NextGenPSD2 Overview

Introduction

The majority of European ASPSPs wish to provide a dedicated API interface to meet their PSD2 commitments and in order to avoid the provision of a fall-back solution, they must release compliant test versions of their PSD2 APIs by March 14th, 2019.

That's a short time frame to meet a fairly complex challenge but by committing to a solid foundational solution now, organizations both minimise the risk of missing important regulatory deadlines as well as positioning themselves to benefit from the significant opportunity that Open Banking, and Open APIs more generally, offer.

The Identity and Access Management challenges PSD2 presents can be divided into two categories: the provision of **Strong Customer Authentication** (SCA) and the delivery of **Open APIs**.

Strong Customer Authentication

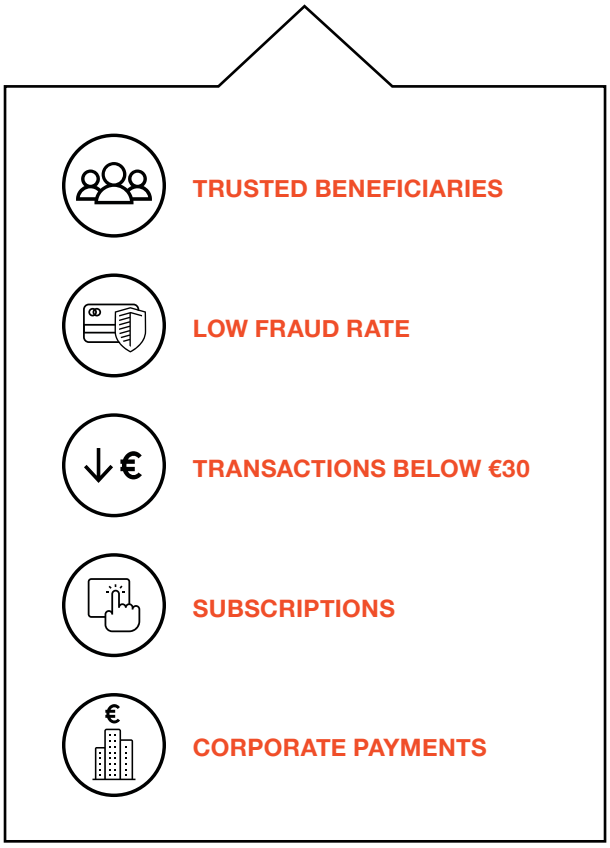
PSD2 mandates that SCA is enforced for new services it introduces as well as for some existing customer journeys. **Examples include:**

- ✓ Authorizing the sharing of data with a TPP
- ✓ Online access to some account transaction data
- ✓ Cardholder not present online payments
- ✓ Online Modification of key personal data such as address

SCA is defined as an authentication based on the use of at least two of the following factors:

SCA Exemptions

A number of interactions are exempt from the SCA requirement so it is not sufficient to enforce a blanket security policy. A PSD2 solution must be able to apply policy to determine when SCA is required in order to minimise customer friction.



Open APIs

To comply with PSD2, financial organizations are making their **payment** and **account** APIs accessible to TPPs. Examples include:

✓ Initiating payments from a bank account (PISP)

✓ Viewing bank account transaction data (AISP)

These Open API flows often require **SCA**, but not always. For example, within an AISP flow, data sharing with a TPP mandates SCA only the first time in a 90-day period.

The NextGenPSD2 Specification

The Berlin Group is leading the way in mainland Europe in providing a standard that addresses many of the demands of PSD2 and has published the NextGenPSD2 Specification. NextGenPSD2 primarily focuses on defining the interfaces a TPP will use, the technical characteristics of those interfaces, and the security features that protect them.

The security features break down as follows:

✓ **Identification of the TPP by the ASPSP** - based on the use of eIDAS certificates at the transport and application layers

✓ **ASPSP identification by the TPP** - achieved using transport layer security

✓ **Authentication of the PSU with SCA** - with associated policy to limit friction

✓ **Protection of data using encryption** - based on TLS

✓ **Detection and prevention of fraud** - based on PSU device data and other signals

Different Approaches to SCA: The NextGenPSD2 Specification details four approaches to implementing SCA security flows: Redirect, OAuth, Decoupled, and Embedded. The ASPSP determines which of these approaches it will make available to the TPP. ForgeRock provides full support for all of these approaches and has the inbuilt capability to handle the variable scopes mandated by the OAuth variant in particular.

Just Comply or Truly Compete?

Financial organizations must decide to simply comply with the PSD2 regulation or use it as a springboard to compete in the new Open API economy.

ForgeRock firmly believes that in the near future, the quality of your PSD2 implementation and broader API offering will be a determining factor for customers choosing a bank. As TPPs begin to offer innovative services using banking APIs, customers will start to expect the ability to make use of these third-party services. Additionally, there is the scope to monetize non-mandatory APIs.

As such, your provision of these services must be robust and flexible. Develop a transformative user experience for your customers that enables them to control who can access their data and what can be done with it.

ForgeRock for NextGenPSD2

The ForgeRock platform addresses the challenges presented by PSD2 and provides a solid foundation for the NextGenPSD2 Specification.

Strong Customer Authentication

ForgeRock Intelligent Authentication addresses the balance between the need for simple administration of secure, risk-aware authentication scenarios, while maintaining a low friction login experience for your customers. An intuitive tree-based approach supports plugin nodes from the ForgeRock Marketplace provided by our technology partners. Using such nodes, you can easily integrate with a range of multi-factor authentication services.

With Authorization Policy, PSD2 exemptions can be defined and managed centrally, ensuring that SCA is only enforced when it is required.

Redirect, OAuth, Decoupled, and Embedded flows can be supported by using the ForgeRock platform comprehensive REST API framework.

/ NextGenPSD2

- ✓ **Authentication of the PSU with SCA**
- ✓ **Detection and prevention of fraud**

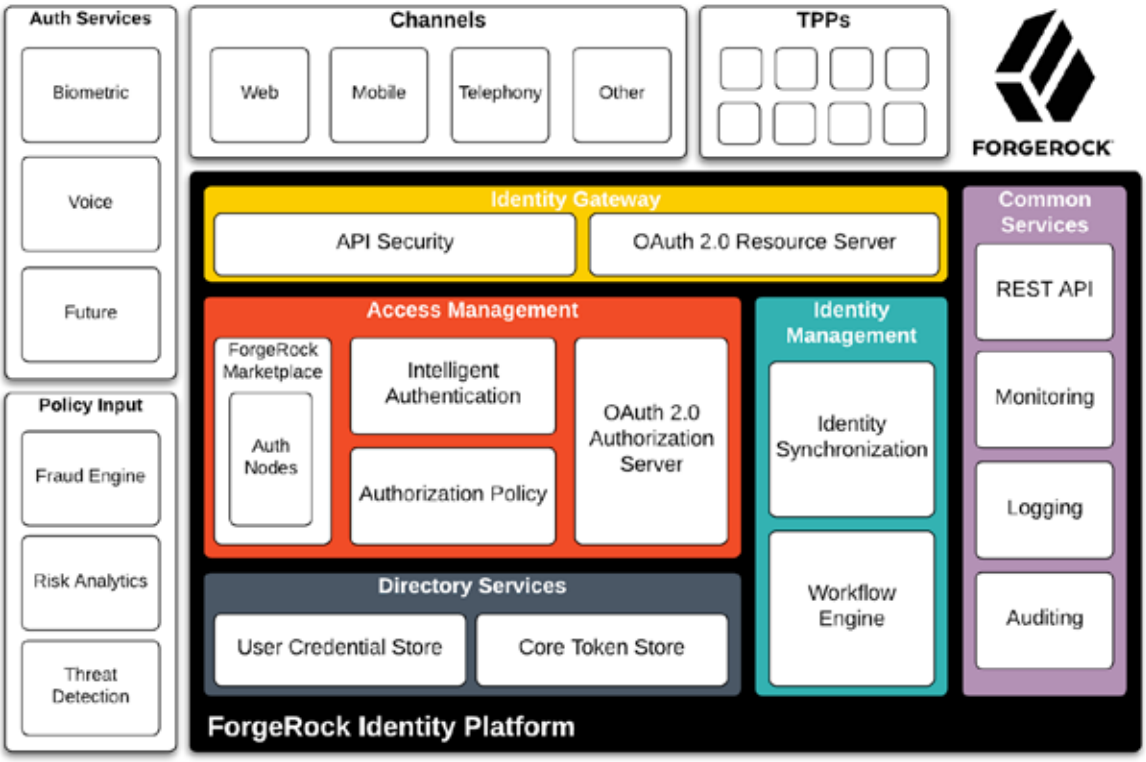
Open APIs

Payment and account APIs can be made available securely through the use of the ForgeRock Identity Gateway, which can protect APIs by exposing them as an OAuth 2.0 Resource Server. Identity Gateway can be rapidly integrated with the ForgeRock OAuth 2.0 Authorization Server and Authorization Policy to ensure that SCA has been achieved before permitting access to APIs.

Identity Gateway can also be configured to enforce the use of eIDAS certificates to identify TPPs and secure the transport layer.

/ NextGenPSD2

- ✓ **Identification of the TPP by the ASPSP**
- ✓ **ASPSP identification by the TPP**
- ✓ **Protection of data using encryption**



TPP and Consent Management

The onboarding, management, and, if required, removal of TPP access is crucial. ForgeRock Data Synchronization and Workflow Engine allows you to define a structure for managing TPP data and business governance processes for the approval of TPPs, which would include checks against combined National Competent Authority directories.

Availability, Scale and DevOps

The ForgeRock platform is designed to support massive scale in a highly resilient manner. It can be deployed in a fully automated way with elasticity to meet spikes in demand with affordable infrastructure. ForgeRock is ready out of the box to be deployed using Docker and Kubernetes technologies. Helm scripts and examples are provided to get you up and running immediately.

Conclusion

PSD2 presents financial services organizations with a number of complex identity and access challenges to solve. The ForgeRock platform enables organizations to rapidly enable Strong Customer Authentication and deploy Open APIs to implement the NextGenPSD2 Specification. You can both comply with the regulatory deadlines and have the flexible platform you need to compete, today and in the future.

Our UK Open Banking Experience

Here at ForgeRock, we have been involved in Open Banking long before the PSD2 RTS was ratified. We provide the leading UK Open Banking reference ASPSP and were the first vendor to provide a certified compliant platform. We are committed to providing the reference bank through to V4 of the standard when it will fully align with PSD2. We also host a sandbox directory that allows TPPs not yet approved by the regulators to be able to participate in the Open Banking development ecosystem.

Our customers include HSBC, Lloyds, Allianz, BNP Paribas, BinkBank, Bayern LB, Vantive and more. With some of the largest banks in the world as our customers, support for hackathons, participation in industry events and engagement with the standards bodies we are uniquely placed to bring that wealth of experience to PSD2 in Europe.

Glossary

AISP: Account Information Service Provider
ASPSP: Account Servicing Payment Services Provider
API: Application Programming Interface
PISP: Payment Initiation Service Provider
PSD2: Second Payment Services Directive
SCA: Strong Customer Authentication
TPP: Third Party Provider

/ABOUT FORGEROCK

ForgeRock®, the leader in digital identity management, transforms how organizations build trusted relationships with people, services, and things. Monetize customer relationships, address stringent regulations for privacy and consent (GDPR, HIPAA, Open Banking, etc.), and leverage the internet of things with ForgeRock. We serve hundreds of brands, including Morningstar, Vodafone, GEICO, Toyota, and Pearson, as well as governments like Norway and Canada.