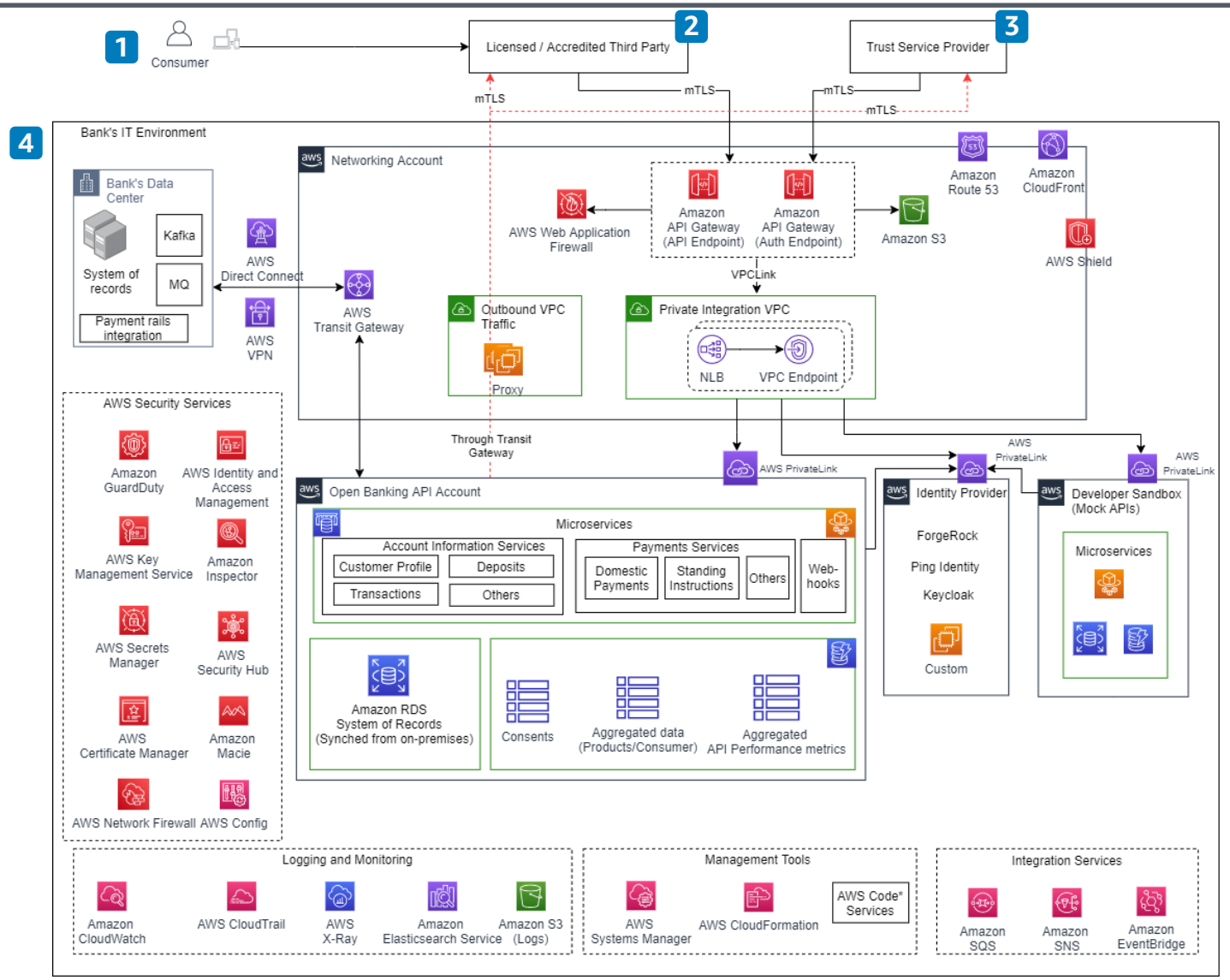
Open Banking on AWS

Use Amazon Web Services to open APIs for third parties and help you implement Open Banking regulations.



Overview

1 A consumer accesses the licensed or accredited third party application - and provides consent to the third party to access consumer data or make a payment submission request.

2 Third parties in Open Banking can be defined as authorized institutions that provide value-added services on top of the consumer's regular banking needs, such as accounts information (balance check, recent transactions, statements) and payments (payment to merchants, people and registered payees). This approach enables use cases such as spend analysis, credit decisioning, payments for ecommerce transactions, and more.

3 A Trust Service Provider (TSP) is a trusted entity authorized by a supervisory government body to verify the authenticity of banks and third parties, and issue digital certificates to third parties.

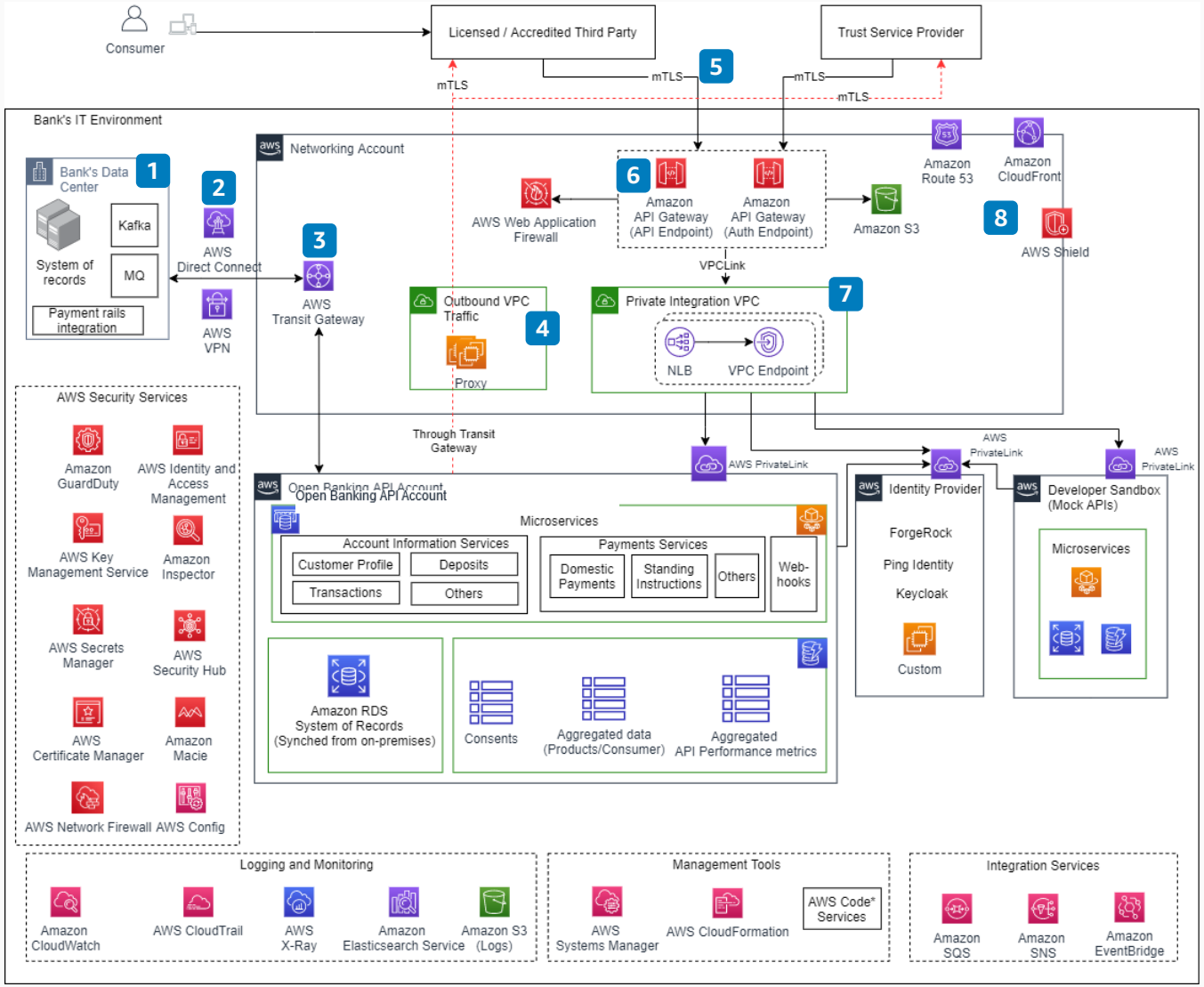
4 A bank's IT environment, comprised of its AWS environment and data centers.

Reviewed for technical accuracy September 7, 2021

AWS Reference Architecture

Open Banking on AWS

Use Amazon Web Services to open APIs for third parties and help you implement Open Banking regulations.



Description (Part 1 of 2)

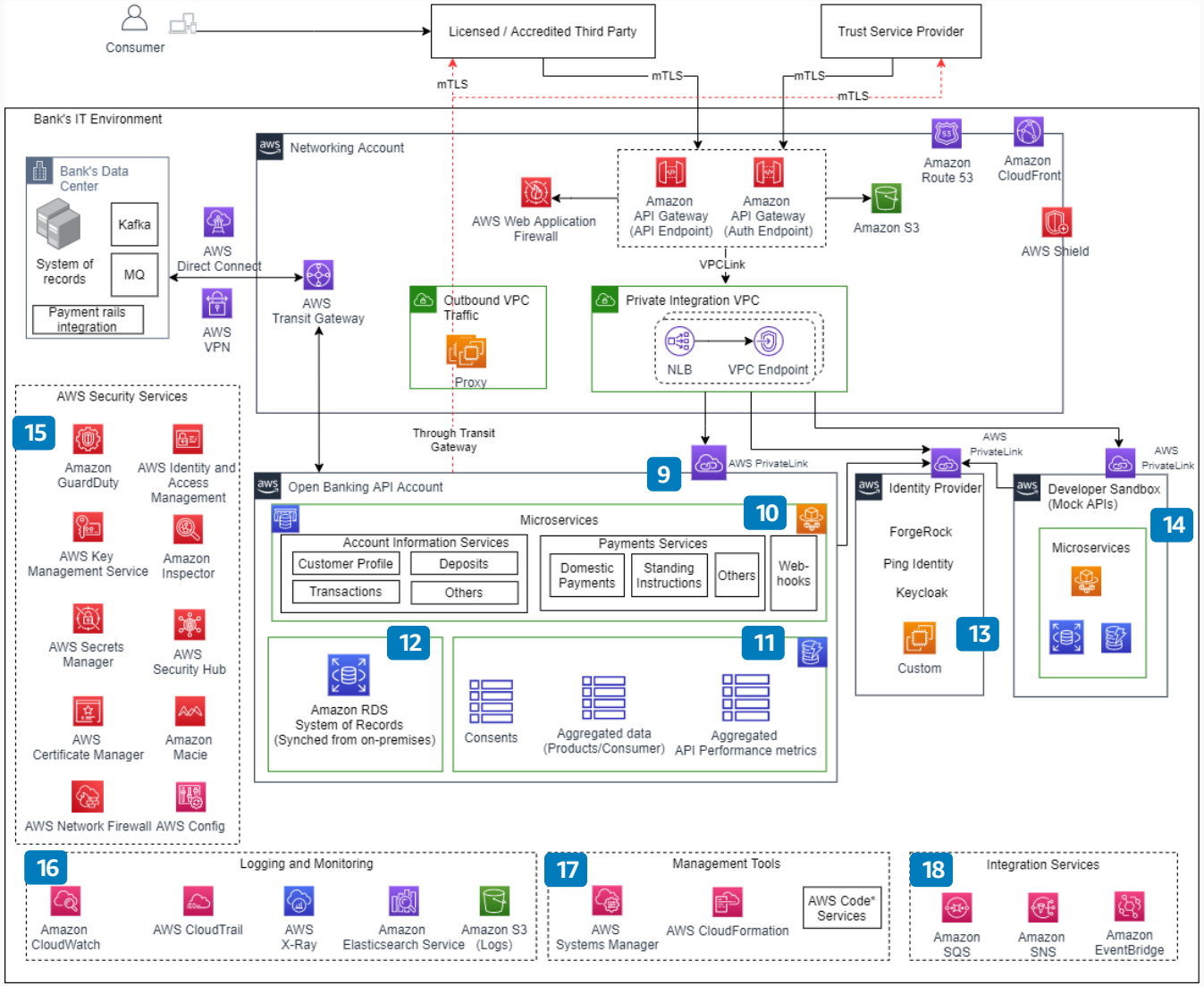
1. Streaming technologies such as Apache Kafka and queueing mechanisms like message queue (MQ) send and receive all new and updated transactions between the core banking systems and AWS.
2. The bank's data center is connected to AWS using a combination of **AWS Direct Connect** and **AWS Site-to-Site VPN**. Two diverse **AWS Direct Connect** connections are recommended for maximum resiliency.
3. **AWS Transit Gateway** serves as the central hub on AWS to manage interconnectivity between workloads running in different AWS accounts. It shares the **AWS Direct Connect** and VPN connection with other workloads in the bank.
4. An outbound VPC provides secure outbound access via a proxy, such as Squid.
5. Mutual TLS (mTLS) provides transport layer security; banks authenticate accredited third parties and provide access tokens to them for calling Open Banking APIs.
6. **Amazon API Gateway** provides the API management layer that exposes open banking APIs and Authorization APIs. **AWS WAF** (Web Application Firewall) integrates with the API Gateway for web protection. **Amazon Simple Storage Service (Amazon S3)** serves as a trust store, where public certificates of clients are stored for validating requests by API Gateway. Additionally, banks perform checks against a TSP to validate the authenticity and status of third parties.
7. API Gateway uses a private integration VPC and **AWS PrivateLink** to connect to the private subnets hosting microservices in other AWS accounts.
8. **Amazon Route 53** provides traffic management and domain name resolution. **Amazon CloudFront** provides a content delivery network (CDN) that banks can use for exposing static data. **AWS Shield** (automatically available with CloudFront) protects against L3/L4 DDoS. **AWS Shield Advanced** (requires sign up) gives additional protection.

Reviewed for technical accuracy September 7, 2021

AWS Reference Architecture

Open Banking on AWS

Use Amazon Web Services to open APIs for Third-parties and help you implement Open Banking regulations.



Reviewed for technical accuracy September 7, 2021

AWS Reference Architecture

Description (Part 2 of 2)

9 **AWS PrivateLink** provides secure private connectivity on the Amazon network between VPCs and services hosted on AWS or on-premises.

10 Open Banking API specifications for Account Information and Payments services are implemented using multiple container-based microservices hosted using **Amazon Elastic Container Service (Amazon ECS) with AWS Fargate**. Caching of customer account information is done using **Amazon ElastiCache**. Webhooks for payment status are hosted in this layer.

11 **Amazon DynamoDB** stores consumer consents, aggregated data, and API performance metrics.

12 **Amazon Relational Database Service (Amazon RDS)** holds a copy of the system of record which is synchronized in near real-time from the bank's core system.

13 Identity provider (IdP) for OAuth 2.0 implementation resides in separate AWS account so that other workloads in the bank can consume it securely. Customers can choose from AWS partners that provide IdP functionality or build a custom IdP.

14 A separate developer sandbox is required for the third party to integrate with the bank's AWS environment and build their products.

15 AWS security services help enhance security posture. For example, **Amazon GuardDuty** monitors for malicious activity and unauthorized behavior; **AWS Security Hub** provides a comprehensive view of security alerts and security posture across AWS accounts. For more guidance, see Best Practices for Security, Identity & Compliance.

16 Logs from all services are collected in **Amazon S3** then analyzed and monitored by **Amazon Elasticsearch Service**.

17 Management tools like **AWS Systems Manager** provide configuration management; **AWS CloudFormation** deploys environment; AWS code services enable CI/CD.

18 **Amazon EventBridge**, **Amazon Simple Queue Service (Amazon SQS)**, and **Amazon Simple Notification Service (Amazon SNS)** provide notification capability between services.