Mit freundlicher Unterstützung:

Informationstag "Elektronische Signatur und Vertrauensdienste"

Gemeinsame Veranstaltung von TeleTrusT und VOI

Berlin, 18.09.2018

Herzlich willkommen!

Christian Seegebarth, Bundesdruckerei GmbH

Motivation The EU Single Market Strategy

- Single Market of Goods
- Single Market for Services
- Stronger European Networks
- ....

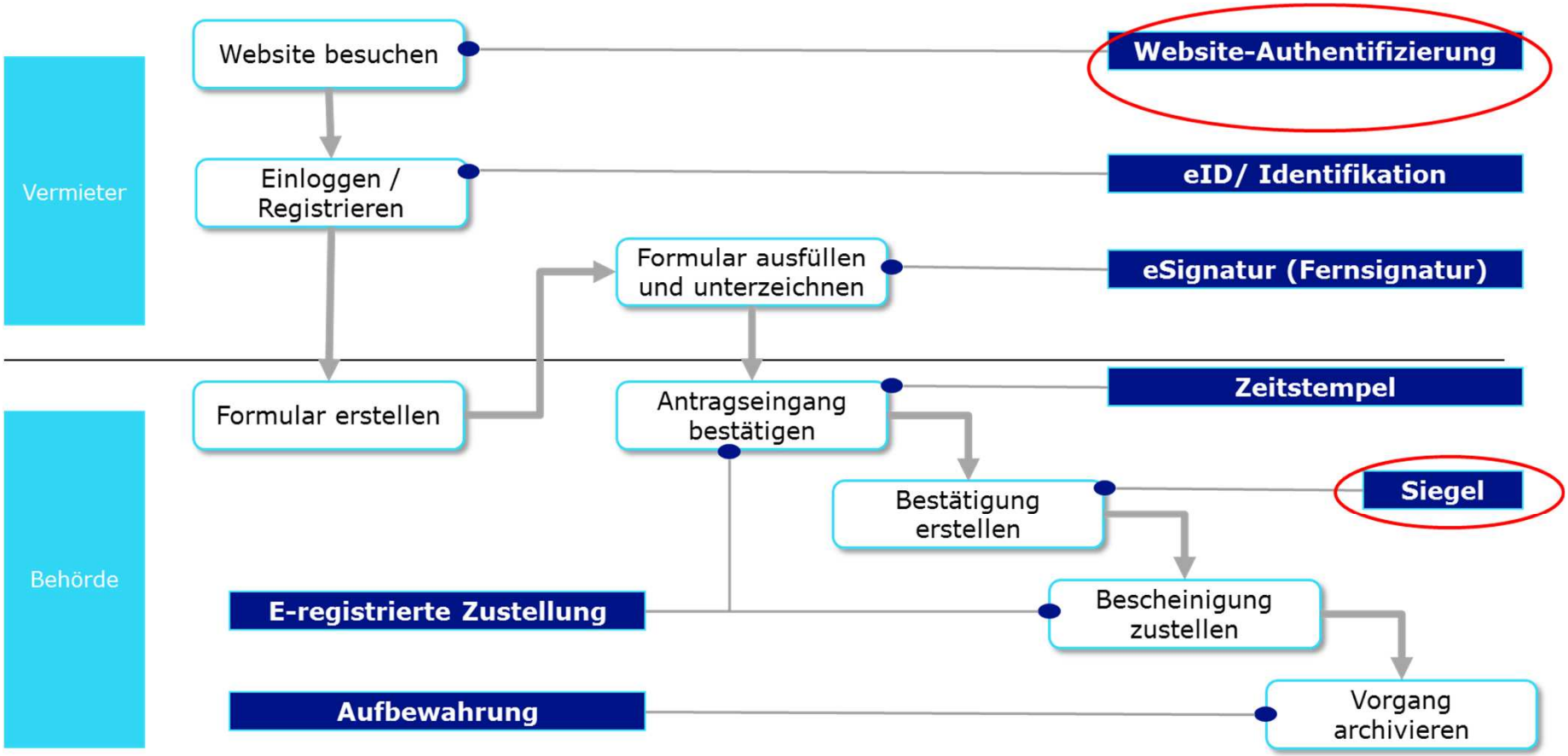
SEPA
Single Euro Payments Area

eIDAS-Verordnung (Regulation no 910 / 2014)

Ziel	▪ Schaffung eines **digitalen Binnenmarkts** der eID-Mittel und VDAs in Europa ▪ Festlegung eines **Rechtsrahmens für betroffene Dienste** ▪ **Gegenseitige Anerkennung** der notifizierten eID–Systeme ▪ 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
eIDAS-Mittel in Arbeit	▪ PSD2 - Second Payment Service Directive -> RTS (QWACs, Siegel, SCA) ▪ AML 4 - Fourth Anti Money Laundering Directive Kundenidentifikation (Customer Due Diligence (CDD) - Glücksspiel) ▪ PAD - Payment Account Directive ▪ EU Better Regulation Toolbox: TOOL #23 ICT Assessment, The Digital Economy and Society

29. Juli 2017 Vertrauensdienstegesetz ist in Kraft getreten und löst SigG ab

Typischer E-Transaktions-Workflow – Beispiel Bundesmeldegesetz



Das Siegel – die elektronische Unterschrift für die juristische Person

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

Anwendung

- eIDAS Art. 35 (2): Vermutung der Unversehrtheit der Daten und der Richtigkeit der Herkunftsangabe der Daten
- eIDAS Durchführungsgesetz (Abschnitt Vergabe)
- RTS on SCA der PSD2 ab Q3 2019 (Zahlungsdiensterichtlinie 2)
  TR-RESISCAN

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

Das qualifizierte Website-Zertifikat für juristische und natürliche Personen (QWAC)

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 (QWAC - qualified website Authetication certificate)
- Eine Zertifizierung nach der BSI TR-03145 erfüllt die technischen und organisatorischen Sicherheitsanforderungen der eIDAS-Verordnung für qualifizierte Webseitenzertifikate

Technische Umsetzung

- Funktionsweise analog zum klassischen SSL/ TLS-Zertifikat
- Vertrauensstellung wird durch europäischer Vertrauensliste (Trusted Services List) erbracht

Anwendung

- RTS der PSD2 ab Q3 2019

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

Ausblick - In Zukunft wird die Bankenwelt zur API Economy

heise online > News > 2014 > KW 25 > Urteil zu Screen Scraping: BGH legt schriftliche Urteilsbegründung vor

Urteil zu Screen Scraping: BGH legt schriftliche Urteilsbegründung vor

21.06.2014 15:23 Uhr – Tobias Haar vorlesen

Der Bundesgerichtshof (BGH) hat mit Urteil vom 30. April 2014 entschieden, dass das sogenannte Screen Scraping (das maschinengesteuerte Auslesen von Webseiten) nicht per se gegen das Wettbewerbsrecht verstößt.

Der Bundesgerichtshof (BGH) hatte eine Klage gegen Screen Scraping im April in zentralen Fragen abgewiesen. Nun liegt auch die schriftliche Urteilsbegründung vor. Gegen das maschinengesteuerte Auslesen seiner Webseiten (Screen Scraping) geklagt hatte RYANAIR. Der Anbieter verkauft preisgünstige Linienflüge ausschließlich über seine Webseite und ein

Ziele

- Harmonisierung des europäischen Zahlungsverkehrsmarkt
- Neue Zahlungsdienste
- Grenzüberschreitender Zahlungsverkehr
- API Economy
- Starke Kundenauthentifizierung
- Datenschutz
- Preiswertere Zahlungsdienste

PSD2 = API - Screen Scraping + SCA

- FinTechs sollen neue Zahlungsdienste entwickeln, benötigen dafür eine Lizenz, die durch die BaFIN oder dergl. vergeben wird (eindeutig in Europa)
- Zahlungsdienstleister (Banken) müssen die Kontodaten etc. je nach Anwendungsfall über eine kontrollierte Schnittstelle zur Verfügung stellen

PSD 2 - qualifizierte Zertifikate

- EBA: RTS on PSD2 Artikel 34 (1) und 34 (3) schreiben qualifizierte eIDAS-Mittel zur Identifikation des TPP vor und fordert auch entsprechende auswertbare Attribute

  For the purpose of identification, as referred to in Article 30(1)(a), payment service providers shall rely on qualified certificates for **electronic seals** as referred to in Article 3 (30) of Regulation (EU) No 910/2014 or for **website authentication** as referred to in Article 3 (39) of that Regulation.

- (3) For the purposes of this Regulation, **qualified certificates for electronic seals** or for **website authentication** referred to in paragraph 1 shall include, in a language customary in the sphere of international finance, additional specific attributes in relation to each of the following:
  - (a) the role of the payment service provider, which maybe one or more of the following: (i) a**ccount servicing**; (ii) **payment initiation**; (iii) **account information**; (iv) **issuing of card-based payment instruments**;
  - (b) the name of the **competent authorities** where the payment service provider is registered.

- Diese Daten erfordern ein nationales, zentrales Register, welches bei der BaFin aufgebaut werden muss Artikel 14, PSD2, da sie im Antragsprozess mit verarbeitet werden sollen. Der Zahlungsdienstleister muss prüfen, ob es sich um einen registrierten und damit autorisierten TPP handelt.
  - Bei nicht autorisiertem Zahlungen entsteht ein Anspruch des Nutzers gegenüber des Zahlungsdienstleisters (Artikel 73)
  - Bei durch den TPP ausgelösten Zahlungen entsteht ein Anspruch des kontoführenden Institutes gegenüber den TPP
- **Das führt zur notwendigen sicheren Identifikation der zugreifenden TPP**

Ausschnitt der PSD 2 Stakeholder und ihre Rollen

- EBA beauftragt durch die Kommission (PSD2)
  - ein europäisches Register aufzubauen (ITS)
  - Schnittstellen zwischen TTP und Bank zu definieren (RTS)
- Nationale Aufsichtsbehörden (NCA oder FSA Artikel 14, PSD 2) sind beauftragt ein nationales Zulassungsregister zu betreiben
  - BaFin in Deutschland
  - Finacial Conducrt Authority (UK)
  - Banco de Espangna (ES) und 29 weitere siehe Bild
- European Retail Payment Board – EZB Arbeitsgruppe
  - 3 Unterarbeitsgruppen z.B API Evaluation Group und Kontakt zu ETSI
- ETSI ESI STF spezifiziert Zertifikatsprofil TS 319 495 und ist in Abstimmung mit EBA und NCA über den Antragprozess
- API Initiativen:
  - Berlin Group – Standardisierung (BdB, BVR, VÖB, DSGV, Deutsche Bank, Hypo, DZ Bank, VISA, SRC, Worldline)
  - UK Open Banking Europe Kontakte zu ETSI
  - CAPS
  - Polnische Initiative
- Deutsche Kreditwirtschaft (GBIC) – Anforderungen der TPP Schnittstelle technisch, organisatorisch, funktional
- European Payment Council (EPC)
- ISO/TC68 SC2 „security of TPP architectures" Arbeitsgruppe der ISO

EUROPEAN UNION	Competent Authority
AUSTRIA	Financial Market Authority (FMA)
BELGIUM	National Bank of Belgium (NBB)
BULGARIA	Financial Supervision Commission (FSC)
CROATIA	Hrvatska Narodna Banka (HNB)
CYPRUS	Central Bank of Cyprus (CBC)
CZECH REPUBLIC	Czech National Bank (CNB)
DENMARK	finanstilsynet (FSA)
ESTONIA	FINANTSINSPEKTSIOON (FSA)
FINLAND	Finanssivalvonta (FIN-FSA)
FRANCE	Autorité de Controle Prudentiel (ACPR) "Regafi"
GERMANY	Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)
GREECE	Bank Of Greece
HUNGARY	Magyar Nemzeti Bank (MNB)
IRELAND	Central Bank of Ireland (CBI)
ITALY	Banca d'Italia
LATVIA	Finansu un Kapital Tirgus Komisija (FKTK)
LITHUANIA	Bank of Lithuania (LB)
LUXEMBOURG	Commission de Surveillance du Secteur Financier (CSSF)
MALTA	Malta Financial Services Authority (MFSA)
NETHERLANDS	De Nederlandsche Bank (DNB)
POLAND	Komisja Nadzoru Finansowego (KNF)
PORTUGAL	Comissão do Mercado de Valores Mobiliários (CNVM)
ROMANIA	Banca Nationala a Romaniei (BNR)
SLOVAKIA	Narodna Banka Slovenska (NBS)
SLOVENIA	Banka Slovenije (BSI)
SPAIN	Banco de Espana (BDE)
SWEDEN	Finansinspektionen (FI)
UNITED KINGDOM	Financial Conduct Authority (FCA)

NON-EU	Competent Authority
ICELAND	Fjármálaeftirlitið (FME)
LIECHTENSTEIN	Finanzmarktaufsicht Liechtenstein (FMA)
NORWAY	Finanstilsynet (FSA)
SWITZERLAND	Swiss Financial Market Supervisory Authority (FINMA)

PSD 2 Teilnehmer der PSD2 PKI

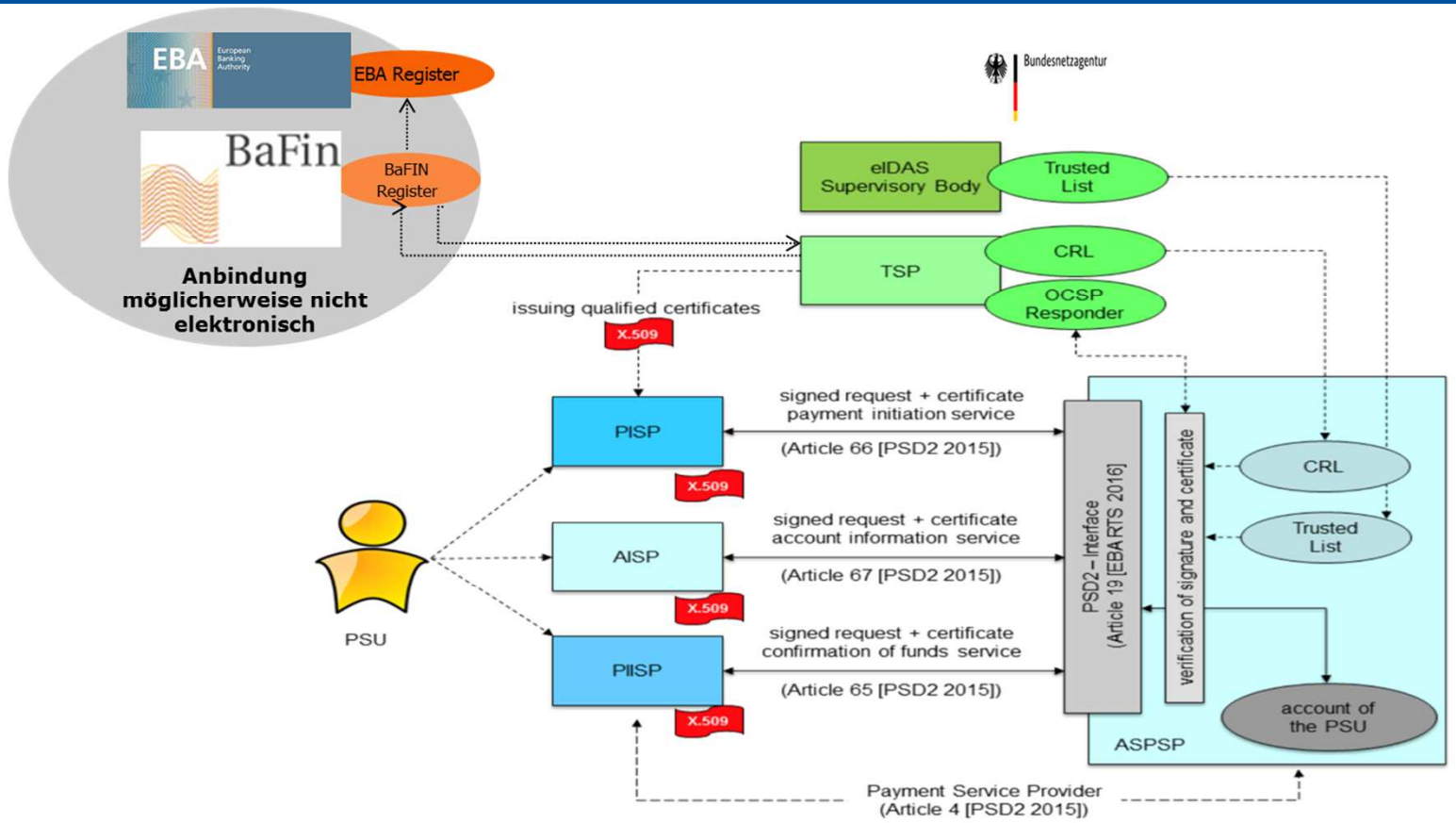
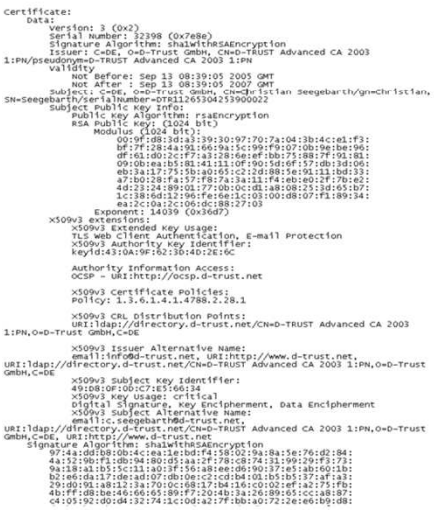


Figure 1: Participants of the PKI at the usage level

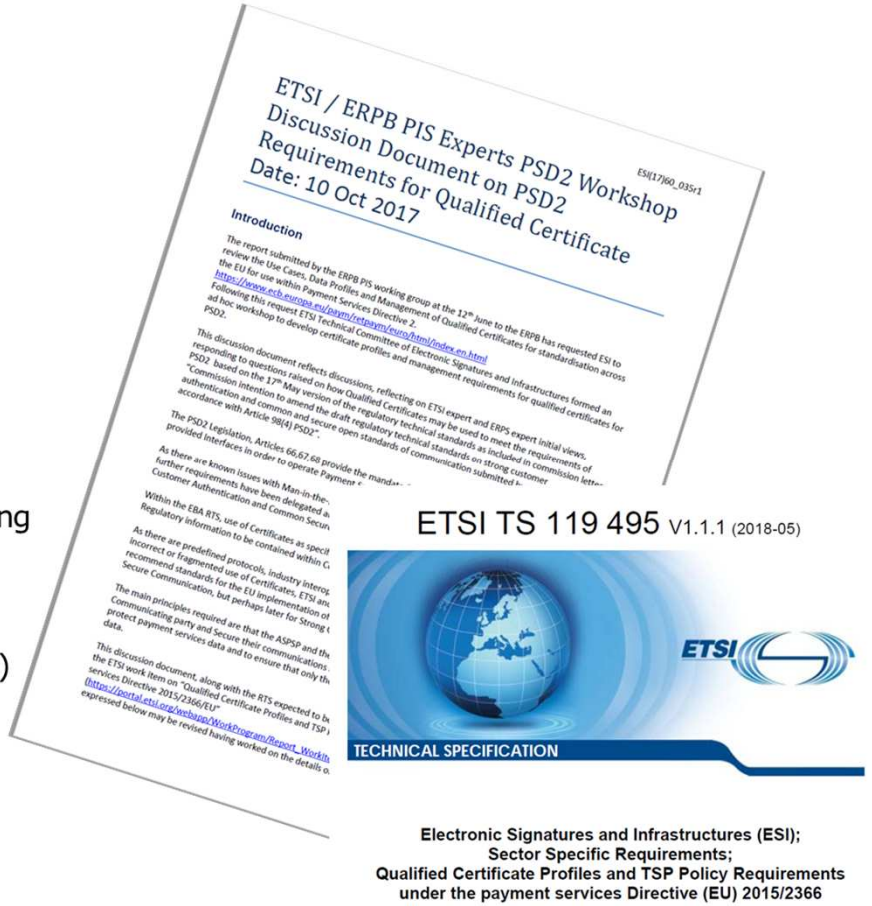
Standardisierung ETSI

At its plenary meeting of the 10th October, the European Telecommunications Standards Institute (ETSI) agreed to create a set of standards for PSD2 eIDAS certificates, in accordance with the EBA RTS.



Inhalt

- Zertifikatsprofil
- Zertifikatsverwaltung
  - Antragsweg
  - Sperrungen
- Richtlinien (Policies)



Wie bekomme ich ein Zertifikat

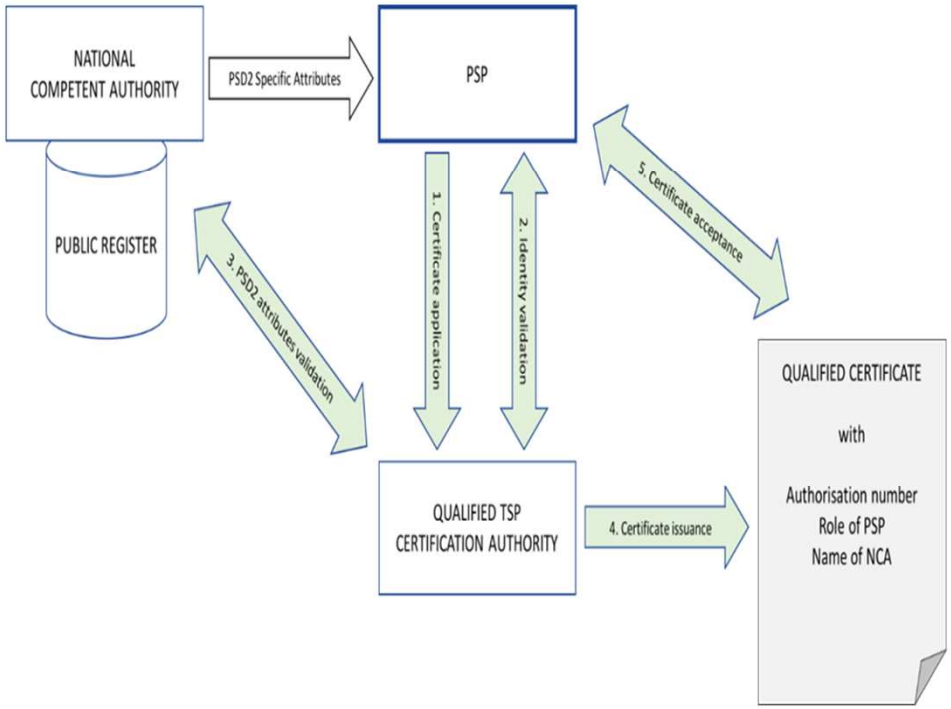
1. Erlaubnis- / Registrierungsverfahren

BaFin

Antragstellung	Verfahren Zugang zu sensiblen Zahlungsdaten	Geschäftsfortführung im Krisenfall	Satzung/Gesellschafts-vertrag
Angaben zum/r Antragsteller/in	Verfahren Sicherheitsvorfälle sicherheitsbez. Kundenbeschwerden	Erfassung statistischer Daten (nicht KID)	Name des Abschlussprüfers (nicht KID)
Geschäftsmodell	Unternehmens-steuerung	Sicherheitsstrategie	Geschäftsleiter
Geschäftsplan	Sicherungs-anforderungen (nicht ZAD und KID)	Kontrollmechanismen zur Erfüllung der Anforderungen gem. §§ 27 und 53 ZAG 2018 (nicht KID)	Inhaberkontrolle (nicht KID)
Nachweis Anfangskapital (nicht KID)	Absicherung im Haftungsfall (wenn ZAD und KID erbracht werden)	Geldwäscheprävention	Organisatorischer Aufbau

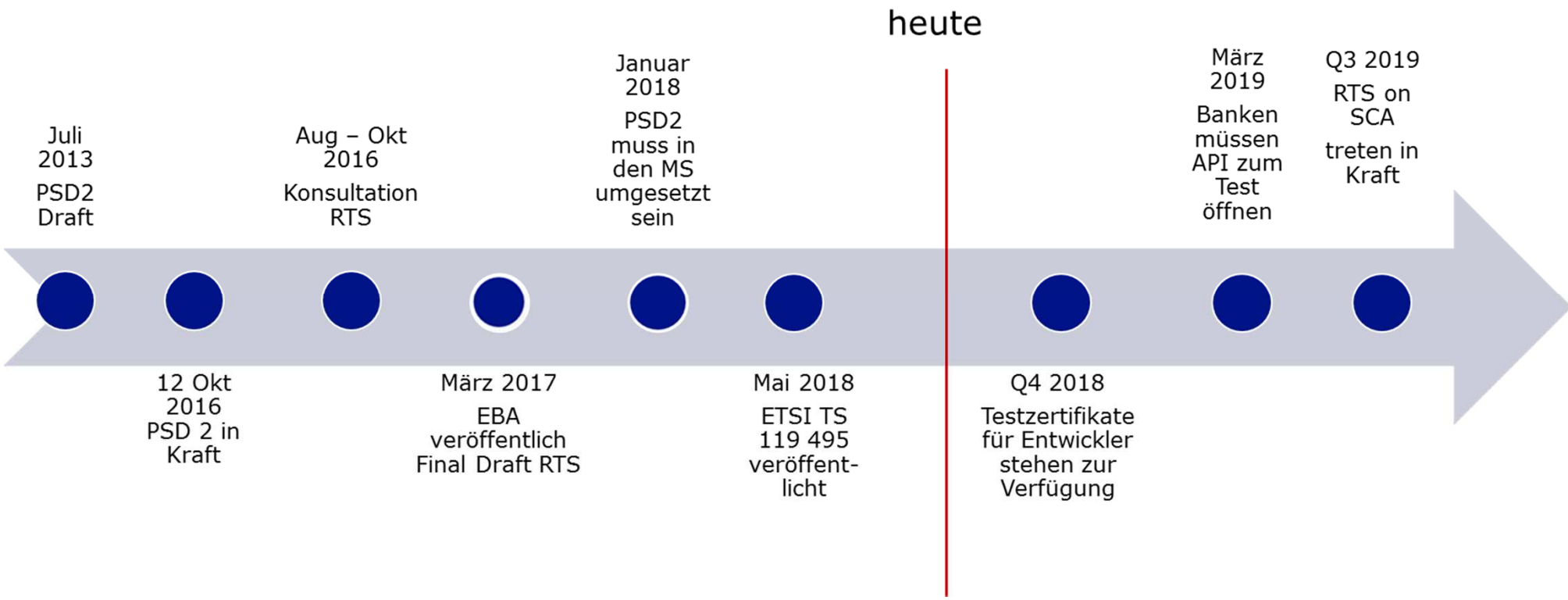
Quelle: BaFin Erlaubnisverfahren und laufende Aufsicht

2. Zertifikatsbeantragung



Quelle: ETSI TS 119 495

Zeitliche Entwicklung der PSD2 und des RTS



Christian Seegebarth
Senior Expert Trusted Solutions

E-Mail: Christian.Seegebarth@bdr.de
Telefon: +49-30-2598 3942

Vielen Dank.

Hinweis: Diese Präsentation ist Eigentum der Bundesdruckerei GmbH.
Sämtliche Inhalte – auch auszugsweise – dürfen nicht ohne die Genehmigung der Bundesdruckerei GmbH vervielfältigt, weitergegeben oder veröffentlicht werden.

© 2017 by Bundesdruckerei GmbH.

- Die PSD2 definiert die Notwendigkeit starker Kundenauthentifizierung (Artikel 97, PSD2)

1) Die Mitgliedstaaten stellen sicher, dass ein Zahlungsdienstleister eine starke Kundenauthentifizierung verlangt, wenn der Zahler

a) online auf sein Zahlungskonto zugreift,

b) einen elektronischen Zahlungsvorgang auslöst, q

c) über einen Fernzugang eine Handlung vornimmt, die das Risiko eines Betrugs im Zahlungsverkehr oder anderen Missbrauchs birgt.

- Die PSD2 definiert starke Kundenauthentifizierung (Artikel 4, 30 PSD2):

„starke Kundenauthentifizierung" eine Authentifizierung unter Heranziehung von mindestens zwei Elementen der Kategorien **Wissen** (etwas, das nur der Nutzer weiß), **Besitz** (etwas, das nur der Nutzer besitzt) oder **Inhärenz** (etwas, das der Nutzer ist), **die insofern voneinander unabhängig sind, als die Nichterfüllung eines Kriteriums die Zuverlässigkeit der anderen nicht in Frage stellt**, und die so konzipiert ist, dass die Vertraulichkeit der Authentifizierungsdaten geschützt ist.

- Dynamischer Code der Transaktion (Erwägungsgrund 95, PSD2)

Zahlungsdienste, die über das Internet oder über andere Fernkommunikationskanäle angeboten werden und nicht davon abhängig sind, an welchem Ort sich das für die Auslösung des Zahlungsvorgangs verwendete Gerät oder das verwendete Zahlungsinstrument tatsächlich befinden, **sollten daher die Authentifizierung von Zahlungsvorgängen durch dynamische Codes enthalten**, damit der Nutzer stets Klarheit über den Betrag und über den Empfänger der Zahlung hat, die er veranlasst

- Wann muss SCA NICHT eingesetzt werden:
  - Ausnahmen über nachweisbares Transaktionsrisikomanagement (TRA)
  - Kontaktlose Transaktion < 50 EUR oder < 5 Transaktionen
  - Transaktionen <30 EUR oder < 5 Transaktion Summe < 100 EUR
  - Fahrkarten oder Parkscheine etc.
  - Daueraufträge Überweisungen auf das eigenen Konto