Poster: Retrofit – Enabling Interoperable E2EE Communication Through 6G Cellular Architectures

Sudheesh Singanamalla
University of Washington
sudheesh@cs.washington.edu

Richard Anderson
University of Washington
anderson@cs.washington.edu

Kurtis Heimerl
University of Washington
kheimerl@cs.washington.edu

***Abstract*—Cellular networks are the de-facto source of digital identity for a majority of the users in the world due to their ability to provide unique subscriber identities bound to a usable phone number through a SIM card. As cellular network operators embrace public key cryptography for authentication and identity in 6G networks marking a move from symmetric key based identities in previous generations, it opens up opportunities for E2EE communications. Policy regulations across the world mandate cellular interoperability across geographies which are implemented through private network interconnections or through the Internet making the communication channels of these networks heavily standardized and protocol agnostic, allowing any transport and application protocols such as E2EE communications to be *retrofit* over the network layer addressing their interoperability concerns. The deployment of verifiable key directories (VKDs), and relevant monitoring infrastructure within cellular networks enables key verifiability and improves operator trustworthiness. This marks a paradigm shift allowing the traditionally closed source and proprietary cellular network's key directories to be audited making compelled surveillance and lawful intercept extremely challenging. This poster presents an emerging application for transparency systems in cellular networks and presents the advantages, opportunities, and challenges.**

I. Introduction

The European Union mandates interoperability of end-to-end encrypted (E2EE) messaging between competitors in the recently enforced Digital Markets Act regulation while recent research efforts highlight the range of technical and policy challenges involved [1]. The interoperability mandates result in a fundamental change to the centralized architecture of popular E2EE messaging platforms such as WhatsApp, or Signal among others and various architectures have been proposed to address this challenge – from client only changes to the introduction of trusted proxy infrastructure. However, we argue that such interoperability has long existed in cellular communications deployed around the world, and present an alternative position supporting the migration of today's centralized E2EE messaging infrastructure to cellular infrastructure.

Despite addressing interoperability concerns, cellular network communications were largely considered insecure due to various attacks allowing operators and law enforcement to intercept and surveil communications, and the existence of downgrade attacks or protocol vulnerabilities. Recent 4G LTE, and 5G networks have been able to successfully address the challenges securing radio and core networking layers preventing attacks like SS7. However, the insecurity due to the ability of operators to intercept communications remains a concern resulting in general hesitation around operator trustworthiness.

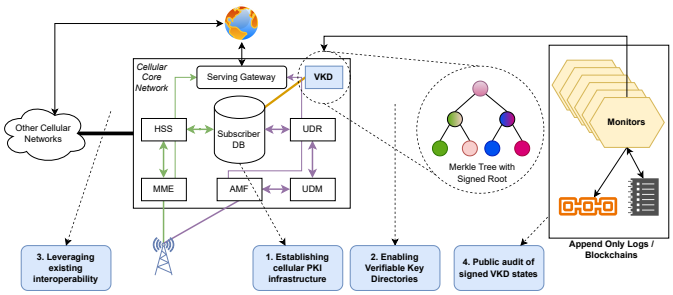


Fig. 1. Changes required to existing 4G (green) and 5G (purple) communication flow from a carrier base station to the cellular core network. By leveraging existing interoperability between cellular networks and the Internet, establishing public key subscriber identities, and the introduction of VKDs – we enable interoperable E2EE communications with other cellular carriers and Internet based communication applications. VKDs maintain signed auditable datastructures such as merkle trees which are globally audited and monitored by the existing certificate transparency monitors on the web or by blockchains.

The evolution of next generation 6G cellular networks are seeing the adoption of public key cryptography to maintain user identities for authentication to the cellular networks, migrating away from the symmetric key based identities in existing 5G or older generation networks. In this work, we posit that it is valuable to make these key directories verifiable, and the flexibility in defining the upcoming 6G standards create an opportunity for the deployment of VKD infrastructure within cellular networks. As a part of this work, we advocate for the following positions: *(1)* The migration of cellular network identity infrastructure towards the usage of public keys help enable E2EE communications between subscribers in addition to addressing the existing intent of mutual authentication and enables interoperable E2EE communications due to existing interoperability mechanisms, and *(2)* The deployment of verifiable key directories (VKDs) in cellular networks improves trustworthiness of the network operators and enables the ability to perform public audits of changes to the operator managed directories making it difficult for cellular operators to perform equivocation attacks and intercept communications [3], thus improving privacy in existing cellular infrastructure.

II. Opportunities in Cellular Networks

Enabling Public Key Infrastructure (PKI) in cellular networks, combined with their existing interoperability capabilities allow trustworthy interoperable E2EE communications when verifiable subscriber public key directories are established enabling updates to insecure standards like SMS and making communication between E2EE platforms interoperable. We present our proposal in Figure 1.

A. Cellular Public Key Infrastructure (PKI) Efforts

Current centralized E2EE messaging providers rely on the sybil tolerance properties of cellular networks to bootstrap user identities on their platforms leveraging the uniqueness of phone numbers as identifiers. Internally, cellular network operators have only more recently begun to rely and use public key cryptography to maintain subscriber identities, opening up opportunities to deploy E2EE cellular communications by leveraging existing widely adopted standards such as X3DH to establish a shared secret between parties, followed by a double ratcheting algorithm for sending and receiving encrypted communications. However, these mapped subscriber $\longleftrightarrow$ public key directories are currently not publicly auditable or transparent – enabling operators to equivocate and intercept communications either maliciously, through compromised infrastructure, or by legal compulsion. Unlike the Web PKI infrastructure with many root certificate authorities (CA) able to issue certificates or delegate signing to sub CAs to validate the identity of a server, the eSIM cellular PKI has a single root of trust operated and managed by GSM Association (GSMA) through two partnering CAs – Cybertrust and DigiCert. There exists no equivalent of the Web TLS certificate transparency (CT) ecosystem in cellular networks to audit for fake certificates binding a phone number to multiple cellular identifiers across network providers. Additionally, no measurement or audit efforts have ever been performed in public raising concerns about the trustworthiness and correctness of the CA making the network operators trusting the root CAs vulnerable to covert surveillance due to compelled cert-creation attacks.

We propose the deployment of transparency infrastructure into cellular networks and argue that the deployment of key transparency infrastructure in cellular networks improves trustworthiness. Repurposing the existing certificate transparency ecosystem to support cellular CAs allow for the same CTLog infrastructure to be used for both Internet and cell networks.

B. Transparency Infrastructure Deployments

We propose cellular network operators deploy key transparency infrastructure by converting existing subscriber $\leftrightarrow$ public key directories maintained by the operators into VKDs. Furthermore, we anticipate network operators deploying public append-only ledgers or extend the existing usage of blockchains in the telecom sector to periodically publish signed commitments of the VKD state which can be audited by other peers in the network, independent auditors, or by the clients – ensuring global key consistency, authenticity and integrity.

C. User Identifier Collisions & Keying Material

Cellular networks interoperate between other networks both within and outside their geographic boundaries. Such network connectivity allows cellular network operators to establish various transport protocols such as SCTP, TCP, or QUIC over which session based protocols such as TLS and custom application specific protocols such as messaging, video, or voice are implemented. The deployment of VKDs by multiple network operators and the emergence of auditors in the ecosystem for monitoring keys bring to light two key problems to enable interoperable E2EE messaging: 1) Collisions of user identifiers across providers, and 2) Retrieving keying material associated with the recipient without performing broadcast lookups for mapped user identities across multiple providers either by the sender client or the sending service provider.

However, the challenge of identifying the recipient service provider to route communications to has been addressed through extensive standardization in cellular networks allowing network operators to efficiently communicate with other networks using a prefix based namespace which is encoded into the IMSI/SUCI standard and allocated to cellular operators by the International Telecommunications Union. Piggybacking on existing telecommunications infrastructure signifcantly reduces the complexity for the clients and the service providers while removing the need for deploying additional network architectures to support interoperable communication. The unique identification standards for subscribers prevent user identifier collisions allowing network operators to maintain the subscriber's public key in their directories with a valid IMSI. The prefixed nature of these IMSI's allow operators to identify the necessary VKD containing the recipient's records and request the mapped public key and associated cryptographic commitments validating the correctness of the key state.

III. Conclusion & Challenges

While the arguments for migrating key transparency infrastructure to cellular networks is compelling, there are many technical, legal, and policy challenges that remain to be addressed. At a high level, sharding existing large verifiable key directories such as those maintained by WhatsApp, or Signal to cellular network operators make it challenging to setup auditing infrastructure such as monitors to verify the integrity and correctness of the key directories and associated proofs. Additionally, for large group based communications, clients might be forced to download proofs from multiple key directories which could be large and impact performance for clients in regions of poor network connectivity. Similar to the Internet ecosystem, monitoring infrastructure might need to be altruistically setup posing important sustainability concerns. Despite an anti-censorship or pro-encryption view in this paper, the deployment of these systems may affect or even prevent government intelligence efforts which could be enforced through legal warrants in existing cellular networks [2], [4], or for anti-abuse mechanisms to prevent spam and compliance to messaging regulations [5].

References

[1] J. Len, E. Ghosh, P. Grubbs, and P. Rösler, "Interoperability in end-to-end encrypted messaging," *Cryptology ePrint Archive*, 2023.

[2] R. Levinson-Waldman, "Hiding in plain sight: A fourth amendment framework for analyzing government surveillance in public," *Emory LJ*, vol. 66, p. 527, 2016.

[3] M. S. Melara, A. Blankstein, J. Bonneau, E. W. Felten, and M. J. Freedman, "CONIKS: Bringing key transparency to end users," in *24th USENIX Security Symposium (USENIX Security 15)*, 2015, pp. 383–398.

[4] S. K. Pell and C. Soghoian, "Your secret stingray's no secret anymore: The vanishing government monopoly over cell phone surveillance and its impact on national security and consumer privacy," *Harv. JL & Tech.*, vol. 28, p. 1, 2014.

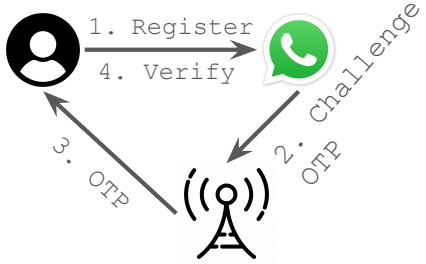
[5] S. Singanamalla, A. Mehra, N. Chandran, H. Lohchab, S. Chava, A. Kadayan, S. Bajpai, K. Heimerl, R. Anderson, and S. Lokam, "Telechain: Bridging telecom policy and blockchain practice," in *ACM SIGCAS/SIGCHI Conference on Computing and Sustainable Societies (COMPASS)*, 2022, pp. 280–299.

Retrofit – Enabling Interoperable E2EE Communication Through 6G Cellular Architectures

Sudheesh Singanamalla, Richard Anderson and Kurtis Heimerl

Paul G. Allen School of Computer Science and Engineering, University of Washington

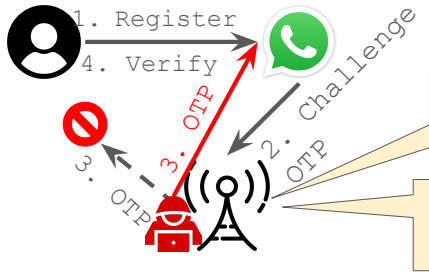
Introduction and Motivation



1. Need for **interoperability** between messaging/communication providers (DMA Act)
2. **Bootstrap problem:** Registering with E2EE services requires cellular identities

Attack Scenarios

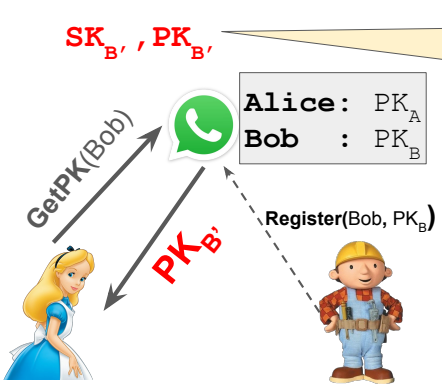
Rogue Telecom Operators



Knows exactly which user and the OTP in **plaintext**

Denial of Service (DoS) attack preventing user registration.

Non-interoperable & Equivocable E2EE Services



Equivocated Key Pair resulting in MITM. (Due to **compromise/legal compulsion**)

Addressed through Key Transparency Mechanisms such as CONIKS [1], or Parakeet [2] establishing **Verifiable Key Directories (VKDs)**

Solution: Changes to Cellular Networks

Current 4G/5G databases bind symmetric keys to subscribers.

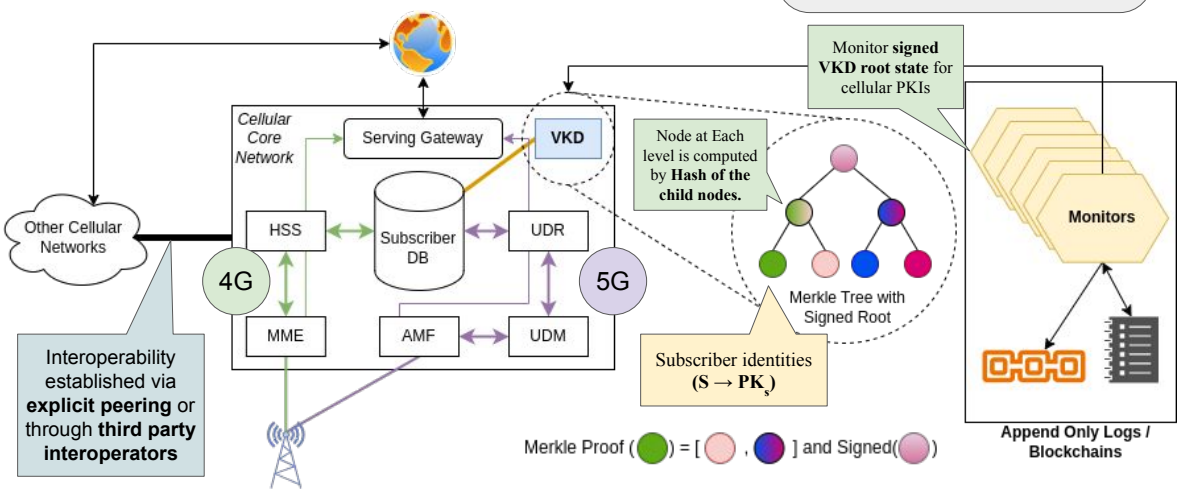
Upgrade to Public Key bindings for subscriber identity

Establish **authenticated data structures** over subscriber identities through the introduction of **Verifiable Key Directories (VKDs)** as a new microservice.

Standardized VKDs and existing cellular **interoperability** and connectivity to Internet based VKDs allow **discovery**, **key resolution**, while maintaining **integrity** guarantees.

Deploy or Leverage existing **certifying** (GSMA), **logging and monitoring** infrastructure (Certificate Transparency Logs), or Blockchains (Consortium [3], or Public ledgers) for **VKD states**.

1. Existing TEEs and eSIM Infrastructure can be updated in 6G to maintain attested public key identities.
2. Advocating for VKDs to be made integral parts of 6G standards



Interoperability established via **explicit peering** or through **third party interoperators**

Challenges

1. **Large cryptographic proof sizes** for multi-network communications
2. Increased **stress on existing transparency infrastructure** and might require altruistic setup posing sustainability challenges.
3. Potential impacts on government intelligence efforts and **increased challenges for law enforcement**
4. Addressing **spam** in encrypted communications.

References

[1] Melara, Marcela S., et al. "CONIKS: Bringing key transparency to end users." 24th USENIX Security Symposium (USENIX Security 15). 2015.

[2] Malvai, Harjasleen, et al. "Parakeet: Practical key transparency for end-to-end encrypted messaging." Cryptology ePrint Archive (2023).

[3] Singanamalla, Sudheesh, et al. "Telechain: Bridging telecom policy and blockchain practice." ACM SIGCAS/SIGCHI Conference on Computing and Sustainable Societies (COMPASS). 2022.