

# Powering Business-critical **Operator Based Search** for Telecom Giant

User authentication and verification has evolved vastly over the years. Using a mobile number to log in to websites, applications, etc. is expected to be default by users. Our customer's key solution does just that. A universal and secure mobile based login solution. One of the key functionalities was to securely search and discover the user's number across various network operators and pass the authentication to the requesting service provider. The sheer magnitude of local network operators across geographies and their millions of users across each of these operators made this a mammoth task.

## Technologies

- Apigee
- ELK Stack
- AWS
- PostgreSQL

## About the Customer

Our customer, a leading tech firm in the communications space, has millions of daily users interacting with their systems for business needs. As a front runner in the space, our customer aimed to shape the future of communications through innovative products and solutions.

## Business Challenges

Several service providers like online retail, communications, media, online application and several others across the globe offer mobile numbers as an option for login and authentication. Mobile number also acts as a layer of security for these applications. One thing all these service providers need in common is to quickly find out which operator the user belonged to and take appropriate actions for the functioning of their applications. Our customer's solution aimed at doing just that.

Each market (country/region) has several operators, and each operator has several million users. In most cases, many users have multiple numbers across operators. This made it complex for service providers who want to offer their services to everyone in a local market. The key challenge for our customer was to identify an effective way to offer a discovery function through which each service provider could easily obtain which operator to contact to authenticate a particular user.

## Our Solutions

DigitalAPICraft (DAC), partnered with the customer to build an API-based operator discovery solution and offer it as a part of their existing solution ecosystem. This service would help identify operators based on the user's mobile number. DAC assessed the customer's existing setup and ecosystem to identify the API requirements and proposed a modularized solution based on functionality.

The first phase of the project involved onboarding all the operators and service providers to use the solution through respective APIs. This was key for the solution to succeed. The two APIs that were pivotal in this stage were:



Operator Registry API: To set and update the metadata of the mobile network operator



Developer Registry API: To set and update the developer and service providers' data

The second stage of the project was complex in nature as it involved building discovery APIs to provide operator details to the service providers. The complexity resided on the fact that the operator details had to be furnished based on different responses from different third-party vendors.

DAC crafted the solution by proactively assessing the data protection laws and policies of each country and also laws pertaining to cross country requests too.

Dynamic UI customization was another key aspect of the project to support various service providers. This helped service providers customize the look and feel based on their requirements and guidelines.

All proxies were deployed on Apigee Edge and DAC took complete end-to-end responsibility from installation to support and maintenance. Every step of the solution was implemented and achieved keeping security as utmost priority.

## Security Highlights

Security was of utmost importance at every juncture of the project. It was critical to take into consideration all the security requirements as there were several regions, operators and systems involved. There were three levels of security:

### API Level Security

Sensitive data encrypted while sending the response.

JWS and JWE was used for encryption.

Used security best practices to protect the services:

- ▶ Spike Arrest
- ▶ Json threat protection
- ▶ XML threat protection

### Instance Level Security

Includes setting up of:

- ▶ Bastion host
- ▶ Clam Antivirus
- ▶ AWS config

### Network Level Security

- ▶ Amazon Guardduty
- ▶ Security Groups
- ▶ Network ACL
- ▶ VPC peering
- ▶ TLS Encryption

## Support & Maintenance

- ▶ DAC was responsible for migration of the product from public cloud to private cloud.
- ▶ DAC manages the customer's entire infrastructure and is responsible for complete maintenance.
- ▶ World class technical support around the clock (24x7x365).
- ▶ Software upgrades: OPDK, OS Security, Tomcat, RDS, Grafana, Nagios, ELK, JDK, TLS.
- ▶ Upgrade and downsizing of the instances was carried out based on resource utilization.

The project was successfully implemented and both teams exhibited great synergies. DAC was able to help the customer to meet the delivery as per customer expectation. Some of the key highlights are listed as follows:

- ▶ Successful implementation and on-time delivery of customer's APIs for more than 2 years.
- ▶ Testcase implementation covering end-to-end scenarios.
- ▶ Agile approach and delivery methodology adopted throughout.
- ▶ Design and implementation done as per the customer's processes.

## Key Highlights

- ▶ Over 6 major releases on a yearly basis which includes the enhancements and changes to the discovery services.
- ▶ Responsible for customer data backup and recovery (component level and Image backup).
- ▶ Comprehensive monthly analytics report to help customer take informed business decisions.
- ▶ Complete ownership for ELK setup for logging and analytics as there were latency issues in their existing setup.
- ▶ Several best practices were followed as part of the development and delivery. Comprehensive documentation setup.
- ▶ Achieved 35% reduction in operational cost through infrastructure analysis, enhancements and change implementation.

**300+**

APIs Successfully  
Built

**400k**

Data Calls  
per Day

**90+**

Operators  
Onboarded

**9000**

Service Providers  
Onboarded

## Technology and Tools

- ▶ Apigee
- ▶ AWS
- ▶ ELK
- ▶ Postman
- ▶ Mocha and Chai (testing framework for automation)
- ▶ Node.js
- ▶ Nagios
- ▶ Git
- ▶ Pagerduty
- ▶ MySQL
- ▶ Grafana
- ▶ SSL/JWT/JWE
- ▶ Postgres

Interested in talking to our experts?  
Drop us a note!

[marketing@digitalapicraft.com](mailto:marketing@digitalapicraft.com)

DigitalAPICraft, through its products and services, helps global brands establish their API Ecosystem and transform into a truly Experience Enterprise. As a leading end-to-end digital transformation partner, our API-led approach enables retail, banking, insurance, telecom, and media companies to offer delightful customer experience, transform business processes and boost operational efficiency.

DigitalAPICraft has been awarded “Delivery Partner of the Year for APAC 2017 – Google Cloud” and is a Premier Google-Apigee partner. Over three consecutive years (2020, 2019 & 2018), DigitalAPICraft is recognized as one of the fastest-growing technology companies by Deloitte in its Technology Fast 50 India and twice (2019 & 2018) in Technology Fast 500 Asia Pacific rankings.

Located in USA, UK and India, and with customers across the globe, DigitalAPICraft brings extensive product and platform experience to help enterprises with digital strategy and consulting, disruption engineering, end-to-end DevOps, experience engineering and much more.

For more information visit [www.digitalapicraft.com](http://www.digitalapicraft.com)