ForgeRock®

Overview

Consumer Data Right (CDR) Open Banking

Introduction

As deadlines for compliance with Consumer Data Rights (CDR) regulations rapidly approach, most Australian banks face the challenge of meeting those requirements while finding and implementing the right solutions for the long term. Most wish to deploy a dedicated application programming interface (API) to open up new offerings. In order to effectively comply and compete in today's market, they need a solution that minimises risk yet allows them to benefit from the significant opportunity that open application programming interfaces (APIs) offer.

Critical to complying with CDR is the ability to provide open APIs that allow customer account data – transactions, balances, and so forth - to be shared securely with a third-party Data Recipient. To do so requires an identity and access management (IAM) solution that enables secure sharing of consumer data in three primary categories: multi-factor authentication, consent, and consent management flows, and the delivery of open APIs.

Knowledge

Possession

Inherence

Multi-Factor Authentication

CDR mandates that multi-factor authentication (MFA), in the form of a one-time password (OTP), be enforced during authentication and prior to the gathering of customer consent.

Examples of where MFA is required now, and will possibly be required in the future, include:

- Authorising the sharing of data with a Data Recipient
- Managing of consent
- Online access to some account transaction data
- Online modification of key personal data, such as mobile phone number, home, and delivery address

Consent and Consent Management Flows

Data Holders are required to confirm that a customer has granted consent to the data being shared with the Data Recipient. To achieve this, the Data Holder must:

- Allow customers to authorise a third-party (the Data Recipient) to access their data
- Authenticate and verify the third-party is who they claim to be
- Enable security APIs to understand and implement the data access provided in the consent

In essence, these requirements are a means of establishing and maintaining both **consent** and **trust**, critical tenants of CDR Open Banking and Open APIs.

Secure gathering of customer consent

Simple and low friction consent journey

Rich and intuitive consent management dashboard

Automated and manual revocation of consent

Secure, flexible & future proof consent data model

Open APIs

To comply with CDR Open Banking, financial organisations will make their account APIs accessible to Data Recipients. Examples include:

- Viewing customer details, direct debits and scheduled payments
- Viewing bank account transaction data

These Open API flows will require authorisation based on the consent provided by the customer.

Open Banking

For Open Banking, CDR specifications primarily focus on defining the interfaces a Data Recipient will use, the technical characteristics of those interfaces, and the security features that protect them.

The security features are as follows:

- First layer of Data Recipient identification by the Data Holder based on the use of MTLS (Mutual Transport Layer Security) certificates
- Second layer of Data Recipient identification by the Data Holder based on the SSA (Software Statement Assertion) provided by the ACCC Registry
- Authentication of the customer with MFA, with associated policy to limit friction
- Protection of data using encryption based on transport layer security (TLS)
- Detection and prevention of fraud based on customer device data and other signals

Different Approaches to Authentication

The CDR specification currently details two approaches to implementing authentication security flows: Hybrid OIDC (OpenID Connect) and CIBA (Client Initiated Back-Channel Authentication). Hybrid OIDC is well known and adopted in the industry, with CIBA being newer and less prevalent, but with major advantages to security and the customer journey. The bank determines which of these approaches it will make available to the Data Recipient.

Just Comply or Truly Compete?

Financial organisations must decide to simply comply with the CDR 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 CDR implementations and broader API offerings will be a determining factor for customers choosing a bank. As Data Recipients begin to offer innovative services using banking APIs, customers will start to expect the ability to make use of these third-party services. Additionally, non-mandatory APIs can be monetised.

Provision of these services must be robust and flexible. With a modern IAM platform, financial institutions can develop a transformative user experience for customers that enables them to control who can access their data and what can be done with it.

Intelligent 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 consumers. 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 MFA services.

With fine-grained authorisation policies, CDR exemptions can be defined and managed centrally, ensuring that authentication is only enforced when it is required.

CDR Open Banking

- Authentication of Data Recipients with Multi-Factor Authentication
- Detection and Prevention of Fraud

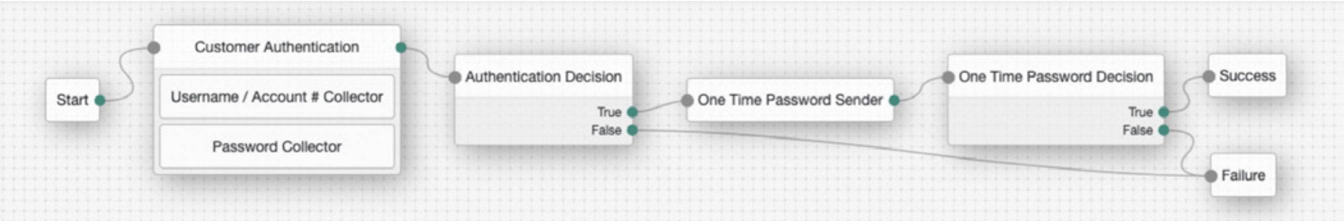
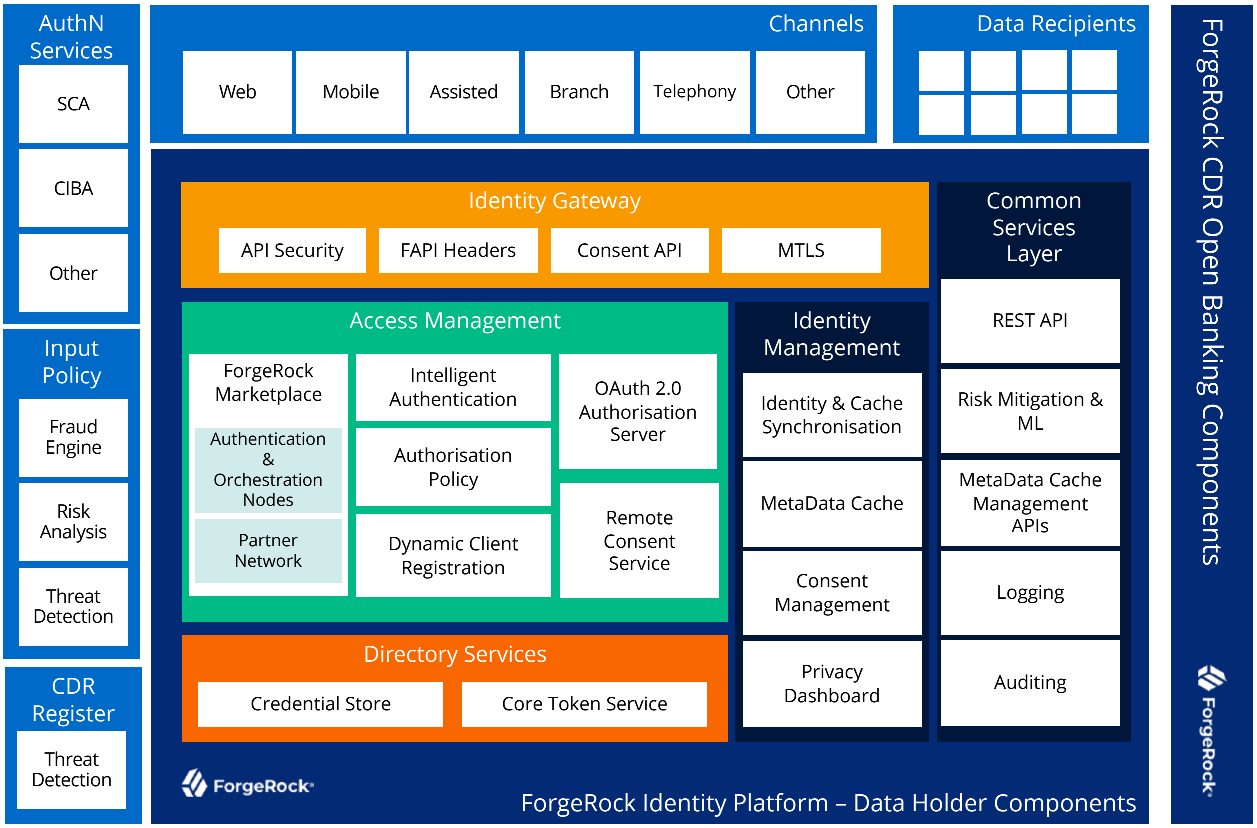


Figure 1. Tree-based Approach



ForgeRock provides full support for both of the OIDC Hybrid and CIBA approaches and can handle the variable scopes mandated by the OIDC variant in particular. ForgeRock also intends to support any emerging technologies that may supersede those currently required by the standard.

A huge advantage of the nodes mentioned above is their flexibility. For instance, should any of the authentication flows, standards, or policies change, it is a simple matter of modifying the authentication journey via a drag-and-drop intelligent journey orchestration.

These orchestration "trees" have numerous additional capabilities. They can reach out to fraud and biometrics engines, as well as monitor and meter authentication to detect bottlenecks and break points, amongst a wealth of other features.

CDR Open Banking

› Identification of the Accredited Data Recipient (third-party service provider) by the Data Holder (Bank)

› Data Holder identification by the Accredited Data Recipient

› Protection of data by encryption

› Scalable, flexible consent engine

› Industry-leading customer journey orchestration capability

Data Holder and Consent Management

The onboarding, management, and, if required, removal of Data Recipient access is crucial. ForgeRock data synchronisation and workflow engine enables you to define a structure for managing Data Holder data and business governance processes for the approval of Data Recipients, which would include checks against combined the Australian Competition and Consumer Commission (ACCC) CDR Registry.

The same workflow engine, fine-grained authorisation, and consent and policy enablement capabilities built into the platform also support the User-Managed Access (UMA) standard. Combined with our cutting-edge graph-like relationship modelling, organisations are able to model, manage, and enforce the lifecycle management of consent.

Ultimately, organisations can leverage a profile and privacy dashboard built to handle the rigors of the General Data Protection Regulation (GDPR). This solution provides a simple and intuitive interface for consumers to manage their consent.

Availability, Scale and DevOps

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

MetaData Cache

The CDR specification states that Data Holders must store a copy of the CDR Registry's Data Recipient details. This includes ADR's Legal Entity Identifier, Data Recipient Brands and Software Products. Further, updates to Data Recipient details must be replicated within 5 minutes of the change occurring in the CDR Register.

ForgeRock provides a number of components to make this tricky requirement a breeze:

- Complete Data Recipient Data Model and MetaData Cache data storage
- Connector to the CDR Registry to handle initial load, updates and ongoing MetaData Cache lifecycle management
- A mock CDR Registry, allowing ForgeRock customers to immediately begin testing their integration with the CDR Registry in their own ecosystem

Conclusion

Open Banking presents financial services organisations with a number of complex identity and access challenges to solve. The ForgeRock platform enables organisations to rapidly enable strong customer authentication and deploy Open APIs to implement the CDR specification. You can both comply with the regulatory deadlines and have the flexible platform you need to compete, today and in the future.

Our Open Banking Experience

ForgeRock is heavily involved in both Open Banking and CDR. In Europe, the leading UK Open Banking reference bank relies on ForgeRock for identity access management and compliance with their Open Banking Regulations. ForgeRock was the first vendor to provide a certified compliant platform. We also host a sandbox directory that enables third-parties not yet approved by the regulators to be able to participate in the Open Banking development ecosystem.

ForgeRock customers include HSBC, Lloyds, Allianz, BNP Paribas, BinkBank, Bayern LB, Vantiv, and more.

With some of the largest banks in the world as customers, participation in industry events, engagement with the standards bodies, and support for hackathons, ForgeRock is uniquely placed to bring that wealth of experience to CDR in Australia.

ForgeRock's Global Experience

› Two of the CMA9 use ForgeRock for Open Banking and PSD2

› Leader in FSI and Banking Open APIs across Europe, Asia, and the US

› Multiple reference sites across Australia and New Zealand

Glossary

ACCC: Australian Competition and Consumer Commission

ADR: Authorised Data Recipient

API: Application Programming Interface

CDR: Consumer Data Right

MFA: Multi-Factor Authentication

OTP: One-Time Password

About ForgeRock

ForgeRock, the leader in digital identity, delivers modern and comprehensive Identity and Access Management solutions for consumers, employees and things to simply and safely access the connected world. Using ForgeRock, more than a thousand global customer organizations orchestrate, manage, and secure the complete lifecycle of identities from dynamic access controls, governance, APIs, and storing authoritative data – consumable in any cloud or hybrid environment. The company is privately held, and headquartered in San Francisco, California, with offices around the world. For more information and free downloads, visit **www.forgerock.com** or follow ForgeRock on social media.

Follow Us

ForgeRock