CORE®

PUBLIC HEARING DER EBA

Zu starker Authentifizierung und sicherer Kommunikation im Rahmen der PSD II

Holger Friedrich
Dr. Waldemar Grudzien

30. September 2016
COREtechmonitor | Blogpost

Key Facts

- EBA schärft wesentliche Aspekte des RTS (Regulatory Technical Standards) zu starker Kundenauthentifizierung und sicherer Kommunikation im bargeldlosen Zahlungsverkehr
- Diskussion I: SCA (Starke Kundenauthentifizierung) nur einmalig im Monat bei AISP (Kontoinformationsdienst-Providern)
- Diskussion II: Stärkung SCA
- Bestätigung: Nutzung PSD II-Schnittstelle verpflichtend für TPPs (Drittdienstleister) (Screen Scraping verboten)
- Fazit: Stärkung SCA setzt keine direkten Impulse für RBA-Technologien frei, auch wenn auf Synergien für andere Anwendungsfälle (z.B. digitale Identität im Rahmen eIDAS) hingewiesen wird

Report

1. KONTEXT

Am 23. September 2016 fand die öffentliche Anhörung der EBA zum RTS „Regulatory Technical Standards specifying the requirements on strong customer authentication and common secure communication under PSD II“ statt. Als regulärer Bestandteil der Konsultationsphase bietet die öffentliche Anhörung regelmäßig eine Zusammenfassung der ersten Konsultationsphase und einen Ausblick auf die zu erwartende Ausprägung der RTS. Ausgehend von den Kernpunkten der Ausgestaltung der RTS, die sich in dem im August 2016 veröffentlichten Konsultationspapier widerspiegeln [vgl. Post „Kundenauthentifizierung im bargeldlosen Zahlungsverkehr: Auswirkungen des neuen RTS (Regulatory Technical Standards) im Kontext PSD II“], werden nachfolgend die wesentlichen Diskussionspunkte der Anhörung dargestellt.

Die Kernpunkte der Ausgestaltung und die Diskussionspunkte können als Zwischenstand der Detaillierung der PSD II zu den zwei Aspekten (1) starke Kundenauthentifizierung und (2) sichere Kommunikation im bargeldlosen Zahlungsverkehr gesehen werden, da der am 12. August veröffentlichte RTS bis zum 12. Oktober 2016 kommentiert werden kann. Die EBA plant die Veröffentlichung des finalen Entwurfs des RTS für das erste Quartal 2017. Gleichwohl stellen die im Rahmen des bisherigen Prozesses gegebenen Verlautbarungen der EBA eine gewichtige Meinungsäußerung dar, die ggf. Eingang in den finalen RTS finden könnten. Die wichtigsten Einlassungen werden im Folgenden vorgestellt und initial bewertet.

2. EINLASSUNGEN DER EBA IM DETAIL

Die PSD II ist in ihren grundlegenden Aussagen nicht durch die EBA zu verändern, wie sie in der Anhörung mehrfach deutlich machte. Das Mandat der EBA bezieht sich auf die Ausgestaltung regulatorisch-technischer Richtlinien für ausgewählte Aspekte zur Umsetzung der PSD II.

Wesentlich in der aktuellen Diskussion sind neben den Abläufen zur starken Kundenauthentifizierung und der Sicherung der Vertraulichkeit und Integrität der User Cre

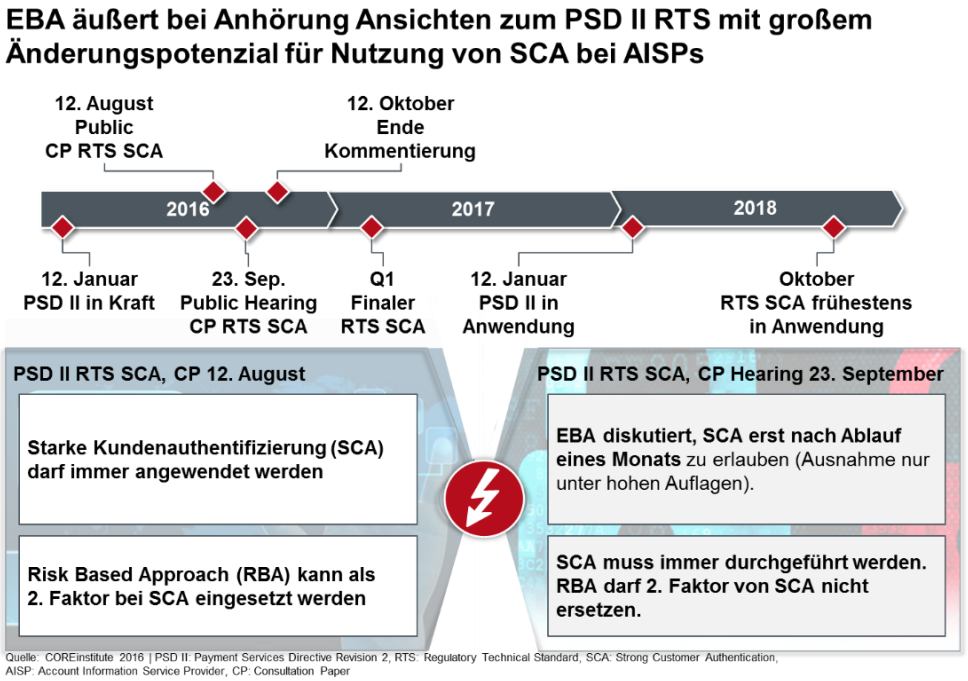

Abbildung 1: Ansichten der EBA zur Anwendung von Ausnahmeregeln zum SCA bei AISPs nach Anhörung am 23. September i.V.m. RTS SCA Entwurf vom 12. August

dentials die Regelungen zu den Ausnahmen von der starken Kundenauthentifizierung. Bisher galt die Regel, eine starke Kundenauthentifizierung (SCA = Strong Customer Authentication) immer anwenden bzw. anfordern zu können für den Abruf von Kontoinformationen. Nach neuem Diskussionsstand würde sich dies ändern: Eine SCA dürfte erst nach Ablauf eines Monats erneut angefordert werden. Der frühere Einsatz von SCA wäre nicht erlaubt. Für die Durchführung einer SCA zu einem früheren Zeitpunkt werden den Instituten hohe Hürden auferlegt. Die EBA bittet um Kommentierung dieser Idee.

Eine grundsätzliche Änderung erfahren hat die Bewertung des risikobasierten Ansatzes im Rahmen der Kundenauthentifizierung. Bis zur Anhörung durfte eine kontoführende Bank jeden Kontozugriff stark authentifizieren, konnte aber auch auf SCA verzichten und für den zweiten Faktor nur RBA anwenden. In der Diskussion im Hearing machte die EBA deutlich, dass auch der zweite Faktor gar nicht mehr über RBA realisiert werden kann. Die EBA begründet ihre Ansicht mit zwei Argumenten:

1. Verletzung des level playing field: Ein mögliches Szenario wäre, dass die kontoführende Bank nur Prüfungen nach RBA durchführt, während sie von TPPs (Third Party Provider) SCA verlangen und diese damit benachteiligen
2. Schadensquote im Onlinebanking: Nach Einschätzung der EBA reicht der risikobasierte Ansatz nicht aus, um nachhaltig Schäden im Onlinebanking niedrig halten oder reduzieren zu können. Als Evidenz für diese Einschätzung bezieht sich die EBA einzig auf „einige kleine Händler und einige Länder“.

Zur Schnittstelle für TPPs bestätigte die EBA ihre Auffassung hinsichtlich der mandatorischen Nutzung einer Bankenschnittstelle für TPPs. Demnach müssen TPPs eine durch

die Bank zur Verfügung gestellte Schnittstelle für die PSD II-Funktionen PISP, AISP und PIISP verwenden und dürfen keine anderen Zugangswege wie Screen Scraping nutzen. Die Schnittstelle muss die gleiche Funktionalität bieten und die gleichen Daten zur Verfügung stellen wie das Onlinebanking über Webbrowser.

3. FAZIT

Durch das jüngste Hearing der EBA zum RTS der SCA wurden über die Schärfung der PSD II hinaus zwei wesentliche Änderungen in die Diskussion eingebracht: Durchführung SCA nicht vor Ablauf eines Monats, keine Anwendung RBA für zweiten Faktor der SCA.

Sollten Banken Ausnahmeregelungen zu SCA für Kontoinformationsdienste nicht nutzen dürfen, wird das unserer Ansicht nach Auswirkungen auf die Convenience und Sicherheit im Banking und im bargeldlosen Zahlungsverkehr haben.

Der Bedeutungsverlust von RBA könnte nicht nur zu einem Rückgang bei der Nutzung, sondern auch bei der Forschung zu RBA in Europa führen. Darunter würden auch zukunftsweisende Technologien wie Device Fingerprinting, Behaviour Analytics und Biometrie leiden. Die Stärkung der SCA gegenüber der RBA setzt keine direkten Impulse für RBA-Technologien frei, auch wenn auf Synergien für weitere Anwendungsfälle (z.B. im Kontext eID) durch die EBA hingewiesen wird.

Sources

EBA, 2016

https://www.eba.europa.eu/news-press/calendar?p_p_auth=5HgT-FilL&p_p_id=8&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&_8_struts_action=%2Fcalendar%2Fview_event&_8_eventId=1548209

EBA, 2016

https://www.eba.europa.eu/-/eba-consults-on-strong-customer-authentication-and-secure-communications-under-psd2

COREtechmonitor, 2016
http://www.coretechmonitor.com/de/auswirkungen-rts-psd-ii/

Holger Friedrich ist Managing Director bei CORE. Er verfügt über 20 Jahre Beratungserfahrung im Bankensektor, wo er u.a. die Leitung der Planung und Implementierung der IT-Ziellandschaft bei der Fusion zweier Banken übernahm. Zuletzt verantwortete er die Konzeption eines IT-Programms im Großkundengeschäft zur Ablösung verschiedener Investment-Banking-Systeme durch eine moderne OTC-Plattform.

Mail: holger.friedrich@coretransform.com

Dr. Waldemar Grudzien ist Transformation Engineer bei CORE und verfügt über langjährige Erfahrung in einem nationalen Verband des Finanzsektors, wo er den Bereich Retail Banking und Banktechnologie verantwortete. Dabei fokussierte er sich hauptsächlich auf die Sicherheitsregulierungen der Finanzindustrie und deren technologische Auswirkungen auf IT-Infrastrukturen.

Mail: waldemar.grudzien@coretransform.com

COREinstitute
Am Sandwerder 21-23
14109 Berlin | Germany
www.coreinstitute.org
Phone: +49 30 16344 020
office@coreinstitute.org

COREtransform GmbH
Am Sandwerder 21-23
14109 Berlin | Germany
www.coretransform.de
Phone: +49 30 26344 020
office@coretransform.de

COREtransform GmbH
Limmatquai 1
8001 Zürich | Helvetia
www.coretransform.ch
Phone: +41 442 610 143
office@coretransform.ch

COREtransform Ltd.
One Canada Square
London E14 5DY | Great Britain
www.coretransform.co.uk
Phone: +44 203 319 0356
office@coretransform.co.uk