

# Electronic Signatures and Certificates in Healthcare




Filip De Meyer

Dept. of Medical Informatics Gent

Phone: +32 9 240 34 40

E-mail: [Filip.DeMeyer@rug.ac.be](mailto:Filip.DeMeyer@rug.ac.be)



# Why do you require a signature on a document ?

- ◆ Prove that the author/sender is the one he claims to be (identity and roles).
- ◆ Prove that writing/sending the document is something he wanted to do.
- ◆ Prove that the content has not changed and is complete (integrity requirement).
- ◆ Date (and time) stamping.



Give e-docs legal value



# Electronic Signatures:

- ◆ Signature dynamics
- ◆ Biometrics: voice, fingerprint, face, retina,...
- ◆ Key based cryptographic functions
  - Public key cryptography



**Digital** signatures are  
based on public key  
cryptography



# Digital signature definition

*A digital signature of a plaintext is the result of the encryption of the hash result of the plaintext with the private encryption key of the sender (author)*



# A digital signature is a function of

- ◆ The plaintext (or message) on which the message is generated
- ◆ The private key of the person who is signing

A handwritten signature is independent of the context and is only function of the signature dynamics of the person who signs



# Cryptographic key pair & certificates

- ◆ Key pair for encryption for confidentiality
- ◆ Key pair for digital signature
- ◆ Key pair for authentication
- ◆ Identity certificate (public key certificate)
- ◆ Attribute certificate(s)
  - Professional qualification
  - Professional registration
  - Professional role(s)

# Signature Key Management

- ◆ Generate key pair
- ◆ Private (signature creation) key handling
  - Put in a highly secure environment (smartcard)
  - Personalise the smartcard
  - Generate pincode
  - Distribute pincode and smartcard
- ◆ Public (signature verification) key handling
  - Create a certificate (bind the ID to the key-pair)
  - Publish the certificate (directory)
  - Follow-up: revocation





# Trust in signature only when

- ◆ private keys are kept private in a very secure and tamperproof environment by the key holder



Store private keys into a smartcard

- ◆ Association between public key and the key holder is guaranteed.



A TSP should issue key certificates





# Trust Service Provider (TSP)

An entity which can be used by other entities as a trusted intermediary in a communication or verification process, or as a trusted information service provider

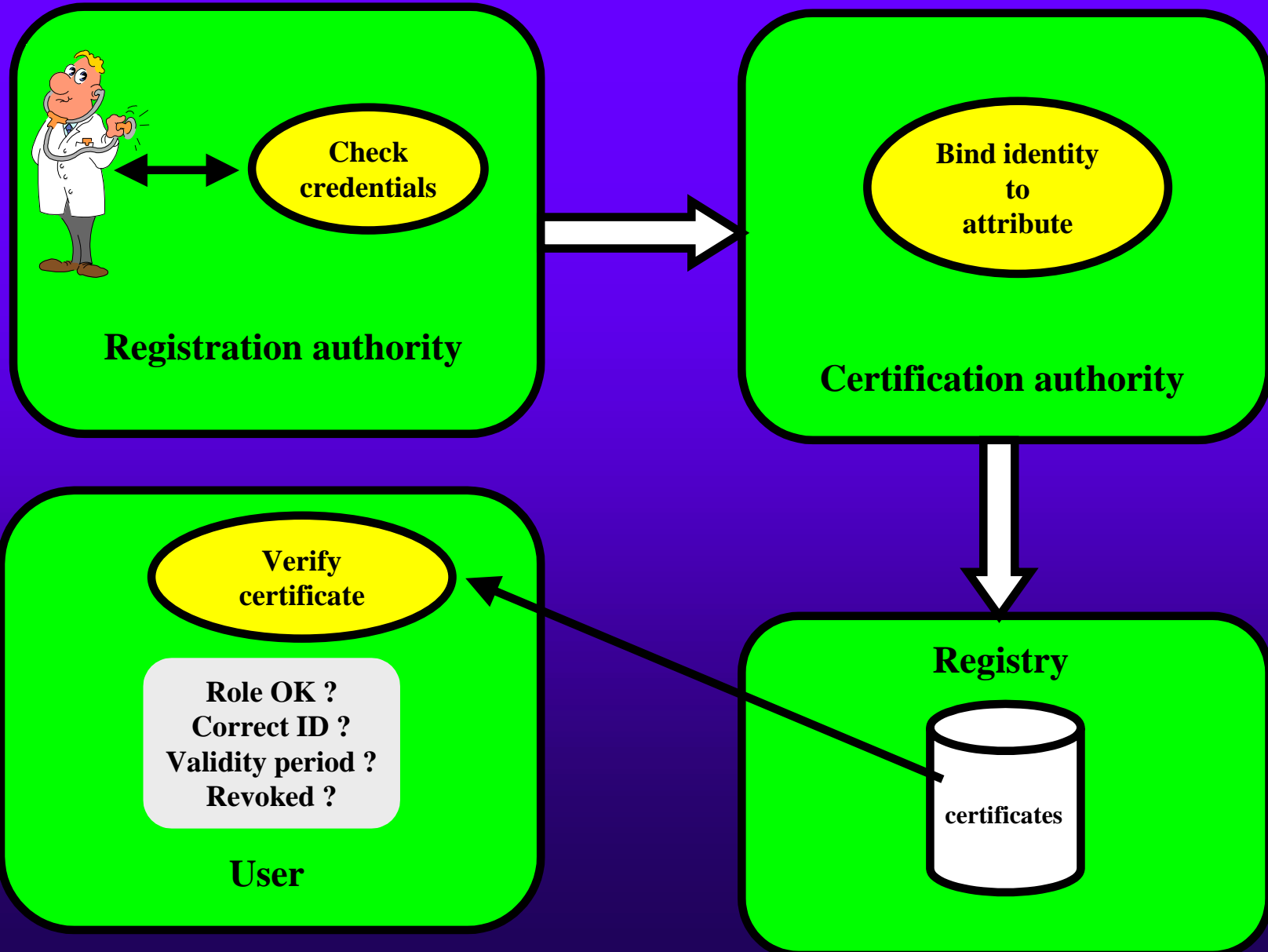
- ◆ Certification authorities
- ◆ Attribute authorities
- ◆ Registration authorities
- ◆ Time Stamping authorities
- ◆ Privacy enhancing service providers (pseudonymisation)



# Trust Service Providers (signatures)

- ◆ Registration Authority (RA)
  - Verifies credentials:
    - Identity
    - Attribute: mandate, quality, ...
- ◆ Certification Authority (CA)
  - Puts the conclusion of the RA into an electronic certificate
  - The certificate is electronically signed by the CA
  - The signed certificate is sent to a directory service provider

# Certification of attributes

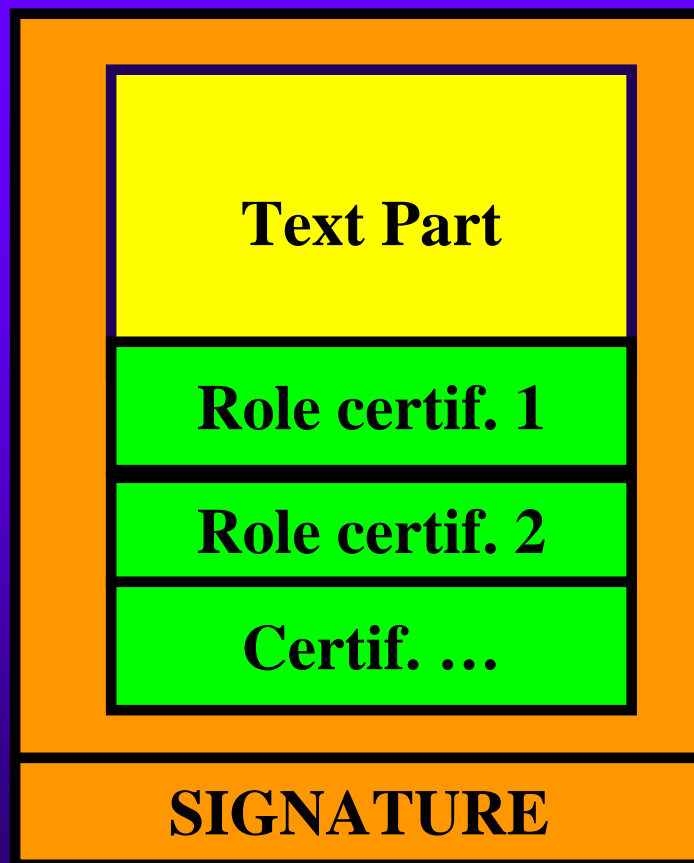


A single, old-fashioned metal key with a circular bow and a notched bit, resting on a textured, light-colored surface. The key is positioned vertically on the left side of the slide.

# Different approaches

- ◆ One identity to many roles
  - One signature per natural person
  - Mandates, roles, qualities, etc. are expressed in an attribute certificate
  - Is close to the real world situation
  - A role/certificate -> privacy protection
- ◆ One identity to one capability
  - One (different) signature per attribute
  - A different role = different signature

# Structure of a signed document





# Conflict situations: abuse of a function (certificate)

- Same in both approaches
- Cannot be prevented on the signature level
- Similar as in paper based world: cannot be prevented at all
- On the application level: warn the user for abusive use of certificates
- Present pick-list of certificates to the signatory

## You are about to **sign** a document

### The reference for the document is:

Filename: **C:\requests\doc000503.rtf**

Date of last update: **4<sup>th</sup> May 2000**

Author: **Mary, secretary of Dr. Jekyll**

Subject: **request for information on Homer Simpson to VUB**

Filesize: **35.254 bytes**

### Identification of the Signatory

Name: **James Jekyll**

Signature certificate ID: **15668de4** issued by: **KSZ-BCSS**

Certificate is valid until: **5/1/2009**

### Check one or more certificates:

<b>Cert_ID/issuer</b>	<b>Role</b>	<b>valid</b>
<input checked="" type="checkbox"/> Order/01586	Medical Doctor	1/1/99
<input type="checkbox"/> Order/15862	General practitioner - Brussels	3/12/10
<input checked="" type="checkbox"/> UCL/2658	Head of Dept. – ORL/UCL	2/1/05
<input type="checkbox"/> DKV/2561	Insurance Physician	1/6/01

**Warning:** you can be held liable for inappropriate use of certificates according to law with reference xx

**ACCEPT**

**CANCEL**



# Legislative Framework

- ◆ Social Security Royal Decree (16 Oct 1998)
- ◆ European Directive 1999/93/EC on a Community Framework for electronic signatures
- ◆ Belgian Bill on the operation of certification service providers for the application of electronic signatures (Belgian Chamber of Representatives, Doc 050322/001)





# European Directive

**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

## **Advanced electronic signature:**

- Uniquely linked to signatory
- capable of identifying the signatory
- Created using means the the signatory can maintain under his sole control
- Linked to the data so that any subsequent change of data is detectable



# Directive (continued)

- ◆ No creation of certificates without the knowledge of the holder
- ◆ Accreditation for certificate service providers is voluntary
- ◆ Uses the term 'electronic signature' and not 'digital signature' -> technology independent
- ◆ Member states must comply before 19<sup>th</sup> July 2001



# Belgian el. Signature legislation

- ◆ Bill (Wetsontwerp, Project de Loi) for certification (el. Signature)
- ◆ DOC 500322/001 (16.12.99)
- ◆ <http://www.dekamer.be/documents/322/1.pdf>
- ◆ Bill for acceptance of el. Sign for Justice Dept. (21.6.2000, Doc 5000038/007)



# Belgian Signature initiatives: other

## ◆ Agora Project

- Federal project
- Public administrations (Finance, economic affairs, X-road databank, national statistics institute, national register, ...)
- Agreements on technical aspects
- Distinction: personal ID and mandate

## ◆ Royal decree 12.3.2000: modernisation of public administration