Bundesministerium Finanzen

KIRAS Sicherheitsforschung

FFG Promoting Innovation.



TelCrit

Cybersecurity Assessment of Modern Mobile Communication Services in Austrian 4G/5G Networks

A project funded under the **KIRAS** programme

Scientific Final Report

September 2026

Project number	59103683
Programme	KIRAS security research programme of the Federal Ministry of Finance (BMF)
Duration	04/2025 – 09/2026 (12 months + 6-month cost-neutral extension)
Consortium lead	SBA Research gGmbH
Partners	Kibosec GmbH; Rundfunk und Telekom Regulierungs-GmbH (RTR, end user)

TelCrit has been funded by the Austrian security research programme KIRAS of the Federal Ministry of Finance (BMF).

Summary

The project TelCrit systematically investigated the security of modern mobile network and communication services, with a focus on the Austrian market. Security- or privacy-relevant vulnerabilities and configuration weaknesses were identified at every Austrian mobile network operator examined, among others in the areas of VoLTE and VoWiFi.

The analysis of RCS further revealed a strong dependency on Google Jibe: all Austrian providers examined rely on this infrastructure. International measurements confirmed that Austria is not an exception in this respect – around 98 % of the RCS servers identified in the project are controlled by Google. This underlines the growing importance of digital sovereignty for modern communication infrastructures.

In addition, new attack techniques and vulnerabilities were identified in widely used instant messaging services. In the course of responsible disclosure, concrete countermeasures were developed together with the affected vendors and subsequently rolled out. The project results were presented at international scientific and security conferences, received a Best Paper Award, and attracted broad national and international media attention.

TelCrit thus makes a concrete contribution to improving the security and transparency of modern communication infrastructures and, at the same time, establishes a scientific basis for their future security assessment.

Bundesministerium Finanzen

KIRAS Sicherheitsforschung

FFG Promoting Innovation.

Consortium and Project Organisation

Consortium

SBA Research gGmbH (consortium lead, scientific partner)
SBA Research has an extensive track record in mobile network security research and had previously disclosed vulnerabilities and misconfigurations at Austrian operators (e.g., CVE-2024-22064). It was responsible for the technical implementation and the scientific work.

Kibosec GmbH (company partner)
Kibosec is an independent IT-security consultancy with expertise in telecommunications and standardisation and international connections (e.g., ETSI TC CYBER). Its expertise in data protection (GDPR) was of particular value given that RCS is partially provided via foreign infrastructure.

Rundfunk und Telekom Regulierungs-GmbH (RTR, end user)
As the national regulatory authority, the RTR helped to set meaningful priorities based on current market developments and legislation, mediated between researchers and operators, and is the primary recipient of the results.

Course of the Project

The original objectives remained relevant and realistic throughout the project. Their relevance even increased due to the progressing transition to 4G/5G-based communication services and the growing importance of Internet-based messaging.

The main deviation from the original plan concerned the prioritisation of the technical work. Owing to unexpectedly extensive results and their high scientific and societal relevance, the focus was temporarily shifted from the radio layer to the Internet layer (VoWiFi, RCS, and related Internet-based communication services). In particular, the vulnerabilities identified in instant messengers required a coordinated disclosure process with Meta that lasted several months and involved regular – at times several times a week – technical meetings to analyse the problems and to develop and evaluate countermeasures. The deferred radio-layer work was completed later in the project. To accommodate the additional work, the project duration was extended by six months (from 12 to 18 months) at no additional cost. These adjustments had no negative impact on the achievement of the overall objectives; rather, they allowed particularly relevant results to be investigated in the required technical depth.

Contents

Summary i

Consortium and Project Organisation ii

1 Introduction 1
- 1.1 Mobile Networks as Critical Infrastructure . . . 1
- 1.2 Technological Transition: From Circuit Switching to IP-based Services . . . 1
- 1.3 Security Implications of the Technological Transition . . . 2
- 1.4 Project Objectives and Research Questions . . . 2
- 1.5 Summary of Contributions . . . 3
- 1.6 Structure of this Report . . . 3

2 Technical Background 5
- 2.1 IP Multimedia Subsystem and VoLTE . . . 5
- 2.2 Voice over Wi-Fi . . . 6
- 2.3 Radio Access Security and the SIM Card . . . 8
- 2.4 Rich Communication Services . . . 9
- 2.5 End-to-End Encrypted Instant Messengers . . . 9

3 Research Design and Methodology 12
- 3.1 Overall Research Design . . . 12
- 3.2 Measurement Perspectives . . . 12
  - 3.2.1 In-vivo Measurements . . . 12
  - 3.2.2 Static Client Analysis . . . 13
  - 3.2.3 Extended Server-side Analysis . . . 14
- 3.3 Scope . . . 14
- 3.4 Ethical Considerations and Responsible Disclosure . . . 15

4 Target State: Standards and Best Practices 16
- 4.1 Sources and Classification . . . 16
- 4.2 Radio Access . . . 17
- 4.3 VoWiFi and IMS Access Security . . . 17
- 4.4 IMS Signalling: Identities and Privacy . . . 18
- 4.5 Rich Communication Services . . . 19
- 4.6 End-to-End Encrypted Instant Messengers . . . 19
- 4.7 Observations . . . 19

5 Radio Layer and IMS Signalling 21
- 5.1 Radio Link Security Configuration . . . 21
- 5.2 Automated Security Testing of the IMS . . . 22
  - 5.2.1 Approach . . . 22
  - 5.2.2 Overview of Results . . . 23
- 5.3 Privacy Leakage due to Missing SIP Header Filtering . . . 24
- 5.4 Caller-ID Spoofing . . . 25
- 5.5 Further Findings . . . 26
- 5.6 Discussion . . . 27

6 Internet Layer: Voice over Wi-Fi **28**
6.1 Starting Point: Prior Global VoWiFi Studies . . . 28
6.2 Beyond L1: SIM-based Analysis of Austrian Deployments . . . 28
6.2.1 Missing ePDG Authentication by Certificate . . . 29
6.2.2 Insecure Cryptography Across All Layers . . . 29
6.2.3 Longitudinal View on Static Keys . . . 30
6.3 Discussion . . . 30

7 Internet Layer: Rich Communication Services **32**
7.1 Methodology . . . 32
7.2 Results . . . 32
7.3 Discussion: Digital Sovereignty . . . 33

8 Internet Layer: Mobile Instant Messengers **34**
8.1 Silent Delivery Receipts . . . 34
8.2 Prekey Depletion in WhatsApp . . . 34
8.3 Enumeration at Scale . . . 35
8.4 Privacy Leakage in Apple iMessage . . . 35
8.5 Discussion . . . 35

9 Responsible Disclosure, Dissemination, and Impact **36**
9.1 Responsible Disclosure . . . 36
9.2 Scientific Publications . . . 36
9.3 Presentations and Community Events . . . 37
9.4 Media Coverage . . . 37

10 Conclusion and Outlook **38**

Bibliography **39**

Contact **43**

1 Introduction

1.1 Mobile Networks as Critical Infrastructure

Mobile networks are among the most important communication infrastructures in Austria. Beyond private and business communication, they are the primary access path to emergency services and play a central role in the coordination of crisis and disaster response. In exceptional situations such as natural disasters or large-scale power outages ('blackouts'), smartphones and base stations can remain operational for several hours thanks to batteries and backup power supplies. Mobile networks are therefore often among the last communication systems that remain available when other infrastructure fails. Uninterrupted, secure, and trustworthy mobile communication is consequently a prerequisite for the functioning of modern society, and mobile networks are rightly regarded as critical infrastructure.

Vulnerabilities and misconfigurations in mobile networks can compromise all three classic protection goals of information security: the *confidentiality* of calls and messages (e.g., eavesdropping), their *integrity* (e.g., manipulation of the signalled caller identity), and their *availability* (e.g., blocking of services, including emergency calls). Because a small number of operators serve almost the entire population, a single weakness in the configuration of one operator can affect millions of subscribers at once.

1.2 Technological Transition: From Circuit Switching to IP-based Services

Operating several network generations in parallel is costly, and the spectrum used by 2G and 3G is needed for the roll-out of 4G and 5G. Austrian mobile network operators (A1, Magenta, and Drei) have therefore started to shut down their legacy infrastructure, beginning with the 3G sunset in 2024. From a cybersecurity perspective, this transition is generally positive: the long-term support of legacy generations has repeatedly been exploited in the past, for instance by IMSI catchers or by downgrade attacks that jam 4G/5G frequencies to force devices into the weaker 2G security model.

With the paradigm shift to fully packet-switched networks, voice and messaging services are no longer provided by dedicated circuit-switched domains but by the IP Multimedia Subsystem (IMS), which is based on Internet protocols such as the Session Initiation Protocol (SIP):

- **Voice over LTE (VoLTE)**, and its 5G counterpart Voice over New Radio (VoNR), carries calls over the cellular radio access network.
- **Voice over Wi-Fi (VoWiFi)**, also known as Wi-Fi calling, builds on VoLTE and allows subscribers to reach the operator's IMS over any Internet connection, e.g., a regular Wi-Fi access point. Calls can thus be placed and received even without cellular coverage (e.g., in basements or shielded buildings).
- **Rich Communication Services (RCS)** is intended to replace SMS and MMS with a feature-rich messaging service. Depending on the operator, the RCS back-end is operated by the operator itself or by a third party such as Google. RCS is enabled by default on Android and has recently also been rolled out on Apple devices.

VoLTE, VoWiFi, and RCS are supported by Android and iOS as well as by all major Austrian operators and thus form the basis of modern mobile communication. In addition, over-the-top

(OTT) instant messengers such as WhatsApp, Signal, and iMessage now carry a large share of everyday messaging and are, for many users, the de facto successor of SMS.

1.3 Security Implications of the Technological Transition

Security mechanisms have been improved gradually with every network generation, and the decommissioning of legacy technologies has the potential to raise the overall level of mobile network security for all Austrian users. At the same time, the roll-out of new – and therefore less familiar – technologies carries the risk of misconfiguration. Such systems are often deployed under time pressure and tested primarily for functionality rather than security. Previous studies have shown that many of the security mechanisms specified for 4G are not enabled or not mandatory in practice, which in extreme cases results in newer systems being less secure than their predecessors. Production systems of Austrian operators have been affected by such issues in the past [21], underlining the need for continuous evaluation.

Several properties of modern mobile communication make an independent assessment particularly important:

- **Opacity for users.** Neither Android nor iOS offers a uniform way to inspect the security parameters (e.g., ciphers or key exchange methods) of a connection. Moreover, the device decides autonomously whether a call is carried via VoLTE or VoWiFi, or whether a message is delivered via SMS or RCS.
- **Connectivity over security.** Out of concern for locking out subscribers with outdated devices, operators may tolerate insecure configurations and fallback options, which in turn facilitate downgrade attacks.
- **Availability and emergency services.** Operators restrict access to VoWiFi, for instance by IP-based geoblocking, which can have adverse effects on the availability of emergency calls [20].
- **Data protection and sovereignty.** If services such as RCS are operated on foreign infrastructure, the current practice has to be evaluated from a data-protection and digital-sovereignty perspective.

Before TelCrit, no systematic and cross-provider assessment of these aspects existed for the Austrian market. The technologies and configurations deployed in practice were opaque to users and to the national regulatory authority alike.

1.4 Project Objectives and Research Questions

The overall objective of TelCrit was a comprehensive, cross-provider assessment of the cybersecurity of modern voice and messaging services in Austrian 4G/5G mobile networks. For each operator, the project aimed to determine the communication technologies in use (VoLTE, VoWiFi, RCS) and their security configuration (e.g., ciphers, key exchange, certificates, authentication, and geoblocking). Following the two access paths to the IMS in 4G/5G networks, the analysis was split into a *radio layer* (VoLTE) and an *Internet layer* (VoWiFi, RCS, and – as an extension during the project – OTT instant messengers). The work was guided by the following research questions:

RQ1
Which security mechanisms and configuration parameters are required or recommended for VoLTE, VoWiFi, and RCS by current standards and industry guidelines (3GPP, ETSI, GSMA, IETF), and which are deprecated? *(target state)*

RQ2
Which technologies, security mechanisms, and configurations are actually deployed by Austrian mobile network operators and on commonly used end devices, and where do they deviate from the target state? *(actual state)*

RQ3
Which risks for privacy, data protection, availability (including emergency calls), and digital sovereignty result from current deployments, e.g., through geoblocking or the use of foreign server infrastructure?

RQ4
Which security and privacy properties do the Internet-based messaging services that complement or replace SMS – RCS and OTT instant messengers – provide in practice, in particular with respect to metadata leakage?

1.5 Summary of Contributions

The main contributions of TelCrit are:

- **Target state** (Chapter 4): a consolidated baseline of required and deprecated security parameters for radio access, VoWiFi, IMS, RCS, and messengers.
- **Radio layer and IMS** (Chapter 5): multiple known VoLTE/VoWiFi vulnerabilities are still present in Austrian networks, including privacy leaks through unfiltered SIP headers (A1, Drei) and arbitrary caller-ID spoofing (Magenta).
- **VoWiFi** (Chapter 6): all Austrian operators accept deprecated key exchange parameters and weak or missing protection of SIP signalling, and none authenticates its ePDG by certificate.
- **RCS** (Chapter 7): all Austrian operators – like about 98 % of operators worldwide – rely on Google Jibe, raising concerns of digital sovereignty.
- **Messengers** (Chapter 8): new metadata attacks on WhatsApp, Signal, and iMessage, including the enumeration of all 3.5 billion WhatsApp accounts, which led to countermeasures by Meta.
- **Tools and dissemination** (Chapter 9): open-source measurement tooling, publications at RAID (Best Paper), WOOT, NDSS, CCS, and WiSec, and coordinated disclosure to all affected parties.

1.6 Structure of this Report

Chapter 2 introduces the technical background of IMS-based services, RCS, and end-to-end encrypted instant messengers. Chapter 3 describes the research design, the measurement methodology, and the scope of the study. Chapter 4 summarises the target state derived from standards

and guidelines. The results of the actual-state analysis are presented in Chapter 5 (radio layer and IMS signalling), Chapter 6 (VoWiFi), Chapter 7 (RCS), and Chapter 8 (instant messengers). Chapter 9 documents responsible disclosure, dissemination, and impact, and Chapter 10 concludes the report with recommendations and an outlook.

2 Technical Background

This chapter introduces the technologies examined in TelCrit. We first describe the IP Multimedia Subsystem (IMS) as the common service platform of 4G/5G voice and messaging and its two access paths, VoLTE and VoWiFi (Sections 2.1 and 2.2). We then summarise the security mechanisms of the radio access and the role of the SIM card (Section 2.3), followed by Rich Communication Services (Section 2.4) and end-to-end encrypted instant messengers (Section 2.5). Throughout the report, we use the terminology introduced with LTE; later generations partly introduced new names for equivalent components and services (e.g., VoLTE is called Voice over New Radio, VoNR, in 5G).

2.1 IP Multimedia Subsystem and VoLTE

In 2G and 3G networks, voice calls are handled in a dedicated circuit-switched (CS) domain that is strictly separated from packet-switched (PS) data services and reserves resources for each call. From 4G onwards, voice calls and other multimedia services are handled in the PS domain by the IMS [1]. Although security mechanisms have been strengthened with every generation, this architectural change also introduces new classes of vulnerabilities: telecom equipment in the CS domain was largely proprietary and reachable only through a few well-defined interfaces, whereas IMS services are built on Internet protocols, are frequently implemented as virtualised, software-defined network functions (partly based on open-source components), and – in the case of VoWiFi – are intentionally reachable from the public Internet.

Architecture. Figure 2.1 shows the simplified architecture of an LTE network with its two access paths to the IMS. In the case of *VoLTE* (3GPP access), the user equipment (UE) attaches to a base station (eNodeB) of the radio access network (RAN). The Serving Gateway (S-GW) and the Packet Data Network Gateway (P-GW) in the Evolved Packet Core (EPC) assign IP addresses per Access Point Name (APN) and route traffic to the respective packet data networks. For voice services, the UE connects to the dedicated `ims` APN, over which it reaches the IMS core.

Within the IMS, SIP signalling is handled by a set of Call Session Control Functions (CSCFs): the *Proxy-CSCF* (P-CSCF) is the first point of contact for the UE, the *Interrogating-CSCF* (I-CSCF) is the entry point for requests from other networks, and the *Serving-CSCF* (S-CSCF) is the central registrar and session controller in the home network. In practice, these roles are often implemented by Session Border Controllers (SBCs). Application servers provide supplementary services (e.g., voicemail or conference calls), media resource functions process media streams, and media gateways interconnect the IMS with the public switched telephone network and legacy CS domains [1].

Session Initiation Protocol. The Session Initiation Protocol (SIP) [40] is a text-based, HTTP-like request/response protocol for establishing and controlling multimedia sessions. Core methods include `REGISTER`, `INVITE`, `ACK`, `BYE`, `CANCEL`, and `OPTIONS`; responses use three-digit status codes. Requests are routed via proxy servers, which may add, modify, or remove header fields. SIP messages carry a considerable amount of metadata in these header fields, e.g., the identity of the caller as asserted by the network, information about the device and its software, the access network in use, or routing information of the core network. For the security and privacy of a deployment, it is therefore crucial which headers the network accepts from a UE,

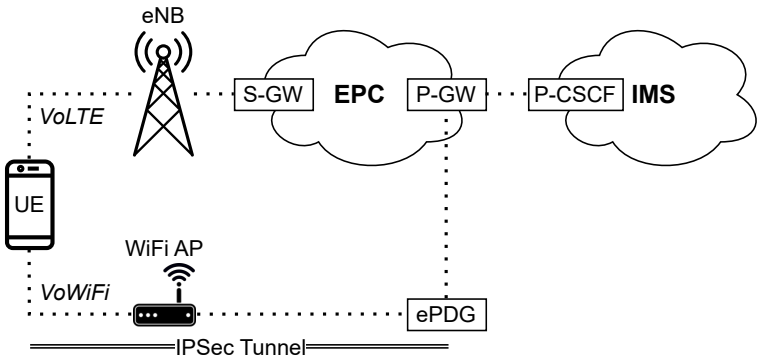


Figure 2.1: Simplified LTE architecture for VoLTE (3GPP access via the radio access network, top) and VoWiFi (untrusted non-3GPP access via Wi-Fi and the ePDG, bottom). Both paths terminate in the same IMS core [20].

which headers it sanitises, and which information it forwards to the other party of a call. While SIP is used for signalling, the actual audio stream is transported via the Real-time Transport Protocol (RTP).

IMS registration and security. Before it can place or receive calls, the UE registers with the IMS. The first `REGISTER` request is answered with a `401 Unauthorized` response that contains an authentication challenge (IMS AKA), which the UE solves using the credentials stored on its SIM card. At the same time, the UE and the P-CSCF negotiate the protection of all subsequent SIP traffic using the security mechanism agreement for SIP (`ipsec-3gpp`) [10], which establishes IPsec security associations in transport mode between the UE and the P-CSCF. Whether this layer actually provides confidentiality and integrity protection depends on the negotiated algorithms, and encryption on this layer is optional in many deployments [21].

Since operators usually run a single IMS for all access technologies and network generations, the application-layer behaviour of a deployment is largely independent of whether the IMS is accessed via VoLTE or VoWiFi. This property is exploited in Chapter 5, where VoWiFi serves as a more accessible entry point for analysing the IMS configuration that is also used for VoLTE.

2.2 Voice over Wi-Fi

VoWiFi transports IMS traffic over *untrusted non-3GPP access* networks, typically arbitrary Wi-Fi networks connected to the Internet. The UE establishes an IPsec tunnel to the operator's Evolved Packet Data Gateway (ePDG), which is reachable from the public Internet, and from there traffic is forwarded to the P-GW and the IMS (Figure 2.1, bottom). The security of VoWiFi is thus built on IPsec and the Internet Key Exchange protocol version 2 (IKEv2) [29], in a variant profiled by 3GPP [14].

ePDG discovery. The UE locates the ePDG of its home operator through a fully qualified domain name that is standardised in 3GPP TS 23.003 [12]:

`epdg.epc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org`

where the mobile country code (MCC) and mobile network code (MNC) uniquely identify each operator. Consequently, the ePDGs of all operators worldwide can be enumerated by resolving these names, which enables Internet-scale measurements without the need for SIM cards [20, 21].

Nested protection layers. A VoWiFi connection consists of a stack of nested tunnels, which we refer to as layers L1 to L3 (Figure 2.2) [21]:

L1 – IKEv2 (phase 1).
In the `IKE_SA_INIT` exchange, the UE proposes its supported security associations (SAs), i.e., encryption and integrity algorithms, pseudo-random functions, and Diffie-Hellman (DH) groups, together with a key share for its preferred DH group. The ePDG selects one proposal or requests a different DH group. After this exchange, all subsequent IKE messages are encrypted and integrity-protected with keys derived from the DH shared secret.

L2 – IPsec tunnel (phase 2).
Protected by L1, the UE and the ePDG authenticate each other in the `IKE_AUTH` exchange using EAP-AKA [7] with the credentials of the (U)SIM, optionally complemented by an ePDG certificate. IKEv2 implicitly creates the first `CHILD_SA`, an IPsec tunnel into the EPC through which the UE obtains an IP address in the `ims` APN – functionally equivalent to VoLTE access.

L3 – SIP/`ipsec-3gpp`.
Inside this tunnel, the UE registers with the P-CSCF and protects SIP (and optionally RTP) traffic with IPsec in transport mode, as described in Section 2.1.

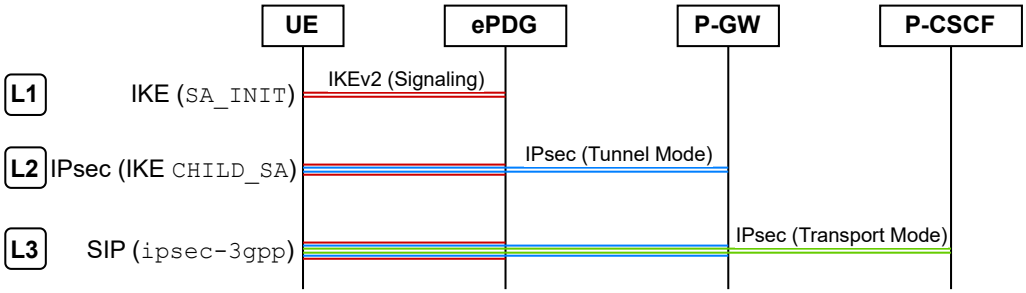


Figure 2.2: Nested protection layers of a VoWiFi connection: IKEv2 signalling (L1), the IPsec tunnel between UE and ePDG (L2), and SIP protected by `ipsec-3gpp` between UE and P-CSCF (L3) [21, 47].

Two properties of this construction are particularly relevant for security. First, the keys of the parent and child SAs are periodically renewed through new DH exchanges, whereas the endpoints are not re-authenticated. An attacker who is able to break the L1 key exchange therefore gains the ability to read and rewrite traffic on the first two layers [21]. Second, since encryption on L3 is often optional, the same attacker may subsequently also take over the SIP layer, effectively controlling all three layers.

Diffie-Hellman groups. The strength of the L1 key exchange depends on the negotiated DH group (Table 2.1). Already in 2015, breaking the 768-bit MODP group (DH1) was estimated to be within reach of academic teams and the 1024-bit group (DH2) within reach of nation-state adversaries [5]. The IETF accordingly deprecated weak groups for IKEv2 [37], and 3GPP gradually adapted the IKE profile in TS 33.210 [13]: DH2 was recommended until 2011, subsequently demoted, and finally prohibited ('shall not use') in 2016, while elliptic-curve groups were added as recommended options. For performance reasons, servers may precompute their

public DH values from a temporarily fixed private key. This is acceptable only if the key is rotated frequently and never shared between different DH groups; otherwise, an attacker can break the key on a weak group and reuse it for stronger ones [15].

Group	Size	Type	Status	Group	Size	Type
DH1	768 bit	MODP	never specified by 3GPP	DH19	256 bit	ECP
DH2	1024 bit	MODP	deprecated	DH20	384 bit	ECP
DH5	1536 bit	MODP	never specified by 3GPP	DH21	521 bit	ECP
DH14	2048 bit	MODP		DH25	192 bit	ECP
DH15	3072 bit	MODP		DH26	224 bit	ECP
DH16	4096 bit	MODP		DH31	Curve25519	

Table 2.1: Diffie-Hellman groups relevant for VoWiFi (IANA numbering) and their status in the 3GPP IKE profile [13, 21].

Client provisioning. Unlike many other cellular parameters, which are announced by the network or stored on the SIM card, the VoLTE/VoWiFi ecosystem lacks a comprehensive auto-configuration mechanism. Operating system and modem vendors therefore ship databases of operator-specific configurations with their firmware, which define everything from tunnel and IKE settings to IMS and codec parameters [21]. Apple distributes them as carrier bundles (`.ipcc` files); Qualcomm-based devices load binary modem configuration files (`.mbn`) from the modem image; Samsung stores the VoWiFi settings in an XML file in the system partition; and Google Pixel devices with Tensor chipsets rely on Android's generic carrier configuration, frequently falling back to default values. These files determine which algorithms a device proposes and accepts and are therefore a valuable source for the static client analysis (Section 3.2).

2.3 Radio Access Security and the SIM Card

On the radio path, LTE protects signalling and user traffic between the UE and the network with algorithms negotiated during the attach procedure [4]. The UE announces the ciphering (EEA) and integrity (EIA) algorithms it supports, and the network selects one of them according to an operator-configured priority list. Available algorithms are the null algorithms EEA0/EIA0 (no protection), SNOW 3G-based EEA1/EIA1, AES-based EEA2/EIA2, and ZUC-based EEA3/EIA3. The null algorithms provide no protection: while EIA0 is restricted to unauthenticated emergency calls, EEA0 remains a permitted choice of the network, and its use disables the confidentiality of the radio link. Which algorithm an operator selects in practice cannot be observed from a regular smartphone, but can be measured with a software-defined radio setup in which the advertised capabilities of the UE are fully controllable (Chapter 5).

The (U)SIM card stores the subscriber's long-term secret and performs the authentication and key agreement (AKA) computations for network access, IMS registration, and EAP-AKA in VoWiFi. It communicates with the modem via application protocol data units (APDUs). Inspecting, modifying, and relaying this communication (*SIM tracing* and *SIM tunnelling*) is an established research technique used to observe hidden SIM activity, extract session keys, fuzz interfaces, or reuse a single SIM card at remote measurement locations [22].

2.4 Rich Communication Services

Rich Communication Services (RCS) originated as the mobile industry's response to the success of over-the-top (OTT) instant messengers. After initial fragmented deployments (e.g., RCS-e, marketed as 'joyn' in several European countries from 2012), the GSMA, operators, and Google – which had acquired the RCS platform provider Jibe Mobile in 2015 – agreed in 2016 on a common *Universal Profile*. Google subsequently rolled out RCS in its Messages app worldwide, also for subscribers of operators without their own RCS deployment. Apple added RCS support in iOS 18, and end-to-end encryption based on the Messaging Layer Security (MLS) protocol was standardised in Universal Profile 3.0 in 2025 [16].

Auto-configuration. Unlike VoLTE and VoWiFi, RCS has a standardised HTTP-based auto-configuration mechanism [26, 27]. A client discovers the auto-configuration server (ACS) of its operator via the domain `config.rcs.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org` (or an operator-specific suffix) and requests its configuration document via HTTPS, providing information about the client, its supported profile and services, and the subscriber. The ACS authenticates the subscriber using one of several methods – one-time passwords delivered by (possibly invisible) SMS, the Generic Bootstrapping Architecture (GBA), OpenID Connect, or, in earlier specification versions, the identity of an existing cellular connection – and returns an XML document that contains, among others, the addresses and credentials required for the subsequent IMS registration. As for VoWiFi, the standardised domain names make it possible to measure the deployment landscape at Internet scale (Chapter 7).

Access and deployment models. RCS is an IMS service and uses SIP for signalling. In a *native* deployment, the RCS client registers with the operator's own IMS, either via the radio access network or via the ePDG, often sharing a single registration with voice services. Alternatively, operators can outsource RCS to a hosted platform, most prominently *Google Jibe*. In this case, the client maintains a separate registration and connects directly over the Internet to Jibe's P-CSCF, bypassing the operator's internal infrastructure entirely (Figure 2.3). From a user's perspective, both variants are indistinguishable; from a data-protection and sovereignty perspective, however, they differ fundamentally, since in the latter case signalling and message metadata are processed by a third party.

Capability discovery. Before communicating with a contact, RCS clients determine whether the contact uses RCS and which services (e.g., chat, file transfer, or video calls) both clients support. This *capability discovery* is realised either by exchanging SIP `OPTIONS` requests, in which both clients announce their supported feature tags, or via a presence server from which the capabilities published by other clients can be fetched [26]. In both cases, a querying party learns information about the target's client, which can be sufficient to fingerprint the client implementation behind an arbitrary phone number [16].

2.5 End-to-End Encrypted Instant Messengers

OTT messengers such as WhatsApp (with about 3.5 billion accounts), Signal, and iMessage have largely replaced SMS for everyday communication. All three provide end-to-end encryption (E2EE), which ensures that the service operator cannot read message contents. As a consequence, much of the protocol logic – including validation of messages and recovery from

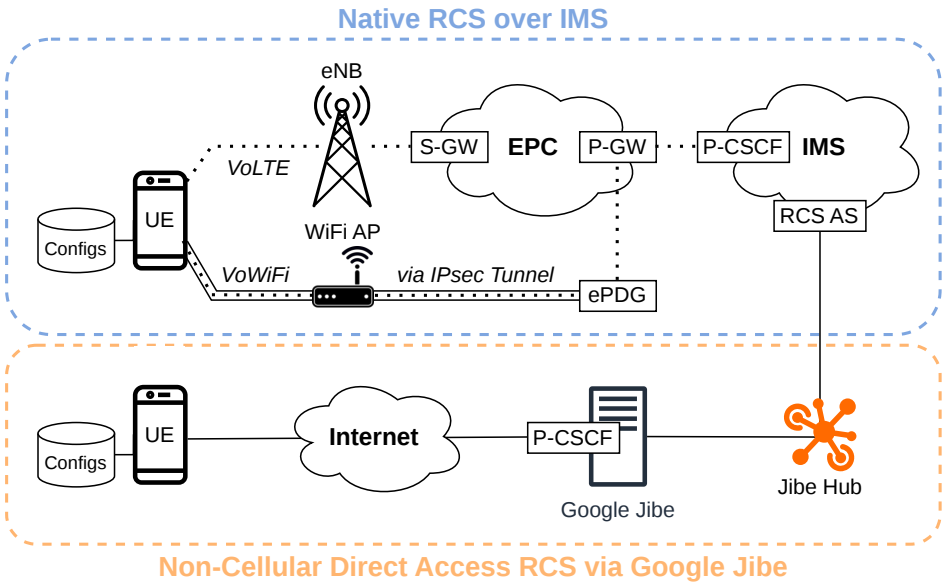


Figure 2.3: Native RCS via the operator's IMS (top) compared to direct non-cellular access to RCS hosted on Google Jibe (bottom) [16].

decryption failures – is shifted from the server to the clients, and the server is reduced to a forwarder of encrypted messages [24].

The Signal protocol and prekeys. Signal and WhatsApp use the Signal protocol [34, 38, 45]. To enable a sender (Alice) to establish an encrypted session with a recipient (Bob) who is currently offline, each device deposits a *prekey bundle* on the server. It consists of a long-term identity key, a medium-term *signed prekey* that is rotated periodically, and a stash of *one-time prekeys*, each of which is handed out at most once. Alice fetches Bob's bundle and derives the initial shared secret from several DH computations (X3DH [34]; Signal has since moved to the post-quantum variant PQXDH [31]). Subsequent messages are protected by the double ratchet [38], which continuously derives fresh keys. The one-time prekey is essential for forward secrecy of the first messages of a session: if it is missing, the initial messages are protected only by Bob's long-term and signed prekeys, and an attacker who later compromises these keys can decrypt recorded messages until the signed prekey is rotated [23]. Operating this mechanism requires the server to hand out and each client to replenish one-time prekeys – a procedure that itself has privacy and availability implications (Chapter 8).

Multi-device support. WhatsApp, Signal, and iMessage allow users to operate several devices (e.g., a smartphone and desktop or tablet companions) under one account. They follow a *client-fanout* approach: each device holds its own key pair, and the sender encrypts every message individually for each device of the recipient as well as for its own other devices (Figure 2.4) [6, 35]. A necessary consequence is that the number of devices associated with an account – and, as shown in Chapter 8, further properties of these devices – is exposed to any party that can request the keys of that account.

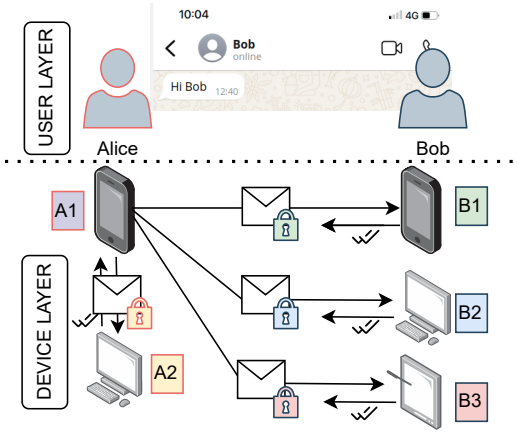


Figure 2.4: Client-fanout in multi-device messaging: Alice's message is individually encrypted for each of Bob's devices and for her own companion device; each receiving device returns a delivery receipt [24].

Delivery receipts. Messengers acknowledge the progress of a message: a *server acknowledgement* (single check mark) indicates that the server has queued the message, a *delivery receipt* (two check marks) indicates that the recipient device has received and successfully decrypted it, and an optional *read receipt* indicates that the user has opened it. While read receipts can be disabled, delivery receipts cannot, since they are required by the protocol, e.g., to allow the sender to delete ephemeral key material and to trigger re-encryption after decryption failures. The round-trip time between sending a message and receiving the delivery receipt reflects the state and network connection of the recipient device and has been shown to leak coarse location information [42].

Contact discovery. Messengers that use phone numbers as identifiers allow users to discover which of their contacts are registered by uploading (hashes of) the phone numbers in their address book to the server. Since the service must answer such queries for legitimate users, the mechanism inherently allows checking arbitrary phone numbers for registration; rate limiting is the primary defence against large-scale enumeration [25].

iMessage. Apple's iMessage follows the same client-fanout principle but differs in its architecture. To send a message, a device queries Apple's Identity Services (IDS) for the push tokens and public keys of all devices registered to the recipient's handle (phone number or e-mail address), encrypts the message per device, and delivers it via the Apple Push Notification service (APNs), which stores it for offline devices; large payloads and attachments are uploaded in encrypted form to iCloud [6]. On the device, iMessage is not a single sandboxed application but is implemented by several system daemons, which process incoming messages – including a dedicated sandboxed parsing service (BlastDoor) – before they are shown to the user [17].

3 Research Design and Methodology

This chapter describes how TelCrit approached the research questions stated in Section 1.4. It outlines the overall research design (Section 3.1), the three complementary measurement perspectives used for the actual-state analysis (Section 3.2), the scope of the study (Section 3.3), and the ethical framework (Section 3.4).

3.1 Overall Research Design

The research design follows a *target/actual comparison*:

1. **Target state (*Soll*).** Based on current specifications (3GPP, ETSI, IETF) and industry guidelines (GSMA), we determined which configuration parameters and security mechanisms an operator should support and enable according to the standards and best practice, and which settings are deprecated and should no longer be used in production systems (Chapter 4).
2. **Actual state (*Ist*).** Previous studies have shown that there is often a considerable mismatch between recommended standards and the configurations actually deployed. We therefore empirically measured the technologies and configurations used in Austrian production networks and on commercially available end devices. Following the two access paths to the IMS in 4G/5G networks, the actual-state analysis was conducted separately for
   (i) the *radio layer* (VoLTE, Chapter 5), and
   (ii) the *Internet layer* (VoWiFi, RCS, and instant messengers, Chapters 6 to 8).
3. **Assessment.** Deviations between target and actual state were assessed with respect to confidentiality, integrity, availability, privacy, and digital sovereignty. Relevant findings were reported to the affected parties through coordinated (responsible) disclosure (Chapter 9).

In addition to searching for new weaknesses, the project translated vulnerabilities that were already known from the scientific literature into reproducible, partially automated test procedures and evaluated them against Austrian networks and current end devices. This made it possible to determine whether previously documented issues persist in deployed systems – a question that a purely standards-based assessment cannot answer.

3.2 Measurement Perspectives

The security parameters actually negotiated by a smartphone are normally not visible to its user, and neither the operators' core networks nor the devices' baseband implementations are open to inspection. TelCrit therefore combined three complementary perspectives to obtain a realistic and robust picture of the security configuration in use.

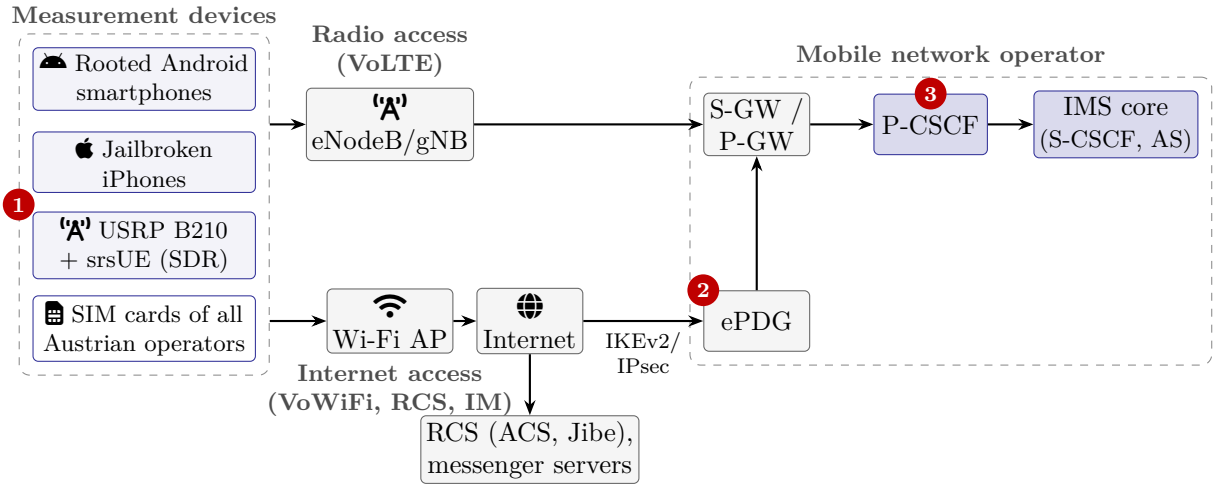
3.2.1 In-vivo Measurements

To obtain unbiased results, we used commercially available hardware – mobile modems and smartphones – to observe the security configurations negotiated in the production networks

of Austrian operators ('in vivo'). Since the protocols and parameters in use are hidden from regular users, we relied on a set of rooted Android smartphones and jailbroken iPhones that allow the relevant information to be retrieved during live operation, e.g., from IMS signalling, IPsec security associations, and diagnostic interfaces.

For more flexibility when testing the configurations supported on the radio layer, commercial devices were complemented by a software-defined radio setup (USRP B210 with the open-source srsRAN user equipment *srsUE*). This setup allows individual parameters, such as the advertised security capabilities, to be modified freely, which is not possible with commercial basebands. In addition, a low-cost SIM tracing and tunnelling setup [22] was developed to observe and relay the communication between the SIM card and the modem (Chapter 5).

Figure 3.1 summarises the in-vivo setup. The same set of devices and SIM cards of all Austrian operators (A1, Magenta, Drei, and spusu) was used for both access paths, which allows the configuration observed via the radio access network to be compared directly with that observed via the Internet.



1 Radio parameters (announced security capabilities, selected EEA/EIA algorithms) from modem diagnostics and SDR logs

2 IKEv2 proposals, selected algorithms, and IPsec keys of the tunnel between UE and ePDG (L1/L2)

3 IMS registration and SIP signalling incl. `ipsec-3gpp` parameters (L3), shared by VoLTE and VoWiFi

Figure 3.1: In-vivo measurement setup. Commercial devices with privileged access and an SDR-based UE connect to the production networks of Austrian operators via the radio access network (VoLTE) and via the Internet (VoWiFi, RCS, instant messengers). Security parameters are recorded at the marked observation points.

3.2.2 Static Client Analysis

Because IMS services lack a universal auto-configuration mechanism, operators ship their preferred connection settings to their customers' devices in the form of carrier configuration files that are bundled with the operating system or the baseband firmware. These files determine, among other things, which algorithms a device proposes or accepts when establishing a connection. In previous work, we presented a method to extract these client-side parameters for different smartphone vendors (e.g., Apple, Samsung, Xiaomi) [21]. Within TelCrit, this static

analysis was applied to the configurations of Austrian operators and extended to IMS-specific settings.

3.2.3 Extended Server-side Analysis

For the server-side perspective on VoWiFi and RCS, we used dedicated measurement clients that emulate regular smartphones and thereby establish their own connections to the Internet-facing servers of the respective services. Such scripts allow the parameters supported by a server to be tested automatically and exhaustively, including worst-case scenarios in which insecure settings are tolerated as a fallback and thus facilitate downgrade attacks. The relevant servers are located either by querying the corresponding files from the SIM card (e.g., using a PC/SC reader) or by resolving standardised domain names derived from the operator's mobile country code (MCC) and mobile network code (MNC).

VoWiFi (and similarly VoLTE) connections are protected by several nested layers (Section 2.2): the IKEv2 key exchange with the operator's Evolved Packet Data Gateway (ePDG) (*L1*), the IPsec tunnel between the device and the ePDG (*L2*), and the `ipsec-3gpp` protection of SIP signalling towards the Proxy Call Session Control Function (P-CSCF) (*L3*). Our previous studies aimed at global coverage of all operators worldwide and therefore had to be designed to work without SIM cards; they were consequently limited to the outermost layer L1. For the Austrian market, SIM cards of all relevant operators were acquired, which enabled the analysis of the deeper layers L2 and L3, i.e., IMS registration, SIP signalling, and call handling.

For RCS, no noteworthy open-source client implementation existed at the start of the project, and the proprietary clients on smartphones are only of limited use for systematic tests. A dedicated RCS measurement client was therefore implemented within the project (Chapter 7). Similarly, to analyse proprietary instant messengers (WhatsApp, Signal, iMessage), the relevant protocols were reverse-engineered and research clients or dedicated measurement tools were developed (Chapter 8).

3.3 Scope

Operators. The evaluation covered all three Austrian mobile network operators with their own radio access network – A1 Telekom Austria (A1), T-Mobile Austria (Magenta), and Hutchison Drei Austria (Drei). Mobile virtual network operators (MVNOs) usually rely on the infrastructure of one of these operators; exceptions such as *spusu*, which uses the radio network of Drei but operates its own IMS core, were included where relevant. Beyond the Austrian market, several measurements (VoWiFi geoblocking, VoWiFi key exchange, and RCS deployments) were conducted at a global scale in order to put the Austrian results into an international context.

Services. The assessment focused on the voice and messaging services of the post-3G era: VoLTE, VoWiFi, and RCS. Since RCS is positioned as the mobile industry's answer to OTT messengers, and since these messengers share the same end devices and much of the same threat model, the scope was extended during the project to the most widely used instant messaging services (WhatsApp, Signal, and iMessage).

Parameters. Beyond the technologies in use, the assessment covered

- cryptographic parameters (ciphers, integrity algorithms, key exchange methods, Diffie-Hellman groups) including tolerated fallback options,

- authentication methods (e.g., EAP-AKA, certificates),
- deviations from specifications and the use of deprecated settings,
- previously reported vulnerabilities (e.g., manufacturer default keys),
- privacy aspects such as information leaked in signalling messages,
- availability aspects such as geoblocking and its effects on emergency calls, and
- the location and ownership of the server infrastructure (e.g., for RCS), which is relevant for data protection and digital sovereignty.

3.4 Ethical Considerations and Responsible Disclosure

Identified vulnerabilities and misconfigurations were communicated promptly to the affected operators and vendors in a coordinated (responsible) disclosure process and – for Austrian operators – to the RTR, which acted as the project's end user (*Bedarfsträger*). All findings concerning instant messengers were likewise disclosed to the respective vendors – Meta (WhatsApp), the Signal Foundation, and Apple (iMessage) – in comprehensive disclosure processes before publication (Chapter 9).

Experiments targeting individual users were conducted exclusively on accounts and devices of the research team or of participants who gave explicit written consent. For measurements at scale, such as the enumeration of WhatsApp accounts, the research team was identifiable via its university IP addresses and abuse contacts, the collected data was analysed only in aggregated form, and raw data was neither published nor retained beyond the analysis.

4 Target State: Standards and Best Practices

The first step of the research design (Section 3.1) was to establish, for each examined technology, which security mechanisms and configuration parameters the relevant standards and industry guidelines require or recommend, and which settings are deprecated and should no longer be used in production. This target state serves as the reference against which the measurements in Chapters 5 to 8 are assessed.

4.1 Sources and Classification

The analysis covered the 3GPP specifications (published by ETSI) for the security of the radio access, of non-3GPP access, and of IMS access; the IETF RFCs that define the underlying Internet protocols and their algorithm requirements; the GSMA specifications for RCS; and, for OTT messengers, which are not subject to formal standardisation, the published protocol specifications and security white papers of the vendors. Table 4.1 lists the most relevant documents.

Document	**Subject**
3GPP TS 33.401 [4]	Security architecture of LTE, incl. radio link algorithms
3GPP TS 33.402 [14]	Security of non-3GPP access (ePDG, IKEv2, EAP-AKA)
3GPP TS 33.210 [13]	Network domain security; IKE/IPsec profile
3GPP TS 33.203 [3]	Access security for IMS (IMS AKA, `ipsec-3gpp`)
3GPP TS 24.229 [2]	IMS call control based on SIP (header handling, identities)
3GPP TS 23.003 [12]	Numbering and addressing (ePDG, emergency ePDG, and ACS domain names)
RFC 7296, 8247 [29, 37]	IKEv2 and its algorithm requirements
RFC 8221 [48]	Algorithm requirements for ESP
RFC 3261, 3323, 3325 [28, 39, 40]	SIP, privacy mechanism, asserted identity
GSMA RCC.07, RCC.14 [26, 27]	RCS client specification and device configuration
Signal specifications, vendor white papers [6, 34, 45]	End-to-end encrypted messaging

Table 4.1: Main documents considered in the target-state analysis.

Since requirements change between releases, a reference release had to be chosen. We used 3GPP Release 16, the first release with a complete 5G specification, which has been functionally frozen since 2020 and can reasonably be expected to be implemented in current production networks. For IETF documents, the latest version was used. Following the normative language of the documents, algorithms and options marked as prohibited ('shall not', 'MUST NOT') or discouraged ('should not', 'SHOULD NOT') were classified as *insecure*; all remaining options were considered acceptable [47]. The analysis was complicated by the sheer size of the specification corpus, its dense web of cross-references, and requirements that are at times formulated inconsistently or imprecisely across documents.

4.2 Radio Access

For LTE, the UE announces its supported ciphering (EEA) and integrity (EIA) algorithms, and the network selects one of each according to an operator-configured priority list [4]. The UE's capabilities are echoed back in the integrity-protected security mode command, which protects the negotiation against bidding-down by an external attacker. The null integrity algorithm EIA0 may only be used for unauthenticated emergency calls. The null ciphering algorithm EEA0, in contrast, remains a permitted choice of the network, so that the confidentiality of the radio link depends on the operator's configuration (Section 5.1).

4.3 VoWiFi and IMS Access Security

For VoWiFi, the target state has to be defined separately for each of the three protection layers (Section 2.2). Table 4.2 summarises the insecure algorithms per layer.

L1 – IKEv2 key exchange. The IKE profile of 3GPP (TS 33.210) has evolved considerably (Figure 4.1). The 1024-bit MODP group DH2 was mandatory until 2011, then demoted to 'mandatory, but not recommended', and finally prohibited in 2016: 'For security reasons, the use of Diffie-Hellman MODP groups less than 2048-bit shall not be supported.' At the same time, elliptic-curve groups (DH19, later DH20 and Curve25519) were added. The groups DH1 and DH5 were never part of the 3GPP profile. The IETF likewise deprecated weak groups for IKEv2 in general [37]. In addition, servers should not reuse private DH values across groups or over extended periods, since this facilitates attacks on the stronger groups [15].

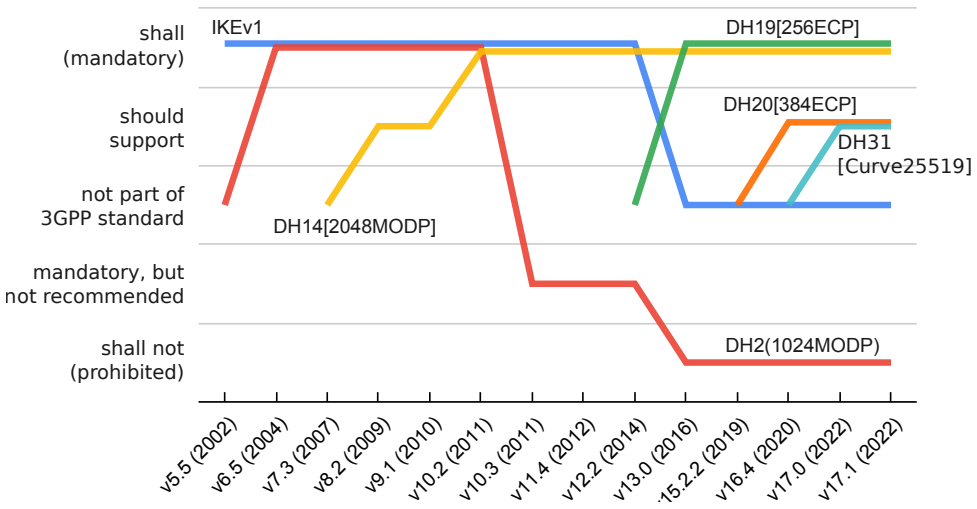


Figure 4.1: Development of the DH groups in the 3GPP IKE profile (TS 33.210, `IKE_SA_INIT`) across specification versions. LTE started with version 8; IKEv1 has been phased out since version 12 [21].

L2 – ESP tunnel. For the ESP algorithms, TS 33.210 refers to RFC 8221: only the algorithms listed there shall be used. Consequently, DES and 3DES encryption as well as HMAC-MD5-96 integrity protection are considered insecure. The null encryption algorithm is listed for compatibility reasons, but provides no confidentiality and was therefore considered insecure

for tunnels over untrusted networks. HMAC-SHA1-96 is still permitted but downgraded in RFC 8221 and scheduled for removal.

L3 – IMS access security. TS 33.203 defines the algorithms for `ipsec-3gpp` directly. `des-ede3-cbc` and `hmac-md5-96` have been removed, and null integrity protection is only acceptable in combination with AES-GCM. For access over untrusted networks, the protection of SIP signalling by `ipsec-3gpp` is mandatory, i.e., an IMS registration without a `Security-Client` negotiation must not be accepted; null encryption is formally permitted, but leaves SIP signalling protected only by the outer tunnel. If the P-CSCF cannot accept a proposal, it shall respond with an error.

Layer	Reference	Considered insecure
Radio link	TS 33.401	EEA0 (permitted, but no confidentiality); EIA0 outside unauthenticated emergency calls
L1 (IKEv2)	TS 33.210	DH1 (768 bit), DH2 (1024 bit), DH5 (1536 bit); static or reused DH private keys
L2 (ESP)	TS 33.210, RFC 8221	DES, 3DES, NULL encryption; HMAC-MD5-96 (HMAC-SHA1-96 scheduled for removal)
L3 (`ipsec-3gpp`)	TS 33.203	`des-ede3-cbc`, `hmac-md5-96`; null integrity (except AES-GCM); missing L3 protection; null encryption (context-dependent)

Table 4.2: Target state: algorithms and options classified as insecure per layer, based on 3GPP Release 16 and current IETF requirements [21, 47].

Authentication and identity privacy. In IKEv2 for VoWiFi, the UE is authenticated by EAP-AKA using the credentials of the SIM card [7, 14]. The specifications provide for the ePDG to authenticate itself by means of a certificate, but whether devices request and verify such certificates is left to per-operator configuration. Since the UE sends its identity before the ePDG is authenticated, EAP-AKA provides temporary identities (pseudonyms) to avoid disclosing the IMSI; these, however, do not prevent an active attacker from requesting the permanent identity. The target state therefore comprises ePDG certificates that are enforced by the devices, complemented by the use of pseudonyms.

Availability and emergency calls. VoWiFi is intended to be usable independently of the radio network, and devices should use it for emergency calls when no cellular emergency service is available. Operators can designate a dedicated emergency ePDG via the domain [12]

`sos.epdg.epc.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org`.

Access restrictions based solely on the source IP address are not foreseen by the standards and would also affect emergency calls [20].

4.4 IMS Signalling: Identities and Privacy

Caller identity. In the IMS, the network – not the device – is responsible for the caller identity. A UE may indicate a preferred identity, but the P-CSCF shall only accept identities that belong to the registered subscription and asserts the identity towards the rest of the network

by means of the `P-Asserted-Identity` header [2, 28]. Identity information supplied by the UE in other headers must not be trusted. At the national level, anti-spoofing provisions introduced by the RTR are additionally intended to prevent the unauthorised use of Austrian numbers in voice calls.

Privacy and topology hiding. Asserted identities and network-internal information may only be passed on within a trust domain [28]. When a request leaves the trust domain, or when the caller requests privacy (e.g., caller-ID suppression), the network shall remove the corresponding identity information [2, 39]. Location-related headers such as `P-Access-Network-Info` are intended for the operator and are to be removed before a request leaves the trust domain, and operators can hide their internal topology at the network border. Headers that are not required by the remote party – e.g., the `User-Agent` of the other party or proprietary headers – should not be forwarded, both for privacy reasons and to reduce the attack surface of SIP parsers in remote devices.

4.5 Rich Communication Services

For RCS, the GSMA specifies an HTTPS-based auto-configuration: the client retrieves its configuration from the operator's auto-configuration server, which must authenticate the subscriber before returning credentials, e.g., by a one-time password delivered by SMS, by the Generic Bootstrapping Architecture (GBA), or via OpenID Connect [26, 27]. The verification of the client's authenticity and of the integrity of the client platform is optional and left to implementers, and GBA-based authentication is marked as a candidate for future deprecation. Capability discovery is part of the standard and inherently reveals which services a contact's client supports. Standardised end-to-end encryption, based on the Messaging Layer Security protocol, was only introduced with Universal Profile 3.0 in 2025 [16]. The standards do not restrict *who* operates an RCS service; aspects of data protection and digital sovereignty therefore have to be assessed separately.

4.6 End-to-End Encrypted Instant Messengers

For OTT messengers, the target state is defined by the security goals stated in the protocol specifications and vendor documentation. The Signal protocol aims at confidentiality with forward secrecy from the first message onwards, which requires that a one-time prekey is available for every new session [34]; signed prekeys are to be rotated periodically, with suggested intervals between a week and a month [23]. WhatsApp and Apple describe comparable guarantees in their security documentation [6, 45]. None of these documents, however, specifies requirements regarding metadata such as delivery receipts, device information, or the rate at which contact discovery may be queried. Protection against the metadata leakage investigated in Chapter 8 is thus not part of any formal target state, which is a finding in itself.

4.7 Observations

The target-state analysis leads to three general observations that are relevant for the interpretation of the measurement results:

- **Deprecation without enforcement.** Weak algorithms have been prohibited for up to a decade (e.g., DH2 since 2016), but the standards do not define timelines or procedures for phasing them out in deployed networks and devices.
- **Optional security mechanisms.** Several important protections – ePDG certificates, encryption on L3, radio link ciphering, client authenticity in RCS – are optional or configuration-dependent. The security level of a deployment is therefore determined by operator and vendor choices rather than by the standard itself.
- **Blind spots.** Metadata protection in messengers and the question of who operates a communication service (e.g., hosted RCS platforms) are not addressed by the standards at all.

5 Radio Layer and IMS Signalling

This chapter presents the actual-state analysis of the radio access path (VoLTE) and of the IMS signalling that VoLTE shares with VoWiFi. We first describe measurements of the radio link security configuration of the Austrian operators (Section 5.1). We then present our approach for the automated security testing of the IMS (Section 5.2) and discuss its two most relevant results in detail: privacy leakage due to missing SIP header filtering (Section 5.3) and caller-ID spoofing (Section 5.4). Further findings are summarised in Section 5.5.

5.1 Radio Link Security Configuration

Commercial basebands do not allow the security capabilities that a device announces to the network to be changed. To determine which ciphering algorithms the Austrian operators accept and prefer on the radio link, we therefore used a software-defined radio (USRP B210) running the open-source LTE user equipment srsUE [41]. The UE was first configured to support all EPS encryption algorithms (EEA0–EEA3). After a successful attach, the algorithm selected by the network was removed from the UE's capabilities, and the procedure was repeated until no connection could be established any more. This yields the order of preference configured by each operator (Table 5.1).

Operator	ZUC (EEA3)	SNOW 3G (EEA1)	AES (EEA2)	NULL (EEA0)
A1	1	2	3	4
Magenta	3	2	1	4
Drei	1	3	2	4

Table 5.1: Order in which the Austrian operators selected the EPS encryption algorithms offered by an SDR-based UE (1 = first choice). All operators select the null algorithm only as a last resort, but still accept it if no other algorithm is offered [41].

All three operators prefer one of the three cryptographic algorithms and select the null algorithm EEA0 only as a last resort. Interestingly, the preferences among the cryptographic algorithms differ between operators, with two of three operators preferring the Chinese ZUC-based algorithm over AES. All operators, however, still established a connection without encryption when EEA0 was the only algorithm offered by the UE. Since the UE's security capabilities are integrity-protected and echoed back by the network during the security mode procedure [4], this does not directly enable a downgrade by an external attacker; it does, however, show that the networks tolerate unencrypted radio links for regular subscribers, e.g., for misconfigured or manipulated devices. A second SDR platform (LimeSDR) could not establish a stable connection to any of the operators, presumably due to insufficient clock accuracy.

As a by-product of the measurement infrastructure, the project also improved the tooling for SIM-based measurements: *SIMulator* ports the SIM tracing and tunnelling capabilities of our MobileAtlas platform [19] to a 4 USD microcontroller (Raspberry Pi Pico) and was presented at ACM WiSec 2025 [22]. It allows the communication between SIM card and modem to be inspected, modified, and relayed with minimal hardware effort.

5.2 Automated Security Testing of the IMS

The main part of the radio-layer work addressed the IMS signalling that VoLTE shares with VoWiFi. It was carried out largely within the master's thesis of R. Wittek [47], which was supervised within the project.

5.2.1 Approach

A considerable body of research on VoLTE and VoWiFi security has been published over the past decade [8, 11, 30, 32, 36, 43, 44]. However, most studies evaluated their findings against a handful of operators or devices only, and it remained unclear whether the reported vulnerabilities – and the recommended fixes – apply to other deployments. Rather than searching for isolated new bugs, we therefore systematically collected known vulnerability classes and re-evaluated them against all Austrian IMS deployments:

1. **Identification:** findings from publications, talks, and selected blog posts were collected and merged if their verification is identical; findings whose root cause lies in the IMS application layer were kept in scope.
2. **Formalisation:** each finding was translated into a test procedure with preconditions, verification steps, and result categories (*fully* or *partially reproducible*, *not reproducible*, *not applicable*, *not testable*); 3GPP Release 16 served as the reference for classifying algorithms as insecure.
3. **Verification:** the procedures were executed against the Austrian operators (and, for client-side findings, against ten smartphones covering all major baseband vendors), where possible in automated form.
4. **Impact assessment:** the security and, in particular, the privacy impact of each reproducible finding was assessed, using the GDPR notion of personal data as a guideline.

Test subjects. Resolving the standardised ePDG domain names for all MCC/MNC combinations registered in Austria yields four separate IMS cores: A1 (shared with its brands bob, yesss!, and Georg), Magenta (shared with the MVNO HoT), Drei, and spusu, an MVNO that uses Drei's radio network but operates its own IMS core. Vendor artefacts in the SIP signalling (proprietary URI parameters, call-ID formats, user-agent strings) indicate Huawei session border controllers at A1 and ZTE equipment at Drei, and show that Magenta migrated from Huawei-specific to Mavenir-based components during the project period – consistent with the operator's announced move to a cloud-native IMS [47].

VoWiFi as access path. Measurements via the radio access network require a commercial device with a working IMS client, are difficult to automate, and are prone to artefacts of proprietary baseband components. Since operators use the same IMS core for VoLTE and VoWiFi (Section 2.1), the application-layer behaviour of the IMS can equivalently – and far more conveniently – be tested via the ePDG; this equivalence was confirmed for the Austrian operators. Building on the open-source IMS client of the Osmocom project, the tool *epdg-peek* was developed (Figure 5.1). It packages the client into a container that reads the IMSI from a SIM card attached via a PC/SC reader, resolves the operator's ePDG, establishes the IPsec tunnels using EAP-AKA with the SIM card, and executes test scripts inside a dedicated network namespace. Key material is logged automatically so that all layers can be decrypted, and several

containers can be run in parallel or orchestrated for tests involving a caller and a callee. Since tests can be repeated cheaply, the results have high confidence. The tooling has been published as open-source software and can equally be used by operators for their own black-box testing.

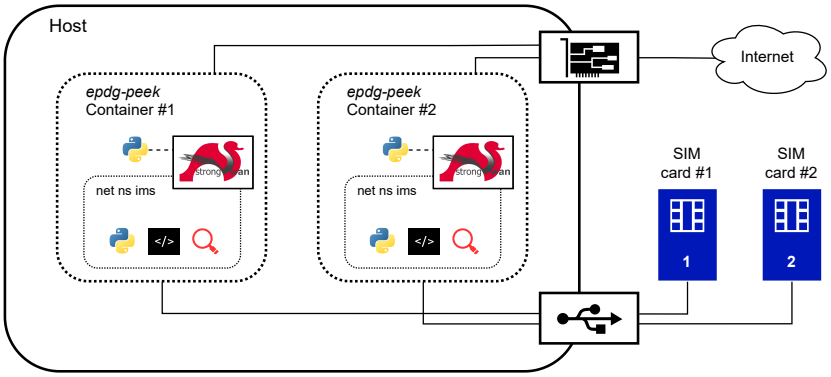


Figure 5.1: Architecture of *epdg-peek*: each container establishes the VoWiFi IPsec tunnels with a SIM card connected via PC/SC and runs automated tests against the operator's IMS in a separate network namespace [47].

5.2.2 Overview of Results

The approach resulted in eleven finding classes, nine of which are based on prior work (partly extended) and two of which were newly identified in the project. Table 5.2 summarises the results. **Ten of the eleven finding classes were reproducible** for at least one Austrian operator or current end device, although several of them were first published around ten years ago together with recommendations for mitigation. The two findings with the highest practical relevance – privacy leakage due to missing SIP header filtering and caller-ID spoofing – are discussed in detail in Sections 5.3 and 5.4; the remaining findings are summarised in Section 5.5. F10 and F11, which concern the IPsec configuration of the ePDG, are discussed together with the other VoWiFi results in Chapter 6.

	Finding class	**A1**	**Magenta**	**Drei**	**spusu**
F01	Direct Internet connectivity via the IMS bearer	∘	∘	∘	∘
F02	Missing isolation between subscribers	∘	▲	∘	–
F03	Leaked session information (misrouted RTP)	•	•	•	▲
F04	Unprivileged app access to IMS interfaces		2 of 10 devices		
F05	No billing of arbitrary data	–	•	–	•
F06	**Incomplete sanitisation of SIP headers**	•	∘	•	–
F07	**Spoofing of the caller number**	∘	•	–	–
F08	Logging of sensitive information on devices		5 of 7 Android devices		
F09	Unexpected early media (audio before answer)	▲	∘	▲	–
F10	ePDG does not present a certificate	•	•	•	•
F11	Support of insecure cryptography	•	•	•	•

• fully reproducible ▲ partially reproducible ∘ not reproducible – not applicable or not testable

Table 5.2: Reproduction of known VoLTE/VoWiFi vulnerability classes against the Austrian IMS deployments (MVNOs sharing an IMS are merged) and current end devices [47].

5.3 Privacy Leakage due to Missing SIP Header Filtering

SIP messages traverse several network elements between caller and callee, each of which may add header fields – for instance about the device, its software, the access network, or internal routing. The standards therefore expect operators to remove or rewrite information at the borders of their network that is not required by the remote party, both to protect subscriber privacy and to hide the internal network topology. Missing filtering turns SIP signalling into a side channel through which the called party (or the caller) learns more than intended; forwarded attacker-controlled headers can moreover be used to deliver malicious input to the SIP parsers of remote devices.

Test design. The test follows the scheme in Figure 5.2: a SIP sender triggers or injects a header, and the messages received by the callee via the operator's IMS are searched for it. Seven scenarios were tested: (H1) forwarding of an arbitrary custom header, (H2) forwarding of the caller's `User-Agent`, (H3) exposure of the callee's `User-Agent` in responses, (H4) reuse of the caller's `Call-ID`, which may embed the device's IP address, (H5) exposure of the caller's number despite caller-ID suppression (CLIR), (H6) exposure of the location (`P-Access-Network-Info`), and (H7) exposure of IMEI or IMSI. In addition, seven 'header confusion' attacks recently described by Wang et al. [44] were tested, which exploit ambiguities in identity-related headers (e.g., `P-Asserted-Identity`, `Remote-Party-ID`, duplicate or malformed `From` headers) to influence the identity presented to the callee.

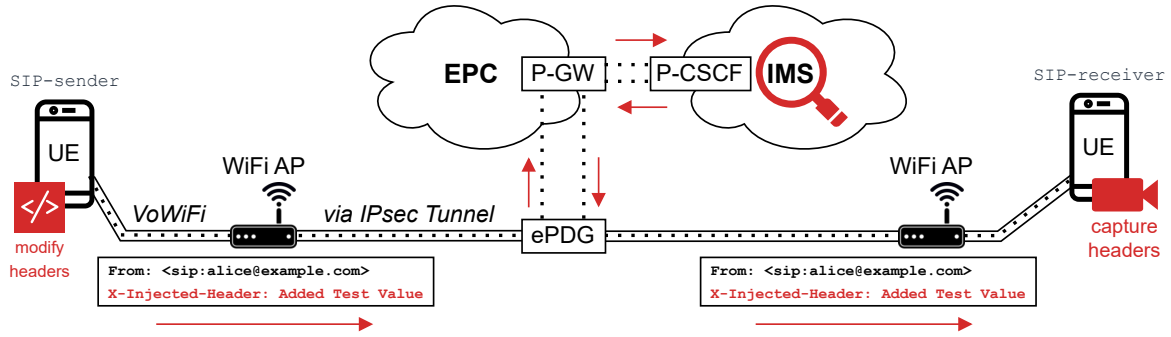


Figure 5.2: Test of SIP header sanitisation: a header injected by the sender is searched for in the messages received by the callee via the operator's IMS [47].

Operator	H1 custom	H2 UA fwd.	H3 UA resp.	H4 Call-ID	H5 CLIR	H6 location	H7 IMEI/IMSI
A1	•	•	•	◦	•	◦	◦
Magenta	◦	◦	◦	◦	◦	◦	◦
Drei	–	•	•	◦	◦	◦	◦
spusu	–	–	–	–	–	–	–

• header exposed ◦ filtered – not testable

Table 5.3: Results of the SIP header sanitisation tests [47].

Results. Table 5.3 summarises the results. A1 forwarded arbitrary custom headers to the called party and exposed the `User-Agent` of the remote party in both directions – in the `INVITE`

towards the callee and in the provisional responses (`180 Ringing`, `183 Session Progress`) towards the caller. Since Android devices typically include their model name in this header, a caller learns the device model of the callee before the call is even answered, and vice versa; for calls to voicemail systems or via third-party gateways, the software of these systems is revealed. Drei likewise exposed the remote `User-Agent` in both directions. Most notably, for calls with suppressed caller identification from certain A1 business subscriptions, the `From` header was correctly anonymised, but the caller's number was still transmitted to the called party in the proprietary header `X-VPNADN` – undermining the very purpose of number suppression. Of the header confusion attacks, one succeeded at A1: an identity placed in the legacy `Remote-Party-ID` header of an `INVITE` appeared in the `From` header received by the callee, presumably because of the generally missing filtering of such headers. This was tested only towards a SIP-based callee in the same network; direct manipulation of the `From` header, as discussed in Section 5.4, was rejected by A1. For Magenta, no unsanitised headers were found for the tested set; malformed requests were answered gracefully, although the responses revealed how the server had parsed the input. At Drei, the custom header and confusion tests could not be performed because the P-CSCF did not handle SIP over TCP in a standard-compliant way, and spusu could not be tested for lack of a second SIM card. Across operators, detailed error messages in `Warning` headers and malformed responses revealed further information about the internal parsing of the servers, and the vendor fingerprints described in Section 5.2 were themselves only visible because of incompletely filtered headers.

Impact. The exposure of the device model and software version is personal information in the sense of the GDPR and facilitates targeted attacks against known vulnerabilities of a specific device; in shared-number scenarios (e.g., company hotlines), it can even identify which person is calling. The leakage of the number of a caller who explicitly requested suppression is a direct privacy violation. Recent incidents abroad show that the same class of issue can have even more severe consequences: at a UK operator, unfiltered headers revealed the cell identifier, and thus the coarse location, of any called subscriber [46]. The results were reported to the affected operators as part of the responsible disclosure process (Chapter 9).

5.4 Caller-ID Spoofing

In the IMS, the network – not the device – is responsible for asserting the identity of the caller: the P-CSCF is expected to verify that the identity claimed by a registered UE belongs to its subscription and to insert a trustworthy `P-Asserted-Identity` before the call leaves the operator's network. Legitimate exceptions exist, e.g., business numbers shared between desk and mobile phones, but these are explicit opt-in features and were excluded from testing.

Test design. Using epdg-peek, a test subscriber placed calls in which all occurrences of the own number in the outgoing `INVITE` (the `From` header and, optionally, the `P-Asserted-Identity`) were replaced by a different number. Three types of spoofed numbers were tested – a number of the same operator, a number of another Austrian operator, and a foreign number – all of them strictly under the control of the research team. The test was considered successful if the called party was presented with the spoofed number.

Results. At Magenta, the network accepted the client-provided number in all three cases and presented it to the called party (Table 5.4). Because the operator itself treated the spoofed number as the calling number, the attack does not depend on the callee's network or technology:

Operator	Same operator	Other Austrian operator	Foreign operator
A1	∘	∘	∘
Magenta	•	•	•
Drei	–	–	–
spusu	–	–	–

• spoofed number presented to callee ∘ call rejected – not testable

Table 5.4: Results of the caller-ID spoofing test [47].

the spoofed number is also displayed to subscribers of other operators and in circuit-switched networks. A1, in contrast, consistently rejected such calls with `403 Forbidden` (but see the `Remote-Party-ID` confusion attack in Section 5.3). Drei and spusu could not be tested for the technical reasons given in Section 5.3.

Impact. Caller-ID spoofing is a central building block of fraud and social-engineering attacks, as it allows calls to appear to originate from trusted numbers such as banks, authorities, or personal contacts, and to bypass blocklists of known malicious numbers. The finding is particularly relevant in Austria, since the anti-spoofing provisions introduced by the RTR are specifically intended to prevent the unauthorised use of Austrian numbers in voice calls. The observed ability of any subscriber to signal arbitrary Austrian numbers conflicts with these regulatory requirements and shows that the security of modern telephony depends not only on encryption and authentication, but equally on the correct implementation of regulatory requirements in the signalling configuration. The finding was reported to the operator and the RTR as part of the responsible disclosure process (Chapter 9).

5.5 Further Findings

The remaining finding classes are summarised briefly [47]:

- **Isolation and billing (F01, F02, F05).** No operator provided direct Internet access via the IMS bearer, but spusu allowed DNS resolution via the servers announced in the VoWiFi tunnel, a narrow data channel. At Magenta, two subscribers could communicate directly via their IMS addresses if these were located in the same IPv6 `/44` subnet. Neither form of traffic was billed.
- **Session information and device-side access (F03, F04).** At all operators, RTP packets reached the signalling bearer around call setup – at Magenta for up to minutes, because the voice bearer is only established once the call is answered. Together with unprivileged access to the IMS interface, which was possible on two of ten devices, a malicious app could detect and disrupt calls without the corresponding permission [32].
- **Sensitive information in device logs (F08, new).** On five of seven Android devices, IMS components wrote sensitive data to the system log, including the IMSI, cell identifiers, SIP authentication responses, and – on one device – the IKE and IPsec keys of the VoWiFi tunnel, merely obfuscated by a trivially invertible encoding.
- **Unexpected early media (F09, new).** At A1 and Drei, the caller's audio was transmitted to the callee's device already during the ringing phase for calls from certain networks, so that a modified client could record what the caller says before the call is answered.

5.6 Discussion

The results show that improvements in the standards do not automatically translate into secure deployments: vulnerability classes documented in the literature for up to a decade remain reproducible in current Austrian networks and devices. At the same time, the operators differ considerably – an operator that is robust against one class of attack (e.g., Magenta regarding header filtering) may be vulnerable to another (caller-ID spoofing), and the behaviour of an operator can change substantially with a change of the core network vendor, as observed for Magenta during the project. A purely standards-based assessment cannot capture these differences, which underlines the value of independent, repeatable measurements in production networks. The formalised test procedures and the open-source tooling lower the barrier for such continuous testing, both for researchers and for operators themselves.

The analysis is subject to limitations. Only Austrian operators could be tested systematically, and several tests were not possible for Drei (non-compliant TCP handling in the P-CSCF) and spusu (lack of a second SIM card, registration problems with rooted devices). The device selection covers all major baseband vendors but is not representative of the market.

6 Internet Layer: Voice over Wi-Fi

VoWiFi is the part of the mobile network that is intentionally exposed to the Internet: every ePDG can be reached by anyone who resolves its standardised domain name. This makes VoWiFi both an attractive target and a convenient object of measurement. This chapter first summarises the results of our two global VoWiFi studies published before the project, which formed its starting point (Section 6.1), and then presents the SIM-based analysis of the Austrian deployments carried out within TelCrit, which extends these studies from the outer tunnel layer to the full protocol stack (Section 6.2).

6.1 Starting Point: Prior Global VoWiFi Studies

Key exchange. In *Diffie-Hellman Picture Show* [21], we analysed the IKEv2 key exchange of layer L1 from the client side (carrier configuration files of Apple, Samsung, Google, and Qualcomm-based devices) and from the operator side (Internet-wide scans of all resolvable ePDGs). Most operators still announced and accepted DH groups weaker than 2048 bit, contrary to the 3GPP specifications, and only 42 % requested an upgrade when a client chose a weaker group although both sides supported a stronger one. On the client side, a 5G baseband chipset of a major vendor silently accepted the 768-bit group DH1 – never part of any 3GPP specification – which we exploited in a man-in-the-middle experiment. Most strikingly, at least 13 operators on three continents, with an estimated 140 million subscribers and including an Austrian operator, used the same globally static set of ten private DH keys (CVE-2024-22064). All of them had deployed their core network from the same vendor (ZTE), and anyone with knowledge of these keys could decrypt the L1 key exchange of their subscribers. The issue was remediated through coordinated disclosure.

Geoblocking. In *Why E.T. Can't Phone Home* [20], we measured the reachability of the ePDGs of operators worldwide from more than 200 countries. A substantial share of operators (14.6 % for IPv4, 65.2 % for IPv6) block access from abroad at the DNS or IKE level, presumably to protect roaming revenues. Since such blocking does not distinguish between regular and emergency calls, it can prevent travellers from placing emergency calls over Wi-Fi exactly in situations in which VoLTE roaming is unavailable – an increasingly relevant scenario with the shutdown of 2G and 3G networks. In Austria, Magenta requires an additional subscription package for VoWiFi while roaming and decides about access only after authentication, i.e., based on the subscriber identity rather than on the source IP address. The findings were reported to the GSMA, BEREC, and EENA.

Limitation. Both studies were designed for global coverage and therefore had to work without SIM cards. They were consequently limited to the unauthenticated part of the outer layer L1 – the `IKE_SA_INIT` exchange – and could not assess the IPsec tunnel (L2), the IMS registration, or the SIP protection (L3).

6.2 Beyond L1: SIM-based Analysis of Austrian Deployments

With SIM cards of all Austrian operators and the epdg-peek tooling described in Section 5.2, TelCrit extended the analysis to all three layers [47]. The tests were carried out as authenticated connections, so that parameters negotiated only after EAP-AKA authentication could be

evaluated as well; for comparison, the German operator O2, which uses the same IMS vendor as Magenta, was included. The classification of insecure parameters follows 3GPP Release 16: for L1, DH groups below 2048 bit are prohibited (TS 33.210); for L2, only the ESP algorithms listed in RFC 8221 may be used, excluding DES, 3DES, and HMAC-MD5-96; and for L3, 3GPP TS 33.203 no longer permits `des-ede3-cbc` and `hmac-md5-96`. The null encryption algorithm is formally part of the specifications but was considered insecure for access over untrusted networks.

6.2.1 Missing ePDG Authentication by Certificate

Within IKEv2, the UE sends its identity – typically derived from the IMSI – in the first `IKE_AUTH` message, before the ePDG has proven its own identity. Unless the ePDG additionally authenticates itself with a certificate that the device verifies, an attacker controlling a Wi-Fi network can impersonate the ePDG and collect the permanent identities of all devices that connect – an IMSI catcher that requires no radio equipment [8]. Using the tool epdg-cert, we therefore tested whether ePDGs present a certificate when requested.

None of the four Austrian IMS deployments (A1, Magenta, Drei, spusu) presented a certificate; all started the EAP authentication without one, leaving devices no possibility to authenticate the ePDG before disclosing their identity. The same holds internationally: of the ten operators for which Samsung's carrier configuration enables certificate validation, only two (Telstra, Maxis) actually presented a certificate, while two others started the EAP exchange without one – which would prevent properly configured devices from connecting – and the remaining results were inconclusive. A global scan found further operators presenting certificates, several of them with a mismatch between the certificate and the announced ePDG identity.

6.2.2 Insecure Cryptography Across All Layers

Table 6.1 summarises the insecure algorithms accepted by the operators on the three layers.

	L1: IKE DH group			**L2: ESP**				**L3: `ipsec-3gpp`**			
Operator	DH1	DH2	DH5	NULL	DES	3DES	MD5	NULL	3DES	MD5	skip
A1 (Georg)	◦	•	•	◦	◦	◦	◦	•[a]	◦	◦	◦
Magenta (HoT)	◦	•	◦	◦	◦	◦	◦	•	◦	◦	◦
Drei	•	•	•	•	•	•	•	•	•	•	◦
spusu	◦	•	◦	◦	◦	◦	◦	•	◦	•	•
O2 (Germany)	◦	•	◦	◦	◦	•	◦	•[a]	◦	•	◦

• insecure option accepted ◦ rejected [a] null encryption is the *only* option offered by the operator

Table 6.1: Insecure algorithms accepted by the ePDG (L1, L2) and the P-CSCF (L3) in authenticated tests (MVNOs sharing infrastructure in brackets). 'skip': registration without any L3 protection accepted. HMAC-SHA1-96, which is scheduled for removal, was accepted by all operators on L2 [47].

L1. All operators still accept the 1024-bit group DH2, which has been prohibited by 3GPP since 2016. A1 and Drei additionally accept DH5, and Drei even DH1 – groups that were never specified for 3GPP use at all. Since clients typically also support DH2, an active attacker could attempt to downgrade the key exchange to a group within reach of well-resourced adversaries [5, 21].

L2. A1, Magenta, and spusu accept only permitted ESP algorithms (apart from HMAC-SHA1-96, which is still permitted but scheduled for removal). Drei, in contrast, accepts DES, 3DES, HMAC-MD5-96, and even the null cipher for the IPsec tunnel between UE and ePDG, i.e., a configuration in which the tunnel provides no confidentiality at all.

L3. The protection of SIP signalling between UE and P-CSCF is weak at all operators. All accept null encryption, and at A1 null encryption is the *only* option offered, so that SIP signalling is protected only by the outer tunnel. Drei additionally accepts 3DES and HMAC-MD5-96, and spusu accepts HMAC-MD5-96 and even a registration without any `ipsec-3gpp` protection, although this layer is mandatory for access over untrusted networks. At Magenta, null encryption was no longer accepted in August 2025 but reappeared in 2026, possibly in connection with the migration of the IMS core. Further irregularities included identical authentication nonces returned by different P-CSCFs of Drei, and P-CSCFs of spusu that answered unacceptable proposals with different, unrequested parameters instead of an error, contrary to TS 33.203.

These layers compound: if L3 is unencrypted, the confidentiality of SIP signalling depends entirely on L1/L2, and thus on a key exchange that at every Austrian operator can still be negotiated with a deprecated DH group.

6.2.3 Longitudinal View on Static Keys

To assess the sustainability of the remediation of the static ZTE keys, unauthenticated L1 scans were analysed over more than two years (February 2024 to August 2026), combining a dedicated daily DH2 scan with the data of our public longitudinal VoWiFi measurements [9, 47]. The Austrian operator Drei, which was affected in 2024, remained fixed throughout. At seven other operators, however, the static keys *reappeared* after a verified fix – in one case only on a single server behind a load balancer, which served the static keys in slightly less than 10 % of key exchanges – and three operators that had never fixed the issue were still serving static keys in August 2026. Moreover, identical combinations of DH key and nonce were observed repeatedly across different operators presumably using the same vendor (e.g., four times between Drei and a Spanish operator over more than a year), and a previously unknown static key was found at three operators in Japan, Kiribati, and Mongolia, presumably served by another vendor's ePDG. These observations show that a single successful disclosure is not sufficient: fixes can be undone by software updates, hardware replacements, or partially upgraded server pools, and only continuous monitoring can detect such regressions.

6.3 Discussion

Across all layers, the VoWiFi deployments of the Austrian operators show the same pattern as the global studies: security mechanisms exist in the standards but are not enforced, and deprecated options are kept for compatibility long after they have been prohibited. This 'technical debt' results from functional over-provisioning combined with the lack of a defined deprecation procedure for cryptographic algorithms in the 3GPP ecosystem. The results also differ substantially between operators – from Magenta, which rejects all insecure L2 options, to Drei, which accepts the null cipher on L2 – which is not visible to customers when choosing an operator.

From the perspective of the research questions, the analysis yields concrete recommendations: operators should (i) remove DH groups below 2048 bit and all deprecated ESP algorithms from their ePDGs, (ii) enforce integrity and confidentiality protection on L3 instead of accepting null encryption or no protection at all, (iii) deploy ePDG certificates so that devices can authenticate

the ePDG before disclosing their identity, and (iv) avoid purely IP-based geoblocking, which also affects emergency calls. Since fixes can regress, continuous and independent longitudinal monitoring is an essential complement to one-off assessments.

7 Internet Layer: Rich Communication Services

RCS is positioned as the successor of SMS and MMS and is enabled by default on Android and, since iOS 18, also on iPhones. From a data-protection perspective, the central question is *who* operates the RCS infrastructure of the Austrian operators, since this party processes the signalling and metadata of the communication. As no usable open-source RCS client existed at the start of the project, dedicated measurement tooling was developed within the master's thesis of P. Frenzel [16].

7.1 Methodology

RCS clients obtain their configuration from an auto-configuration server (ACS) of their operator, which is located via standardised domain names derived from MCC and MNC (Section 2.4). Using SIM cards of all three Austrian network operators, the configuration documents returned after authentication were retrieved by intercepting the traffic of Google Messages on a rooted test device. To put the Austrian results into context, a measurement client was developed that resolves about three million candidate ACS domains worldwide and emulates the initial, unauthenticated configuration requests of a client. Responses were attributed to Google's Jibe platform based on Google's published IP ranges, the TLS certificate, and Jibe-specific response patterns. The scan was rate-limited, and only identifiers of the team's own devices or IMSIs with all subscriber digits set to zero were used.

7.2 Results

Austria. All three Austrian network operators – A1, Magenta, and Drei – rely on Google Jibe for RCS. Their configuration documents assign subscribers identities under domains of the form `<operator>.rcs.telephony.goog`, contain Google-specific configuration sections (e.g., the endpoints of Google's messaging API and of the key server for end-to-end encryption), and configure a registration with an IMS operated by Google, separate from the operator's own IMS (Figure 2.3). For Austrian RCS users, signalling and message metadata are therefore not processed by their mobile operator, but by Google.

International context. Austria is no exception. Of about three million queried domains, 2,048 resolved, corresponding to at least 1,633 operators worldwide. Using a conservative classification, **about 98 % of the responding operators are served by Google Jibe**. Independent implementations were found only at a handful of operators (e.g., in the US, India, South Korea, and China); only Russia and China do not use Jibe at all (Figure 7.1).

Capability discovery and client fingerprinting. Using a reverse-engineered lookup function of Google Messages, the capabilities announced via RCS capability discovery were queried for all combinations of the test SIM cards and the three dominant clients (Google Messages, Samsung Messages, and Apple Messages). The announced capability sets differ clearly between the clients – including deprecated, duplicated, and non-standard Google-specific tags – while the influence of the operator is negligible. Knowing only a phone number, anyone can thus determine whether its owner uses RCS and which client, and hence which platform, is used.

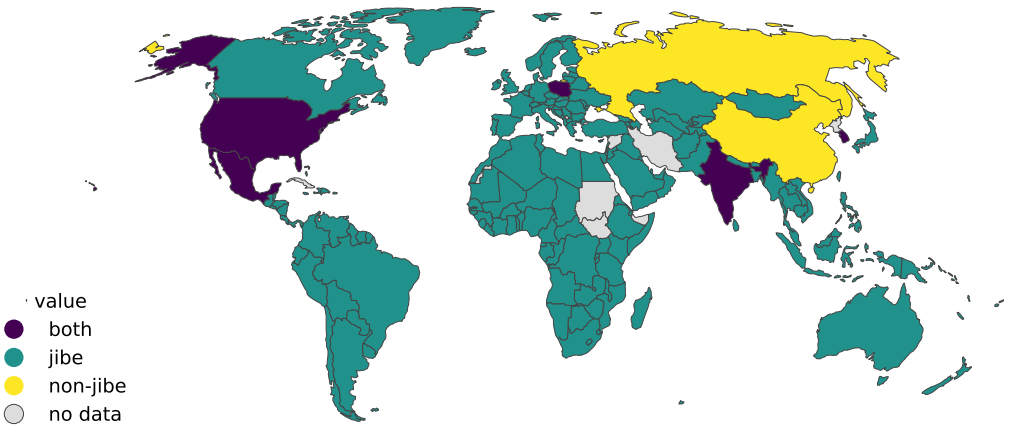


Figure 7.1: RCS implementations used by the operators of each country, based on the global auto-configuration scan. Countries without observed deployments may nevertheless offer RCS [16].

7.3 Discussion: Digital Sovereignty

RCS was conceived as an open, operator-driven standard and as a decentralised alternative to proprietary OTT messengers. In practice, the server infrastructure of almost all operators worldwide – including all Austrian operators – is provided by a single US company, which also develops the dominant RCS client on Android. A communication service that is increasingly replacing SMS, traditionally provided by the operators themselves, thus depends on the infrastructure of a single non-European provider.

This concentration is relevant from several perspectives. It concerns *digital sovereignty*, as Austria and Europe have little control over a service that is becoming part of everyday communication and is subject to foreign jurisdiction and political decisions – the absence of Jibe in Russia, presumably also due to sanctions, illustrates that access to such services can depend on geopolitics. It concerns *privacy and data protection*, as a single company gains access to the metadata of RCS communication across operators and countries, which would be considerably more fragmented if operators hosted RCS themselves. And it amplifies the *impact of vulnerabilities*, as any weakness in the common implementation affects almost all RCS users worldwide at once. The results provide an empirical basis for discussing these dependencies with operators and the regulator.

8 Internet Layer: Mobile Instant Messengers

For many users in Austria, OTT messengers such as WhatsApp, Signal, and iMessage have largely replaced SMS, and they are the main competitors of RCS. Since they run over the same mobile networks and devices, and since the analysis of RCS raised the question of which metadata a messaging service exposes, the scope of the Internet-layer analysis was extended to these services during the project. In contrast to RCS, they provide end-to-end encryption by default, which is often equated with comprehensive privacy. Our work shows that this is not the case: even when message contents are protected, protocol mechanisms such as delivery receipts, multi-device support, prekey distribution, and contact discovery leak information about users and their devices. The results are summarised briefly below; details can be found in the respective publications (Table 8.1).

Publication	**Services**	**Main finding**
Careless Whisper [24] (RAID 2025, Best Paper)	WhatsApp, Signal	Silent delivery receipts allow covert monitoring of online status, devices, and activity, and resource exhaustion
Prekey Pogo [23] (WOOT 2025)	WhatsApp	Targeted depletion of one-time prekeys degrades forward secrecy and leaks device information
Hey there! [25] (NDSS 2026)	WhatsApp	Enumeration of 3.5 billion accounts via contact discovery without effective rate limiting
Blue Bubbles, Red Flags [17] (CCS 2026)	iMessage	Device/OS fingerprinting, per-device targeting, online status, and coarse location

Table 8.1: Project publications on mobile instant messengers.

8.1 Silent Delivery Receipts

Delivery receipts cannot be disabled, since they are needed by the protocol (Section 2.5). We showed that not only regular messages but also reactions, edits, deletions, and even malformed messages – which are silently discarded by the receiving device – trigger delivery receipts, while nothing is displayed to the recipient [24]. By sending such ‘silent pings’ at high frequency, an attacker who only knows the phone number of a WhatsApp or Signal user can monitor each of the target’s devices individually, infer whether they are online, for some devices whether the screen is on, and which operating system they run, and derive daily routines and activity patterns – without any notification on the target’s side. The same channel enables resource exhaustion: on WhatsApp, we caused hidden data traffic of 13.3 GB per hour and battery drain of 14–18 % per hour on the victim’s device. The work received the Best Paper Award at RAID 2025.

8.2 Prekey Depletion in WhatsApp

Forward secrecy for the first messages of a new session relies on one-time prekeys stored on the server (Section 2.5). We demonstrated a targeted attack that depletes the one-time prekeys of individual WhatsApp devices by repeatedly requesting prekey bundles [23]. Afterwards, new

sessions with the victim are established without a one-time prekey, so that initial messages lose forward secrecy for the lifetime of the signed prekey. The replenishment and distribution procedure moreover leaks information about the victim's devices and has implications for availability.

8.3 Enumeration at Scale

Contact discovery inherently allows checking whether a phone number is registered (Section 2.5). We showed that WhatsApp's contact discovery could be queried at a rate of more than a hundred million phone numbers per hour without effective rate limiting, which allowed us to enumerate all 3.5 billion active accounts worldwide [25]. Beyond the registration status, the data included profile information and public keys, which allowed a census of the user base (e.g., an Android share of 81 %), revealed that nearly half of the phone numbers leaked in the 2021 Facebook data breach are still active on WhatsApp, and uncovered the reuse of identical X25519 keys across different devices and phone numbers, indicating insecure custom clients or fraudulent activity. In the course of an intensive, months-long disclosure process, countermeasures were developed together with Meta and rolled out (Chapter 9).

8.4 Privacy Leakage in Apple iMessage

In cooperation with researchers from the University of Applied Sciences Stralsund and the Hasso Plattner Institute, the analysis was extended to iMessage [17]. An attacker who knows a victim's phone number or e-mail address can silently fingerprint the device type and operating system version of each of the victim's devices – information that facilitates targeted exploitation – and can address individual devices selectively. Delivery receipts additionally reveal a device's online status and coarse location, which can also be derived from attachment uploads. All attacks are invisible to the victim.

8.5 Discussion

Across all four studies, the same pattern emerges: end-to-end encryption protects message contents, but not the metadata generated by the protocol mechanisms that are necessary to operate a messaging service at scale. The attacks require no interaction by the victim and, in most cases, only knowledge of the victim's phone number – which, as the enumeration study shows, can be collected for an entire platform. Because a handful of platforms serve billions of users, such weaknesses affect a large share of the Austrian population at once. Protecting against them requires design changes by the platform operators, e.g., rate limiting and coarser timing of receipts, stricter validation of messages before acknowledging them, and effective limits on contact discovery. All findings were disclosed to the affected vendors (Chapter 9).

9 Responsible Disclosure, Dissemination, and Impact

9.1 Responsible Disclosure

Responsible disclosure was an integral part of the communication of results. The anomalies and vulnerabilities identified at Austrian mobile network operators – including privacy leaks in SIP headers and a configuration that allowed arbitrary caller-ID spoofing – were communicated to the relevant stakeholders. The vulnerabilities identified in WhatsApp were disclosed to Meta in a process that extended over several months and involved regular, at times several-times-weekly technical meetings. The project results directly informed the design and evaluation of countermeasures, which were subsequently implemented and rolled out by Meta, improving security for a global user base.

9.2 Scientific Publications

The project results were published at high-ranking international venues:

- **Gabriel K. Gegenhuber**, Maximilian Günther, Markus Maier, Aljosha Judmayer, Florian Holzbauer, Philipp É. Frenzel, Johanna Ullrich. *Careless Whisper: Exploiting Silent Delivery Receipts to Monitor Users on Mobile Instant Messengers.* RAID 2025 – **Best Paper Award** [24].
- **Gabriel K. Gegenhuber**, Philipp É. Frenzel, Maximilian Günther, Aljosha Judmayer. *Prekey Pogo: Investigating Security and Privacy Issues in WhatsApp's Handshake Mechanism.* USENIX WOOT 2025 [23].
- **Gabriel K. Gegenhuber**, Philipp É. Frenzel, Maximilian Günther, Johanna Ullrich, Aljosha Judmayer. *Hey there! You are using WhatsApp: Enumerating Three Billion Accounts for Security and Privacy.* NDSS 2026 [25].
- Viktor E. Garske, Swantje Lange, **Gabriel K. Gegenhuber**, David Schmidt, Andreas Noack, Jiska Classen. *Blue Bubbles, Red Flags: Investigating Privacy Leakage in Apple iMessage.* ACM CCS 2026 [17].
- **Gabriel K. Gegenhuber**, Philipp É. Frenzel, Adrian Dabrowski. *SIMulator: SIM Tracing on a (Pico-)Budget.* ACM WiSec 2025 (extended abstract) [22].
- **Gabriel K. Gegenhuber**. *Security and Privacy Measurements in Cellular Networks: Novel Approaches in a Global Roaming Context.* ACM CCS 2025 (Doctoral Symposium) [18].

In addition, the following theses were written and supervised within the project:

- Robert Wittek. *Automated Phreaking: Consolidation of VoLTE and VoWiFi Security Testing.* Master's thesis, TU Wien, 2026, supervised by **Gabriel K. Gegenhuber** [47].
- Philipp É. Frenzel. *An Empirical Study of Global RCS Deployments.* Master's thesis, TU Wien, 2026, supervised by **Gabriel K. Gegenhuber** [16].

- Philip A. Magnus. *Nosy Neighbors: Analyzing Multi-Profile Isolation on eUICCs.* Master's thesis, FH Campus Wien, 2026, supervised by **Gabriel K. Gegenhuber** [33].
- Johannes Brückl. *Old Issues, New Packaging: Bringing Transparency to VoWiFi Security via Longitudinal Measurements.* Bachelor's thesis, University of Vienna, 2026, supervised by **Gabriel K. Gegenhuber** [9].

The project further builds on our previous studies on VoWiFi key exchange [21] and VoWiFi geoblocking [20].

9.3 Presentations and Community Events

Beyond the scientific venues, the results were presented to the international security community at DEF CON 33 and DEF CON 34, Ekoparty, and the ISMK MSC conference. At national level, results were presented and discussed with stakeholders from research, industry, and cybersecurity at the NCC-AT community event of the FFG and at the CERT.at Security Stammtisch. A final presentation and discussion of the results with the RTR takes place on 12 November 2026, after the formal end of the project.

9.4 Media Coverage

The results attracted broad national and international media attention, including coverage by WIRED, The Independent, heise.de, and derStandard.at, thereby raising public awareness of security and privacy risks in modern communication services.

10 Conclusion and Outlook

TelCrit provided the first systematic, cross-operator assessment of modern voice and messaging services in Austrian mobile networks. The transition to 4G/5G has not automatically raised the level of security: the standards offer strong protection mechanisms, but many of them are optional, and deprecated options remain accepted long after their prohibition. At every Austrian operator examined, security- or privacy-relevant weaknesses were found – from deprecated key exchange parameters and missing ePDG certificates to unfiltered SIP headers and caller-ID spoofing. Beyond the operators' own infrastructure, RCS in Austria depends entirely on Google, and widely used messengers leak metadata despite end-to-end encryption.

Operators should remove deprecated algorithms, enforce protection on all layers, filter SIP signalling at their network borders, and verify caller identities. For the regulator, the results provide an empirical basis for enforcing anti-spoofing requirements and for discussing dependencies such as the centralisation of RCS.

A key lesson of the project is that one-off measurements provide only a snapshot: within the observation period, previously fixed static keys reappeared at several operators, and the configuration of an Austrian operator changed substantially with the migration of its IMS core. A single assessment therefore guarantees little about the security of the next software update or vendor change. This underlines the importance of regular, independent audits of mobile communication infrastructure – for instance by research institutions, by the regulator, or by the operators themselves – ideally in the form of longitudinal measurements that detect regressions and newly introduced weaknesses early. The open-source tooling developed in TelCrit can support such efforts and can be extended to upcoming technologies such as VoNR in 5G standalone networks.

Bibliography

[1] 3GPP. IP Multimedia Subsystem (IMS); stage 2. Technical Specification TS 23.228, 3rd Generation Partnership Project, 2024. Version 18.7.0.

[2] 3GPP. IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); stage 3. Technical Specification TS 24.229, 3rd Generation Partnership Project, various releases.

[3] 3GPP. 3G security; access security for IP-based services. Technical Specification TS 33.203, 3rd Generation Partnership Project, various releases.

[4] 3GPP. 3GPP System Architecture Evolution (SAE); security architecture. Technical Specification TS 33.401, 3rd Generation Partnership Project, various releases.

[5] David Adrian, Karthikeyan Bhargavan, Zakir Durumeric, Pierrick Gaudry, Matthew Green, J. Alex Halderman, Nadia Heninger, Drew Springall, Emmanuel Thomé, Luke Valenta, Benjamin VanderSloot, Eric Wustrow, Santiago Zanella-Béguelin, and Paul Zimmermann. Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice. In *22nd ACM Conference on Computer and Communications Security (CCS)*, 2015.

[6] Apple. Apple platform security guide. `https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf`, 2024.

[7] Jari Arkko and Henry Haverinen. Extensible authentication protocol method for 3rd generation authentication and key agreement (EAP-AKA). RFC 4187, Internet Engineering Task Force, 2006.

[8] Jaejong Baek, Sukwha Kyung, Haehyun Cho, Ziming Zhao, Yan Shoshitaishvili, Adam Doupé, and Gail-Joon Ahn. Wi Not Calling: Practical Privacy and Availability Attacks in Wi-Fi Calling. In *Proceedings of the 34th Annual Computer Security Applications Conference (ACSAC '18)*, pages 278–288, 2018.

[9] Johannes Brückl. Old Issues, New Packaging: Bringing Transparency to VoWiFi Security via Longitudinal Measurements. Bachelor's thesis, University of Vienna, 2026.

[10] Gonzalo Camarillo, Vesa Torvinen, Jari Arkko, Aki Niemi, and Tao Haukka. Security mechanism agreement for the Session Initiation Protocol (SIP). RFC 3329, Internet Engineering Task Force, 2003.

[11] Sreepriya Chalakkal, Hendrik Schmidt, and Shinjo Park. Practical attacks on VoLTE and VoWiFi. Whitepaper ERNW-60, ERNW Enno Rey Netzwerke GmbH, 2017.

[12] ETSI. Digital cellular telecommunications system (Phase 2+) (GSM); UMTS; LTE; 5G; numbering, addressing and identification. Technical Specification ETSI TS 123 003 V17.10.0, ETSI, 2023.

[13] ETSI. 3G security; Network Domain Security (NDS); IP network layer security. Technical Specification ETSI TS 133 210, ETSI, various releases.

[14] ETSI. 3GPP System Architecture Evolution (SAE); security aspects of non-3GPP accesses. Technical Specification ETSI TS 133 402, ETSI, various releases.

[15] Dennis Felsch, Martin Grothe, Jörg Schwenk, Adam Czubak, and Marcin Szymanek. The Dangers of Key Reuse: Practical Attacks on IPsec IKE. In *27th USENIX Security Symposium (USENIX Security 18)*, pages 567–583, 2018.

[16] Philipp É. Frenzel. An Empirical Study of Global RCS Deployments. Master's thesis, TU Wien, 2026.

[17] Viktor E. Garske, Swantje Lange, Gabriel K. Gegenhuber, David Schmidt, Andreas Noack, and Jiska Classen. Blue Bubbles, Red Flags: Investigating Privacy Leakage in Apple iMessage. In *Proceedings of the 2026 ACM SIGSAC Conference on Computer and Communications Security (CCS '26)*. ACM, 2026.

[18] Gabriel K. Gegenhuber. Security and Privacy Measurements in Cellular Networks: Novel Approaches in a Global Roaming Context. In *32nd ACM Conference on Computer and Communications Security (CCS)*, 2025.

[19] Gabriel K. Gegenhuber, Wilfried Mayer, Edgar Weippl, and Adrian Dabrowski. MobileAtlas: Geographically Decoupled Measurements in Cellular Networks for Security and Privacy Research. In *32nd USENIX Security Symposium (USENIX Security 23)*, 2023.

[20] Gabriel K. Gegenhuber, Philipp É. Frenzel, and Edgar Weippl. Why E.T. Can't Phone Home: A Global View on IP-based Geoblocking at VoWiFi. In *Proceedings of the 22nd Annual International Conference on Mobile Systems, Applications and Services (MobiSys '24)*. ACM, 2024.

[21] Gabriel K. Gegenhuber, Florian Holzbauer, Philipp É. Frenzel, Edgar Weippl, and Adrian Dabrowski. Diffie-Hellman Picture Show: Key Exchange Stories from Commercial VoWiFi Deployments. In *33rd USENIX Security Symposium (USENIX Security 24)*, 2024.

[22] Gabriel K. Gegenhuber, Philipp É. Frenzel, and Adrian Dabrowski. SIMulator: SIM Tracing on a (Pico-)Budget. In *Proceedings of the 18th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '25), Extended Abstract*. ACM, 2025.

[23] Gabriel K. Gegenhuber, Philipp É. Frenzel, Maximilian Günther, and Aljosha Judmayer. Prekey Pogo: Investigating Security and Privacy Issues in WhatsApp's Handshake Mechanism. In *19th USENIX WOOT Conference on Offensive Technologies (WOOT 25)*, 2025.

[24] Gabriel K. Gegenhuber, Maximilian Günther, Markus Maier, Aljosha Judmayer, Florian Holzbauer, Philipp É. Frenzel, and Johanna Ullrich. Careless Whisper: Exploiting Silent Delivery Receipts to Monitor Users on Mobile Instant Messengers. In *Proceedings of the 28th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2025)*, 2025.

[25] Gabriel K. Gegenhuber, Philipp É. Frenzel, Maximilian Günther, Johanna Ullrich, and Aljosha Judmayer. Hey there! You are using WhatsApp: Enumerating Three Billion Accounts for Security and Privacy. In *Network and Distributed System Security Symposium (NDSS 2026)*, 2026.

[26] GSMA. Rich communication suite – advanced communications services and client specification. Official Document RCC.07, GSM Association, 2026. Version 17.0.

[27] GSMA. Service provider device configuration. Official Document RCC.14, GSM Association, 2026. Version 13.0.

[28] Cullen Jennings, Jon Peterson, and Mark Watson. Private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks. RFC 3325, Internet Engineering Task Force, 2002.

[29] Charlie Kaufman, Paul E. Hoffman, Yoav Nir, Pasi Eronen, and Tero Kivinen. Internet key exchange protocol version 2 (IKEv2). RFC 7296, Internet Engineering Task Force, 2014.

[30] Hongil Kim, Dongkwan Kim, Minhee Kwon, Hyungseok Han, Yeongjin Jang, Dongsu Han, Taesoo Kim, and Yongdae Kim. Breaking and Fixing VoLTE: Exploiting Hidden Data Channels and Mis-implementations. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS '15)*, pages 328–339, 2015.

[31] Ehren Kret and Rolfe Schmidt. The PQXDH key agreement protocol. Signal specification, `https://signal.org/docs/specifications/pqxdh/`, 2023.

[32] Chi-Yu Li, Guan-Hua Tu, Chunyi Peng, Zengwen Yuan, Yuanjie Li, Songwu Lu, and Xinbing Wang. Insecurity of Voice Solution VoLTE in LTE Mobile Networks. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS '15)*, pages 316–327, 2015.

[33] Philip A. Magnus. Nosy Neighbors: Analyzing Multi-Profile Isolation on eUICCs. Master's thesis, FH Campus Wien, 2026.

[34] Moxie Marlinspike and Trevor Perrin. The X3DH key agreement protocol. Signal specification, `https://signal.org/docs/specifications/x3dh/`, 2016.

[35] Moxie Marlinspike and Trevor Perrin. The Sesame algorithm: Session management for asynchronous message encryption. Signal specification, `https://signal.org/docs/specifications/sesame/`, 2017.

[36] Ralph Moonen. VoLTE phreaking. HITB Security Conference, HAXPO, Amsterdam, 2019.

[37] Yoav Nir, Tero Kivinen, Paul Wouters, and Daniel Migault. Algorithm implementation requirements and usage guidance for the Internet Key Exchange Protocol Version 2 (IKEv2). RFC 8247, Internet Engineering Task Force, 2017.

[38] Trevor Perrin and Moxie Marlinspike. The double ratchet algorithm. Signal specification, `https://signal.org/docs/specifications/doubleratchet/`, 2016.

[39] Jon Peterson. A privacy mechanism for the Session Initiation Protocol (SIP). RFC 3323, Internet Engineering Task Force, 2002.

[40] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler. SIP: Session Initiation Protocol. RFC 3261, Internet Engineering Task Force, 2002.

[41] SBA Research. MobileAtlas: SDR feasibility study. `https://github.com/sbaresearch/mobile-atlas/tree/main/sdr-feasibility`, 2025.

[42] Theodor Schnitzler, Katharina Kohls, Evangelos Bitsikas, and Christina Pöpper. Hope of Delivery: Extracting User Locations From Mobile Instant Messengers. In *Network and Distributed System Security Symposium (NDSS 2023)*, 2023.

[43] Guan-Hua Tu, Chi-Yu Li, Chunyi Peng, Yuanjie Li, and Songwu Lu. New security threats caused by IMS-based SMS service in 4G LTE networks. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16)*, pages 1118–1130, 2016.

[44] Qi Wang, Jianjun Chen, Jingcheng Yang, Jiahe Zhang, Yaru Yang, and Haixin Duan. SIPConfusion: Exploiting SIP Semantic Ambiguities for Caller ID and SMS Spoofing. In *Network and Distributed System Security Symposium (NDSS 2026)*, 2026.

[45] WhatsApp. WhatsApp encryption overview: Technical white paper. `https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf`, 2023.

[46] Daniel Williams. O2 VoLTE: Locating Any Customer with a Phone Call. `https://mastdatabase.co.uk/blog/2025/05/o2-expose-customer-location-call-4g/`, 2025.

[47] Robert Wittek. Automated Phreaking: Consolidation of VoLTE and VoWiFi Security Testing. Master's thesis, TU Wien, 2026.

[48] Paul Wouters, Daniel Migault, John Mattsson, Yoav Nir, and Tero Kivinen. Cryptographic algorithm implementation requirements and usage guidance for encapsulating security payload (ESP) and authentication header (AH). RFC 8221, Internet Engineering Task Force, 2017.

Bundesministerium Finanzen

KIRAS Sicherheitsforschung

FFG Promoting Innovation.

Contact

Contact details

SBA Research gGmbH
DI Dr. Gabriel K. Gegenhuber (project lead)
Floragasse 7, 1040 Vienna, Austria
ggegenhuber@sba-research.org
https://www.sba-research.org