Secure Patterns for Internet CrEdentials
Internet-Draft
Intended status: Experimental
Expires: 4 September 2025

Y. Song
L. Li
D. Wang
F. Liu
Huawei

3 March 2025

SPICE Use Cases in Telecom Network
draft-song-spice-telecom-usecases-00

Abstract

This document describes use cases of the credential specific to the telecom network. It aims to propose benefits and scenarios regarding to introducing the credential to the telecom network, which can provide more scenarios and directions to Secure Patterns for Internet CrEdentials (SPICE) specifications.

Requirements Language

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 [RFC2119].

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 4 September 2025.

Copyright Notice

Table of Contents

1. Introduction

The future telecom network will be user-centric, with rich application scenarios, and more consideration of user requirements. For example, users may need to apply and present proof of attributes to get services from operators or other organizations, thus telecom network needs to support issuance, storage and verification of proof of attributes. Verifiable credentials have flexible templates of claims, and are able to implement verification on demand, which can bring many benefits to the future network. This document will describe the use cases of credential in two aspects: for users of the telecom network, the credentials can introduce the concept of attribute to the network, and enable derivation of temporal subscriptions; for network entities, such as network functions (NFs) or base stations, credentials can not only facilitate cross-domain authentication, but also be used to precisely describe the functionalities of these network entities.

2. Use Cases

This document makes no request of IANA.

2.1. Telecom User Credentials

2.1.1. Notional Architecture of Using Credentials for Telecom User

Traditionally after signing a contract with a telecom operator, the user will obtain a subscription identity and the corresponding symmetric key issued by the operator for the user and store this information inside the device (e.g. cell phone, SIM/eSIM), and the subscription information will be stored inside the operator's network. Then the user can access the operator's network and request services (e.g., making and receiving calls). The operator's network consists of access network (including base stations) and core network (including various Network Functions (NFs) that provide services such as access, authentication, and exposure). When the user's cell phone accesses the operator's network, the operator can retrieve the subscription information from core network and verify the user's identity based on it. The operator can also establish a connection with Over-The-Top (OTT) providers.

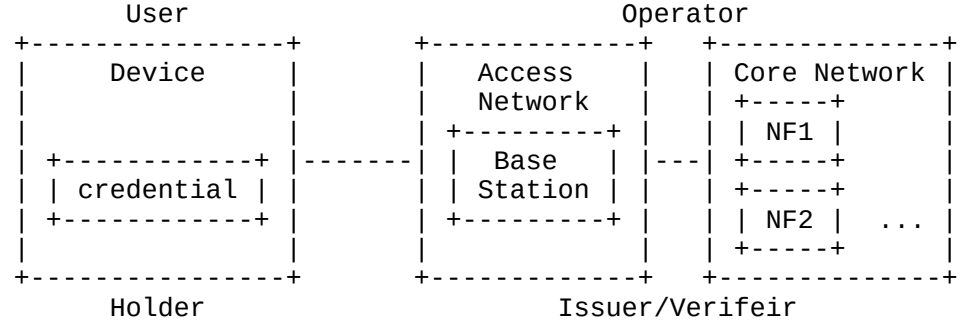

Figure 1: Notional architecture of using credentials for telecom user

In this use case, the user is the holder of the Verifiable Credentials (VCs), while the operator or OTT providers can act as both the issuer and the verifier of the credentials. These credentials can be stored within the SIM/eSIM, taking advantage of its secure storage capabilities. Additionally, they may also be stored on the user's cell phone.

2.1.2. Introduce Attributes into Telecom Network

At present, when a user subscribes to a telecom operator, a subscription identifier is issued. This identifier is bound to the user's subscription information stored in the operator's core network, enabling the operator to identify the user. However, the current subscription information in the telecom network lacks the ability to describe the user's real-world natural attributes (e.g. job, age, degree).

Looking ahead, there will be scenarios in which it is necessary to introduce attributes into the telecom network. For example, delivery workers can apply for verification of their job - related attributes and present the proof to the telecom operator. After successful verification, the operator can tag their calls. Consequently, customers can easily identify that the calls are from legitimate delivery workers rather than impostors.

In such cases, it is beneficial to introduce VCs. Operators or OTT providers have the capability to issue VCs to users, which serve as reliable proofs of users' attributes. VCs issued by OTT providers can be verified by operators, and conversely, those issued by operators can be verified by OTT providers. This innovative approach simplifies users' daily lives significantly. Moreover, it has the potential to transform the operator's reputation into tangible commercial value, enabling a wider range of business scenarios and bringing numerous benefits to the network.

2.1.3. Enable the User to Derive Temporal Subscription

In the future, there will likely be scenarios where users need to obtain temporary subscription information which should grant access to the same or a reduced set of services compared with the original user's subscription. Consider the following cases: when a user's child participates in a one-week summer camp abroad or a friend is visiting for a short period but has difficulty making prior arrangements, the user might wish to utilize their own subscription to assist these individuals in obtaining a short-term subscription from the operator.

Presently, the subscription information within the telecom network is static, and updating it is a cumbersome process. To meet the requirements of such temporary usage scenarios, users may need to request multiple SIM/eSIMs. Currently, the network allows users to either pre-sign a tariff contract with multiple lines or order multiple SIM/eSIM tariff plans with different identities and keys. However, these methods are not only cost-inefficient but also offer limited customization in terms of services. As the number of

services for multiple devices continues to expand, it becomes increasingly complex for users to manage different identities and keys.

The introduction of VCs into the telecom network can revolutionize the customization of users' subscription information and streamline identity and key management. Users can apply for temporary sub-VCs based on the VCs issued by the operator and distribute them to relatives, friends, or connected devices such as electronic watches, monitors, robots. Sub-VCs enable access to the telecom network with the equal or fewer permissions compared to the primary user. This approach endows users with enhanced flexibility and simplicity in managing their identities and keys, effectively resolving the issues associated with current subscription management methods.

2.2. Telecom Network Element Credentials

2.2.1. Notional Architecture of Using Credentials for Telecom Network Element

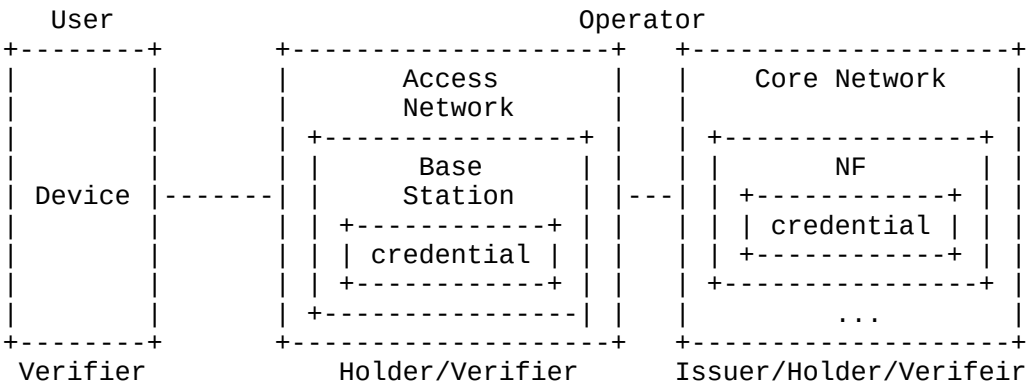

Figure 2: Notional architecture of using credentials for telecom network element

In this use case, network entities such as base stations and NFs assume the role of credential holders. The operator typically functions as the issuer of these credentials. The verifiers can be either other network entities or user devices (e.g. cell phone, SIM/ eSIM).

2.2.2. Achieve Cross-Domain Authentication

Currently within the telecom network, upon deployment, network elements such as NFs and base stations acquire certificates from the operator's Certificate Authority (CA). These certificates are typically based on the X.509 described inRFC 5280 [RFC5280] format and contain the public keys of the NFs and base stations. Their verification is restricted to entities that have pre-installed the CA's public key. Moreover, the issuance, update, and revocation of these certificates are solely controlled by the CA.

As the telecom industry continues to evolve, the network ecosystem is expected to involve multiple stakeholders. With the growing cooperation and interaction among multiple operators, and the emerging trend of inviting other organizations, such as manufacturers and OTT providers, to participate in network construction, the telecom network will support multi-party trust. Additionally, the continuous emergence of new application scenarios, such as smart city, and real-time augmented reality services across different regions, has led to need for dynamic network. In this scenario, network entities will likely face the urgent need for seamless authentication by entities in other network domains, and self-oriented management of identities and keys.

The traditional certificate-based authentication model, which relies solely on the operator's CA, may not be sufficient to meet the requirements of this more complex and collaborative environment. The introduction of VCs offers a solution. These credentials can be issued by various trusted entities, including different operators and OTT providers, thus establishing trust across different network domains. Additionally, network entities can actively apply for VCs or trigger the update and revocation of VCs. This not only enables on-demand key rotation based on security requirements or changing network conditions but also aligns with the requirements of dynamic network construction.

2.2.3. Provide Endorsement for Device Information

The functionality of network entities is represented and stored in the telecom network in the form of static profiles. These profiles are established solely during the registration process and undergo minimal modification thereafter. For instance, an NF profile typically includes details such as the NF Type, Instance ID, supported Public Land Mobile Network (PLMN), capability information, and priority information.

In the future, as the telecom network involving multiple operators and OTT providers in network construction, a network with multi-party trust will emerge. In such an environment, network entities may register across different network domains. For example, NFs may need to join the networks of other operators, and thus they need to provide their NF profiles and register with those receiving operators. Challenge occurs that the receiving operator requires a reliable method to determine the authenticity and trustworthiness of the provided NF profile.

By using VCs to describe network entity information, the home operator or OTT of the network entity can provide an endorsement. Then, the receiving operators or OTTs in another network domain can verify the VC, ensuring that the network entity information described within it is accurate and legitimate. This not only ensures the security and trustworthiness of cross-domain interactions but also equips the network with the flexibility necessary to meet the dynamic requirements of the evolving telecom network ecosystem.

3. Further work on telecom credentials

The further work regarding the introduction of verifiable credentials may encompass the following aspects:

* Credential Generation and Storage Support: Network entities and mobile phones need to be enabled to support the generation and storage of verifiable credentials. This requires the implementation of appropriate software and hardware mechanisms within these devices to create, securely store, and manage the credentials.

* Authentication and Authorization Based on Credentials: Network entities and mobile phones should be able to achieve authentication and authorization processes using verifiable credentials. For example, during the connection of a mobile phone to a network entity, the phone can present its verifiable credential, and the network entity can authenticate the phone based on the credential’s information and grant appropriate authorization for services.

* Privacy Protection through Selective Disclosure: The use of verifiable credentials should enable privacy protection through selective disclosure. Network entities and mobile phones should have the ability to disclose only the necessary information from the credentials as required by the specific context. For instance, in a certain service request, a mobile phone may only need to disclose its identity-related information from the credential, without revealing other sensitive details such as personal preferences or location history.

4. Security Considerations

There is no security and privacy issues in this document.

5. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/rfc/rfc5280>.

Authors' Addresses

Yurong Song
Huawei
Email: songyurong1@huawei.com

Lun Li
Huawei
Email: lilun20@huawei.com

Donghui Wang
Huawei
Email: wangdonghui124@huawei.com

Fei Liu
Huawei
Email: liufei19@huawei.com