BUNDESDRUCKEREI

Vertrauensdienste gemäß eIDAS und PSD2

30.03.2017
BITKOM Roundtable Digitale Identitäten & Banking - smart, secure, usable, Frankfurt
Dr. Kim Nguyen
Fellow (Bundesdruckerei GmbH), Geschäftsführer (D-Trust GmbH)

BUNDESDRUCKEREI

Agenda:

- **eIDAS: Eine kurze Einführung**
- **eIDAS und PSD2: qualifizierte Vertrauensdienste und ihre Anwendung in Finanzdienstleistungen**

Kernpunkte der eIDAS-Verordnung (Regulation no 910 / 2014)

BUNDESDRUCKEREI

Ziel	▪ Schaffung eines **digitalen Binnenmarkts** der eID-Mittel und TSP in Europa ▪ **Gegenseitige Anerkennung** der notifizierten eID – Systeme ▪ Festlegung eines **Rechtsrahmens für betroffene Dienste** ▪ Schaffung einer **gemeinsamen Grundlage für sichere elektronische Interaktion** zwischen Unternehmen, Bürgern und öffentlichen Verwaltungen
Betroffene Dienste	▪ Notifizierte Systeme (eID) (Identifizierung/Authentisierung) und Vertrauensdienste (TSP) ▪ **Ausgenommen**: Geschlossene Nutzergruppen der Privatwirtschaft oder der Behörden, z.B. EGVP, Firmenkarten, Register
Status	▪ In Kraft getreten August 2014 - **Durchführungsrechtsakte als Verbindung von technischen Normen und Verordnung müssen noch geschaffen werden** ▪ Im Forum elektronische Vertrauensdienste AK A (TeleTrusT) und AG B (Bitkom) können aktuelle Vorschläge der Durchführungsakte kommentiert werden

Durch den gesetzgeberischen Charakter für die Mitgliedsstaaten müssen SigG/SigV angepasst werden

BUNDESDRUCKEREI

neue Produkte

Fortgeschrittene / qualifizierte Signaturen (auch fernausgelöst)

Fortgeschrittene / Qualifizierte Websitezertifikate

Fortgeschrittene/ qualifizierte Siegel

Vertrauens-dienste

Elektronische Einschreib-Zustelldienste

Fortgeschrittene / qualifizierte Zeitstempel

Elektronisches Dokument

Prüf – und Bewahrungsdienste

NEU: Das Siegel – die elektronische Unterschrift für die juristische Person

BUNDESDRUCKEREI

Definition

- Dienen als Nachweis, dass ein elektronisches Dokument von einer juristischen Person ausgestellt wurde und belegen die Unversehrtheit und den Ursprung des Dokuments

Ausprägungen

- Fortgeschrittenes Siegel
- Qualifiziertes Siegel
  (Unterschied: Sichere Siegelerstellungseinheit + qualifiziertem Zertifikat)

Technische Umsetzung

- Fernsiegelung analog zu der Fernsignierung

✗ Ersatz für persönliche Unterschrift

✓ Herkunftsnachweis

Rechts-wirkung

- eIDAS Art. 35 (2): Für ein qualifiziertes elektronisches Siegel gilt die Vermutung der Unversehrtheit der Daten und der Richtigkeit der Herkunftsangabe der Daten, mit denen das qualifizierte elektronische Siegel verbunden ist.

Behördensiegel und Unternehmensstempel werden ins Internetzeitalter überführt – rechtsverbindlich und europaweit anerkannt

BUNDESDRUCKEREI

Funktionsweise

Vertrauensdiensteanbieter stellt ein elektronisches Zertifikat aus, welches

- die entsprechende juristische Personen eindeutig identifiziert;
- die technischen Komponenten für Signatur, Authentisierung und Verschlüsselung beinhaltet;
- optional auch Zertifikatsattribute enthalten kann, z.B. HR- oder IHK Nummer, Umsatzsteueridentifikationsnummer, Arbeitgebernummer.

BUNDESDRUCKEREI

- **Siegelführende Stellen:**
  Kommunale Behörden (Finanzämter, Standesämter, Ausländerbehörden, …), Landesbehörden, Bundesbehörden, Polizei, Gerichte, Schulen, Hochschulen, Kirchen, IHKs**,** usw.
  für Beglaubigungen / Urkunden / Zeugnisse usw.
  - ➢ Elektronisches Siegel als

    „Amtliches Siegel" im Internet

- **Private Wirtschaftsunternehmen und Organisationen:**
  Elektronisches Siegel als Pendant zum Firmenstempel / Briefpapier, um Absender- und Dokumentenechtheit zu garantieren. (z.B. Versicherungen, Banken)
  - ➢ Elektronisches Siegel als

    „Personalausweis für Unternehmen" im Internet

BUNDESDRUCKEREI

- **Klassischer Ansatz mit Siegelkarte:**

Das Siegelzertifikat befindet sich auf einer sicheren Siegelerstellungseinheit im Besitz der Siegelführenden Person (autorisierte Mitarbeiter der juristischen Person).

- **Fernausgelöster Siegel als Service**

Das Elektronisches Siegel (Siegelschlüsselpaar) befindet sich auf einem Hard Security Module des Vertrauensdiensteanbieters (VDA). Vertreter der juristischen Person authentifiziert sich gegenüber dem Service des VDA und autorisiert den Siegelprozess.

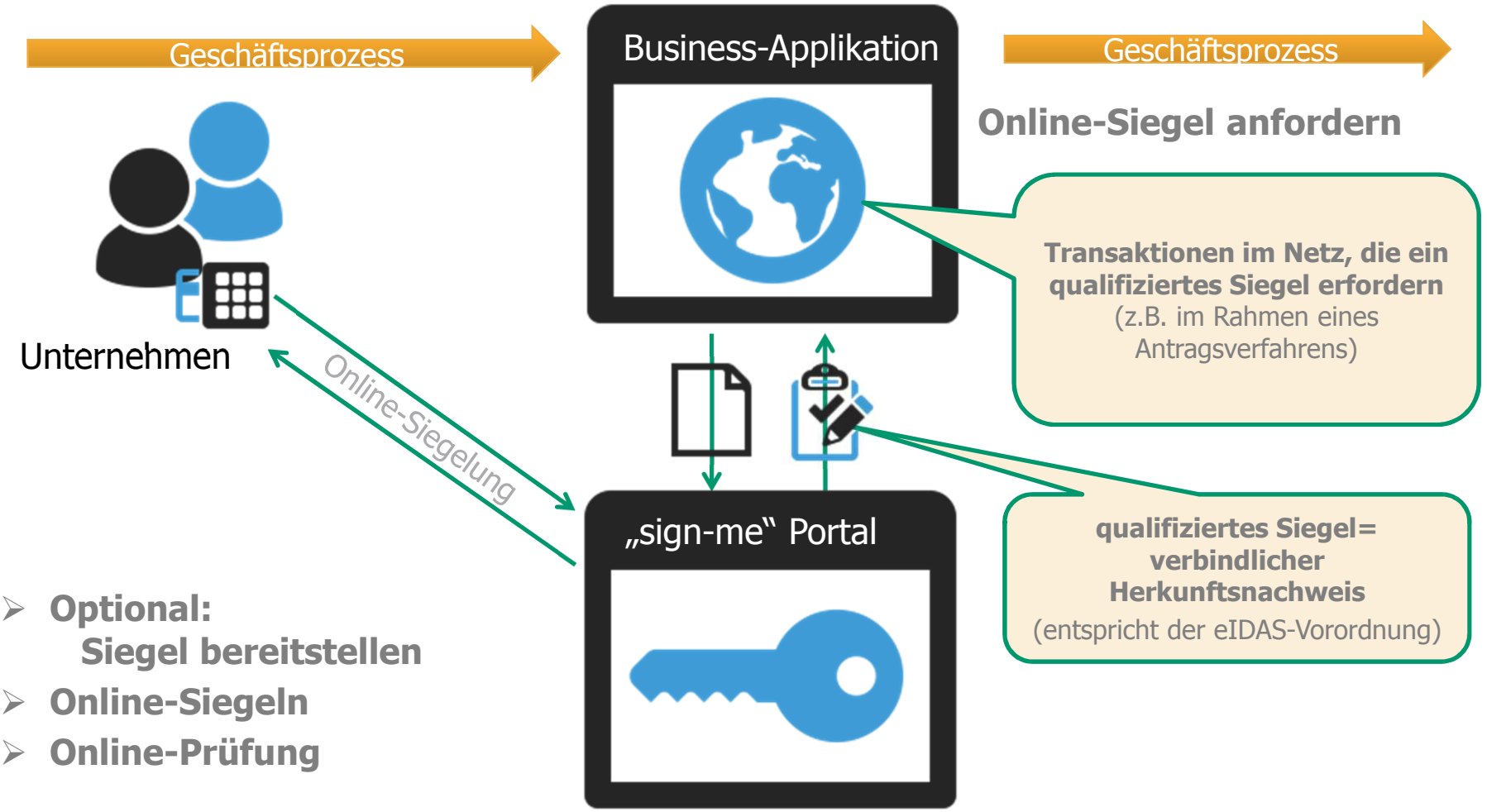
USPs einer Siegelkarte

- Physisches Element
- Liegt in Hoheit der Siegelführenden Person
- Für manuelle Prozesse bestens geeignet
- Kontrollierte Übergabe an den Stellvertreter möglich
- Kann in der gewohnten Weise eines Siegels benutzt werden
- Kann sicher weggeschlossen werden
- Vermeidung der Neu-Authentisierung der Siegelführenden Personen (z.B. bei Wechsel der mobilen Devices)

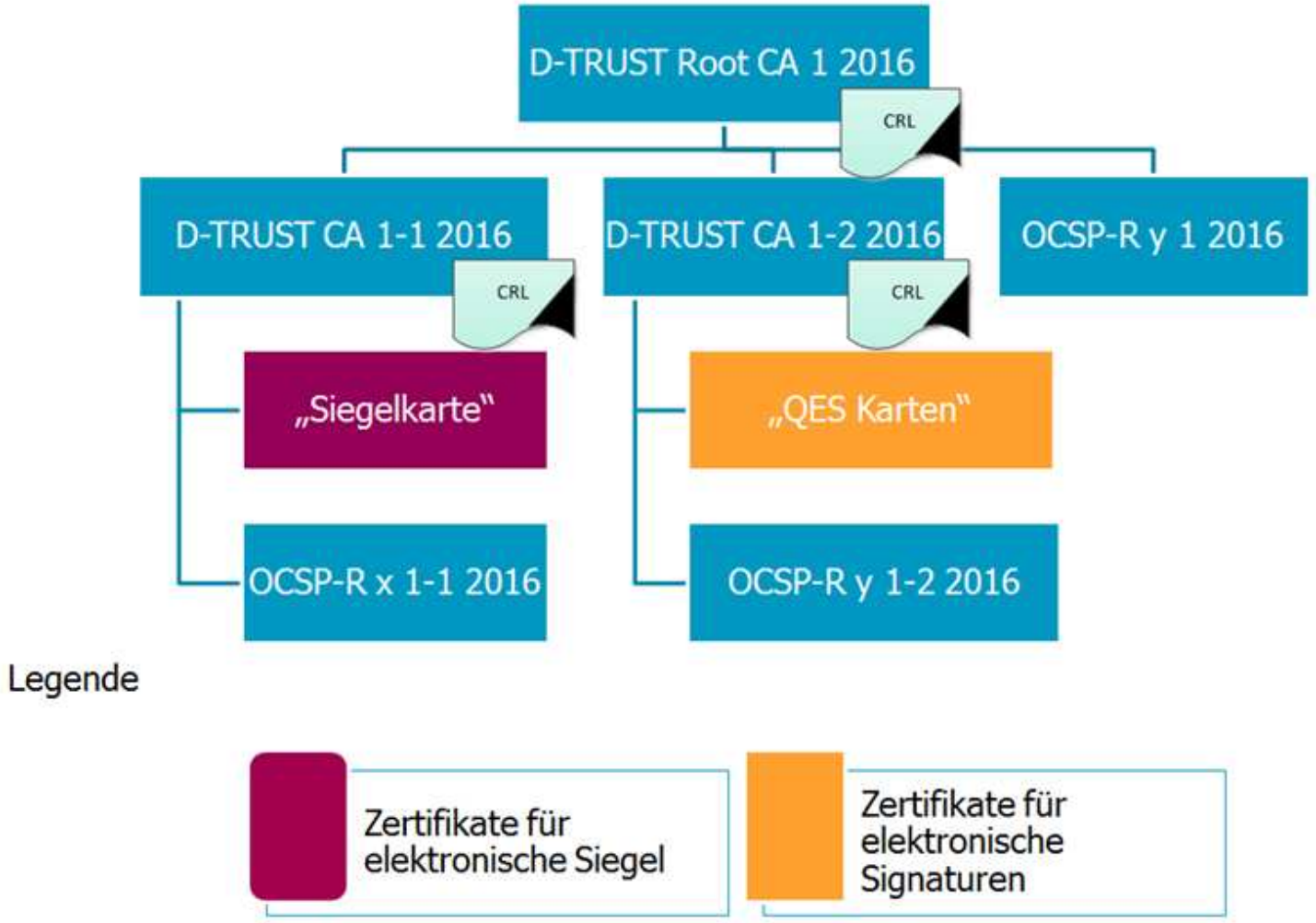
➢ Verfügbar ab Q1/2017

BUNDESDRUCKEREI

Business-Integration



- **Optional: Siegel bereitstellen**
- **Online-Siegeln**
- **Online-Prüfung**


D-TRUST Root CA 1 2016
CRL
D-TRUST CA 1-1 2016
CRL
D-TRUST CA 1-2 2016
CRL
OCSP-R y 1 2016
„Siegelkarte"
„QES Karten"
OCSP-R x 1-1 2016
OCSP-R y 1-2 2016
Legende
Zertifikate für elektronische Siegel
Zertifikate für elektronische Signaturen

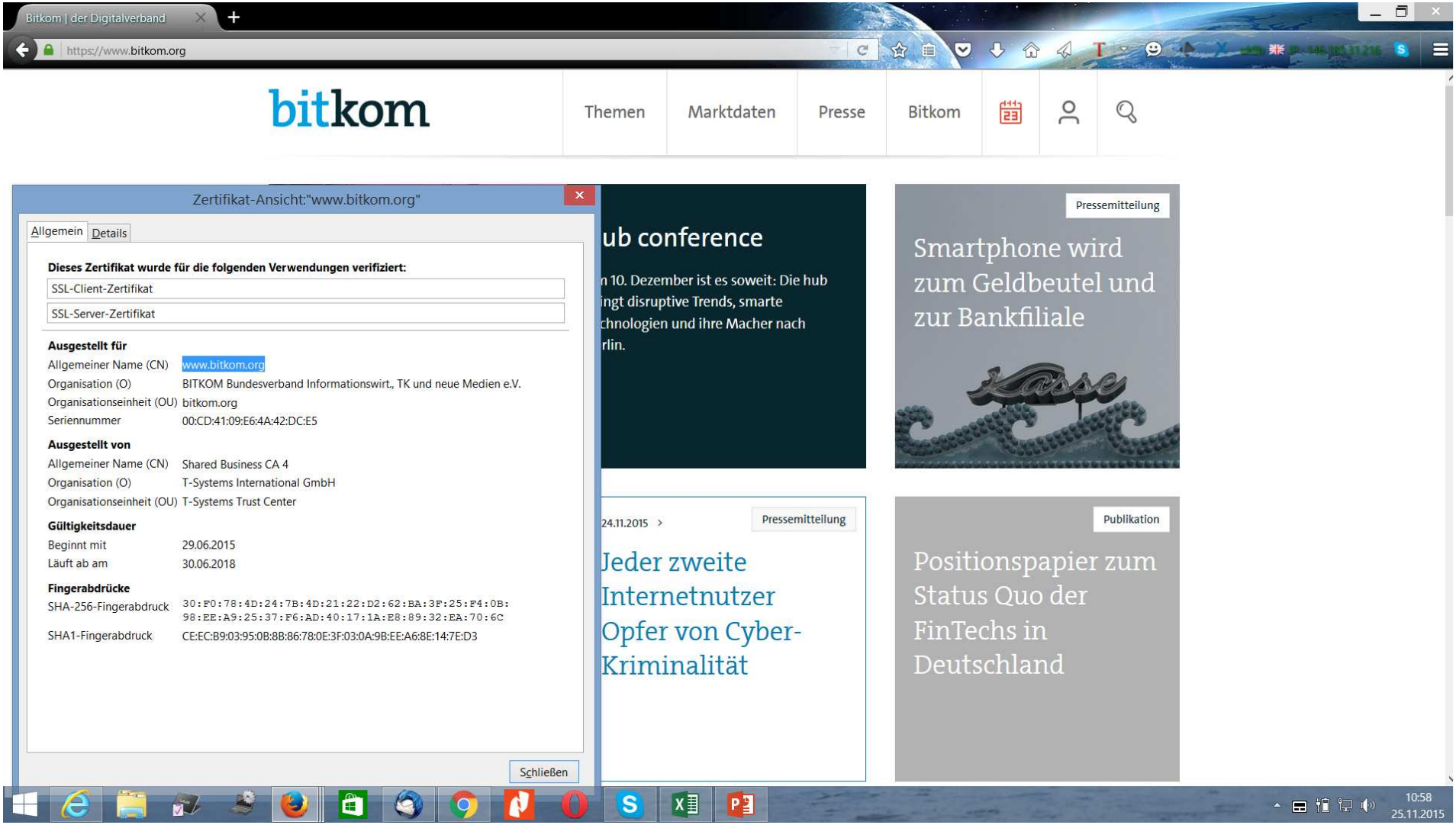
NEU: Das qualifizierte Website-Zertifikat

BUNDESDRUCKEREI

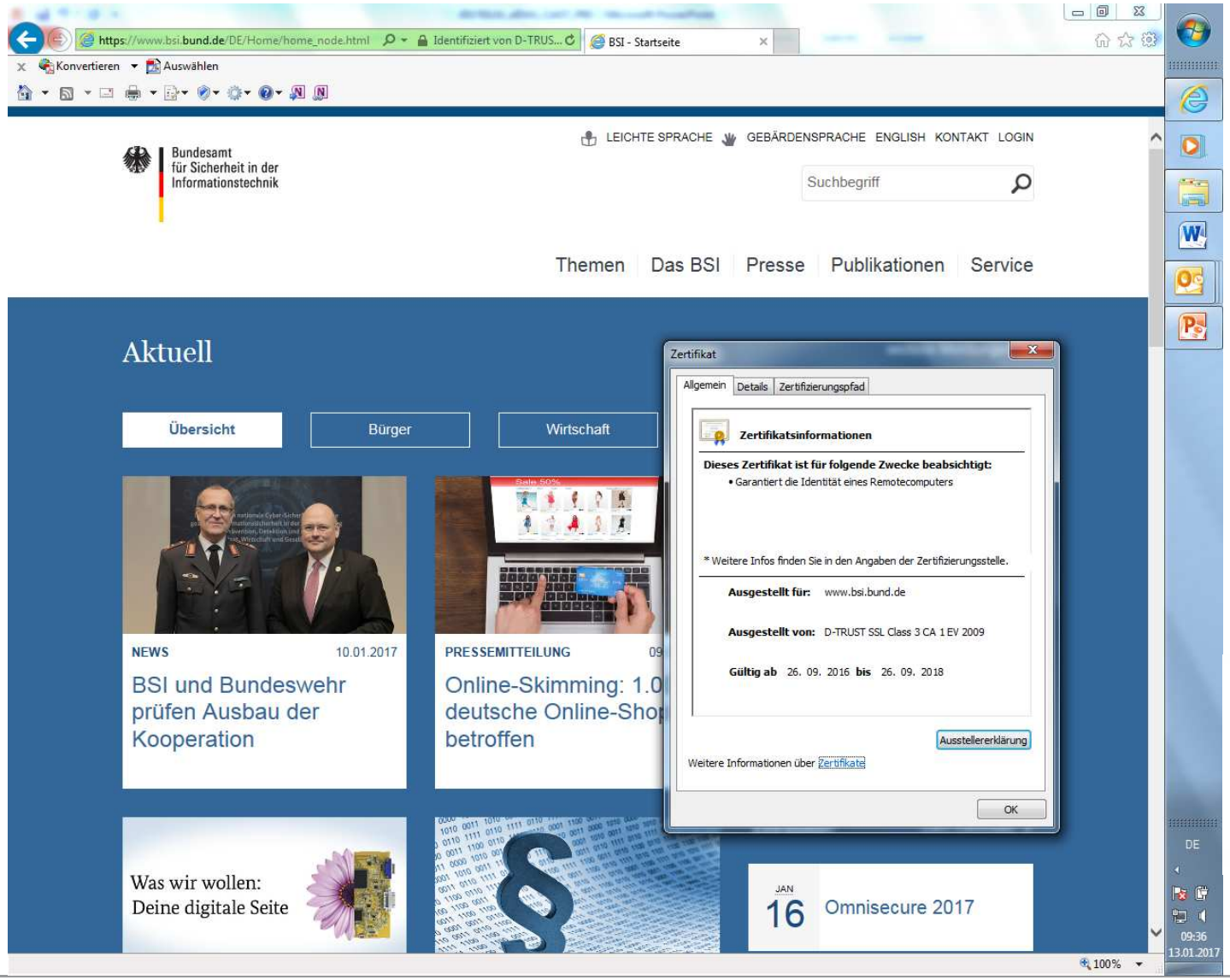
Definition	▪ Ermöglicht die Authentifizierung einer Website und verknüpft die Website mit der natürlichen oder juristischen Person, der das Zertifikat ausgestellt wurde.
Ausprägungen	▪ Qualifiziertes „SSL/ TLS"-Zertifikat, welches den Besitz der angegebenen Domain garantiert
Technische Umsetzung	▪ Funktionsweise analog zum klassischen SSL/ TLS-Zertifikat ▪ Vertrauensstellung wird durch europäischer Vertrauensliste (Trusted Services List) erbracht

Der Vertrauensstatus eines qualifizierten Website-Zertifikats ist unabhängig vom Rootstore der Betriebssysteme und Browser.

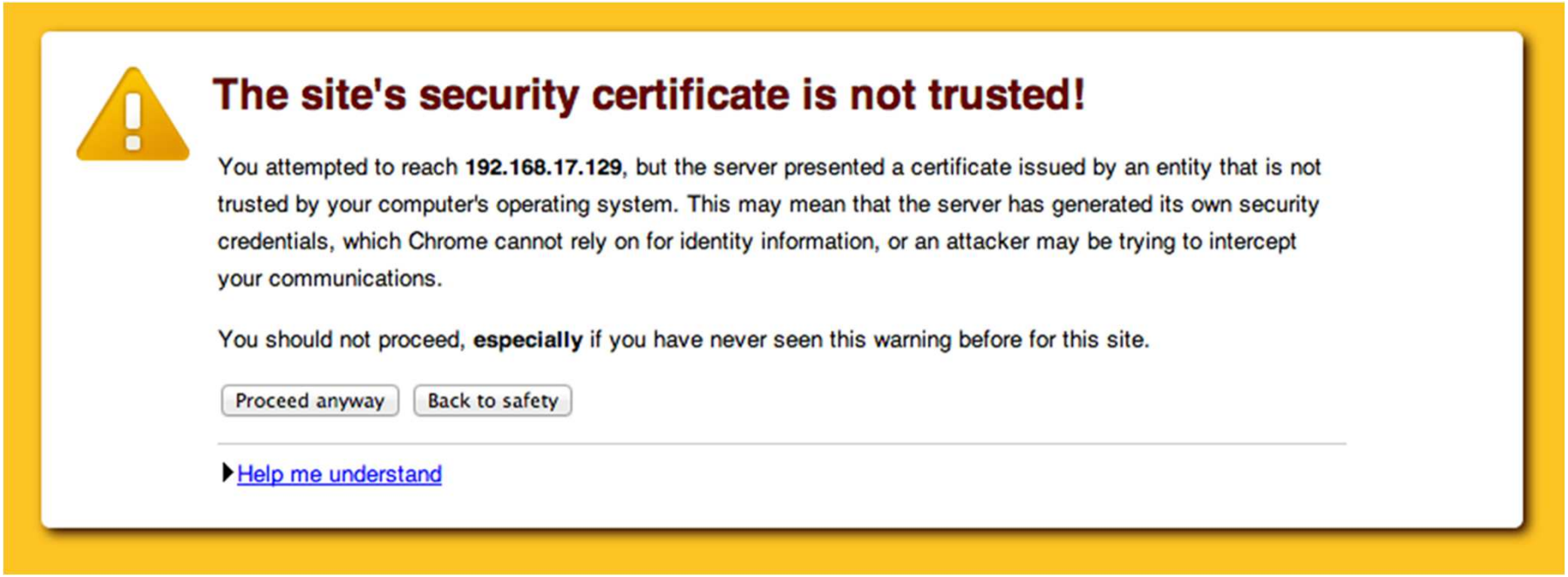
NEU: Das qualifizierte Website-Zertifikat



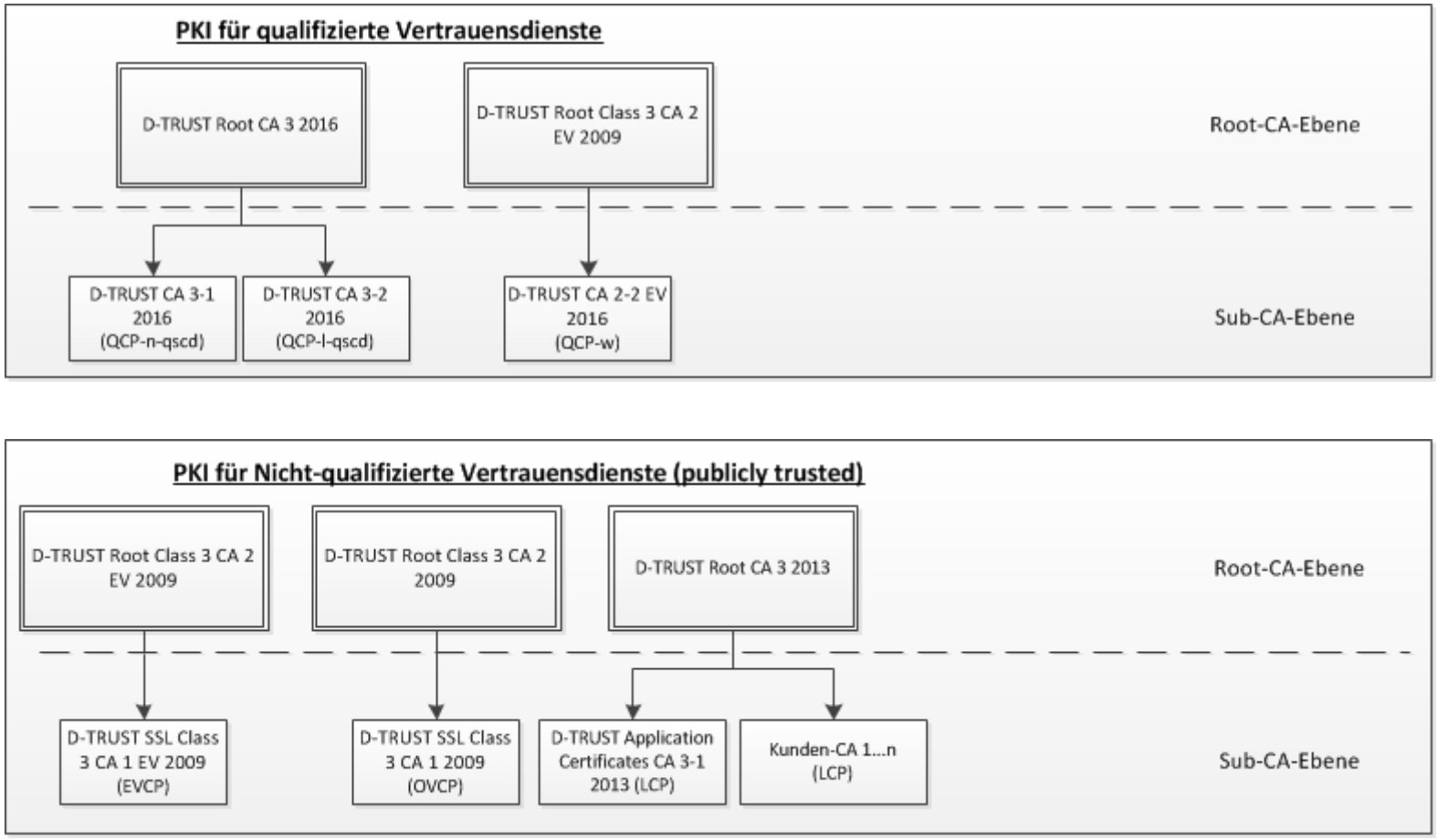
NEU: Das qualifizierte Website-Zertifikat



BUNDESDRUCKEREI



Qualifizierte/publicly trusted PKIn



Zertifikat

Die Zertifizierungsstelle der TÜV Informationstechnik GmbH bescheinigt hiermit dem Unternehmen

D-TRUST GmbH
Kommandantenstraße 15
10969 Berlin

für den Vertrauensdienst

D-TRUST qualified Seal ID card

die Erfüllung aller relevanten Anforderungen der

Verordnung (EU) Nr. 910/2014 (eIDAS) für die Erstellung von qualifizierten Zertifikaten für elektronische Siegel.

Die Anlage zum Zertifikat ist Bestandteil des Zertifikats und besteht aus 3 Seiten.

Dieses Zertifikat gilt nur in Verbindung mit dem Konformitäts-bewertungsbericht.

eIDAS TÜVIT 2017 Trusted Site

Zertifikat gültig bis 30.01.2019

Certificate ID: 9728.17

© TÜVIT - TÜV NORD GROUP - www.tuvit.de

Essen, 30.01.2017

Dr. Christoph Sutter
Leiter Zertifizierungsstelle

TÜV Informationstechnik GmbH
TÜV NORD GROUP
Langemarckstraße 20
45141 Essen
www.tuvit.de

DAkkS Deutsche Akkreditierungsstelle D-ZE-12033-01-00

Bundesamt für Sicherheit in der Informationstechnik

Urkunde

über die Verleihung des Qualifikationsstatus als Vertrauensdiensteanbieter gemäß eIDAS-Verordnung

BSI-eIDAS-0001-2017

Vertrauensdiensteanbieter
D-Trust GmbH

Vertrauensdienst
D-Trust qualified EV SSL ID

Bereich
Erstellung, Überprüfung und Validierung von Zertifikaten für die Website Authentifizierung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) verleiht hiermit dem Vertrauensdiensteanbieter D-Trust GmbH für den im Bereich der Erstellung, Überprüfung und Validierung von Zertifikaten für die Website-Authentifizierung erbrachten Vertrauensdienst D-Trust qualified EV SSL ID den Qualifikationsstatus gemäß Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 (eIDAS-Verordnung).

Der Vertrauensdiensteanbieter sowie der erbrachte Vertrauensdienst erfüllen die Anforderungen an qualifizierte Vertrauensdiensteanbieter, bzw. qualifizierte Vertrauensdienste für Website-Authentifizierung gemäß eIDAS-Verordnung.

Diese Urkunde gilt nur in Verbindung mit dem Bescheid BSI-eIDAS-0001-2017.

Diese Urkunde ist keine Empfehlung des genannten Vertrauensdiensteanbieters/-dienstes durch das BSI.

Bonn, den ##. März 2017
Bundesamt für Sicherheit in der Informationstechnik
Im Auftrag

Bernd Kowalski
Abteilungspräsident

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189, D-53175 Bonn • Postfach 20 03 63, D-53133 Bonn
Tel.: +49 (0)228 9582-0 • Fax: +49 (0)228 9582-5400 • Internet: www.bsi.bund.de

BUNDESDRUCKEREI

Agenda:

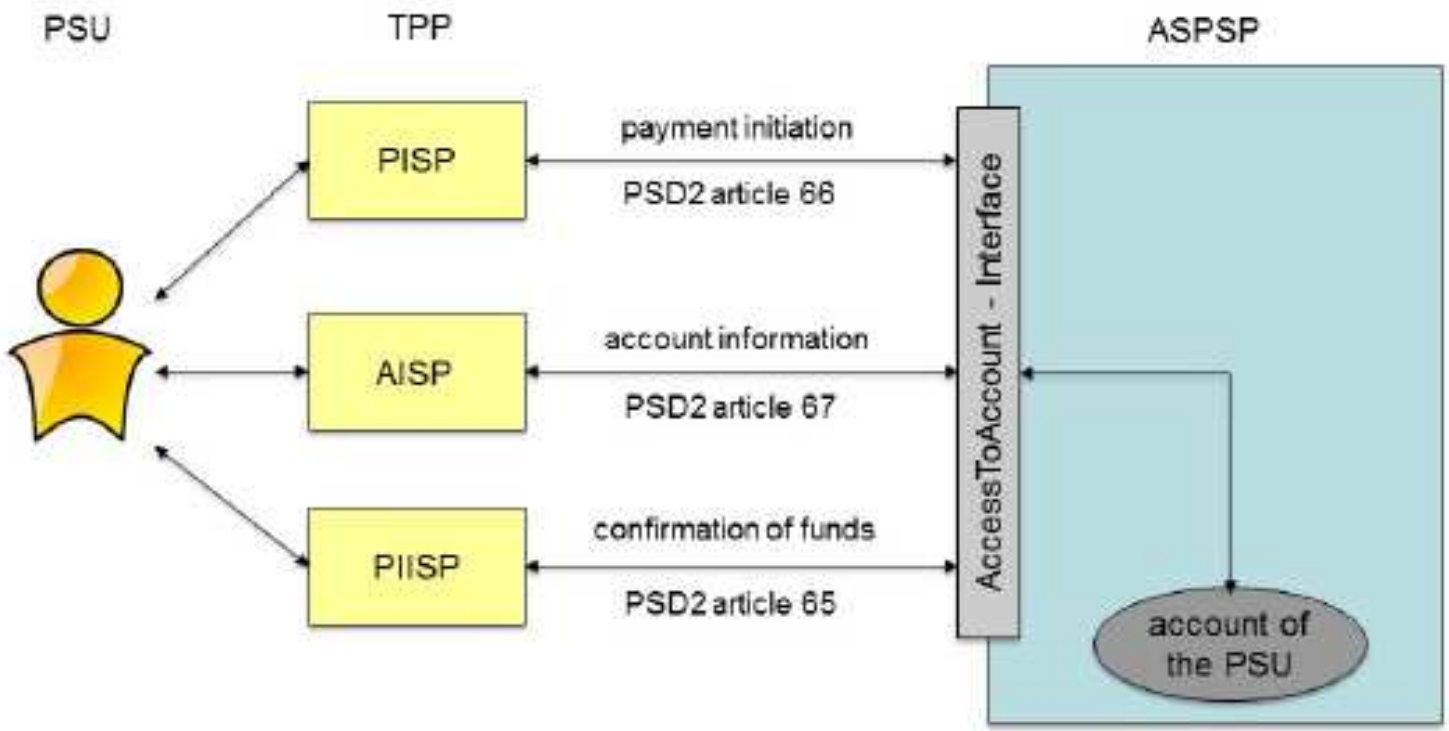
- **eIDAS: Eine kurze Einführung**
- **eIDAS und PSD2: qualifizierte Vertrauensdienste und ihre Anwendung in Finanzdienstleistungen**

Gemäß PSD2 dürfen dritte Zahlungsdienstleister (TPP) für neu regulierte Dienstleistungen auf Konten bei einem kontoführenden Institut zugreifen

- Bestätigung der Verfügbarkeit eines Geldbetrags (Artikel 65)
- Zahlungsauslösedienste (Artikel 66)
- Kontoinformationsdienste (Artikel 67)

Das Kontoführende Institut muss den TPP eine Schnittstelle zur Verfügung stellen, damit diese die benötigten Kontozugriffe ausführen können

- Nur online-fähige Zahlungskonten sind hiervon betroffen


PSU
TPP
ASPSP
PISP
AISP
PIISP
payment initiation
PSD2 article 66
account information
PSD2 article 67
confirmation of funds
PSD2 article 65
AccessToAccount - Interface
account of the PSU

BSI, 2017

Zwei Arten von Zertifikaten werden explizit erwähnt:

- Qualifizierte Webseitenzertifikate nach eIDAS
- Qualifizierte Siegel nach eIDAS

Qualifizierte Webseitenzertifikate können zur Absicherung des „Verkehrswegs" mittels Verschlüsselung und zur Identifikation der Partner mittels Authentisierung genutzt werden

Qualifizierte Siegel können zur Prüfung der Authentizität einer Anfrage durch eine juristische Person (in diesem Falle TPP) genutzt werden.

TPP muss sich bei seinen Zugriffen gegenüber dem kontoführenden Institut identifizieren

- Identifizierung muss grenzüberschreitend funktionieren

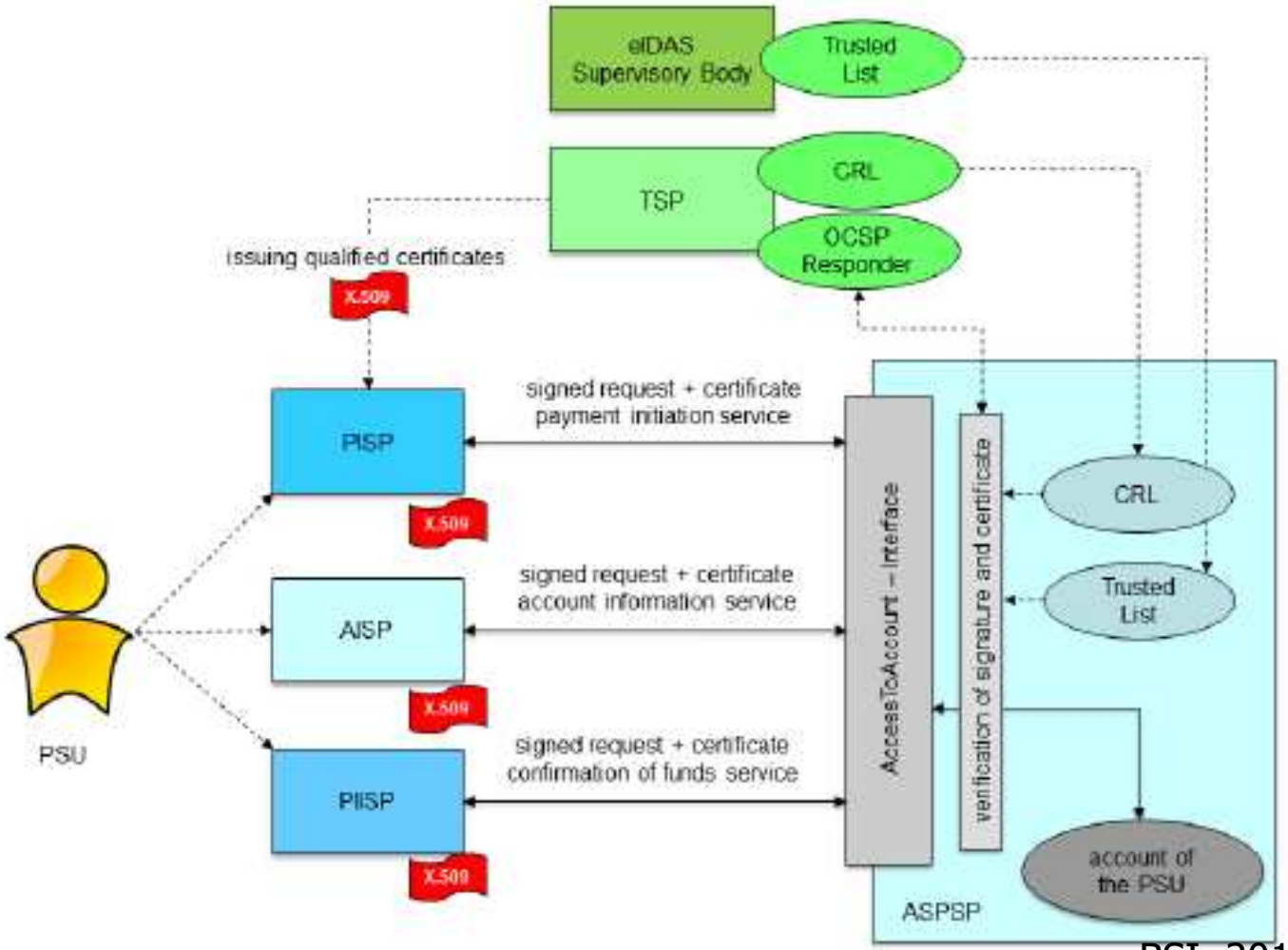
Diese Identifizierung muss ein genügendes Vertrauensniveau erfüllen.

Warum?

- Bei nicht autorisierten Zahlungen entsteht ein Anspruch der PSU gegenüber dem kontoführenden Institut (Artikel 73)
- Bei über PISP ausgelösten Zahlungen entsteht hieraus ein Anspruch des kontoführenden Instituts gegenüber dem PISP (Artikel 73 2.)
- Dieser Anspruch kann nur durchgesetzt werden, falls die Identifizierung des PISP entsprechend eindeutig und sicher ist

EBA RTS, Artikel 20 fordert folgerichtig, dass die Identifizierung der TPP auf der Nutzung qualifizierter Zertifikate gemäß der eIDAS Verordnung basieren muss

- Der Begriff der Identifizierung eines TPP wird im Sinne einer Authentifizierung des TPP verwendet
- Vertrauen in die Identifizierung nur über Zertifikate und PKI
- Benötigtes Vertrauensniveau der Identifizierung hierdurch sichergestellt
- Ausgabe der Zertifikate durch Vertrauensdiensteanbieter mit Status qualifiziert
- Vertrauensdiensteanbieter erfüllt benötigtes Sicherheitsniveau
- Zulassung und Aufsicht der Vertrauensdiensteanbieter über eIDAS-Verordnung sichergestellt
- Verteilte Root über Trusted Lists der Aufsichtsbehörden
- Grenzüberschreitende Anerkennung der Zertifikate sichergestellt


eIDAS
Supervisory Body
Trusted
List
TSP
CRL
OCSP
Responder
issuing qualified certificates
X.509
PISP
signed request + certificate
payment initiation service
X.509
AISP
signed request + certificate
account information service
X.509
PIISP
signed request + certificate
confirmation of funds service
X.509
PSU
AccessToAccount – Interface
verification of signature and certificate
CRL
Trusted
List
account of
the PSU
ASPSP

BSI, 2017

Welche Anforderungen entstehen aus der PSD2 an die zertifikatsbasierte Identifizierung der TPP?

- Durch Verifizieren des Siegels einer eingehenden Nachricht und des Zertifikats und der Authentizität der Transportverbindung müssen die folgenden Punkte sichergestellt sein:
- Der Absender (TPP) verfügt über eine entsprechende Zulassung durch die nationale Aufsichtsbehörde
- Diese Zulassung wurde nicht entzogen
- Durch den Inhalt des Zertifikats muss der TPP (europaweit) eindeutig identifiziert werden
- Durch den Inhalt des Zertifikats muss erkennbar sein, welche Zugriffsrechte der TPP hat, d.h. in welcher Rolle er den Zugriff durchführt

EBA RTS, Artikel 20 regelt die Identifizierung des TPP anhand des Zertifikatsinhalts:

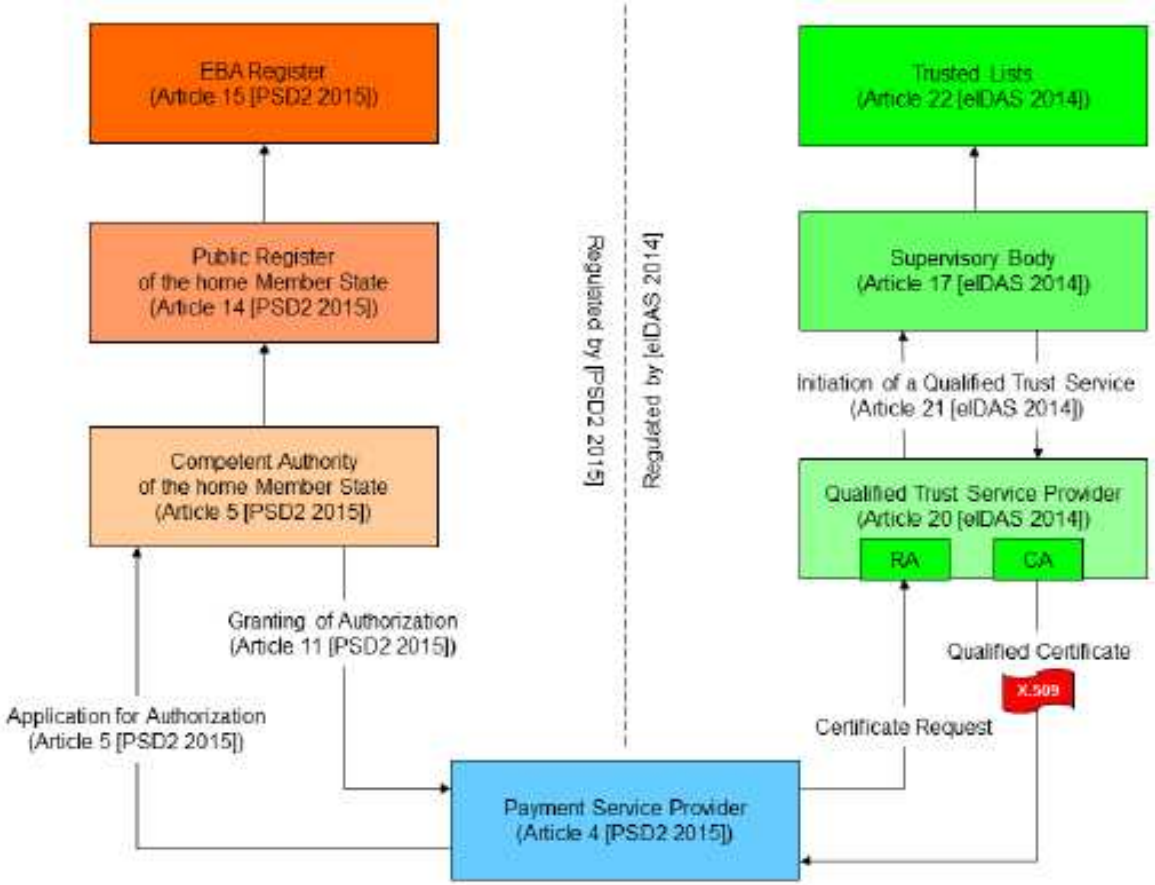
- Zertifikat muss Name der nationalen Aufsichtsbehörde enthalten
- Zertifikat muss Registrierungsnummer des TPP enthalten, die bei

der Zulassung des TPP vergeben wird

- Über diese beiden Werte ist die eindeutige Identifizierung des TPP sichergestellt
- EBA RTS, Artikel 20 regelt ebenfalls, dass die Rolle des TPP in dem Zertifikat enthalten sein muss (z.B. durch OID basierte Kodierung)

Vertrauensdiensteanbieter kann beim Ausstellen der Zertifikate nicht alleine sicherstellen, dass die PSD2-spezifischen Anforderungen erfüllt sind

- Hierfür werden Informationen der nationalen Aufsichtsbehörde über die Zulassung der TPP benötigt
- Diese Information muss in einer vertrauenswürdigen Art zur Verfügung stehen
- Diese Information muss korrekt und vollständig zur Verfügung stehen
- Bei Änderungen müssen diese zeitnah zur Verfügung stehen
- Nur bei geeigneter Zusammenarbeit können die Zertifikate und damit die Identifizierung der TPP das notwendige Vertrauensniveau erreichen


EBA Register
(Article 15 [PSD2 2015])
Public Register
of the home Member State
(Article 14 [PSD2 2015])
Competent Authority
of the home Member State
(Article 5 [PSD2 2015])
Granting of Authorization
(Article 11 [PSD2 2015])
Application for Authorization
(Article 5 [PSD2 2015])
Payment Service Provider
(Article 4 [PSD2 2015])
Regulated by [PSD2 2015]
Regulated by [eIDAS 2014]
Trusted Lists
(Article 22 [eIDAS 2014])
Supervisory Body
(Article 17 [eIDAS 2014])
Initiation of a Qualified Trust Service
(Article 21 [eIDAS 2014])
Qualified Trust Service Provider
(Article 20 [eIDAS 2014])
RA
CA
Qualified Certificate
X.509
Certificate Request

BSI, 2017

BUNDESDRUCKEREI

Fazit:

- **Die eIDAS Verordnung schafft einen EU weiten interoperablen Rahmen zur Nutzung von digitalen Identitäten**
- **Die Produkte qualifiziertes Webseitenzertifikat und Siegel können ideal zur Umsetzung der Anforderungen der PSD2 eingesetzt werden.**
- **Die spezifischen Anforderungen der PSD2 lassen über PKI (markt)übliche Mechanismen und Prozesse abbilden.**
- **Qualifizierte Produkte sind bereits jetzt am Markt verfügbar.**

BUNDES DRUCKEREI

Vielen Dank für Ihre Aufmerksamkeit!

Dr. Kim Nguyen
E-Mail: kim.nguyen@bdr.de
Telefon: +49-30-2598 1194