# Trustworthy Local Breakout

Mukesh Thakur[1,2,*] and Yki Kortesniemi[2,3]

[1]*Ericsson Finland, Hirsalantie 11, 02420 Jorvas, Kirkkonummi, Finland*
[2]*University of Helsinki, Fabianinkatu 28, Finland*
[3]*Aalto University, Otakaari 1, FI-02150 Espoo, Finland*
*E-mail: mukesh.thakur@ericsson.com; mukesh.thakur@helsinki.fi; yki.kortesniemi@helsinki.fi; yki.kortesniemi@aalto.fi*
[*]*Corresponding Author*

Received 09 August 2025; Accepted 01 December 2025

## Abstract

The newer generations of mobile networks (e.g., fifth generation) provide increasingly lower latencies in the home operator's (HO's) network, and there is similar expectation from subscribers while roaming. Moreover, regulations, like the EU's Roam Like At Home, mandate that the roaming subscribers receive comparable service quality without additional charge from the visited operator (VO) in the roaming country. However, the currently most widely adopted roaming approach, home routed, adds significant latency because the roaming traffic traverses all the way back to the HO, while with local breakout, the subscriber is served locally by the VO, resulting in lower latency. Yet, local breakout has not been adopted by most operators, primarily because of trust issues in tracking the data used by a roaming subscriber, which currently is only done by the VO. This paper presents a trustworthy local breakout (LBO) solution that addresses the trust issue by having both the roaming user equipment and the VO keep record of data usage, thus leveraging their opposing incentives to keep both parties accurate. In addition, the solution streamlines the 5G registration process by enabling authentication

*Journal of ICT Standardization, Vol. 14_1,* 1–36.
doi: 10.13052/jicts2245-800X.1411

and authorization directly with the VO, thus significantly speeding up the registration. The solution utilizes verifiable credentials to record the subscriber's usage information and for the 5G registration. The analysis demonstrates that the registration process is streamlined, and usage information is now more trustworthy compared to the current LBO.

**Keywords:** Roaming, local breakout, home routed, certificates, verification credentials, 5G registration.

## 1 Introduction

With the fifth generation (5G) of mobile networks and the sub-10 ms latencies they enable, the demand for Internet usage has significantly increased due to use-cases such as cloud gaming, immersive augmented reality (AR)/virtual reality (VR) experience, and seamless high definition video conferencing [1]. Also, this demand is no longer limited to within the mobile operators' home networks but extends also to mobile users (subscribers) traveling abroad, where they now expect the same low-latency Internet access for their applications [2]. The solution to meet this demand is *roaming*, where the subscriber can access the mobile services (voice, SMS, Internet, etc.) outside the coverage areas of their home operator (HO) by connecting to the networks of select other operators known as the visited operator (VO)[1] [3]. Furthermore, regulation such as the EU's *Roam Like at Home* [4] explicitly mandates that, within the EU, the VO must offer service quality comparable to that of the HO without charging the subscriber extra, thereby reinforcing the importance of good quality of service (Qos), including latency, while roaming.

To serve roaming subscribers with Internet access, 5G operators typically use the *home-routed (HRO)* roaming approach [5] specified by the Third Generation Partnership Project (3GPP) [6] in the late 1990s. With HRO, all Internet traffic of a roaming subscriber is routed via their HO, which adds extra latency compared to accessing the Internet directly from the VO's network, thereby significantly degrading the subscribers' QoS [5], particularly with latency-sensitive services such as voice-over-IP (VoIP) calls [7]. In addition, as the new generations of mobile networks (e.g., 5G) have lowered

[1]Roaming service within the country the home operator itself is already serving is called national roaming, which is typically only used in countries where operators do not have sufficient national coverage. This paper focuses on international roaming, which means roaming services in other countries.

the latency in the HO's network, the subscribers' expectations of acceptable latency have increased, making the additional latency of HRO an increasingly severe problem for users.

To address this latency, the 3GPP in the mid-2000s specified an alternative roaming solution called *local breakout (LBO)* that allows the VO to provide direct access to Internet, which significantly reduces the latency and increases resource efficiency, but prevents the HO from monitoring the subscribers' QoS as the data no longer flows via the HO [3]. In practice, despite the clear benefit to the subscriber, operators have not widely adopted LBO, a key reason being the intrinsic lack of trust between the HO and VO for billing, policy enforcement, and quality of service (QoS) guarantees [8]. With LBO, the VO alone keeps a record of the subscriber's network usage and the HO has to implicitly trust the VO as neither the HO nor the subscriber have any means to verify the accuracy of this information, which the VO now has a potential financial incentive to manipulate in the form of over-reporting the data usage. With policy and QoS, the HO similarly remains unsure whether the VO is actually enforcing all the necessary policies as well as guaranteeing the agreed QoS while roaming. Thus, if the trust issue regarding this information can be sufficiently addressed, LBO becomes a more adoptable solution for the operators, and with it the roaming subscriber QoS can be improved and the roaming latency would be similar to the latency achievable within the HO's network.

Another issue with roaming is that whenever a roaming subscriber enters a VO's network, the subscriber must first authenticate with their HO, which requires multiple messages between the subscriber device and the HO, and the same process is repeated whenever the subscriber has to re-authenticate in the same VO network (after they, e.g., rebooted their mobile phone). Involving the HO in this operation every time is inefficient and slows down the registration process, again negatively affecting the subscriber experience.

To address these roaming issues, a patent [9] suggests the idea of using the subscriber's device as an additional source to record usage data and using certificates for registration, but the patent does not detail any concrete solution nor a detailed analysis of the approach. This paper builds on top of this patent by introducing *trustworthy local breakout (TLBO)*, a detailed concrete solution that addresses the trust problem by also recording the data usage with the subscriber's device, uses the same approach to track the provided QoS, as well as streamlining the reregistration process by enabling local registration of the subscriber with the VO, along with analysis of the solution. The key research questions in this paper are:

1. RQ1: How can a TLBO solution be designed involving the subscriber's device and how does this affect the trustworthiness of the solution?
2. RQ2: How can the reregistration process of the UE while roaming using credentials be streamlined?

The key contribution of this paper is the complete protocol of the *TLBO* solution with detailed analysis. The benefits of TLBO are two-fold: first, it provides the HO with a trustworthy way of monitoring both the data usage and quality of service of the roaming subscriber by leveraging the opposing incentives of the subscriber and the VO. Second, the solution optimizes the current 5G reregistration process by allowing the VO to validate the roaming subscriber's credentials locally (i.e. without the HO's involvement). The analysis demonstrates that, with TLBO, the subscriber can benefit from a similar latency both roaming and at home and the 5G registration process uses 60% less messages exchange between the VO and the HO compared to the current HRO solution. Also, the UE data usage information is now more trustworthy because the HO receives a verified usage record maintained by both the UE and the VO. Finally, although this solution has been designed for 5G, with the improved trustworthiness and reduced latency, it becomes even more relevant for the next generations of mobile networks.

The remainder of the paper is structured as follows: Section 2 describes the 5G registration process in the home network and while roaming, current roaming solutions and their limitations, and identifies the requirements for a TLBO solution. The design of the solution is presented in Section 3, and Section 4 analyzes it. Section 5 presents the discussion, and finally, Section 6 concludes the paper.

## 2 Roaming in the 5G Network

In a 5G network, a home operator provides subscribers with basic services such as voice, SMS, and data along with value-added services including voicemail, call forwarding, call waiting, streaming, etc. Most of these services can also be provided to the subscriber while roaming, although some services like streaming might be restricted within the home network. Furthermore, the roaming network operator (visiting operator) does not always have the capabilities to offer all these specific services because of regulatory restrictions, interoperability issues (difference in network configurations of the two operators), or technical limitations (e.g., the roaming operator might not support 5G features like near-zero latency and high reliability) [10]. In

practice, these differences and how they should be addressed are covered by the roaming agreement between the HO and VO, which is periodically updated to reflect the evolving regulatory, technical, and business needs. Of all the services available to a roaming subscriber, this paper focuses on the Internet services while roaming.

The rest of this section describes the 5G registration of a UE in both the home network and while roaming, the current roaming solutions and their limitations, and identifies the requirements for a TLBO solution.

### 2.1 5G Registration in a Home Network

To access a 5G network, the mobile network user (subscriber) must first obtain a subscription from a mobile network operator who becomes their *home operator (HO)* [3]. To be able to provide this service, the HO maintains subscription information that includes personal information necessary for the HO to manage the subscription as well as registration information such as a unique subscription identifier and the authentication keys necessary to register and authenticate the subscriber with the mobile network [11]. Subscription information also includes the subscription plan selected by the subscriber such as prepaid (pays in advance and recharge when needed), postpaid (monthly billing), and enterprise plans that include unlimited calls, data and Microsoft 365 access, as well as the charging information including tariff details, last payment date, next payment date, etc. The HO stores all this information in its database and shares some of it (such as subscription identifier and authentication keys) via an (embedded) subscription identity module, (e)SIM, [12] to the subscriber's device called the *user equipment* (UE), typically a mobile phone.

The subscription identifier is used to identify, register, and authenticate the subscriber's UE within the HO's network and while roaming. There are three main types identifiers: international mobile subscriber identity (IMSI) introduced with the 2G networks, and the subscription permanent identifier (SUPI) and subscription concealed identifier (SUCI) that were introduced with 5G networks to improve the privacy of subscribers [11]. The IMSI is a unique number assigned to each UE with a key privacy limitation: when the UE wants to access the network, it must authenticate to the HO by sending the IMSI over the radio channel without any encryption. This exposes the UE to potential tracking by malicious actors, as anyone within range can monitor this signal [3]. To address this issue, in the 5G network the IMSI has been replaced with another globally unique permanent identifier called

the subscription permanent identifier (SUPI), which is partially encrypted within another *temporary* identifier called the subscription concealed identifier (SUCI) used during authentication. The SUCI can only be decrypted by the target UE and the HO as only they have access to the keys needed for decrypting the SUPI. This makes the UE anonymous on the network, thus improving the privacy of the subscriber. However, under some circumstances, e.g., unauthenticated emergency registration (dialing an emergency number – 112/911) or for operational reasons (troubleshooting and network performance optimization), the UE sends the SUPI without any encryption. In practice, more often than necessary, HOs configure the SUCI to be generated using nullscheme (i.e., no encryption), resulting in the UE sending the unconcealed SUPI instead of SUCI, thereby undermining the original purpose of the SUCI in protecting subscriber privacy [5].

In 5G, there are three different types of authentication mechanism to ensure interoperability between traditional and new systems. The first two are traditional methods, 5G authentication and key agreement (5G-AKA) [13] and 5G extensible authentication protocol – AKA' (EAP-AKA') [14], are both based on a challenge-and-response protocol and use the pre-shared authentication key between a UE and its HO [15]. Although both mechanisms provide essentially the same level of security, the EAP-AKA' is a widely supported protocol, extending its use beyond the 3GPP networks.

The third, newer, registration mechanism is the 5G extensible authentication protocol – transport layer security (EAP-TLS) [16] that uses digital certificates [17] for authentication rather than pre-shared keys that can be vulnerable to interception. This makes it the most secure registration mechanism [18]. So far, EAP-TLS has mainly been adopted for enterprise networks and Internet of Things (IoT) use cases. As this certificate-based authentication is already supported, it can be leveraged in the design of the TLBO solution as discussed in Section 3.2.

### 2.2 5G Registration While Roaming

Roaming is a 3GPP [6] solution introduced with the 2G networks that enables a subscriber to access mobile service even when outside their HO's network coverage by allowing the subscriber to connect to the networks of the VOs with which the HO has roaming agreements. Without roaming, the subscriber would either have to rely on local networks such as WiFi (which typically has limited coverage) for Internet access or purchase a new local subscription from the VO. However, both options come with drawbacks such as losing

access to the original regular phone number and subscription services, as well as having to pay for two sets of services, making the experience less convenient. Similarly, the subscriber could purchase alternative connectivity service, e.g., satellite based such as Starlink [19], but again this requires a compatible device and a different type of connectivity subscription. So, the most convenient (though sometimes still quite expensive) solution for the subscriber is to continue using their existing device and subscription (and phone number, etc.) through roaming.

To access mobile services via a VO, a roaming subscriber must first register to their HO so that the HO knows, e.g., where to direct the subscriber's incoming calls and messages. Here, the key element is the SUCI that includes an encrypted part of the SUPI, the HO's country code, and an identifier used to distinguish the HO within the country [3]. The UE sends the SUCI to the VO, who uses the last two attributes to determine the correct HO for registration. The VO then sends the HO both the subscriber's SUCI and the VO's own identifier, which the HO saves in order to route voice calls and messages to the UE.

The registration process is initiated by the UE that sends a registration request to the VO. To ensure secure communication, the VO then establishes an encrypted tunnel with the HO for transmitting the authentication request. After the successful registration (including authentication) of the UE, the HO sends the VO the subscription data, which typically includes static subscriber information, whether roaming is allowed for that subscriber, roaming restrictions, access type (3GPP, non-3GPP), UE usage type (e.g., normal UE, voice centric UE, data centric UE, IoT device, etc) mobility restriction, and the QoS profile [20], based on which the VO starts serving the UE [10, 18, 21]. Figure 1 illustrates the steps involved in this registration process:

1. As soon as a roaming UE's radio module is activated in the coverage area of the VO (e.g., airplane mode is deactivated) the UE sends a registration request to the VO.
2. The VO requests the UE to identify itself.
3. The UE sends its SUCI to the VO.
4. Using the SUCI, the VO identifies the UE's (subscriber's) HO, and sends the authenticate request, with the SUCI and VO identifier (VO ID) to the HO.
5. The HO decrypts the SUPI from the SUCI and generates an authentication vector (AV). The AV contains RAND (a random number), AUTN (an authentication token that is bound to the HO's identity), and HXRES* (hash of expected response of UE).

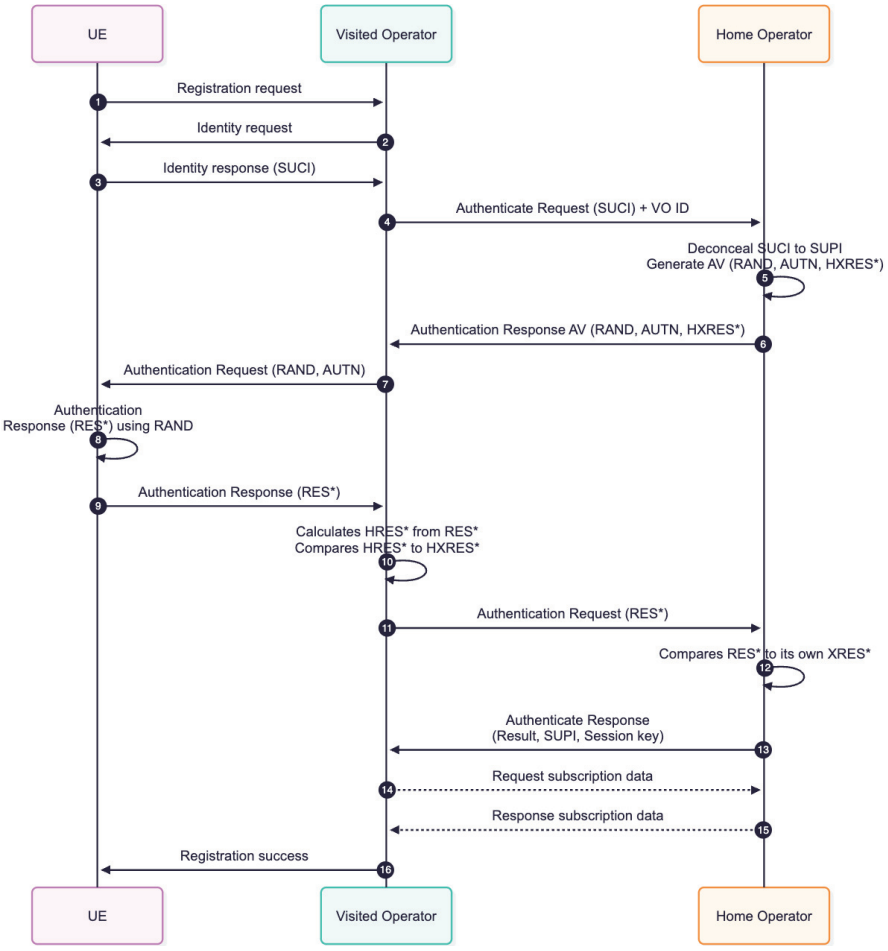


**Figure 1** UE registration while roaming in a 5G network.

6. The HO sends the AV to the VO that stores the HXRES*.
7. The VO forwards the RAND and the AUTN to the UE.
8. The UE authenticates its HO with the AUTN and calculates the response (RES*) using RAND and the authentication key in the (e)SIM.
9. The UE sends the RES* to the VO.
10. The VO calculates the HRES* from the RES* and compares the HRES* with the expected response, HXRES*.
11. If they match, the VO send RES* to the HO.

12. The HO compares the RES* with its own XRES*. If verification is successful, authentication is successful; if not, the UE must restart the registration process.
13. The HO sends an authentication response message to the VO, with SUPI and a session key which the VO uses to establish secure communication with the UE. Typically, the session key expiry is operator specific and the key is refreshed when, e.g., the key expires or if the UE re-authenticates with the HO.
14. The VO requests the subscription data from the HO.
15. The HO sends the subscription data to the VO.
16. The VO sends a registration success message to the UE.

From Figure 1 it is clear that the 5G registration process requires multiple messages between the roaming UE, the VO and the HO. This process can be triggered multiple times, for instance, if the UE connects with a new VO because of connectivity issues with the earlier VO or the UE moves to a coverage area of a new VO or if the UE context information (subscription, session, etc.) maintained by the VO expires (set based on HO policy) or the HO's policy, operational issues such as if the UE loses signal, reconnecting after signal lost because of drained UE battery, connectivity issues, restarts, etc. Each reregistration triggers all the message exchange between the VO and the HO, with optional steps 14 and 15, given the subscription data are still valid and there were no changes such as location, access type, or VO. Nonetheless, the current registration process leads to traffic overhead and additional delays for the subscriber, so this paper looks at streamlining this process as part of the trustworthy local breakout solution.

### 2.3 Current Roaming Solutions

Figure 2 illustrates the *key entities* involved in the roaming process: the roaming user equipment (UE), the home operator, the visited operator, and the Internet.[2]

To provide roaming services in 5G networks, the 3GPP [6] has currently standardized two roaming solutions, *home routed (HRO)* and *local breakout (LBO)* [3]. As shown in Figure 2, with HRO, the UE's Internet traffic is routed via a secure tunnel between the VO and the HO (arrow 4). In contrast, with

[2]In addition to the Internet, the home operator can also provide some subscribers with access to other data networks [3] such as private/enterprise networks. This paper focuses only on Internet access as the other data networks may require additional security arrangements.

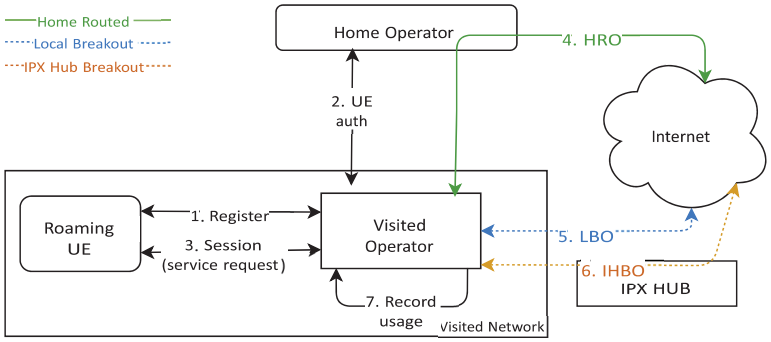


**Figure 2** Entities in 5G roaming. The green arrow 4 represent the home routed roaming solution, while the dotted blue arrow 5 represents the local breakout. Finally, the orange arrow 6 represents IPX hub breakout.

LBO, all the UE's Internet traffic is served by the VO that directly connects to the Internet (arrow 5).

The roaming UE, after successfully authenticating with its HO (arrows 1–3), is able to access the Internet. The VO keeps a record of the amount of network services used by the roaming UE, which HO then financially compensates. The frequency of reporting depends on the roaming agreement between the HO and the VO, the most common being hourly or daily allowing for efficient processing of the billing. In some cases, for high-priority or business roaming, the reporting could be in real or near real-time [10]. Often, roaming charges can be quite high; however, within the European Union, the *Roam Like at Home* regulation launched in 2017 [4] mandates that the VO provides the network services to the roaming UE at a similar cost as the HO, without significant additional charge [4].

Of the two roaming solutions, mobile operators practically always prefer the HRO solution because it provides several advantages for the HO, especially that the HO has full control of the subscriber's data usage. This is because the HO can meter the Internet usage of the roaming UE, thereby ensuring accurate billing [5]. Similarly, the HO can ensure that the UE has the same services (e.g., voicemail, premium content subscription, for which the VO may not have added support) available even while roaming, thus providing consistency of service across different VO networks [3, 5]. However, at the same time, the HRO has several significant disadvantages, particularly in terms of latency, cost, and efficiency in the use of network resources. As all roaming UE traffic is routed via the HO, (sometimes significant) additional latency always occurs with the traffic, thus lowering

the QoS. This becomes particularly problematic in real-time communications such as calling with apps and online gaming, where delays have an adverse affect on the subscriber's experience. Moreover, the "Roam Like at Home" initiative [4] requires that the VO provides the same network quality as the HO. However, a study [22] conducted by the EU in 2021 revealed that with HRO the roaming subscribers experienced 62% worse latency compared to non-roaming subscribers, thereby significantly degrading the quality of service (QoS), and the latency becomes significantly worse with intercontinental roaming, e.g., the web page loading time can increase by 150% [5]. Additionally, both the HO and the VO must allocate resources to handle all roaming UE's traffic, leading to less efficient resource utilization in the home and visited network that increases operational costs [5].

In contrast, with LBO the roaming UE's Internet access requests are served by the VO directly [3, 5], which addresses the latency issue, thus improving the QoS and making the LBO more suitable for real-time applications. Also, LBO does not require the HO to allocate resources for internet usage, resulting in reduced operational costs, while the HO compensates the VO for providing the services to the roaming UE. However, LBO also introduces some significant challenges, especially when it comes to trusting the VO to accurately report the data usage of the roaming UEs. The HO no longer has any mechanisms to verify the reported data usage, which could potentially lead to misuse as the VO now has an incentive to over-report data usage, and the VO could be providing the roaming UE an otherwise worse QoS than promised in the roaming agreement. In this context, [8] provide a conclusion that although LBO provides a promising solution for better QoS and reduced latency by routing traffic via the VO, the adoption of LBO has been hindered by challenges in trust and policy enforcement between operators.

To provide better QoS compared to HRO, the GSMA [23] has proposed a new routing approach, the IPX hub breakout (IHBO) [24, 25], where the Internet traffic is routed through centralized interconnection hubs that facilitate communication and data exchange between mobile network operators through service level agreements. So far, there are already some deployed hubs, typically located at major interconnection points or data centres. This means that the IHBO cannot offer the same low latency as LBO, though in some cases it could provide lower latency than HRO, particularly if the hub is geographically closer to the roaming UE. However, this is not guaranteed, as the physical location of the hub and UE can still vary significantly, thus increasing latency of the roaming UE compared to LBO. Moreover, the IHBO might enhance trust at inter-operator level as the IPX hub acts as a neutral

intermediary that is responsible for ensuring secure, reliable traffic routing. However, this requires the operators to trust a third party that increases dependency on complex coordination with IPX providers, and the introduction of a third party also significantly increases the costs. Thus, with IHBO the QoS improvement is inconsistent, the trust issues are not fully eliminated, and there are significant additional costs.

As an alternative to traditional roaming, mobile network aggregators (MNAs) [26] have emerged to support cross-border connectivity, particularly for Internet of Things and enterprises. The MNAs such as Google Fi [27], Twilio [28], and Soracom [29] provide a unified platform that abstracts the complexity of managing roaming agreement by offering global SIMs capable of connecting to multiple mobile networks as home networks. Although MNAs streamline the commercial and operational aspects of roaming agreement, they provide alternative mechanism to package and access mobile services for specific customer segments only as these convenient services come with additional costs.

To address the trust issues of LBO, a patent [9] has proposed the idea of using certificates to register the UE and record the roaming UE's data usage by the UE, which is then verified and matched by the VO against its data records for the UE. Thus, this patent addresses the enhancement of the trust between operators in local breakout; however, it does not provide a complete protocol nor address the visibility of QoS. This paper expands on the patent by proposing the complete protocol along with analysis of the solution.

### 2.4 5G QoS with LBO

In 5G, quality of service (QoS) is a mechanism by which HO ensures that the subscriber receives the promised network performance for their services in terms of key metrics such as latency, throughput, packet loss, jitter, and service availability. As shown in Listing 1, these metrics are derived from key parameters such as:

1. 5G QoS identifier (5QI) that defines the QoS service class, e.g., 5QI $= 2$ for video conference (low latency), 5QI $= 9$ for live streaming (high throughput, relaxed latency).
2. Priority level, which defines the importance of different traffic flows (e.g., emergency calls).
3. Guaranteed bit rate (GBR) that specifies the minimum data rate guaranteed for a service (e.g., video calls require GBR to maintain a smooth user experience).

4. Maximum bit rate (MBR), defines the maximum allowed data rate for the service.
5. Packet error rate (PER) that defines the acceptable level of packet loss for the service.
6. Package delay budget (PDB), which defines the maximum time a packet can take to reach its destination (e.g., video conferencing typically has a PBD of ca. 150 ms)

```
{
    {
        "serviceName": "VideoStreaming", "qosProfile": {
            "5QI": 2,
            "priorityLevel": 30,
            "gbr": {
                "uplink": "2Mbps",
                "downlink": "10Mbps"
            },
            "mbr": {
                "uplink": "10Mbps",
                "downlink": "25Mbps"
            },
            "packetDelayBudget": "150ms",
            "packetErrorRate": "1e—4"
        }
    }
}
```

**Listing 1** Example of a video streaming QoS profile.

The HO defines the QoS policy and monitors its enforcement per subscriber, session, and service. Even when a subscriber is roaming with LBO, the HO is responsible for maintaining the QoS by monitoring the QoS key metrics (e.g., per session). However, the QoS provided by the VO may not always exactly align with the HO's policy due to the difference in the VO's network capabilities, service restrictions, or variation in QoS mapping, in which case the HO QoS parameter must be mapped to the VO's QoS parameters.

## 2.5 Requirements of the TLBO Solution

The state of current roaming solutions can be summarized as follows. First, from a QoS and efficiency point of view, LBO is clearly the superior roaming solution compared to HRO and IHBO, but it suffers from trust issues

that have hindered its wide-spread usage. Second, none of the existing or proposed solutions provide complete protocol to effectively enhances LBO's preferability for the operators. Third, subscribers' roaming experience can be further improved by streamlining the current registration process. Based on this summary, the following key requirements must be addressed to create a more trustworthy LBO solution:

1. R1: Enhance trust in data usage reports: The HO must have a mechanism to ensure the UE data usage report is trustworthy.
2. R2: Quality of service visibility: The home operator must have sufficient visibility of the QoS its roaming UE has been provided by the VO to ensure adherence to agreed performance expectations and policies.
3. R3: Registration efficiency: The VO should be able to (re)register the UE, without sending registration messages to the HO.

## 3 Trustworthy Local Breakout

This section describes the design of trustworthy local breakout (TLBO), which is developed on top of the idea presented in the patent [9]. It first presents the overall approach of TLBO, then describes the certificates used to carry the essential information, and finally the detailed protocol flow.

### 3.1 Solution Overview

The key element of the TLBO is utilizing the UE as an additional source for data usage and QoS information. This works particularly well as a UE and VO have, by nature, opposing incentives to misrepresenting the data, i.e., a misbehaving UE would like to under-report their data usage to reduce costs, while a misbehaving VO would like to over-report the data usage for additional compensation from the HO. These opposing incentives help ensure that the UE and VO are likely to accurately report all data, thus enhancing the trustworthiness of this information.

To satisfy the requirement R1, *enhance trust in data usage reports*, the roaming UE keeps its own usage record and sends it to the VO at the agreed frequency. The VO compares its own record with that of the UE, and forwards the matched record to the HO, thus facilitating the continued usage of TLBO. If, however, the record does not match, the VO informs the HO and falls back to the HRO roaming (to avoid future inconsistencies). This then leads to lower QoS and poor user experience for the UE, which can also reflect badly on the VO if this happens too often, so both the UE and VO have an incentive to comply with the TLBO and the joint reporting practice.

To address the requirement R2, *quality of service visibility*, the UE adds the QoS metrics (service type, latency, packet loss, jitter, etc.) for the agreed services to the same usage record. A sufficiently comprehensive report is important because, in the case of HRO, the HO serves the roaming UE giving it full visibility over data usage and QoS for specific services. However, with TLBO, the HO has much reduced visibility of the UE's usage records and service specific QoS provided by the VO. Therefore, the report allows the HO to assess whether the agreed QoS terms with the VO were met and, if not, the HO can re-negotiate QoS with the VO.

The frequency with which the UE submits the reports to the VO is a policy decision that the HO and the VO agree on during their roaming contract negotiation process. This frequency can be, e.g., time-based (near real-time, hourly, daily, etc.) or data-cap-based (e.g., every 50 MB for low data caps, every 1 GB for higher data caps). Choosing the reporting frequency is a balancing act as too frequent reporting creates unnecessary traffic between the VO and HO, undermining the requirement of reducing constant HO contact, while too infrequent reporting may cause the HO to lose oversight of the services the VO provides to the UE. Finally, the frequency can also be dynamic to reflect the frequency of observed problems at the service level or in the joint reporting, providing all parties with an additional incentive to better comply.

Finally, to fulfil the requirement R3, *registration efficiency*, the HO issues the roaming UE a certificate with the required registration information, which the UE is able to use to prove to the VO that it is authorized to (re)register in its network without sending multiple registration messages to the HO, thus streamlining the registration process significantly. The only message VO sends is UE's location when the UE for the first time registers to the VO network. If for any reason the certificate-based verification fails, the VO triggers the traditional 5G registration process as a fallback mechanism to register the UE.

Figure 3 summarizes the TLBO process. The UE presents the certificate (discussed in Section 3.2) used for registration (UERoamingVC – arrow 1). The VO verifies the certificate and registers the UE for network access.

```
{
    "roamingPolicies": {
        "roamingNotification": {
            "dataUsageThresholdMB": 100 // MB before sending notification
            "voiceUsageThresholdMinutes": 10 // minutes before sending ,→ notification
            "smsUsageThresholdCount": 10 // SMS count before sending ,→ notification
        },
```

```
        "tariff": {
            "dataTariffMB": 0.01, // price in dollar per MB
            "voiceTariffMinutes": 0.001, // price in dollar per minutes
            "smsTariffCount": 0.001, // price in dollar per sms
        },
        "qosProfiles": [{
                "serviceName": "VideoStreaming",
                "qosProfile": {}
            }
        ]
    }
}
```

**Listing 2** Example of the latest roaming information.

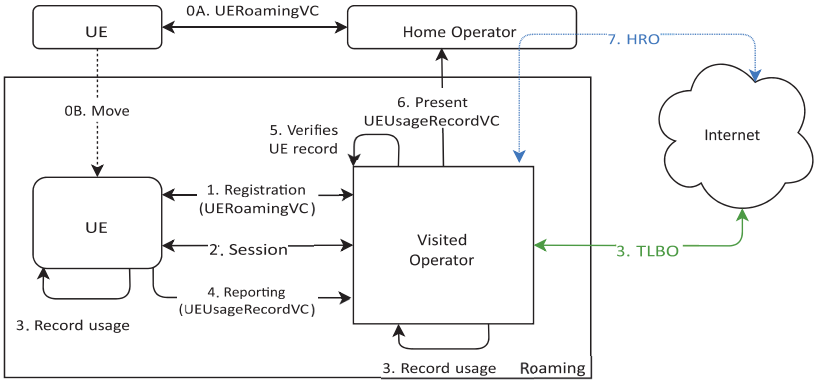


**Figure 3** Overview of the trustworthy local breakout solution with the key entities and their interactions.

With the first UE–VO registration, the VO also sends its ID to the HO and the HO sends the latest roaming information to the VO (Listing 2 depicts an example roaming policy). Additionally, with the VO ID, the HO is now able to forward the incoming calls and sms to the UE. Next, the VO establishes a session (arrow 2) with the UE, and serves the UE via TLBO (arrow 3) enabling faster internet access directly from the VO's network. At this point, both the UE and the VO start recording the network usage and QoS data (arrow 3). At the agreed frequency, the UE sends usage record certificate (e.g., in Listing 2) to the VO (arrow 4), which compares it to its own record (arrow 5). If the comparison is successful, the VO continues to serve the UE via TLBO (arrow 6) and sends the matched records to the HO; otherwise, the VO sends the two mismatched records (its own and the one from the UE) to the HO with the message that record comparison has failed and then falls back to the home routed roaming (arrow 7).

### 3.2 Certificates

As shown in Figure 3, in the TLBO, both the registration information (arrow 1) and the usage, QoS data (arrows 4–6) are not communicated directly from the source of the information to the intended recipient, but are passed via a third party (UE and VO, respectively), who has an incentive to modify the information to their own advantage. To ensure the trustworthiness of the information, it needs to be stored in an unmodifiable data structure that ensures the integrity and authenticity of the information.

To achieve this, the TLBO uses certificates [17], which provide a structured and unmodifiable way to store data. These certificates rely on issuer's digital signature to ensure that the data remain unmodifiable and that the issuer is who they claim to be. The signature is created using the issuer's private key and can be verified using its corresponding public key. If any modification to the data is attempted, the signature verification fails, and tampering is instantly detected. Additionally, to prevent replay attack, a random nonce and an expiry time are utilized to ensure the freshness of the requests.

There are several suitable certificate solutions such as public key infrastructure (PKI) [17] and verifiable credentials (VCs) [30]. However, in the TLBO, the certificate must support a flexible schema detailing the structure of the certificate as the information in each certificate depends on the subscribed services. PKI along with separate extension [31] supports flexible schema, but a more effective solution is VCs, which natively support a flexible schema. Typically, a VC issuer digitally signs these schemas, which are publicly available for the verifier to validate [30].

For the TLBO, two certificates are required: the *UERoamingVC* for the registration of the roaming UE and the *UEUsageRecordVC* for the roaming UE's usage record. A summary of both certificates is given in Table 1.

**Table 1** Summary of the TLBO verifiable certificates

| Credentials | Purpose | Issuer | Holder | Verifier | Content |
|---|---|---|---|---|---|
| UERoamingVC | Authorizes the UE to access services from the visiting network | HO | UE | VO | Listing 3 |
| UEUsageRecordVC | Ensures the data used and QoS received by the roaming UE | UE | VO | HO | Listing 4 |

```
{
"issuer": "https://operator.example/issuers/1",
"credentialSubject": {
    "id": "did:key:zDnaextBqyt9YYb9n334FzvFbo9bgWkdopNKA8mZ nRHA8J7Bq",
    "staticRoamingPolicy": {
        "isRoamingAllowed": true,
        "roamingRestricting": "EU only" // "None"
        "preferredRoamingType": "localBreakout",
        "fallbackRoamingType": "homeRouted", }
},
"proof": {
    "type": "DataIntegrityProof",
    "created": "2025−06−26T19:52:17Z",
    "verificationMethod": "did:key:zDnaextBqyt9YYb9n334FzvFbo9bgWkdopNKA8mZ
    nRHA8J7Bq",
    "cryptosuite": "ecdsa−rdfc−2019",
    "proofPurpose": "assertionMethod",
    "proofValue": "z4nZmBLXxztUcpX7ALxKqVj8ZsGK9XW7T9PgbE2vrrYf9FQoA719
  NEebtTgn7fnPTNFuGBY9CEquLdAPjaWXEgwtF" }
}
```


**Listing 3** Example of a UERoamingVC.

A HO issues a *UERoamingVC* to a UE. The UE then presents this certificate to the VO, which authenticates the UE and allows it to use its network. This can happen without the VO sending registration signals to the HO, as *UERoamingVC* includes all the necessary information such as the UE identifier, HO ID, static roaming policy, preferred roaming option, and fallback roaming option, data handling policy. A sample *UERoamingVC* is illustrated in Listing 3.


```
{
    "@context": [
      "https://www.w3.org/2018/credentials/v1",
      "https://www.3gpp.org/uerecord/vc/context/v1"
    ],
    "id": "urn:uuid:123e4567−e89b−12d3−a456−426614174000",
    "type": ["VerifiableCredential", "UEUsageRecordVC"],
    "issuer": "did:ue:123456abcdef", // UE is the issuer,
    "issuanceDate": "2025−02−20T12:00:00Z",
    "credentialSubject": {
      "id": "did:3gpp:visitedOperator:208−01", // VO identifier
      "roamingType": "LocalBreakout",
      "validityRegion": "EU",
      "totalDataConsumed": {"uplink":
```

```
        "2.01Gb",
        "downlink": "7.89Gb"
      },
      "sessionId": "session−2025−02−18−123456",
      "serviceQoS": [
        {
          "serviceType": "Video Conferencing",
          "throughput": "12.5Mbps",
          "latency": "50ms",
          "jitter": "12ms",
          "packet_loss": "1.2%"
        }
        ....., .....
      ]
    },
    "proof": {
      "type": "DataIntegrityProof",
      "created": "2025−04−27T17:58:34Z",
      "verificationMethod": "did:ue:123456abcdef#key−1",
      "cryptosuite": "ecdsa−rdfc−2019",
      "proofPurpose": "assertionMethod",
      "proofValue": "z5gCBzvpHbsJoeuuy5Z54rKQwkGzBZkmapRZZAKKW4ervhBGG
      Tay"
  }
}
```


**Listing 4** Example of a UEUsageRecordVC.

A *UEUsageRecordVC* (in short usage record) is the amount of data a roaming UE has consumed while roaming along with the corresponding perservice QoS metrics received from the VO. This usage record is digitally signed by the UE and sent to the VO, which validates the UE's signature and matches with its own UE usage record on how much data it has provided to the UE as well the QoS metrics per service. The VO further digitally signs this record to indicate it agrees with the data and presents it to the HO for final verification of the digital signatures of the UE and the VO as well as usage record of the UE. An example of a UEUsageRecordVC is illustrated in Listing 4 and its key attributes are as follows:

1. Visited operator identifier: A unique identifier of the VO that allows the HO to verify that the usage record is associated with the VO that presents the record.
2. Session identifier: A unique identifier associated with the UE's recorded data usage. The VO uses this identifier to match with the corresponding

session for the recorded data. Since, there can be multiple reports per session, a sequence number is appended to the session identifier e.g., sessionidentifier+01.
3. Total data usage: The total amount of data (uplink, downlink) consumed per reporting frequency.
4. Issuance date: The exact time at which the VC was issued.
5. Service QoS: It is a list of services (e.g., video conferencing, live streaming) with their respective QoS parameters (e.g., latency, throughput, etc.).
6. UE proof: A digital signature of the usage record is stored in this attribute.

### 3.3 Solution Operation

This section describes the detailed operations of the TLBO based on the following three assumptions. First, there is an existing roaming agreement between the HO and the VO that allows the roaming UE to register with the VO. Second, the UE gets a UERoamingVC from the HO with LBO as the preferred roaming option. Finally, both operators comply with the terms of the roaming agreement.

The next four subsections describe the 5G registration process, followed by the session establishment procedure, then the local breakout, and finally the reporting mechanism of the TLBO.

#### 3.3.1 5G registration

As soon as a roaming UE is powered on or airplane mode is deactivated, it begins to search for a preferred VO and initiates the 5G registration process. The UE chooses the VO based on the list of roaming operators (VOs) stored in its SIM, or the HO directs the roaming UE to connect to the preferred VO by rejecting the connection via a non-preferred VO [10].

The protocol for registering the UE to the VO takes the following steps, as depicted in Figure 4:

1. The UE sends a registration request to a preferred VO.
2. The VO sends an identity request message with a replay protection parameters, e.g., a nonce and its expiry time, to the UE.
3. The UE verifies the freshness of the nonce by checking the expiry time and, on success, sends the digitally signed proof of UERoamingVC together with the nonce to the VO.

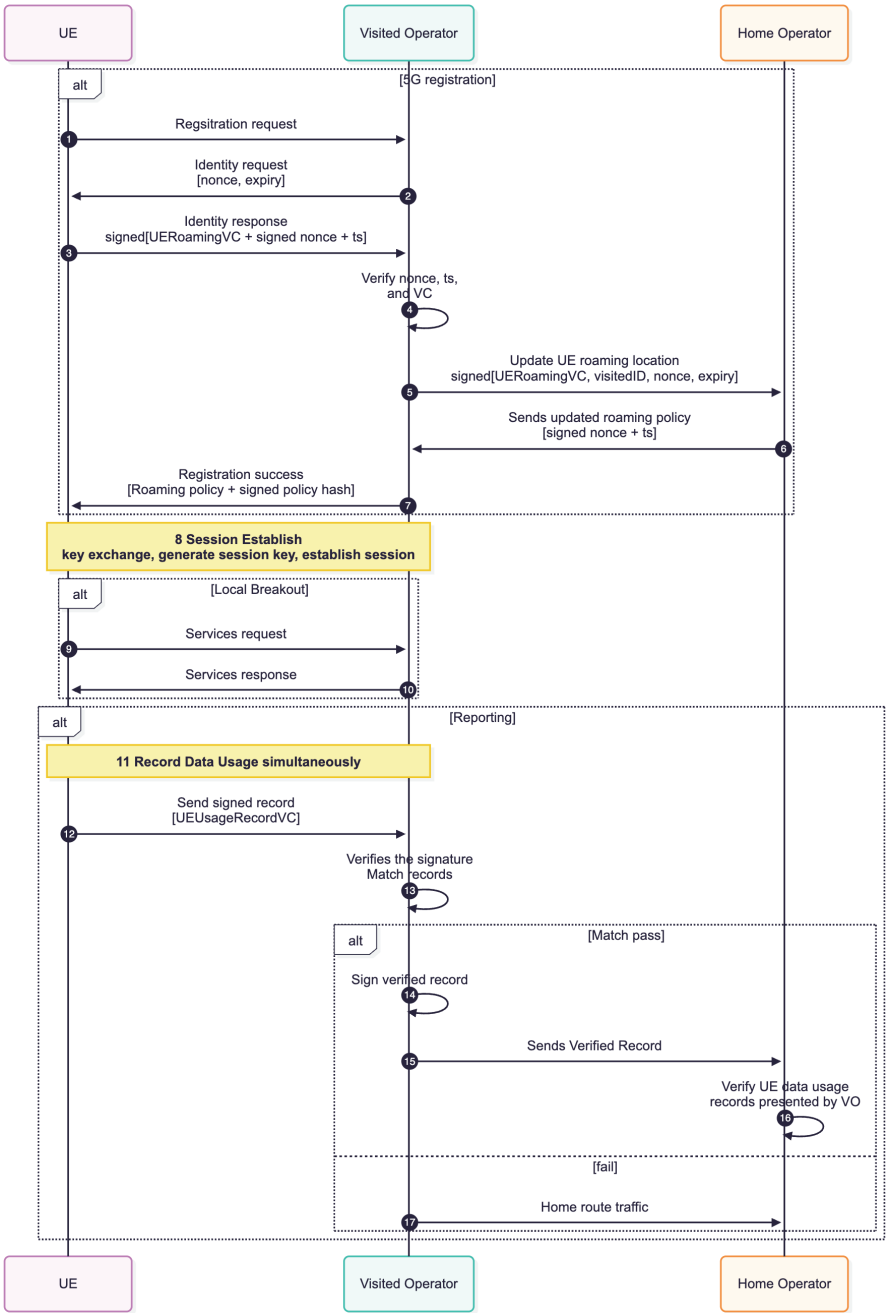


**Figure 4** Streamlined sequence flow of the trustworthy 5G local breakout solution.

4. The VO verifies that the nonce matches the one it previously sent in Step 2 and checks it has not expired. The VO then verifies both the UE's signature and the issuer's signature of the VC. However, if the nonce has expired, the VO repeats Step 2. Also, if either signature verification fails, the VO may fall back to the standard 5G registration process as detailed in Section 2.2.
5. The VO sends UE roaming location along with UERoamingVC digitally signed proof of its (visitedID) together with the nonce to the home operator.
6. The HO verifies the UE's identifier from the UERoamingVC as well as the proofs. On success, it responds with the updated roaming policies and timestamp to the VO.
   (a) The HO could send a reject response if the VO is not the preferred operator and steer the UE towards the preferred VO [10].
7. The VO stores the up-to date information of roaming policy, e.g., datacaps and the policy, which is proof that the VO has agreed to serve the UE based on the up-to date information. The VO sends registration success message to the UE.

#### 3.3.2 Session establishment

8. The VO and UE do a key exchange to generate a session key (using protocol such as elliptic curve Diffie–Hellman [17]). This session key is used to establish a session, similarly to how a session is currently established in the 5G system.

#### 3.3.3 Local breakout

9. Using this session, the UE starts requesting for services from the VO.
10. The VO serves the UE via LBO.

#### 3.3.4 Reporting

11. The UE and the VO both start recording data usage and QoS.
12. The UE sends the UEUsageRecordVC to the VO following the frequency policy received from the HO.
13. The VO checks the signature of the usage record and matches with its own record to verify the accuracy.
14. If record verification is successful, the VO also signs the UEUsageRecordVC.
15. The VO sends the double-signed record to the HO.

16. The HO verifies the signature of both the VO and the UE from the presented UEUsageRecordVC. It also checks the QoS received by the UE and whether this QoS matches the agreed QoS with the VO.
17. If there is discrepancy, then the fallback mechanism is triggered, that is, VO switches to routing UE traffic through HRO until the issue is resolved.

## 4 Analysis

This section details how the TLBO design satisfies all the requirements listed in 2.5. It also addresses the research questions: *"How can a TLBO solution be designed involving the subscriber's device and how does this affect the trustworthiness of the solution?"* (RQ:1) and *"How can the reregistration process of the UE while roaming using credentials be streamlined?"* (RQ:2).

### 4.1 Enhance Trust in Data Usage Reports (R1)

The TLBO design enhances trustworthiness of the data usage information by providing the HO with an additional source of the roaming UE's data usage report. Unlike the current LBO approach, where the HO relies solely on the report provided by the VO, who has an incentive to over-report, the TLBO uses the roaming UE as an additional source, who has an incentive to under-report the data usage. The TLBO design uses verifiable credentials (VCs), specifically the UEUsageRecordVC, to report the UE's data usage, which is digitally signed by the UE and ensures that the record was created by the UE, and any tampering with the record invalidates the signature, thereby making tampering easily detectable. Further, the VO then matches the reported data with the record it maintains for the UE. The record match ensures that the UE is not under-reporting, else usage record will not match. The record is digitally signed by the VO and sent to the HO, which verifies each party's signature and checks the record match. If the match has failed, then the HO will notify the VO and might trigger fall-back to HRO roaming (as discussed in Section 2.3) to avoid any further mismatch or discrepancies. This is true also for the case if the VO has over-reported, which will result in the mismatch record thereby the HO decides to fall-back to HRO. As soon as HRO is triggered, the UE will notice the added latency to its services, since the traffic traverses all the way to the HO, and the VO no longer handles the UE traffic locally.

Although the UE and VO have opposing incentives to behave, which helps to ensure accurate reporting by both parties, there is still the possibility

of mismatched reporting. This could be e.g. due to operational issues such as poor coverage area of the VO, deliberate record manipulation by a compromised UE or VO, or the UE might have connectivity issues or a drained battery. To mitigate these risks, the VO and the HO can make policy decision on how to handle it. For example, a predefined tolerance level for discrepancies (e.g., less than 1% of the usage limit) can be agreed so that the VO continues to serve the UE via TLBO and handles compensation using the agreed mechanism. However, if there are discrepancies that exceed the tolerance level, the VO would notify the HO and request re-routing the traffic via HRO until these discrepancies are addressed, affecting the QoS of the UE. Given these consequences, both parties are likely to act in good faith.

Other potential cases of mismatch could be, for instance, if the VO has some technical issue in accurately recording the UE's usage data. In this case, the mismatch will happen with all roaming UEs and hence all the traffic will end up being HRO. The HO might notice this pattern and inform the VO of the potential issue. Alternatively, the issue might be with only specific UE type (model of a mobile phone), e.g., an issue in the library used for creating records, and thus there is mismatch of the records. In this case, the VO could monitor the mismatch patterns of these UE type and inform the HO (and the UE's manufacturer) about the possible issue with the specific UE type. In some case, it could be, only individual UE has issue in accurately recoding the usage data, thereby gets its traffic HRO. In this case, HO marks this UE as suspicious and monitors it again with the next VO, and if the problem does not persist, the UE is allowed to use TLBO normally, else HRO and it could signal the UE to, e.g., restart the device for potential troubleshooting. In any case, these are not design issues, rather, they are operational issues that arise because of, e.g., the UE or network configurations.

Despite the fact that the UE recording data usage enhances the HO confidence, the UE remains the least trustworthy entity in the mobile network. This is because the UE is within the subscriber's control, and in theory a malicious subscriber could modify the usage record stored in the SIM/eSIM to under-report for their financial gain. However, with TLBO, the VO always matches the UE record with the record it has maintained for the UE, thereby detecting the manipulated record. Repeated detection of such behavior could lead the UE to be served via HRO, leading to a decrease in QoS and in worst case blacklisting the UE. This ensures that subscribers have minimal incentive to manipulate records, ultimately safeguarding the reliability of data usage reporting. Further, SIM/eSIM is a secure module with hardware level security and, typically, tampering with the data is practically impossible for

a subscriber. If needed, the records can be stored in an alternative secure module, such as a trusted platform module (TPM) [32], which is expected to be supported by the next generation of SIM technology, integrated SIM (iSIM) [12].

Furthermore, a malicious UE could potentially collaborate with a malicious VO to over bill the HO, provided the UE gets some compensation from the VO. For this, the compromised UE could provide its signing keys to the VO, who creates and signs both records. Alternatively, the UE could also just generate false, large records that the VO would happily sign to over-report. In any case, the HO has to pay the VO for reported roaming records. However, frauds like this would require a very highly skilled attacker and active collaboration between both parties. If suspected by the HO, it could lead to investigation, potentially leading to blacklisting the UE and damaging the VO's reputation. Nevertheless, for the majority of the subscribers, this is unlikely as the keys in the e/SIM has hardware-level security, which is tamper-resistant [33]. If necessary, another type of secure module such as a trusted platform module [32] could be used, if needed. Given the difficulty and risks involved, such cases would be limited in practice.

In some case, the UE and the VO might collaborate together to force HRO, thereby increasing the resource usage in the HO network. However, in this case, neither part (UE/VO) would benefit as the UE will get lower QoS and since there is no LBO, the VO resources are less used, thereby effecting its roaming data revenue.

Another possible concern might be the feasibility of storing the latest UEUsageRecordVC and related data to the eSIM, which is traditionally optimized for storing mobile-network related data such as cryptographic keys and mobile subscription profiles [7], and typically has limited storage. However, most modern eSIMs have memory from several KB (512 KB) to a MB to accommodate multiple subscription profiles and extended functionalities [33, 34]. The size of a typical UEUsageRecordVC is approximately 4 KB, assuming that the record has VC metadata, QoS profile for multiple services (voice, video, live streaming, web, online gaming), and VC proof, hence, the available memory easily accommodates such records. In addition, since the record is intended to be cumulative and only the latest one has to be kept, long-term storage requirements are minimal.

The alternative roaming breakout solution, IPX hub breakout, discussed in Section 2.3, does enhance trust between operators on the roaming data usage as IPX providers act as intermediaries responsible for ensuring secure and reliable traffic to the roaming UE. However, this requires that the

operators extend their trust to hub providers, which increases dependency and complex co-ordination with third parties – IPX providers. Furthermore, creating and maintaining the hubs is a non-insignificant additional expense the parties would have to cover.

In all of these cases, routing the traffic via HRO always enable the HO to have the most accurate picture of data usage and QoS but at the cost of reduced QoS. The TLBO improves QoS and makes all these potential misuses more difficult to implement compared to LBO, so combined with the inherent opposing incentives TLBO significantly increases the trustworthiness of the usage information, thus addressing RQ1 and the requirement R1 with minimal extra cost to all parties.

### 4.2 Quality of Service Visibility (R2)

The TLBO effectively enhances the QoS visibility by providing the HO with detailed insights into the quality of service experienced by its roaming UE while using TLBO. TLBO achieves this by enabling the UE to record the specific service-level QoS metrics it has received in the usage record, UEUsageRecordVC. This allows the HO to compare the recorded QoS with the agreed-upon QoS policy, ensuring that the VO has met the policy, thus addressing the requirement R2. If QoS requirements are not met, the HO can notify the VO of a potential agreement violation and, in response, prioritize HRO over TLBO for its UE. Repeated policy violations can negatively impact the VO's brand, thus damaging the relation with the roaming operators.

Moreover, timely reporting of the usage data is important for the HO's ability to enforce service quality checks. The reporting frequency is a policy decision for the HO and the VO to agree on. This frequency ensures accurate tracking of data usage, minimizes discrepancies in the records, and maintains service enforcement. However, inconsistency of reporting could indicate potential issues, such as weaker collaboration between operators.

According to [7], "the 5G roaming latency in Europe is awful", with average median roaming latency of around 105 ms, and in some countries up to 200 ms. By contrast, the average median local latency is around 38 ms [7]. These latencies are acceptable with older generations of mobile networks such as 3/4G, where subscribers expected and tolerated higher latency, but the eventual 5G latency goal is below 10 ms [35, 36], which is radically lower than the 100+ ms experience during roaming. With TLBO, roaming latency would be comparable to local latency, thus providing service parity both home and abroad. Also, this enables smooth user experience of services like VoIP, where latency below 50 ms is generally excellent, while latency

approaching 150 ms starts to become problematic [37]. Thus, by reducing the roaming latency to the local latency, the TLBO significantly enhances the QoS and subscriber experience in the roaming case.

The IPX hub breakout solution does potentially improve the QoS of the roaming UE somewhat compared to the HRO, especially in the case if the hub is physically located close to the roaming UE. However, this is not guaranteed, as the physical location of the hub and UE may still vary significantly, thereby still having a significantly higher latency compared to TLBO.

With TLBO, the roaming UE is always served directly by the VO, achieving latency levels similar to local latency, thereby improving the QoS of the UE and at same time recoding the service-level QoS metrics to the usage record VC, providing visibility of the QoS received by the UE to the HO, addressing R2.

### 4.3 Registration Efficiency (R3)

The TLBO design optimizes the current registration process by decreasing the message exchange between the VO and the HO from a total of 6 (4, 6, 11, 13, 14, 15 in Figure 1) to just two messages (5, 6 in Figure 4) for the first UE registration, and to zero messages with any consecutive reregistration of the UE with the same VO. Therefore, the VO no longer needs to exchange multiple messages with the HO for the UE registration.

The TLBO achieves this registration efficiency by incorporating UERoamingVC, which contains all necessary information such as the HO's ID, name, and subscription data necessary for the roaming of the UE. The VC ensures that the roaming information is authentic and has not been tampered with. Also, the VO can independently verify this VC, eliminating the need to query the HO for UE registration, thereby reducing signaling overhead.

Furthermore, the subscription data within the UERoamingVC has the roaming policy to explicitly authorize the UE to access the network via TLBO. This mechanism ensures that both the UE and the VO can establish a secure registration without requiring multiple messages to the HO. As a result, the TLBO effectively improves registration efficiency, thus addressing R3.

While roaming, a UE typically needs to re-register multiple times to the HO because of reasons such as the HO policy, UE registration has expired, the UE has moved to new roaming area, or connected to a new VO. In the conventional registration process, each reregistration would require repeated messaging between the VO and the HO, introducing latency and inefficiency.

However, with TLBO, since the UERoamingVC already has all necessary information and authorization information, the VO can re-register the UE with minimal HO involvement, thus reducing the registration and subscription data messages to the HO, which improves operation efficiency and enhances the overall roaming experience to the user due to faster registration.

In terms of latency, according to the 5G-MOBIX [38], the control plane (e.g., registration, authentication, session) latency of HRO can range up to 200 ms per message just within Europe because of interconnection between operators, which increases with the distance between the HO and the VO [5]. Using the baseline of 200 ms, the current registration process would add around 600 ms, while with TLBO first registration of 200 ms, and reregistration from the same VO, there is no HO latency since there is no request to the HO. This means compared to the current registration process, there is a gain of more than 60% with the TLBO registration and up to 100% with re-registration with the same VO. This is significant improvement in the 5G registration process, thereby effectively addressing RQ2 and making TLBO a compelling alternative to HRO.

A potential consideration of TLBO is that UERoamingVCs increase certificate management as a single UERoamingVC would not be optimal for all the VOs in the world, so each subscriber has to be issued with at least a few UERoamingVCs. Further, these credentials cannot remain valid indefinitely but need to be reissued periodically. This means that while the HO benefits from reduced activity during the registration operations, they have some additional credential issuance to do. Also, with multiple credentials, more UE storage is required. These credentials could be issued per roaming agreements or operator regions, for example, a roaming VC for Europe, Asia, etc. However, these credentials' issuance is a relatively lightweight operation in terms of both computing and cost. Also, the storage requirements are minimal, as credentials typically range from a few hundred bytes to a few kilobytes in size. The current SIM/eSIM are well equipped to handle the storage of these certificates without significant resource constrains.

## 4.4 Summary

The TLBO design introduces a number of changes to the current roaming solution 2. First, for VC based registration, the SIM/eSIM [12] needs to support certificate-based credentials. This credential is already supported by 3GPP [6] with an EAP-TLS registration mechanism [16] and is used for enterprise 5G private networks [18]. Thus, integration of the VC is already possible with the current 5G registration design.

Second, the UE creates a UERoamingVC that is verified by the VO. This introduces an additional step to VC digital signature creation and verification. According to [39], one of the popular digital signature algorithms, the elliptic curve digital signature algorithm (ECDSA), the signature creation time is around 25–35 ms and the verification time is around 70–90 ms in a single threaded CPU. Compared to the round trip latency of the message sent to the HO (200 ms), the signature creation and verification overhead is negligible, and thus, significantly more efficient than sending messages to the HO.

Lastly, the TLBO may introduce minor traffic overhead because of the VO sending the comprehensive UEUsageRecordVC to the VO. However, this limitation is not unique to the proposed solution, as even with HRO, the VO needs to send resource usage information to the HO, so the additional overhead is negligible as long as the reporting frequency (a policy desicion) is not excessively high.

The design of TLBO, therefore, successfully addresses the research questions and meets the outlined requirements. The analysis demonstrates the improved trustworthiness, feasibility, and efficiency of the solution.

## 5 Discussion

The trustworthy local breakout (TLBO) solution streamlines the 5G registration process, improves the QoS for the roaming UE, and addresses the trust issue of the current local breakout solution between the home operator (HO) and the visiting operator (VO). Other solutions discussed in Section 2.3 enable more efficient roaming compared to HRO but the trust and QoS efficiency gap still exists. The patent [9] addresses the trust issue but lacks details and analysis of the solution design. This paper details the complete protocol, the TLBO, that enables local breakout for the roaming UE, including the recording of both data usage and QoS of the UE in verifiable manner, thereby facilitating wider adoption of LBO.

For the HO, the TLBO offers numerous advantages. Most importantly, the ability of the UE to record and report the data usage and QoS in the verifiable manner significantly enhances trust in the roaming scenario. This addresses the main concern associated with LBO, i.e., potential for the VO to over-report. By relying on secure, tamper-proof usage record generated by the UE, the HO can ensure accurate billing settlement, even when the traffic is no longer routed to the HO's network.

Moreover, the TLBO provides a major improvement not available in the existing LBO roaming model, visibility into the QoS received by the roaming

UE while connected to the VO. By allowing the UE to record verifiable QoS metrics, such as latency and throughput, the HO can monitor the performance of the VO. This insight supports a quality-driven service level agreement, helps identify and resolve performance issues, and reinforces the operators' ability to maintain their brand even when the subscriber is abroad.

Further, TLBO offloads the roaming traffic to the VO. Thus, the HO does not have to allocate dedicated resources for the roaming UE, leading to cost savings in both transport and processing resources. This enables HOs to offer more flexible and competitive roaming plans, enhancing customer satisfaction and retention without compromising control over usage data or revenue.

For the roaming subscriber, the TLBO provides noticeable benefits with improved service quality, as the latency remains essentially the same while roaming (assuming the VO has a similar network technology level). In this case, especially latency-sensitive applications such as online-gaming and video conferences benefit from faster response times and stable connections, since the data traffic does not route all the way back to the HO. This performance improvement leads to a better subscriber experience.

Moreover, the UE's ability to record the usage record in a verifiable manner enables the subscriber to gain more accurate insights into their data consumption and QoS received, which can assist in managing the subscriber's roaming costs and expectations.

Additionally, with TLBO, the reduced infrastructure cost of the HO could translate to lower subscriber roaming costs, and at the same time provide improved QoS, thereby addressing the regulation "Roam Like at Home".

For the VO, the TLBO allows local registration and LBO of the roaming UE which is managed by the VO locally, thereby simplifying network operation and allowing direct QoS enforcement. With this, the VO can ensure a higher standard of service and responds more effectively to localized issued affecting roaming subscribers.

Overall, improved QoS while roaming leads to higher subscriber satisfaction, even outside the home network, which ultimately contributes to subscriber retention for the HO. This also opens up an opportunity for premium roaming offerings, increasing the HO's revenue. Similarly, roaming subscribers are more likely to consume high-value services such as virtual reality, augmented reality, and high-quality streaming services that would increase the data usage of the VO, translating to higher revenue for the VO.

The TLBO primarily uses certificates, which makes its deployment feasible as the current 5G system already supports certificate-based authentication

2.3. Hence, implementing the proposed solution is already supported by existing 5G systems.

By allowing the roaming UE to record the usage data and QoS metrics, the TLBO addresses the long-standing challenges of trust, visibility, and performance in roaming scenarios. It facilitates the broader adoption of LBO, which benefits all stakeholders. Thus, this solution provides a solid foundation for improved global mobility that aligns with technical improvement with commercial and user-centric goals. Finally, while technically the TLBO has been designed for 5G, the existing 3GPP support for certificate-based credentials and the key features of the TLBO of enhanced trust and improved QoS potentially make it an essential element in roaming also for the next generations of mobile networks (6G).

## 6 Conclusion

Using the current preferred roaming solution (home routed) to serve the roaming UE is unoptimal because it significantly lowers the QoS compared to LBO, thereby not respecting policies such as "Roam Like at Home". LBO does address the QoS issue; however, there are trust issues between the HO and the VO, as the HO depends on a single source, the VO, to accurately report the roaming UE service usage, with no means to cross-verify this record. Hence, LBO is only seldom used as a roaming solution, although it has been standardized in the 3GPP since 2/3G.

The TLBO solution described in this paper enhances trust between the HO and VO by having both the UE and VO record the service usage data to ensure the data/service has indeed been used by the roaming UE, and that there is no potential for misuse by any of the parties. Further, the solution streamlines the UE registration process by significantly reducing (60%) the number of messages sent between the HO and the VO. Overall, the TLBO improves the roaming subscriber QoS by enabling local breakout as the preferred roaming solution over HRO.

## Acknowledgment

The authors thank Professor Valtteri Niemi, Patrik Salmela, and Andrew Williams for their valuable comments during the writing of the paper.

## References

[1] Ericsson. Ericsson mobility report – mobile data traffic to triple. https://www.ericsson.com/en/press-releases/2023/11/ericsson-mobility-reportresilient-5g-uptake---global-mobile-data-traffic-set-to-triplein-six-years, 11 2023. (Accessed on 2025-01-26).

[2] ITB Berlin. Itb berlin and ipk international: Big global increase in outbound travel in 2023 (february 26, 2024) – the world of itb. https://www.itb.com/en/press/press-releases/news_15168.html, 02 2024. (Accessed on 2025-02-18).

[3] ETSI. 3GPP TS 23.501 (v18.5.0), 5G; System architecture for the 5G System (5GS). Technical report, 3GPP, 05 2024. https://www.etsi.org/deliver/etsi_ts/123500_123599/123501/18.05.00_60/ts_123501v180500p.pdf.

[4] J. Bahrke and C. Manoury. New roaming rules for travellers in the eu. https://ec.europa.eu/commission/presscorner/detail/en/IP_22_4198, 06 2022. (Accessed on 2025-04-15).

[5] A.M. Mandalari, A. Lutu, A. Custura, A.S. Khatouni, O. Alay, M. Bagnulo, V. Bajpai,¨ A. Brunstrom, J. Ott, M. Trevisan, M. Mellia, and G. Fairhurst. Measuring roaming in europe: Infrastructure and implications on users' qoe. *IEEE Transactions on Mobile Computing*, 21(10):3687–3699, 2022.

[6] 3GPP. The 3rd generation partnership project (3gpp). https://www.3gpp.org/ about-us, 2024. [Online; accessed 2025-01-26].

[7] GSMA. RSP Architecture SGP.21 V3.1. Technical report, GSMA, 12 2023. https://www.gsma.com/solutions-and-impact/technologies/esim/wp-content/uploads/2023/12/SGP.21-V3.1.pdf.

[8] V. Vomhoff, H.D. Jang, M. Varvello, S. Geißler, Y. Zaki, T. Hoßfeld, and A. Lutu. Challenges and opportunities for global cellular connectivity. *arXiv*, 2024.

[9] P. Salmela, M. Thakur, and S. Paavolainen. Wo2022258180a1 – data usage records for roaming wireless devices. https://patents.google.com/patent/WO2022258180A1, 09 2021. (Accessed on 2025-07-23).

[10] R. Keller, D. Castellanos, A. Sander, A. Robison, and A. Abtin. Roaming in the 5g system: The 5gs roaming architecture. *Ericsson Technology Review*, 2021(6):2–11, 2021.

[11] ETSI. 3GPP 23003 (v18.6.0), Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Numbering, addressing and identification. Technical

report, 3GPP, 07 2024. https://www.etsi.org/deliver/etsi_ts/123000_123099/123003/18.06.00_60/ts_123003v180600p.pdf.

[12] D.G. Koshy and S.N. Rao. Evolution of sim cards – what's next? In *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pages 1963–1967, 2018.

[13] J. Vollbrecht, J.D. Carlson, L.B., B.D. Aboba, and H. Levkowetz. Extensible Authentication Protocol (EAP). https://www.rfc-editor.org/info/rfc3748, 06 2004. (Accessed on 2025-04-12).

[14] J. Arkko, V. Lehtovirta, and P. Eronen. Rfc 5448 – improved extensible authentication protocol method for 3rd generation authentication and key agreement (eap-aka'). https://datatracker.ietf.org/doc/html/rfc5448, 05 2009. (Accessed on 2025-07-23).

[15] A. Kunz and A. Salkintzis. Non-3gpp access security in 5g. *Journal of ICT Standardization*, 01 2020.

[16] D. Simon, R. Hurst, and B. D. Aboda. Rfc 5216 – the eap-tls authentication protocol. https://datatracker.ietf.org/doc/html/rfc5216,032008. (Accessed on 2025-06-18).

[17] W.J. Caelli, E.P. Dawson, and S.A. Rea. Pki, elliptic curve cryptography, and digital signatures. *Computers Security*, 18(1):47–66, 1999.

[18] X. Huang, T. Yoshizawa, and S.B.M. Baskaran. Authentication mechanisms in the 5g system. *Journal of ICT Standardization*, 05 2021.

[19] Starlink. Starlink. https://www.starlink.com/. [Online; accessed 2025-06-04].

[20] ETSI. 3GPP TS 23.503 (v18.9.0), 5G; 5G System: Unified Data Management Services. Technical report, 3GPP, 03 2025. https://www.etsi.org/deliver/etsi_ts/129500_129599/129503/18.09.00_60/ts_129503v180900p.pdf.

[21] ETSI. 5G; Security architecture and procedures for 5G System (3GPP TS 33.501 version 18.6.0 Release 18). Technical report, 3GPP, 07 2024. https://www.etsi.org/deliver/etsi_ts/123000_123099/123003/18.06.00_60/ts_123003v180600p.pdf.

[22] P. Chawdhry, G. Folloni, S. Lumachi, and S. Luzardi. Roaming performance study – shaping europe's digital future. Technical report, European Commission, 2021. https://digital-strategy.ec.europa.eu/en/library/roaming-performancestudy.

[23] GSMA. Who we are – about us. https://www.gsma.com/about-us/who-we-are/. [Online; accessed 2025-07-23].

[24] D. Gunawan and K. Budiono. Comparative analysis on some possible partnership schemes of global ip exchange providers. *ArXiv*, abs/1404.2989, 2014.
[25] GSMA. Ng.137 ipx requirements. Technical report, GSMA, 2024. https://www.gsma.com/newsroom/wp-content/uploads//NG.137-v1.2.pdf.
[26] D.J. Hyunseok, M. Varvello, A. Lutu, and Y. Zaki. Unraveling the airalo ecosystem. *arXiv*, 08 2024.
[27] Google. Google fi wireless for phone plans & mobile phone deals. https://fi.google.com/about. [Online; accessed 2025-06-04].
[28] Twilio Inc. Twilio communications platform cpaas – twilio. https://www.twilio.com/en-us/cpaas. [Online; accessed 2025-06-04].
[29] Soracom Inc. Cellular iot connectivity platform for m2m devices – soracom. https://soracom.io/home/. [Online; accessed 2025-06-04].
[30] M. Sporny, D. Longley, and D. Chadwick. Verifiable credentials data model v1.1. https://www.w3.org/TR/vc-data-model. (Accessed on 2025-07-23).
[31] S. Boeyen, S. Santesson, T. Polk, R. Housley, S. Farrell, and D. Cooper. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Technical report, RFC Editor, 2008. https://www.rfc-editor.org/info/rfc5280.
[32] Trusted Computing Group. Tpm 1.2 main specification — trusted computing group. https://trustedcomputinggroup.org/resource/tpm-main-specification/. [Online; accessed 2025-06-15].
[33] GSMA. eSIM Whitepaper The what and how of Remote SIM Provisioning. Technical report, GSMA, 03 2018. https://www.gsma.com/solutions-and-impact/technologies/esim/wp-content/uploads/2018/12/esim-whitepaper.pdf.
[34] Hologram Inc. esim vs. iot sim card: 5 differences explained. https://www.hologram.io/blog/esim-vs-iot-sim-card-5-differences-explained/, 05 2025. [Online; accessed 2025-05-21].
[35] R. Kumar, D. Sinwar, and V. Singh. Qos aware resource allocation for coexistence mechanisms between embb and urllc: Issues, challenges, and future directions in 5g. *Computer Communications*, 213:208–235, 2024.
[36] ETSI. 5G; Service requirements for the 5G system (3GPP TS 22.261 version 18.18.0 Release 18). Technical report, 3GPP, 07 2025. https://www.etsi.org/deliver/etsi_ts/122200_122299/122261/18.18.00_60/ts_122261v181800p.pdf.

[37] H. Hasbullah, A. Said, and K. Nisar. The effect of echo delay on voice quality in voip network, 01 2009.

[38] G. Kalem, F. Setaki, A. Georgakopoulos, S. Col, S. Messinis, T. Sari, M. Muehleisen, K. Katsaros, and A. Arda. 5g-mobix: The greece–turkey cross–border corridor 5g deployment and use cases results. In *022 IEEE Future Networks World Forum*, pages 43–48, 10 2022.

[39] K. Chalkias, J. Lindstrøm, D. Maram, B. Riva, A. Roy, A. Sonnino, and J. Wang. Fastcrypto: Pioneering cryptography via continuous benchmarking. In *ICPE 24: 15th ACM/SPEC International Conference on Performance Engineering*, pages 227–234, 05 2024.

## Biographies

**Mukesh Thakur** received his M.Sc. degree in computer science from University of Helsinki, Finland in 2017, and is currently working towards his Ph.D. in computer science. His research interests include mobile networks, distributed ledgers and blockchains, decentralized identifiers and verifiable credentials, and future network technologies.

**Yki Kortesniemi** received his M.Sc. (Tech.) degree in industrial management in 1998, his Lic.Sc. (Tech.) degree in 2003 in computer science from Helsinki University of Technology, Finland, and his D.Sc. (Tech.) degree in networking technology from Aalto University, Finland, in 2015. He has worked on numerous research projects at Helsinki University of Technology and Aalto University including the EU H2020 projects SOFIE and IoT-NGIN. His research interests include information security and privacy, data protection, MyData and legal design, Internet of Things, distributed ledgers and blockchains, and decentralized identifiers and verifiable credentials.