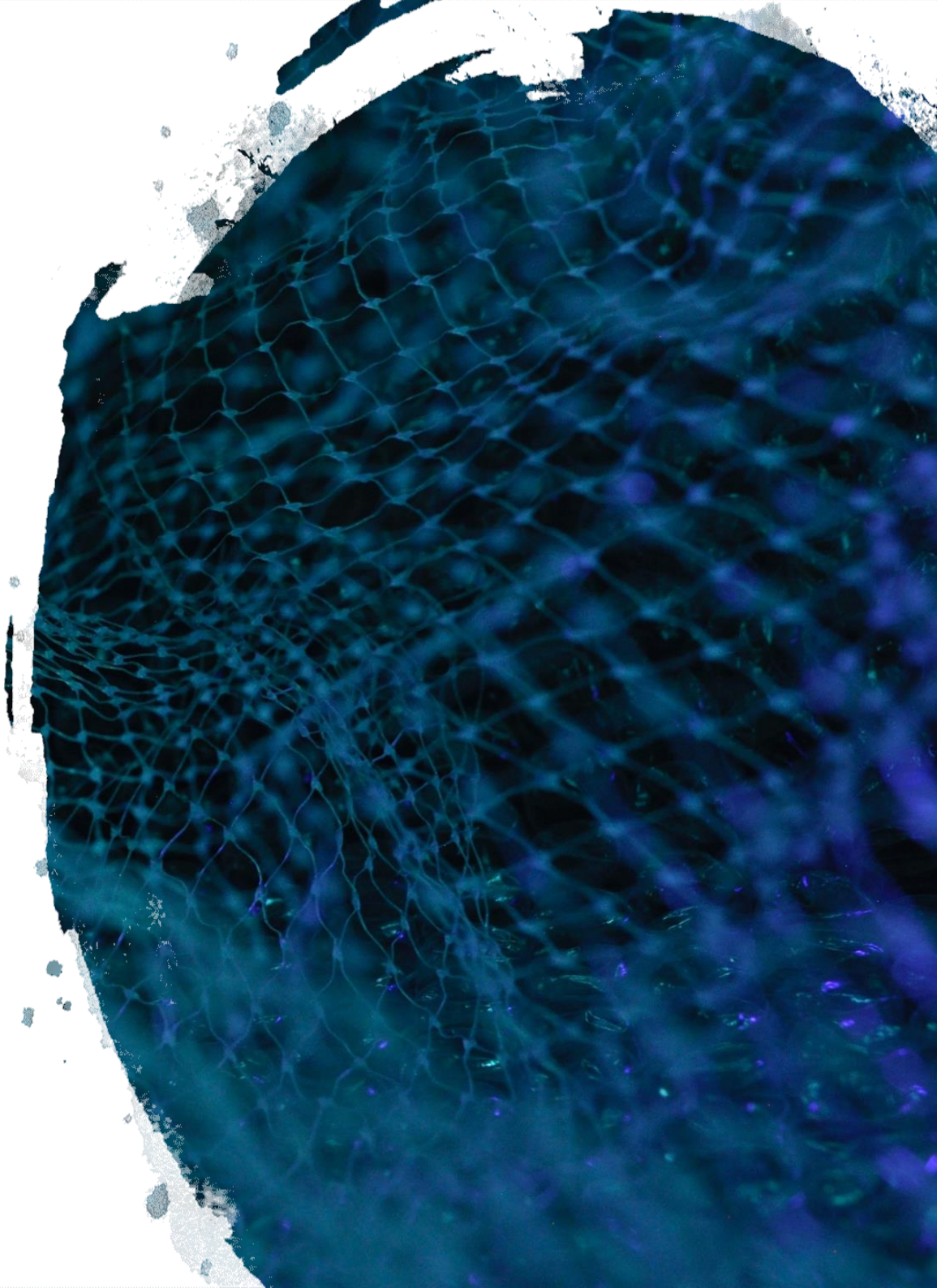
KaurIoT SCEF: T8

The Future Is Now



KaurIoT SCEF: T8

The Future Is Now

The Kauri company presents a novelty:
new SCEF function with unified 3GPP protocols
and highly efficient architecture.

The new technological Flagship Kauri is revolutionizing
the CIoT segment (cellular Internet of things) and marks a new form of interaction between mobile operators and users.

High growth of NB-Iot traffic, efficiency of application development, provision of complex services and reduction of «Time-To-Market» - all that and more becomes possible with Kauri Intelligent software and hardware system.

With Kauri, your mobile network becomes of high-priority for users.

Learn more at: kauri-iot.com

Problems of implementing IoT in the telecom industry

According to the IoT Signals study, one of the main problems of implementing IoT technologies is limited resources, long-term implementation, and lack of skills.

Therefore, not all companies can create a client platform for the Internet of Things (to connect end devices and their centralized management, as well as run the necessary IoT applications).

If the company introduces the technology, then one of the problems facing any telecom operator that provides a service for working with IoT devices will be that users of this network need services that have traditionally been used only by specialists in the field of telecommunications.

IoT users often do not have such qualifications. The software is usually performed outside the operator's internal network, and often outside the trusted zone.

Therefore, there is a need for a technology that, on the one hand, frees the business logic from the need to delve into the structure of cellular communications, and on the other – protects the operator's network from the possible malicious impact of erroneous or malicious actions on the business logic.

KaurIoT SCEF: T8

Problems of implementing IoT in the telecom industry

1. Problems with guaranteed data delivery to devices and their identification (as well as the inability to deliver them simultaneously to a group of devices).

2. Selecting a transport protocol to communicate with the devices, as well as the authentication algorithm.

3. Difficulties with organizing and setting rules for data exchange with devices.

4. The issue of monitoring devices and getting information about them online.

To solve such problems, difficult solutions are created in terms of development and feasibility.

What does this lead to?
To the need to increase the costs: time, labor, financial.

KaurIoT SCEF: T8

Alternative: SCEF

Service Capability Exposure Function (SCEF) – is a function that provides a means to securely disclose services and capabilities provided by 3GPP network interfaces.

SCEF provides a means to discover exposed services and capabilities and provides access to network capabilities through homogeneous network application programming interfaces (eg, network APIs) defined through the T8 interface, and abstracts services from underlying 3GPP network interfaces and protocols

Individual **SCEF** instances can vary depending on what service capabilities are available and what API functions are supported.

SCEF is always in the trusted domain. At the same time, the application can be either in a trusted domain or outside of it.

SCEF functionality can include:
1. Authentication and authorization.
2. Identification of the API consumer.
3. Profile management.
4. ACL management (access control list).

KaurIoT SCEF: T8

What Does This Means in Practice?

SCEF is a mediator between the network and the Application Server (AS), allowing access to the NIDD and 3G network.

One of the problems facing any telecom operator providing a service for working with IoT devices is that the users of this network are interested in services that have traditionally been used by telecommunications specialists only and mainly in the operator's own network. IoT users often lack this qualification. The software is usually deployed outside the operator's internal network, and often outside the trusted zone.

SCEF, on one hand, relieves business logic of the need to look into the cellular structure and, on the other hand, protects the operator’s network from the possible harmful effects of erroneous or malicious actions of business logic SW.

Protection is provided by both: isolation of internal network functions and by traffic regulation. UE (User Equipment) can be accessed using an External Identifier allocated by the carrier almost arbitrarily within the valid domain name suffix. This allows the operator to significantly save the numbering capacity using MSISDN-less UE.

HTTPS is used as the communication protocol, and the encoding of the transmitted information uses JSON text format, which is easily readable by both humans and computers.

KaurIoT SCEF: T8

Non-IP

Non-IP is a situation where the device is not assigned an IP address, and data is transmitted without using the IP protocol.

Traffic for such connections can be transmitted in the following ways:
1. Classic: MME>SGW>PGW and then through the PtP (Point-to-Point) tunnel to AS.
Advantage over IP traffic: smaller size of transmitted packets due to the absence of IP headers and security.

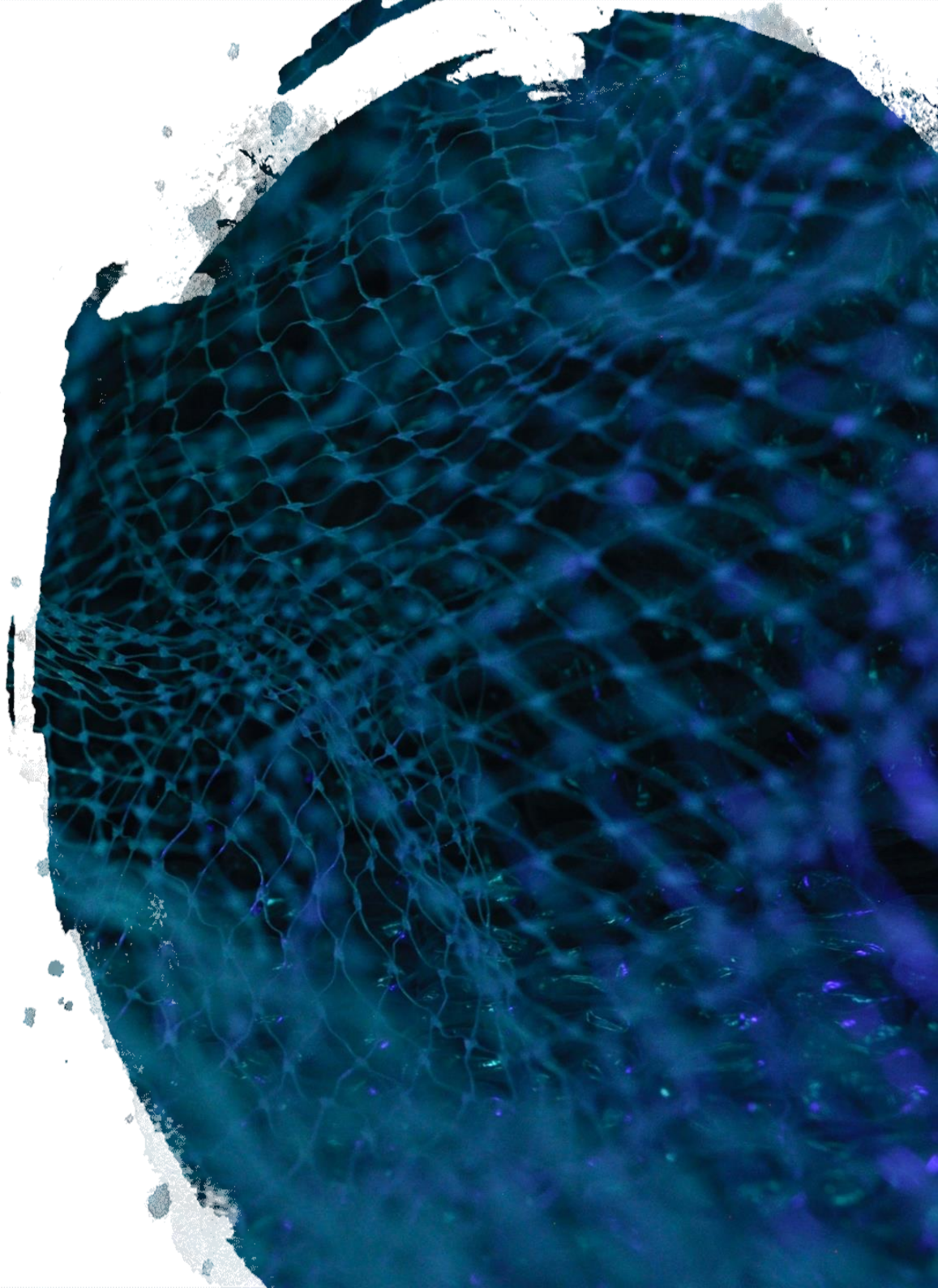
2. Using SCEF: an even faster option, where it is enough to simply send a data packet to the SCEF for a specific external ID (a universal device ID that replaces a phone number or IP address).
Advantage: developers no longer need to implement device authentication algorithms, as the network takes over this function completely.

Why is this good?
1. Reduction energy consumption.
2. Increase battery life.
3. Reduction the cost of developing the device.
4. Reduction development time and improve competitiveness.

Converting network protocols to a familiar API allows SCEF to help developers abstract from difficult mechanisms of interaction with devices. As a result, it is easier to create new services and quickly bring solutions to market.

KaurIoT SCEF: T8

The Goals



KaurIoT SCEF: T8

The Main Goals of SCEF:

1. Ensuring access to the IT capabilities of IoT and NB-IoT via the REST API interface, standardized by ETSI and 3GPP, which allows to implement the safe exposure of services and features provided by the operator network interfaces.

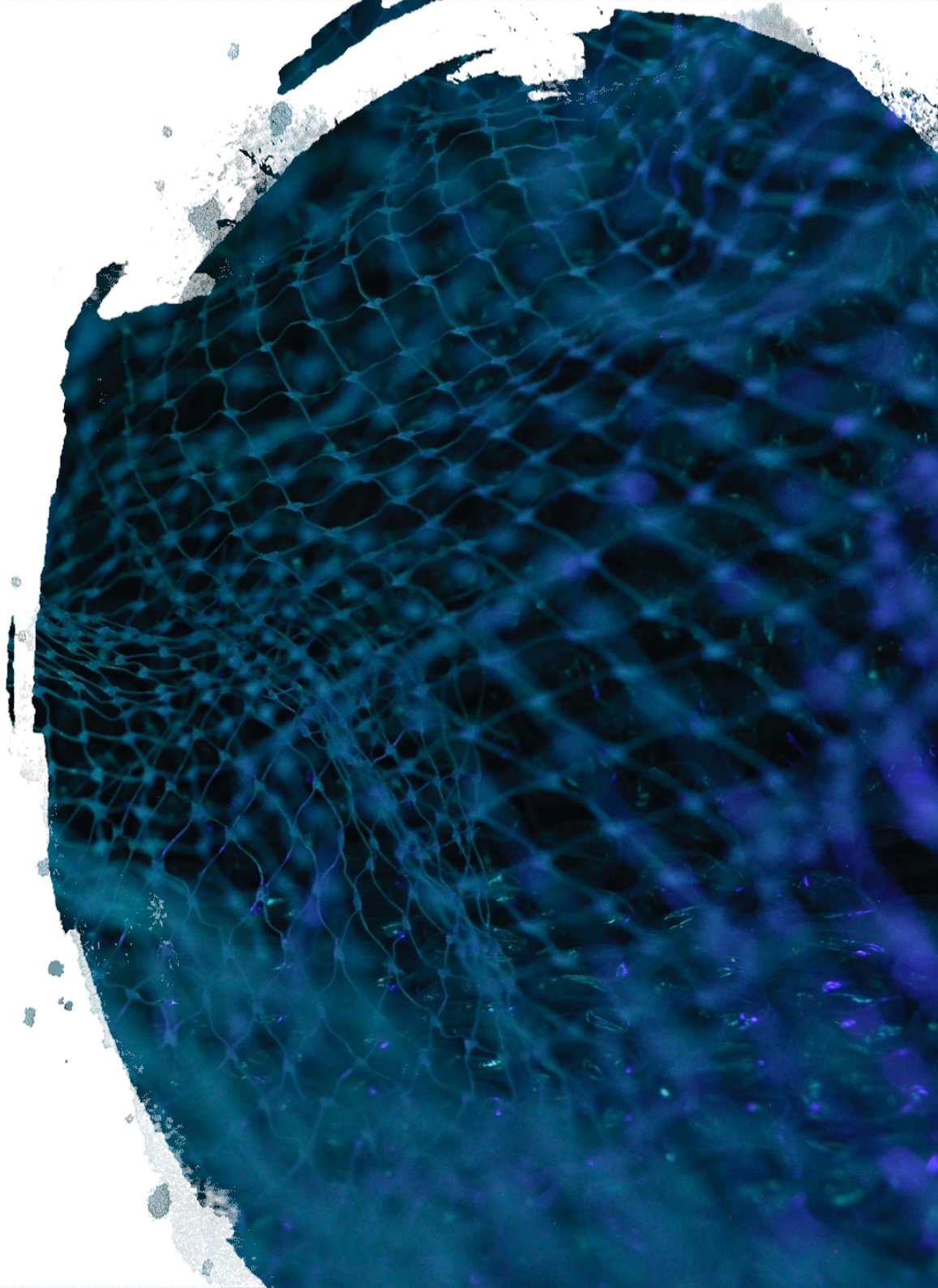
2. Eliminating the need for device identification and authentication, allowing application client servers (Application Server) to receive data and manage devices via a single API interface.
   - The device identifier is not the International Mobile Subscriber Identity (IMSI) or the IP address, as it is now implemented in 2G / 3G / LTE networks, but the External ID, which is defined by the 3GPP standard in a format that is familiar to application developers.

3. The ability to increase the lifecycle of IoT devices in the network and reduce the load on the infrastructure

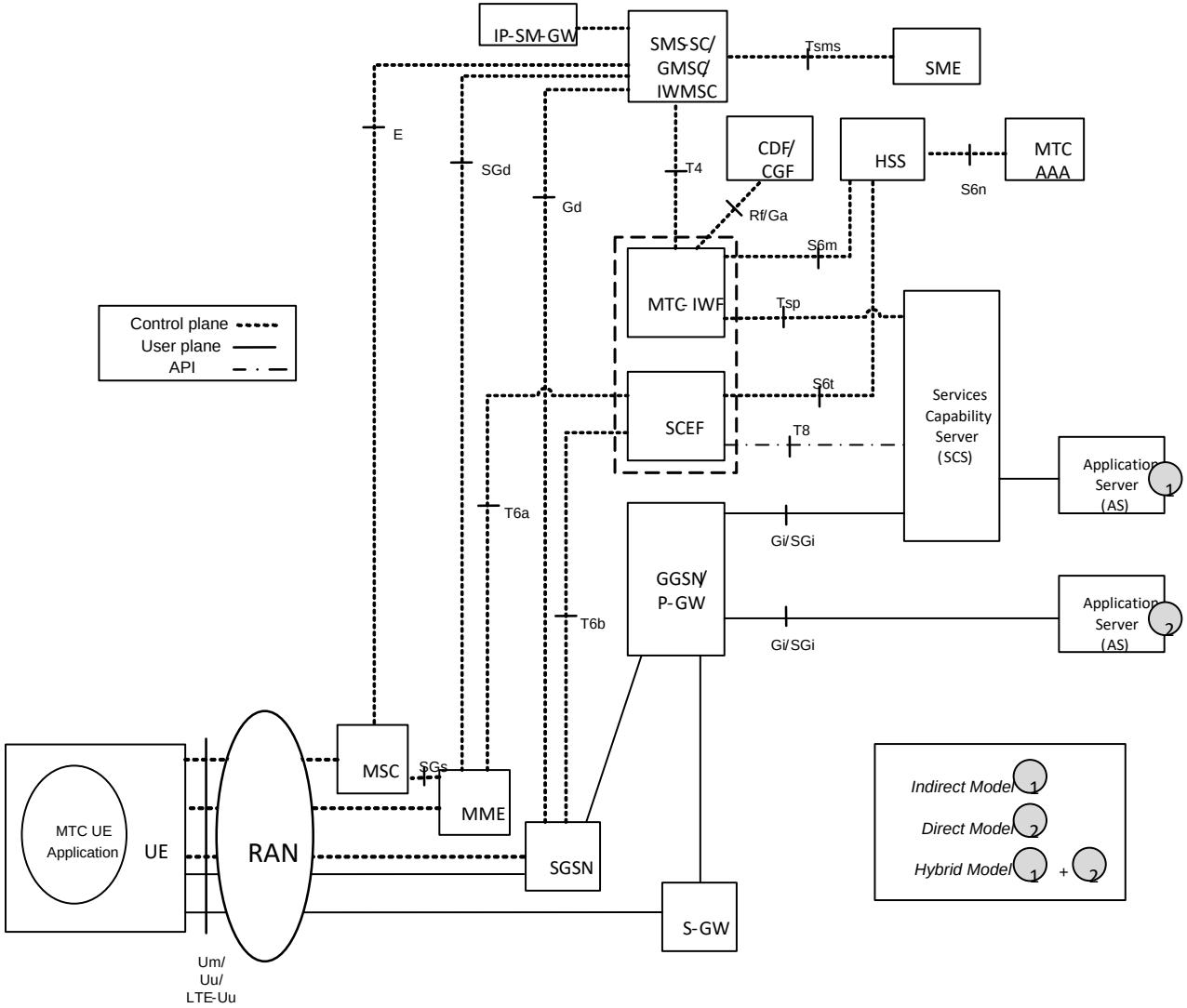
The main objective of SCEF is to simplify work and quickly complete the tasks

KaurIoT SCEF: T8

Solution Architecture



KaurIoT SCEF: T8



3GPP Architecture for Machine-Type Communication (non-roaming)

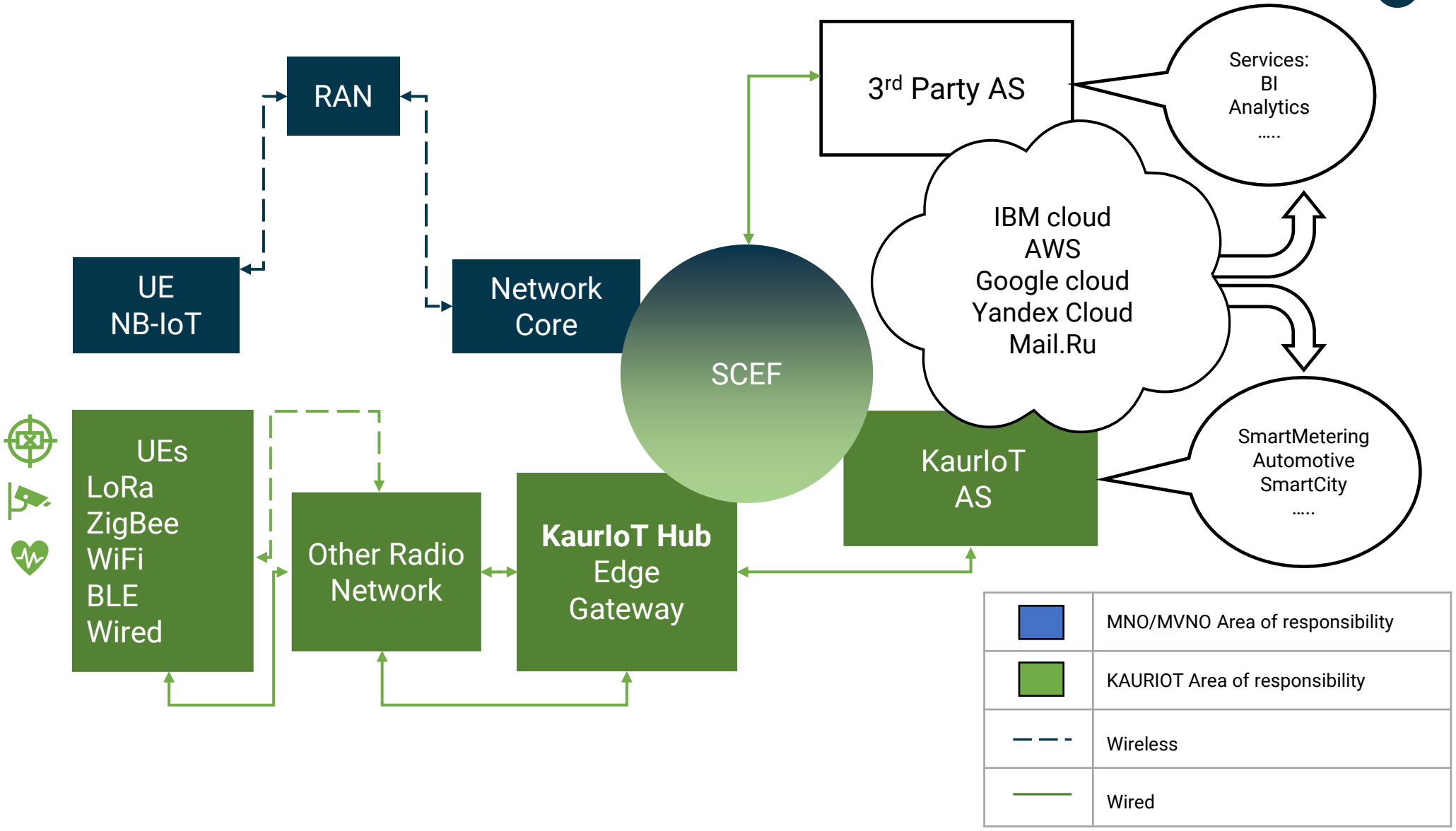
Схема / ETSI:

https://www.etsi.org/deliver/etsi_ts/123600_123699/123682/16.08.00_60/ts_123682v160800p.pdf

SCEF can reside at the edge of the IoT domain, as shown here, or SCEF can reside entirely within the IoT domain, interacting with an external API management platform at the edge.

KaurIoT SCEF: T8

KaurIoT SCEF: T8 and MNO



KaurIoT SCEF: T8

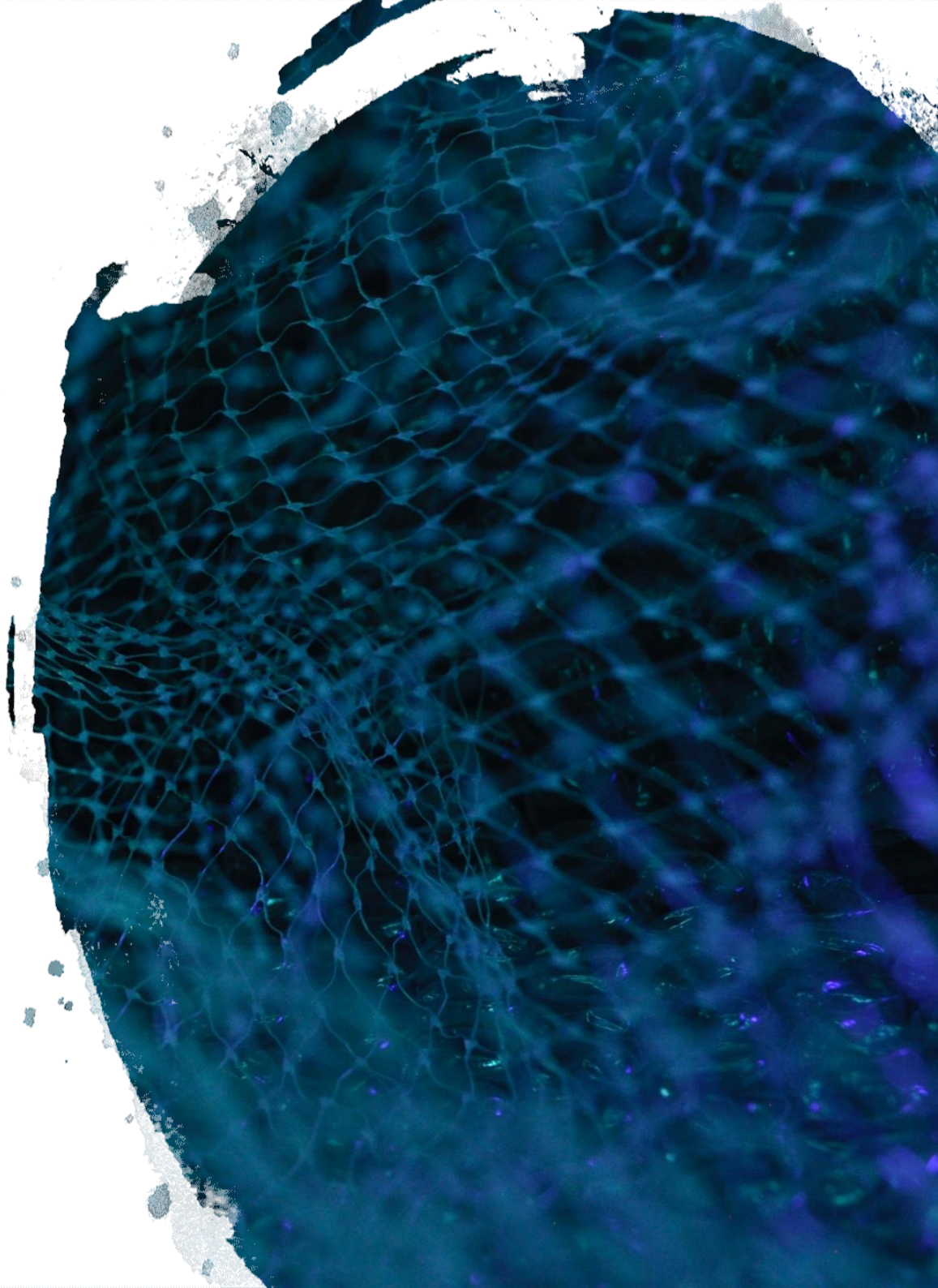
Our Technical Expertise

These schemes are common to SCEF. The specific architecture is refined based on the client's internal infrastructure architecture.

With our expertise in T8, we are able to develop an Application Server that will work via SCEF. If telecom operators already have their own SCEF, we will help develop their own AS

KaurIoT SCEF: T8

The Benefits



KaurIoT SCEF: T8

The Main Benefits:

1 Single Window: Ability to work with unique functionality.

2. Reduced TTM (Time to Market).

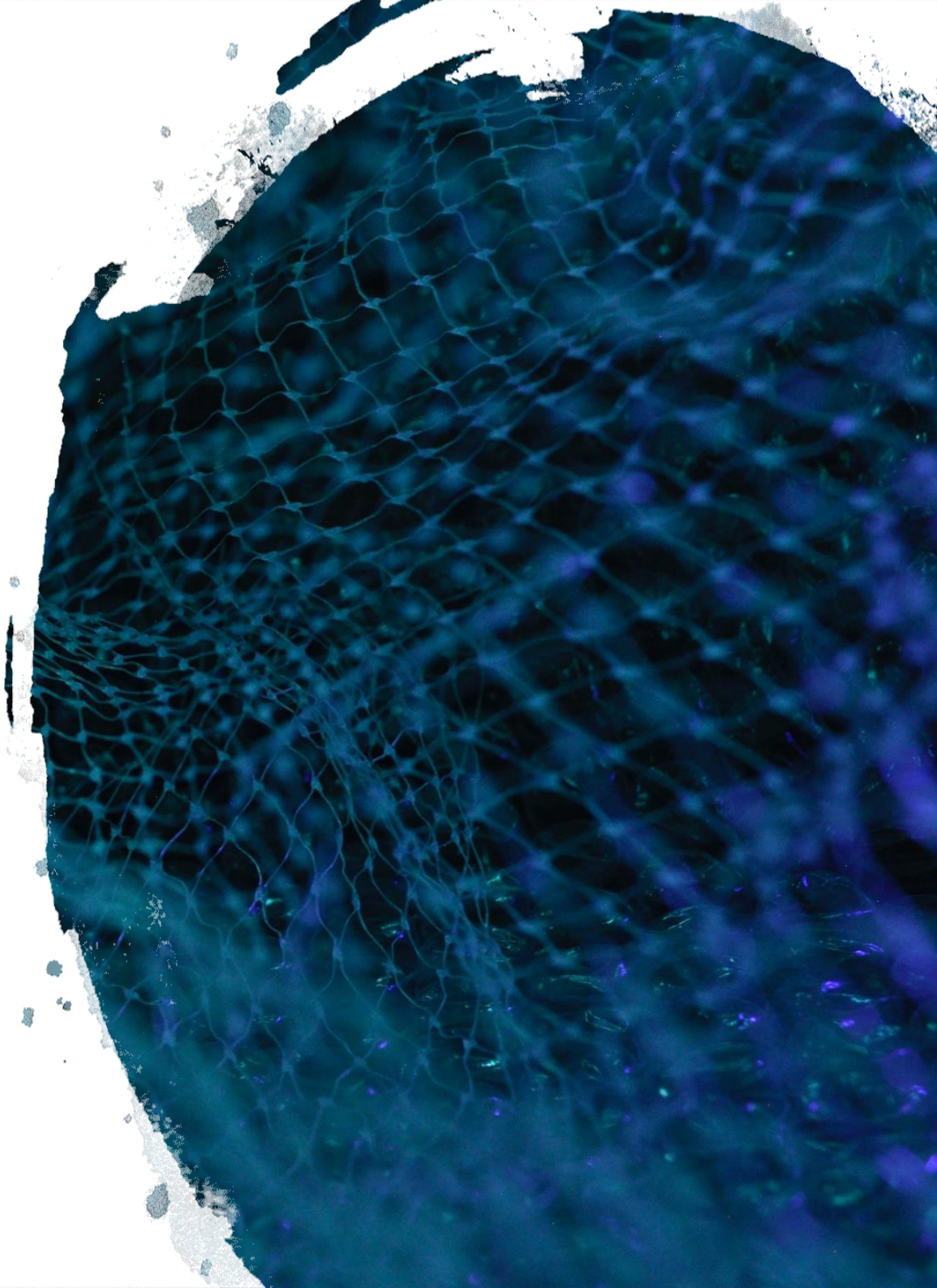
3. Reduction of financial costs for development.

4. An additional interface for implementing quick solutions - your own cases.

The main objective of SCEF is to simplify work and quickly complete the tasks

KaurIoT SCEF: T8

The Popular SCEF Functions



KaurIoT SCEF: T8

The Most Popular SCEF Functions are:

Non-IP Data Delivery for low-power devices.
Functions for NIDD are used to process mobile data and mobile termination if the data used for communication is considered unstructured. Support for non-IP data is a part of the consumer IoT EPS optimization.

Device status monitoring
The event monitoring function tracks specific events in the 3GPP system and makes event monitoring information accessible via SCEF. It allows to identify a 3GPP network element suitable for configuring an event, detecting an event, and reporting an event to authorized users.

For example, to use applications or to maintain a log. If an event is detected, the network can be configured to perform special actions, such as restricting UE access.

KaurIoT SCEF: T8

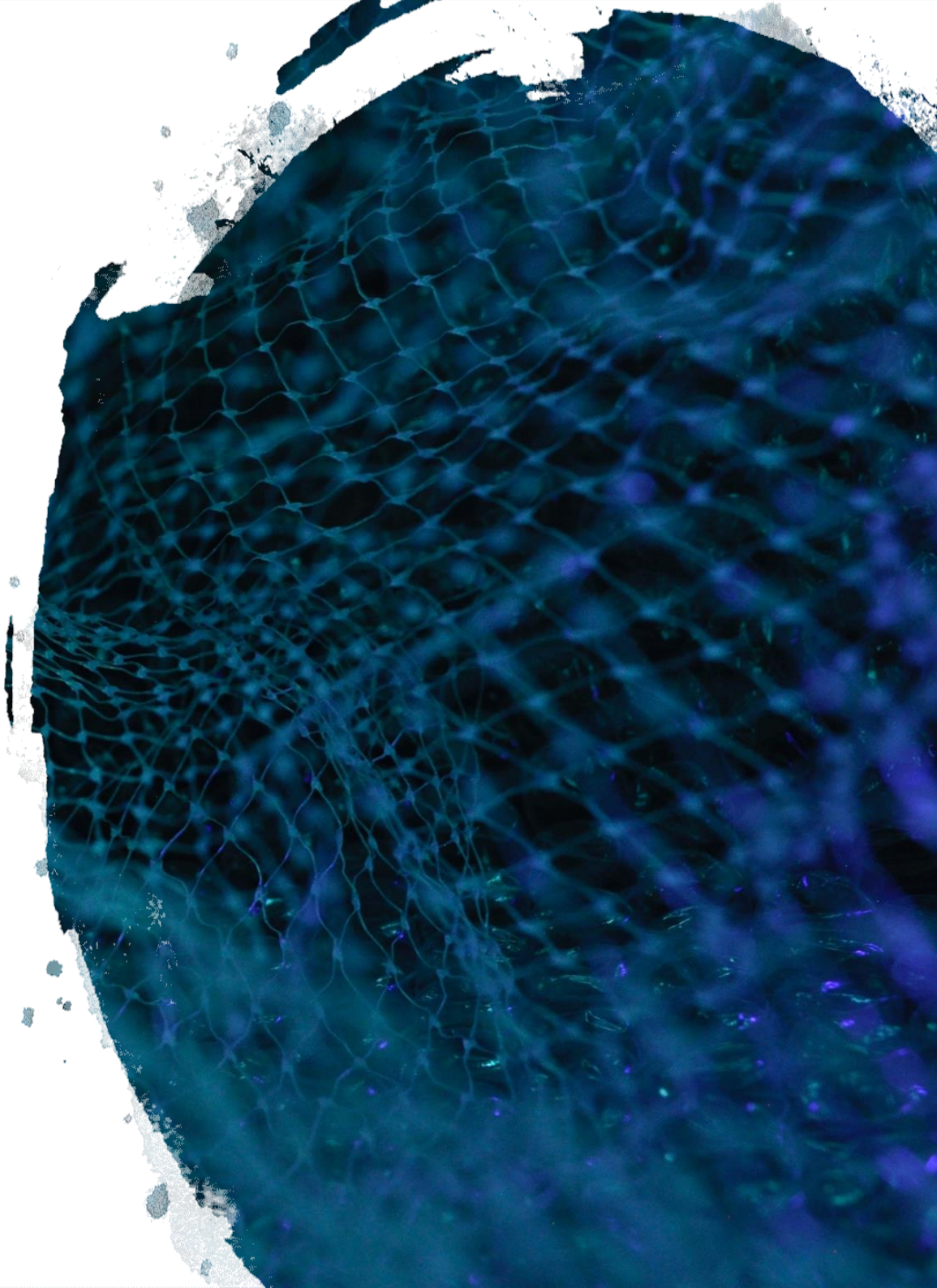
The Most Popular SCEF Functions are:

Starting the device
Starting up the device performs application-specific actions, including communicating with the Service Capability Server (SCS). The memory allows the SCS to send information to the UE via the 3GPP network to cause the UE to perform application-specific actions, which include initiating communication with the SCS for the indirect model or AS in the network for the hybrid model. The device must be started when the IP address for the UE is not available or is not available for the SCS / AS.

The SCEF API exposure function provides the following capabilities:
1. Monitoring of events and status
(allows the SCS / AS to open internal capabilities in the 3GPP core network).
2. Service Configuration
(allows the SCS / AS to assist the 3GPP core network in efficiently configuring core 3GPP network services).
3. SCS / AS and network coordination
(allows the SCS / AS to better coordinate with the 3GPP core network).
4. NIDD

KaurIoT SCEF: T8

Examples of Monitoring Events



Examples of Monitoring Events

Loss of Connectivity
Informs AS that UE is no longer available for data traffic or signal exchange. The event occurs when the "mobile reachability timer" for UE expires on the MME.

In a request for this type of monitoring, AS can specify its "Maximum Detection Time" value - if UE does not show any activity during this time, AS will be informed that UE is not available, indicating the reason. The event also occurs if the UE has been forcibly removed by the network for any reason.

For the network to know that the device is still available, it periodically initiates an update procedure, the Tracking Area Update (TAU). The frequency of this procedure is set by a network timer T3412 or (T3412_extended in the case of PSM), the value of which is transmitted to the device during the Attach procedure or the next TAU.

Mobile reachability timer is usually several minutes longer than T3412. If the UE before the expiration of "Mobile reachability timer" has not made TAU, the network considers it more inaccessible.

Examples of Monitoring Events

UE Reachability
Shows when UE becomes available for DL traffic or SMS. This occurs when the UE becomes available for paging (for eDRX UE) or when the UE switches to ECM-connected (for UE in PSM or eDRX mode), i.e. makes a TAU or sends an uplink package.

Location Reporting
This type of monitoring event allows AS to request UE location data. Either the current location (Current Location) or the last known (Last Known Location, defined by the cell ID from which the device made TAU or transmitted traffic last time) can be requested, which is relevant for the devices in low-power mode (s) like PSM or eDRX.

For "Current Location", AS can request repetitive reports, and MME will inform AS each time the device location has been changed.

Examples of Monitoring Events

Change of IMSI-IMEI Association
When activating this event, SCEF begins to track the change of the IMSI (Sim Card Identifier) and IMEI (Device Identifier) link. When an event occurs, it informs AS. It can be used to automatically transfer an external ID to the device during scheduled replacement operations or serve as an identifier for theft of the device.

It can be used to automatically reassign an external ID to the device during planned replacement work, or serve as an identifier in case of theft of the device.

Roaming Status
This type of monitoring is used by AS to determine whether the UE is in a home network or in a roaming-partner network.

Optionally, the PLMN (Public Land Mobile Network) of the operator in which the device is registered can be transferred.

Examples of Monitoring Events

Communication Failure
This type of monitoring informs AS about failures in communication with the device, based on the reasons for disconnection (release cause code) received from the radio access network (S1-AP protocol).

This event may help to determine the cause of the communication failure due to problems on the network, such as the overload of eNodeb (Radio resources not available) or the failure of the device itself (Radio Connection With UE Lost)

Availability after DDN Failure

Informs the AS that the device has become available after a communication failure. It is used when it is necessary to transfer data to the device, but the previous attempt was unsuccessful, since the UE did not respond to the notification from the network (paging), and the data was not delivered.

If this type has been requested for the UE, then as soon as the device makes an incoming communication, makes a TAU or sends data to uplink, the AS will be informed that the device has become available. Since the DDN (downlink data notification) procedure works between MME and S / P-GW, this type of monitoring is available only for IP devices.

Examples of Monitoring Events

PDN Connectivity Status

Informs the AS when the device status (PDN connectivity status) is changed - connected (PDN activation) or disconnected (PDN deletion).

This can be used by the AS to initiate communication with the UE, or vice versa, to understand that communication is no longer possible. Available for IP and non-IP devices

Number of UEs Present in a Geographic Area

This type of monitoring is used by AS to determine the number of UEs in a specific geographic area.

KaurIoT

Our contacts

Tel: +7 (904) 335-5503
Email: info@kauri-iot.com
Web: kauri-iot.com