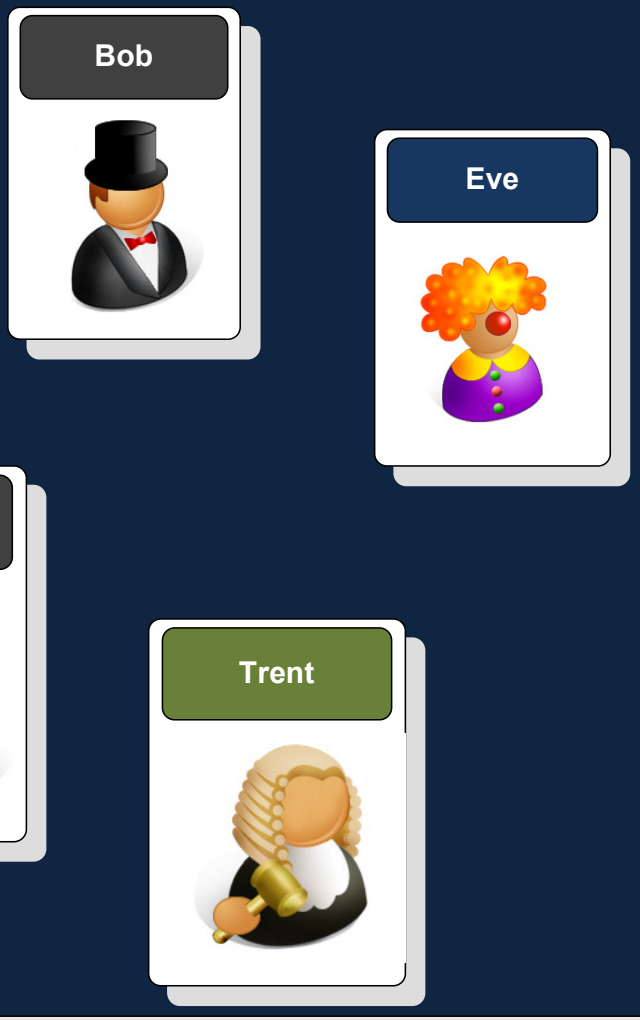
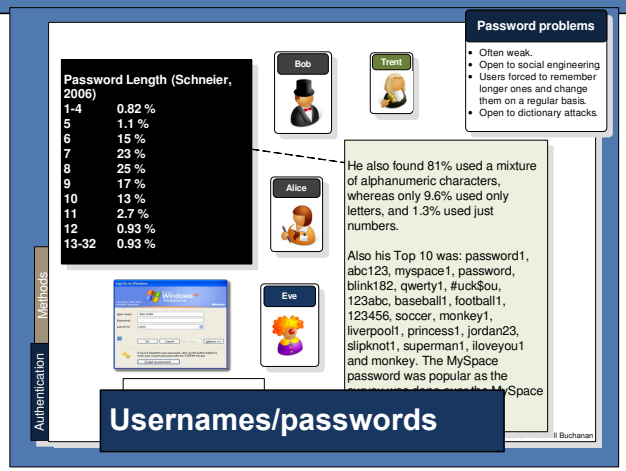
Authentication

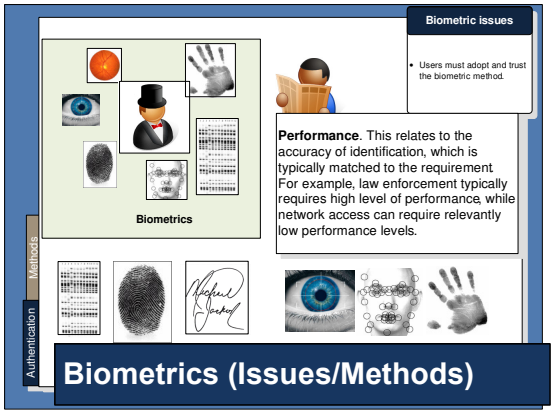
- Introduction
- Methods
- Usernames/passwords
- Biometric issues
- Biometric methods
- Message hash
- Authenticating with private key
- HMAC
- Digital certificates
- Trust
- Cardspace
- Email encryption
- Conclusions



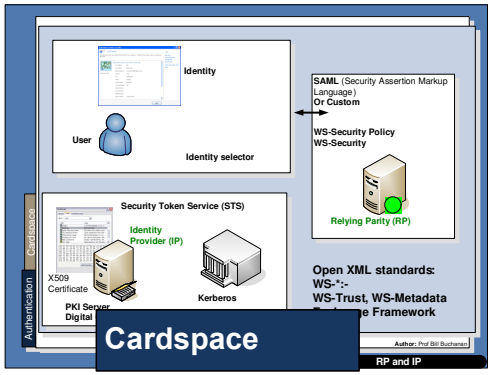
What we're authenticating



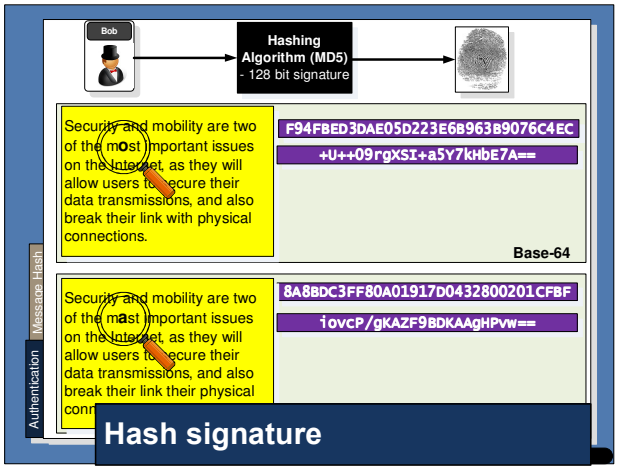
Usernames/passwords



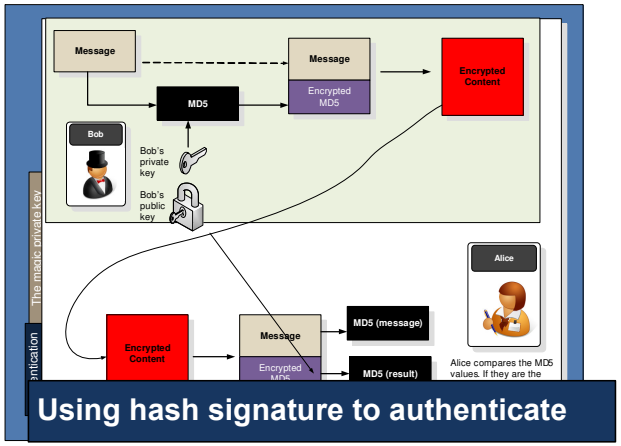
Biometrics (Issues/Methods)



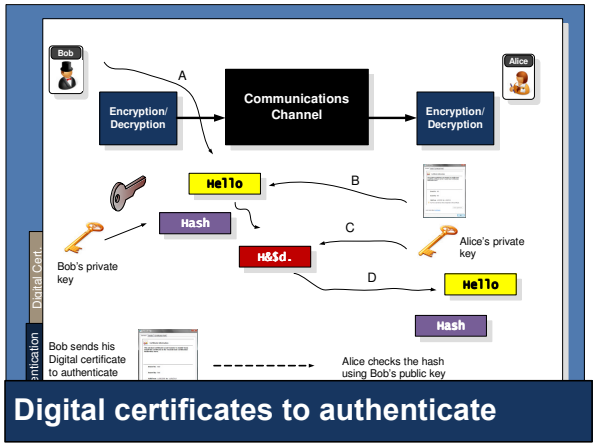
Cardspace



Hash signature



Using hash signature to authenticate



Digital certificates to authenticate

Authentication

Introduction
Methods
Usernames/passwords
Biometric issues
Biometric methods
Message hash
Authenticating with private key
HMAC
Digital certificates
Trust
Cardspace
Email encryption
Conclusions

Introduction

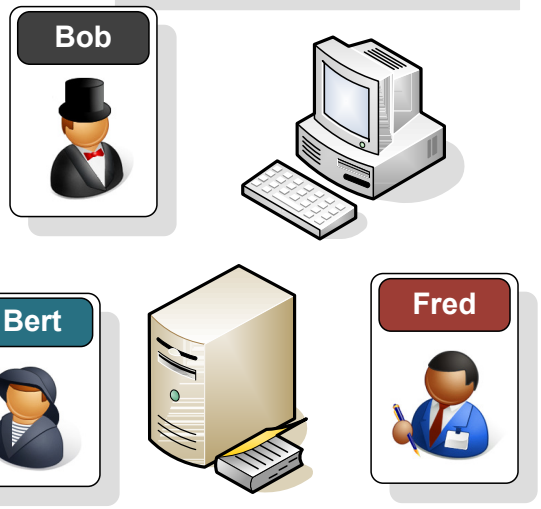
Fundamental principles

Authentication.
Confidence/Assurance.
Privacy/Confidentiality.

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

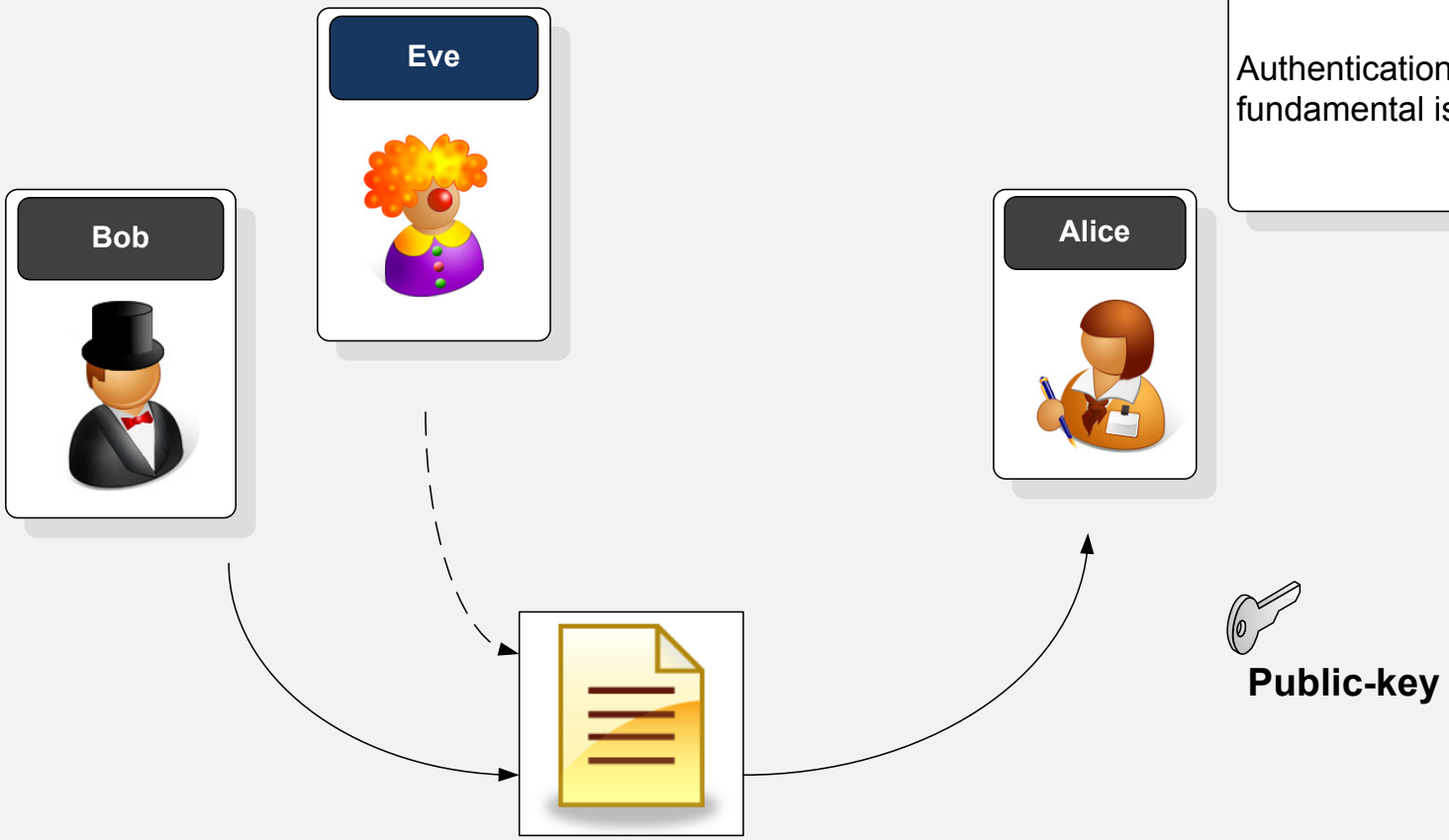
Confidentiality
(Encryption)

Assurance
(Integrity)



Authentication

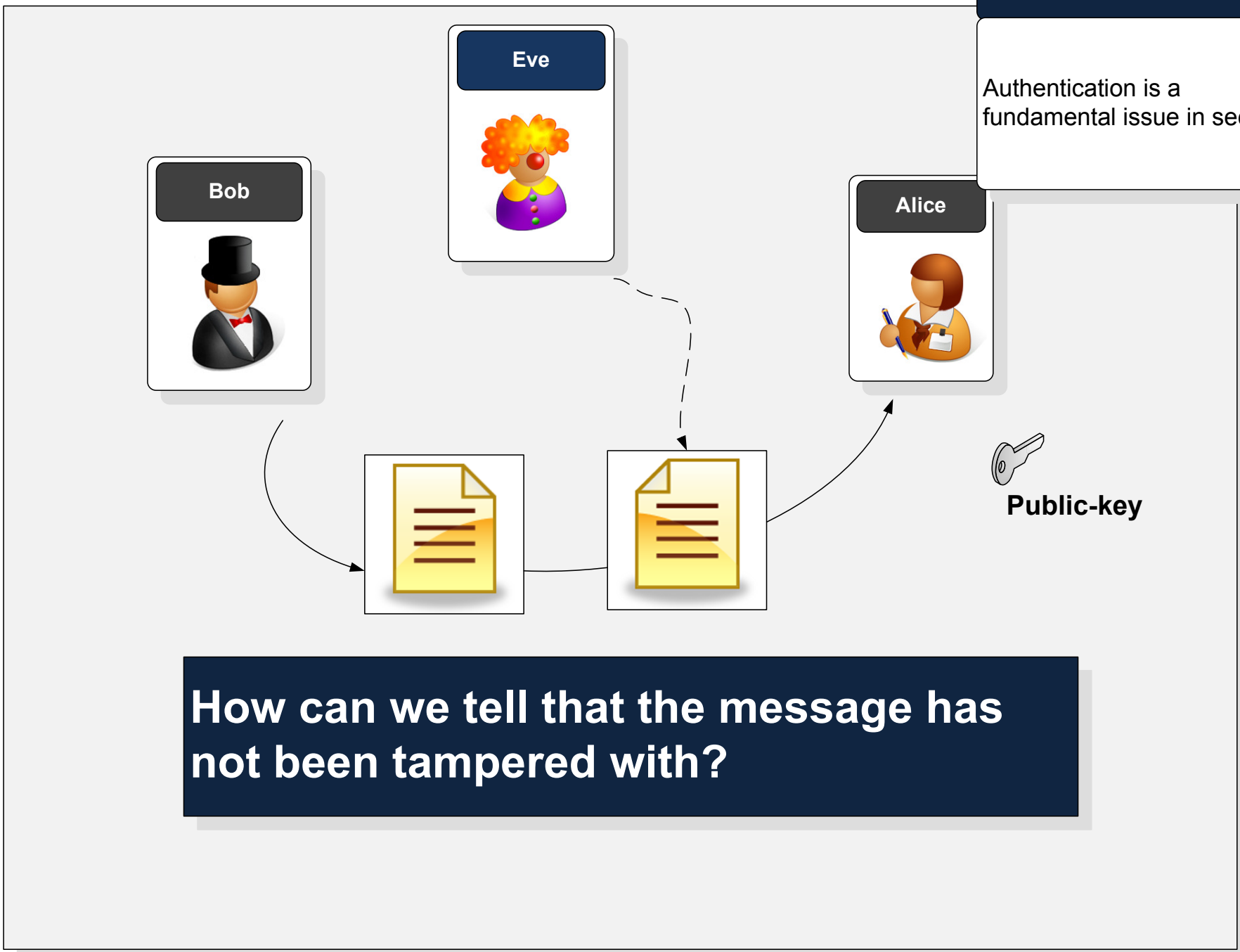
Authentication is a fundamental issue in security.



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

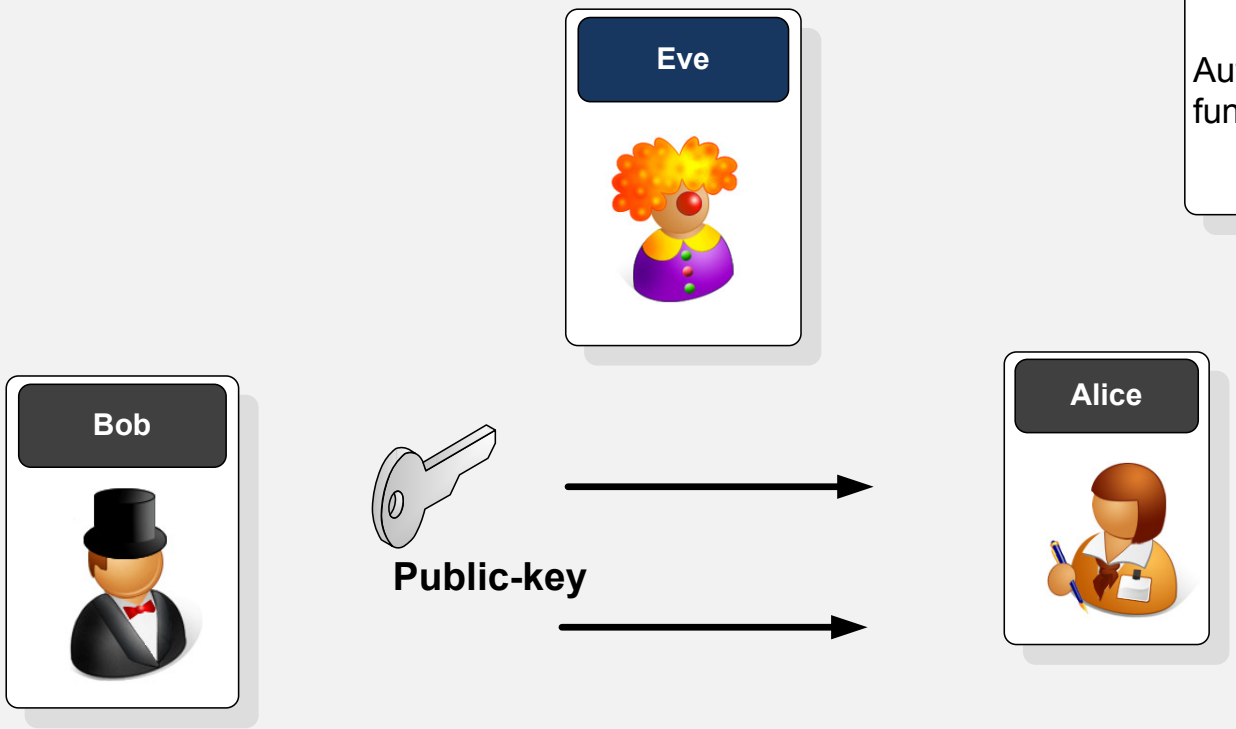
Authentication is a fundamental issue in security.



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

Authentication

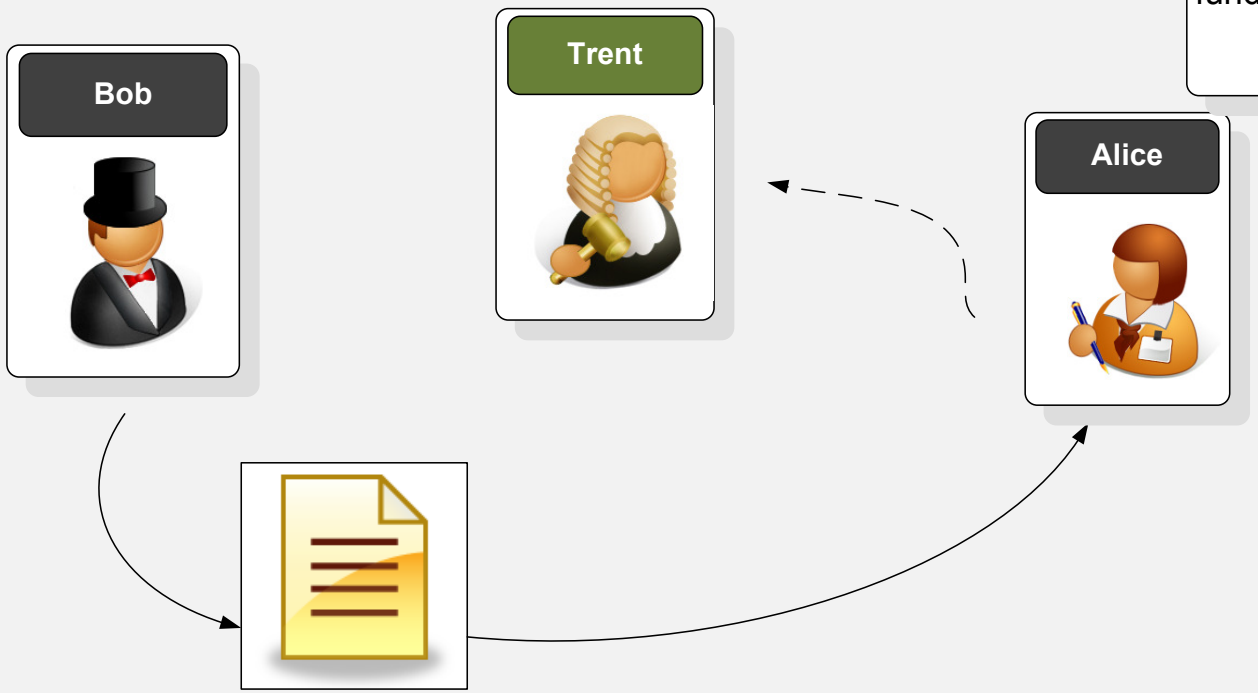
Authentication is a fundamental issue in security.



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.

Authentication

Introduction
Methods
Usernames/passwords
Biometric issues
Biometric methods
Message hash
Authenticating with private key
HMAC
Digital certificates
Trust
Cardspace
Conclusions

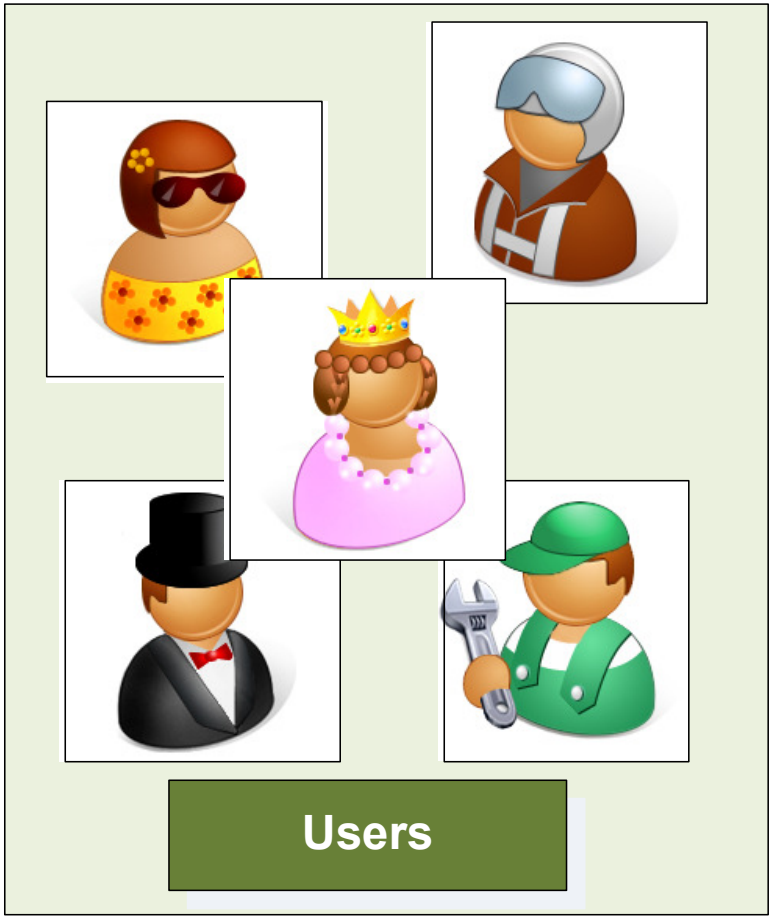
Methods

Authentication

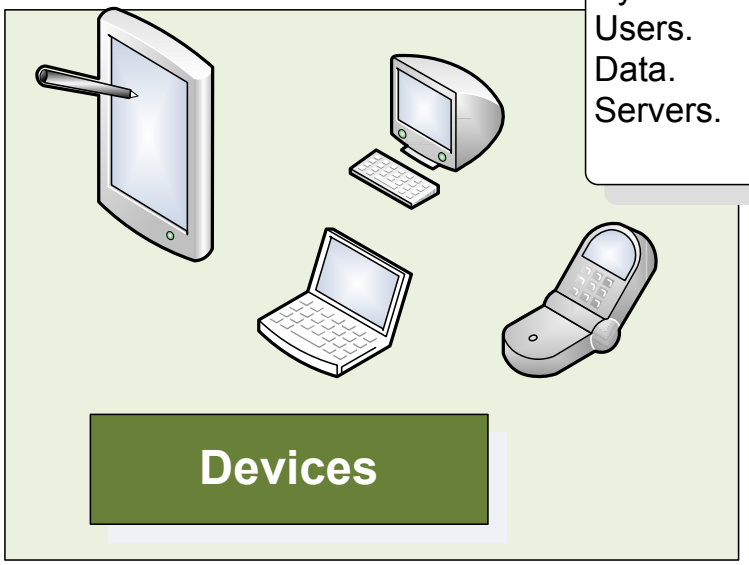
Methods

What to authenticate?

Systems.
Users.
Data.
Servers.

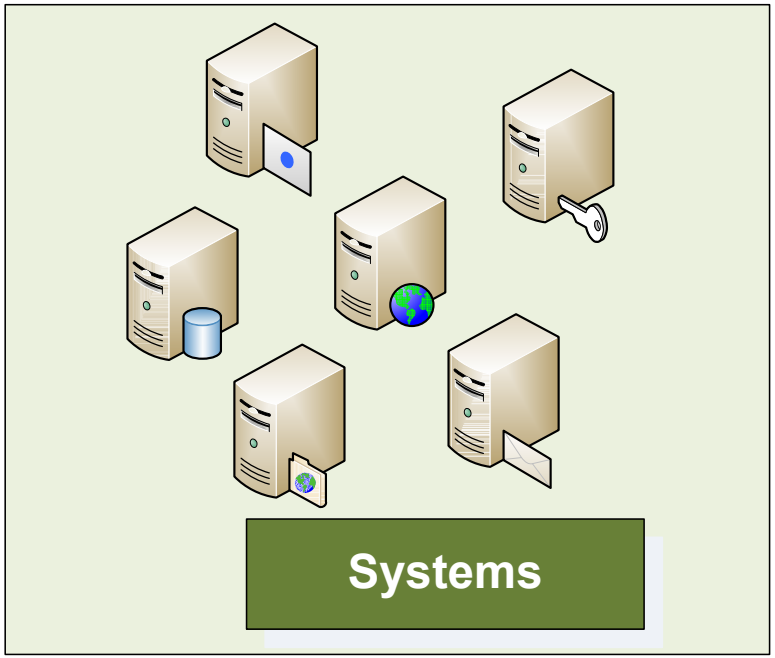


Users



Devices

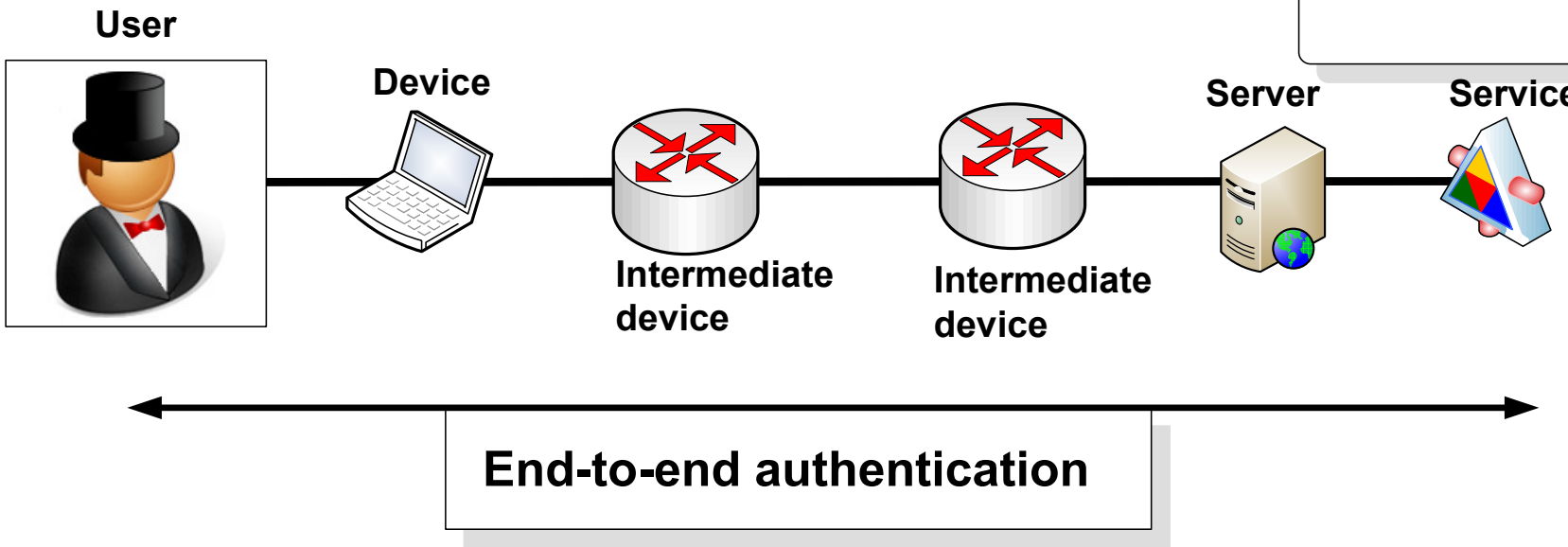
Data

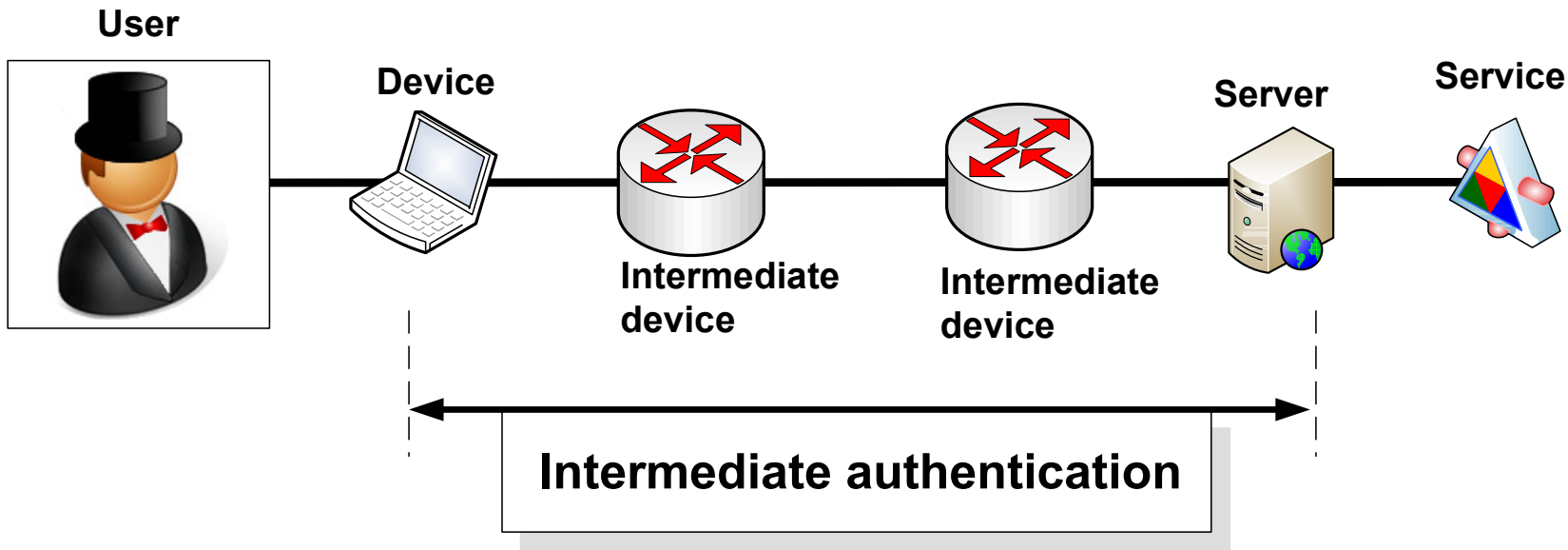


Systems

Where authenticated?

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



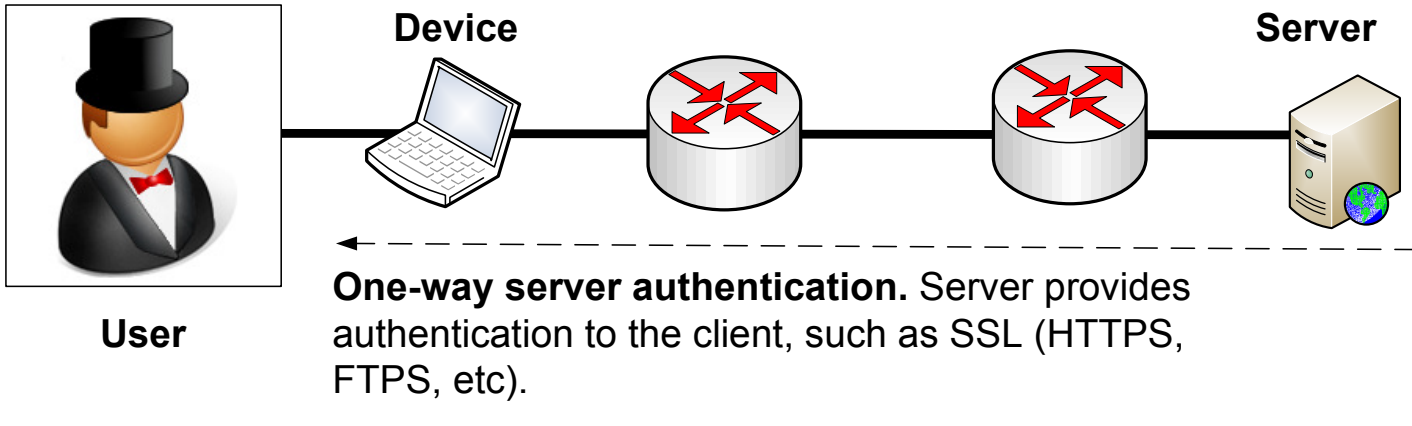


Authentication

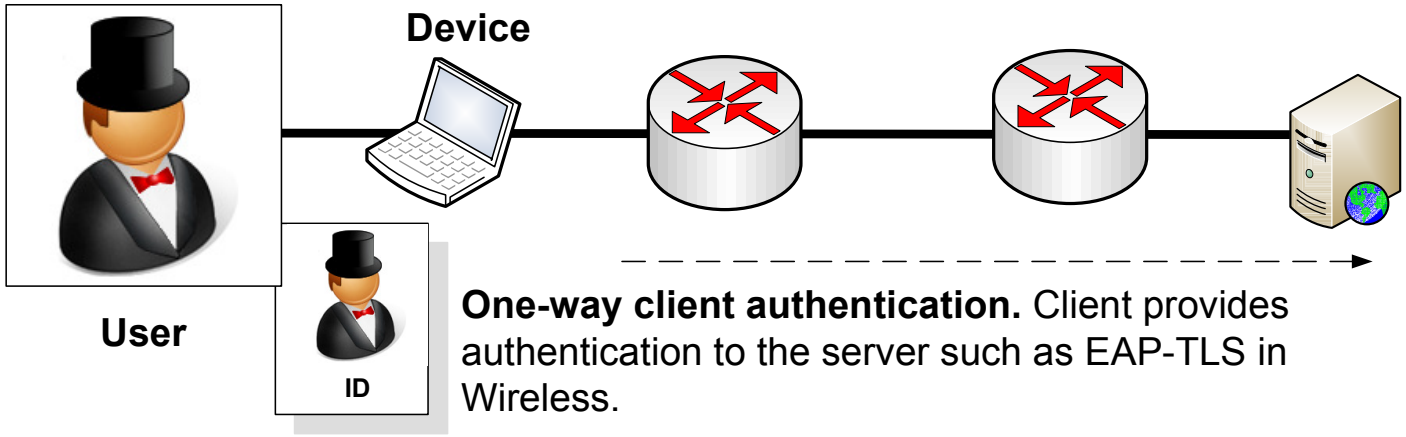
Methods

Authentication type

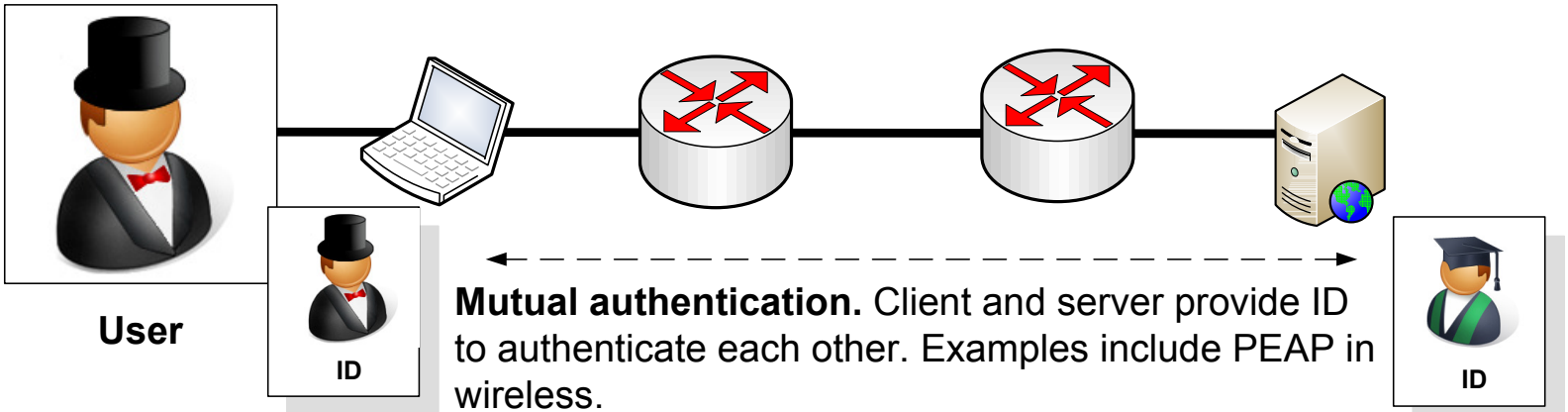
One-way server.
One-way client.
Two-way.



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.

Authentication type

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

User

Device

Intermediate device

Intermediate device

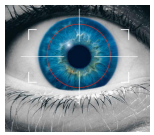
Server

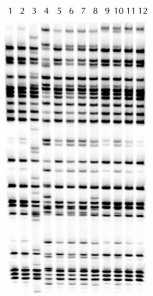
Service

Authentication

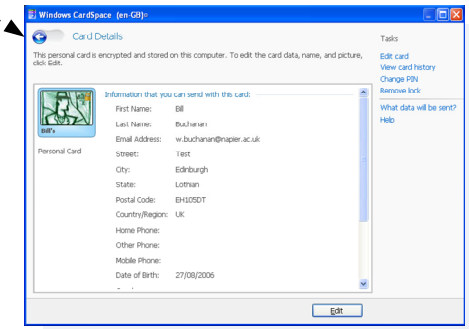
Methods

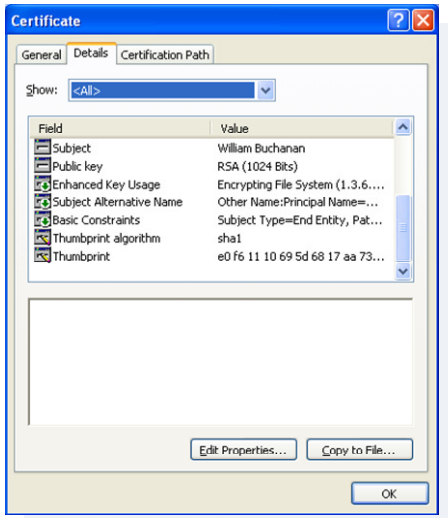
Username/password
Digital Certificate
Token Card
Soft Tokens
Session key
Pass phrase
Biometrics





Device name
Digital Certificate
Pass phrase
MAC address
Encryption key



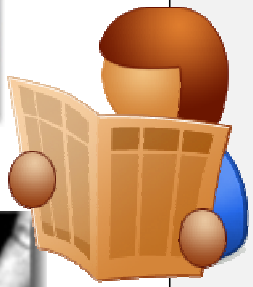


Authentication methods

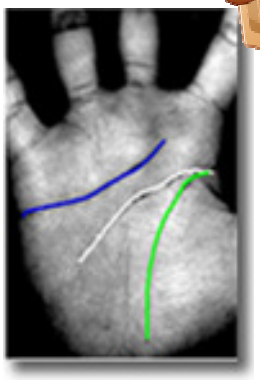
Something you have
Something you know
Something you are

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

Authentication methods

Every authentication method has weaknesses, and, if possible, multiple methods should be used.

Authentication Methods

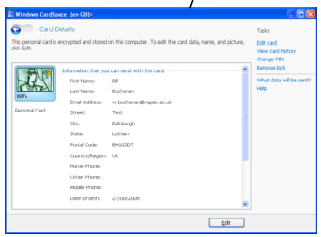
Robustness of authentication

Ease-of-use

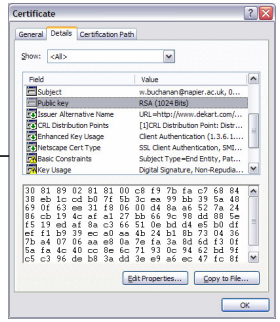
Biometrics

Token Cards/Soft Tokens

S/Key (OTP for terminal login)



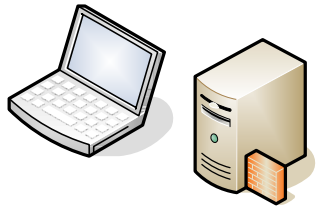
Digital Certificate



Username/password (ageing)

Username/password (static)

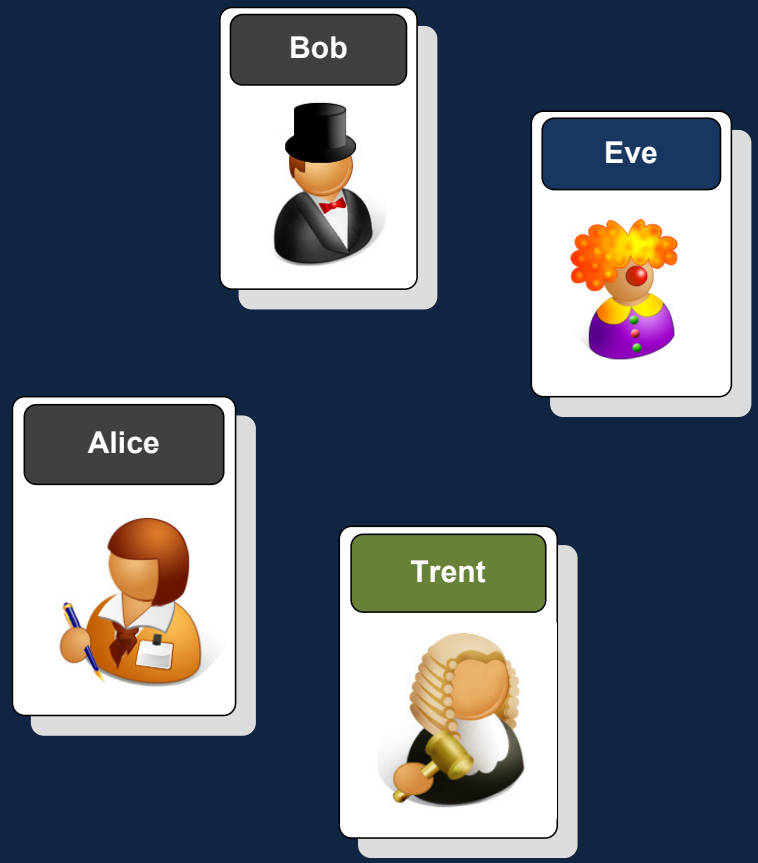
DHCP/Mac address validation



No username/ password

Authentication

- Introduction
- Methods
- Usernames/passwords
- Biometric issues
- Biometric methods
- Message hash
- Authenticating with private key
- HMAC
- Digital certificates
- Trust
- Cardspace
- Conclusions



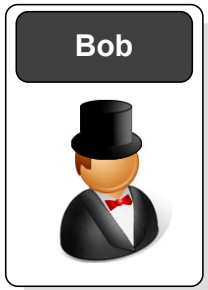
Usernames/Passwords

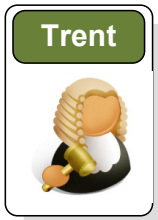
Password problems

- Often weak.
- Open to social engineering.
- Users forced to remember longer ones and change them on a regular basis.
- Open to dictionary attacks.

Top 10 Passwords (Brown, 2006)

10.	'thomas'	(0.99‰)
9.	'arsenal'	(1.11‰)
8.	'monkey'	(1.33‰)
7.	'charlie'	(1.39‰)
6.	'qwerty'	(1.41‰)
5.	'123456'	(1.63‰)
4.	'letmein'	(1.76‰)
3.	'liverpool'	(1.82‰)
2.	'password'	(3.780‰)
1.	'123'	(3.784‰)





Suffer from many problems, especially that the full range of available passwords is hardly ever used.

For example a 10 character password has 8 bits per character, thus it there should be up to 80 bits used for the password, which gives 1,208,925,819,614,629,174,706,176 possible permutations.

Unfortunately the actual number of useable passwords is typically less than 1.3 bits per character, such as the actual bit size is less than **13 bits** (8192).

Password problems

- Often weak.
- Open to social engineering.
- Users forced to remember longer ones and change them on a regular basis.
- Open to dictionary attacks.

Password Length (Schneier, 2006)

1-4	0.82 %
5	1.1 %
6	15 %
7	23 %
8	25 %
9	17 %
10	13 %
11	2.7 %
12	0.93 %
13-32	0.93 %

Bob

Trent

Alice

Eve

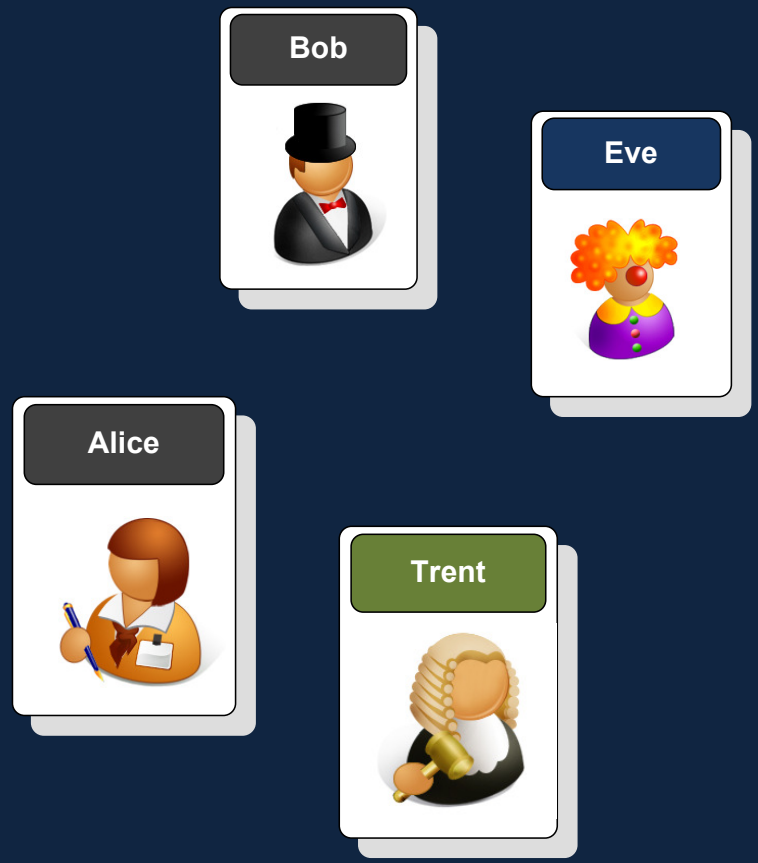
He also found 81% used a mixture of alphanumeric characters, whereas only 9.6% used only letters, and 1.3% used just numbers.

Also his Top 10 was: password1, abc123, myspace1, password, blink182, qwerty1, #uck$ou, 123abc, baseball1, football1, 123456, soccer, monkey1, liverpool1, princess1, jordan23, slipknot1, superman1, iloveyou1 and monkey. The MySpace password was popular as the survey was done over the MySpace domain.

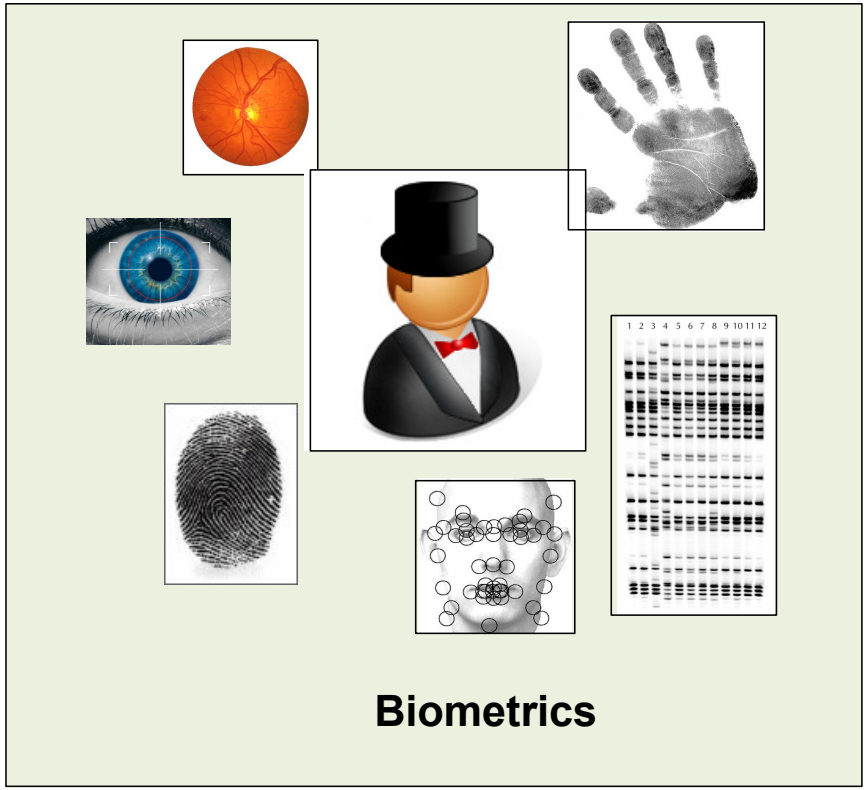
Name of dog 21%
Favourite colour 17%
Mother's maiden name 9%

Authentication

Introduction
Methods
Usernames/passwords
Biometric issues
Biometric methods
Message hash
Authenticating with private key
HMAC
Digital certificates
Trust
Cardspace
Conclusions

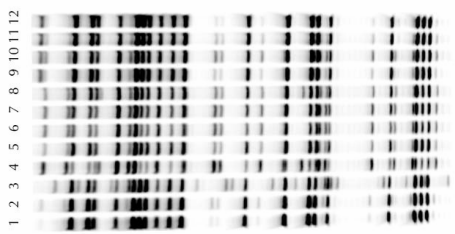


Biometrics Issues

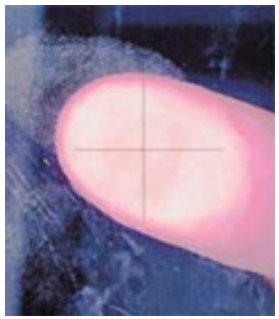


Biometric issues

- Users must adopt and trust the biometric method.

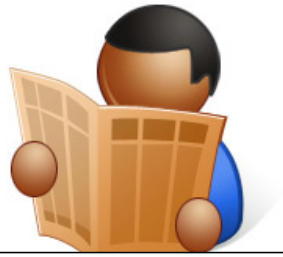


Acceptability
This relates to the acceptable of the usage by users. For example, iris scanning and key stroke analysis are not well accepted by users, while hand scans are fairly well accepted. The acceptability can also vary in application domains, such as fingerprint analysis is not well liked in medical applications, as it requires physical contact, but hand scans are fairly well accepted, as they are contactless.

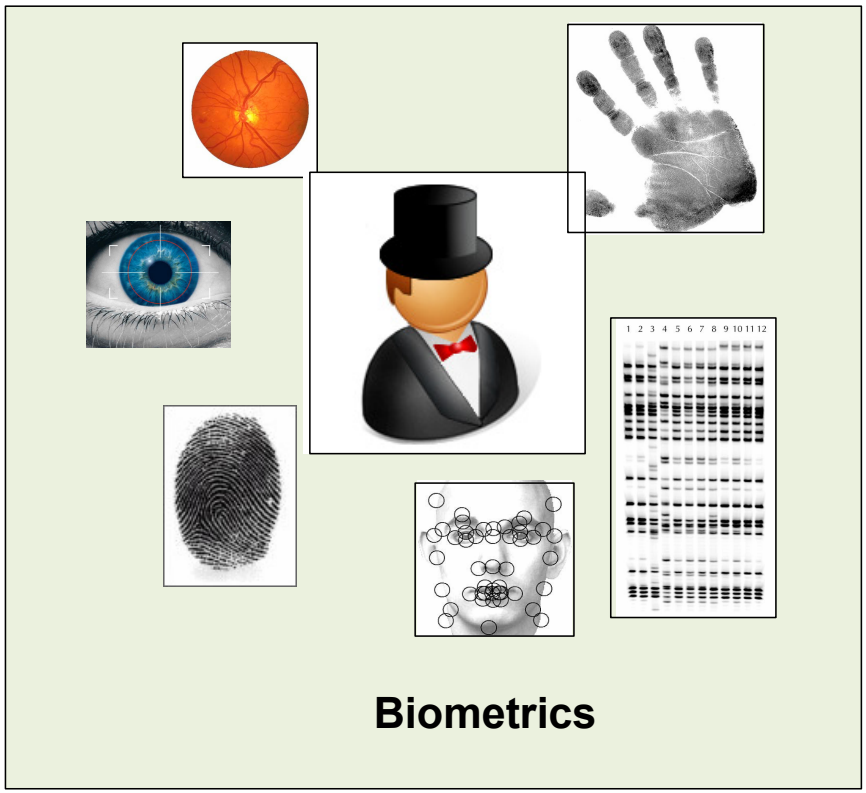


Biometric issues

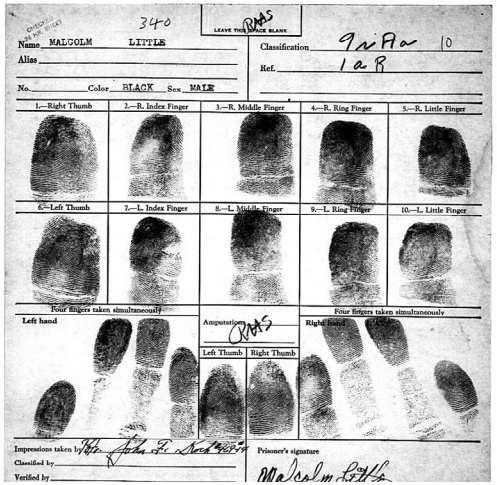
- Users must adopt and trust the biometric method.

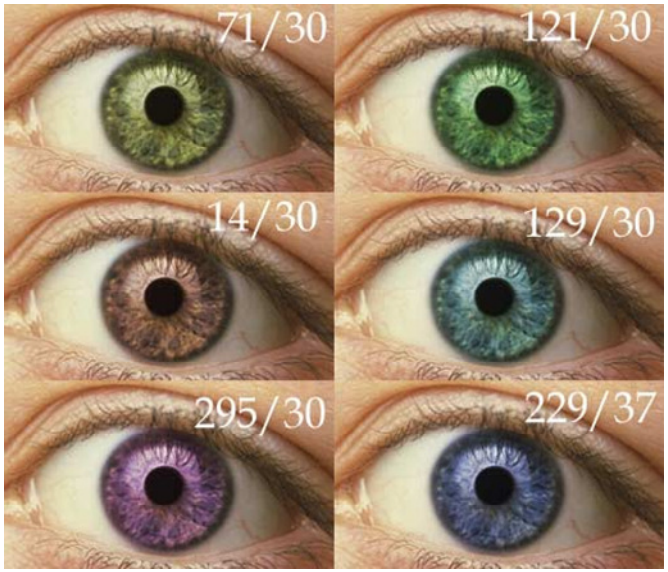


Distinctiveness. This relates to the characteristics that make the characteristic unique.



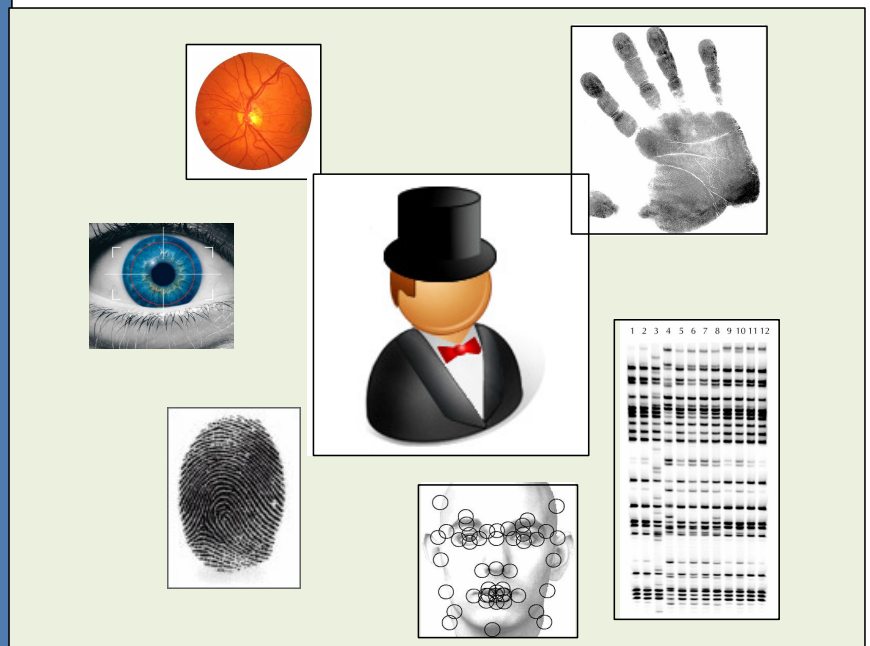
Biometrics





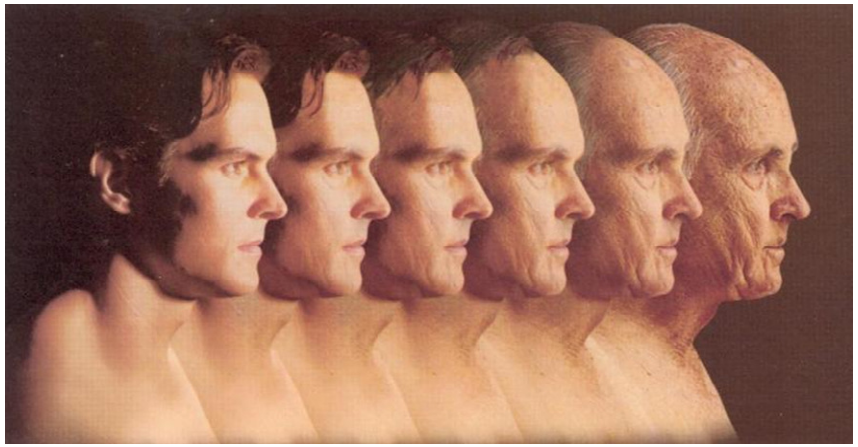
Biometric issues

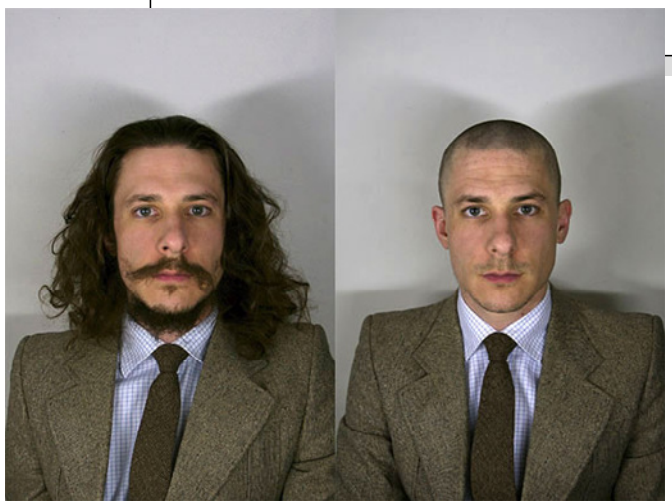
- Users must adopt and trust the biometric method.



Biometrics

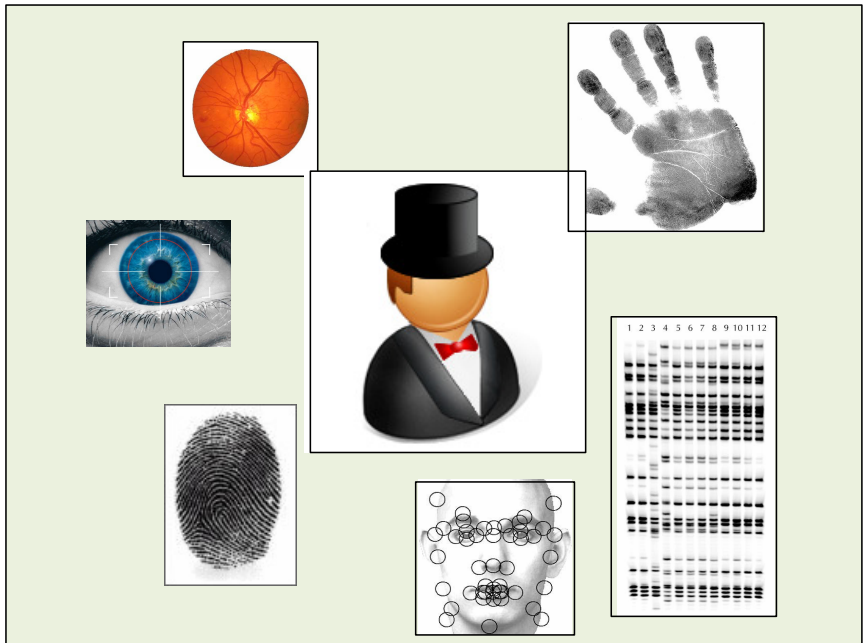
Permanence. This relates to how the characteristic changes over time. Typical problems might be changes of hair length, over a short time, and, over a long time, skin flexibility.





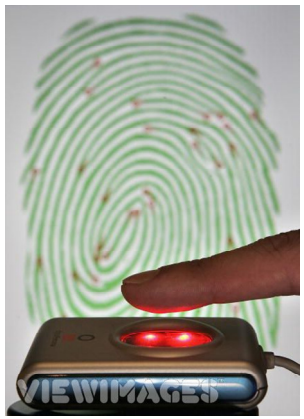
Biometric issues

- Users must adopt and trust the biometric method.



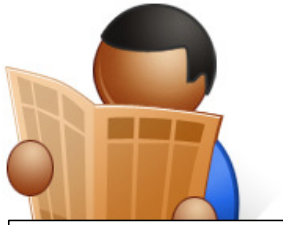
Biometrics

Collectability. This relates to the manner of collecting the characteristics, such as for remote collection (non-obtrusive collection), or one which requires physical or local connection to a scanning machine (obtrusive collection).

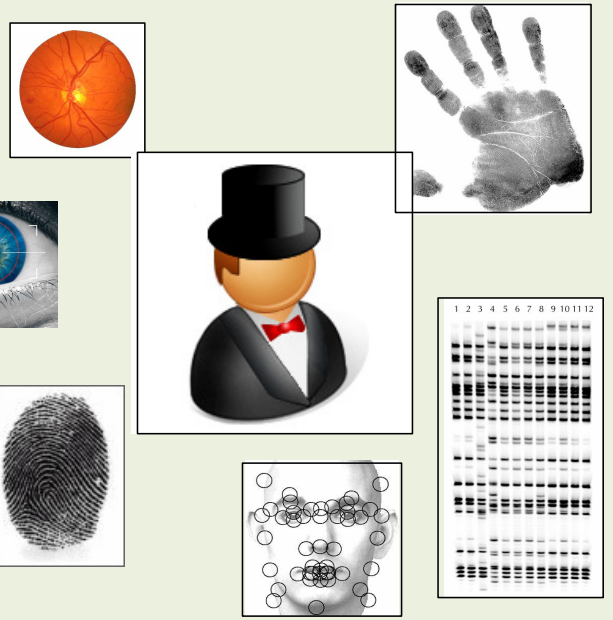


Biometric issues

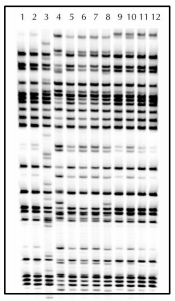
- Users must adopt and trust the biometric method.

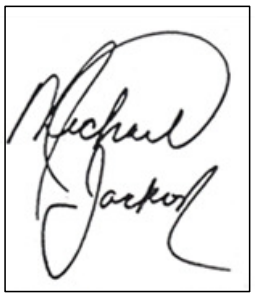


Performance. This relates to the accuracy of identification, which is typically matched to the requirement. For example, law enforcement typically requires high level of performance, while network access can require relevantly low performance levels.

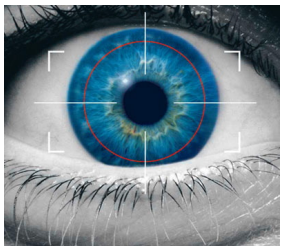


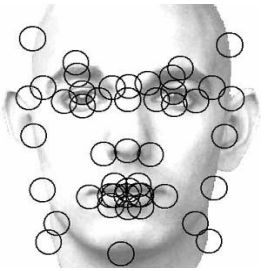
Biometrics





Law enforcement methods

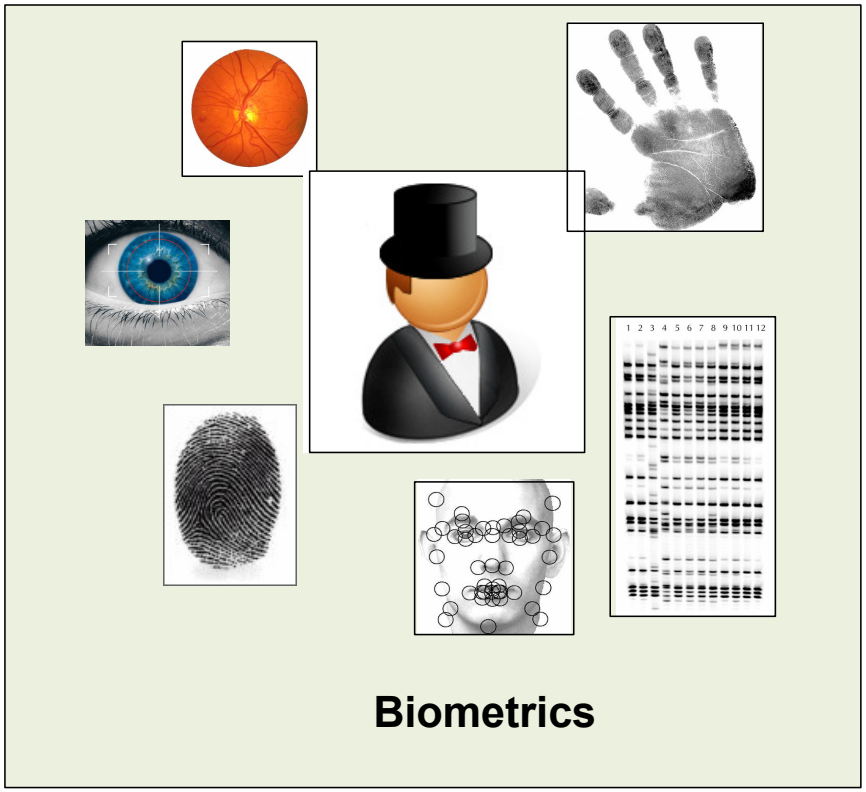




Host/network access

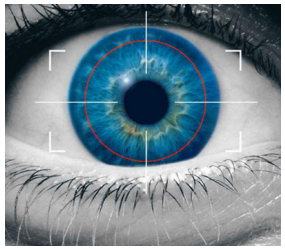
Biometric issues

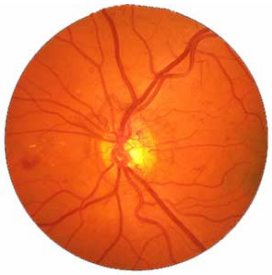
- Users must adopt and trust the biometric method.

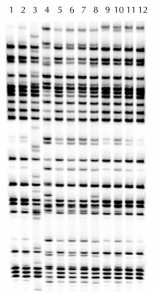


Biometrics

Universality. This relates to human features which translate to physical characteristics such as finger prints, iris layout, vein structure, DNA, and so on.

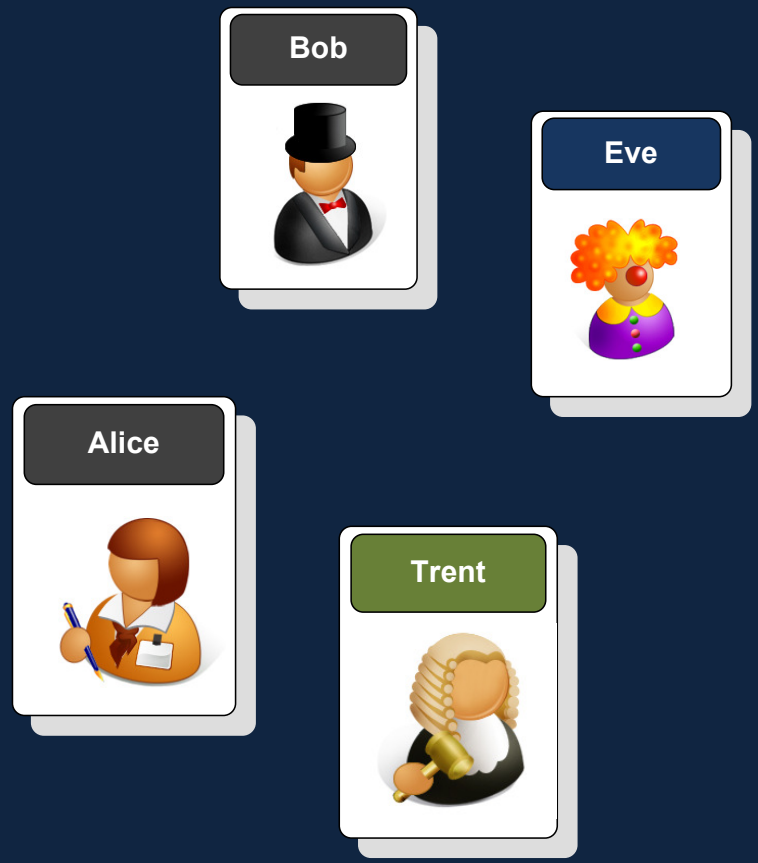






Authentication

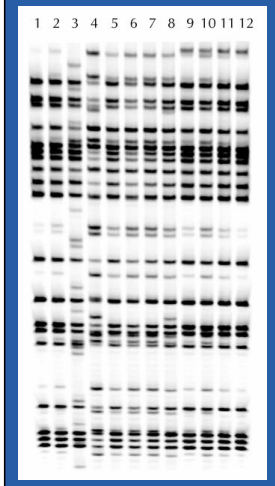
Introduction
Methods
Usernames/passwords
Biometric issues
Biometric methods
Message hash
Authenticating with private key
HMAC
Digital certificates
Trust
Cardspace
Conclusions



Biometrics Methods

DNA/Fingerprints

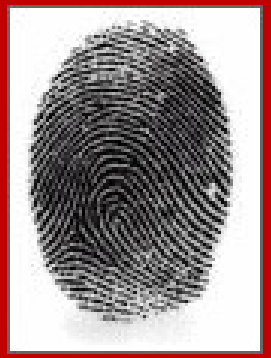
Authentication Methods

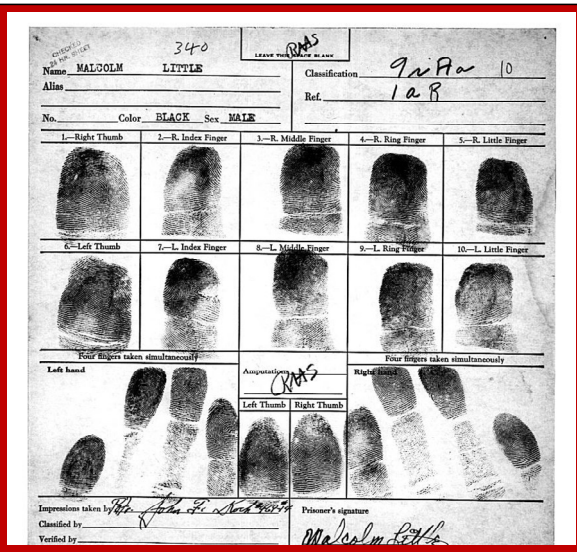


DNA

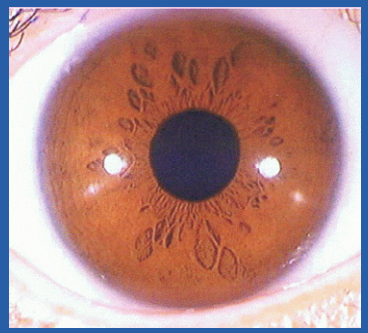
DNA. This involves matching the DNA of the user, and is obviously one of the best methods of authentication, but has many **legal/moral issues**. It is typically only used in law enforcement applications, and also suffers from the fact that other information can be gained from DNA samples such as medical disorders. It is also **costly** as a biometric method, but it is by far the **most reliable**. Also the time to sample and analyze is **fairly slow**, taking at least 10 minutes to analyze. Finally, the methods used to get the DNA, such as from a tissue or blood sample can be fairly **evasive**, but newer methods use hair and skin samples, which are less evasive.

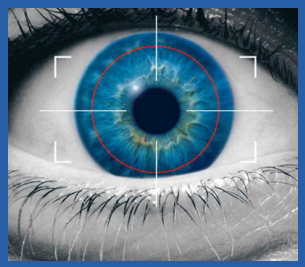
Finger prints. This involves scanning the finger for unique features, such as ridge endings, sweat ports, and the distance between ridges, and comparing them against previous scans. It is one of the most **widely used methods**, and is now used in many laptops for user authentication. Unfortunately, the quality of the scan **can be variable**, such as for: dirty, dry or cracked skin; pressure or alignment of the finger on the scanner; and for surface contamination. The main methods used include thermal, optical, tactile capacitance, and ultra-sound.





Fingerprints

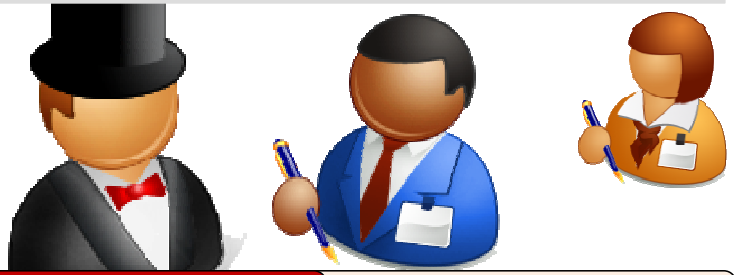




Iris scanning

Iris scanning

- One of the best methods of authentication.
- Everyone has a **unique iris**, which is fairly complex in its pattern.
- **Key characteristic marking** such as the corona, filaments, crypts, pits, freckles, radial furrows and striations.
- Extremely **difficult to trick** the system.
- **Affected by glasses** which affect the quality of the image.
- **Moral issues** associated with this method.
- Fairly **costly** to implement.
- Fairly **evasive** in its usage, where the user must peer into a special sensor machine.
- Accuracy obviously depends on the **resolution of the scanner**, and the distances involved.

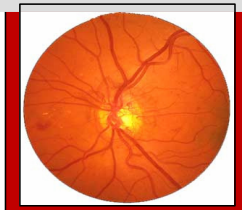


Methods

Authentication

Retina scan

- **Shines** a light into the eye.
- Analyses the **blood vessels** at the back of the eye for a specific pattern.
- **Good method** of authenticating users.
- Needs **careful alignment** for creditable scans.
- May cause some **long term damage** to the eye.

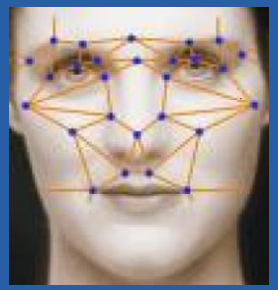


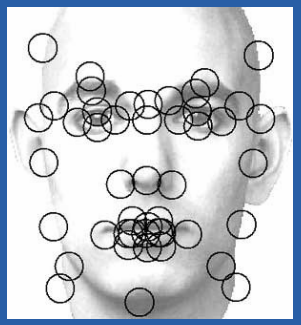
Retina scan

Iris/retina scan

Authentication

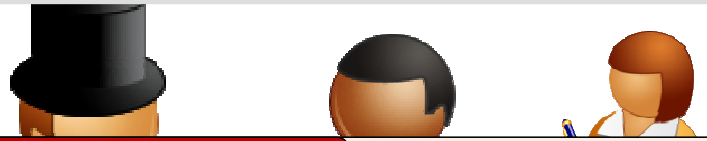
Methods





Face recognition

- Scans the face for either a **2D or 3D image**, and performs pattern.
- Match to determine the **likeness to a known face**.
- **Optical scanning**, also can be infrared (thermal) scanning.
- **Distance between the eyes**, width of forehead, size of mouth, chin length, and so on.
- Suffers from **permanence factors** that cause the face to change, such as facial hair, glasses, and, obviously, the position of the head.
- **Remote scanning** and unobtrusive sensor.
- **Poor match** the further the face is away from the scanner.



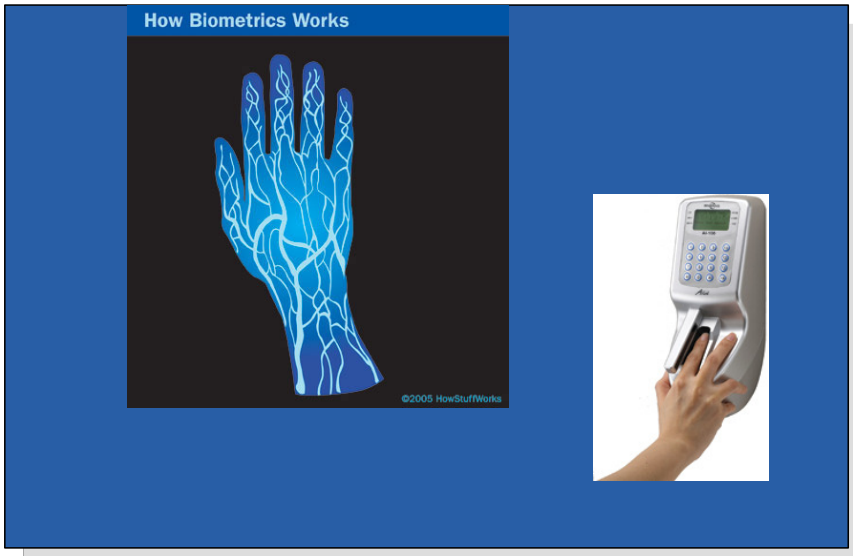
Hand geometry

- **2D or 3D image** is taken of the hand.
- System measures **key parameters,** such as the length of the fingers, the position of knuckles, and so on.
- One of the **most widely used methods**.
- One of the **most acceptable** from a user point-of-view.
- **Can be inaccurate**, and thus should be only used in low to medium risk areas.
- **Typically contactless**, and can handle fairly high volumes of users.
- Main application is typically in building/ **room access**.

Hand geometry

Face recognition/hand geometry

Vein/voice



Vein pattern

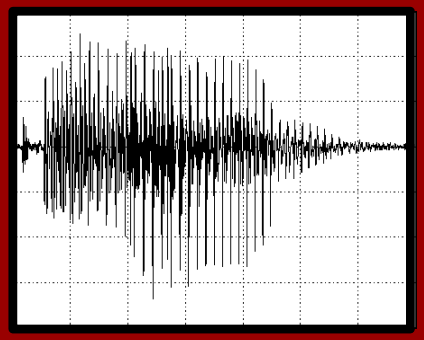
- Scans the back of a hand when it is making a fist shape.
- View structure is then captured by infrared light.
- Finger view recognition is a considerable enhancement to this (where the user inserts their finger into a scanner).
- Produces good results for accurate recognition.

Methods

Authentication

Voice Recognition

- Analyzing speech against a known pattern for a user
- Resonance in the vocal tract, and the shape and size of the mouth and nasal cavities give a fairly unique voice print.
- Used with a limit range of words, such as for passwords or pass phrases.
- Can be used remotely, especially in telephone applications,
- Degrades with background noise, along with changes to a users voice, such as when they have a cold, or when they've being over exercising their voice.



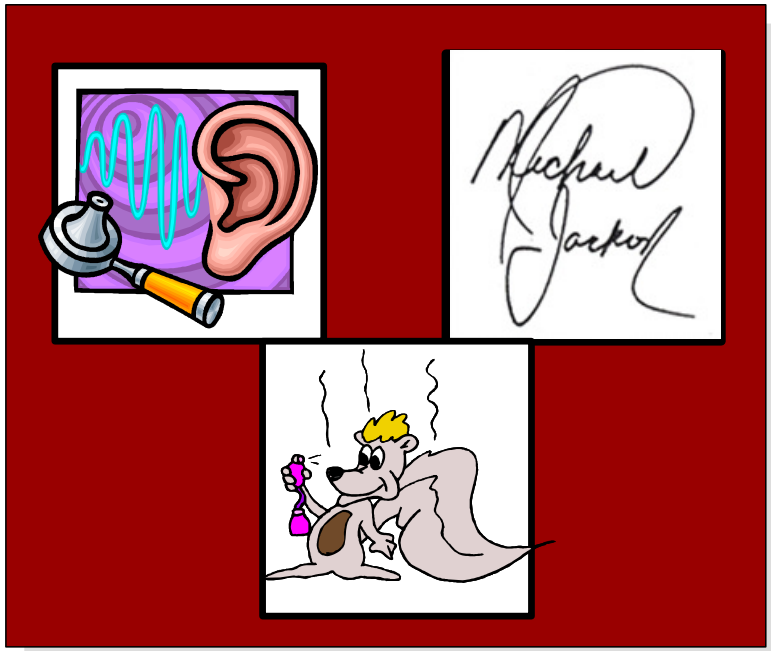
Voice recognition/view scan

Keystroke

- Analyzing the keystrokes of a user, for **certain characteristics**, such as typing speed, typical typing errors, time between certain keys, and so on.
- One of the **least liked** authentication methods, and also suffers from changes of behavior, such as for fatigue and distractions.
- Can be matched-up with other **behavioral aspects** to more clearly identify the user, such as in matching up their mouse stokes, applications that they run, and so on.

Others

- **Ear shape**. Analyzes the shape of the ear, and has not been used in many applications. It is normally fairly obtrusive, and can involve the user posing in an uncomfortable way.
- **Body odor**. Analyzes the body odor of a user, for the chemicals they emit (knows as volatiles), from non-intrusive parts of the body, such as from the back of the hand.
- **Personal signature**. Analyzes the signing process of the user, such as for the angle of the pen, the time taken for the signature, the velocity and acceleration of the signature, the pen pressure, the number of times the pen is lifted, and so on.

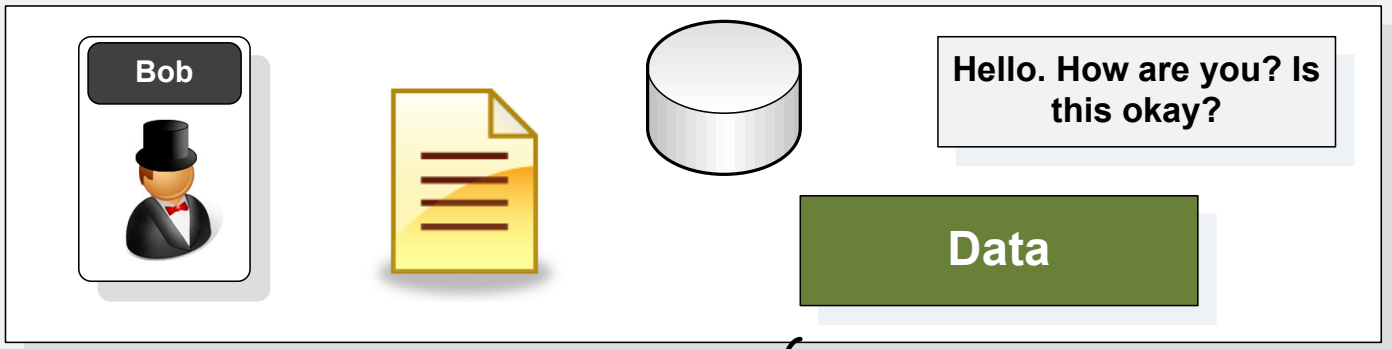


Authentication

Introduction
Methods
Usernames/passwords
Biometric issues
Biometric methods
Message hash
Authenticating with private key
HMAC
Digital certificates
Trust
Cardspace
Conclusions

Message Hash

How do we get a finger-print for data?



With a fingerprint we can hopefully tell if Eve has modified any of the data

Solved by Prof Ron Rivest with the MD5 hash signature.

	Base-64
hello	XUFAKrxLKna5cZ2REBfFkg
Hello	ixqZU8RhEpaoJ6v4xHgE1w
Hello. How are you?	CysDE5j+ZOUbCYZtTdsFiw
Napier	j4NXH5Mkrk4j13N1MFXHtg

	Hex
hello	5D41402ABC4B2A76B9719D911017C592
Hello	8B1A9953C4611296A827ABF8C47804D7
Hello. How are you?	CC708153987BF9AD833BEBF90239BF0F
Napier	8F83571F9324AE4E23D773753055C7B6

hello	qvTGHdzF6KLavt4PO0gs2a6pQ00=
Hello	9/+ei3uy4Jtwk1pdeF4MxdnQq/A=
Hello. How are you?	Puh2Am76bhjqE5lbTWtwsqbdFC8=
Napier	v4GxNaVod2b09GR2Tqw4yopOuro=

Base-64

hello	AAF4C61DDCC5E8A2DABEDE0F3B482CD9AEA9434D
Hello	F7FF9E8B7BB2E09B70935A5D785E0CC5D9D0ABF0
Hello. How are you?	3EE876026EFA6E18EA13995B4D6B70B2A6DD142F
Napier	BF81B135A5687766F4F464764EAC38CA8A4EBABA

Hex

Security and mobility are two of the most important issues on the Internet, as they will allow users to secure their data transmissions, and also break their link with physical connections.

F94FBED3DAE05D223E6B963B9076C4EC

+U++09rgXSI+a5Y7kHbE7A==

Base-64

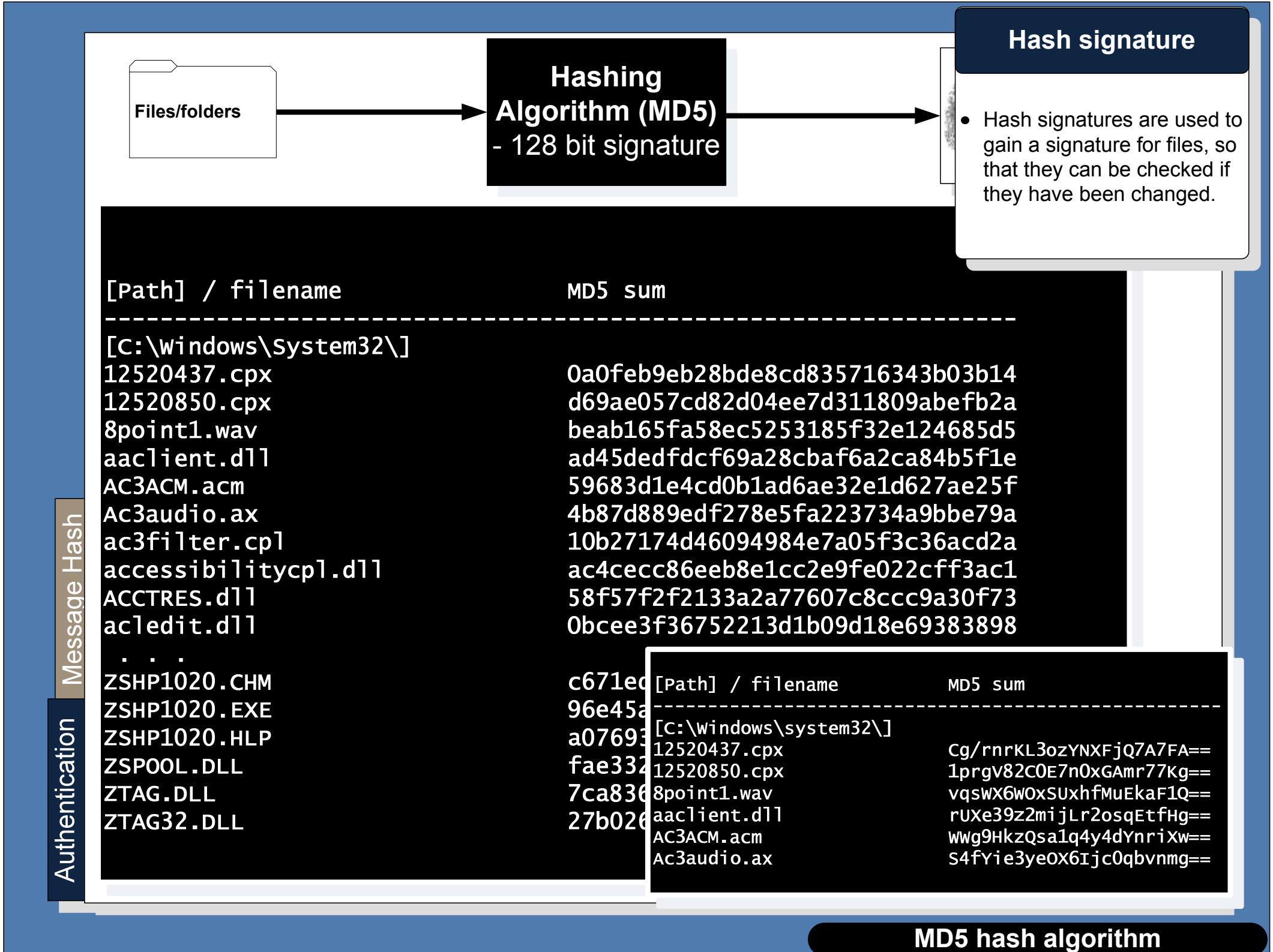
Security and mobility are two of the mast important issues on the Internet, as they will allow users to secure their data transmissions, and also break their link their physical connections.

8A8BDC3FF80A01917D0432800201CFBF

iovcP/gKAZF9BDKAAgHPvw==

Hex

Author: Prof Bill Buchanan


Files/folders
Hashing Algorithm (MD5) - 128 bit signature
Hash signature
Hash signatures are used to gain a signature for files, so that they can be checked if they have been changed.
[Path] / filename MD5 sum
[C:\Windows\System32\]
12520437.cpx 0a0feb9eb28bde8cd835716343b03b14
12520850.cpx d69ae057cd82d04ee7d311809abefb2a
8point1.wav beab165fa58ec5253185f32e124685d5
aaclient.dll ad45dedfdcf69a28cbaf6a2ca84b5f1e
AC3ACM.acm 59683d1e4cd0b1ad6ae32e1d627ae25f
Ac3audio.ax 4b87d889edf278e5fa223734a9bbe79a
ac3filter.cpl 10b27174d46094984e7a05f3c36acd2a
accessibilitycpl.dll ac4cecc86eeb8e1cc2e9fe022cff3ac1
ACCTRES.dll 58f57f2f2133a2a77607c8ccc9a30f73
acledit.dll 0bcee3f36752213d1b09d18e69383898
. . .
ZSHP1020.CHM c671ed
ZSHP1020.EXE 96e45a
ZSHP1020.HLP a07693
ZSPOOL.DLL fae332
ZTAG.DLL 7ca836
ZTAG32.DLL 27b026
[Path] / filename MD5 sum
[C:\Windows\system32\]
12520437.cpx Cg/rnrKL3ozYNXFjQ7A7FA==
12520850.cpx 1prgV82C0E7n0xGAmr77Kg==
8point1.wav vqsWX6WOxSUxhfMuEkaF1Q==
aaclient.dll rUXe39z2mijLr2osqEtfHg==
AC3ACM.acm WWg9HkzQsa1q4y4dYnriXw==
Ac3audio.ax S4fYie3yeOX6IjcOqbvnmg==
Message Hash
Authentication
MD5 hash algorithm

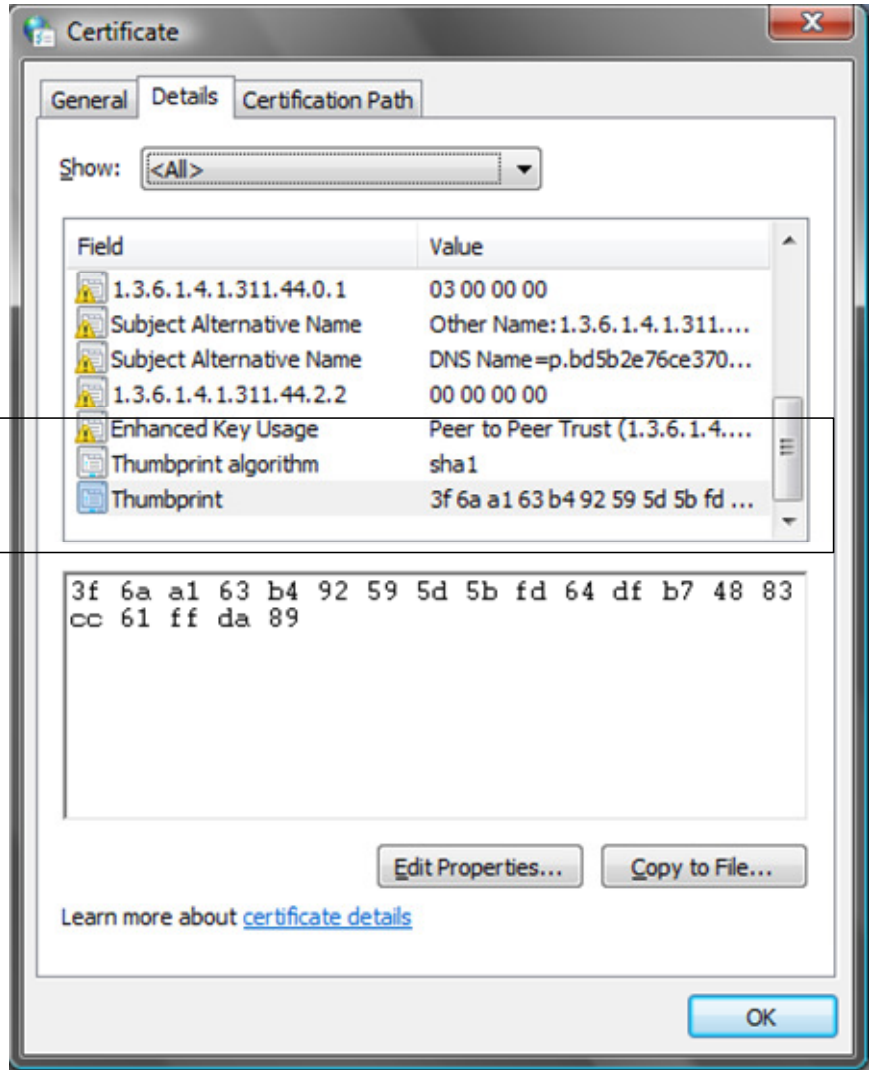
Files/folders

Hashing Algorithm (MD5)
- 128 bit signature

Hash signature

- Hash signatures are used to identify that a file/certificate has not been changed.

Bob



The digital certificate has an SHA-1 hash thumbprint (3f6a...89) which will be checked, and if the thumbprint is different, the certificate will be invalid.

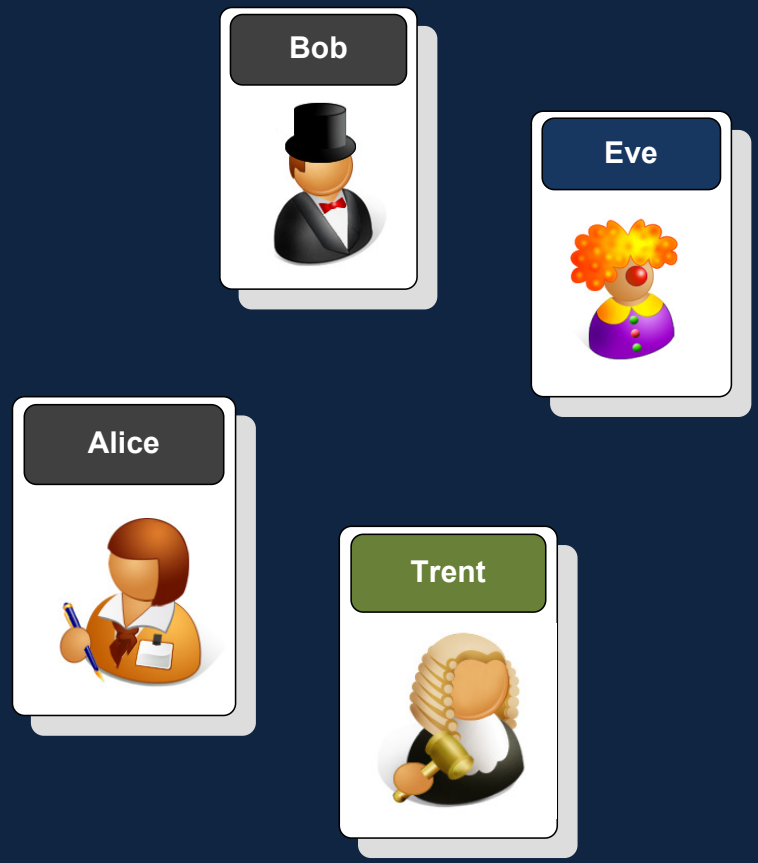
Message Hash

Authentication

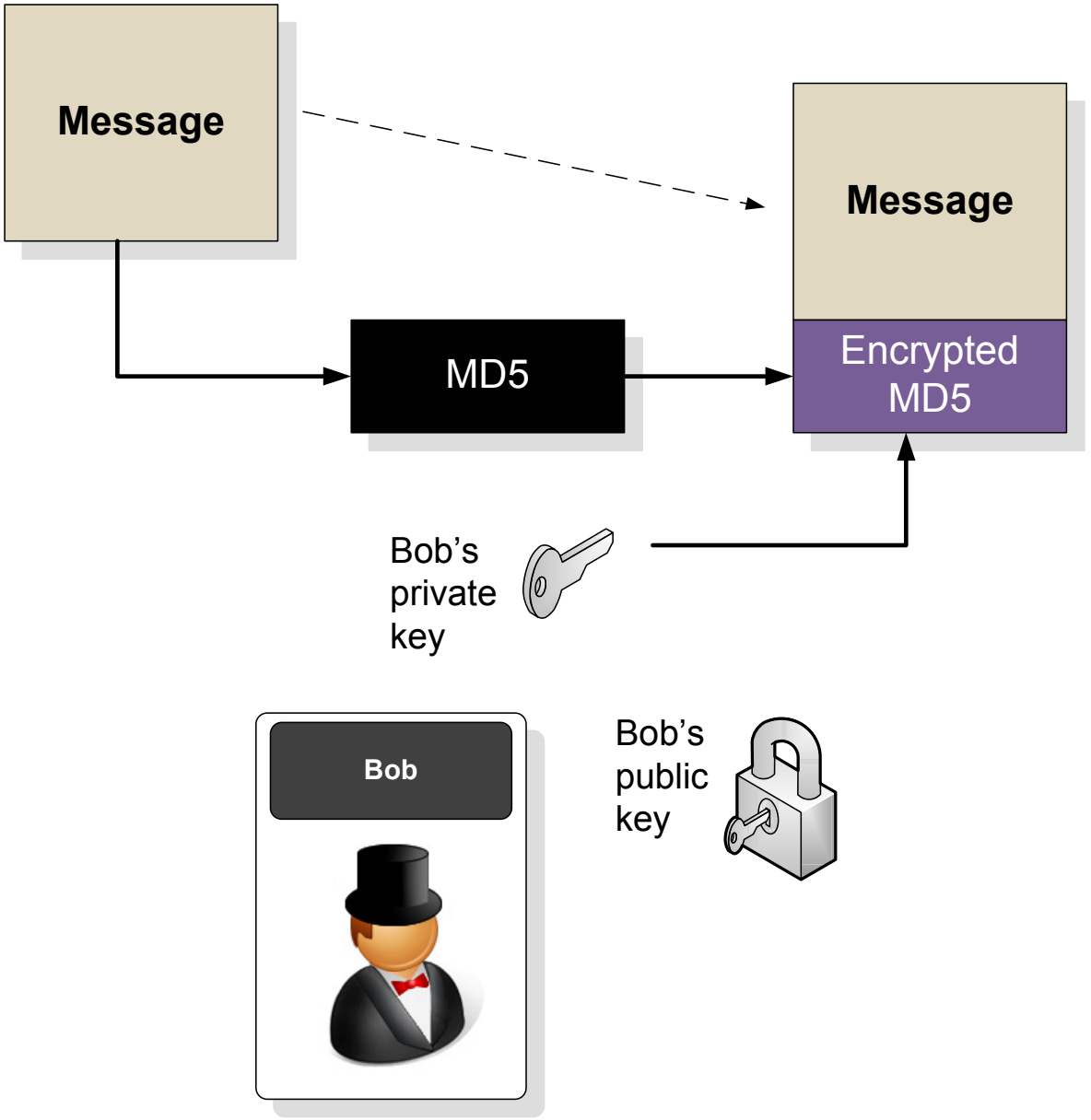
MD5 hash algorithm

Authentication

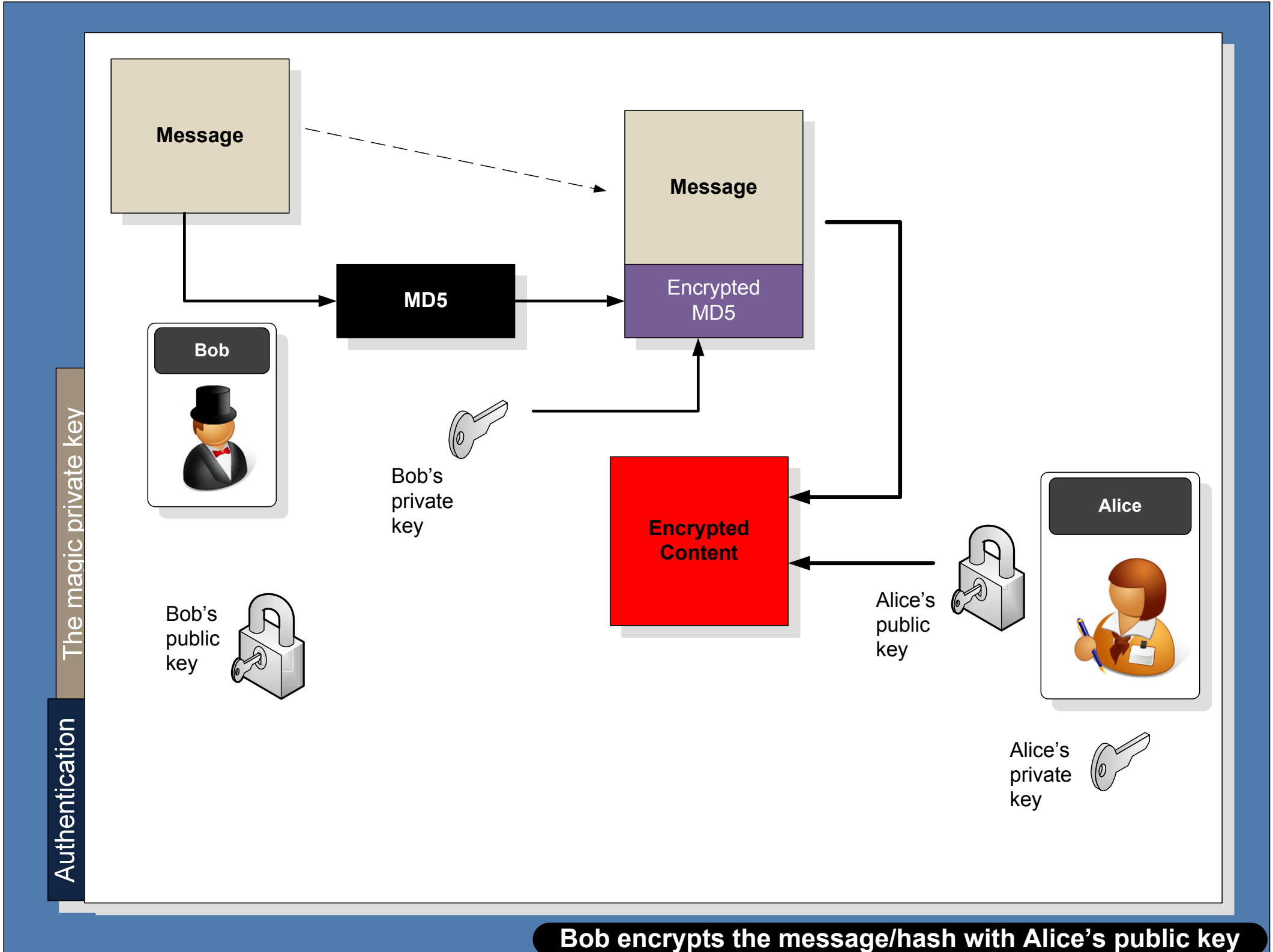
- Introduction
- Methods
- Usernames/passwords
- Biometric issues
- Biometric methods
- Message hash
- Authenticating with private key
- HMAC
- Digital certificates
- Trust
- Cardspace
- Conclusions

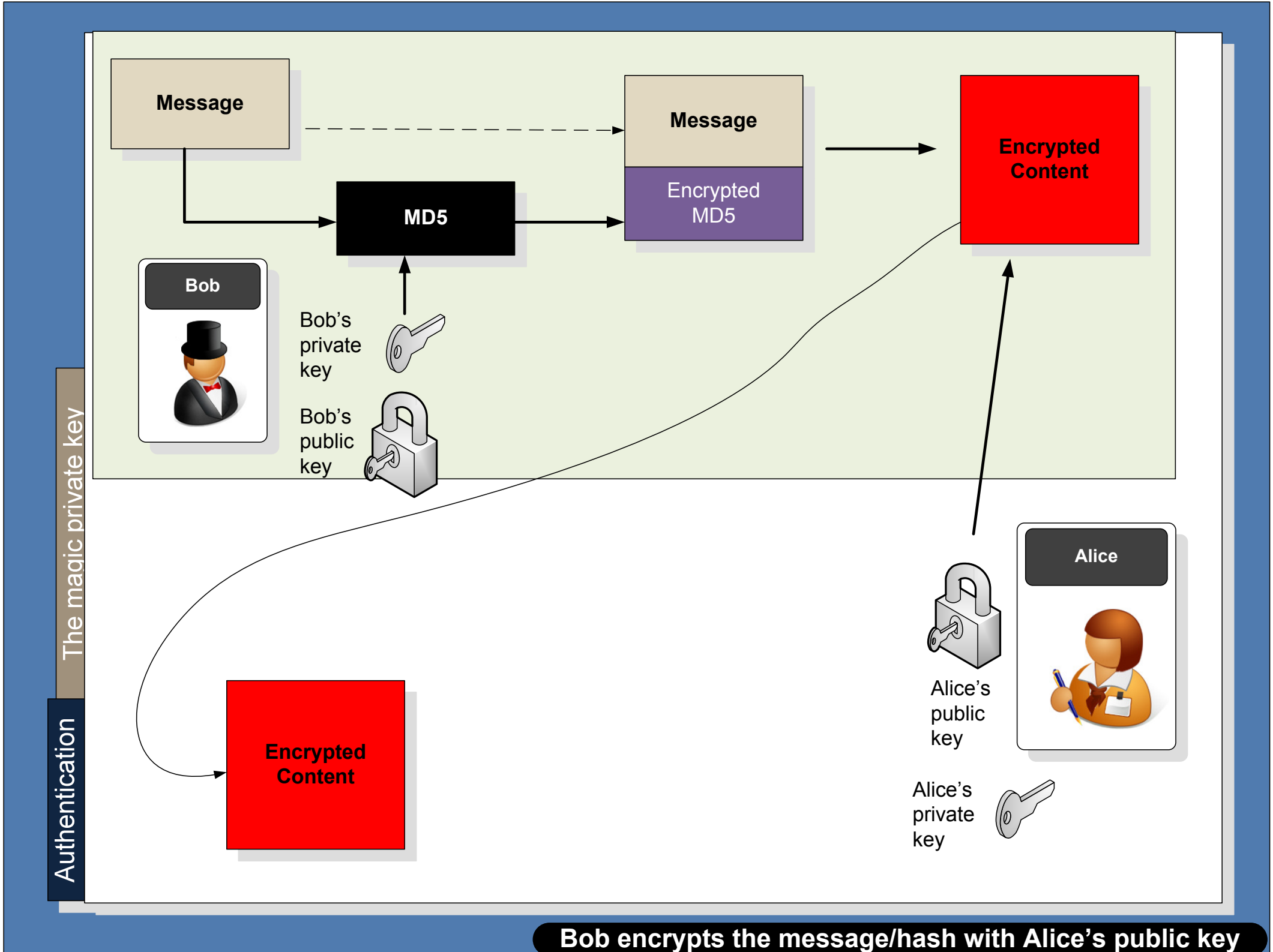


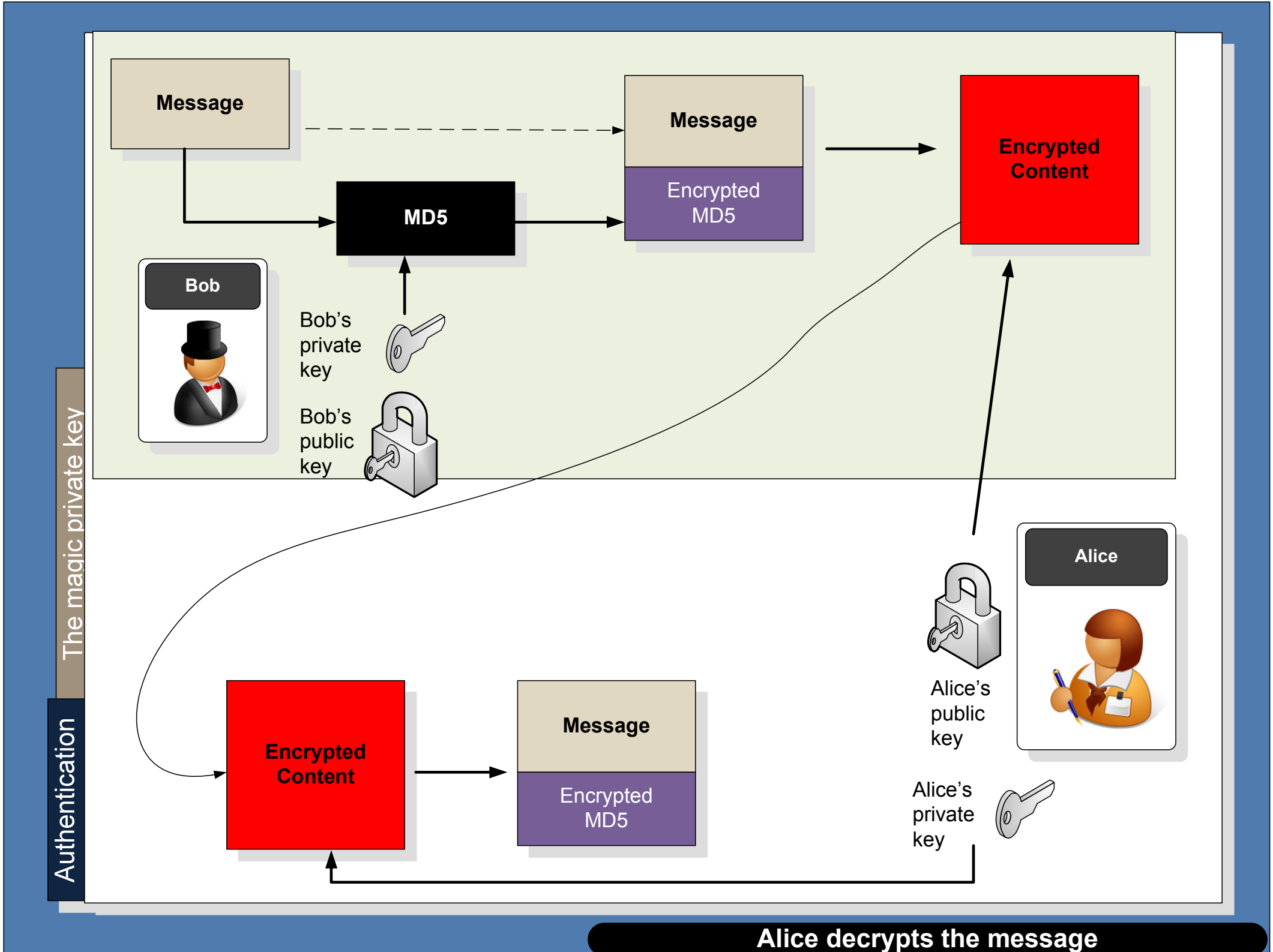
Authenticating with the private key

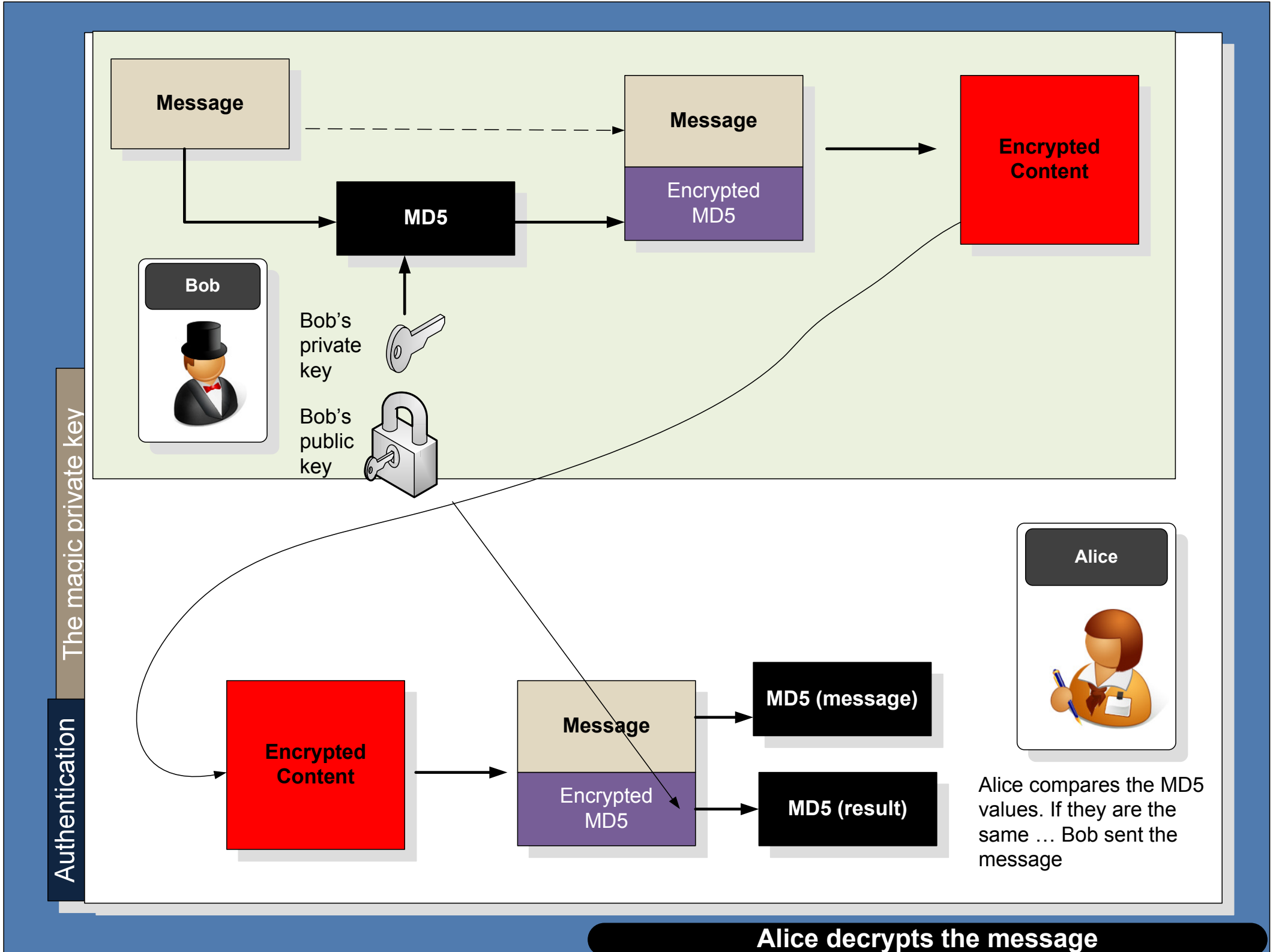


Using Bob's private key to authenticate himself


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

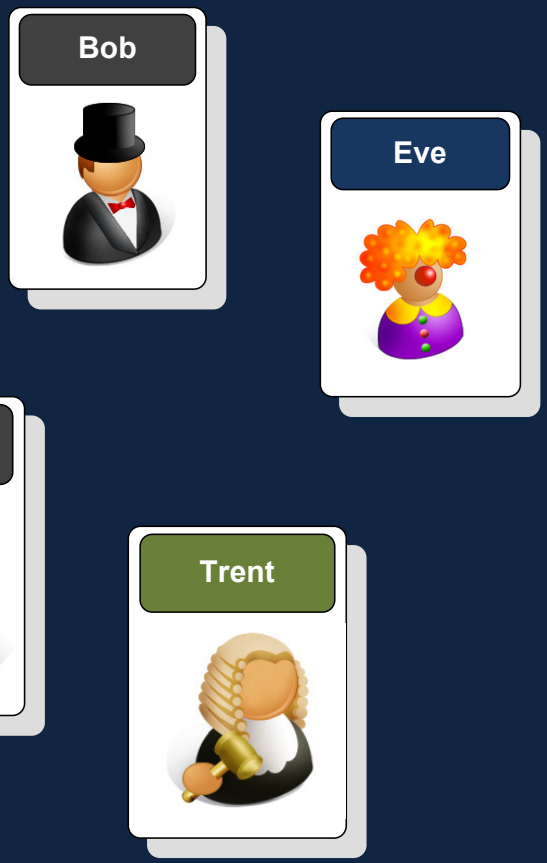

Message
Message
Encrypted MD5
Encrypted Content
MD5
Bob
Bob's private key
Bob's public key
The magic private key
Authentication
Encrypted Content
Alice
Alice's public key
Alice's private key
Bob encrypts the message/hash with Alice's public key


Message
Message
Encrypted MD5
Encrypted Content
MD5
Bob
Bob's private key
Bob's public key
The magic private key
Authentication
Alice
Alice's public key
Alice's private key
Encrypted Content
Message
Encrypted MD5
Alice decrypts the message

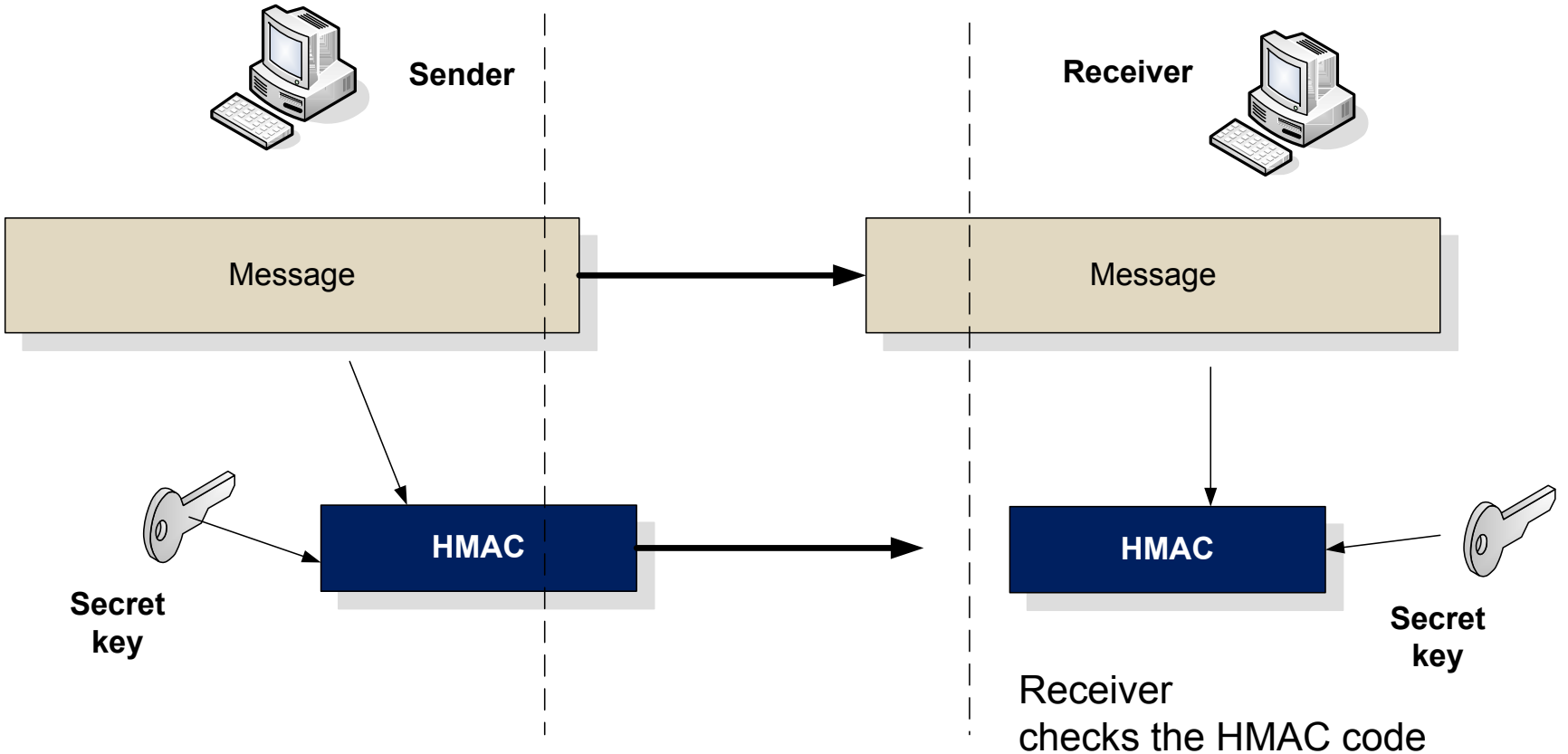

Message
Message
Encrypted MD5
Encrypted Content
MD5
Bob
Bob's private key
Bob's public key
The magic private key
Authentication
Encrypted Content
Message
Encrypted MD5
MD5 (message)
MD5 (result)
Alice
Alice compares the MD5 values. If they are the same … Bob sent the message
Alice decrypts the message

Authentication

Introduction
Methods
Usernames/passwords
Biometric issues
Biometric methods
Message hash
Authenticating with private key
HMAC
Digital certificates
Trust
Cardspace
Conclusions



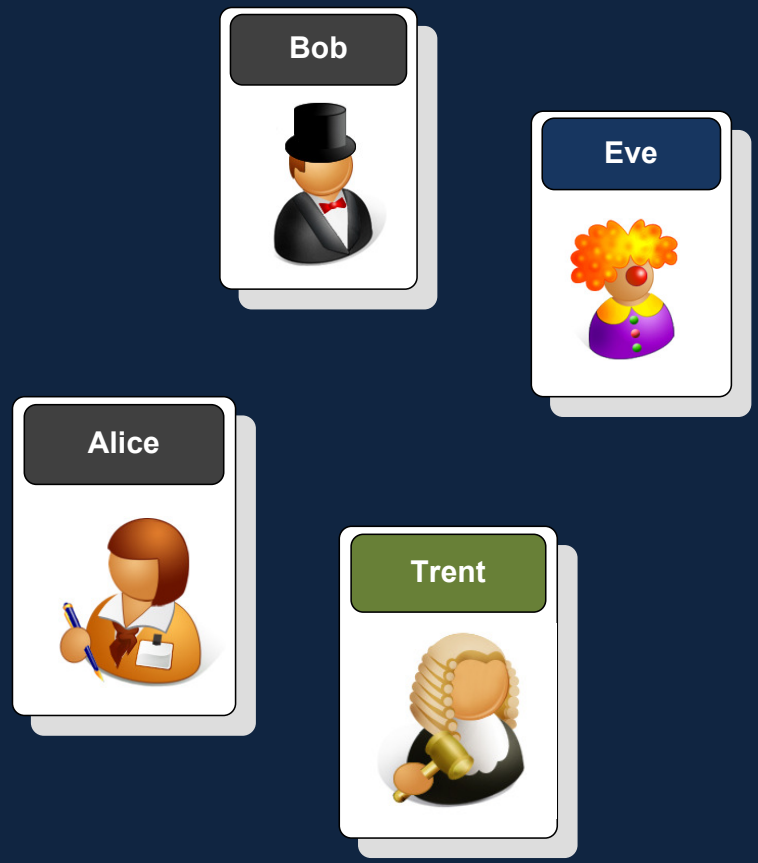
HMAC



Receiver checks the HMAC code against received one – if they match the sender is validated, and the message is also confirmed

Authentication

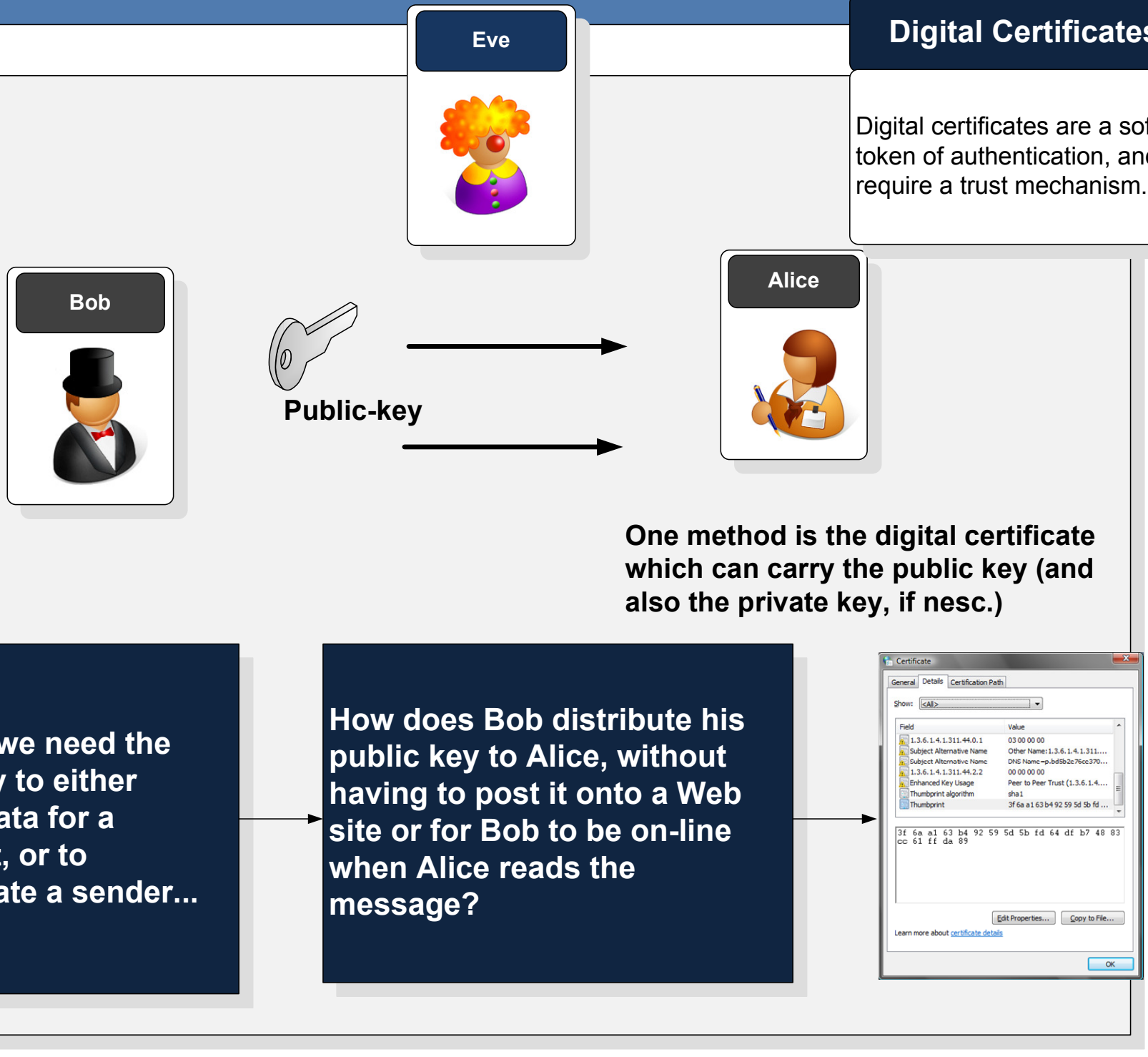
- Introduction
- Methods
- Usernames/passwords
- Biometric issues
- Biometric methods
- Message hash
- Authenticating with private key
- HMAC
- Digital certificates
- Trust
- Cardspace
- Conclusions



Digital Certificates

Digital Certificates

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

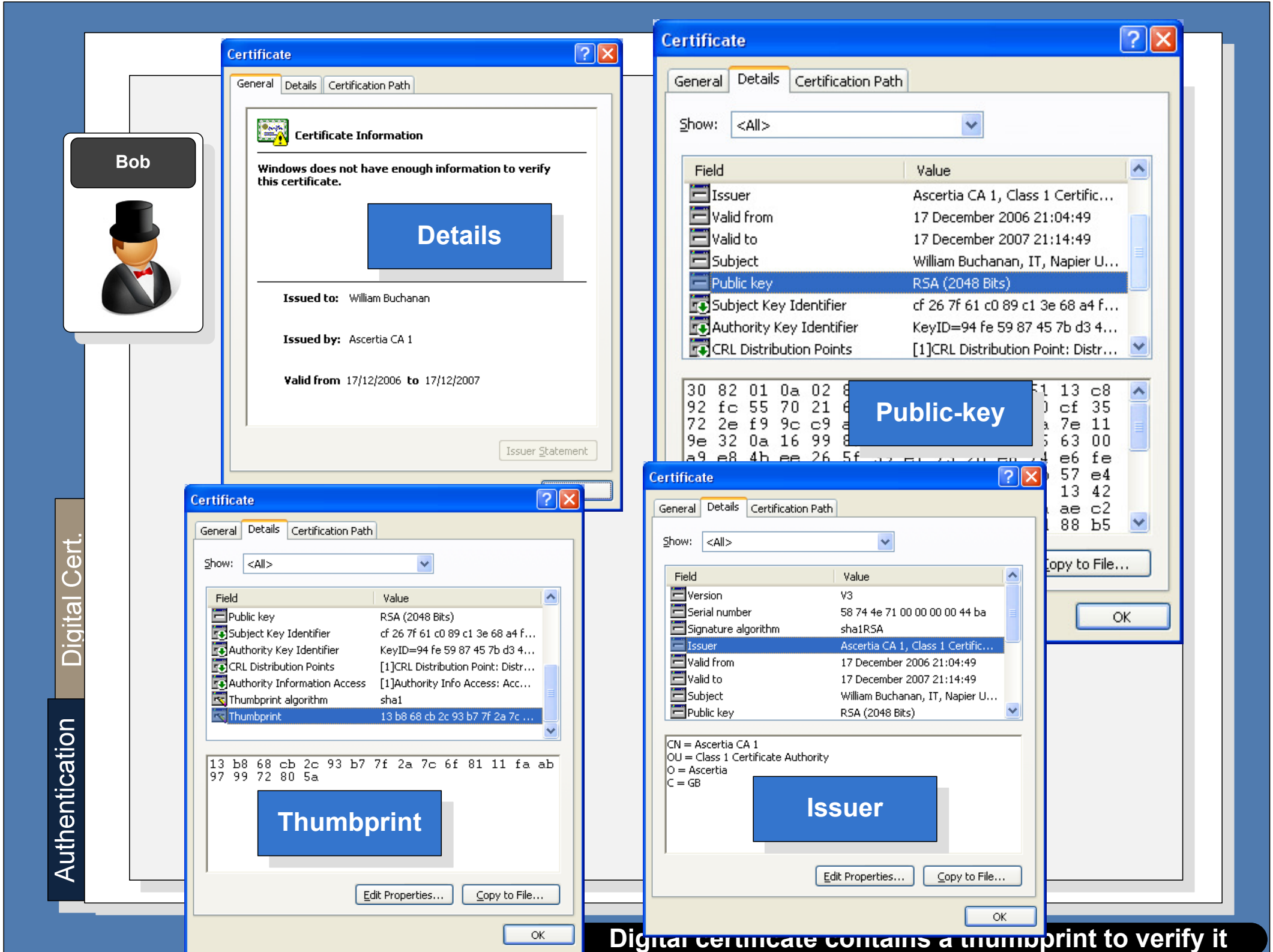


One method is the digital certificate which can carry the public key (and also the private key, if nesc.)

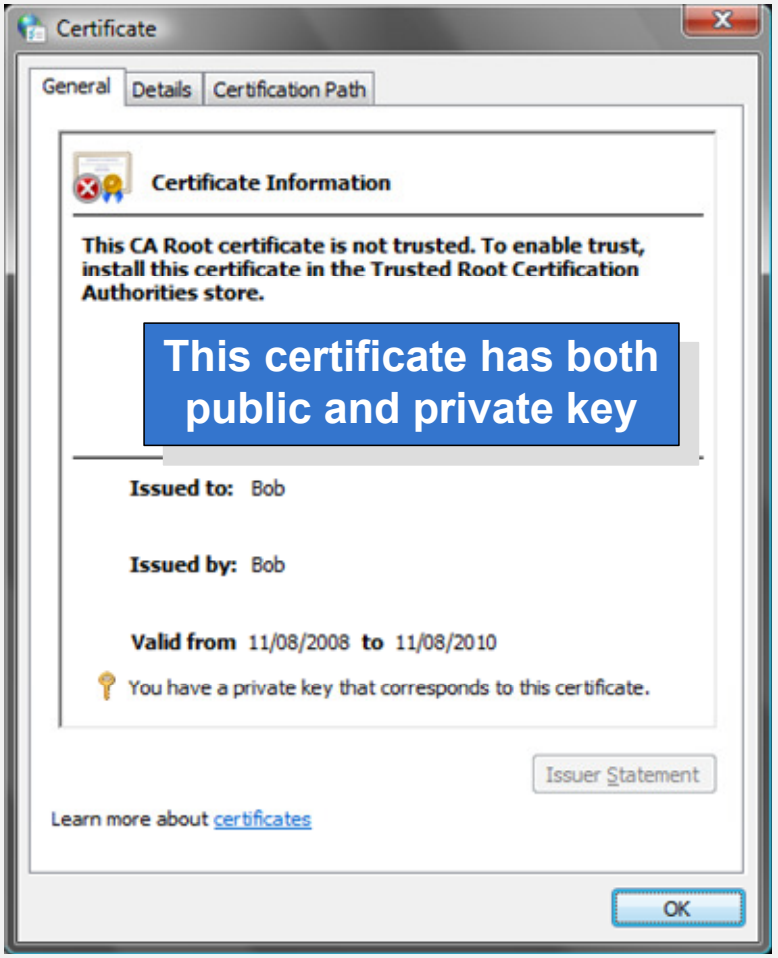
Now that we need the public key to either encrypt data for a receipiant, or to authenticate a sender...

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

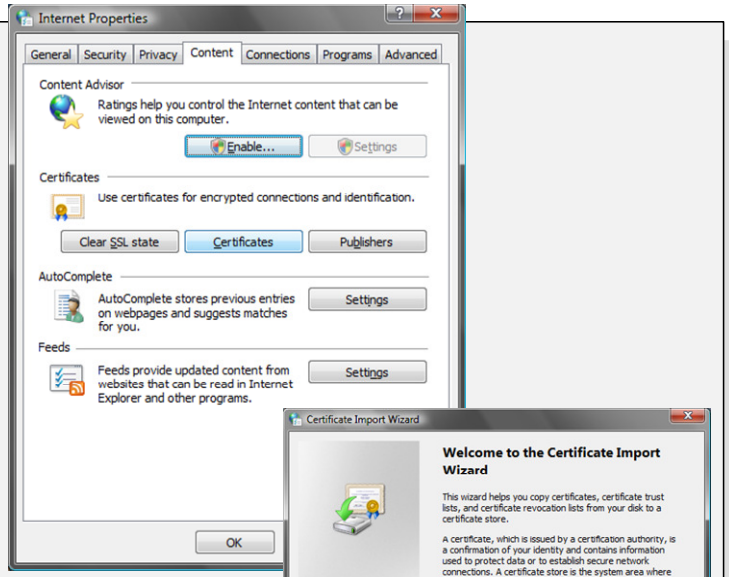
Digital Cert.

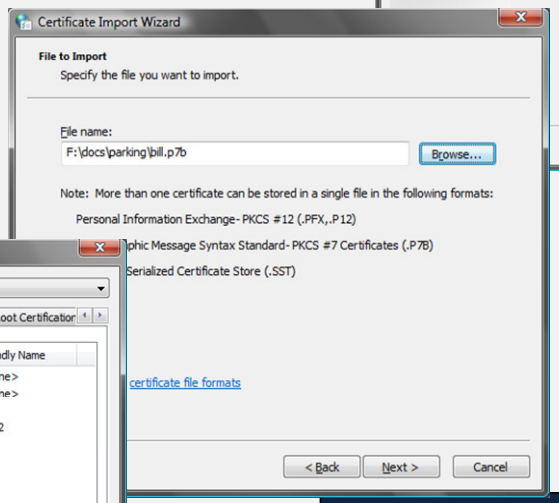
Authentication

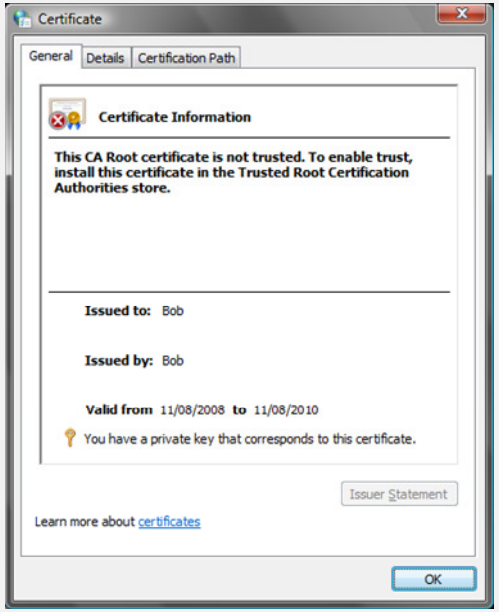
P7b format

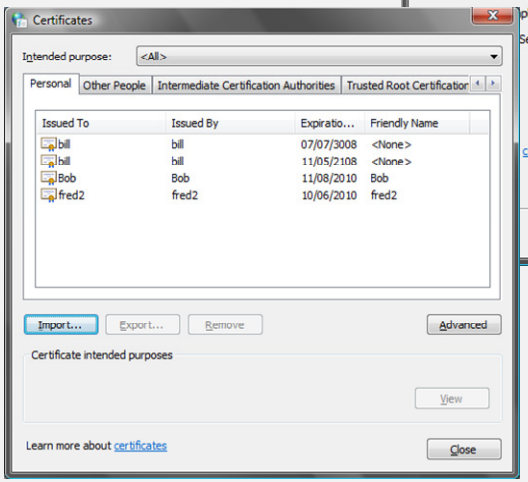
Bob

```
-----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
CCsGAQUFBzAChiJodHRwOi8vb2NzcC5nbG9iYWx0cnVzdGZpbmRlci5jb20vMA0G
CSqGSIb3DQEBBQUAA0EATOCwGJ1tSOkTlupmpjkMl8IdxMmD5WuhszjBlGsMhPxI
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

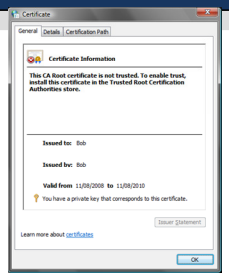
A. Bob creates the message.
B. Bob encrypts with Alice's public key and sends Alice the encrypted message
C. Alice decrypts with her private key
D. Alice receives the message

A

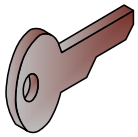
Encryption

Communications Channel

Decryption



Alice sends her digital certificate with her public key on it



Hello

B

C

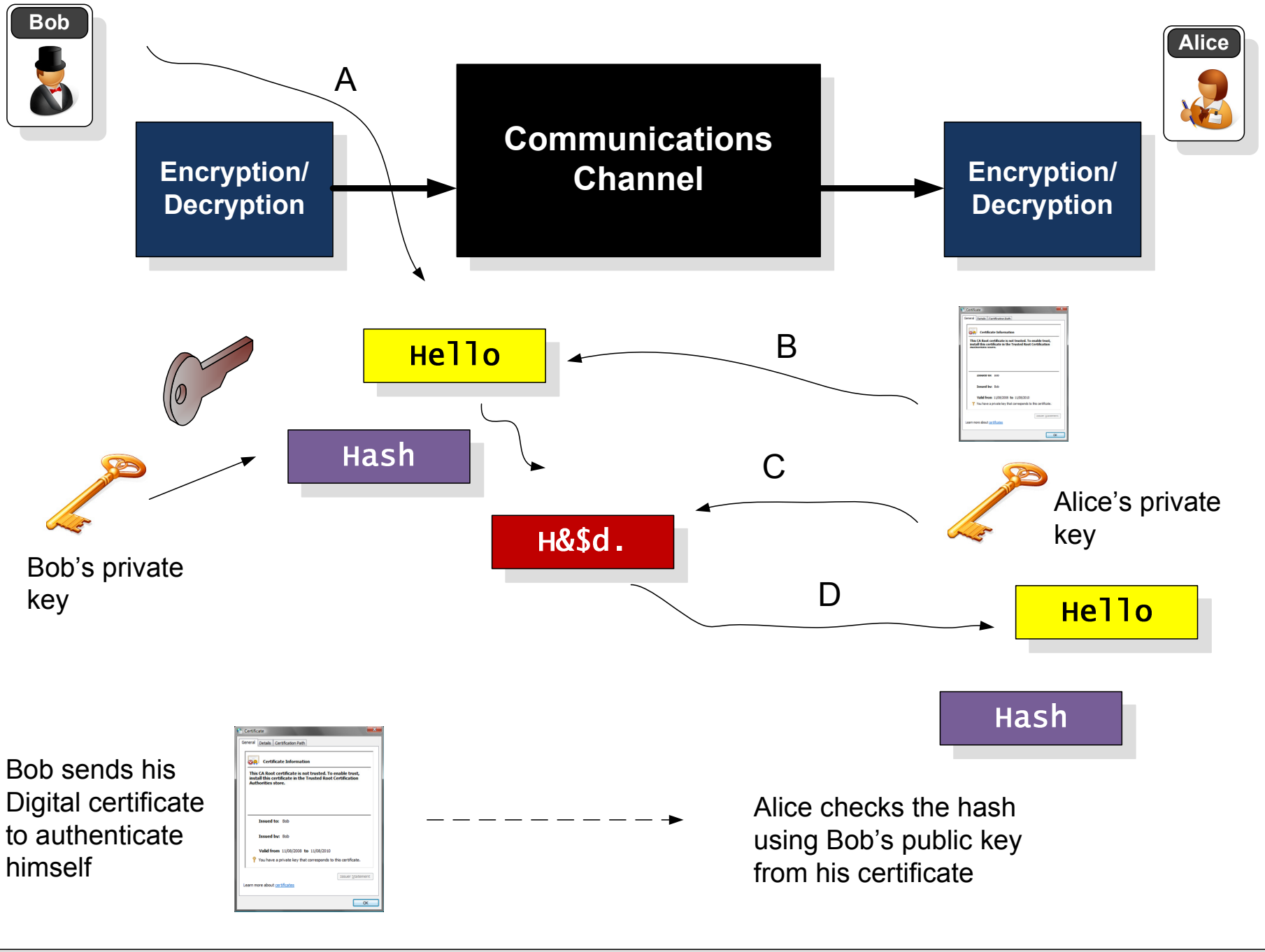
H&$d.

Alice's private key

D

Hello

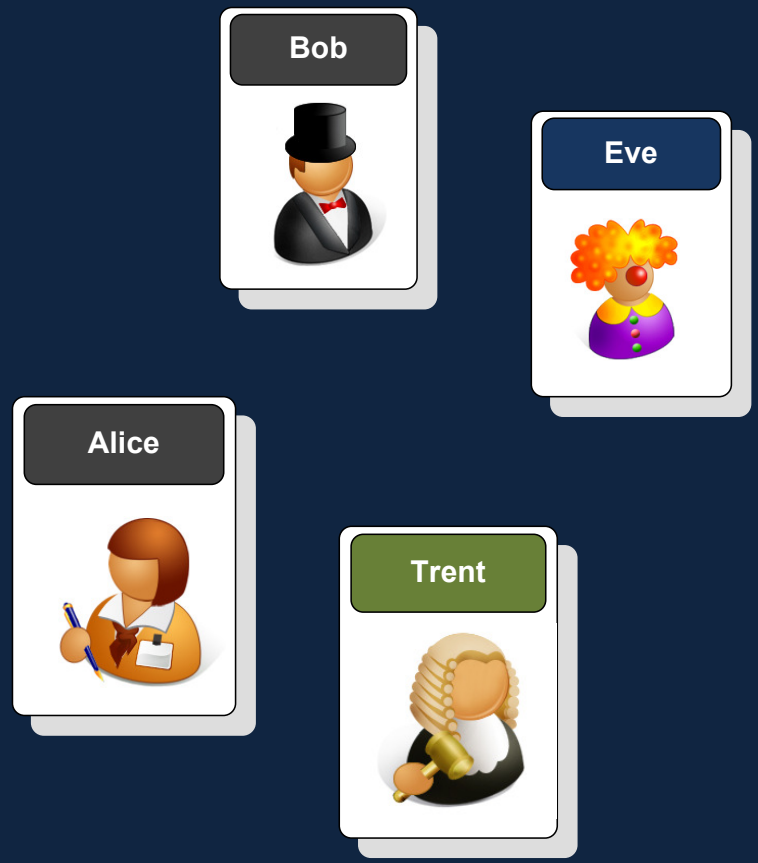
Encrypting messages to Alice



Authenticating Bob

Authentication

- Introduction
- Methods
- Usernames/passwords
- Biometric issues
- Biometric methods
- Message hash
- Authenticating with private key
- HMAC
- Digital certificates
- Trust
- Cardspace
- Conclusions



Trust – meet Trent

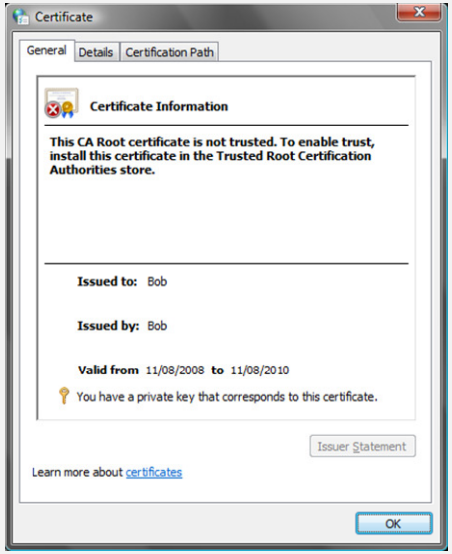
Digital Certificates

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

Eve

Bob

Alice



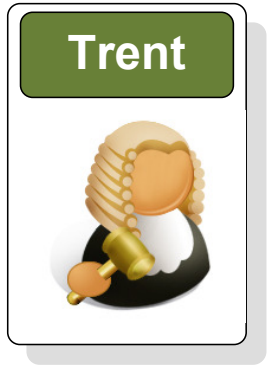
Trent

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

Who can we trust to get the digital certificate from?

Trusted Root CA

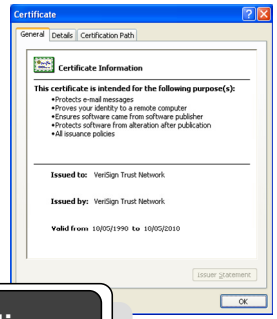
Certificate Authority (CA)
- Able to grant certificates
Examples; Verisign, Entrust, Microsoft Trust.



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

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

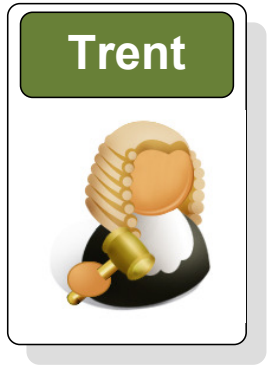
Trusted root certificate



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

Trusted Root CA

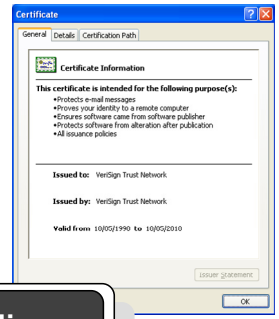
Certificate Authority (CA)
- Able to grant certificates
Examples; Verisign, Entrust, Microsoft Trust.



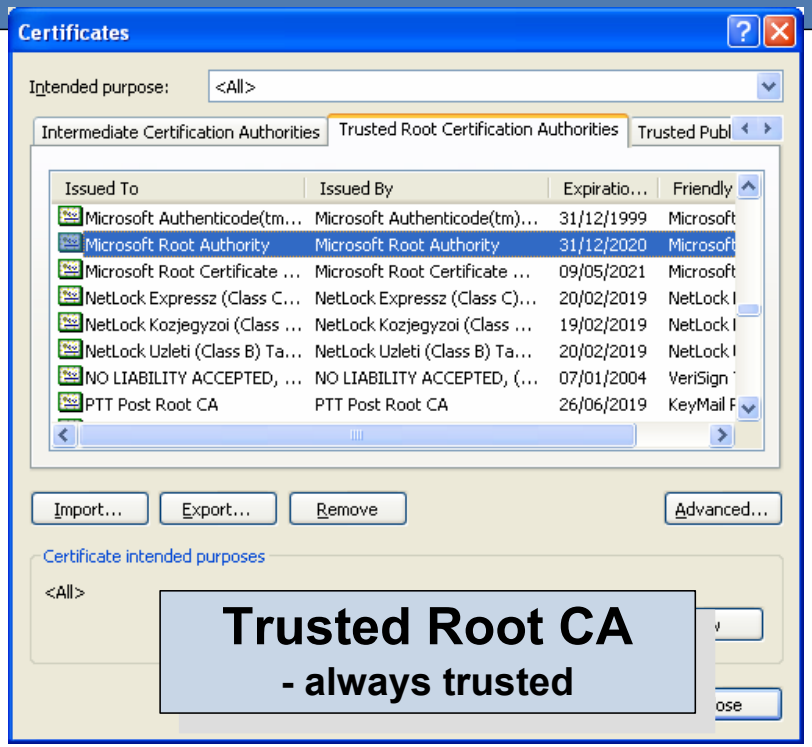
Eve tricks the CA to get a certificate with Bob's name

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.



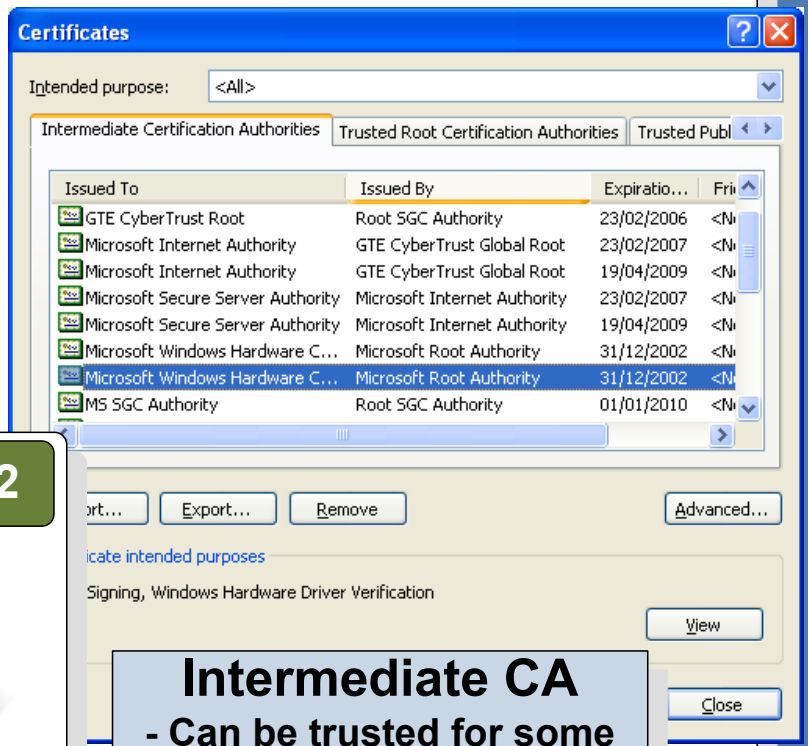
Trusted Root CA

Trent

Certificate purposes:

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

Bob



Trust2

Intermediate CA
- Can be trusted for some things

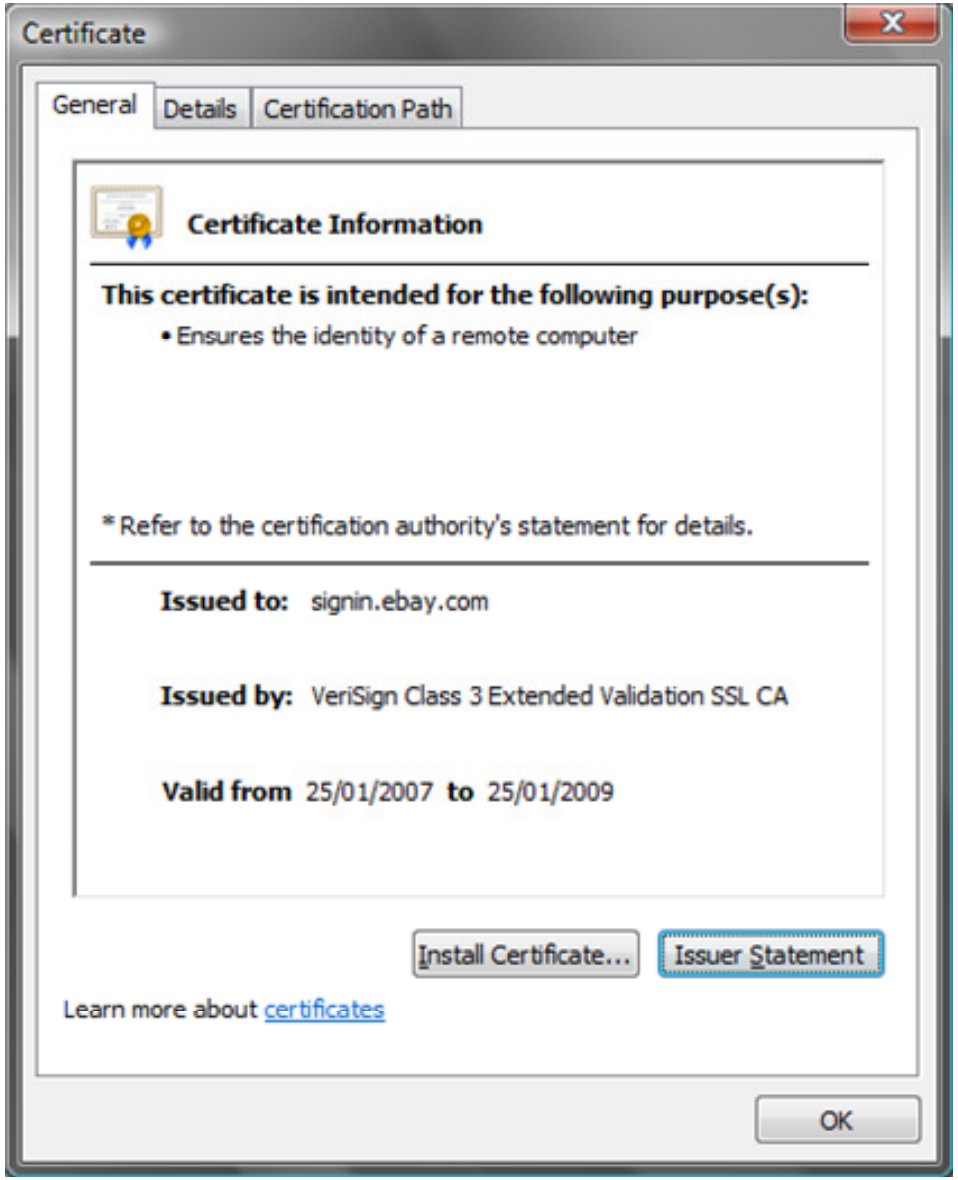
Levels of trust

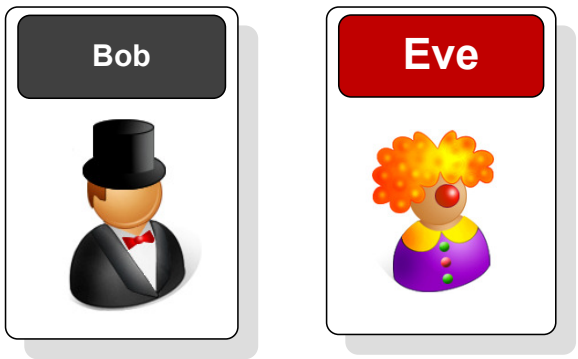
The two main problems with digital certificates are:

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

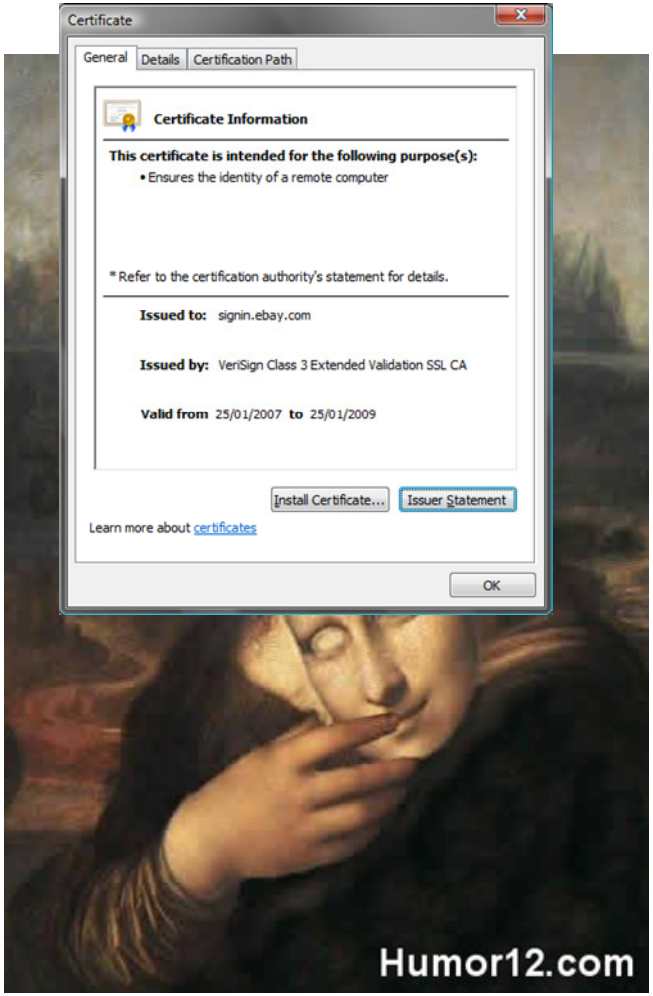
So let's look at a few … are they real or fake?

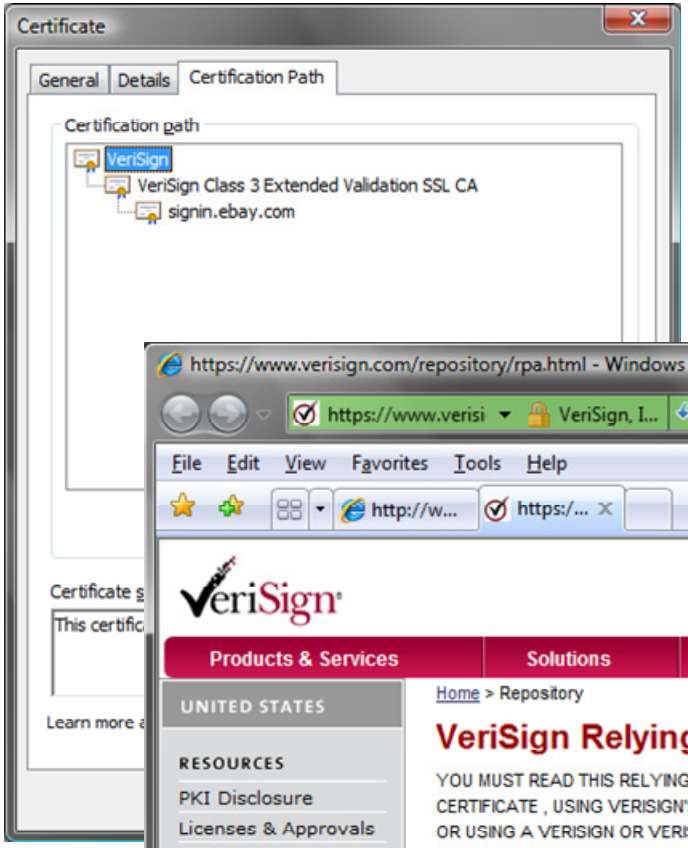

Humor12.com


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
* Refer to the certification authority's statement for details.
Issued to: signin.ebay.com
Issued by: VeriSign Class 3 Extended Validation SSL CA
Valid from 25/01/2007 to 25/01/2009
Install Certificate...
Issuer Statement
Learn more about certificates
OK


Bob
Eve

Real or fake?

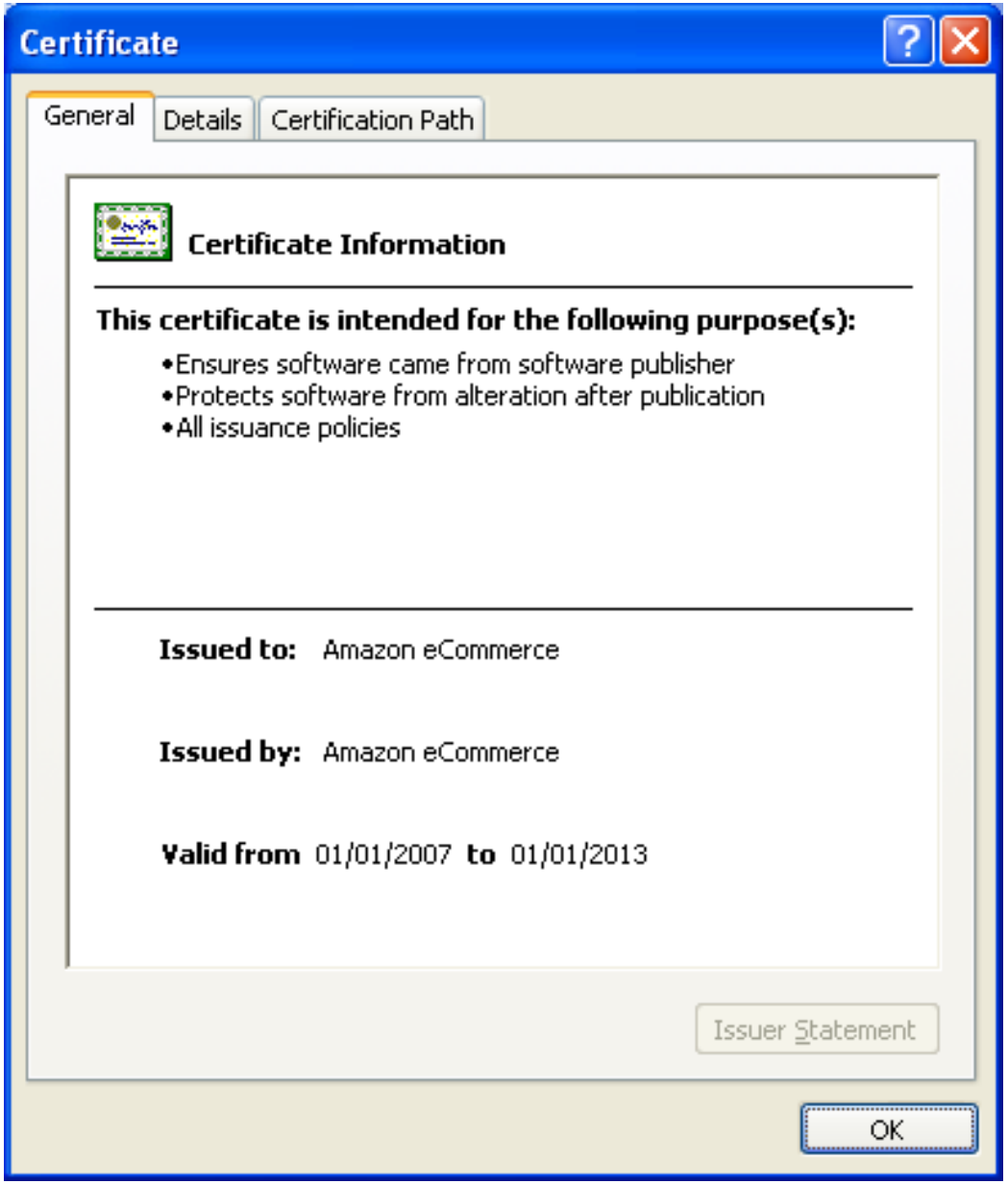




Real!

Real or fake?

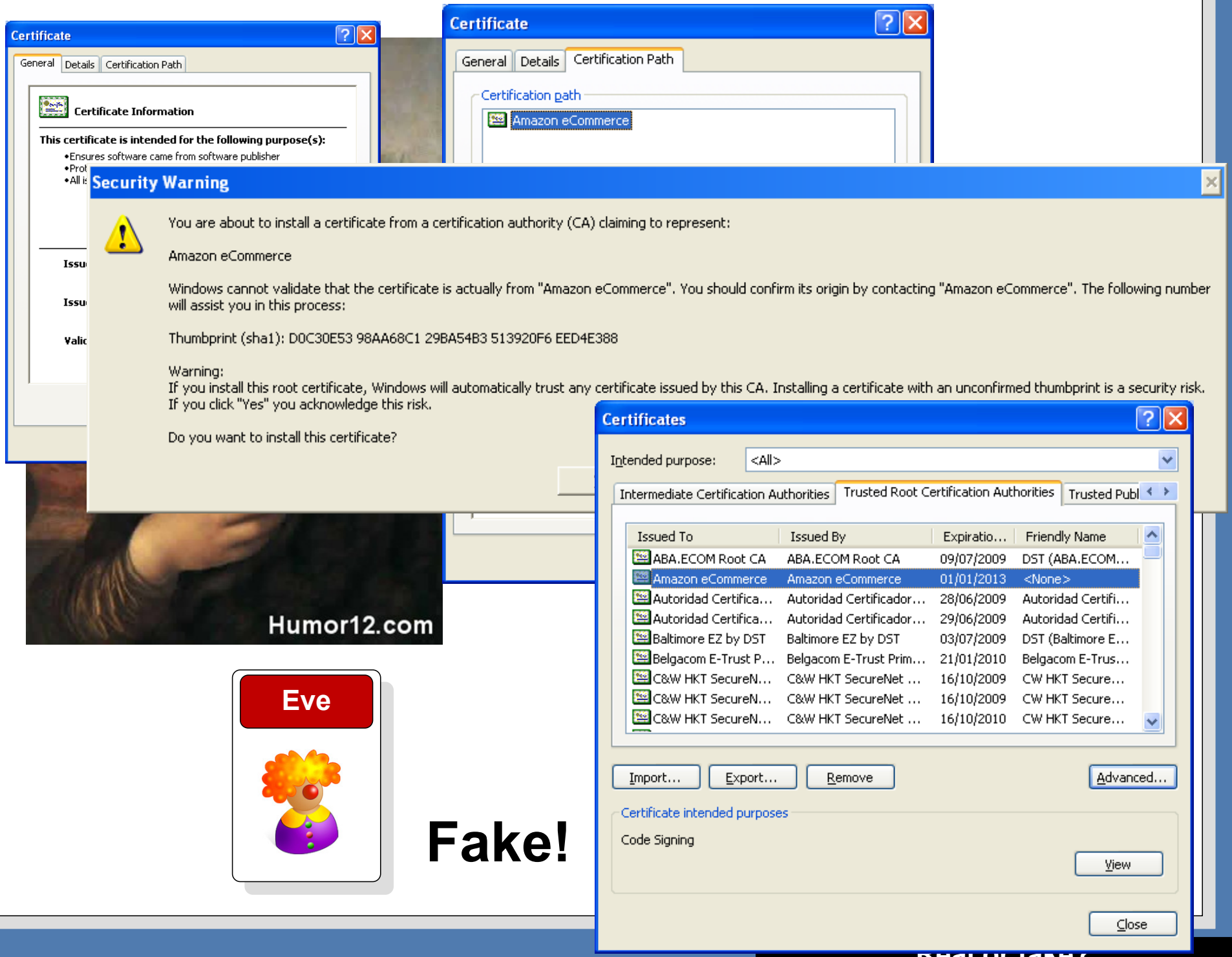

Humor12.com


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
•Ensures software came from software publisher
•Protects software from alteration after publication
•All issuance policies
Issued to: Amazon eCommerce
Issued by: Amazon eCommerce
Valid from 01/01/2007 to 01/01/2013
Issuer Statement
OK

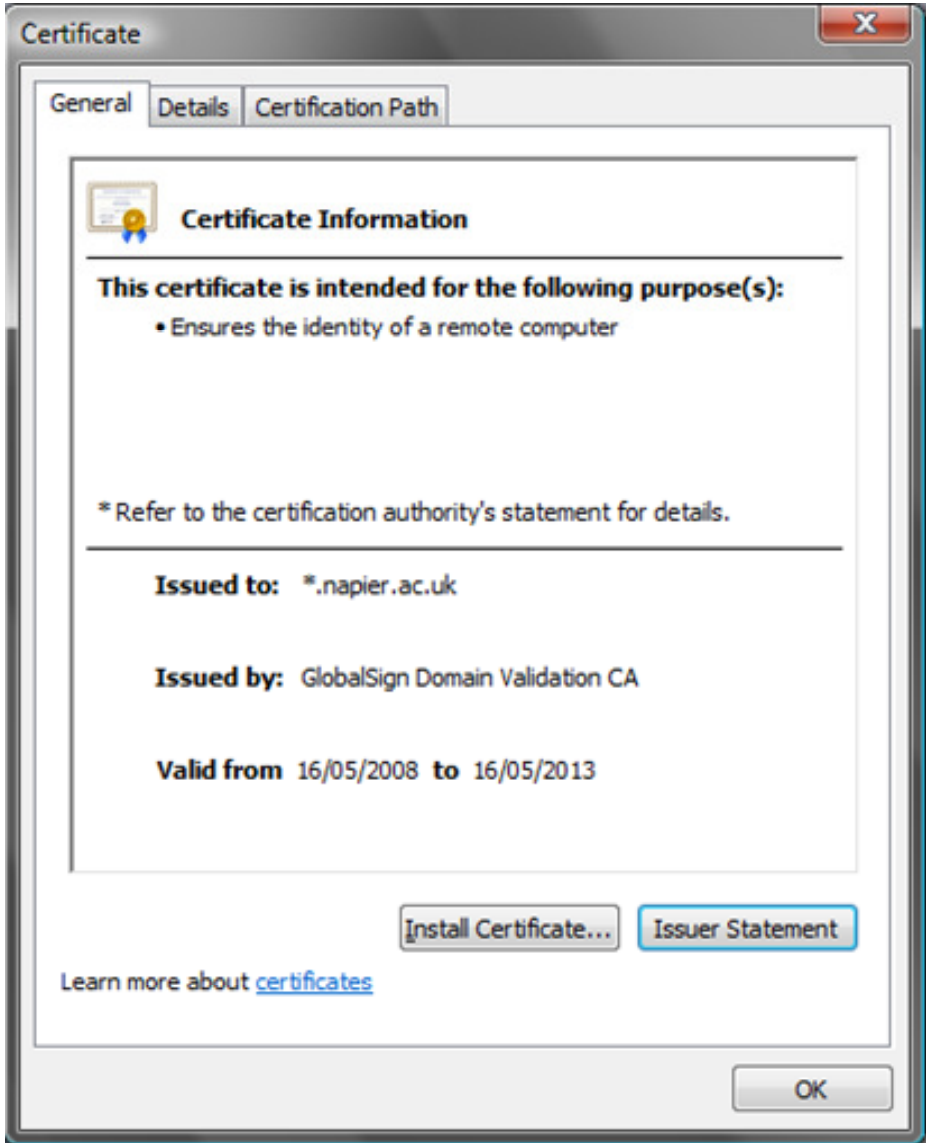

Bob


Eve

Real or fake?


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
•Ensures software came from software publisher
Certificate
General
Details
Certification Path
Certification path
Amazon eCommerce
Security Warning
You are about to install a certificate from a certification authority (CA) claiming to represent:
Amazon eCommerce
Windows cannot validate that the certificate is actually from "Amazon eCommerce". You should confirm its origin by contacting "Amazon eCommerce". The following number will assist you in this process:
Thumbprint (sha1): D0C30E53 98AA68C1 29BA54B3 513920F6 EED4E388
Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.
Do you want to install this certificate?
Humor12.com
Certificates
Intended purpose:
<All>
Intermediate Certification Authorities
Trusted Root Certification Authorities
Trusted Publ
Issued To
Issued By
Expiratio...
Friendly Name
ABA.ECOM Root CA
ABA.ECOM Root CA
09/07/2009
DST (ABA.ECOM...
Amazon eCommerce
Amazon eCommerce
01/01/2013
<None>
Autoridad Certifica...
Autoridad Certificador...
28/06/2009
Autoridad Certifi...
Autoridad Certifica...
Autoridad Certificador...
29/06/2009
Autoridad Certifi...
Baltimore EZ by DST
Baltimore EZ by DST
03/07/2009
DST (Baltimore E...
Belgacom E-Trust P...
Belgacom E-Trust Prim...
21/01/2010
Belgacom E-Trus...
C&W HKT SecureN...
C&W HKT SecureNet ...
16/10/2009
CW HKT Secure...
C&W HKT SecureN...
C&W HKT SecureNet ...
16/10/2009
CW HKT Secure...
C&W HKT SecureN...
C&W HKT SecureNet ...
16/10/2010
CW HKT Secure...
Import...
Export...
Remove
Advanced...
Certificate intended purposes
Code Signing
View
Close
Eve
Fake!

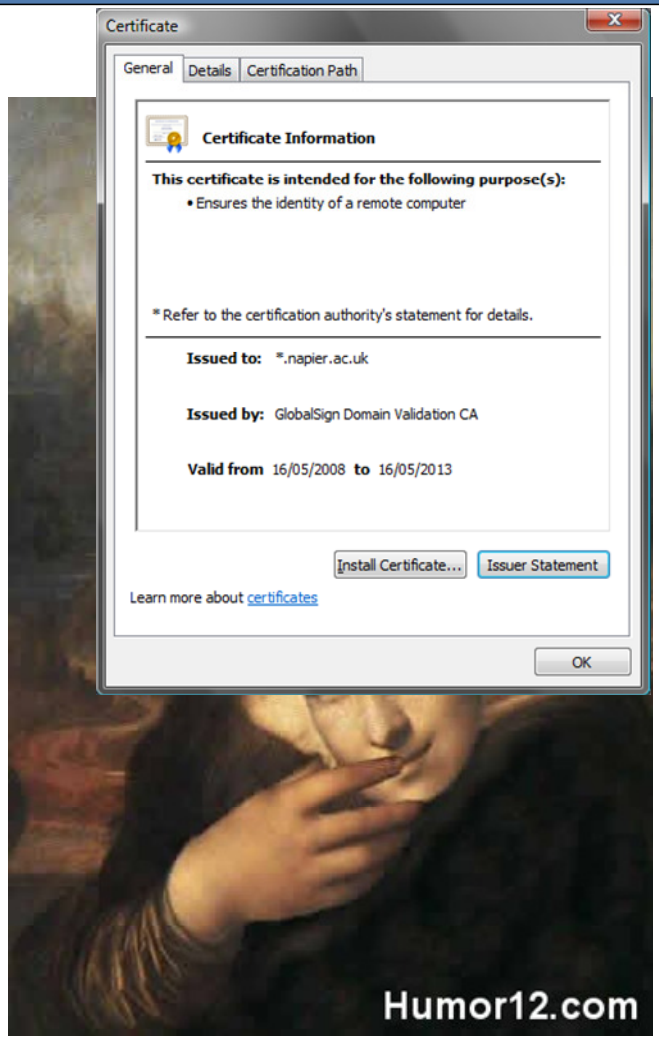

Humor12.com

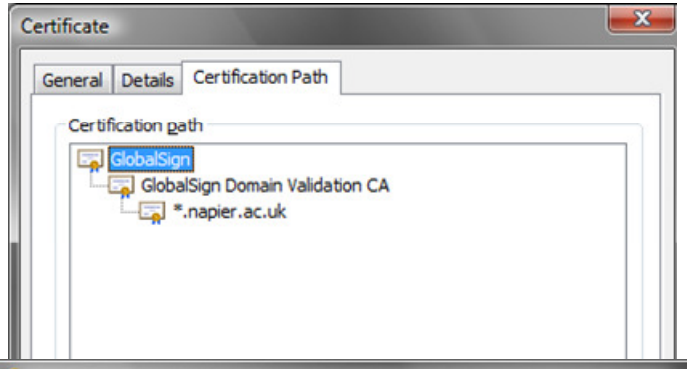

Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
* Refer to the certification authority's statement for details.
Issued to: *.napier.ac.uk
Issued by: GlobalSign Domain Validation CA
Valid from 16/05/2008 to 16/05/2013
Install Certificate...
Issuer Statement
Learn more about certificates
OK

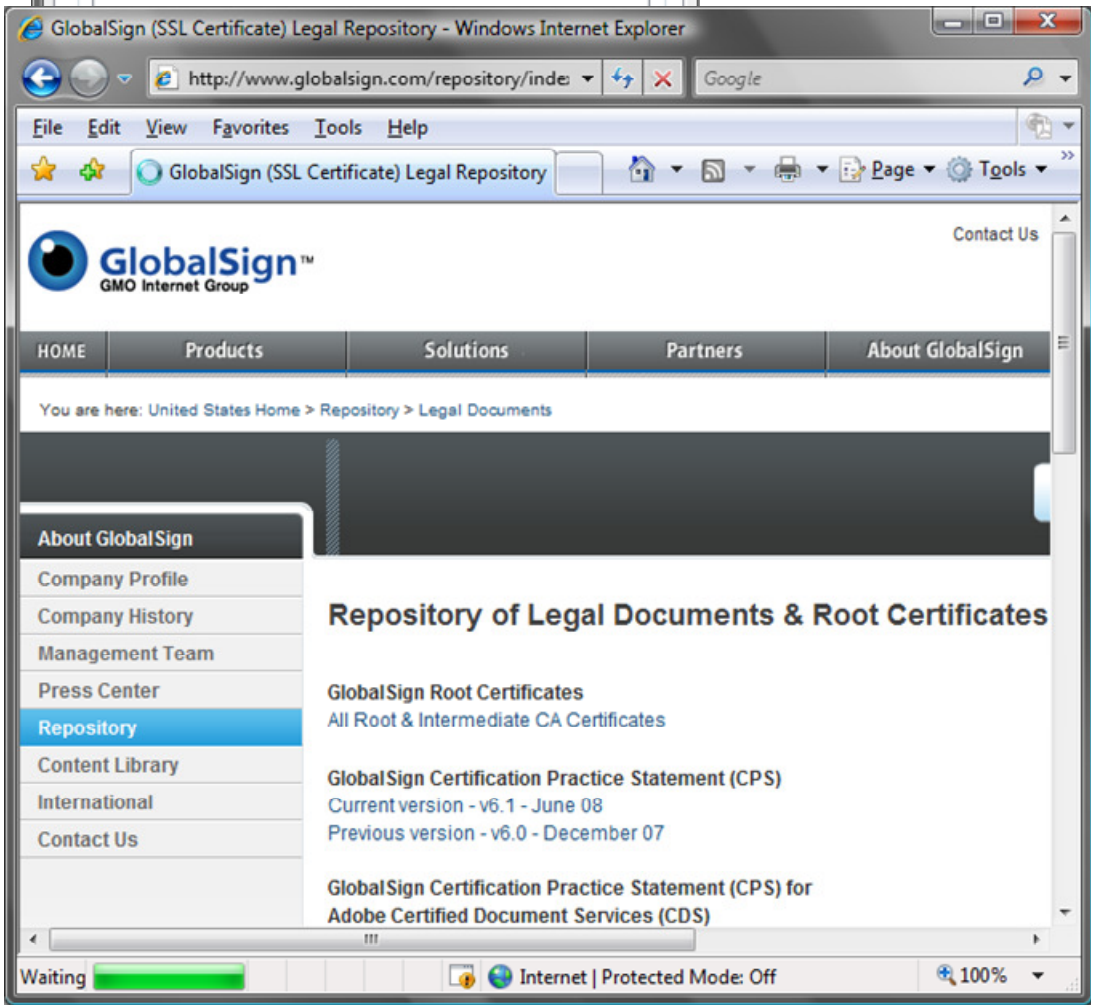

Bob

Eve

Real or fake?





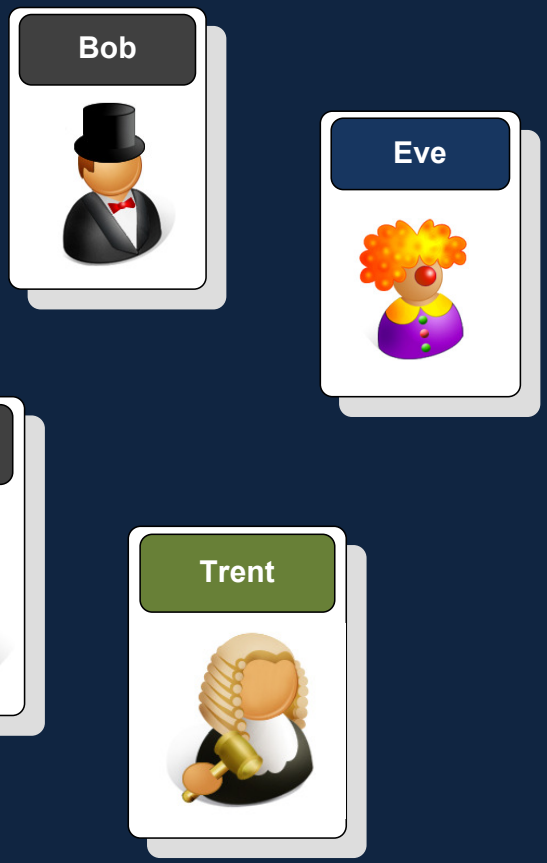


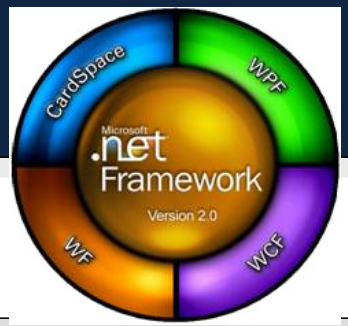
Real

Real or fake?

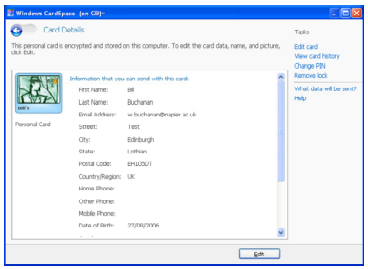
Authentication

- Introduction
- Methods
- Usernames/passwords
- Biometric issues
- Biometric methods
- Message hash
- Authenticating with private key
- HMAC
- Digital certificates
- Trust
- Cardspace
- Conclusions





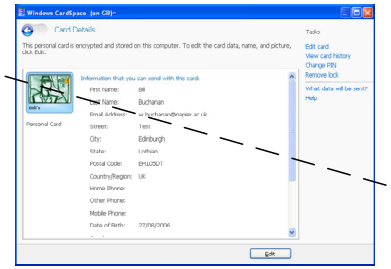
Cardspace



Roaming details

Personal Card

Secure communication of details



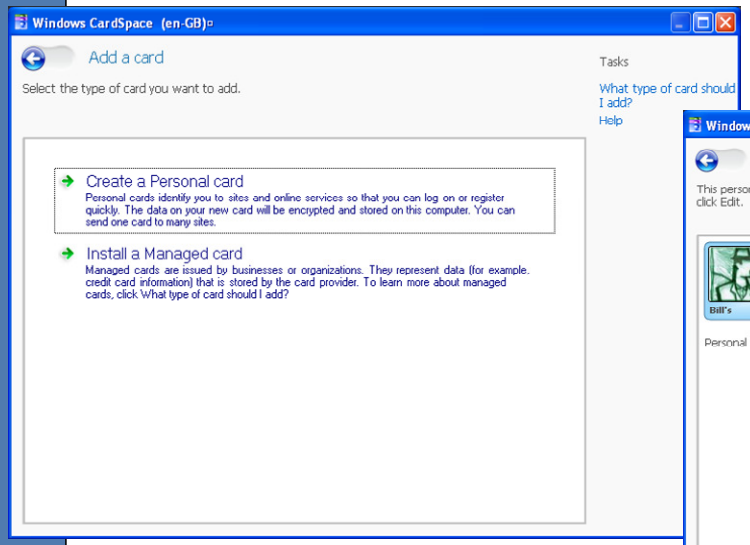
Secure storage of details

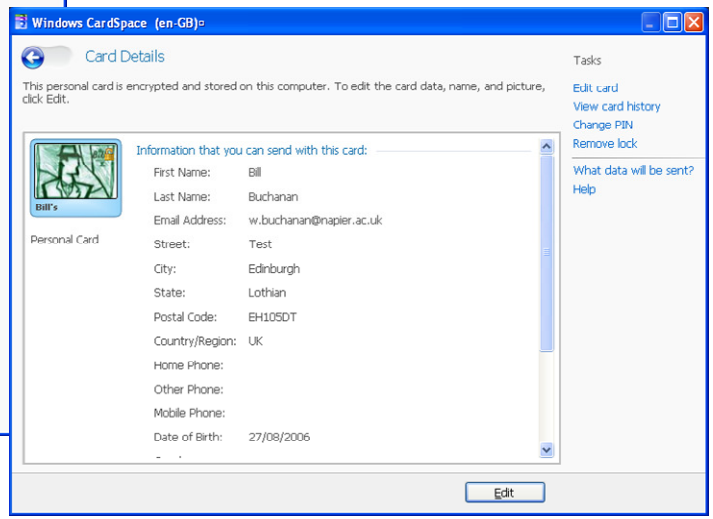
Managed Card
(for on-line purchases, managed logins, and so on

Verification of the user

Off machine storage

Storage of sensitive details
(such as credit card details, passwords, and so on)

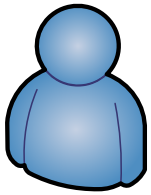


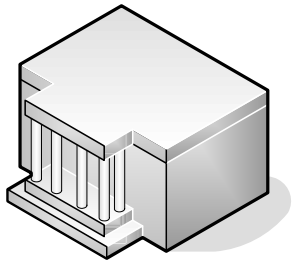


Personal cards:
- Created by the person.
- Encrypted.

Personal information:
Name, addresses, phone numbers, date of birth, and gender.

Additional:
Card name, card picture, and card creation date and a history of the sites where this card was used.

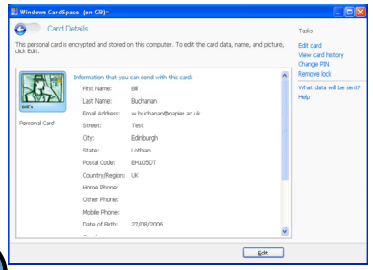




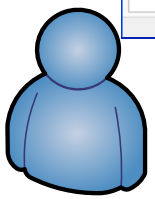
Managed Cards:
- Created by identity provider.
- Encrypted.

Information:
Maintained by IP that provides card.
Stored at site.
Some info on local machine (Card name, when installed, Valid until date, History of card)

Two types of card



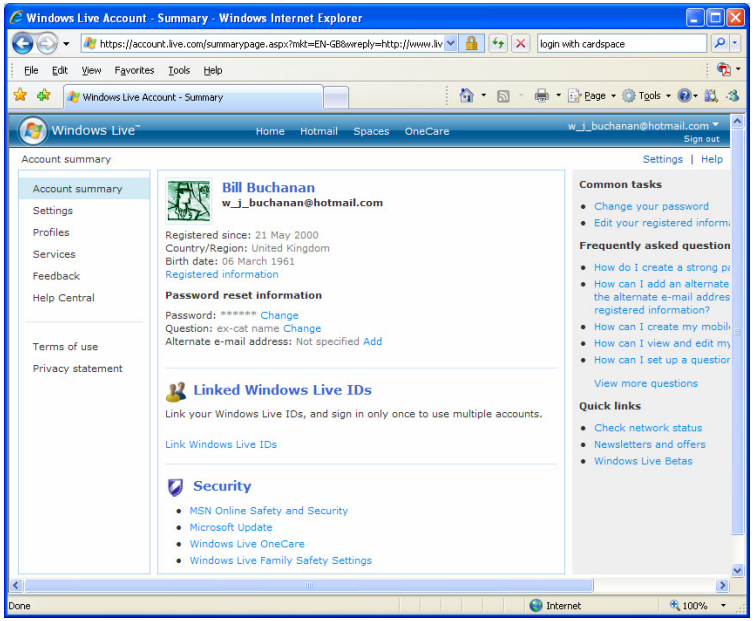
Personal Card

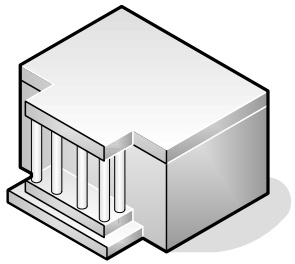


User

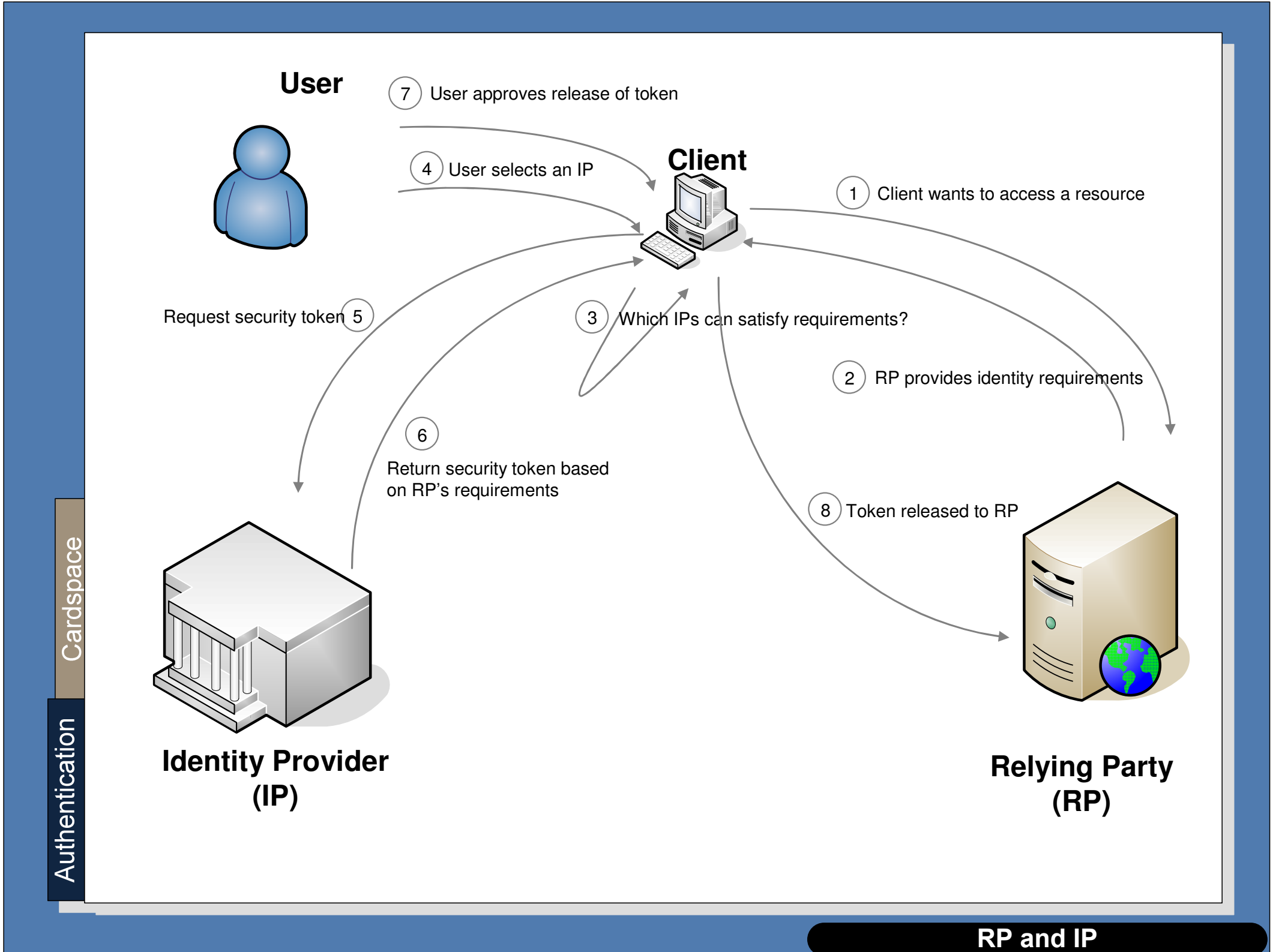
Name, addresses, phone numbers, date of birth, and gender.

Relying Parity (RP)



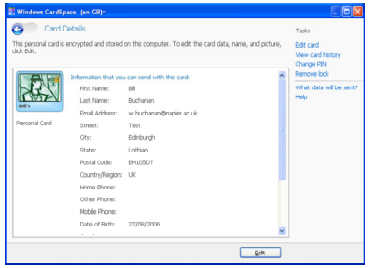


Identity Provider (IP)


User
7 User approves release of token
4 User selects an IP
Client
1 Client wants to access a resource
Request security token 5
3 Which IPs can satisfy requirements?
2 RP provides identity requirements
6
Return security token based
on RP's requirements
8 Token released to RP
Cardspace
Authentication
Identity Provider
(IP)
Relying Party
(RP)
RP and IP

Cardspace

Authentication



Identity

User

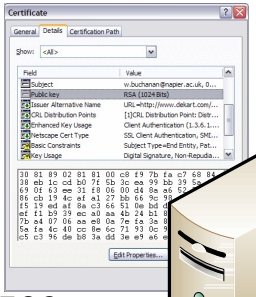
Identity selector

SAML (Security Assertion Markup Language)
Or Custom

WS-Security Policy
WS-Security

Relying Parity (RP)

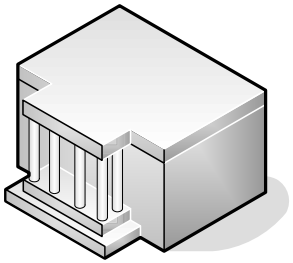
Security Token Service (STS)



X509 Certificate

Identity Provider (IP)

PKI Server
Digital Certificate Granter (Verisign)



Kerberos

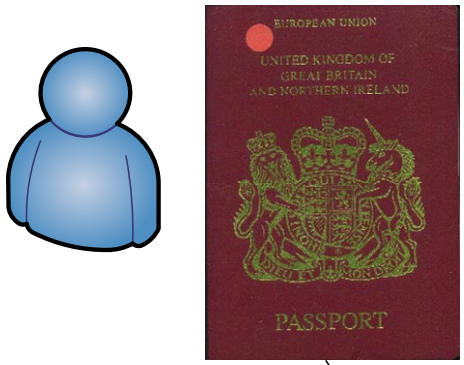
Open XML standards:
WS-*:-
WS-Trust, WS-Metadata Exchange Framework

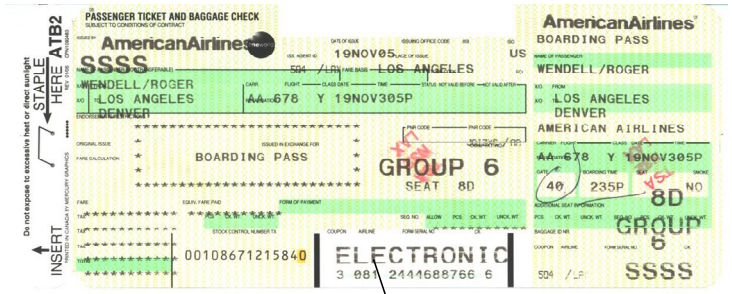
RP and IP

Cardspace

Authentication

Token





STS (Security Token Service)

Check in

Airline security

Relying Party

Trust

RP and IP

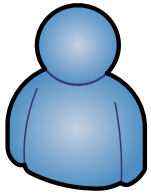
Cardspace

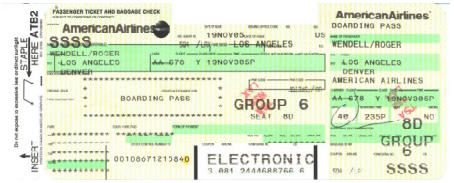
Authentication

STS

Check in

Trust Infrastructure





Token

STS

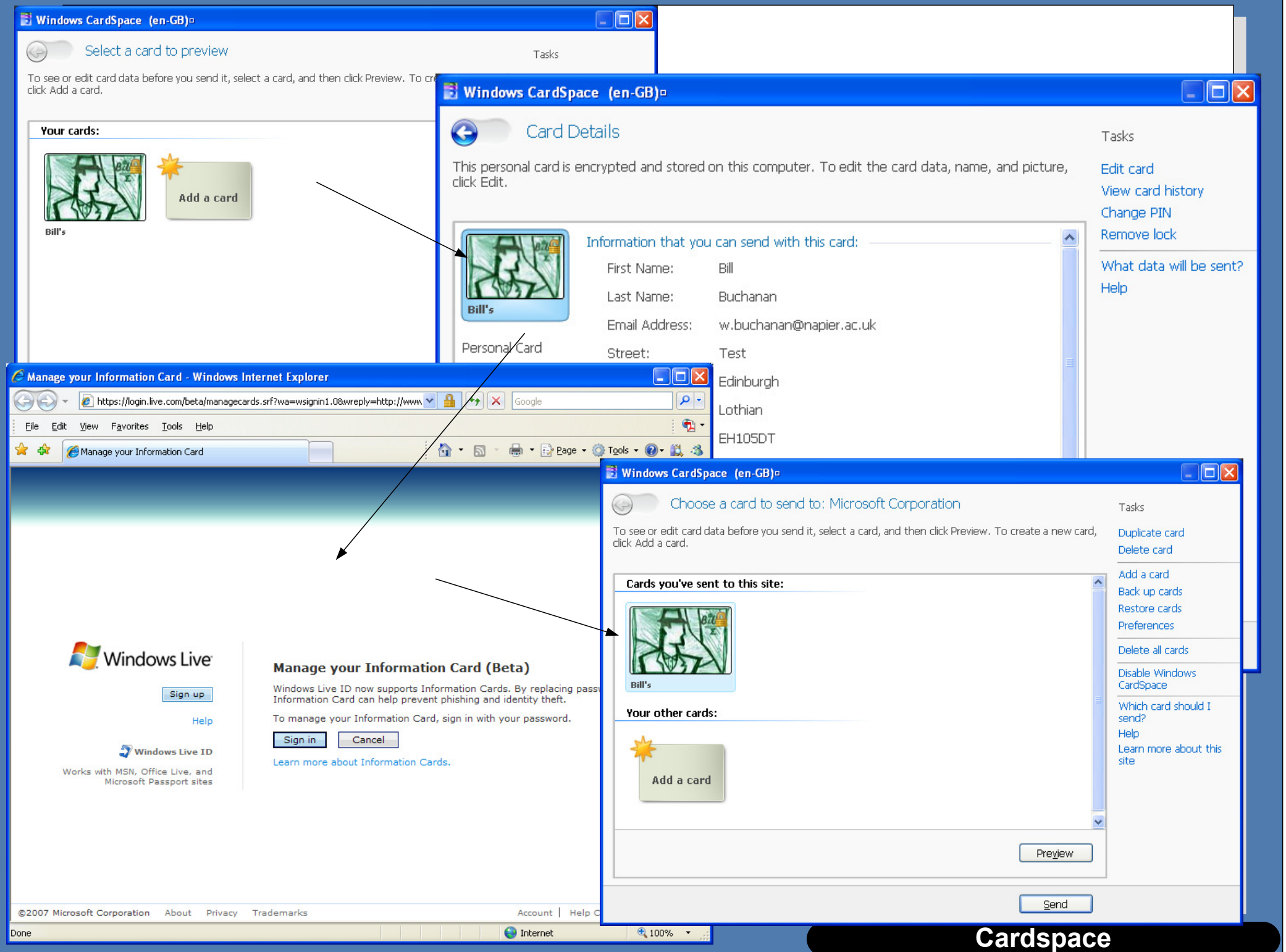
Check in

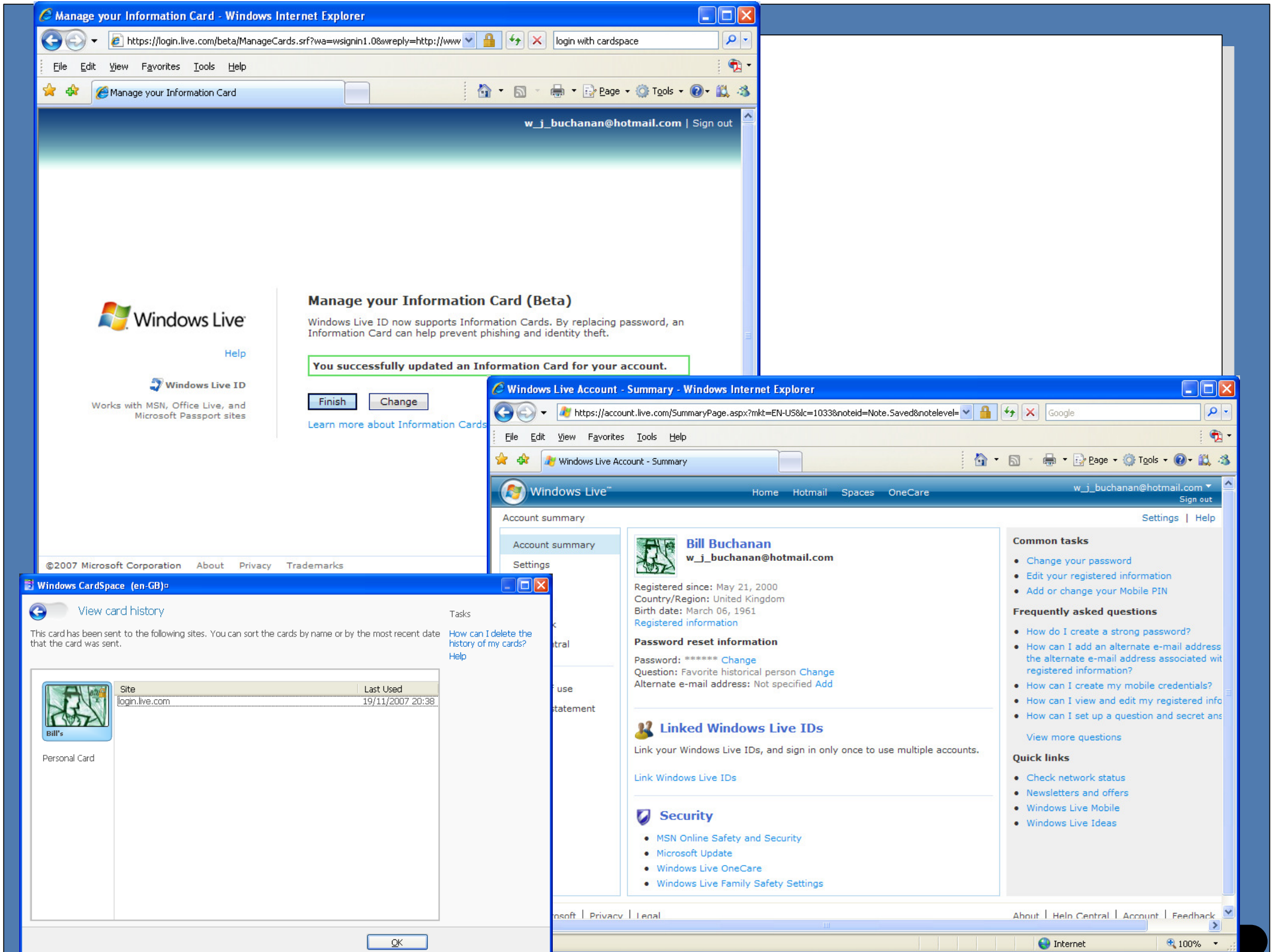
Trust

Airline security

Relying Party

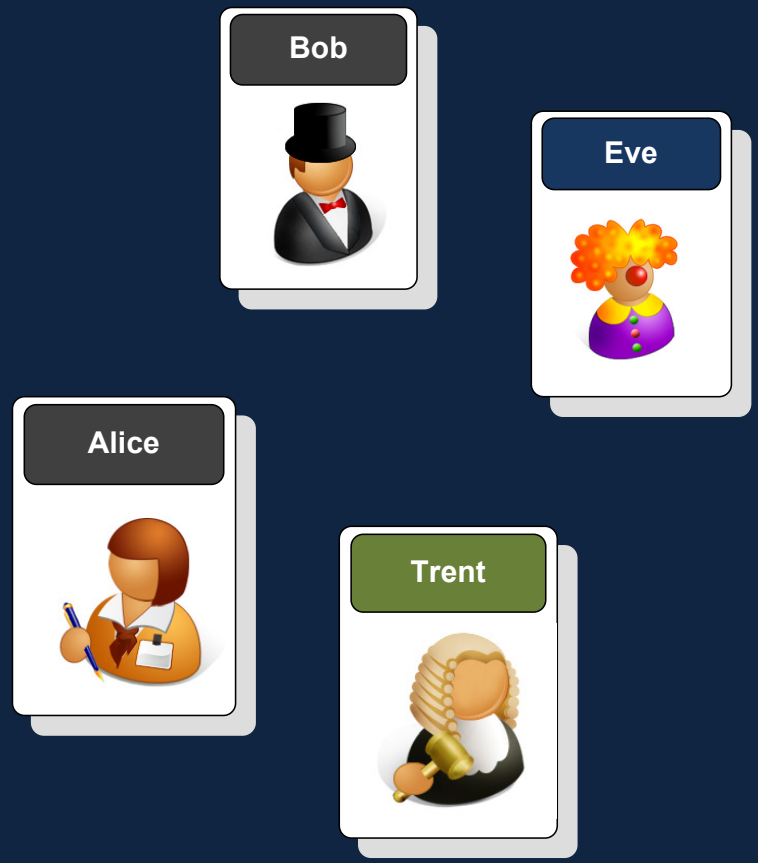
RP and IP


Windows CardSpace (en-GB)
Select a card to preview
Tasks
To see or edit card data before you send it, select a card, and then click Preview. To cr
click Add a card.
Your cards:
Bill's
Add a card
Windows CardSpace (en-GB)
Card Details
This personal card is encrypted and stored on this computer. To edit the card data, name, and picture, click Edit.
Tasks
Edit card
View card history
Change PIN
Remove lock
What data will be sent?
Help
Bill's
Personal Card
Information that you can send with this card:
First Name: Bill
Last Name: Buchanan
Email Address: w.buchanan@napier.ac.uk
Street: Test
Edinburgh
Lothian
EH105DT
Manage your Information Card - Windows Internet Explorer
https://login.live.com/beta/managecards.srf?wa=wsignin1.0&wreply=http://www
Google
File Edit View Favorites Tools Help
Manage your Information Card
Page Tools
Windows Live
Sign up
Help
Windows Live ID
Works with MSN, Office Live, and Microsoft Passport sites
Manage your Information Card (Beta)
Windows Live ID now supports Information Cards. By replacing pass
Information Card can help prevent phishing and identity theft.
To manage your Information Card, sign in with your password.
Sign in
Cancel
Learn more about Information Cards.
©2007 Microsoft Corporation About Privacy Trademarks
Account | Help C
Done
Internet
100%
Windows CardSpace (en-GB)
Choose a card to send to: Microsoft Corporation
To see or edit card data before you send it, select a card, and then click Preview. To create a new card, click Add a card.
Tasks
Duplicate card
Delete card
Add a card
Back up cards
Restore cards
Preferences
Delete all cards
Disable Windows CardSpace
Which card should I send?
Help
Learn more about this site
Cards you've sent to this site:
Bill's
Your other cards:
Add a card
Preview
Send
Cardspace

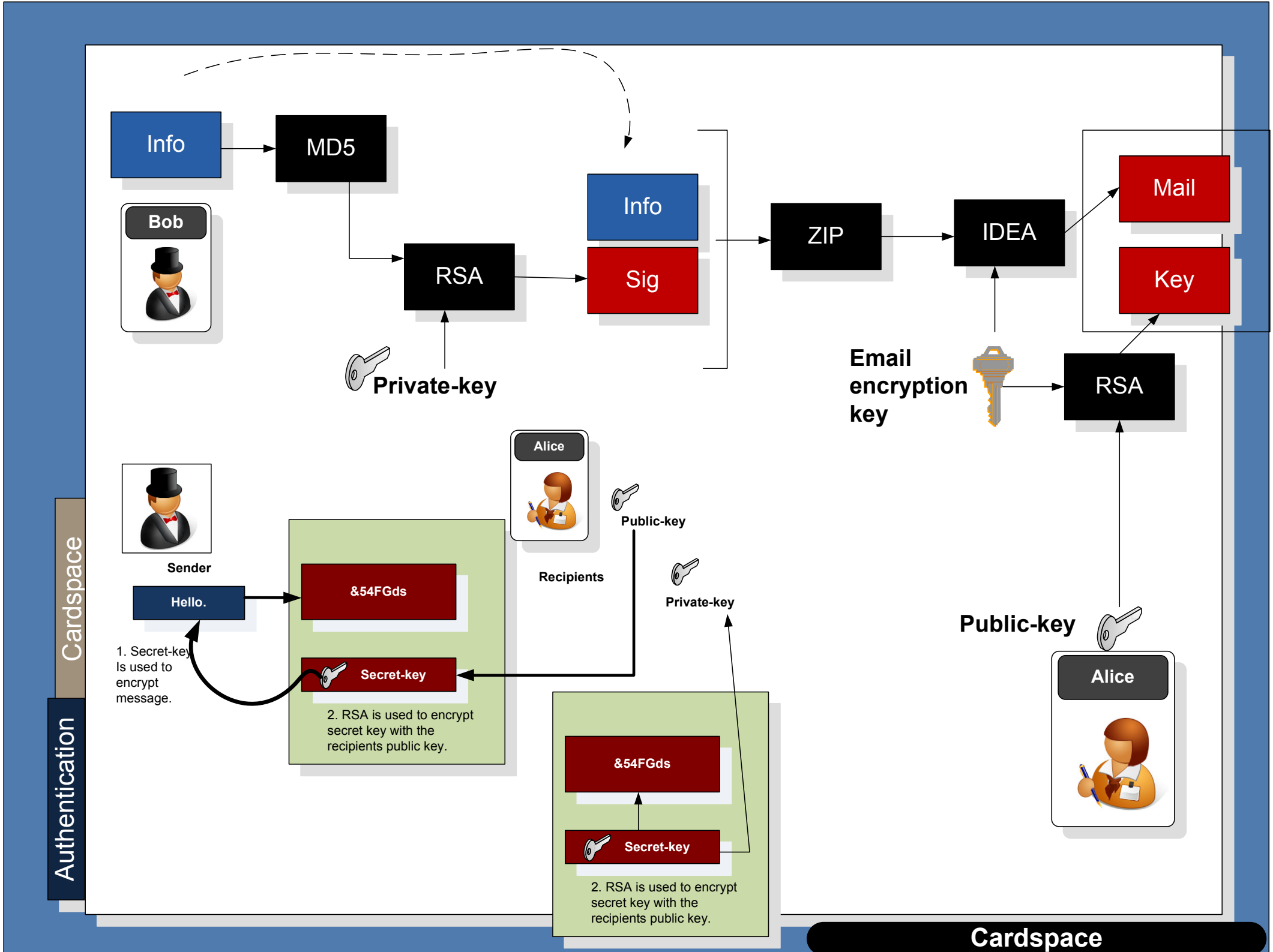

Manage your Information Card - Windows Internet Explorer
https://login.live.com/beta/ManageCards.srf?wa=wsignin1.0&wreply=http://www
login with cardspace
File Edit View Favorites Tools Help
Manage your Information Card
Page Tools
w_j_buchanan@hotmail.com | Sign out
Windows Live
Help
Windows Live ID
Works with MSN, Office Live, and Microsoft Passport sites
Manage your Information Card (Beta)
Windows Live ID now supports Information Cards. By replacing password, an Information Card can help prevent phishing and identity theft.
You successfully updated an Information Card for your account.
Finish
Change
Learn more about Information Cards
©2007 Microsoft Corporation About Privacy Trademarks
Windows Live Account - Summary - Windows Internet Explorer
https://account.live.com/SummaryPage.aspx?mkt=EN-US&lc=1033&noteid=Note.Saved&notelevel=
Google
File Edit View Favorites Tools Help
Windows Live Account - Summary
Page Tools
Windows Live
Home Hotmail Spaces OneCare
w_j_buchanan@hotmail.com
Sign out
Account summary
Settings | Help
Account summary
Settings
Bill Buchanan
w_j_buchanan@hotmail.com
Registered since: May 21, 2000
Country/Region: United Kingdom
Birth date: March 06, 1961
Registered information
Password reset information
Password: ****** Change
Question: Favorite historical person Change
Alternate e-mail address: Not specified Add
Linked Windows Live IDs
Link your Windows Live IDs, and sign in only once to use multiple accounts.
Link Windows Live IDs
Security
MSN Online Safety and Security
Microsoft Update
Windows Live OneCare
Windows Live Family Safety Settings
Common tasks
Change your password
Edit your registered information
Add or change your Mobile PIN
Frequently asked questions
How do I create a strong password?
How can I add an alternate e-mail address
the alternate e-mail address associated wit
registered information?
How can I create my mobile credentials?
How can I view and edit my registered info
How can I set up a question and secret ans
View more questions
Quick links
Check network status
Newsletters and offers
Windows Live Mobile
Windows Live Ideas
About | Help Central | Account | Feedback
Internet
100%
Windows CardSpace (en-GB)
View card history
This card has been sent to the following sites. You can sort the cards by name or by the most recent date that the card was sent.
Tasks
How can I delete the history of my cards?
Help
Site
Last Used
login.live.com
19/11/2007 20:38
Bill's
Personal Card
OK

Authentication

- Introduction
- Methods
- Usernames/passwords
- Biometric issues
- Biometric methods
- Message hash
- Authenticating with private key
- HMAC
- Digital certificates
- Trust
- Cardspace
- Email encryption
- Conclusions

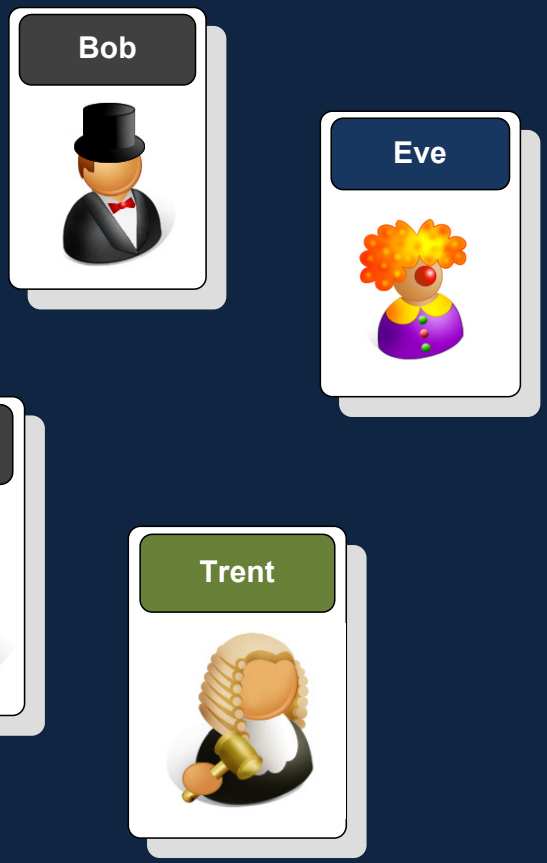


Email encryption


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

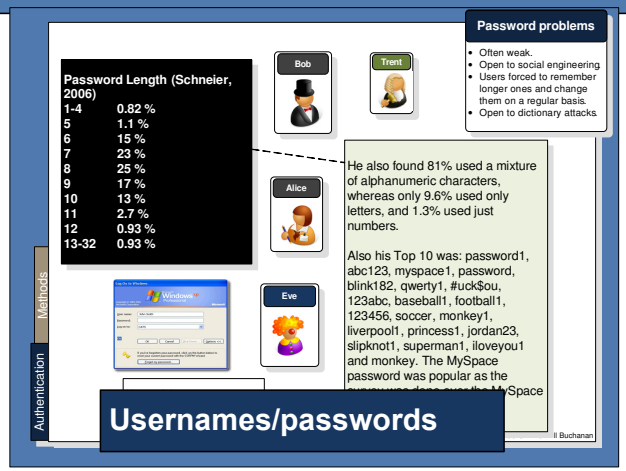
Authentication

Introduction
Methods
Usernames/passwords
Biometric issues
Biometric methods
Message hash
Authenticating with private key
HMAC
Digital certificates
Trust
Cardspace
Email encryption
Conclusions

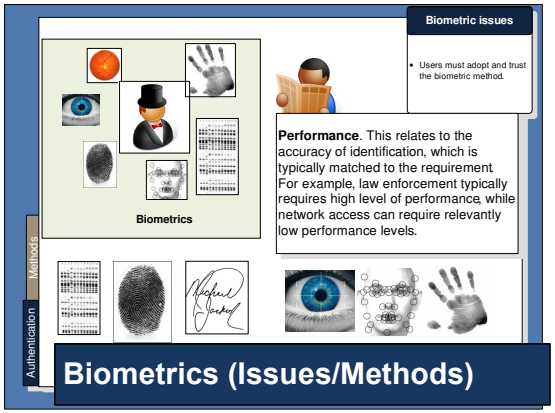


Conclusions

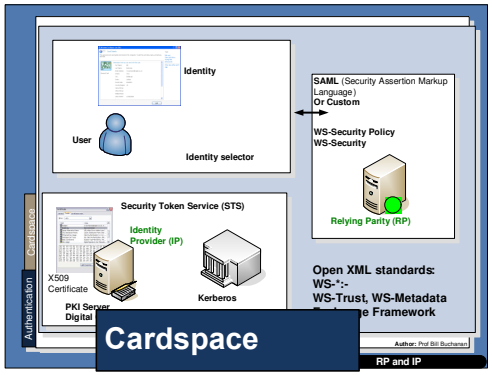
What we're authenticating



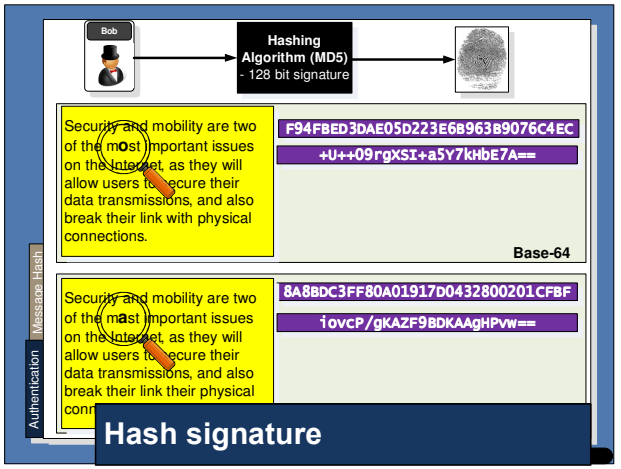
Usernames/passwords



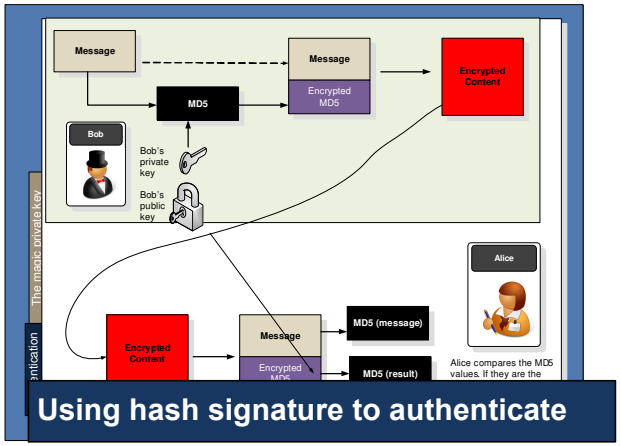
Biometrics (Issues/Methods)



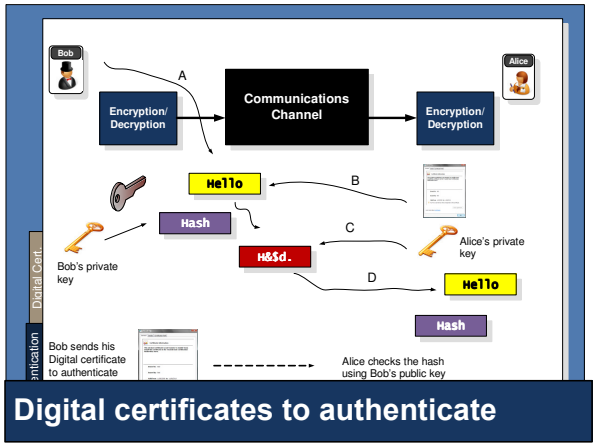
Cardspace



Hash signature



Using hash signature to authenticate



Digital certificates to authenticate