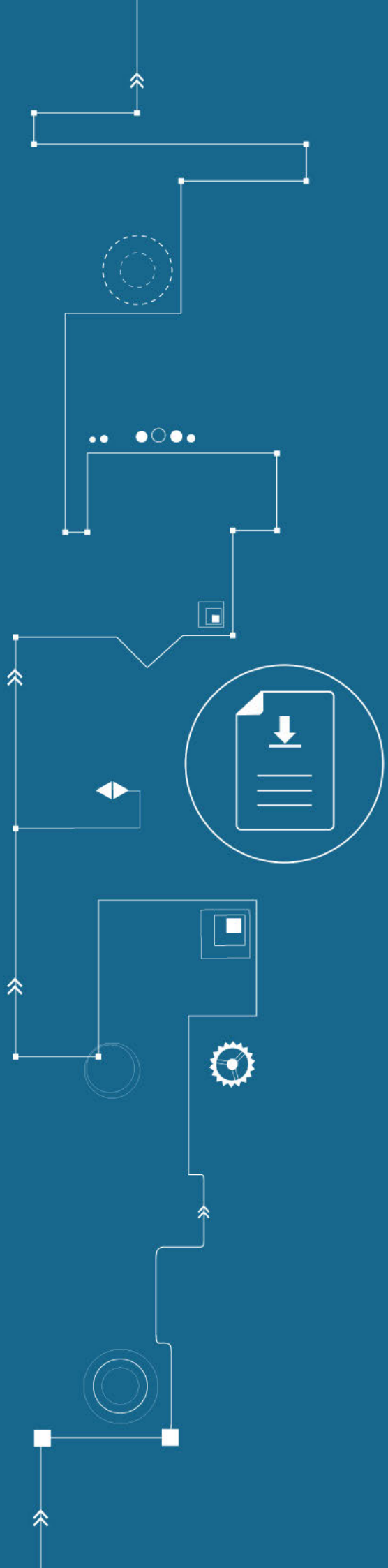
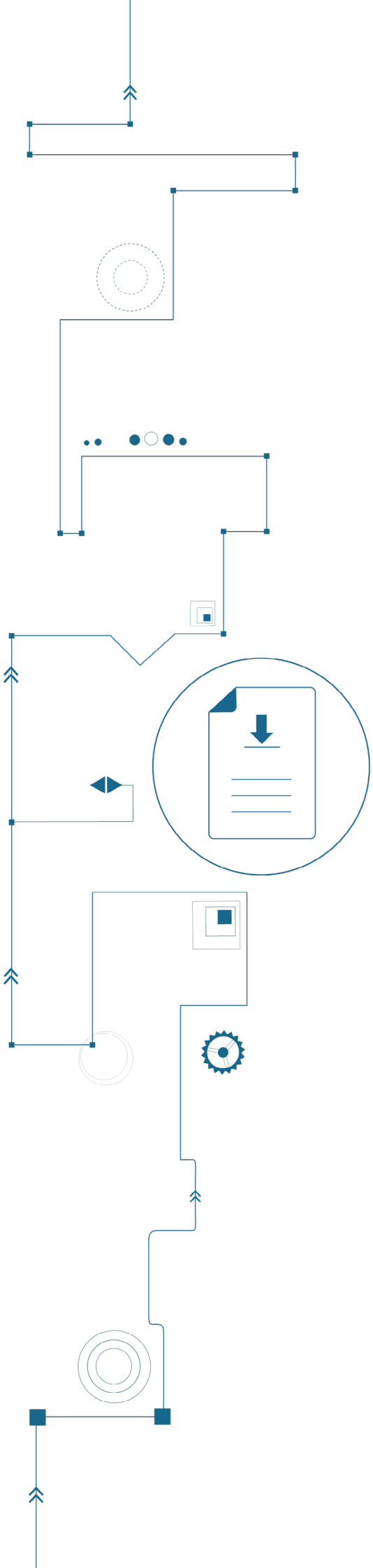
CUBRO
NETWORK VISIBILITY

5G SECURITY

WHITE PAPER

MARCH 2023





CUBRO
NETWORK VISIBILITY

TABLE OF CONTENTS

1. Introduction 3
2. Subscriber and Device Protection 3
3. Network protection 4
4. 5GC security 5
5. Network domains and security 5
6. CSPs and security 6

1. Introduction

5G has introduced a number of improvements in security compared to 4G. 5G standards development has adopted 'Secure by Design' principles, using for example Mutual Authentication and acknowledging that all links could be tapped, but making sure that the encrypted information is worthless when intercepted.

Security is a wide topic and has different angles to it, for example, ITU-T has defined eight security dimensions shown in the table below. While these are important factors, this blog focuses more on the 5G network security measures and attempts to bring how to utilize data regardless of regulation and tight security in the summary section.

Security dimension	Description
Access control	Protects against unauthorized use of network resources
Authentication	Confirms identities and ensures validity of claimed identities
Non-repudiation	Means for associating actions with entities
Data confidentiality	Data protection from unauthorized disclosure
Communication security	Information flow only allowed between authorized end points
Data integrity	Correctness and accuracy of data
Availability	No denial of authorized access to network resources or data
Privacy	Protection of information that might be derived from the observation of network activities

The importance of security is increasing continuously as we become more and more dependent on digital services. The number of connections is increasing exponentially with M2M and IoT. Therefore, aspects such as trusted ID, trusted SW, secure configuration, trustworthy data, protected communication, privacy and physical security are gaining more relevance not only in IoT communication, but in telecommunications in general.

2. Subscriber and Device Protection

5G has several enhancements in subscriber security:

- Protects the confidentiality of the initial non-access stratum (NAS) messages between the device and the network. It is no longer possible to trace user equipment (UE) using current attack methodologies over the radio interface, protecting against man in the middle (MITM) and fake base station (Stingray/IMSI catcher) attacks.

- Home control – a mechanism that requires the home network to check the authentication status of the device in the visited network preventing various roaming fraud types.

- Unified authentication, for example, for WLAN, allowing 5G networks to manage previously unmanaged and unsecured connections.

- User plane integrity checking, ensuring the user traffic is not modified during transit.

- Enhanced privacy protection with the use of public / private key pairs to conceal the subscriber's identity.

UE keys are stored in the Universal Subscriber Identity Module (USIM) and the home environment to enable network access security. There are two trust domains, tamper proof universal integrated circuit card on which the USIM resides as trust anchor and the Mobile Equipment.

Subscription Permanent Identifier (SUPI), equivalent to IMSI in 4G, is encrypted and available as SUCI, Subscriber Concealed Identifier. Naturally, the air interface between UE and gNB is encrypted.

3. Network protection

RAN is separated into Distributed Units (DU) and Central Units (CU). DU doesn't have any access to customer communications. IPSec is typically used for the connection from gNB to backhaul.

On the core side AMF serves as a termination point for NAS security. AMF is co-located with Security Anchor Function (SEAF) that holds the root key for the visited network. Authentication Credential Repository and Processing Function (ARPF) is co-located with UDM and stores long-term security credentials.

5G also introduces a new network architecture element: the Security Edge Protection Proxy (SEPP). The SEPP protects the home network edge, acting as the security gateway on interconnections between the home network and visited networks. Its main functionality includes:

- Application layer security and protection against eavesdropping and replay attacks

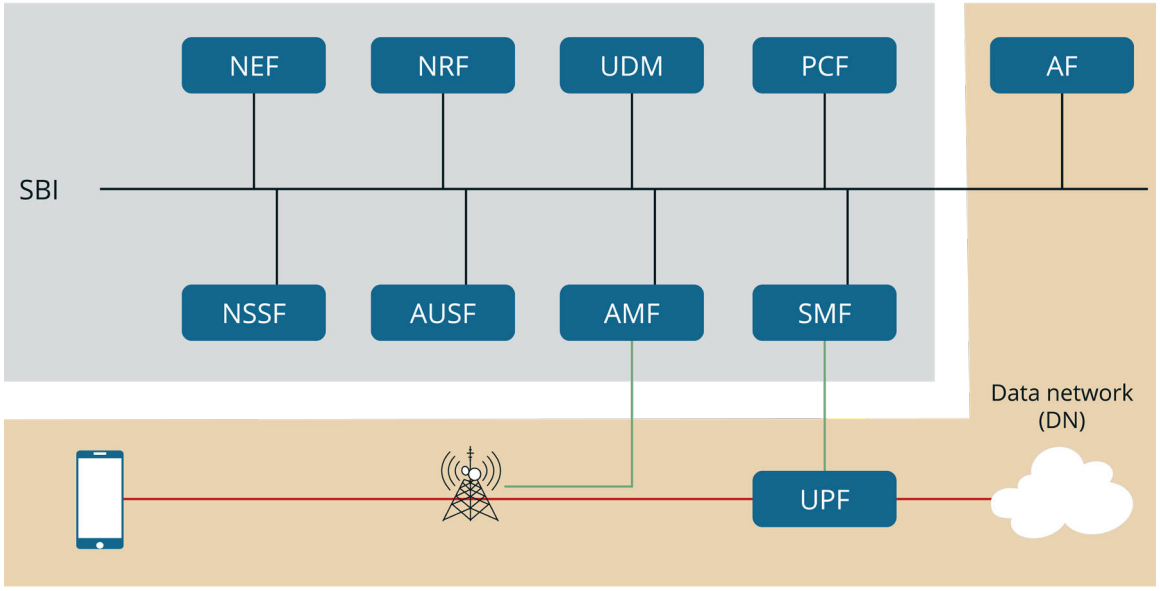
- End-to-end authentication, integrity and confidentiality protection via signatures and encryption of all HTTP/2 roaming messages

- Key management mechanisms for setting the required cryptographic keys and performing the security capability negotiation procedures

- Message filtering and policing, topology hiding and validation of JSON objects, including cross-layer information checking with address information on the IP layer

- Enhanced security of the international roaming services to overcome the existing security risks linked to SS7 and Diameter usage.

4. 5GC security



5GC introduces a new set of protocols and processes to secure the core functions. These include:

- HTTP/2 communication between cloud native functions (CNF) in the core
- TLS providing encrypted communication between all CNF
- HTTP/2 over N32, replacing Diameter over the S6a reference point
- More secure cipher suites

5. Network domains and security

Telecom networks are often divided into four distinctive parts: Access and core network, transport and interconnect network that connects different core networks with each other.

It is clear that 5G has increased security in many ways compared to previous telecom generations. New features such as network slicing and 5GC bring new ways of having a safe network, but they also carry potential dangers. Kubernetes and container security require new thinking in security management, for example secure container lifecycle management is a must.

6. CSPs and security

CSPs are definitely facing a huge challenge with all the security technologies and threats. It is one thing to secure the network properly, but at the same time, the CSP's existence and success depends on how well subscribers are served. Understanding subscriber behaviour is even more important than before.

This creates a bit of a dilemma for the CSPs. How to run a secure network and still have visibility in the subscribers?

Network visibility stays as a cornerstone to understanding what happens in the network. Despite the multi-layer security measures, the data flow and messages need to be decrypted before any actions can be done. The point of decryption gives an opportunity to have legitimate extraction of data, for example from 5GC or from User Plane data after it has run through Security GW.

The increasing number of attacks, regulators' tightened requirements and a huge increase in data volumes demand the CSPs to plan the data extraction points more carefully and, in many cases, even add encapsulated encryption with anonymization. With careful planning and the right solution, monitoring the data and getting insights into subscribers' behaviour is still possible.