5G Remote eSIM Provisioning: Blockchain-based Public Key Delivery

Rono Cheruiyot, Sourav Purification, Simeon Wuthier, and Sang-Yoon Chang
Department of Computer Science, University of Colorado Colorado Springs, Colorado Springs, CO, 80918, USA
Email:- {rcheruiy, spurific, swuthier, schang2}@uccs.edu

***Abstract*—5G technology utilizes an Embedded Subscriber Identity Module (eSIM), which is remotely set up by the Subscription Manager (SM), to replace traditional SIM. eSIM relies on the remote delivery of the core network public key since it lacks a physical chip that would normally have the public key encoded. eSIM uses the digital and remote Public Key Infrastructure (PKI) to deliver the public key. We propose a blockchain approach for secure delivery and verification of SM and eSIM public keys to remove single point of failure and enable authorized-only access to subscriber data hence enhancing authentication security.**

I. Introduction

The traditional Subscriber Identity Module (SIM) is a removable card that stores a user's identity, network authorization, and personal data. Each mobile device uses a SIM card, a type of Universal Integrated Circuit Card (UICC) containing the profile with the International Mobile Subscriber Identity (IMSI) and keys. These are essential for devices to authenticate themselves to Mobile Network Operators (MNOs) using the Authentication and Key Agreement (AKA) protocol [1] [2].

However, embedded SIM (eSIM) technology, as per the Global System for Mobile Communications (GSMA)'s Remote eSIM Provisioning (RSP) Architecture [3], are different in that eSIMs are not removable but are integrated circuits embedded directly into a device's motherboard. This evolution from physical to embedded units enhances functionality, allowing for Over-The-Air (OTA) provisioning. This feature lets users switch mobile network providers remotely without needing a physical SIM card switch. The RSP protocol has versions for both machine-to-machine (M2M) and consumer devices like phones. In this paper, we focus on the consumer device version. In this version, eSIM activation begins when a subscriber signs with an MNO, who then coordinates with a subscription manager server to generate and download the necessary SIM profile, including IMSI and keys, directly to the eSIM upon activation [4].

In Fig. 1, the green color signifies the eSIM ecosystem, the blue color signifies the traditional SIM ecosystem, and the black color indicates unchanged entities through the transition. The eSIM process starts when a subscriber contracts with a MNO, who then requests an eSIM profile generation from the SM. At this stage, the SM and MNO exchange critical details such as IMSI and secret keys, which are subsequently downloaded to the eSIM upon subscriber activation.

Additionally, the Remote SIM Provisioning (RSP) protocol involves Certificate Authorities (CAs) / Certificate Issuers (CI) and their intermediaries issuing certificates to both the SM and eSIM, establishing a trusted relationship anchored by the CAs/CIs. This setup ensures that only CA-certified SMs can securely provision profiles to eSIM devices, blocking unauthorized third parties.

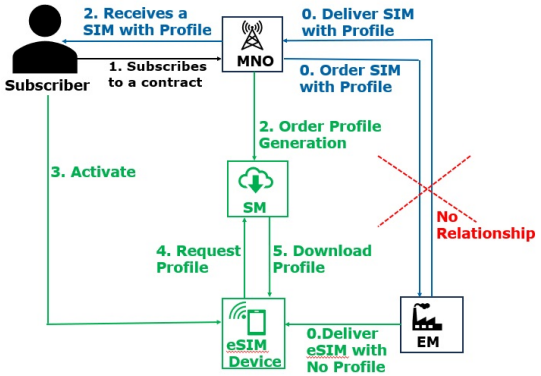

Fig. 1: SIM and eSIM ecosystems. Blue color for SIM, green color for eSIM and black color for unchanged.

With the traditional SIM, MNOs had one-to-one trusted relationships with SIM manufacturers. Hence, SIM profiles were loaded in secure, offline settings, limiting exposure to attacks. However, under eSIM, RSP allows any SM to load profiles onto eSIMs, broadening the potential for attacks, such as CA compromises that lead to the mis-issuance of, or issuance of malicious, certificates.

In this paper, we design a blockchain-based transparent eSIM Public-Key delivery. We propose a framework that uses a decentralized ledger to manage Public-Key certificate data, diminishing dependence on centralized certificate issuers and bolstering security against singular points of failure.

II. Related Work

While eSIM technology is not new, its widespread implementation and the exploration of blockchain for its public key delivery are still evolving, with limited literature available. However, studies like those of [5] and [6] have proposed a blockchain-based framework for Public Key Infrastructure (PKI). These frameworks utilize blockchain to issue, validate, revoke, and manage X.509 digital certificates, taking advantage of blockchain's elimination of single points of failure and providing a transparent, immutable ledger for tracking certificate histories. This approach primarily focuses on managing X.509 digital certificates, which, while crucial for digital security, does not address the unique aspects of eSIM technology, such as the chain of trust and specific security protocols.

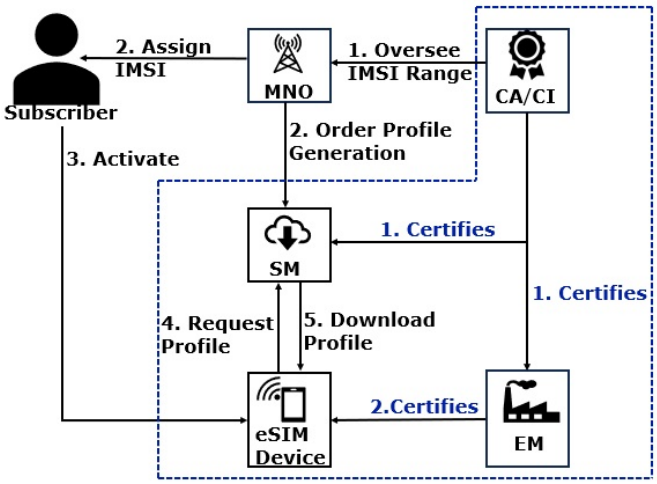

Fig. 2: Remote eSIM Provisioning Process

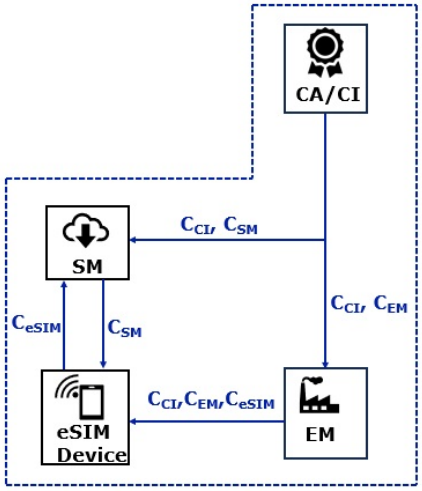

Fig. 3: Public-key Certificate Flow

The use of eSIM as a storage medium for cryptographic keys and managing PKI without third-party CAs has been proposed in [7], although it does not cover the specific remote provisioning processes for eSIMs. With the expected growth of IoT devices in 5G networks, the study in [8] introduces an authentication protocol tailored to the constraints of IoT (M2M) devices, differing from consumer eSIM applications.

III. Background

A. Blockchain

A blockchain is a distributed, authenticated ledger where valid entries are continuously added and shared among participants. Each participant validates an entry before linking it to a record chain. A consensus protocol determines the sequence of these records, and the immutable nature of blockchain allows for a collective agreement on historical data without needing a CA. The existence of a sufficient number of honest nodes preserves the integrity and finality of the record. [9].

Blockchains like Ethereum enable the implementation of smart contracts. These are unchangeable programs stored within the blockchain, and any operation executed by a smart contract is replicated across all nodes, ensuring consistency in perceived outcomes and states of the contract. Once deployed, the smart contract independently manages its functionality and accessibility. The deterministic and adaptable nature of smart contracts allows them to often substitute centralized processing services, offering a decentralized alternative.

B. SIM and eSIM Ecosystems

In the traditional SIM ecosystem, end-users access mobile network services through a process where the MNO and the SIM Manufacturer have an established trust as shown in Fig. 1.

However, under eSIM ecosystem there is no direct relationship between the EM and the MNO, marked by the red cross in Fig. 1. Consumers purchase an eSIM (device) with no profile and then subscribe to a contract with a MNO. The MNO then requests profile generation from the SM, which remotely provisions the profile onto the consumer's eSIM. This eliminates the need for physical SIM cards and allows for OTA provisioning of subscriber profiles. As shown in Fig. 1, the relationship between EM and MNO does not exist before subscription by the consumer. SM facilitates RSP's secure delivery and management of eSIM profiles. Leveraging the framework of PKI, the SM authenticates eSIMs using digital public key certificates, ensuring that the subscriber's identity is validated without a physically hard-coded public key within the chip.

IV. Problem Statement and Goal

The consumer RSP protocol operates under the premise that any entity holding a GSMA-issued certificate, or one linked to the GSMA root CA, is entirely trustworthy. This is similar to Web PKI, where browsers accept domain certificates from any public CA, creating a central vulnerability. Fig. 2 depicts the eSIM provisioning and management workflow, outlining the roles of various entities, where CAs or CIs validate the credentials of SMs and EMs. Once certified by the EM, eSIMs can download profiles onto user devices, enabled by the exchange of public key certificates for verification, as illustrated in Fig. 3, where C_i corresponds to public-key certificate Issued to i. The issue with this is that eSIMs indiscriminately trust any GSMA-certified SM for profile provisioning without any accountability for potential misconduct or certificate misissuance.

Our goal is to improve eSIM security and efficiency by introducing a blockchain-based system for the issuance and verification of public key certificates among eSIM entities.

V. Proposed Design

Our approach utilizes blockchain to decentralize the PKI used in the current eSIM. By integrating blockchain, we establish a distributed storage system that inherently promotes accountability and operational transparency within the RSP.

A. Design of Decentralized Permissioned Blockchain

In our blockchain application, an admission policy regulates a decentralized permissioned system. Only entities authorized

by the GSMA CA or its delegates, including SMs, EMs, eSIMs, and approved MNOs, can participate. For this, only CA/CIs can add new ledger entries, whereas eSIMs and SMs have read-only access for verifying public key certificates. This system records eSIM certificate transactions in a hierarchical structure on the blockchain, tracing from root to intermediate certificates down to the users (eSIMs and SMs) as shown in Fig. 4, ensuring a secure and immutable record of all credential issuance and management activities following the eSIM protocol. In the figure, we have used C_i to correspond to the public key certificate Issued to i.

B. Public Key Delivery

The steps involved in the process as shown in Fig. 4:

Step 1 : *Certificate Request - eSIM Manufacturer (EM) and Subscription Manager (SM)* EM and SM initiate the process by sending a Certificate Signing Request (CSR) to the CA/CI with their identities and public keys.

Step 2a & 2b : *Root CA Validation - CA/CI* The Root CA/CI receives the CSR, validates the identities, and verifies the public keys of EM and SM. Once validated, they issue digitally signed public-key certificates C_{CI}, C_{EM} and C_{CI}, C_{SM} respectively, which are simultaneously registered on the blockchain with key details certificate's public key, issuer, validity period, and other relevant metadata, but not the private key.

Step 3a & 3b : *Intermediate CA Role - EM* Acting as an intermediary CA, the EM receives the root CA certificate, issues a digitally signed public-key certificate, C_{eSIM}, to the eSIM, and chains it to the root certificates. These details are simultaneously registered on the blockchain.

Step 4 : *Certificate Presentation* As part of the initial communication handshake, the eSIM presents its digital certificate to the SM, including the eSIM's public key, issuing CA's signature, and validity period.

Step 5 : *Blockchain Query* The SM queries the blockchain using the certificate identifier to retrieve certificate details after receiving it from the eSIM. The SM verifies the eSIM's certificate against the blockchain data, ensuring attributes match and validating the digital signature using the issuing CA/CI's public key found on the blockchain. The SM also checks the certificate's validity and consults the blockchain's real-time revocation list.

Steps 6 & 7 : *Repeat Verification* Steps 4 & 5 are repeated with the SM sending its certificate to the eSIM.

Secure Channel Establishment After successful mutual verification, the eSIM and SM use their respective private keys and the other's public key to establish a secure, encrypted communication channel.

Future Directions: Our next steps include implementing a blockchain environment, with integrated public key generation software, to oversee eSIM and SM public key delivery and certificate revocation. We will conduct smart contract tests in a controlled environment to ensure their functionality and to validate the public key delivery process for eSIMs and SMs. Our aim is to enhance operational efficiency by evaluating the time needed for key delivery and verification, benchmarking these against conventional systems. While our design is promising, it also point to further research directions to refine the system's efficiency and scalability.

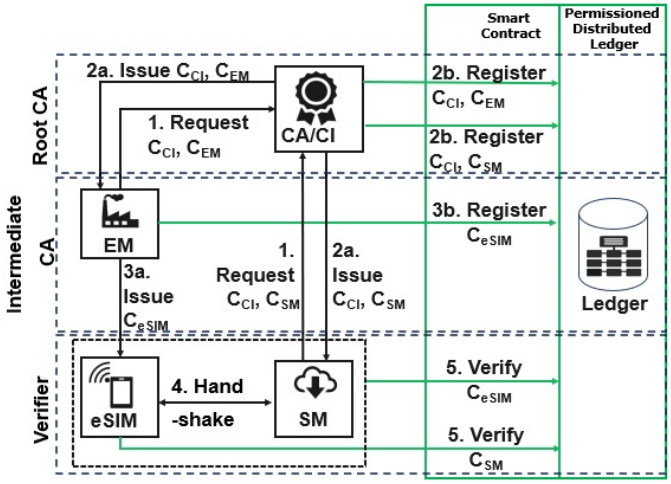

Fig. 4: Blockchain-based eSIM and SM verification

VI. Conclusion

In this paper, we have explored the potential of blockchain technology in enhancing the security of eSIM provisioning and the delivery of public keys. By integrating a blockchain framework within the RSP process, we aim to improve security by decentralizing public key certificate issuance, thus removing single point of failure and granting access to subscriber data only to authorized entities including the eSIMs and SMs.

Acknowledgment

This material is based upon work supported by the National Science Foundation under Grant No. 1922410.

References

[1] S. Holtmanns, V. Niemi, P. Ginzboorg, P. Laitinen, and N. Asokan, *Cellular authentication for mobile and internet services*. John Wiley & Sons, 2008.

[2] A. S. Ahmed, M. Thakur, S. Paavolainen, and T. Aura, "Transparency of sim profiles for the consumer remote sim provisioning protocol," *Annals of Telecommunications*, vol. 76, pp. 187–202, 2021.

[3] GSMA, "Sgp.22 rsp technical specification v2.4," 2021.

[4] S. Samanvita, S. P. Trivedi, and P. Jayanthi, "Testing of esim profile management," in *2021 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON)*, 2021, pp. 1–4.

[5] A. Yakubov, W. Shbair, A. Wallbom, D. Sanda *et al.*, "A blockchain-based pki management framework," in *The First IEEE/IFIP International Workshop on Managing and Managed by Blockchain (Man2Block) colocated with IEEE/IFIP NOMS 2018, Tapei, Tawain 23-27 April 2018*, 2018.

[6] S. Matsumoto and R. Reischuk, "Turning a pki around with decentralized automated incentives," *IEEE SSP, San Jose, CA, US*, 2017.

[7] A. Al Mousa, M. Al Qomri, S. Al Hajri, and R. Zagrouba, "Utilizing the esim for public key cryptography: A network security solution for 6g," in *2020 2nd International Conference on Computer and Information Sciences (ICCIS)*. IEEE, 2020, pp. 1–6.

[8] H. Goswami and H. Choudhury, "An esim-based remote credential provisioning and authentication protocol for iot devices in 5g cellular network," *Internet of Things*, vol. 23, p. 100876, 2023.

[9] M. Crosby, P. Pattanayak, S. Verma, V. Kalyanaraman *et al.*, "Blockchain technology: Beyond bitcoin," *Applied innovation*, vol. 2, no. 6-10, p. 71, 2016.