PSD2 API Solution - Contingency Measures (Fallback)

Addressees:

Business Analysts, Project Managers, Developers, Architects, IT

Authors:

Lars Kieffer, David Schneider, Martin Bierkoch, Bernhard Walliser

Version, date

Version 1.0, June 12th, 2019

Copyright

CREALOGIX (Germany) AG
Breitscheidstraße 10
70174 Stuttgart

www.crealogix.com

Table of Contents

List of figures

Document history

Version	Description (remarks)	Date	Author(s)
0.9	First draft	May 29th, 2019	Lars Kieffer, David Schneider
1.0	Version 1.0	June 12th, 2019	Martin Bierkoch, Bernhard Walliser

1 Introduction

This document describes how TPPs can connect within the contingency measures (fallback) scenario of the PSD2 Solution of Deutsche Kreditbank (DKB) according to RTS Article 33.

The document assumes that you have basic knowledge about Payment Services Directive 2 (PSD2) regulation of the European Union, its terminology and use cases. Please refer to the References section below for an overview and detailed information about the regulation. In addition, you will also find a Glossary below with the most important PSD2 terms. Furthermore, this document assumes that you have read the Functional description of the PSD2 API Solution and the TPP documentation.

2 Description

TPPs uses the DKB regular User Interface (UI) to connect their services.

2.1 Login

Therefore, there will be a separate login form (https://www.dkb.de/Welcome/loginTPPs.xhtml). The TPP will login with the credentials of the PSU. The login form for TPPs consists of the fields “j_username”, “j_password”, “tpp_certificate” and the send button with the id “buttonLogin”. In the field “tpp_certificate” the certificate is expected as a qualified certificate for website authentication (QWAC) in PEM format. The TPP must upload the certificate with every login.

2.2 TPP certificate validation

The certificate will be validated against the trust center where the certificate was issued. The certificate status will be checked and if the role(s) that are included in the certificate are valid.

The certificate validation relies on the official ETSI TS 119 495 standard for QWAC certificate which is based on eIDAS. QSeals are not supported.

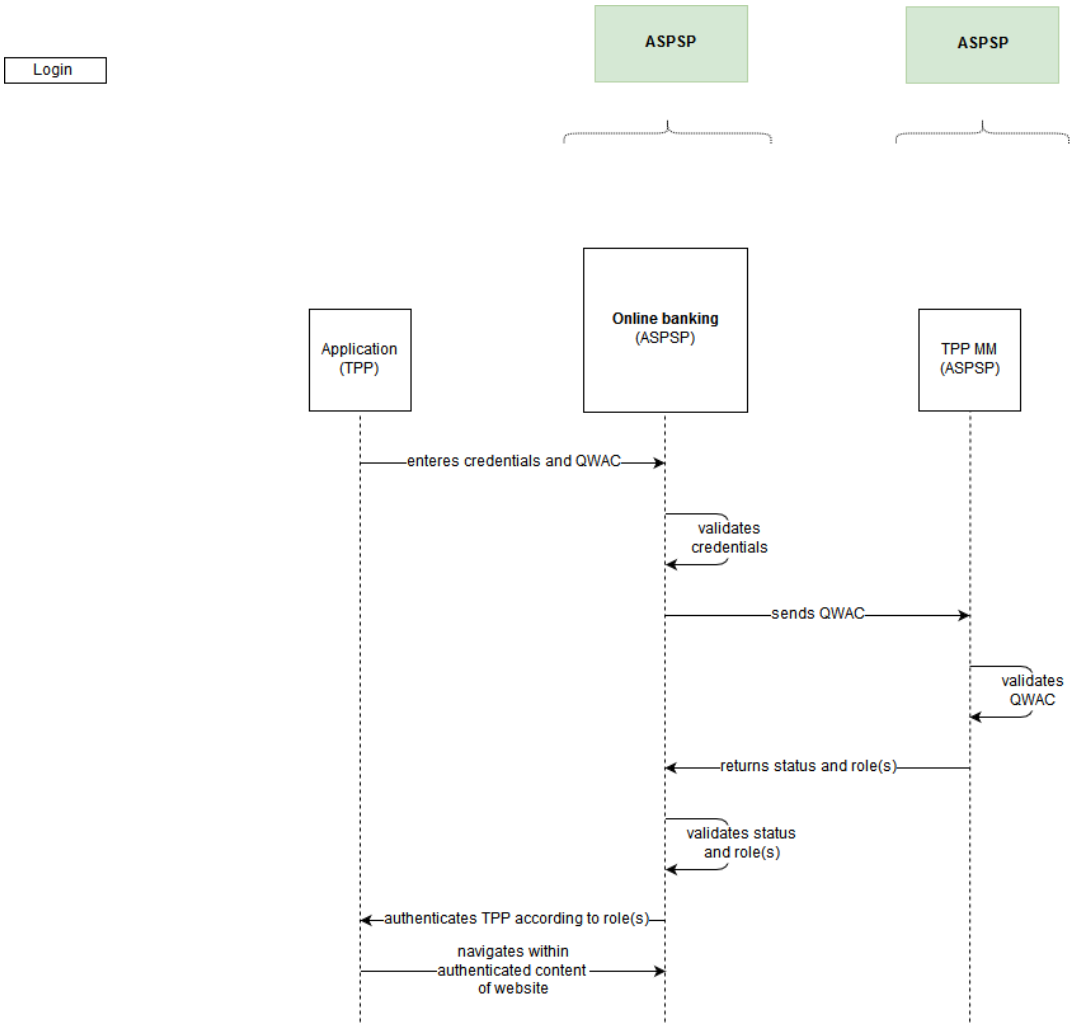

Figure 1 - Workflow Login

After a successful login the TPP can act like the PSU on the UI within the online banking.

2.3 Strong Customer Authentication

The Strong Customer Authentication (SCA) is necessary for each login. The possible SCA methods are chipTAN and TAN2go.

2.3.1 chipTAN

Within chipTAN SCA only manual input is supported. The description (paragraph with the id “chipTANmanual”) on how to use the TAN-Generator is displayed on the following page after the login form. There will be a form (“submitChipTAN”), an input field “tan” and a submit button with the id “submitTan”.

2.3.2 TAN2go

For TAN2go the following page after the login form consists of a form (“submitTAN2go”), an input field “tan” and a submit button with the id “submitTan”.

2.3.3 SCA confirmation

After a successful SCA confirmation the TPP is redirected to the page https://www.dkb.de/DkbTransactionBanking/content/banking/financialstatus/FinancialComposite/FinancialStatus.xhtml?$event=init.

3 References

Description	Hyperlink
Short introduction to PSD2 by Berlin Group Initiative	https://docs.wixstatic.com/ugd/c2914b_c6a8a0dca83e4af8859be266415d3d79.pdf
Directive (EU) 2015/2366 of the European parliament and of the council on payment services in the internal market (PSD2) of 25 November 2015	English: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366 German: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32015L2366
Regulatory Technical Standards on strong customer authentication and secure communication under PSD2 (RTS)	English: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2
Commision delegated regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication	English: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2018:069:TOC German: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=OJ:L:2018:069:TOC
Consultation on RTS specifiying the requirements on strong customer authentication and common and secure communication under PSD2	English: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2/-/regulatory-activity/consultation-paper
Discussion on RTS on strong customer authentication and secure communication under PSD2	https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2/-/regulatory-activity/discussion-paper
EBA Fallback document	https://eba.europa.eu/-/eba-publishes-final-guidelines-on-the-exemption-from-the-fall-back-mechanism-under-the-rts-on-sca-and-csc

NextGenPSD2 Access to Account Interoperability Framework (Berlin Group Standard) • Documentation • Technial documentation / API description • OpenAPI File	https://www.berlin-group.org/nextgenpsd2-downloads
WSO2 API Manager	Description: https://wso2.com/api-management/ Documentation: https://docs.wso2.com/display/AM250/WSO2+API+Manager+Documentation
WSO2 Analytics	https://docs.wso2.com/display/AM250/Analytics
WSO2 Admin Guide	https://docs.wso2.com/display/AM250/Product+Administration

4 Glossary

PSD2 abbreviation	Meaning	Usage
2FA	Two Factor Authentication	
AIS	Account Information Service according to article 4 (16) of [PSD2] and as regulated by article 67 of [PSD2].	This service may be used by an AISP to request information about the account of a PSU. The account is managed by the ASPSP providing the XS2A Interface. Functionality and restrictions of this service comply with the requirements defined by article 67 of [PSD2].
AISP	Account Information Service Provider offering an AIS to its customer. See article 4 (19) of [PSD2].	
ASPSP	Account Servicing Payment Service Provider providing and maintain a payment account for a payer. See article 4 (17) of [PSD2]. For example a bank.	
FCS	Fund confirmation service	This service may be used by a PIISP to request a confirmation of the availability of specific funds on the account of a PSU. The account is managed by the ASPSP providing the XS2A Interface. Functionality and restrictions of this service comply with the requirements defined by article 65 of [PSD2].
eIDAS	**e**lectronic **ID**entification, **A**uthentication and trust **S**ervices is an EU regulation on electronic identification and trust services for electronic transactions in the internal market. It is a set of standards for electronic identification and trust services for electronic transactions in the European Single Market. It was established in EU Regulation 910/2014 of 23 July 2014 on electronic identification and repeals directive 1999/93/EC from 13 December 1999.	
MVP	Minimum Viable Product	Focus on scope in agile development
NA/NCA	National (Competent) Authority. Holds a list of TPPs registered in that particular country.	
PIS	Payment Initiation Service according to article 4 (15) of [PSD2] and as regulated by article 66 of [PSD2].	This service may be used by a PISP to initiate a single payment on behalf of a PSU using a given account of that PSU. The account is managed by the ASPSP providing

		the XS2A Interface. Functionality and restrictions of this service comply with the requirements defined by article 66 of [PSD2].
PISP	Payment service provider offering a PIS to its customer. See article 4 (18) of [PSD2].	
PIISP	Payment Instrument Issuer Service Provider according to article 4 (14) and 45) of [PSD2]. A PIISP can use the service "Confirmation on the availability of funds" as regulated by article 65 of [PSD2].	
PSU	Payment Service User according to article 4 (10) of [PSD2].	
QTSP	Qualified Trust Service Provider, e. g. a trust centre issuing qualified certificates. German: Vertrauensdiensteanbieter (eIDAS)	
SCA	Strong Customer Authentication – authentication procedure based on two factors compliant with the requirements of [PSD2] and [EBA-RTS].	
TPP	Third Party Provider – generic term for AISP/PIISP/PISP.	
TSP/QTSP	Trust Service Provider according to [eIDAS]. Within the context of the XS2A interface specification only qualified TSPs (QTSPs) according to section 3 of [eIDAS] issuing qualified certificates for electronic seals and/or qualified certificates for website authentication which are compliant with the requirements of [EBA-RTS] are relevant.	
XS2A	Access to account interface – interface provided by an ASPSP to TPP for accessing accounts.	
QSealC	Qualified Electronic Seal Certificates	
QWAC	Qualified Website Authentication Certificates	