GSMA

Mobile Number as a Verifiable Credential in eIDAS 2.0 Wallets

October 2023

GSMA

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Antitrust Notice

Introduction

Overview

In view of the importance of mobile number verification to digital security, the GSMA, specifically representing the European Mobile Network Operators involved in identity services in this instance, proposes this whitepaper for the benefit of the nascent eIDAS ecosystem. This whitepaper sets out why and how eIDAS 2.0 Wallets would benefit from the Mobile Number as a Verifiable Credential. The document first examines the current landscape for mobile number verification and the implication of migration towards EUDI wallets. Existing mobile number verification solutions are in use across many digital services including the mobile industry itself. These solutions will need to evolve to integrate successfully in the eIDAS 2.0 framework. This document then studies the feasibility of adding a verified mobile number to the EUDI Wallet as a QEAA issued by the MNO it is currently bound to. This proposal will enable discussions with the eIDAS ecosystem in order to initiate the specification process.

Abbreviations

ARF	Architecture and Reference Framework
EUDI	European Digital Identity
MNO	Mobile Network Operator
PID	Person Identification Data
QEAA	Qualified Electronic Attribute Attestation
QES	Qualified Electronic Seal
QTSP	Qualified Trust Service Provider
VC	Verifiable Credential

Mobile Number Verification: Current landscape and necessary evolution towards eIDAS 2.0

This chapter introduces the current landscape for mobile number verification and the implication of migration towards EUDI wallets. Existing mobile number verification solutions are in use across many digital services including the mobile industry itself. These solutions will need to evolve to integrate successfully in the eIDAS 2.0 framework.

Mobile Number as easy to use universal identifier

Historically, the mobile number has been one of the most popular possession factors in two-factor-authentication by using a One Time Code sent by SMS. The reasons why the mobile number is so popular as an authentication factor are its widespread adoption by the population (nearly everybody uses a mobile phone and has a mobile number), that it can be used to contact the user directly, and that in case of loss or theft of the SIM card it can easily be restored, with the assistance of the helpdesk of the mobile operator.

Furthermore, the phone number is human readable and most people know their mobile phone number by heart, because they often need to share it or fill it out on onboarding forms. A mobile number is highly personal, can be used to identify end-users with high precision, and is highly secure because of the SIM / eSIM technology used; thus the mobile number forms an attractive identifier for many relying parties.

Relying Parties demand secure and seamless migration of existing user accounts when introducing EUDI wallets

For relying parties that currently rely on the mobile number as a second authentication factor, it is imperative when introducing eIDAS2.0 wallets, that the wallet can be added in a secure way to their installed base user accounts. A typical approach for adding a new wallet to an existing user account is letting the user log in with the existing credential method, and then log in within the same session with the wallet.

The disadvantage of such an approach is that it is also susceptible to social engineering attacks, resulting in account takeovers. For example, a fraudster might offer a user in-person assistance with an issue with an application. The fraudster tricks the user into entering their credentials, and when the user has logged in the fraudster adds a wallet controlled by the fraudster as a new login option to the existing user account, and by which the fraud will be committed.

By adding the mobile number as a Verifiable Credential (VC) to the EUDI wallet such fraud scenarios can be prevented, because both the existing account and the wallet will need to contain the same mobile number when adding the wallet as a login option. Today how to add such a Verifiable Credential to the wallet is not yet specified, and the GSMA European Identity Group identifies the need for specification work in this area.

MNOs often use proof of possession of a mobile number in customer life cycle events

For MNOs in particular, possession of a mobile number is important in many customer life cycle events, to determine whether a user is eligible to start a life cycle process. For example, number portability is mandatory in many markets; this allows the user to migrate their existing mobile phone number from one MNO to another MNO, when registering a new subscription. This number portability process is highly popular among consumers, with the majority of "new" subscriptions involving number portability between MNOs.

At the start of a number porting process, it is often checked whether the user is currently in possession of the phone number, to prevent friction caused by (for example) an input mistake on the phone number. Such errors could lead to a user's number being temporarily blocked. In general, for any customer life cycle event which can have serious consequences, it is important for MNOs to check possession of the mobile number in real time.

Number Verify offers in-app mobile number verification today

Number Verify is a service offered by MNOs by which a smartphone app or a web client can verify the mobile phone number(s) active in a handset in real time. GSMA Mobile Connect standard IDY.54 Verified MSISDN[1] is commonly deployed for this purpose. More recently, CAMARA Number Verification[2] has been developed. Both are based on the OpenID Connect protocol suite. In this service, the user enters what their phone number should be in the smartphone app, and this phone number is verified by the app with the mobile network and the SIM card.

Once the user submits the phone number to the app and the end-user consent is asserted, the verification is entirely invisible. Users do not have to go to an authenticator app, there are no PINs to mis-type, no URLs to click on, no socially engineered capture of a shared secret possible and no actions to review and approve. The user cannot be easily socially engineered as there is no information (such as a one-time code) to be phished. The result is a tamper-proof authentication bound to the mobile number.

Silent Authentication

Also, with end user agreement and once the phone number is known in the app, Number Verify can be executed subsequently in the background when needed without any extra user interaction. This makes it very suitable for use in an identity wallet to provide real-time verification of the mobile number with the network and SIM card when sharing the number with relying parties.

[1] https://www.gsma.com/identity/wp-content/uploads/2022/12/IDY.54-Mobile-Connect-Verified-MSISDN-Definition-and-Technical-Requirements-1.0.pdf
[2] https://github.com/camaraproject/NumberVerification

Number Verify specification would need extending to deliver an eIDAS 2.0 compliant Verifiable Credential

The currently deployed Number Verify specification (GSMA IDY.54 Verified MSISDN) however does not describe how to issue and store the mobile number in the wallet and how to present it in an eIDAS compliant interoperable way to the Relying Party. Moreover, the verification result that the mobile network currently delivers to the smartphone app is not an eIDAS 2.0 Verifiable Credential and has its limitations. The GSMA European Identity Group identifies the need for specifications detailing how the mobile number can be added to the wallet in the form of a QEAA issued by the MNO it is currently bound to.

Proposal to add a Verified mobile number to the EUDI Wallet as a QEAA

This chapter studies the feasibility of adding a verified mobile number to the EUDI Wallet as a QEAA issued by the MNO it is currently bound to. This proposal will enable discussions with the eIDAS ecosystem in order to initiate a specification process.

MNO is the authentic source of verified mobile numbers

The MNO is the one and only authentic source which can reliably issue the mobile phone number as a trustworthy credential, since it is the only entity which has the technical capability to check in real time which user is associated with the phone number. Phone number associations can also evolve based on life cycle events, be withdrawn or assigned to another user after some time, for example after a subscription ends or after a user requests a change of phone number.

Proposed approach: verified mobile number as a QEAA

Between the MNO as an authentic source and the EUDI Wallet a Qualified Trust Service Provider (QTSP) role is needed to make sure the attribute is issued as a Qualified Electronic Attribute Attestation (QEAA). What needs to be included in the attestation is that it has been positively verified with the right MNO, and a time stamp at which the verification has been done against the mobile network. The proposal is for the QEAA to include a Qualified Electronic Seal (QES)[3] to prove the time at which the number has been verified by the MNO, and that the content of the QEAA has not been tampered with.

Contract Owner and End User Attributes

There are two kinds of Phone Number Attributes that will need to be added to the EUDI wallet as a VC, depending on the use case.

> The Contract Owner Attribute specifies for which mobile number(s) the wallet holder is the *contract owner*. This Attribute will typically be used in life cycle events by MNOs, for example when registering the SIM card/mobile number when a new mobile number is issued, as is mandatory in many markets today due to local legislation.
>
> The End User Attribute specifies whether the wallet holder is also the actual *end user* of the mobile number. This may for example be used as an identifier to help Relying Parties recognise the wallet holder.

The presentation of the attribute to the Relying Party shall reflect whether it concerns the Contract Owner Attribute, or an End User Attribute. Note that an EUDI wallet may contain just a Contract Owner Attribute, just an End User Attribute, or both at the same time. Also, a wallet can contain multiple Contract Owner Attributes (in case the user has registered multiple contracts in their name), and it can contain multiple End User Attributes, since modern handsets today often have multi-SIM capabilities.

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0281&from=EN, see Annex V

Contract Owner Attribute

The Contract Owner Attribute is typically added to a wallet when the wallet is used to register the contract owner of a new mobile phone number / SIM with an MNO. The user of the wallet can decide at the time of the registration whether the Contract Owner Attribute should be included in his wallet, since adding attributes to a wallet is an optional choice for the wallet holder. At the same time the wallet can ask the wallet holder whether the End User Attribute should be added to the wallet as well.

Note that the Contract Owner Attribute can also be issued in the case of an existing phone number to existing wallets, e.g. in case there is a life cycle event. For this case the wallet holder will log in with the MNO and share the details of their PID, and the MNO will have to compare the details of the PID with the relevant data that the MNO has on file, e.g. in the CRM system (such as name, date of birth, address) before issuing the Contract Owner Attribute to the wallet.

End User Attribute

The End User Attribute is typically added to the wallet on request of the wallet holder, for example when a Relying Party asks for the end user's phone number as an identifier in an onboarding or an authentication process.

The End User Attribute also has to deal with the complication that a physical SIM card may easily have been swapped temporarily between mobile phones. This might be legitimate or fraudulent; for example, a fraudster may have used a victim's phone for a couple of minutes, adding the victim's phone number to the wallet of the fraudster, and then proceeding to use the phone number in a verifiable credential.

For the issuing of the End User Attribute Credential, the end user will need to consent to and enter their phone number in the wallet app, so that the end user understands that their phone number is being added to the wallet. This "claim" of the end user should be signed by the wallet holder, shall be submitted to the MNO during the issuing process and if accepted, the phone number should be stored as a VC for future silent authentication.

(Silently) Authenticating the End User Attribute

When sharing the phone number of the End User Attribute with the relying party, with end user agreement, for improved security the Wallet can (when online) always try to (re-) authenticate the mobile number silently with the MNO. For the authentication process, it is necessary to store the original claim in the wallet, so that:

- the end user does not have to re-enter the phone number repeatedly
- a safety delay can be supported the first time the End User Attribute is added to the wallet

This behaviour is a departure from the usual non real-time attributes that will need to be considered in the Union Toolbox Architecture and Reference Framework specification work. Please note that the same will apply to other attributes like location or any other attributes related to the current environment of the holder.

Extra fraud prevention by registering the End User Attribute with the MNO

An additional fraud prevention option is to offer the wallet holder an optional registration service for the End User attribute, in which the PID of the wallet (or a pseudonym and/or a secure reference of the PID) is registered with the MNO. When registered, the End User Attribute of that particular phone number should only be issued to a wallet that contains a matching PID.

The registration shall be offered optionally, so that the user can decide whether they want to share this data with the MNO, when adding the End User Attribute to a wallet. As an option to the wallet holder, the data that is being used for the registration needs to be persistent, so that for example if the wallet is lost the current registration can still be checked when a new wallet instance is issued.

As an extra fail safe, a safety delay shall generally be used (except when the End User Attribute is the same as the Contract Owner attribute) before an End User Attribute can be presented to a Relying Party when it is issued for the first time, including a warning to the contract owner that an End User Attribute has been issued to a particular wallet for that particular phone number.

In case the end user of a phone number changes, it shall be possible to cancel an end user registration at the MNO, whether this is done by the registered end user or the contract owner.

Revocation Process of Attributes

Both the Contract Owner Attribute and the End User Attribute have to deal with life cycle events that can have impacts on the mobile phone number, and which may cause the need to trigger a revocation event.

The MNO must therefore support a revocation mechanism for both the Contract Owner and the End User Attribute through its QTSP, that can be checked for each transaction in real time without jeopardizing privacy. The revocation process used must follow the same standard as will be used for other attributes in the wallet (this still needs to be specified in the ARF).

Both the End User Attribute and the Contract Owner Attribute needs to be revoked when

- The phone number has changed (but the contract is still in place)
- The contract was terminated without number porting
- The numbers were ported from MNO to MNO (unless a portability process of the Attributes is in place).
- The phone number is recycled and issued to another end user

The Contract Owner Attribute also needs to be revoked when

- The contract has been taken over by another person

Impact of Brokers on the proposed approach

In practice, wallet issuers will be using Brokers such as Aggregators when contracting with the various MNOs. It shall be possible to transport any of the attributes issued by the MNO to the wallet without any privacy or security risk, including in case the VC is transported through a Broker. One issue in particular that needs to be addressed is that a binding is needed between the wallet and the QEAA, so that the Relying Party can see that these two belong together (and that there has not been a falsification by a man-in-the-middle attack).

Additional value-add of MNO information

Fraudulent SIM swap

SIM swap is a legitimate service offered by mobile operators to allow customers to replace their existing SIM with a new one. A SIM swap may be required in the following circumstances:

- A SIM is lost, stolen or damaged;
- A different sized SIM is needed for a new device;
- The customer is porting out their number to a different network

While SIM swap is a necessary and useful service, it has provided an opportunity for fraudsters to obtain and utilise the replacement SIM card to gain access to users' financial and wider service accounts. Fraudsters seek to exploit the two-factor authentication commonly used by financial institutions to provide safe and secure services to customers. A common two-factor authentication method is to send a one-time passcode to the account holder's mobile number. Fraudulent SIM and eSIM swaps exploit weaknesses in the mechanisms that mobile operators use to switch a mobile number over to a new SIM card.

In case the fraudster succeeds, they get hold of a new SIM with the victim's phone number, and the old SIM is blocked. Usually, the fraudster tries to log in immediately with the new SIM and the victim will soon notice that their SIM is not working anymore, hence contacting the MNO, who will block the fraudulent SIM.

Current mitigation for fraudulent SIM swap

The most commonly used mitigation against SIM swap fraud by relying parties today is to check with the MNO whether a new SIM card has been issued very recently, and to restrict transactions accordingly. In most markets the MNOs offer a recent SIM swap check under the service name Account Takeover Protection. GSMA Europe recommends to include such a service in the wallet, and/or share this information with relying parties.

Use of EUDI wallet to prevent or mitigate fraudulent SIM swap

Once the Contract Owner attribute and /or the End User Attribute is registered by the MNO, this information can also be used to prevent abuse of mobile numbers through a fraudulent SIM swap. The Contract Owner attribute can be used as an extra check when issuing new SIM cards, and the End User attribute can be used to prevent the addition of a mobile number to the wallet of a fraudster, in case the fraudulent SIM swap happened anyway. The registration of the Contract Owner and / or End User

Attribute have the potential to offer an improved protection against fraudulent SIM swaps over what is available today, strengthening the case for the EUDI wallet.

Other use cases for Account Takeover Protection

Account Takeover Protection is not useful solely when number verification is used for authentication. Some relying parties verify users with a phone call when suspicious transactions occur. In case of a fraudulent SIM swap fraud, the relying party would be speaking to the fraudster, who would of course confirm the transaction as legitimate. Hence verifications via phone calls can also benefit from Account Takeover Protection.

Conclusion

We have described how relying parties across verticals, including MNOs themselves, require real-time number verification. Existing solutions do not yet deliver an eIDAS 2.0 compliant Verifiable Credential. Mobile Number Operators can check in real-time which user is associated with the phone number. Between the MNO as an authentic source and the EUDI Wallet a Qualified Trust Service Provider (QTSP) role is needed to issue the verified mobile number as a Qualified Electronic Attribute Attestation (QEAA). This QEAA should distinguish whether the mobile number represents a Contract Owner Attribute and/or an End User Attribute. Additional fraud prevention options can leverage the MNO information and processes.

Annex 1

Summary Table of Mobile Phone Number Verifiable Credential Attributes

	Contract Owner Attribute	End User Attribute
Use cases	Life Cycle Events at the MNO	Sharing of the mobile phone number as a user identifier with relying parties
PID Registration of wallet holder	Yes, as Contract Owner	Optional End User Registration by MNO for extra fraud prevention
Support for offline use cases	Yes	No
Revocation trigger	• The phone number has changed (but the contract is still in place) • The contract was terminated without number porting • The numbers were ported from MNO to MNO	
	• The contract is taken over by another person	
Measures to prevent SIM swap fraud	Registration of PID	• Restrict transactions based on time of SIM swap • Registration of PID of wallet holder

Contacts

Elizabeth Wiltshire
Manager, EU Affairs, GSMA
ewiltshire@gsma.com

Helene Vigue
Identity and Data Director, GSMA
hvigue@gsma.com

Andrzej Ochocki
Chair of the European Identity Group, GSMA
Head of Identity, Deutsche Telekom
Andrzej.Ochocki@telekom.de