YesDR Technical Specification

YesDR TS 02.005

Version 1.0.0
Release 1

YesDR Authentication Server Function (YAUSF)

Developed by
Chandhar Research Labs Pvt Ltd
BaSig Wireless Laboratories Pvt Ltd

Contents

1 Scope

This Technical Specification defines the YesDR Authentication Server Function (YAUSF).

YAUSF is responsible for UE authentication procedures in the YesDR core network and acts as the authentication anchor between the Access Management Function (YAMF) and the Unified Data Management (YUDM).

YAUSF is conceptually aligned with the 3GPP AUSF defined in TS 23.502 and TS 29.509.

—

2 References

2.1 Normative References

- YesDR TS 01.001: YesDR Overall Architecture
- YesDR TS 02.001: YesDR Core Network Functions
- YesDR TS 02.004: YesDR Unified Data Management (YUDM)

2.2 Informative References

- 3GPP TS 23.502: Procedures for the 5G System
- 3GPP TS 29.509: Authentication Server Services
- 3GPP TS 33.501: Security Architecture

3 Definitions, Symbols, and Abbreviations

Abbreviation	Description
YAUSF	YesDR Authentication Server Function
YAMF	YesDR Access Management Function
YUDM	YesDR Unified Data Management
YNRF	YesDR Network Repository Function
SUPI	Subscription Permanent Identifier
SUCI	Subscription Concealed Identifier
RES*	Response Star
XRES*	Expected Response Star
HXRES*	Hashed XRES*

4 Functional Overview

YAUSF performs the following functions:

- Validation of serving network authorization
- Retrieval of authentication vectors from YUDM
- Derivation of authentication parameters
- Verification of UE authentication response
- Derivation of session anchor keys

YAUSF SHALL expose service-based interfaces over HTTP/2.

—

5 YAUSF Architecture

YAUSF consists of:

- NRF registration and service discovery client
- Authentication vector cache
- Cryptographic processing engine
- REST-based service interface

YAUSF SHALL register with YNRF and maintain liveness via heartbeat messages.
—

6 Service-Based Interfaces

6.1 Nausf_UEAuthentication

6.1.1 Nausf_UEAuthentication_Request

HTTP Method: POST
URI: /authenticate

Input Parameters:

- SUCI
- GUTI (optional)
- Serving Network Name (SNname)
- AUTS (optional)

Output Parameters:

- RAND
- AUTN
- HXRES*
- Kseaf
- SUPI

—

6.2 Nausf_UEAuthentication_Verify

HTTP Method: POST
URI: /verify

Input Parameters:

- RES*
- SUPI

Output:

- Authentication result

—

7 Authentication Procedures

YAUSF SHALL perform the following steps:

1. Validate serving network authorization
2. Request authentication data from YUDM
3. Compute HXRES*
4. Derive Kseaf from Kausf
5. Store XRES* and Kausf temporarily

—

8 RES* Verification

YAUSF SHALL compare RES* received from YAMF with stored XRES*.

If RES* equals XRES*, authentication SHALL be considered successful. Otherwise, authentication SHALL fail.

—

9 Security Considerations

YAUSF SHALL:

- Protect cached authentication material
- Use secure transport (HTTPS)
- Validate all input parameters

Authentication material SHALL be stored only for the duration of the procedure.

—

10 Error Handling

YAUSF SHALL return appropriate error responses for:

- Unauthorized serving networks
- Invalid authentication data
- RES* mismatches

—

11 Relationship to 3GPP AUSF

YAUSF aligns with the functional behavior of the 3GPP AUSF while:

- Using simplified REST-based interfaces
- Supporting SDR-based research deployments
- Enabling extensibility for AI-assisted security analytics

—