

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)

Firefox

P Accept Online Payments And Mobile Pa...
Paypal, Inc. (US) https://www.paypal.com/uk/webapps/mpp/home-merchant

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

The connection to this website is secure.

More Information...

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

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

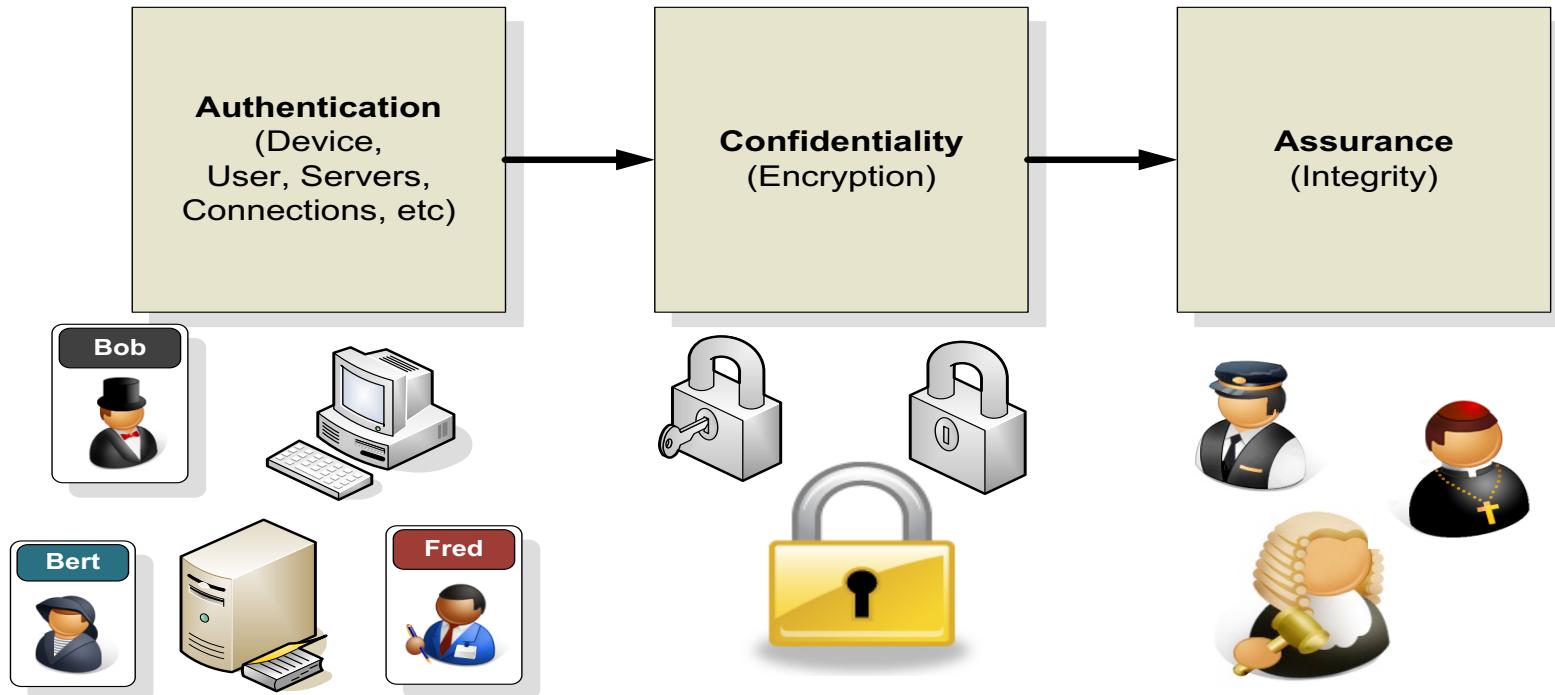
Eve

Bob

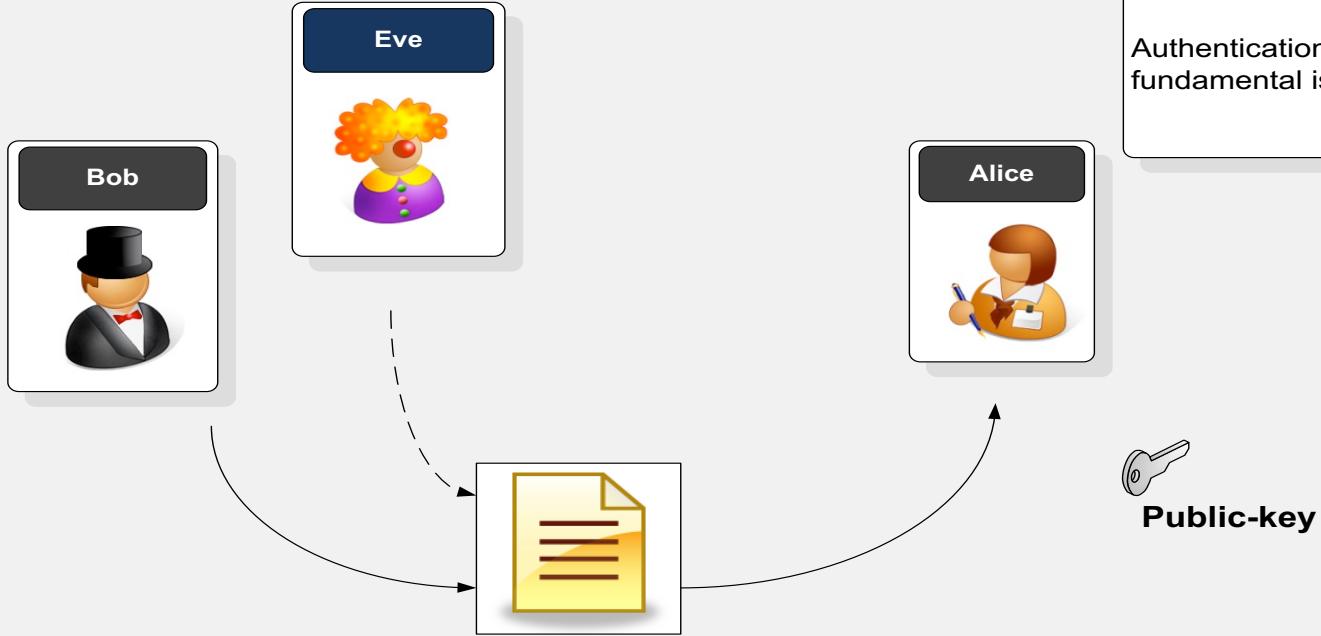


Fundamental principles

Authentication.
Confidence/Assurance.
Privacy/Confidentiality.



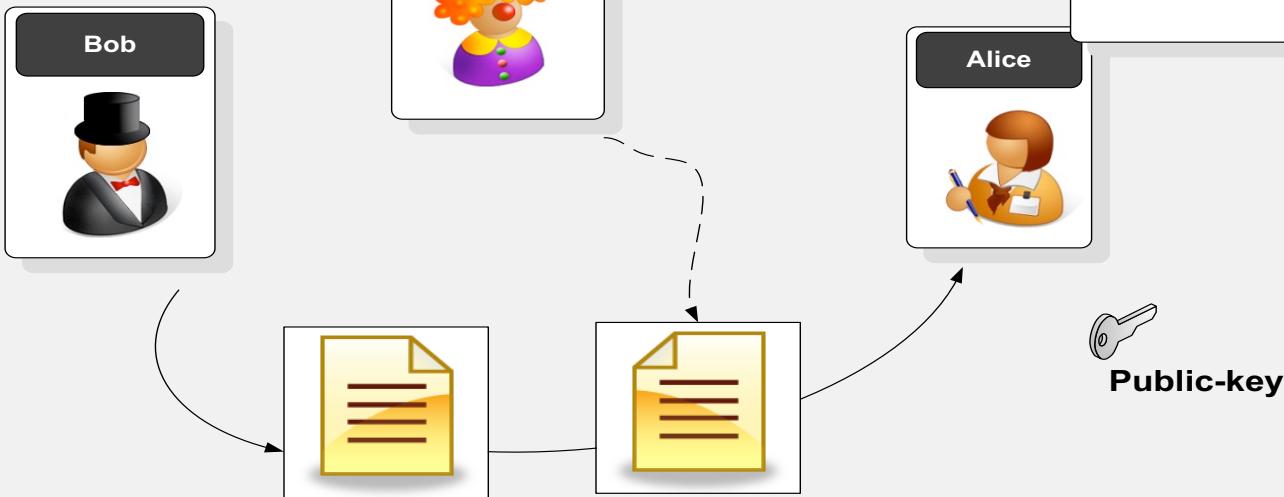
Authentication is a fundamental issue in security.



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

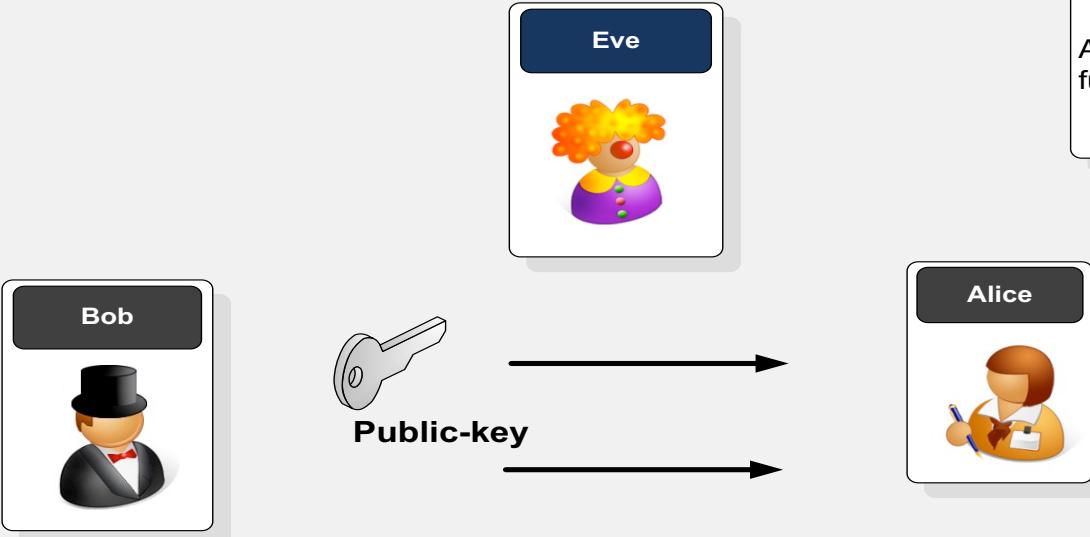
Authentication

Authentication is a fundamental issue in security.



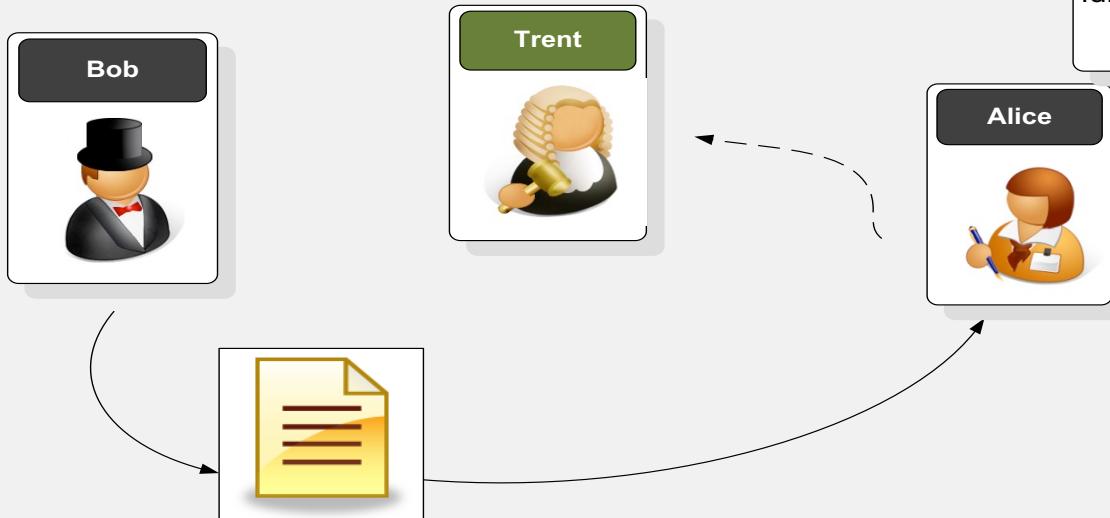
How can we tell that the message has not been tampered with?

Authentication is a fundamental issue in security.



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

Authentication is a fundamental issue in security.



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



Chapter 6: Digital Certificates

Introduction

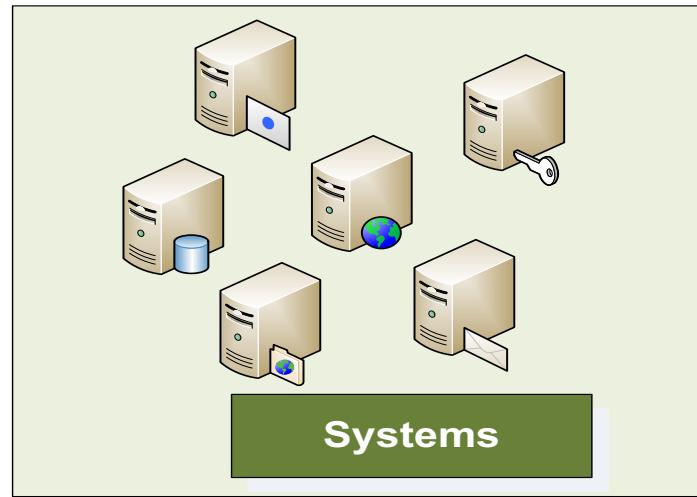
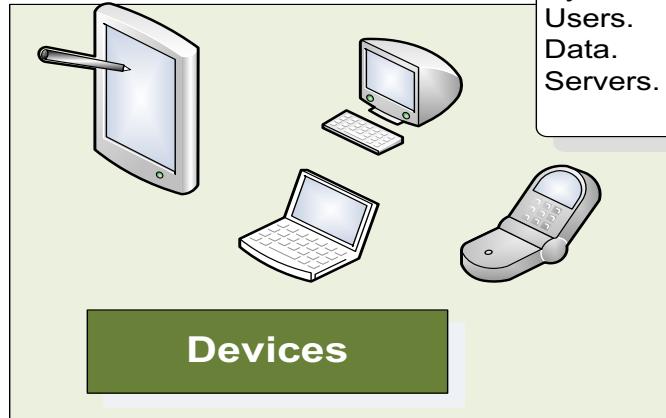
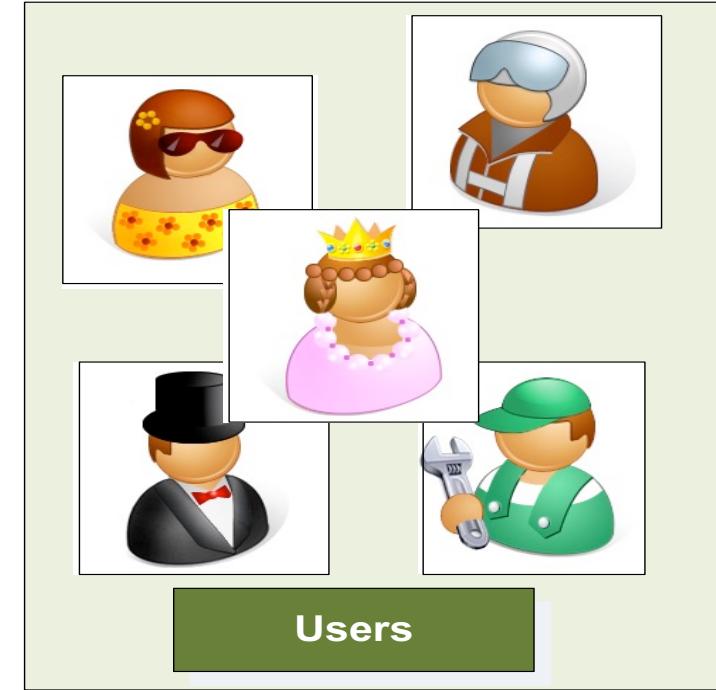
Authentication Methods

Prof Bill Buchanan OBE

<http://asecuritysite.com/crypto06>

<http://asecuritysite.com/encryption>





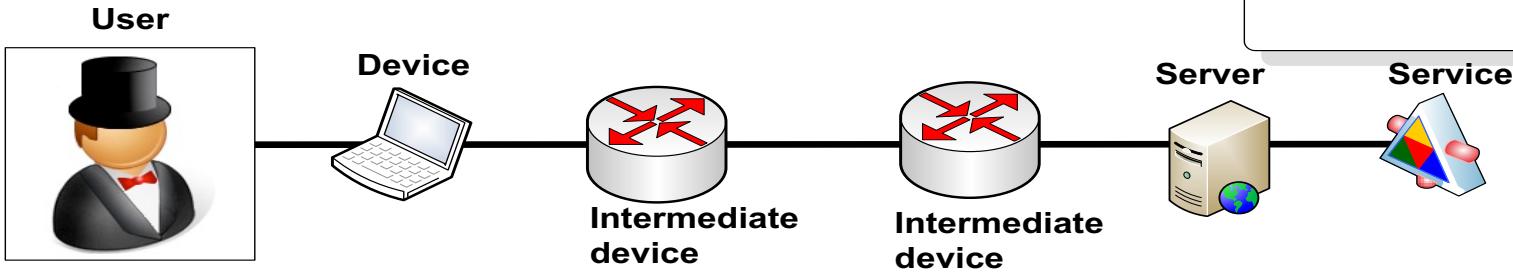
What to authenticate?

Systems.
Users.
Data.
Servers.

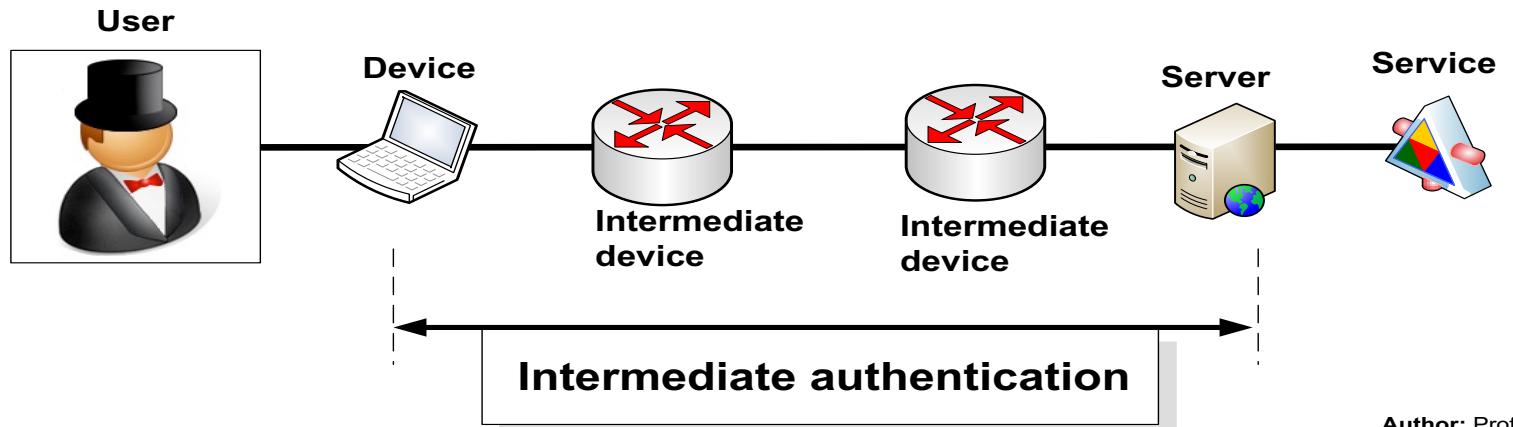
Where authenticated?

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

Authentication Methods



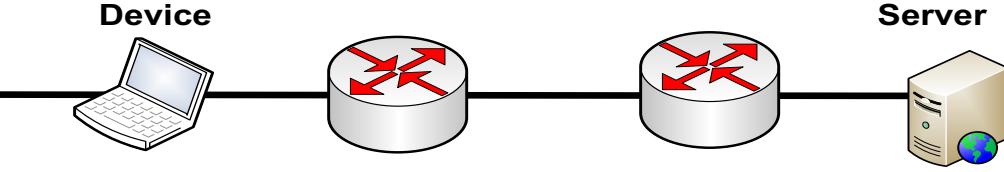
End-to-end authentication



Intermediate authentication



User



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

Authentication type

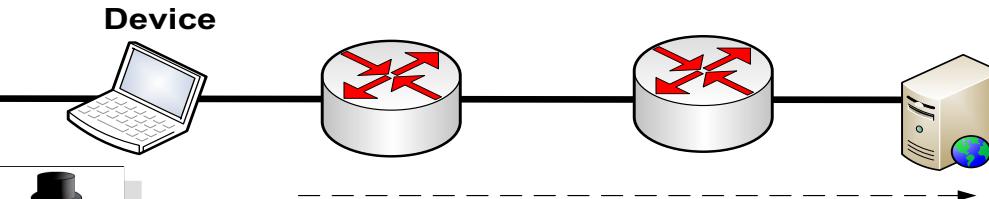
One-way server.
One-way client.
Two-way.



ID



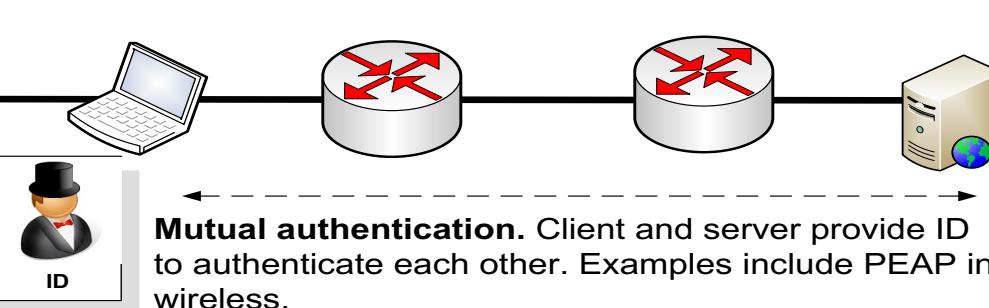
User



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



User

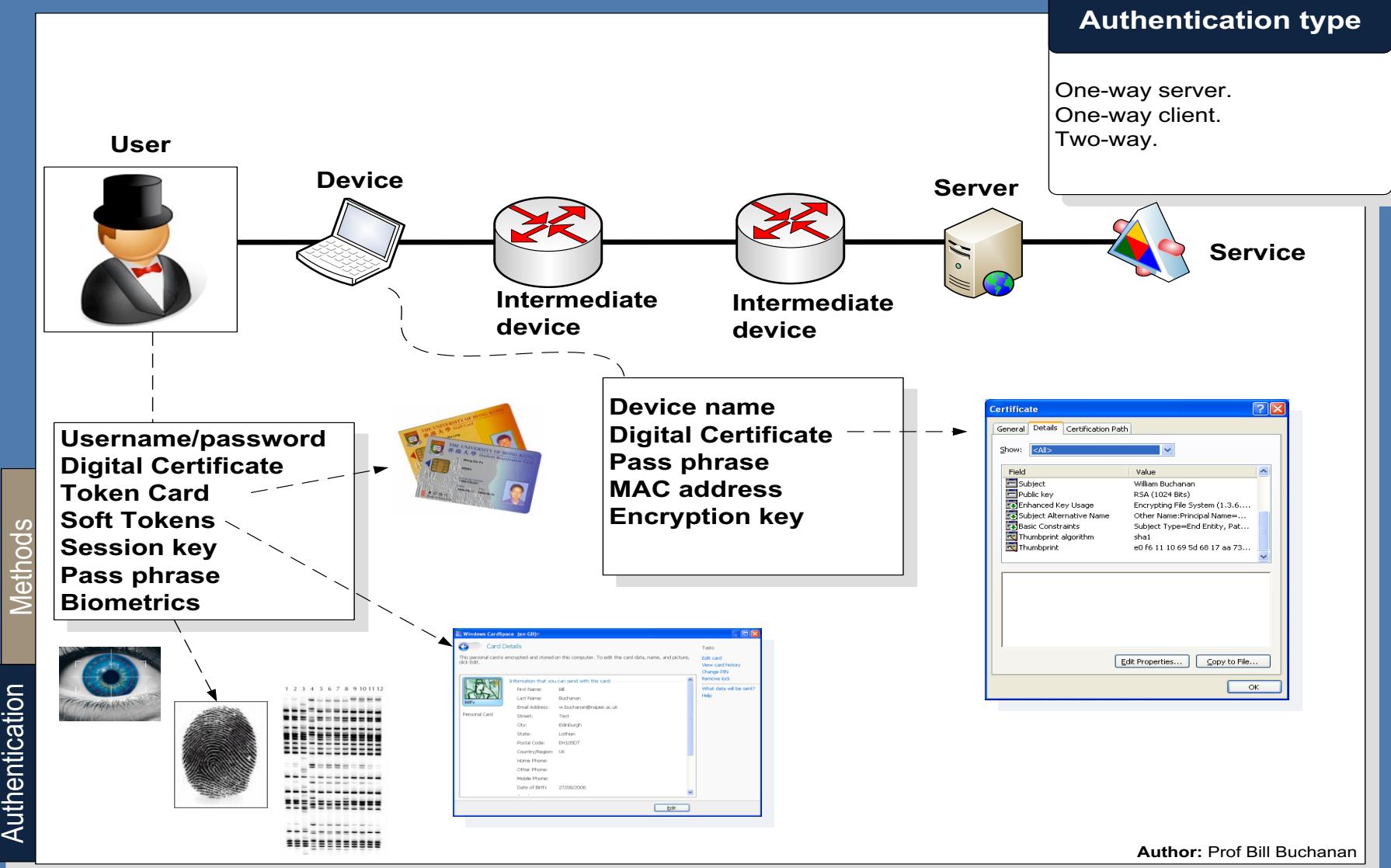


Mutual authentication. Client and server provide ID to authenticate each other. Examples include PEAP in wireless.



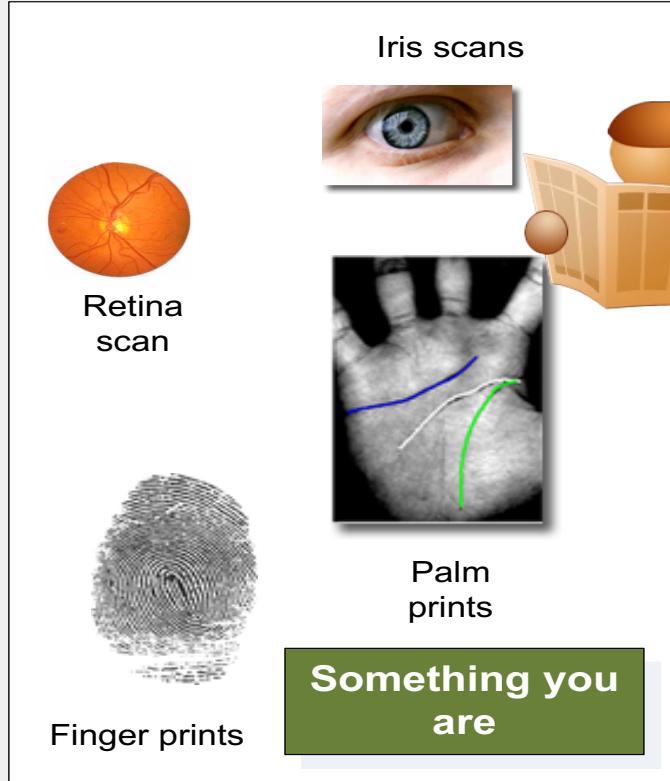
ID

Authentication



Authentication

Methods



Chapter 6: Digital Certificates

Introduction

Authentication Methods

PKI

Digital Certificate Passing

Prof Bill Buchanan OBE

<http://asecuritysite.com/crypto06>

<http://asecuritysite.com/encryption>



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

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

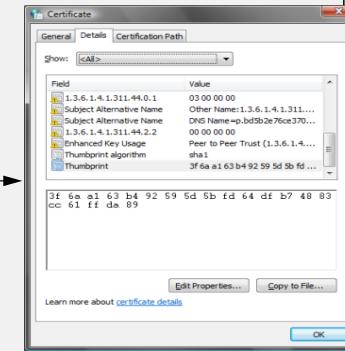


Public-key



Digital Certificates

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



Authentication



Certificate

General Details Certification Path

Certificate Information

Windows does not have enough information to verify this certificate.

Details

Issued to: William Buchanan

Issued by: Ascertia CA 1

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

Issuer Statement

Certificate

General Details Certification Path

Show: <All>

Field **Value**

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

Thumbprint

Edit Properties... **Copy to File...**

OK

Certificate

General Details Certification Path

Show: <All>

Field **Value**

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

Public-key

Certificate

General Details Certification Path

Show: <All>

Field **Value**

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

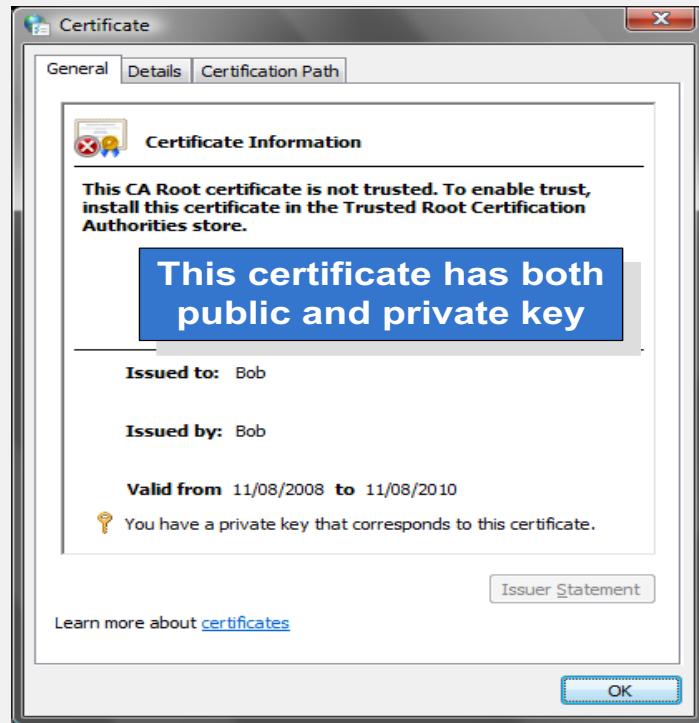
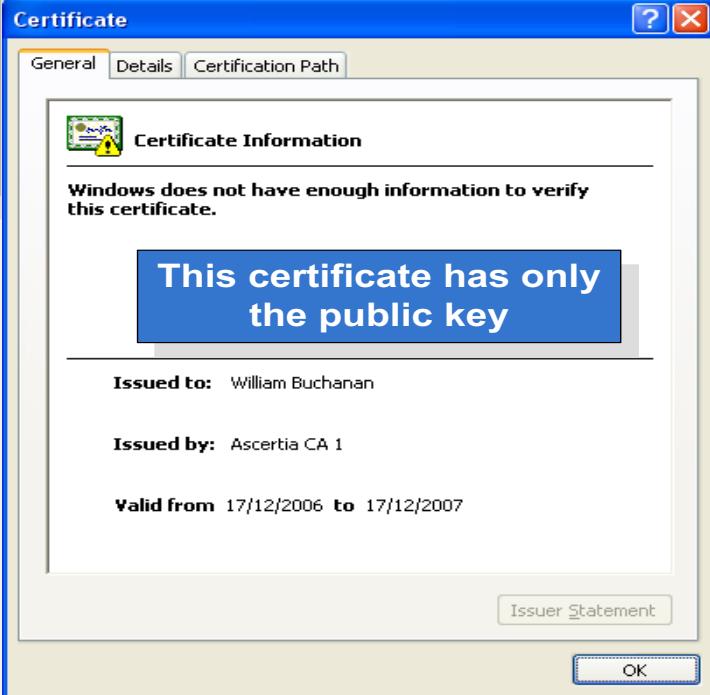
CN = Ascertia CA 1
OU = Class 1 Certificate Authority
O = Ascertia
C = GB

Issuer

Edit Properties... **Copy to File...**

OK

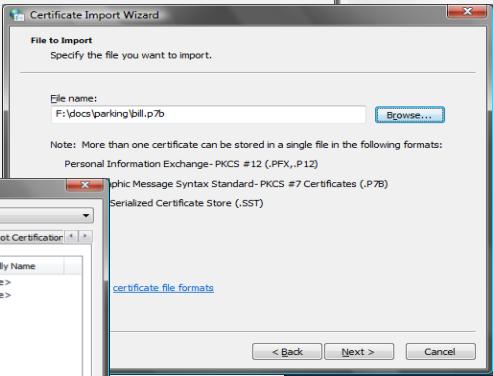
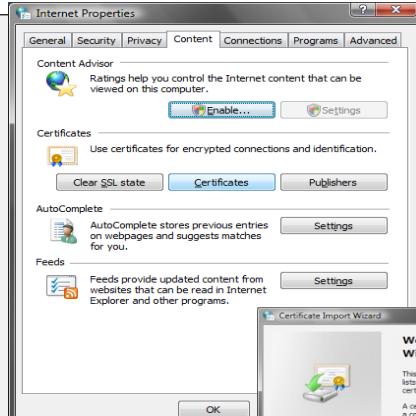
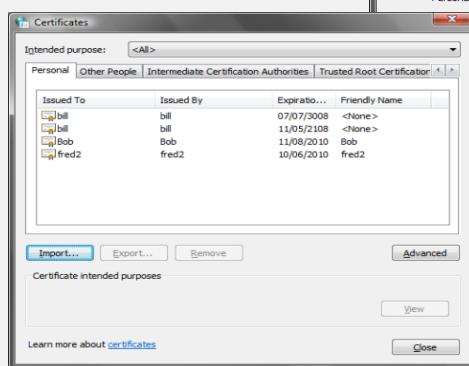
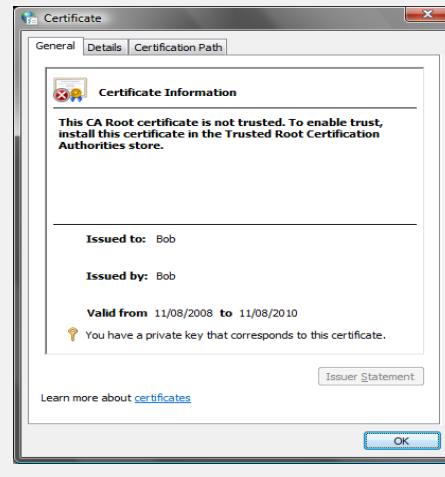
Digital certificate contains a thumbprint to verify it



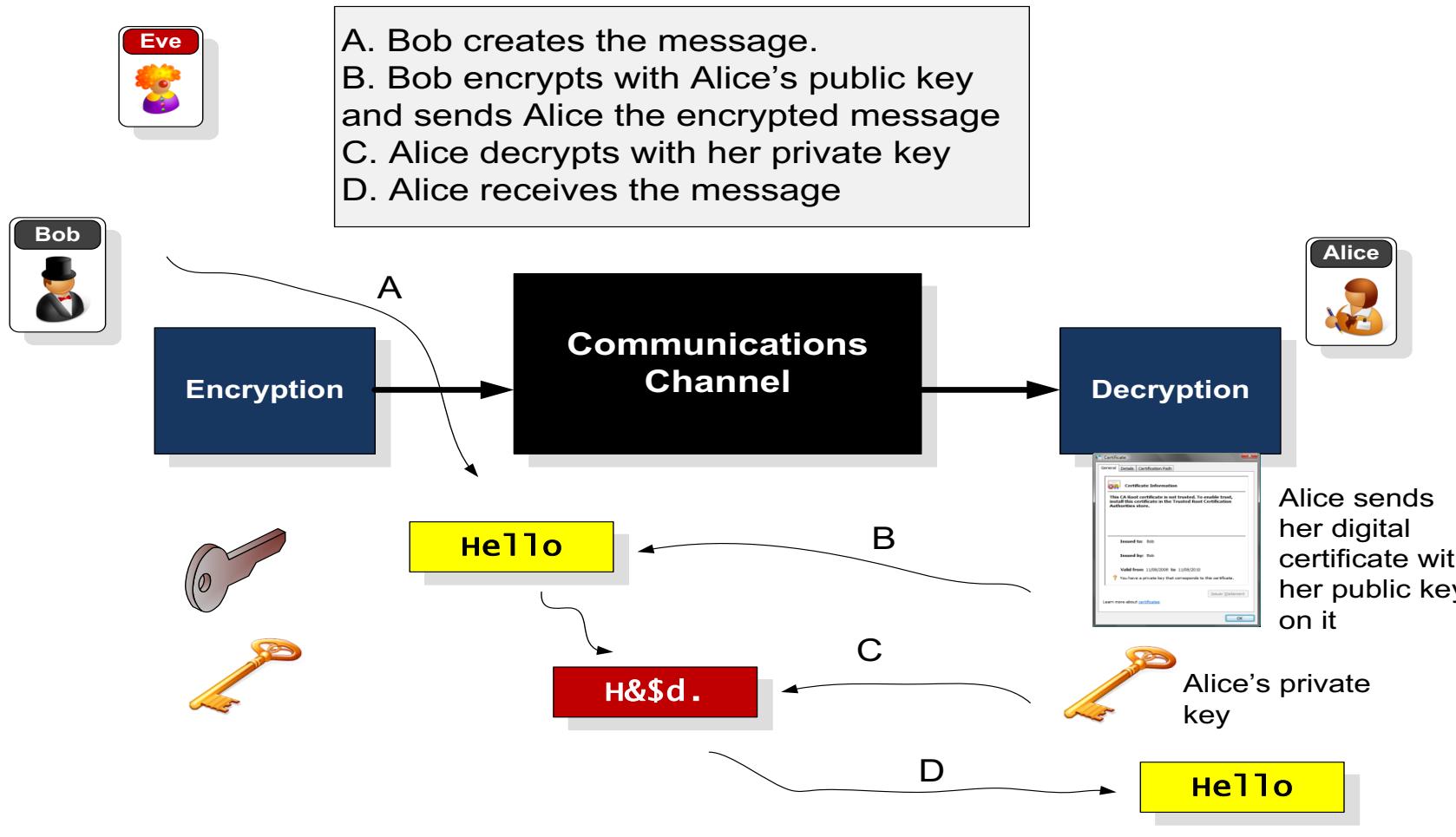
Bob

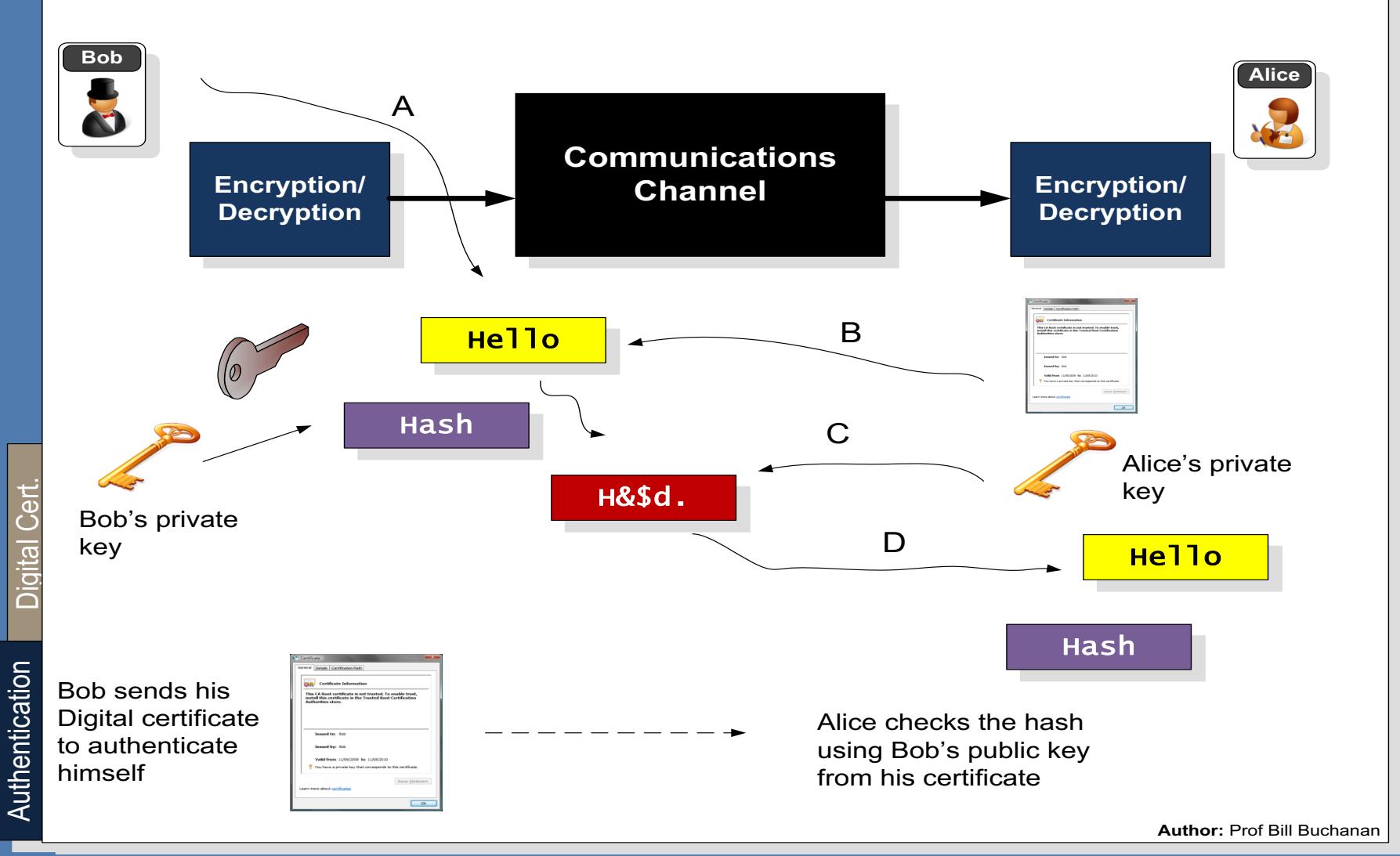
P7b format

```
-----BEGIN CERTIFICATE-----
MIID2zCCA4wgAwIBAgIKWROCQAAAABeujANBgkqhkiG9w0BAQUFADBgMQSwCQYD
VQQGEwJHQiTERMA8GAIUEChMIQXNjZXJ0awExJjkAkgNVBASTHUNSYXNzIDEq02VY
dGlmaWnhdGugQXv0ag9yaXR5MRYwFAYDVQDEwLbc2N1cnRpYsBDSQSAxMB4XDTA2
MTIxNzIxMDQ0OVOxDTA3MTIxNzIxMTQ0OVoewgZ8xJjkAkgkqhkiG9w0BCQEWf3cu
YnvjaGfuYw5AbmFwaVvylMfjLnVmQswCQyDVQQGEwJVSEQMA4GAIUECBMHTG90
ag1hbjEsmBAGA1UEBXMRWrPbmJ1cmndoMRowGAYDVQKExFOYxBpzXlqvW5pdmvY
c210eTELMAkGA1UECMCSVQXGTAxBgNVBAMTEfdpbGpxYw0QnVjaGFUyW4wgE1
MA0GCSqGSIb3QkEBAQAA4IBDwAwggEKAoIBAQCVCFETyJl8VxAhEMRzQ10gM81
ci75nmMs0amjzcB6fhGeMgowMyCoscmQkrVjAknoS+4mXzhncy3mdob+szbwOvaX
M5FOhdsrv+Q86hsk8Cdc+1sqy38TQtufuDns0nfny6tR6q7Cggq08/VjsxNgzk39
iLUf1ahycet/ab60/qwzL4ivsz2nml4dyauyi1hLP1vbppHgde6sdQxWyd0cpfv
ZN7paud5fqBESf06bukCieI47AZRMQj3kHuDt7Mexvw7aoX+nXLPL4wn7IamaxasF
QvhdkycjZ8JQDGatxRCqkk1ztmzw51GKPE7xvu265wJQ5afhp2hY1agMB
AAGjgqEXM1BEzAdBgnVHO4EFgouzy/YccJwT5opPHPL1cQkk01kjwwywDVR0j
BFww0AU1P5Zh0v700k6CorvRMw91fVkb8mhP609MDsxCza1BgNVBAYTAKdCMREw
DwYDVQKEwhBc2N1cnRpYTEZMCgA1UEAxMQXNjZXJ0awEgum9vdCBQYIBDTBn
BgNVHR8ERjBEMEkgQKA+hjxodHRw018vd3dLmfzY2vydg1hLmnb9pbmxpbmVD
QS9jcmxzL0FzY2vydg1hQ0ExNsYXNzMS5jcmnwPgYIKwvBBQUHAQEEMjAwMC4G
CCsGAQUFBzAChiJodHRw018vb2NzC5nb9iYw0CnVzdGZpbmR1c15j2b20vMA0G
CSqGSiB3DQEBBQAA0EATOCwgJ1tS0kTlupmpjkml8idxMmD5wuhszb1GsMhPxI
H+vXhL9yaow+Prpzy7ajS4/3xxu8vRANhyU9yU4qda==
-----END CERTIFICATE-----
```



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





Chapter 6: Digital Certificates

Introduction

Authentication Methods

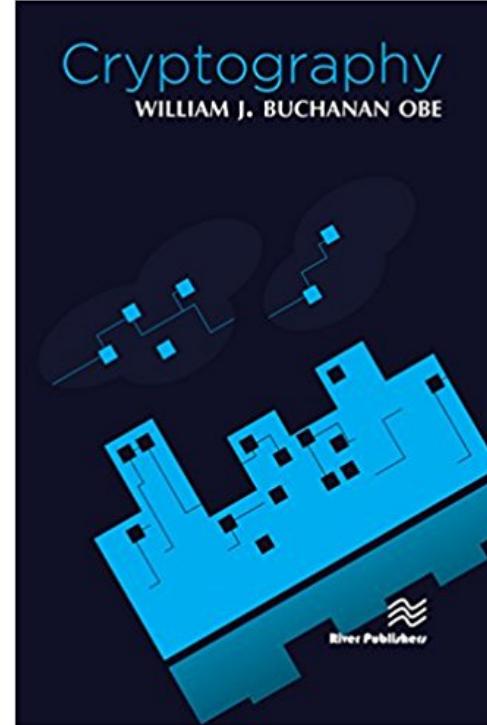
PKI

Digital Certificate Passing

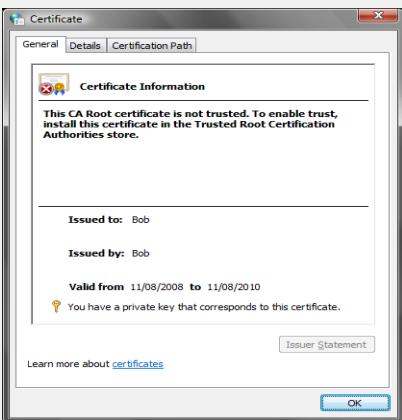
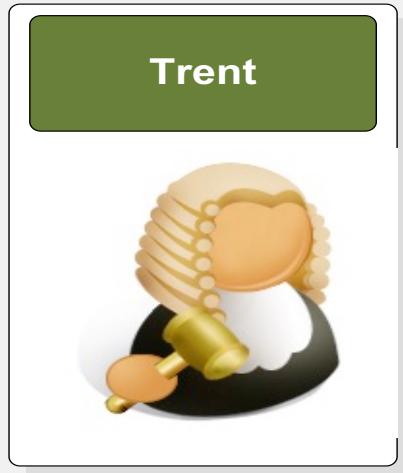
Prof Bill Buchanan OBE

<http://asecuritysite.com/crypto06>

<http://asecuritysite.com/encryption>



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



Digital Certificates

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

Trusted Root CA



Certificate Authority (CA)

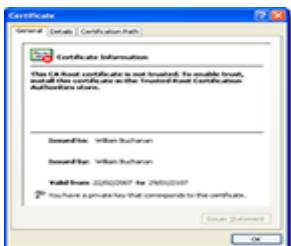
- Able to grant certificates

Examples; Verisign, Entrust, Microsoft Trust.

Trent

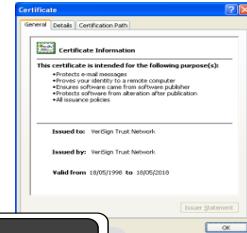


The Trusted Root CE (Trent) checks Bob's identity and creates a certificate which he signs



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.

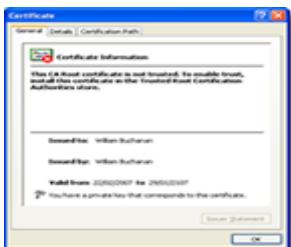
Alice



Author: Prof Bill Buchanan



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



Trusted Root CA



Certificate Authority (CA)

- Able to grant certificates

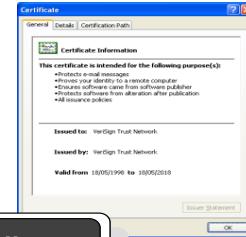
Examples; Verisign, Entrust, Microsoft Trust.

Trent



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

Trusted root certificate



Alice



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

Author: Prof Bill Buchanan

Certificates

Intended purpose: <All>

Intermediate Certification Authorities Trusted Root Certification Authorities Trusted Publ

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

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

Certificate intended purposes <All>

Trusted Root CA
- always trusted

Trusted Root CA



Certificate purposes:

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

Certificate

General Details Certification Path

Certificate Information

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

Self signed
- Can never be trusted

Issued to: William Buchanan

Issued by: William Buchanan

Valid from 22/02/2007 to 29/01/2107

You have a private key that corresponds to this certificate.

Issuer Statement OK



Trust2



Certificates

Intended purpose: <All>

Intermediate Certification Authorities Trusted Root Certification Authorities Trusted Publ

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

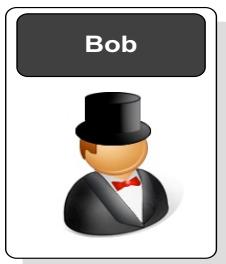
Import... Export... Remove Advanced...

Certificate intended purposes

Signing, Windows Hardware Driver Verification

Intermediate CA
- Can be trusted for some things

Levels of trust



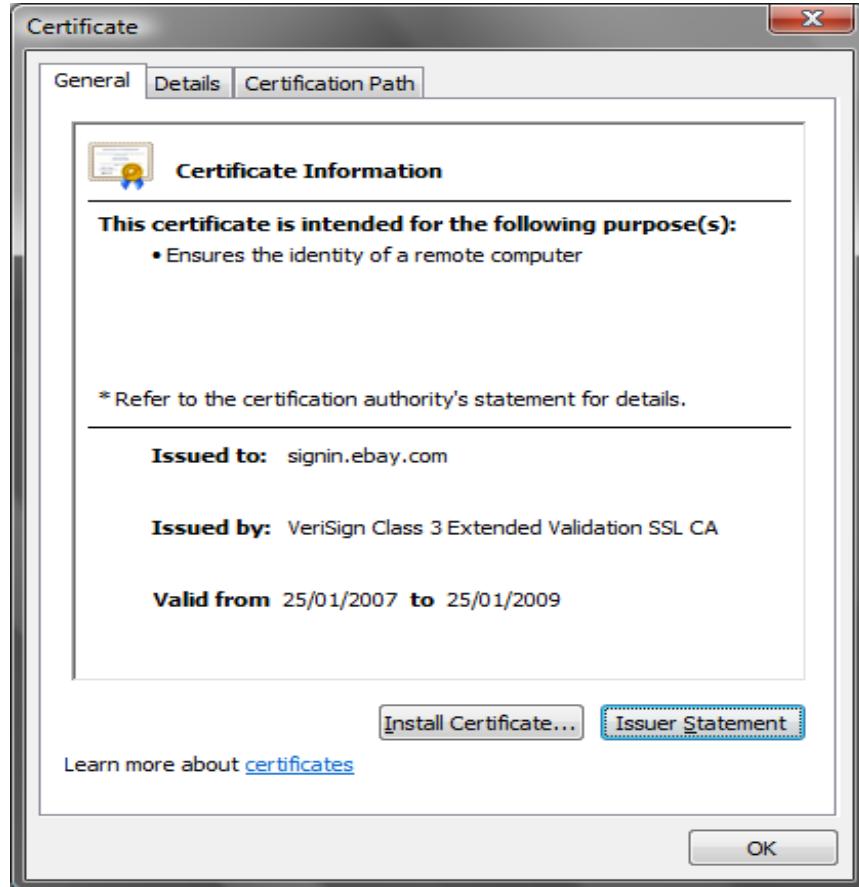
The two main problems with digital certificates are:

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

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



Real or fake?



Author: Prof Bill Buchanan

Real or fake?



Certification path

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

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

File Edit View Favorites Tools Help

Products & Services Solutions Support About VeriSign

UNITED STATES

RESOURCES

PKI Disclosure
Licenses & Approvals
E-Sign
Publications

Home > Repository

VeriSign Relying Party Agreement

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

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

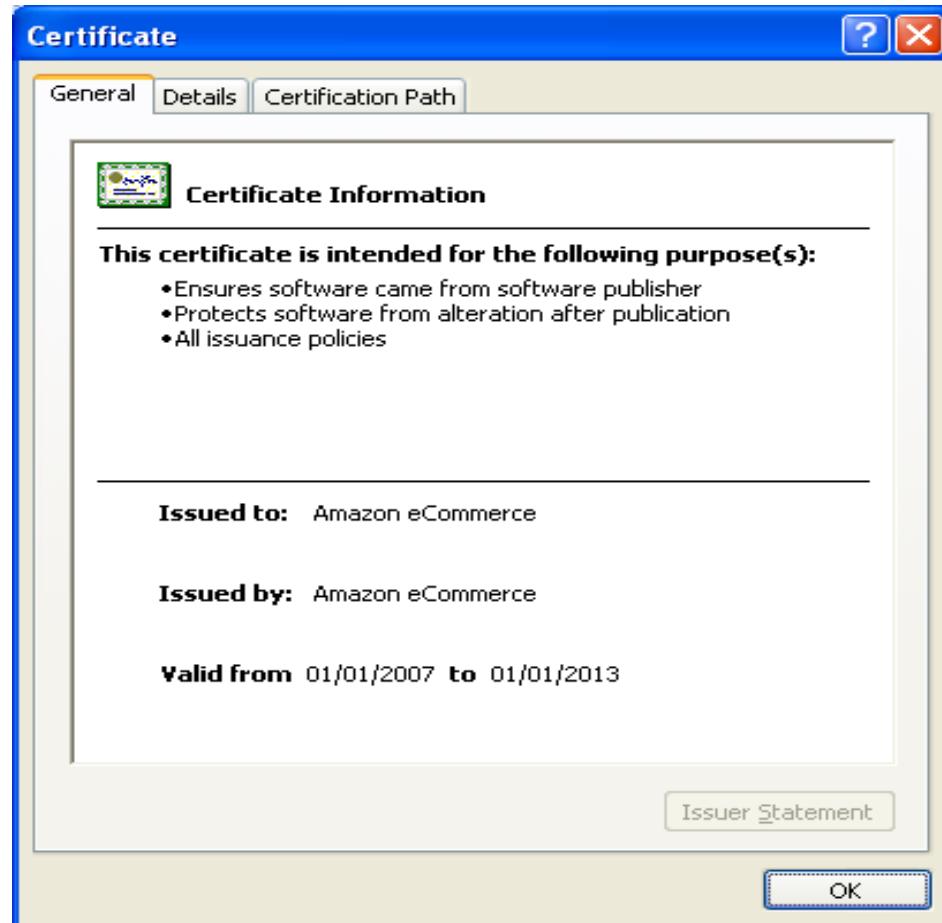
2. Definitions.
"Certificate" or "Digital Certificate" means a message that, at least, states a name or identifier for the Subscriber, contains the Subscriber's public key, identifies the Certificate's serial number, and contains a digital signature of the issuing CA.



Real!

Author: Prof Bill Buchanan

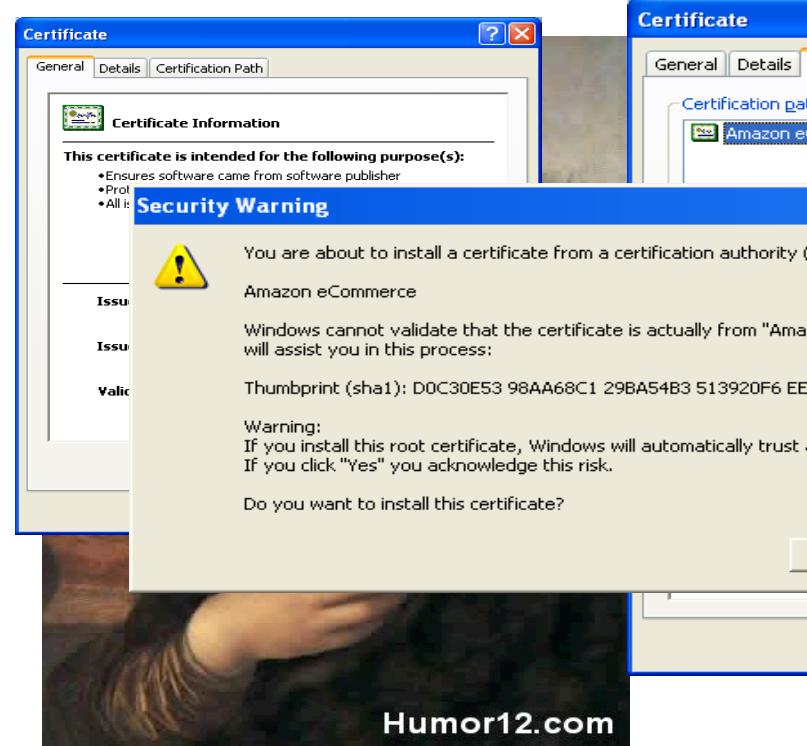
Real or fake?



Real or fake?

Author: Prof Bill Buchanan

Real or fake?



Certificates

Intended purpose: <All>

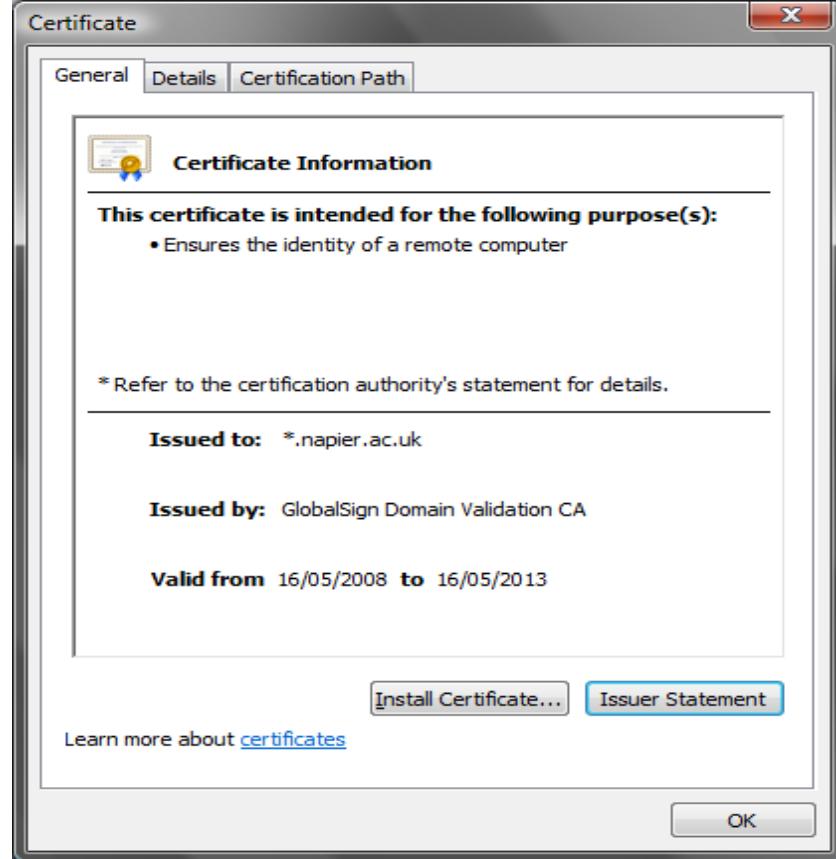
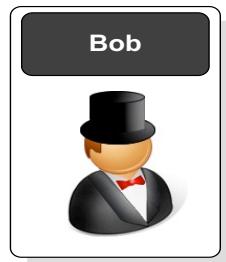
Intermediate Certification Authorities Trusted Root Certification Authorities Trusted Public Key

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

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

Certificate intended purposes

Code Signing View Close



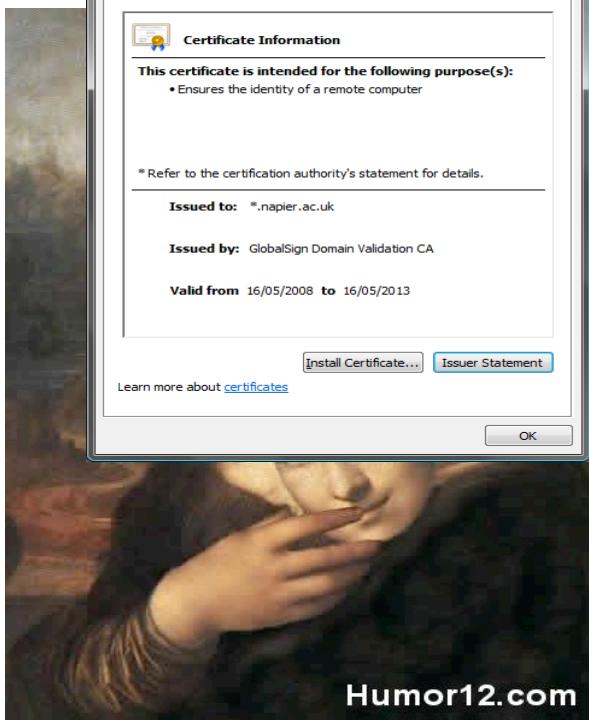
Real or fake?

Author: Prof Bill Buchanan

Real or fake?



Real



Author: Prof Bill Buchanan

Real or fake?

The screenshot shows a Windows Internet Explorer window displaying the GlobalSign (SSL Certificate) Legal Repository. The URL is <http://www.globalsign.com/repository/index.html>. The page title is "GlobalSign (SSL Certificate) Legal Repository - Windows Internet Explorer". The navigation bar includes File, Edit, View, Favorites, Tools, and Help. The main content area features the GlobalSign logo and a menu bar with HOME, Products, Solutions, Partners, and About GlobalSign. A sidebar on the left is titled "About GlobalSign" and lists Company Profile, Company History, Management Team, Press Center, Repository (which is selected), Content Library, International, and Contact Us. The main content area displays the "Repository of Legal Documents & Root Certificates". It lists "Global Sign Root Certificates" and "All Root & Intermediate CA Certificates". Below that is the "GlobalSign Certification Practice Statement (CPS)" with links to "Current version - v6.1 - June 08" and "Previous version - v6.0 - December 07". At the bottom, it mentions "GlobalSign Certification Practice Statement (CPS) for Adobe Certified Document Services (CDS)". The status bar at the bottom of the browser window shows "Waiting" and "Internet | Protected Mode: Off".

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



Bob's Private Key



Bob's Public Key



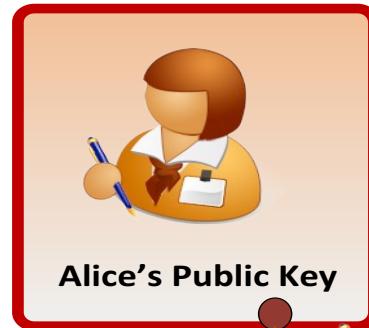
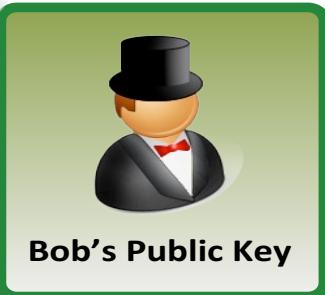
Alice's Public Key



Alice's Private Key



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





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





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



Eve



Trent



MegaCorp



Alice's Public Key



Bob's Private Key



Hello Alice,
Wish you were
here!
- Bob



Bob's Public Key



Alice's Public Key



Alice's Private Key



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



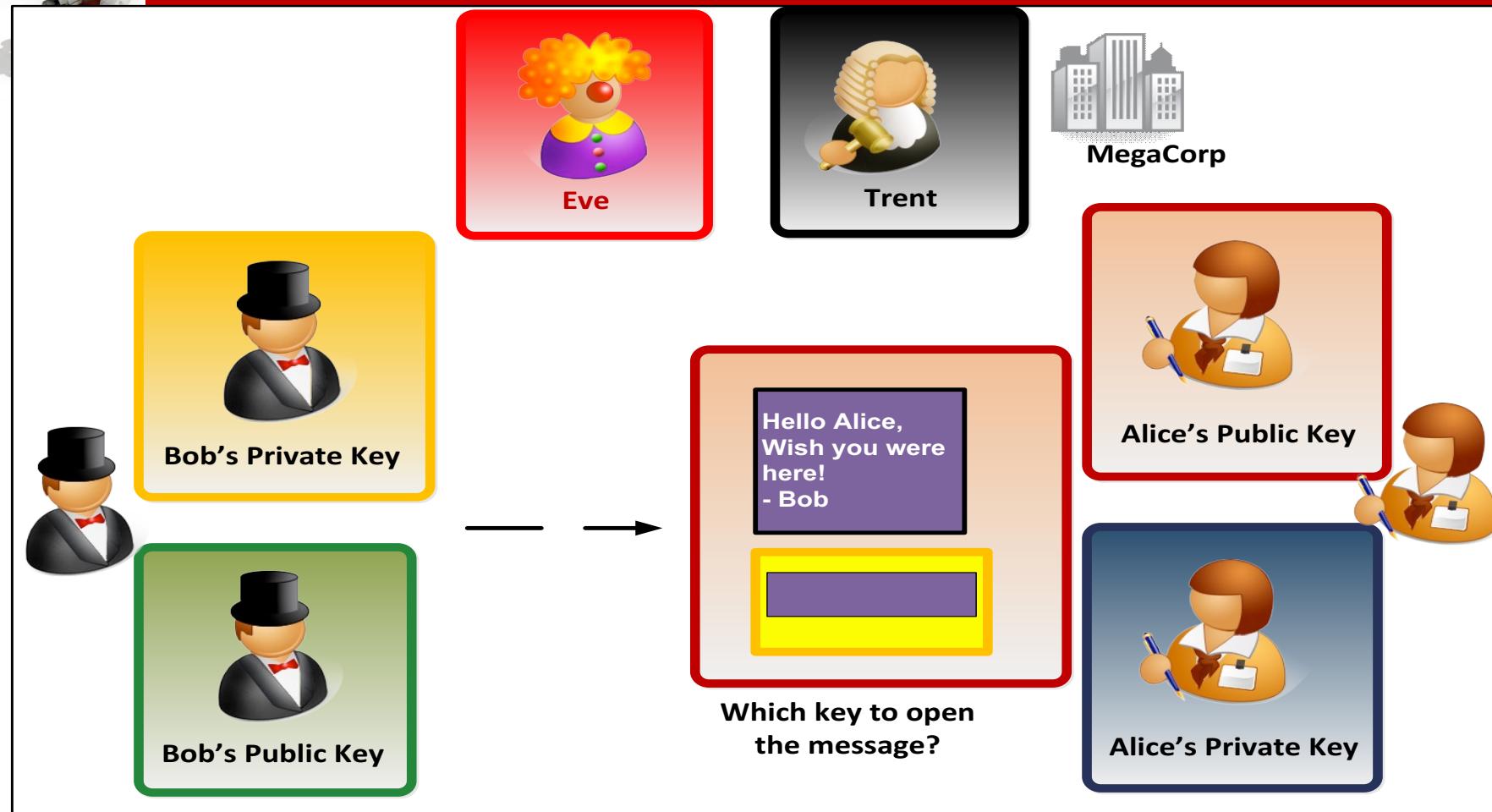


Public key encryption ... secret ... identity ... trust



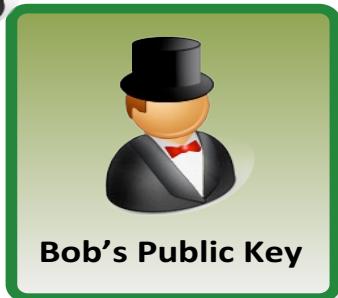


Public key encryption ... secret ... identity ... trust



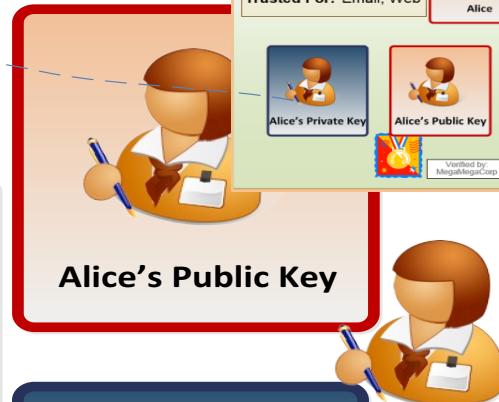


Public key encryption ... secret ... identity ... trust



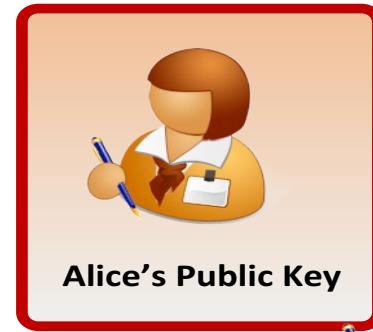
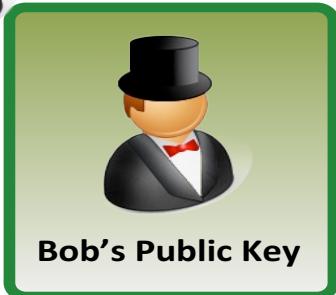
Hello Alice,
Wish you were
here!
- Bob

Which key to open
the message?





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



Hello Alice,
Wish you were
here!
- Bob





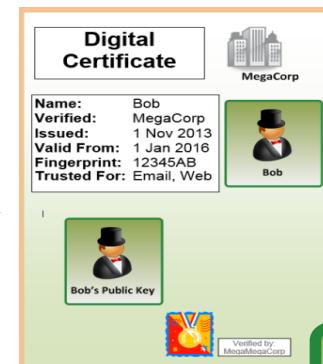
Public key encryption ... secret ... identity ... trust



Bob's Private Key



Bob's Public Key



Hello Alice,
Wish you were
here!
- Bob



Bob's Public Key



Alice's Public Key



Alice's Private Key





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

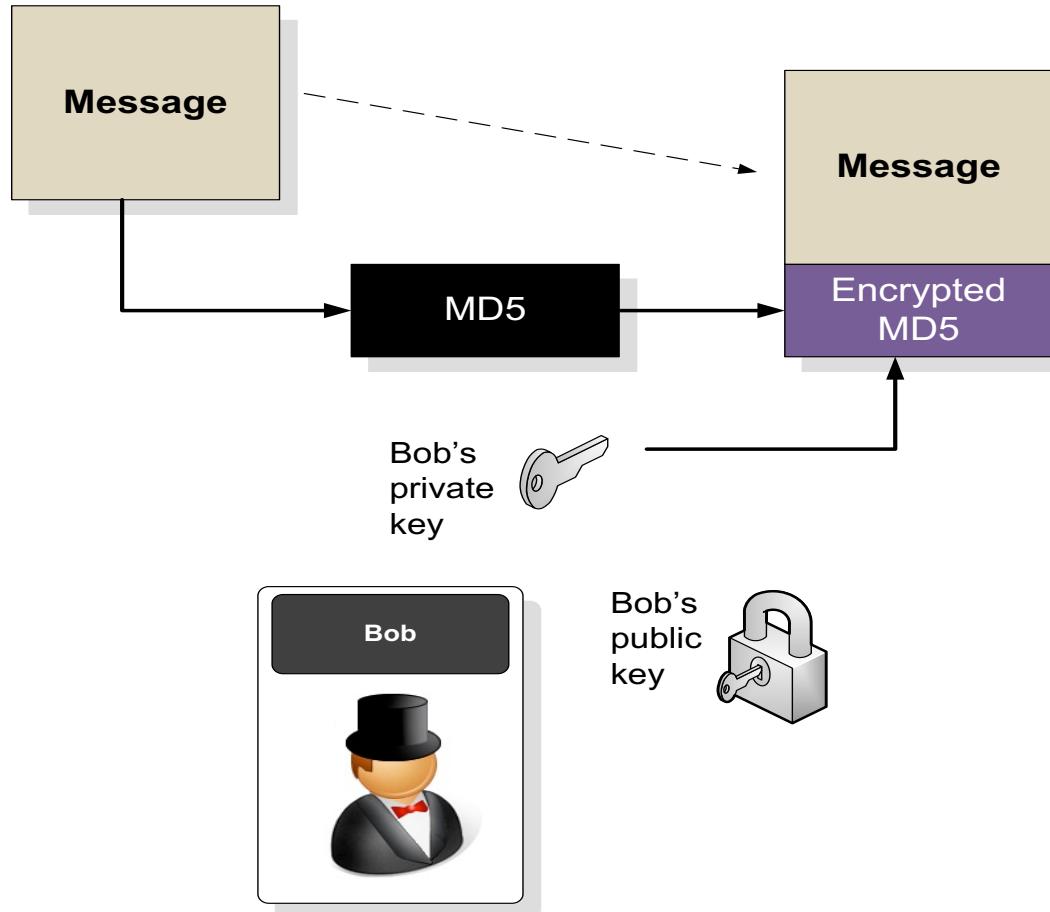


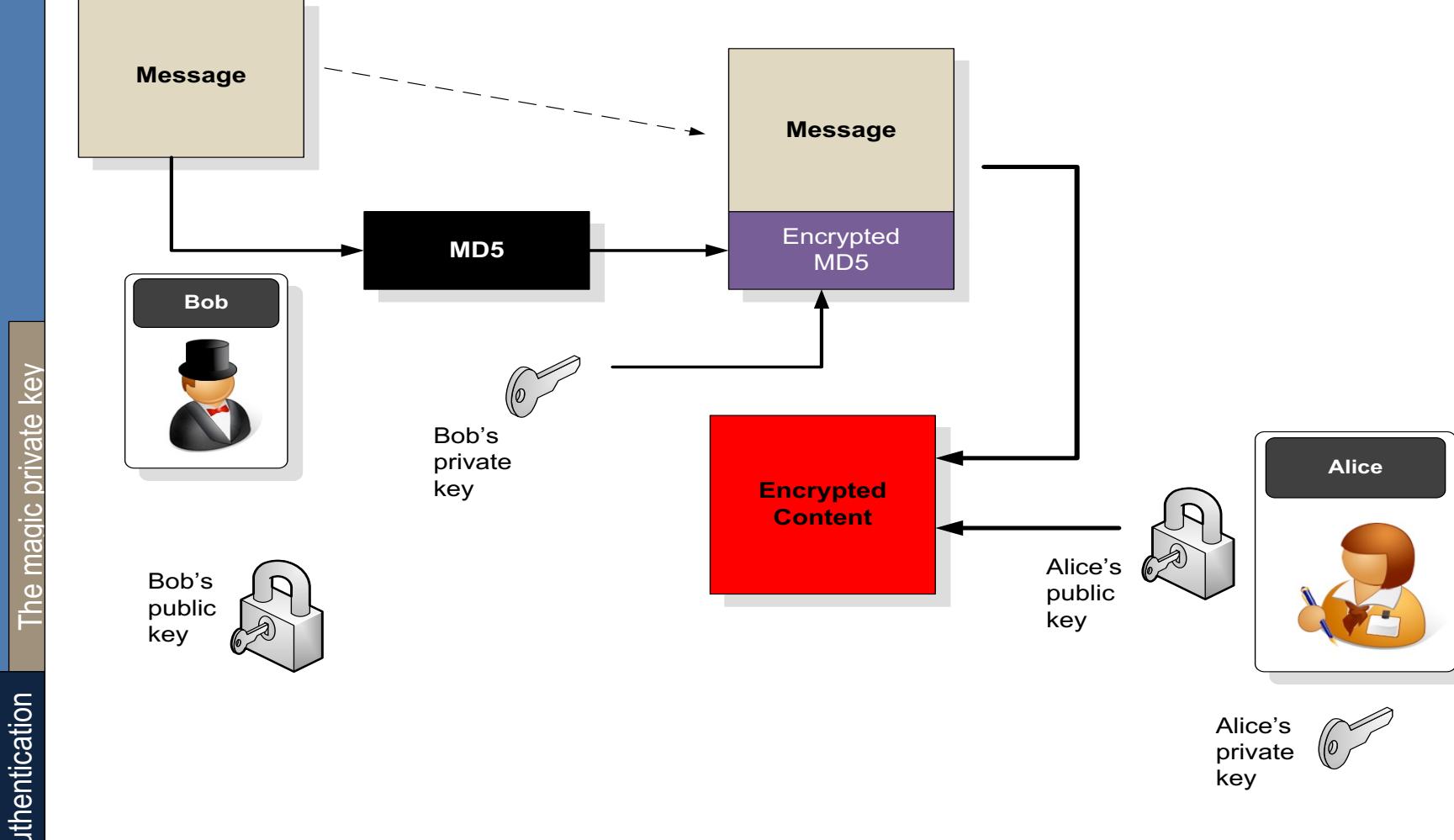
MegaCorp



Hello Alice,
Wish you were
here!
- Bob







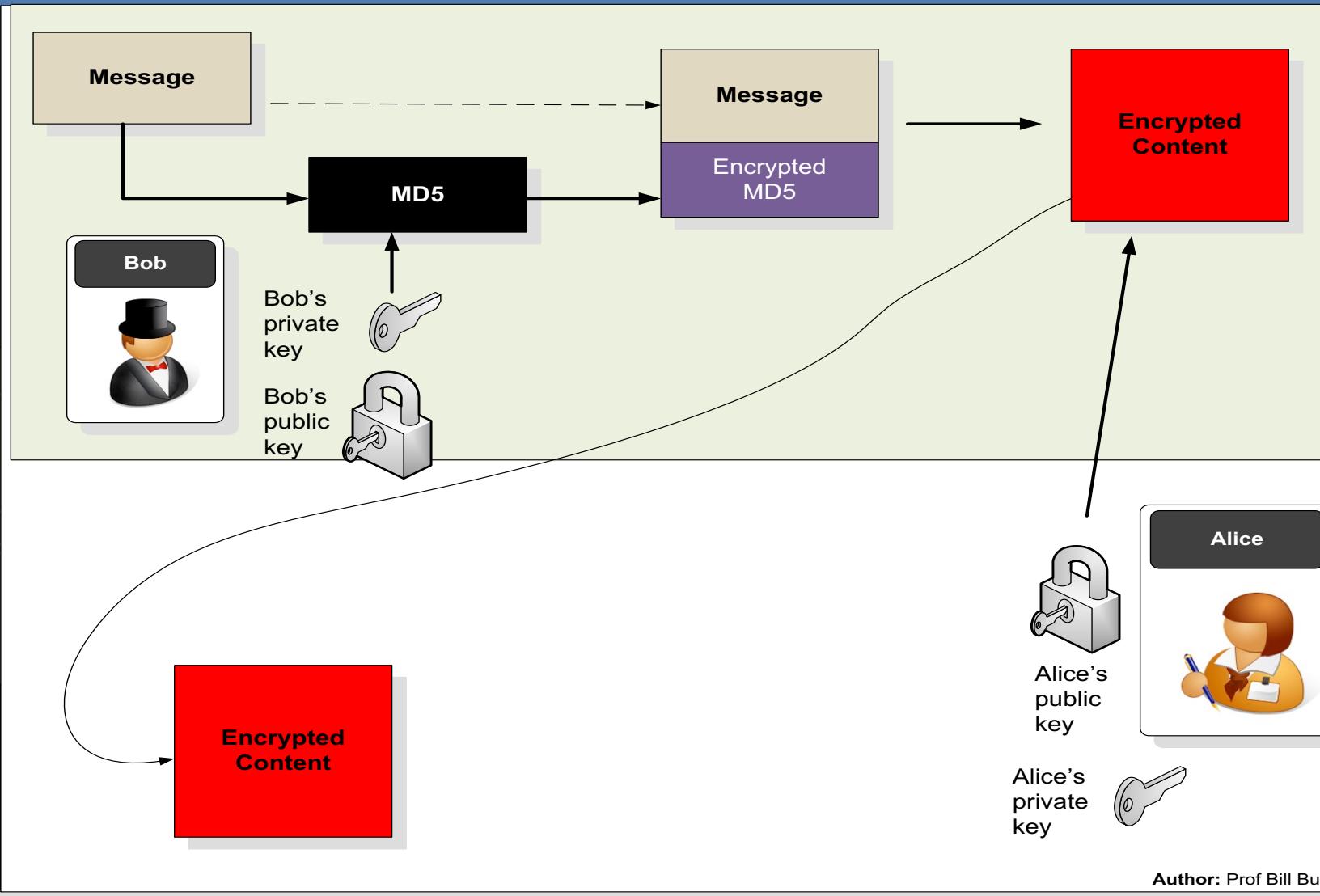
Authentication

Author: Prof Bill Buchanan

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

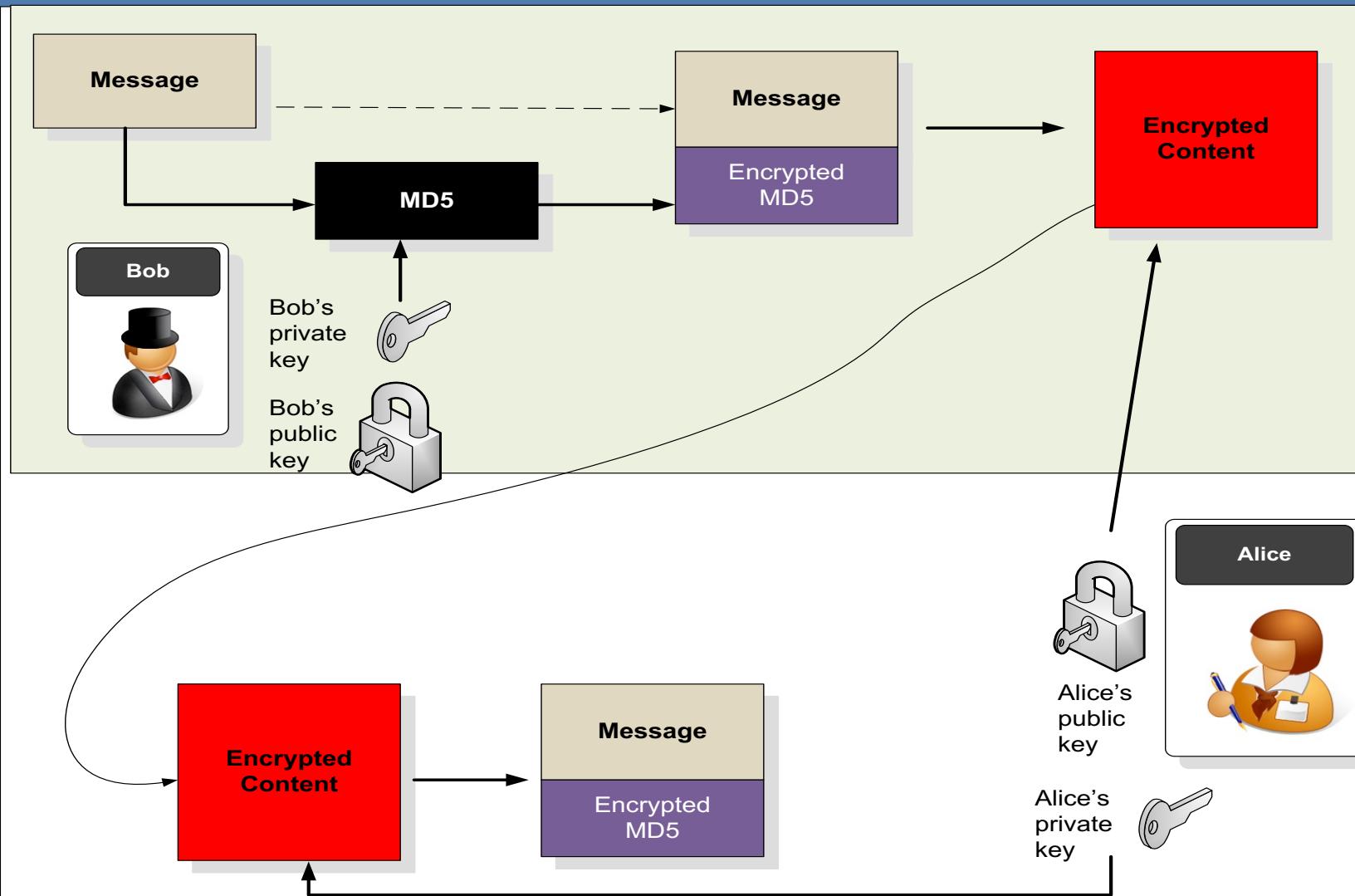
Authentication

The magic private key

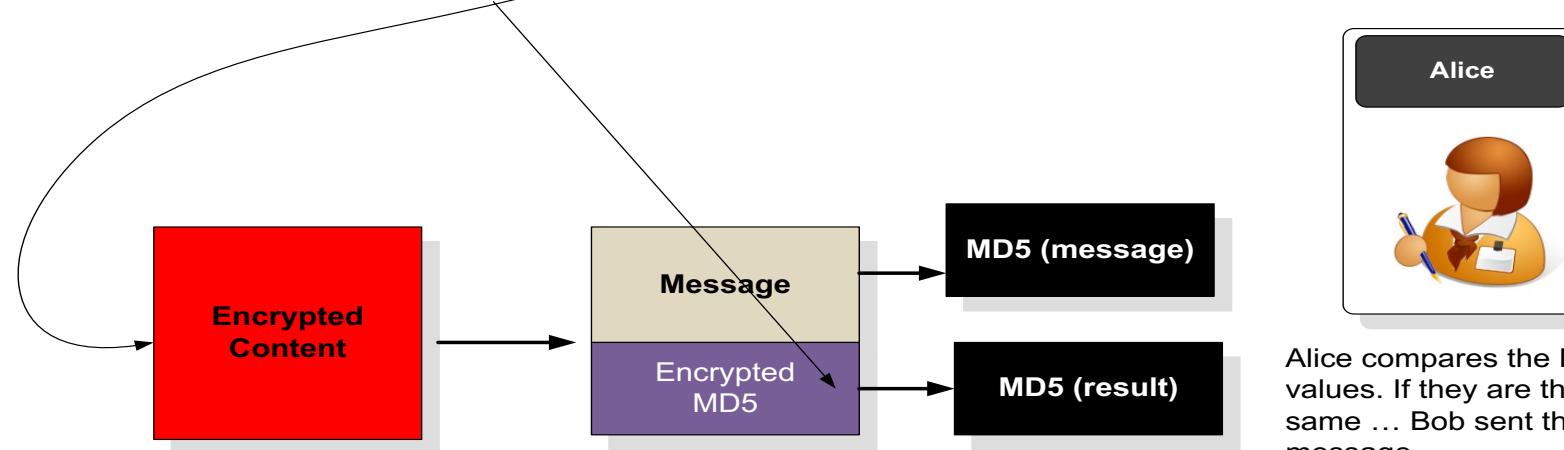
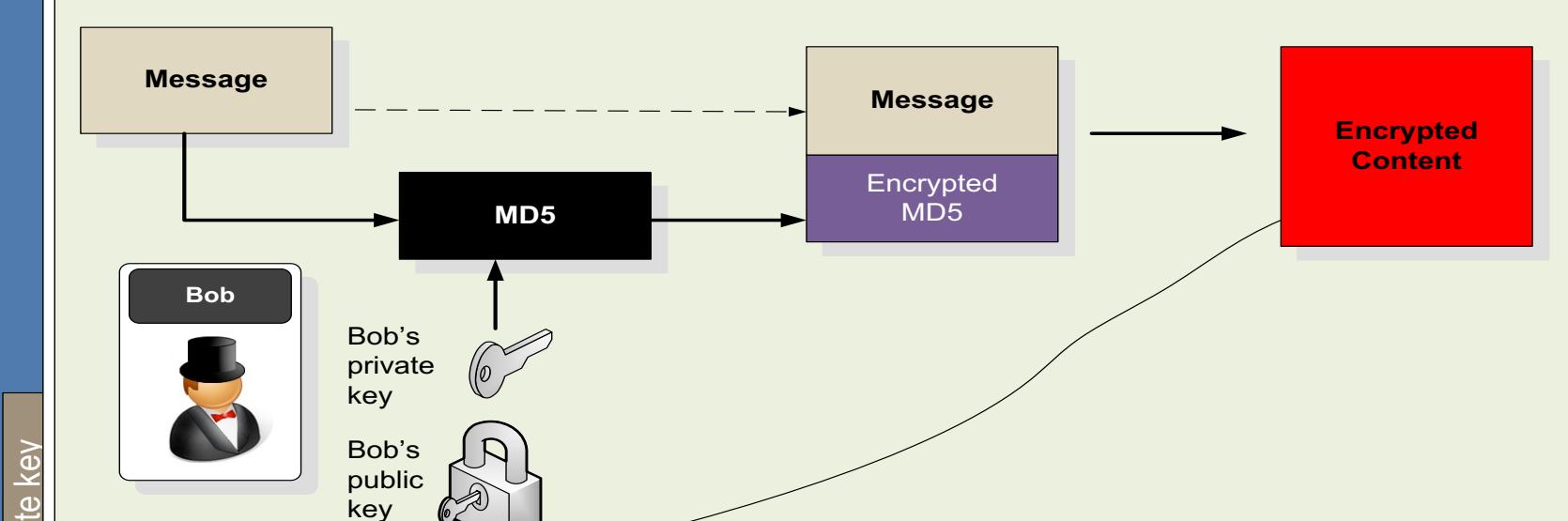


Authentication

The magic private key



Authentication



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>



