Using

AnIML

in Regulated Environments

Dr. Maren Fiege, Waters GmbH

PittCon 2008, New Orleans, LA, USA

March 4, 2008

Content

- Regulations

- Some Definitions

- Compliance Features in AnIML

- FDA guidance documents for the industry:
  — 21 CFR 820 (Medical Devices)
  — 40 CFR 160 (Environmental GLPs)
  — 21 CFR 11 (Electronic Records/Signatures Rule)
  — 21 CFR 110 and following (Food)
  — 21 CFR 210, 211 (Pharmaceuticals)
  — 21 CFR 312 (Clinical)
  — 21 CFR 58 (GLPS for non clinical studies)
  — GALP (Good Automated Practices for EPA)
- EPA
  — CROMERR

Electronic record

"any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system."

"Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine."

"Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:

(1) The printed name of the signer;

(2) The date and time when the signature was executed; and

(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout)."

Electronic Signatures

"*Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.*"

"Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review."

Accuracy

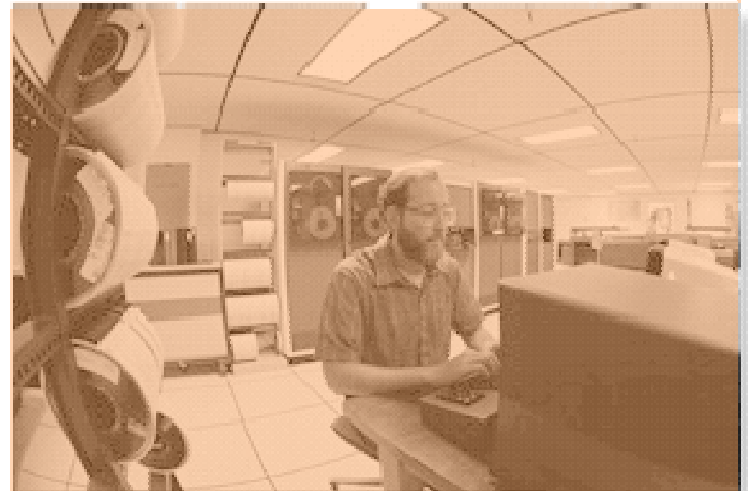"*The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency.*"
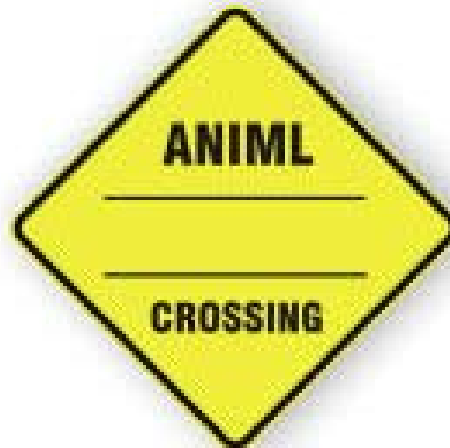
Electronic records must be reproducible in electronic and paper form (including audit trail and metadata) in general and upon request.

- Long term stability of data formats
- Independence from software vendor
- Easy integration of data in existing applications
- Easy translation of data if required
- Enhance productivity by making archived data available as an expert knowledge resource corporate wide
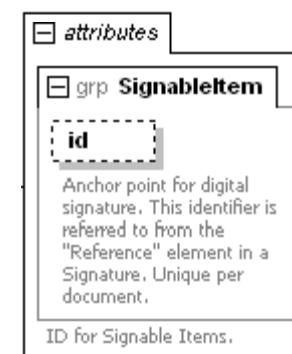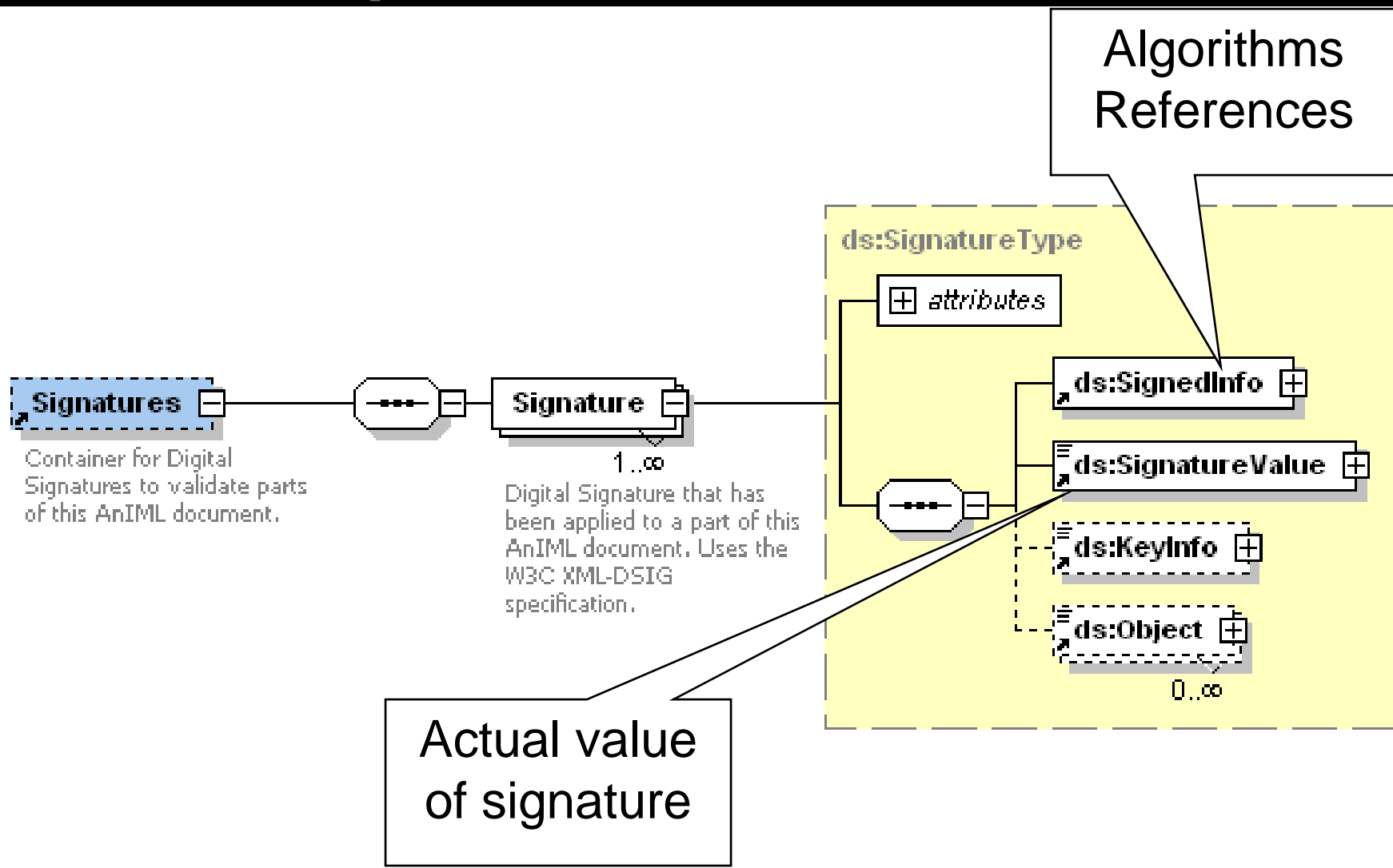
- Protect (parts of) AnIML Document from undetected tampering

- "Signable Items"

  - XML document is "serialized"

  - Cryptographic hash function is applied

  - Result is encrypted by an asymmetric key algorithm

  - a single-byte difference would invalidate the digital signature

- Multiple signatures with variable coverage

- Uses the XML DSIG* standard by the W3C/IETF

  — Timestamping, roles, PKI integration

  — Uses standard algorithms

Diagram:

☐ attributes

☐ grp **SignableItem**

    id

Anchor point for digital signature. This identifier is referred to from the "Reference" element in a Signature. Unique per document.

ID for Signable Items.

* XML-Signature Syntax and Processing Specification
http://www.w3.org/TR/xmldsig-core/

Waters
THE SCIENCE OF WHAT'S POSSIBLE.™

Algorithms
References

ds:SignatureType

Signatures

Container for Digital
Signatures to validate parts
of this AnIML document.

Signature

1..∞

Digital Signature that has
been applied to a part of this
AnIML document. Uses the
W3C XML-DSIG
specification.

attributes

ds:SignedInfo

ds:SignatureValue

ds:KeyInfo

ds:Object

0..∞

Actual value
of signature

Keeps track of Changes
made to the Document

Really?

When?

Who?

What?

Why?

What?

Where?

- XML-based
  - — Human readable (although not meant to be read)
- Uses standard tools
  - — XML schema
  - — XML-DSIG
  - — Base64 encoding