



UE Context Transfer Support

- [Feature Summary and Revision History, on page 1](#)
- [Feature Description, on page 1](#)
- [How It Works, on page 3](#)
- [Feature Configuration, on page 5](#)

Feature Summary and Revision History

Summary Data

Table 1: Summary Data

Applicable Product(s) or Functional Area	AMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Documentation	Not Applicable

Revision History

Table 2: Revision History

Revision Details	Release
First introduced.	2022.01.0

Feature Description

AMF supports the UE Context Transfer message at source and target AMF. The following CLI configurations are added:

- `allow-interplmn-supi-transfer`
- `horizontal-key-derivation`
- `use-source-key`
- `use-source-pcf`

UE Context Transfer at Source AMF:

- Sends UE Context with SUPI value to target AMF as per the CLI configuration, when source AMF and target AMF are in different PLMN
- Uses either existing keys or generates new keys, and sends the keys to target AMF during context transfer as per the CLI configuration
- Starts `context-transfer-guard` timer (configured with greater than zero (0)), when `UeRegStatusUpdateReqData` contains transfer status as TRANSFERRED

On expiry of the `context-transfer-guard` timer, source AMF performs the following:

- Triggers the UDM Deregistration internally to clear the local `ueContext`
- When the UE Context Transfer reason is `INIT_REG`, it updates the SMF to release the PDU context
- It releases PDU sessions in the `toReleaseSessionList`
- The UE-validation reason is handled as follows:
 - Without registration request
 - By omitting integrity check
 - Responding with appropriate data to target AMF
- Clears PCF association, when target AMF sends `pcfReselectedInd` in transfer update
- Handles reject indication received from target AMF
- Performs horizontal key derivation as per the CLI configuration
- Transfers URI with SUPI as `ueContextId` to target AMF
- Sends DRX, GMM capability IEs to target AMF
- Increments transfer failure counters including `NOT_TRANSFERRED` counters
- Doesn't send `SeafData` in transfer response in `MOBI_REG_UE_VALIDATED` when the Individual `ueContext` is identified with SUPI

UE Context Transfer handling at Target AMF:

- Sends Reject Indication to source AMF through `StatusUpdate` message when authentication or security fails

The security algorithm mismatch is handled as follows:

- Authenticates when integrity check fails
- Recomputes the keys as per the algorithm received from AUSF

- Regenerates all the keys and ignores the keys received from source AMF.
- Sends failure to source AMF when authentication or security check fails
- The SUPI as UeContextID is handled as follows:
 - Sends Identity request to UE when message integrity check fails
 - Performs UE authentication with obtained SUPI from UE
 - Sends SUPI as UeContextId, and UE-validated in UeContextTransferReq to source AMF
- Ignores the PCF information obtained from the source AMF and selects the new PCF based on the CLI configuration. Informs the selection of new PCF using pcfReselectedInd to source AMF in UeRegStatusUpdateReq.

How It Works

This section describes how this feature works.

Call Flows

This section describes the key call flow for this feature.

UE Context Transfer Call Flow

This section describes the UE Context Transfer call flow.

Figure 1: UE Context Transfer Call Flow

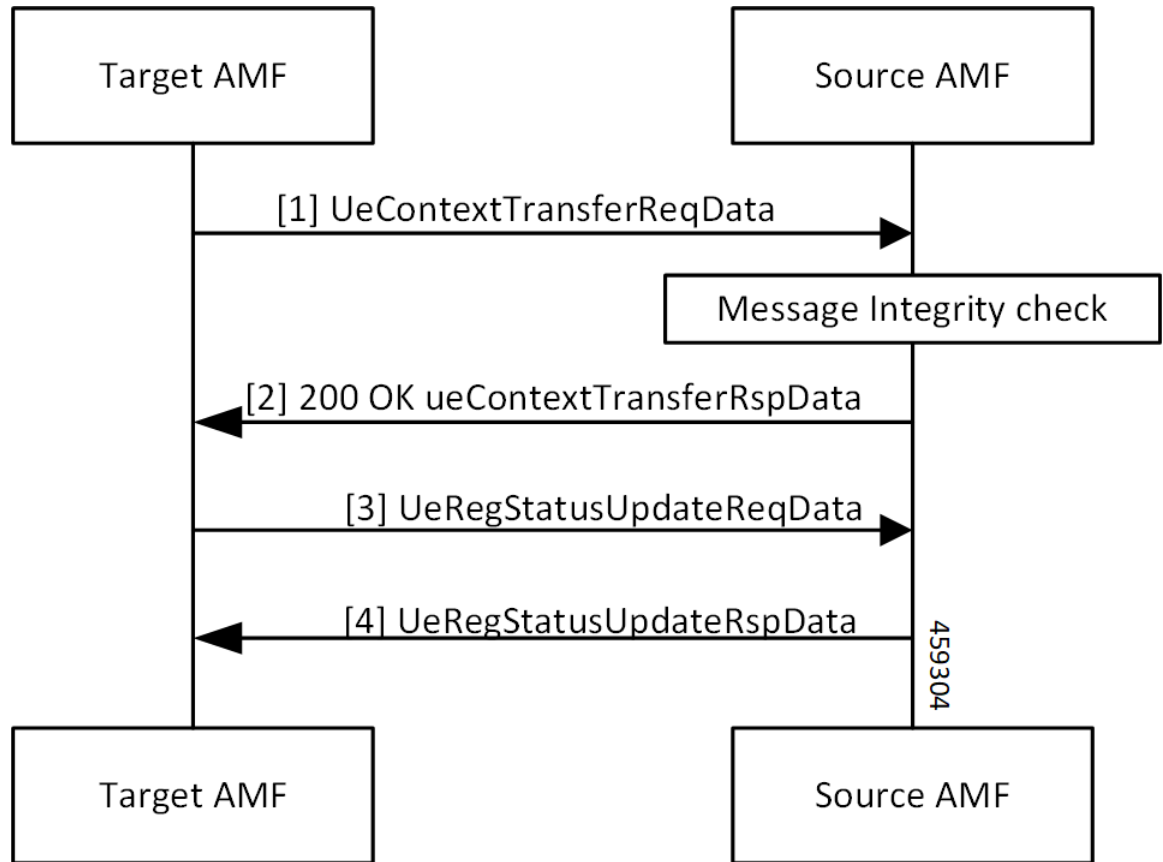


Table 3: UE Context Transfer Call Flow Description

Step	Description
1	The target AMF sends the UeContextTransferReqData to the source AMF.
2	The source AMF performs message integrity check. It responds with 200 OK UeContextTransferRspData to the target AMF.
3, 4	The target AMF sends UeRegStatusUpdateReqData to the source AMF and receives a response.

Limitations

This feature has the following limitations in this release:

- Non-3GPP access, trace requirements and event subscriptions are not supported.
- In this release, source and target AMF (T-AMF) are expected to have same S-NSSAI configured. As a result, any PDU sessions that belong to S-NSSAIs not supported on T-AMF are not validated and are not dropped.

- Target AMF selects new PCF and sends `PcfReselectedInd` as true even if CLI is configured to use PCF provided by source AMF.

Feature Configuration

To configure this feature, use the following configuration:

```

config
  amf-global
    call-control-policy policy_name
    policy ue-ctx-transfer
      allow-interplmn-supi-transfer { true | false }
      horizontal-key-derivation { true | false }
      use-source-key { true | false }
      use-source-pcf { true | false }
    exit
  timers
    context-transfer-guard value guard_time_value
  end

```

NOTES:

- **allow-interplmn-supi-transfer { true | false }**—Specify true or false. If configured true, the source AMF sends UE context with SUPI. The default value is **false**.
- **horizontal-key-derivation { true | false }**—If configured true, the source AMF generates a new key every time. The default value is **false**.
- **use-source-key { true | false }**—If configured true, the target AMF uses a key received from the source AMF. The default value is **true**.
- **use-source-pcf { true | false }**—If configured false, the target AMF sends **pcfReselectedInd** as true in TransferUpdate and the source AMF clears the PCF association. The default value is **true**.
- **context-transfer-guard *guard_time_value***—Specify the context transfer guard timer value in seconds. The AMF starts this timer on receiving the TransferUpdate. On expiry, AMF clears the PDUs locally. **context-transfer-guard** value must be an integer in the range of 0—35712000. The default value is zero (0).

Configuration Example

The following is an example configuration.

```

config
  amf-global
    call-control-policy CCP1
    policy ue-ctx-transfer
      allow-interplmn-supi-transfer true
      horizontal-key-derivation true
      use-source-key true
      use-source-pcf true
    exit
  timers

```

```
context-transfer-guard value 50
end
```