GSMA™

LinkedIn Live

TS.43 Entitlement Server Implementation: Real-World Challenges and Proven Solutions

Tuesday, 24 June | 2pm (BST)

BOOKMARK NOW

GSMA Working Groups

Scan to learn more about GSMA Working groups

Scan the QR code or email workinggroups@gsma.com for more information

GSMA

GSMA

Five reasons you should join GSMA Membership

Discover how we can transform your business

Agenda

Today's LinkedIn Live session will cover:

Introduce GSMA TS.43 Working Group

- Jean-Philippe Cormier, TS.43 group (TSGVVEC) Chair, **Google**

TS.43 use cases: RCS Activation and Phone Number Verification

- Nacho Blázquez, **HCLTech**

TS.43 Android: Satellite Connectivity, eSIM Transfer, RCS, Phone Number Verification

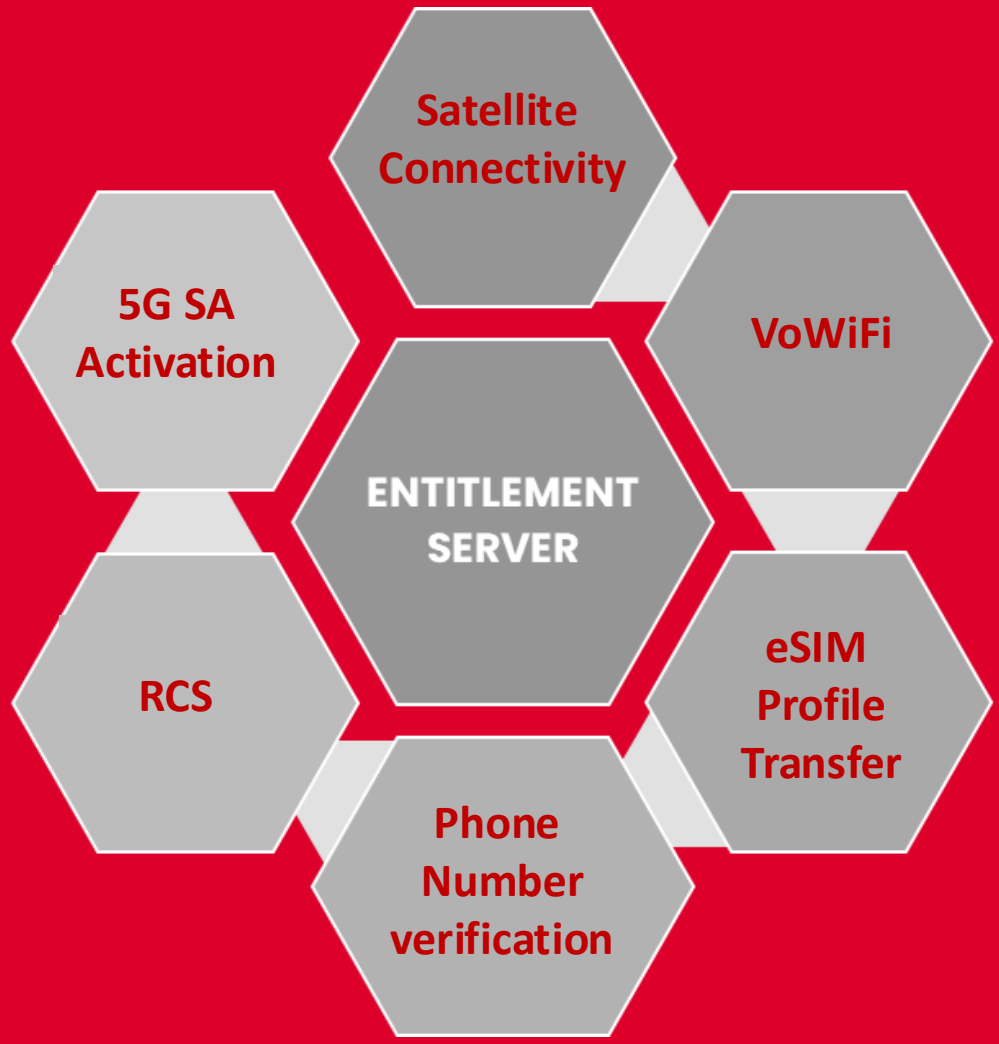
- Pavan Nuggehalli, **Google**

TS.43 use cases: eSIM Profile Transfer and 5G SA Activation

- Florian Schmitt, GSMA Terminal Steering Group Chair, **Deutsche Telekom AG**

Q&A

Please share your question on the chat



GSMA

Jean-Philippe Cormier

TSG VVEC Chair
Google

,

Nacho Blazquet

HCLTech Chief Architect BSS/Entitlements
HTCLTech

Pavan Nuggehalli

3GPP Standard
Google

Florian-Leon Schmitt

Terminal Steering Group Chair
Deutsche Telekom AG

GSMA TS.43 Group (aka TSG VVEC) Overview

Jean-Philippe Cormier

TSG VVEC Chair
Google

GSMA

TS.43 and GSMA Terminal Services Group VoWiFi and VoLTE Entitlement Configuration

This GSMA TSG group has active participation from the MNO, OEM and Entitlement Configuration server community.

All working to bring new use cases to the standard and rolling them rapidly to meet market demand.

TS.43 enables dozens of complex commercial use cases for MNOs that include more than just service entitlement.

Non-Terrestrial Network access, 5G slicing, eSIM activation and the next generation operator authentication are just the tip of the iceberg.

TS.43 created a thriving ecosystem with more than 50 MNOs worldwide commercially deployed, each with multiple use cases.

The nature of the standard allows MNOs to deploy their use cases ‘in-house’, while also enabling a large number of entitlement configuration server vendors to succeed.

© GSMA 2025

TS.43 Use Cases:

RCS Activation and Phone Number Verification

Nacho Blazquet

HCLTech Chief Architect
BSS/Entitlements
HTCLTech

GSMA

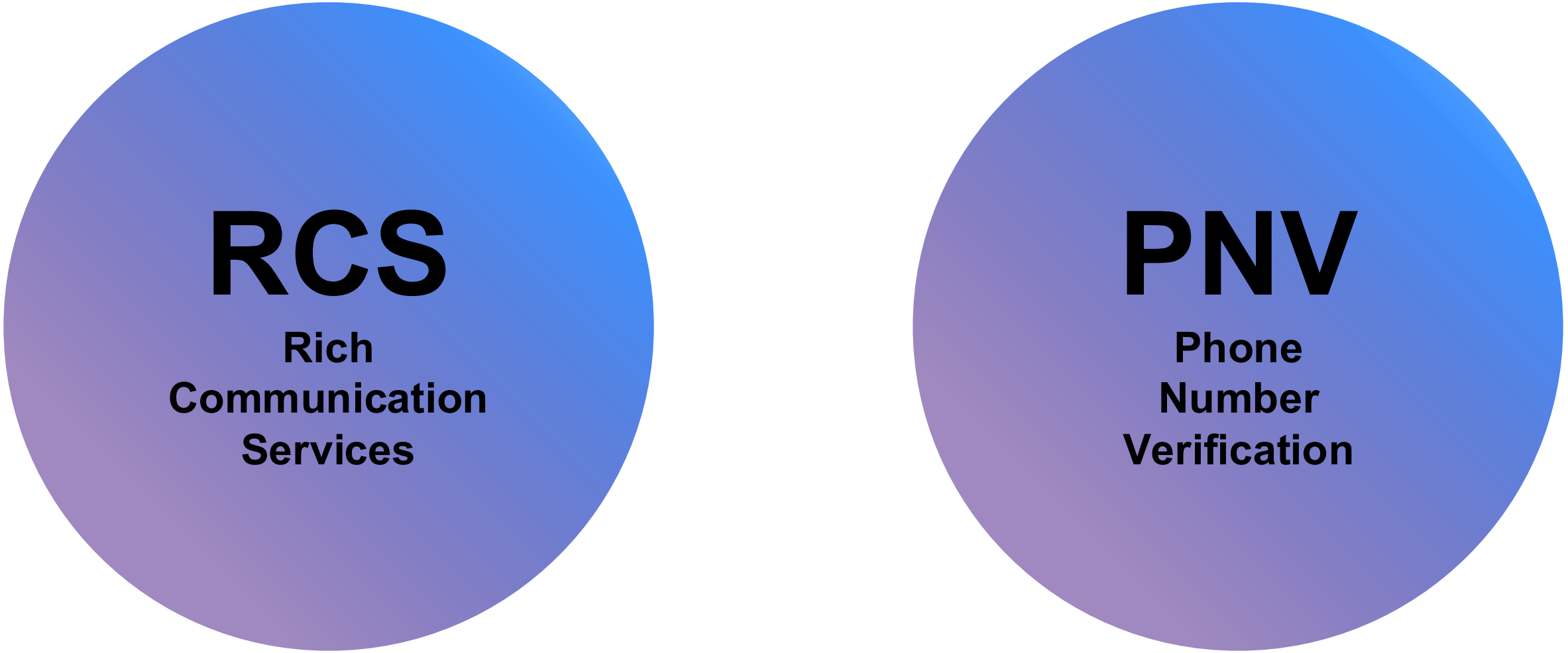
HCLTech | Supercharging Progress™

RCS activation and Phone Number Verification

TS.43 Webinar

Nacho Blázquez
HCLTech Chief Architect BSS/Entitlements

RCS and PNV



Copyright © 2025 HCLTech

Rich Communication Services

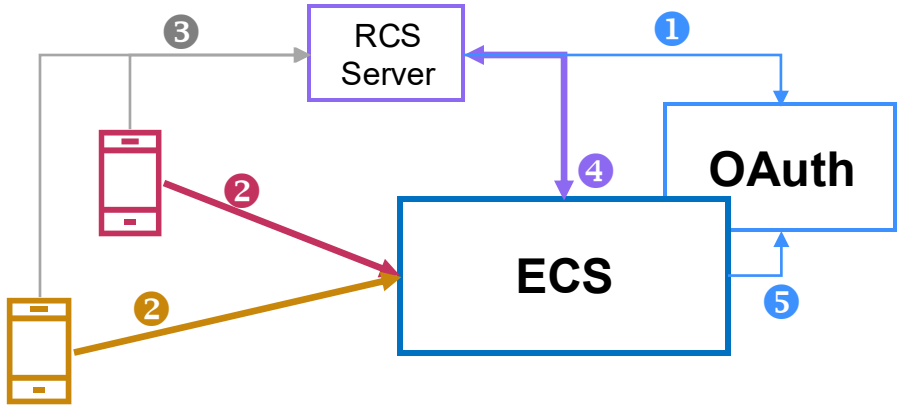
RCS Service Configuration with Entitlements

Messaging Interoperability between OS

- ✓ Silent activation replacing SMS.
- ✓ Deactivation API is currently out of scope of TS.43 but can be included in Entitlement Configuration Server (**ECS**).

Interfaces required for activation

- ❖ TS.43 Temporary Token
- ❖ Non-TS.43 Temporary Token
- ❖ TS.43 GetSubscriberInfo
- ❖ OAuth Server for RCS Authentication



How it works

1. At some point on time RCS request for an access_token
2. TS.43 or non-TS.43 device requests a TemporaryToken to ECS.
3. Device requests RCS onboarding using TemporaryToken
4. RCS Server requests MSISDN (and IMSI) to ECS using **getSubscriberInfo** with **TemporaryToken.**
5. ECS validates access_token (introspection) and provides information to RCS Server to 'onboard' device for RCS service

Copyright © 2025 HCLTech
HCLTech

Phone Number Verification

Validating MSISDN through Entitlement Server (TS.43 spec)

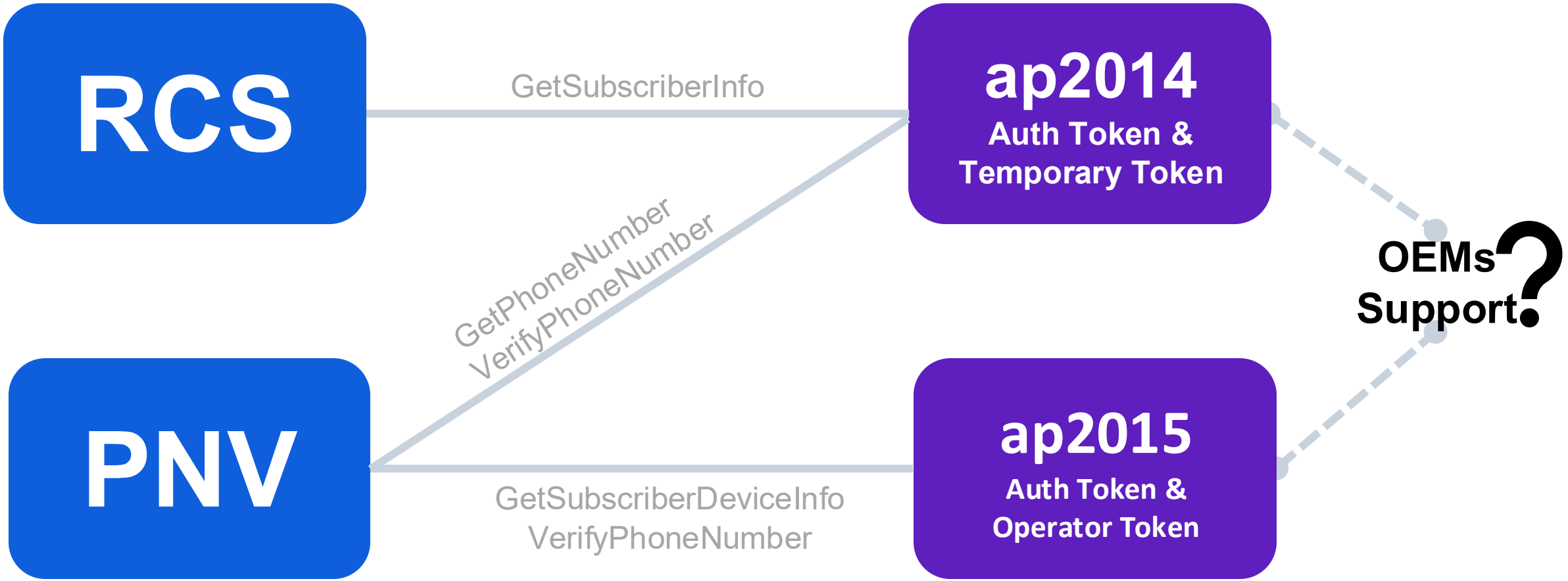
TS.43 enables multiple ways to verify the MSISDN

- Getting MSISDN and comparing with the one provided by the APP:
  - **GetPhoneNumber** / **GetSubscriberInfo** (from **device**): Returns the phone number associated to the devices triggering the request. Number verification can be done in device.
  - **GetPhoneNumber** / **GetSubscriberInfo** (from **App server**): Returns the phone number associated to the devices sharing the token for Authentication. Number verification can be done in device or in server side. App Server authenticates using **Temporary Token**.
- Sending MSISDN for validation in the request
  - **verifyPhoneNumber** (from **device**). Device using internal Authentication validates the provided MSISDN.
  - verifyPhoneNumber (from App Server). Server using **Temporary Token** interacts with ECS to verify the provided MSISDN.
  - **verifyPhoneNumber** (from **3rd Party APP** or **Server**). **Operator Token** is used for authentication when 3rd Party APP or Server can't perform EAP-AKA AuthN.

Copyright © 2025 HCLTech

RCS and PNV implementation

Two use cases and two application IDs



ap2014 & ap2015 are application IDs defined in TS.43

Copyright © 2025 HCLTech

HCLTech

Why Operator token?

Challenge

- ✓ Customers value **silent & secure authentication** solutions, like MSISDN Seamless Authentication which enables a secure and silent authentication process with MNO assets.

Solution

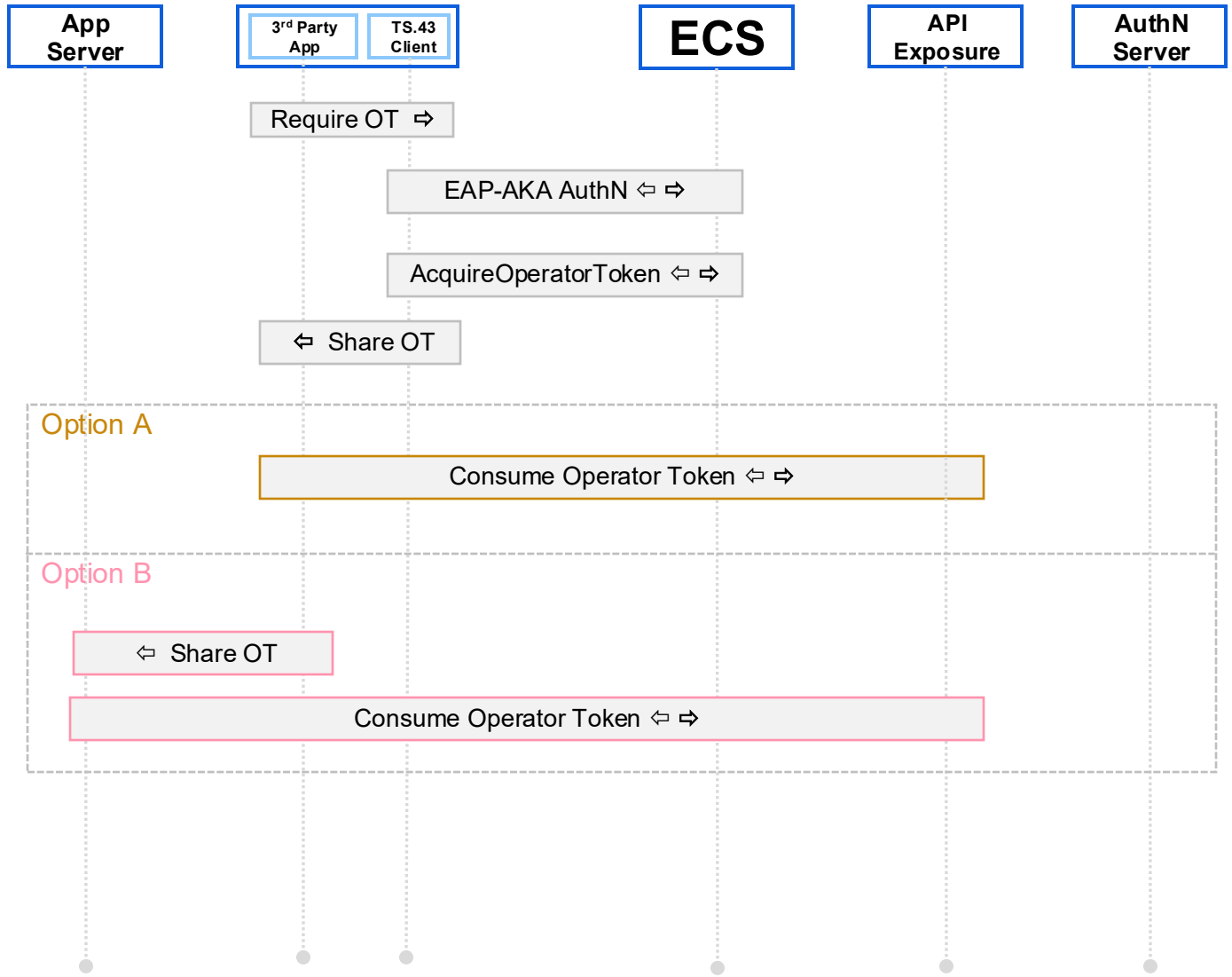
- ✓ **EAP-AKA** solution as the preferred candidate to resolve the challenge (EAP-AKA uses SIM/eSIM assets for AuthN)
- ✓ **ECS is a trusted end point** and available is many Operators. TS.43 defines how devices interacts with ECS.
- ✓ EAP-AKA functions are provided by Operating System APIs. Today, some can be consumed by applications, that obtained MNO Privileges and/or consent from OS manufacturers
- ✓ Requires to define suitable **API and a native OS Client** that would enable 3rd party apps to have a universal and secure MSISDN seamless authentication method.

Goals

- ✓ Relying on SIM capabilities (secret keys) and not on the network.
- ✓ Reachable over Web browsers & native apps and available for any services.

Usage

- ✓ **GSMA TS.43** (Operator Token Consumption) and **GSMA ASAC.01-Seamless Authenticator subsystem enhancement for TS.43 Operator Token** define some consumption examples.



Copyright © 2025 HCLTech
HCLTech

Temporary or Operator Token (TT vs. OT)

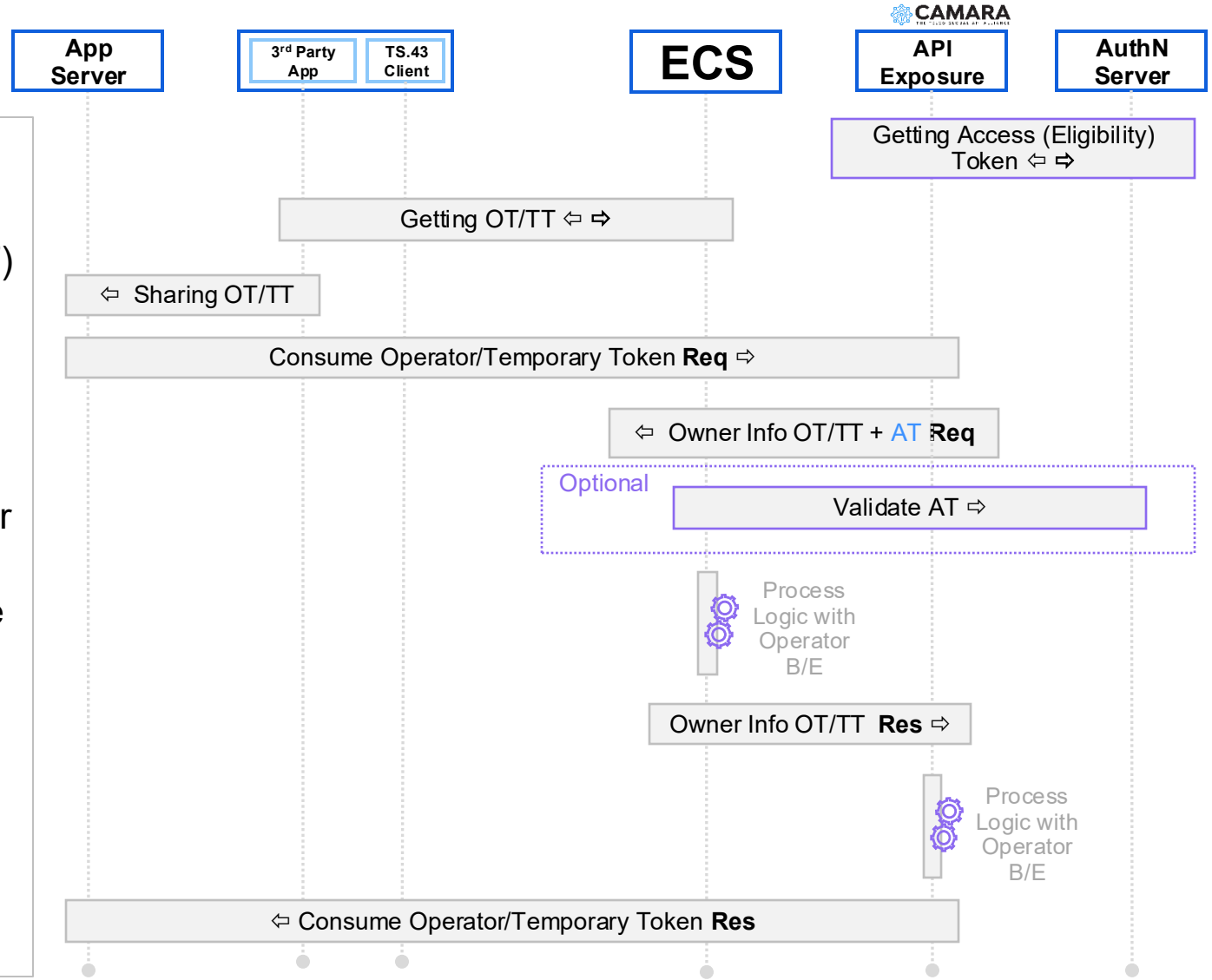
Getting Device Info

Use case

API exposure requires to know which **customer** is the owner of the Operator/Temporary Token (OT/TT) **to be used as primary key** to interact with backends.

How it works

- ✓ App Server uses OT/TT to access some Operator Resources (ex. API exposure).
- ✓ API additional to validate OT/TT, it requires some information about the user/device (MSISDN; IMSI) so it requires interacting with ECS.
- ✓ ECS will interact with backend (if needed) to get the info and provide the proper response.
- ✓ API will use the user/device info to interact with the Operator backend and provide a response to App. Server.



Copyright © 2025 HCLTech
HCLTech

Conclusion

TS.43 provides different tools/features which can be used to define the flow in different ways.

Operators should discuss with device vendors and entitlement server providers to define what's the best approach for them.

Copyright © 2025 HCLTech

HCLTech | Supercharging Progress™

hcltech.com

TS.43 Use Cases:

Satellite Connectivity, eSIM Transfer, RCS, Phone Number Verification

Pavan Nuggehalli

3GPP Standard
Google

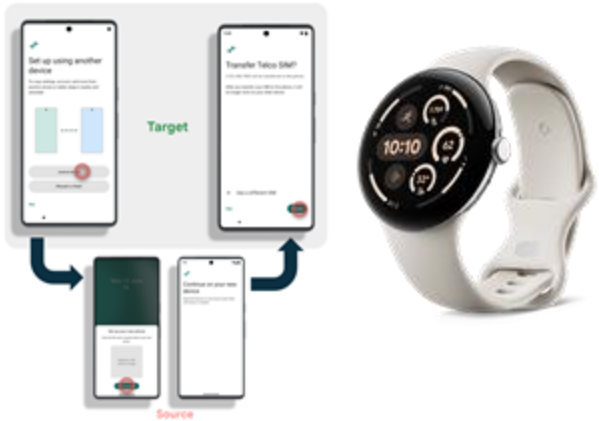
GSMA

TS.43 in Android

Pavan Nuggehalli

Android’s commitment to TS.43

Satellite connectivity



eSIM transfer

User Identity e.g., RCS, Phone Number Verification

A single industry-wide solution benefits CSPs, Vendors, and OEMs

VoWiFi

Data Boost, Meteredness

Satellite Connectivity on Android

How does Android become aware that the phone is connected via Satellite?

Android uses PLMN-id to identify satellite networks

How can a CSP manage access?

TS.43 helps Android identify these PLMNs

- Allowed PLMN and Barred PLMNs

How can a CSP control which services are allowed?

TS.43 based entitlement supports

- Per-subscriber control
- Emergency + Messaging (SMS, RCS)
- Emergency + Messaging + “Lite” data
- Emergency + Messaging + data
- Emergency + Messaging + data + voice

Satellite Connectivity on Android

Why TS.43?

A unified method to manage entitlements for satellite connectivity

- Feature discovery and awareness
- Direct subscription management by CSPs
  - Limit unwanted traffic
  - Provide differentiated service

TS.43 mechanisms

- Entitlement status for SatMode
- List of allowed and barred PLMNs
- List of Allowed services e.g. Messaging, Data, Voice

On-Device Service Activation for eSIM

Why TS.43?

- ODSA provides the most seamless and integrated eSIM activation experience
- Baked into Android's out of the box experience using quick device pairing
- Enables self-serve digital flows for CSPs and improves customer experience

TS.43 mechanisms

- (p/e)SIM-to-eSIM transfer via TS.43 TempToken procedure in combination with
  - D2D proximity
  - Screen lock security challenge
- Provides Primary and Companion device transfer and activation flows
- Supports cross-platform subscription transfer using TempToken approach

Identity:
RCS, Phone Number Verification

Why TS.43?

- Enables 2FA using SIM-based cryptography
- Provides higher level of security and reliability for apps as compared to SMS OTPs
- Native and seamless platform experience on Android

TS.43 mechanisms

- Leverages TS.3 TempToken mechanism as the core building block
- Allows CSPs to deploy one token delegation solution for multiple use cases
- RCS: GetSubInfo provides SIM Id, MVNO info
  PNV: Get/Verify operations for dev needs

Android is TS.43 ready, are you?

Make your IT/BSS TS.43 ready

Internal CSP IT/BSS systems are proprietary and complex, causing delay

By working early with your internal IT teams to make your network TS.43 ready, rollouts can be smoother, faster and less costly

Let's unify around TempToken

The vast optionality of the TS.43 spec opens many ways of realizing TS.43 use cases.

For speed & agility, lets unify around the spec compliant Android implementation using TempToken

Invest once and rollout out many

To optimize the effort and integration cost, CSPs can implement one project with multiple use cases at the same time

Thank you

TS.43 Use Cases:

eSIM Transfer and 5G SA Activation

Florian-Leon Schmitt

Terminal Steering Group Chair
Deutsche Telekom AG

GSMA

TS.43 Entitlement Server

Florian Schmitt, Deutsche Telekom AG

DT Entitlement Server

Ecosystem Support

2017 support of first iOS devices

2021 support of first Android devices

2022 productive support of TS.43

Use Case Support

Phone number Verification

eSIM profile activation

- Primary Device ODSA
- Companion Device ODSA

5G SA activation

Operator Token

Country Support

Operation started in German network

Further integrations rolled out in:

- Austria
- Croatia
- Slovakia
- more on the roadmap

DT is developing and operating an in-house Solution of Entitlement Server

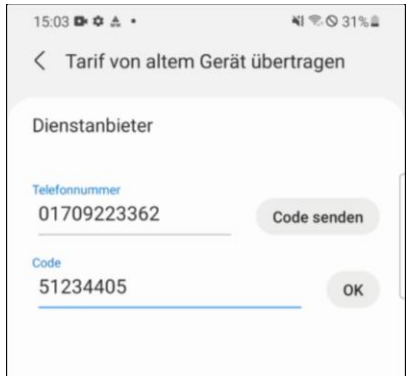
eSIM Profile Transfer - History

First implementation on iOS

2020

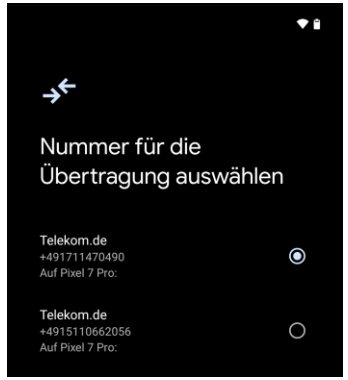
First proprietary Android implementation, based on SMS-OTP

2021



First TS.43 implementation based on temporary-token

2023



Android platform support of TS.43

Supported on 7 device OEMs

2025

Cross platform

5G SA Activation

5G SA Activation

Background: For migrating devices from 5G-NSA to 5G-SA, rollouts needed to work as flexible as possible

Customers want to see immediate success, after booking an “SA” option

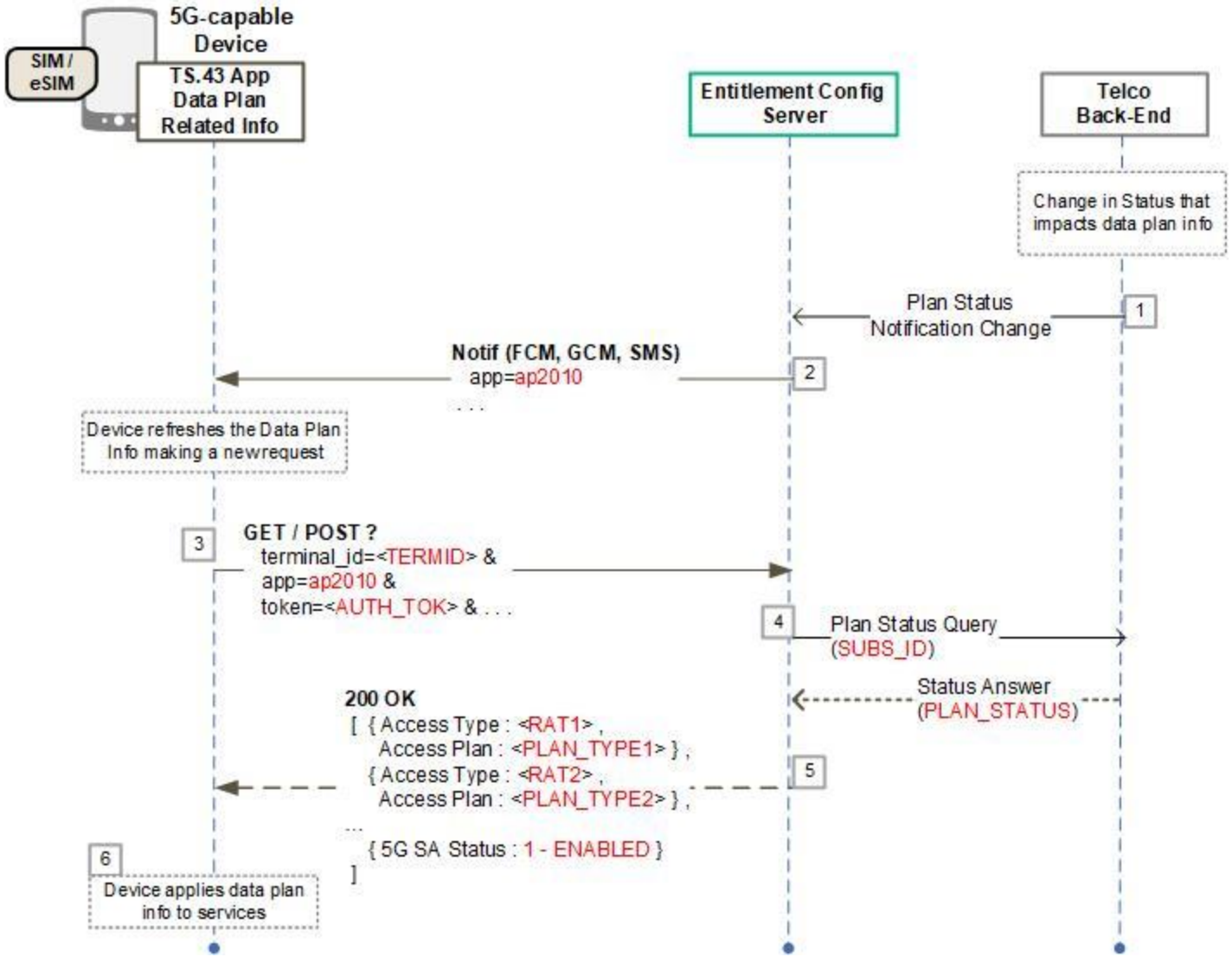
Problem: Devices in the field were usually camping on 5G-NSA

Initiating 5G-SA activation (N1) required a Powercycle of the device

Solution: Using the TS.43 DataPlan Use Case, the Network can indicate network status flexibly

Device can instantly react and connect to 5G-SA (N1), when indicated by network

5G SA Activation - Flow



5G SA Activation

Why TS.43 ?

- TS.43 is an established specification in the industry, well understood and adopted by key organizations
- TS.43 offers plenty of good tools and vehicles to utilize
- TSG-VVEC is a well-functioning group with high-quality output
- GSMA working groups are contribution based, new features are always welcome
- Standardization encourages adoption & decreases fragmentation

Thank you

Deutsche Telekom AG
Florian Schmitt
Florian-leon.Schmitt@telekom.de

GSMA™

Q&A

Survey

Scan to participate

Please take a moment to complete this short survey

- It will take just 2 mins
- GSMA Confidential (Disclaimer Note: All responses will be anonymous)
- Thank you!

GSMA

GSMA™

TS.43 Entitlement Server Implementation

Second Session: 2nd July 14:00 UK time