



Workshop: Network API Hackathon

Presented By:
Prasham Jain
Sr. Technology Strategy Advisor
Rogers Communications

LAND ACKNOWLEDGEMENT

Agenda

- Welcome Remarks
- Introduce speakers
 - Ali Zaman – Principal Product Manager, Microsoft
 - Nicholas Manolakos - Senior Development Architect, Rogers Communications
- Introduction to Network APIs
- Team Formation Guidelines
- Hackathon Schedule
- Q&A

Rogers x UBC

5G Research Partnership

Rogers and UBC have been engaged in a Collaborative 5G Research Partnership since 2019.

- The first 5G smart campus in North America
- **12+** 5G enabled testbed across both UBC campus
- **23** 5G research projects funded in numerous verticals
- Pipeline for new talent



Hackathon Preview

Theme: Network APIs

Dates: October 4th - 6th, 2024

Location: ICICS Building Atrium

Audience: UBC students enrolled in a science, engineering or business program

Tools/Resources: Workshop, Mentors, Git Repo, Sample Code, Rogers API Sandbox, Test Devices

Hosted By



Sponsored By



ERICSSON

GSMA™

 ROGERS

Our Speakers



Nicholas Manolakos

Senior Development Architect
Rogers Communications



Ali Zaman

Principal Product Manager
Microsoft

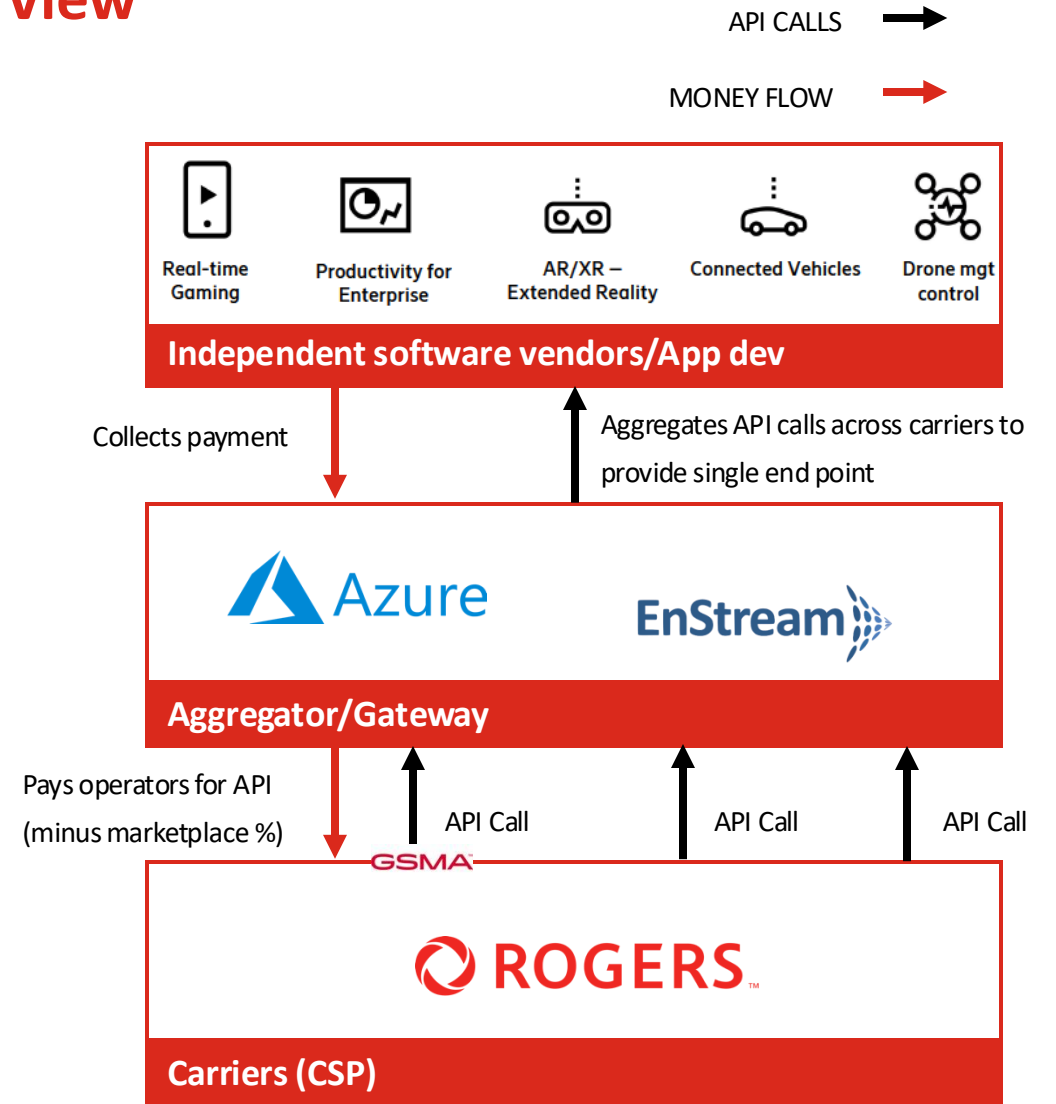
Project RAPID - Introduction and Program Overview

Network APIs / Network as a Service

- Network APIs allow ISVs to get information out of a network and configure a network
- They are a big step in the monetization of 5G networks
- Network APIs are not new but at MWC 2023, GSMA announced a standardization program that is bringing carriers together to create more value to the ISVs and allow operators to capture a significant market share
- Near-term market focus is on APIs addressing anti-fraud and identity use cases

Benefit to Developers

- Allows developers to configure networks based on application needs rather than work around their limitations
- Provides an interoperable, simplified and scalable way to validate user information for account creation/access and to prevent fraud.



Background: GSMA Open Gateway Network API

What is GSMA Open Gateway?

Framework of common Network APIs designed to provide universal access to operators' networks for developers

GSMA Open Gateway Footprint

47

Mobile Operator Groups

239

Mobile Networks

65%

Connections around the world

Key Industry Forums



Governing body defining the technical and business principle for NaaS with the establishment of the GSMA Open Gateway



Service APIs
App-centric developer oriented

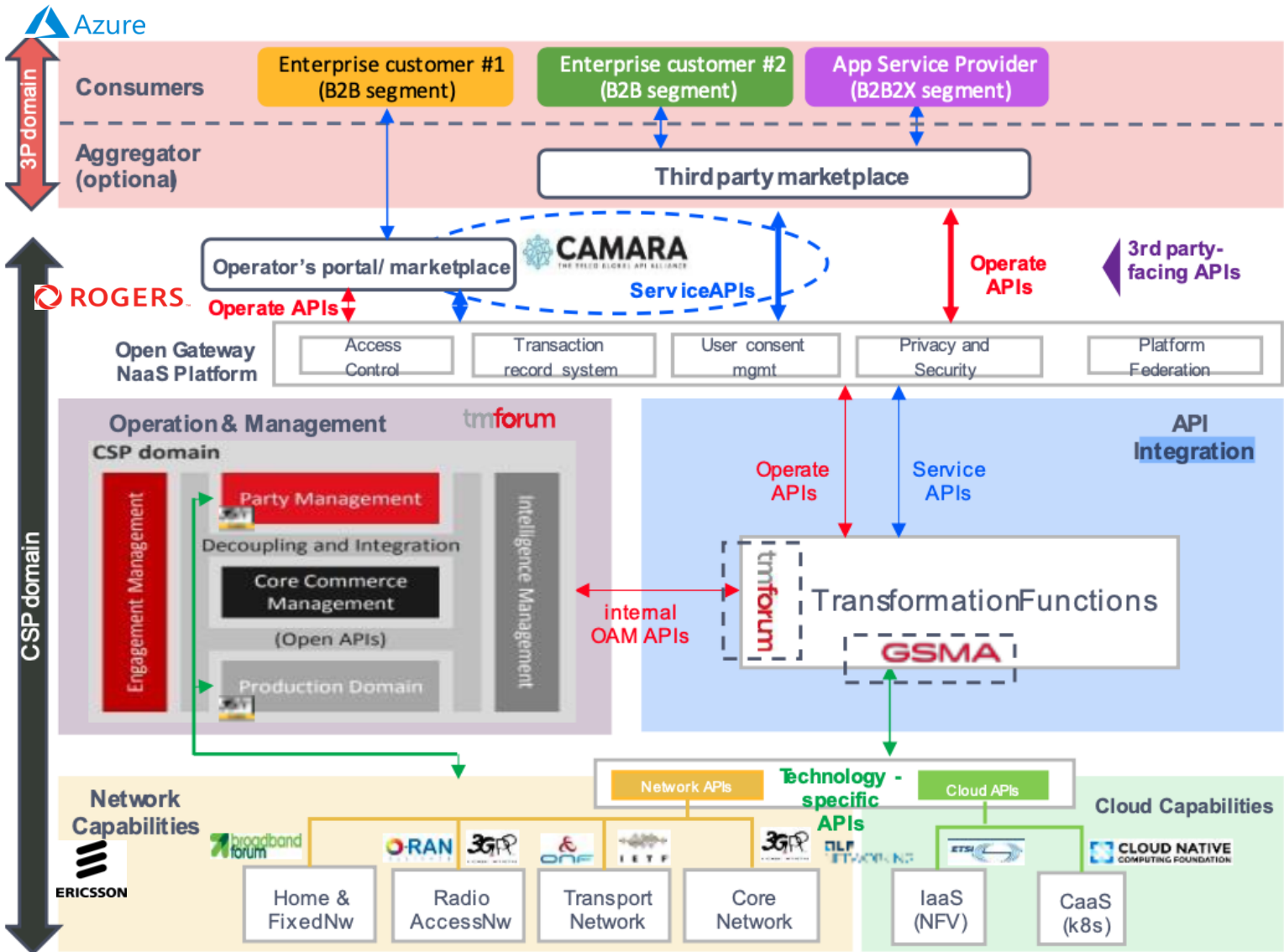
CAMARA is an open-source project defining the standardize spec and design of APIs



Operate APIs
Management oriented

Dedicated group defining how APIs services are to be operated and managed.

Ecosystem: GSMA Open Gateway NaaS system architecture



3rd Party-facing APIs

Service APIs
App-centric, developer-oriented
Apache2.0 lic, user -friendly , easy -to-use
Example: QoD, verifylocation, device status, Sim Swap,
Includes some management functionality used from the apps (in-app OAM APIs)

Hosted by **CAMARA**
Contributed by OpenGateway partners , directly or supported by bodies like
GSMA **5GFF** **tmforum**
bridge alliance **CableLabs**

Operate APIs
Management oriented
Easy-to-implement , easy -to-use, simple
Example: register, account, monitor, issue mgmt, order/purchase, pay...
Provides an easy integration of the NaaS Platform with marketplaces /portals
Contributed by OpenGatewaypartners hosted by **tmforum**

Technology -specific APIs
Technical capability oriented, standard, (FRAND) deterministic
Example: policysetting parameter setting information check..
Contributed by specific domain SDOs
ORAN **ETSI** **3GPP** **CLOUD NATIVE**
7 broadband forum **ETSI** **ONF** **ETSI** **LINUX**



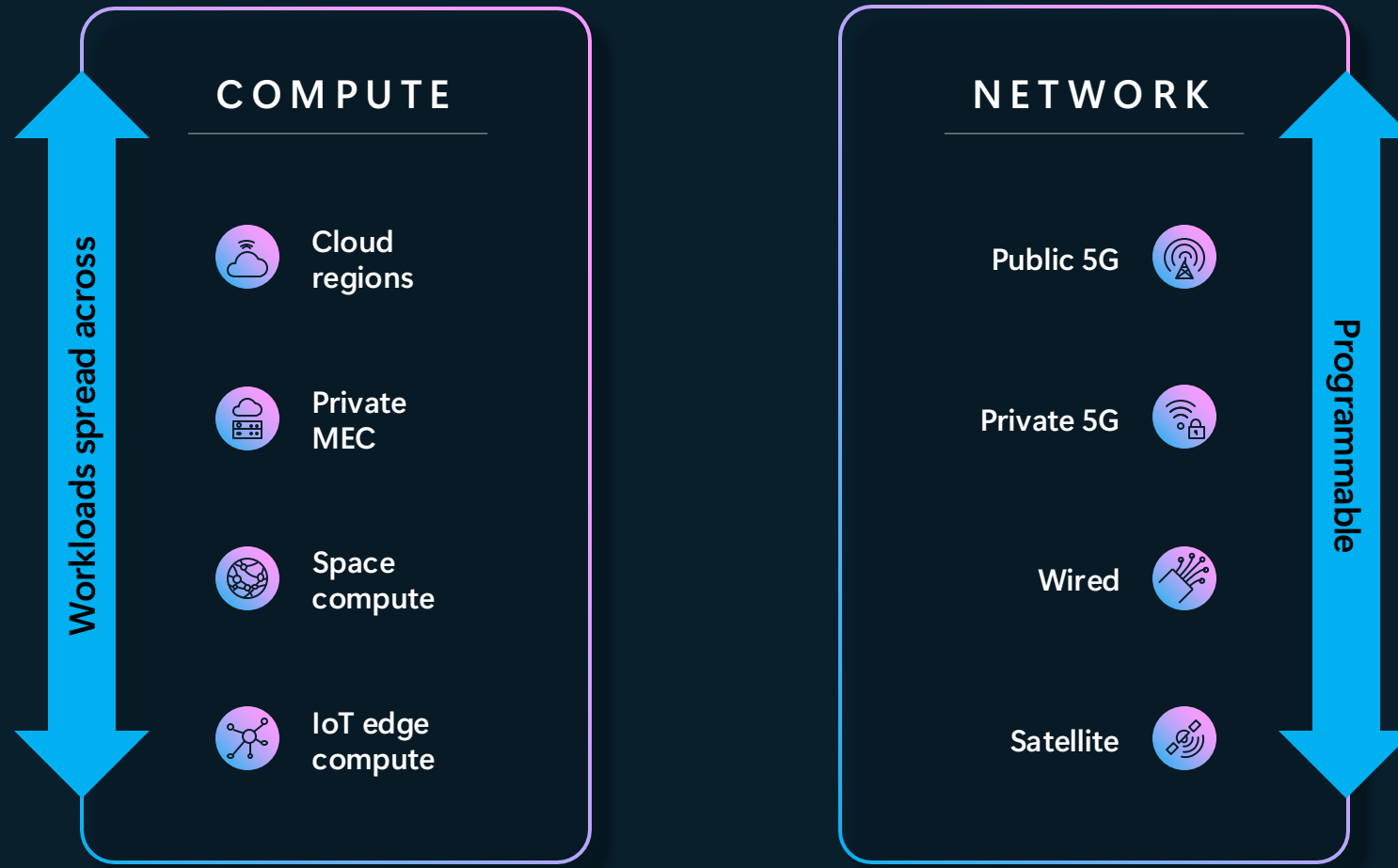
Azure Programmable Connectivity

Presented by:

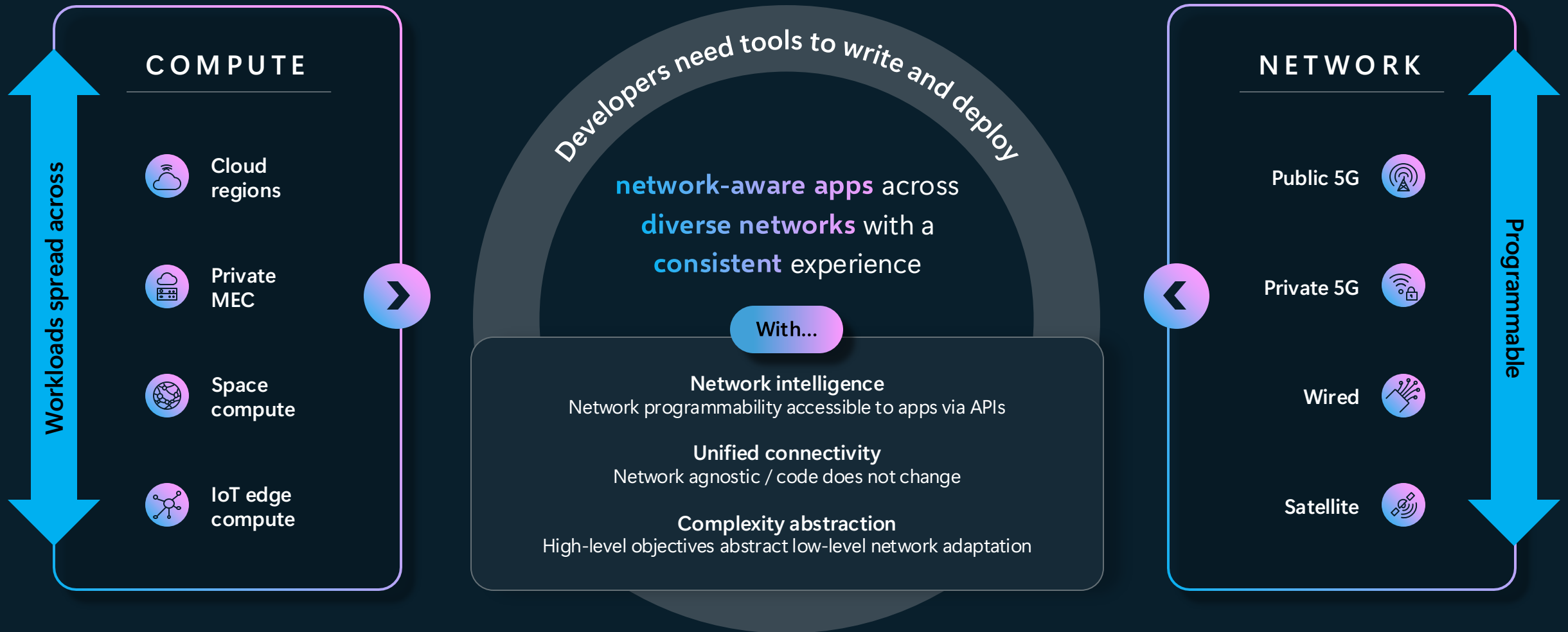
Ali Zaman
Principal Product Manager
Azure for Operators










Modern connected applications evolution



Network programmability



Key CAMARA network APIs

Network API	Description	Key benefits
 SIM swap	Check the last time that a SIM card was changed	<ul style="list-style-type: none">• Anti-fraud check
 Number verify	Authenticate mobile device seamlessly to eliminate friction from SMS one-time passwords	<ul style="list-style-type: none">• Password-less login• Fast and secure mobile/application registration
 Location	Obtain geographical location of devices based on network technologies, it can be hyper-precise on 5G stand alone	<ul style="list-style-type: none">• GPS replacement when it is not alternative• Hyper-precise in 5G SA• Centralized management
 Quality on demand	Request for higher level of quality for the application's traffic	<ul style="list-style-type: none">• Improves connectivity (e.g., latency, jitter) in crowded places• Guarantees reliable stable connection for critical applications
 Discovery	Identify all edge points available for an application to run or for an end-device to connect with latency information	<ul style="list-style-type: none">• Dynamic cloud usage• Movement of workloads
 Device status	Check if a device is connected to the network, losing connection and/or roaming	<ul style="list-style-type: none">• IoT device monitoring• Selection of applications capabilities based on roaming state
 Carrier billing	Request payment via user's mobile operator reflected on user's phone bill	<ul style="list-style-type: none">• Seamless purchase of digital content

Challenge for developers and operators

DEVELOPERS

Need seamless unified experience to infuse applications with new network capabilities across all modern operator networks

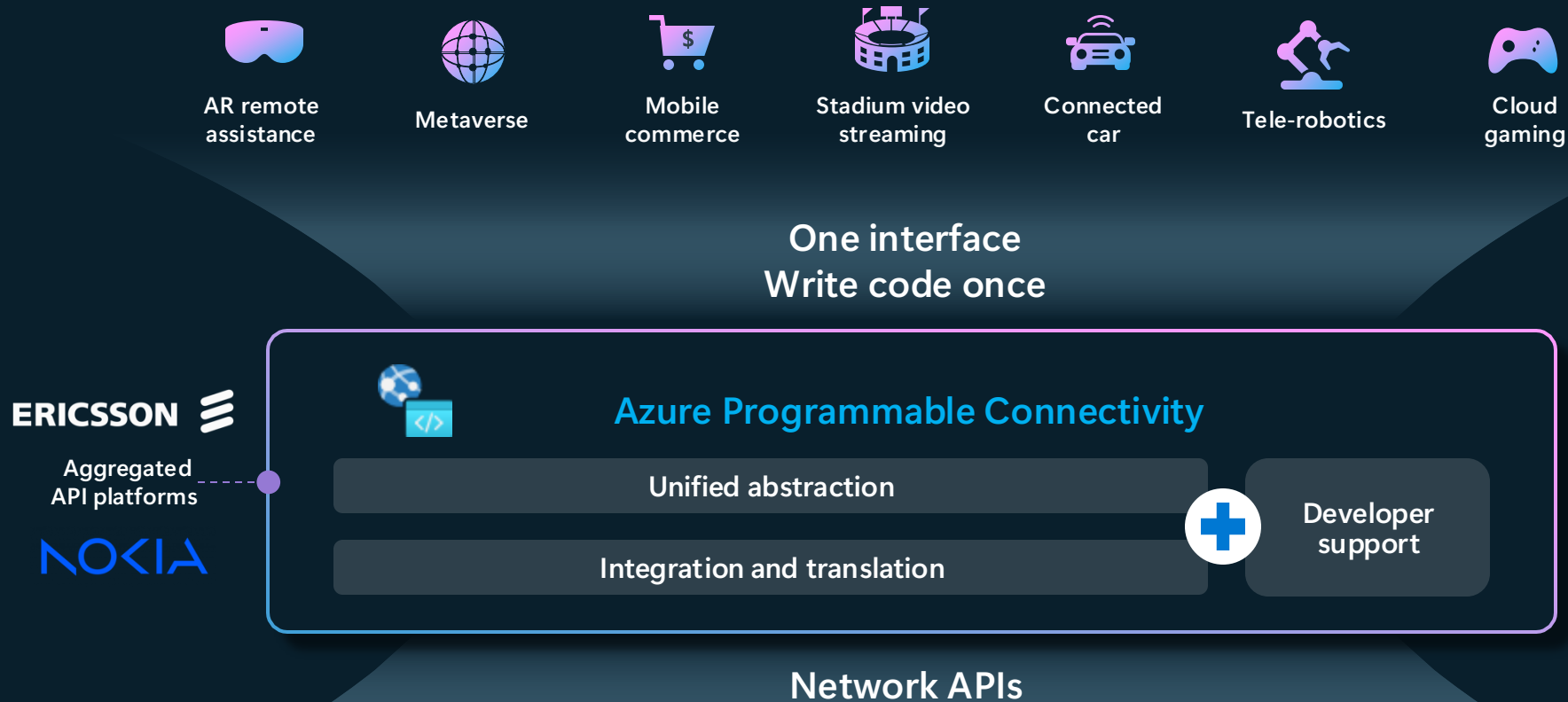
AZURE


Provides developers a streamlined experience abstracting the complexities of using network APIs and enabling operators to seamlessly differentiate their offerings

OPERATORS

Need access to developer ecosystems to monetize new network capabilities


Azure Programmable Connectivity—solving the challenge





Location
Open Gateway


The API allows an application to check if a mobile device is in proximity of a given location.



SIM Swap
Open Gateway

The API checks the last time that the SIM card associated with a mobile number (MSISDN) has changed.

+ Add



Number Verif
Open Gateway

The API enables s authentication of device by the mo developer reques phone number of used to access its

Network APIs added to this APC Gateway


Edit

Delete

Network API	Country/Region
-------------	----------------

Add SIM Swap APIs

APC Network APIs



SIM Swap
Open Gateway

The API checks the last time that the SIM card associated with a mobile number (MSISDN) has changed.

Brazil

Canada

France

Germany


Singapore

Spain

United Arab Emirates

United Kingdom

United States of America

Pay-As-You-Go 

Claro

Remove

View plan details


Pay-as-you-go

TIM

+ Add

Hide plan details

Features	Limits	Pricing
SIM Swap API provides the customer the ability to obtain information on any recent SIM pairing change related to the User's mobile account	This API derives from the GSMA Mobile Connect Account Takeover Protection specification and provides 2 operations: <ul style="list-style-type: none">POST retrieve-date : Provides timestamp of latest SIM swapPOST check: Checks if SIM swap has been performed during a past period (defined in the request with 'maxAge' attribute)	Per API call

Pay-As-You-Go 




Vivo

Remove

View plan details

To change the Country/Region selection, remove any Offerings you have added.

APC initial focus: Anti-fraud network APIs

Network API	Description	Key benefits
 SIM swap	Check the last time that a SIM card was changed	<ul style="list-style-type: none">• Anti-fraud check
 Number verify	Authenticate mobile device seamlessly to eliminate friction from SMS one-time passwords	<ul style="list-style-type: none">• Password-less login• Fast and secure mobile/application registration
 Device location	Obtain geographical location of devices based on network technologies; it can be hyper-precise on 5G stand alone	<ul style="list-style-type: none">• GPS replacement when it is not alternative• Hyper-precise in 5G SA• Centralized management

halo.car

Providing mobility by improving access to electric vehicles

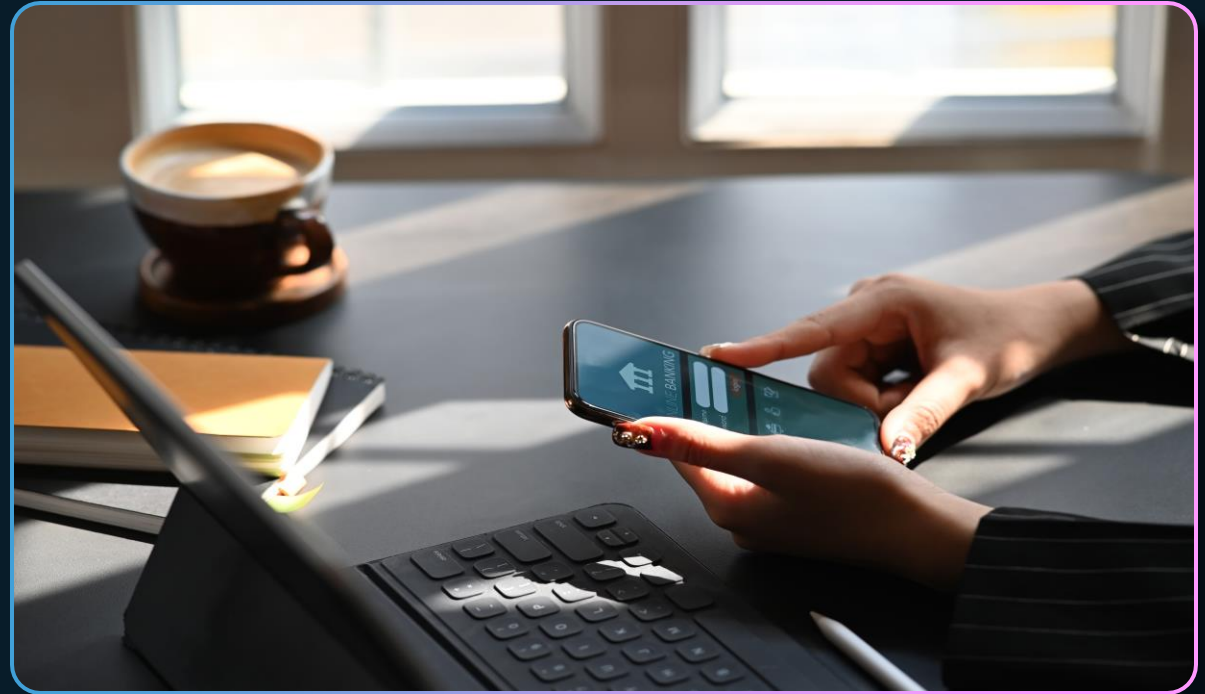
- Halo' provides remotely piloted cars through a mobile app, driven over LTE/5G.
- Using a QoD API, network congestion is mitigated , even in dense areas like the Las Vegas strip





Itaú enhances Transaction Security with Antifraud APIs

- **Enhanced protection**
Utilizes geographical data to safeguard customer accounts from unauthorized access, ensuring security across diverse regions
- **Location verification**
Open Gateway Location API confirms real-time location of customers engaging in mobile app transactions





NAGRA, the media & entertainment technology division of the Kudelski Group, protects subscribers against SIM card fraud

- NAGRA Scout provides intelligent home network security
- A broadband subscriber can add family members to monitor their home network activity
- **SIM verification**
Open Gateway SIM swap API confirms that SIM has not been changed (phone hijacked)



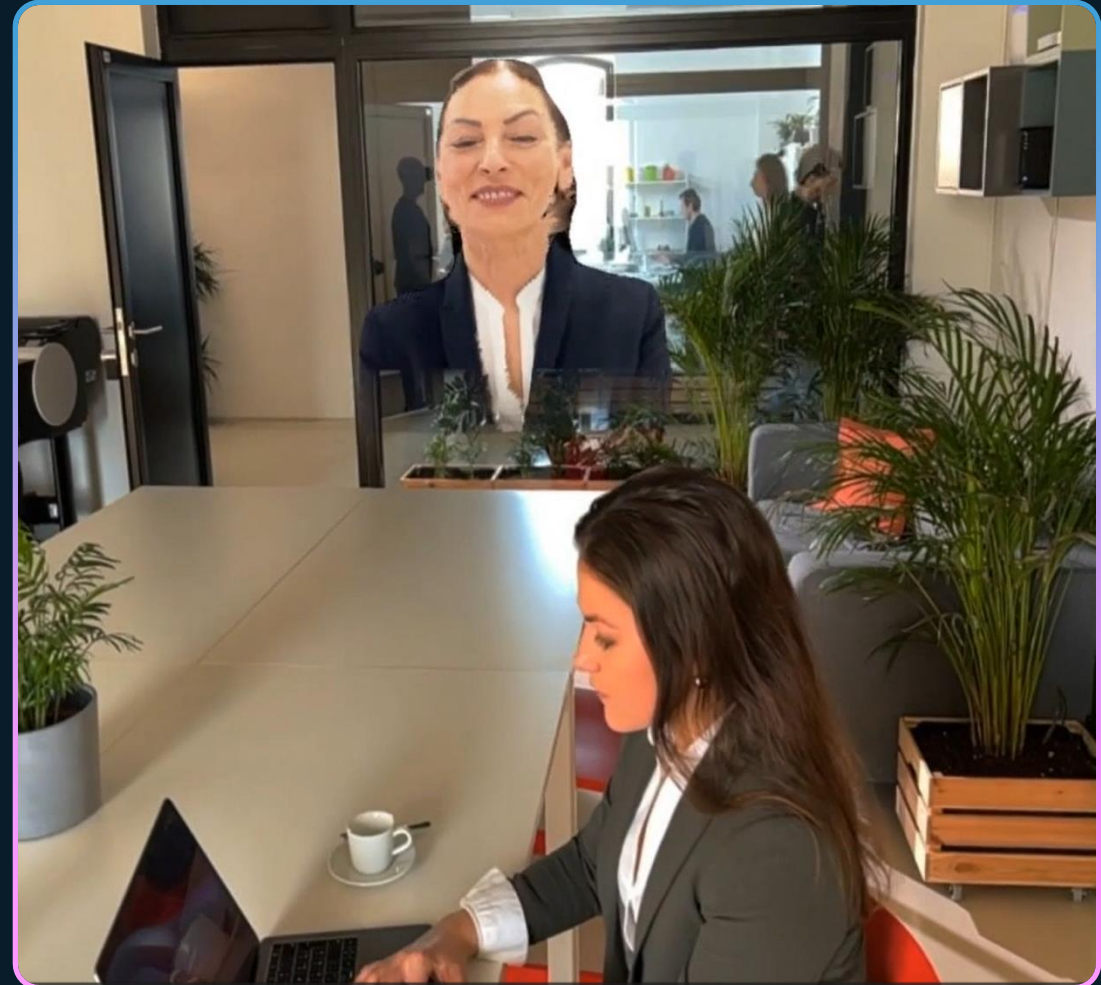


MATSUKO

Holgraphic presence

MATSUKO's innovative technology streams people as 3D holograms with one camera, creating the feeling of physical presence and emotional connection in remote communication.

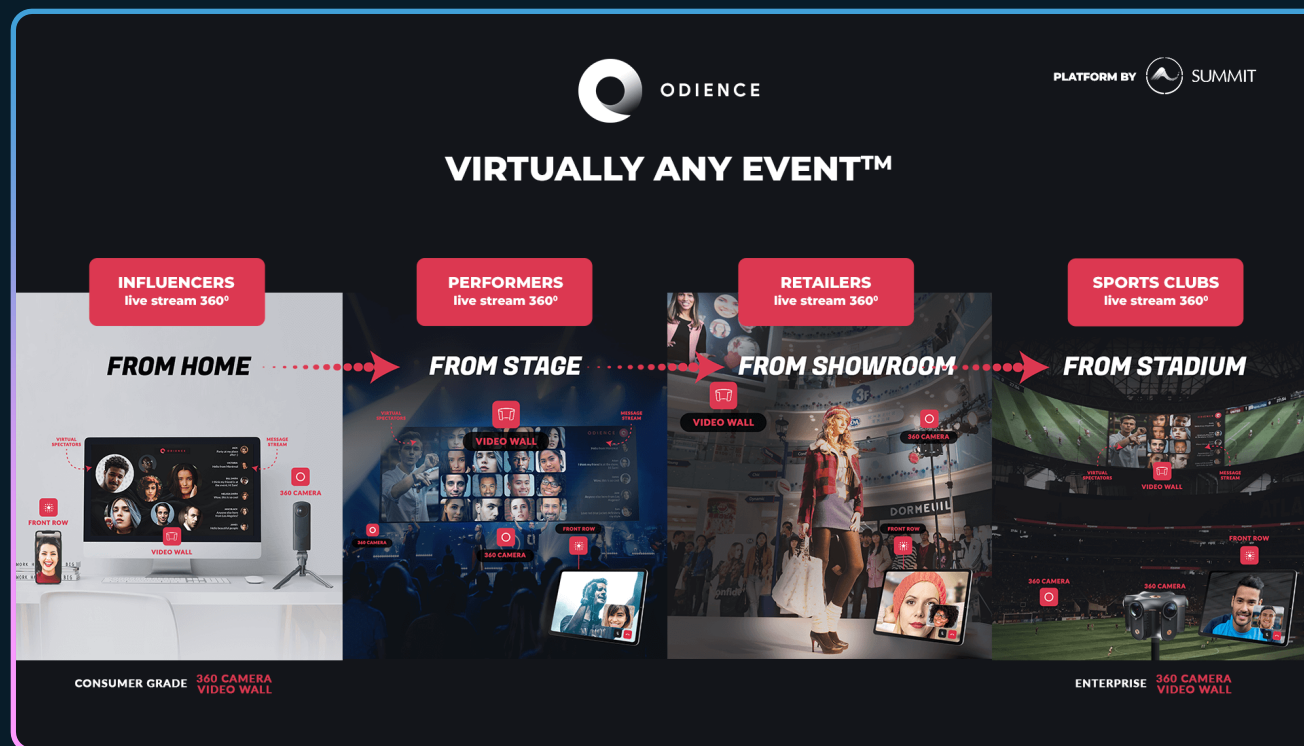
- APC provides access to QoD network APIs from multiple operators
- Delivers smooth and natural movement of holograms on 5G by reducing latency and ensuring high bandwidth.





Odience 360° live-streaming platform delivers high-quality interactive event experiences to virtual audiences

- APC provides access to QoD APIs, enabling enterprises to stream broadcast-quality 360 Virtual Reality 8K video to the Odience platform
- Sustained high bandwidth and low latencies ensure high quality 360 video mobile devices with a smooth user experience.



Closing remarks and next steps



Azure Programmable Connectivity, bridges networks and applications, rewriting the rules of connectivity



Learn more about Azure Programmable Connectivity
aka.ms/AzureProgrammableConnectivity

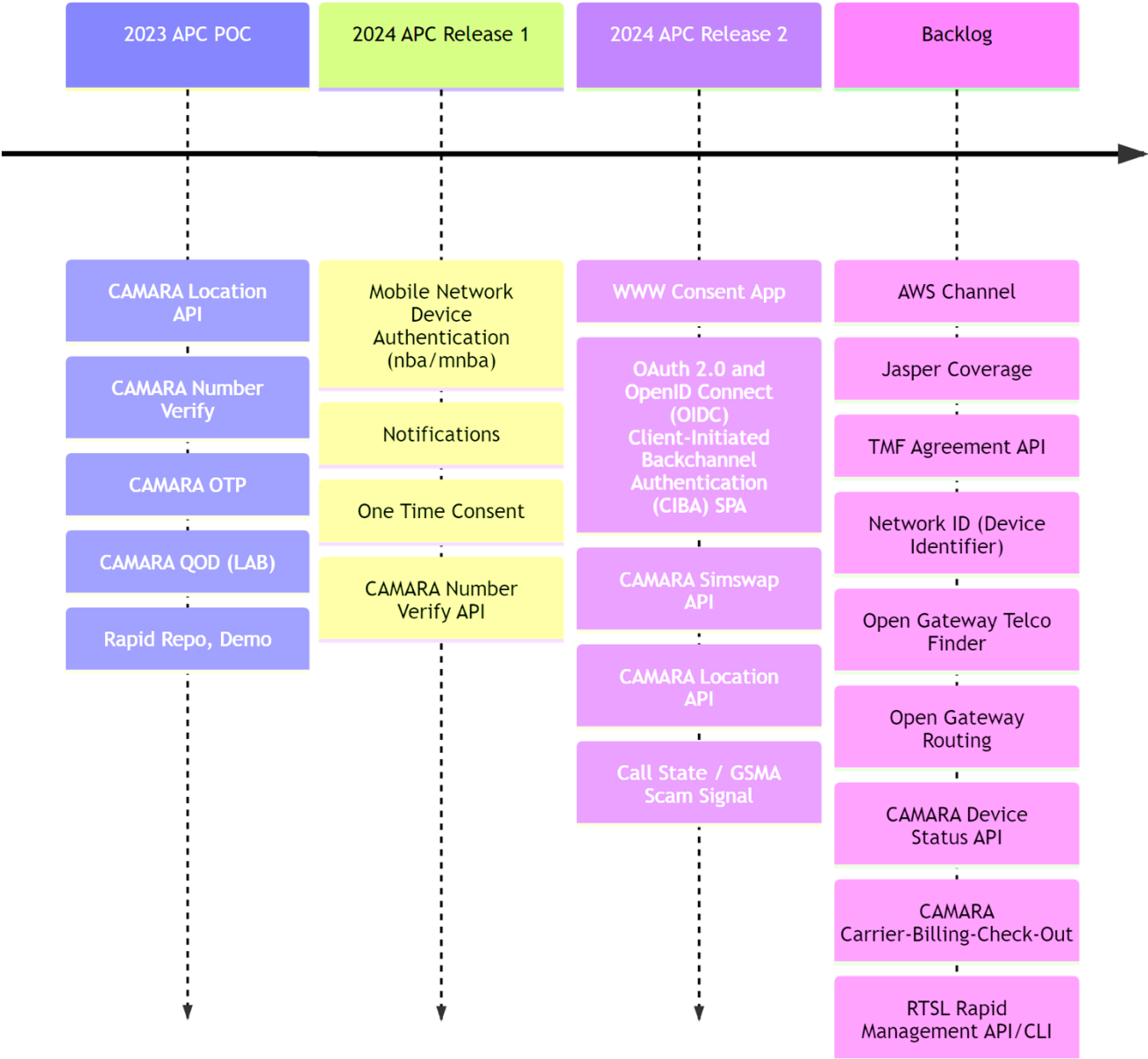


GSMA Camara Standardized API List

API Portfolio		Anti-Fraud	Mobile Connectivity/Value-Added Services		Fixed Connectivity	Cloud & Edge	Payments
API Product Family	Subscriber Identity	Location	Network Quality/Optimization	Network Quality/Optimization	MEC	Payment and Charging	
CAMARA API	Device Status Check connectivity status of UE	Device Location Verification UE location check to proximity of a given location	Connectivity Insights Check if networking requirements are met	Home Device QoD Enable configuration to users WiFi connectivity	Simple Edge Discovery Enable discovery to closest edge-cloud node to connect	Carrier Billing Enable purchases to request payment via carrier billing system	
	IMEI Fraud Check if IMEI is blacklisted	Geofencing Enable changes base on geographic position	Mobile Quality on Demand Enable time bounded network configuration		Traffic Influence Geographic Traffic optimization for Edge Application Server		
	KYC Fill-in Pull customer info from operator database	Location retrieval Retrieve location via Mobile network	WebRTC Add communications capabilities (video, voice, etc.)				
	KYC Match Check customer info from operator database						
	Number Verification Authentication of UE by Mobile network						
	SIM Swap Check last time the SIM card has changed						
	One Time Password (SMS) Send short-lived one time password via SMS						
	Blockchain Public Address Bind/unbind public addresses						

24

Rogers Roadmap



Network API Use Cases



ACCOUNT CREATION
Validate a is person is who they claim.



ACCOUNT ACCESS
Prevent fraudulent account access.



DEVICE MANAGEMENT
Track and manage any SIM powered device.



QUALITY OF SERVICE
Prioritize latency based on application needs.

PHONE NUMBER: (555) 555-5555

INFO PROVIDED

- First Name
- Last Name
- Login Location
- Address
- City
- Postal Code

INFO VERIFIED

- ✓ First Name
- ✓ Last Name
- ✗ Device Location
- ✗ Address
- ✓ City
- ✗ Postal Code



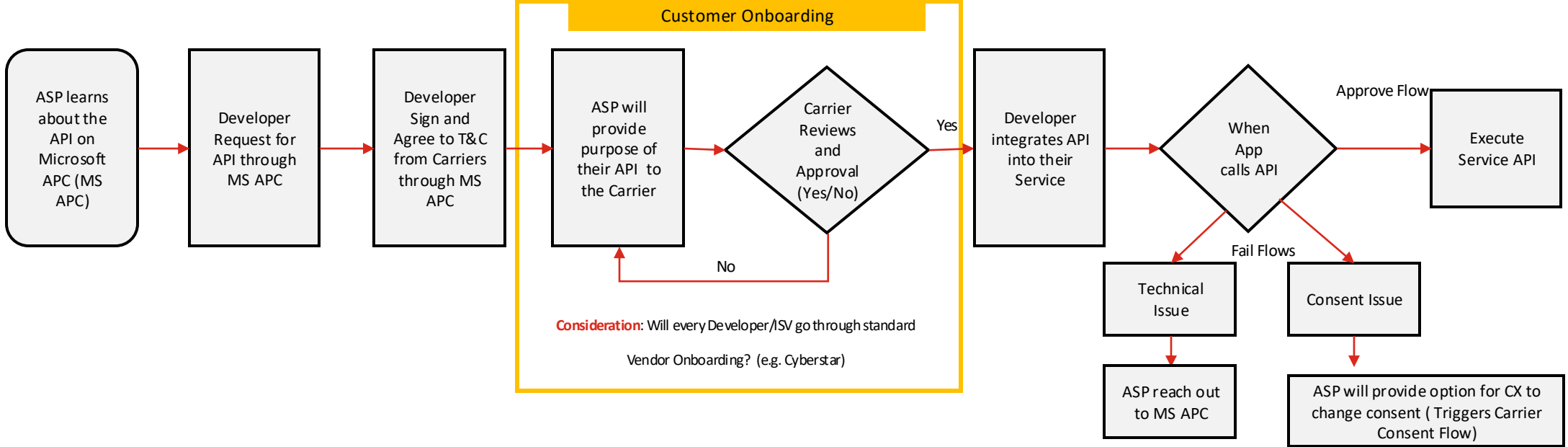
Fraud Detected

PHASE 1 FOCUS: Fraud Prevention and Digital Identity Use Cases

Device Location Verification – B2B/B2B2C Flow

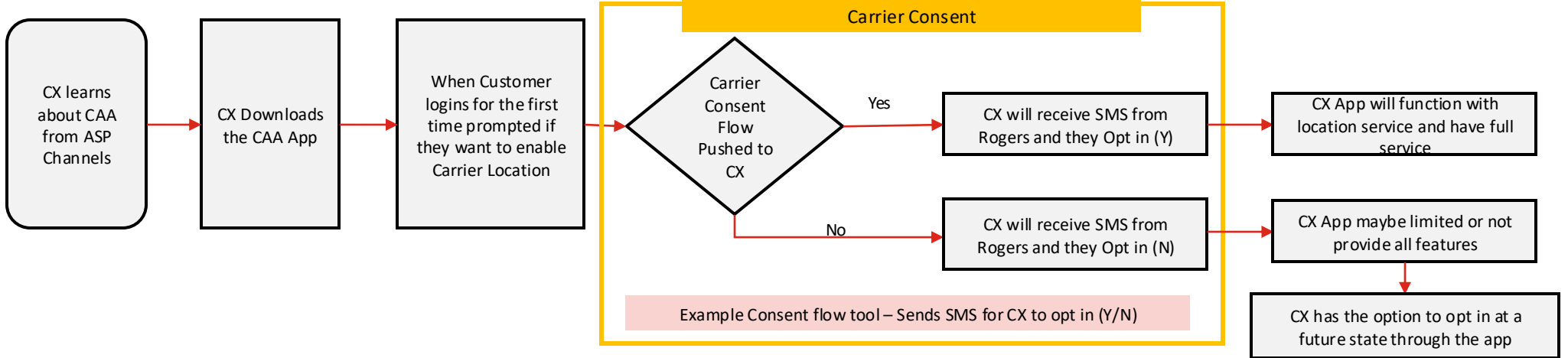
B2B

ASP Developer Flow



B2B2C

Customer (CX) Flow



Location API

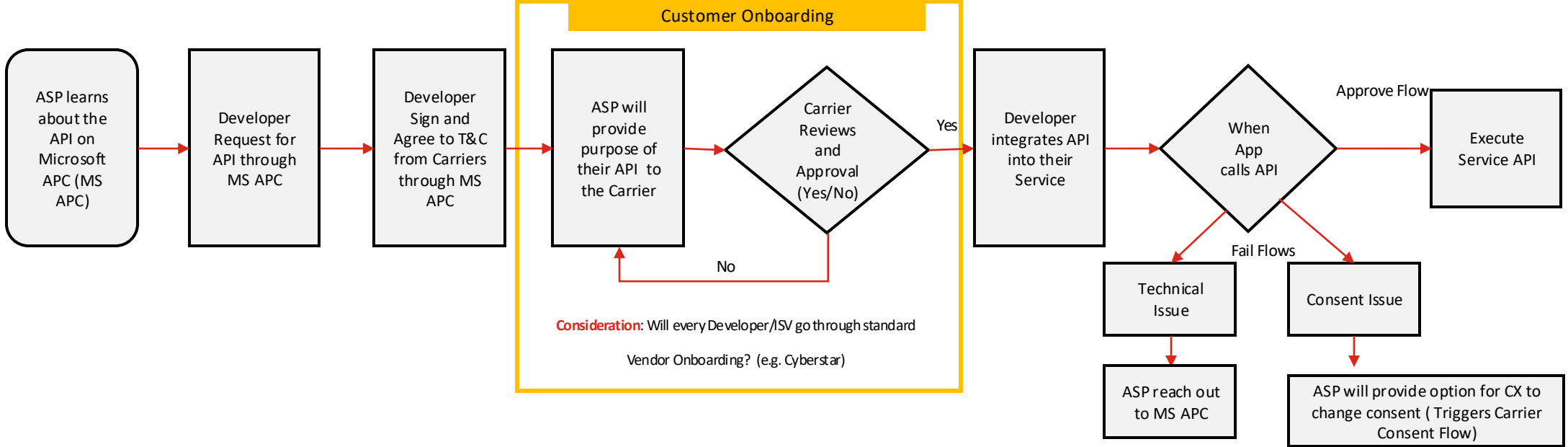
Location Verification Sharing with APC GSMA Opengateway Outh2 OIDC CIBA Flows

- 1. Consent Request Initiation:** CA Auto Insurance decides to request real-time location data from Maria to offer a personalized insurance quote. CA sends a custom SMS to Maria, containing a secure link to initiate the consent process. This message explains the “Purpose”, “Period”, and “Scope” of the location data sharing, in line with Rogers’ and Microsoft Azure APC’s privacy policies.
- 2. CIBA Authentication Initiation:** Upon Maria clicking the link, instead of being directed to a login page, a CIBA flow is initiated. Rogers, acting as the IDP, receives a backchannel authentication request from CA. Rogers verifies if the request is legitimate and if Maria has previously granted consent for such requests.
- 3. Authentication and Consent Notification:** Rogers sends a notification to Maria’s registered device, asking her to authenticate and approve the data-sharing request. Maria authenticates using her preferred method (e.g., biometrics, one-time password) via the Rogers app or website, which ensures her identity is confirmed securely without redirecting her to a login page.
- 4. Informed Consent and Approval:** Post-authentication, Maria is presented with detailed consent information within the Rogers app or notification interface. This step reaffirms the “Purpose”, “Period”, and “Scope” of sharing her location data. Maria reviews and grants consent through this interface, streamlining the process.
- 5. Token Issuance and Data Sharing:** Once Maria consents, Rogers notifies CA through the backchannel that consent has been granted. Rogers issues a token to CA, enabling them to access Maria’s real-time location data through the Rogers CAMARA Location API. This ensures that CA receives the necessary data to provide a personalized insurance quote to Maria.
- 6. Security and Verification:** Rogers continues to use robust verification protocols to confirm the authenticity of the location data and the security of Maria’s account. This step is crucial for maintaining trust and ensuring that the data shared is accurate and secure.
- 7. Consent Revocation and Lifecycle Management:** After the agreed-upon period ends or at any time Maria decides to revoke her consent, Rogers facilitates this process, ensuring that CA no longer has access to her location data. Rogers manages the consent lifecycle, adhering to privacy standards and regulations, and records all transactions for audit and compliance purposes.

Sim Swap Verify – B2B/B2B2C Flow

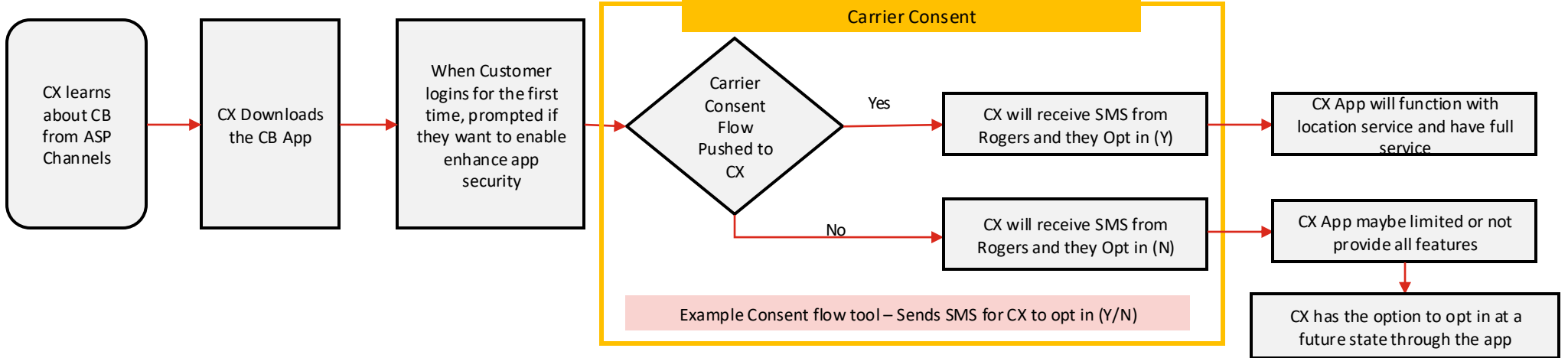
B2B

ASP Developer Flow



B2B2C

Customer (CX) Flow



SIMSWAP API

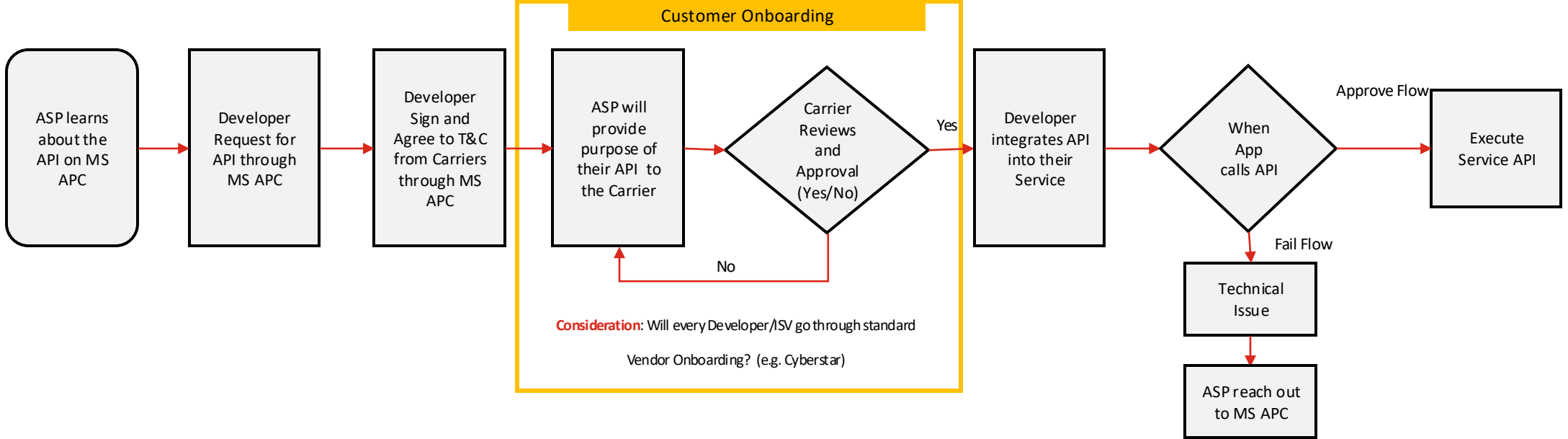
SIMSWAP for Fraud Prevention with APC GSMA Opengateway Outh2 OIDC CIBA Flows

- 1. Consent Request Initiation:** When Eleni applies for a new credit card using her banking app, the Royal Bank of Canada (RBC) decides to verify the legitimacy of her SIM card to prevent fraud. RBC sends Eleni a custom SMS, containing a secure link to initiate the consent process for SIMSWAP data sharing. The SMS explains the “Purpose”, “Period”, and “Scope” of the SIMSWAP data sharing, in line with the privacy policies of Rogers and Microsoft Azure APC.
- 2. CIBA Authentication Initiation:** Instead of directing Eleni to a traditional login page after she clicks the link, a CIBA authentication flow is initiated. Rogers, acting as the Identity Provider (IDP), receives a backchannel authentication request from RBC. Rogers verifies if the request is valid and checks if Eleni has pre-authorized such requests.
- 3. Authentication and Consent Notification:** Rogers sends a notification to Eleni’s registered device, prompting her to authenticate and approve the SIMSWAP data-sharing request. Eleni authenticates via the Rogers app or website using her preferred method (e.g., biometrics, one-time password), ensuring a secure and seamless user experience without needing to manually log in.
- 4. Informed Consent and Approval:** After successful authentication, Eleni is presented with the consent information directly within the Rogers app or through a secure notification. This interface clearly outlines the “Purpose”, “Period”, and “Scope” of sharing her SIMSWAP data with RBC. Eleni reviews the information and grants her consent within this secure environment.
- 5. Token Issuance and Data Sharing:** Once Eleni has consented, Rogers informs RBC through the backchannel that the consent has been granted. Rogers then issues a token to RBC, enabling them to access Eleni’s SIMSWAP data through the Rogers CAMARA SIMSWAP API. This process ensures that RBC can securely verify the SIMSWAP event as part of Eleni’s credit card application, enhancing security and fraud prevention measures.
- 6. Security and Verification:** Throughout this process, Rogers employs stringent security measures to verify the authenticity of the SIMSWAP data and the integrity of Eleni’s account. This step is crucial for maintaining the security of the transaction and ensuring that the data shared is accurate and protected against unauthorized access.

Number Verify – B2B/B2B2C Flow

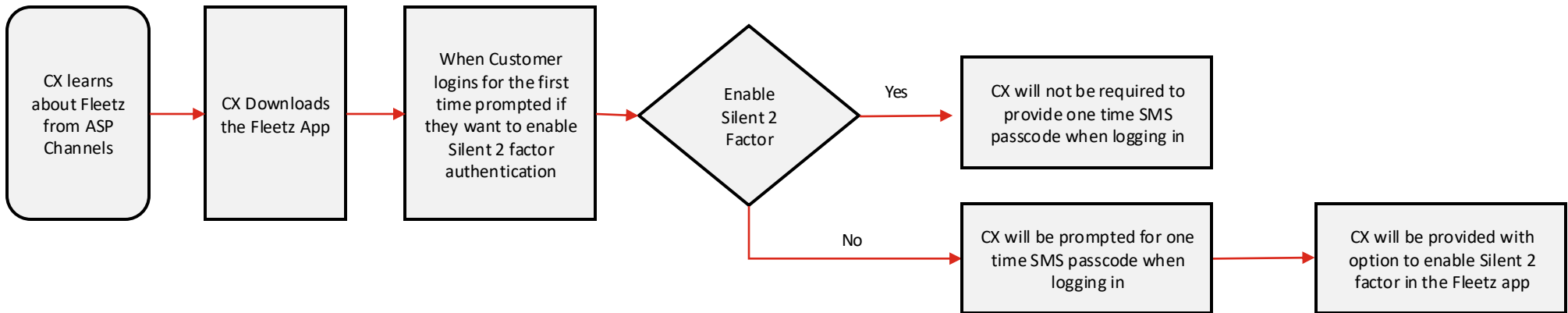
B2B

ASP Developer Flow



B2B2C

Customer (CX) Flow



Number Verification API

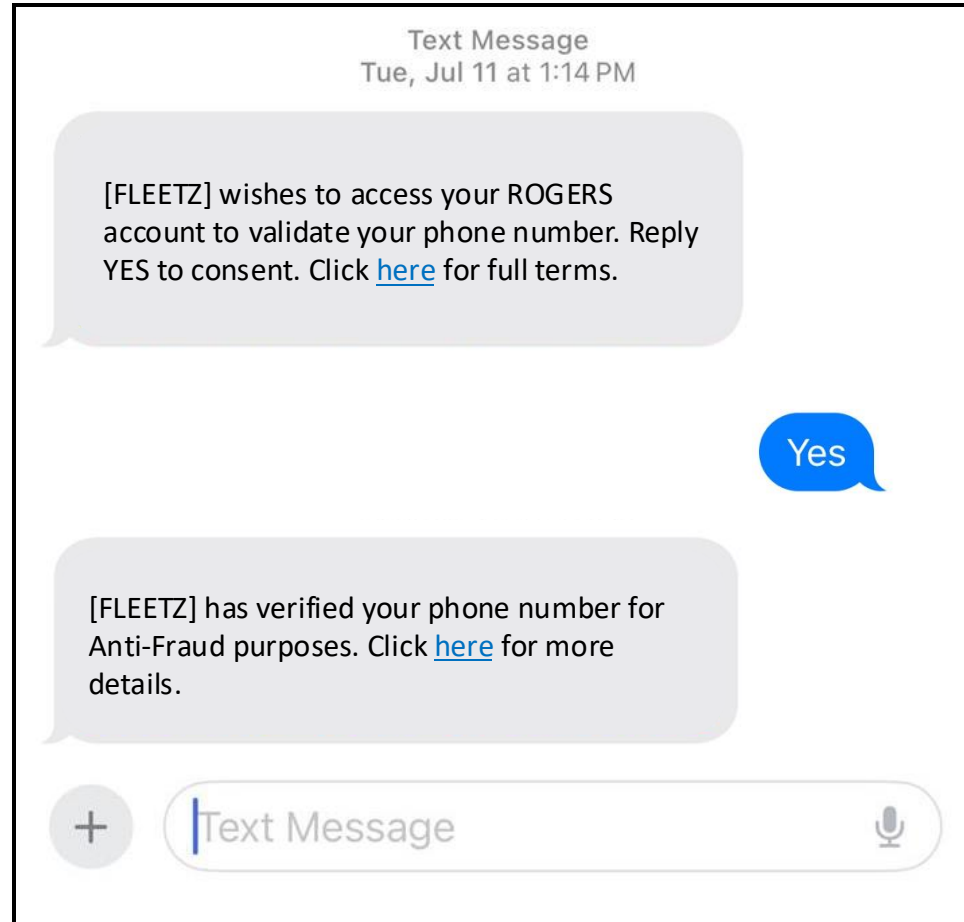
Number Verification for Silent Login (using Authorization Code Flow)

John, a Rogers subscriber, is using his mobile to apply to rent a home. The landlord has integrated Rogers CAMARA Number Verify API through Microsoft Azure Programmable Connectivity (APC) to offer secure and seamless rental application services. Committed to transparency and customer privacy, the landlord initiates a consent request to John, outlining the “Purpose”, “Period”, and “Scope” of the number verification data sharing under the stringent Terms of Service and Privacy Policy upheld by Rogers and Microsoft Azure APC. This allows John to silently log in to the landlord’s website without having to remember a password.

1. **Consent Request Initiation:** John receives a custom SMS from the landlord, containing a secure link to opt-in for number verification data sharing. This step initiates the transparent data-sharing process.
2. **Authentication and Consent:** Clicking the link, John is directed to a secure Rogers authentication page. He logs in using his Rogers.com credentials, affirming his identity and ensuring a secure transition to the consent phase.
3. **Informed Consent:** On the Consent page, John is presented with detailed information regarding the “Purpose”, “Period”, and “Scope” of sharing his number verification data. Rogers and the landlord ensure John has all the information needed to make an informed decision.
4. **Agreement and Data Sharing:** Upon clicking “I Agree”, John explicitly consents to share his number verification data with the landlord. Rogers promptly notifies the landlord, enabling access to John’s number verification data through the Number Verify API. This crucial step ensures the landlord can provide a secure rental application process, reflecting John’s specific needs and circumstances.

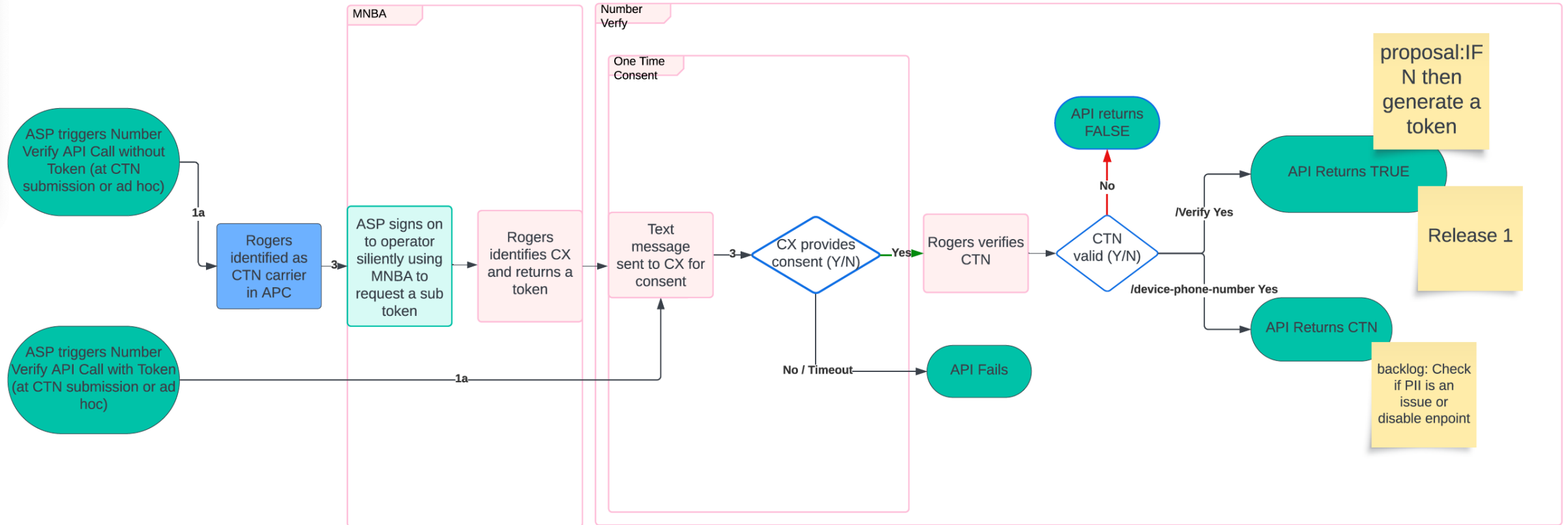
Consent Process Example

Number Verify API: Checking a customer's device CTN (customer telephone number) attached to their active SIM matches the provided CTN



Number Verify – B2B2C Flow

Validates the provided phone number matches the phone number of the device in use.



ASP: Application Service Provider (also known as ISV)

CX: Customer

CTN: Customer Telephone Number

APC: Azure Programable Connectivity

MNBA: Mobile Network Based Authentication

Getting Started – Number Verification Spec



[NV@Swagger Editor](#) Spec

```
curl -X POST "{basename}/number-verification/v0/verify" \  
-H "Authorization: Bearer {your_access_token}" \  
-H "Cache-Control: no-cache" \  
-H "accept: application/json" \  
-H "Content-Type: application/json" \  
-d '{  
  "phoneNumber": "+1416XXXXXXX"  
}'
```

Bash Shell Example using curl command

*For the purpose of the hackathon, you will be provided a basename and access token against our sandbox proxy and not Microsoft Azure Programmable Connectivity Platform

Getting Started Rogers Repository

Getting Started Repository - [questsin/UBC-Rogers-CAMARA-Hackathon: UBC Rogers CAMARA Hackathon \(github.com\)](https://github.com/questsin/UBC-Rogers-CAMARA-Hackathon)



Team Formation

- Team must have a minimum of 5, and a maximum of 8 members. **Capacity:** 10 Teams
- Teams recommended to have at least 2 members each with a business major and a science/engineering major.
- If you know who you want to work with, select ONE person to email raymond.chau@ubc.ca:
 - Names and UBC email IDs of all identified team members
 - Deadline: October 1st by Noon PDT.

Note: Each member must have individually registered for the hackathon using a UBC email.

- Final team assignments shall be notified via email no later than October 2nd.

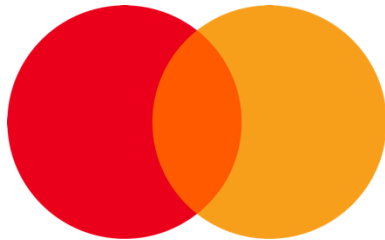
Schedule (Tentative)

Date	Time	Activity (Location: ICICS Atrium)
Oct 4 th	4:30 pm	Team Check-In
	5:00 pm -6:30 pm	Welcome Remarks Ground Rules and Housekeeping Ice Breaker Onboarding to Sandbox Environment Distribution of Test Devices
	7:00 pm	Dinner
Oct 5 th	9:00 am	Welcome Back and Check-in
	9:30 am	Breakfast
	10:00 am – 11:00 am	AM Office Hours – Drop In
	12:30 pm	Lunch
	2:00 pm – 3:00 pm	PM Office Hours – Drop In
	7:00 pm	Dinner
Oct 6 th	9:00 am	Welcome Back and Check-in
	9:30 am	Breakfast
	10:00 am – 11:00 am	AM Office Hours – Drop In
	12:30 pm	Lunch
	1:00 pm – 3:00 pm	Final Presentations
	4:00 pm	Winner Announcements and Closing Remarks

Prizes

1st Place

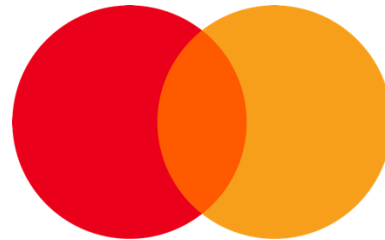
\$500/pp



mastercard

2nd Place

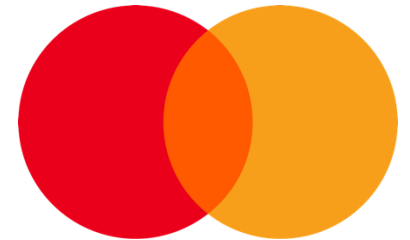
\$300/pp



mastercard

3rd Place

\$150/pp



mastercard

Q&A