Network based Tokens
Version 1.0
28 February 2025

Security Classification: Non-Confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Copyright © 2025 GSM Association

Disclaimer

The GSMA makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Compliance Notice

The information contain herein is in full compliance with the GSMA Antitrust Compliance Policy.

Table of Contents

1 Introduction 3
1.1 Overview 3
2 Scope 3
2.1 Definitions 4
2.2 Abbreviations 4
2.3 References 5
2.4 Conventions 5
3 Use Case Summary 5
3.1 RCS 5
3.2 Open Gateway 5
3.3 Enterprise Slicing 7
3.4 Emergency Services 7
3.5 Remote maintenance 7
3.6 Unnatended remote devices 8
3.7 Slicing-based Consumer Services 8
4 Current ecosystem impact 8
5 Conclusions 10
6 Document History 11
7 Other Information 11

1 Introduction

1.1 Overview

Authentication mechanisms are essential for operators to verify the identity of customers, thus protecting sensitive resources and data from unauthorized access. These mechanisms help prevent fraud as industries require stringent security and access control measures. Furthermore, the implementation of strong authentication and authorization systems is crucial to maintain customer confidence, ensuring that their data and services are protected from unwanted access. This allows only authorized users or applications to access specific resources and data, avoiding potential security breaches and maintaining confidentiality.

However, for such approaches to be successful the required technology shall be supported by all stakeholders in the ecosystem (Device OS, CSPs, developers). The objective of this white paper is to describe the possible use cases associated to a standard utilizing network token-based authentication technologies to raise industry interest and adoption of such mechanisms.

In this context, network-based tokens as described in GSMA Permanent Reference Documents TS.43 [4] and ASAC.01 [5], provide secure and certifiable authentication and authorization solutions when third party applications running on an end-user´s mobile device consume network services.

2 Scope

The objective of this whitepaper is to inform and raise the industry interest for the need to strengthen the authentication mechanisms for certain sensitive use cases through the introduction of network-based tokens.The document describes a set of possible use cases that will require network-based token capabilities, and additionally identifies the requirements on the different actors to implement the proposed mechanisms: OS developers, application developers and network operators.

2.1 Definitions

Term	Description
App Token	An App token [4] is a network-based token used by third-party applications to authenticate itself when requesting access to certain MNO resources. Application backends acquire app tokens by presenting their client credentials to the ECS. App tokens convey the identity of the application, independently of the subscriber/user context.
Authentication	It is a process that verifies the identity of someone or something.
Authorization	It is a process of verifying what the requestor have access to.
Network-based token	A temporary credential generated by using MNO assets, like the SIM card, which can be used on several use cases.
Operator Token	An Operator Token [4][5] is a network-based token that allows eligible third-party applications to authenticate subscribers/end-users via Open Gateway or through bilateral agreements. It is intentionally designed without a specific data structure, giving the maximum flexibility on use cases implementation regarding the information exchanged between the MNO and the application. Client applications acquire operator tokens from the ECS after the subscriber is properly authenticated. Each operator token is issued to a specified client application and conveys the identity of an individual subscriber/end-user. Operator tokens provide a standardised subscriber authentication mechanism, especially useful for applications that require access across multiple networks.

2.2 Abbreviations

Term	Description
B2B	Business to Business
B2B2C	Business to Business to Customer
B2C	Business to Customer
CSP	Communications Service Providers
ECS	Entitlement Configuration Server
eMBB	Enhanced Mobile Broadband
IMSI	International Mobile Subscriber Identity
MDM	Mobile Device Management
MNO	Mobile Network Operator
MSISDN	Mobile Station Integrated Services Digital Network
MVP	Minimum Viable Product
MVNO	Mobile Virtual Network Operator
OGW	Open Gateway
OTP	One-Time Password
OTT	Over The Top
PTT	Push-to-Talk
RCS	Rich Communications Services

Term	Description
SMS	Short Message Service
OS	Operating System

2.3 References

Ref	Doc Number	Title
[1]	RFC 2119	“Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner, March 1997. Available at http://www.ietf.org/rfc/rfc2119.txt
[2]	RFC 8174	Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words https://www.rfc-editor.org/info/rfc8174
[3]	RCS	Rich Communication Services - Networks (gsma.com)
[4]	TS.43 v12	TS.43 Service Entitlement Configuration (gsma.com)
[5]	ASAC.01	ASAC.01 v1.0 (gsma.com)

2.4 Conventions

“The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC 2119 [1] and clarified by RFC8174 [2], when, and only when, they appear in all capitals, as shown here.”

3 Use Case Summary

This section outlines a set of use cases where network-based tokens are a key enabler component in the industrialisation of the service.

3.1 RCS

RCS enhances traditional SMS messaging by offering a suite of service capabilities, including group chat, file transfers, typing notifications, and more. It aims to provide a modern messaging experience akin to popular OTT platforms [3]. While RCS presents opportunities for enhanced communication, challenges such as client verification and interconnection with other RCS providers may arise.

A new method was defined [4] for RCS to obtain the MSISDN of the user without disclosing information about the IMSI. Additionally, this method replaces the SMS OTP method. RCS clients receive a network-based token from the entitlement server, which is sent to the RCS configuration servers on their request. Upon verification of the token by the RCS configuration server with the network, the information is returned, including the MSISDN and information on the MVNO.

3.2 Open Gateway

In the Open Gateway context, the Operator Token generated by the network in the Entitlement Configuration Server (ECS) is used for subscriber authentication. This token can be used by applications as a method of subscribers’ identification for any API within Open Gateway.

The use of Operator Token addresses the key issues identified by operators in Open Gateway regardless of the connection type (including Wi-Fi). It avoids authentication failures associated

with VPN connections, prevents the authentication threads associated with tethering connections and allows a proper routing of requests through channel partners. The aim is also to achieve a compatible solution with the main device OS developers.

Operator Token capabilities provide significant improvements to the user experience, compared to existing authentication mechanisms e.g. by using device IP. The ability to authenticate regardless of the access network enables end-users to avoid switching the connection type and to achieve authentication via Wi-Fi smoothly even when mobile network is congested or not available.

Reducing human intervention improves user experience and furthermore prevents end-users from abandoning a service because of complexity, which is also beneficial for customers in B2B2x scenarios.

One specific use case where this solution can be applied is number verification with silent authentication, where the operator token is used to verify the end-user´s phone number without human intervention (e.g., avoiding SMS OTP procedures).

Operator Tokens do not necessarily mandate the usage of Open Gateway. Another option is to implement them based on bilateral agreements between apps & Operators, or with the help of a carrier privileged app on the device. The Operator Token is intentionally designed as a transparent parameter, meaning there is no specific structure or content mandated in the protocol. This gives maximum flexibility depending on the intended use. If implemented, any other relevant parameter could be transferred between Operator and application, allowing for many more use cases.

3.3 European Digital Identity Wallet

The use of Operator Token [5] enables some of the use cases addressed in the European Digital Identity Wallet.

The primary objective of the European Digital Identity Wallet is to promote trusted digital identities for all Europeans allowing users to be in control of their own online interactions and presence. It can be seen as a combination of several products and trust services that enable users to securely request, obtain and store their information, allowing them to access online services, share data about themselves, and to electronically sign/seal documents. Some examples are listed below.

- **Mobility and digital driving licence:** The EUDI Wallet may enable a fully digital European Driving Licence for online and offline scenarios. It could link to a series of further attestations offered by public or private providers covering legal requirements (e.g. Certificate of Professional Capacity) or business requirements and standards (e.g. for road tolling) in the road transport area.

- **Health:** Easy access to health data is crucial in both national and cross-border contexts. Based on the experience from the EU Digital COVID Certificate, the EUDI Wallet would enable access to patient summaries, ePrescriptions, etc.

- **Education / Diploma:** Providing documents for qualification recognition procedures can be costly and time-consuming for end-users, companies and employers, education and training providers, and other academic institutions. The EUDI Wallet can be a repository for educational digital credentials as electronic attestations of attributes and a means for exchanging them.

- **Digital Finance:** The EUDI Wallet could facilitate payment authentication with a high degree of security and enable a frictionless experience in payments.

3.4 Enterprise Slicing

Enterprise slicing is one of the key segments for the B2B business. The operator can offer connectivity solutions for enterprise employees avoiding classical VPN connections, supporting new functionalities, security, and improved quality of service for the corporate segment. A typical use case is to provide enterprise intranet access to work applications installed on employee´s devices.

An App token mechanism provides a standard way to identify, authenticate and authorize specific applications within the end-user device to access the enterprise slice. As it is a standard method its massive adoption would make it work over any terminal operating system. Then it would not be necessary to implement proprietary solutions such as MDM to map applications to an enterprise slice. Additionally, it is possible to implement the use case with enterprise and personal devices (Bring Your Own Device).

3.5 Emergency Services

A typical example is the deployment of emergency services over a prioritised slice. In such a scenario, it's critical that only first responders have access to the slice and only authorised applications can use the slice to ensure service delivery and integrity.

A possible use case could be to provide an emergency slice to police forces for their communications, such as a Push to Talk (PPT) application. Each officer would carry a device with an operator-authorised PTT application to direct their communications traffic through the emergency slice while the rest of the applications in the device access the default eMBB slice. Since it will be a critical service, the proposal is to rely on Operator Token mechanism for subscriber authentication on the PTT application and App Token mechanism to authenticate and authorize the application requesting the traffic on the specific network slice deployed for the use case.

This ensures that only users with valid permissions execute the service by using seamless authentication methods for subscribers and applications. Network-based tokens also leverage real-time control over who uses the slices which is key in an emergency communications environment.

3.6 Remote maintenance

Within 5G a successful use case deployed in the B2B space is remote or assisted maintenance, where an employee operates in a critical site and then is guided by a remote specialist or an AI based application.

In such scenarios maintaining quality for the communication is critical to avoid possible human disaster. The slice usage has to be limited to the application required to execute the use case. Such control for the slice access can be done by application token.

3.7 Unattended remote devices

A typical IoT use case is to deploy unattended devices for remote monitoring or remote-control use cases applied to utilities. One of the main problems is the initial provisioning and the potential modifications of the credentials for such devices to log in to the proper application.

To avoid human intervention or out of band networks, Operator token can provide the proper capabilities to perform a seamless authentication and identification of the device on such use cases.

3.8 Slicing-based Consumer Services

The residential segment is a potential target for operators to offer their customers enhanced connectivity and differentiated services. This could ensure that the customer gets the best network experience to enjoy services without interruption or congestion.

Currently end-users cannot define the applications that make usage of the slices contracted with the carrier. As an example, it is assumed that a video slice will be accessed by all the applications categorised as video by the device OS store. However, due to volume-limited data packages a user may decide to restrict his premium connectivity only to a certain set of video applications. An App token can be used to identify the applications enabled by the end-user to consume its premium connectivity.

To achieve the above, operators should have visibility of the identity of the application and the subscriber behind the App token request.

Enhancement to this use case can also be foreseen where content platforms would need to enforce end-user authentication by leveraging Operator token for number verify for instance.

4 Current ecosystem impact

In order to enable the previous use cases and some others to come, the following ecosystem actors shall support the implementation requirements of network-based tokens as defined in [4] and [5]:

- Network Operators
- Device OS providers
- Vertical Application

In B2C, B2B, B2B2x use cases, the customer and/or end-user will not have to implement anything specific: he will simply use his application that will transparently manage the required network-based tokens by interacting with the network and the device OS.

However, in some cases, the customer and/or end-user may have to contractually agree on some specific terms and conditions with his network operator and/or application providers to benefit from the services enabled by network-based tokens use.

Table 1 describes the relevance and the current impact on the different actors involved in each network-based token mechanism to understand the requirements to cover if existing.

Actor	App Token Requirements	Operator Token Requirements
Device OS	OS shall support the capability to expose an API letting application frontends to provide an App Token when requesting a network connection. OS shall implement a TS.43 client supporting the App Token use case described in TS.43 [4] to authenticate apps with the network operator (validate the App Token). OS shall enforce properly the application traffic mapped with the App Token provided by the application.	OS shall support the capability to expose an API letting application frontends to request an Operator Token. OS should implement a TS.43 client supporting the Operator Token use case described in [4].
Network Operator	Network operator shall implement an Entitlement Server supporting the App Token use case described in [4]. Entitlement Server shall generate App Tokens for the application backend. Entitlement Server shall validate App Tokens upon validation requests coming from end-users' devices. Currently main Entitlement Server providers open to include App Token use case in their roadmaps.	Network operator should implement an ECS supporting the Operator Token use case described in [4]. Network operator shall generate Operator Tokens [4][5] for the application frontends at the Auth Server. Network operator shall validate Operator Tokens upon validation requests coming from application backends. Upon a successful Operator Token validation, shall provide the agreed information with the application (i.e. depending on the OGW API consumed).
Application	Application backend shall request an App Token for every application frontend that needs to access to a specific network resource (typically a network slice) within the operator. Application frontend shall provide the App Token to the end-user device OS when requesting network connection. It can manage as many App Tokens as needed by the application.	Application frontend shall request an Operator Token to the device OS through an API. Application backend shall provide the Operator Token to the network operator when consuming concrete network capabilities.
End-user	The end-user should have control on the applications making usage of his premium connectivity (i.e. a network slice) in B2C scenarios.	End-users can enjoy simpler and seamless authentication methods.
Customer	The customer should have control on the applications within his devices making usage of his premium	Customer could leverage on Operator Token the authentication

Actor	App Token Requirements	Operator Token Requirements
	connectivity (i.e. a network slice) in B2B and B2B2x scenarios.	and identification of its end-users in B2B2x scenarios.

Table 1: Current ecosystem impact

5 Conclusions

This paper describes the advantages of network-based tokens for the telco service industry. The technical capabilities offered by network-based token have been proven by their use in the RCS service and they have a significant potential impact on new services and opportunities for operators.

The solutions will provide clear means for:

- Authorised apps and developers to identify end-users. An imminent use case is an enhanced number verify process.
- B2B and B2C customers to select the applications allowed to consume their specific premium connectivity. This is required to ensure critical use cases to behave properly or to have control from the user on premium data consumption.

Whilst the demand for these capabilities seems clear, an industry endorsement is needed to foster their adoption. Furthermore, it is important to create the greater interest in network-based token mechanism through the development of MVPs that can efficiently and practically demonstrate the benefit of this mechanism.

In order to benefit from these capabilities and to support future use cases, not only network operators but also device OS providers and application developers have to endorse GSMA standards [4][5] in order to ensure a wide market penetration.

Exposing these capabilities through OGW could help in fostering MVPs and industry adoption of these mechanisms.

Document Management

6 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	Feb 2025	Approved	Technology Group	GSMA

7 Other Information

Type	Description
Document Owner	Technology Group
Editors / Company	Ian Pannell / GSMA

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.