5G-ENSURE

(Project Number— 671562)

Privacy Enablers

madalina.baltatu@telecomitalia.it

luciana.costa@telecomitalia.it

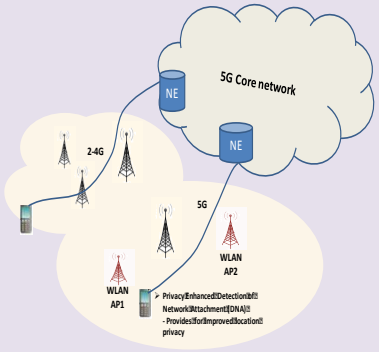
dario.lombardo@telecomitalia.it

Privacy Enablers

Privacy enhanced identity protection

Provide protection against identity disclosure (and, consequently, unauthorized user tracking), by preventing or making more difficult IMSI catching attacks.

Device identifier(s) privacy

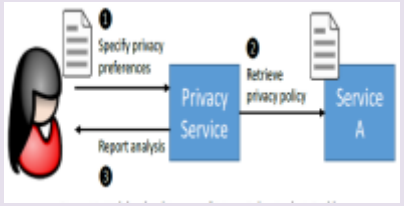


Limit exposure of device identifiers and prior points of attachment, and therefore, limit the ability to track a device.

SIM or Device-based Anonymization

Provide anonymization techniques on the user's device or UICC (SIM), offering protection against disclosure of sensitive information stored mainly on the SIM.

Privacy Policy Analysis

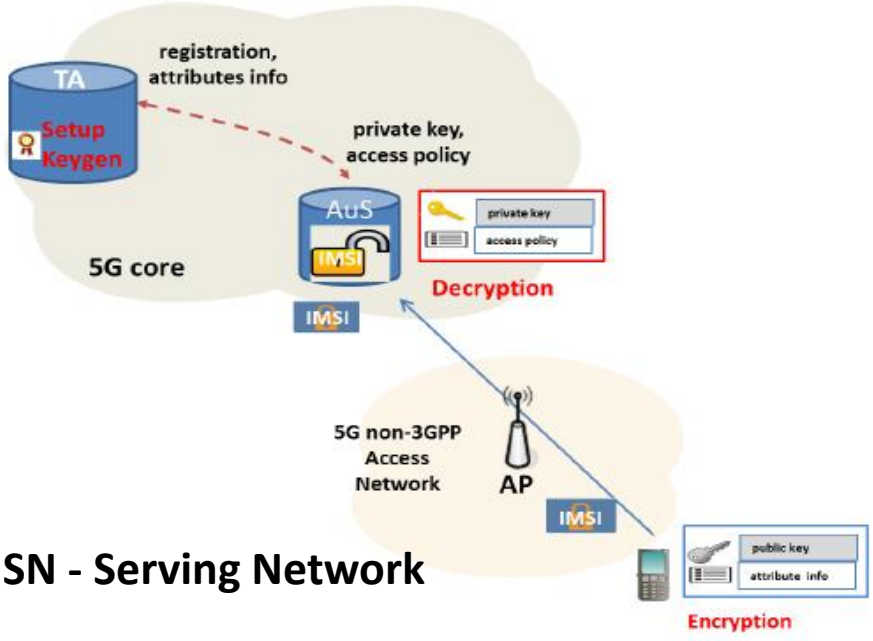


Enables users to analyse the privacy policy of a service and compare it to their pre-defined preferences at app install time or 5G connection time

Privacy enablers - Open Specification

Privacy Enhanced Identity Protection (R1)

SN-centric approach

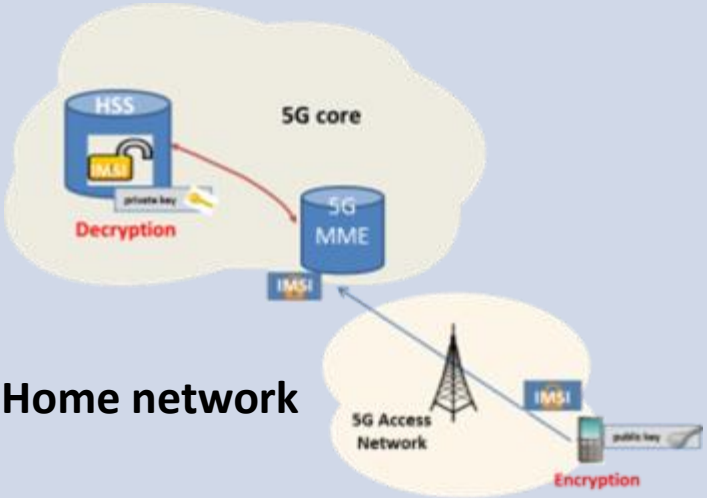


SN - Serving Network

ABE-based serving network centric IMSI encryption scheme to encrypt and decrypt a given IMSI at the SN without any assistance of HN. Entire IMSI is protected.

Privacy Enhanced Identity Protection (R2)

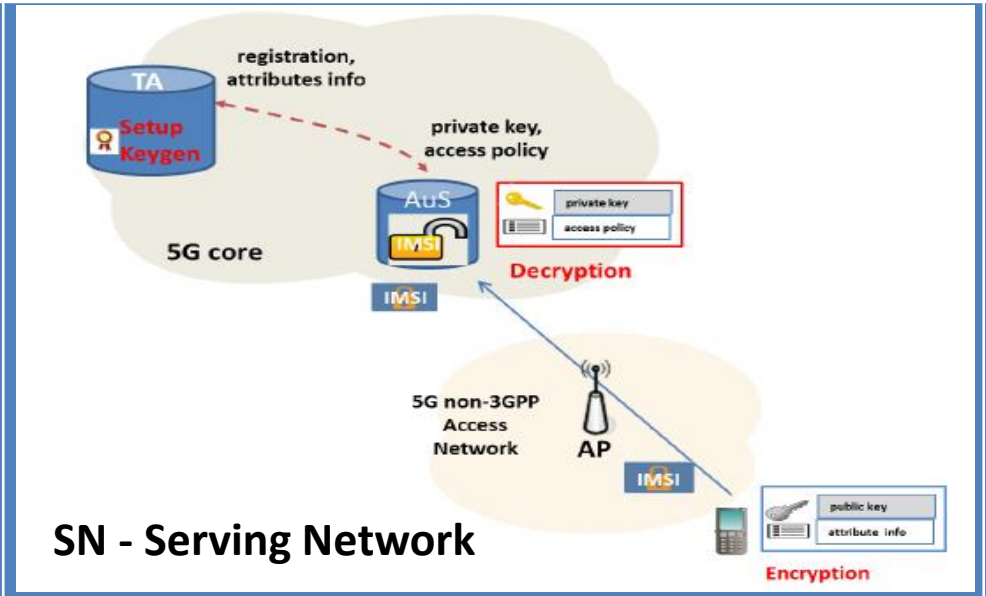
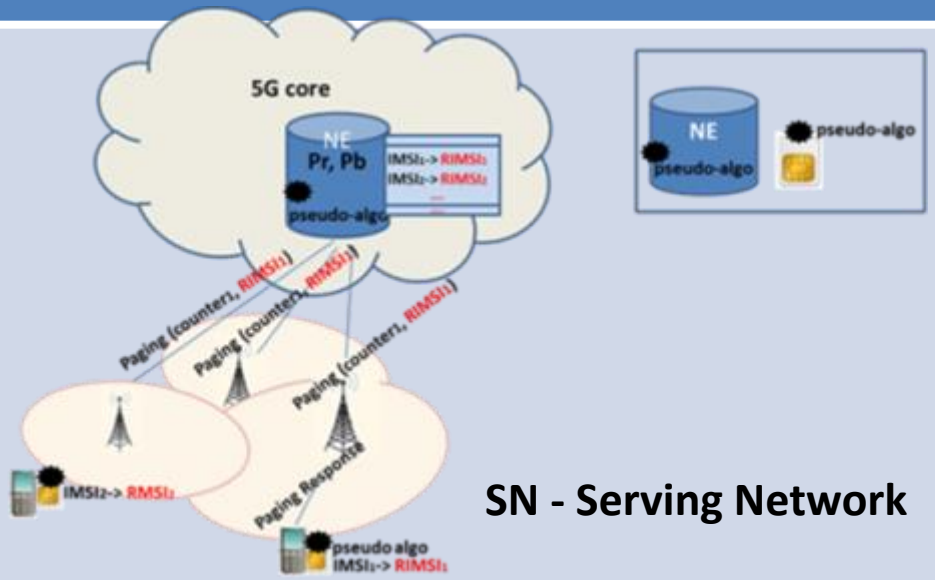
HN-centric approach



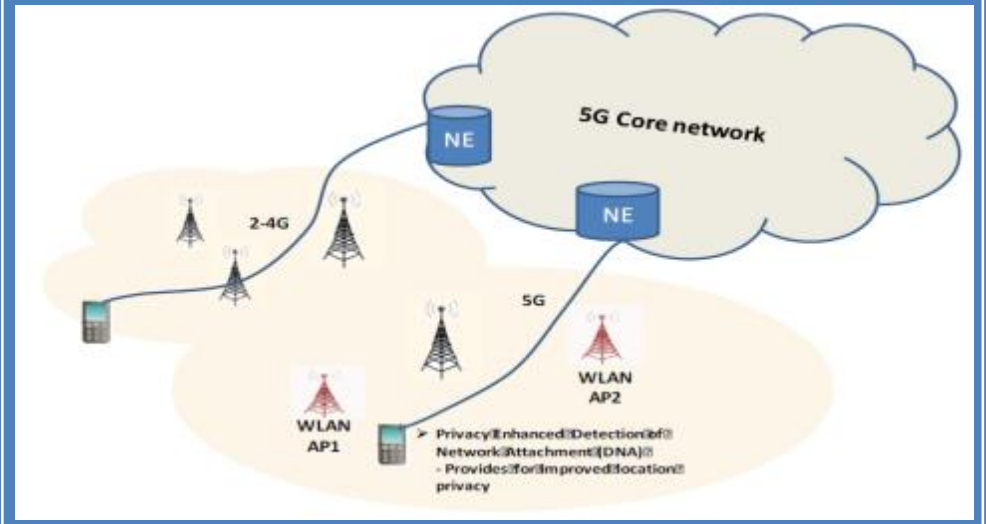
HN – Home network

Home centric IMSI Protection based on a traditional public key approach, where the public key of the home network is used by UE to encrypt IMSI. MCC, MNC not protected.

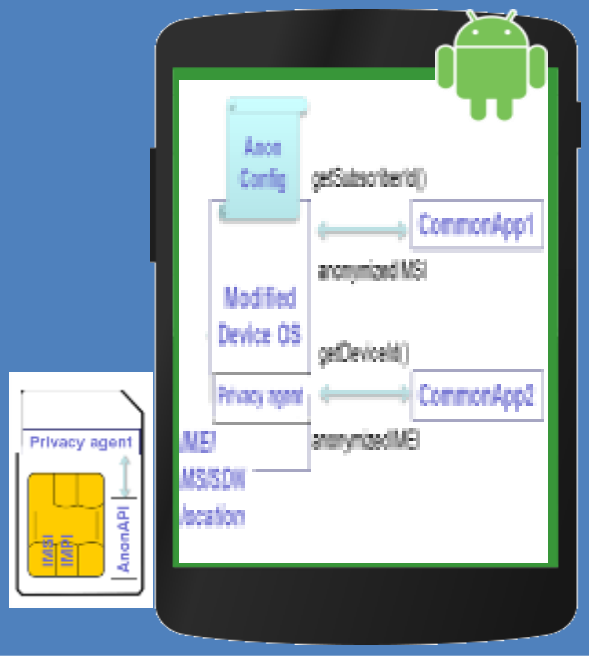
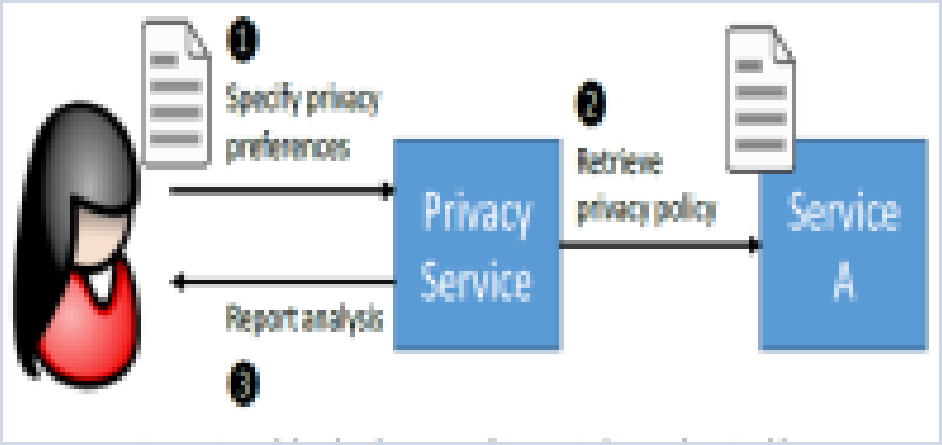
Privacy enablers - Implementation

Privacy Enhanced Identity Protection (R1)		A cryptographic library that implements the KP-ABE encryption scheme to encrypt and decrypt a given IMSI. The library also provides the setup and key generation functions.
Privacy Enhanced Identity Protection (R2)		IMSI Pseudonymization: pseudorandom dynamic pseudonyms generated by serving network and UE or only by network.

Privacy enablers Open Specification

Device Identifier(s) Privacy (R1&R2) *In DHCP – DNA (Detection of Network Attachment protocol)*		Dummy MAC addresses generation mechanism in the attachment phase and randomization of link layer (MAC) addresses. Anonymous and optimised address selection for network attachment protocols.

Privacy enablers - Open Specification

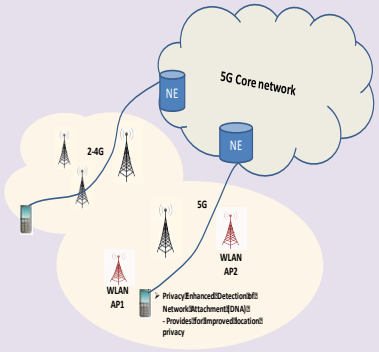
Device-based Anonymization		Modified Android OS able to anonymize the IMSI to selected applications and an integrated tool to configure user's privacy options for installed apps.
Privacy Policy Analysis		Mechanisms for users to analyse the privacy policy of a service and compare it to their preferences at app install time or connection time over 5G.

Privacy Enablers

Privacy enhanced identity protection

Provide protection against identity disclosure (and, consequently, unauthorized user tracking), by preventing or making more difficult IMSI catching attacks.

Device identifier(s) privacy

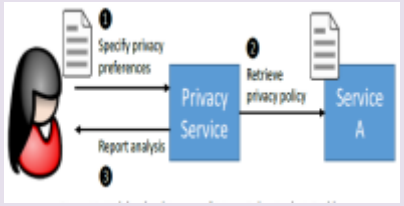


Limit exposure of device identifiers and prior points of attachment, and therefore, limit the ability to track a device.

SIM or Device-based Anonymization

Provide anonymization techniques on the user's device or UICC (SIM), offering protection against disclosure of sensitive information stored mainly on the SIM.

Privacy Policy Analysis

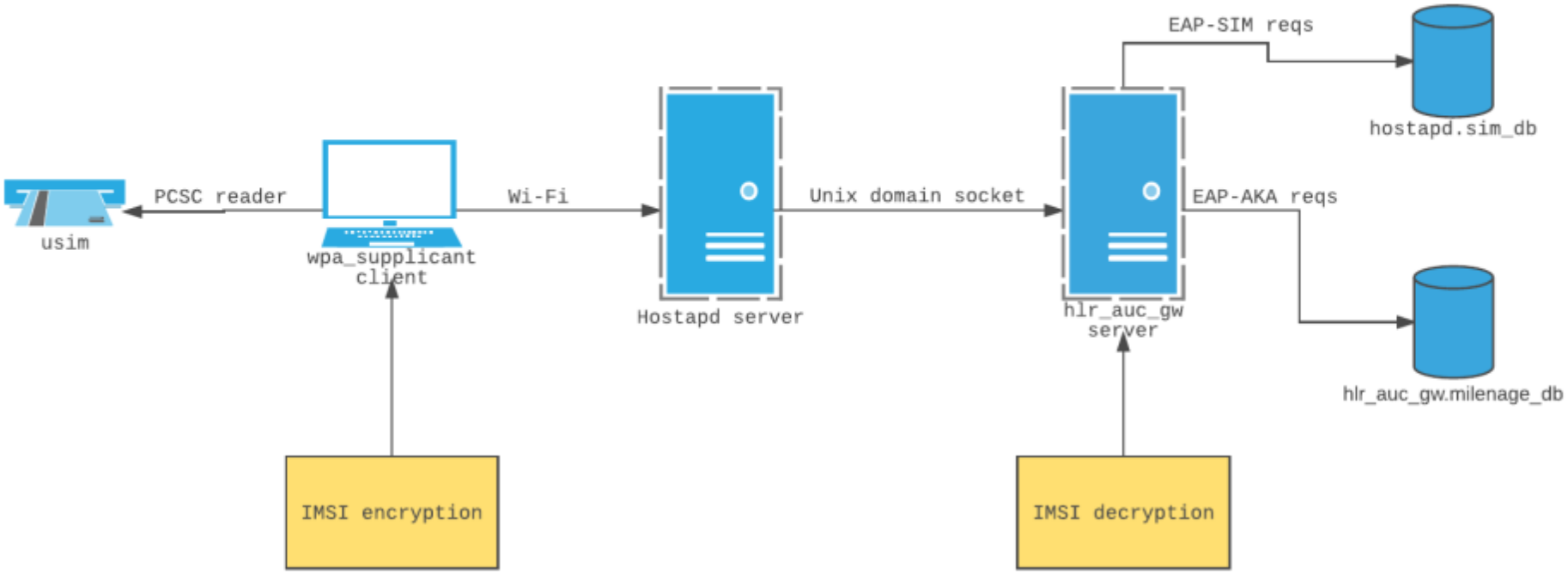


Enables users to analyse the privacy policy of a service and compare it to their pre-defined preferences at app install time or 5G connection time

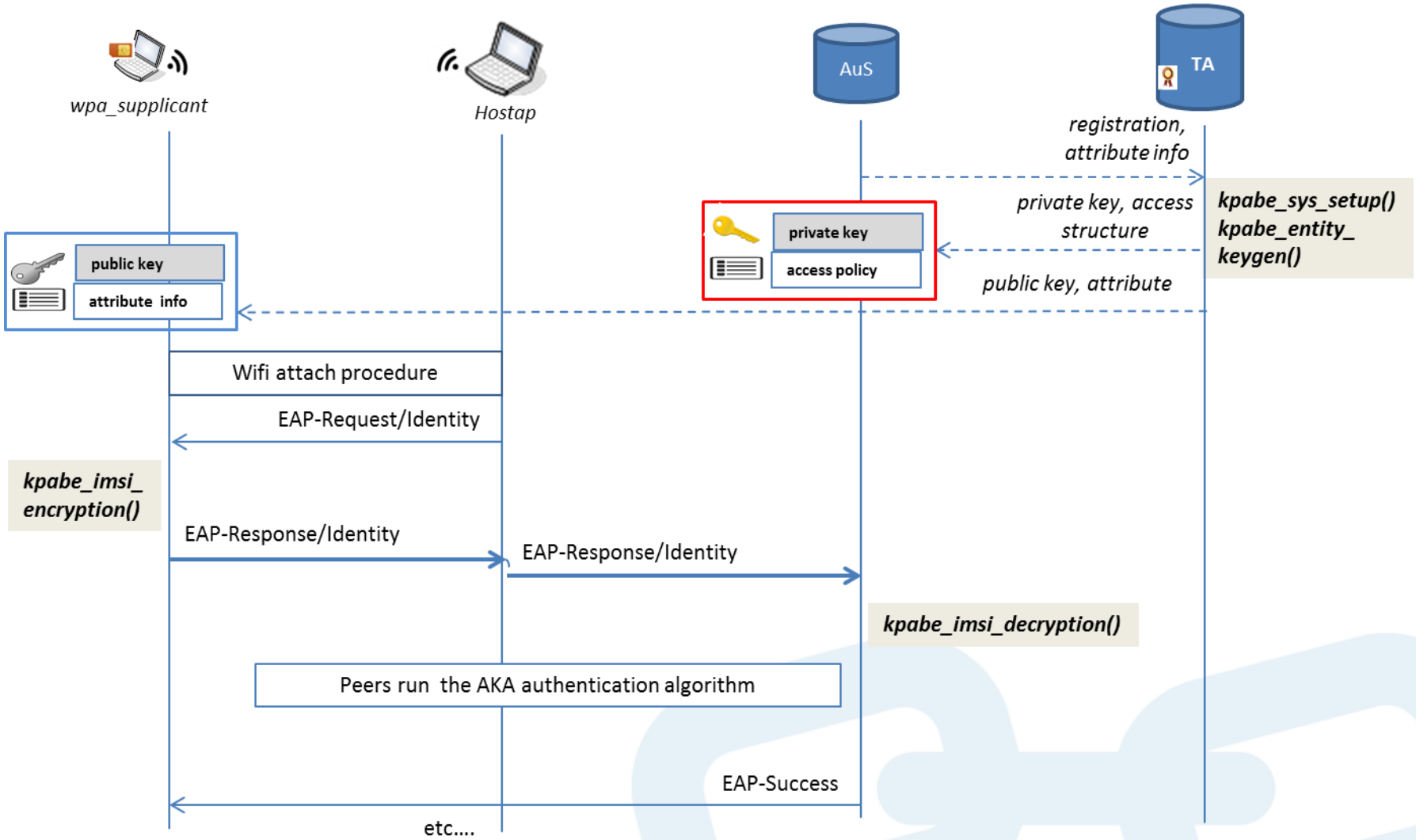
Privacy Enhanced Identity Protection

- **Rationales:**
  - Increased user privacy in 5G by adding PII (personally identifiable info) protection
  - Counteract IMSI catching attacks possible in previous networks (where IMSI is sent in clear text in a number of NAS procedures)
- **Features:**
  - IMSI Encryption (in 2 flavors – SN and HN-centric)
  - IMSI Pseudonymization (second release)
- **IMSI Encryption:**
  - Based on a KP-ABE cryptosystem [3]

Demo video - architecture



Demo video - interactions



References

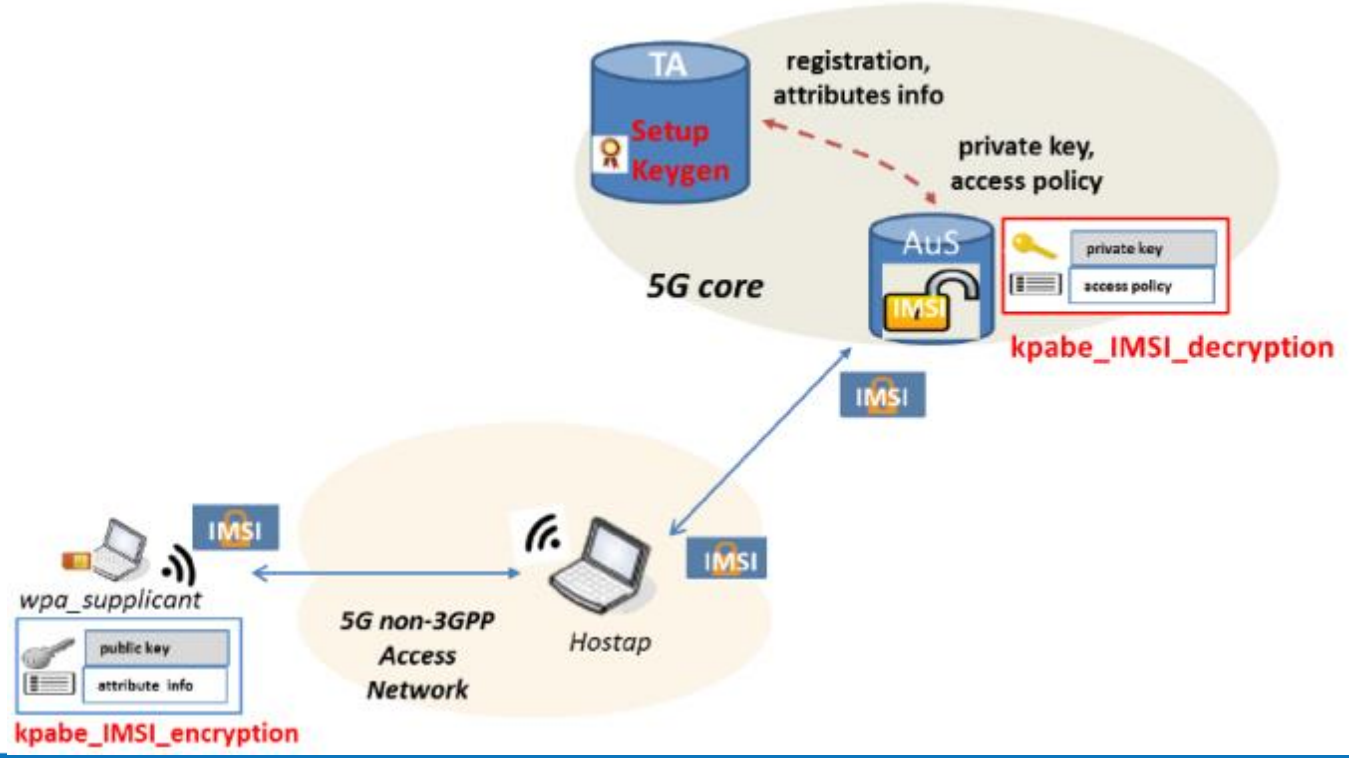
1. www.5gensure.eu
2. 5G ENSURE Deliverable D3.2, “5G-PPP security enablers open specifications (v1.0))”
3. Goyal, Pandey, Sahai, Waters, Attribute Based Encryption for Fine Grained Control of Encrypted Data, https://eprint.iacr.org/2006/309.pdf
4. PBC, The Pairing-Based Cryptography Library, https://crypto.stanford.edu/pbc/
5. he GMP library, the GNU Multiple Precision Arithmetic library, https://gmplib.org/
6. D3.4 5G-PPP Security Enablers Documentation (v1.0) – Enabler Privacy Enhanced Identity Protection, 671562 5G-ENSURE Privacy Enhanced Identity Protection
7. Libcelia, a static Linux library implementing primitive kpabe operations, https://github.com/gustybear/libcelia
8. hostapd, IEEE 802.11 AP, IEEE 802.1X/WPA/WPA2/EAP/RADIUS Authenticator, https://w1.fi/hostapd/

Thank you!

Backup slides

Encryption of Long Term Identifiers (R1): use case

- The kpabe_imsi_encryption() function (from the libkpabe library) is integrated in the wpa_supplicant, the component on the client side that implements the EAP-AKA authentication protocol. The IMSI is encrypted using the network AAA server's public key and the corresponding attribute.
- The kpabe_imsi_decryption() function (from the libkpabe library) is integrated in the authentication server (AuS). The IMSI is decrypted by using the private key corresponding to the access policy that is matched by the attribute.

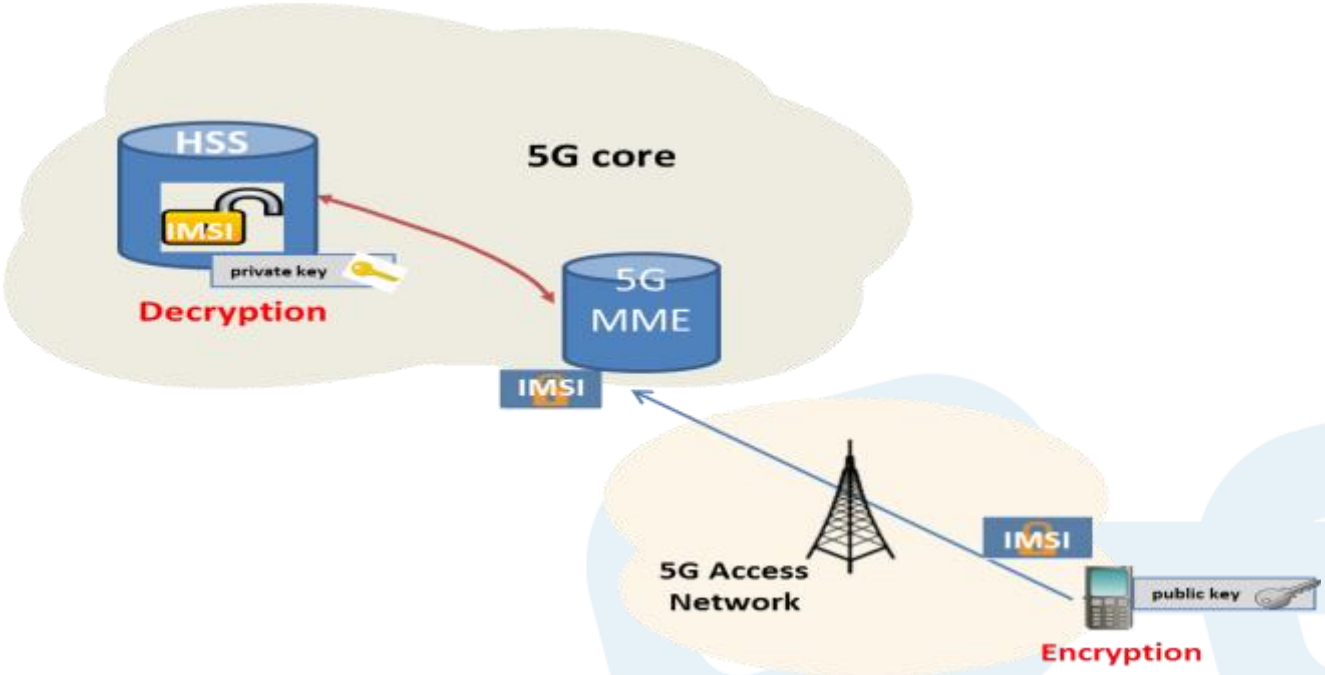


Encryption of Long Term Identifiers (R1): algorithms

- Cryptographic library that implements the KP-ABE encryption.
- **Setup**: runs on a trusted authority server TA. At the cryptographic system initialization time, TA generates a public parameter (public key) and a master key. The latter is only known by the TA server.
- **Keygen:** runs on the TA server and generate the private keys to trusted entities based on the user access policy. An entity entitled to perform decryption requests the provisioning of the private key by presenting an access policy over an attribute (or a set). The randomized key generation algorithm takes as input the public parameters (public key), the master key and the access policy. It outputs the private key which is able to decrypt all IMSIs encrypted under the attributes that satisfy the access policy.
- **Encryption**: runs on the client components, e.g., on the UE devices. The randomized encryption algorithm takes as input the user identity (i.e., the IMSI) to be encrypted, an attribute or set of attributes, and the public key. It outputs the ciphertext, i.e., the encrypted IMSI. In this way only the authentication servers which have the decrypted key generated with the correct access policy (that matches the encryption attributes) will be able to decrypt the ciphertext.
- **Decryption:** the decryption algorithm runs on an authorized network element (i.e., the authentication server). It takes as input the ciphertext, which was encrypted under the set of attributes, the public key parameter and the private key for access control. The output is the IMSI in clear text if the attributes included in the ciphertext satisfy the access policy.

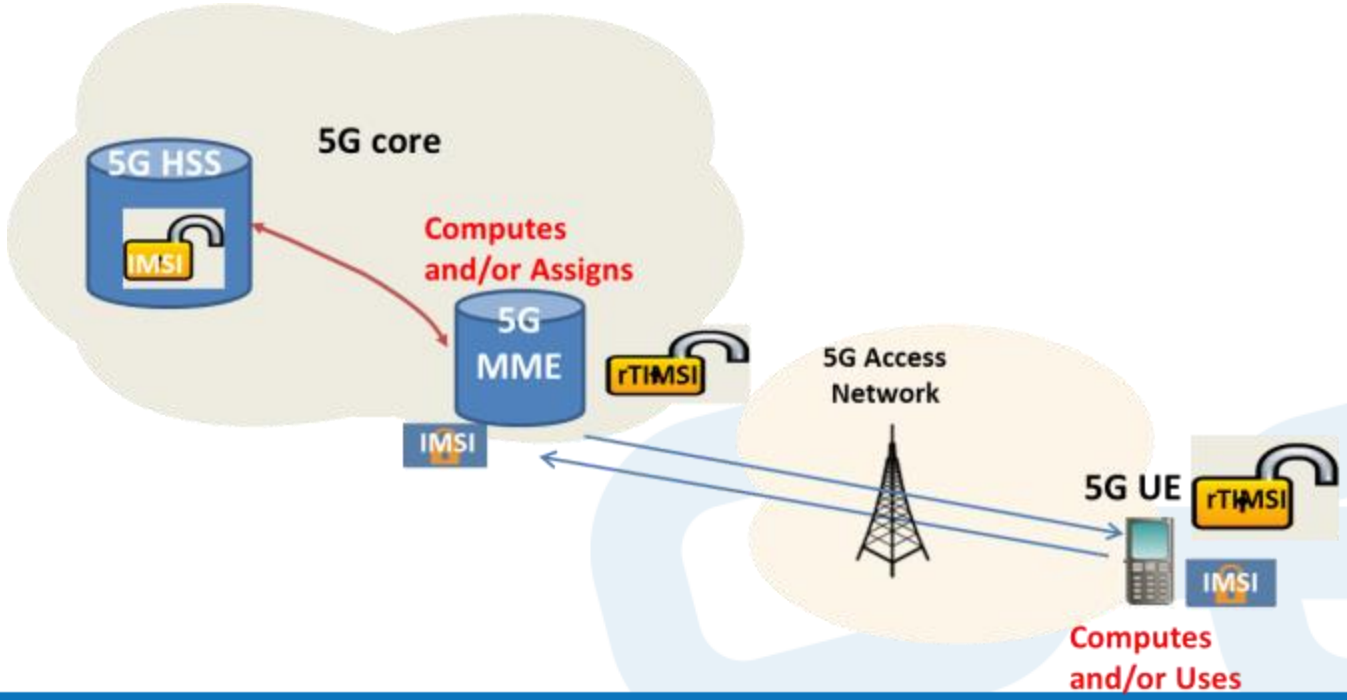
Home centric IMSI protection (R2)

- Based on a traditional public-key scheme
- UE uses the public key of its home network (HN) to encrypt parts of the IMSI (key can be stored on the UEs in advance, e.g. on the USIM card)
- No need of deploying additional infrastructure for key management, such as a PKI, except for a revocation/update mechanism in case of key compromise.
- HN responsible of performing the decryption and sharing afterwards the clear-text IMSI to the rest of the network elements on the system that may need it.
- Visited Network (MME) may need IMSI in clear text for Lawful Interception.



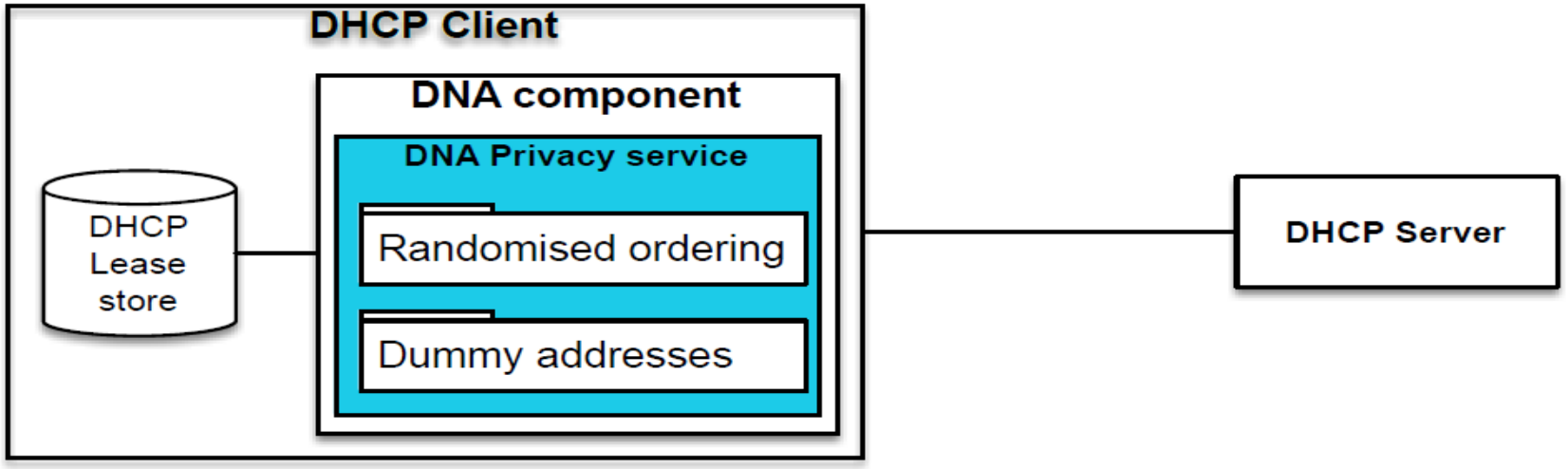
IMSI Pseudonymization (R2)

- Complement the “Encryption of Long Term Identifiers” feature to avoid exposing user permanent or long term identities on (at least) the air interface (i.e., in Attach Requests with GUTI, Identity Responses, Paging Requests).
- Pseudorandom dynamic pseudonyms (rTIMSI) can be generated in the same way both by the network and UE, by using a pseudonym-derivation algorithm with a shared secret key.
- Pseudonyms always used instead of IMSIs in response to an Identity Request, in a Paging Request, etc., and are consumed by usage (“one-time”).
- Alternatively, the network generates the pseudonyms for the entire Tracking Area and maintains the state for each UE.



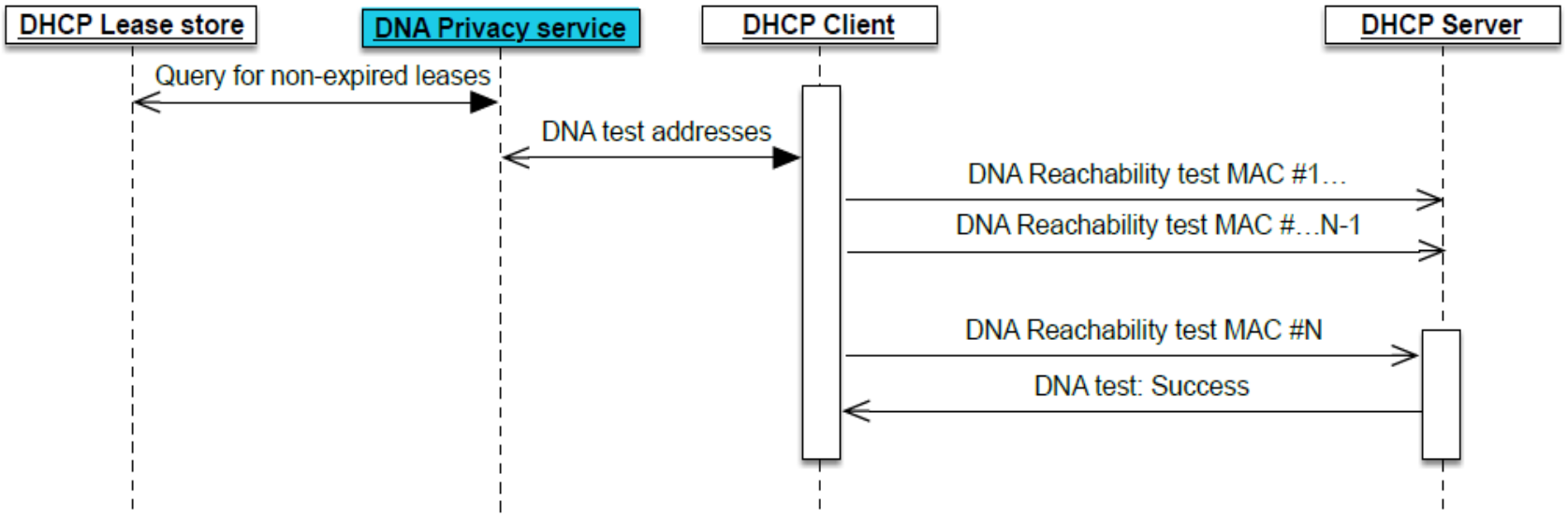
Device Identifier(s) Privacy (R1): components

- The enabler operates within the system DHCP services
- The DHCP client initiates a protocol exchange for each new connection and stores any unexpired leases in the DHCP lease store.
- The Detection of Network Attachment (DNA) protocol is enacted when the client has active leases in the DHCP lease store and it has connected at the link-layer by
- Randomised ordering component: the ordering of the leases used in the DNA reachability tests is randomised to reduce the potential likelihood to derive the user's previous locations
- Dummy addresses component: for each new point of attachment it injects dummy MAC addresses into the DNA protocol adding noise to any path-based inferences.



Device Identifier(s) Privacy (R1): DNA privacy service

- For each lease, the MAC and IP addresses of the router, and the assigned IP of the client is used to perform a ‘reachability test’.
- The reachability test’ is based on ARP request packet directed at the router’s MAC address proposing the use of a candidate IP address.
- If a match is found in the ARP reply, then the host continues to use that IPv4 address

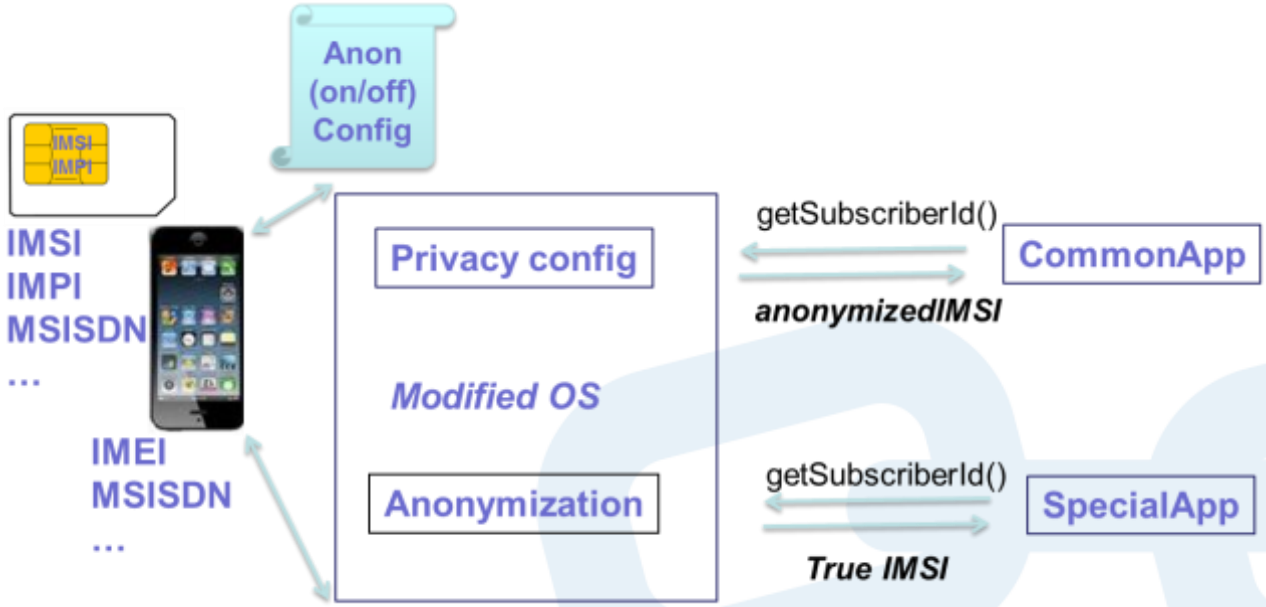


Device Identifier(s) Privacy (R2)

- Enhance approaches to provide for anonymised and optimised address selection for network attachment protocols which builds on release one features.
- Enhanced address anonymity providing for protection of device identifiers and prior points of attachment, and therefore, limit the ability to track a device.
- The second release will provide the following enhancements to the release one functionality:
  - Pre-analysis phase of the address anonymity metrics
    - The set of existing DNA addresses will be analysed before use to ascertain their potential anonymity metrics.
  - Dynamically optimised choice of address randomisation and dummy addresses
    - The choice of random addresses may be influenced by a range of factors including inferred ownership (OUI), location, sensitivity, user privacy settings.

Device-based Anonymization

- Aims to provide anonymization techniques on the user's device, offering protection against disclosure of sensitive information stored mainly on the SIM.
- The privacy/anonymization configuration (or profile) is directly controlled by the user, who can activate different anonymization profiles stored on the device.
- Depending on the information to be anonymized, the device implements a specific anonymization algorithm at the lowest possible layer in the device OS stack, and offers the means to the user to selectively activate and then deactivate the anonymization.



Privacy Policy Analysis

- Privacy policy specification: encoding service privacy policy.
  - support the loading of a privacy policy into the enabler. Which particular standard to use for the privacy policy is yet to be defined.
- Privacy preferences specification: encoding users' preferences.
  - allow the user to define their privacy preferences. The particular standard to use for this is yet to be defined.
- Comparison of policies and preferences: compare the selected service policies with the user's expressed preferences.
  - the selected service policies will be compared with a user's expressed preferences and the user will be presented with the analysis in a clearly understandable form.