

5G & Privacy

Silke Holtmanns, HAIC Talk 2023



5G Enables Many Business Cases



Source: Elisa



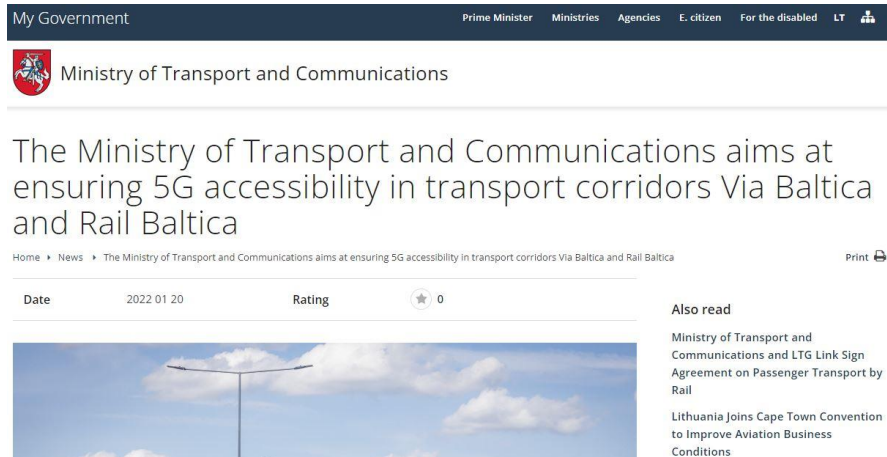
Erillisverkot starts procurement of end user devices for the broadband Virve 2.0 service

Erillisverkot starts procurement of 3GPP compliant 4G/5G end user devices to be used in Virve 2.0 service. Procurement will be done by using a Dynamic Purchasing System (DPS).

4G, 5G, PUBLIC SAFETY NETWORKS



Source: Erillisverkko



Source: <https://sumin.lrv.lt/en/news>

5G Security in the News

NEWS ITEM

Tackling Security Challenges in 5G Networks

The EU Agency for Cybersecurity (ENISA) proposes good practices for the secure deployment of Network Function Virtualisation (NFV) in 5G networks.

Published on February 24, 2022



Threat Intelligence | 8 MIN READ | ARTICLE

An Emerging Threat: Attacking 5G Via Network Slices

A successful attack against 5G networks could disrupt critical infrastructure, manipulate sensor data, or even cause physical harm to humans.



Tara Seals
Managing Editor, News, Dark Reading

June 08, 2022



TechBeacon
App Dev & Testing Enterprise IT Security GUIDES CONFERENCES [SUBSCRIBE](#)

[Home](#) / [Security](#) / [Information Security](#)
Aug 6, 2020 | Security Blogwatch

NSA warning on location tracking: 'Stop using your phone'

Richi Jennings
Your humble blogwatcher, dba RJA

The US National Security Agency, military and related roles. The guidance is "insecure."

SecurityIntelligence
[Home](#) / [Application Security](#)

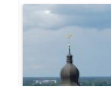
Edge Computing and 5G: Will Security Concern Outweigh Benefits?

HOME MARKETS COMPANIES OPINION SPECIALS TECH PF PORTFOLIO SHOWS

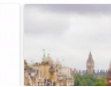
Today's Paper Latest News Economy Finance Current Affairs International Management Strategic

JUST IN Apollo, Reliance Industries consortium said to make binding bid for Boots

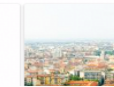
You are here: [Home](#) » [Companies](#) » News



Helsinki - Riika
€25



Helsinki - Lontoo
€49



Helsinki - Milar
€139

After United States, Canada bans China's Huawei, ZTE from 5G networks

After the US, Canada has now moved to ban Chinese telecommunication giants Huawei and ZTE from its 5G networks in order to ensure the "long term safety of our telecommunications infrastructure".

huawei 5G

NEWSLETTERS
Sign up to read our regular email newsletters

NewScientist

News Podcasts Video **Technology** Space Physics Health More [Shop](#) [Courses](#) [Events](#)

Russia and Ukraine are both weaponising mobile phones to track troops

Mobile phones ping signals to nearby communications towers, allowing both Ukrainian and Russian soldiers to track the movement of opposition forces

TECHNOLOGY 11 April 2022
By [Chris Stokel-Walker](#)

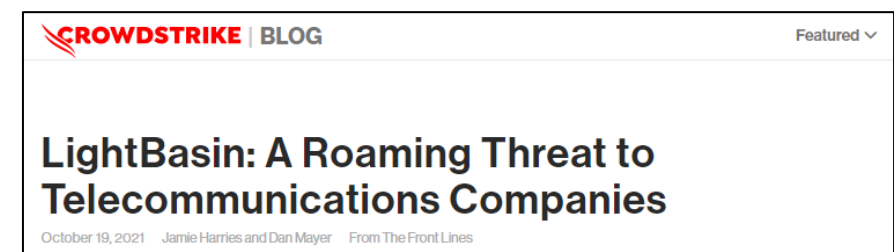
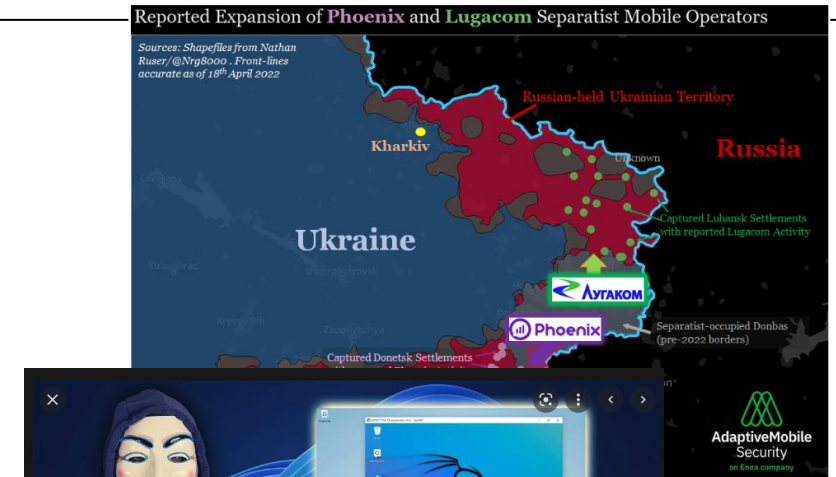
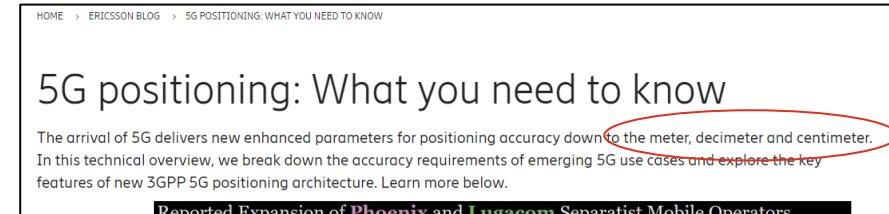
5G – What is the difference?

Key Differences To Previous Network Generations

- 5G was made for new business use cases, not for "normal users"
- 5G networks open-up (a lot of external interfaces e.g. through edge computing)
- 5G for private networks
 - As "bubble networks" (sometimes called dedicated networks)
 - As "connected to public network" e.g. finnish military
- 5G has a completely different "internal" working
 - Usage of HTTP & RestAPI (the same things you use when shopping at Amazon)
 - Interfaces for (nearly) everything
 - Cloud native is not only possible, but key enabler
 - Nearly everything can run in the cloud (and wherever)
 - User databases can be anywhere
 - Data flows can follow whatever path and are independent of the control flows for your services
- Many critical services and companies will be using 5G
 - Essential reliance on 5G

Why are 5G Networks so attractive for attackers?

- Everything is now online (amount of interesting data increased)
- 5G uses IT protocols, for which there are many hacking tools and specialized software available
- Quality of data increases with 5G e.g., location tracking in cm range
- Reliance on communication for all sectors of society
- Linkage between physical and virtual world (e.g., logistics, military)
- Attackers like nation states use telco networks for attacks for many years, but it is not commonly known
- Malware distribution and attacks using telecommunication networks e.g., using SMS or phishing calls has increased
- Mobile core networks will use legacy, IT technology and 5G specific technology, this mix opens up many opportunities to move through the network
- Complexity and insecurities allow deniability for attackers



Types of Privacy in 5G



Over-the-air privacy

- Confidentiality of your communication between your phone and the base station



Core network privacy

- Location privacy
- Communication data privacy



Cloud Privacy

- Hosting of data (including PII)



Edge and private network privacy

- Interfaces for extracting location information and steering of data flows

Privacy in 5G

Over-the-air Privacy

False Base Stations (Stingrays/IMSI-catchers) are used to:

- Intercept calls, SMS, data
- Track the permanent identifier (IMSI) and with that the user (for 2G, 3G and 4G)

Not all networks are the same!

- 2G networks -> easy to attack
- 3G networks -> a tiny bit harder
- 4G networks -> things get difficult
- 5G networks -> very hard

How it works:

- Force the phone into using a lower generation protocol

Suspected Paris Bomb Was Actually an IMSI-Catcher



Source: <https://commsrisk.com/suspected-paris-bomb-was-actually-an-imsi-catcher/>

Privacy in 5G

Core Network – Location Privacy

The backend "the core network":

- Needs to know where you are
- Can not send out "where are you messages" over the whole country e.g. when a call is incoming
- Need to evaluate where you may go to enable good handovers, even if you are in a high speed train to Oulu

5G and Location Quality

- In 4G triangulation -> not bad
- In 5G up to centimeter range

5G Location Capabilities

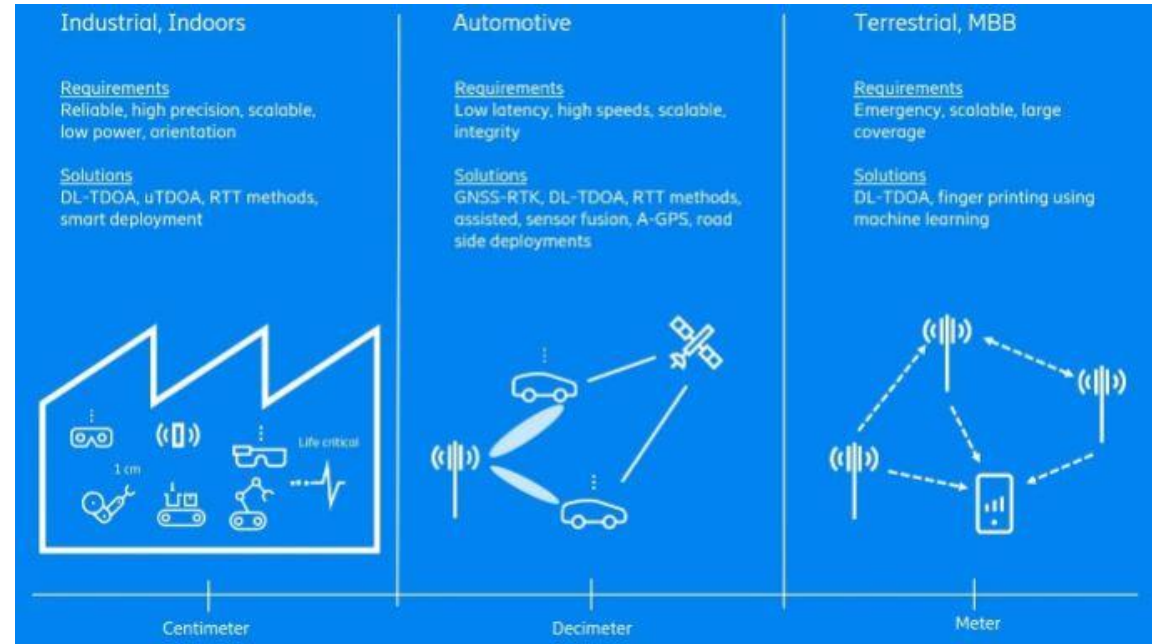


Figure 1: Requirements and specific solutions of 5G use cases with possible 5G positioning accuracy range

Source: <https://www.ericsson.com/en/blog/2020/12/5g-positioning--what-you-need-to-know>

Privacy in 5G

Core Network – Data Privacy

The backend "the core network":



- Can see all your SMS in cleartext
- Can see all your data traffic in cleartext (that is why HTTPS is a good idea when browsing and VPN for company connect)
- Can steer where your data flows (e.g. when roaming the cheapest route is chosen)
- When you roam, your data/SMS/voice goes in clear between all parties and all intermediaries over submarine or other cables

5G may encrypt the traffic between the nodes

- Including potentially user data
- Not mandatory, at operator discretion (and it costs money)
- 5G roaming data privacy **between** networks is unlikely in the near future, most of it today is still 2G protocols



Submarine communication cables crossing the Scottish shore at Scad Head on [Hoy, Orkney](#).
By The original uploader was Jmb at English Wikipedia. - Transferred from en.wikipedia to Commons., CC BY 2.5,
<https://commons.wikimedia.org/w/index.php?curid=2111378>




TOP SECRET//SI//OC//NOFORN

FAIRVIEW

FAIRVIEW DEFINED

- (TS//SI//NF) Large SSO Program involves NSA and Corporate Partner (**Transit, FAA and FISA**)
- (TS//SI//REL FVEY) Cooperative effort associated with mid-point collection (cable, switch, router)
- (TS//SI//NF) The partner operates in the U.S., but has access to information that transits the nation and through its corporate relationships provide unique accesses to other telecoms and ISPs



(TS//SI//NF)

5

TOP SECRET//SI//OC//NOFORN

(TS//SI//NF)

<https://www.propublica.org/article/a-trail-of-evidence-leading-to-atts-partnership-with-the-nsa>

5G Privacy

Cloud Privacy

5G is "cloud native":

- Meaning things are designed to be easily put into the cloud (containers in 5G and virtual machines 4G)
- Nearly everything is currently to be designed to be able to go into the cloud (even part of the antenna/base station software i.e, ORAN)
- Cloud can be anywhere (usually no location pinning)
 - Includes your user data and control data (who you called, location etc)
 - Regulators want to have cloud in EU / Fin (note private networks have different rules, depends on NIS2 implementation)
 - Lawful interception has to be run in country
- Vendors cooperate with Google, Azure, AWS but also have home-cooked cloud
- Operators, vendors, cloud provider compete on private 5G market

AWS Private 5G
Deploy, manage, and scale a private mobile network
Get started with AWS Private 5G

Google Cloud unveils private wireless network portfolio
By Linda Hardesty · Jun 14, 2022 09:00pm
Google Cloud | Celona | Rethink Wireless | Adept

Microsoft Partner
Gold Application Development
Gold Application Integration
Gold Application Lifecycle Management
Silver Data Analytics
Silver Data Platform

Ericsson
Smarter industries with Ericsson Private 5G and Microsoft Azure

Nokia
Nokia and Google Cloud partner to develop new, cloud-based 5G radio solutions
Press Release
Nokia and Google Cloud partner to develop new, cloud-based 5G radio solutions
The two companies will develop 5G solutions combining Nokia's Radio Access Network (RAN), Open RAN, and Cloud RAN, with Google's edge computing platform
Building on recent partnership announced in February, new collaboration between Nokia and Google Cloud will deliver additional 5G monetization opportunities for CSPs
15 March 2021

Privacy in 5G

Edge and Private Network Privacy

5G enables many new business cases:

- Services can "pull" information from the network e.g. data bandwidth, location, signal strength, movement direction etc using Internet style APIs
- Services can ask to "steer traffic", "add content" or "redirect"
- API security is currently not sufficient - high risk of compromise
- Slicing is a good idea, but not widely deployed and security needs improvements

Private Networks and Public Networks will be connected

- Attackers may move laterally

Source: <https://www.ericsson.com/en/service-orchestration/network-exposure>

ericsson.com	Products and solutions ^	Discover v	Transforming enterprises v	Future technologies v	About us v
5G RAN			IoT Platform		
5G Transport			Managed Services		
Core network and automation			Mission Critical Communications		
Dedicated Networks			Network Services		

How can network exposure serve 5G use cases?

The rich set of APIs allow third-party authorized applications to monitor and configure the network's behavior for a number of different subscribers (connected devices with different applications). The 5G core network expose standard APIs to the internal or external developer ecosystem to be called on and consumed by their applications and use cases.

Network exposure provides the capability to convert technical features and standardized network APIs. When addressing a developer community with limited to no telecom competence, it is important that the offered service APIs address the specific needs from developers of different industry segments.

To simplify 5G programmability for the developer communities different standard network APIs are combined into easy-to-use service APIs composed that hide the complexity of networks.

Slicing CVD

CVD-
2021

0047

Silke Holtmanns

AdaptiveMobile Security

Source: <https://www.gsma.com/security/gsma-mobile-security-research-acknowledgements/>

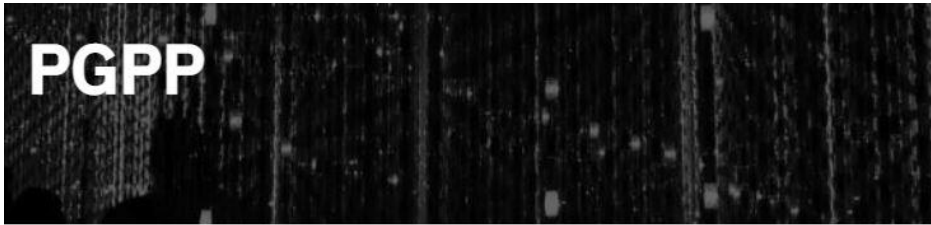
What can you do?



Improving the Air Privacy?

Pretty Good Phone Privacy (PGPP) by INVISV

The main feature of the PGPP systems is to protect the users identity against tacking on the air and by its mobile operator.



What Is Pretty Good Phone Privacy?

Mobile Network Privacy: Mobile Pro and Mobile Core

Pretty Good Phone Privacy (PGPP) is a fundamentally new type of service that gives you private mobile connectivity. In traditional mobile networks, you are identifiable by your IMSI, a permanent, globally unique identifier that is stored in your SIM card and sent to mobile towers when your phone is on. Because your IMSI never changes, and your phone connects to towers based on location and signal strength, mobile networks can track who you are and where you are located at all times. Because of this, the IMSI leaves an indelible location history, which has been used by mobile providers and numerous others, for virtually every person on the planet. IMSIs are also targeted and captured by third-party attackers using devices known as IMSI catchers, also known as Stingrays, to track a user's presence and activity in a given location.

PGPP thwarts tracking by decoupling the user from their IMSI. We created a [peer-](#)

PGPP Plan Details

Mobile Pro (\$90/mo)

- Mobile location and metadata privacy - thwarts tracking by the mobile network and others, and hides unique descriptive information that pinpoints your communication and Internet activities.
- Mobile ID changes - Provides 30 random mobile ID (IMSI) changes per month, using oblivious authentication during changes. ID changes are on demand. This decouples you as a user from each ID your phone is given, and neither INVISV nor the mobile provider know which ID you received.
- Unlimited high-speed mobile data - includes travel roaming across a wide range of countries (US/EU) and a wide range of mobile networks.
- PGPP Relay service - Provides Internet privacy utilizing the dual-hop architecture (see below), in partnership with Fastly.

Mobile Core (\$40/mo)

- Mobile location and metadata privacy - Thwarts location tracking by the mobile network and hides unique descriptive information that pinpoints your communication and Internet activities.
- Mobile ID changes - Provides 8 random mobile ID (IMSI) changes per month, using anonymous authentication during changes. ID changes are on demand. This decouples you as a user from each ID your phone is given, and neither INVISV nor the mobile provider know which ID you received.
- Moderate amount of high-speed mobile data - High-speed data up to 300 MB / day (9 GB / month), rate limited to 256 Kbps once daily limits are reached. Includes travel roaming across a wide range of countries (US/EU) and a wide range of mobile networks.
- PGPP Relay service included - Provides Internet privacy utilizing the dual-hop architecture (see below), in partnership with Fastly.

Relay (\$5/mo)

- Internet privacy utilizing the dual-hop architecture - In partnership with Fastly, this plan ensures your IP address and all your network usage on both WiFi and mobile data are decoupled, and your browsing hidden from connectivity providers including us at INVISV (unlike with a VPN).
- In the dual-hop architecture, when a user uses the Internet, the network traffic (including the name of the site and any data sent/received) is encrypted using TLS so INVISV (the first hop) and the Internet Service Provider do not know where the request is going or what it contains. The second hop, Fastly, is a content delivery network that will connect the request to its destination but will not know who it's from or the actual content of the request/browsing.
- **This plan is a supplemental privacy feature for those with existing Internet connectivity through WiFi or a mobile plan. This plan by itself does not provide mobile data service.

Confusion

But an operator needs to track the user to deliver the service????????????????????????????????

Started investigating

- identity approach of PGPP and its impact**
- location privacy of PGPP and the side effects**
- obligations of PGPP as a service provider e.g. for lawful interception and emergency calls**

For such a service to be attractive and successful, scalability, network operation impact, legal obligations, technical side effect play all an essential role

Material Used for the Analysis

- **PGPP, "What Is Pretty Good Phone Privacy",
<https://invisv.com/articles/pretty-good-phone-privacy.html>**
- **Paul Schmitt, Barath Raghavan, "Pretty Good Phone Privacy", Usenix (2021),
<https://www.usenix.org/conference/usenixsecurity21/presentation/schmitt>**
- **Paul Schmitt, Barath Raghavan, "Pretty Good Phone Privacy", (2020),
<https://arxiv.org/abs/2009.09035> This document has large overlap with the Usenix paper,**

Disclaimer, some of the functionalities I had to guess, how they would work!

First some Homework - How do things work

- Focus of PGPP is the **IMSI (International Mobile Subscriber Identity)**.
- In 5G the IMSI was replaced by the **SUPI (Subscription Permanent Identifier)**, which is basically the IMSI and some additional network information
- **IMSI and SUPI are both permanent identifier** for the subscription and relate to your SIM card, they do not change.
- For the technology purists, we actually have a UICC (Universal Integrated Circuit Card) with a USIM (Universal SIM) application on it, strictly speaking a SIM card is a 2G card and the usage of it is not allowed for 4G or 5G. But everybody calls a UICC card a SIM card, so we will not break this habit here.
- 5G is no longer using the permanent identities over the air but uses temporary identities that only reveal the home operator. **SUCI (Subscription Concealed Identifier) and 5G-GUTI (5G Global Unique Temporary Identifier)**
- Your phone has in addition its own identity and that is called **IMEI (International Mobile Equipment Identity)**

Location Areas and PGPP

- A mobile phone needs to be tracked to be able to deliver data and services through the "right" antenna. PGPP provides location privacy through "merging" of potential areas where the user might be.
- Those areas are called Tracking Areas (TA). The **Tracking Area List (TAL)** is a list of adjecant mobile network cells (i.e. area belonging to one antenna) where the user might be.
- PGPP generates a TAL list on the fly for each user in the AMF (which would be run by PGPP) by selecting **random cells and combining them to a TAL**.
- The reason, why they chose that approach is due to misuse of paging messages, but this is actually no longer true as those "bugs" were fixed by 3GPP.

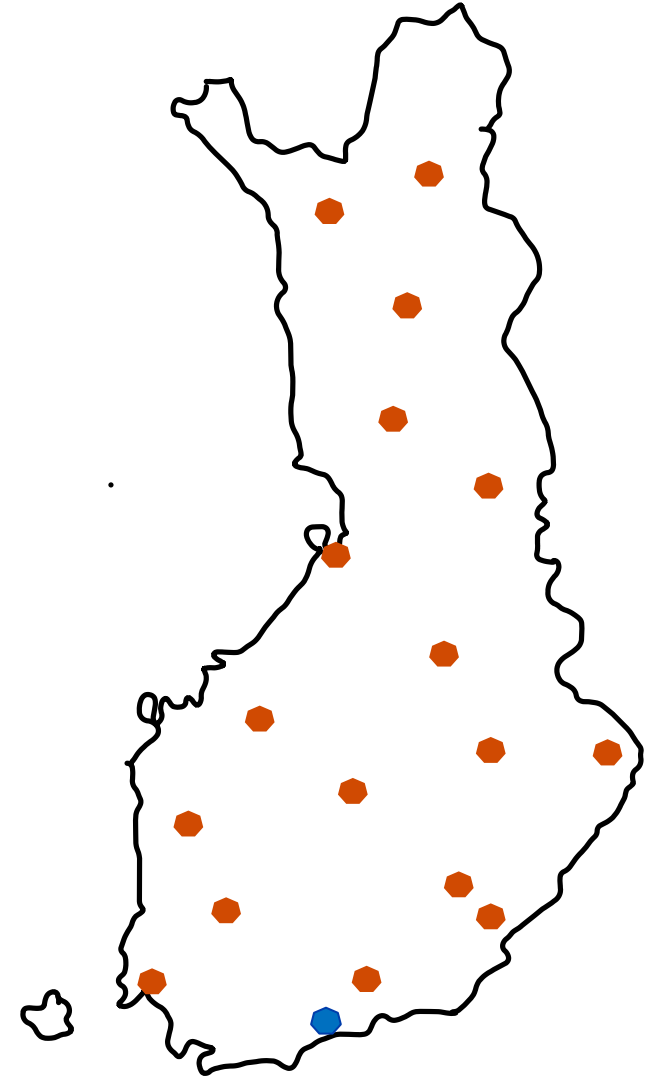


Figure: Example real (blue) and additional random tracking areas (orange) for a country like Finland

Impact from User Perspective

Air Security Impact (1/2)

Background:

- Permanent ids in plain can be used on the air interface to track users
- SIM card and operator have a shared key
- Shared key is used to derive many further keys for integrity, confidentiality, authentication.

Based on the available information from the article and Usenix conference, we could conduct three potential approaches of **PGPP for identity privacy protection**:

- (1) **all subscriptions have the same permanent identity and the same key**
- (2) **all subscriptions have the same permanent identity and different keys**
- (3) **all subscriptions have different random identities and different keys**

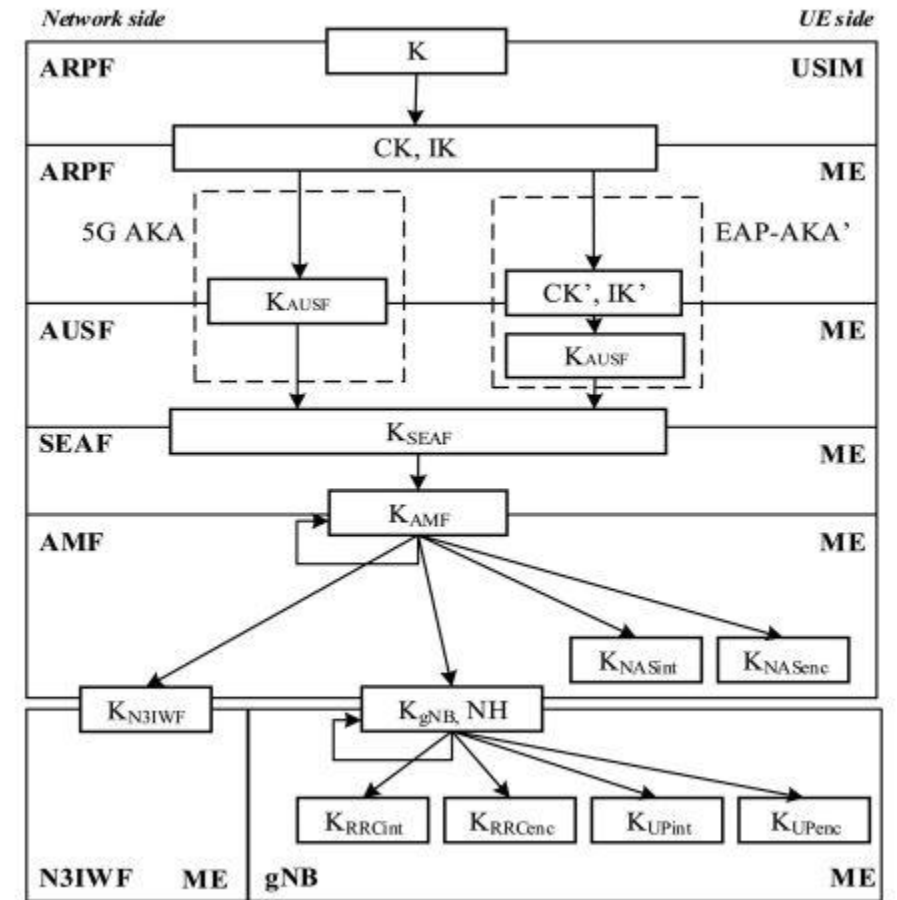
Usenix paper mentions approach (1) -> we assume that this was done also commercially

Air Security Impact (2/2)

Assumed approach: All the same key and same identity

Cryptographical issue: The key derivation parameters for the security would be nearly the same. The only parameter in the key generation process that we could identify as different was a radio channel parameter.

Potential attack might be easier to perform and the risk of brute force attacks increases. In general it is safe to say that the strength of the keys is weaker. This impact would not be the case for approaches (2) and (3) which use different keys.



Transferring Trust

Instead of trusting your operator you have to trust the privacy service provider

PS. Your operator may still track you through your IMEI (depends on phone)

PGPP Plan Details

Mobile Pro (\$90/mo)

- Mobile location and metadata privacy - thwarts tracking by the mobile network and others, and hides unique descriptive information that pinpoints your communication and Internet activities.
- Mobile ID changes - Provides 30 random mobile ID (IMSI) changes per month, using oblivious authentication during changes. ID changes are on demand. This decouples you as a user from each ID your phone is given, and neither INVISV nor the mobile provider know which ID you received.
- Unlimited high-speed mobile data - includes travel roaming across a wide range of countries (US/EU) and a wide range of mobile networks.
- PGPP Relay service - Provides Internet privacy utilizing the dual-hop architecture (see below), in partnership with Fastly.

Mobile Core (\$40/mo)

- Mobile location and metadata privacy - Thwarts location tracking by the mobile network and hides unique descriptive information that pinpoints your communication and Internet activities.
- Mobile ID changes - Provides 8 random mobile ID (IMSI) changes per month, using anonymous authentication during changes. ID changes are on demand. This decouples you as a user from each ID your phone is given, and neither INVISV nor the mobile provider know which ID you received.
- Moderate amount of high-speed mobile data - High-speed data up to 300 MB / day (9 GB / month), rate limited to 256 Kbps once daily limits are reached. Includes travel roaming across a wide range of countries (US/EU) and a wide range of mobile networks.
- PGPP Relay service included - Provides Internet privacy utilizing the dual-hop architecture (see below), in partnership with Fastly.

Relay (\$5/mo)

- Internet privacy utilizing the dual-hop architecture - In partnership with Fastly, this plan ensures your IP address and all your network usage on both WiFi and mobile data are decoupled, and your browsing hidden from connectivity providers including us at INVISV (unlike with a VPN).
- In the dual-hop architecture, when a user uses the Internet, the network traffic (including the name of the site and any data sent/received) is encrypted using TLS so INVISV (the first hop) and the Internet Service Provider do not know where the request is going or what it contains. The second hop, Fastly, is a content delivery network that will connect the request to its destination but will not know who it's from or the actual content of the request/browsing.
- **This plan is a supplemental privacy feature for those with existing Internet connectivity through WiFi or a mobile plan. This plan by itself does not provide mobile data service.

Roaming Impact

- **Roaming will likely not work with PGPP (Usenix paper states otherwise)**
- **5G Session Management Function (SMF) is a 5G Service Based Architecture entity and uses RestAPI (not diameter). The usage of a Diameter Edge Agent will not guarantee roaming interoperability.**
- **Visited network can not identify the subscriber for charging, air security and mobility:**
 - If all subscriptions have the same identifier, how would the visited network be able to differentiate between two inbound users with the same identity?
 - If the PGPP identity does not even contain the home operator name, the visited network would not even know which operator to contact for the authentication vectors. The 5G concealed identifier has for that purpose that contains the home-operator.
 - The visited operator can potentially disable authentication and confidentiality (on his own risk of course), but integrity is mandatory by the standards. Without those authentication vectors, there is no data session.
- **The visited network also would not know how to charge correctly, if there are several users with the same identity.**
- **The Policy Control Function (PCF) which enforces policies for a user (e.g. what kind of services a user can use etc), how to handle different policies for the same identity?**

SMS and Voice Calls

- There are basically two types of SMS and voice.
- Modern version using IP and the "classical" that uses telecommunication protocols (SMS over NAS).
- If PGPP is deployed then the modern version for SMS and voice calls will work as it is just another data service.
- But you will not be able to make outgoing classical voice calls or send classical SMS (SMS over NAS).
- This would require a permanent identifier i.e. (1) and (2) (one id to rule them all) would not work. If (3) random id is used, then a mapping table is needed in the core network, which would defy the idea of identity privacy coming from your mobile operator.

SIM Exhaustion

Exhausting the counter that protects against replay attacks

There is a little counter in your SIM card, it is called **Sequence Number (SQN)**

This counter needs to be in **synchronization between the network and the SIM card** (else the keys used do not match)

In PGP assume you have a large range of SIM cards with the same IMSI, then the counter is different for each of them in the SIM card. This leads to **frequent synchronization errors** between the subscriber database and the SIM cards.

There is **a re-synchronization procedure** which fixes this problem by basically jumping ahead, but the counter has a limit. In normal operation this would not be a problem, as such incidences are not that common, but if you have hundred thousands of cards with different counters, then the **counter "jumps" may become quite large and your SIM card counter might become exhausted**.

In a small set of PGP deployments, that would not be noticeable, but in a wide scaled deployment, that could become an issue.

-> Does not scale

Subscriber Database Handling Issues

For some actions in the mobile network, the subscriber database is contacted e.g. to identify which area to page the user or if he is travelling abroad.

If there are now several subscriptions with the identical identifiers, then the databases usually search and when the first match is found it is used and not the whole database is searched through.

This is simple efficiency, there exist some proprietary means to handle this kind of "special situation", but they are not standardized and it is not clear that they would work in this case.

Therefore, when such a request is made to the database, the chances are high the "wrong" user is identified.

Emergency Calls

In an emergency situation you may want to let the responders know, where you actually are.

If you make an emergency call (note, that classic voice call may not work), then your operator would have several subscription identifiers with that are the same, but with different locations.

The found granularity of the locations will no longer be very good (PGPP merges areas to make it harder).

The only way out of this would be for the PGPP operator (who is in control of at least some part of the AMF) and the mobile operator to switch off PGPP for emergency calls.

This then poses the question, if the mobile operator can switch of PGPP and we consider him untrusted, what would stop the mobile operator not to switch it off at some other time?



Impact from Operator Perspective

Fraud Risk

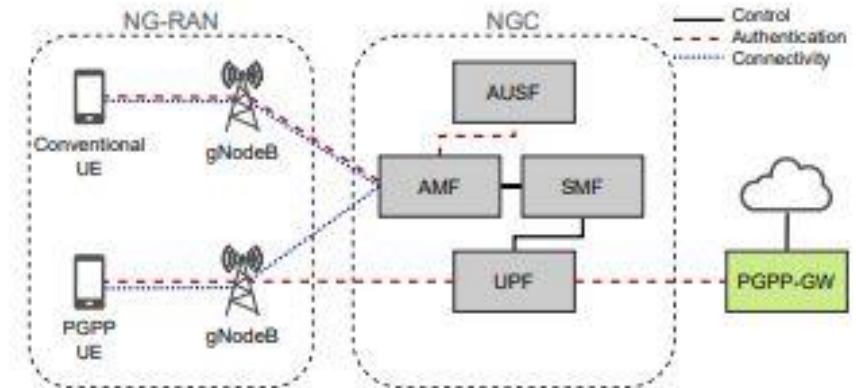


User authenticates only to PGPP Gateway.

The UPF is configured to have a fixed tunnel to a PGPP-GW, which can be located outside of the PGPP operator's network.

There is no linkage between the data session and the PGPP gateway authentication.

- How would the operator know that you are an authorized user for the data service, the operator may need to support an additional interface to verify that the user has authenticated to the gateway.
- How to make sure that the user is really going through the right PGPP gateway, once he got the IP address.
- How to create charging data reliably?



Impact of Random Tracking Areas (1/2)

Connectivity Impact

Tracking Area List (TAL) contains the area where the user really is and some adjacent areas where the user might or soon might be. This enables fast handovers and reachability, even if you are in a fast train.

In PGPP those that list is a random list. Therefore, if you move fast and have an incoming message, the cell where you are that moment will not send a paging message i.e. **you will not get the message.**

The original TAL area idea is also to avoid frequent area updates.

PGPP tested some approach with grouping base stations, but that then increases the overall amount of cells that are part of the TAL.

Impact of Random Tracking Areas (2/2)

Network Load Impact

Large TALs **increase the control traffic amount** in the core network e.g. more area updates.

PGPP inventors studied the impact of the increased load and its impact on the amount of users each base station can handle.

There it was quite clear, that the larger the tracking areas are the **less users each base station can handle**.

When using widely PGPP a **mobile operator would need to place more base stations** to compensate this effect without having any benefit from this himself.

Impact of Random Tracking Areas (2/2)

Energy Consumption vs Privacy

Random **TAL list results in much more area updates**

Many messages in the network and on the air interface, both **increase energy consumption.**

When there is the need to contact the user then all the base stations in the tracking area list need to send out a paging message.

Due to the design the network would not know which of the areas would be the one where the user really is.

In PGPP the TAL list is supposed to be as large as possible to provide good location privacy, the larger the areas are, the higher the energy consumption for paging messages.

Legal Considerations

Not a lawyer !! – but this may cause some issues

Mobile operators are obliged in many countries to reveal the location of a suspect based on an authorized government request. Typically, the governmental agencies utilize the phone number, IMEI or IMSI of the suspect through dedicated lawful interception interfaces.

If now PGPP is used, this may cause difficulties for the mobile operator to fulfil his duty. The mobile operator would not be able to use the IMSI/SUPI for user identification and also could not provide the location of the user.

The duty of supporting the governmental agencies may then fall upon the PGPP to provide then the real user location and identity.

We did not find any suggestion in the PGPP material how to handle this kind of situation or what would be a potential responsibility split between mobile operator and the PGPP partner.

Inventing the wheel twice?

PGPP claims to rectify errors and oversights made by the 3GPP

5G has many improvements to protect against location tracking over the air interface were made, many of those were not considered by PGPP. <https://www.ericsson.com/en/blog/2019/5/fighting-imsi-catchers-5g-cellular-paging-privacy>

If features are used by operator, they make many things of PGPP obsolete (if you trust your operator)

The **air interface then no longer uses a permanent identifier**, but uses instead several changing temporary identifiers (SUCI/5G-GUTI).

PGPP paper seems to assume that the SUPI (5G Subscription Permanent Identifier) is used the same way as the IMSI. This is actually not the case. They claim, that SUPI based paging i.e. the permanent identifier is broadcasted and then the "right" phone answers is a risk. But this possibility has been removed by 3GPP in 2018 https://www.3gpp.org/ftp/tsg_ran/WG2_RL2/TSGR2_AHs/2018_07_NR/Docs/R2-1809621.zip

5G introduces a concealed identifier that replaces the SUPI and supports roaming. For the air interface new temporary short-lived identifiers were introduced to avoid tracking the users. It should be mentioned, that those measures are only effective, **if the network is supporting all those features and has a 5G core network.**

Summary

There are many privacy risks in 5G

Location privacy is only one of them

PGPP is good research, but assumed implementation has quite many side effects and the latest standardization efforts are not taken into account

What you can do?

- If you are a private user:
 - Check out security news about your provider
 - Check out if they publish security certifications
 - Read the fine print of marketing, is the core also 5G (location privacy needs a 5G core?)
- If you are a business user:
 - Service Level Agreements !!
 - Certifications and compliance proof (e.g., EU 5G Toolbox)

Thank you

pwc.fi

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers Oy, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2022 PricewaterhouseCoopers Oy. All rights reserved. Not for further distribution without the permission of PwC. “PwC” refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm’s professional judgment or bind another member firm or PwCIL in any way.