



C.I.R.S.F.I.D
Alma Mater Studiorum Università di Bologna
Research Centre of History of Law,
Philosophy and Sociology of Law,
Computer Science and Law

ESignature

Seminar “Legal Informatics in Italy”

Bologna, 18 June 2003

Michele Martoni

martoni@cirfid.unibo.it



Why Signatures?

LEGAL CONCEPTION OF SIGNATURE

General Purposes of Signing

- **Evidence** a distinctive mark of the signer
- **Ceremony** calls attention to the act
- **Approval** implies approval intent
- **Efficiency** validation of the document



Why Signatures?

LEGAL CONCEPTION OF SIGNATURE

Requisite Attributes of Signatures

- **Signer Authentication** proof of identity
- **Document Authentication** proof of subject
- **Approval** no-repud. act require conscious intervention
- **Efficiency** provide maximum assurance with reasonable effort

Michèle Martoni © 2003



Why ESignatures?

WHY ELECTRONIC SIGNATURE:

1. **IDENTIFICATION FUNCTION** to identify the person signing
2. **AUTHENTICATION FUNCTION** to indicate that person's approval of the information contained in that data message
3. **INTEGRITY FUNCTION** to indicate that the record has not been altered

Michèle Martoni © 2003

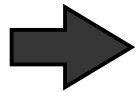


Electronic Signatures

European Commission Definition

Directive No. 1999/93/EC

Electronic signature means data in electronic form which are attached to or logically associated with other electronic data and which serve as a **method of authentication** [art. 1]



TECHNOLOGY NEUTRAL

Michèle Martoni © 2003



Electronic Signatures

The following technologies are forms of electronic signatures at various level (and are used in combination to provide added security):

PIN (Personal Identification Number) or Password

– a set of numbers or characters shared only by the system and the user, and usually encrypted if the authentication occurs over an open network;

Smart Card

– a plastic card similar to a credit card, except that it contains a microprocessor (chip) that can generate, store, and process data, and can be programmed to be activated only when the user enters a PIN or other identifier;

...

Michèle Martoni © 2003



Electronic Signatures

Biometrics – technologies for measuring and analyzing human body characteristics such as fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements to authenticate their identity. Biometric devices consist of a reader or a sensor, software that converts the received information into digital form (i.e. a series of binary digits or bits) and if the data are analyzed, a database to store an individual's known biometric data with the entered biometric data.

Digital signature – [...]

DIGITAL SIGNATURE IS A SPECIAL TYPE OF ELECTRONIC SIGNATURE

Michèle Martoni © 2003

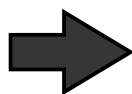


Digital Signature

Italian Digital Signature Definition

Presidential Decree No. 445 of 28 December 2000

Digital signature means the result of a computer-based process (validation) implementing an asymmetric cryptographic system consisting of a public and a private key, whereby the signer asserts, by means of the private key, and the recipient verifies, by means of the public key, the origin and integrity of a single electronic document or a set of such documents.



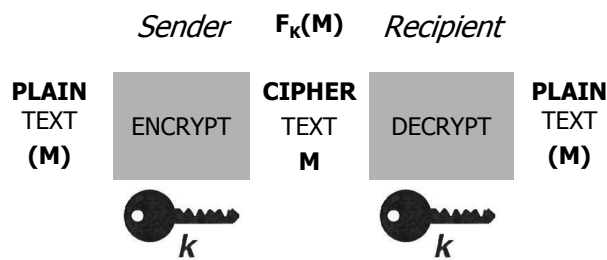
the CHOICE
ASYMMETRIC CRYPTOGRAPY

Michèle Martoni © 2003



Symmetric Crypto. [1]

One key (**K**) to encrypt
The same key (**K**) to decrypt
Only a key (K) to encrypt and decrypt



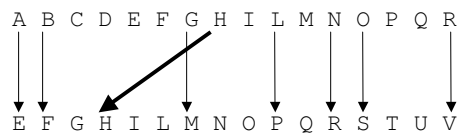
Michèle Martoni © 2003



Symmetric Crypto. [2]

Traspositiv Method

KEY (K): alphabetical distance



KEY = 4

BOLOGNA \Rightarrow **FSPSMRE**

Michèle Martoni © 2003



Symmetric Crypto. [3]

THE LIMIT KEY TRANSMISSION

We have to communicate our key to the recipient of the message. **How ???**

He could use our key to sign a message and we aren't able to get **the difference !!!**

Michèle Martoni © 2003



Asymmetric Crypto. [1]

One key (**K_{PRIV}**) to encrypt

A different key (**K_{PUB}**) to decrypt

Two different – BUT RELATED – keys (K_{PRIV} K_{PUB})

• **Private key (K_{PRIV})** - known only to the sender of a message

• **Public key (K_{PUB})** - known by, well, the public

Michèle Martoni © 2003



Asymmetric Crypto.[2]

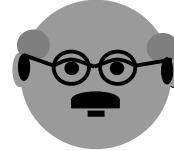


Alice

TRANSMISSION of the KEYS
UNCERTAIN CHANNEL

← P (prime number) & $\geq Y$ →

$Y = 7$ e $P = 11$



Bob

A segreto = 3	B segreto = 6
$K = Y^A \pmod{P}$ [$K = 7^3 \pmod{11} = 2$]	$H = Y^B \pmod{P}$ [$H = 7^6 \pmod{11} = 4$]
Comunica K (=2)	Comunica H (=4)
$Z = H^A \pmod{P}$ [$Z = 4^3 \pmod{11} = 9$]	$W = K^B \pmod{P}$ [$W = 2^6 \pmod{11} = 9$]

The Enemy could intercept K & H but
he isn't able to calculate keys
Z = W = KEY = 9 !!!

Michele Martoni © 2003

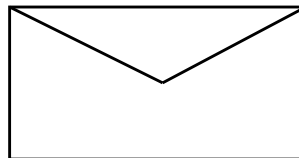


Asymmetric Crypto.[3]

1 – Chiper Text (but *not sign*)

Alice

($K_{\text{PUB}}^{\text{Bob}}$)



Bob

($K_{\text{PRIV}}^{\text{Bob}}$)

- 1. Security** of the content of the message
- 2. "Not" Authentication** of the message

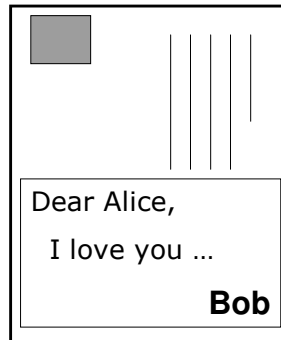
Michele Martoni © 2003



Asymmetric Crypto.[4]

2 - Sign Text (but *plain*)

Alice
($K_{\text{PRIV Alice}}$)



Bob
($K_{\text{PUB Alice}}$)

1. "Not" Security of the content of the message
2. Authentication & Integrity of the message

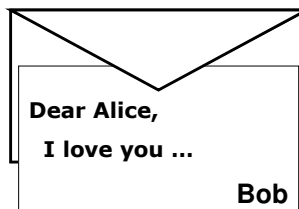
Michèle Martoni © 2003



Asymmetric Crypto.[5]

3 - Sign&Chiper Text

Alice
($K_{\text{PRIV Alice}}$)
($K_{\text{PUB Bob}}$)



Bob
($K_{\text{PUB Alice}}$)
($K_{\text{PRIV Bob}}$)

1. Security of the content of the message
2. Authentication & Integrity of the message

Michèle Martoni © 2003



Asymmetric Crypto. [6]

THE LIMIT
TIME OF
CALCULATION

Michèle Martoni © 2003



Hash Function [1]

WHAT'S?

A hash function H is a transformation that takes an input m and returns a fixed-size string, which is called the hash value h (that is, $h = H(m)$).

The basic requirements for a **cryptographic hash function** are as follows.

- The input can be of any length.
- The output has a fixed length.
- $H(x)$ is relatively easy to compute for any given x .
- $H(x)$ is one-way.
- $H(x)$ is collision-free.

Michèle Martoni © 2003



Hash Function [2]

...

A hash function H is said to be *one-way* if it's **hard to invert** where “hard to invert” means that given a hash value h , it is **computationally infeasible** to find some input x such that $H(x) = h$.

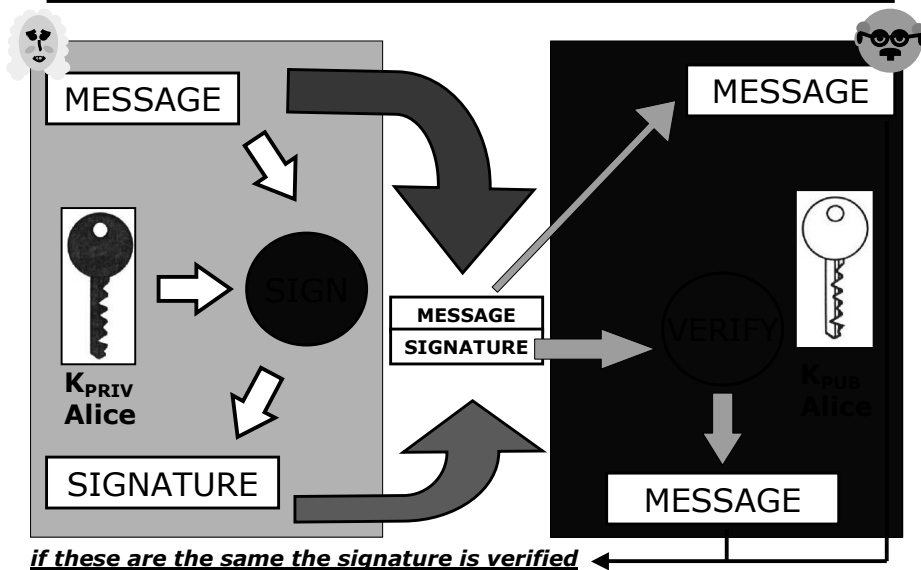
If, given a message x , it is computationally infeasible to find a message y not equal to x such that $H(x) = H(y)$, then H is said to be a *weakly collision-free* hash function.

A *strongly collision-free* hash function H is one for which it is computationally infeasible to find any two messages x and y such that $H(x) = H(y)$

Michèle Martoni © 2003



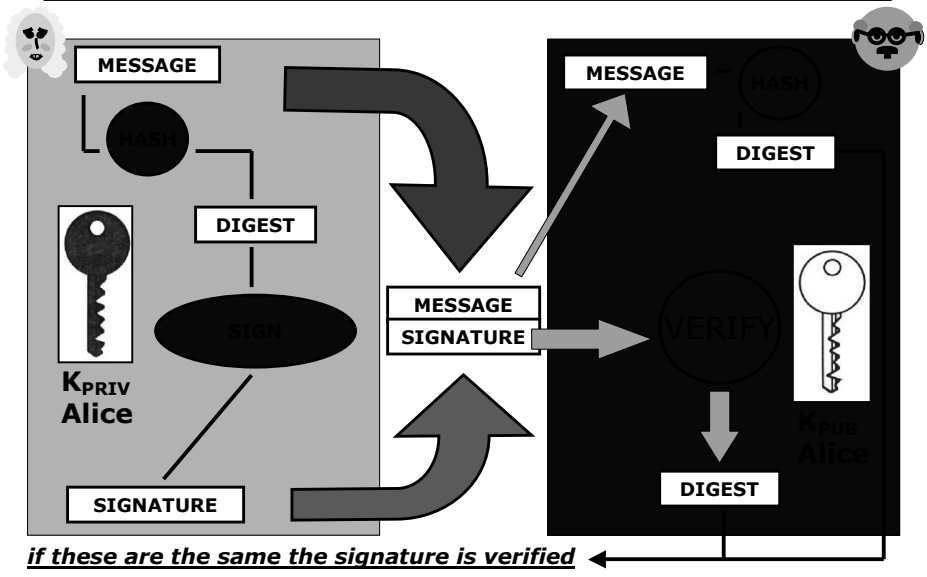
SIGN ... no *hash* [1]



Michèle Martoni © 2003



SIGN ... & *hash* [2]



REAL Identity?

I can obtain keys with a false identity ...
for example using a software like **PGP**...
Nobody verify my **real identity** before...





TTP [1]

Trusted Third Part

Certification & Registration Authority [CA&RA]

Certification means the result of a computer-based process that is applied to the **public key** and that can be detected by validation systems, whereby

the **public key is certified unique to its holder,**

the **holder is identified,**

the **period of validity of the key** and the expiry date of the corresponding certificate are set ...

Michèle Martoni © 2003



TTP [2]

Certification authority *means*

- 1) the **PUBLIC or PRIVATE entity**
- 2) that effects the **certification**
- 3) issues the public key **CERTIFICATE**
- 4) makes the public key and the corresponding certificate **PUBLICLY AVAILABLE**
- 5) and publishes and updates certificate **suspension** and **revocation** lists

Michèle Martoni © 2003



TTP [3]

Examples of X.509 Certificate

Data:
 Version: 0 (0x0)
Serial Number:
 02:41:00:00:01
Signature Algorithm: MD2 digest with RSA Encryption
Issuer: C=US, O=RSA Data Security, Inc.,
 OU=Secure Server Certification Authority
Validity:
 Not Before: Wed Nov 9 15:54:17 1994
 Not After: Fri Dec 31 15:54:17 1999
Subject: C=US, O=RSA Data Security, Inc.,
 OU=Secure Server Certification Authority
Subject Public Key Info:
Public Key Algorithm: RSA Encryption
Public Key:
 Modulus:
 00:92:ce:7a:c1:ae:83:3e:5a:etc
 Exponent: 65537 (0x10001)
 Signature Algorithm: MD2 digest with RSA Encryption
Signature:
 88:d1:d1:79:21:ce:e2:8b:e8:f8:c1etc

Cert. Authority ID	1
Certificate Number	
Issuer ID	
Issuer Public Key	
Validity Period	
Hash part 1	2
Cert. Authority Signature	3

Michèle Martoni © 2003



TTP_Time Stamping

Certification authority effects

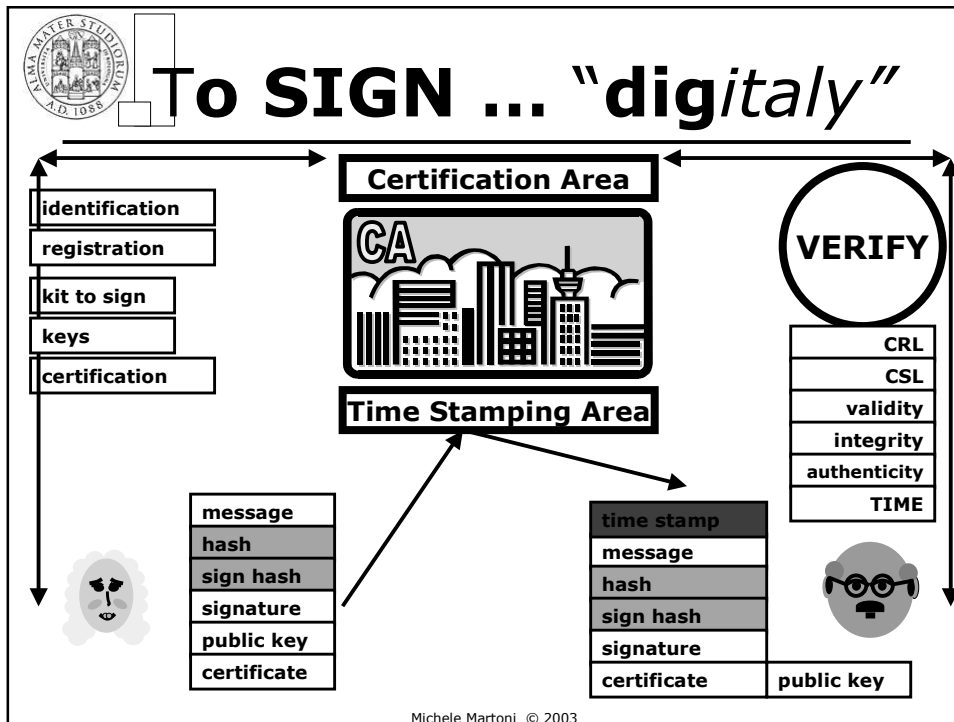
➡ **Validation by time-stamp** that means

the result of a computer-based process under which one or more electronic documents are **marked with a date and time** that are **legally valid** against **third parties**

Michèle Martoni © 2003



To SIGN ... "digitaly"

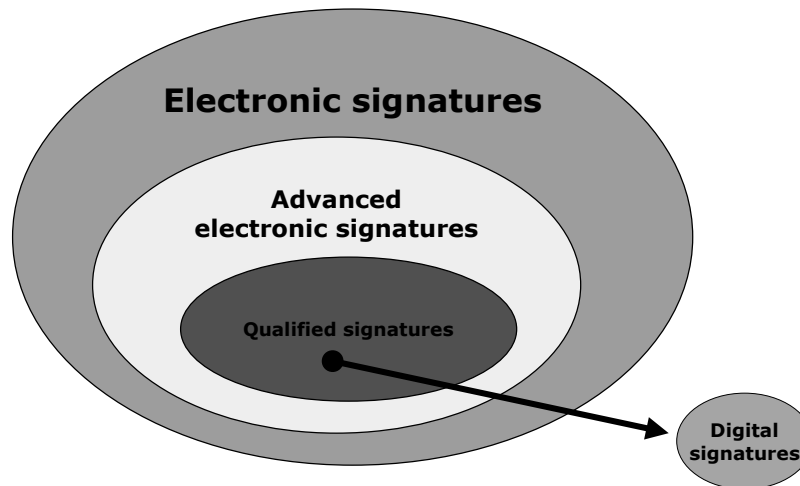


Norm

- Law N. **59/1997**
- Presidential Decree N. **513/1997**
- Prime Minister Decree **08/02/1999**
- European Directive N. 1999/**93/EC**
- Presidential Decree N. **445/2000**
- Legislative Decree N. **10/2002**



Now? ... Future!



(*) Scheme by EESSI – European Electronic Signature Standardization, www.ict.etsi.org

Michela Martoni © 2003



Useful LINKS

www.aipa.it
www.europa.eu.int
www.ict.etsi.org
www.innovazione.gov.it
www.uncitral.org
www.eema.org/ecaf

www.gnupg.org
www.pgp.com
www.rsasecurity.com
www.findlaw.com/01topics/10cyberspace/index.html

[...]

Michela Martoni © 2003



Thank you ... Bye !

DR. Michele Martoni

CIRSFID
University of Bologna

martoni@cirfid.unibo.it
051.277231

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP Pincaware 6.0.2

```
mQGIBD0aRBAADy170aqY965YCZbvs/umsenpeP799XXMn39Ls+tlNupLod
rgHLQOMtdyG8NWYkXozZmEHVWdPSeThYLSSAbZWkjgk2yF78HmW0GdV
Ktr2mYVDE5Wjbs5SNVMeLQbwqhs+c5VID9BBT0VBBUHCQzNaMYwCpwo6
1+wW1PjRZyglEaia+AcBYMDR0G1h+KqwsaZl0Xjg7maW5Eak3yJlUeTb3
1k4APETVNTOUTUSC:0E1Lj+uaa0a0TPVVSSTBMBXKX7e5rHj0v0QmABMde
pLd2GANNYPLabOG1260z2BU98KD2XofLarpD311ueqRmaTjgwe5wZyq
RwE3AdKks+hb8VOC6W4d8gN3Se5L4p8BjQWNG6R8jGAA0f0Dza5Fvz
n0PdVTWsdM:UFQ5M4wAKOMAU1NPNXMrp+66Qv3M+Kj60D30077RZ2aNo
aB0mewWdEagYPRM+XGCMRatGmqmUcDmdeSUW77QpTWjWGVZSBN
YX0k25pDvaYX0k25pQGNpcanZpZS3bualhy5pd60AFEEBECABEFAJvBOAF
CQFDaEAcMAQAACRCy74u0k7JaeGAI4WNRBACVikjXZPabhaqYSLGSAFC
W0wagZLZLECLXUM7Xv17f55a0EFPsE68AMAMwdd1ck0ErxPdqhNa0MS
EH22+ZD899j3yHsMh0HDC79FrxMRjEDYMP6NYKof0Egung6qZQh1
AFMBoHwq0MShH0PK44HBRPyvMX36RAGdIS7ZCZQ2wSMLF6HjgCoi+Lz3k
XXu11JfPmJDCqg53y9LX0wvC8Dy0rWqULB95L4E5T7h0bLOCDabaaW
mTjg0W9WAWlcc0z090akda0409ZLXKHHTLpJWV4dFFPZS6ZVA55
Wc9uK8FXN3dyDhLwYc59WmFm7Zz0wGqf0ag03jg1DcC8gBYkX0
P1YThbeSC0eSRBZAM2+4DUUdD3jccx5WY209P1B8D8XVGDn1WMaF04
0cTWBdNQMG6GmMjEaSePOGAKUAYEY18KcKcaGAMZyApsqvYDnmW6fQ
CCBa8TCDImpF1B55s8YILBbmaquCNV6UwcywACAgvLKAZGMD0MpsKoi
q07RadoYtaSH4kRECK8VApdhe1TP0x0jzZVdQBYMWMyntGSMRQwv1
0E49ZHLjaneAYVW11KH10p4+XvT+GKJwXBV86Bkwsh0+wLEqK2P0L4a
KHUVZjZD6gR8jgDXBZqP8V820+5wR7JGQe5E6V0y3zjgB80wCvA0kx
1PPhgYU480Y5e8XLU84wvVB9wVcYIEZLU6CmaLcCua0O54G8YB4M0QR/
mzZIdUSXawncy2UY7q1MWajDqMfPb5G9R20M0rpp27NWVXc38gOCZ
Dc3p0f04d0+Tt01p0W096m0FDV0j0j0K08086k0k0v0L0B0yP0m0XV
036NwYAc0a07ED48dD1YQEMX08HDMZ0aZ0a0VTVS0j2850bV5Z20a9989
0y15p10V0690PccaaZz09n04M+G0mL0e4bYKZ4PVQRLB8RAgAM8Q89
KwT0BQldw7AAa0ELLS0LSJ0maH0a0648NTP8M6H-GROOFPy0odsH0aAJF
KpSLho79LVtqPvmz+5E
+e53a
-----END PGP PUBLIC KEY BLOCK-----
```