Attribuut-gebaseerde elektronische handtekeningen en de eIDAS-verordening

- Yong Yong Hu, Pieter Wolters, Bart Jacobs en Fabian van den Broek
- To appear (I think)

PART 1: THE LEGALESE

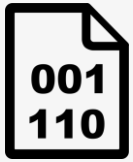
Wet vs. Digital

- Identity of the signatory
- Expression of intent

- Identity of the signatory
- Integrity of the document
- Non-repudiation

Digital vs. Electronic

- Digital signatures



- Electronic signatures

Electronic signatures (legal effect)

- No discrimination against signatures in electronic form
- 3 types
  - Electronic signatures
  - Advanced electronic signatures
  - Qualified electronic signatures

Electronic signatures (legal effect)

- No discrimination against signatures in electronic form
- 3 types
  - Electronic signatures
  - Advanced electronic signatures
  - Qualified electronic signatures == handwritten signature

Electronic signatures (legal effect)

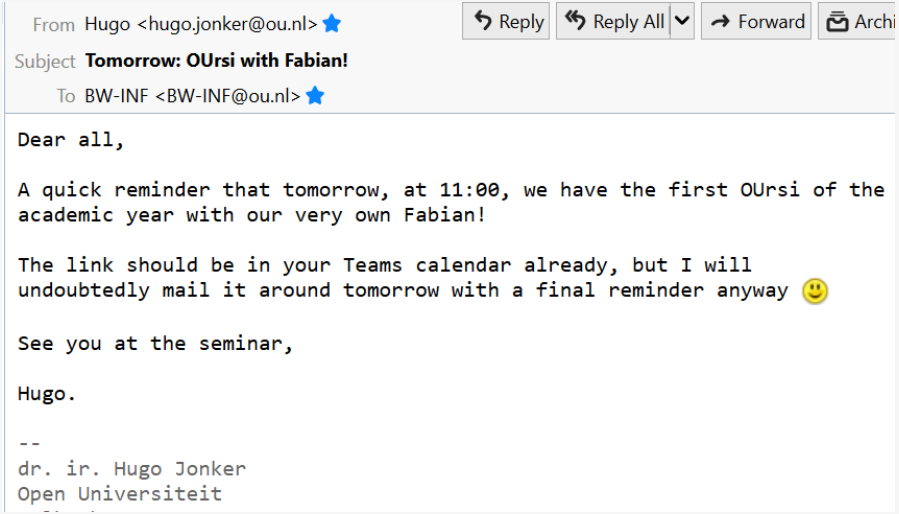
- No discrimination against signatures in electronic form
- 3 types
  - Electronic signatures
  - Advanced electronic signatures
  - Qualified electronic signatures == handwritten signature
- Qualified in one member state ➔ qualified in all member states

Electronic signature (definition)

data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;

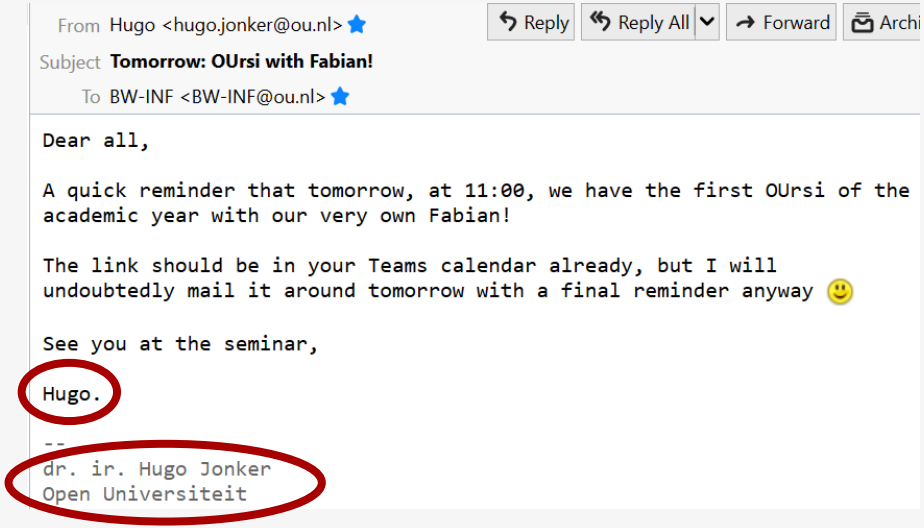
Electronic signature (definition)

data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;



Electronic signature (definition)

data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;



Advanced electronic signatures

(a) it is uniquely linked to the signatory;

(b) it is capable of identifying the signatory;

(c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and

(d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

Qualified electronic signatures

(a) it is uniquely linked to the signatory;

(b) it is capable of identifying the signatory;

(c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and

(d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

\+ The signature is made with a Qualified certificate

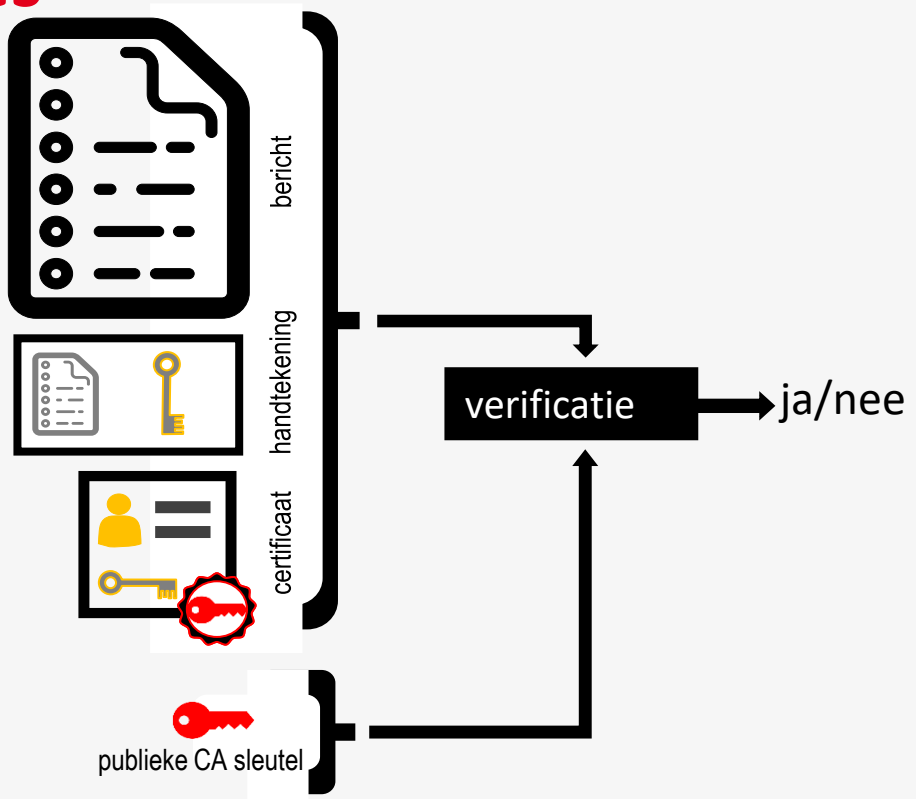
PART 2: THE TECHNICAL

Standard digital signatures

- Standard digital signatures often rely on certificates
  - ➔ Certificate-based signatures (CBS)

Standard digital signatures

- Standard digital signatures often rely on certificates
  - ➔ Certificate-based signatures (CBS)

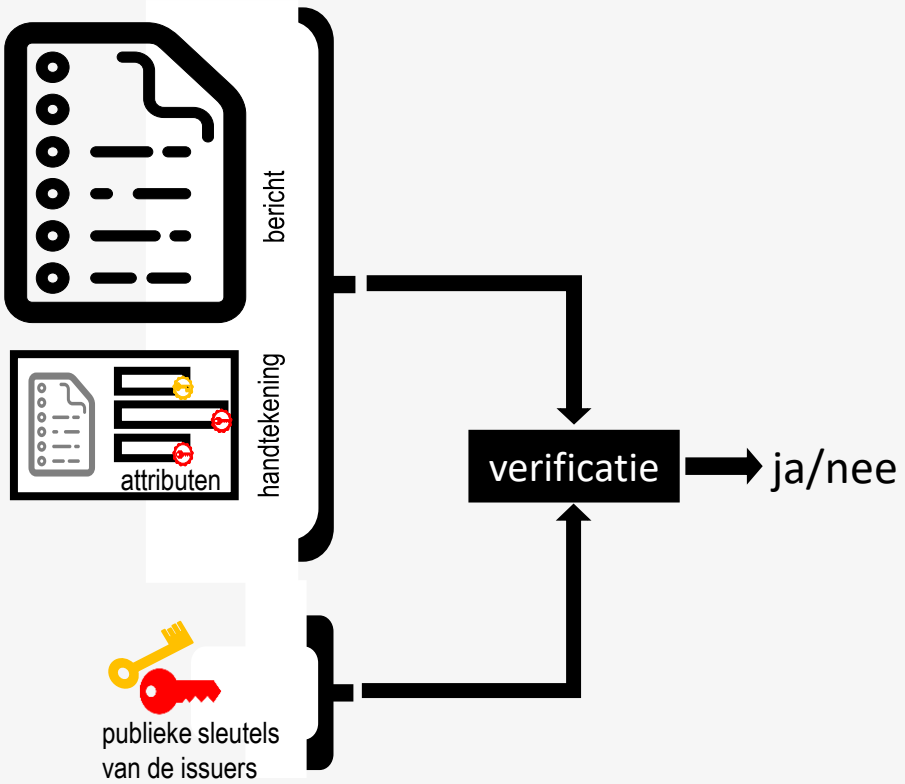


Attibute-based digital signatures (ABS)

- Do not use certificates
- Verified attributes are added to the signature

Attibute-based digital signatures (ABS)

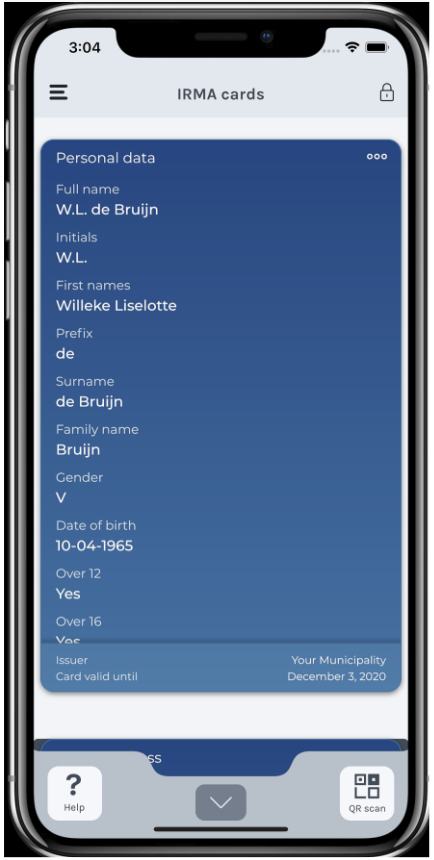
- Do not use certificates
- Verified attributes are added to the signature



CBS vs. ABS

- CBS
  - Certificate-based
  - Rigid
  - Linkable
  - Always identifying
  - Supported by the legal framework
- ABS
  - Attribute-based
  - Flexible
  - Unlinkable
  - Possibly non-identifying
  - Supported by the legal framework?

IRMA


3:04
IRMA cards
Personal data
Full name
W.L. de Bruijn
Initials
W.L.
First names
Willeke Liselotte
Prefix
de
Surname
de Bruijn
Family name
Bruijn
Gender
V
Date of birth
10-04-1965
Over 12
Yes
Over 16
Issuer
Your Municipality
Card valid until
December 3, 2020
Help
QR scan

PART 3: THE SYNTHESIS

ABS and the legal framework?

Attribute-based signatures:

- lack certificates

ABS and the legal framework?

Attribute-based signatures:

- lack certificates


data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;


it is uniquely linked to the signatory;


it is capable of identifying the signatory;


it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and


it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.


The signature is made with a Qualified certificate

ABS and the legal framework?

Attribute-based signatures:

- lack certificates
- can be anonymous

ABS and the legal framework?

Attribute-based signatures:

- lack certificates
- can be anonymous

data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;

it is uniquely linked to the signatory;

it is capable of identifying the signatory;

it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and

it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

The signature is made with a Qualified certificate

The legal framework is being revised

Working with legal scholars

- Legal misconceptions
  - Signatures are almost never required
  - What is ‘identiying’?

- Writing in Dutch
- Research as arguing a position

- Multi-disciplinary vs. Inter-disciplinary

BEDANKT VOOR UW AANDACHT

Open Universiteit

WWW.OU.NL