Auf dem Weg zur Umsetzung der PSD2-Richtlinie

Detlef Hühnlein · Tina Hühnlein · Tobias Wich · Daniel Nemmert
Michael Rauh · Stefan Baszanowski · Mike Prechtl · René Lottes

ecsec GmbH
vorname.nachname@ecsec.de

Zusammenfassung

Der vorliegende Beitrag liefert einen kompakten Überblick über die hinsichtlich der sicheren und standardkonformen Umsetzung besonders relevant erscheinenden Aspekte der so genannten „Payment Services Directive 2“ (PSD2) [2015/2366/EU] samt den zugehörigen technischen Regulierungsstandards [EBA-RTS] für die Authentifizierung und die Kommunikation gemäß Artikel 98. Außerdem werden Umsetzungsvorschläge für die notwendigen Schnittstellen zwischen den involvierten Zahlungsdienstleistern auf Basis von internationalen Standards skizziert und damit zusammenhängende Sicherheitsaspekte erörtert.

1 Einleitung

Durch die Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, die auch als zweite Zahlungsdienstleisterrichtlinie bzw. international als „Payment Services Directive 2“ (PSD2) bekannt ist, werden kontoführende Zahlungsdienstleister (z.B. Kreditinstitute) verpflichtet, anderen Zahlungsdienstleistern unter gewissen Umständen Zugriff auf das Zahlungskonto eines Zahlungsdienstnutzers zu gewähren. Mit dieser neuen Anforderung, die ursprünglich unter dem Begriff „Access to Account“[1] eingeführt wurde, wird das Verhältnis zwischen Kunde und Bank in ganz Europa neu definiert. Da damit möglicherweise disruptive Veränderungen im europäischen Zahlungsverkehrsmarkt einhergehen können, aber umgekehrt die notwendigen Standards hierfür bislang nur schemenhaft erkennbar sind und durch die neu eingeführten Schnittstellen möglicherweise neuartige Bedrohungen entstehen, erscheint es geboten, sich frühzeitig intensiv mit den neuen regulatorischen Anforderungen und ihrer sicheren und standardkonformen Umsetzung zu befassen.

Vor diesem Hintergrund werden in Abschnitt 2 die wesentlichen regulatorischen Rahmenbedingungen zur sicheren Umsetzung der PSD2-Richtlinie zusammengetragen, bevor in Abschnitt 3 ein grober Vorschlag für die Realisierung der für den Kontozugriff notwendigen Schnittstellen entwickelt und in Abschnitt 4 schließlich ein Ausblick auf mögliche zukünftige Entwicklungen gewagt wird.

[1] Siehe Artikel 29a von [2013/0624/COD] (Access to accounts maintained with a credit institution).

P. Schartner · A. Baumann (Hrsg.) · D•A•CH Security 2017 · syssec (2017) 278-290.

2 Regulatorische Rahmenbedingungen

2.1 Die PSD2-Richtlinie (EU) 2015/2366

Durch die PSD2-Richtlinie [2015/2366/EU] werden die bisherigen Rahmenbedingungen für Zahlungsdienste in Europa[2] dahingehend fortgeschrieben, dass nun insbesondere[3] zwischen

- **kontoführenden Zahlungsdienstleistern** (Account Servicing Payment Service Provider, ASPSP) (siehe Artikel 4, Nr. 17 und Nr. 12),
- **Zahlungsauslösedienstleistern** (Payment Initiation Service Provider, PISP) (siehe Artikel 4, Nr. 18 und Artikel 66) und
- **Kontoinformationsdienstleistern** (Account Information Service Provider, AISP) (siehe Artikel 4, Nr. 19, Artikel 33 und Artikel 67)

unterschieden wird. Da die Zahlungsauslösedienstleister und Kontoinformationsdienstleister im Zuge der PSD2-Richtlinie auf das Zahlungskonto des Zahlungsdienstnutzers zugreifen dürfen, werden diese im vorliegenden Beitrag auch zusammenfassend als „**zugreifende Zahlungsdienstleister**“ bezeichnet.

Nach **Artikel 66** (Vorschriften für den Zugang zum Zahlungskonto im Fall von **Zahlungsauslösediensten**) haben Zahler das Recht, einen so genannten Zahlungsauslösedienstleister für das Auslösen einer Zahlung zu verwenden, der sich vor jeder Transaktion gegenüber dem kontoführenden Zahlungsdienstleister authentifizieren muss.

Gemäß **Artikel 67** (Vorschriften für den Zugang zu Zahlungskontoinformationen und deren Nutzung im Fall von **Kontoinformationsdiensten**) haben Zahlungsdienstnutzer das Recht, über einen so genannten Kontoinformationsdienstleister lesend auf ein Zahlungskonto zuzugreifen.

Gemäß **Artikel 97** (Authentifizierung) wird eine **starke Kundenauthentifizierung** verlangt, wenn der Zahler

(a) online auf sein Zahlungskonto zugreift,

(b) einen elektronischen Zahlungsvorgang auslöst, wobei im Fall eines Fernzahlungsvorgangs die Elemente Betrag und Zahlungsempfänger dynamisch in die zur Authentifizierung vorgelegten Daten einfließen müssen, oder

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

Gemäß Artikel 97 (3) müssen Zahlungsdienstleister angemessene Sicherheitsvorkehrungen für den Schutz der Vertraulichkeit und Integrität der personalisierten Sicherheitsmerkmale treffen und nach Artikel 97 (5) muss „der kontoführende Zahlungsdienstleister dem Zahlungsauslösedienstleister und dem Kontoinformationsdienstleister gestatten, sich auf die Authentifizierungsverfahren zu stützen, die er dem Zahlungsdienstnutzer […] bereitstellt.“

---

[2] Siehe insbesondere 2007/64/EG, 2009/110/EG, 2009/924/EG, 2011/83/EU und 2015/751/EU.

[3] Darüber sind in Anhang I der PSD2-Richtlinie [2015/2366/EU] weitere Zahlungsdienste aufgeführt, die jedoch im vorliegenden Beitrag nicht näher betrachtet werden.

Es erscheint wichtig hervorzuheben, dass die Anforderung aus Artikel 97 (5) [2015/2366/EU] das aus dem föderierten Identitätsmanagement[4] wohlbekannte und in Abbildung 1 dargestellte „Dreiecksverhältnis“ zwischen dem Zahlungsdienstnutzer (User), dem kontoführenden Zahlungsdienstleister (Identity Provider) und dem zugreifenden Zahlungsdienstleister (Service Provider) impliziert. Nähere Betrachtungen zur Ausgestaltung dieser Schnittstellen, die im vorliegenden Fall neben der starken Authentifizierung gemäß Artikel 97 auch die fachlich notwendige Funktionalität gemäß Artikel 66 und 67 bereitstellen müssen, finden sich in Abschnitt 3.

Gemäß **Artikel 98** der PSD2-Richtlinie [2015/2366/EU] erarbeitet die European Banking Authority (EBA) in Zusammenarbeit mit der Europäischen Zentralbank (EZB) **technische Regulierungsstandards** (Regulatory Technical Standards, RTS), die insbesondere

(a) die Erfordernisse des Verfahrens zur starken Kundenauthentifizierung gemäß Artikel 97,

(b) etwaige Ausnahmen von der Pflicht zur starken Authentifizierung,

(c) Anforderungen hinsichtlich des Schutzes der Vertraulichkeit und Integrität der personalisierten Sicherheitsmerkmale und nicht zuletzt

(d) „Anforderungen an gemeinsame und sichere offene Standards für die Kommunikation zwischen kontoführenden Zahlungsdienstleistern, Zahlungsauslösedienstleistern, Kontoinformationsdienstleistern, Zahlern, Zahlungsempfängern und anderen Zahlungsdienstleistern zum Zwecke der Identifizierung, der Authentifizierung, der Meldung und der Weitergabe von Informationen sowie der Anwendung von Sicherheitsmaßnahmen“ spezifizieren.

2.2 Der technische Regulierungsstandard gemäß Artikel 98

Der finale Entwurf [EBA-RTS] dieses technischen Regulierungsstandards für die Authentifizierung und die Kommunikation gemäß Artikel 98 der PSD2-Richtlinie [2015/2366/EU] wurde im Februar 2017 der Europäischen Kommission zur Prüfung vorgelegt. Er legt unter anderem fest, dass Zahlungsdienstleister im Regelfall

- geeignete Maßnahmen zur Transaktionsüberwachung vorsehen müssen, um unautorisierte oder betrügerische Zahlungstransaktionen zu erkennen (Artikel 2),
- bei der Anwendung von starken Authentifizierungsverfahren einen einmalig gültigen und fälschungssicheren Authentifizierungscode erzeugen, diesen mit einem Fehlbedienungszähler von höchstens fünf schützen und ein automatisches Logout nach fünf Minuten ohne Benutzerinteraktion realisieren müssen (Artikel 4),
- den Zahler über Betrag und Zahlungsempfänger informieren und diese Informationen in den Authentifizierungscode einfließen lassen müssen (Artikel 5),
- geeignete Maßnahmen vorsehen müssen, um einem Missbrauch der Authentifizierungsfaktoren entgegenzuwirken, wobei
  - bei wissensbasierten Authentifizierungsfaktoren insbesondere die Vertraulichkeit der Daten zu schützen ist (Artikel 6),
  - bei besitzbasierten Authentifizierungsfaktoren die Replikation des Gegenstands verhindert werden soll (Artikel 7) und
  - bei inhärenzbasierten Authentifizierungsfaktoren die Wahrscheinlichkeit für eine fälschliche Akzeptanz sehr gering sein muss (Artikel 8).

[4] Siehe z.B. [Hühn08], [HüRZ10], [HSW+12] und [HWSH14].

Hierbei müssen die Authentifizierungsfaktoren unabhängig sein und bei der Nutzung von Mehrzweckgeräten muss die Separation mindestens durch getrennte sichere Ausführungsumgebungen erfolgen (Artikel 9).

In [EBA-RTS] Kapitel 3 (Artikel 10-18) sind eine Reihe von Ausnahmefällen definiert, in denen auf eine starke Kundenauthentifizierung verzichtet werden kann. Dies umfasst beispielsweise den Fall, wenn

- nur lesend auf den Kontostand oder die Transaktionen der letzten 90 Tage zugegriffen werden soll, sofern es sich nicht um den allerersten Zugriff handelt und eine starke Authentifizierung vor weniger als 90 Tagen erfolgt ist (Artikel 10),
- eine kontaktlose Zahlung mit einem Wert bis zu 50 Euro bzw. seit der letzten starken Authentifizierung weniger als fünf Transaktionen mit einem Wert bis zu 150 Euro durchgeführt worden sind (Artikel 11),
- eine Bezahlung an einem unbeaufsichtigten Zahlungsterminal für die Bezahlung eines Fahrscheins oder Parktickets erfolgt (Artikel 12),
- es sich um eine Zahlung an vertrauenswürdige Empfänger oder eine wiederkehrende Zahlung (Artikel 13) handelt,
- die Zahlung an sich selbst erfolgt und beide Konten des Zahlers und Zahlungsempfängers beim gleichen Institut geführt werden (Artikel 14),
- der Zahlbetrag 30 Euro nicht übersteigt bzw. der kumulierte Betrag aus den letzten bis zu fünf Transaktionen seit der letzten starken Authentifizierung den Betrag von 100 Euro nicht übersteigt (Artikel 15) oder
- eine ausgefeilte transaktionsbasierte Risikoanalyse gemäß Artikel 16 erfolgt.

[EBA-RTS] Kapitel 4 (Artikel 19-24) spezifiziert Sicherheitsanforderungen für den Schutz der Vertraulichkeit und Integrität der personalisierten Sicherheitsmerkmale, wobei neben generellen Anforderungen (Artikel 19) auch Anforderungen für die Erzeugung und Übermittlung (Artikel 20), die Zuordnung der Sicherheitsmerkmale zum Zahlungsdienstnutzer (Artikel 21), die Auslieferung der Sicherheitsmerkmale, Authentifizierungstoken und Software (Artikel 22), die Erneuerung (Artikel 23) und schließlich die Vernichtung, Deaktivierung und Sperrung (Artikel 24) vorgesehen sind.

Insgesamt erscheint hier erwähnenswert, dass die Anforderungen zur starken Kundenauthentifizierung gemäß Artikel 97 [2015/2366/EU] und den Artikeln 6-9 und 19-24 [EBA-RTS] ziemlich genau den Anforderungen zur dynamischen[5] und auf mindestens zwei Authentifizierungsfaktoren aus unterschiedlichen Kategorien[6] basierende Authentifizierung bei einem elektronischen Identifizierungssystem mit Sicherheitsniveau „substanziell“ gemäß Artikel 8 der eIDAS-Verordnung [2014/910/EU] entsprechen. Deshalb ist es perspektivisch vorstellbar, dass Bezahltransaktionen eines Tages nur noch mit geeigneten elektronischen Identifizierungsmitteln autorisiert werden und man somit in Europa buchstäblich „mit seinem guten Namen“ bzw. aus Datenschutzgründen unter entsprechenden Pseudonymen bezahlen kann.

In [EBA-RTS] Kapitel 5 (Artikel 25-31) sind Anforderungen für „gemeinsame und sichere offene Standards für die Kommunikation“ spezifiziert. Dies umfasst im ersten Abschnitt gene-

[5] Siehe Anlage zu [2015/1502/EU], Abschnitt 2.3.1, lit. 1.

[6] Siehe Anlage zu [2015/1502/EU], Abschnitt 2.2.1, lit. 1.

relle Anforderungen für die sichere Identifikation der involvierten Geräte, wie z.B. Zahlungsverkehrsterminals, und Maßnahmen gegen die unautorisierte Umleitung der Kommunikation (Artikel 25) sowie Maßnahmen zur detaillierten Protokollierung und Nachvollziehbarkeit von relevanten Ereignissen (Artikel 26).

In Artikel 27 (1) ist festgelegt, dass ein kontoführender Zahlungsdienstleister, der ein onlinefähiges Zahlungskonto anbietet, mindestens eine Schnittstelle anbieten muss, die (a) die Identifikation des zugreifenden Zahlungsdienstleisters und den sicheren Zugriff für (b) Kontoinformationsdienstleister und (c) Zahlungsauslösedienstleister ermöglicht.

Gemäß Artikel 27 (2) kann diese Schnittstelle eigenständig realisiert sein, oder es kann sich um eine bereits von Zahlungsdienstnutzern regelmäßig verwendete Schnittstelle handeln.

Diese Schnittstelle stützt sich für die Authentifizierung der Nutzer auf die vom kontoführenden Zahlungsdienstleister verwendeten Verfahren (Artikel 27 (3)) und erlaubt

(a) den zugreifenden Zahlungsdienstleistern den Authentifizierungsvorgang zu starten,
(b) während des Authentifizierungsvorgangs eine Kommunikationsverbindung zwischen den involvierten Zahlungsdienstleistern aufzubauen und aufrecht zu erhalten und
(c) die Integrität und Vertraulichkeit der persönlichen Sicherheitsmerkmale und Authentifizierungscodes zu gewährleisten.

Gemäß Artikel 27 (4) müssen die vom kontoführenden Zahlungsdienstleister angebotenen technischen Schnittstellen auf internationalen oder europäischen Standards basieren und entsprechend dokumentiert[7] sein. Spezifikationsänderungen müssen regelmäßig mindestens drei Monate vor der Implementierung einer Änderung verfügbar gemacht werden (Artikel 27 (5)) und kontoführende Zahlungsdienstleister sind verpflichtet, den zugriffsberechtigten Zahlungsdienstleistern eine entsprechende Testmöglichkeit zur Nutzung der Schnittstelle und entsprechende Unterstützungsleistungen anzubieten (Artikel 27 (6)).

Sofern vom kontoführenden Zahlungsdienstleister eine eigenständige Schnittstelle bereitgestellt wird, muss diese genauso verfügbar, performant und ausfallsicher sein, wie die bereits anderweitig genutzten Schnittstellen (Artikel 28 (1)). Zu diesem Zweck müssen kontoführende Zahlungsdienstleister die Verfügbarkeit und Performanz der Schnittstelle regelmäßig überwachen, der Aufsichtsbehörde bei Bedarf entsprechende Statistiken zukommen lassen und etwaige Mängel umgehend beheben (Artikel 28 (2)). Gemäß Artikel 28 (3) muss die eigenständige Schnittstelle Elemente, Komponenten oder Nachrichtentypen aus [ISO20022] nutzen. Schließlich muss gemäß Artikel 28 (4) eine geeignete Notfallplanung für die angebotene Schnittstelle existieren, die den zugriffsberechtigten Zahlungsdienstleistern alternative Nutzungsmöglichkeiten während des Ausfalls aufzeigt.

Gemäß Artikel 29 (1) [EBA-RTS] müssen für die Identifizierung[8] der Zahlungsdienstleister qualifizierte Zertifikate für elektronische Siegel gemäß Artikel 3 (30) oder qualifizierte Zertifikate zur Webseitenauthentifizierung gemäß Artikel 3 (39) der eIDAS-Verordnung [2014/910/EU] genutzt werden.

---

[7] Die vollständigen zur Interoperabilität notwendigen Spezifikationen müssen zumindest solchen Zahlungsdienstleistern zur Verfügung stehen, die einen entsprechenden Zulassungsantrag bei ihrer zuständigen Aufsichtsbehörde gestellt haben. Außerdem müssen kontoführende Zahlungsdienstleister auf ihrer Webseite eine Zusammenfassung der Dokumentation veröffentlichen.

[8] Artikel 29 (1) [EBA-RTS] verweist auf einen nicht existierenden Absatz (a) in Artikel 21 (1). Deshalb wird vermutet, dass es sich um einen editorischen Fehler handelt und eigentlich Artikel 27 (1) (a) gemeint ist.

Diese Zertifikate müssen

- gemäß Artikel 29 (2) als Registrierungsnummer[9] im Zertifikat die Zulassungsnummer des Zahlungsdienstleisters[10],
- nach Artikel 29 (3) (a) in englischer Sprache die Rolle des Zahlungsdienstleisters[11] und
- gemäß Artikel 29 (3) (b) den Namen der zuständigen Zulassungsbehörde

enthalten. Allerdings fordert Artikel 29 (4), dass durch diese Angaben im Zertifikat die Interoperabilität nicht beeinträchtigt werden darf. Um eine Registrierungsnummer in ein qualifiziertes Zertifikat für juristische Personen aufzunehmen, sieht der dafür maßgebliche [EN319412-3] im `subject`-Element des Zertifikates die Verwendung des ASN.1-Elementes `organizationIdentifier` aus [X.520] vor, wobei Zertifikate einen oder mehrere semantische Identifikatoren gemäß [EN319412-1] (Abschnitt 5) enthalten können. Unglücklicherweise sind in [EN319412-1] (Abschnitt 5.1.4) derzeit nur drei für den vorliegenden Fall leider unpassende Varianten[12] vorgesehen, so dass hier offenbar Standardisierungsbedarf existiert, der im dafür „zuständigen" Standardisierungsgremium ETSI ESI[13] bereits aktiv adressiert wird.

Gemäß Artikel 30 (1) [EBA-RTS] müssen Zahlungsdienstleister für den Schutz der Integrität und Vertraulichkeit starke Verschlüsselungsmechanismen einsetzen. Die zugreifenden Zahlungsdienstanbieter dürfen Kommunikationssitzungen mit dem kontoführenden Zahlungsdienstleister nur so lange wie nötig offenhalten und müssen diese terminieren, sobald die angeforderte Aktion beendet ist (Artikel 30 (2)). Sofern parallele Netzwerkverbindungen für eine bestimmte Aktion notwendig sind, müssen diese sicher miteinander verbunden werden (Artikel 30 (3)) und es müssen eindeutige Identifikatoren und Verweise für die technische Kommunikationsverbindung, den Zahlungsdienstnutzer und die fachliche Transaktion verwendet werden (Artikel 30 (4)). Sofern die Übermittlung der personalisierten Sicherheitsmerkmale und Authentifizierungscodes über die zugreifenden Zahlungsdienstleister erfolgt, müssen diese jederzeit zuverlässig für deren Vertraulichkeit[14] sorgen und andernfalls den Zahlungsdienstnutzer und den Herausgeber der personalisierten Sicherheitsmerkmale über den Verlust der Vertraulichkeit informieren (Artikel 30 (5)).

Artikel 31 regelt schließlich einige Details hinsichtlich der durch die Artikel 66 und 67 von [2015/2366/EU] skizzierten fachlichen Schnittstellen und in den Artikeln 32 und 33 wird schließlich das unmittelbare Inkrafttreten des technischen Regulierungsstandards in allen Mitgliedsstaaten, die Umsetzungsfrist von 18 Monaten sowie die Überprüfung und mögliche Anpassung desselben geregelt.

---

[9] Siehe Anlage III und IV (c) der eIDAS-Verordnung [2014/910/EU].

[10] Siehe Artikel 14 von [2015/2366/EU] und Artikel 8 von [2013/36/EU].

[11] Hierbei sind kontoführende Zahlungsdienstleister, Kontoinformationsdienstleister, Zahlungsauslösedienstleister und Zahlungskartenherausgeber zu unterscheiden.

[12] „VAT" für die Umsatzsteuer-ID, „NTR" für die Handelsregisternummer und die Option für länderspezifische Festlegungen.

[13] Siehe https://portal.etsi.org/TBSiteMap/esi/ESIActivities.aspx .

[14] Der erste Satz in Artikel 30 (5) [EBA-RTS] ist folgendermaßen gefasst: „Account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments shall ensure that where they communicate personalised security credentials and authentication codes, these are not readable by any staff at any time."

3 Schnittstellen für den Kontozugriff

In diesem Abschnitt soll die technische Ausgestaltung der durch die PSD2-Richtlinie geforderten Schnittstellen zwischen kontoführenden Zahlungsdienstleistern, Zahlungsauslösedienstleistern, Kontoinformationsdienstleistern, Zahlern, Zahlungsempfängern und anderen Zahlungsdienstleistern näher betrachtet werden.

3.1 Generelle Überlegungen und Überblick

Wie bereits erwähnt, impliziert Artikel 97 (5) [2015/2366/EU], im Einklang mit Artikel 27 (3) (a) [EBA-RTS], das in Abbildung 1 dargestellte „Dreiecksverhältnis“, bei dem der Zahlungsdienstnutzer vom zugreifenden Zahlungsdienstleister (Zahlungsauslösedienstleister oder Kontoinformationsdienstleister) vor Abwicklung einer fachlichen Transaktion gemäß Artikel 66 oder 67 zur starken Kundenauthentifizierung an den kontoführenden Zahlungsdienstleister umgeleitet wird.

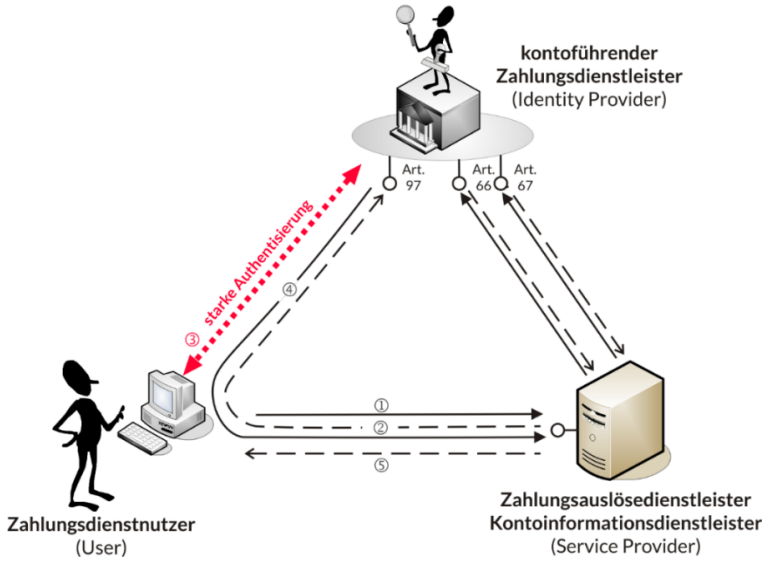

Abb. 1: Zusammenwirken der Zahlungsdienstleister gemäß PSD2-Richtlinie

Gemäß Artikel 27 (4) [EBA-RTS] müssen die vom kontoführenden Zahlungsdienstleister angebotenen technischen Schnittstellen auf internationalen oder europäischen Standards basieren und gemäß Artikel 28 (3) [EBA-RTS] – zumindest im Fall einer eigenständigen Schnittstelle – Elemente, Komponenten oder Nachrichtentypen aus [ISO20022] nutzen.

3.2 API für die starke Authentifizierung (Art. 97)

Die Schnittstelle zur starken Authentifizierung gemäß Artikel 97 [2015/2366/EU] kann[15] durch den Einsatz eines geeigneten Föderationsprotokolls von den fachlichen Schnittstellen gemäß

[15] Hier ist zunächst festzuhalten, dass der Einsatz eines standardisierten Föderationsprotokolls zur Entkopplung der starken Authentifizierung von den fachlichen Schnittstellen in [EBA-RTS] nicht explizit gefordert ist und man deshalb darauf verzichten könnte. Auf der anderen Seite ist eine solche Entkopplung für die effiziente Wartung und Pflege des Systems sehr wichtig, da andernfalls bei jeder Änderung der Authentisierungstechnologie auch die fachlichen Schnittstellen angepasst werden müssten. In Verbindung mit der Anforderung für kontoführende Zahlungsdienstleister aus Artikel 27 (4), dass die von ihnen angebotenen Schnittstellen internationalen oder europäischen Standards folgen *müssen* („Account servicing payment service providers *shall* ensure that their interface(s)

Artikel 66 und 67 der PSD2-Richtlinie [2015/2366/EU] weitgehend entkoppelt werden. Zu den aus heutiger Sicht[16] relevanten internationalen Standards, die eine starke Authentifizierung[17] in einem in Abbildung 1 dargestellten Dreiecksverhältnis ermöglichen, zählt insbesondere die im OASIS Security Services (SAML) TC[18] entwickelte „Security Assertion Markup Language" (SAML) (Version 2.0) [SAML2] und das auf dem OAuth 2.0 Framework [RFC6749] basierende „OpenID Connect" [OIDC].

Während sich die beiden Protokolle in technischen Details[19] unterscheiden, so unterstützen beide die in Abbildung 1 skizzierte Architektur und könnten deshalb grundsätzlich beide als Grundlage zur Realisierung von PSD2-spezifischen Schnittstellen herangezogen werden. Somit wäre es theoretisch denkbar, sowohl auf Basis von SAML als auch auf Basis von OpenID Connect eine entsprechende PSD2-Schnittstelle zu spezifizieren, wobei für die fachlichen Schnittstellen gemäß Artikel 66 und 67 grundsätzlich sowohl SOAP-[20] als auch REST[21]-basierte Webservices genutzt werden können.

Auf der anderen Seite wünscht sich vermutlich nicht nur die deutsche Kreditwirtschaft[22], dass ein einziger europaweit abgestimmter einheitlicher Standard entwickelt wird. Da Artikel 28 (3) [EBA-RTS] die Nutzung von Elementen, Komponenten oder Nachrichtentypen aus [ISO20022] verlangt[23], würde eine strenge Auslegung dieser Anforderung tendenziell möglicherweise eher für eine komplett XML- und somit SAML-basierte Lösung sprechen. Auf der anderen Seite wurden inzwischen erste Vorschläge[24] für REST-basierte Schnittstellen zur Umsetzung der PSD2-Richtlinie vorgelegt, so dass man in der Praxis voraussichtlich auch bzw. möglicherweise insbesondere REST-basierte Schnittstellen vorfinden wird.

Unabhängig von der detaillierten technischen Umsetzung müssen die in Abbildung 1 aufgeführten Schnittstellen unterstützt werden.

---

follows standards of communication which are issued by international or European standardisation organisations."), erscheint der Einsatz eines standardisierten Föderationsprotokolls somit zumindest äußerst empfehlenswert.

[16] Weitere Protokolle für das föderierte Identitätsmanagement, die jedoch aus heutiger Sicht weniger relevant sind, umfassen beispielsweise OpenID (siehe [HWSH14], Abschnitt 2.2.3) oder das auf Basis von WS-* realisierte CardSpace (siehe [PrSt10], Abschnitt 2.3).

[17] Die starke Authentifizierung im engeren Sinne (Schritt 3 in Abbildung 1) wird hier nicht näher betrachtet. Vielmehr wird für eine Übersicht über aktuell eingesetzte Technologien zur starken Authentifizierung auf [2FA.jetzt] verwiesen.

[18] Siehe https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security .

[19] Beispielsweise basiert [SAML2], genau wie [ISO20022], auf XML und bietet dem zugreifenden Zahlungsdienstleister einen einzigen Kommunikationsendpunkt an, der über ein konzeptionell sehr einfaches Request-Response-Protokoll angesprochen wird, während [OIDC] auf dem leichtgewichtigeren JSON-Format aufsetzt, aber drei Kommunikationsendpunkte und mehrere Nachrichten pro Authentifizierungsvorgang benötigt.

[20] Für die Nutzung von SAML in Verbindung mit SOAP-basierten Webservices kann auf [WSS-SAML] oder [SAML-Bind] (Abschnitt 3.2) aufgebaut werden.

[21] Beim Einsatz von REST-basierten Webservices kann [OIDC] oder das SAML-OAuth-Profil gemäß [RFC7522] genutzt werden.

[22] [DeKr16], O1 fordert: „Es darf für die technische Kommunikation nur eine einzige Schnittstelle geben, die europaweit standardisiert und für alle Drittdienste und Anwendungsszenarien einheitlich ist."

[23] Artikel 28 (3) [EBA-RTS] ist folgendermaßen gefasst: „Account servicing payment service providers shall also ensure that the dedicated interface uses ISO 20022 elements, components or approved message definitions, for financial messaging."

[24] Vgl. [BankID], [OID-FAPI] und [OpBa-RW].

Bei allen Zugriffen auf die fachlichen Schnittstellen wird gemäß Artikel 27 (1) (a) i.V.m. Artikel 29 (1) [EBA-RTS] eine Identifikation des zugreifenden Zahlungsdienstleisters unter Verwendung von qualifizierten Zertifikaten für elektronische Siegel gemäß [2014/910/EU] Artikel 3 (30) oder qualifizierten Zertifikaten für die Website-Authentifizierung gemäß [2014/910/EU] Artikel 3 (39) gefordert. Da die geforderte *Identifikation des zugreifenden Zahlungsdienstleisters* nur dann mit Zertifikaten für die Website-Authentifizierung erfolgen könnte, wenn der kontoführende Zahlungsdienstleister den Verbindungsaufbau initiieren oder den anfragenden Zahlungsdienstleister „zurückrufen" würde, ist klar, dass für die Identifikation des zugreifenden Zahlungsdienstleisters qualifizierte Zertifikate für elektronische Siegel gemäß [2014/910/EU] Artikel 3 (30) genutzt und folglich elektronische Siegel gemäß [2014/910/EU] Artikel 3 (25) erstellt werden müssen.

Wie das aus regulatorischen Gründen notwendige elektronische Siegel sinnvoller Weise in die Abläufe integriert wird, hängt davon ab, ob an den fachlichen Schnittstellen (siehe Abbildung 1) SOAP oder REST verwendet wird und ob OAuth 2.0 oder eine andere Autorisierungstechnologie zum Einsatz kommt. Beim Einsatz von OAuth 2.0 bietet es sich beispielsweise an, das elektronische Siegel zur Realisierung eines starken Bindings bei der OAuth Client Authentication[25] einzusetzen. Alternativ kann das elektronische Siegel direkt zur Autorisierung der fachlichen Aufrufe genutzt werden, wobei letztlich bei einer XML-basierten Nachricht eine digitale Signatur gemäß [EN319132-1] bzw. bei einer JSON-basierten Nachricht eine digitale Signatur gemäß [RFC7515][26] erstellt werden kann. Es erscheint erwähnenswert, dass das zur Identifikation geforderte elektronische Siegel *kein* qualifiziertes elektronisches Siegel gemäß [2014/910/EU] Artikel 3 (27) sein muss, sondern auch ohne eine qualifizierte elektronische Siegelerstellungseinheit erstellt werden kann.

3.3 API für Zahlungsauslösedienstleister (Art. 66)

Für das Auslösen eines Zahlungsvorgangs gemäß Artikel 66 der PSD2-Richtlinie [2015/2366/EU] kann der Zahlungsauslösedienstleister die in Abbildung 2 skizzierte fachliche Schnittstelle (Application Programming Interface, API) nutzen, bevor die Zahlung vom Zahlungsdienstnutzer über eine starke Kundenauthentifizierung gemäß Artikel 97 autorisiert wird.

Wie in Abbildung 2 dargestellt, kann sich diese Schnittstelle (z.B. für die Identifikation des Zahlers (`Dbtr`), Zahlungskontos (`DbtrAcct`), Zahlungsempfängers (`Cdtr`), Konto des Zahlungsempfängers (`CdtrAcct`), Buchungstexts (`Purp`) sowie des Betrags (`Amt`)) auf Datenstrukturen aus [ISO20022] (`CreditorPaymentActivationRequestV06`, pain.013.001.06) stützen und muss gemäß Artikel 27 (1) (a) i.V.m. Artikel 29 (1) [EBA-RTS] ein elektronisches Siegel tragen.

[25] Siehe [RFC6749] (Abschnitt 3.2.1) und [RFC7800] und zum Vergleich [RFC7522], [RFC7523] und [CBS+17].

[26] Hier sei erwähnt, dass in ETSI ESI mit der Standardisierung von fortgeschrittenen JSON-Signaturen (JAdES) begonnen wurde.

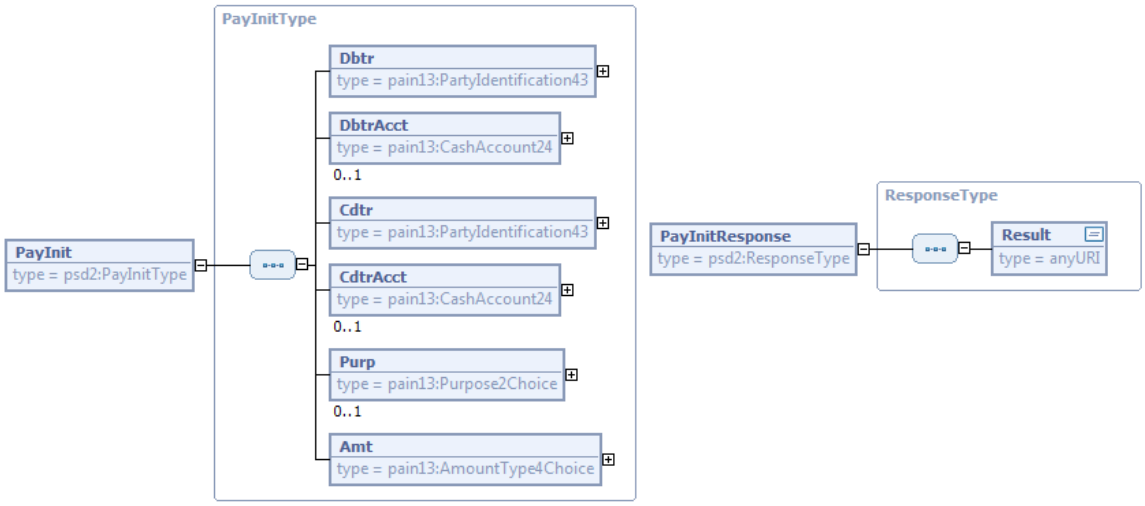

Abb. 2: Schnittstelle zum Auslösen eines Zahlungsvorgangs (Art. 66)

3.4 API für Kontoinformationsdienstleister (Art. 67)

Auch die Schnittstelle zum Abrufen von Kontoinformationen kann sich, wie in Abbildung 3 dargestellt, auf Datenstrukturen aus [ISO20022] stützen, wobei in diesem Fall die Verwendung der Nachricht `BankToCustomerAccountReportV06` (camt.052.001.06) gut als Basis geeignet erscheint.

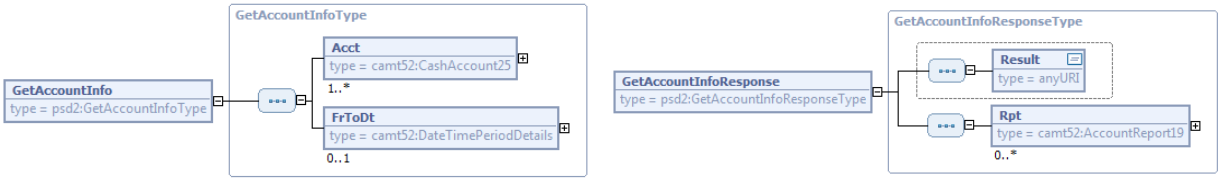

Abb. 3: Schnittstelle zum Abrufen von Kontoinformationen (Art. 67)

Die spezifischen Zugriffsregeln (z.B. selbstinitiierter Zugriff durch den Kontoinformationsdienstleister bis zu vier Mal täglich[27] und dass beim erstmaligen Zugriff und nach 90 Tagen wieder eine starke Authentifizierung erfolgen muss[28]) können z.B. über entsprechende Access Tokens gemäß [RFC6749] realisiert werden.

4 Zusammenfassung und Ausblick

Im vorliegenden Beitrag wurden die wesentlichen Anforderungen aus [2015/2366/EU] und [EBA-RTS] für das so genannte „Access-to-Account"-Interface zusammengetragen und eine Umsetzung auf Basis internationaler Standards, wie z.B. [ISO20022] und [SAML2] bzw. [OIDC], skizziert. Ob sich der in [DeKr16] geäußerte Wunsch der deutschen Kreditwirtschaft nach einem einheitlichen Standard für diese Schnittstelle erfüllt, ist vor dem Hintergrund der

[27] Siehe Artikel 31 (5) [EBA-RTS].

[28] Siehe Artikel 10 [EBA-RTS].

bereits vorgelegten unterschiedlichen Ansätze wie z.B. [OpBa-RW] und [OID-FAPI] leider noch unklar.

Danksagung

Dieser Beitrag ist teilweise im Rahmen des FutureTrust-Projektes entstanden, das unter dem Förderkennzeichen No. 700542 Fördermittel aus dem Forschungs- und Innovationsprogramm „Horizont 2020“ der Europäischen Union erhalten hat. Darüber hinaus möchten wir uns bei Detlef Hillen und Hans-Rainer van den Berg für fruchtvolle Diskussionen bedanken.

Literatur

[2013/0624/COD] Council of the European Union: Proposal for a Directive of the European Parliament and the Council on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC – Confirmation of the final compromise text with a view to agreement, 2013/0264 (COD), June 2nd 2015, http://data.consilium.europa.eu/doc/document/ST-9336-2015-INIT/en/pdf

[2013/36/EU] Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen, zur Änderung der Richtlinie 2002/87/EG und zur Aufhebung der Richtlinien 2006/48/EG und 2006/49/EG, http://data.europa.eu/eli/dir/2013/36/oj

[2014/910/EU] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, http://data.europa.eu/eli/reg/2014/910/oj

[2015/1502/EU] Durchführungsverordnung (EU) 2015/1502 der Kommission vom 8. September 2015 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel gemäß Artikel 8 Absatz 3 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt, http://data.europa.eu/eli/reg_impl/2015/1502/oj

[2015/2366/EU] Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG, http://data.europa.eu/eli/dir/2015/2366/oj

[2016/679/EU] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, http://data.europa.eu/eli/reg/2016/679/oj

[2FA.jetzt] Verbandsübergreifende Arbeitsgruppe zur Förderung der starken Authentisierung im Internet: Starke Authentisierung – jetzt, https://2fa.jetzt (2017)

[BankID] BankID Norge AS: OpenID Connect Provider (preview), https://confluence.bankidnorge.no/confluence/pages/viewpage.action?pageId=90636700, (2017)

[CBS+17] B. Campbell, J. Bradley, N. Sakimura, T. Lodderstedt: Mutual TLS Profile for OAuth 2.0, IETF Internet Draft, https://tools.ietf.org/html/draft-ietf-oauth-mtls-02

[DeKr16] Deutsche Kreditwirtschaft: Anforderungen an eine Datenschnittstelle für Drittdienste, Finale Version, 26.02.2016, https://die-dk.de/media/files/2016-02-22_DK_-_Whitepaper_-_Requirements_data_interface_final_1.2_de.pdf

[EBA-RTS] European Banking Authority: Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2), 23 February 2017, http://www.eba.europa.eu/documents/10180/1761863/Fnal+draft+RTS+on+SCA+and+CSC+ under+PSD2+%28EBA-RTS-2017-02%29.pdf

[EN319132-1] ETSI EN 319 132-1: Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures, V1.1.1, 2016, http://www.etsi.org/deliver/etsi_en/319100_319199/31913201/01.01.01_60/en_31913201v010101p.pdf

[EN319412-1] ETSI EN 319 412-1: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures, Version 1.1.1, 2016, http://www.etsi.org/deliver/etsi_en/319400_319499/31941201/01.01.01_60/en_31941201v010101p.pdf

[EN319412-3] ETSI EN 319 412-3: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons, Version 1.1.1, 2016, http://www.etsi.org/deliver/etsi_en/319400_319499/31941203/01.01.01_60/en_31941203v010101p.pdf

[HüRZ10] D. Hühnlein, H. Roßnagel, J. Zibuschka: Diffusion of Federated Identity Management, Sicherheit 2010, S. 25-36, http://www.ecsec.de/pub/Sicherheit2010.pdf

[HSW+12] D. Hühnlein, J. Schmölz, T. Wich, B. Biallowons, M. Horsch & T. Hühnlein: Standards und Schnittstellen für das Identitätsmanagement in der Cloud, DACH Security 2012, http://www.ecsec.de/pub/2012_DACH_IdM.pdf, (2012)

[HWSH14] D. Hühnlein, T. Wich, J. Schmölz, H.-M. Haase: The evolution of identity management using the example of web-based applications, it - Information Technology 56(3): S. 134-140, http://ecsec.de/pub/2014_IT.pdf, (2014)

[Hühn08] D. Hühnlein: Identitätsmanagement – Eine visualisierte Begriffsbestimmung, Datenschutz und Datensicherheit (DuD), S. 163-165, 2008, http://www.ecsec.de/pub/2008_DuD_Glossar.pdf

[ISO20022] ISO 20022: Financial services – Universal financial industry message scheme, Part 1-8

[OIDC] N. Sakimura, J. Bradley, M. Jones, B. de Medeiros, C. Mortimore: OpenID Connect Core 1.0, November 8, 2014, http://openid.net/specs/openid-connect-core-1_0.html

[OID-FAPI] N. Sakimura, A. Saxena, A. Nadalin: OpenID Financial API (FAPI) WG, http://openid.net/wg/fapi/, (2017)

[OpBa-RW] Open Banking Ltd.: Read/Write APIs, Version 1.0.0, https://www.openbanking.org.uk/read-write-apis/

[PrSt10] ProSTEP iViP: PSI 7 Recommendation, Enterprise Rights Management, Annex B, Cross-Enterprise-ID – Technical Recommendation, 2010, http://www.prostep.org/fileadmin/freie_downloads/Empfehlungen-Standards/ProSTEP_iViP/PSI_SP2_7_0.9_Annex_B.pdf

[RFC6749] D. Hardt: The OAuth 2.0 Authorization Framework, IETF RFC 6749, (2012)

[RFC7515] M. Jones, J. Bradley, N. Sakimura: JSON Web Signature (JWS), IETF RFC 7515, (2015)

[RFC7522] B. Campbell, C. Mortimore, M. Jones: Security Assertion Markup Language (SAML) 2.0 Profile for OAuth 2.0 Client Authentication and Authorization Grants, IETF RFC 7522, (2015)

[RFC7523] M. Jones, B. Campbell, C. Mortimore: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants, IETF RFC 7523, (2015)

[RFC7800] RFC 7800: M. Jones, J. Bradley, H. Tschofenig: Proof-of-Possession Key Semantics for JSON Web Tokens (JWTs), (2016)

[RoBe17] Roland Berger: Successfully navigating changes to payments regulation, Payment Services Directive 2 – A strategic and technological challenge, 2017, https://www.rolandberger.com/publications/publication_pdf/roland_berger_payment_services_directive_2_final.pdf

[SAML2] S. Cantor, J. Kemp, R. Philpott, E. Maler: Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0., https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf, (2005)

[SAML-Bind] S. Cantor, F. Hirsch, J. Kemp, R. Philpott, E. Eve Maler: Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, https://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf, (2005)

[WSS-SAML] R. Monzillo, C. Kaler, A. Nadalin, P. Hallam-Baker, C. Milono: Web Services Security SAML Token Profile Version 1.1.1, OASIS Standard, http://docs.oasis-open.org/wss-m/wss/v1.1.1/wss-SAMLTokenProfile-v1.1.1.pdf, (2012)

[X.520] Recommendation ITU-T X.520 (10/2012): Information technology – Open Systems Interconnection – The Directory: Selected attribute types