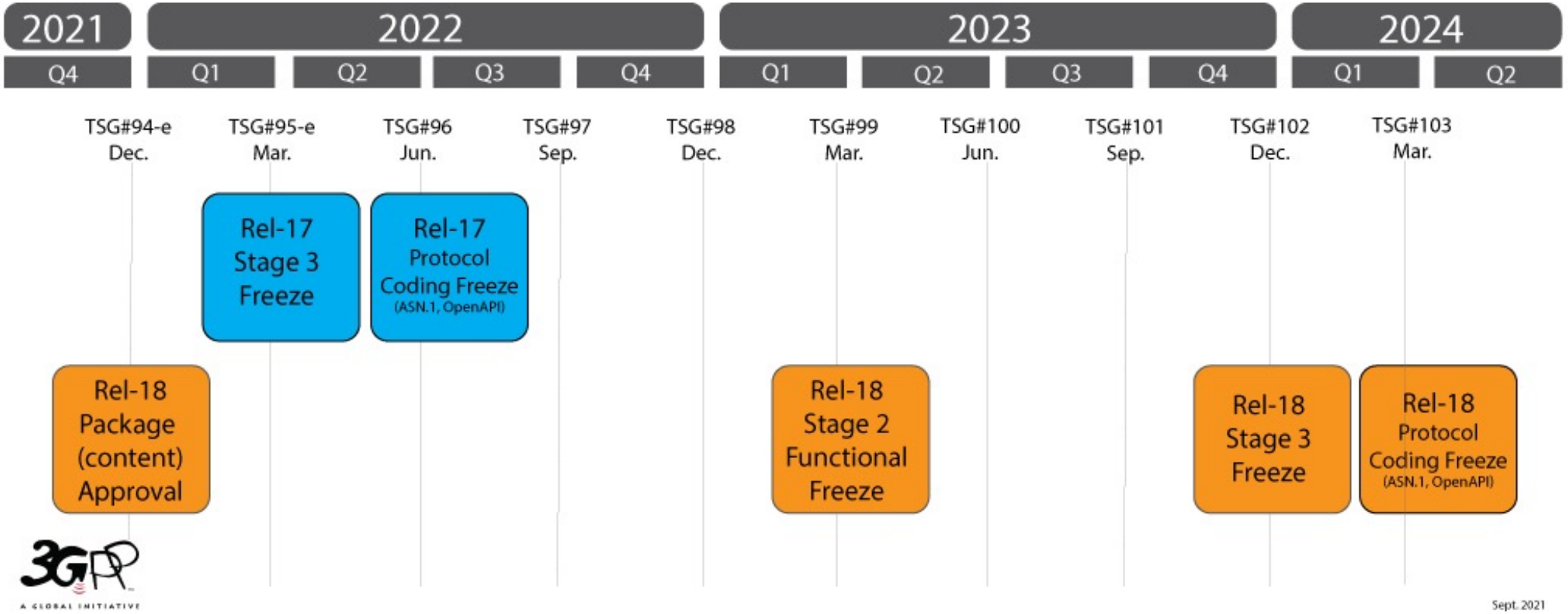
5G Security Update

Human Rights Protocol Considerations, IETF 113, Vienna, John Preuß Mattsson, Ericsson

3GPP Generations and Releases

— 3GPP operates in generations every 10 years (2G, 3G, 4G, 5G, 6G), half generations every 5 years (GPRS, HSPA, LTE Advanced, 5G Advanced), as well as releases every 1-2 years.
— Most 2G and 3G networks globally will be phased out by 2025.
— 3GPP is currently working on Rel-17 and Rel-18



Battle Against IMSI catchers

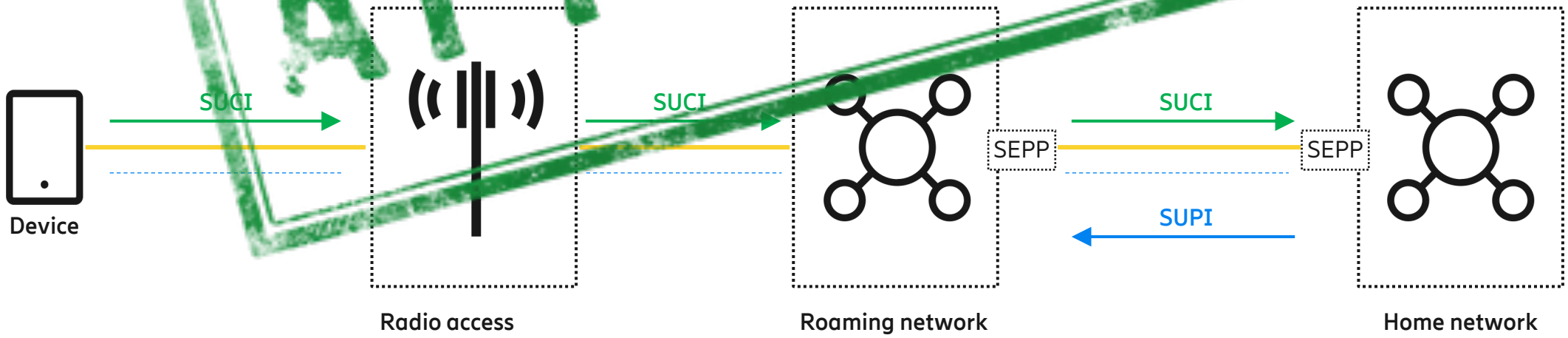
5G: An End to the Battle Against False Base Stations?

Many mitigations against false base stations are part of the 5G standard.

- Encryption of permanent identifier
- Strict refreshment of temporary identifier
- Decoupling of permanent identifier from the paging mechanism
- Integrity protection of user plane traffic
- Secure radio redirections
- False base station detection

Most important is encryption of permanent identifiers. When this is enabled the permanent identifier is never sent in clear over the air.

- Encryption is done using a public key stored in the device. Uses state-of-the-art cryptography like Curve25519.
- In 5G, the long-term identity is called SUPI. SUPI is often an IMSI. An encrypted SUPI is called SUCI.

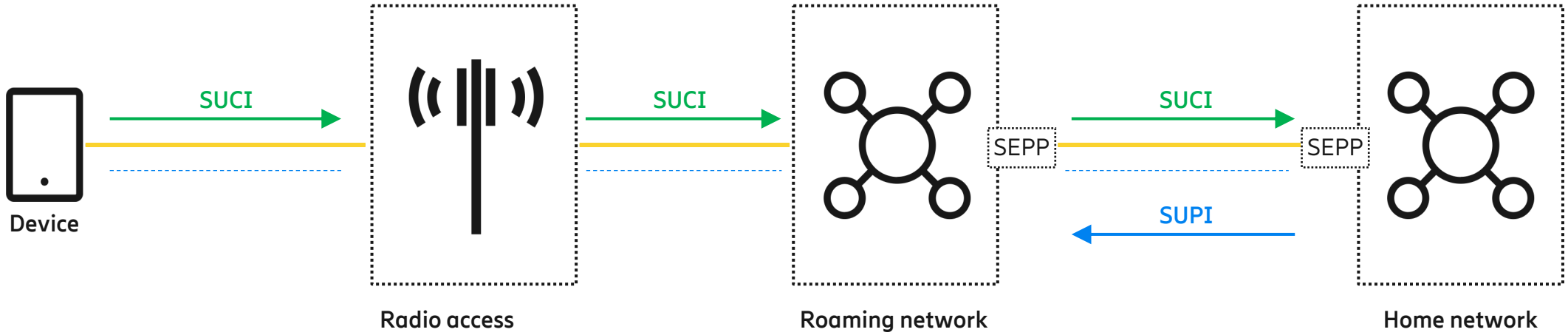


An End to the Battle Against False Base Stations?

- Encryption of permanent identifier is mandatory to support but optional to use, which is not considered best practice anymore.
  - Likely that SUCI encryption will be widely used in large parts of the world. Check with your home operator.

- An IMSI consist of Mobile Country Code (MCC), Mobile Network Code (MNC), and a Mobile Subscription Identification Number (MSIN). Only the MSIN is encrypted. When a NAI (username@realm) is used, only the username is encrypted. This is similar to the @realm in the IETF standard Extensible Authentication Protocol (EAP).
  - A roaming user may therefore be tracked or identified by eavesdropping on MCC+MNC or @realm.
  - Hard problem to solve. Realm is needed for routing. More academic research would be welcome.

- With secure radio redirections an attacker cannot easily trick a connected phone to downgrade to 4G, 3G, or 2G.
  - However, the phone may initially connect to a false 2G base station and an attacker might jam 5G frequencies.
  - Android 12 introduced a 2G kill switch. This is is great news. I have been requesting this for a long time.



Recent Tracking of Mobile Identities

Spying Cell Towers May Be Spread Across **US**

Tom's Guide - 3 Sep 2014

Also known as "**IMSI catchers**," they're used by law enforcement in many ... "A lot of these interceptors are right on top of **U.S. military bases**," Goldsmith told ...

Phone Firewall Identifies Rogue Cell Towers Trying to ...

In-Depth - Wired - 3 Sep 2014

Daily Mail

Russian spies are tracking British former special forces teams by their mobile numbers

Russia has been using phone data captured by its spies operating in the UK to target British former special forces teams in Ukraine.

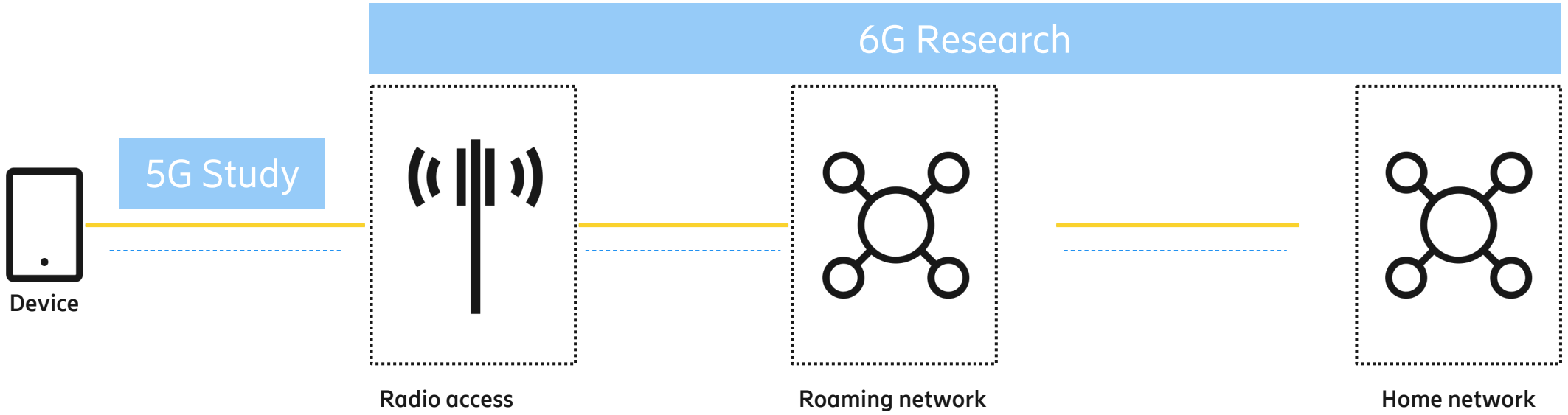
New Studies on Privacy of Identifiers in 5G and 6G

Ongoing 3GPP Rel-18 study on privacy of identifiers over radio access in 5G.

- 5G has many kinds of identifiers (SUCI, S-NSSAI, 5G-GUTI, CAG Identifier, C-RNTI) and parameters transmitted over the air.
- Study will investigate possible privacy attacks using 3GPP identifiers and suggest potential remeditions.
- One issue is variable-length NAIs (e.g., john.mattsson@ericsson.com) highlighted in the paper "Nori: Concealing the Concealed Identifier in 5G".
- Another issue is attackers linking identifiers transmitted over radio access with each-other, with other long-term identifiers, or with other information such as location and time, potentially using novel methods such as AI/ML.

Ongoing research on how to minimize any privacy sensitive identifiers and parameters in 6G network nodes.

- Privacy sensitive identifiers and parameters should be shared and stored on an as-needed basis.



Zero Trust Architecture Inside and Between Networks

Service Based Architecture (SBA) and Interconnect Security (N32)

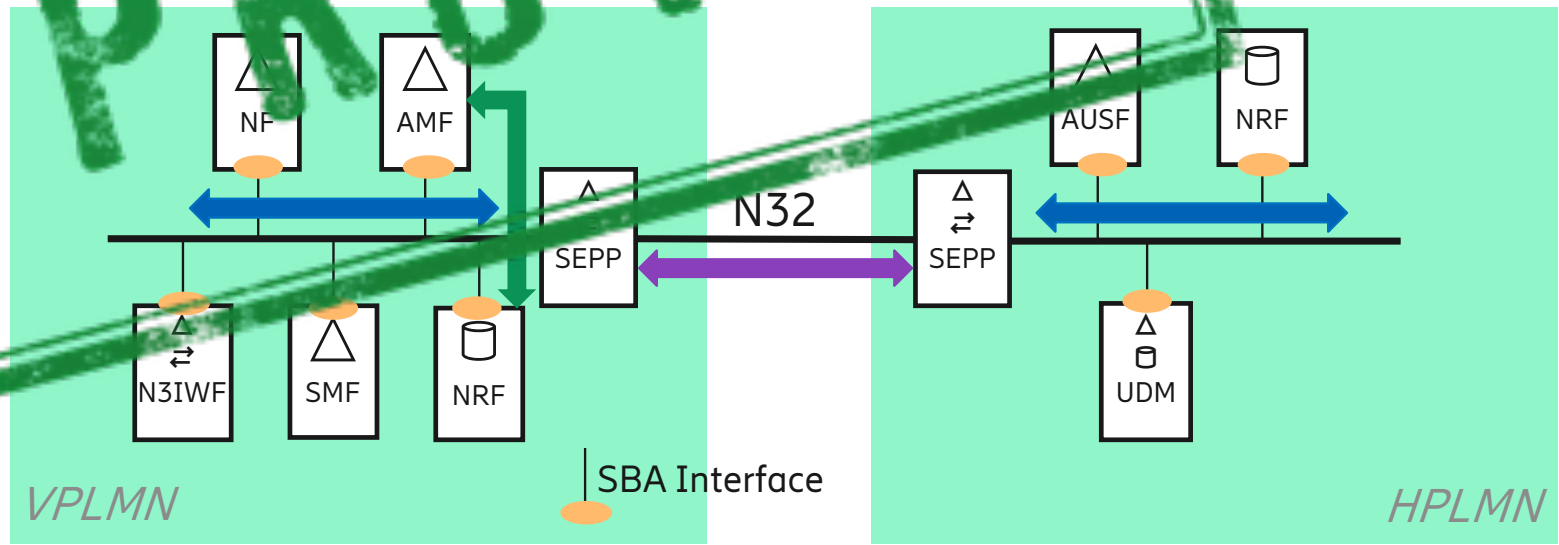
Zero Trust Architecture: SBA and N32 security for communication inside and between core networks. Takes threats from legacy interconnect networks into account from the start.

Interconnect Provider gets information on a need-to-know basis. Modifications made during interconnect are logged and signed.

TLS 1.3 with mutual authentication is mandatory to support for all Network Functions.

OAuth2.0 is mandatory to support for access authorization in SBA.

JSON Object Signing and Encryption (JOSE) are used for N32 application layer security.



Limiting Impact from Compromised Long-term Keys with PFS and Diffie-Hellman

Limiting Impact from Compromised Long-term Keys

Report: **Spies Stole** SIM Encryption **Keys**
BankInfoSecurity.com - 21 Feb 2015
A British-American intelligence team hacked into Gemalto, the world's largest maker of SIM cards, resulting in the theft of numerous encryption **keys** for the cards ...

How American and British **spies** hacked the world's largest ...
Quartz - 20 Feb 2015

The NSA Has the Master **Key to** Unlock Your Phone's Messages
Gizmodo - 19 Feb 2015

Sim card database hack gave US and UK **spies** access to ...
In-Depth - The Guardian - 20 Feb 2015

Questions About the Alleged Gemalto Hack
Blog - Wall Street Journal (blog) - 20 Feb 2015

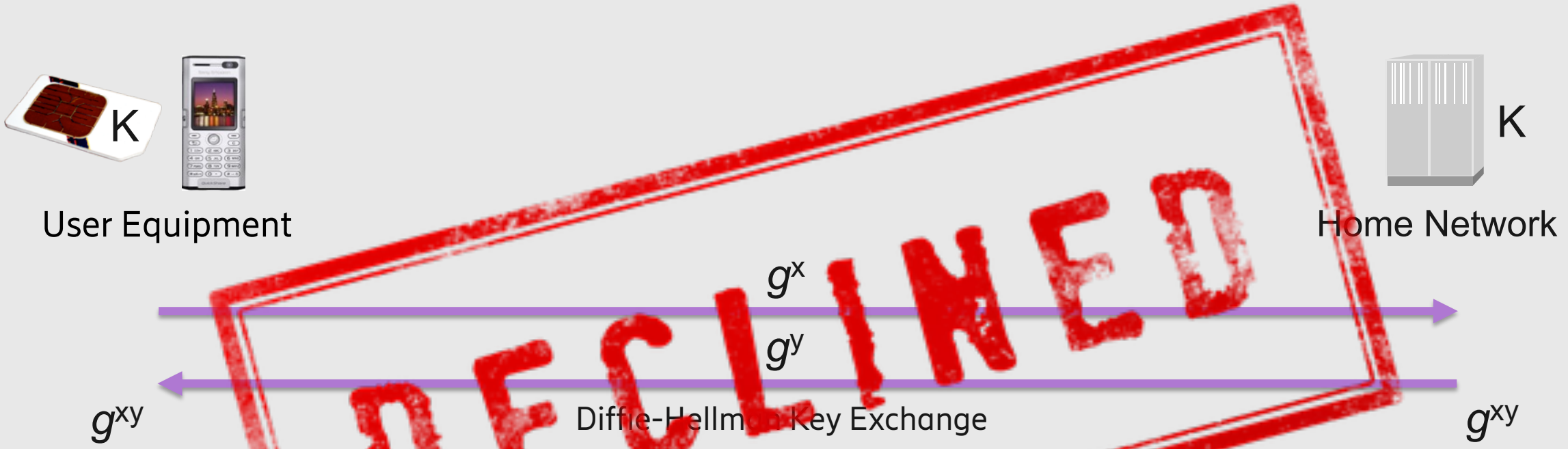
Mobile phones hacked: can the NSA and GCHQ listen to all ...
In-Depth - The Guardian - 20 Feb 2015

The Conversation

Gemalto hack shows
how far we are from
deciding acceptable 'security norms'

This “great SIM heist”
targeted Gemalto because
it produces billions of mobile phone SIM cards for 450 telecoms providers w…

What is PFS and Diffie-Hellman and How Do They Help?



- With Perfect Forward Secrecy (PFS), compromise of long-term keys does not lead to compromise of past session keys. Often achieved with Ephemeral Diffie-Hellman which also mitigates future passive attacks.
- Many older security protocols do not have PFS. In 5G, EAP authentication can be used for all types of access. Private 5G networks can use **EAP-TLS**. Ongoing work in IETF and 3GPP to define **EAP-AKA with PFS**. This effectively mitigates pervasive monitoring.
- For SBA and N32, 5G core networks support TLS 1.3 which always use Ephemeral Diffie-Hellman.

The Great SIM Heist and Forward Secrecy

- *"The great SIM heist was a disaster for cellular security. The extension of the heist is not known, and the report from Gemalto was a joke trying to sweep thing under the rug. Potentially billions of secret keys where compromised, enabling pervasive monitoring on a global scale. The heist did not only enable tracking of users, but also passive eavesdropping of communication from these devices as well as installation of malware."* https://mailarchive.ietf.org/arch/msg/emu/mc3iCXqsjbPgu2NK1usxdO_vtC8/

- Unfortunately, the proposal *"New KI: Existing authentication procedure lacking the PFS property"* to address this significant weakness and add forward secrecy to 5G-AKA was **objected by companies from France, UK, and US. No technical reasons were given.** Support from Swedish, Finish, Chinese, German, and US companies. https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_97_Reno/Report/MeetingReport__SA3_97.docx

- To use the terminology be Keith Martin, there is no mechanism for access authentication in public 5G networks with *"acceptable security norms"*. There is also no authentication mechanisms compliant with zero-trust principles.

- Ericsson is currently driving EAP-AKA-FS in IETF EMU but it is currently only approved for private networks.

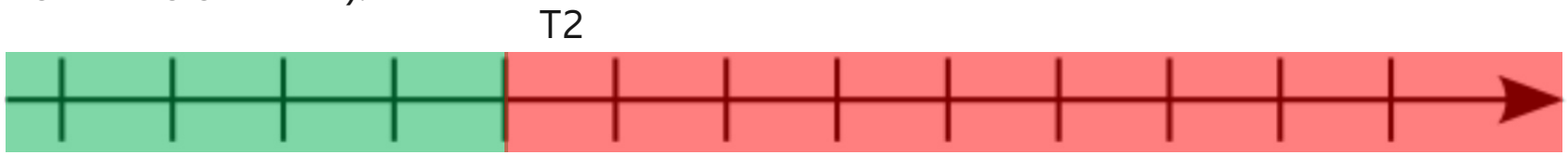
Access Authentication in 5G

- Access authentication in 5G is called primary authentication while the term secondary authentication is used for user connections to set up user plane connections to data networks outside of the mobile operator domain.
- Public 5G networks are the traditional type of mobile networks. Private 5G are indented to be used by a single enterprise or organization such as industrial facilities, hospitals, ports, and other mission-critical infrastructure.
- While the term SIM card is often used in popular media, the USIM is technically just an application that can reside on a removable UICC, an embedded UICC, or integrated in a Trusted Execution Environment (TEE).

	Client Identity Protection	Forward Secrecy / Zero Trust	Authentication	Primary Authentication
5G-AKA	Optional	Not supported	PSK (stored in USIM)	Public or Private
EAP-AKA'	Optional	Not supported	PSK (stored in USIM)	Public or Private
EAP-AKA-FS	Optional	Mandatory	PSK (stored in USIM)	Private
EAP-TLS 1.2	Optional and slow	Optional	Certificate	Private
EAP-TLS 1.3	Mandatory	Mandatory	Certificate	Private
EAP-TTLS 1.2	Mandatory	Optional	Anything	Private
EAP-TTLS 1.3	Mandatory	Mandatory	Anything	Private

Current Best Practice for Diffie-Hellman

- **Forward secrecy only limits the effect of key leakage in one direction** (compromise of a key at time T2 does not compromise some key at time T1 where T1 < T2).



- Protection (from passive attackers) in the other direction (compromise at time T2 does not compromise keys at time TX) can be achieved by rerunning EC(DHE).

- Using the terms in RFC 7624 *"Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement"*, forward secrecy without rerunning EC(DHE) does not stop an attacker from doing **static key exfiltration**. Frequently rerunning EC(DHE) forces an attacker to do **dynamic key exfiltration (or content exfiltration)**.
  - Static key exfiltration (transfer of keys happens once or rarely)
  - Dynamic key exfiltration (transfers of keys happens frequently)
  - Content exfiltration (transfer of content instead of keys)

- **Forcing attacker to do dynamic key exfiltration (or content exfiltration) should be considered best practice.** This significantly increases the risk of discovery for the attacker. **RFC 7624 (2015) is great and should be referenced and followed much more.**

Current Best Practice for Diffie-Hellman

- **Assuming breach (e.g. key exfiltration) and minimizing the impact from breach is an essential part of zero-trust.**
  - *"The Zero Trust security model assumes that a breach is inevitable or has likely already occurred"* https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF
  - *"If a breach does occur, minimizing the impact of the breach is critical."* https://www.google.com/search?channel=crow5&client=firefox-b-d&q=limit+impact+of+breach+zero+trust
- ANSSI (France) (2015) recommendation for IPsec is to rerun ephemeral Diffie-Hellman at least every hour or every 100 GB. Nothing special about IPsec. **This should be considered best practice for all non-constrained protocols and systems.**

R12

If available, one shall activate the PFS property in IKEv2 second phase (a.k.a "quick mode") using a Diffie-Hellman key exchange or its elliptic curve variant.

R13

It is recommended to force the periodic renewal of the keys, e.g. every hour and every 100 GB of data, in order to limit the impact of a key compromise.

- The Double Ratchet Algorithm enables frequent Diffie-Hellman in the Signal protocol.

Current Best Practice for Diffie-Hellman

- How is TLS 1.3 (RFC 8446) (2018) doing? Not so great actually. The psk_ke marked as "Recommended = Y" do not offer client identity protection or forward secrecy. TLS 1.3 removed the possibility to frequently do ephemeral Diffie-Hellman in long-lived connections. **The KeyUpdate mechanism only gives forward secrecy.**

Value	Description	Recommended	Reference
0	psk_ke	Y	[RFC8446]
1	psk_dhe_ke	Y	[RFC8446]

3GPP have forbidden cipher suites without forward secrecy in (D)TLS 1.2. Allowed again in (D)TLS 1.3 as it is "recommended by the IETF". **IETF needs to be better at labelling everything weak as "NOT RECOMMENDED".**

- RFC8446bis will have considerations regarding key exfiltration and frequently rerunning EC(DHE) after merging a PR suggested by me. **Frequent ephemeral Diffie-Hellman can be achieved by frequently setting up new connections.** https://github.com/tlswg/tls13-spec/commit/d80dbfff912f5520ae5bd2ec6a7126c1dc54dd13

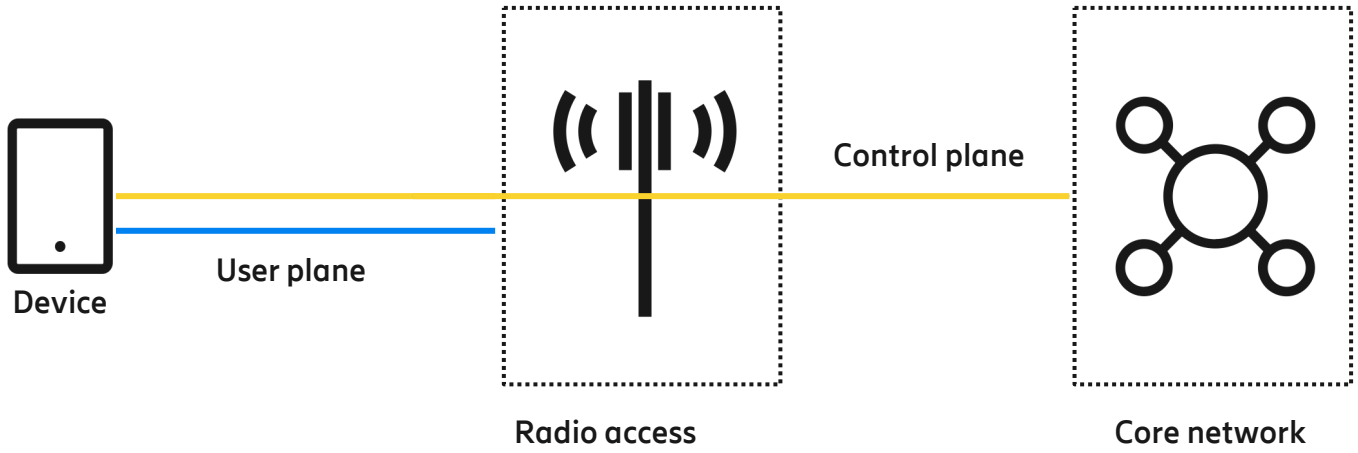
- TLS 1.3 is used in much more than just the Web. (D)TLS connections lasting many months are not uncommon. Setting up new connections is easy in some cases, hard in others. **Use of (D)TLS 1.3 still require strict profiling.**
  - EAP-TLS 1.3 (RFC 9190) forbids use of psk_ke and cipher suites without confidentiality.
  - RFC6083bis (DTLS over SCTP) used in 3GPP will be redesigned to enable frequently setting up new DTLS 1.3 connections with ephemeral Diffie-Hellman.
  - Likely more deployments than RFC6083 in 3GPP where setting up new connections is problematic.

Authenticated Encryption in User Plane

Authenticated Encryption in User Plane

- In 2G, both control and user plane used unauthenticated encryption.
- In 3G and 4G, the control plane use authenticated encryption while the user plane use unauthenticated.
- From 5G release 16 onwards, support for full rate User Plane integrity protection is mandatory to support but optional to use.

- Authenticated encryption is not only needed for integrity protection but also to provide acceptable confidentiality. Unauthenticated encryption does not protect against adaptive chosen-ciphertext attacks which is best practice.
  - Most user plane data is protected on the transport or application layer using e.g., HTTPS.



3GPP/GSMA Algorithms

— All weak 3GPP algorithms are from the 2G generation.
— ETSI SAGE will soon publish new 256-bit high-performance software friendly algorithms for later 5G releases and 6G.

Cipher	Proprietary	Proprietary	Proprietary	AES	Keccak
Input key size	128	128	128	128	128, 256
Output key size	54	54	64	128	128, 256
Name	COMP-128-1	COMP-128-2	COMP-128-3	MILENAGE	Tuak

Figure 1: 3GPP/GSMA algorithms for authentication and key generation - Green algorithms are secure while red algorithms only offer 64-bit security or less.

Cipher	Proprietary	Proprietay	KASUMI	KASUMI	KASUMI	SNOW 3G	SNOW 3G	AES	AES	ZUC	ZUC
Key size	64	64	64	128	128	128	128	128	128	128	128
Mode	XOR	XOR	f8-mode	f8-mode	CBC-MAC	XOR	CW-MAC1	CTR	CMAC	XOR	CW-MAC2
Type	ENC	ENC	ENC	ENC	INT	ENC	INT	ENC	INT	ENC	INT
Tag size					32		32		32		32
GSM	A5/2	A5/1	A5/3	A5/4							
GPRS	GEA1	GEA2	GEA3	GEA4	GIA4	GEA5	GIA5				
UMTS				UEA1	UIA1	UEA2	UIA2				
LTE						128-EEA1	128-EIA1	128-EEA2	128-EIA2	128-EEA3	128-EIA3
NR						128-NEA1	128-NIA1	128-NEA2	128-NIA2	128-NEA3	128-NIA3

Figure 2: 3GPP/GSMA algorithms for encryption and integrity protection - Green algorithms are secure while red algorithms only offer 64-bit security or less.

User Consent in Mobile Networks

User Consent in Mobile Networks

- Under the GDPR (and other privacy laws around the world), consent must be freely given, specific, informed, unambiguous, and retractable.
- Many applications and use cases in the 5G system require the storage and processing of user data. In such cases, user consent is required.
- 3GPP TR 33.867 studies user consent and gives recommendations for some use cases.
- Conclusion that user consent parameters are stored as subscription data in the 5G core. Not perfect, but a good tradeoff.
- Current implementation of EU "cookie law" has a lot of disadvantages (horrible pop-ups that the users click past without reading, geo-blocking).

References

- IRTF 106 HRPC 5G Security, false base stations and IMSI catchers, and the great SIM heist and the need for PFS
  https://datatracker.ietf.org/meeting/106/materials/slides-106-hrpc-5g-presentation-00
- 3GPP TS 33.501 Security architecture and procedures for 5G System
  https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169
- EMnify, Global 2G and 3G Phase Out / Sunset: What Do We Know So Far?
  https://www.emnify.com/blog/global-2g-phase-out
- EFF, VICTORY: Google Releases “disable 2g” Feature for New Android Smartphones
  https://www.eff.org/deeplinks/2022/01/victory-google-releases-disable-2g-feature-new-android-smartphones
- 3GPP SP-211364 New WID for Study of privacy of identifiers over radio access
  https://www.3gpp.org/ftp/Information/WI_Sheet/SP-211364.zip
- 3GPP TR 33.870 Study of privacy of identifiers over radio access
  https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3977
- Prueß Mattsson, Nakarmi, “Nori: Concealing the Concealed Identifier in 5G”
  https://arxiv.org/pdf/2105.10440.pdf
- 3GPP Meeting Report for TSG SA WG3 meeting: 97
  https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_97_Reno/Report/MeetingReport__SA3_97.docx
- IETF EMU Mailing list, Re: [Emu] EAP-AKA' and Re: WG adoption call for draft-arkko-eap-aka-pfs
  https://mailarchive.ietf.org/arch/msg/emu/mc3iCXqsjbPgu2NK1usxdO_vtC8/

References

— IETF RFC 7624 Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement
https://datatracker.ietf.org/doc/html/rfc7624

— ANSSI Recommendations for securing networks with IPsec
https://datatracker.ietf.org/doc/html/rfc9190

— IETF RFC 9190 EAP-TLS 1.3: Using the Extensible Authentication Protocol with TLS 1.3
https://datatracker.ietf.org/doc/html/rfc9190

— IETF draft-ietf-emu-aka-pfs Forward Secrecy for the EAPl Method for Authentication and Key Agreement (EAP-AKA' FS)
https://datatracker.ietf.org/doc/html/draft-ietf-emu-aka-pfs

— Ericsson, A summary of 3GPP Release 16, 5G phase 2: Security and RAN
https://www.ericsson.com/en/blog/2021/4/3gpp-release-16-5g-phase-2-security-ran

— Ericsson, The evolution of cryptography in mobile networks and how to secure them in the future
https://www.ericsson.com/en/blog/2021/6/evolution-of-cryptographic-algorithms

— Ericsson, User consent in telecom and 3GPP standardization
https://www.ericsson.com/en/blog/2020/11/5g-privacy-user-consent-3gpp

— 3GPP TR 33.867 Study on user consent for 3GPP services
https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3824