Digital / Electronic Signatures

PET Workshop 2003 Dresden

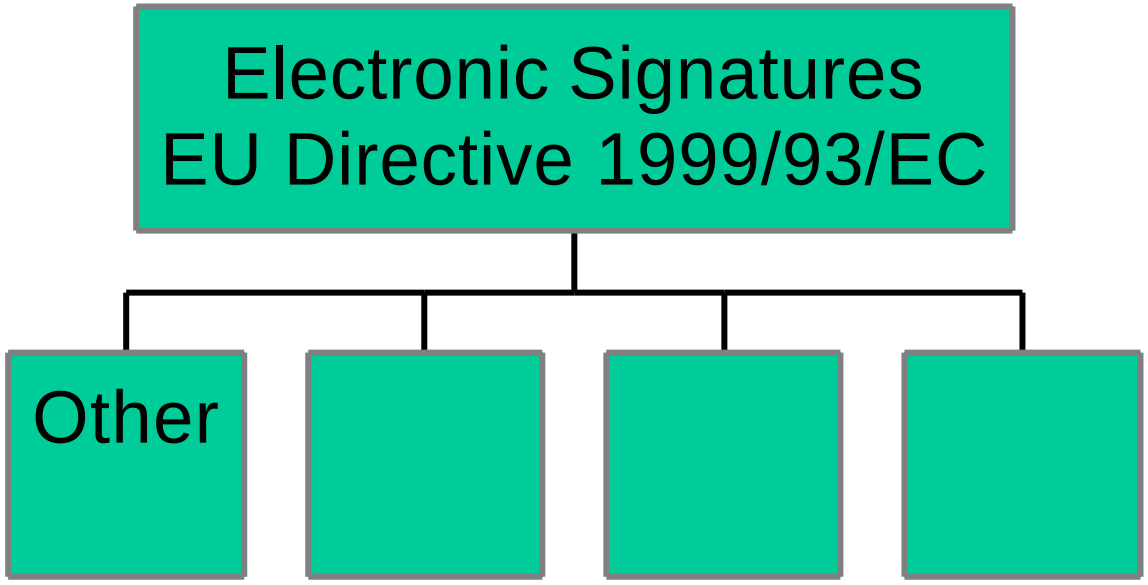
Henry Krasemann
ICPP Schleswig-Holstein

UNABHÄNGIGES LANDESZENTRUM
FÜR DATENSCHUTZ SCHLESWIG-HOLSTEIN

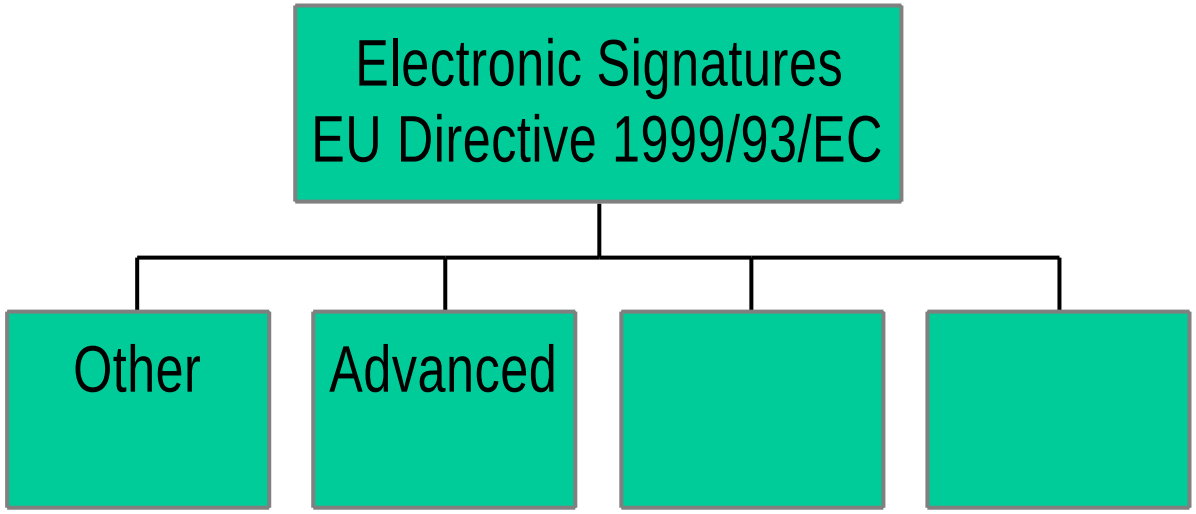
Use of Pseudonyms in Digital Signatures

- Pseudonym instead of name in certificate (no further data)
- States are free to allow use of pseudonyms (e.g. German law wants use of Pseudonyms)
- Indicated by the entry „PN“
- Restriction who can reveal Pseudonym

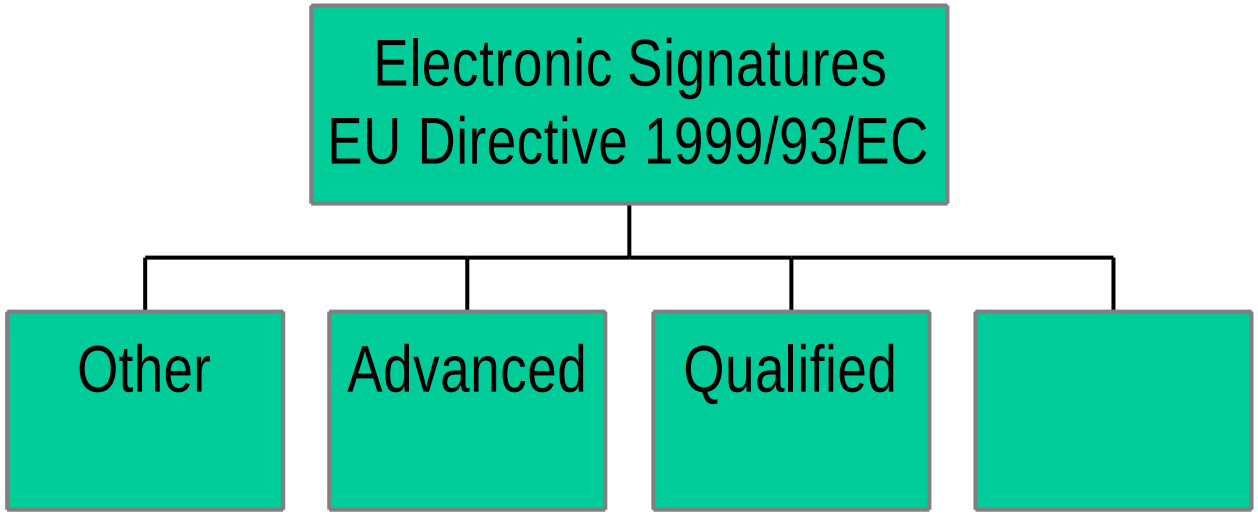
Different Types of Electronic Signatures



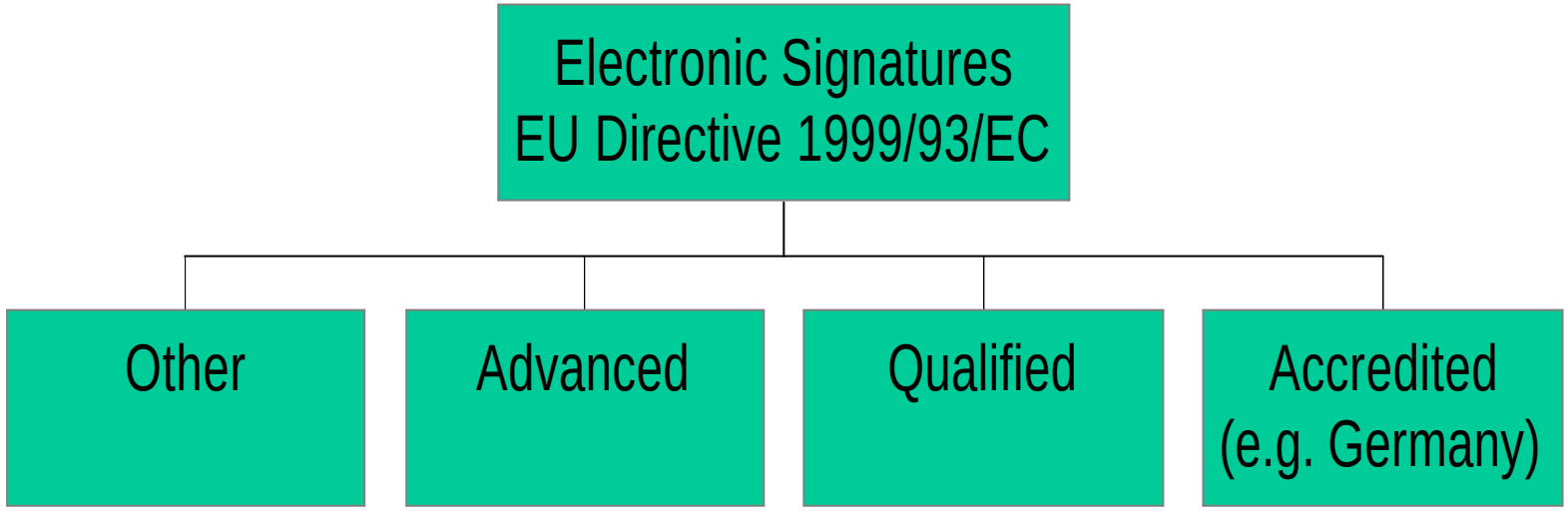
Different Types of Electronic Signatures



Different Types of Electronic Signatures



Different Types of Electronic Signatures



Other Electronic Signatures

- Means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication
- E.g. PGP
- Also scanned handwritten signature pasted under email

Advanced Electronic Signatures

- It is uniquely linked to the signatory
- it is capable of identifying the signatory
- it is created using means that the signatory can maintain under his sole control
- it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable

Qualified Electronic Signature

- Requirements of advanced Signature
- *and* signature must have been caused with a safe signature construction unity
- *and* signature must be based on a valid qualified certificate at the time of its production

Accredited Electronic Signature

- „Qualified Electronic Signature based on voluntary accreditation“
- Qualified Electronic Signature + Pre-Permission
- Prove the fulfilment of the duties for qualified signatures before start

Legal Effects

2 Questions:

- **A. Satisfy legal requirements (e.g. Standard in Germany no particular form requirements)**
- **B. Admissible as evidence in legal proceedings**

Satisfy legal requirements

Accredited

Particulary Administration

Qualified

Same manner as handwriting
(relation to paper based data)

Advanced / Other

Like normal EMail
Where law doesn't require particular form

Evidence in legal proceedings

Accredited

Highest probative value
Presumption of law

Qualified

High probative value
Presumption of law e.g. § 292 ZPO (Germany)

Advanced / Other

Low Probative Value
Full proof necessary / Free Evaluation of Evidence

Liability

- Certification-service-provider is liable for damage caused to any entity or legal or natural person who reasonably relies on that certificate (accuracy of information contained in certificate; identification of signatory etc.)

Questions / Problems

- Acceptance of pseudonyms in reality
- Acceptance of certificates of third countries
- Which algorithms are secure / what if change?
- How to do new signing when old method becomes unsecure?
- What is in case of corruption?