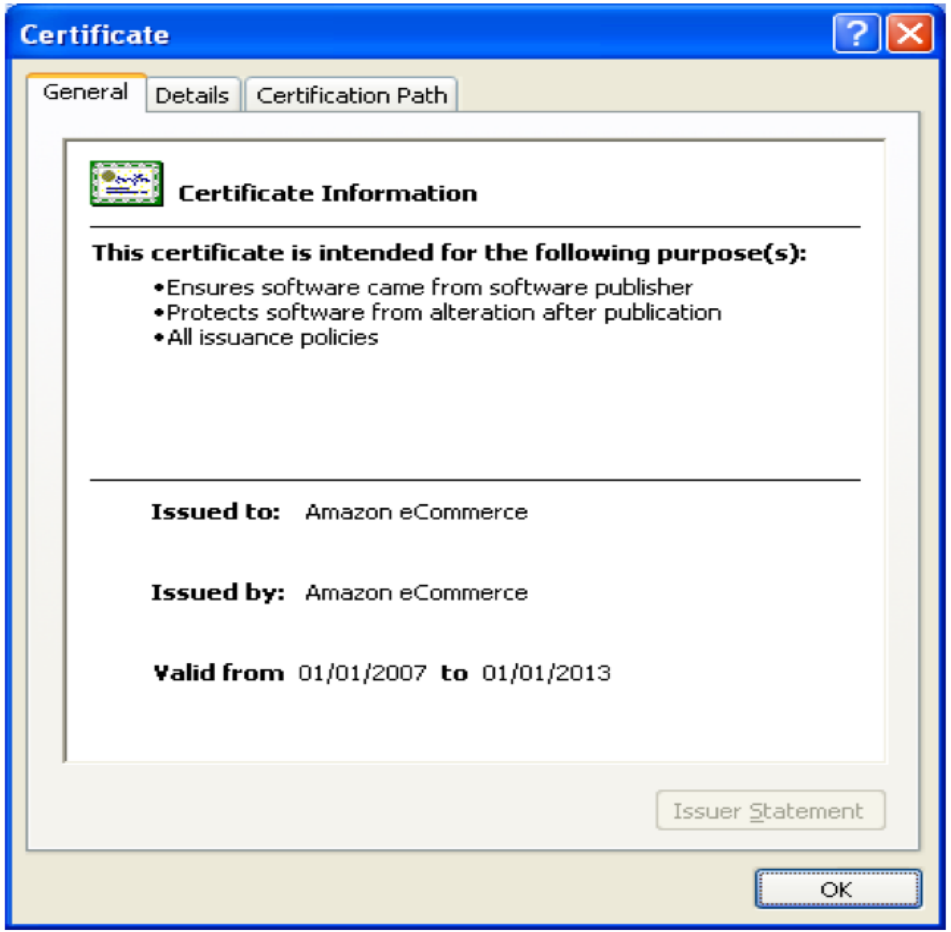
Author: Prof Bill Buchanan





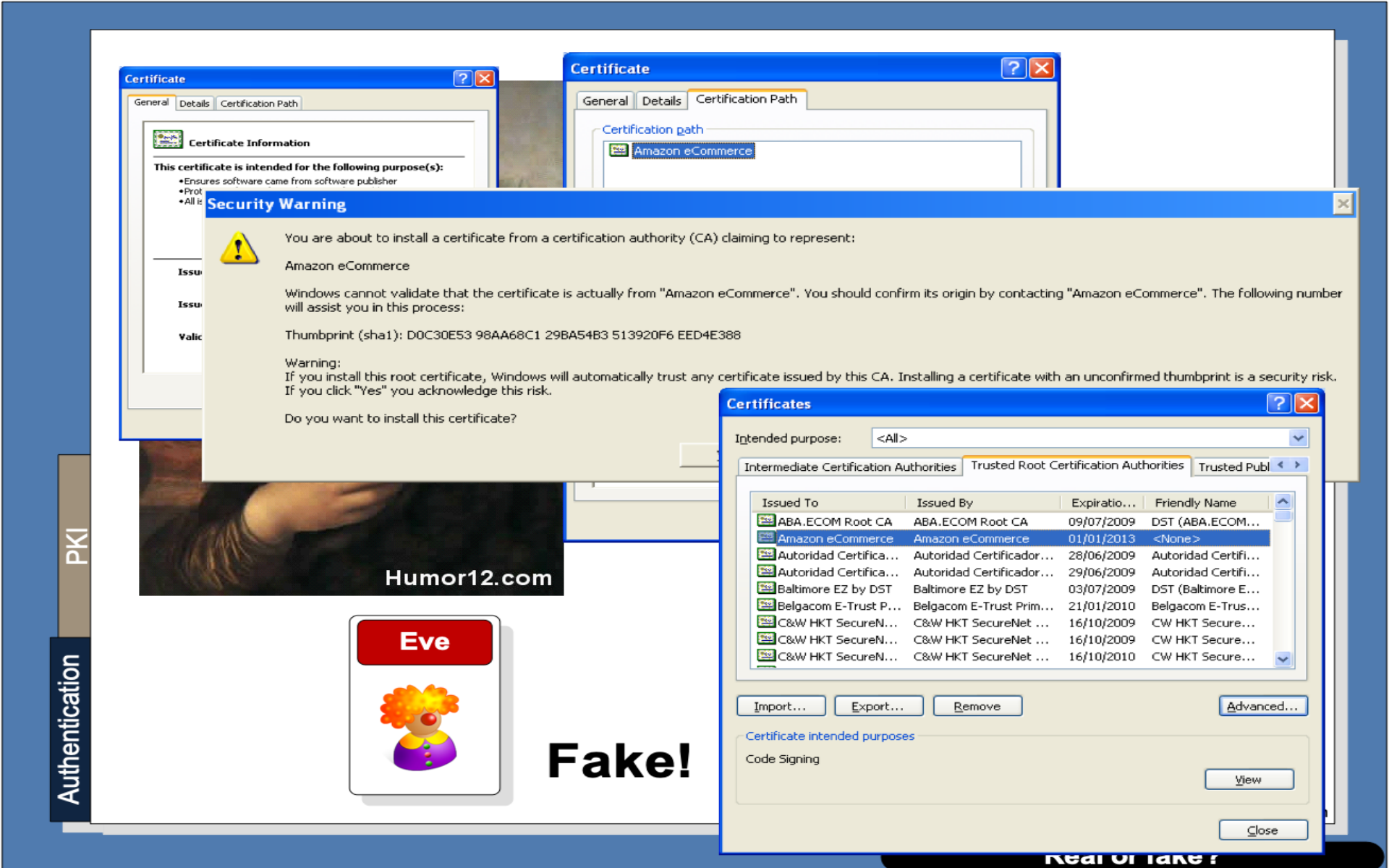
Real!

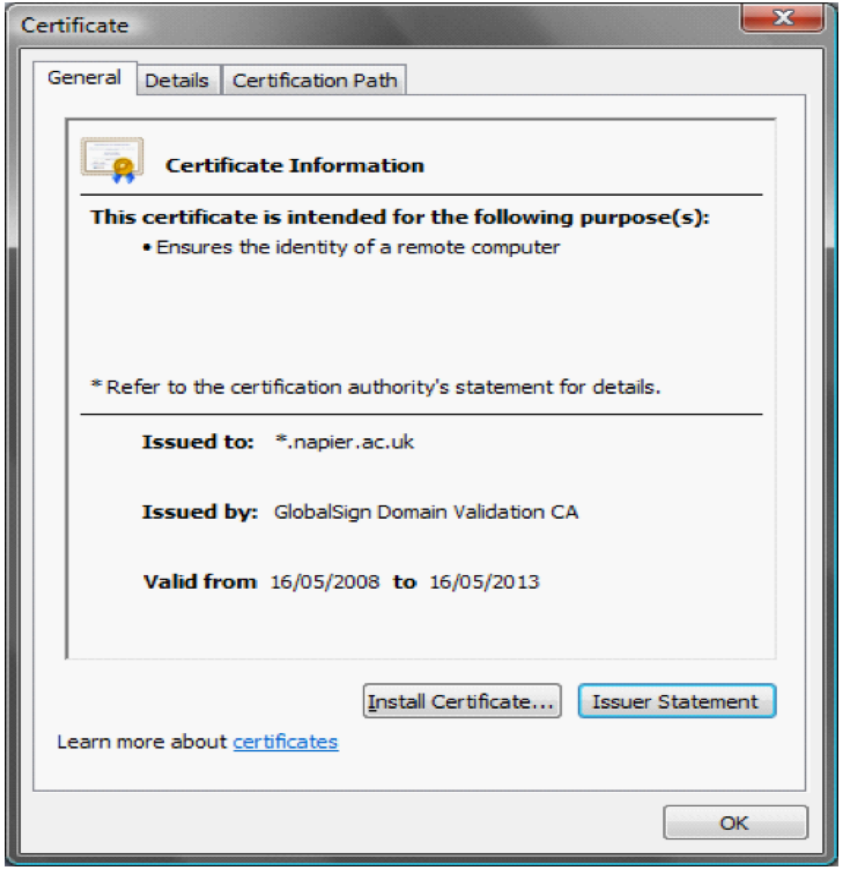
Author: Prof Bill Buchanan



Real or fake?

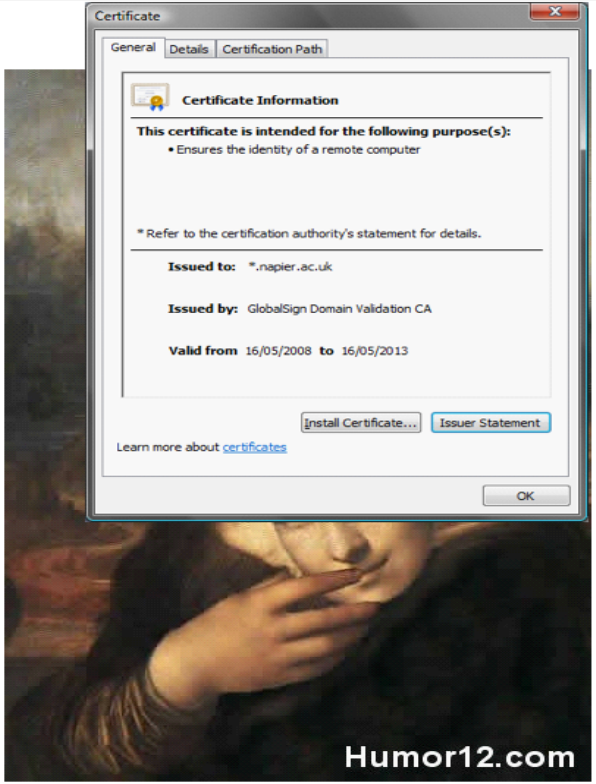
Author: Prof Bill Buchanan

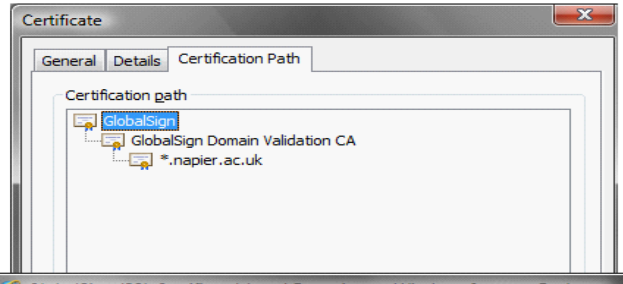

Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
•Ensures software came from software publisher
Certificate
General
Details
Certification Path
Certification path
Amazon eCommerce
Security Warning
You are about to install 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?
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
Humor12.com
Eve
Fake!
PKI
Authentication



Real or fake?

Author: Prof Bill Buchanan





Real

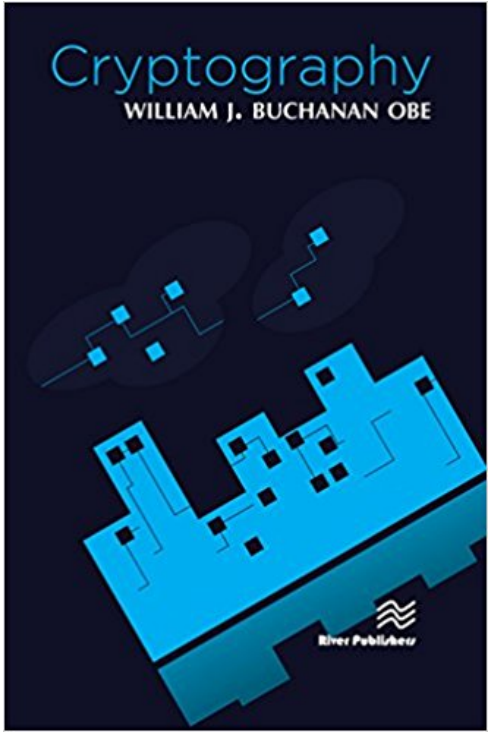
Author: Prof Bill Buchanan

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

Eve

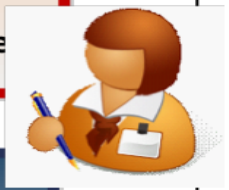
Trent

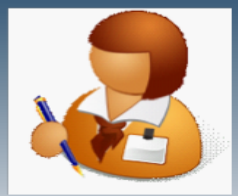
MegaCorp

ob's Private Key

Bob's Public Key

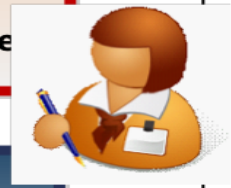
Alice's Public Ke

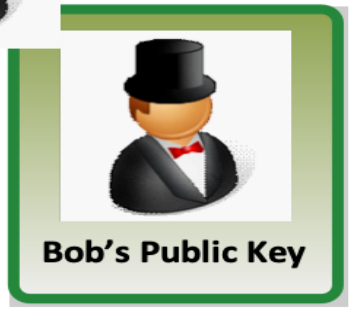




Alice's Private Key

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

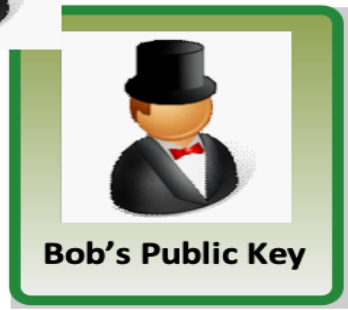
Alice's Public Key

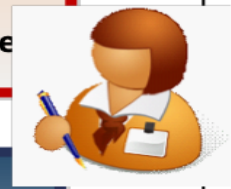
Alice's Private Key

Public key encryption … secret … identity … trust

Hello Alice,
Wish you were here!
- Bob

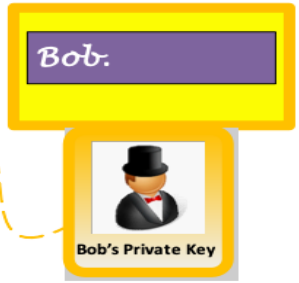
Bob.

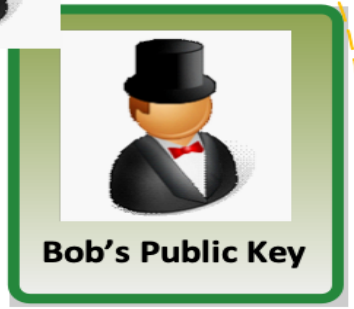


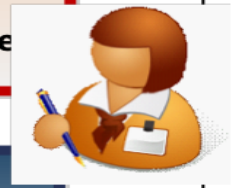


Public key encryption … secret … identity … trust

Hello Alice,
Wish you were here!
- Bob

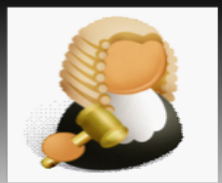






Public key encryption … secret … identity … trust

Eve

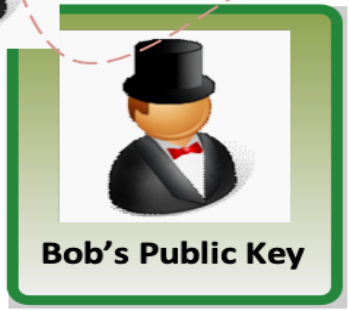


Trent

MegaCorp

Alice's Public Key

ob's Private Key



Bob's Public Key

Alice's Public Key

Alice's Public Ke

Alice's Private Key

Public key encryption … secret … identity … trust

Eve

Trent

MegaCorp

ob's Private Key

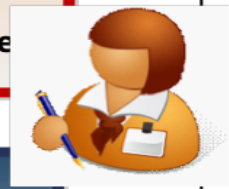
Bob's Public Key

Hello Alice,
Wish you were here!
- Bob

Bob.

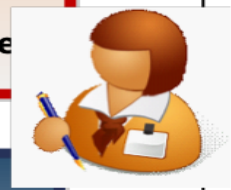
Which key to open the message?

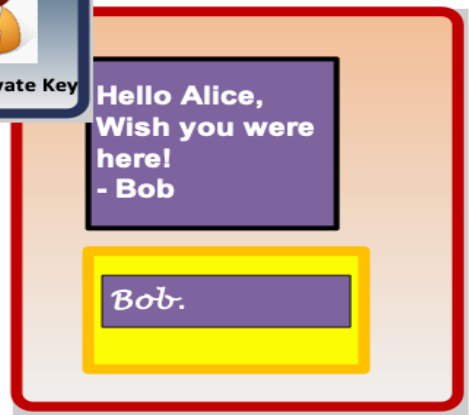
Alice's Public Ke



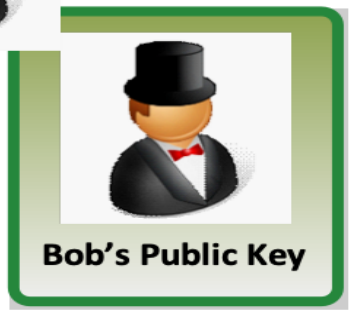
Alice's Private Key

Public key encryption … secret … identity … trust

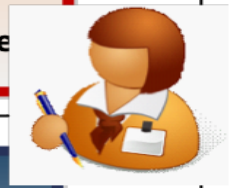




Which key to open the message?

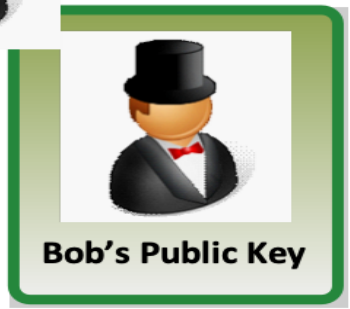


Public key encryption … secret … identity … trust

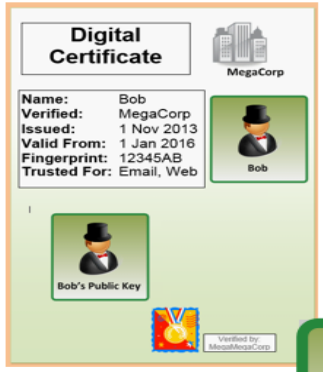


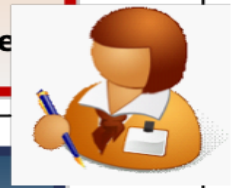
Hello Alice,
Wish you were here!
- Bob

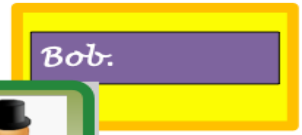
Which key to we open the signature with?

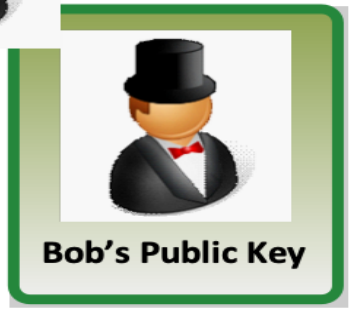


Public key encryption … secret … identity … trust

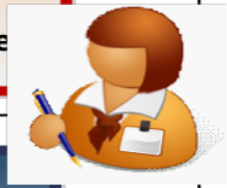




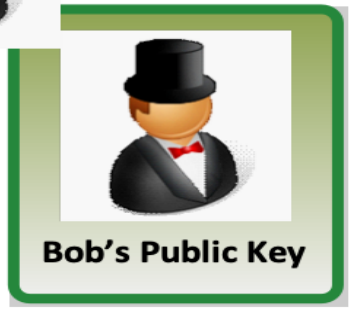




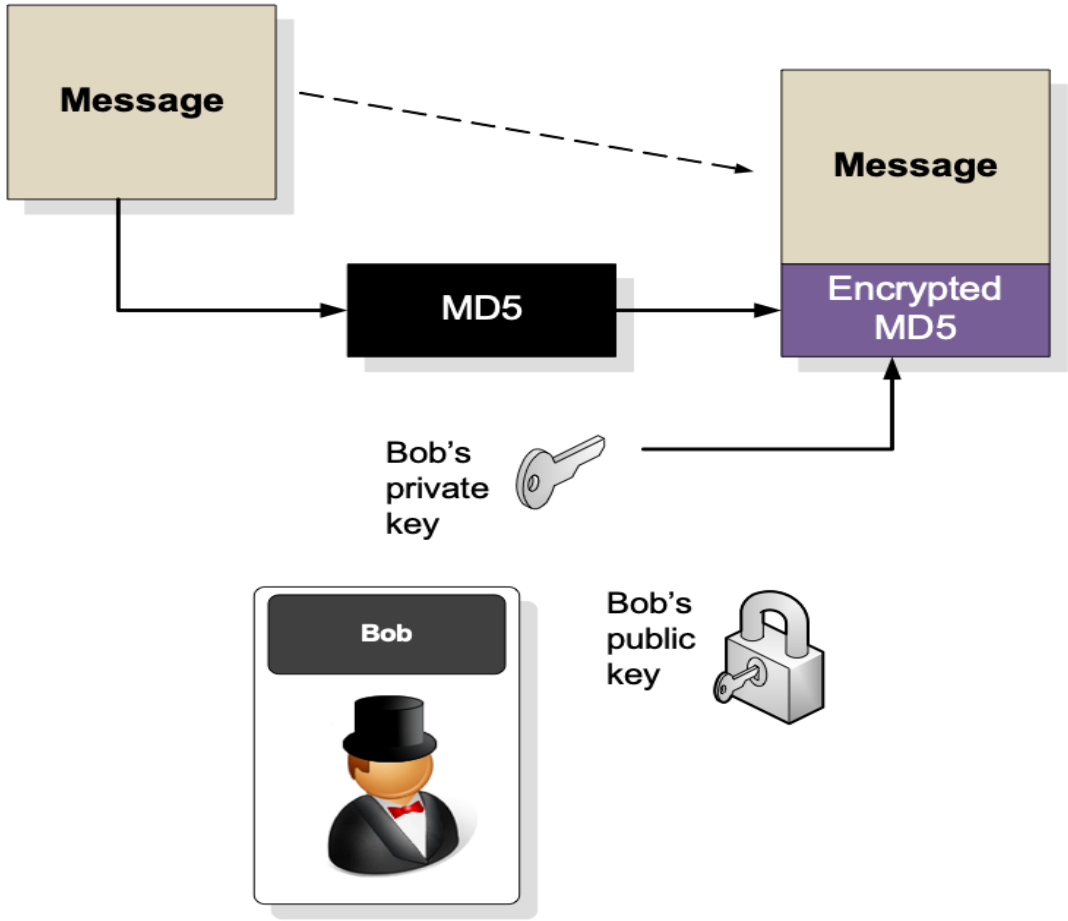
Public key encryption … secret … identity … trust



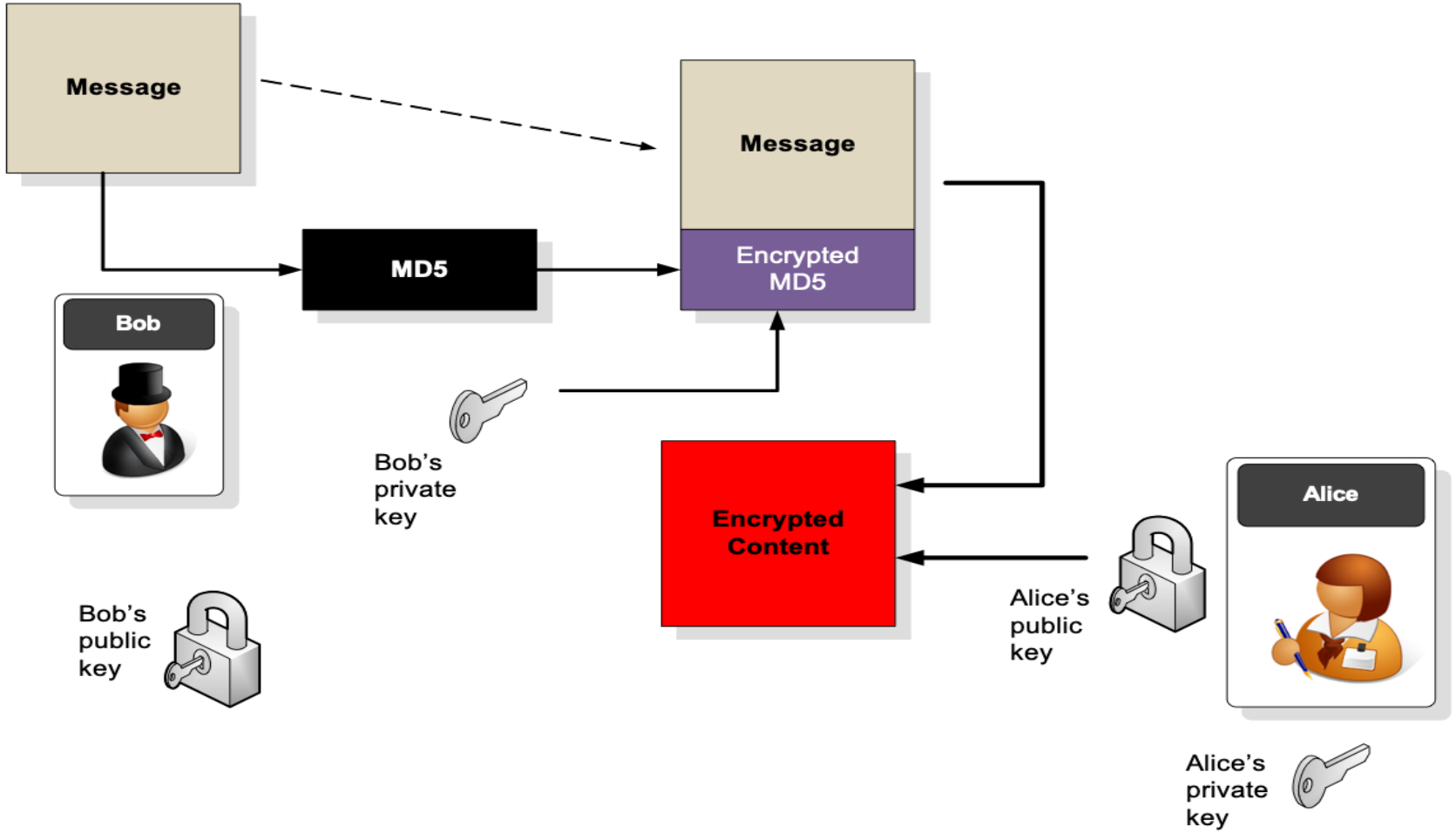
Hello Alice,
Wish you were here!
- Bob



Bob.

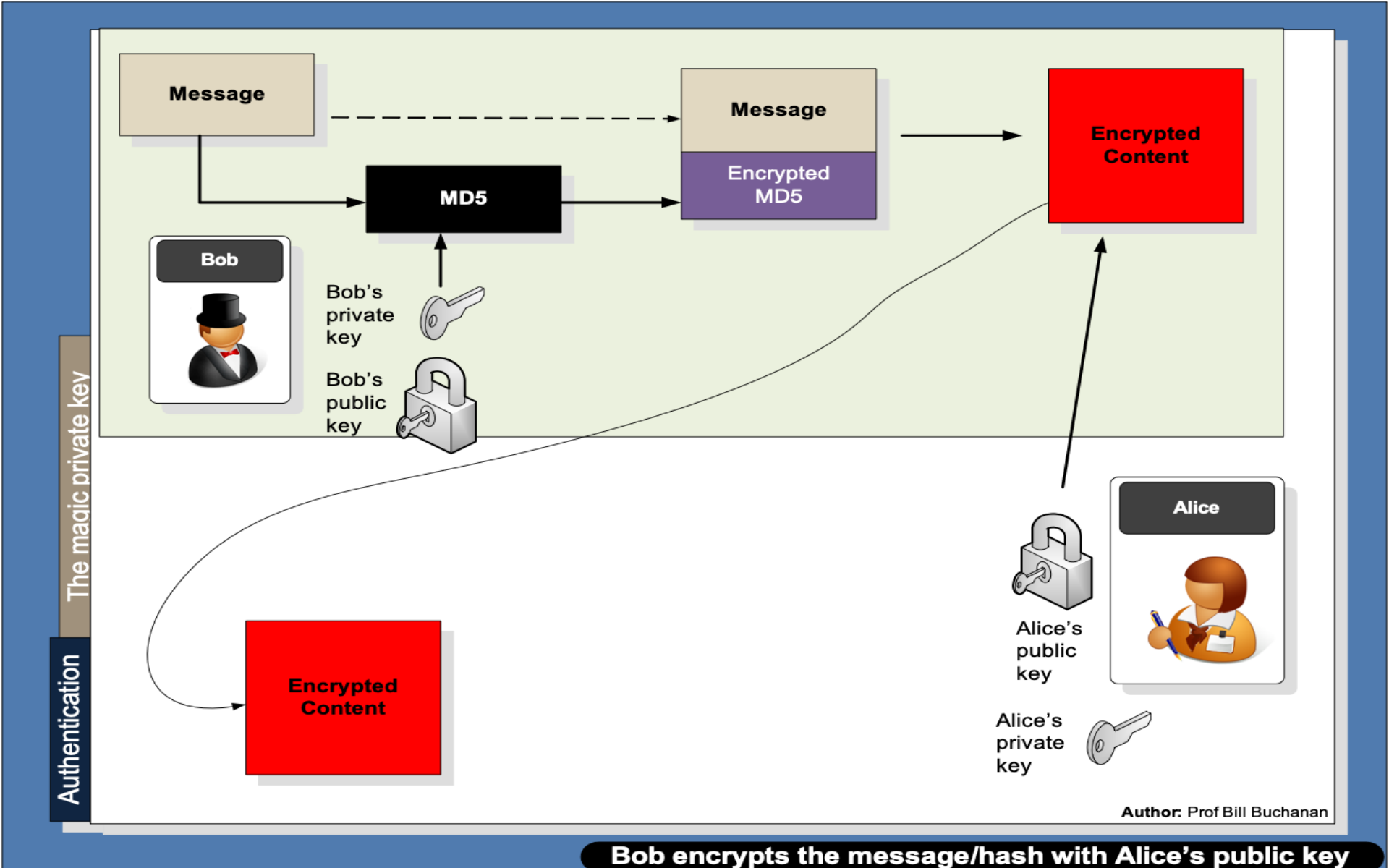


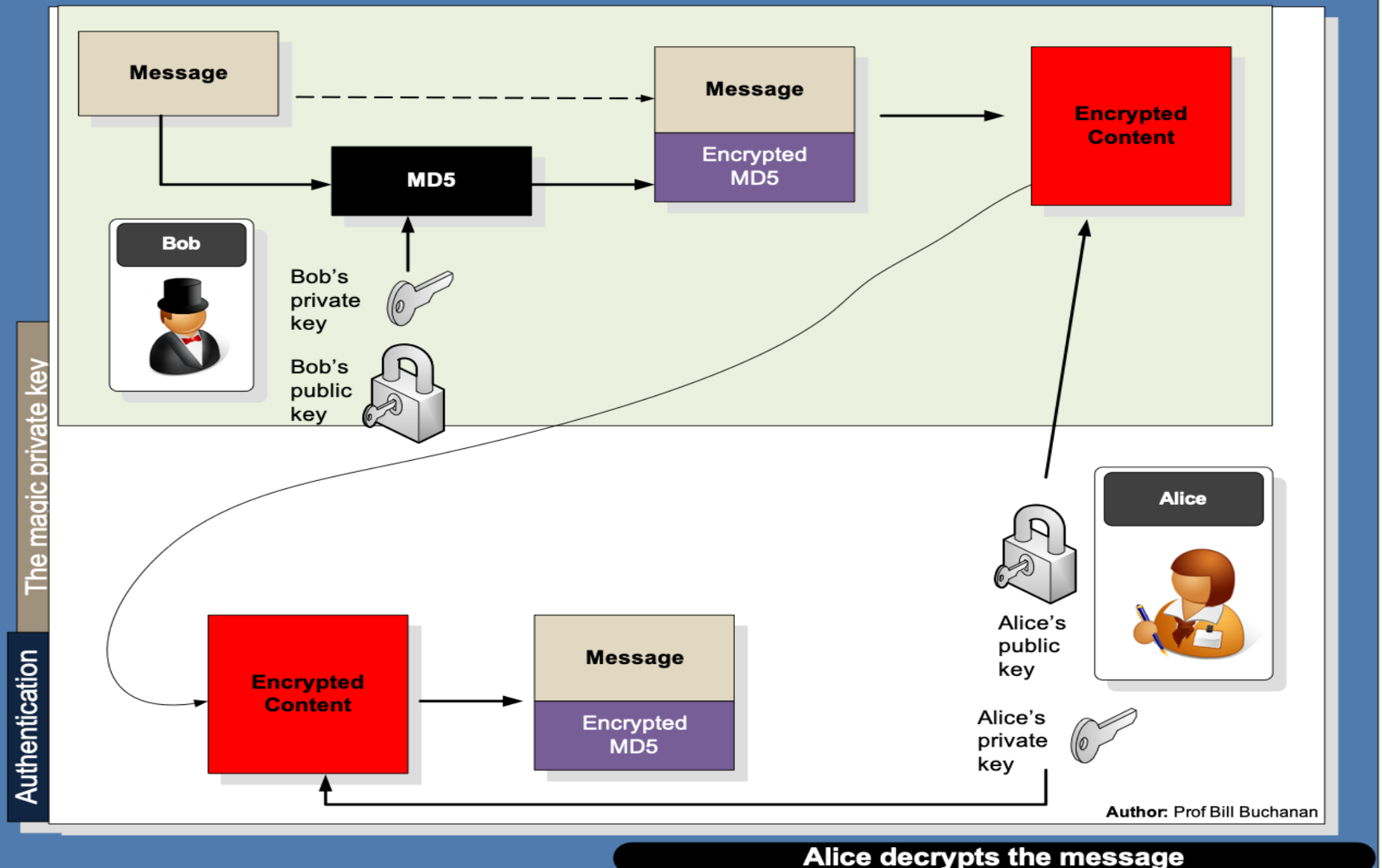
Author: Prof Bill Buchanan



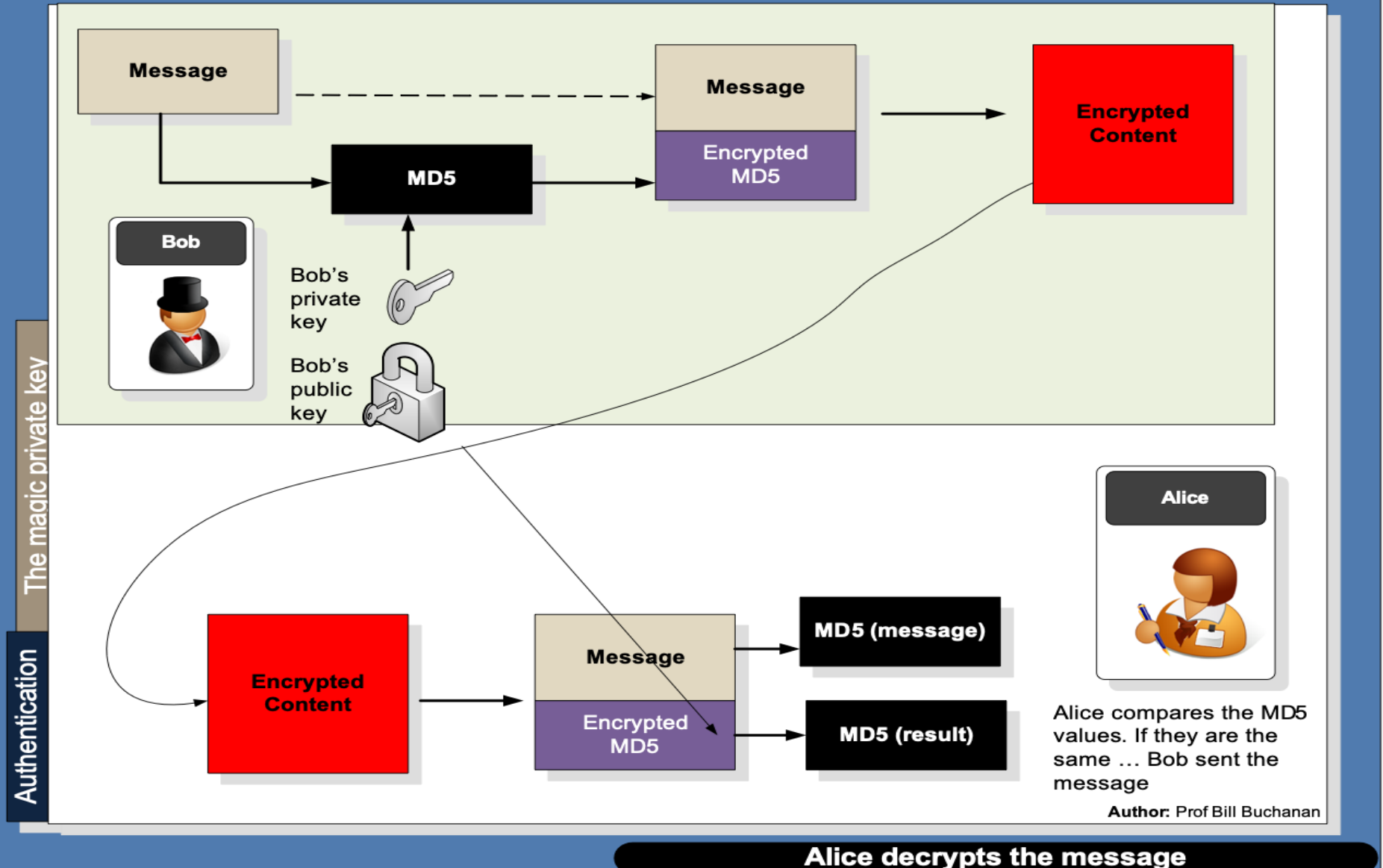
Author: Prof Bill Buchanan

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


Message
Message
Encrypted MD5
MD5
Encrypted Content
Bob
Bob's private key
Bob's public key
The magic private key
Authentication
Encrypted Content
Alice
Alice's public key
Alice's private key
Author: Prof Bill Buchanan
Bob encrypts the message/hash with Alice's public key



Alice decrypts the message

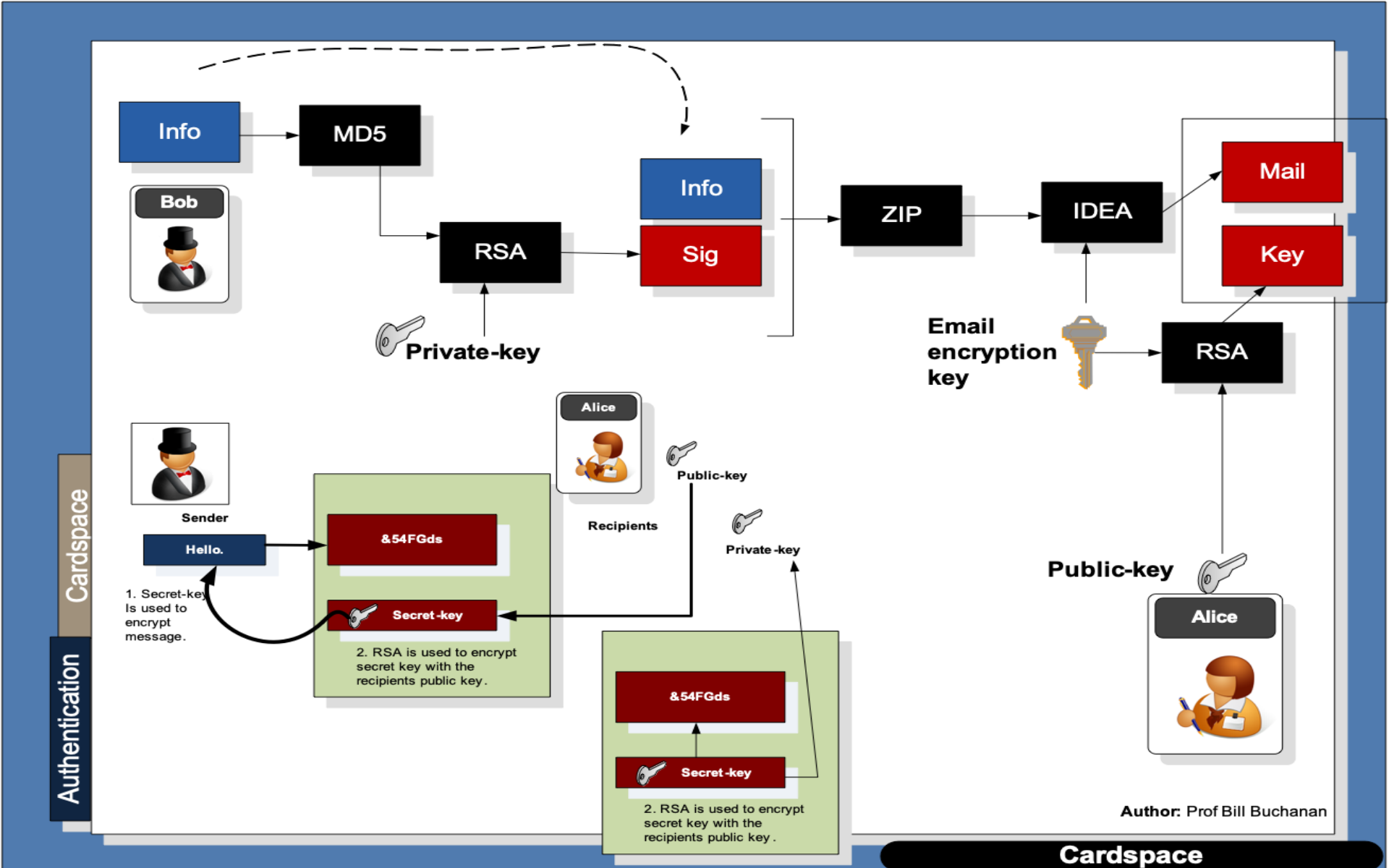

Message
Message
Encrypted MD5
Encrypted Content
MD5
Bob
Bob's private key
Bob's public key
The magic private key
Authentication
Alice
Encrypted Content
Message
Encrypted MD5
MD5 (message)
MD5 (result)
Alice compares the MD5 values. If they are the same … Bob sent the message
Author: Prof Bill Buchanan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

Chapter 6: Digital Certificates

Introduction
Authentication Methods
PKI
Digital Certificate Passing

Prof Bill Buchanan OBE

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


Info
MD5
Bob
RSA
Info
Sig
Private-key
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