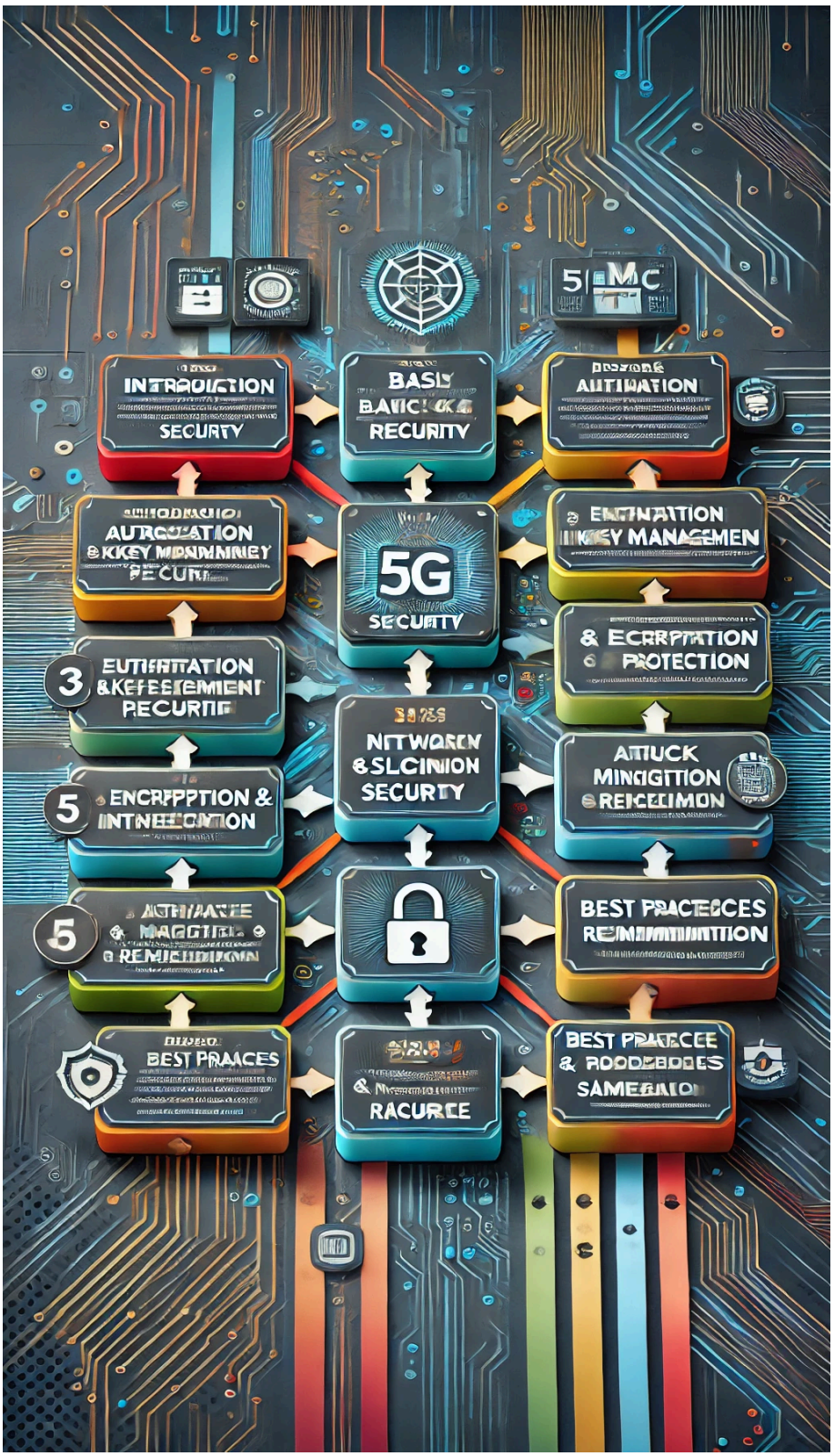
7. 5G Mobile Communication System Security Guide



1. Copyright Notice

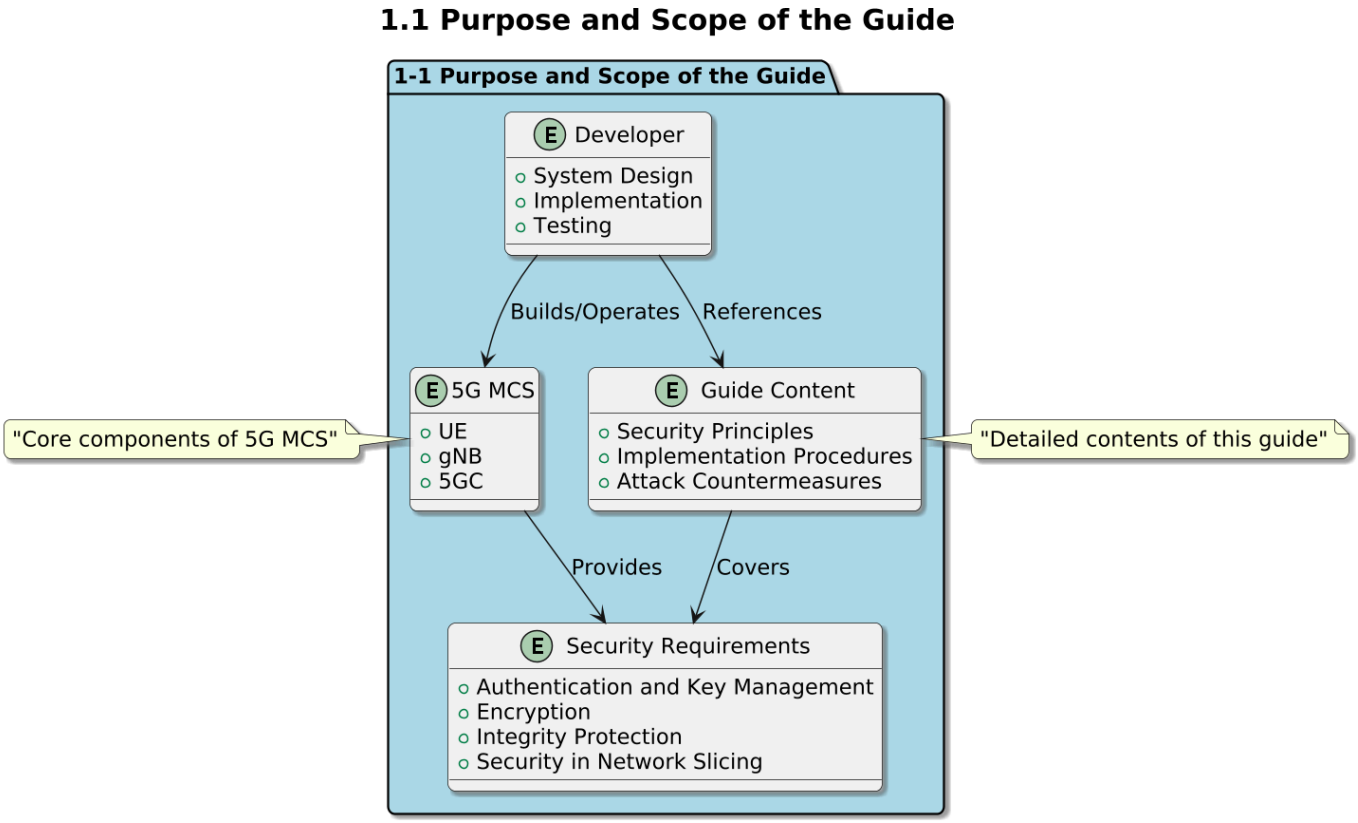
2. Disclaimer

The information in this document is provided based on currently available data; however, no guarantees are made regarding its accuracy or completeness. The copyright holder and related organizations assume no responsibility for any damages resulting from the use of this document.

Table of Contents

Chapter 1: Introduction

1.1 Purpose and Scope of the Guide



This guide aims to provide comprehensive security guidance for developers involved in the construction and operation of 5G MCS. Focusing on UE, gNB, and 5GC, it covers best practices for designing and implementing secure, high-performance, and feature-rich 5G MCS.

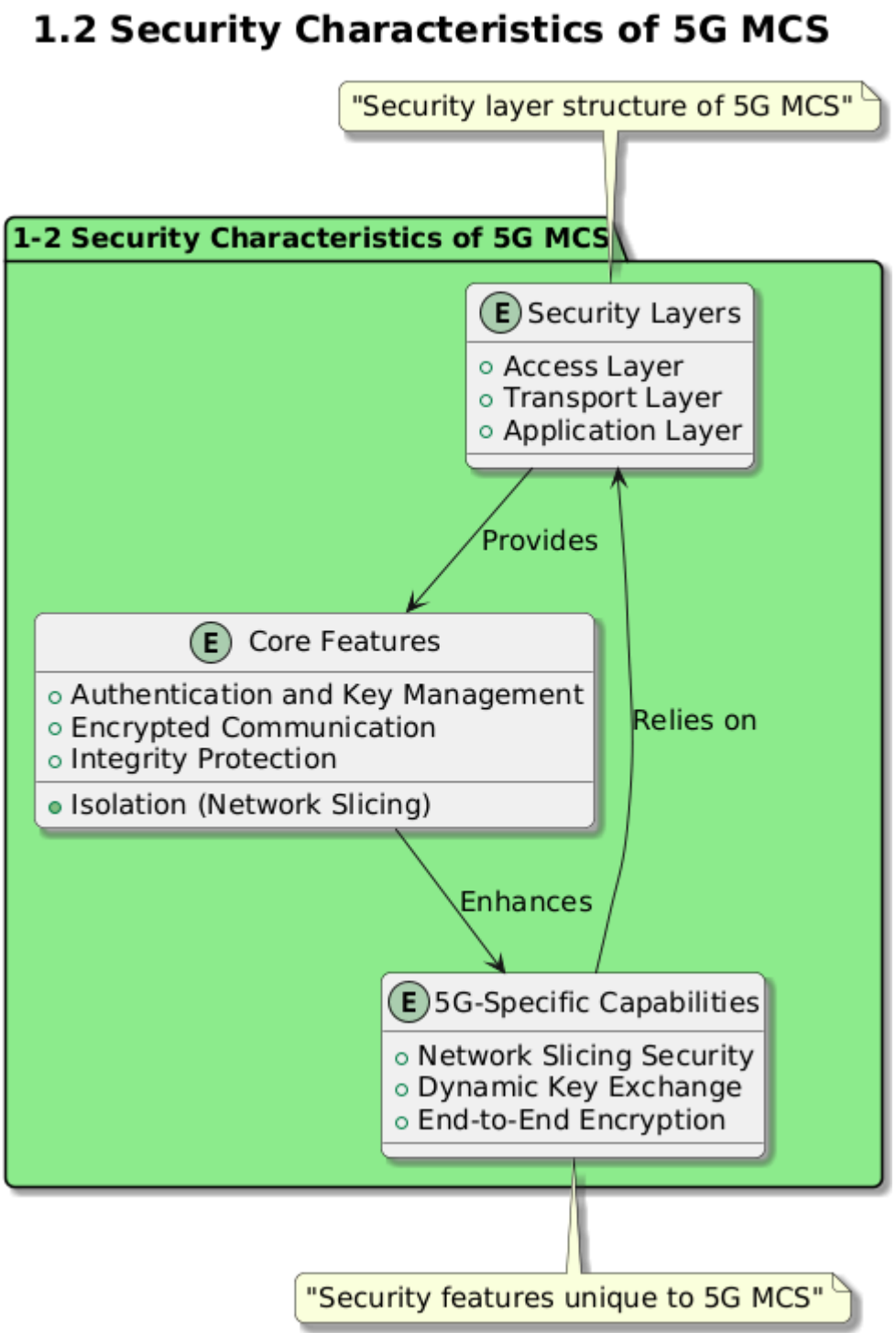
1.1.1 Purpose

- **Clarification of Security Principles:**
  This guide clarifies security requirements in 5G MCS including authentication, encryption, integrity protection, and network slicing security.
- **Provision of Implementation Guidelines:**
  It provides concrete implementation methods and configuration examples for security functions.
- **Support for Attack Countermeasures:**
  It introduces defense mechanisms against common attack methods and techniques to mitigate vulnerabilities.
- **Developer Support:**
  It comprehensively organizes useful information to assist developers in addressing challenges during the design and operation of 5G MCS.

1.1.2 Scope

- **System Configuration:**
  Security requirements for UE, gNB, and 5GC, as well as enhancements to the security of communication between these components.
- **Target Users:**
  Designers, developers, and operational administrators of 5G MCS.
- **Technical Areas:**
  Authentication protocols (5G-AKA, EAP-AKA'),
  Encryption and integrity algorithms (e.g., AES, HMAC),
  Security policy management in network slicing.

1.2 Security Characteristics of 5G MCS



The security characteristics of 5G MCS have significantly evolved compared to traditional communication systems. They include the following key attributes:

1.2.1 Layered Security

Access Layer:

- Provides authentication and encryption to protect communication between UE and gNB
- Encrypts and ensures integrity for RRC and NAS signaling

Transport Layer:

- Secures backhaul communications between gNBs and between gNB and 5GC using IPsec or TLS

Application Layer:

- Implements end-to-end data encryption

1.2.2 Dynamic Security Management

Authentication and Key Management:

- Employs dynamic key exchange based on the 5G-AKA protocol
- Supports distributed key management with periodic key rotation

Dynamic Slicing Security:

- Allows flexible application of security policies per network slice

1.2.3 End-to-End Encryption

- Encrypts both user-plane and control-plane communications
- Ensures data protection even across security boundaries

1.2.4 5G-Specific Security Features

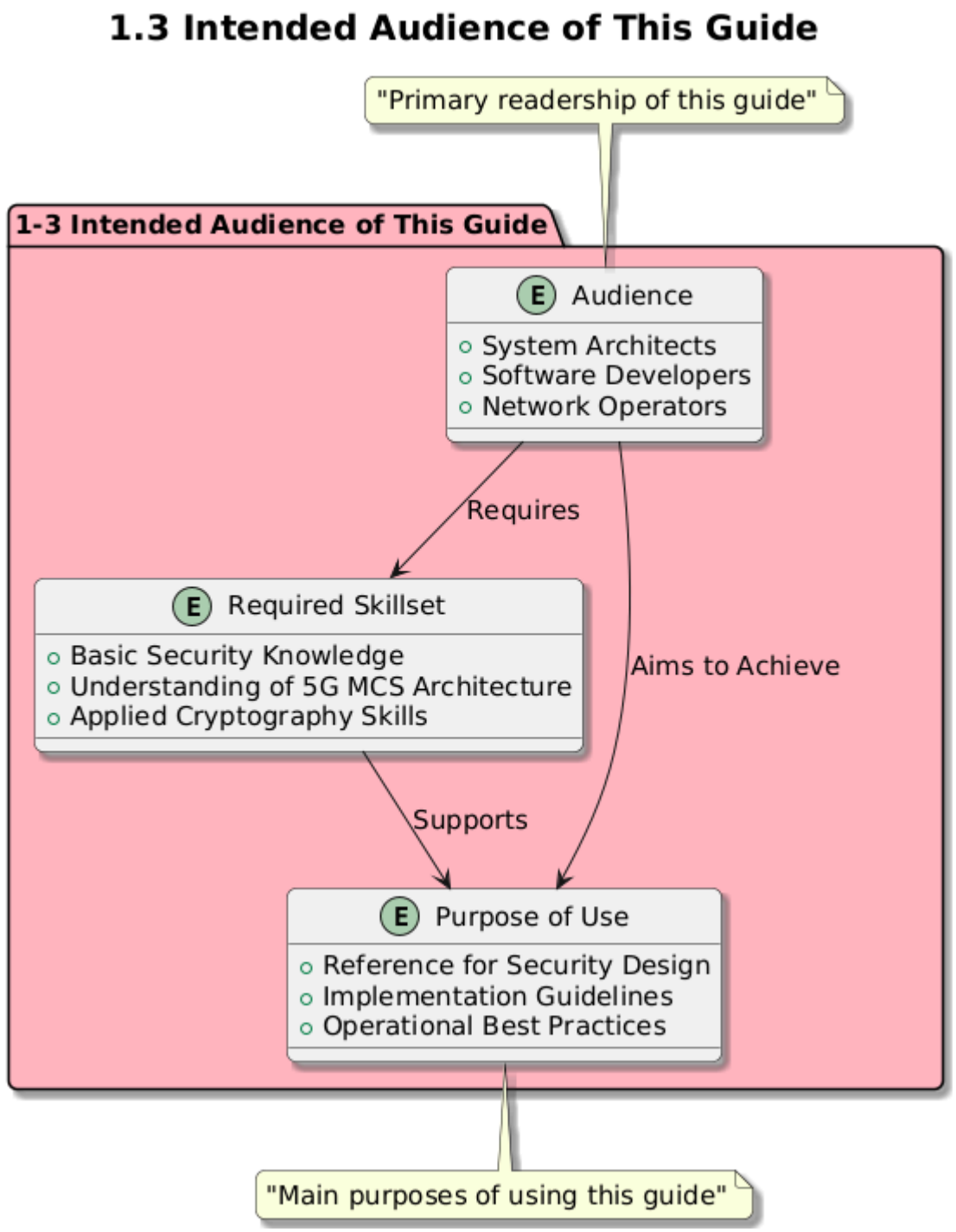
Network Slicing:

- Each slice maintains an independent security domain
- Supports SLA-based security requirements

Response to New Threat Models:

- Addresses security in virtualized infrastructure and open interfaces

1.3 Intended Audience of This Guide



This guide is primarily intended for the following readership. It outlines specific use cases depending on the reader's role and responsibilities.

Target Audience

System Architects:

Technical professionals involved in designing 5G MCS architecture and defining its security requirements.

Software Developers:
Engineers responsible for implementing security features in 5G MCS.
Network Operations Administrators:
Specialists managing security monitoring and vulnerability handling in live 5G MCS environments.

Required Skillset

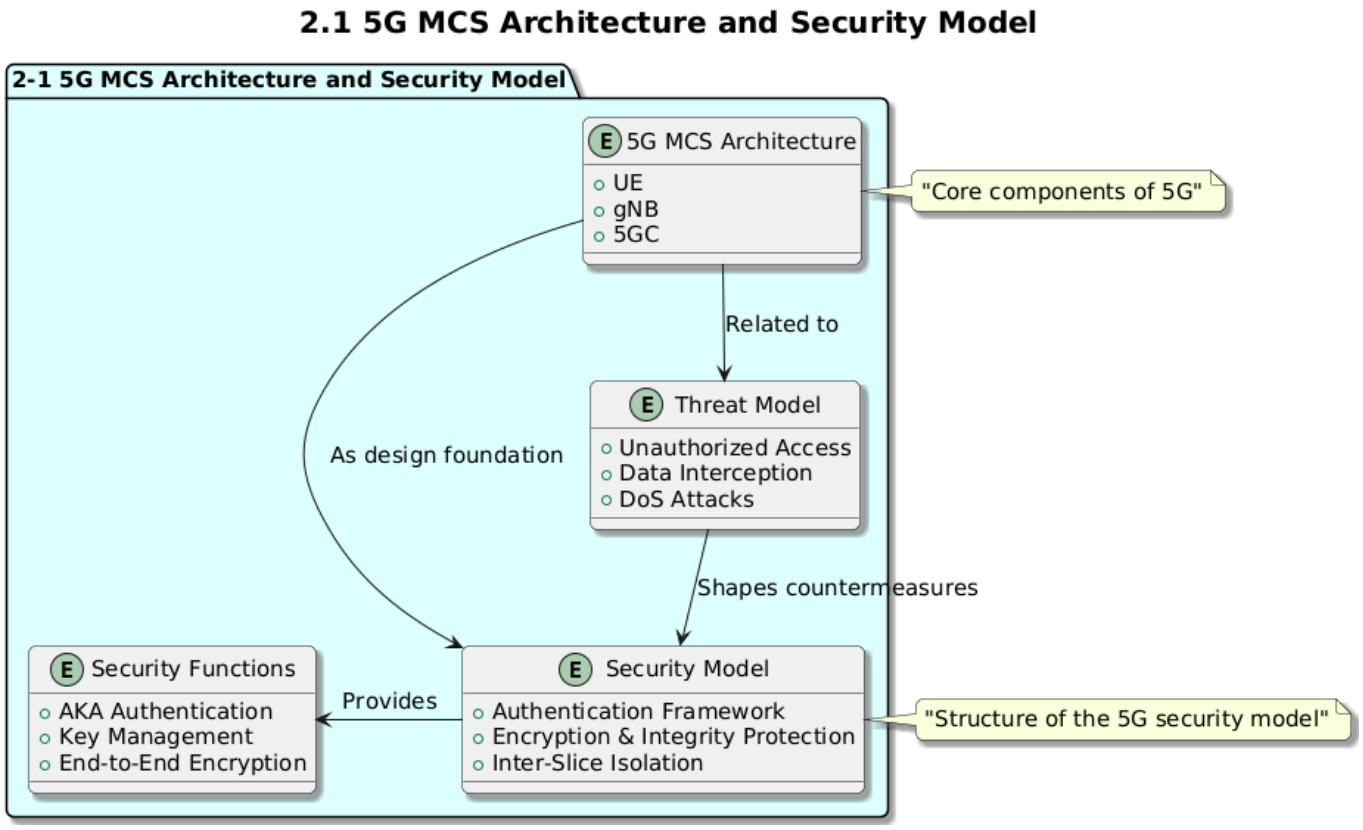
Basic Security Knowledge:
Fundamentals of encryption, authentication, and key management.
Understanding of 5G MCS Architecture:
Knowledge of interfaces and communication protocols between UE, gNB, and 5GC.
Applied Cryptography Skills:
Practical use of technologies such as AES, HMAC, TLS/IPsec.

Purpose of Use

Reference for Security Design:
Design guidance for building a secure 5G MCS.
Implementation Guidelines:
Concrete procedures and key considerations when implementing security functions.
Operational Best Practices:
Techniques for managing security risks and responding to incidents during system operation.
Readers are encouraged to reference this guide according to their specific roles, using the visual structure for guidance. Additional sections provide further detail where needed.

Chapter 2: Basic Concepts of 5G MCS Security

2.1 5G MCS Architecture and Security Model



Components of the 5G MCS Architecture

5G MCS is built upon a high-performance and flexible architecture, consisting of the following core components:

UE:

User equipment that accesses 5G services.

gNB:

A communication hub that connects UE to the 5GC.

5GC:

The core network that manages traffic and provides services.

Characteristics of the 5G MCS Security Model

Authentication Framework:

Robust authentication based on the 5G-AKA protocol.

Implements end-to-end authentication from UE to 5GC.

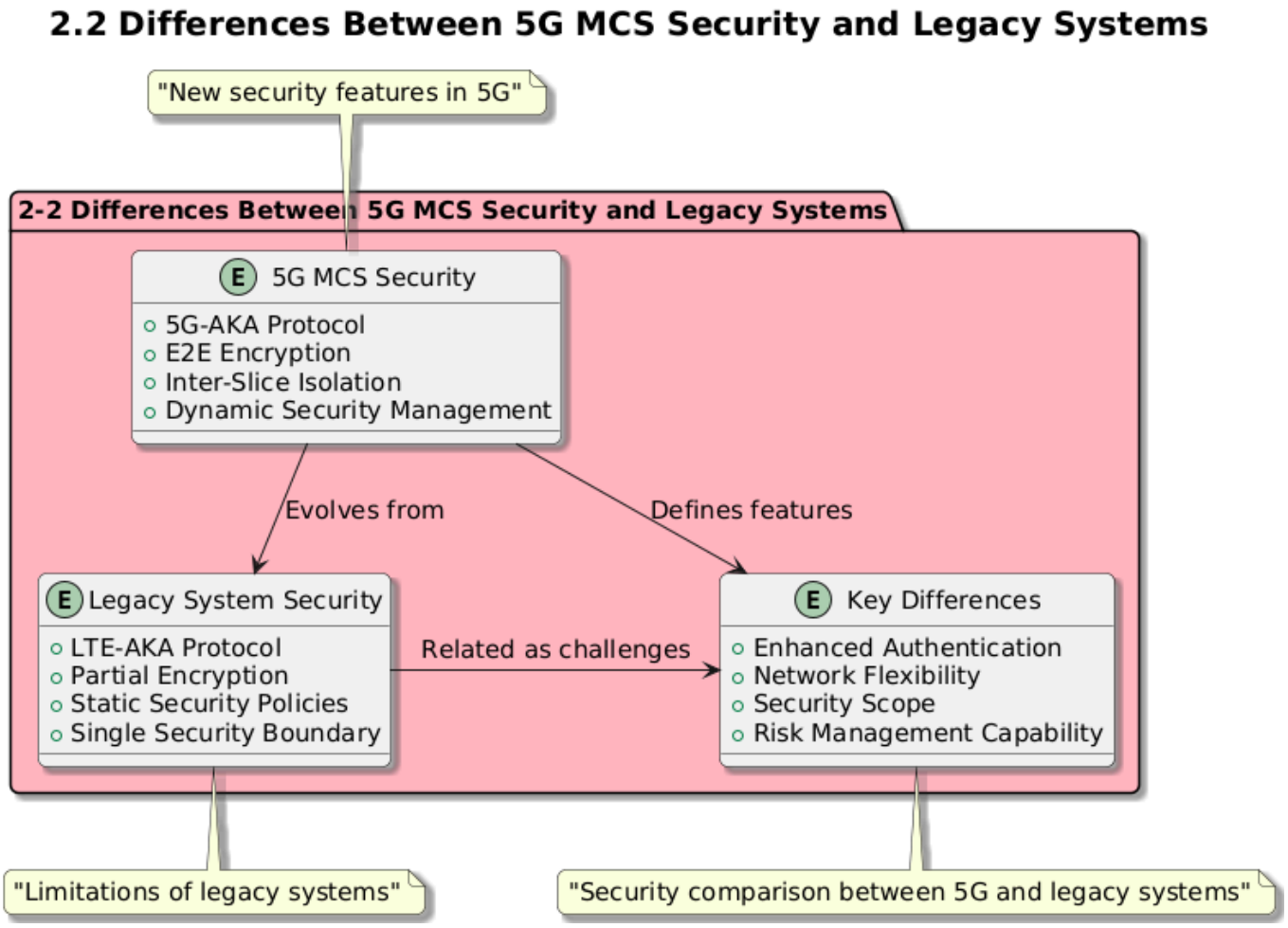
Encryption and Integrity Protection:
Encrypts both user-plane (U-Plane) and control-plane (C-Plane) traffic.
Prevents data tampering and interception.
Inter-Slice Isolation:
Applies independent security policies to each network slice, localizing potential security risks.

Associated Threat Models

Unauthorized Access:
Protects against attacks that attempt to steal authentication credentials.
Data Interception:
Uses encryption to prevent eavesdropping on communication paths.
DoS Attacks:
Applies traffic control techniques to ensure network availability.

The diagram above visually represents the relationships between the architecture, security model, functions, and threats. Other sections can also be translated and expanded upon if needed.

2.2 Differences Between 5G MCS Security and Legacy Systems



5G MCS Security Characteristics

5G-AKA Protocol:

Adopts an advanced authentication protocol to secure communications from the UE to the 5GC.

E2E Encryption:

Provides full end-to-end encryption for enhanced privacy compared to legacy systems.

Inter-Slice Isolation:

Applies individual security policies per Network Slice to reduce inter-slice risks.

Dynamic Security Management:

Enables real-time threat detection and flexible policy updates.

Legacy System Security

LTE-AKA Protocol:

The existing authentication mechanism is not as robust as in 5G.

Partial Encryption:

Only specific communication segments are encrypted, lacking full E2E protection.

Static Security Policies:

Policies are difficult to modify and not suited for real-time responses.

Single Security Boundary:

The network is managed as a single domain, meaning a breach can have wide-reaching impacts.

Key Differences

Enhanced Authentication:

5G introduces new authentication technologies, significantly improving security.

Network Flexibility:

With Network Slicing, 5G enables more granular and isolated security controls.

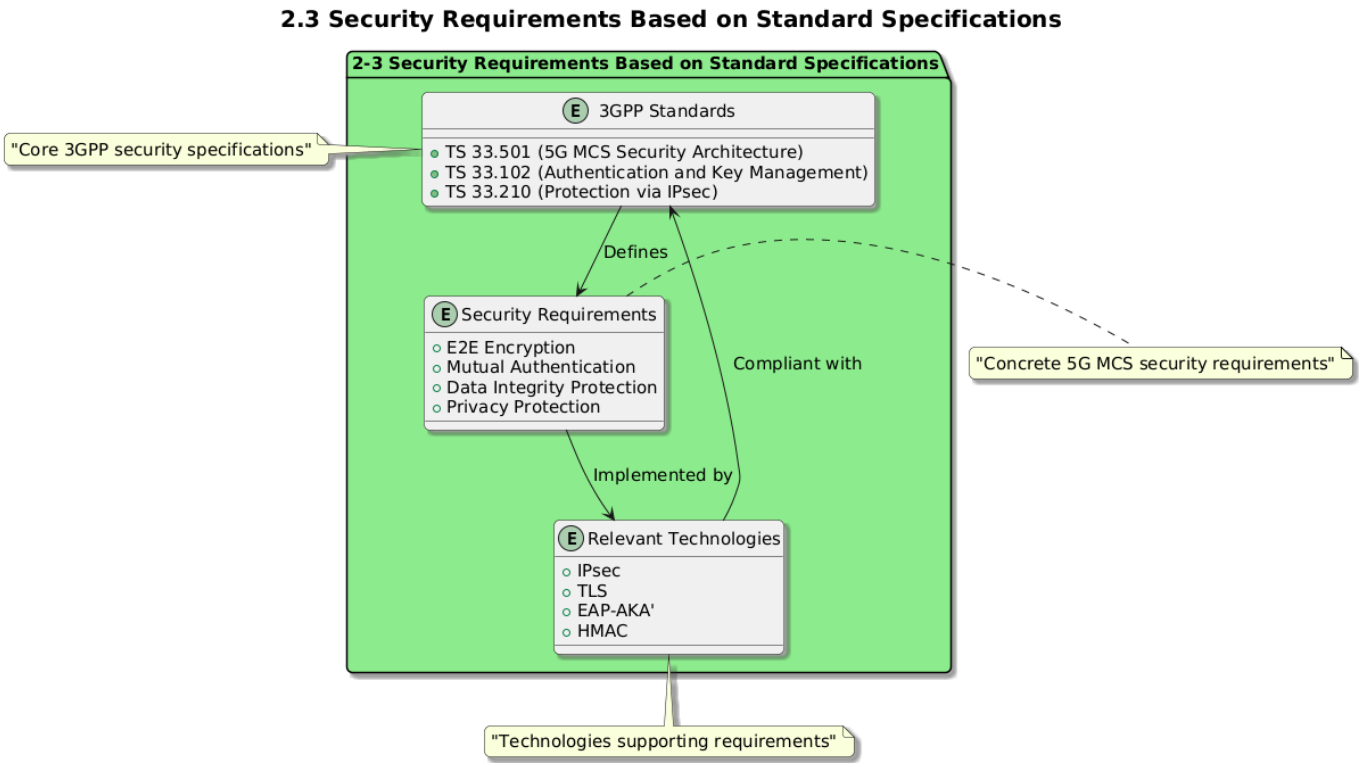
Security Scope:

5G enables complete end-to-end protection across the system.

Risk Management Capability:

Dynamic policy updates allow for immediate response to emerging threats.

2.3 Security Requirements Based on Standard Specifications



3GPP Standards

The security design of 5G MCS is based on the following 3GPP standard specifications:

TS 33.501:

Defines the security architecture for 5G MCS.

TS 33.102:

Details the processes for authentication and key management.

TS 33.210:

Specifies methods for protecting network communication using IPsec.

Key Security Requirements

E2E Encryption:

Encrypts the entire communication path to protect user privacy.

Mutual Authentication:

Ensures bidirectional authentication between the UE and the 5GC.

Data Integrity Protection:

Prevents data tampering through integrity checks.

Privacy Protection:

Includes anonymization of subscriber-related data.

Relevant Technologies

The security requirements defined by 3GPP are realized using the following technologies:

IPsec:

Provides encryption at the network layer.

TLS:

Ensures secure communication at the application layer.

EAP-AKA':

An authentication protocol adopted in 5G.

HMAC:

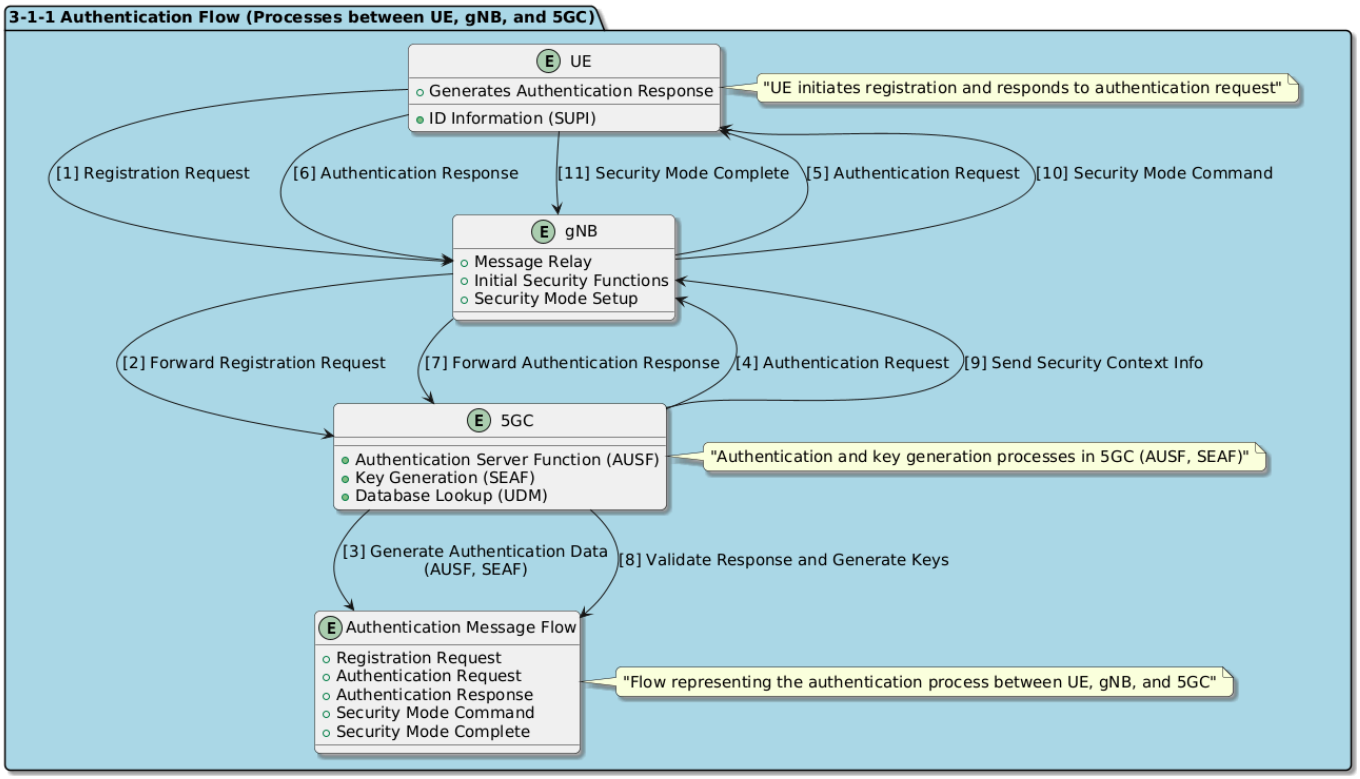
A mechanism to verify data integrity.

Chapter 3: Authentication and Key Management

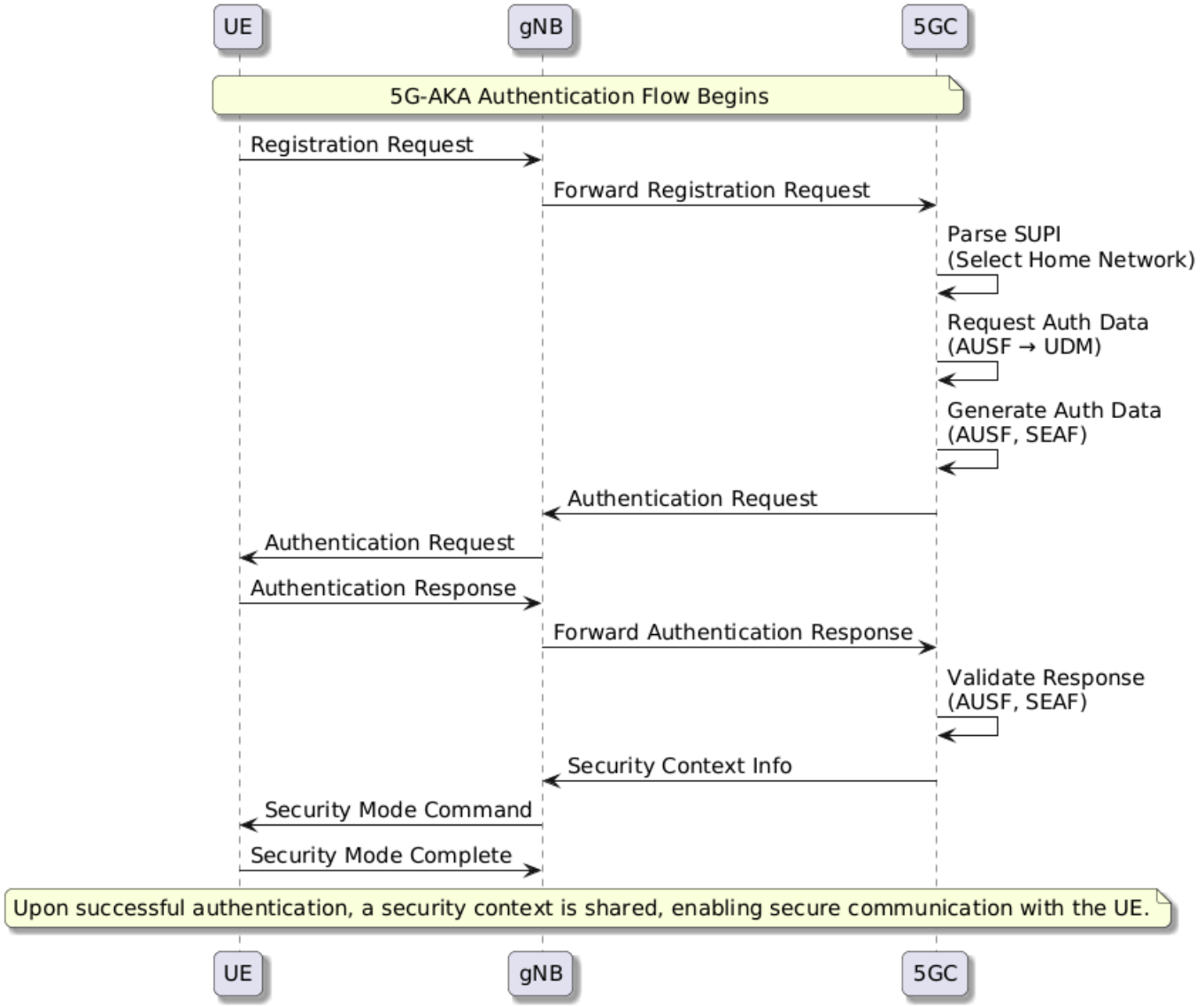
3.1 AKA Protocol (5G-AKA) Mechanism

3.1.1 Authentication Flow (Processes between UE, gNB, and 5GC)

3.1.1 Authentication Flow (Processes between UE, gNB, and 5GC)



3-1-1 Authentication Flow (Processes between UE, gNB, and 5GC)



Overview of the Authentication Process

The 5G-AKA protocol is used to establish secure communication between the UE, gNB, and 5GC, especially involving modules such as AUSF, SEAF, and UDM. The process involves the following steps:

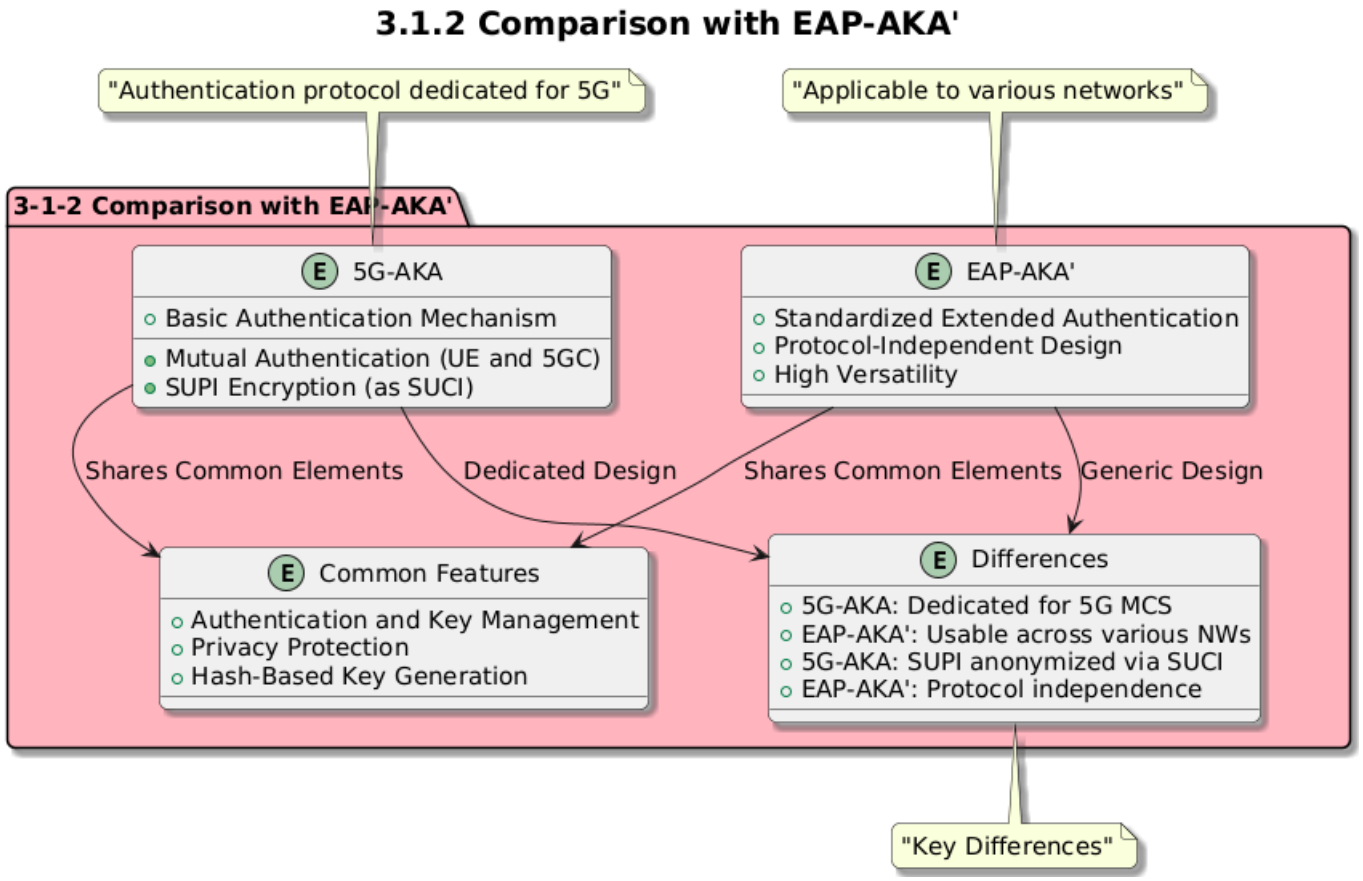
- **Registration Request by UE:**
  The UE initiates authentication using its SUPI (Subscriber Permanent Identifier) and sends a Registration Request to the gNB.
- **Message Relay by gNB:**
  The gNB forwards the Registration Request to the 5GC and may also perform initial security functions.
- **Authentication Handling in 5GC:**
  AUSF handles the authentication request and verifies subscriber data with the UDM. SEAF generates temporary session keys.
- **Sending the Authentication Request:**
  The 5GC generates an Authentication Request and sends it to the UE via the gNB.

- **Authentication Response by UE:**
  The UE processes the Authentication Request and generates an Authentication Response, which is forwarded by the gNB to the 5GC.
- **Verification and Key Generation by 5GC:**
  The 5GC validates the response and generates the security context, then transmits the related info to the gNB.
- **Establishment of Security Mode:**
  The gNB sends a Security Mode Command to the UE, and the UE completes it by responding with Security Mode Complete.
- **Result:**
  After completing key exchange and mutual authentication, secure communication between the UE and the network is established.

Enhancements in the Protocol

- **Mutual Authentication:**
  Ensures that both the UE and the 5GC verify each other's identities.
- **Enhanced Privacy Protection:**
  Encrypts the SUPI (sent as SUCI) to protect user identity.
- **Efficient Key Management:**
  Keys are hierarchically structured and generated at each step to streamline management.

3.1.2 Comparison with EAP-AKA'



Common Features

- Authentication and Key Management:
  Both protocols support mutual authentication between UE and 5GC.
- Privacy Protection:
  Mechanisms exist to protect user identity and sensitive data.
- Hash-Based Key Generation:
  Both use hash functions to strengthen security during key derivation.

Key Differences

- Purpose:
  - 5G-AKA:
    Tailored specifically for 5G MCS, using SUCI to anonymize SUPI.
  - EAP-AKA':
    Protocol-agnostic design, usable in Wi-Fi and other access networks.
- Design Philosophy:
  - 5G-AKA:
    Specifically designed for 5G network architecture.
  - EAP-AKA':
    General-purpose protocol designed for broader network compatibility.
- Enhanced Privacy:
  - 5G-AKA:
    Converts SUPI to SUCI for improved anonymity.

Use Cases

- 5G-AKA:
  Used for mobile user authentication within the 5G MCS.
- EAP-AKA':
  Used for authentication in public Wi-Fi networks and similar access environments.