RE: Call for Proposals -"From Connectivity Gaps to Smart Solutions: Designing 5G Networks for Rural Innovation- 5G Intelligent Villages"

Securing the Future of Rural Finance: 5G UPI Solutions with Blockchain and Advanced Network Functions

Arpit Kumar
GMMS Labs, dungeon@gmms.xyz

Abstract

The rapid evolution of financial technologies demands innovative solutions that ensure both speed and security in transactions. This project introduces a Unified Payments Interface (UPI) prototype integrated with advanced 5G network functions, specifically the Authentication Server Function (AUSF) and Policy Control Function (PCF), to create a robust and secure platform for financial transactions. By leveraging 5G's ultra-low latency and network slicing capabilities, the prototype enables real-time financial operations while isolating sensitive transactions from other network traffic to mitigate cyber-attacks.

Incorporating zero-knowledge proofs within the AUSF allows for strict user authentication, ensuring sensitive credentials remain confidential even during the verification process. Meanwhile, the PCF, empowered by smart contracts, automates policy enforcement within dedicated network slices, providing end-to-end encryption and minimizing vulnerabilities. This integration not only enhances transaction security but also prepares the system for future scalability and compliance with global financial regulations.

This project is particularly impactful for rural India, where reliable and secure financial transactions can significantly boost economic inclusion and growth. By addressing critical vulnerabilities in traditional financial systems through a trustless architecture, the system reduces the potential for single points of failure and enhances data integrity. Blockchain's inherent transparency and security features ensure compliance with stringent regulatory requirements while maintaining high throughput and low latency, essential for seamless financial transactions. This pioneering approach sets a new standard for secure financial operations in the 5G era, offering a scalable and future-ready solution that could bridge the financial gap in underserved rural areas.

Motivation

Motivation to achieve Aatmanirbhar Bharat(Self-reliance India). to develop '5G Intelligent Villages' by leveraging the transformative power of 5G technology to uplift rural communities. This comprehensive approach addresses critical pillars such as agriculture, education, healthcare, governance, and sustainability. Proposals are invited to enable effective utilization of Ultra-Reliable Low-Latency Communication (URLLC) and massive Machine Type Communication (mMTC) aspects of 5G in selected villages, showcasing the advantages of 5G connectivity. Proposals can also include plans for establishing 5G connectivity in areas without existing coverage. This initiative aims to unite telecom service providers, sensor manufacturers, CCTV suppliers, and IoT providers on a single platform to explore and exploit the potential advantages of 5G, serving as a hub for research and development in this field.

Alignment

This project aligns with the Aatmanirbhar Bharat vision and the '5G Intelligent Villages' initiative by leveraging 5G technology to uplift rural communities:

1. **Fostering Self-Reliance:** By developing a UPI prototype integrated with advanced 5G technologies like AUSF and PCF, this project supports self-reliance in creating secure, scalable financial systems critical for India's digital economy. Encouraging domestic innovation in telecommunications and financial technology reduces dependence on foreign technologies and promotes local expertise and solutions.
2. **Extending 5G Coverage:** The project's focus on deploying 5G for secure financial transactions includes plans to extend 5G connectivity to unserved areas, thus bringing advanced communication services to underserved regions.
3. **Holistic Development:** This project not only promotes self-reliance but also contributes to the holistic development of rural communities, aligning with the broader goals of Aatmanirbhar Bharat and the 5G Intelligent Villages initiative.

1.Introduction

The increasing demand for secure and efficient financial transactions, especially in rural and underserved regions, has led to the exploration of innovative technologies that bridge the gap between speed and security. The Unified Payments Interface (UPI) has revolutionized the digital payment landscape in India, providing a seamless and instantaneous payment experience. However, with the proliferation of 5G technology, there is a pressing need to enhance UPI's security and scalability to meet the future demands of financial transactions.

5G technology introduces several advanced network functions that can be leveraged to secure financial transactions. Among these, the Authentication Server Function (AUSF) and the Policy Control Function (PCF) play crucial roles in ensuring robust authentication and policy enforcement. By integrating zero-knowledge proofs (ZKPs) within the AUSF, we can achieve strict user authentication without compromising sensitive credentials, ensuring that the verification process remains confidential and secure. This property of ZKPs—where the prover convinces the verifier of a statement's truth without revealing any additional information—is critical in protecting user privacy in financial transactions.

The PCF, empowered by smart contracts, further strengthens security by automating policy enforcement within dedicated network slices. Network slicing, a key feature of 5G, allows for the isolation of sensitive financial operations from other network traffic, thereby reducing the risk of cyber-attacks and ensuring end-to-end encryption. The use of smart contracts within PCF ensures that security policies are consistently applied, minimizing vulnerabilities and enhancing data integrity.

Blockchain technology, with its inherent transparency and immutability, complements these advanced network functions by providing a trustless architecture that eliminates single points of failure. The integration of blockchain into this system not only enhances security but also ensures compliance with global financial regulations, a critical requirement for the future scalability of UPI.

This project aims to develop a prototype that integrates UPI with 5G's advanced network functions, leveraging AUSF, PCF, and blockchain to create a secure and scalable platform for financial transactions. By addressing critical vulnerabilities in traditional financial systems and preparing the infrastructure for future challenges, this work sets a new standard for secure financial operations in the 5G era, particularly in rural areas where financial inclusion is paramount.

1.1 **Contribution**

Integration of Zero-Knowledge Proofs in AUSF: We propose a novel integration of zero-knowledge proofs (ZKPs) within the Authentication Server Function (AUSF) of 5G networks to enhance user authentication in UPI transactions. Our approach ensures that sensitive user credentials remain confidential throughout the authentication process, leveraging ZKPs' ability to prove the truth of a statement without revealing any additional information. This integration significantly enhances the security of financial transactions by protecting user data even during the verification process, a critical requirement for maintaining privacy in digital payments.

Smart Contracts-Enabled PCF for Policy Enforcement: We introduce the use of smart contracts within the Policy Control Function (PCF) to automate policy enforcement across dedicated network slices. By leveraging the programmability and self-executing nature of smart contracts, we ensure that security policies are consistently applied within isolated slices, minimizing vulnerabilities and enhancing the integrity of financial operations. This approach not

only automates the enforcement of policies but also enables dynamic and context-aware adjustments to security protocols based on real-time network conditions.

Blockchain-Based Trustless Architecture: Our contribution includes the integration of blockchain technology to create a trustless architecture that eliminates single points of failure in financial transactions. By using blockchain's inherent transparency and immutability, we enhance the security and compliance of the UPI system with global financial regulations. This integration ensures that all transactions are recorded in a tamper-proof ledger, providing an auditable trail that meets stringent regulatory requirements while maintaining the efficiency needed for real-time financial operations.

Scalable and Secure UPI Prototype: We will develop a prototype that integrates UPI with advanced 5G network functions, including AUSF, PCF, and blockchain. This prototype not only addresses critical vulnerabilities in traditional financial systems but also prepares the infrastructure for future scalability. Our system is designed to handle the increasing demand for secure digital payments, particularly in rural areas where financial inclusion is crucial. By leveraging 5G's ultra-low latency and network slicing capabilities, our solution ensures that financial transactions are both fast and secure, setting a new standard for the future of digital payments.

Performance Benchmarking and Comparison: To validate our approach, we will conduct extensive performance benchmarking and comparisons with existing solutions. Our prototype demonstrates superior security and efficiency, particularly in scenarios involving large-scale transactions and high throughput. We provide detailed comparisons of authentication times, policy enforcement latencies, and transaction processing speeds, highlighting the significant improvements achieved through our integration of 5G network functions with UPI. These results underscore the potential of our system to revolutionize financial transactions in the 5G era.

2. Potential Impact

Economic Inclusion and Empowerment:

By integrating UPI with 5G's advanced network functions, this project can significantly enhance financial inclusion in rural India. Secure, reliable, and fast digital payment systems will empower rural populations, enabling them to participate more fully in the digital economy. This can lead to increased access to financial services, including savings, credit, and insurance, which are critical for economic growth and poverty reduction.

Enhancing Agricultural Productivity:

The secure and reliable financial infrastructure provided by this project can facilitate smoother transactions for agricultural inputs and outputs, reducing transaction costs and delays. Farmers can benefit from timely payments and better access to markets, ultimately leading to improved productivity and income stability.

Boosting Rural Entrepreneurship:

A secure and scalable digital payment infrastructure can stimulate rural entrepreneurship by providing a reliable platform for small and medium enterprises (SMEs) to conduct business. Entrepreneurs in rural areas will be able to access wider markets and manage their finances more efficiently, fostering local economic development.

Strengthening Governance and Transparency:

Blockchain integration ensures transparency and immutability in financial transactions, which can significantly reduce corruption and financial mismanagement. This transparency can also be extended to government disbursements and subsidies, ensuring that funds reach the intended beneficiaries without leakage.

Sustainable Rural Development:

By creating a financial infrastructure that is both scalable and secure, the project supports sustainable development in rural areas. It lays the groundwork for the adoption of other smart technologies, such as IoT for agriculture and telemedicine, which can further enhance the quality of life in rural communities.

Educational Opportunities:

Financial security and inclusion can also have indirect benefits for education. With better access to financial resources, families can invest in education, leading to higher enrollment rates and better educational outcomes, which are essential for long-term development.

Health and Social Services:

Secure financial transactions can facilitate the delivery of health and social services in rural areas, such as direct benefit transfers for healthcare services or insurance payouts. This could improve access to health services and enhance the overall well-being of rural populations.

Scalability and Replicability:

The solutions developed in this project can serve as a model for other regions, both within India and globally. The integration of 5G, blockchain, and advanced network functions in financial systems is a forward-looking approach that can be replicated in other underserved areas, driving global innovation in rural finance.

Resilience Against Cyber Threats:

By leveraging advanced security features like zero-knowledge proofs, smart contracts, and network slicing, this project will enhance the resilience of rural financial systems against cyber threats. This is particularly important as rural areas increasingly adopt digital technologies, making them potential targets for cybercriminals.

Contributing to Aatmanirbhar Bharat:

The project directly contributes to the Aatmanirbhar Bharat initiative by fostering domestic innovation and reducing reliance on foreign technologies. The development of a robust, homegrown financial infrastructure will strengthen India's position as a leader in digital innovation and financial inclusion.

3. **Preliminaries**

In this section, we provide an overview of the existing Unified Payments Interface (UPI) architecture and its current integration with network functions in financial transactions. UPI, developed by the National Payments Corporation of India (NPCI), is a real-time payment system that facilitates inter-bank transactions through a single mobile application interface, allowing for seamless money transfers between accounts. It relies on traditional network security protocols, which, while effective, face challenges in scaling to meet the demands of emerging technologies like 5G. The advent of 5G networks introduces new possibilities for enhancing UPI's performance through ultra-low latency, high throughput, and network slicing capabilities, but also necessitates more robust security measures. To address these challenges, we explore the integration of 5G's Authentication Server Function (AUSF) and Policy Control Function (PCF) with UPI, alongside advanced cryptographic techniques like zero-knowledge proofs and blockchain, laying the groundwork for a more secure and scalable financial transaction framework in the 5G era.

3.1 Unified Payments Interface

Product Overview

UPI is a multi-channel platform that caters to the varied needs related to digital payment of end-users.

- **Channel**
  - **Online (**by using QR and/or mobile apps**)**
  - **Online + Offline (**by using QR and / or on-device wallet**)**
  - **Offline (**by using IVR on feature phones**)**
- **Products**
  - **Payments types (**P2P, P2M, P2P2M, P2G, G2P, B2B**)**
  - **UPI Collect (**Pull funds from the intended remitter**)**
  - **IPO on UPI (**Subscribe for IPO on NSE and BSE**)**
  - **Credit on UPI (**Payments by using Rupay credit Card**)**
  - **NRE Accounts (**NRI & NRE from 10 countries can make payments without Indian mobile number**)**
  - **More**

- **Key Use Cases**
    - **P2P payment, Bill payment, Retail Store**
    - **Fuel station, Restaurant**
    - **Travel booking, Credit Card Payment**
    - **Recharge and Collections, Subsidy Pay-outs**
    - **Online + Physical Shopping, Hotels, IPO Investment**

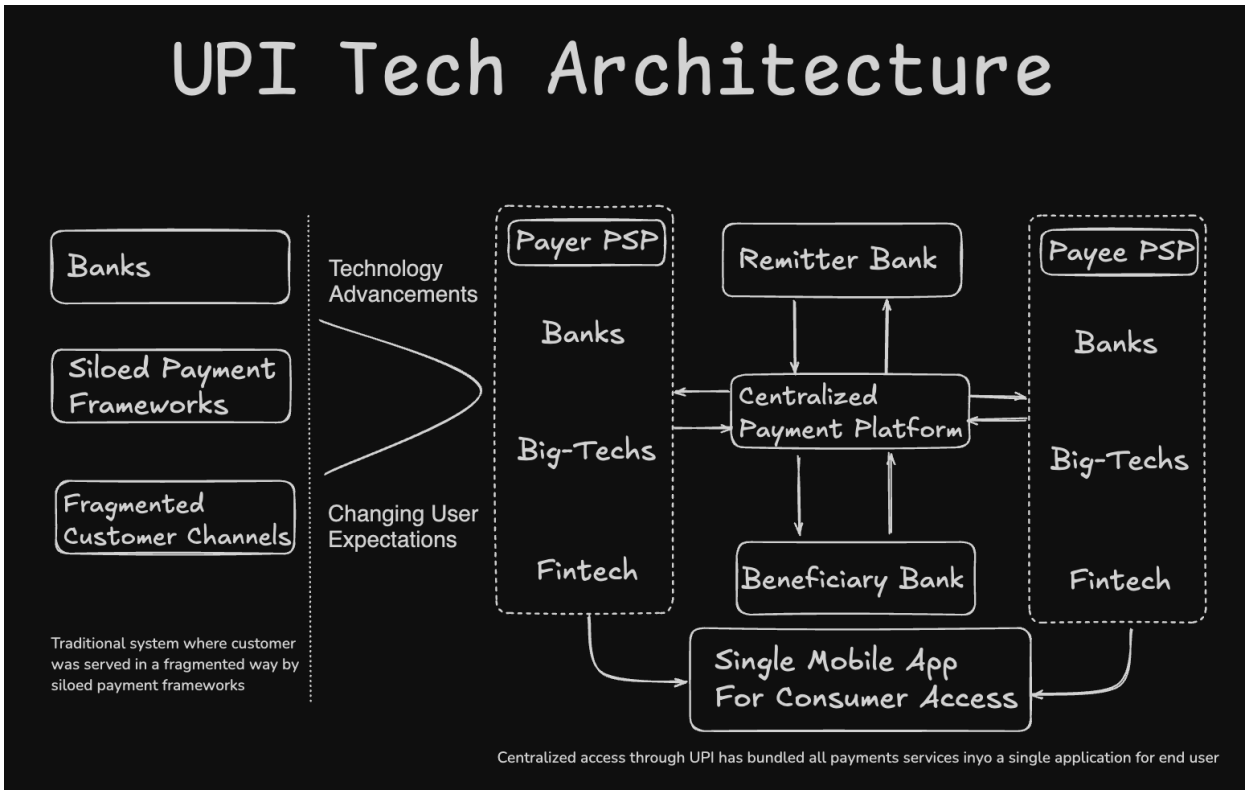
The key characteristics of UPI has added value for the end-users in terms of access to financial services, and standardisation.

- **Multiple Features (**Rich features embedded into payments like RTP, mandates etc., to enable streamlined low-value payment acceptance and settlement flow**)**
- **Open Banking (**Adaptive framework can be provided to MNOs and FinTechs**)**
- **Runs on Proxies (**Trust and Security: Overlay Account details**)**
- **Integrated with various payment channels** (Seamless integration with multiple channels of payment ecosystem)
- **Instant Payment** (Instant fund transfer: 24X7, 365 days. Also, real-time payments using Feature phones)
- **Interoperable platform** (Displace cash by enabling easy access to funds in any account across the country)
- **API Driven (**Multiple use cases can be integrated seamlessly using APIs**)**
-

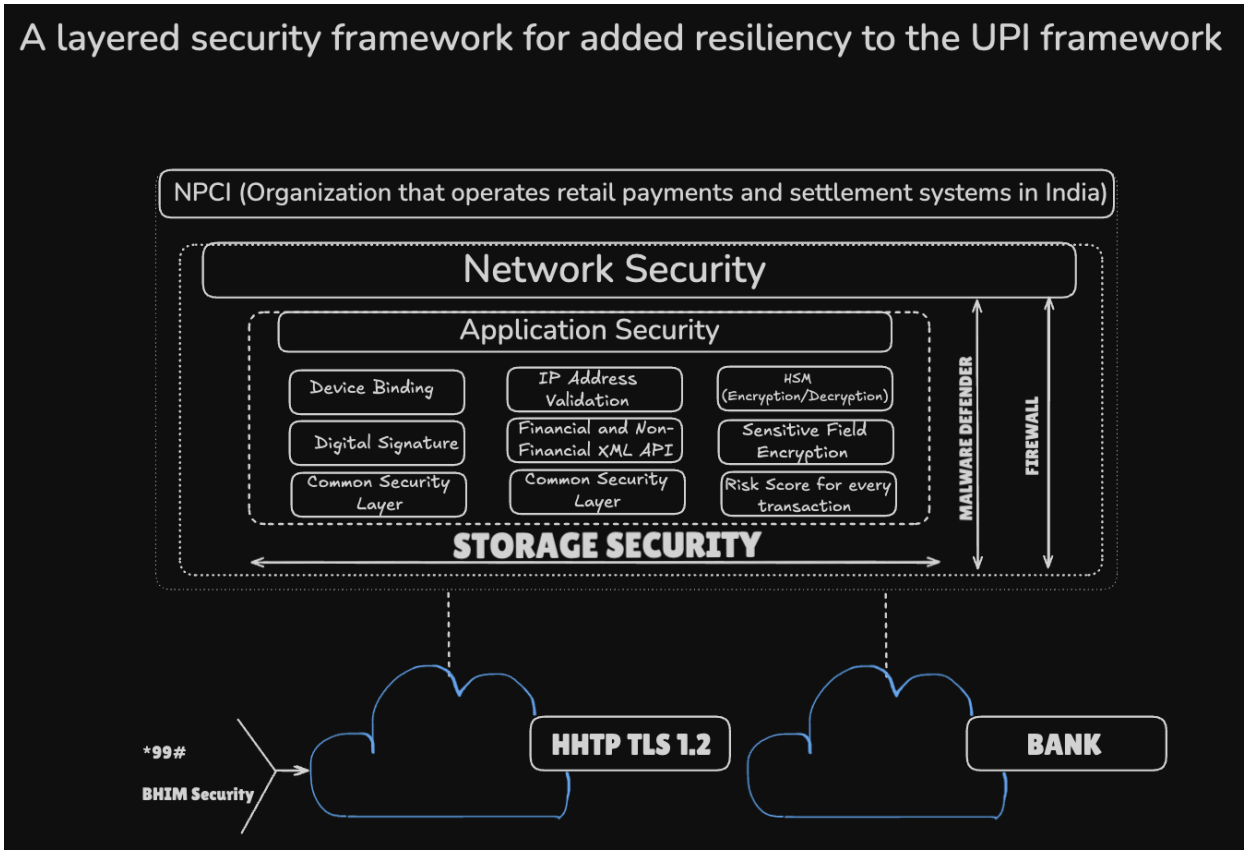
India has built an ambitious platform for digital payments, including a system for sending rupees between any bank or smartphone app – **Bill Gates**

Tech Architecture

The tech architecture of UPI has simplified the traditional payment systems, unbundled new services, and benefited the stakeholders across the ecosystem.



The central anti-fraud framework of UPI, which uses real-time and dynamic security protocols, has been able to address end-user fear related to fraudulent activities.



3.2 Network Slicing

In the 3GPP 5G core architecture, the user plane and control plane functions are separated.

- Control plane capabilities, for instance, session management, access authentication, policy management, and user data storage are independent of the user plane functionality.
- The user plane handles packet forwarding, encapsulation or de-capsulation, and associated transport level specifics.

This separation leads to the distribution of the user plane functions close to the edge of network slices (e.g., so as to reduce latency) and to be independent of the control plane.[1]
The main 5G core network entities are the Authentication server function (AUSF), Unstructured data storage network function (UDSF), Network exposure function (NEF), NF repository function (NRF), Policy control function (PCF), Unified data management (UDM), Network Slice Selection Function (NSSF), Communication Service Management Function (CSMF), AMF, SMF, and UPF. The AMF (as a function of the CP) controls UEs that have been authenticated to use the services of the operator and manages the mobility of the UEs across the gNBs. The SMF (again part of the CP) manages the sessions of UEs, while AMF transmits the session management messages between the UEs and SMF. UPF (as part of the UP) performs the processing and forwarding of the user data. NSSF (as a function of the CP) is responsible for the management and orchestration of network slices. CSMF (as a function of the CP) translates the requirements of services to requirements relating to network slices.[1] 5G Core network functions can be

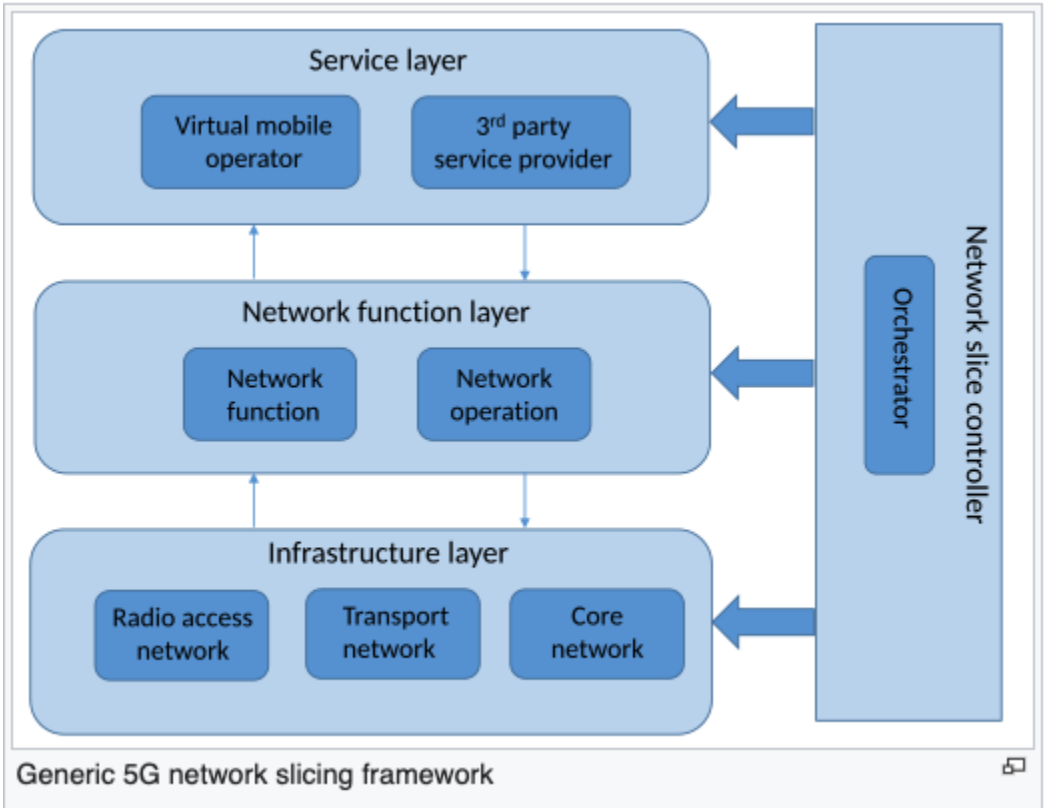
sliced to support specific services for different UEs. Thanks to the modular nature of the 5G core, the network functions of the 5G core can be split and shared between different network slices to reduce management complexity.[1] In general, we can perform 5G core network slicing in two ways. We can implement dedicated core network functions per network slice. In this architecture, each network slice has a set of completely dedicated core network functions (e.g., AUSF, AMF, SMF, and UDM). The UEs can access various services from network slices and different core networks. Alternatively, we can share some control plane functions between the network slices while others such as user plane functions are slice specific (e.g., UPF). AMF is usually shared by several network slices, while SMF and UPF are usually dedicated to specific network slices. The AMF function will be shared between different network slices in order to reduce the mobility management signaling when the UE uses the services of different network slices simultaneously. For example, UE location management or the control signaling between the UE and the old AMF will be reduced when it will be connected to the new AMF of another network slice. Also, UDM and NSSF are typically shared by all network slices to reduce the management complexity of network slices.

Key Concepts

The "one-size-fits-all" network paradigm employed in the past mobile networks (2G, 3G and 4G) is no longer suited to efficiently address a market model composed of very different applications like machine-type communication, ultra reliable low latency communication and enhanced mobile broadband content delivery.
Network slicing emerges as an essential technique in 5G networks to accommodate such different and possibly contrasting quality of service (QoS) requirements exploiting a single physical network infrastructure.
The basic idea of network slicing is to "slice" the original network architecture in multiple logical and independent networks that are configured to effectively meet the various services requirements. To quantitatively realise such concept, several techniques are employed:

- Network functions: they express elementary network functionalities that are used as "building blocks" to create every network slice.
- Virtualization: it provides an abstract representation of the physical resources under a unified and homogeneous scheme. In addition, it enables a scalable slice deployment relying on NFV that allows the decoupling of each network function instance from the network hardware it runs on.
- Orchestration: it is a process that allows coordination of all the different network components that are involved in the life-cycle of each network slice. In this context, SDN is employed to enable a dynamic and flexible slice configuration.

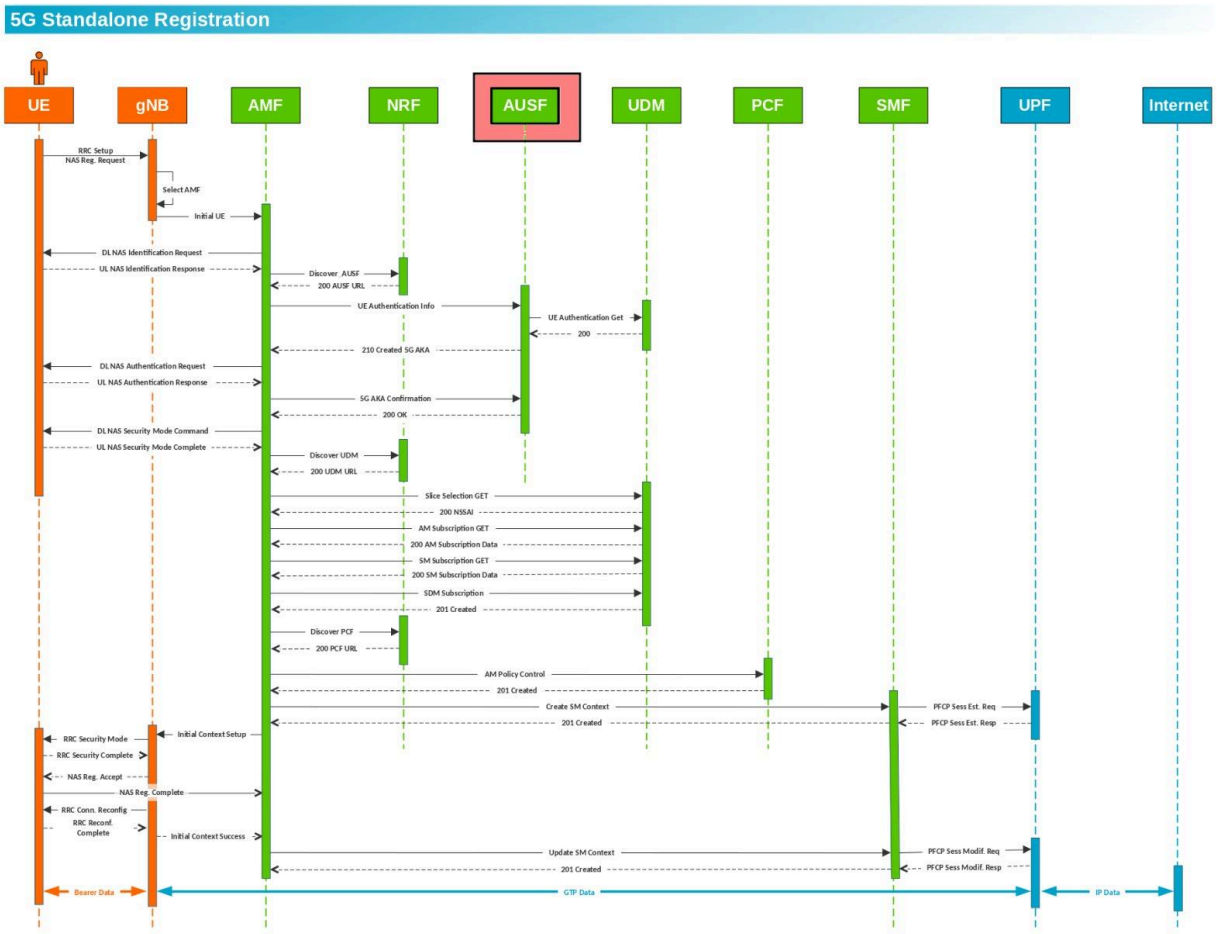
Architecture



Generic 5G network slicing framework

Service Layer: Interfaces with network entities to unify service requirements and create service instances based on SLA demands.
Network Function Layer: Chains network functions over virtual infrastructure to create network slices that meet service requests.
Infrastructure Layer: Provides the physical network resources required to host the network functions that compose each slice.
Network Slice Controller: Manages slice creation and lifecycle, coordinating across layers to ensure SLA compliance and flexible resource management.

3.3 AUSF/PCF



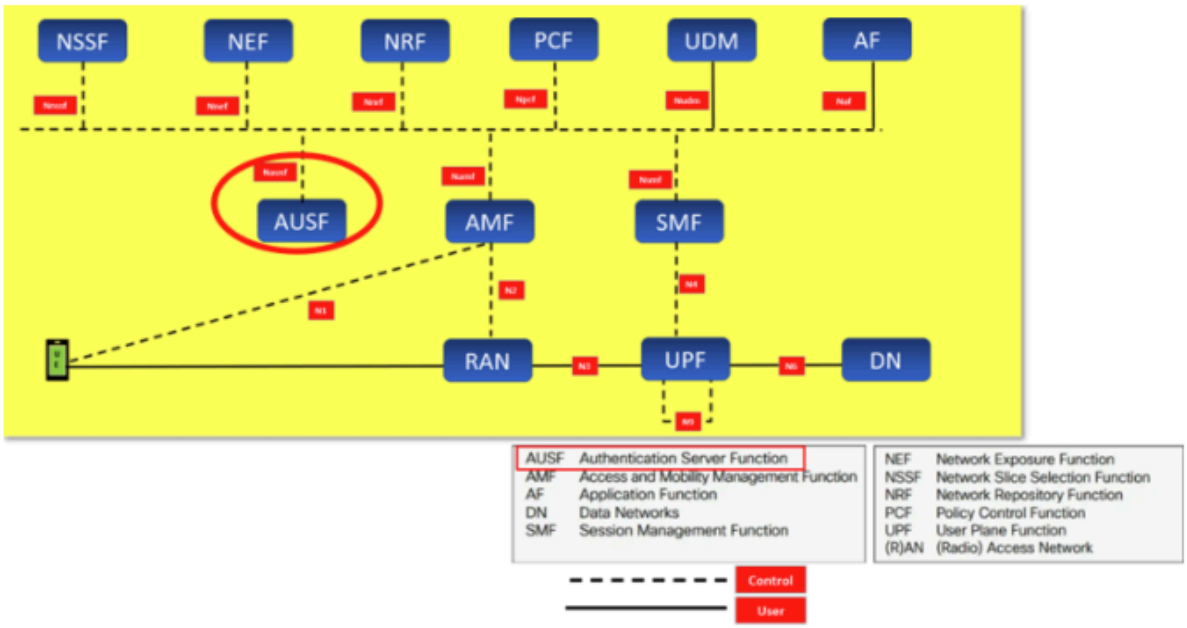
Together, AUSF and PCF are pivotal in ensuring the security and efficiency of 5G networks. AUSF secures the network by authenticating users, while PCF manages how network resources are utilized and ensures that the network operates according to established policies. Their roles become even more critical when applied to sensitive operations like financial transactions, where security and reliability are paramount.

AUSF (Authentication Server Function)

The Authentication Server Function (AUSF) is a critical component in the 5G core network architecture. It is responsible for managing the authentication of user equipment (UE) connecting to the network. As part of the broader 5G Authentication Framework, AUSF ensures that only legitimate users gain access to the network, playing a key role in verifying user identities and protecting network resources from unauthorized access.

Function of AUSF:

- **Authentication**: When a subscriber tries to access the 5G network, the AUSF performs authentication by verifying the subscriber's identity and checking whether they have the proper credentials to access the network.
- **Authorization**: After authentication, the AUSF performs authorization by checking whether the subscriber has the appropriate authorization to access specific network functions or services.
- **Security context**: The AUSF determines the appropriate security context for the subscriber based on their identity, subscription data, and authorization level.
- **Mobility management**: The AUSF interacts with other network functions, such as the Access and Mobility Management Function (AMF), to manage subscriber mobility and handover procedures.
- **Session management**: The AUSF supports session management, including the establishment, maintenance, and termination of 5G network sessions.
- **Subscriber data management**: The AUSF interacts with the Unified Data Management (UDM) function to manage subscriber data and profiles.



- **Authentication and key agreement (AKA)**: The AUSF support the AKA protocol, which is used for mutual authentication between the subscriber and the network. The AKA protocol provides a secure mechanism for exchanging keys and establishing a secure communication channel between the subscriber and the network.
- **Subscriber privacy**: The AUSF is responsible for protecting subscriber privacy by managing subscriber identity and authentication information. It ensures that subscriber data is protected and not disclosed to unauthorized parties.

- **Subscription data management**: The AUSF interacts with the UDM to manage subscription data and profiles for 5G subscribers. This includes managing subscriber profiles, policies, and authentication credentials.
- **Security protection**: The AUSF provides security protection against attacks and threats, such as replay attacks, man-in-the-middle attacks, and denial-of-service attacks. It uses advanced security mechanisms, such as encryption and authentication, to protect against these threats.
- **Network slicing**: The AUSF supports network slicing, which allows the 5G network to be divided into multiple logical networks to support different use cases and applications. It ensures that subscribers are authenticated and authorized for the appropriate network slice based on their identity and subscription data.
- **Interoperability**: The AUSF supports interoperability between different 5G network elements and interfaces, ensuring that subscribers can access 5G services and applications regardless of the network provider or location.

3.3.1 Services provided by AUSF [3GPP TS 33.501 version 16.3.0 Release 16]

General

The AUSF provides UE authentication service to the requester NF by **Nausf_UEAuthentication**. For AKA based authentication, this operation can be also used to recover from synchronization failure situations. Clause 14.1.2 describes the Nausf_UEAuthentication_Authenticate service operation. The services listed here are used in procedures that are described in clause 6 of the present document. Since AUSF is completely security-related, all service operations are described in the present document. TS 23.501 [2], clause 7.2.7, only lists the services and TS 23.502 [8], clause 5.2.10, provides the reference to the present document.

3. 3. 1. 1 **Nausf_UEAuthentication service**

Service operation name: Nausf_UEAuthentication_authenticate.

Description: Authenticate the UE and provides related keying material.

Input, Required: One of the options below.

1. In the initial authentication request: SUPI or SUCI, serving network name.
2. In the subsequent authentication requests depending on the authentication method: a. **5G AKA**: Authentication confirmation message with RES* as described in clause 6.1.3.2 or Synchronization Failure indication and related information (i.e. RAND/AUTS). b.

EAP-AKA': EAP packet as described in RFC 4187 [21] and RFC 5448 [12], and Annex F.

Input, Optional: None.

Output, Required: One of the options below.

1. Depending on the authentication method:
    1. **5G AKA**: authentication vector, as described in clause 6.1.3.2 or Authentication confirmation acknowledge message.
    2. **EAP-AKA'**: EAP packet as described in RFC 4187 [21] and RFC 5448 [12], and Annex F.
2. Authentication result and if success the master key which are used by AMF to derive NAS security keys and other security key(s).

Output, Optional: SUPI if the authentication was initiated with SUCI.

3. 3. 1. 2 **Nausf_SoRProtection service**

Service operation name: Nausf_SoRProtection.

Description: The AUSF calculates the SoR-MAC-IAUSF as specified in the Annex A.17 of this document using UE specific home key (KAUSF) along with the steering information received from the requester NF and delivers the SoRMAC-IAUSF and CounterSoR to the requester NF. If the ACK Indication input is present, then the AUSF shall compute the SoR-XMAC-IUE and return the computed SoR-XMAC-IUE in the response. The details of the SoR header is specified in TS 24.501 [35].

Input, Required: Requester ID, SUPI, service name, SoR Header.

Input, Optional: ACK Indication, list of preferred PLMN/access technology combinations.

Output, Required: SoR-MAC-IAUSF, CounterSoR or error (counter_wrap).

Output, Optional: SoR-XMAC-IUE (if the ACK Indication input is present, then the SoR-XMAC-IUE shall be computed and returned).

3. 3. 1. 3 **Nausf_UPUProtection service**

Service operation name: Nausf_UPUProtection.

Description: The AUSF calculates the UPU-MAC-IAUSF as specified in the Annex A.19 of this document using UE specific home key (KAUSF) along with the UE Parameters Update Data received from the requester NF and delivers the UPU-MAC-IAUSF and CounterUPU to the requester NF. If the ACK Indication input is present, then the AUSF shall compute the

UPU-XMAC-IUE and return the computed UPU-XMAC-IUE in the response. The details of the UE Parameters Update Data is specified in TS 24.501 [35].

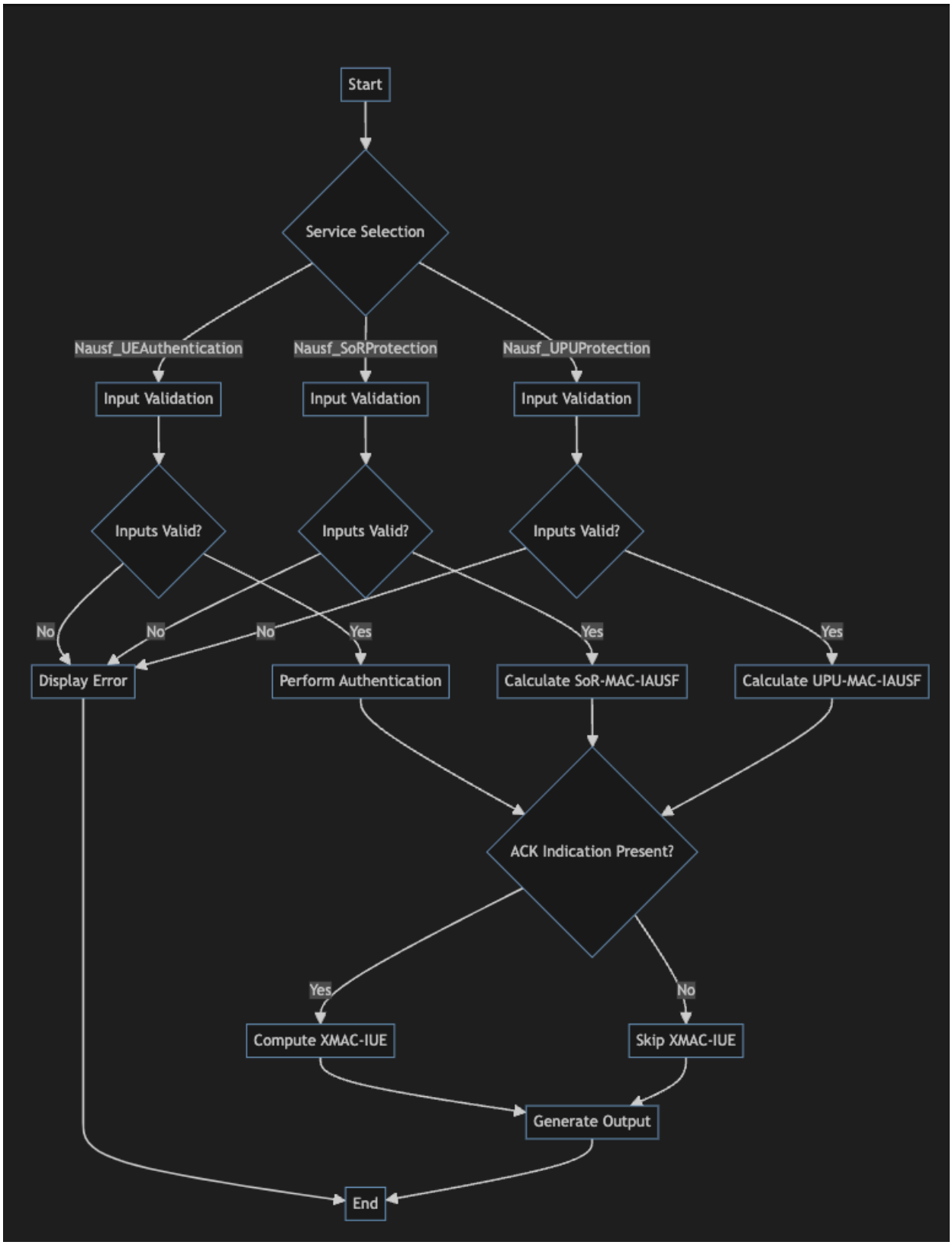
Input, Required: Requester ID, SUPI, service name, UE Parameters Update Data.

Input, Optional: ACK Indication.

Output, Required: UPU-MAC-IAUSF, CounterUPU or error (counter_wrap).

Output, Optional: UPU-XMAC-IUE (if the ACK Indication input is present, then the UPU-XMAC-IUE shall be computed and returned).

AUSF Service Operation Processes



This flowchart represents the AUSF service operation process as described in the selected text. It includes the main steps: Start, Service Selection, Input Validation, Service Process, ACK Indication Check, Output Generation, and End.

PCF (Policy Control Function)

The Policy Control Function (PCF) is another essential component of the 5G core network, responsible for policy management and enforcement across the network. It ensures that the network operates according to predefined rules and policies, optimizing resource usage, enforcing Quality of Service (QoS), and managing network slices.

Key Functions of PCF:

- **Policy Management**: PCF defines and manages policies that govern how network resources are allocated and used. These policies can dictate bandwidth allocation, traffic prioritization, and other network behaviors to ensure optimal performance and compliance with service-level agreements (SLAs).
- **Dynamic Policy Enforcement**: PCF can dynamically enforce policies in real-time based on the current network conditions and user demands. It works with the Access and Mobility Management Function (AMF) and the Session Management Function (SMF) to apply these policies across different parts of the network.
- **Quality of Service (QoS) Control**: PCF ensures that the network meets the QoS requirements for different services, such as voice, video, and data. By enforcing QoS policies, PCF helps maintain a consistent and reliable user experience.

The Policy Control Function, or PCF, is arguably one of the most important of the 5G Service-Based Architecture (SBA) Network Functions. It represents an evolution of the 4G Policy and Charging Rules Function (PCRF), which added capabilities to request and monitor service quality, on a per session basis. As well as retaining these session-based capabilities, the PCF adds additional functions, including control of network slicing, and new control mechanisms for UE activities, such as roaming and mobility management.
In the 5G Service-Based Architecture (SBA), the Policy Control Function (PCF) performs the same function as the Policy and Charging Rules Function (PCRF) does in 4G networks, but with additional functionality.
Arguably, the PCF is one of the most important of the 5G Network Functions, as policy and charging control will play a critical role in the evolving 5G ecosystem by providing visibility into and control over the use of differentiated network services in real time.

From PCRF to PCF

The PCRF is used in 4G / LTE networks to assist service data flow detection, policy enforcement, and flow-based charging, which ensures the reliable monitoring of services or use cases and the charges associated with each.

It also enables the reconfiguration of policies to effectively manage Quality of Service (QoS), charging, quota, optimisation, and admission control, and offers a number of benefits:

- Real-time management of the network and subscriber policy
- Effective routing and scheduling of network traffic
- Centralised view of subscriber context from device, network, location, and billing data
- Data-based insights into revenue assurance and bandwidth management
- Premium differentiated voice services to the user(s)
- Prioritising calls to emergency numbers in next-generation networks

The 5G PCF, meanwhile, supports the unified policy framework that governs network behaviour by providing policy rules for control plane functions (such as network slicing, roaming and mobility management) and subscription information for the policy decisions taken, and by supporting new 5G QoS policy and charging control functions.
It builds on the PCRF by adding more functionality that enhances agility and flexibility in a dynamic, cloud-native environment.

The main functions of the PCF include:

- Implement end-to-end policy management, from devices to applications
- Define policies for different slices, supporting diverse 5G use cases such as enhanced mobile broadband (EMBB), ultra-reliable and low-latency communication (URLLC), massive IoT, and more
- Enable service exposure to external applications
- Gain advanced BI insights with real-time analytics, altering the business strategy and creating new offerings on the fly
- Leverage data to create custom differentiated services for retail and enterprise customers

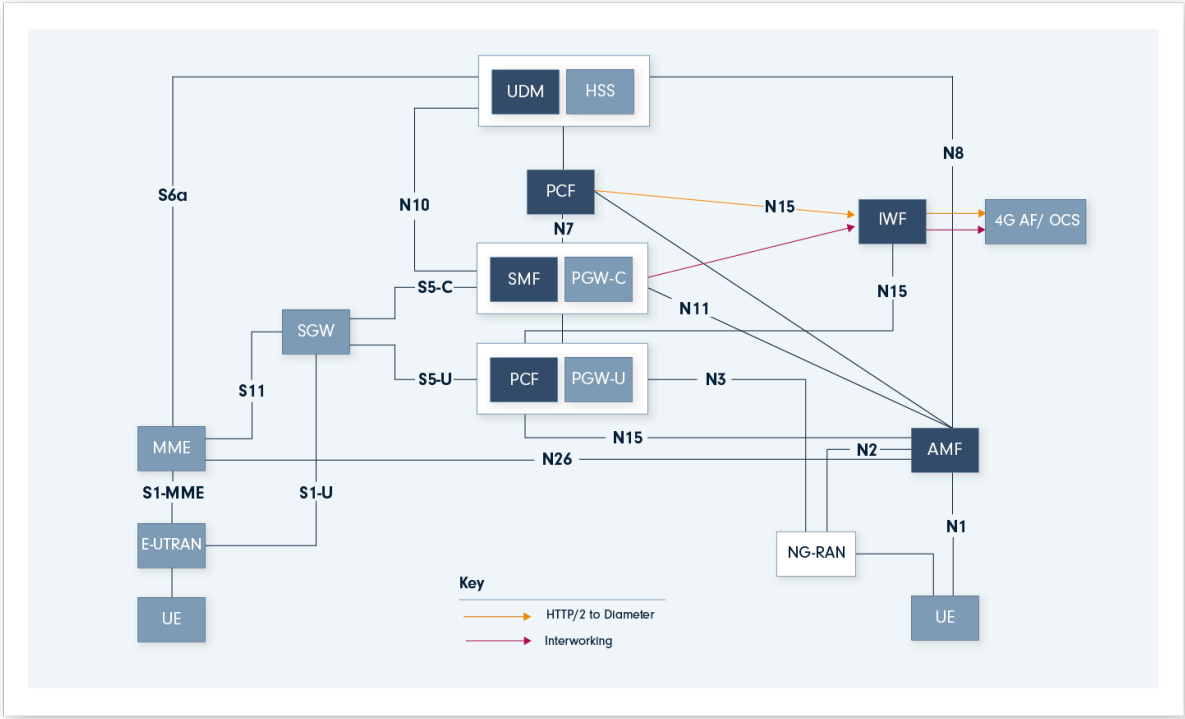
The PCF offers service providers multiple advantages, including efficient management of policies in a 5G network via an intuitive graphical interface; preparing the network to support massive IoT (mIoT) without compromising QoS; reducing network management costs; and enabling providers and MNOs to differentiate themselves with tailored offerings to consumer and enterprise customers.

Ensuring a unified policy framework

As such, the PCF supports a unified policy framework within the 5G infrastructure for governing network behaviour. It uses the policy subscription information stored in the User Data Repository (UDR) to provide policy rules to network functions (SMF/AMF).
The PCF uses a standard REST-based interface to integrate with the AMF for access and mobility policy, and the SMF for session management policy. Interfaces supported by the PCF

are described in numerous standards. For example, the interface with the SMF is covered in 3GPP TS 29.508, 5G System; Session Management Event Exposure Service, Stage 3.

Figure 1 – PCF interworking between 4G and 5G network service domain



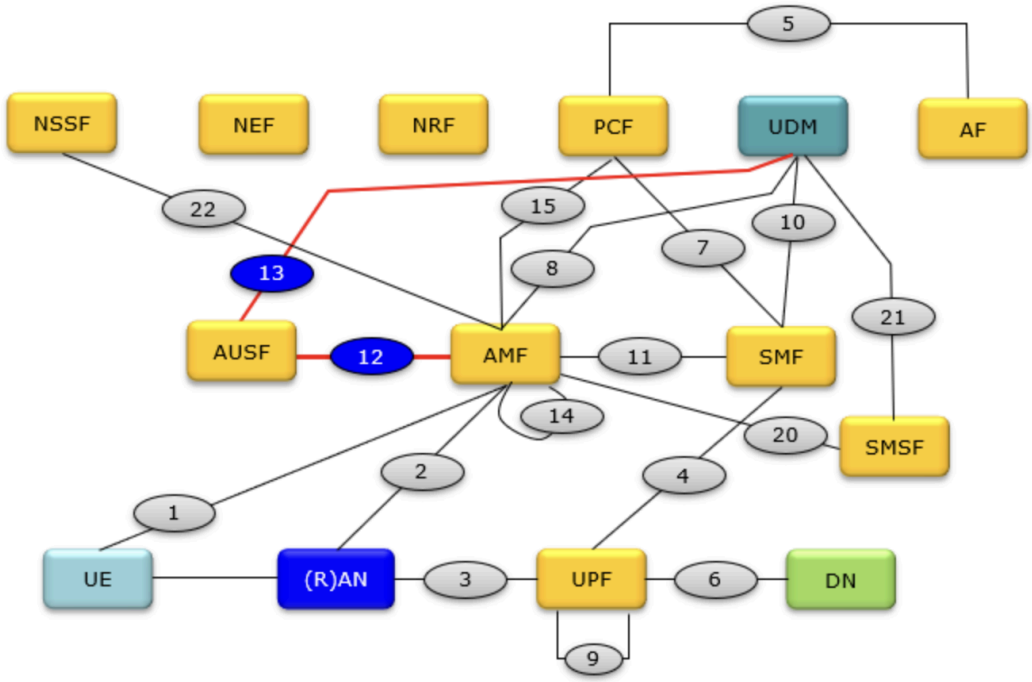
Source: Emblasoft
However, of course, the migration towards 5G will not happen overnight, which creates two challenges:

- Many operators will need to deploy PCF and PCRF solutions in parallel.
- Many services will span both 5G and 4G domains, so the appropriate AAA procedures must be observed in each. A solution to these challenges is to enable interworking between new, 5G PCF solutions and legacy PCRF functions.

What's required is a cloud-native policy converged solution that can help service providers avoid multiple platform migrations and leapfrog the policy solution directly to the industry-defined 5G SBA. Having a secure and flexible policy converged solution is fundamental when seeking new revenue streams beyond connectivity and striving to take advantage of cloud-native technologies and 5G.

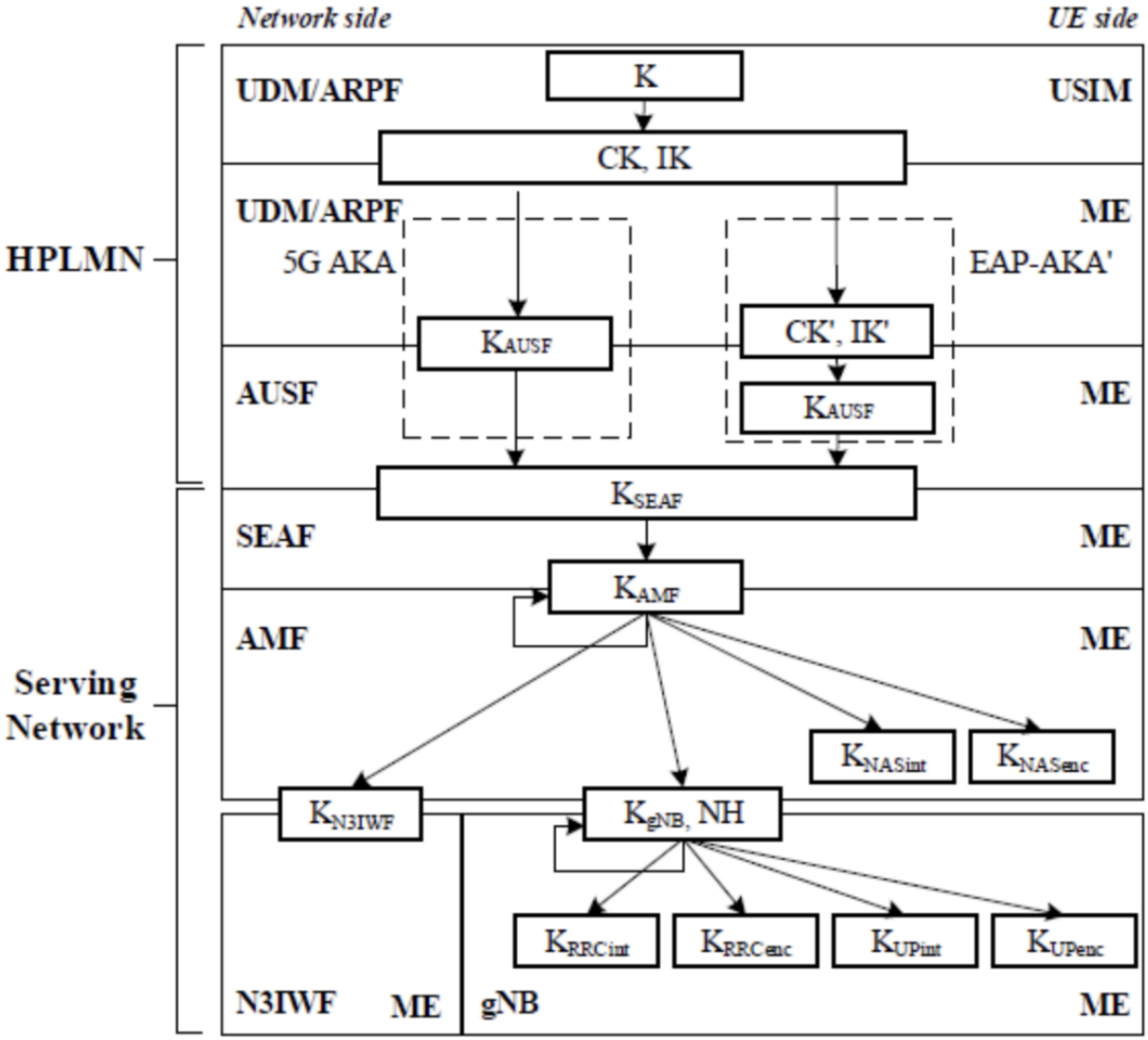
All 5G Network Functions

The entire signaling path for Authentication process is UE <-- N1--> AMF <--N12-->AUSF<--N13-->UDM, but the main focus on this note is the core network process along AMF <--N12-->AUSF<--N13-->UDM. This core network signaling path is highlighted in blue ellipse and red lines shown below.



NF Name	NF Acronym	Analogous EPC element
Authentication Server Function	AUSF	MME / HSS (Authentication)
Access and Mobility Management Function	AMF	MME
Unstructured Data Storage Function	UDSF	N/A
Network Exposure Function	NEF	N/A
Network Slice Specific Authentication and Authorization Function	NSSAAF	N/A
Network Slice Selection Function	NSSF	N/A
Policy Control Function	PCF	PCRF
Session Management Function	SMF	MME / PGW-C
Unified Data Management	UDM	HSS (DB Front End)
Unified Data Repository	UDR	HSS (User Database)
User Plane Function	UPF	SGW-U / PGW-U
UE radio Capability Management Function	UCMF	N/A
Application Function	AF	AF (IMS)
Network Data Analytics Function	NWDAF	N/A
CHarging Function	CHF	CSCF

Key Hierarchy Generation in 5GS



NOTICE: There are several functions involved in one 5G authentication, we are focusing only on AUSF and improve it with the principle of modern cryptography by using zero knowledge proofs.

3.4 Smart Contracts

Etymology

By 1996, Nick Szabo was using the term "smart contract" to refer to contracts which would be enforced by physical property (such as hardware or software) instead of by law. Szabo described vending machines as an example of this concept. In 1998, the term was used to

describe objects in rights management service layer of the system The Stanford Infobus, which was a part of Stanford Digital Library Project.

Introduction

Smart contracts are the fundamental building blocks of the decentralised application layer. They are computer programs stored on the blockchain that follow "if this then that" logic, and are guaranteed to execute according to the rules defined by its code, which cannot be changed once created.
Nick Szabo coined the term "smart contract". In 1994, he wrote an introduction to the concept, and in 1996 he wrote an exploration of what smart contracts could do .
Szabo envisioned a digital marketplace where automatic, cryptographically-secure processes enable transactions and business functions to happen without trusted intermediaries.

Trust in conventional contracts

One of the biggest problems with a traditional contract is the need for trusted individuals to follow through with the contract's outcomes.

A digital vending machine

A simple metaphor for a smart contract is a vending machine, which works somewhat similarly to a smart contract - specific inputs guarantee predetermined outputs.

- You select a product
- The vending machine displays the price
- You pay the price
- The vending machine verifies that you paid the right amount
- The vending machine gives you your item

The vending machine will only dispense your desired product after all requirements are met. If you don't select a product or insert enough money, the vending machine won't give out your product.

Automatic Execution

The main benefit of a smart contract is that it deterministically executes unambiguous code when certain conditions are met. There is no need to wait for a human to interpret or negotiate the result. This removes the need for trusted intermediaries.

Predictable Outcomes

Traditional contracts are ambiguous because they rely on humans to interpret and implement them. For example, two judges might interpret a contract differently, which could lead to inconsistent decisions and unequal outcomes. Smart contracts remove this possibility. Instead, smart contracts execute precisely based on the conditions written within the contract's code. This precision means that given the same circumstances, the smart contract will produce the same result.

Public Records

Smart contracts are useful for audits and tracking. Since Ethereum smart contracts are on a public blockchain, anyone can instantly track asset transfers and other related information. For example, you can check to see that someone sent money to your address.

Privacy Protection

Smart contracts also protect your privacy. Since Ethereum is a pseudonymous network (your transactions are tied publicly to a unique cryptographic address, not your identity), you can protect your privacy from observers.

Visible Terms

Finally, like traditional contracts, you can check what's in a smart contract before you sign it (or otherwise interact with it). A smart contract's transparency guarantees that anyone can scrutinise it.

Smart Contract in PCF

Integrating **smart contracts** in **PCF** to automate the enforcement of policies within network slices. Smart contracts ensure that policies are consistently applied and can be dynamically adjusted based on real-time network data.

Key Advantages of Using Smart Contracts as PCF:

1. **Automated Policy Enforcement:**
    - Smart contracts can be programmed with specific rules and conditions that automatically trigger actions when certain criteria are met. This eliminates the need for manual intervention in policy enforcement, ensuring that policies are applied consistently across the network.
2. **Transparency and Trust:**
    - Since smart contracts are executed on a blockchain, their operations are transparent and verifiable by all stakeholders. This transparency fosters trust among users, network operators, and regulators, as the policy enforcement process is open to scrutiny and cannot be tampered with.
3. **Immutable and Secure Policy Rules:**
    - Once deployed, smart contracts cannot be altered without consensus from the involved parties. This immutability ensures that the policy rules remain secure and consistent, reducing the risk of unauthorized changes that could compromise network integrity.
4. **Real-Time Policy Adjustments:**
    - Smart contracts can be designed to react in real-time to changes in network conditions or user behavior. For instance, if a network slice experiences congestion, the smart contract could automatically adjust bandwidth allocation policies to maintain Quality of Service (QoS) standards.
5. **Decentralized Control:**

    - Using smart contracts for PCF decentralizes policy control, reducing reliance on a central authority. This can enhance the resilience of the network by distributing control across multiple nodes, making it harder for any single point of failure to disrupt network operations.
6. **Compliance with Regulatory Requirements:**
    - Smart contracts can encode regulatory compliance rules directly into the network's operational framework. This ensures that all policy decisions are made in accordance with legal and regulatory standards, which is particularly important in sectors like finance where compliance is critical.
7. **Dynamic and Scalable Policy Management:**
    - As 5G networks scale and become more complex, smart contracts can manage a wide range of policies across different network slices and services. They enable the PCF to handle diverse requirements, such as those of different applications, devices, and user groups, efficiently and effectively.

Project Case: Financial Transactions in 5G Networks

- In this case, financial transactions, smart contracts can be used to enforce transaction-related policies within dedicated network slices. For example, a smart contract could automatically enforce a policy that prioritizes financial transaction traffic over other types of data during peak hours, ensuring that critical financial operations are not delayed. This integration ensures that the PCF is capable of maintaining the integrity and performance of the network, even under high loads, while also providing an auditable trail of all policy enforcement actions.

By leveraging smart contracts as part of the PCF, 5G networks can achieve a higher level of automation, security, and efficiency in managing network policies, making them well-suited to handle the demands of next-generation applications, including secure financial transactions and other mission-critical services.

3.5 Zero Knowledge Proofs

History

Zero-knowledge proofs were first conceived in 1985 by Shafi Goldwasser, Silvio Micali, and Charles Rackoff in their paper "The Knowledge Complexity of Interactive Proof-Systems".This paper introduced the IP hierarchy of interactive proof systems (see interactive proof system) and conceived the concept of knowledge complexity, a measurement of the amount of knowledge about the proof transferred from the prover to the verifier. They also gave the first zero-knowledge proof for a concrete problem, that of deciding quadratic nonresidues mod m. Together with a paper by László Babai and Shlomo Moran, this landmark paper invented interactive proof systems, for which all five authors won the first Gödel Prize in 1993.
In their own words, Goldwasser, Micali, and Rackoff say:

Of particular interest is the case where this additional knowledge is essentially 0 and we show that [it] is possible to interactively prove that a number is quadratic non residue mod m releasing 0 additional knowledge. This is surprising as no efficient algorithm for deciding quadratic residuosity mod m is known when m's factorization is not given. Moreover, all known NP proofs for this problem exhibit the prime factorization of m. This indicates that adding interaction to the proving process, may decrease the amount of knowledge that must be communicated in order to prove a theorem.

Introduction

In cryptography, a **zero-knowledge proof** or **zero-knowledge protocol** is a method by which one party (the prover) can prove to another party (the verifier) that some given statement is true, while avoiding conveying to the verifier any information beyond the mere fact of that statement's truth. The intuition underlying zero-knowledge proofs is that it is trivial to prove possession of the relevant information simply by revealing it; the hard part is to prove this possession without revealing this information (or any aspect of it whatsoever).
In light of the fact that one should be able to generate a proof of some statement only when in possession of certain secret information connected to the statement, the verifier, even after having become convinced of the statement's truth, should nonetheless remain unable to prove the statement to further third parties.
In the plain model, nontrivial zero-knowledge proofs (i.e., those for languages outside of BPP) demand interaction between the prover and the verifier. This interaction usually entails the selection of one or more random challenges by the verifier; the random origin of these challenges, together with the prover's successful responses to them notwithstanding, jointly convince the verifier that the prover does possess the claimed knowledge. (If interaction were absent, then the verifier, having obtained the protocol's execution transcript—that is, the prover's one and only message—could replay that transcript to a third party, thereby convincing the third party that the verifier too possessed the secret information.)
In the common random string and random oracle models, non-interactive zero-knowledge proofs exist, in light of the Fiat–Shamir heuristic.These proofs, in practice, rely on computational assumptions (typically the collision-resistance of a cryptographic hash function).

A zero-knowledge proof of some statement must satisfy three properties:

1. **Completeness**: if the statement is true, an honest verifier (that is, one following the protocol properly) will be convinced of this fact by an honest prover.
2. **Soundness**: if the statement is false, no cheating prover can convince an honest verifier that it is true, except with some small probability.
3. **Zero-knowledge**: if the statement is true, no verifier learns anything other than the fact that the statement is true. In other words, just knowing the statement (not the secret) is sufficient to imagine a scenario showing that the prover knows the secret. This is formalized by showing that every verifier has some simulator that, given only the statement to be proved (and no access to the prover), can produce a transcript that "looks like" an interaction between an honest prover and the verifier in question.

The first two of these are properties of more general interactive proof systems. The third is what makes the proof zero-knowledge.

Variants of zero-knowledge

Different variants of zero-knowledge can be defined by formalizing the intuitive concept of what is meant by the output of the simulator "looking like" the execution of the real proof protocol in the following ways:

- We speak of *perfect zero-knowledge* if the distributions produced by the simulator and the proof protocol are distributed exactly the same. This is for instance the case in the first example above.
- *Statistical zero-knowledge*[13] means that the distributions are not necessarily exactly the same, but they are statistically close, meaning that their statistical difference is a negligible function.
- We speak of *computational zero-knowledge* if no efficient algorithm can distinguish the two distributions.

Zero knowledge types

- Proof of knowledge: the knowledge is hidden in the exponent like in the example shown above.
- Pairing based cryptography: given $\mathrm{f}(x)$ and $\mathrm{f}(y)$, without knowing x and y, it is possible to compute $\mathrm{f}(x \times y)$.
- Witness indistinguishable proof: verifiers cannot know which witness is used for producing the proof.
- Multi-party computation: while each party can keep their respective secret, they together produce a result.
- Ring signature: outsiders have no idea which key is used for signing.

Applications

Authentication systems

Research in zero-knowledge proofs has been motivated by authentication systems where one party wants to prove its identity to a second party via some secret information (such as a password) but doesn't want the second party to learn anything about this secret. This is called a "zero-knowledge proof of knowledge". However, a password is typically too small or insufficiently random to be used in many schemes for zero-knowledge proofs of knowledge. A zero-knowledge password proof is a special kind of zero-knowledge proof of knowledge that addresses the limited size of passwords.

More ZKPs application

- Ethical behavior
- Nuclear disarmament
- Blockchains
- Decentralised Identifiers and more

Zero-knowledge proof (ZKP) systems

ZKP System	Publication year	Protocol	Transparent	Universal	Plausibly Post-Quantum Secure	Programming Paradigm
Pinocchio[37]	2013	zk-SNARK	No	No	No	Procedural
Geppetto[38]	2015	zk-SNARK	No	No	No	Procedural
TinyRAM[39]	2013	zk-SNARK	No	No	No	Procedural
Buffet[40]	2015	zk-SNARK	No	No	No	Procedural
ZoKrates[41]	2018	zk-SNARK	No	No	No	Procedural
xJsnark[42]	2018	zk-SNARK	No	No	No	Procedural
vRAM[43]	2018	zk-SNARG	No	Yes	No	Assembly
vnTinyRAM[44]	2014	zk-SNARK	No	Yes	No	Procedural
MIRAGE[45]	2020	zk-SNARK	No	Yes	No	Arithmetic Circuits
Sonic[46]	2019	zk-SNARK	No	Yes	No	Arithmetic Circuits
Marlin[47]	2020	zk-SNARK	No	Yes	No	Arithmetic Circuits
PLONK[48]	2019	zk-SNARK	No	Yes	No	Arithmetic Circuits
SuperSonic[49]	2020	zk-SNARK	Yes	Yes	No	Arithmetic Circuits
Bulletproofs[24]	2018	Bulletproofs	Yes	Yes	No	Arithmetic Circuits
Hyrax[50]	2018	zk-SNARK	Yes	Yes	No	Arithmetic Circuits
Halo[51]	2019	zk-SNARK	Yes	Yes	No	Arithmetic Circuits
Virgo[52]	2020	zk-SNARK	Yes	Yes	Yes	Arithmetic Circuits
Ligero[53]	2017	zk-SNARK	Yes	Yes	Yes	Arithmetic Circuits
Aurora[54]	2019	zk-SNARK	Yes	Yes	Yes	Arithmetic Circuits
zk-STARK[55]	2019	zk-STARK	Yes	Yes	Yes	Assembly
Zilch[36]	2021	zk-STARK	Yes	Yes	Yes	Object-Oriented

Zero-Knowledge Proofs in AUSF (Authentication Server Function)

The Authentication Server Function (AUSF) is a critical component in 5G networks responsible for authenticating users and devices, ensuring that only legitimate entities gain access to network resources. Integrating zero-knowledge proofs (ZKPs) into the AUSF enhances security by allowing the authentication process to be both verifiable and confidential without exposing sensitive information.

Key Features of Zero-Knowledge AUSF:

1. **Confidential Authentication:**
    - Zero-knowledge proofs enable the AUSF to verify the identity of a user or device without requiring the disclosure of private data such as passwords or biometric information. This ensures that sensitive credentials are never exposed, even during the authentication process, significantly reducing the risk of data breaches.
2. **Proof of Identity without Data Exposure:**
    - In a zero-knowledge AUSF, a user can prove they possess a secret (such as a private key or a password) without revealing the secret itself. For example, the AUSF can confirm that a user knows a password without the user ever sending the password to the server. This enhances the security of the authentication process by minimizing the data exchanged over the network.
3. **Resistance to Replay Attacks:**
    - By employing ZKPs, the AUSF can generate fresh, non-reusable proofs for each authentication attempt. This dynamic nature of zero-knowledge proofs ensures that even if an attacker intercepts the proof, they cannot use it to impersonate the user in future sessions, thereby thwarting replay attacks.
4. **Minimal Data Exchange:**
    - Zero-knowledge proofs typically involve a minimal amount of data being sent between the prover (user) and the verifier (AUSF). This makes the authentication process more efficient and less susceptible to interception, as there is less information for potential attackers to capture.
5. **Scalability and Flexibility:**
    - Zero-knowledge AUSF can be adapted to various authentication scenarios, including multi-factor authentication (MFA), where users may need to prove knowledge of multiple secrets without revealing any of them. This scalability makes zero-knowledge AUSF suitable for diverse applications within 5G networks, from consumer devices to IoT systems.
6. **Compliance with Privacy Regulations:**
    - By ensuring that sensitive information is never exposed during the authentication process, zero-knowledge AUSF helps network operators comply with stringent privacy regulations such as GDPR. This is particularly important in sectors where the protection of personal data is paramount, such as finance and healthcare.

Project Case: Financial Transactions

- In the context of secure financial transactions over 5G networks, a zero-knowledge AUSF ensures that users can authenticate themselves to financial services without revealing their private keys or other sensitive credentials. For instance, a user could prove that they possess the correct private key to authorize a transaction without ever transmitting the key itself. This reduces the risk of fraud and enhances the security of the transaction process, making zero-knowledge AUSF an ideal solution for high-stakes financial operations.

By integrating zero-knowledge proofs into the AUSF, 5G networks can offer a higher level of security for user authentication, protecting sensitive information while maintaining the efficiency and scalability required for modern digital services.

4. Persona

UPI is used by mass number of consumers and this project is consumer focused for :

Individuals or businesses using the UPI-based application to perform secure financial transactions.(Consumers)

- **Role:** End users initiate transactions, authenticate themselves, and interact with the UPI platform for payments and other financial services.
- **Needs:** Secure, fast, and reliable financial transactions with minimal friction during the authentication process.

Companies providing mobile network services, responsible for managing the network slices that support the UPI platform.(MNOs)

- **Role:** MNOs deploy and manage AUSF and PCF to ensure secure network slice operations, specifically tailored for the UPI service.
- **Needs:** Efficient, secure network management to support seamless operations of UPI transactions.

Companies providing the hardware and software infrastructure required for 5G networks, including AUSF and PCF components.(Telecom Network Provider)

- **Role:** Support the deployment and operation of the underlying network technologies that enable secure slice operations.
- **Needs:** Reliable and scalable infrastructure to support high volumes of transactions with minimal downtime.

Government and industry bodies overseeing financial transactions and telecommunications.(Regulatory Authorities)

- **Role:** Ensure that the UPI system complies with regulatory standards and guidelines for data protection, cybersecurity, and financial integrity.
- **Needs:** Compliance with regulations and continuous monitoring to prevent cyber-attacks and ensure the safety of financial transactions.

Team designing and building this project.(Applicant of this proposal)

5. End to End Solution

Our project offers a holistic end-to-end solution for enhancing financial transactions in rural areas by integrating cutting-edge technologies with 5G infrastructure. The solution encompasses the following components:

UPI Prototype Integration:

Unified Payments Interface (UPI): At the core of our solution is the UPI, which provides a seamless and instantaneous digital payment experience. This prototype will be enhanced with advanced 5G functionalities to ensure high-speed and secure transactions.

2. Advanced 5G Network Functions:

Authentication Server Function (AUSF): We integrate zero-knowledge proofs within the AUSF to bolster user authentication. This ensures that sensitive user credentials remain confidential throughout the authentication process, protecting privacy and enhancing security.

Policy Control Function (PCF): Smart contracts are embedded within the PCF to automate policy enforcement across dedicated network slices. This feature isolates sensitive financial operations from other network traffic, ensuring end-to-end encryption and minimizing vulnerabilities.

3. Blockchain Integration:

Trustless Architecture: Blockchain technology is used to create a tamper-proof ledger for all transactions, ensuring transparency and immutability. This integration enhances the security and compliance of the UPI system with global financial regulations and eliminates single points of failure.

4. Real-Time Performance:

Ultra-Low Latency: The use of 5G's ultra-low latency ensures real-time transaction processing, crucial for maintaining a smooth and efficient payment experience.

Network Slicing: 5G network slicing allows us to isolate sensitive financial transactions within dedicated network slices, reducing the risk of cyber-attacks and improving overall security.

5. Scalability and Future-Readiness:

Future Scalability: The solution is designed to scale with the increasing demand for digital payments, accommodating future growth and evolving technological advancements.

Regulatory Compliance: The system is built to meet stringent global financial regulations, ensuring that it remains compliant and secure as financial regulations evolve.

6. **Performance Benchmarking:**

Extensive Testing: We will conduct rigorous performance benchmarking to evaluate authentication times, policy enforcement latencies, and transaction processing speeds. These benchmarks will demonstrate the superiority of our solution over existing systems, particularly in high-throughput and large-scale scenarios.

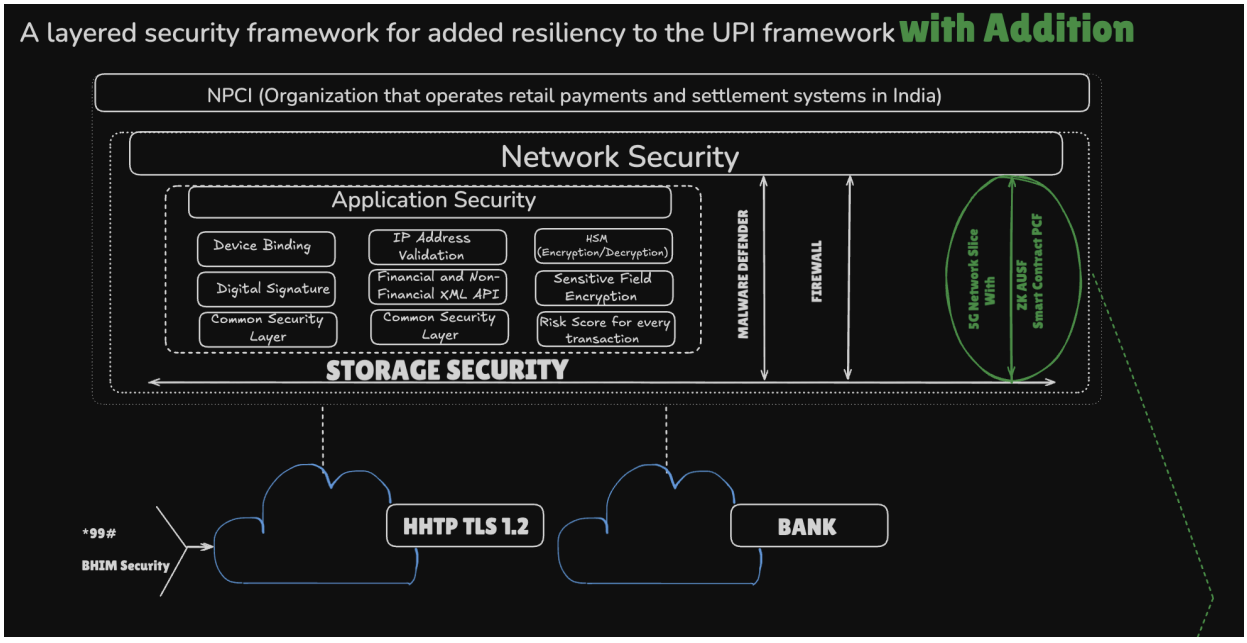
7. **Deployment and Impact:**

Rural Implementation: The solution will be deployed in selected rural areas, with plans to extend 5G connectivity to underserved regions. This deployment aims to enhance financial inclusion and drive economic growth in these communities.

Community Upliftment: By improving the reliability and security of financial transactions, our solution contributes to the broader goal of uplifting rural communities, aligning with the Aatmanirbhar Bharat and '5G Intelligent Villages' initiative.

6. Architecture

The UPI tech architecture remains the same but we provide additional layer in Network Security.



6.1 **Zero Knowledge AUSF**

The ZK-AUSF protocol leverages ZKBoo (Zero Knowledge Boolean Circuits using garbled circuits and multi-party oblivious transfers) to enable privacy-preserving authentication in the context of a 2PC (Two-Party Computation) framework. In this protocol, the focus is on ensuring minimal information disclosure while achieving robust authentication. ZKBoo empowers a prover (e.g., the User Equipment or UE) to authenticate itself to a verifier (e.g., the Authentication Server Function or AUSF) without disclosing the actual credentials. This is accomplished by securely computing the required functions using garbled circuits and oblivious transfer techniques.

The first contribution of this protocol is the application of ZKBoo's approach to the AUSF architecture, where authentication is framed as a Two-Party Computation problem. By employing garbled circuits, the protocol ensures that the prover's credentials remain confidential while the verifier performs the necessary computations to validate the authentication process. The use of multi-party oblivious transfers further enhances the privacy and security of the interaction.

Our second contribution addresses the challenge of privacy in authentication protocols. The ZK-AUSF protocol ensures that even though the verifier does not learn the prover's credentials, it can still verify the authenticity of the provided proof. This is achieved through zero-knowledge proofs that maintain the integrity of the authentication process without revealing sensitive information. This approach represents a significant advancement in achieving secure and privacy-preserving authentication in modern 5G networks.

Keywords: ZKBoo, zero-knowledge proofs, Two-Party Computation, garbled circuits, multi-party oblivious transfers, authentication protocols.

The **ZK-AUSF** protocol ensures that the **AUSF** can authenticate the user based on their credentials without learning sensitive information about them, leveraging the ZKBoo framework. The computation is divided into two parties:

1. **Prover (UE - User Equipment)**: The user with credentials who wants to authenticate to the network.
2. **Verifier (AUSF - Authentication Server Function)**: The network entity responsible for validating the UE's credentials.

Using ZKBoo, the UE can prove the correctness of its identity via a **zero-knowledge proof** by performing computations on Boolean circuits and sharing garbled circuits with the AUSF. The AUSF verifies the computation while ensuring confidentiality.

High-Level ZK-AUSF Protocol Steps:

1. **Setup**:

    - The UE and AUSF agree on a common function (e.g., a Boolean circuit representing the authentication algorithm, such as verifying the random challenge `RAND` and authentication token `AUTN`).
    - The function will verify if the UE's secret (its credentials) matches the expected values stored by the AUSF, without revealing those secrets.
2. **Prover's Computation (UE)**:
    - The UE (prover) uses its credentials, such as **SUPI**, **RAND**, and **AUTN**, to compute a response `RES` and session key `K_seaf` using a Boolean circuit representing the authentication algorithm (e.g., AKA algorithm).
    - The UE garbles the circuit using ZKBoo's three-party sharing scheme, which creates **garbled circuits** based on the authentication logic.
    - For each gate of the Boolean circuit, the UE generates a **commitment** and splits the computation into **three shares**, which are then used in **multi-party oblivious transfers**.
3. **Proof Generation**:
    - The UE sends the **garbled circuits** to the AUSF, along with commitments to each share of the Boolean circuit.
    - The UE also provides a zero-knowledge proof showing that the garbled circuit's output (e.g., the computed `RES`) is consistent with its credentials and does not leak any private information.
    - The proof consists of three parts: the Boolean circuits, the commitments to the shares, and the result of the computation (output of the garbled circuit).
4. **Verifier's Computation (AUSF)**:
    - The AUSF verifies the UE's proof by checking the commitments and evaluating the garbled circuit using **multi-party oblivious transfers** (MOT).
    - The AUSF verifies that the output of the garbled circuit is consistent with the expected output based on its stored authentication challenge `RAND` and `AUTN`.
    - If the garbled circuit evaluation succeeds, the AUSF accepts the proof and authenticates the UE.
5. **Session Key Generation**:
    - Upon successful verification, the AUSF and UE agree on a **session key** (e.g., `K_seaf`), ensuring a secure communication channel for further exchanges.
    - The key is derived from the garbled circuit's output and allows the UE and AUSF to establish a **security context** for future encrypted communication.

Detailed Protocol Steps:

Step 1: Initialization

- The UE (prover) and AUSF (verifier) agree on a Boolean circuit that represents the 5G-AKA authentication process, including computation of the response `RES` and generation of the session key `K_seaf`.

- The UE holds its private credentials (e.g., `SUPI`, `AUTN`, `RAND`) and will prove knowledge of a correct response based on these without revealing the actual credentials.

Step 2: Prover (UE) - Garbled Circuit Creation

- The UE generates a **garbled circuit** that computes the AKA response and session key based on its private input.
- For each gate in the Boolean circuit, the UE computes:
    - A **garbled version** of the gate.
    - Three **shares** of the inputs for each gate, following ZKBoo's approach.
- The UE sends the **garbled circuit** and shares to the AUSF.

Step 3: Multi-Party Oblivious Transfer (MOT)

- The AUSF uses **oblivious transfer** to receive two of the three shares for each gate from the UE, ensuring it does not learn the UE's private inputs.
- The oblivious transfer ensures that the AUSF can compute the output of the garbled circuit without seeing the intermediate values of the UE's private credentials.

Step 4: Verification and Commitment Checking

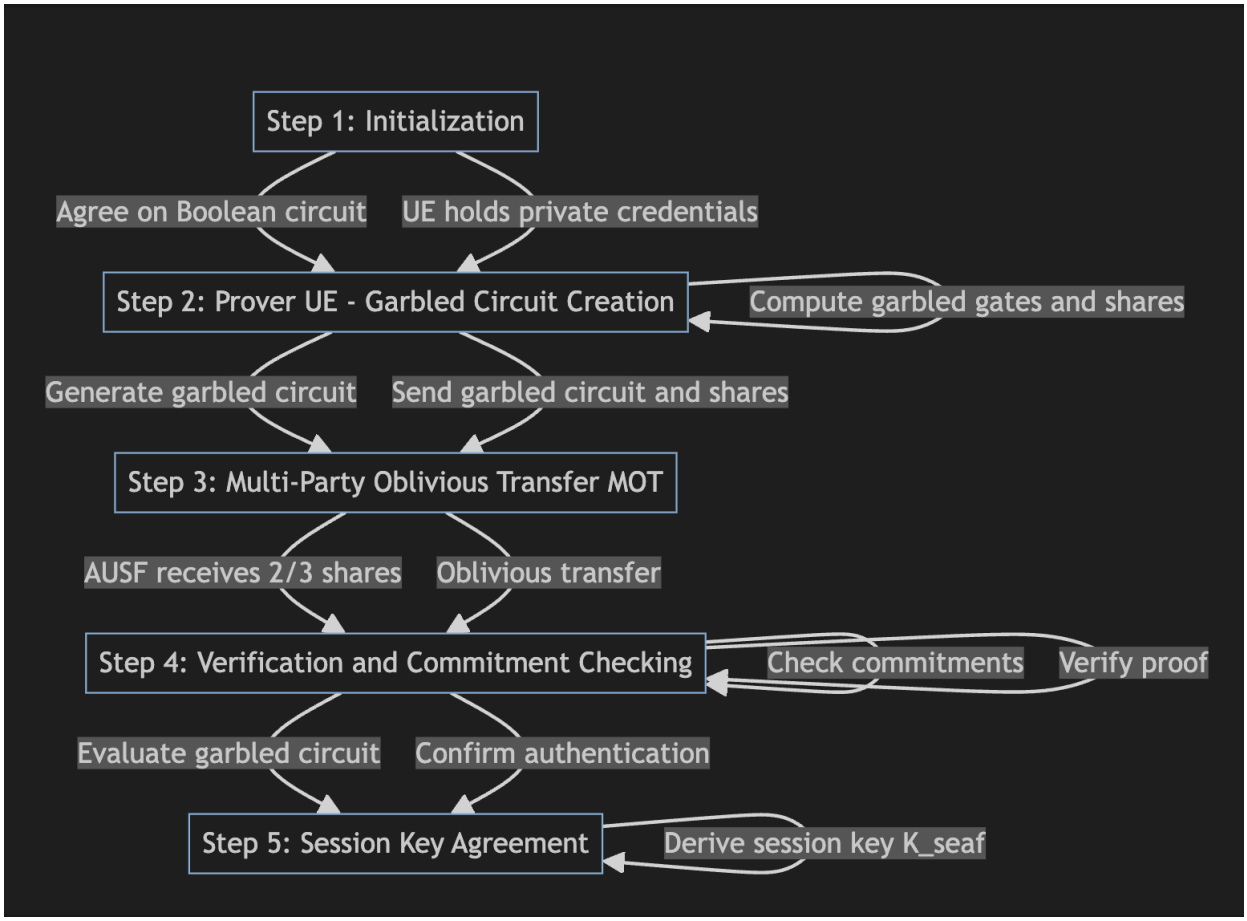
- The AUSF checks the commitments to the garbled circuit and verifies that the outputs match the expected values.
- The AUSF evaluates the garbled circuit and verifies the proof, ensuring that the response `RES` is valid without learning the UE's credentials.
- If the verification passes, the AUSF confirms that the UE has been authenticated.

Step 5: Session Key Agreement

- If the authentication is successful, the AUSF and UE use the garbled circuit's output to derive the session key `K_seaf`.
- The session key is then used to secure future communications between the UE and the network.

Security Guarantees:

- **Zero Knowledge**: The AUSF learns nothing about the UE's credentials, but can still verify that the UE holds valid credentials.
- **Soundness**: If the UE tries to authenticate with incorrect credentials, the AUSF will reject the proof, ensuring the protocol's correctness.
- **Privacy**: The UE's secrets (e.g., `SUPI`, `AUTN`) remain hidden even during the verification process.



Conclusion:

This **ZK-AUSF** protocol ensures secure, privacy-preserving authentication in 5G networks by shaping the AUSF authentication process as a **Two-Party Computation (2PC)** using ZKBoo's approach. By leveraging **garbled circuits** and **multi-party oblivious transfers**, this design provides zero-knowledge guarantees, allowing the UE to prove its identity without revealing sensitive information to the AUSF. The session key agreement further ensures that future communications are securely encrypted, completing the zero-knowledge-based authentication process.

6.2 Smart Contract PCF

The Smart Contract PCF (Policy Control Function) protocol introduces a novel approach to automating policy enforcement and network management in 5G networks through the use of smart contracts. This protocol integrates smart contracts with the Policy Control Function (PCF) to create a robust and flexible framework for managing network policies and ensuring secure communications. The core innovation lies in leveraging blockchain technology to automate and enforce policies within dedicated network slices, thereby enhancing security and operational efficiency.

Our first contribution is the design of a smart contract-based PCF system that utilizes blockchain's transparency and immutability to enforce network policies. By encoding policy rules and enforcement mechanisms into smart contracts, the protocol ensures that policies are applied consistently and transparently across network slices. This approach not only streamlines policy management but also reduces the potential for human error and operational inefficiencies.

The second contribution of this protocol is the integration of end-to-end encryption and automated policy enforcement. Smart contracts manage the dynamic allocation of resources and the application of security measures based on predefined policies, allowing for real-time adjustments and compliance with regulatory requirements. This results in a highly secure and adaptable network environment that can respond swiftly to changes in network conditions and policy requirements.

Keywords: Smart Contracts, Policy Control Function, blockchain, network slicing, automated policy enforcement, 5G network management.

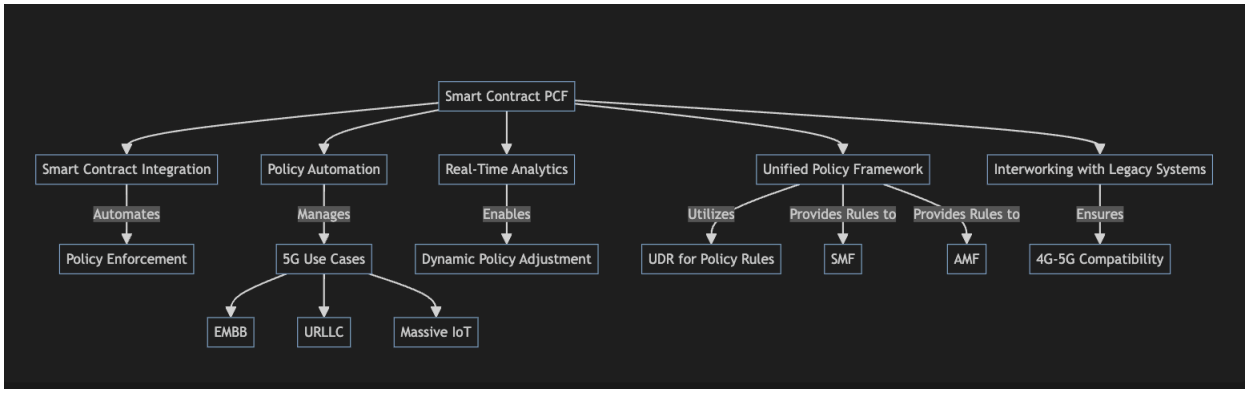
The Policy Control Function (PCF) is a critical component of the 5G Service-Based Architecture (SBA), extending the capabilities of the 4G Policy and Charging Rules Function (PCRF). While the PCRF provides policy enforcement and flow-based charging in 4G networks, the PCF enhances these functions with advanced features for network slicing, roaming, and real-time policy management. This protocol aims to leverage smart contracts to automate policy enforcement, streamline network management, and provide robust security through blockchain integration.

Protocol Design:

1. **Smart Contract Integration:** The Smart Contract PCF protocol integrates smart contracts into the PCF architecture to automate the definition, enforcement, and management of network policies. Smart contracts encode policy rules and control mechanisms, ensuring consistent and transparent policy enforcement across network slices.
2. **Policy Automation:** By utilizing blockchain's transparency and immutability, the protocol automates policy enforcement processes, reducing the potential for human error and operational inefficiencies. Smart contracts manage policies for various 5G use cases, including enhanced mobile broadband (EMBB), ultra-reliable low-latency communication (URLLC), and massive IoT.
3. **Real-Time Analytics:** The Smart Contract PCF protocol supports advanced business intelligence (BI) insights with real-time analytics. This capability enables service providers to dynamically adjust policies, create new offerings, and respond to changing network conditions and user demands.
4. **Unified Policy Framework:** The protocol supports a unified policy framework for managing network behavior. It utilizes policy subscription information from the User Data

Repository (UDR) to provide policy rules to network functions, such as the Session Management Function (SMF) and Access and Mobility Management Function (AMF).

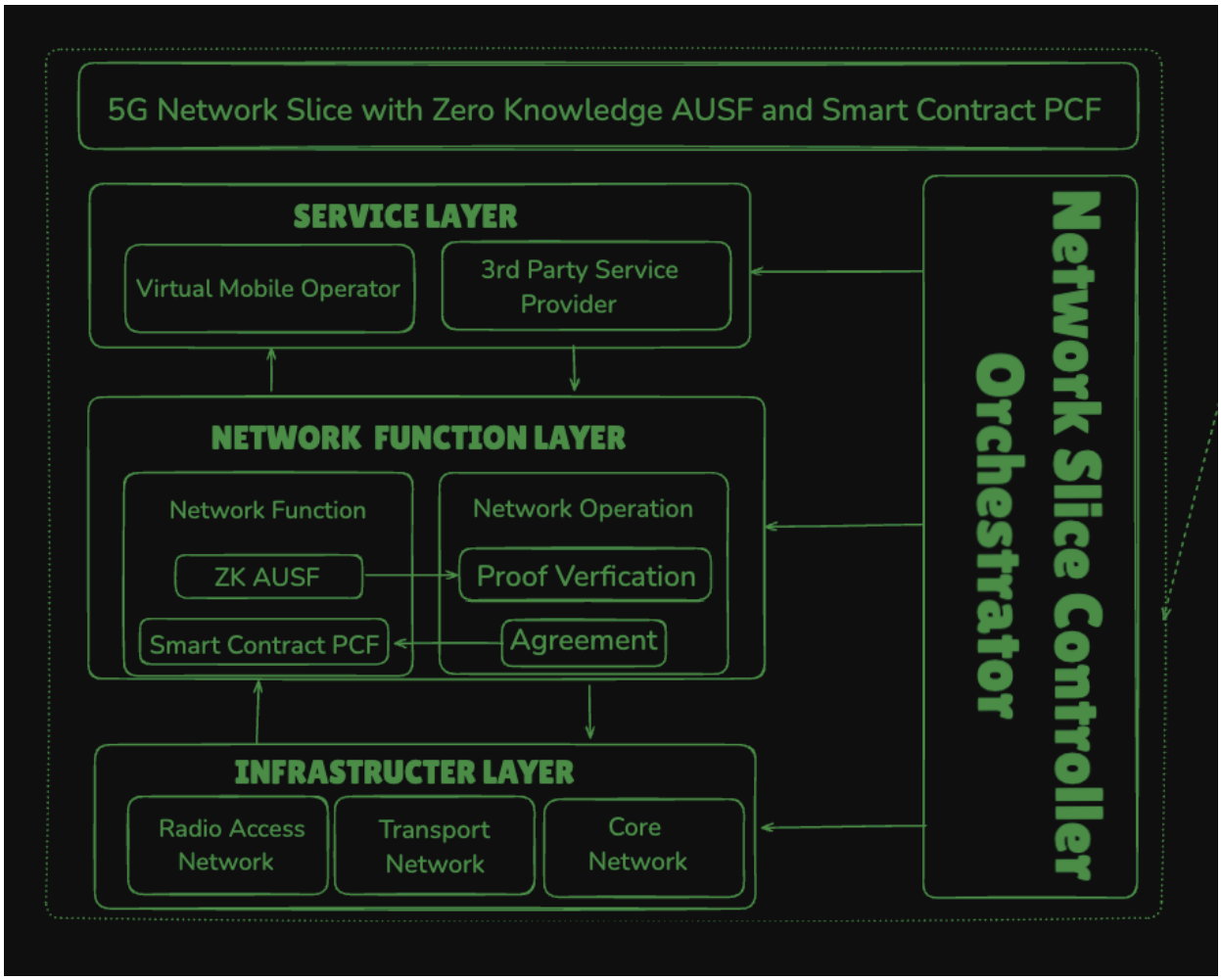
5. **Interworking with Legacy Systems:** To address the challenge of transitioning from 4G to 5G, the Smart Contract PCF protocol includes provisions for interworking with legacy PCRF functions. This ensures a smooth migration and compatibility between 4G and 5G network domains.



Conclusion. The Smart Contract PCF protocol represents a significant advancement in policy control and management for 5G networks. By integrating smart contracts and blockchain technology, the protocol enhances policy enforcement, improves operational efficiency, and provides a scalable solution for managing complex 5G network requirements. This approach aligns with the goals of a cloud-native, flexible, and secure 5G infrastructure.

6.2 **High Level Architecture**

5G network slice incorporating ZK AUSF and Smart Contract PCF represents a cutting-edge solution for secure and efficient financial transactions, particularly for Unified Payments Interface (UPI) systems. In this architecture, the ZK AUSF (Zero-Knowledge Authentication Server Function) employs zero-knowledge proofs to authenticate users without disclosing sensitive information, leveraging techniques such as garbled circuits and multi-party oblivious transfers for enhanced privacy and security. Complementing this, the Smart Contract PCF (Policy Control Function) utilizes blockchain technology to automate and enforce network policies, ensuring robust policy management through smart contracts. This combination enables real-time control of network resources and dynamic policy enforcement, while blockchain integration guarantees immutable and transparent transaction records. The result is a secure, scalable, and efficient network slice that not only supports the demands of modern financial transactions but also aligns with regulatory requirements and enhances overall system integrity.



This is an outline HLD and will modify while implementation.

7. 5G use cases

1. Secure Financial Transactions with UPI Integration

- **Description:** Deployment of UPI integrated with 5G network functions such as AUSF and PCF to ensure secure, low-latency financial transactions. This includes the use of blockchain for secure, immutable transaction records.
- **Impact:** Facilitates instant and secure financial transactions, critical for rural economic growth and financial inclusion.

2. Digital Identity Verification using Zero-Knowledge Proofs

- **Description:** Use of zero-knowledge proofs (ZKPs) for secure and private digital identity verification within the AUSF for financial services. This ensures user privacy while maintaining robust security.

- **Impact:** Enhances trust in digital financial services by protecting user data during authentication, crucial for adoption in rural areas.

3. Smart Contracts for Automated Policy Enforcement

- **Description:** Implementation of smart contracts within the PCF to enforce financial and data security policies automatically. These contracts can dynamically adjust to network conditions, ensuring continuous compliance and security.
- **Impact:** Automates policy enforcement, reducing the risk of human error and ensuring consistent application of security protocols.

4. Network Slicing for Secure Financial Operations

- **Description:** Utilization of 5G network slicing to create dedicated, secure slices for financial transactions. This isolates sensitive operations from other network traffic, reducing the risk of cyber-attacks.
- **Impact:** Guarantees secure and reliable financial services by protecting critical data and operations from network vulnerabilities.

5. Remote Banking and Financial Services

- **Description:** Deployment of remote banking solutions enabled by 5G's ultra-reliable low-latency communication (URLLC). These services include virtual banking, video-based customer service, and secure mobile banking apps.
- **Impact:** Provides rural populations with access to banking services without the need for physical bank branches, improving financial inclusion.

6. IoT-Enabled Financial Inclusion

- **Description:** Integration of IoT devices with 5G to enable financial services like micro-loans and insurance through automated data collection (e.g., crop health, weather conditions). Data is securely transmitted over 5G for processing and decision-making.
- **Impact:** Facilitates access to financial products tailored to the needs of rural communities, improving economic resilience and financial inclusion.

7. Blockchain for Supply Chain Financing

- **Description:** Use of blockchain to track and verify transactions in supply chain financing, ensuring transparency and trust between small-scale farmers and financial institutions.
- **Impact:** Enables rural businesses to access financing by providing secure, verifiable transaction histories, thereby boosting economic activity.

8. Real-Time Data Analytics for Financial Risk Management

- **Description:** Deployment of 5G-enabled real-time data analytics platforms for monitoring financial transactions and detecting fraud or other risks. These platforms can be integrated with UPI to provide instant risk assessments.
- **Impact:** Enhances the security and reliability of financial services by enabling proactive risk management and fraud detection.

9. Rural E-Governance Services

- **Description:** Leveraging 5G to deliver secure e-governance services related to finance, such as subsidy distribution, tax payments, and social security benefits directly to rural citizens.
- **Impact:** Simplifies access to government services for rural populations, ensuring transparency and reducing corruption in financial distributions.

10. Mobile Wallets and Microfinance Solutions

- **Description:** Deployment of 5G-enabled mobile wallets and microfinance platforms that can operate in low-bandwidth rural environments, providing access to small-scale financial services.
- **Impact:** Increases financial access for unbanked or underbanked rural populations, enabling economic growth and development.

Conclusion

This proposal provides a new ability to people living in rural areas , Dablong , Assam, where they can do UPI transaction just with bare minimum 5G network.