Implementing PDF-based eIDAS trust services

Bernd Wild
intarsys AG, Member of the Board of PDF Association

Dr. Bernd Wild,
Member of the Board of PDF Association

eIDAS – electronic Identification and Trust Services

- REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
- Officially published on 28.08.2014

Dr. Bernd Wild,
Member of the Board of
PDF Association

The relevant trust services of eIDAS

www.pdfa.org

TIMESTAMPS
Qualified timestamps

SIGNATURES
Qualified signatures
(person-related)
local and remote signatures

SEALS
Qualified seals
(organization-related)

ELECTRONIC DOCS
Non-discrimination

ELECTRONIC DELIVERY
Secure message delivery services

LTP + VALIDATION
Longterm preservation
Validation of signatures, timestamps and seals

Dr. Bernd Wild,
Member of the Board of
PDF Association

eIDAS and PDF

- Vast majority of all electronically signed documents are PDF documents
  - „electronic paper“ for static representation
  - ISO standard of document format with integrated electronic signature
- ETSI standards for signing PDF („PAdES“)
  - Explicitly referenced within Implementing Acts
- eIDAS aims at „digitally everywhere“
  - PDF as ubiquitous format

Dr. Bernd Wild,
Member of the Board of
PDF Association

eIDAS - Electronic signature and seals

- Non-discrimination as evidence in legal proceedings (art. 25.1-34.1)
- Legal effect (art.25.2-34.2)
  - e-Signature:
    - Only for natural persons
    - Assimilation to handwritten signature
  - e-Seal:
    - Only for legal entities
    - Integrity of the data and correctness of the origin
- Recognition in all MS of a qualified electronic signature/seal based on a qualified certificate issued in one member state (art.25.3-34.3)

Dr. Bernd Wild,
Member of the Board of
PDF Association

eIDAS - Electronic time stamp

- Non-discrimination as evidence in legal proceedings (art.39.1)
  - Legal effect (art.39.2)
    - Accuracy of the date and time it indicates
    - Integrity of the data to which the date and time are bound
  - Requirements for qualified e-time stamp (art.40)
    - Binds the date and time to data in such a manner as to reasonably preclude undetectable changes to the data
    - Based on accurate time source linked to UTC
    - Signed with an AES or sealed with an AESeal of the QTSP – or by some equivalent method

Dr. Bernd Wild,
Member of the Board of
PDF Association

eIDAS - Electronic documents

- Non-discrimination of electronic documents compared to paper documents as evidence in legal proceedings (art.44)
  - Ensures validity and legal certainty of cross-border electronic transactions through the impossibility for Courts to reject a document on the grounds that it is in electronic form

Dr. Bernd Wild,
Member of the Board of
PDF Association

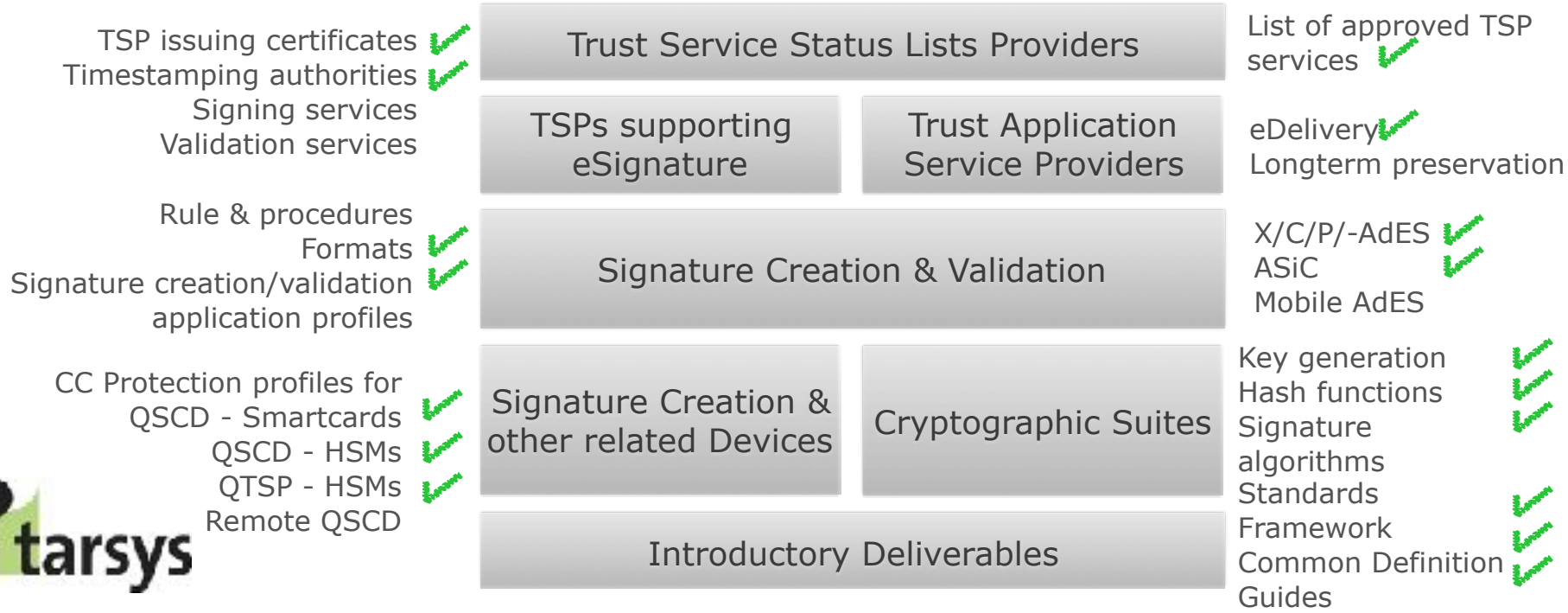
Implementing Acts

NO.	DOMAIN	TITLE
2015/296	eID	24 February 2015 , IA on procedural arrangements for MS cooperation on eID
2015/1501	eID	8 September 2015, IA on the interoperability framework
2015/1502	eID	8 September 2015, IA on setting out minimum technical specifications and procedures for assurance levels for electronic identification means
2015/1984	eID	3 November 2015, IA on defining the circumstances, formats and procedures of notification
2015/806	Trust Services	22 May 2015, IA on the form of the EU Trust Mark for Qualified Trust Services
2015/1505	Trust Services	8 September 2015, IA on laying down technical specifications and formats relating to trusted lists
2015/1506	Trust Services	8 September 2015, IA on laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by
2016/650	Trust Services	25 April 2016 , IA on laying down standards for the security assessment of qualified signature and seal creation devices

intarsys

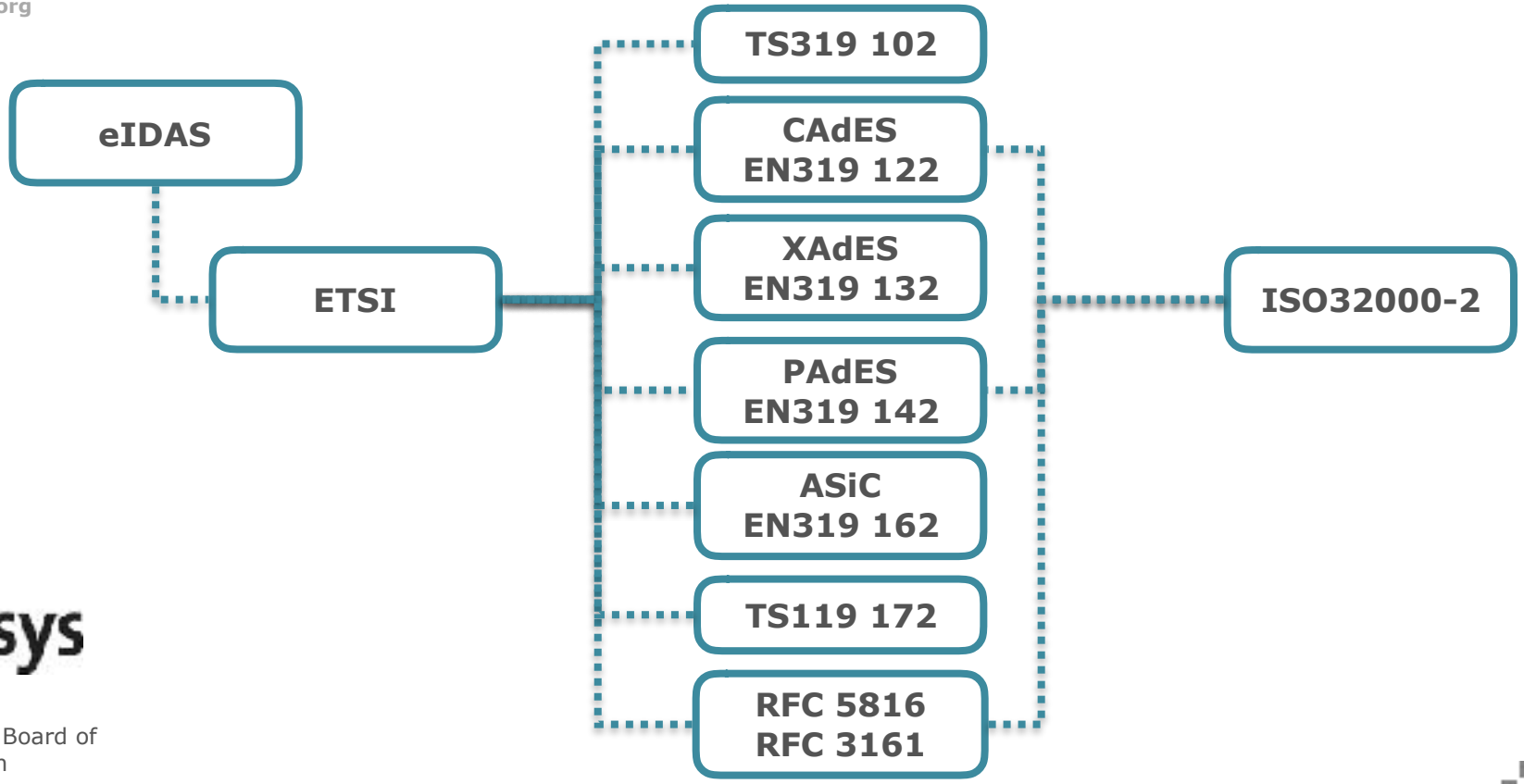
Dr. Bernd Wild,
Member of the Board of
PDF Association

ETSI/CEN Standardization Areas



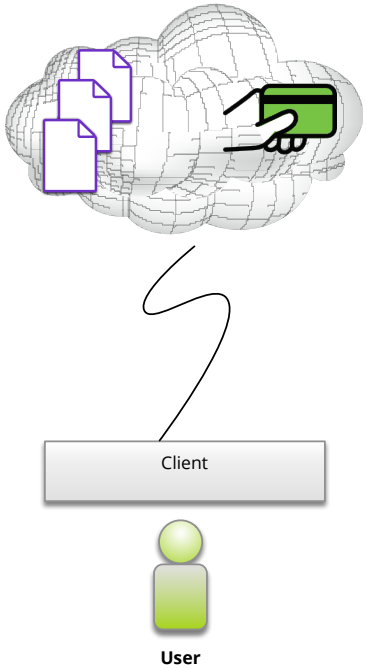
Dr. Bernd Wild,
Member of the Board of
PDF Association

ISO 32000-2 and Signing Standards



Dr. Bernd Wild,
Member of the Board of
PDF Association

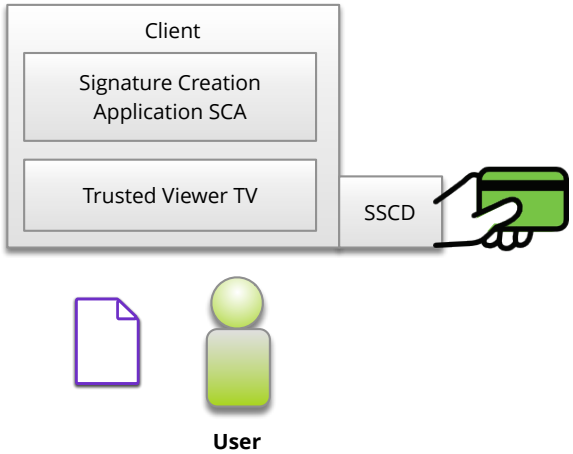
Signature Architecture Cloud



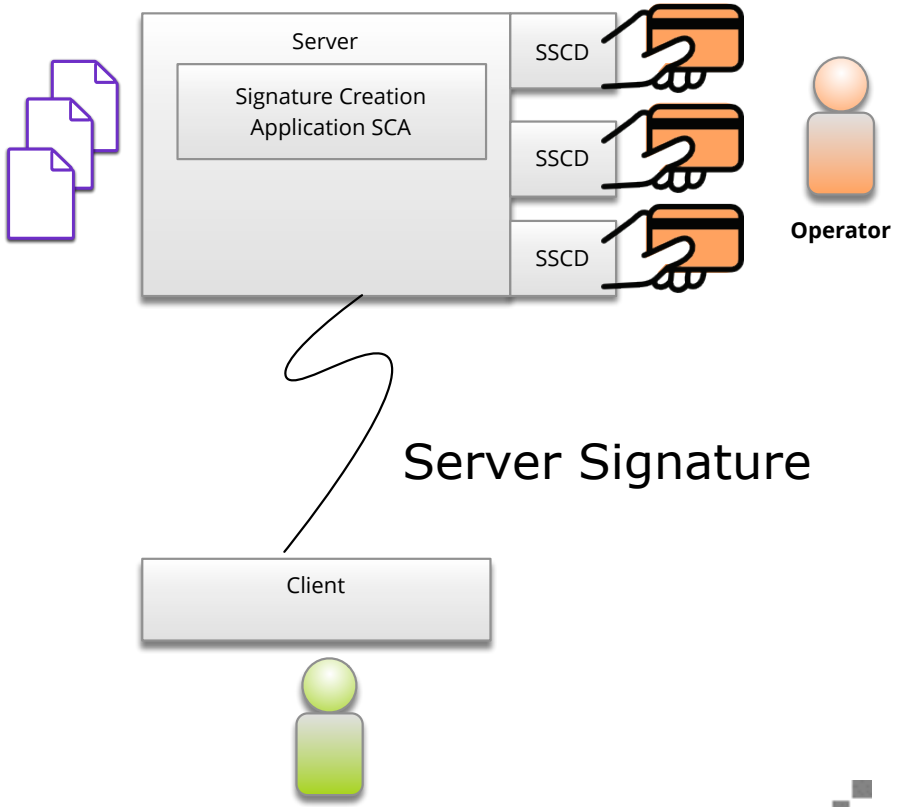
Dr. Bernd Wild,
Member of the Board of
PDF Association

Classical Signature Architectures

Client Signature



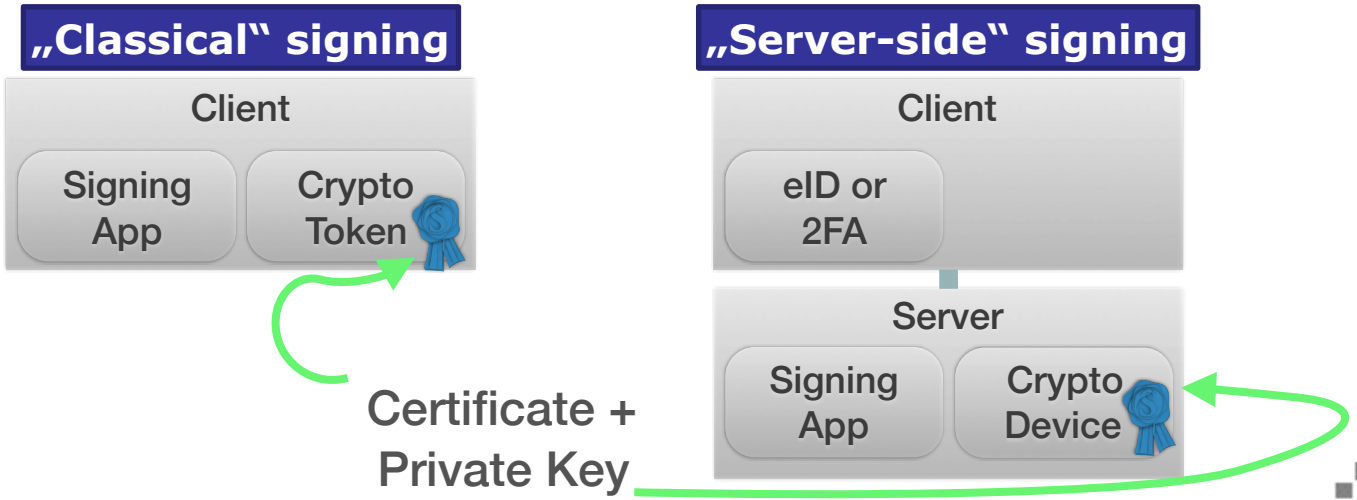
Server Signature



Dr. Bernd Wild,
Member of the Board of
PDF Association

Remote signing or server-side signing

- Article 3.7.c of eIDAS Regulation: *… it is created using e-signature creation data that the signatory can … use under his/her sole control*
- No specific hardware token (e.g. Smartcard) on client side needed
- Secure eID and/or 2FA (Two-Factor-Authorization) become more important
- Better integration in business processes



Dr. Bernd Wild,
Member of the Board of PDF Association

Building a standard for cloud signatures

A new industry consortium to pioneer
open digital signatures for mobile and the web

#OpenSignature

CLOUD
SIGNATURE
CONSORTIUM

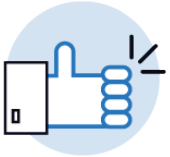
Why Cloud Signatures?

- Simpler certificate handling
  - No complex renewal procedures
  - No loss or theft of token
  - Storing of private key in high-secure environment

- Keeping documents in the Cloud without download
  - Sign documents in the Cloud, no download of large documents
  - Interface to Cloud DMS, Web DMS

- Secure transactions, signing-to-go
  - Web Browser, mobile devices (smartphones), desktop

- Simpler, faster, better!
  - No smartcards or USB tokens, no driver installation, zero dependency of client platform



Dr. Bernd Wild,
Member of the Board of
PDF Association

The actual State of Cloud Signature

- Cloud-based signatures are available since many years
  - But not on a „qualified" level —> not legally binding
- Market penetration was difficult
  - Conflict between user experience and intransparent national legal regulations
- Technological and regulation evolution
  - eIDAS Regulation mentions «Remote Electronic Signatures» and trust services, who offer the creation of qualified signatures on behalf of the client
- Number of existent solutions
  - Proprietary APIs
  - No interoperability
  - Various APIs, authentification mechanisms, certificate enrollment procedures etc.

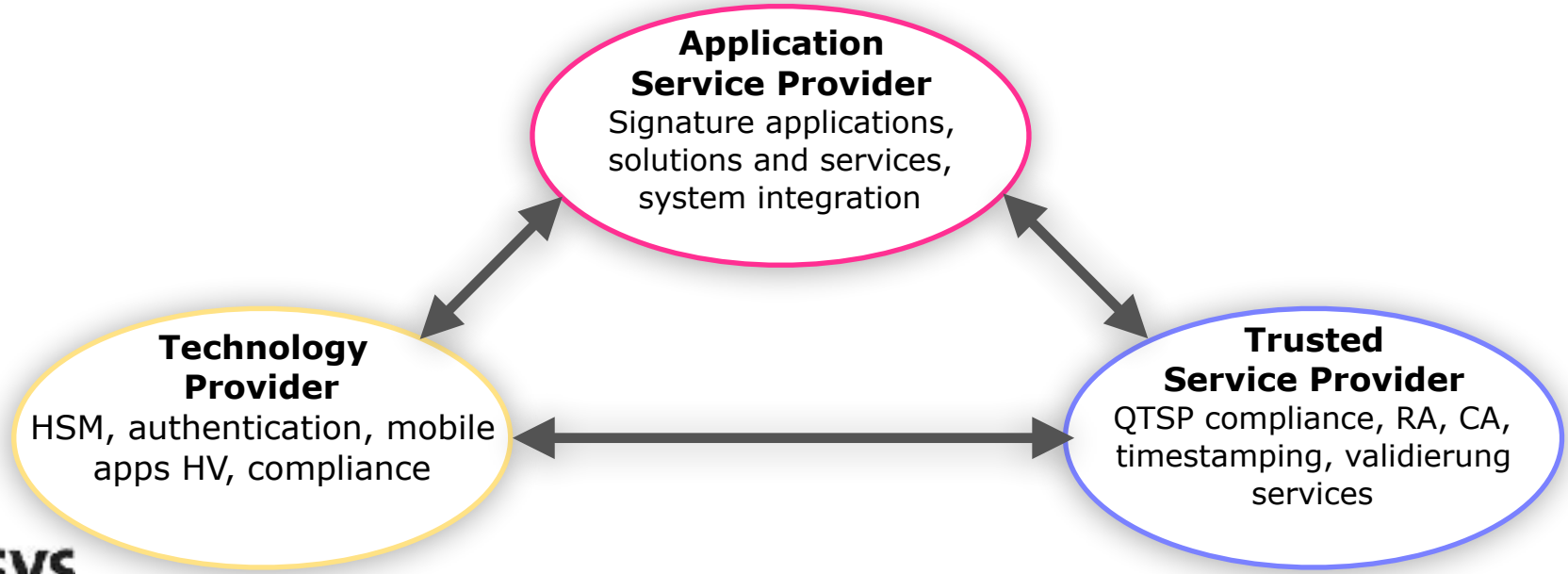
Dr. Bernd Wild,
Member of the Board of
PDF Association

The CSC

- Early 2016 foundation of Cloud Signature Consortium
  - Internationale companies and experts from industry and universities
  - Solution providers, technology companies and trust service providers
  - Some overlapping with ETSI ESI group
- Creation of a common architecture and components for a 3-pillow architecture
- Technical specification of protocols and APIs for interoperable solutions
- Publication of the specifications

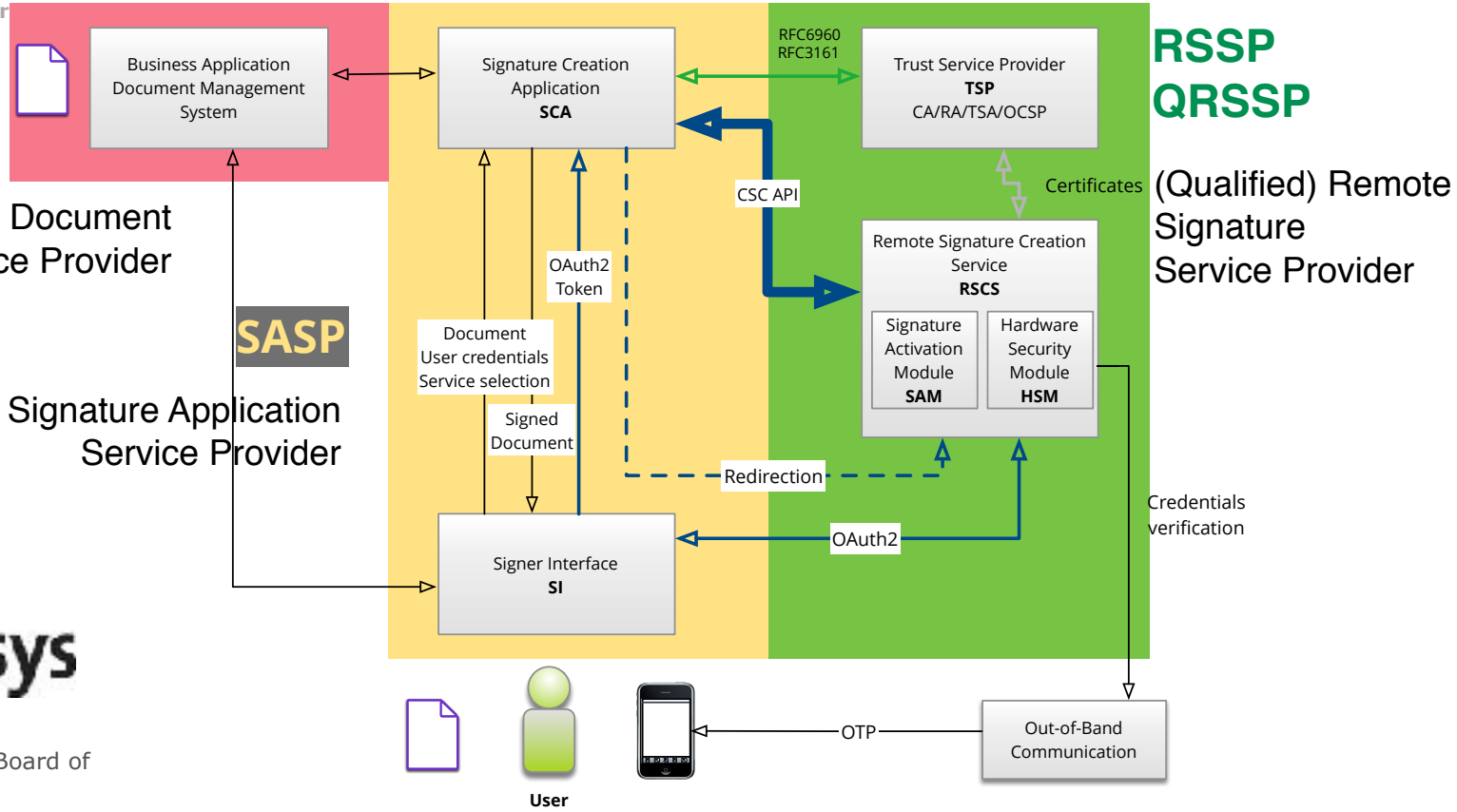
Dr. Bernd Wild,
Member of the Board of
PDF Association

Background CSC



Dr. Bernd Wild,
Member of the Board of
PDF Association

The CSC Architecture – Service Provider



Dr. Bernd Wild,
Member of the Board of
PDF Association

New eIDAS Trust Service: Longterm Preservation

- Article 34:
  Qualified preservation service for qualified electronic signatures
  1. A qualified preservation service for qualified electronic signatures may only be provided by a qualified trust service provider that uses procedures and technologies capable of extending the trustworthiness of the qualified electronic signature beyond the technological validity period.

- Does this mean longterm preservation of (signed) documents?
- In search for appropriate longterm container formats
  - Signature data
  - Payload data
  - Meta data
  - Verification data

Dr. Bernd Wild,
Member of the Board of
PDF Association

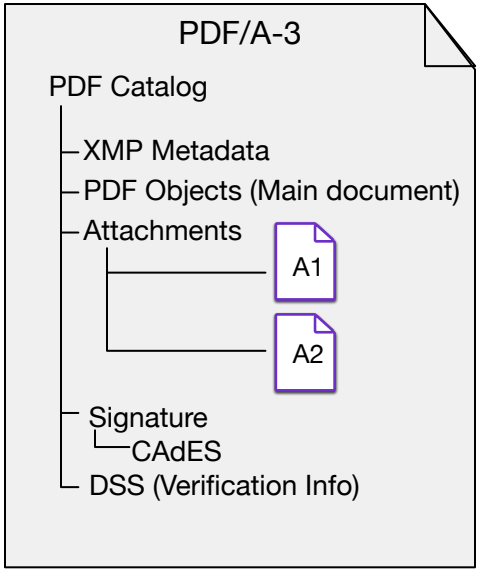
PDF/A-3 as Cryptographic Longterm Archive Container

- Possible archive container formats
  - XAIP
    - Base of TR-ESOR TR-03125
    - XML format
  - XFDU
    - ISO Standard ISO 13527:2010
    - XML format
  - ASiC
    - CEN Standard EN 319 162
    - ZIP format
  - PDF/A-3
    - ISO Standard ISO 19005-3
    - Signatures compliant with ETSI/EN standards

Dr. Bernd Wild,
Member of the Board of
PDF Association

PDF/A-3 as Cryptographic Longterm Archive Container

- PDF/A-3 as data package format for information and evidence preservation



Please refer to „Datenpakete zur Informations- und Beweiswerterhaltung – ein Vergleich", D·A·CH Security 2017,5.-6.9.2017, München

Dr. Bernd Wild,
Member of the Board of
PDF Association

Reasons for Cryptographic Longterm Archive Container

- Self-contained document format
  - Identical reproduction of the document possible (all necessary resources included)
- Storing of arbitrary meta data
- Storing of multiple documents / data files

- Integrity protection
  - Integrated Integrity protection
  - Container encompasses all necessary informations for verification

Signatures
Evidence Records

- Mechanism for securing cryptographic keys

Hash Trees
Timestamps

Dr. Bernd Wild,
Member of the Board of
PDF Association

Could PDF/A-3 do the job?

- Self-contained document format
  - Identical reproduction of the document possible (all necessary resources included)
  - YES (unique selling point)
- Storing of arbitrary meta data
  - YES, BUT actually only via XMP; awkward)
- Storing of multiple documents / data files
  - YES, BUT PDF/A-3 requires always a „primary document“, even when dummy
  - NO versioning on attachment level

Dr. Bernd Wild,
Member of the Board of
PDF Association

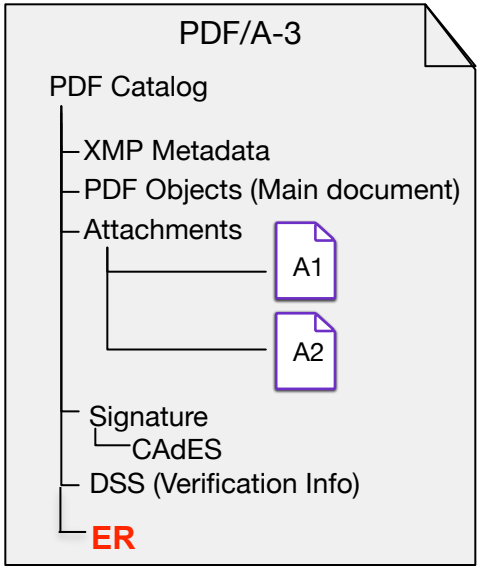
Could PDF/A-3 do the job?

- Integrity protection
  - Integrated Integrity protection
  - Container encompasses all necessary informations for verification
  - OK, BUT PAdES signatures are always embedded and related to the whole PDF/A-3 document
- Mechanism for securing cryptographic keys
  - PARTIAL, on a per (embedded) PDF document base via PAdES-LTA profile possible; not practicable for a big number of documents

Dr. Bernd Wild,
Member of the Board of
PDF Association

Requirements for a more suitable PDF/A-x

- Native support of Evidence Records (related to file attachments)
- Relationship between PDF(/A) and signature / meta data attachments
- Alternative to XMP for storing meta data
- In summary: a suitable PDF/A-3+ should be like ASiC plus PDF part



Dr. Bernd Wild,
Member of the Board of
PDF Association

Thank you! Any questions?

Dr. Bernd Wild,
Member of the Board of
PDF Association

Get in touch: bernd.wild@pdfa.org
Web site: www.pdfa.org
Twitter: PDFassocation