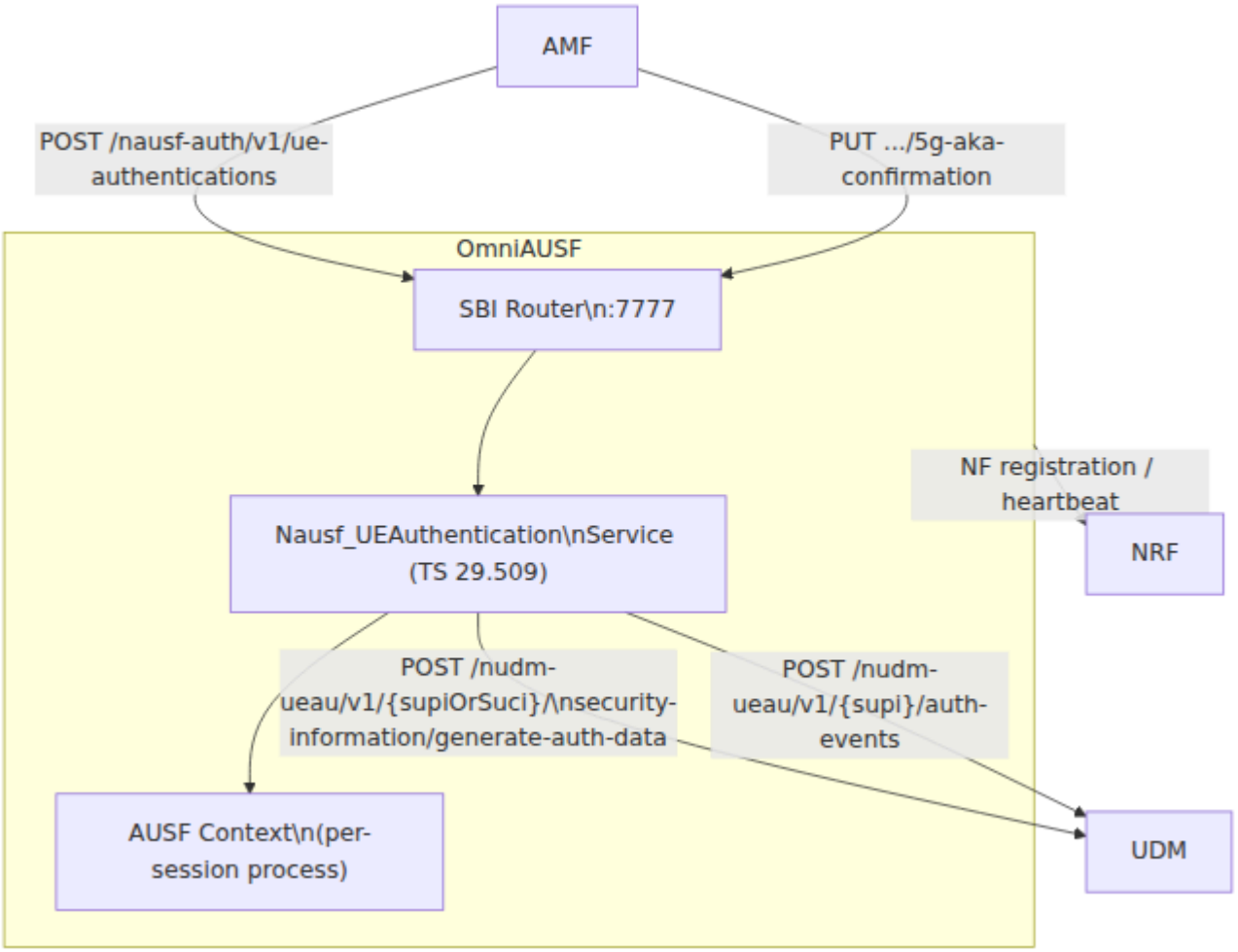
OmniAUSF Operations

1. Component Overview

OmniAUSF is the standalone Authentication Server Function (AUSF) for the Omnitouch 5G core. It orchestrates 5G-AKA authentication between the AMF and UDM, verifying UE authentication responses and deriving session keys. OmniAUSF was previously co-located within OmniUDM and is now deployed as an independent NF with its own SBI endpoint.

Each authentication session is managed by a dedicated process (process-per-auth-session). Authentication context is held in-memory for the duration of the authentication exchange and deleted on completion or failure.



2. 3GPP Role and Spec References

Aspect	Reference
AUSF functional definition	TS 23.501 Section 6.2.8
Nausf_UEAuthentication service	TS 29.509
5G-AKA authentication	TS 33.501 Section 6.1.3
HXRES*/HRES* computation	TS 33.501 Annex A.5
KSEAF derivation	TS 33.501 Annex A.6
UDM authentication data generation	TS 29.503 Section 5.2.2
SQN resynchronisation	TS 33.102 Section 6.3.5, TS 33.501 Section 6.1.3.4

3. SBI Endpoints

All endpoints are HTTP/1.1 with `Content-Type: application/json`.

Nausf_UEAuthentication (TS 29.509)

Method	Path	Description	Success
POST	`/nausf-auth/v1/ue-authentications`	Initiate UE authentication (AMF -> AUSF)	201 Created
PUT	`/nausf-auth/v1/ue-authentications/{authCtxId}/5g-aka-confirmation`	Confirm 5G-AKA (AMF sends RES*)	200 OK

Error Responses

HTTP Status	Cause	Condition
404	USER_NOT_FOUND	UDM returned 404 for the subscriber
401	AUTHENTICATION_FAILURE	HRES* does not match HXRES*
500	SYSTEM_FAILURE	Internal error or UDM unreachable

4. Configuration Reference

OmniAUSF is configured via Elixir application environment under the `:omniausf` key.

Example Configuration

```
config :omniausf,
  sbi_scheme: "http",
  sbi_addr: "127.0.0.19",
  sbi_port: 7777,
  nrf_uri: "http://127.0.0.10:7777",
  udm_uri: "http://127.0.0.12:7777",
  mcc: "999",
  mnc: "70",
  heartbeat_interval: 10_000
```

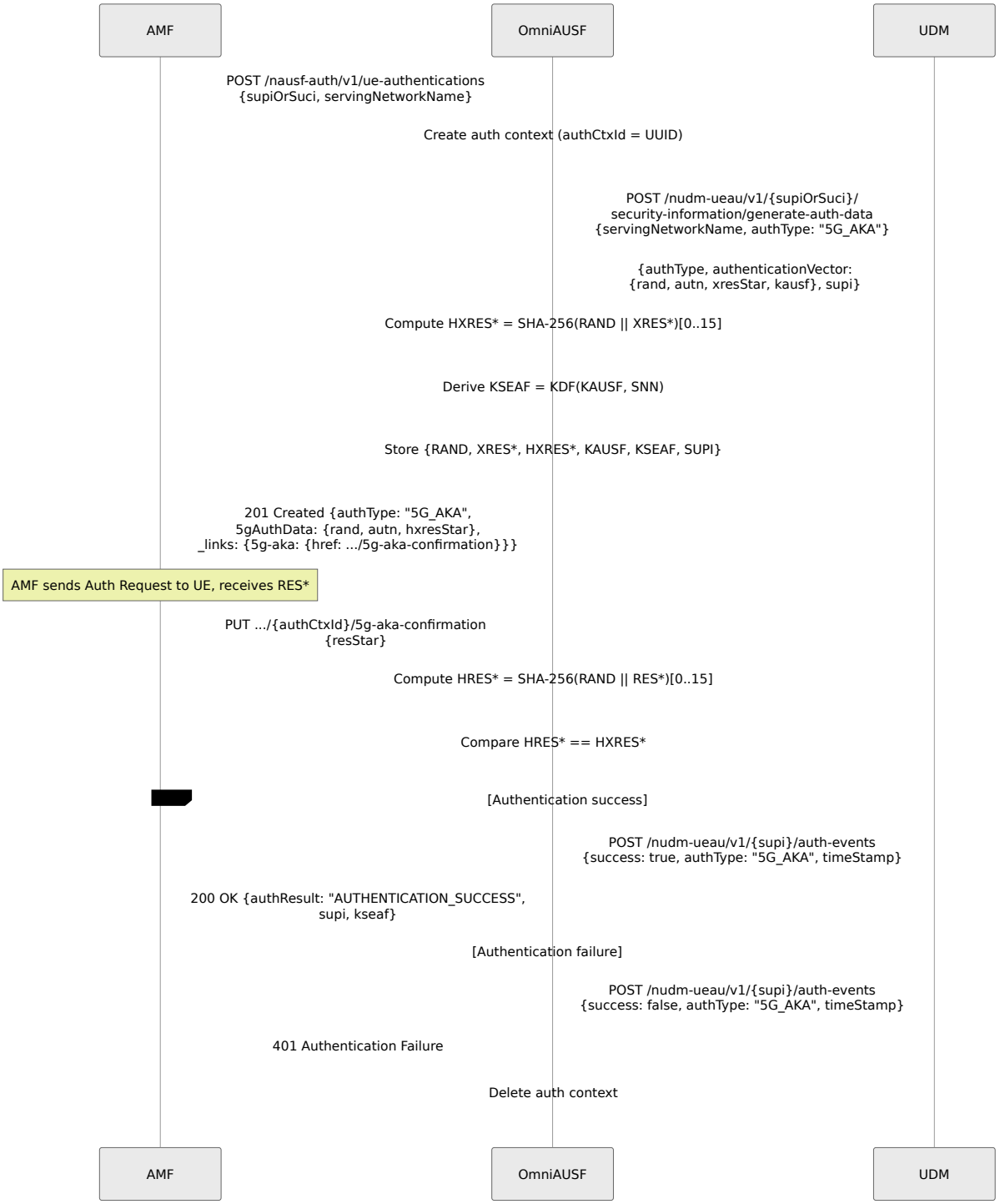
Parameter Table

Parameter	Type	Default	Description
`sbi_scheme`	string	`"http"`	URI scheme for the SBI HTTP server
`sbi_addr`	string	`"127.0.0.19"`	IP address th SBI HTTP server binds to
`sbi_port`	integer	`7777`	TCP port the SBI HTTP server listens on
`nrf_uri`	string	`"http://127.0.0.10:7777"`	Base URI of the NRF for NF registration and heartbea
`udm_uri`	string	`"http://127.0.0.12:7777"`	Base URI of the UDM for authenticatio vector generation and auth event storag
`mcc`	string	`"999"`	Mobile Country Code for the serving PLMN

Parameter	Type	Default	Description
`mnc`	string	`"70"`	Mobile Network Cod for the serving PLMN
`heartbeat_interval`	integer (ms)	`10000`	Interval at which OmniAUSF sends NRF heartbeat PATCH requests

5. Key Procedures

5.1 5G-AKA Authentication Flow



6. Prometheus Metrics

AUSF Metrics

Metric	Type	Tags	Descrip
`omni_ausf.auth.count`	counter	`result`	Total authentic operations (initiated/succe
`omni_ausf.nrf.registration.status`	gauge	`nf_type`	NRF registratio (1=registered,
`omni_ausf.active_contexts.count`	gauge	--	Number of acti UE authenticat contexts

BEAM VM Metrics

Metric	Type	Description
`beam.memory.total`	gauge	Total BEAM memory in bytes
`beam.memory.processes`	gauge	Memory used by Erlang processes
`beam.memory.system`	gauge	System memory (ETS, atoms, code)
`beam.processes.count`	gauge	Number of Erlang processes
`beam.vm.uptime`	gauge	VM uptime in seconds

7. Known Limitations

ID	Area	Description
AUSF-1	In-memory state	Authentication contexts are stored in memory only. State is lost on process restart. Active authentication sessions will fail on AUSF restart; the AMF must re-initiate authentication
AUSF-2	EAP-AKA'	Only 5G-AKA is supported. EAP-AKA' authentication method (TS 33.501 Section 6.1.3.1) is not implemented
AUSF-3	Resync forwarding	The AUSF does not independently handle `resynchronizationInfo`; it passes through to UDM. The AMF must include `resynchronizationInfo` in the initial authentication request

8. Troubleshooting

Authentication fails with 404 User Not Found

The UDM returned 404 for the subscriber. Confirm:

1. `udm_uri` is reachable from the OmniAUSF host.
2. The subscriber IMSI exists in the UDM/UDR/HSS backend.
3. The SUCI presented by the AMF is correctly formatted.

Authentication fails with 401 Authentication Failure

The AUSF computed HRES* from the received RES* and it did not match the stored HXRES*. This indicates the UE's credentials (Ki, OPc) do not match those in the backend, or the RAND/AUTN were corrupted in transit.

UDM unreachable (500 Internal Error)

Check `udm_uri` configuration and network connectivity. The AUSF logs `AUSF auth failed for {supiOrSuci}: {reason}` on UDM communication failure.

Authentication context not found on confirmation

The `authCtxId` in the PUT request does not match any active context. Contexts are deleted after successful or failed confirmation, and are lost on AUSF restart. The AMF must re-initiate authentication.