

Implementing a Scalable Access Management Solution using Amazon Cognito and API Gateway

Description:

XYZ infotech is a blockchain development company and technology solutions provider for the financial world. XYZ infotech enables financial institutions to realize new revenue-generating and operational efficiency use cases.

Their flagship product, XYZ Blockchain, enables financial institutions to be at the forefront of the global adoption of digital assets.

XYZ infotech Blockchain empowers financial institutions to issue, trade, clear, and settle digital assets, all while remaining fully compliant with the strictest regulatory standards.

Scenario:

The XYZ infotech's Engineering team has set out to implement an authentication and authorization module that would secure all application logins and API access in a secured, scalable and cost-effective manner.

Challenge/Requirements:

You identified the following security requirements:

Security Requirement 1: The solution also needed to support integration with Enterprise Identity Providers (IDP) via SAML.

Security Requirement 2: The solution needs to support fine-grained access control and user entitlement management.

Security Requirement 3: The developed APIs should not directly be exposed to the public.

Reference Solution Architecture:

