eIDAS Regulation in the context of Cybersecurity:

Electronic seals and website certificates: Two sides of a (gold) medal?
AGENDA

1. eIDAS Strategic View
2. Website Certificates
3. Electronic Seals
4. Identification of Legal Persons
5. Business Integration
6. Synthesis
eIDAS 2012: Pan European Trust Services

- eRegistered Delivery
- Timestamps
- eSeals
- Website-Auth
- eSignature
- crossborder eID
eIDAS: Pan European Trust Services

- eRegistered Delivery
- Timestamps
- eSeals
- Website-Auth
- eIDAS
- crossborder eID
- eSignature

11.11.2015
eIDAS: Pan European Trust Services in Force since 9/14

- eHealth
- eBanking
- eGovernment
- eBusiness
- eTender eContrating
NEW APPROACH FOR LEGAL FRAMEWORK: EU EIDAS- REGULATION

• EU regulation “on electronic identification and trust services for electronic transactions in the internal market”.

• Added Mutual recognition of electronic identification [E-ID]

• Extended Supervision of “Certification Service Providers” to “Trust Service Providers”, includes “proactive supervision”

• Qualified Electronic trust services:
  > Electronic signatures interoperability and usability,
  > **Electronic seals** interoperability and usability,
  > Time stamping,
  > Electronic delivery service,
  > Electronic documents admissibility,
  > Website authentication.
NEW APPROACH FOR LEGAL FRAMEWORK:
EU EIDAS- REGULATION

> website authentication certificates (aka Q WACs)
CA/B-FORUM: PHISHING IN 2006
Fig 3.1, IE7 address bar for a site with a high-assurance SSL certificate (showing the identity of the site from the SSL certificate)

Fig 3.2, IE7 address bar for a site with a high-assurance SSL certificate (altering in the name of the Certification Authority who identified the site)

- **Green URL** shows up for high assurance certs
- **Name of Organization** that cert is issued to
- **CA** that performed the “high assurance” authentication
• Website authentication services provide a means by which a visitor to a website can be assured that there is a genuine and legitimate entity standing behind the website. ..../......

• this Regulation should lay down minimal security and liability obligations for the providers and their services. To that end, the results of existing industry led initiatives, for example the Certification Authorities / Browsers Forum - CA/B Forum, have been taken into account.

• (38) 'certificate for website authentication' means an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued;

• (39) 'qualified certificate for website authentication' means a certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV;
TeleTruST - Bundesverband IT-Sicherheit e.V.

Sichere Verbindung

Firefox hat überprüft, dass Sie über eine sichere Verbindung mit der Seite verbunden sind. Diese wird betrieben von:

TeleTruST - Bundesverband IT-Sicherheit e.V.
Berlin
Berlin, DE

Verifiziert von: D-Trust GmbH

Veranstaltungen

1. TISP
2. TESS
3. Cyber Security Challenge
4. IT Security made in Germany

11.11.2015

ISSE 2015

17. ISSE-Konferenz: 10. - 11.11.2015 in Berlin

Die 17. "Information Security Solutions Europe Conference" (ISSE), ein Gemeinschaftsprojekt der eema (European Association for e-Identity and Security) und TeleTruST, findet am 10. und 11.11.2015 im Hotel Palace Berlin statt, um erneut internationale Experten aus Forschung und Wirtschaft zum fachlichen Austausch über aktuelle IT-Sicherheitsthemen, IT-Sicherheitsszenarien, Studienergebnisse und Verfahren zusammenzuführen.


TeleTruST verantwortet die Leitung des ISSE-Programmkomitees, stellt das Konferenzzprogramm zusammen und verleiht auf der Konferenz den "TeleTruST Innovation Award".


Schwerpunkte des Konferenzzprogramms:
TeleTruST - Bundesverband IT-Sicherheit e.V.

Sichere Verbindung

Firefox hat überprüft, dass Sie über eine sichere Verbindung mit der Seite verbunden sind. Diese wird betrieben von:

TeleTruST - Bundesverband IT-Sicherheit e.V.
Berlin
Berlin, DE

Verifiziert von: D-Trust GmbH

Weitere Informationen

Veranstaltungen

TISP
TESO
Cyber Security Challenge
IT Security made in Germany

17. ISSE-Konferenz: 10. - 11.11.2015 in Berlin

Die 17. "Information Security Solutions Europe Conference" (ISSE), ein Gemeinschaftsprojekt der eema (European Association for e-Identity and Security) und TeleTruST, findet am 10. und 11.11.2015 im Hotel Palace Berlin statt, um erneut internationale Experten aus Forschung und Wirtschaft zum fachlichen Austausch über aktuelle IT-Sicherheitsthemen, IT-Sicherheitsszenarien, Studienergebnisse und Verfahren zusammenzuführen.


Schwerpunkte des Konferenzprogramms:
Qualified WACS
without Rootstore Integration or TSL Acceptance

The site's security certificate is not trusted!

You attempted to reach 192.168.17.129, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications.

You should not proceed, especially if you have never seen this warning before for this site.

Proceed anyway  Back to safety

Help me understand
NEW APPROACH FOR LEGAL FRAMEWORK:
EU EIDAS- REGULATION

> electronic seals
DEFINITION/CLASSIFICATION

Article 3(25) of the eIDAS Regulation

"Electronic seal" means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity.

- Two (security) levels
  - "Advanced electronic seal"
  - "Qualified electronic seal"

Public authority seal and company stamp are being transported into the age of the Internet – reliable, legally binding, recognised throughout Europe.
DEFINITION/CLASSIFICATION

Article 36 of the eIDAS Regulation

"Advanced electronic seal" is an electronic seal that meets the following requirements:

- it is uniquely linked to the creator of the seal;
- it is capable of identifying the creator of the seal;
- it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and
- it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable.

"Qualified electronic seal"

- is an advanced electronic seal;
- which is created by a qualified electronic seal creation device; and
- that is based on a qualified certificate for electronic seals.
Aims of the electronic seal

Article 59 and 65; Section 5, Article 35 (1) of the eIDAS Regulation

- Evidence that an electronic document was issued by a legal person
- Confirmation of the origin and integrity of a document
- Legal effect and admissibility as evidence in legal proceedings
- Authentication of documents issued by legal persons
- Authentication of digital assets of legal persons (!)

- No signature as „willfull act“ replacement
- Electronic seal as proof of origin of a document
DEFINITION/CLASSIFICATION

Principles of operation

Trust service providers issue an electronic certificate that

- clearly identifies the relevant legal persons;
- contains the technical components for signing, authentication and encryption;
- can also contain certificate attributes, such as number in the Commercial Register or Chamber of Industry and Commerce, VAT ID No., employer number.
TARGET GROUPS

• Seal managing offices
  Municipal authorities (tax offices, registry offices, aliens' registration authorities, etc.), federal-state authorities, government authorities, police, courts, schools, universities, churches, chambers of industry and commerce, etc. for certification/deeds/certificates, etc.
  ➢ Electronic seal as an
    "official seal" on the Internet

• Private-sector businesses and organisations:
  Electronic seal as the counterpart to the company stamp/stationary in order to guarantee the authenticity of the sender and document (e.g. insurance companies, banks)
  ➢ Electronic seal as
    "ID for companies" on the Internet
Silent application....

- **Legal person**
  - (Seals)
  - Hash value
- **Authentication process**
- **Seals/Verification**
- **Result and handover**
OPTIONS FOR USE

- **For public authorities**
  - Electronic certification and deeds
  - Certificate for professional qualifications/certificates

- **For private companies**
  - Business tax returns
  - Electronic contract awarding
  - Issuing electronic bids
  - Signing electronic invoices

- **For private companies and public authorities**
  - Issuing electronic information and notices
  - E-mail security (signature and encryption)
  - Business to Government identification
  - Evidence for electronic archives/replacement scanning
APPLICATION EXAMPLES

Statutory health insurance companies

- Notices
- Information regarding services
- Information regarding applicable statutory conditions
- Information regarding increases/reductions in contributions
- Overview of contribution payments, and much more

- Are sent on paper as bulk letters
- Electronic seal guarantees the authenticity of the sender and document when this letter is sent in electronic form
- Allows legal persons to change from paper-based documents to electronic documents while maintaining legal effect
Electronic Seals versus Website Authentication.
EIDAS DEFINITION IN THE ANNEX

Qualified Website Certificates

(b) - for a legal person: the name and, where applicable, registration number as stated in the official records,
– for a natural person: the person's name;

(c) for natural persons: at least the name of the person to whom the certificate has been issued, or a pseudonym. If a pseudonym is used, it shall be clearly indicated;

for legal persons: at least the name of the legal person to whom the certificate is issued and, where applicable, registration number as stated in the official records;

(d) elements of the address, including at least city and State, of the natural or legal person to whom the certificate is issued and, where applicable, as stated in the official records;

(e) the domain name(s) operated by the natural or legal person to whom the certificate is issued;

Qualified Seal

(b)- for a legal person: the name and, where applicable, registration number as stated in the official records,
– for a natural person: the person's name;

(c) at least the name of the creator of the seal and, where applicable, registration number as stated in the official records;
Identification of a legal person
The semantics of id-etsi-qcs-SemanticsId-Legal shall be as follows. When the legal person semantics identifier is included, any present organizationIdentifier attribute in the subject field shall contain information using the following structure in the presented order:

- 3 character legal person identity type reference;
- hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and
- identifier (according to country and identity type reference).

The three initial characters shall have one of the following defined values:

1) "VAT" for identification based on a national value added tax identification number.
2) "NTR" for identification based on an identifier from a national trade register.
OVERVIEW OF LEGAL PERSONS IN GERMANY

a. Public bodies
b. Associations, foundations
c. Co-operatives
d. Corporations
e. Partnerships
f. Freelance professions

Other semantic identifiers for legal persons must be introduced at national and international level so that seals can be issued according to eIDAS.
Generally speaking, the fields of application for seals and web certificates are very different.

The identification requirements for a legal person are largely identical where seals and web certificates are concerned.

This means that a user only needs to be identified just once and can request and use both services via a trust service provider.
Enrico Entscheew  
E-mail: enrico.entscheew@bdr.de  
Telephone: +49 (0) 30-2598-3070

Arno Fiedler  
Dienstleister  
E-Mail: arno.fiedler@nimbus-berlin.com  
Telephone: +49-172-3053272

Please note: This presentation is the property of Bundesdruckerei GmbH. All of the information contained herein may not be copied, distributed or published, as a whole or in part without the approval of Bundesdruckerei GmbH. Copyright 2015 by Bundesdruckerei GmbH.