axonect

Reimagine Mobile Network Seamless Authentication with

GSMA TS43 ASAC.01 v1.0 & Axonect Entitlement Server

AXIATA DIGITAL LABS

Introduction

The mobile landscape is exploding with applications that have become woven into the fabric of our daily lives. From payments and bookings to self-care and essential services, these apps require secure and seamless authentication for both customer identification and transaction authorization. Traditionally, mobile apps have relied on network operators for user verification, leading to a patchwork of methods like header enrichment, OTPs, and SSO – each with drawbacks impacting practicality, security, or user experience. Recognizing these limitations, GSMA has taken a bold step forward with their extended Technical Specification TS43 - Service Entitlements, called ASAC.01 v1.0. This innovative approach promises a secure and seamless authentication mechanism, finally addressing the challenges of the past. While industry adoption is on the horizon, Axonect Entitlement Server is committed to embracing this specification. With this future-proof solution on our roadmap, we aim to provide a standardized and innovative path towards a seamless authentication experience.

The Need for Seamless Authentication

Imagine using your favorite mobile app, whether for payments, booking flights, or managing healthcare – doesn't involve a flurry of login credentials or frustrating authentication steps. Seamless authentication aims to achieve just that. It's a user-centric approach that prioritizes a smooth and frictionless experience while maintaining robust security.

Current Approaches and Their Drawbacks

While seamless authentication is ideal, mobile network operators (MNOs) have traditionally relied on various methods to verify users and sessions for mobile applications. However, these methods often fall short in achieving a perfect balance between security and convenience. Let's explore some common methods and their limitations.

1. Header Enrichment: This involves the MNO adding information about the user (like their MSISDN or location) to the network data packets. While convenient, header enrichment can raise privacy concerns as it exposes user data to multiple parties. Additionally, it lacks the flexibility to handle complex authentication scenarios. Later the header was enriched with encoded data only to be decoded at the consumption level. However, a limitation is there, as the header enrichment can only be done for http requests. Furthermore, the issue is there when the customer is using Wi-Fi or tethering (Smartphone Mobile Hotspot (SMHS)), the header enrichment information is not entirely accurate.
2. One-Time Passwords (OTPs): OTPs offer an extra layer of security by requiring a temporary code for logins. While effective, they can be cumbersome and prone to delays or technical glitches, disrupting the user experience.
3. Single Sign-On (SSO): SSO allows users to log in to multiple applications with a single set of credentials. This simplifies things for users, but it can raise security concerns if a single breach compromises access to multiple accounts. Additionally, SSO often relies on third-party providers, introducing complexities in integration and potential points of failure.

These methods highlight the challenges MNOs face in striking a balance between security and user experience.

Traditional approaches often have drawbacks in terms of,

Privacy

Exposing user data beyond what's necessary for authentication.

Security

Reliant on single points of failure or vulnerable to breaches.

Convenience

Disrupting user experience with cumbersome steps or delays.

ASAC0.1 v1.0

Recognizing the limitations of traditional methods, GSMA has introduced a groundbreaking solution – GSMA TS43 ASAC.01 v1.0. This specification revolves around a revolutionary concept which is **Operator Tokens**.

Understanding Operator Token

Imagine a secure digital container holding information that uniquely identifies a user's home Mobile Network Operator (MNO). This container, called an Operator Token, acts as a portable credential. It empowers mobile applications to verify a user's identity and MNO affiliation, regardless of the network they're currently connected to (cellular or Wi-Fi) even when roaming.

Proposed Architecture

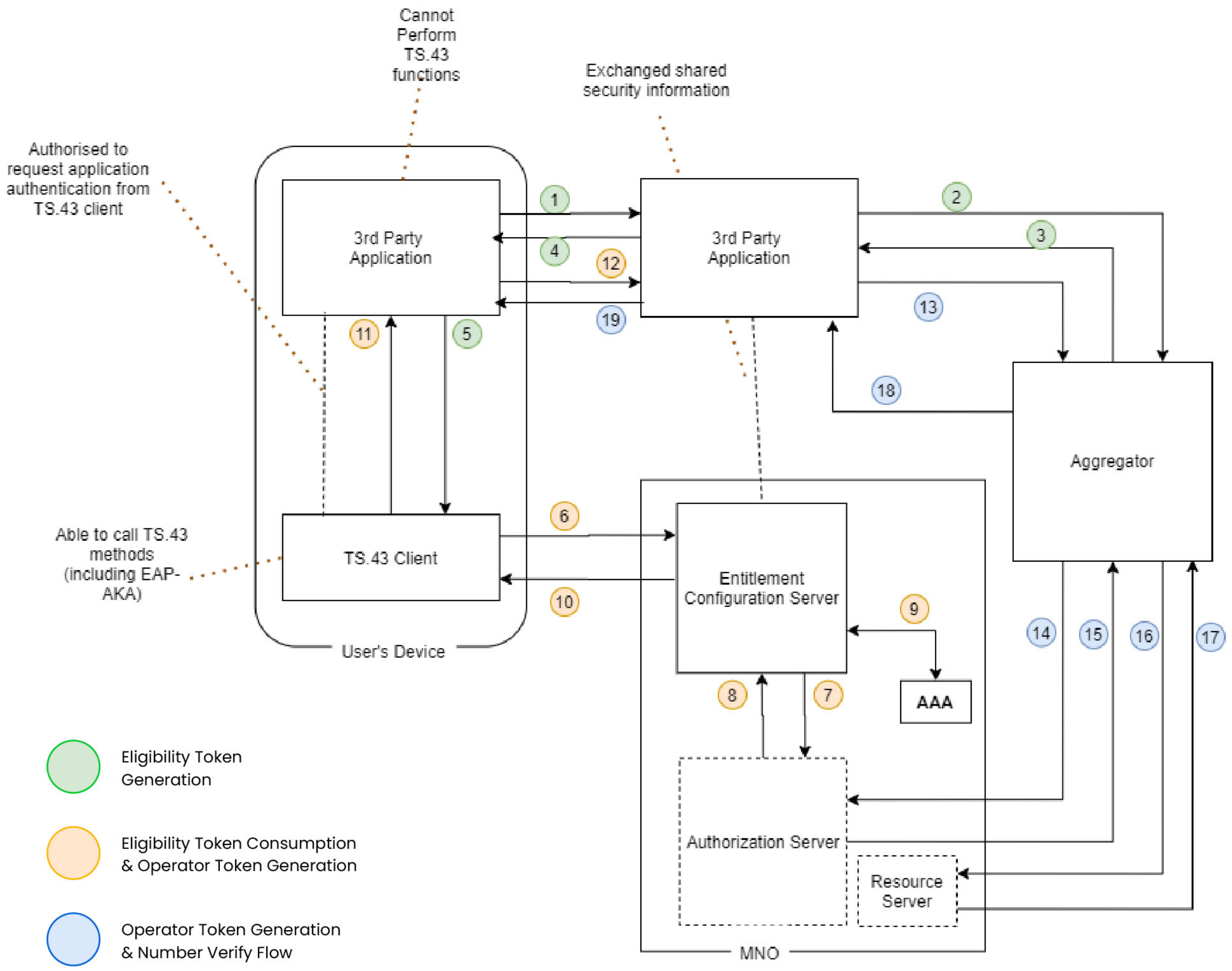
Cannot Perform TS.43 functions
Exchanged shared security information
Authorised to request application authentication from TS.43 client
3rd Party Application
3rd Party Application
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
Aggregator
Able to call TS.43 methods (including EAP-AKA)
TS.43 Client
User's Device
Entitlement Configuration Server
AAA
Authorization Server
Resource Server
MNO
Eligibility Token Generation
Eligibility Token Consumption & Operator Token Generation
Operator Token Generation & Number Verify Flow

Figure 1 : ASAC.01 Architecture

Component Definitions

Component	Description
3rd Party Application	Mobile Application/Web client which needs to authenticate its users. (Both front end and Back end)
Aggregator	A common gateway module connecting multiple MNOs and exposing the "Number Verify API"
Entitlement Configuration Server	Entitlement Server
Authorization Server	Operator token generation/validation
TS.43 Client	In-built service on customers device (Mobile/Tablet etc.) supported by its operating system.
AAA	Authentication, Authorization, Account module on MNO's network for EAP-AKA authentication.

Call flow

The whole number verification flow can be broken down into 3 main levels. Those are,

1. Eligibility token generation
2. Eligibility token consumption and Operator token generation
3. Operator token consumption and complete number verify.

Now let's deep dive into the call flow,

Eligibility Token Generation:

1. The 3rd party application initiates the Number Verification flow with the aggregator. Calling Number Verify API (This API can be an implementation of CAMARA Number Verify API)

2. The Aggregator generates the Eligibility token. (This can have multiple implementations like Aggregator generating eligibility token or aggregator get the token generated by the authorization server.) and sends the request back as a http 302 redirection for 3rd party application.

3. 3rd party application follows the redirection, and it directs to the TS 43 client in built to user's device.

Eligibility Token Consumption and Operator Token Generation:

1. TS43 Client on the user's device, interacts with the Eligibility Token and initiates communication with the user's home MNO.

2. Interaction with home MNO is done via two steps. The first one is to validate TS43 client with MNO's Entitlement Server called pre-validation. This is based on DIAMETER EAP-AKA protocol. In this stage, MNO can identify the identification of the user in MSISDN level. The second one will be based on APIs exposed via Entitlement Server to validate eligibility token and generate Operator token.

3. Authorization Server Verification: The Entitlement Server interacts with the Authorization Server to verify the Eligibility Token's validity and the legitimacy of the request.

4. Upon successful verification, the Authorization Server issues an Operator Token containing information about the user and their home MNO. This token is securely transmitted to the user's device TS43 client.

5. Ts 43 client then presents this information to the 3rd party app in the form of http redirection.

Operator Token Consumption and Number Verification:

1. The aggregator interacts with the user's MNO using the information within the Operator Token (without revealing the MSISDN). This allows verification of the phone number's existence and association with the user's home MNO.

2. MSISDN Retrieval: In some scenarios, depending on specific regulations or use cases, the MNO might utilize EAP-AKA to authenticate the user on their network. This is the only step where the MSISDN might be revealed. With user consent, the MNO could share the verified MSISDN with the aggregator.

3. Verification Result: The aggregator receives the verification result from the MNO (confirmed or not confirmed) and relays it back to the 3rd party application.

Limitations in the implementation

While GSMA's TS43 ASAC.01 v1.0 offers a promising approach to seamless and secure authentication, there are limitations to consider:

1. Industry Adoption: The most significant barrier is the current lack of widespread adoption across the industry. While the GSMA has introduced the specification, it requires buy-in from various stakeholders, particularly Original Equipment Manufacturers (OEMs) who need to integrate the TS43 Client API into their devices. Apple specifically uses their proprietary version of EAP-AKA and they may not be providing this for third party validations as of now.

2. Integration Challenges: Integrating ASAC with existing network infrastructures and mobile applications can be complex. MNOs need to adapt their systems to handle Operator Tokens and interact with the Authorization Server. Third-party application providers will also need to adjust their development processes to leverage Operator Tokens/TS 43 clients within their authentication flows.

3. Regulatory Considerations: Depending on the region and specific use cases, there might be regulatory hurdles to address. Data privacy regulations and user consent requirements need to be carefully considered when handling user information within Operator Tokens.

4. Potential for Misuse: As with any new technology, there's always a potential for misuse. MNOs and service providers need to implement robust security measures to prevent unauthorized access or manipulation of Operator Tokens.

Axonect Entitlement Server

Axonect Entitlement Server is a robust and feature-rich platform designed to streamline entitlement management for various applications, particularly within the mobile network operator (MNO) space. As you embark on implementing GSMA's ASAC for secure and seamless authentication, Axonect Entitlement Server provides a solid foundation with its current feature set and a roadmap aligned with future advancements.

Current Strengths for Seamless Entitlement Management

1. Proven eSIM Management: Axonect Entitlement Server offers comprehensive functionalities for managing eSIM deployments, including provisioning for secondary devices like Apple Watches.
2. Streamlined Workflows: Features like eSIM plan transfer between iPhones demonstrate Axonect Entitlement Server's ability to manage complex entitlement scenarios efficiently.
3. Robust Administration: The Axonect Control Center (Unified Interface for Axonect) empowers MNOs with centralized configuration management, audit trails, and user access controls.
4. Focus on Security: Security is a cornerstone of Axonect Entitlement Server, adhering to industry standards, this focus on data protection aligns perfectly with the secure nature of GSMA's ASAC and Operator Tokens.

A Roadmap Aligned with Future Needs

While the current features provide a strong foundation, Axonect Entitlement Server's roadmap demonstrates a commitment to continuous improvement.

1. Expanding Device Support: Planned support for Samsung Gear/Watch and other device types signifies adaptability, making the platform well-positioned for future advancements in the connected device landscape.
2. Advanced Entitlement Management: Features like VoLTE/VoWiFi entitlements and tethering entitlements showcase the platform's ability to handle a wider range of service entitlements – a capability that will be crucial as ASAC integration evolves.
3. GSMA ASAC.01 Support: Axonect Entitlement Server will focus on implementing workarounds for ASAC.01 for operators to get the advantage of.

A Flexible Approach for Collaborative Innovation:

The proposed flexible approach to development is particularly noteworthy. This ensures that Axonect Entitlement Server can adapt to evolving needs as ASAC adoption matures. By prioritizing collaboration, we can work together to shape the future of secure and seamless mobile network authentication.

In conclusion, Axonect Entitlement Server's current strengths, commitment to future advancements, and flexible approach make it the ideal platform for MNOs to leverage GSMA's ASAC for secure and seamless mobile network authentication. With Axonect Entitlement Server as your foundation, you can unlock a future of streamlined workflows, enhanced security, and a platform that adapts to the ever-changing mobile network landscape.

References

GSMA ASAC.01-v1.0 - https://www.gsma.com/newsroom/wp-content/uploads//TS.43-v11.0-Service-Entitlement-Configuration.pdf

Cyber 2 Tower - 11th Floor Jl HR Rasuna
Said Blok X-5 Kav 13 Kuningan South
Jakarta 12950, Indonesia

Level 11, Parkland, 33 Park Street,
Colombo 2, Sri Lanka

Axiata Tower, 25 Jalan Steen Sentral 5,
Kuala Lumpur Sentral 50470 Kuala
Lumpur, Malaysia

CONTACT US

axonect

@ info@axonect.com

axonect.com