D3.2

Integration of Trustworthy Disaggregated Computing Architecture

Funded by
the European Union

Revision v1.0

Work package	WP3
Task	T3.2, T3.3, T3.4, T3.5
Dissemination level	PU – Public, fully open. e.g., website
Deliverable type	R – Document, report (excluding periodic and final reports)
Due date	30-09-2024
Submission date	30-08-2024
Deliverable lead	Cyberus Technology (CYB)
Version	v1.0
Authors	Marco Bertuletti (ETH), Romain Beurdouche (EUR), Gian Michele Dell'Aera (TIM), Werner Haas (CYB), Efstathios Katranaras (SEQ), Laurent Petit (NNF), Michael Roitzsch (BI), Frida Strömbeck (CHAL)
Contributors	Work package partners (see below)
Reviewers	Michael Roitzsch (BI)

Abstract

The COREnext architecture is finalized across terminal devices, base station, and edge cloud. Feedback from component development is integrated to inform validation of architectural building blocks in WP6 as well as trustworthiness in WP2.

Keywords

architecture, terminal device, base station, edge cloud, trustworthiness, efficiency

Document Revision History

Version	Date	Description of change	Contributor(s)
v0.1	24-04-2024	initial table of contents and outline	Michael Roitzsch (BI)
v0.2	28-08-2024	content to added for all sections	Marco Bertuletti (ETH), Romain Beurdouche (EUR), Gian Michele Dell'Aera (TIM), Werner Haas (CYB), Efstathios Katranaras (SEQ), Laurent Petit (NNF), Michael Roitzsch (BI), Frida Strömbeck (CHAL)
v1.0	30-08-2024	final edits after review	Michael Roitzsch (BI)

Contributing Partners

Abbreviation	Company name
BI	BARKHAUSEN INSTITUT
EAB	ERICSSON
CHAL	CHALMERS
CYB	CYBERUS TECHNOLOGY
EUR	EURECOM
SEQ	SEQUANS
RAD	RADIALL
TIM	TELECOM ITALIA
WINGS	WINGS ICT SOLUTIONS
NOK	NOKIA NETWORKS GERMANY
NNF	NOKIA NETWORKS FRANCE
IIIV	NNF/IIIV LABS

Disclaimer

The information, documentation and figures available in this deliverable are provided by the COREnext project's consortium under EC grant agreement **101092598** and do not necessarily reflect the views of the European Commission. The European Commission is not liable for any use that may be made of the information contained herein.

Copyright Notice

Executive Summary

COREnext deliverable D3.2 incorporates results from component improvements researched in WP4 (digital) and WP5 (analogue) into an overall system architecture supporting:

- terminal devices,
- base station, and
- edge cloud applications.

As such it marks the completion of architecture-level research and provides feedback to the final report on trustworthiness (D2.3). More importantly, it also defines the general framework for lab validation activities in WP6.

Main drivers of the proposed architecture are:

- more energy efficient data processing (fixed function accelerators, vector processing extensions, many-core processor arrays),
- more energy efficient data movement (polymer microwave fibre interconnect),

paired with

- better isolation of heterogeneous compute components (HW/SW co-designed M3 platform, FPGA multi-tenancy)
- extended authentication (RF fingerprinting, Trusted Execution Environments (TEE), token-based access)

Key performance indicators for the envisioned use cases in automotive, extended reality, and smart city applications are latency, throughput, and power consumption parameters, as well as implications regarding hardware overhead, isolation properties, and attack surface reduction.

Table of Contents

List of Figures

List of Tables

Acronyms and Definitions

IoT	Internet of Things
KPI	Key Performance Indicator
PMF	Polymer Microwave Fiber
RF	Radio Frequency
TEE	Trusted Execution Environment

1 Introduction

The official project summary defines the goal of the COREnext project as 'a computing architecture and digital components for sustainable and trustworthy B5G and 6G processing.' Work package 3 is labelled 'Trustworthy Disaggregated Computing Architecture' which can be described in simpler terms as a design approach that separates the hardware components of a computing system into independent, modular units. This allows for greater flexibility, scalability, and resource optimization. Obviously, such a new architecture introduces novel challenges that its components must be designed to overcome. Energy efficiency of existing off-the-shelf components is insufficient and foregoing a monolithic approach heightens the demand for built-in security features.

Deliverable D3.2 has to be seen in broader project context as it builds on the component descriptions from D3.1 and incorporates feedback from work in the digital and analogue domain performed in work packages 4 and 5 with their corresponding deliverables D4.2 (Heterogeneous acceleration for efficient processing), D4.3 (Trustworthy computation and orchestration), and D5.1 (First concepts for trustworthy radio links through HW imperfections and localisation). In essence, this document refers to the combination of individual technological advancements to create a cohesive and functional system.

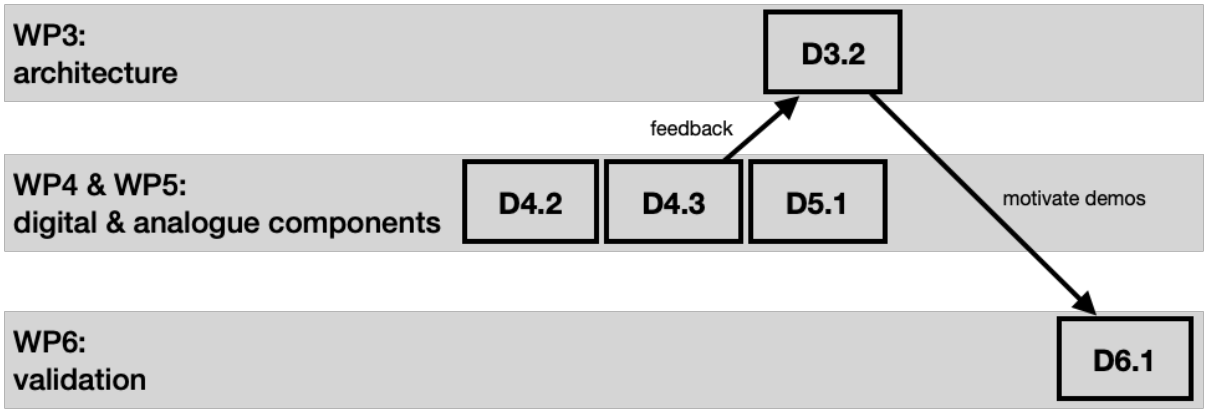

Figure 1: Overview of deliverables connected to D3.2 and the flow between them

D3.2 serves as bridging document between the technical research and development activities (WP4/5) and the use cases enabled by next generation mobile communication. COREnext decided to investigate:

- extended reality,
- automotive infrastructure, and
- smart city applications.

Hence, the following content consolidates results and provides feedback to work package 2 which looks at the requirements with a specific focus on the trustworthiness aspect. Furthermore, D3.2 feeds into work package 6 where results from the proposed architecture with its individual components are validated in the lab against WP2's use cases.

The usage scenarios for D3.2's architecture remain the same as already identified in D3.1, namely

- terminal devices,
- base stations, and
- edge cloud.

While base stations are likely under tight control by the manufacturer, we expect terminal devices may include untrusted 3rd party elements and similarly edge cloud scenarios where part of base station functionality is consolidated and processed with common (=untrusted) datacentre hardware. Section 2 of this document provides further details and discusses the associated cost/benefit trade-offs.

Section 3 provides further details on the use cases. Starting from a generic analysis of the processing requirements it lists the specific requirements that must be met to make the COREnext architecture a viable alternative. These requirements are objective in nature, that is we list physical quantities that can be measured. The corresponding validation will be performed as part of WP6 using proof-of-concept-style demonstrators.

As opposed to the tangible properties discussed in section 3, more abstract aspects related to security are the topic of section 4. Starting point is the assumption that next generation mobile communications will extend to machines as first-class network citizens. Hence the analysis is performed from an Internet-of-Things (IoT) point of view and ranges from traditional IT security concepts to PHY-level considerations.

2 Component Needs

As already outlined in preceding D3.1, COREnext aims to contribute trusted base station and terminal architectures with the additional wrinkle of incorporating 3rd party application platforms. To enable the intended use cases, it is paramount to improve on the current state-of-the-art both in the analogue and digital domains with respect to operational efficiency and system trustworthiness. These two dimensions lead to work at component level in the four quadrants depicted in **Table 1**.

	Digital	Analogue
Efficiency	Power-efficient signal processing	Power-efficient high-throughput interconnect
Trustworthiness	Heterogeneous compute platform with TEEs	Radio link authentication and infrastructure attestation

Table 1: Four quadrants of COREnext components

Given the expected growth in mobile traffic from ubiquitous machine to machine communication, energy efficiency becomes a 'make or break' system property. It can be considered in two complementary dimensions, namely data processing and data transport. The necessary improvements are delivered on digital and analogue level, respectively. However, digital signal processing must still be compliant with protocol standards which define latency and throughput requirements. D3.1 identified data rates of at least 100 Gbps and 10x end-to-end latency reduction as targets for WP4/D4.2. Results regarding interconnect energy efficiency improvements are expected towards the end of the COREnext project so they are not considered in D3.2.

Trustworthiness inherently lacks objective, measurable parameters akin to latency or energy consumption. Instead, authentication and isolation properties serve as indirect indicators for system security evaluation. D3.1 suggested radio link level authentication as promising candidate to bolster physical layer security. WP5/D5.1 identified parameters suitable for RF fingerprinting which were picked up by the corresponding digital processing analysis in WP4/D4.3. Data processing, for example by applying machine learning to fingerprinting algorithms, falls within D4.2's accelerator research, though. D4.3's main contributions are concepts for component isolation and orchestration: a microkernel-based system architecture, virtualisation of accelerator resources like DSPs and FPGAs, and management functionality suitable for IoT scenarios. Evaluating the associated overhead in terms of hardware resources and latency increase are subject of ongoing research.

2.1 Power-Efficient Signal Processing

D4.2 addresses the **heterogeneous signal processing platform** for PHY and MAC developed in COREnext project. While the trustworthiness aspects are analysed in D4.3, D4.2 focuses on the processing capabilities required for the platform. The components developed and described in the deliverable are based on the RISC-V Instruction Set Architecture (ISA), which offers two main advantages: it is **open source**, and it is **extensible**. Being an open-source ISA, RISC-V is transparent to the user, enhancing the trustworthiness of the component. As an extensible ISA

it allows the development of telecommunication-specific extensions, opening opportunities for hardware-software co-design.

Three aspects were analysed in the design of the heterogeneous platform. First, the processing platform will occupy a **Remote Unit (RU)** or a **Distributed Unit (DU)** of 5G and beyond-5G networks. Its position in the telecommunication infrastructure is strategic to reduce the user-experienced latency and improve the quality of service. Therefore, the platform must address the most compute-intensive functions of 5G New Radio physical layer and medium access control layer, in uplink and downlink.

Second, the processing platform must host **programmable** components. Programmability must be considered as one of the soft key performance indicators (KPIs) of the implemented hardware. COREnext develops reconfigurable and programmable hardware, following a Software Defined Radio (SDR) paradigm. Most of the network functions are implemented in software, rather than on application-specific circuits. This allows us to keep up with a fast-evolving standard, reduce the time-to-marked of a baseband processing solution, and increase the return on investments of the deployed network components.

Third, the developed components must align to **hard latency-throughput and power-area consumption KPIs**. D4.2 presents the development progress of a ManyCore and a Vector RISC-V programmable Processors for the lower and high PHY. The ManyCore processor executes a 5G-PUSCH symbol, in a high load use-case in <2ms. Power simulations in the post-Place and Route stage demonstrate an average power consumption of < <6W. The design, including 1024 cores and 4MiB of SRAM occupies an area of 82mm2 in 12nm technology. The high speed-up obtained by optimizing the RVV-ISA of the Vector Processor compared to a scalar ISA suggests that merging the ManyCore and the Vector paradigm could bring further advantages. To complete the functions required to implement all the PHY on the execution platform and move it to the RU, according to 5G split 7.3, we chose to trade off programmability with latency and energy efficiency. We offload the FEC task to a specialized accelerator. On the designed accelerator we obtained throughput up to 1200 Gb/s for coded streams and 1000 Gb/s for uncoded streams, which is not a bottleneck for executing lower PHY in the ManyCore and Vector Processors. The placed and routed FEC accelerator occupies 5mm2 in 28nm technology.

In D4.2 we also describe the architecture of a scheduling accelerator for the MAC layer. A RISC-V SoC including a 64b programmable Linux-capable host is used to offload tasks to the accelerator, again bringing programmability into focus. The SoC including the accelerator is currently under development (more details can be found in D4.2). Measurement on a prototype or FPGA implementation is planned, to extract all the relevant KPIs.

2.2 Heterogeneous Compute Platform with TEEs

Accelerated signal processing as described above must be part of an overall architecture to isolate signal data flows. When data streams from multiple tenants are processed by a single device, for example on a base station serving multiple terminals, the data flowing between the different accelerators must be separated. On the other hand, any security primitives and corresponding

orchestration and resource management must not add prohibitive overheads as the data flows between different accelerators and general-purpose processor cores.

This need for **strong yet efficient isolation** becomes even more apparent as third-party applications become integrated into the radio access network (RAN) with initiatives like O-RAN. There, code from third-party developers will run within the RAN to allocate and configure data streams from terminal devices while interacting with external infrastructure in first- or third-party clouds.

Work package 4 delivers four component contributions to address this need:

- the M³ microkernel-based system,
- FPGA multi-tenancy,
- digital signal processor virtualization, and
- an Internet-of-Things (IoT) management layer.

These components employ **control of communication paths** by a trusted orchestrator as a key mechanism for isolation. This principle is exemplified by the **M³ platform,** which is a co-designed hardware and microkernel-based software architecture for systems-on-chip (SoC) compute devices. Each compute resource is placed in its own isolated tile. Any communication between tiles is passed through a special security component, the Trusted Communication Unit (TCU), which enforces a communication policy. These policies are programmed into the TCU by the M³ kernel, which abstracts communication rights with a capability system that higher-level resource managers can use.

Within such an SoC platform, compute resources can be a mix of general-purpose cores and accelerators. Two kinds of accelerators are **FPGAs and DSPs,** which pose specific challenges when securely multiplexing such a device amongst different tenants. Based on virtualization and attestation techniques, work package 4 offers solutions. While M³-based SoCs can be scaled from terminal to base station needs, high-capacity deployments, require aggregating multiple SoCs across a network. Solutions like Data Processing Units (DPUs) and **Trusted Execution Environments (TEEs)** become relevant for security in distributed service environments. Within work package 4, the M³ platform will be extended with such TEEs. Using such a distributed trust infrastructure, an **IoT management layer** can orchestrate and trust-evaluate terminal devices such as Internet-of-things device fleets.

These components delivered by work package 4 will individually be evaluated according to their costs and benefits. Since these are trustworthiness-enhancing components, their benefit lies in a security enhancement that can be quantified by their capability to separate clients and their communication paths. Costs on the other hand come as additional hardware investments or runtime latency overheads. We refer to deliverable D4.3 for more details.

2.3 Power-Efficient High-Throughput Interconnect

To enable the disaggregated and distributed data processing expected in next generation mobile communications, highly efficient, high speed, short-range links for up to a few meters distance are required. Sub-THz communication over plastic fibre can offer data transfer rates beyond 100 Gbps over a single lane. The polymer microwave fibre (PMF) is an interesting alternative due to its

potentially low cost, and energy efficiency. With less than 1 pJ/bit energy consumption, the technology is orders of magnitude more energy efficient than conventional electrical cables and compete with optical communications for distances up to a few meters.

Compared to optical fibres, PMFs are less sensitive to temperature variations. Furthermore, the alignment to the PMF is much simpler because of the larger size of the PMF, thus offering a more robust solution. Ultra-high data rates can be achieved by using a larger bandwidth instead of higher order modulation schemes.

The transceiver complexity can be kept limited and the energy consumption low. They can be implemented using silicon technologies such as CMOS and SiGe, and they do not require expensive extensions such as the silicon photonics or III/V photonic platforms needed to implement optical active cables.

The signal link can be implemented with connectors attached to the PMF fibre end and efficient circuit to fibre transitions that can be implemented in low-cost packaging technologies such as organic printed circuit boards (PCB) or embedded wafer level packaging (eWLP), where the transition is implemented in the form of antennas radiating into the fibre.

The fibres are fabricated using plastic polymers such as Teflon (PTFE) or polyolefins (HDPE-preferred for better sustainability over PTFE) and benefit from low-cost industrial extrusion fabrication processes, leveraging plastic fibres originally developed for other applications such as ink jet printing and medical applications. Several geometries are considered, from hollowed cylinder section to solid rods and more complex geometries as the cross-shaped PMF developed at BINP, with diameters ranging from 2mm (for the D-band) down to 0.9mm (for the H-band).

Proper optimized design must be developed to get the best RFIC to PMF coupling and preserve the signal integrity of the high data rate communication.

The chip to PMF interconnection is crucial. As Europe plans to ban PTFE, used for high performance PCB, alternative technologies allowing the implementation of modules required between the chip and the PMF such as diplexers are highly desired. For this reason, the AFSIW (Air-Filled Substrate Integrated Waveguide) technology introduced at BINP will be developed and investigated for operation at D-band and beyond. Such a scheme would provide a more sustainable approach to reach the interconnection needs.

2.4 Radio Link Authentication and Infrastructure Attestation

All radio transmitters are impacted by imperfections, mainly in the RF front end, introducing distortions and errors in the transmitted signal, which can cause the constellation of the transmitted signal to deviate from the ideal shape. The concept of RF Fingerprinting is to exploit these unique hardware impairments in transmitters to identify and authenticate radio equipment such as UEs and access points, to increase the trustworthiness and security of telecommunications at the physical layer. This basic concept has been known for decades but remained too limited to be used for physical layer security on a large scale.

An example of early work on RF Fingerprinting is the paper [ELL01]. While this paper is two decades old, it shows clearly the idea behind the RF Fingerprinting concept: identifying transmitters based on their unique features, caused by non-linearities, in the transmitted electromagnetic spectrum. It also introduces three fundamental characteristics for the RF Fingerprint to be exploitable, that are still valid today:

- **Uniqueness:** To be able to identify a radio based on these features they must be unique for each radio.
- **Consistency:** To be able to perform identification based on fingerprints, these fingerprints must be consistent irrespective of the elapsed time between them.
- **Universality:** The fingerprint characteristic should appear nearly identical regardless of the receiver equipment.

The use of machine learning algorithms for automated RF Fingerprint recognition is a more recent development and enables the use of the RF Fingerprinting concept for physical layer security at the network level. The idea behind using ML for RF Fingerprinting is to train a model using a set of labelled RF fingerprint data, which consists of a collection of signals transmitted by various wireless devices.

Labelled RF fingerprint data can be obtained during the training phase when one collects RF fingerprint data from each UE and labels it with a unique identifier that corresponds to the identity of each specific UE. Once the machine learning model has been trained, the unique fingerprint for each UE is stored in a database. During the inference phase, when a UE sends a signal, the IQ samples are then fed into the machine learning model, which compares them to the stored fingerprints in the database to determine the identity of the UE.

In COREnext, we are focusing on applying the RF Fingerprinting concept in the context of physical layer security. In other words, we focus on increasing the trustworthiness of radio links through knowledge on unique hardware imperfections from a radio nodes perspective.

For this purpose, we defined our work scenario as being the authentication of a UE by a radio access node (e.g. base station, access point, etc.) in the context of wireless communication (5G, 6G, LTE, Bluetooth, WIFI, etc.).

3 Trustworthy Computing Architecture

In Deliverable D3.1, we have sketched a COREnext architecture for the three tiers terminal devices, base stations, and edge cloud (see Figure 2). We have separated the tiers into areas, where we believe hardware developed by COREnext is most beneficial and areas where we will integrate and augment existing hardware and operating system stacks. This leads us to four innovation areas:

- terminal devices based on COREnext hardware,
- terminal devices based on third-party hardware,
- COREnext base stations, and
- mobile edge cloud nodes based on third-party hardware.

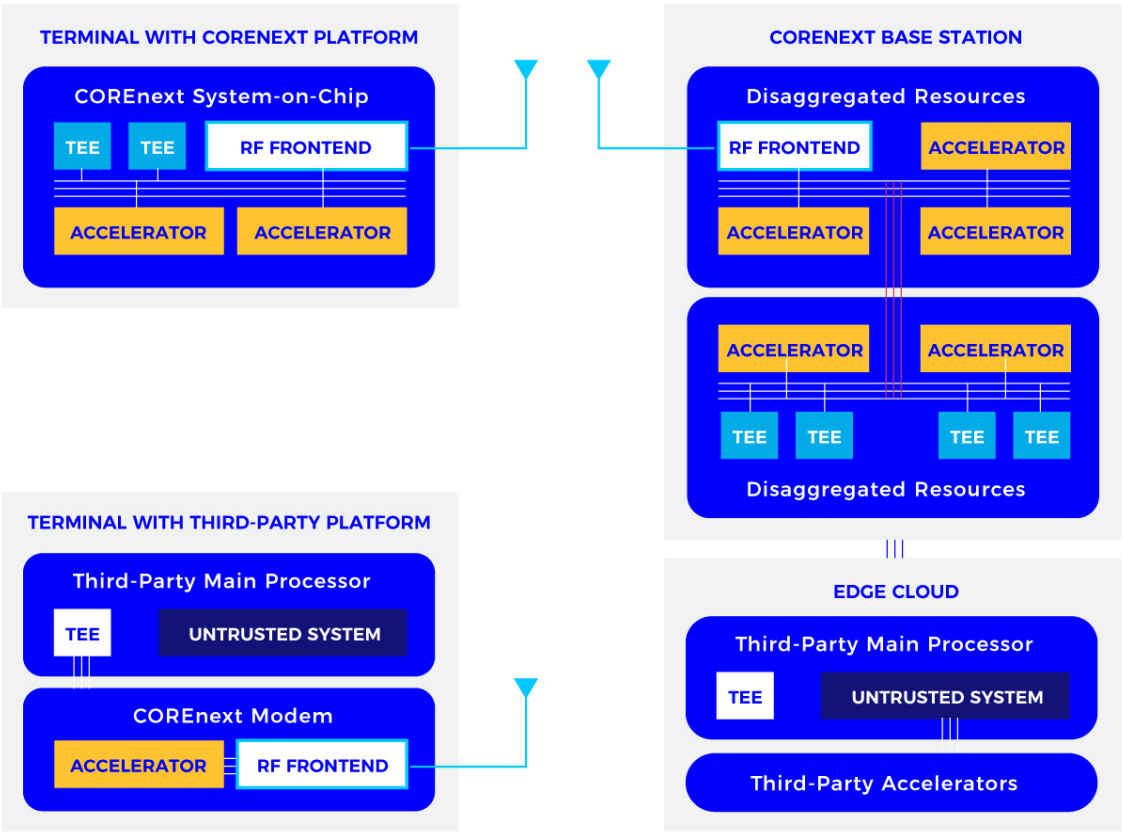

Figure 2: COREnext architecture with highlighted component innovations

Further, we have identified component needs to implement this architecture, which we summarized as:

- novel signal processing accelerators (marked yellow in the figure),
- novel high-throughput interconnects (marked red in the figure),
- radio link authentication and infrastructure attestation (marked blue in the figure), and
- novel heterogeneous trusted execution environments (marked cyan in the figure).

Deliverable D3.1 handed these needs to work packages 4 and 5. In this deliverable (D3.2), we now map the innovations developed in these two component work packages back to our architecture.

We refine the architecture and derive criteria and performance indicators for the validation of our work in work package 6.

3.1 Terminal

Terminal devices cover a wide variety of form factors, performance envelopes, and energy constraints. Everything from a tiny IoT sensor to a self-driving car is a terminal device in mobile network connectivity. Due to this diversity, we assume we need to cater for devices that will fully transition to a COREnext-provided compute and communication solution as well as for devices that will continue to use existing compute platforms and operating system stacks.

3.1.1 Terminals with COREnext Compute Platform

Devices designed from the ground up for new use cases can utilize the COREnext platform for both communication and compute. The COREnext SoC in these devices leverages purpose-built accelerators and cores with instruction set extensions to perform 6G signal processing efficiently. Orchestration between these accelerators is based on the M³ architecture, which integrates accelerators and general-purpose cores in a trustworthy way.

Trusted Execution Environments (TEEs) shield compute environments from manipulation and allow outside parties to verify their integrity. Such verification can be used for fleets IoT devices to assess that software deployed in the field is in a trustworthy state. Within COREnext, we enhance state-of-the-art TEEs with accelerator integration to combine the trustworthiness benefits of TEEs with the efficiency benefits of accelerators. For large-scale IoT deployments in critical infrastructure, both efficiency and trustworthiness are key parameters.

In addition to critical infrastructure, we see COREnext terminals applicable in medical devices, as well as industrial and personal robotics use cases. These particularly privacy-sensitive areas benefit from COREnext's **trustworthiness-by-design** approach of protecting sensitive data with strong hardware-level isolation. Using COREnext-developed radio link authentication, the terminal can check the validity of the base station it connects to, which is especially relevant in campus networks. With this technique, data protection on device can be extended to the network infrastructure by sending sensitive data only to an attested remote environment.

Components relevant for terminal architecture	Cost	Benefit
Novel signal processing accelerators ▪ RISC-V-based many-core arrays ▪ RISC-V cores with vector extensions ▪ FEC and MAC accelerators	Chip area	Latency, Performance per Watt
Novel heterogeneous trusted execution environments ▪ M³ architecture with TEEs ▪ IoT management orchestration	Added latency, Hardware cost	Isolation, Attack surface reduction
Radio link authentication and infrastructure attestation ▪ Base station validation	Added signal processing	Early authentication

3.1.2 Terminals with Third-Party Platform

We must assume that terminal devices with non-COREnext compute stacks will continue to exist. These devices will utilize COREnext technology within the radio modem, using the same signal processing accelerators for increased efficiency as COREnext terminals. However, they will use a third-party SoC as the basis for compute workloads. This SoC will be governed by a third-party operating system and application stack. Examples for such devices are future versions of Android and iOS phones as well as upcoming device categories such as mixed-reality glasses.

When integrating a COREnext modem, these devices gain access to advanced 6G radio functionality. In particular, 6G is positioned to include **sensing capabilities,** where radio frequencies are used both for communication and radar-like scanning of the physical environment. Especially in mixed-reality applications, such sensing capabilities enable new use cases for positioning and contextual awareness of augmented reality content. However, sensing comes with wide-ranging **privacy implications.** A continuous and invisible stream of environmental information is captured, even for bystanders with no opportunity to opt out. If such sensitive data is made available without precaution to the third-party operating system and applications within the non-COREnext compute environment, data protection can no longer be enforced by design. While COREnext does not work on sensing capabilities themselves, we need to address this challenge to trustworthiness.

We postulate that the third-party compute environment must offer its own flavour of TEEs that can be verified from the COREnext modem. In this way, the third-party hardware can **prove to the modem,** which software service is running within the TEE. Only if such a service is deemed trustworthy, the modem will establish an encrypted tunnel to the TEE and stream sensing data through this tunnel. The third-party operating system and applications never gain any visibility of the sensitive data, because it is encrypted. Key material for decryption is only known to the service running within the TEE. Regulatory measures must be set up to audit the software of sensing services running in these TEEs to assure their trustworthiness and award them granular permissions to access sensing data. We also envision the use of memory-safe languages and formal verification to substantiate the trustworthiness of sensing software.

It should be a **regulatory requirement** for third-party compute platforms to offer such TEEs. Sensing data should never be made available to such platforms without verified and audited TEE protection.

Components relevant for terminal architecture	Cost	Benefit
Novel signal processing accelerators ▪ RISC-V-based many-core arrays ▪ RISC-V cores with vector extensions ▪ FEC and MAC accelerators	Chip area	Latency, Performance per Watt
Novel heterogeneous trusted execution environments ▪ regulatory requirement for third-party TEEs to access sensing data from modem	Policy process	Privacy protection

3.2 Base Station

The base station accumulates data streams from many users and performs signal processing on them. Therefore, challenging requirements on efficiency and trustworthiness must be addressed. Efficiency of the signal processing is needed to handle the data volume with low latency and adequate power consumption to reach sustainability targets. Trustworthiness is needed such that data from different users is securely separated. With O-RAN, **code from third-party developers** will run within the RAN to allocate and configure data streams from terminal devices while interacting with external infrastructure in first- or third-party clouds. These O-RAN apps must also be securely **sandboxed and isolated** from user data.

To provide this high degree of trustworthiness, we again rely on the M³ architecture as the foundational layer. It integrates different compute resources such as accelerators and general-purpose cores with a deny-by-default approach to communication control. Data exchange between these compute resources is only allowed, when it is necessary to fulfil a functional requirement. The compute resources for signal processing efficiency draw from the same set of accelerators developed by COREnext: RISC-V-based many-core arrays, RISC-V cores with vector extensions, accelerators for FEC and MAC.

Base stations may also integrate FPGAs and DSPs, for which COREnext implements multi-tenancy based on virtualization and attestation techniques. Such multi-tenancy allows to offer these compute resources also to O-RAN apps written by third-party developers. To ensure isolation and integrity of O-RAN apps and other infrastructure software components, we expect to utilize TEEs as trusted and attested execution containers. Compared to state-of-the-art TEE solutions, the COREnext TEEs added to the M³ architecture allow **secure interaction between heterogeneous compute resources** and software running on general-purpose processors. This level of integration allows to combine efficient accelerator access with the strong isolation afforded by TEEs. Like in terminals, TEEs can technically enforce regulatory rules for the handling of sensing data.

With the radio interface, base stations offer an attack surface that is by construction publicly available. COREnext offers **radio fingerprinting** as a first line of defence. The radio signals of terminals are analysed, and a terminal identity is verified before signal data reaches deeper stages of the processing and networking infrastructure.

Base station deployments must scale from densely populated urban environments to countryside locations as well as from high-volume rush hour periods to low-traffic nighttime. Simultaneously, the physical environment may be challenging in terms of antenna placement and placement of the corresponding processing hardware. To offer flexibility and scalability, base stations can employ **resource disaggregation** by clustering compute hardware into pools shared amongst multiple radio units. Compute hardware from these pools can be assigned flexibly based on current demand. A key requirement for such an architecture is a low-latency, high-capacity, energy-efficient interconnect. COREnext is developing such an interconnect based on polymer fibres to enable such novel disaggregated base station topologies.

Components relevant for base station architecture	Cost	Benefit
Novel signal processing accelerators ▪ RISC-V-based many-core arrays ▪ RISC-V cores with vector extensions ▪ FEC and MAC accelerators	Chip area	Latency, Performance per Watt
Novel heterogeneous trusted execution environments ▪ M³ architecture with TEEs ▪ FPGA multi-tenancy ▪ DSP virtualization	Added latency, Hardware cost	Isolation, Attack surface reduction
Radio link authentication and infrastructure attestation ▪ Terminal validation	Added signal processing	Early authentication
Novel high-throughput interconnects ▪ Polymer microwave fibres	Hardware investment	Energy usage per Bit

3.3 Edge Cloud Nodes

Cloud infrastructure is an area, where we assume deployment of third-party datacentre hardware. While the M³ architecture can be scaled to datacentre workloads, the accelerator developments in COREnext are specialized for signal processing workloads. As a building block for security, we do assume TEEs in the edge cloud, either provided by third-party processors or by M³-based COREnext hardware. Such TEEs are the basis for attestable compute environments that terminal devices can use to **securely offload computation.** Using remote attestation, a terminal can cryptographically ascertain the validity of a TEE and establish an end-to-end encrypted secure communication channel to the TEE. This channel can then be used for offloading of compute workloads to cloud infrastructure, that are too demanding for the terminal (like AI workloads with large models) or that require data only available from a central vantage point in the cloud (like fused sensor data from multiple IoT devices). The FPGA multi-tenancy and DSP virtualization solutions can be used to offer acceleration capabilities to software running in the edge cloud.

Components relevant for edge cloud architecture	Cost	Benefit
Novel heterogeneous trusted execution environments ▪ M³ architecture with TEEs ▪ FPGA multi-tenancy ▪ DSP virtualization ▪ IoT management orchestration	Added latency, Hardware cost	Isolation, Attack surface reduction

4 Validation of the Architecture

4.1 Performance Range for Example Scenarios

Quality of Service in a commercial base station is configured depending on the use case and the load could be scaled with demand in the limit of licensed spectrum. So, there is not one typical usage scenario for a base station. Transmission quality is another factor that can make the processing requirement vary a lot from one case to another.

Though, recorded performance and loads in experimental setups give a quantified order of how much a computing device could be loaded by running a network. The processing time of a slot - a fixed bandwidth and time interval – is recorded on a restricted compute resource for several well-defined configurations through simulation.

The uplink traffic creates the most significant part of computation load at the base station. Configurations with high data rate achieved with optimistic assumptions on the radio conditions are the most compute intensive especially if the radio conditions are relatively bad in reality. For example, the processing of a slot in the uplink direction with a bandwidth of 100MHz, a MCS – an indicator of data density within the resource - of 20 and a SNR - representing the noise level relative to the signal level – of 5.9dB, can hold a single 4.3GHz x86 core with 512 bits SIMD ISA extension for up to 2.5 milliseconds. With an additional DSP the same task is done in 1.1 milliseconds. Better radio conditions of course reduce the processing time. With the same setup with one x86 core, the processing time shrinks to 1.9 milliseconds with a SNR of 9.2dB and to 1.6 milliseconds with a SNR of 13.1dB. The amount of data to process and the slot processing time are proportional to the amount of radio resource - which is the bandwidth -. They increase with the bandwidth. 100MHz is the higher bandwidth that could be tested. The MCS is an index that represents the density of data fitted within the available resources through the technic of modulation. The processing time of course increases with the density represented by this MCS. 20 corresponds to the higher density that could be tested.

As stated here above, the load on the system varies a lot with the use cases. On the opposing hand of the previous case of maximum possible load, the standard also allows to operate a base station with a 5 MHz bandwidth and a MCS of 0 for which, with a SNR of –1dB, the processing of an uplink slot takes only 0.08 milliseconds with the same single x86 core.

This shows again how it is important to adopt a scalable design for the computing devices running a network.

4.2 Component Validation Targets

Based on the scenarios considered in WP3 and the four component quadrants listed earlier in **Table 1**, we envision the following four validations to corroborate our findings with lab experiments:

- Accelerators for signal processing workloads
- Baseband workload emulation on an M³ platform using trusted execution environments
- RF fingerprinting classification
- Interconnect using polymer microwave fibre

KPIs for the M³-based validation are the power consumption at different throughput/latency operating points. Target goals for signal processing are derived from envisioned 6G performance metrics such as peak data rates exceeding 100 Gbps with end-to-end latencies <1ms and 10-100 times energy efficiency compared to current 5G technology. These numbers also inform the interconnect validation. The use cases considered in WP2 list the following requirements for its terminal devices:

- Latency < 5ms
- Throughput < 500 Mbps
- Battery life > 10 years

Validation of RF fingerprinting should be seen foremost as feasibility analysis of technologies strengthening trustworthiness of the system. However, it is expected to gain quantitative insight into the associated overhead in terms of additional hardware and performance impact.

4.3 Use Case Fit

In D2.1 3 Use Cases were identified, each representing a different family of services that 6G has to address:

- The **Extended Reality** Use Case is analysed as an example of the "Enhanced human communication and Entertainment", this a large family of use-cases for 6G networks that aims to enable more immersive and realistic interactions between people. The goal of this use case is to provide a highly immersive and interactive experience to users.
- The **Automotive Infrastructure** Use Case is an example of the "Enhanced Machine Communication" family wherein robots, vehicles, drones, or a generic not-human being interact with another not-human being or with a dedicated/public infrastructure. The goal of this use case is to enhance the safety, efficiency, and overall experience of vehicles and transportation systems.
- The **Smart City** Use Case is used to represent the "Intelligent Management" family where advanced technologies such as artificial intelligence (AI), machine learning (ML), and data analytics are exploited to automate and optimize business processes. The goal of this use case is leveraging on IoT devices, data analytics, and AI to optimize urban operations and improve the quality of life for citizens.

In the table below a list of End-to-End requirements are summarized for the three analysed use cases. The values are extrapolated by experimental service deployment (by TIM) where the definition "Not Critical" requirement means that the value is supported by the already available technologies:

Use Case	One to two key KPIs you plan to evaluate
Extended Reality	• **Latency**: lower than 20ms • **Throughput**: 30 Mbps - 40 Mbps per connected user • **Power consumption**: Not Critical • **Reliability**: Not Critical (except for safety applications) • **Number of Connected Devices**: Not Critical

Automotive Infrastructure	• **Latency**: 5 ms – 10 ms in Safety use case, otherwise lower than 100ms • **Throughput**: lower than 500 Mbps, depending on the information transmitted • **Power consumption**: Not Critical in Automotive • **Reliability**: 99.999% or more • **Number of Connected Devices**: 100 – 1000 connected devices to an Infrastructure Node
Smart City	• **Latency**: Not Critical • **Throughput:** Not Critical • **Power consumption**: up to 10 Years of battery life • **Reliability**: 99% - 99.9% • **Number of Connected Devices**: up to 10.000 IoT per km^2

The Extended Reality shows a critical E2E latency to be guaranteed, since the increase of latency can lead to Motion Sickness in the user. The amount of throughput to transmit is in the range of 30 Mbps – 40 Mbps per user when a Completely new Reality must be transmitted to the client. This is critical in use cases where multiples user experiment XR in the same location. The XR devices can highly consume battery life, especially because GPU hardware is contained in these devices. This hardware can be remoted at the server to reduce the power consumption but generally this is not a critical requirement. The Use Case reliability could be critical only in Safety scenario like remote driving or surgery, but in D2.1 this use case is inserted to extend the way to communicate or entertain.

The Automotive Infrastructure is often associated to safety scenarios that needs to guarantee an E2E latency lower than 10ms. The exchanged messages have typically small size, but in case of the exchange of images/videos, for example in the presence of Intersection Movement Assist (IMA) when multiple vehicles approach a large intersection, the data transmission in the system could arrive to several Mbps. The power consumption typically is not a problem for cars and at least in case of pedestrians or cyclists the software is installed on the smartphone or a similar device with around 1 day of battery life. The number of vehicles connected to a node of the infrastructure could become critical in dense urban areas where multiple devices try to connect to the same radio access.

The Smart City scenario involves a massive number of sensor/devices transmitting data with flexible periodicity. Both amount of data and latency are not critical in this use case, since typical transmissions are scheduled to minimize the battery consumption of the sensors that in some cases could not easily be changed. In some scenarios because of the position of the sensor the battery life must be also 10 years. For some types of safety sensors, like sensors for flame detectors or for structural health monitoring, a good level of reliability is required, while in other information collected by sensors the reliability could be relaxed. In any case, the number of devices that must be handled by the infrastructure could be massive.

5 Considerations for Future Smart IoT Architectural Needs

Looking beyond the COREnext component advancements, we discuss anticipated future architectural needs and practical considerations around smart IoT use cases. With 6G networks' low latency and sensing capabilities, we expect personal robotics, medical devices, and other large-scale and safety-critical scenarios as emerging trends. The following aspects describe practical security aspects that are outside of the research focus of COREnext but that must be considered architecturally in future mobile communication deployments.

5.1 Security in Cellular IoT Modems

In the past few years, there has been a notable rise in interest concerning security in a wide range of smart devices and computing systems. The complexity of this evolving IoT technological landscape further contributes to the general sense of insecurity, with people often finding it challenging to discern the actual risks associated with IoT devices. We discuss below the security aspects surrounding the integration of a cellular modem in an IoT device and the level of complexity required for security in such devices, concluding on important defence techniques and guidelines for efficient heightened security in future architectures. More information can be found in Sequans white paper [1].

5.1.1 Overview of Security on Cellular IoT Devices

Cellular IoT devices can be generally seen as a sum of two spaces: Host/Application and Cellular communication modem, as has also been described above. The application code is exclusively owned by the manufacturer and market-available application processors often termed as microcontroller units (MCU), each equipped with built-in security features such as a secure area, secure cryptographic engine, tamper detection, encrypted access to external memory and other advanced secured functions, run that code. Our focus here is on the other space, i.e., addressing the security aspect when integrating with a cellular modem for an IoT device, and especially low-power wide-area (LPWA) cellular modems for low-bandwidth IoT for industrial, smart city, smart home, and agriculture applications. These LPWA technologies (e.g., LTE-M and NB-IoT) target devices with reduced cost/complexity and power consumption while requiring high coverage and connection density capabilities.

A cellular modem constitutes a complex system including millions of lines of code and multiple sub-systems, inherently making it challenging to achieve complete security or absolute trust. It is thus important first to understand the threat/security level aimed to address which varies based on the application's importance (data sensitivity, access control requirements, etc.), industry, and potential impact of breaches. Generally, The CIA triad (Confidentiality, Integrity, Availability) provides a comprehensive framework for developing robust security strategies. Other concepts like identity protection for authenticity and accountability are often considered extensions to the CIA triad, enhancing the overall security posture. Below, we discuss briefly how these concepts apply to LPWA cellular modems.

a) **Confidentiality: safeguard data from unauthorized access to ensure privacy**

The data passing through the cellular modem is supposed to be encrypted by the application. So, spying on this data shouldn't provide meaningful information and application can randomize its data transmission patterns to safeguard such info from a nearby RF sniffer.

b) Integrity: ensure information accuracy/reliability to prevent unauthorized alterations

Integrity can be achieved by using cryptographic techniques such as message authentication codes (MACs) and digital signatures. These methods ensure that data remains unchanged and authentic.

c) Availability: ensure information/resources are accessible by authorized entities when needed

Denial of Service (DoS) attacks aim to disrupt the normal functioning of a device, network, service, or website by employing various methods to block or overwhelm the targeted system with excessive traffic. Remote attacks can be detected and mitigated on the network side while local attacks (physically damaging the device, removing the antenna, employing a nearby jammer) cannot be avoided.

d) Identity protection: safeguard user identities & prevent unauthorized access, tampering, theft

Subscriber identity information, including the International Mobile Subscriber Identity (IMSI), is stored on SIM cards, which act as secure elements. The SIM card holds unique cryptographic keys, employing algorithms like A3 for authentication and A8 for key generation, ensuring the integrity of subscriber identity. In parallel, dual authentication processes establish mutual trust between the mobile device and the network. Advanced encryption standards, such as A5/3, secure communication channels, protecting against eavesdropping and data interception.

Overall, it is apparent thar LPWA cellular modems inherently possess baseline security. In the realm of 3GPP networks (4G LTE and 5G), robust measures, including strong authentication, encryption, and SIM card security, ensure authorized access. Distinct treatments for signalling and user plane traffic, along with firewalls and intrusion prevention, bolster defence against diverse attacks. 5G's network slicing allows tailored security, prioritizing user privacy and adhering to regulations. Ongoing standards compliance maintain a consistently high security level.

5.1.2 Defence Techniques & Guidelines for Heightened Security

While cellular networks are inherently designed to be secure, it is crucial to acknowledge that they are not entirely immune to threats. To proactively address potential vulnerabilities, additional defensive measures need to be applied on the modem side to mitigate the risk of potential attacks:

a) Cellular module with secure boot and secure upgrade

Secure Boot ensures that only authorized and digitally signed software runs during a device's startup, guarding against malicious code during the boot process. It prevents unauthorized or tampered updates, maintaining the security and reliability of the device. Secure Upgrade focuses on the secure and controlled process of updating software or firmware to prevent the installation of unauthorized updates. Together, these mechanisms contribute to the overall security of computing devices, protecting against bootloader-level attacks and potential vulnerabilities introduced through software updates, ensuring a reliable way to revert to the original state in case the modem faces a security compromise.

b) Trusted vendor

Choosing an LPWA cellular module from a vendor who owns both the chipset and firmware enhances security through integrated development and unified security policies. This approach

enables faster responses to emerging threats with seamless updates and patches. The streamlined compatibility resulting from tight integration reduces the risk of security issues due to interoperability challenges. Quality assurance is improved as the vendor can conduct rigorous testing across both chipset and firmware components. The holistic security approach covers various levels, from hardware to software, providing a layered defence against potential threats.

c) Soldered SIM

As opposed to a plastic removable SIM, utilizing a soldered SIM card (eSIM) in the final deployed product, or even better using the Integrated SIM (iSIM) in the cellular chipset when this option is available, can enhance security by integrating the SIM directly into the IoT device's hardware. This integration reduces the risk of unauthorized removal or tampering, making it more challenging for attackers to compromise the SIM or manipulate its data. The soldered SIM design provides a more physically secure connection, enhancing the overall integrity and resilience of the mobile device's communication and authentication processes. There have been recent incidents involving IoT devices where the plastic SIM cards were stolen, primarily for the value of their associated data plans. An unintended consequence of this theft was a Denial of Service (DoS) on these IoT devices.

d) Private PDN

Private Packet Data Network (PDN) is a dedicated and isolated network established for a specific organization or entity. A private PDN puts the device on a private network, only accessible from the customer backend through a VPN access provided by the MNO. Utilizing a private PDN for IoT devices offers enhanced security and isolation, creating a dedicated environment that minimizes exposure to external threats and unauthorized access. This approach ensures the separation of IoT device traffic from public networks. When using private PDN, the devices are not accessible from the Internet, reducing considerably the risk of data interception and unauthorized surveillance compared to basic IoT devices. Private PDNs also provide the flexibility to implement customized security policies, tailoring protocols to safeguard sensitive IoT data. By isolating devices in a private network, the attack surface is reduced, mitigating the risk of external attacks and potential compromise of critical systems. Furthermore, organizations gain better control over access, limiting exposure to vulnerabilities and unauthorized entities. Attacking the device from the network would require successfully hacking either the application backend or the MNO, in which case the device attack becomes meaningless.

5.2 RAN and Device Architecture Security Aspects for Ambient IoT

3GPP has recently started a study on supporting IoT communication technology powered by battery-less IoT, i.e., devices with no energy storage capability or with energy storage that does not need manual replacement or recharging, which can harvest their needed energy from other sources. This so called Ambient IoT (A-IoT) technology is expected to further support the automation and digitalization of various industries and new markets requiring IoT devices of very small size, complexity, and power consumption, e.g., business inventory operations or device control via commands. Multiple studies at 3GPP are currently ongoing, including several aspects at service and system level as well as radio access network (RAN) level [2] [3] [4]. Among other topics, the work on Ambient IoT want to ensure the development of secure, efficient, and scalable cellular

solutions for this rapidly expanding IoT ecosystem. The RAN study confirmed that aspects such as encryption and data integrity, as well as authentication and authorization (when needed) are required functionalities. At RAN and device architecture level, we foresee in the following several security-related key areas that need to be encompassed.

5.2.1 Secure Storage of Data

Ambient IoT devices will follow the cellular paradigm on registering to the network for authentication/identification, fast and low energy access/communications sessions, etc. Thus, they should comprise memory unit(s) to store relevant key device context (e.g., device ID), communication information and other parameters. For Ambient IoT, the energy used to store (static power consumption) and access (read/write power consumption) this information will be of paramount importance. Non-volatile memory (NVM), such as EEPROM or MTP memory, may be essential to save security relevant data configured or indicated to the device. However, such memory is costlier and consumes more power during access (especially write) operations compared to volatile memory, such as SRAM, which is typical for registers used to cache temporary information during communication. A-IoT device must balance the cost and power consumption against the need to store important data securely. Thus, there must be a balanced design of key information bytes size to store in NVM as well as of the operation modes supported, that also considers cost and power consumption at the device.

5.2.2 Protection of Device Identifier

Different formats of device identifiers are considered for various stages of device communication and management. These identifiers must be managed securely to prevent unauthorized access and ensure efficient device tracking and inventory. Long permanent ID that includes info on, e.g., MNO, application owner, and session instance (or as in the electronic product code (EPC) format of RFID technology) will be long and probably not safe to communicate between a) reader and controlled, or b) reader and device. For the former case a long-temporary ID can be consider which is not exposed to devices and controller handles the mapping unique device IDs. For the latter case, a short-temporary ID can be considered where assignment and mapping to permanent/long-temporary IDs is handled by the reader. The final design will need to consider the burden caused to device to store temporary IDs and to the network nodes to additionally manage mapping relationships.

5.2.3 Security-Enabled Procedures

At initial attachment and initial access, multiple A-IoT devices may need to connect to a reader. In that case, they will probably have to follow a contention-based procedure before minimal security keys are exchanged to establish secure connectivity. This process may include a wake-up/trigger signal, timing acquisition for synchronization purposes, transmission of system information transmission, etc. The design of the initial attachment and access procedures may consider lightweight methods that encompass security aspects withing the triggering process, such as interrogation wake-up signals, with devices feeding back identification parameters, and may involve encoded security challenges.

Furthermore, ensuring that devices can be securely authenticated and authorized within the network is crucial. This requirement includes also robust paging procedures to ensure that the appropriate devices are triggered by the reader each time. On the other hand, with the need to optimize energy consumption, single-step approaches (e.g., traffic data delivered together with paging) to reduce device wake-up time and ping-pong communications may be the only feasible approaches. Handling device IDs securely to prevent exposure and potential security breaches should also be considered into the design of such procedures.

5.2.4 Security for Control Information

The control channels between reader and device and vice versa (currently termed as PRDCH and PDRCH in 3GPP terminology) will carry the essential control information, including device authentication, authorization, and security commands. Ensuring the secure transmission of this control information is critical to maintaining the integrity and confidentiality of the IoT ecosystem. However, the legacy (4G/5G) PDCP-based AS-level security is too complex and costly for A-IoT devices. Instead, physical layer can be considered to provide such security functionality, e.g., though the use of scrambling techniques for generating the control channels between reader and device. For example, dedicated sequences can be devised that scramble payload bits before channel coding, contrary to legacy methods which use scrambling of coded bits for interference randomization (there is no forward-error correction expected in reader/device control channels).

5.3 Robust Encryption at the Physical Layer

The security of communicated data depends on the ability to encrypt the transmit data such that only the authorized receivers can interpret the message. One of the ways to reduce the probability of interception of transmitted carriers by an unauthorized node such as man-in-the-middle interceptors [5] [6] is to provide a degree of security in the physical layer. As we also discussed in section above for A-IoT, introducing security in PHY can be an efficient way to alleviate the higher-layer security cost/complexity. A most promising approach for future investigation is to apply a combination of signal processing and antenna techniques.

5.3.1 Security with DSP Techniques

Regarding signal processing, promising techniques involve scrambling the constellation points of the signal of interest in accordance with a key generated through RF finger printing in the physical layer [7] (see **Figure 3**). The constellation is de-scrambled with the same key at the receiver to restore the original constellation for demodulation.

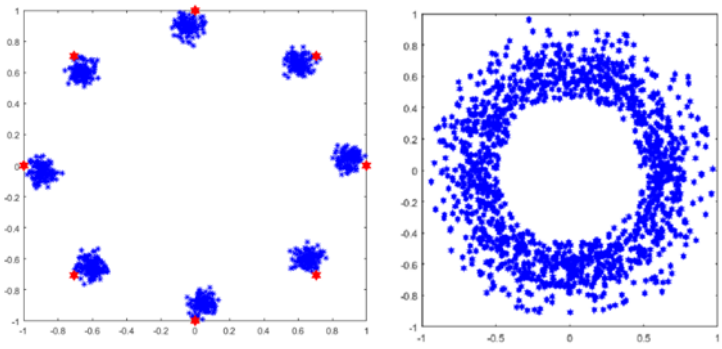

Figure 3: Constellation encryption of an 8-PSK modulated signal, left: original, right: encrypted

5.3.2 Security with Antenna Techniques

On the other hand, promising antenna techniques involve directional modulation [8] [7], where a constellation symbol $a_n \angle \Theta_n$ (in polar form) is decomposed into two symbols $a1_n \angle \Theta 1_n$ and $a2_n \angle \Theta 2_n$ such that:

$$a_n \angle \Theta_n = a1_n \angle \Theta 1_n + a2_n \angle \Theta 2_n$$

$a1_n \angle \Theta 1_n$ could be transmitted from a first transmitter on modulated carrier c1(t) and $a2_n \angle \Theta 2_n$ could be transmitted from a second transmitter on modulated carrier c2(t) and the two carriers are combined spatially using narrow beam directive antennas focused on a common receiver such that they combine appropriately only at the intended receiver. At any time instant 't', the intended receiver would receive the vector sum c1(t) and c2(t) which is the intended modulated carrier. In example **Figure 4**, the two transmitters towards the intended receiver are targeted by the two transmitters (with antennas spaced at least two wavelengths apart) by directing the main lobes of their antenna's radiation pattern towards the receiving antenna of the receiver.

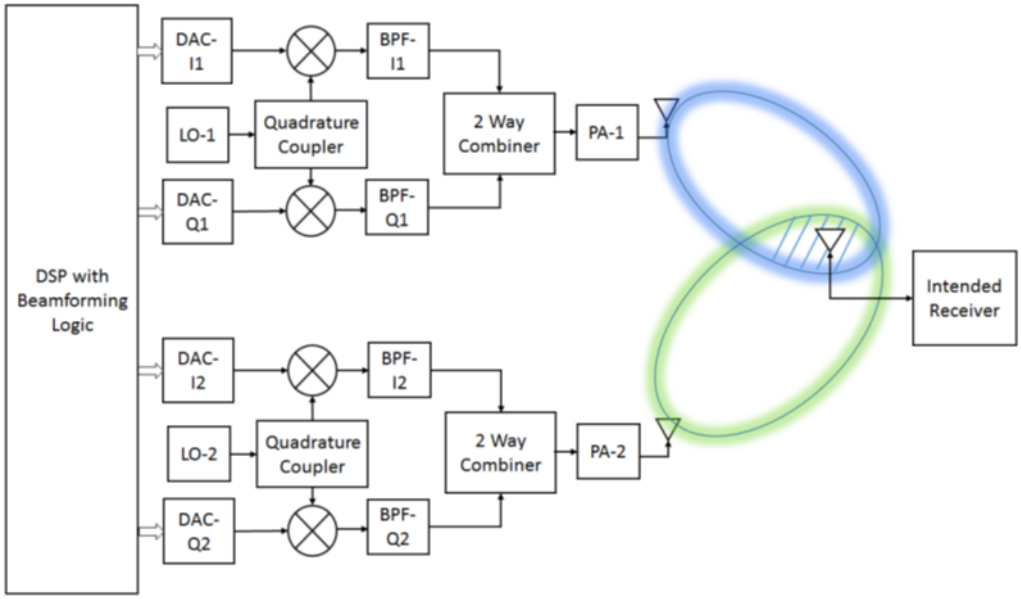

Figure 4: Generalized scheme of directional modulation

5.3.3 Combined Approach for Robust PHY Security

For an adverse node to be able to decrypt data transmitted over the air, it must first be able to receive the signal transmitted by an authentic or friendly node and demodulate the RF carrier to recover the baseband or information carrying part. A key aspect for design of effective security schemes is to thwart the ability of an adverse node from even receiving and demodulating a signal of interest. Future development on system design can involve a combination of the abovementioned schemes to evolve a robust PHY encryption system.

6 Conclusion

The COREnext project must be seen in the context of next generation (B5G/6G) communication with its increased demand for better performance and higher security. Based on generic assumptions regarding technology evolution and specific use cases elaborated in D2.1 we have developed an initial architecture concept which was outlined in D3.1 and identified required innovation both in the digital and analogue domain with respect to increased energy efficiency and improved security properties.

Based on the results from the corresponding component-level work in WP4 and WP5 as detailed in deliverables D4.2, D4.3, and D5.1 and incorporated in this deliverable D3.2 we conclude that our initial proposal remains plausible. Early component-level figures show promising performance improvements with respect to digital signal processing compared to current off-the-shelf hardware. Similarly, we identified improvements with respect to trustworthiness stemming from extra authentication and better isolation.

This report provides consolidated feedback to the use case analysis in WP2 and, more importantly, guides system level validation activities in WP6. We are looking forward to full baseband signal processing using a combination of M³'s base architecture, novel data processing and interconnect components, and the integration of RF fingerprinting and trusted execution environments bolstering trustworthiness.

7 References

[1] Sequan, „White Paper: Addressing Security in Cellular IoT Modems," https://sequans.com/addressing-security-in-cellular-iot-modems-lp, 2024.

[2] 3GPP, „Study on Ambient-power-enabled Internet of Things," TR 22.840, V19.0.0, 2023.

[3] 3GPP, „Sudy on Ambient IoT (Internet of Things) in RAN," TR 38.848, V18.0.0, 2023.

[4] 3GPP, „Study on Solutions for Ambient IoT (Internet of Things) in NR," RP-234058, 2023.

[5] B. Katz, C. Sahin und K. Dandekar, „Real-time Wireless Phyiscal Layer Encryption," in *17th IEEE Annual Wireless and Microwave Technology Conference (WAMICON)*, 2016.

[6] P. Ramabadran et al., „A Novel Physical Layer Encryption Scheme to Counter Eavesdroppers in Wireless Communications," in *25th IEEE International Conference on Electronics, Circuits and Systems (ICECS)*, Bordeaux, France, 2018.

[7] P. Ramabadran et al., „A Novel Physical Layer Authentication with PAPR Reduction Based on Channel and Hardware Frequency Responses," *IEEE Transactions on Circuits and Systems I: Regular Papers,* Bd. 67, Nr. 2, p. 526–539, 2020.

[8] Y. Ding und V. Fusco, „Improved Physical Layer Secure Wireless Communications Using a Directional Modulation Enhanced Retrodirective Array," in *31st URSI General Assembly and Scientific Symposium (GASS)*, 2014.

[9] 3GPP, „Sudy on Solutions for Ambient IoT (Internet of Things) in NR," RP-234058, 2023.