claredi

HIPAA and Electronic Signatures

NCVHS

December 8, 2004

Kepa Zubeldia, M.D.

Topics

- HIPAA Statute Text
- Types of signature
- Encryption, Decryption, PKI
- Electronic vs. Digital signatures
- Digital Certificates
- PKI Standards
- Signature Standards

PL 104-191 HIPAA

Sec. 1173 (a)

- (1) IN GENERAL. The Secretary shall adopt standards for transactions, and data elements for such transactions, to enable health information to be exchanged electronically, that are appropriate for—
  - (A) the financial and administrative transactions described in paragraph (2); and
  - Other financial and administrative transactions determined appropriate by the Secretary, consistent with the goals of improving the operation of the health care system and reducing administrative costs.

Sec. 1173 (e) Electronic Signature

- Sec. 1173 (e) Electronic Signature.
  - (1) STANDARDS. The Secretary, in coordination with the Secretary of Commerce, shall adopt standards specifying procedures for the electronic transmission and authentication of signatures with respect to the transactions referred to in subsection (a)(1).
  - (2) EFFECT OF COMPLIANCE. Compliance with the standards adopted under paragraph (1) shall be deemed to satisfy Federal and State statutory requirements for written signatures with respect to the transactions referred to in subsection (a)(1).

Questions

- Standard procedures for “transmission” and “authentication” of signatures.
  - What did they mean ?
- For the HIPAA standard transactions
  - None of which require a signature today.
- But…
  - In the future some claims attachments may require signatures (e.g. consents).
  - In the future some new transactions may require signatures (e.g. scripts, medical record)

Food for thought

- HIPAA Signatures are separate from HIPAA Security requirements.
- Signature as a proof of “intent” rather than a security mechanism?
- What does it mean to “sign” an EDI file?
  - Most of the time the EDI data content is “obscure” to the untrained eye.
  - Intent?
  - Consent?
  - Assertion?
  - Or is it just a data integrity security protection?

Electronic Signature

- An electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by the person with the intent to sign the record.

Electronic Signatures in Global and National Commerce (ESIGN) Act, Signed into law by President Bill Clinton on June 30, 2000

Electronic Signatures

- ESIGN Act passed in the summer of 2000
- Allows electronic record keeping
- Allows electronic signatures
  - Must have the “intent” to sign
  - Any electronic “mark” may be used
  - Technology independent
  - Risk of using “weak” methods
  - Simple to explain

Sample audio signature

🔊

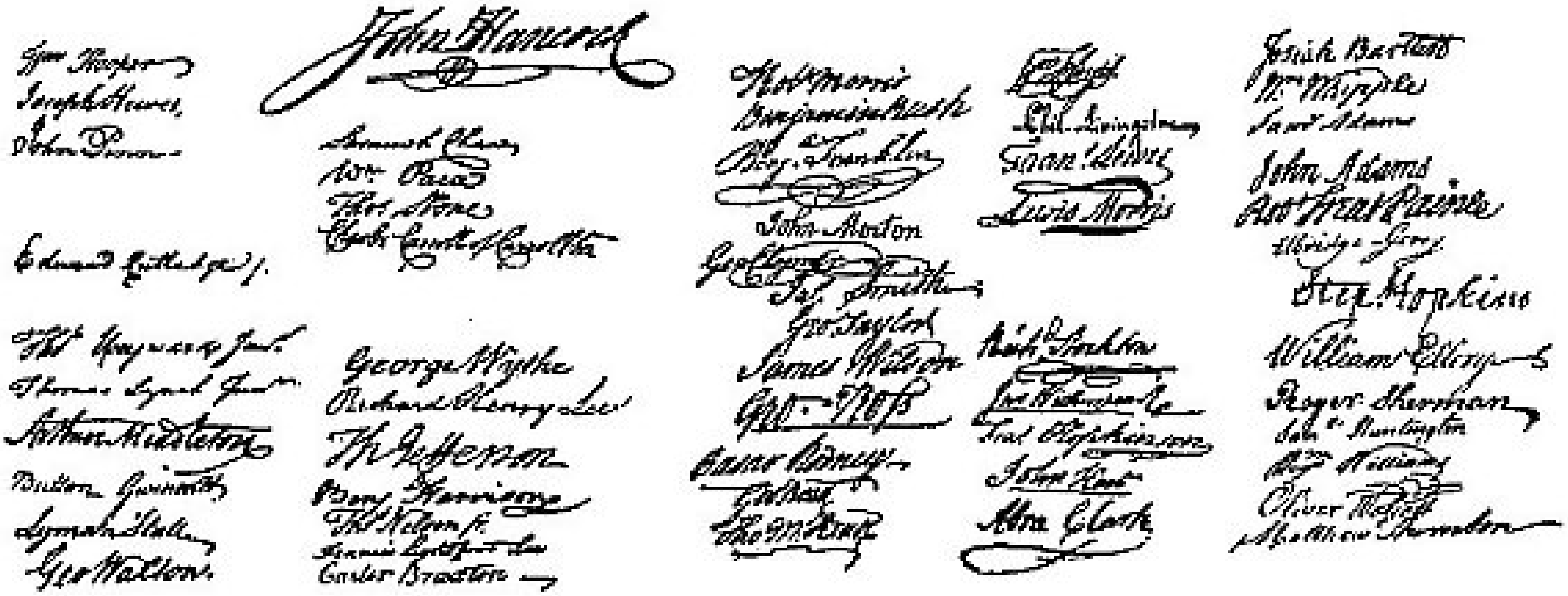
- Legally valid. Effective.
- Low Tech. Easy to understand.
- Easy to capture by most PCs.
- Weakly bound to the document.
- Easy to forge.

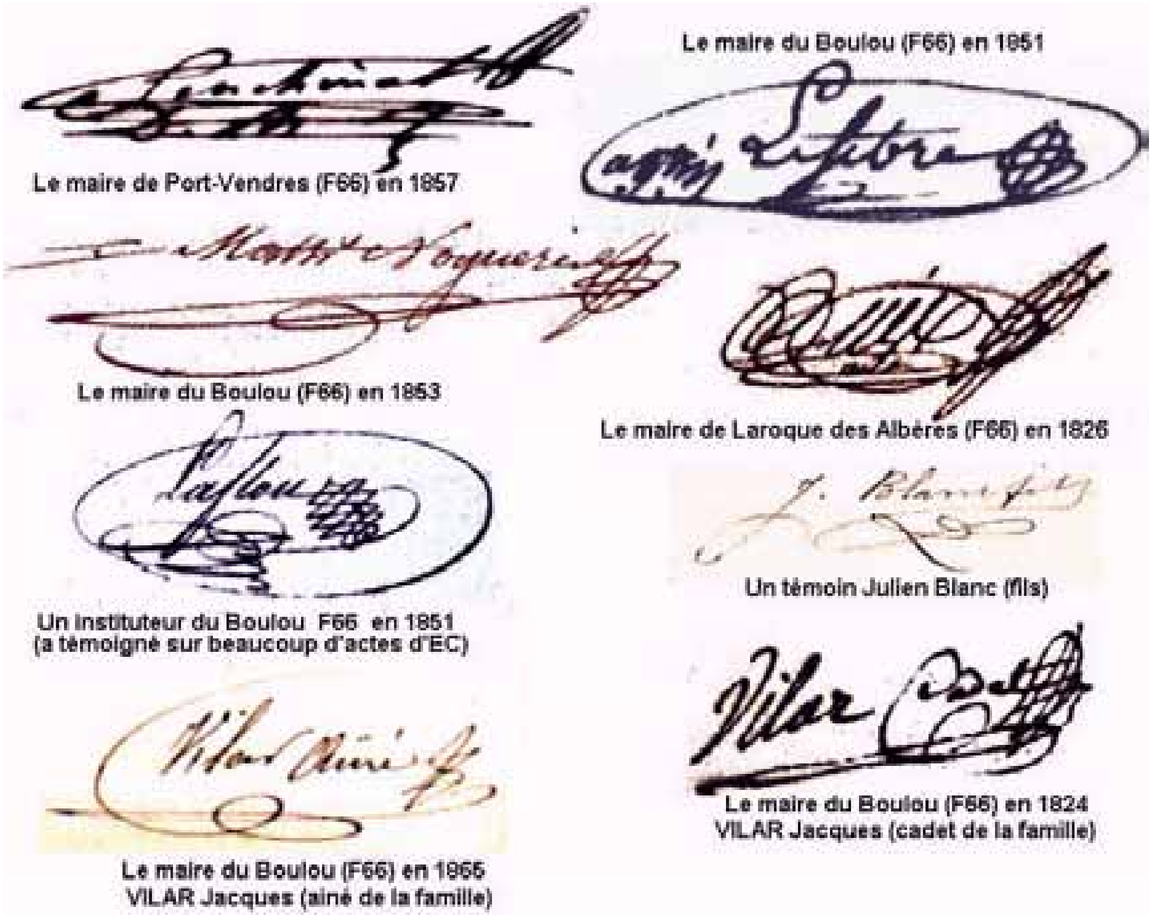
Sample Electronic Signature

- Used by UPS drivers, CompUSA, Service Merchandise, etc.

Bart Simpson

- Simple implementations
  - Weak method, easy to copy.
- Strong technology is also available: “Signature Dynamics”
  - Linked to the document
  - Prevents duplication
  - Can use a digital certificate


Wm Hooper
Joseph Hewes,
John Penn
Edward Rutledge 1.
Thos Heyward Junr.
Thomas Lynch Junr.
Arthur Middleton
Button Gwinnett
Lyman Hall
Geo Walton.
John Hancock
Samuel Chase
Wm. Paca
Thos. Stone
Charles Carroll of Carrollton
George Wythe
Richard Henry Lee
Th Jefferson
Benja. Harrison
Thos Nelson jr.
Francis Lightfoot Lee
Carter Braxton
Robt Morris
Benjamin Rush
Benja. Franklin
John Morton
Geo Clymer
Jas. Smith
Geo. Taylor
James Wilson
Geo. Ross
Caesar Rodney
Geo Read
Tho M:Kean
Wm Floyd
Phil. Livingston
Frans. Lewis
Lewis Morris
Richd. Stockton
Jno Witherspoon
Fras. Hopkinson
John Hart
Abra Clark
Josiah Bartlett
Wm. Whipple
Saml Adams
John Adams
Robt Treat Paine
Elbridge Gerry
Step. Hopkins
William Ellery
Roger Sherman
Saml Huntington
Wm Williams
Oliver Wolcott
Matthew Thornton



Le maire de Port-Vendres (F66) en 1857

Le maire du Boulou (F66) en 1851

Le maire du Boulou (F66) en 1853

Le maire de Laroque des Albères (F66) en 1826

Un instituteur du Boulou F66 en 1851
(a témoigné sur beaucoup d'actes d'EC)

Un témoin Julien Blanc (fils)

Le maire du Boulou (F66) en 1824
VILAR Jacques (cadet de la famille)

Le maire du Boulou (F66) en 1865
VILAR Jacques (aîné de la famille)

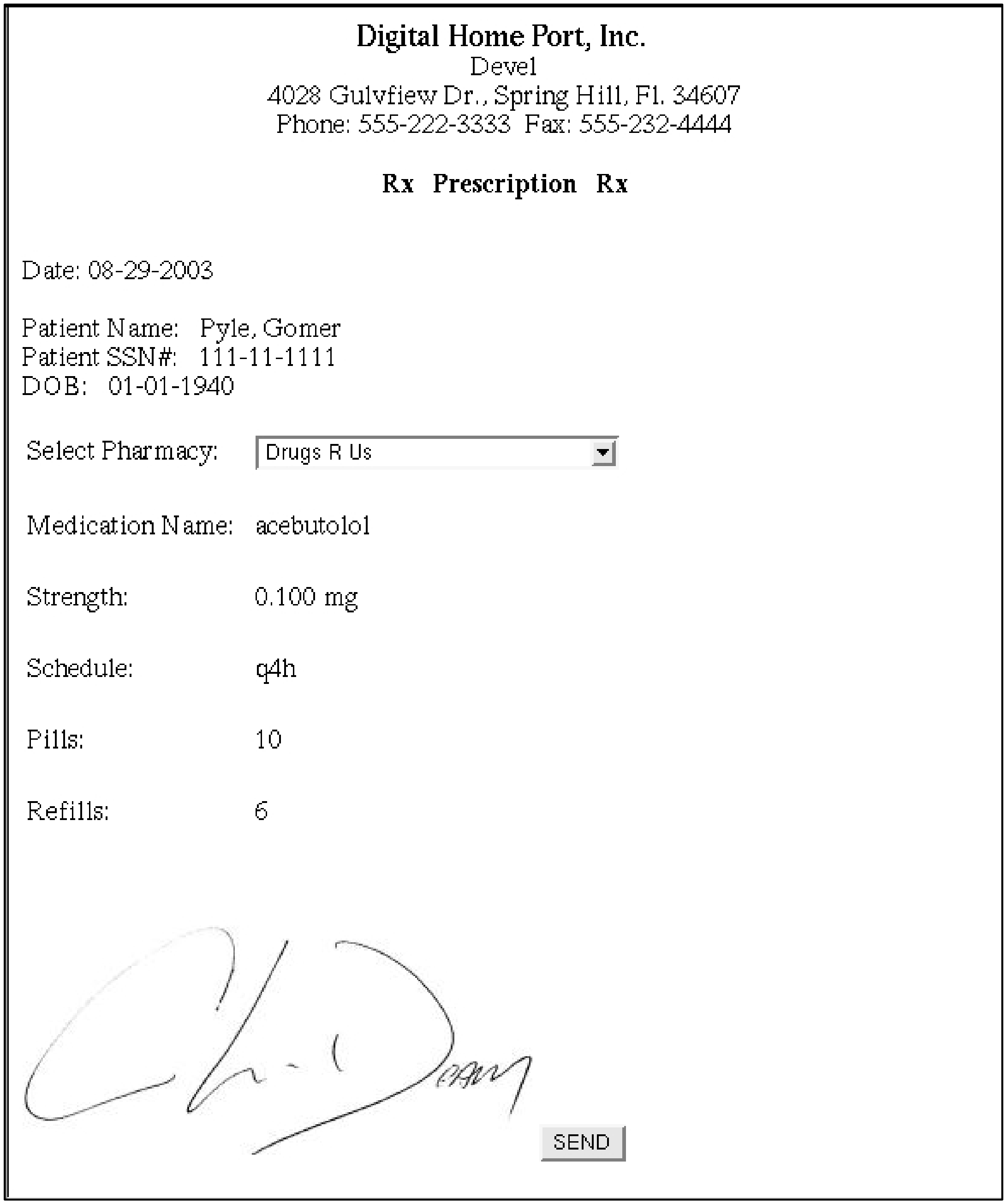
Signature Dynamics

- Signature characteristics captured in real time
  - X and Y coordinates
  - Pressure, Velocity, Acceleration
  - Time
- Signed with a stylus on a digitizing pad
- Associated with a specific signed document through a “hash”
  - If the document changes, signature is invalidated
- Signer’s identity can be determined
  - Forensic signature analysis as on paper signatures
  - Digital Certificate issued by a Certification Authority

Signature Dynamics in Practice

- Legally binding in all 50 states and in some foreign countries
  - ESIGN Act binding in USA
  - Used by the IRS for tax forms
- Technology-dependent
  - PenOp, Topaz, Cyber-SIGN, others
  - **No** interoperability among competing systems

Please Sign.



Digital Home Port, Inc.
Devel
4028 Gulvfiew Dr., Spring Hill, Fl. 34607
Phone: 555-222-3333 Fax: 555-232-4444

Rx Prescription Rx

Date: 08-29-2003

Patient Name: Pyle, Gomer
Patient SSN#: 111-11-1111
DOB: 01-01-1940

Select Pharmacy: Drugs R Us

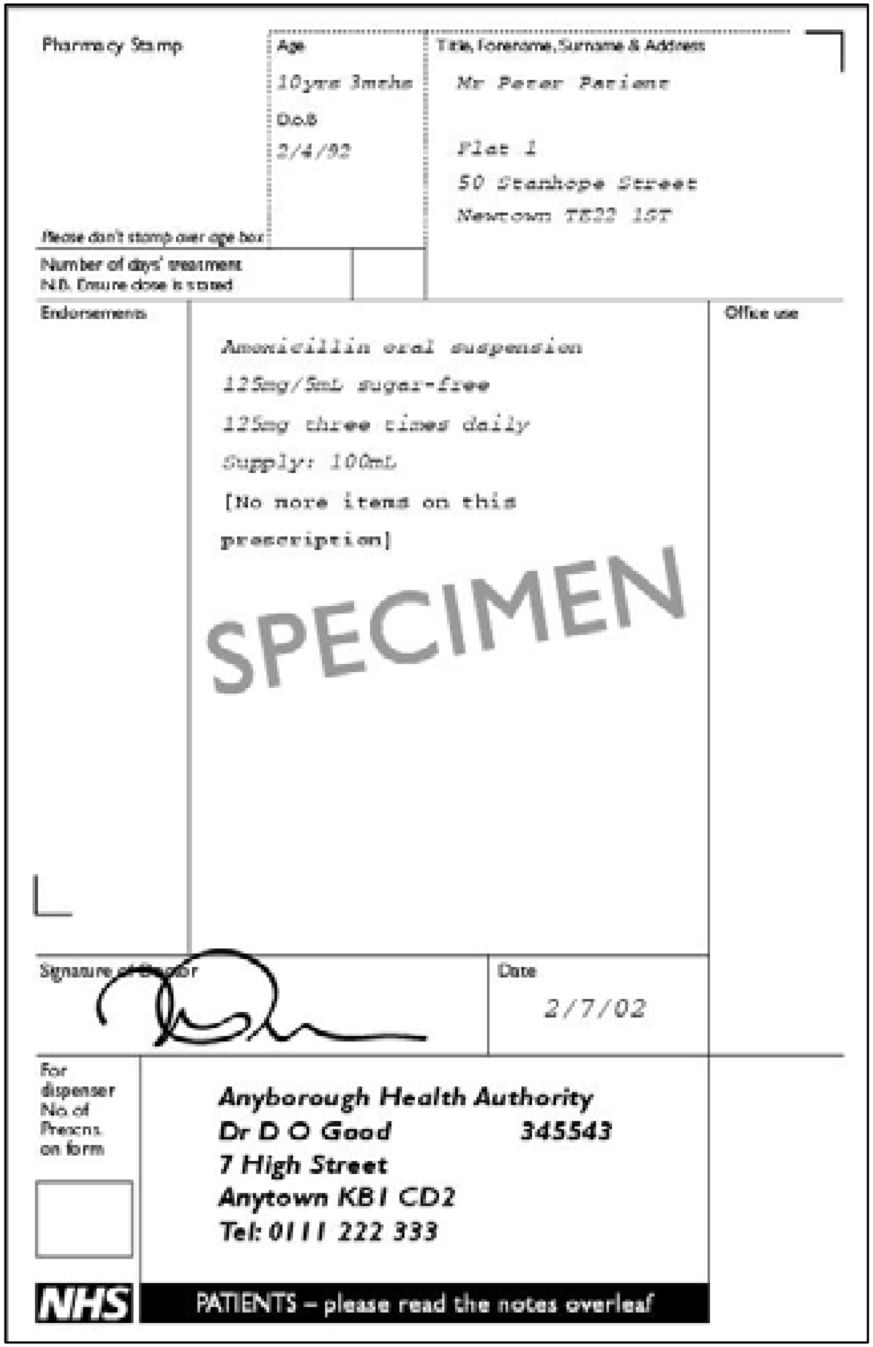
Medication Name: acebutolol

Strength: 0.100 mg

Schedule: q4h

Pills: 10

Refills: 6



Pharmacy Stamp

Age
10yrs 3mths
D.o.B
2/4/92

Title, Forename, Surname & Address
Mr Peter Patient

Flat 1
50 Stanhope Street
Newtown TE22 1ST

Please don't stamp over age box

Number of days' treatment
N.B. Ensure dose is stated

Endorsements

Amoxicillin oral suspension
125mg/5mL sugar-free
125mg three times daily
Supply: 100mL
[No more items on this
prescription]

SPECIMEN

Office use

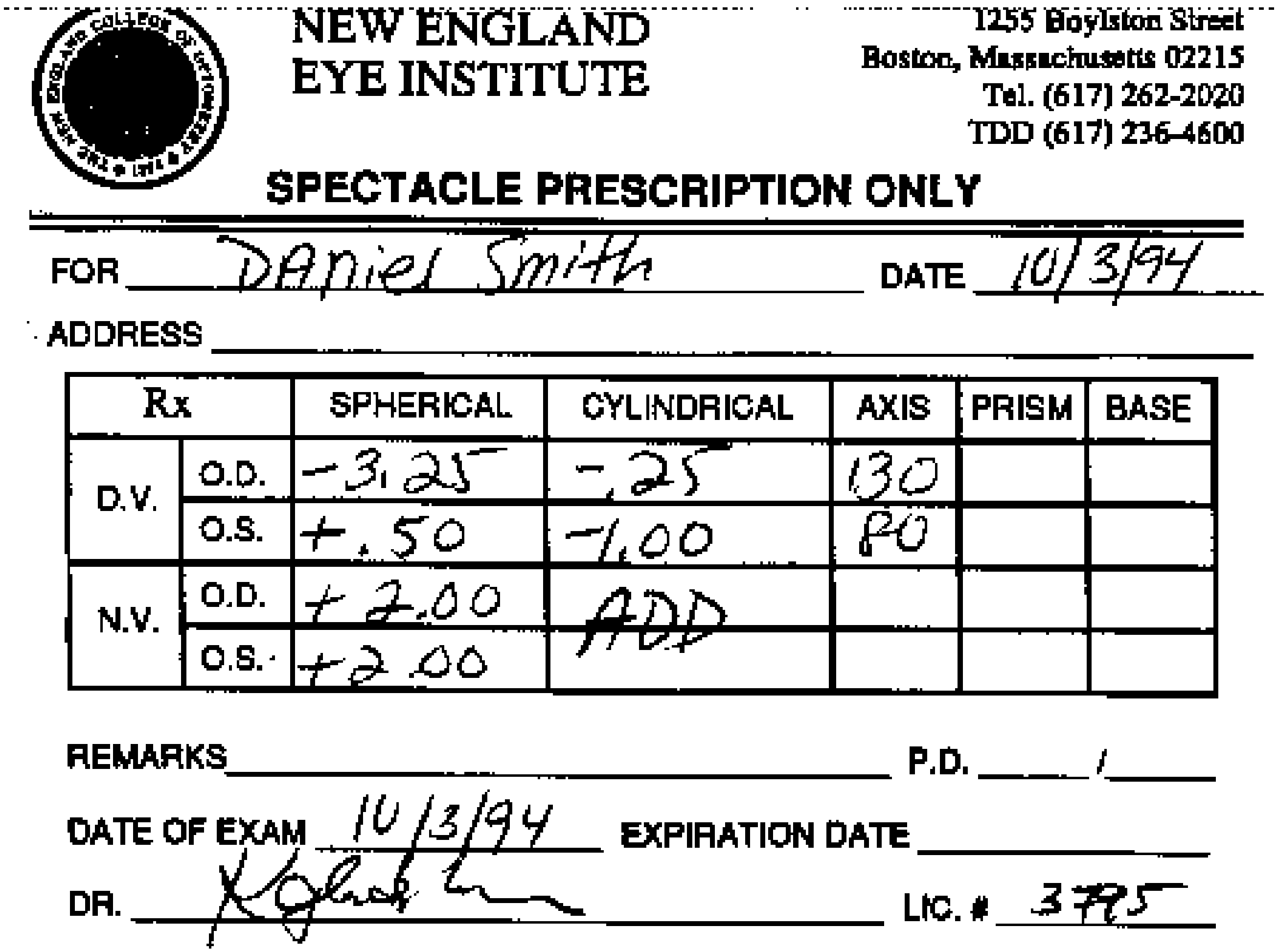
Signature of Doctor

Date
2/7/02

For dispenser
No. of Prescns. on form
□

Anyborough Health Authority
Dr D O Good 345543
7 High Street
Anytown KB1 CD2
Tel: 0111 222 333

NHS
PATIENTS – please read the notes overleaf



NEW ENGLAND
EYE INSTITUTE

1255 Boylston Street
Boston, Massachusetts 02215
Tel. (617) 262-2020
TDD (617) 236-4600

SPECTACLE PRESCRIPTION ONLY

FOR Daniel Smith DATE 10/3/94

ADDRESS

Rx		SPHERICAL	CYLINDRICAL	AXIS	PRISM	BASE
D.V.	O.D.	-3.25	-.25	130		
	O.S.	+.50	-1.00	80		
N.V.	O.D.	+2.00	ADD			
	O.S.	+2.00				

REMARKS P.D. /

DATE OF EXAM 10/3/94 EXPIRATION DATE

DR. LIC. # 3795

HIPAA Requirements

- Standard for electronic transmission
- Standard for authentication
- For HIPAA transactions

Electronic Signature (of another kind)

HP5006A Signature Analyzer

HP’s patented Signature Analysis technique enables the HP5006A to generate a compressed, four digit “fingerprint” or signature of the digital data stream at a logic node. Any fault associated with a device connected through the node will force a change in the data stream and, consequently, produce an erroneous signature.

Message Digest

- One-way transformation of an entire message into a single number
  - Checksum
    - Simple algorithm produces 1 byte checksum
    - Validates a short number (credit card, NPI)
  - CRC
    - More complex algorithm produces 2-3 bytes
    - Validates longer data streams (TCP/IP, SNA)
  - Cryptographic hash
    - Complex algorithm produces 16-32 bytes
    - Validates large amounts of data

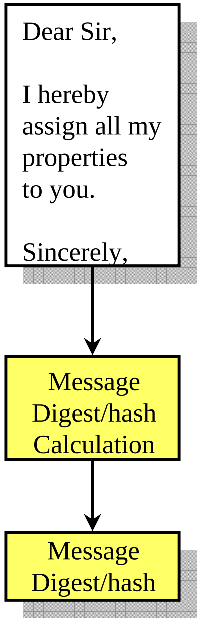
Message Digest (Hash) Properties

- Any change in the original data stream produces a different hash
- The transformation cannot be reversed: You cannot obtain the original data from the hash
- Changes are not predictable: Given a data set, you cannot predict what was changed from the hash
- No collisions: No two messages give the same hash
- Algorithm is well known (e.g., MD5, SHA-1)

Examples of MD5 hash

- Text: “This is an example of MD5”
- MD5: `6090d33aa1c3b8885cfb2522c5d2189e`
- Text: “This is another example of MD5”
- MD5: `19b9f4e9fe548830439332a520504f40`
- Text: “This”
- MD5: `a0311b12ed8180f815965a24044a3add`
- Text: HR3103.PDF file (HIPAA Law)
- MD5: `35054013a8cd7ec700c0e903660183ed`

Message Digest Process



Dear Sir,

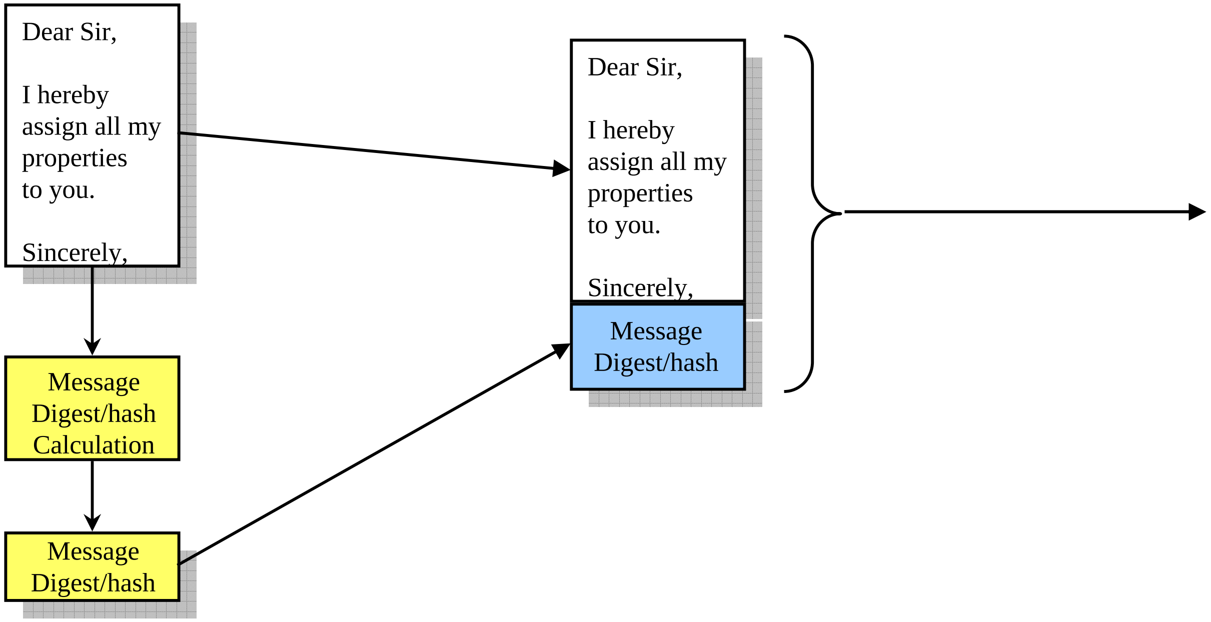
I hereby assign all my properties to you.

Sincerely,

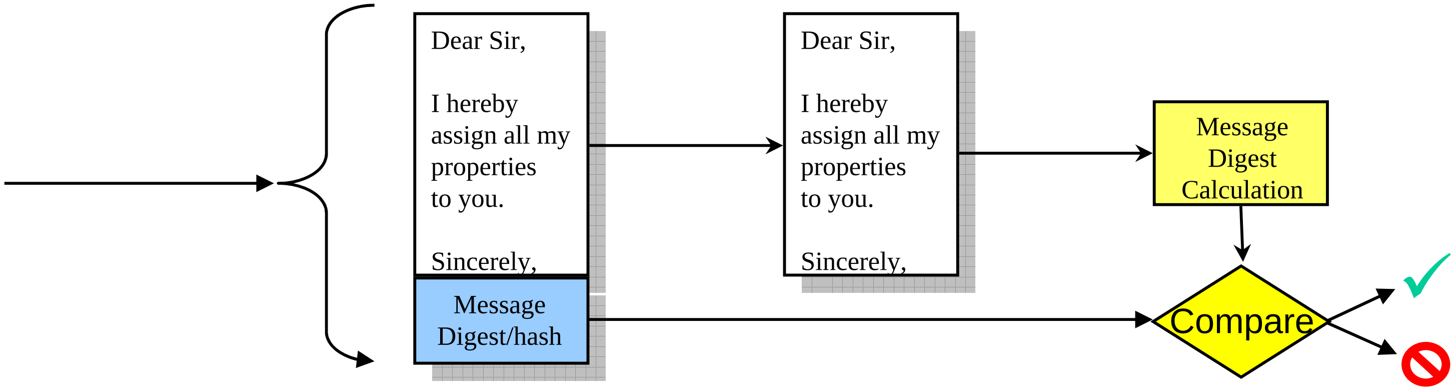
Message Digest/hash Calculation

Message Digest/hash

Message Digest Process



Integrity Verification


Dear Sir,
I hereby assign all my properties to you.
Sincerely,
Message Digest/hash
Dear Sir,
I hereby assign all my properties to you.
Sincerely,
Message Digest Calculation
Compare

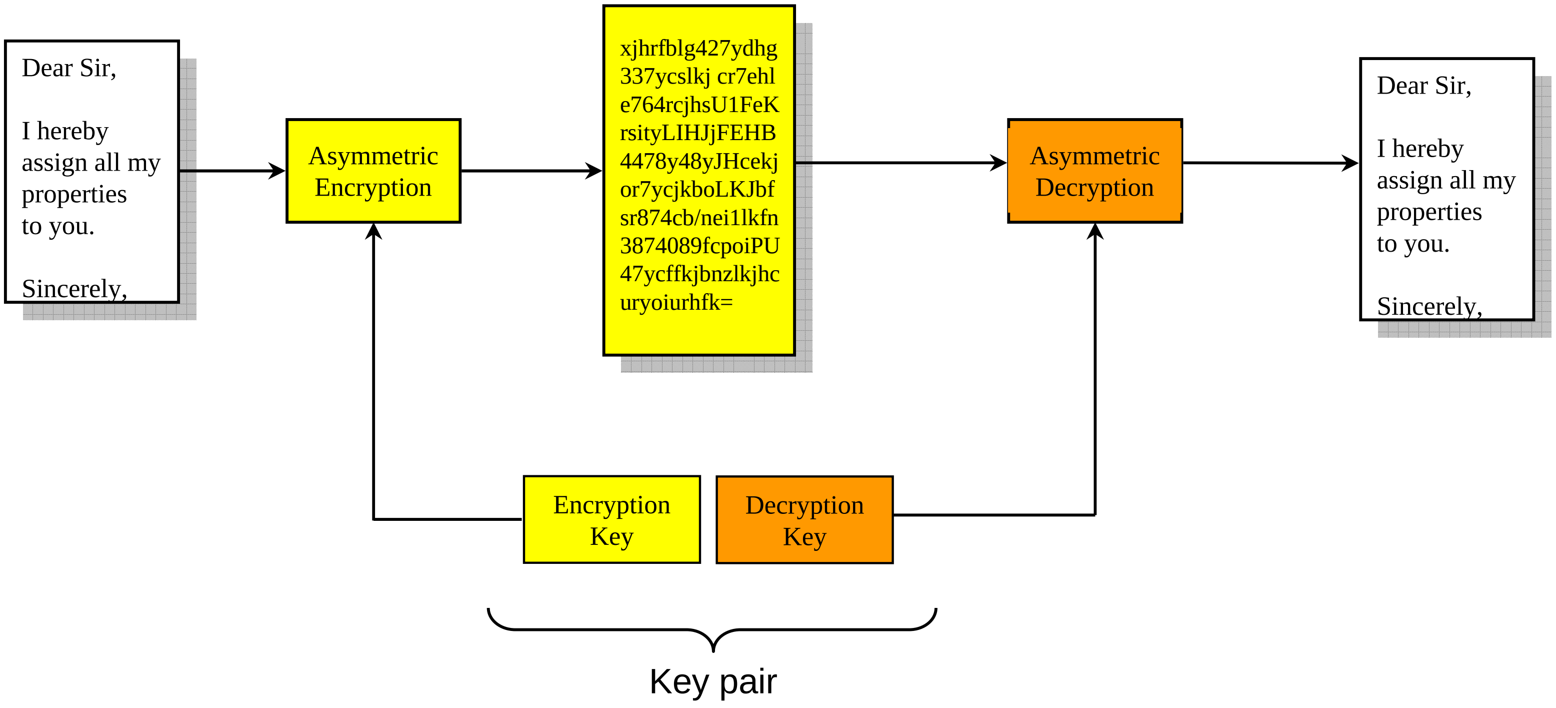
Concepts

- Message Digest / Hash is a “fingerprint” of the document(s)
- Any changes in the document will result in a different hash
- The hash does not prevent changes in the document, but detects the changes
- The hash helps preserve the integrity of the document and acts as a tamper-evident seal
    - Remember how the Tylenol tampering in the ’80s forever changed how pharmaceutical products are packaged

Asymmetric Encryption

- Asymmetric, or Public Key Encryption
  - Each trading partner has a “key pair”, one of the keys of the pair can reverse the encryption operation of the other key of the pair. One key is made available publicly. The other key, kept private, cannot be derived from the public key.
  - One key per entity, scales linearly.
  - Encrypt/decrypt with asymmetric algorithms is a very slow process, usable only for short data sets

Asymmetric Encryption (not really…)



Dear Sir,

I hereby
assign all my
properties
to you.

Sincerely,

Asymmetric
Encryption

xjhrfblg427ydhg
337ycslkj cr7ehl
e764rcjhsU1FeK
rsityLIHJjFEHB
4478y48yJHcekj
or7ycjkboLKJbf
sr874cb/nei1lkfn
3874089fcpoiPU
47ycffkjbnzlkjhc
uryoiurhfk=

Asymmetric
Decryption

Dear Sir,

I hereby
assign all my
properties
to you.

Sincerely,

Encryption
Key

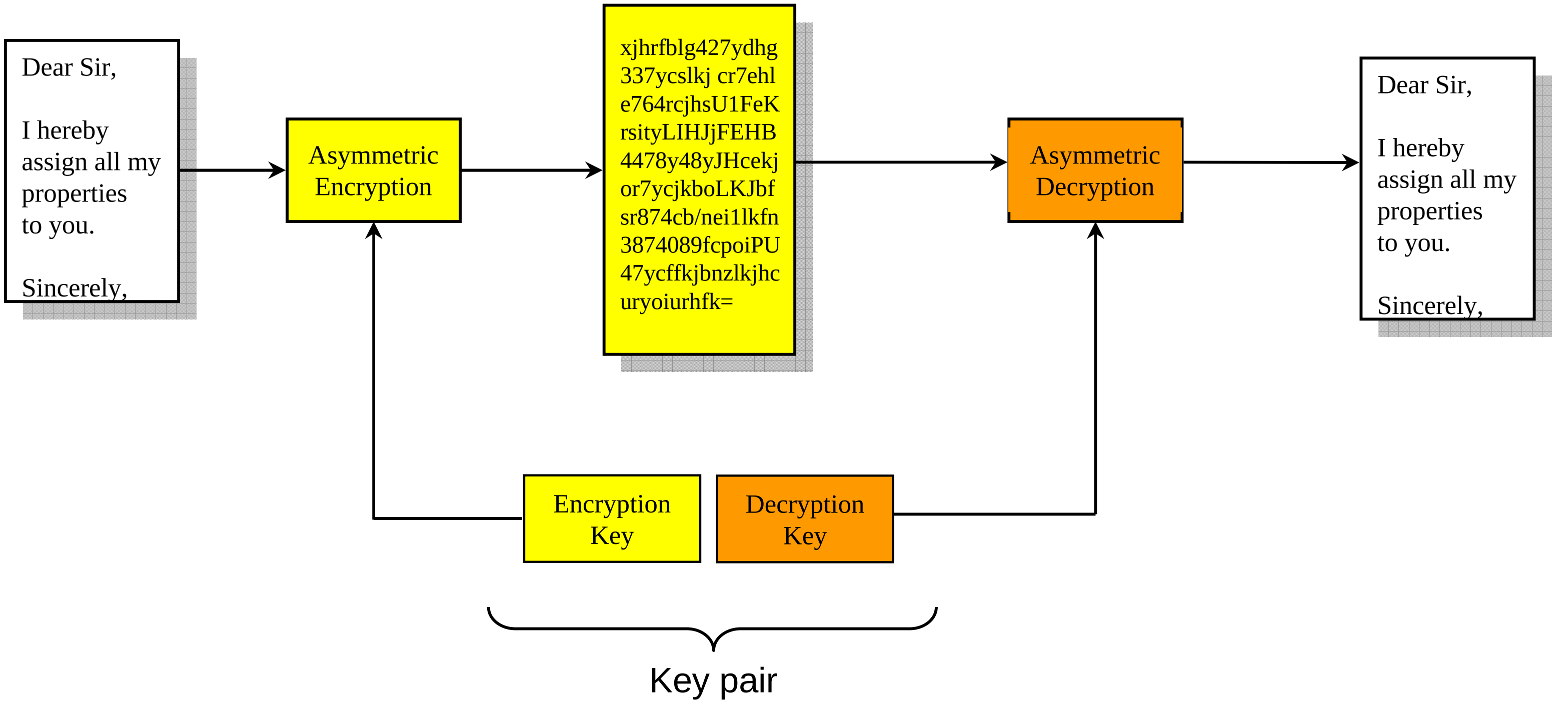
Decryption
Key

Key pair

Asymmetric Encryption

- Matching pair of keys is unique
- Knowing one of the keys in the pair does not give any information about the other key
- One key in the pair can be published
  - I publish my decryption key to the world
  - Only I have the corresponding encryption key
    - Keep it as a closely guarded secret
  - You, or anybody else, can decrypt something from me using my published decryption key
  - Only I could have encrypted it with my secret key

Asymmetric Encryption (not really…)



Dear Sir,

I hereby assign all my properties to you.

Sincerely,

Asymmetric Encryption

xjhrfblg427ydhg
337ycslkj cr7ehl
e764rcjhsU1FeK
rsityLIHJjFEHB
4478y48yJHcekj
or7ycjkboLKJbf
sr874cb/nei1lkfn
3874089fcpoiPU
47ycffkjbnzlkjhc
uryoiurhfk=

Asymmetric Decryption

Dear Sir,

I hereby assign all my properties to you.

Sincerely,

Encryption Key

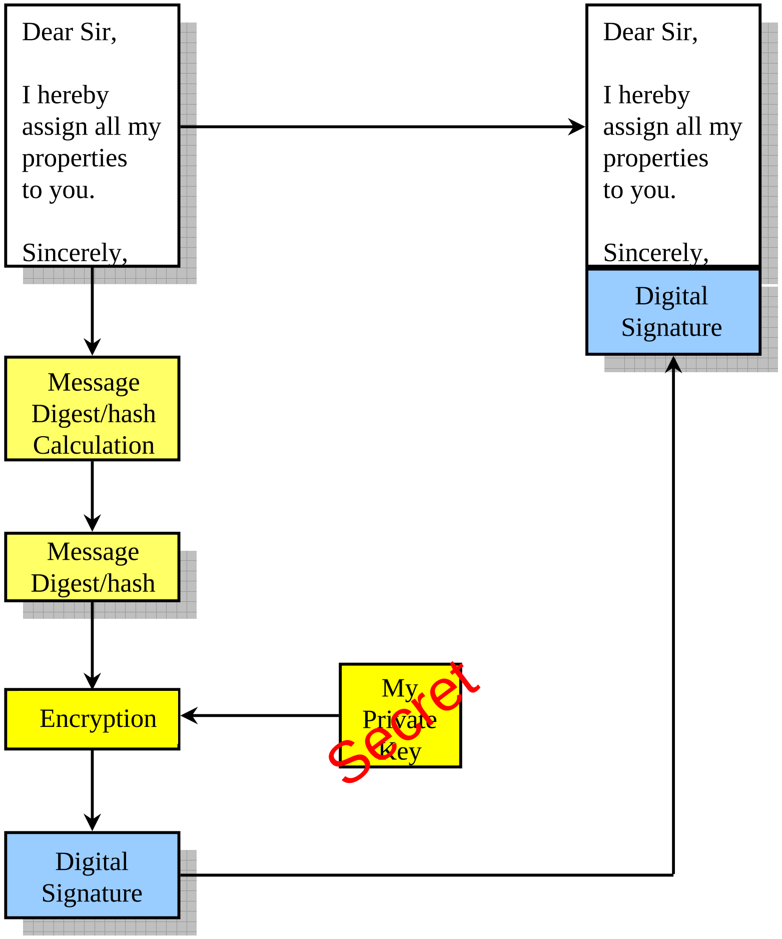
Decryption Key

Key pair

How is this useful?

- Putting both concepts together
    - Message Digest / Hash
    - Asymmetric encryption
        - Encrypt the hash
            - What do I get?

Digital Signature Process

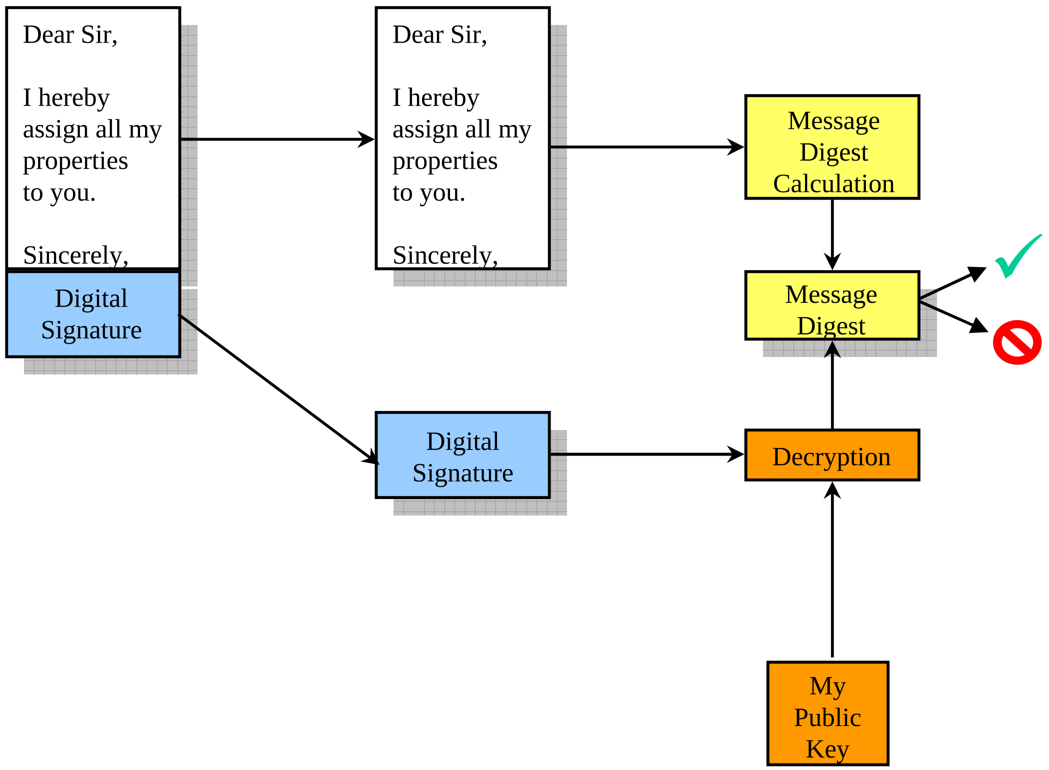


Only I could have encrypted the hash in this manner with my secret key. Nobody else has a key like mine.

Digital Signature Process

- Calculate the hash of the file or document to be signed.
    - Or part of a document if only that part is to be signed.
        - Example: HL7v3 “To be signed” tags
- Encrypt the hash with my private key to produce a “digital signature”
    - Combination of hash of the document and a secret that only I possess
- Attach the digital signature to the document

Signature Verification By Receiver



Dear Sir,

I hereby assign all my properties to you.

Sincerely,

Digital Signature Verification Process

- Detach the “digital signature” from the document
- Decrypt the “digital signature” with the public key of the signer
  - I know who the presumed signer is
  - I have access to his/her public key
- Calculate the hash of the document
- Match the calculated hash with the one obtained from the digital signature
  - Match: Good signature
  - No a match: Either the document was tampered with or the signer’s secret key was not used

Sample PGP signed message

```
From: kepa.zubeldia@claredi.com
Date: Mon, 16 Nov 1998 19:03:30 -0600
Subject: Message signed with PGP
MIME-Version: 1.0
Content-Type: text/plain; charset=US-ASCII
Content-Transfer-Encoding: 7bit


-----BEGIN PGP SIGNED MESSAGE-----

Bill,

This is a message signed with PGP, so you can see how much overhead PGP
signatures introduce.  Compare this with a similar message signed with S/MIME.
Does this make the point that we will have interoperability problems ?

Kepa

-----BEGIN PGP SIGNATURE-----
Version: PGP for Personal Privacy 5.0
Charset: noconv

iQCVAwUBM+oTwFcsAarXHFeRAQEsJgP/X3noON57U/6XVygOFjSY5lTpvAduPZ8M
aIFalUkCNuLLGxmtsbwRiDWLtCeWG3k+7zXDfx4YxuUcofGJn0QaTlk8b3nxADL0
O/EIvC/k8zJ6aGaPLB7rTIizamGOt5n6/08rPwwVkRB03tmT8UNMAUCgoM02d6HX
rKvnc2aBPFI=
=mUaH
-----END PGP SIGNATURE-----
```

Sample S/MIME signature

```
From: kepa.zubeldia@claredi.com
Date: Mon, 16 Nov 1998 19:03:08 -0600
Subject: Message signed with S/MIME
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="simple boundary"


--simple boundary
Content-Type: text/plain; charset=US-ASCII
Content-Transfer-Encoding: 7bit

Bill,

This is a message signed with S/MIME, so you can see how much overhead S/MIME
signatures introduce.  Compare this with a similar message signed with PGP.
Does this make the point that we will have interoperability problems ?

Kepa


--simple boundary
Content-Type: application/octet-stream; name="smime.p7s"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7s"
```

MIIQQwYJKoZIhvcNAQcCoIIQNDCCEDACAQExCzAJBgUrDgMCGgUAMAsGCSqGSIb3DQEHAaCCDnww
ggnGMIIJL6ADAgECAhBQQRR9a+DX0FHXfQOVHQhPMA0GCSqGSIb3DQEBBAUAMGIxETAPBgNVBAcT
CEludGVybmV0MRcwFQYDVQQKEw5WZXJpU2lnbiwgSW5jLjE0MDIGA1UECxMrVmVyaVNpZ24gQ2xh
c3MgMSBDQSAtIEluZGl2aWR1YWwgU3Vic2NyaWJlcjAeFw05NzAxMjcwMDAwMDBaFw05ODAxMjcy
MzU5NTlaMIIBFzERMA8GA1UEBxMISW50ZXJuZXQxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMTQw
MgYDVQQLEytWZXJpU2lnbiBDbGFzcyAxIENBIC0gSW5kaXZpZHVhbCBTdWJzY3JpYmVyMUYwRAYD

```
VQQLEz13d3cudmVyaXNpZ24uY29tL3JlcG9zaXRvcnkvQ1BTIEluY29ycC4gYnkgUmVmLixMSUFC
LkxURChjKTk2MSYwJAYDVQQLEx1EaWdpdGFsIElEIENsYXNzIDEgLSBOZXRzY2FwZTEWMBQGA1UE
AxMNS2VwYSBadWJlbGRpYTErMCkGCSqGSIb3DQEJARYca2VwYS56dWJlbGRpYUBlbnZveS1uZWlj
LmNvbTBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQDTpPphGGti96yriSSzajE8HQXv9yCxWDfzFKQs
KAd8SRyClY7GjNJxbwQGddqNIUTy6NKbVAoDhhSvB4kaT+mPAgMBAAGjggcIMIIHBDAJBgNVHRME
AjAAMIICHwYDVR0DBIICFjCCAhIwggIOMIICCgYLYIZIAYb4RQEHAQEwggH5FoIBp1RoaXMgY2Vy
dGlmaWNhdGUgaW5jb3Jwb3JhdGVzIGJ5IHJlZmVyZW5jZSwgYW5kIGl0cyB1c2UgaXMgc3RyaWN0
bHkgc3ViamVjdCB0bywgdGhlIFZlcmlTaWduIENlcnRpZmljYXRpb24gUHJhY3RpY2UgU3RhdGVt
ZW50IChDUFMpLCBhdmFpbGFibGUgYXQ6IGh0dHBzOi8vd3d3LnZlcmlzaWduLmNvbS9DUFM7IGJ5
IEUtbWFpbCBhdCBDUFMtcmVxdWVzdHNAdmVyaXNpZ24uY29tOyBvciBieSBtYWlsIGF0IFZlcmlT
aWduLCBJbmMuLCAyNTkzIENvYXN0IEF2ZS4sIE1vdW50YWluIFZpZXcsIENBIDk0MDQzIFVTQSBU
ZWwuICsxICg0MTUpIDk2MS04ODMwIENvcHlyaWdodCAoYykgMTk5NiBWZXJpU2lnbiwgSW5jLiAg
QWxsIFJpZ2h0cyBSZXNlcnZlZC4gQ0VSVEFJTiBXQVJSQU5USUVTIERJU0NMQUlNRUQgYW5kIExJ
QUJJTElUWSBMSU1JVEVELqAOBgxghkgBhvhFAQcBAQGhDgYMYIZIAYb4RQEHAQECMCwwKhYoaHR0
cHM6Ly93d3cudmVyaXNpZ24uY29tL3JlcG9zaXRvcnkvQ1BTIDARBglghkgBhvhCAQEEBAMCB4Aw
NgYJYIZIAYb4QgEIBCkWJ2h0dHBzOi8vd3d3LnZlcmlzaWduLmNvbS9yZXBvc2l0b3J5L0NQUzCC
BIcGCWCGSAGG+EIBDQSCBHgWggR0Q0FVVElPTjogVGhlIENvbW1vbiBOYW1lIGluIHRoaXMgQ2xh
c3MgMSBEaWdpdGFsIApJRCBpcyBub3QgYXV0aGVudGljYXRlZCBieSBWZXJpU2lnbi4gSXQgbWF5
IGJlIHRoZQpob2xkZXIncyByZWFsIG5hbWUgb3IgYW4gYWxpYXMuIFZlcmlTaWduIGRvZXMgYXV0
aC0KZW50aWNhdGUgdGhlIGUtbWFpbCBhZGRyZXNzIG9mIHRoZSBob2xkZXIuCgpUaGlzIGNlcnRp
ZmljYXRlIGluY29ycG9yYXRlcyBieSByZWZlcmVuY2UsIGFuZCAKaXRzIHVzZSBpcyBzdHJpY3Rs
eSBzdWJqZWN0IHRvLCB0aGUgVmVyaVNpZ24gCkNlcnRpZmljYXRpb24gUHJhY3RpY2UgU3RhdGVt
ZW50IChDUFMpLCBhdmFpbGFibGUKaW4gdGhlIFZlcmlTaWduIHJlcG9zaXRvcnkgYXQ6IApodHRw
czovL3d3dy52ZXJpc2lnbi5jb207IGJ5IEUtbWFpbCBhdApDUFMtcmVxdWVzdHNAdmVyaXNpZ24u
Y29tOyBvciBieSBtYWlsIGF0IFZlcmlTaWduLApJbmMuLCAyNTkzIENvYXN0IEF2ZS4sIE1vdW50
YWluIFZpZXcsIENBIDk0MDQzIFVTQQoKQ29weXJpZ2h0IChjKTE5OTYgVmVyaVNpZ24sIEluYy4g
IEFsbCBSaWdodHMgClJlc2VydmVkLiBDRVJUQUlOIFdBUlJBTlRJRVMgRElTQ0xBSU1FRCBBTkQg
CkxJQUJJTElUWSBMSU1JVEVELgoKV0FSTklORzogVEhFIFVTRSBPRiBUSElTIENFUlRJRklDQVRF
IElTIFNUUklDVExZClNVQkpFQ1QgVE8gVEhFIFZFUklTSUdOIENFUlRJRklDQVRJT04gUFJBQ1RJ
Q0UKU1RBVEVNRU5ULiAgVEhFIElTU1VJTkcgQVVUSE9SSVRZIERJU0NMQUlNUyBDRVJUQUlOCklN
UExJRUQgQU5EIEVYUFJFU1MgV0FSUkFOVElFUywgSU5DTFVESU5HIFdBUlJBTlRJRVMKT0YgTUVS
Q0hBTlRBQklMSVRZIE9SIEZJVE5FU1MgRk9SIEEgUEFSVElDVUxBUgpQVVJQT1NFLCBBTkQgV0lM
TCBOT1QgQkUgTElBQkxFIEZPUiBDT05TRVFVRU5USUFMLApQVU5JVElWRSwgQU5EIENFUlRBSU4g
T1RIRVIgREFNQUdFUy4gU0VFIFRIRSBDUFMKRk9SIERFVEFJTFMuCgpDb250ZW50cyBvZiB0aGUg
VmVyaVNpZ24gcmVnaXN0ZXJlZApub25ZXJpZmllZFN1YmplY3RBdHRyaWJ1dGVzIGV4dGVuc2lv
biB2YWx1ZSBzaGFsbCAKbm90IGJlIGNvbnNpZGVyZWQgYXMgYWNjdXJhdGUgaW5mb3JtYXRpb24g
dmFsaWRhdGVkIApieSB0aGUgSUEuMA0GCSqGSIb3DQEBBAUAA4GBADt0b/js6suvBuWU33mL6NnO
T/tcoNH/tdH5AGLEgy4PSEHD1eWCpWiYZy6u1RbPs1OOkj4ukO/OUZJczmU0uflzhNslj8d7cdy0
QRGLarFRhTT5g7qm3P2RAVhngfO9lz6RwyVQHwETHLI8FJeeKYnSfQeQvVQWjHIAVmVKNbFFMIIC
eTCCAeKgAwIBAgIQUh81HfJwfgArvspZhwTVOTANBgkqhkiG9w0BAQIFADBfMQswCQYDVQQGEwJV
```

```
UzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4xNzA1BgNVBAsTLkNsYXNzIDEgUHVibGljIFByaW1h
cnkgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwHhcNOTYwNjI3MDAwMDAwWhcNOTkwNjI3MjM1OTU5
WjBiMREwDwYDVQQHEwhJbnRlcm5ldDEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4xNDAyBgNVBAsT
K1ZlcmlTaWduIENsYXNzIDEgQ0EgLSBJbmRpdmlkdWFsIFN1YnNjcmliZXIwgZ8wDQYJKoZIhvcN
AQEBBQADgY0AMIGJAoGBALYUps9N0AUN2Moj0G+qtCmSY44s+G+W1y6ddksRsTaNV8nD/RzGuv4e
CLozypXqvuNbzQaot3kdRCrtc/KxUoNoEHBkkdc+a/n3XZ0UQ5tul0WYgUfRLcvdu3LXTD9xquJA
8lQ5vBbuz3zsuts/bCqzFrGGEp2ukzTVuNXQ9z6pAgMBAAGjMzAxMA8GA1UdEwQIMAYBAf8CAQEw
CwYDVR0PBAQDAgEGMBEGCWCGSAGG+EIBAQQEAwIBBjANBgkqhkiG9w0BAQIFAAOBgQDB+vcC51fK
EXXGnAz6K3dPh0UXO+PSwdoPWDmOrpWZA6GooTj+eZqTFwuXhjnHymg0ZrvHiEX2yAwF7r6XJe/g
1G7kf512XM59uhSirguf+2dbSKVnJa8ZZIj2ctgpJ6o3EmqxKK8ngxhlbI3tQJ5NxHiohuzpLFC/
pvkN27CmSjCCAjEwggGaAgUCpAAAATANBgkqhkiG9w0BAQIFADBfMQswCQYDVQQGEwJVUzEXMBUG
A1UEChMOVmVyaVNpZ24sIEluYy4xNzA1BgNVBAsTLkNsYXNzIDEgUHVibGljIFByaW1hcnkgQ2Vy
dGlmaWNhdGlvbiBBdXRob3JpdHkwHhcNOTYwMTI5MDAwMDAwWhcNOTkxMjMxMjM1OTU5WjBfMQsw
CQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4xNzA1BgNVBAsTLkNsYXNzIDEgUHVi
bGljIFByaW1hcnkgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwgZ8wDQYJKoZIhvcNAQEBBQADgY0A
MIGJAoGBAOUZv22jVmEtmUhx9mfeuY3rt56GgAqRDvo4Ja9GiILlc6igmyRdDR/MZW4MsNBWhBiH
mgabEKFz37RYOWtuwfYV1aioP6oSBo0xrH+wNNePNGeICc0UEeJORVZpH3gCgNrcR5EpuzbJY1zF
4Ncth3uhtzKwezC6Ki8xqu6jZ9rbAgMBAAEwDQYJKoZIhvcNAQECBQADgYEAUnO6mlXc3D+CfbCQ
mGIqgkx2AG4lPdXCCXBXAQwPdx8YofscYA6gdTtJIUH+p1wtTEJJ0/8o2Izqnf7JB+J3glMj3lXz
zkST+vpMvco281tmsp7I8gxeXtShtCEJM8o7WfySwjj8rdmWJOAt+qMp9TNoeE60vJ9pNeKomJRz
O8QxggGPMIIBiwIBATB2MGIxETAPBgNVBAcTCEludGVybmV0MRcwFQYDVQQKEw5WZXJpU2lnbiwg
SW5jLjE0MDIGA1UECxMrVmVyaVNpZ24gQ2xhc3MgMSBDQSAtIEluZGl2aWR1YWwgU3Vic2NyaWJl
cgIQUEEUfWvg19BR130DlR0ITzAJBgUrDgMCGgUAoIGxMBgGCSqGSIb3DQEJAzELBgkqhkiG9w0B
BwEwIwYJKoZIhvcNAQkEMRYEFE5W9YE9GtbjlD5A52LLaEi96zCKMBwGCSqGSIb3DQEJBTEPFw05
NzA4MDcxODQwMTBaMFIGCSqGSIb3DQEJDzFFMEMwCgYIKoZIhvcNAwcwDgYIKoZIhvcNAwICAgCA
MAcGBSsOAwIHMA0GCCqGSIb3DQMCAgFAMA0GCCqGSIb3DQMCAgEoMA0GCSqGSIb3DQEBAQUABEDI
3mvHr3SAJkdoMqxZnSjJ+5gfZABJGQVOfyEfcKncY/RYFvWuHBAEBySImIQZjMgMNrQLL7QXJ/eI
xIwDet+c
```

```
--simple boundary--
```

The MIME signature block is much longer than the PGP signature because the MIME signature block includes both the signature itself and the corresponding digital certificate of the signer.

HIPAA Requirement

- Standard specifying procedures for electronic transmission of the signature

Where is the industry?

- Variety of hashing algorithms
  - MD5 and SHA-1 are the most common
  - Snefru, N-Hash, MD2, MD4, SHA, RIPE-MD, HAVAL, GOST, MDC-2, MDC-4, others
- Variety of signature encryption algorithms
  - RSA and DSA are the most common
  - ElGamal, GOST, Schnorr, Ong-Schnorr-Shamir, ESIGN, Elliptic Curve, others
- Variety of encryption key sizes
  - 1024 or 2048 bits recommended for RSA or DSA
- Variety of encodings of the resulting “signature”
  - ASN.1 and PGP are the most common, with base64 coding
  - XML and proprietary encodings are also used
- Variety of data content included in the “signature”
  - Hash, signature timestamp, signature usage indicators, digital certificate, etc.

Commercial Availability

- Most electronic mail software packages can digitally “sign” the entire message
  - Some can also digitally “sign” attachments
  - Very few can “sign” only a part of a message
- Other non-email software also implements signatures
  - Adobe Acrobat, PGP, PKZIP, signatures on Microsoft COM objects, signed Java beans, etc.
- X12 implements digital signature of an entire Transaction Set as part of the X12 syntax itself
- HL7 v3 has XML signature and authentication tags indicating the parts “to be signed” in the CDA
- **Interoperability** of the signature is the biggest problem

Authentication

- Signature Authentication
  - Was this signature written by this person?
    - Judge asks: “Is this your signature?”
- Document Authentication
  - Is this the document you signed?
- Entity Authentication
  - Is this the person whom he/she claims to be?

- Deeply inter-related concepts

HIPAA Requirement

- Standard specifying procedures for electronic authentication of the signature
  - Authentication of the signature vs. authentication of the context:
    - Signer (individual, program, hardware, entity)
    - Document being signed
    - Intent
    - Timestamp
- Thought… What is the use of a signature if we do not authenticate the context?

Traditional Signature Authentication

- Witnessed and personal knowledge
  - Witnessed signature
    - Signed in front of a State, Federal or other officer
  - Notary Public certification
- Signature Card
  - Used by banks
- Established record of the signer
  - Medical records, prescriptions
- Established by business context
  - Used in commerce, contracts, checks, etc.
- Expert witness
  - Forensic signature experts for court cases

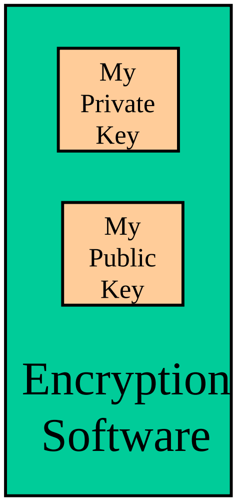
Authentication Technology

- Signature Dynamics
  - Compare signature dynamics with a registered template for that signer
    - Approximate comparison by forensics expert
    - Template can be "certified" by a Certification Authority
- Digital Signature
  - Compare the "public key" with a key registered for that signer
    - Exact comparison by a program
    - Key can be "certified" by Certification Authority

Authentication by a Third Party

- In addition to the **template** or the **public key**, other components may be authenticated by the Certification Authority
  - Legal Name
  - Validity dates of the certificate
  - Certified “attributes” of the signer
    - Identification number (DEA)
    - Access privileges, clearances
    - Signature privileges
    - Biometric (picture, fingerprint, retinal scan, etc.)
    - Other “certificate extensions”

Digital Certificate

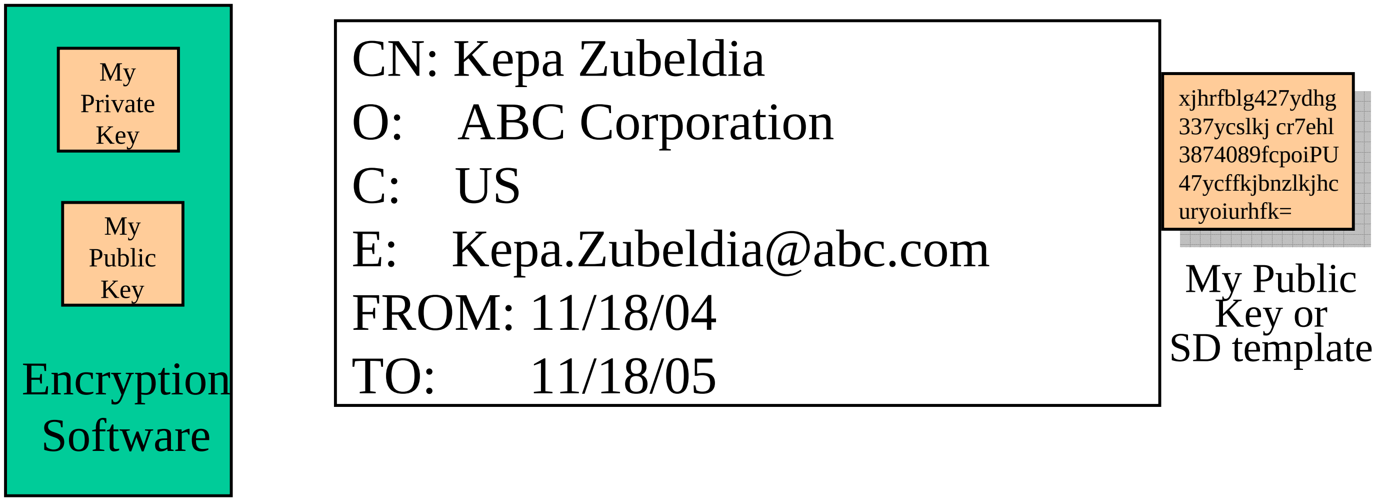


My Private Key

My Public Key

Encryption Software

Digital Certificate



My Private Key

My Public Key

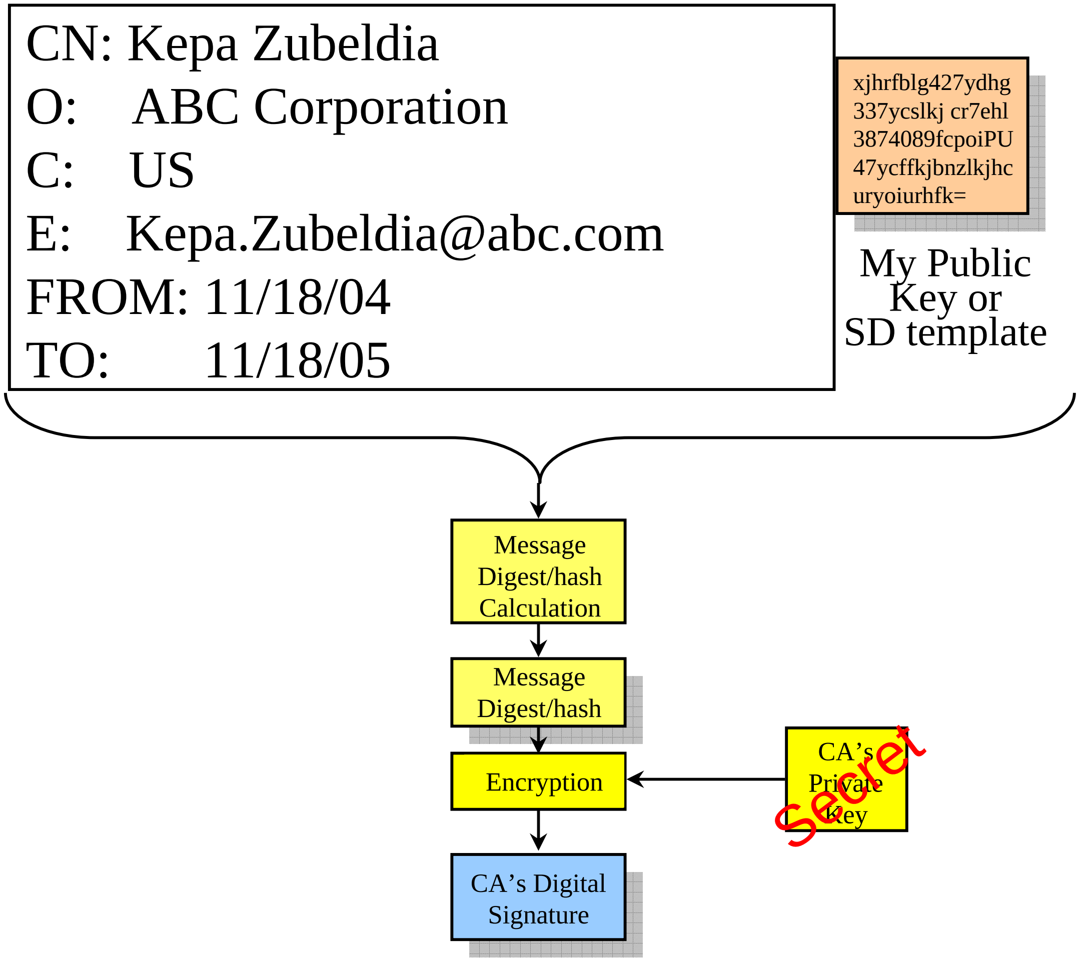
Encryption Software

CN: Kepa Zubeldia
O: ABC Corporation
C: US
E: Kepa.Zubeldia@abc.com
FROM: 11/18/04
TO: 11/18/05

xjhrfblg427ydhg
337ycslkj cr7ehl
3874089fcpoiPU
47ycffkjbnzlkjhc
uryoiurhfk=

My Public Key or SD template

Digital Certificate



CN: Kepa Zubeldia

O: ABC Corporation

C: US

E: Kepa.Zubeldia@abc.com

FROM: 11/18/04

TO: 11/18/05

xjhrfblg427ydhg
337ycslkj cr7ehl
3874089fcpoiPU
47ycffkjbnzlkjhc
uryoiurhfk=

My Public Key or SD template

Message Digest/hash Calculation

Message Digest/hash

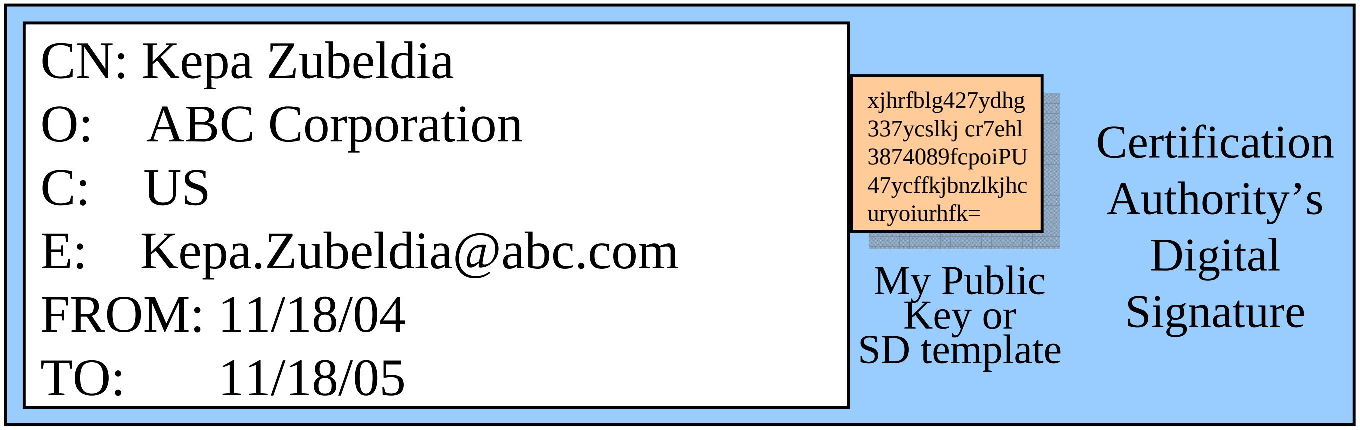
Encryption

CA's Private Key

Secret

CA's Digital Signature

Digital Certificate



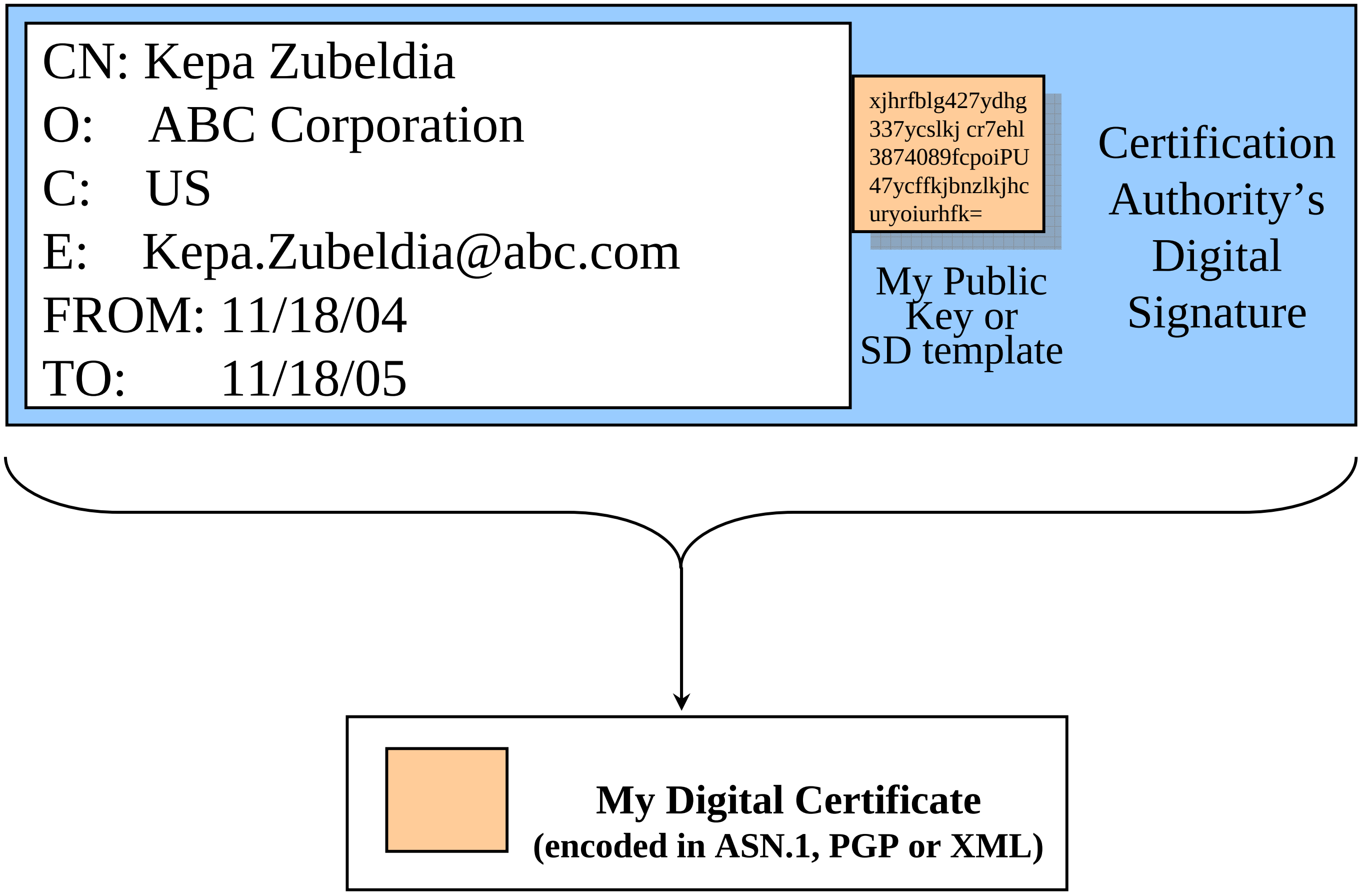
CN: Kepa Zubeldia
O: ABC Corporation
C: US
E: Kepa.Zubeldia@abc.com
FROM: 11/18/04
TO: 11/18/05

xjhrfblg427ydhg
337ycslkj cr7ehl
3874089fcpoiPU
47ycffkjbnzlkjhc
uryoiurhfk=

My Public Key or SD template

Certification Authority's Digital Signature

Digital Certificate



CN: Kepa Zubeldia
O: ABC Corporation
C: US
E: Kepa.Zubeldia@abc.com
FROM: 11/18/04
TO: 11/18/05

xjhrfblg427ydhg
337ycslkj cr7ehl
3874089fcpoiPU
47ycffkjbnzlkjhc
uryoiurhfk=

My Public Key or SD template

Certification Authority’s Digital Signature

My Digital Certificate
(encoded in ASN.1, PGP or XML)

Digital Certificate

- Binds the identity of an individual with a Public Key or a Signature Dynamics template.
    - Authenticates the owner of a Public Key or Signature Dynamics template.
- Electronic conveyor for transmission of a Public Key or Signature Dynamics template
    - Public Key or SD template incorporated inside certificate
    - Not a transmission of the signature
- Issued by a Trusted Third Party
    - Certification Authority (CA)
- May be revoked by the CA before the expiration date if the Private Key is compromised

Certificates and Digital Signatures

- Certificates attest to the identity of the owner of an encryption key or signature dynamics template
  - Issued by a Certification Authority.
- Certification Authority validates the identity of the signer

- Digital signatures “protect” a file or Email against tampering and identify the signer
  - Issued by the owner of the signed document
- The digital signature validates the document itself

Digital Certificate vs. Digital Signature

- Digital Certificate is a particular expression of one kind of digital signature
  - Signed material is included inside the certificate
  - Signed material may be a public key
  - Signed by a third party Certification Authority
    - But “self signed” certificates are also common
  - Well defined and universally used Digital Certificate standard format
    - X.509 Version 3
    - Variety of “certificate extensions” in use
      - These are not standard from implementation to implementation

Digital Signature

- Signed material totally variable
  - Entire text file, PDF, digital image, XML marked-up text, EDI transaction, or a part of it
- Signature and signed material relationship
  - Packaged as one file
    - Signature sent inside document (XML, HL7)
    - Document inside crypto-container (PGP, S/MIME)
  - Packaged as separate files
    - Interoperability with not-signature-enabled applications
- Signature and digital certificate relationship
  - Certificate included with each signature
  - Certificate available from a repository (CA, other)
- Signature encoding
  - No dominant standard
    - ASN.1, XML, PGP, S/MIME, etc.

Industry Progress

- PKI establishment
  - Certification Authorities
    - Root CA, Bridge CA, Federal PKI Bridge
  - Certification Policies
    - Authentication rules, CA operations, etc.
  - Certificate Revocation
    - Large CRLs, on-line certificate validation
  - Certificate Extensions
    - ASTM standard X.509v3 healthcare extensions
  - PKI software deployment
    - Supported by Microsoft and others

Problems

- Signature interoperability
  - **No** standards for digital or electronic signatures in universal use
- Certificate interoperability
  - Good. Some certificate extensions are “ignored”
- Certification Authority interoperability
  - Federal PKI Bridge
- Technology is very complex
  - Deployment has been much slower than originally predicted
    - AMA Digital Certificate, FDA certificates

PKI Benefits

- Increase trust in electronic transactions
- Certificates can be used for distribution of signature and encryption keys
- Enable secure transactions over the Internet
- Certificate and key management are simplified if there is a standard that everybody uses
- Cost of certificates should go down as volume increases with widespread adoption

PKI Issues

- The best interoperable results are produced by single vendor solutions
- Certificate maintenance is expensive
- I know my trading partners better than the CA
  - I want to be my own CA and reduce my costs
  - Forget interoperability, it works for me
- I have a digital certificate, now what?
  - No standards for signatures, encryption, single sign-on or other uses of the certificate

- Sec. 1173 (e) Electronic Signature.
  - (1) STANDARDS. The Secretary, in coordination with the Secretary of Commerce, shall adopt standards specifying procedures for the electronic transmission and authentication of signatures with respect to the transactions referred to in subsection (a)(1).
  - (2) EFFECT OF COMPLIANCE. Compliance with the standards adopted under paragraph (1) shall be deemed to satisfy Federal and State statutory requirements for written signatures with respect to the transactions referred to in subsection (a)(1).

Contact

Kepa Zubeldia
President and CEO
Kepa.Zubeldia@claredi.com
(801) 444-0339 x205