5G Cloud SDM
Technical Scope of Work

Updates		
Version	Date	Comments
1	13/12/2019	RFP submission version

TABLE OF CONTENTS

1. Introduction

Customer is launching the present Request For Proposal (RFP) process to select suppliers and products for 5G Cloud Subscriber Data Management (also called Cloud SDM or vSDM). In the rest of the document common SDM naming might be used to cover both legacy bare metal SDM (current in prior to the migration) and Cloud SDM (target after migration). In this RFP, the target SDM refers to the products that support a distributed data repository and multiple network applications, such as HLR, EPC-HSS, IMS-HSS, MNP, EIR, HSM inherited from the legacy solution as well as new 5G network functions on both data repository and network applications layers.

Customer intends to implement new 5G Cloud Subscriber Data Management (SDM) solution. The selected SDM platform will take over and will ensure smooth migration of the commercial services provided today through existing SDM (HLR/AUC, EPC-HSS, IMS-HSS, EIR) and will support new 5G components defined by 3GPP standards (UDM, AUSF, UDR, UDSF, 5G EIR).

The target SDM solution will be hosted on Cloud infrastructure (IaaS) following ETSI NFV standards. In this RFP, two scenarios will be considered for the IaaS environment:

- Scenario #O where IaaS is provided by Customer
- Scenario #V where IaaS is provided by Cloud SDM supplier (a.k.a. VNF Vendor)

Note that additional new 5G components are required to support 5G in standalone architecture out of the SDM scope. They are covered in dedicated RFP for 5GC (5G Core) and Signalling (SCP) scopes. In these RFPs, the same IaaS scenarios are required.

This document describes the technical requirements of Customer for an SDM solution with the required legacy functions: Home Location Register equipment (HLR) including the Authentication Centre (AuC) and High Security Module (HSM), IMS/LTE Home Subscriber Server (HSS), Equipment Identity Register (EIR). It also covers the requirements for the new 5G functions: Unified Data Management (UDM), Authentication Server Function (AUSF), User Data Repository (UDR), Unstructured Data Storage Function (UDSF) and 5G Equipment Identity Register (EIR) evolution. Finally the document specifies the requirements regarding additional elements: Element Manager (EM), VNF Manager (VNFM), Provisioning interfaces, Data extraction…, required to operate the SDM.

THE SUPPLIER is invited to describe very precisely the paths and the steps to reach the target SDM solution, with the required capacity, including the subscriber growth projections for network dimensioning and network functionality.

THE SUPPLIER is also invited to provide a commercial offer associated to this evolution and different phases of evolution on Customer ’s network from 2021 to 2025. This quotation shall be consistent with the commercial requirements addressed as part of this RFP.

The quotation is expected for commercial customers database (with forecasts given in Chapter 2.3), but shall also include a Test bed.

The information provided by THE SUPPLIER shall include notably the following pricing information:

- Equipment supply - the unit price of all the quoted hardware equipment on the basis of the Network predictions (for Scenario #V and HSM if applicable)
- Software licensing - the SW releases prices (baseline SW + SW features)
- Hardware and software release upgrade
- I&C services

- Maintenance and Repair services
- Project Management Services
- Trainings
- Migration
- Test bed

The information contained in this document is confidential. THE SUPPLIER must not disclose any information without prior written authorization from Customer Group or Customer .

Statement of compliance and Questions:

THE SUPPLIER shall state item by item compliancy to the requirements described in the documents and indicated by a mark "**Rxx**". Supplier's answer to each item should start with the level of compliance:

COMPLIANT / PARTIALLY COMPLIANT / NOT COMPLIANT.

If *COMPIANT* is used, THE SUPPLIER shall indicate whether the proposed solution is available off-the-shelf (as part of THE SUPPLIER's existing corporate product portfolio) or will be provided as part of the initial delivery to Customer , after Customer specific customization.

In case *PARTIALLY COMPLIANT* applies, THE SUPPLIER shall indicate in which extend the delivery deviates from the requirement and whether full compliancy will be achieved as part of a future roadmap delivery.

Please mind that we will assume that all requirements answered as *COMPLIANT and PARTIALLY COMPLIANT* are quoted and included in the TCO.

The Supplier will detail all answers including COMPLIANT ones. All COMPLIANT answers but not detailed will not be considered.

In the document several questions are also raised. They are indicated by a mark "**Qxx**" (xx=number of the question). **THE SUPPLIER will answer all of these questions** in return, using this document (table answer provided below each question). **All questions will be answered in the same document with as much detail as possible.** Any reference to external generic documents will not be taken into consideration.

2. Network and dimensioning inputs

2.1. Network Overview

The following table give an overview of the installed equipment in Customer network:

Node	Provider	Type	Software version	Planned upgrades
Legacy SDM	ZTE	ATCA	4.18.10	

MSC R4	MSC-S	Ericsson	BC2.1	18A	
	MGW	Ericsson	GMPv4	17	
STP		Oracle	Eagle 5	R46.5	
DRF		Oracle	HP	DSR8.1	
SMSC		Huawei	Huawei	V300R002C90LG0108	
MMSC		Huawei	Huawei	V100R002C91LG0002SPC007	
Voice Mail		Huawei	Huawei	V001R002C80	
USSD GW		Huawei	Huawei	SCPmam-6.0.0.131	
SGSN/MME		Ericsson	MK8, MK10	1.31	
S/PGW+GGSN		Ericsson	SSR8020	1.10	
ePDG		Ericsson	SSR8020	1.3	
AAA		Nokia	8950/HP	18.5	
SCP IN		Nokia		PPS4.4	
IMS I/S-CSCF		Nokia	CFX	18.5	
IMS AS		Nokia	OpenTAS	18.5	
Provisioning		In house			
PCRF		Ericsson	Virtual for VoLTE/TSP 6.1 for data	1.1.1/15B	

Rem: New 5G network functions out of SDM scope are not given in the previous table. They are also part of a sourcing process (RFP).

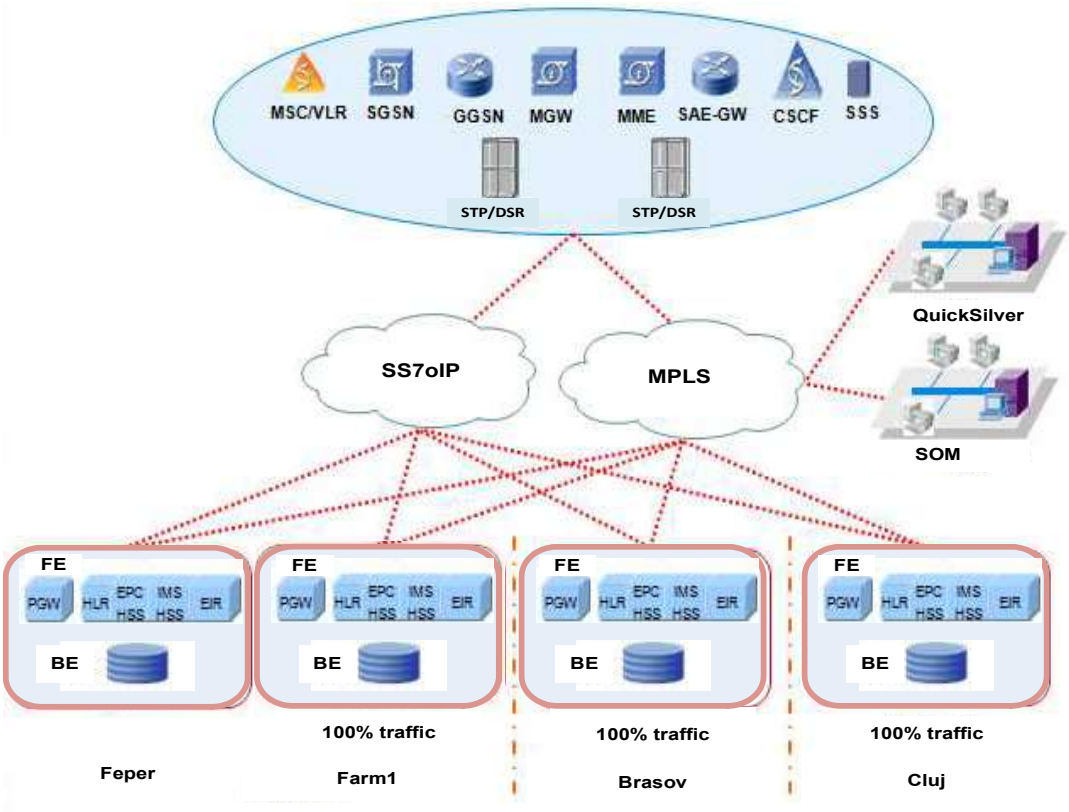
Q1 THE SUPPLIER will indicate and give evidence of IOTs with these Suppliers/releases. The Supplier will indicate and give evidence of IOT tests performed, indicating the type and release.

Answer

R1 If any above IOT tests or with any future equipment provider not listed above have not been performed THE SUPPLIER has to commit on performing IOT tests with the Customer suppliers before introducing a new SDM product/release in Customer network.

Compliancy

The Customer network elements connected to the SDM solution are presented in the schema below:



The Customer IaaS architecture and physical/logical components on which SDM VNFs will be implemented are presented in the description below (scenario #O):

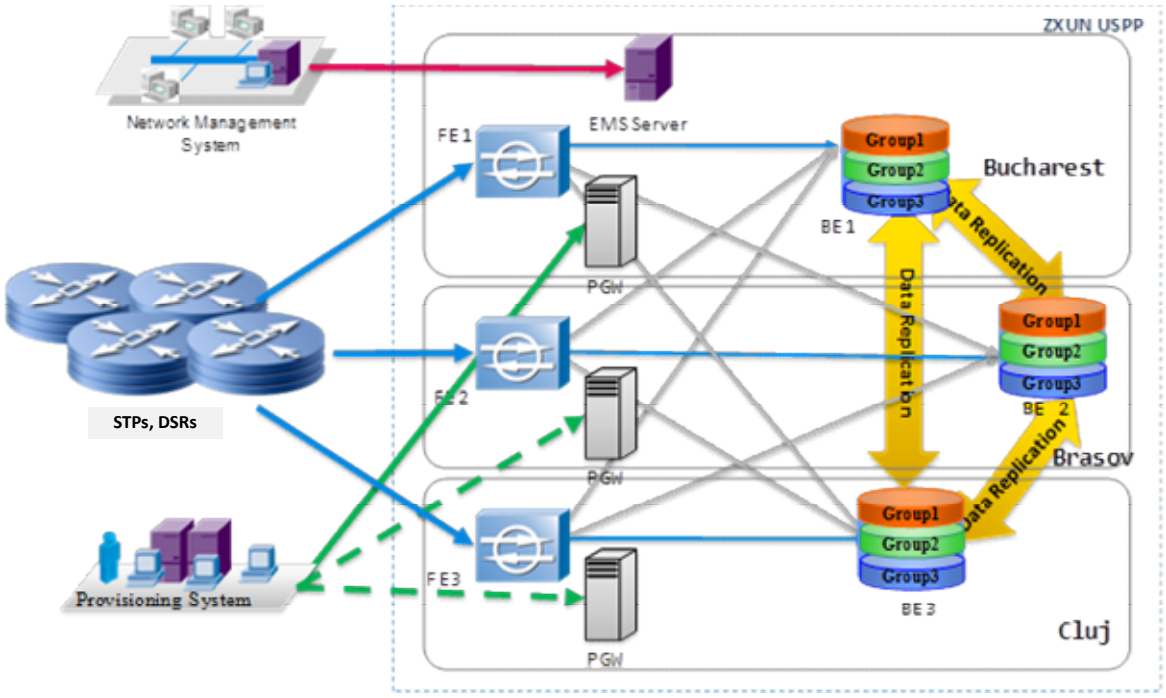
Bucharest and Cluj National Datacentres are now available and Brasov NGPoP it is the next to be deployed.
Transition from G3 HW to G4 HW will be made in the near future.

2.2. SDM solution overview

The Customer current Subscriber Data Management (SDM) for legacy functions is provided by ZTE and is based on the separation of the application logic and network integration from subscriber data. Current version is V4.18.10P2b.

The SDM architecture hosts application and subscriber data for a number of functionalities: HLR/AUC, EPC-HSS, IMS-HSS, EIR.

The SDM architecture consists in geographically spread Front-End and Back-End servers and provides the listed functionalities for Customer customer base.



* Group1/2/3 means HLR and EPC-HSS/IMS-HSS/EIR replicated over the 3 sites

FE and BE servers on the same site are connected through dedicated routers. Inter-site connectivity is going on the Customer IP-MPLS network routers.

The new target SDM will have to cover these current legacy functions as well as new 5G network functions: UDM, AUSF, UDR, UDSF, 5G-EIR

It has to be noted that Customer is currently experiencing 5G Customer City involving current SDM or dedicated SDM.

5G Customer Cities project covers for the moment four main Cities, with a limited number of sites, in NSA implementation, experiencing multi-vendor RAN strategy:

- Bucharest with Huawei
- Cluj with Samsung
- Iasi with Huawei
- Timisoare with Nokia

Customer City architecture is covered by NSA implementation, based on existing 4G SDM & EPC legacy infrastructure, already upgraded to support 5G NR. Customer 's commercial 5G subscriber's provision:

- Commercial APNs: net
- No SIM change for 5G subscription activation

2.3. Volume forecast and dimensioning inputs

Following sections provide forecasts of 2G/3G, EPC-HSS, IMS-HSS, EIR and new 5G Subscribers base evolution over 5 years and associated Traffic models. These figures will allow to define the capacity evolution requirements over the next five years.

In its answers, THE SUPPLIER will also take into account the following dimensioning assumptions:

- Dimensioning is performed taking into account a 6 months margin on subscribers and traffic forecasts.
- The SDM system shall accommodate with the partial or complete loss of one out 2 sites (in case of 1+1 configuration) or two out of 3 sites (in case of 1+1+1 configuration) without any service disruption by providing local and geographical redundancy. The remaining node(s) shall be able to accommodate the 100% peak traffic figures without any congestion or transaction loss.
- When one site is down the remaining "system load" shall be lower than 60%
- The remaining site shall support 100% of entire network traffic without service affecting
- The maximum system load and signalling link usage reached in case of the most critical fault cannot exceed the minimum value between first load threshold regulation value and 80%.

Q2 THE SUPPLIER shall clarify which KPI is used to determinate "system load" which resource consumption is measured (vCPU, mem, …).

Answer

Customer expects the system to support the rapid restart of one complete MSC and all the Location update procedures initiated by dependant MS (3 million MS per MSC).

Q3 THE SUPPLIER shall describe the behaviour of its SDM in such condition: regulation? What are the regulation mechanisms? Is it prioritisation of Location update procedures vs. others process to reach rapidly normal working condition?

Answer

Q4 In the situation of complete MSC/SGSN/MME/CSCF/AAA restart and to avoid regulation, additional processing capabilities may be necessary. THE SUPPLIER will indicate the additional capacity that will be required. We can consider in this case that all SDM sites are working and complete capacity can be used to support MSC/SGSN/MME/CSCF/AAA restart.

Answer

2.3.1. Subscribers base evolution

Forecast of estimated Provisioned and active subscribers evolutions but also Ported numbers (MNP on SDM) evolution over the next five years are given in the following table:

Subscribers base (kUsers)	End 2021	End 2022	End 2023	End 2024	End 2025
Provisioned subscribers in Database (UDR)					
Provisioned subscribers:					

- HLR profile	19M	19M	19M	19M	19M
- EPC-HSS profile					
- MBB + IoT/MTC	10M	10M	10M	10M	10M
- IMS-HSS profile					
- VoLTE	5M	6M	7M	8M	8.5M
- IMS fixed	300K	300K	300K	300K	300K
- VoWifi	10M	10M	10M	10M	10M
- 5G profile (B2B)					
- eMBB	8.1 K	16.1 K	28.2 K	37.6 K	37.6 K
- uRLLC	2.7 K	5.3 K	11.3 K	22.6 K	28.2 K
- mIoT	6.1 K	16.1 K	33.9 K	52.7 K	56.4 K
- FWA	4.1 K	8.0 K	14.1 K	18.8 K	18.8 K
5G profile(B2C - eMBB)	140k	270k	425k	640k	950k
Active subscribers: - HLR active sub.	10.5M	10.5M	11M	11M	11M
- EPC-HSS active sub.					
- MBB+IoT/MTC	5.5M	6M	6.5M	7M	7M
- IMS-HSS active sub.					
- VoLTE	3.3M	4.3M	5.3M	6.3M	7M
- IMS fixed	300K	300K	300K	300K	300K
- VoWifi	87k	120k	170k	220k	250k
- 5G active sub. (B2B)					
- eMBB	1.32 K	17.28 K	43.71 K	64.48 K	73.45 K
- uRLLC	0.2 K	2.8 K	7.1 K	10.4 K	11.9 K
- mIoT	0.1 K	0.9 K	2.8 K	6.3 K	8.9 K
- FWA	0.2 K	2.8 K	8.5 K	14.6 K	17.8 K
5G profile(B2C - eMBB)	20k	100k	200k	310k	600k

Definition:

- An active subscriber is a subscriber provisioned in the data repository who is generating monthly network messages (See also Licensing metric document).
- Provided EPC-HSS volumes cover 4G (LTE). It also includes 5G NSA if applicable.
- Provided IMS-HSS volumes cover VoLTE, VoWifi and fixed IMS.
- Provided 5G volumes cover eMBB, uRLLC, mIoT and FWA on SA architecture.
- Remarque: by default all 4G subscriber are allow to do VoWIFI

Q5 THE SUPPLIER shall provide a tool for querying active subscribers, total number of active subscribers and per application (HLR, EPC HSS, IMS HSS, UDM). The query result file should be in a standard readable format (ASCII, txt, csv, etc). The query filters shall be used in case of different results wanted:

- Total number only
- Total number and different parameters on operator discretion (IMSI, MSISDN, PVI, PUI, type of access (2G/3G/4G/5G), etc.) for each active subscriber.

Answer

2.3.2. Traffic models

2.3.2.1. HLR Traffic model evolution

The HLR Traffic model is calculated in terms of units of MAP traffic per Active Subscriber in the weekly busy hour.

Customer is considering the following MAP requests for defining the HLR traffic profile, all other type of traffic is considered as negligible:

HLR Traffic profile - MAP	End 2021	End 2022	End 2023	End 2024	End 2025
SRI	0.75	0.75	0.8	0.8	0.8
SRI for SM	0.65	0.65	0.70	0.70	0.70
UL CS	0.2	0.2	0.2	0.2	0.2
UL SGSN	0.65	0.65	0.70	0.70	0.70
SAI	2.1	2.1	2.3	2.3	2.3
USSD	0.004	0.004	0.004	0.004	0.004

2.3.2.2. EPC-HSS Traffic model evolution

The EPC-HSS Traffic model is calculated in terms of units of Diameter traffic per LTE active subscriber in the weekly busy hour. Only LTE Active Subscribers generate the EPC-HSS traffic.

Customer is considering the following Diameter requests for defining the EPC-HSS traffic profile:

EPC-HSS Traffic Model - Diameter	End 2021	End 2022	End 2023	End 2024	End 2025
S6a - AIR	2.80	2.80	2.95	2.95	2.95
S6a - ULR	1.6	1.6	1.7	1.7	1.7
S6a - NOR	0.3	0.3	0.3	0.3	0.3
S6a - PUR	0.1	0.1	0.1	0.1	0.1
S6a - CLR	0.1	0.1	0.1	0.1	0.1

This Diameter Traffic has to be added to the MAP Traffic at Busy Hour for EPC-HSS subscribers.

2.3.2.3. IMS-HSS Traffic model evolution

The IMS-HSS Traffic model is calculated in terms of units of Diameter traffic per IMS-HSS and concerns VoLTE, VoWifi and fixed IMS. Active Subscriber in the weekly busy hour. Only IMS Active Subscribers generate the IMS-HSS traffic:

HSS-IMS Traffic Model - Diameter	End 2021	End 2022	End 2023	End 2024	End 2025
Cx - UAR	3.2	3.2	3.5	3.5	3.5
Cx - MAR	1	1	1.2	1.2	1.2

Cx - SAR	1.4	1.4	1.5	1.5	1.5
Cx - LIR	1.9	1.9	2	2	2
Sh - SNR	0.7	0.7	0.8	0.8	0.8
Sh - UDR	4.3	4.3	4.6	4.6	4.6
Sh - PUR	0.4	0.4	0.5	0.5	0.5
SWx - MAR	9	9	9	9	9
SWx - SAR	12	12	12	12	12
ratio of register with SIP digest authentication	5%	5%	4%	4%	4%
ratio of register with AKA authentication	95%	95%	96%	96%	96%

For information Sh transparent data size for each IMS subscriber is 18kb.

This Diameter Traffic has to be added to the MAP and EPC-HSS Traffic at Busy Hour for these IMS-HSS subscribers.

All other type of traffic is considered negligible.

2.3.2.4. 5G Traffic model evolution

The UDM, AUSF traffic model is calculated in terms of units of HTTP NF services operations traffic per 5G active Subscriber in the weekly busy hour. Only 5G Active Subscribers generate the UDM/AUSF traffic:

5G Traffic Model - HTTP	End 2021	End 2022	End 2023	End 2024	End 2025
Nausf_UEAuthentication Service					
Nausf_SoRProtection Service					
Nausf_UPUProtection Service					
Nudm_SubscriberDataManagement Service - Get - Subscribe - Unsubscribe - Notification					
Nudm_UEContext Management Service - Registration - Deregist.Notif. - Deregistration - Get - Update - P-CSCF-Rest.N.					
Nudm_UEAuthentication Service - Get - ResultConfirm.					

Nudm_EventExposure Service - Subscribe - Unsubscribe - Notify					
Nudm_ParameterProvision Service - Update					

The Nudr traffic for UDM storage can be deduced from Nudm traffic.

All other type of traffic is considered negligible.

For the 5G NFs dimensioning, THE SUPPLIER should extrapolate the 5G traffic model from the EPC-HSS traffic model considering the 5G active users forecasts. THE SUPPLIER will provide the resulting 5G traffic model used therefore.

2.3.2.5. EIR Traffic model evolution

The EIR and 5G-EIR Traffic model is calculated in terms of units of MAP and HTTP traffic per Active Subscriber in the weekly busy hour.

Customer is considering the following operations for defining the EIR traffic profile:

EIR Traffic model – MAP/HTTP	End 2021	End 2022	End 2023	End 2024	End 2025
MAP_CHECK_IMEI	0.8	0.8	0.8	0.8	0.8
N5g-eir_EquipmentIdentityCheck	0.8	0.8	0.8	0.8	0.8

2.3.3. Subscriber Profile

Subscriber profile to be taken into account is given in the table below:

CS profile (per subscriber)	
Subscriber Data	**Profile**
IMSI	1
MSISDN / IMSI	1,1
%CS	100%
GBS 20	0%
BS26	100%
GBS 30	85%
FAX62	10%
SMS-MO	100%
SMS-MT	100%
Camel	100%
Ocsi service profile	100%
Tcsi service profile	100%
Mcsi service profile	0%
Tifcsi service profile	0%
Dcsi service profile	0%

Smtcsi service profile	0%
Vtcsi service profile	0%
Mgcsi service profile	0%
Sscsi Service profile	0%
Ucsi Camel service	50%
Ugcsi Camel service	100%
Gprscsi service profile	0%
Smocsi service profile	0%
Supplementary services	100%
Nb of Call Forwarding type	5
Nb of Call Forward number / type	1
% of provisioned Call Forwarding	100%
% of activated Call Forwarding	100%
Nb of Call barring type	5
% of provisioned Call Barring	100%
% of activated Call Barring	50%
Nb of ODB type	10
% of activated ODB	5%
General call services	100%
OSSScode activated	1
CLIP / CLIR	100%
COLP / COLR	0%
Call waiting	100%
Call hold	100%
Multi-Party	30%

PS profile (per subscriber)	
Subscriber Data	**Profile**
APN + related QoS	5
Barring of GPRS services	5%

EPC profile (per LTE, non 3GPP, 5G NSA subscriber)	
Subscriber Data	**Profile**
APN + related QoS	5

IMS profile (per IMS subscriber)	
Subscriber Data	**Profile**
IMSI	1
IMPI	1
Authentication method	1
IMPU	3
Nb of barred IMPU	1 (temporary IMPU derived from IMSI)
Nb of non-barred IMPU	2 (Tel-URI + SIP-URI)
IRS number (per sub)	1
Number of IMPU in IRS	3
Service Profile number (per sub)	1
Nb of iFC per service profile	4
Default S-CSCF	6 names
Offline Charging Address	2 CCF names

For multiSIM profile: Maximum Number of IMPU in IRS is 7.

5G profile (per subscriber)	
Subscriber Data	**Profile**
SUPI	1
GPSI	1
S-NSSAI	4
DNN + related QoS	5

2.4. Capacity

In the following section THE SUPPLIER shall answer to each question for all the below application configuration scenarios:

1. HLR
2. HLR + EPC-HSS
3. HLR+EPC-HSS+IMS-HSS
4. HLR+EPC-HSS+IMS-HSS+EIR

The answers shall consider the traffic and profile data provided in chapter 2.3.

Q6 THE SUPPLIER shall specify the dynamic capacity of one Front End VNF component

Answer

Q7 THE SUPPLIER shall specify the maximum static capacity (number of subscribers) of one Back End VNF component

Answer

Q8 THE SUPPLIER shall specify the parameters (if any) which can impact the static dimensioning (e.g. % of GPRS subscribers, % of UMTS subscribers, number of PDP models) and to provide the associated static capacity for various values of theses parameters.

Answer

Q9 THE SUPPLIER shall provide the list and the value of the dimensioning parameters of the equipment :

- Network parameters (e.g. maximum number of SCP addresses) (SCP standing for Service Control Point).
- Data per subscriber (e.g. Camel data, GPRS data, LTE data….).

Answer

2.4.1. Provisioning capacity

The KPI's (Key Performance Indicator) that describe the QoS on the provisioning plane are:

- Provisioned Subscriber volume per hour
- Subscriber Retrieve Processing delay (ms): read a subscriber in the DB
- Subscriber Create Processing delay (ms)
- Subscriber Update Processing delay (ms)
- Subscriber Delete Processing delay (ms)

THE SUPPLIER shall fill in the below table considering 2 scenarios:

- 0% signaling traffic
- 70% signaling traffic

For each scenario THE SUPPLIER shall duplicate the table and fill in for:

- Unitary command run (one command – one response)
- Bulk provisioning

Q10 THE SUPPLIER shall indicate the QoS Performance Indicators (described above) for managing specific transactions.

Answer

	Provisionned Subscriber volume per hour *min/max/average*	Subscriber Retrieve Processing delay (ms) *min/max/average*	Subscriber Create Processing delay (ms) *min/max/average*	Subscriber Update Processing delay (ms) *min/max/average*	Subscriber Delete Processing delay (ms) *min/max/average*
HLR Only					
- HLR Profile customer					
HLR + EPC-HSS					
- HLR Profile only customer					
- HLR Profile + EPC customer					
HLR + EPC-HSS + 5G SA					
- HLR Profile only customer					
- HLR Profile + EPC customer					
- HLR Profile + EPC + 5G SA customer					
HLR + EPC-HSS + IMS-HSS					
- HLR Profile only customer					
- HLR+EPC customer					
- IMS customer					
- HLR Profile + EPC + IMS customer					
HLR + EPC-HSS + IMS-HSS + 5G SA					
- HLR Profile only customer					
- HLR+EPC customer					
- IMS customer					
- HLR Profile + EPC + IMS customer					
- HLR Profile + EPC + 5G SA + IMS customer					
HLR + EPC-HSS + IMS-HSS + EIR					
- HLR Profile only customer					
- HLR+EPC customer					

- IMS customer					
-EIR database					
- HLR Profile + EPC + IMS customer					

Q11 In the case of 60 different simultaneously sessions (parallelism) performing basic operations on the SDM solution (e.g. create/update/read a different SDM subscriber), THE SUPLIER shall indicate:

- Qualify and quantify the impacts on its performances.
- Do these impacts depend on the FE configurations (one Application dedicated or Multi-Application)?

Answer

2.4.2. NMS capacity

The KPI's (Key Performance Indicator) that describe the QoS on the NMS plane are:

- Alarm volume per second:
- Failure Detection Latency: delay for the Network Management System to detect a failure (retrieved from Agent) and send to IS (to the Operator)
- Distant Operation query latency: delay for the Network Management System to process and answer the query done by the IS (Operator)
- Number of Simultaneous Sessions on NMS: Number of Simultaneous sessions active on the Network Management System opened by the IS (operators)

THE SUPPLIER shall fill in the below table considering 2 scenarios:

- 0% signaling traffic
- 70% signaling traffic

Q12 THE SUPPLIER shall indicate the QoS Performance Indicators (described above) for managing specific transactions.

Answer

	Alarm volume per second *min/max/average*	**Failure Detection Latency** *min/max/average*	**Distant Operation query latency** *min/max/average*	**Number of Agents per NMS** *min/max/average*	**Number of Simulataneous Sessions on NMS** *min/max/average*
HLR Only					
- HLR Profile customer					
HLR + EPC-HSS					
- HLR Profile only customer					
- HLR Profile + EPC customer					
HLR + EPC-HSS + 5G SA					
- HLR Profile only customer					
- HLR Profile + EPC customer					
- HLR Profile + EPC + 5G SA customer					
HLR + EPC-HSS + IMS-HSS					
- HLR Profile only customer					
- HLR+EPC customer					
- IMS customer					
- HLR Profile + EPC + IMS customer					
HLR + EPC-HSS + IMS-HSS + 5G SA					
- HLR Profile only customer					
- HLR+EPC customer					
- IMS customer					
- HLR Profile + EPC + IMS customer					

- HLR Profile + EPC + 5G SA + IMS customer					

HLR + EPC-HSS + IMS-HSS + EIR

- HLR Profile only customer					
- HLR+EPC customer					
- IMS customer					
-EIR database					
- HLR Profile + EPC + IMS customer					

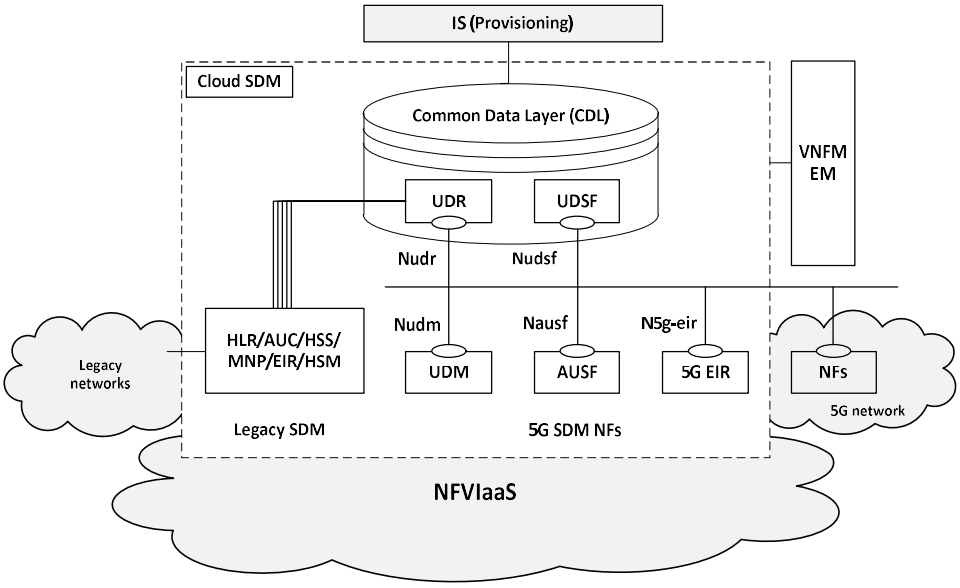
3. Technical requirements

3.1. Section overview

This section highlight the Technical specifications of the target 5G Cloud SDM solution that Customer plans to deploy in its network. It also defines some basic terminology that will be used throughout this document.

3.2. Main concepts

Customer 5G Cloud SDM main concepts:



- Separation of the data repository layer in a Common data layer (CDL), for both structured (UDR) and non-structured (UDSF) data and different network functions (legacy functions: HLR/AUC, HSS, EIR, MNP and new 5G network functions: UDM, AUSF, 5G EIR).
- Both data repository and network functions composing Cloud SDM are implemented as VNF on top of a Cloud infrastructure (NFVI / IaaS) in the target architecture.
- Cloud SDM is operated with Network Management System (NMS) including both EM (Element Manager) and VNFM (VNF Manager) also supported on Cloud infrastructure as a target.
- Cloud SDM is integrated within both legacy 3GPP 2G/3G/4G/IMS and non 3GPP networks through the relevant IP-based standardized interfaces as well as new 5G network using service based REST APIs for the other 5G network functions.
- Both data repository and network functions are implemented considering local and geographical redundancy. In particular, the data in the data repository is shared by 1, 2 or n logical partitions. These partitions are located on several VNFs replicated in real-time (geographic redundancy).
- Strong resilience: 99,999% of network availability, efficient recovery mechanisms that guarantee service continuity even in case of site disaster or faulty software
- Unique point of Provisioning for the Information System based on SOAP interface

3.3. Cloud SDM Target architecture and ecosystem

THE SUPPLIER shall propose the number of sites for the solution based on the best compromise between cost and redundancy. The required resilience is at least 99.999%. THE SUPPLIER shall give strong arguments for proposed solution.

In target architecture, the system must be geographically redundant meaning that the remaining site(s) are able to support the full load without any traffic interruption and service degradation. The system should be also able to detect faulty sub system and isolate it in order to guarantee the service.

The proposed solution shall be fully functional and shall include:

- Subscriber Data Management (SDM) supporting **HLR, AUC, HSS, HSM and EIR** legacy functions and **UDM, AUSF, UDR, UDSF and 5G EIR** new 5G functions.
- OSS/NMS (EM, VNFM) components
- SDM tool for profile mass extraction and modification
- Provisioning items, if any, to connect SDM to Customer provisioning system
- Any other solution mandatory items not listed above.

In this respect THE SUPPLIER is required to indicate and quote all HW and SW items that are mandatory. The same request is for any other mandatory SDM solution HW and/or SW (OSS/NMS, tools, etc). The dimensioning data are given in chapter 2.3 “Volume forecast and Dimensioning inputs”.

The system will be connected to Customer IP Backbone.

The traffic remaining on one site (e.g. traffic involving one site VNFs) will not be transported by the backbone or the Customer LAN.

THE SUPPLIER will provide as part of his solution internal and redundant Layer two switching infrastructure to support those kind of traffic and allow traffic aggregation before reaching the backbone. If the solution doesn’t include it, THE SUPPLIER has to provide clear requirements in order to integrate its solution.

R2 THE SUPPLIER is asked to dimension SDM solution based on the dimensioning inputs given in previous sections (§2.3) and taking into account the redundancy.

Compliancy

R3 THE SUPPLIER shall clarify compliancy with the ability to provide a scalable solution adapted to the customer’s capacity needs and volume evolution over time. Dimensioning guidelines, covering VNF components, vCPUs, RAM memory, VM image size, ephemeral and persistent storage, vNICs interfaces, maximum static and dynamic capacity... shall be provided and shall consider proposed redundancy configurations.

Compliancy

R4 THE SUPPLIER will provide a high level design diagram of proposed solution. The design diagram shall include all mandatory items (HW and SW components).

Compliancy

R5 THE SUPPLIER shall clarify how the SDM solution should best be integrated on the IP network.

Compliancy

R6 THE SUPPLIER shall describe the needs for switching or routing functions. THE SUPPLIER shall indicate whether listed switching or routing functions shall be provided by THE SUPPLIER or shall be provided by Customer .

Compliancy

R7 THE SUPPLIER shall indicate its requirements in terms of type and amount of ports, needed to interface with the IP network.

Compliancy

R8 THE SUPPLIER shall clarify compliancy with the ability to provide accurate power consumption and footprint figures for proposed architecture alternatives and will provide such figures taking the deployment / migration plan into account

Compliancy

Q13 THE SUPPLIER shall provide description of the ways the different types of overloads are identified (thresholds) and clarify availability of the possible protection mechanisms to cope with such overload situations including containment and coordination with peers.

Answer

Q14 THE SUPPLIER shall demonstrate the availability of automatic and/or manual procedure applied on the SDM solution to recover from hardware or software issues. The way pieces of hard or software would be brought back in service and the way the system would act in such cases shall be clarified by THE SUPPLIER.

Answer

Q15 THE SUPPLIER will explain the system behaviour in case of completely link failure between 2 sites (inter-POP), each hosting data storage and network VNFs (these 2 sites are mirrored – each having the same subscriber data repository) and assuming that SIGTRAN/DIAMETER/HTTP connections for Network functions are up and running. In this case the replication of data repository is not possible during the link failure. THE SUPPLIER will explain associated resilience mechanism and possible impact on services.

Answer

Q16 THE SUPPLIER will specify if the replication is local/geographical and real-time or asynchronous.

Answer

Q17 THE SUPPLIER will detail the data repository replication mechanism.

Answer

Q18 THE SUPPLIER will explain the redundancy mechanism that will be provided and how this mechanism will work. The Supplier will list all the possible defaults and explain associated resilience mechanism and possible impact on services.

a. one complete site failure (FE, BE VNFs)

b. two complete sites failure (FE, BE VNFs) applicable for 1+1+1 configuration

c. one site FE VNFs failure

d. two sites FEs VNFs failure applicable for 1+1+1 configuration

e. one site BE VNFs failure

f. two sites BEs VNFs failure applicable for 1+1+1 configuration

g. data repository replication link between one site and remaining sites down,

h. any other possible failure situation

Answer

Q19 THE SUPPLIER will describe the required traffic flows over the IP backbone for each type of traffic (signalling, replication, provisioning, management, etc.). The answer will consider all applications required: HLR, EPC-HSS, IMS-HSS and UDM/AUSF.

Answer

Q20 THE SUPPLIER will compute the necessary IP backbone bandwidth necessary to ensure the resilience (for instance, at the re-start/re-synch of one site). THE SUPPLIER will consider the worst case scenario only (requiring the maximum capacity) based on traffic volume considering dimensioning data provided in paragraph 2.3 “Volume forecast and Dimensioning inputs”. The bandwidth will be also separately computed for each flow (e.g. O&M flow, Replication flow, Signalling flow, Provisioning flow, etc). The answer will be split per application HLR, EPC-HSS, IMS-HSS and UDM/AUSF.

Answer

Q21 In case of traffic passing through a security solution (external of current platform), what type (protocol used, packet types and size), throughput and number of sessions we need to take into consideration? THE SUPPLIER will consider the worst case scenario only (requiring the maximum capacity) based on traffic volume considering dimensioning data provided in paragraph 2.3 Traffic mix and capacity evolution. THE SUPPLIER will answer for each flow (e.g. O&M flow, Replication flow, Signalling flow, Provisioning flow, etc). The answer will be split per application HLR, EPC-HSS, IMS-HSS and UDM/AUSF.

Answer

Q22 THE SUPPLIER will indicate the QoS requirements necessary to ensure the best performance of the system:

- round trip delays
- packet loss tolerance
- IP availability
- routers reconfiguration

- farthest distance between sites
- and all other specific IP backbone requirements

In case of one of the constraints is not enforced, THE SUPPLIER will describe potential impacts it might have on the global network behaviour.

Answer

3.4. Hardware and Application Roadmap

3.4.1. Hardware Roadmap

Initial hardware deliverables (for scenario #V and HSM if applicable) should be done using the latest available and released types and technologies for each node of the solution. Aim is to delay hardware replacements as much as possible.

Q23 THE SUPPLIER shall list for all kinds of proprietary and 3rd part hardware which technology and type / model is used as part of the initial installations.

Answer

To have a better view on the lifecycle and corresponding support of the used hardware, the long term hardware roadmap is required.

Q24 THE SUPPLIER shall provide for all kinds of proprietary and 3rd party hardware the long-term roadmap, indicating used technology, type / model, release reference, commercial availability and applicable end-date (last delivery, end-date for spare parts replacement, end of support).

Answer

3.4.2. Application Roadmap

Initial deliverables should be done using the latest available and released software version. Aim is to benefit from the most complete (complying with listed functional requirements), yet stable software version.

Q25 THE SUPPLIER shall list for all relevant software versions as part of the initial installations for both legacy functions, 5G functions and OSS components.

Answer

To have a better view on the lifecycle and corresponding support of the commercialized software, the long term software / application roadmap is required.

Q26 THE SUPPLIER shall provide the full long-term software roadmap, indicating release reference, included functionalities, commercial availability and applicable end-date (last delivery, end of support,..)

Answer

It is important for the network operator to have a view on minimum hardware requirements (IaaS technology, type, vendor, version) to support the commercial available software / application releases. When referring to minimum hardware requirements for a given software /

application release, we assume that all hardware versions above this minimum requirement, will also support this given software / application release.

Q27 THE SUPPLIER shall provide the full long-term view on the software and hardware compatibility, indicating the minimum hardware requirements for each commercial available software release and application. Also confirmation of above statement on hardware versions above the minimum requirements shall be provided

Answer

3.5. HLR, EPC-HSS, IMS-HSS, EIR functional requirements

R9 The general technical features required for the HLR, EPC-HSS and IMS-HSS are those mentioned in the SDM General Technical Requirements provided with this RFP. It includes mainly the specifications of the following standards:

- 3GPP specifications up to R16
- ITU and ETSI specifications.

THE SUPPLIER is asked to provide the detailed content of the release and to precise the version of the supported 3GPP standard (SoC to provide)

Compliancy

R10 THE SUPPLIER shall quote HLR, EPC-HSS, IMS-HSS and EIR functionality on the basis of the features listed hereafter. All services currently used in Customer network should be available and provided in new SDM solution, meaning that “feature parity” is required.

In case no equivalent feature can be found in the solution, a workaround solution shall be provided by THE SUPPLIER at no additional cost. Nevertheless the additional cost on other Customer systems (IT and/or Network) due to that workaround will be quoted by Customer and added to the final cost of the solution.

Compliancy

3.5.1. Standard features

R11 Here are the main current standard HLR and EPC-HSS features in use on legacy SDM that THE SUPPLIER must provide in the SDM solution:

- Call forwarding unconditional
- Call forwarding on busy subscriber
- Call forwarding on subscriber not reachable
- Call forwarding on no reply
- Call forwarding by default
- Call waiting
- Call Hold
- Multiparty
- Circuit switch data services
- Connected Line Identification Services
- Call Barring
- CAMEL phase 1 & 2 & 3 & 4

- O-CSI/T-CSI suppression in HPLMN OR/AND VPLMN
- CAMEL ATSI/ATMO
- MAP_NOTE_SUBSCRIBER_DATA_MODIFIED
- Unstructured SS Data, GSM Phase 2
- Closed User Group
- Explicit Call Transfer
- PLMN Specific Supplementary Services (OSSS flags)
- Multimedia priority services
- Subscription Based Network Access
- GSM Restoration: MAP RESET management
- Termination of Calls on MAP_cancel_location
- Subscriber Fraud Detection and Limitation
- HSPDA and Enhanced HSPDA support in HLR
- Ring Back Tones
- EMLPP
- Roaming
- PDP profile (QoS profile)
- ISDN Bearer Capability / GSM Bearer Capability translation depending on ITC
- Single/Multi-Numbering
- MultiSIM
- Location services based on ATI / PSI / ALR
- MAP version (application context)
- ODB (Operator Determined Barring)
- CLIR
- CLIP
- Fax
- Video telephony bearer
- SMS management
- Area Restriction Data (ARD)
- ADD (auto device detect) function
- LTE standard features including CSFB, Roaming Retry, RFSP and SMS over IP
- VoLTE and VoWifi features including SrVCC, T-ADS, Anchoring, Multi-SIM/IMPI, Supplementary data synchronization between CS & IMS, Auto-provisioning
- IMS standard features including AS transparent data over Sh, shared IMPU, PSI
- Diameter Overload Indication Conveyance (DOIC)
- IPV6 and IPV4-IPV6 interworking support
- Support of Zh interface
- Support of S6c interface
- Support of S6d interface
- Support of Cx interface
- Support of SWx interface

Compliancy

3.5.2. HLR behaviour while roaming

R12 Customer requires specific HLR behavior when CAMEL is not supported in VLR (subscriber is roaming) or requested CAMEL phase is higher in roaming VLR.

This includes possibility per subscriber to:

- Release call (default value)
- Continue call
- Barring of All Outgoing Calls
- Barring of all Outgoing International Calls
- Barring of all Outgoing International Calls Excepted those directed to the Home PLMN country
- Barring of All Outgoing Calls except SMS
- Restrict roaming
- Return OCSI mark
- Not return OCSI mark

Compliancy

R13 Roaming restriction lists mechanism is used to control roaming access of Customer subscribers (with or without CAMEL) in VPLMNs. The control is not only for location but also for availability of only certain services in profile. There should be distinct roaming lists for CS access, PS access.

Compliancy

R14 Customer requires that different services to be controlled based on user location (if it is located in HPLMN or VPLMN or to a particular VLR/SGSN). These services should be induced in CS or / and PS domain. The services are not limited to the list below:

- Speech
- SMS
- Fax
- Data csd
- Video call
- ODB
- Call forward
- Call barring
- CLIP
- CLIR
- CW
- CH
- MPTY
- USSD
- ARD
- STN-SR
- APN
- MultiSIM

Compliancy

R15 If the subscriber is not allowed to roam when located in the VLR/SGSN, HLR returns a failure reason: roaming not allowed in the location update response. However it should be possible to set other failure reasons codes if subscriber is not allowed to roam. The options should be:

- Unknown subscriber;
- System failure;
- Data loss;
- Unexpected subscriber.

Compliancy

R16 When a subscriber roams to a network with a roaming agreement and the SMSC address is set to the address of the SMSC different then SMSC of the home network, the MSC in the roaming network does not allow the subscriber to send short messages. When the subscriber initiates location update, even if the subscriber has not subscribed to the BOIEXH-SMS service, the HLR sends this supplementary service to the MSC in the roaming network, which restricts the subscriber from sending short messages. HLR should support this feature and the activation should be done at system level for all the subscribers

Compliancy

R17 Customer requires that for some Customer CAMEL subscribers the OCSI mark to be inhibited when roaming in visited PLMN. This option should be provisioned in subscriber profile.

Compliancy

R18 HLR should support sending OCSI mark based on user location (HPLMN or VPLMN or a specific VLR) regardless of the GT and / or SK is used. For example SK1 and GT1 for subscriber1 should be sent in VPLMN1 (when user is located in VPLMN1 (VLR1)). When user is located in VPLMN2 (VLR2) then SK1 and GT1 should not be sent. The operator should have the flexibility of configuring this triggering mechanism at VLR level not only at HPLMN and VPLMN level.

Compliancy

3.5.3. USSD Relay

R19 The aim of this feature is to be able to shunt from the call flow the HLR during an USSD session. Normally all USSD messages transit by the HLR, but it implies the use of a huge number of HLR internal resources because of long USSD sessions (more 120 seconds) required by several USSD services deployed in Customer . The aim of the feature is to avoid to use inefficiently the resources and to free them as soon as possible. The principle is to relay USSD at SCCP level, ie to use VLR address as Calling Party address and send the message to USSD Server, so that all the subsequent messages will be exchanged between USSD Server and VLR directly.

Compliancy

3.5.4. Short number translation for CF

R20 The HLR shall be able to translate short number when a CF configuration is updated/created.

When CF is for instance populated with 555 (short number for VM routing), the HLR shall translate the destination with the correct long number.

Compliancy

3.5.5. CF limitations

R21 Customer requires the possibility in HLR to limit CF to national numbers only for national subscriber and to a limited number of countries.

This feature has to be applicable for a particular set of users, other set of users could not have this limitation.

Vendor is requested to clearly describe the implementation of this feature. And describe the flexibility of their implementation in this regards.

Compliancy

3.5.6. Roaming restriction List

R22 Customer uses the roaming restriction lists on HLR/HSS associated to subscription, in 2/3G (E164 based) and in 4G (E212 based) and WLAN/VoWiFi (Visited-Network-Identifier).

THE SUPPLIER is requested to clearly describe the implementation of this feature. And describe the flexibility of their implementation in this regards.

Compliancy

3.5.7. Roaming Management

R23 Customer requires a very flexible management of the possible MAP versions for user in roaming. The supported maximum MAP versions per ACN have to be defined per Visited Operator (PLMN), and different maximum values have to be possible for Voice & Data. Eventual fall back on Voice MAP version negotiation shall not influence the Data MAP version negotiation and vice versa. Differentiation should be offered between incoming and outgoing dialogues.

THE SUPPLIER is requested to describes the flexibility of its implementation in this regards and provide example of scenario with different operators in the same country

Compliancy

3.5.8. UDM/HSS Interworking

R24 To insure smooth interworking between 4G and 5G domains the target solution should support interactions between UDM and HSS, in the areas of authentication keys sharing, mobility management (e.g. cancel registration…), IMS interworking (e.g. T-ADS query…), SMS-MT delivery in particular.

THE SUPPLIER is requested to describe precisely its implementation on HSS whether it is based on proprietary interface and/or standardized interface (3GPP R16 TS 23.732) as well as availability dates.

Compliancy

3.5.9. Specific features

3.5.9.1. HLR specific features

R25 HLR should have a mechanism of avoiding sending MAP PRN message while LU procedure is ongoing for a subscriber.

Compliancy

R26 In case a remote peer is not responding to cancel location the SDM should buffer all cancel location messages for at least 4 hours. During the 4 hours it should send to the peer the cancel location messages with an operator set frequency (for example one message to every 5 seconds). The buffer size should store at least 5M messages.

Compliancy

R27 The HLR should support dynamic data merge (location update and SS (supplementary service)) when recovering from dual primary state (one isolated site).

Compliancy

R28 Customer uses Operator Specific Supplementary Services (OSSS) feature:

1. Flag C for CRBT (Colour Ring Back Tone): is an intermittent audio tone that a caller in a classical telephone system hears after dialling a number, when the called party is receiving a ringing signal.

2. Flag 1 to E for different services.

OSSS flags must be provisioned independently for:
- MO calls, MT calls

OSS Flag is referring to PLMN specific SS (16 SS Codes) as described in 3GPP TS 29.002.

Compliancy

R29 The operator should be able to add to a subscriber profile an Operator specific supplementary services code, to grant him a PLMN specific service. In the subscriber's profile the operator should be able to decide whether the OSSS code must be sent or not to the HPLMN's VLR.

Compliancy

R30 In the HLR, distinction should be done between OSSS code invoked in TC case and OSSS code invoked in OC case and it should be possible to allocate simultaneously TC OSSS code and OC OSSS code.

Compliancy

R31 Customer requires that for CAMEL subscribers the TCSI mark to be inhibited when located in HPLMN. The inhibition should be independent of service keys (SK) used. For example, in case of two subscribers that have the same TCSI SK in the profile, one might have TCSI mark inhibited and the other one might have TCSI mark sent to GMSC.

Compliancy

R32 Customer requires that HLR to limit the maximum number of times that the called number can be forwarded during a call. The limit should be configured at system level for all subscribers.

Compliancy

R33 Customer requires the possibility to set at system level a default timer for CFNRy (call forward no reply). This timer should be set per bearer (e.g. speech, fax, data) and will be override by the timer value set in the subscriber profile (set by operator or by mobile terminal).

Compliancy

R34 Customer requires the possibility in HLR that the operator to provide in subscriber profile the call forward by default (CFD) service. The service will activate one , more or all call forward services from a subscriber profile when the subscriber deregister from mobile terminal the call forward number. When the subscriber register a forward to number this number will override the call forward by default number for the type of call forward.

The call forward by default number should be set per subscriber. The service should be set per subscriber.

The CFD should have its own CFNRy timer set per subscriber.

The system should allow operator to choose the overridden call forward services (ex. CFD will override both call forward on busy and call forward on no reply).

Example: one subscriber profile has provisioned call forward on busy, call forward on no reply and call forward on no reachable services but not activated. As long as the subscriber does not activate from mobile any forwarded to number all mentioned call forward services don't act.

The operator provisions call forward by default service in subscribe profile and the call forward by default number is voice mail number. Automatically call forward on no reply and call forward on no reachable services for that subscriber are activated to voice mail number and start to act. When subscriber register from mobile another number for call forward on no reply the new forwarded to number will override voice mail number but only for call forward on no reply. Call forward on no reachable service will remain active to voicemail number. When subscriber deregister the number (cancel call forward on no reply from mobile) the call forward on no reply service will remain active and the forwarded to number will be again the voice mail number.

All this time call forward on busy remains not activated.

Sending of CFD should be controlled in HPLMN and VPLMN or for specific VLR address.

Compliancy

R35 HLR should be able to check the link between CFD and CFB, CFNRy and CFNRc based on the following rules:

- When CFD is registered HLR should check if whether the corresponding common CFB, CFNRy and CFNRc are provisioned. If they are not then HLR should reject CFD number registration
- When CFD is registered HLR should check interaction with CB (call barring) and ODB
- If CFD number is registered and the operator needs to deprovision a corresponding common CFB, CFNRy and CFNRc then HLR must deny the operation.

Compliancy

R36 Support of HSPA+ standard extension: 3GPP 24.008. The HLR shall support in the subscriber profile parameters a maximum bandwidth of 256 Mbps downlink and uplink.

The SUPPLIER is requested to indicate also the maximum rate for HSDPA and HSUPA supported in the actual release and the price policy if not included in the basic feature list.

Compliancy

R37 Tracing using the mobile identity allows Customer to obtain call path information on a specific mobile station's call connection from different network elements in the network together with traffic data and other events related to the call.

Compliancy

R38 The HLR should offer the possibility to define PDP profiles characterized by an APN name and a set of QoS attributes (traffic class, transfer delay, Maximum UL/DL bit rate, Guaranteed UL/DL bit rate, delivery order, Residual BER…). PDP profiles are allocated to subscribers to describe the upper limit of the GPRS service they can reach. More than 5 PDPs can be assigned to one subscriber profile.

Compliancy

R39 PDP type should allow IPv4, IPV6 and PPP.

Compliancy

R40 The modification of a PDP profile characteristics should induce data updating for all the subscribers concerned in the HLR as well as in the visited network entities.

Compliancy

R41 HLR should be able to control sending of an APN or QoS (PDP model) based on user location (HPLMN and VPLMN or a specific SGSN address). One APN can be sent for some subscribers only in HPLMN and the same APN can be sent for other subscribers in VPLMN (or to a specific or more SGSN GT addresses).

Compliancy

R42 Customer requires that the APN "*" to be supported. APN "*" shall be assigned to a PDP model. That PDP shall be provisioned in subscriber profile. If APN "*" is assigned in a subscriber profile and that subscriber sets an APN not included in his profile (e.g. APN=X), the characteristics of APN "*" overrides the characteristics of APN=X.

Compliancy

R43 Customer requires that for some own subscribers roaming in some foreign PLMNs some supplementary services to be inhibited without any modification in subscriber profile. When Customer subscriber locates in HLPMN the supplementary services become active. The restriction should be applicable per subscriber, per supplementary service and per PLMN.

Compliancy

R44 The enhanced multi-level precedence and preemption (eMLPP) is a supplementary service that is used to ensure a normal conversation of the subscriber with higher priority by preemption, queuing, directed retry, and forced handover.

The eMLPP is a supplementary service offered by the GSM system. The eMLPP service allows a subscriber to initiate calls with different priorities. The network side employs different channel assignment strategies for the subscribers according to the priorities. If the network is congested, the call with higher priority is served preferably.

The eMLPP service requires the support from MS to ensure that the subscriber can initiate calls of different priorities under different situations. A normal conversation of the subscribers with higher priority is ensured by preemption, queuing, directed retry, and forced handover. With

this service, the high-priority subscribers have an advantage in call establishment rate and completion rate compared with the lower-priority subscribers according to different priority configurations in a network.

Compliancy

R45 Customer requires that the call barring activation/deactivation by subscriber to be allowed both by using or not a password. The option for asking a password for changing call barring status is set by Customer in each subscriber profile that has call barring service. A default password shall be provided when call barring service is assigned to a subscriber profile if not specified. The subscriber shall be able to change any time the password.

Compliancy

R46 There are some cases when a subscriber should be barred when roaming for using MO call, SMS MO, fax, data CSD. When user is in HPLMN all services must be unbarred. In order to comply with this requirement the subscriber is provisioned with a special supplementary service named BORO (barring of all outgoing call when roaming). When subscriber is located in VPLMN the HLR insert BAOC (barring of all outgoing call) to VLR.

Compliancy

R47 Customer requires that HLR shall support ARD in order to provide MSC/VLR and SGSN about the 2G and 3G subscriber's radio access restriction set by the operator (e.g. GERAN not allowed) in a flexible way.

Compliancy

Q28 In order to better understand some implementation of a part of requirements listed above the following contains examples of 4 types of subscribers:

- subscriber1 has OCSI SK (Service Key) 1, TCSI SK2. When located in HPLMN CAMEL mark (OSCI SK1) should not be sent to VLR (localized as "postpay"). TCSI should be inhibited (suppressed) for SK2. When located in VPLMN CAMEL info should be transmitted to visited VLR. TCSI SK2 should also be triggered in VPLMN. Subscriber1 should be allowed to roam (to perform location update) only to set1 of PLMN (set 1 contains 500 PLMNs). Subscriber1 should have access to all services (SMS MO/MT, speech, etc) when roaming in all 500 PLMNs.
- subscriber2 has OCSI SK1, TCSI SK3. When located in HPLMN CAMEL mark (OCSI SK1) should not be sent to VLR. TCSI mark should not be inhibited for SK3!. When roaming in VPLMN CAMEL info should be transmitted to visiting VLR (OCSI SK1). TCSI should be triggered for SK3! Subscriber2 should be allowed to perform location update on set1, as subscriber1
- subscriber3 has OCSI SK4, TCSI SK5. When located in HPLMN CAMEL info should be provided to VLR (prepay subscriber). TCSI mark for SK5 should be inhibited (not triggered). When roaming in VPLMN CAMEL info should also be transmitted to visiting VLR. TCSI SK5 should be triggered. Subscriber3 should be allowed to perform location update on set2 of PLMN (set 2 contains 300 PLMNs and can contain PLMNs from set1). From these 300 PLMNs on 100 subscriber3 has access only to SMS MO/MT and terminating voice calls. On remaining 200 PLMNs subscriber2 should have access to all services.
- subscriber4 has OCSI SK6, TCSI SK2. When located in HPLMN CAMEL info should be provided to VLR (prepay subscriber). TCSI mark for SK2 should be inhibited (not triggered). When roaming in VPLMN CAMEL info should also be

transmitted to visiting VLR. TCSI SK2 should be triggered. Subscriber4 should be allowed to perform location update on set1 - as subscriber1.

THE SUPPLIER is requested to detail the implementation of the services for all 4 subscribers providing also the commands used for provisioning/configuration, printout of subscriber profiles. The Supplier will list all features and specific developments needed for implementing this scenario.

Answer

R48 The system configuration should allow that multiple GTs and SKs be independently configured. Any GT – SK combination should be allowed in subscriber CAMEL profile. Please provide any limitation if exists.

Compliancy

R49 The system should allow provisioning basic services and bearer services with or without subscriber number. The option should be set per subscriber and per basic service or bearer service. THE SUPPLIER shall provide more details on this option, indicating complete list of basic services and bearer services that can be provisioned with and/or without subscriber number.

Compliancy

R50 In some cases a network element (like TAS, AAA) sends Restore message to HLR simulating a VLR to obtain the relative subscriber data. However it is possible that this network element not to send correct CAMEL capability and it will cause HLR to modify the CAMEL capability of the subscribers to the wrong value, and finally affects the normal call services of the subscribers. When the VLR address stored in HLR is not the same as the address carried in Restore message it should be possible for HLR to control returning the data:

- return data to VLR, and update the data in HLR
- return a system error if the VLR address is not consistent (e.g. VLR address is different than TAS address)
- return data to VLR only without updating the data if the VLR address is not consistent.

Compliancy

R51 The operator should be able to make different queries in HLR in order to obtain the number of subscribers located in HPLMN and / or VPLMN split by VLRs, SGSNs, MMEs..

Compliancy

R52 The HLR should support the Routing category (RC) and additional routing category. This RC should be controlled in HPLMN and VPLMN. This is mainly use to support for Nokia route in MSS/ TAS.

Compliancy

R53 The HLR should support synchronizing supplementary services between CS and IMS. Thus HLR must send MAP Note Subscriber Data Modified message to TAS when a supplementary service is modified in HLR. The supplementary services are not limited to the list below:

- Call barring

- Call forward
- Multy party
- CLIP
- CLIR
- CH

Compliancy

R54 There can be some situations when for a particular subscriber HLR does not have any more in its database the VLR address or it is marked as “purged”. TAS sends map restore data to HLR or HLR may receive a registerSS/eraseSS operation when there is no VLR address in its database or it is marked as “purged”. In this case the HLR must reply to restore data and allow SS operation.

Compliancy

R55 There can be some situations when a VoWiFi subscriber has been purged from VLR or there is no VLR address recorded in its database. When TAS sends map restore data the HLR should reply or not with OCSI mark according to analysis

Compliancy

R56 HLR can allow accepting or refusing MAP application contexts or operation codes according to the remote SCCP address. It can only accept the specified MAP application context or operation code for the specified address, and refuse the session of the MAP application context or operation code that is not allowed to be accepted.

Compliancy

R57 HLR should support configuring multiple MCC and MNC list.

Compliancy

R58 There are network elements (most of them located in roaming operators) that do not support XUDT messages. In this case the HLR should be able to encapsulate MAP information into MAP packets to avoid the XUDT encapsulation at the SCCP layer. So the operator should be able to configure in HLR based on the remote network element GT or DPC if to send XUDT messages or UDT messages.

Compliancy

R59 HLR should support configuring a dedicated PS cancel location. The options should be:

- subscriptionWithdraw, indicating that the message type is "subscription withdrawal".
- updateProcedure, indicating that the message type is "location update".
- initialAttachProcedure, indicating that the message type is "initial attach".

The operator should have the possibility to choose one of the above options when deleting the location information.

Compliancy

R60 HLR should support multi SIM / multi device feature. THE SUPPLIER shall provide a full description of this feature for HLR.

Compliancy

R61 Subscribing/unsubscribing to multi SIM/multi device should have no impact in customer experience. The following services should not be affected, should not require device restart/flight mode:

- MO call
- MT call
- data session

Cancel location with “update procedure” option should be sent in order to fulfill this requirement when subscribing/unsubscribing to multi SIM/multi device.

THE SUPPLIER is requested either to provide this feature in its implementation or to clearly explain how similar feature could be implemented.

Compliancy

R62 HLR should support Dual IMSI feature.

Compliancy

R63 The HLR should support sending reset HLR (MAP reset message) with at least the following options:

- to all VLRs/SGSNs
- to specific VLRs/SGSNs
- to all VLRs/SGSNs with IMSI
- to specific VLRs/SGSNs with IMSI
- to all VLR/SGSNs except a list

Compliancy

R64 There are some services that are provisioned in subscriber profile like: GT, SK, APN. Customer requires that it should not be possible to delete a specific APN, GT, SK from HLR/HSS configuration if it is already provisioned (if it is at least one SK,GT, APN) on subscriber profile. There should be a mechanism to restrict this operation..

Compliancy

R65 HLR should support RFSP parameter to be added in subscriber profile. This parameter refers to a frequency selection preference, indicating a policy selected when users access to UTRAN.

Compliancy

3.5.9.2. Specific HLR features related to Machine-to-Machine (M2M)

Machine subscriptions have specific requirements.
The services used by machines are usually limited to data ones. Circuit Switched services are usually not required for machines. On the other hand, they may require some advanced data services not required by humans.

The market has a huge potential of growth thus it might consume a huge number of MSISDN's and there is a risk of exhaustion. Machine wake-up is a compulsory marketing requirement and usually requires support of SMS-MT sent from a server. As per the standard, SMS-MT requires one MSISDN per machine. Non-standard features to avoid MSISDN exhaustion while still supporting machine wake-up might be required in the coming years.

Q29 Is it possible to provision subscription with SMS-MO/MT in the CS domain, PS services and without any other CS one?.

Answer

Q30 Is it possible to provision subscription with only Packet Switched service without MSISDN?

Answer

Q31 Does the HLR support variable-length MSISDN?

Answer

Q32 Normally the MSISDN is 11 digits long, it would be possible to provision MSISDN with 14 digits if variable-length MSISDN is supported?

Answer

Q33 Is it possible for a subscriber to have a subscription with an MSISDN shared by multiple other subscribers? Is there any service restriction in particular but not limited to SMS-MT services over CS Domain?

Answer

Q34 Does the HLR support alphanumeric extension of the MSISDN: CC+NDC+SN+machineId? Is there any restriction in the machineId format? For instance, all telemetry devices of a given company could share the same digital prefix 40 123456789 with an extension that would identify the machine in the company identification plan? Is there any service restriction in particular but not limited to SMS-MT services over CS Domain?

Answer

Q35 The supplier is invited to present any other M2M features that have direct or indirect link with the HLR, available now or in its product roadmap?

Answer

3.5.9.3. EPC-HSS specific features

R66 EPC-HSS should support wild card APN.

Compliancy

R67 EPC-HSS should be able to control sending of an APN or QoS based on user location (HPLMN and VPLMN or a specific MME realm/host address or PLMNId (IMSI)). One APN can be sent for some subscribers only in HPLMN and the same APN can be sent for other subscribers in VPLMN (or to a specific or more MME realm/host address or PLMNId (IMSI)).

Compliancy

R68 PDP type should allow IPv4, IPv6, IPv4IPv6, IPv4 or IPv6.

Compliancy

Q36 THE SUPPLIER shall describe the level of granularity offered by the EPC-HSS to perform Roaming restriction: per PLMN and/or APN and/or access type and/or HR/LBO, etc.

Answer

R69 Customer wants to restrict or allow roaming for LTE subscribers and / or VoWiFi subscribers. EPC HSS should support different roaming lists for EPC access and for non-3GPP access.

Compliancy

R70 It should be possible to have the flexibility to control roaming rights in EPC HSS by creating dedicated EPC roaming lists. These roaming lists should be populated with “visited PLMN IDs (MCC-MNC)” or / and with MME/S4-SGSN realm or / and with MME/S4-SGSN host names.

Compliancy

R71 It should be possible to have the flexibility to set a specific error code in EPC HSS in case roaming is not allowed in specific areas (MMEs/S4-SGSNs or PLMN IDs). It should be possible to choose between DIAMETER_ERROR_RAT_NOT_ALLOWED (5421) or DIAMETER_ERROR_ROAMING_NOT_ALLOWED (5004). For example if in VPLMN1 user is not allow to roam the error code returned in S6a ULR shall be DIAMETER_ERROR_RAT_NOT_ALLOWED (5421) and if in VPLMN2 user is not allow to roam the error code returned in S6a ULR shall be DIAMETER_ERROR_ROAMING_NOT_ALLOWED (5004).

Compliancy

R72 The EPC-HSS should support sending reset EPC-HSS (DIAMETER reset message) with at least the following options:

- to all MMEs/SGSNs
- to specific MMEs/SGSNs
- to all MMEs/SGSNs with IMSI
- to specific MMEs/SGSNs with IMSI.
- to all MME/SGSN except a list

Compliancy

R73 EPC-HSS should support ADD (Auto Device Detect) feature.

Compliancy

R74 EPC-HSS should support SMS over IP feature. HLR/HSS must support its related features, such as IP-SM-GW registration, forwarding “send routing information”, etc.

Compliancy

R75 EPC-HSS should support SRVCC/eSRVCC/vSRVCC feature. It should be possible to provision at subscriber level STN-SR and vSTN-SR.

Compliancy

R76 EPC-HSS should support to set different ARD (Access-Restriction-Data) value for UE to control UE access. For example UE can't have access to some specific RAT networks (like E-UTRAN, WLAN, Handover to Non-3gpp, NB-IOT, NR) to optimize network performance.

Compliancy

R77 EPC HSS should support DOIC (Diameter Overload Indication Conveyance) feature to keep the stability of the network. DOIC is an over load control solution for Diameter network defined by RFC7683. It complies with IETF RFC7683, 3GPP TS29.228, 3GPP TS29.328, 3GPP TS29.272, 3GPP TS29.273, 3GPP TS29.336. One Diameter node can request peer Diameter node to carry out over load control to decrease its own Diameter signalling load.

Compliancy

R78 The operator should be able to make different queries in EPC HSS in order to obtain number of subscribers located in HPLMN and / or VPLMN split by MMEs / S4-SGSNs.

Compliancy

R79 It should be possible by EPC HSS to send ARD and ZC (zone code information) to a specified MME/S4–SGSN during the location update. The MME/S4-SGSN could be located in HPLMN or / and in VPLMN.

Compliancy

R80 EPC HSS should support "SMS in MME" feature (refer to 3GPP TS 23.272 V12.2.0) and "SMS in SGSN" feature (refer to 3GPP TS 23.060 V12.4.0).

Compliancy

R81 EPC HSS should support AAA reset function. During system cutover, the EPC HSS sends to the AAA an HSS Reset message (PPR) that carries a list of affected subscribers. The HSS Reset message should be set to the EPC AAA in the following ways:

- to all AAA
- to a specific AAA or number of AAA
- by specifying an IMSI.

Compliancy

R82 EPC HSS should support RFSP parameter to be added in subscriber profile. This parameter refers to a frequency selection preference, indicating a policy selected when users access to E-UTRAN.

Compliancy

R83 EPC HSS should support 4G speed up to 4Gb/s.

Compliancy

R84 EPC HSS should support 5G speed up to 4Tb/s.

Compliancy

R85 EPC HSS should support 5G NSA restriction by default for all 4G subscribers when 5G NSA option is enabled.

Compliancy

R86 EPC HSS should support 5G NSA roaming restriction for all subscribers or particular subscribers. This restriction should apply per country and/or operator.

Compliancy

R87 EPC HSS should support 5G SA roaming restriction for all subscribers or particular subscribers. This restriction should apply per country and/or operator.

Compliancy

R88 Subscribing/unsubscribing to multi SIM/multi device should have no impact in customer experience. The following services should not be affected, should not require device restart/flight mode:

- MO call
- MT call
- data session

Cancel location with “subscription withdraw” option having a flag set to “reattach required” should be sent by EPC-HSS in order to fulfill this requirement when subscribing/unsubscribing to multi SIM/multi device.

THE SUPPLIER is requested either to provide this feature in its implementation or to clearly explain how similar feature could be implemented.

Compliancy

R89 It should be possible to have the flexibility to control roaming rights in EPC HSS by creating dedicated non-3gpp roaming lists. These roaming lists should be populated with “visited-network-identifier value” in MAR message.

Compliancy

3.5.9.4. IMS-HSS specific features

R90 IMS-HSS should be able to restrict the view of authentication keys (KIs)/passwords after a subscriber is provisioned. The KIs/passwords should not be displayed when the subscriber profile is queried or modified. The same restriction should apply for listing provision logs.

Compliancy

Q37 Please indicate if the IMS-HSS can be used to store service related data managed by IMS Application Servers. If yes, please indicate the maximum size of repository data, the maximum number of data repositories per user and any further important information.

Answer

R91 IMS-HSS should support CS/IMS SS Data consistency solution. According to TS29.364, when IMS HSS sends service transparent data to MMTEL, it should include namespace in the XML data. The definitions of different vendors' namespace are different.

Compliancy

R92 IMS-HSS should support DOIC (Diameter Overload Indication Conveyance) feature to keep the stability of the network. DOIC is an over load control solution for Diameter network defined by RFC7683. It complies with IETF RFC7683, 3GPP TS29.228, 3GPP TS29.328, 3GPP TS29.272, 3GPP TS29.273, 3GPP TS29.336. One Diameter node can request peer Diameter node to carry out over load control to decrease its own Diameter signalling load.

Compliancy

R93 IMS HSS should support CAMEL feature in IMS domain (O-IM-CSI, VT-IM-CSI and D-IM-CSI). IMS HSS must comply with TS 23.278, 23.078, 29.002, 23.008, 23.218, 29.364.

Compliancy

R94 For VoLTE, HLR/HSS shall support multiple CS/IMS SS Data consistency solutions: based on MAP solution and based on Diameter.

Compliancy

R95 For VoLTE, the converged HSS shall support CS/IMS SDS (Service Domain Selection) to determine whether the terminating call is to be delivered to the CS domain or the IMS domain when CS domain and IMS domain are both used to provide the services for the user who subscribes CS/IMS service simultaneously.

Compliancy

R96 IMS-HSS shall support "Data-Reference=IMSPrivateUserIdentity (33)" as described in 3GPP TS29.329 and 3GPP TS29.328.

Compliancy

R97 IMS-HSS shall support sending PNR to TAS if an IMS subscription is deleted from its database if the following conditions are met according to 3GPP TS29.328:

a) " Removal of Public Identity for which the AS has any active subscription other than IMSPublicIdentity (see table 7.6.1) shall be indicated in the DeletedIdentities element."
b) If Public Identity(ies) are deleted and the AS has subscribed to be notified of changes to IMSPublicIdentity(see table 7.6.1), the class DeletedIdentities shall not be used. If Public Identity(ies) are deleted and the AS has not subscribed to be notified of changes to IMSPublicIdentity but has any other subscription active for the deleted identity(ies), the HSS shall notify the AS of the deletion of the identity(ies) using the class DeletedIdentities."

Compliancy

3.6. AUC requirements

The authentication centre (AuC) is a key component of a HLR / HSS. The AuC validates any SIM attempting network connection when a phone has a live network signal.

The AuC provides security to ensure that third parties are unable to use network subscriber services.

R98 THE SUPPLIER shall clarify compliancy with the requirement to define the HLR AUC application and data repository on the SDM solution and provide a description of its related solution. This description shall clarify the secure and confidential handling of the AUC data and its exchange on the interfaces to VLR/SGSN and MME and confirm compliance to the related mechanism as defined in 3GPP TS 33.102 (3G security), TS ETSI GSM 03.20 (2G security) and 3GPP TS 33.401 (LTE security)

Compliancy

R99 The following algorithm used in Customer shall be implemented in the AUC:

- For SIM (GSM): Comp 128-1, specific A3/A8
- For USIM(UMTS): Customized Milenage (Op and Ri-Ci values).

Compliancy

R100 THE SUPPLIER shall support and provide AuC on top of a standalone Hardware Security Module (HSM). This module being certified with Customer country regulations and should be collocated with HLR/HSS for security constraint.

Compliancy

Q38 THE SUPPLIER shall clarify where is located the AuC function in the SDM architecture e.g. in the HLR FE, in the data repository, and the possible interface between the HLR function and the AuC function.

Answer

Q39 THE SUPPLIER shall detail how data are stored in the AuC and how the transport of AuC information is secured over all interfaces across which it is transported (provisioning, for example).

Answer

Q40 THE SUPPLIER shall explain how they handle unknown IMSI/MSISDN queries from network within their distributed architecture. For example, are they rejected at FE level using legacy GSM procedures or are they passed to the database infrastructure for more flexible handling?

Answer

R101 In order to reduce the SQN re-synchronization during authentication it should be possible to define different SQN ranges (SQN IND) per domain: CS, PS, EPS, IMS, 3GPP AAA, GAA security. THE SUPPLIER is requested either to provide this feature in its implementation or to clearly explain how similar feature could be implemented.

Answer

R102 SDM should be able to restrict the view of authentication keys (KIs) after a subscriber is provisioned. The KIs should not be displayed when the subscriber SIM profile is queried or modified. The same restriction should apply for listing provision logs. THE SUPPLIER is requested either to provide this feature in its implementation or to clearly explain how similar feature could be implemented.

Answer

Q41 THE SUPPLIER shall indicate if one or more operator specific authentication algorithms can be implemented. Also indicate any limitation.

Answer

R103 Customer requires a specific authentication algorithm. The A3/A8 algorithm is proprietary. However its design, which uses simple operations such as shuffling/permutations, rotations, and table look-ups, makes it particularly amenable to implementation. The development and implementation effort for this algorithm will be very similar to other algorithms already used in the telecommunications field. The integration of this specific A3/A8 algorithm, therefore, is highly unlikely to pose any technical difficulty or to require any unusual development effort. TH SUPPLIER shall indicate if such operator specific authentication algorithm can be implemented and will indicate the time needed and will quote. THE SUPPLIER shall indicate if any additional hardware is required for the algorithm and shall quote.

Answer

R104 Customer requires that sensitive data (like K4, OPC, etc) to be input and stored in a secure way.

Answer

3.7. CDL requirements

The Common Data Layer (CDL) is a universal database that provides storage services to other applications through standard APIs (Nudr for instance) or proprietary APIs. It allows other applications storing their data as unstructured data (for instance session data) or as structured data (for instance subscription data). It also allows re-exposing the stored data to other applications.

In the target solution the provided CDL will support both UDR and UDSF storage functions capabilities required in 5G architecture.

The UDR provides the following functionalities: Storage and retrieval of subscription data by the UDM, Storage and retrieval of policy data by the PCF, Storage and retrieval of structured data for exposure by the NEF.

The UDSF provides storage and retrieval of information as unstructured data by any NF.

R105 The general technical features required on UDR, UDSF and Common Data Layer database in general are those mentioned in the SDM General Technical Requirements provided with this RFP. It includes mainly the specifications of the 3GPP specifications up to R16.

THE SUPPLIER is asked to provide the detailed content of the release and to precise the version of the supported 3GPP standard (SoC to provide)

Compliancy

3.8. UDM functional requirements

The Unified Data Management (UDM) and the Authentication Server Function (AUSF) are the key new 5G network functions composing the 5G Cloud SDM. These functions are Cloud native.

The UDM provides the following functionalities: Generation of 3GPP AKA Authentication Credentials, User Identification Handling, Support of de-concealment of privacy-protected subscription identifier, Access authorization based on subscription data, UE's Serving NF Registration Management, Support to service/session continuity, MT-SMS delivery support, Lawful Intercept Functionality for outbound roamers and SMS management.

R106 The general technical features required on UDM network function are those mentioned in the SDM General Technical Requirements provided with this RFP. It includes mainly the specifications of the 3GPP specifications up to R16. The same applies for requirements specified in the Security annex of this RFP.

THE SUPPLIER is asked to provide the detailed content of the release and to precise the version of the supported 3GPP standard (SoC to provide).

Compliancy

R107 To insure smooth interworking between 4G and 5G domains the target solution should support interactions between UDM and HSS, in the areas of authentication keys sharing, mobility management (e.g. cancel registration…), IMS interworking (e.g. T-ADS query…), SMS-MT delivery in particular.

THE SUPPLIER is requested to describe precisely its implementation on UDM whether it is based on proprietary interface and/or standardized interface (3GPP R16 TS 23.732) as well as availability dates.

Compliancy

3.9. AUSF functional requirements

The Unified Data Management (UDM) and the Authentication Server Function (AUSF) are the key new 5G network functions composing the 5G Cloud SDM. These functions are Cloud native.

The AUSF provides the support of authentication for 3GPP access and untrusted non-3GPP access.

R108 The general technical features required on AUSF network function are those mentioned in the SDM General Technical Requirements provided with this RFP. It includes mainly the specifications of the 3GPP specifications up to R16. The same applies for requirements specified in the Security annex of this RFP.

THE SUPPLIER is asked to provide the detailed content of the release and to precise the version of the supported 3GPP standard (SoC to provide)

Compliancy

3.10. EIR requirements

The legacy Equipment Information Register (EIR) function and new 5G EIR may be hosted on top of SDM solution.

Q42 In case Customer first deploys HLR, what will be the additional infrastructure requirements necessary to enable the EIR application after?

Answer

Q43 THE SUPPLIER shall explain the possibility that EIR to trigger a notification to an external system on any change of IMEI-IMSI pair. THE SUPPLIER shall provide details on interface type used for notification. THE SUPPLIER shall explain the message sequence of such procedure giving detailed messages format, indicating mandatory/optional fields.

Answer

Q44 Is there any mechanism implemented in EIR of detecting multiple devices having the same IMEI? Can the multiple IMEI list to be retrieved by operator or automatically saved or forwarded to an external element? If yes please provide more details. What is the format of retrieved/saved list?

Answer

Q45 Is it possible to allow IMSI/IMEI association in order to allow calls from IMSI even IMEI is in black list? What about if the same IMEI is set on multiple devices and is in black list, can the operator allow calls only from one IMSI? What are the limitations? Please provide details?

Answer

Q46 Is it possible to allow IMSI/IMEI association in order to allow calls from IMSI when the same IMEI is set on multiple devices and the IMEI is in black list? Is it possible to have more than one association IMSI/IMEI (more IMSI using the same IMEI on the same time) and allow calls from all these IMSIs associated to one IMEI? If yes please indicate how many IMSI can be associated to one IMEI?

Answer

Q47 Is it possible to allow IMSI/IMEI association in order to allow calls only from the associated IMSI and IMEI? When the IMSI is used with a different IMEI (no matter if IMEI is in blacklist or whitelist) the call should be forbidden. What are the limitations? Please provide details?

Answer

Q48 Please describe the EIR behaviour when it detects multiple IMSI with the same IMEI (clone devices).

Answer

R109 EIR should support ADD (Auto Device Detect) feature. If EIR detects the change of the IMEISV or IMSI, EIR sends the subscriber information and UE information to external server.

Compliancy

Q49 Can the EIR be connected to an external central EIR database i.e. including black-listed and grey-listed IMEI's from the other operators of the country? If yes which interface is available for such connection? Please provide details on synchronization process of EIR with central database.

Answer

Q50 THE SUPPLIER shall describe the way all lists (black, white, grey and other lists) are provisioned. Please detail if other provisioning HW/SW than HLR provisioning is needed for EIR.

Answer

Q51 THE SUPPLIER shall indicate the maximum dimension of each list (black, white, grey and other lists) and any constraints. Please indicate the licencing (pricing) model.

Answer

3.11. Software roll-out and optional features

THE SUPPLIER shall indicate the software releases that will be needed during the 5 year time frame and will quote them.

Q52 THE SUPPLIER shall provide the basic features list included in the proposed software and hardware release, for HLR, IMS-HSS, EPC-HSS and EIR separately. THE SUPPLIER shall also provide a detailed description for each feature.

Answer

Q53 THE SUPPLIER shall also provide the list of optional features and pricing options per 1000 user basis for HLR, IMS-HSS, EPC-HSS and EIR separately. The Supplier shall also provide a detailed description for each feature.

Answer

3.12. Backup & Recovery

R110 Backup and recovery solutions shall be provided as part of the proposal. THE SUPPLIER should detail the solution proposed, including hardware, scripts and documentation provided for this task within their answer and requirements onto external components if applicable.

Answer

Q54 Explain how this solution may be applied to small recovery cases, such as the retrieval of a configuration or a log file, within the timescales specified by the SLA.

Answer

Q55 Explain how this solution may be applied to major recovery cases, such as a full platform recovery after a major disk failure or corruption, within the timescales specified within the SLA.

Answer

Q56 Does THE SUPPLIER backup and recovery solution rely on shared media or hardware? If so, provide details here.

Answer

Q57 THE SUPPLIER will confirm the ability to automate the backup of user logs, database, system.

Answer

Q58 THE SUPPLIER shall provide a complete description of backup data. This description shall detail at least: Backup Strategy, the frequency of backups, the retention time; the scope of backup must meet the availability requirements and system health.

Answer

Q59 THE SUPPLIER shall undertake to carry out recovery tests to ensure the availability and integrity of backup data.

Answer

Q60 How long would it take to recover from failure or outage? Does the recovery ensure AUTOMATIC global system integrity?.

Answer

R111 In case of one site power failure the system should automatically recover and be up and running without human intervention.

Answer

R112 The system should have the option to automatically export the backups on external servers by ftp/sftp.

Answer

R113 The offered system should provide a tool used to:

- Query and export entire subscriber database by manual or automatic tasks.
- Query and export database using operator defined filters.
- The query or export result should be in standard formats (e.g. txt, csv).

- The query or export result should be saved locally, remotely or transferred by email or ftp.

Answer

Q61 THE SUPPLIER shall clarify how its system allows performing the dump of part or all of the database content, using different type of criteria. The output has to be in a readable & usable format to be used for command batch generation (using scripts for the update).

Answer

Q62 THE SUPPLIER shall clarify how its system allows performing the Bulk update for user profiles, without help of the Supplier. Which type of data can be updated by batch processing.

Answer

Q63 THE SUPPLIER shall clarify how its system allows performing the mass modification for user database, without help of the Supplier. Which type of data can be updated by mass modification? Is mass modification performed online or offline? If the mass modification is offline the supplier shall describe also the process for uploading the modified database in all system. Please indicate the impact on system performance of database mass modification for both online and offline methods. The supplier will indicate all necessary tools (internal and/or external) needed for such operation. The supplier will quote in optional TCO any optional tool required for mass modification.

Answer

3.13. Network Management

3.13.1. Overview:

The aim of this section is to provide Customer with a full understanding of how Operation and Maintenance routines will be accomplished and to present the different applications available in THE SUPPLIER's operating system. THE SUPPLIER is asked to detail the following points:

Q64 THE SUPPLIER is asked to give description for all the available tools used to achieve the following operation:

- Fault Management
- Configuration Management
- Performance Management
- Security Management
- Log Management
- Software downloading

Answer

Q65 THE SUPPLIER must provide a complete schema describing the NMS architecture with all interfaces and precise the role of each element (Element Manager (EM) and VNF Manager (VNFM)). All VNFs should be connected to these network management elements. Links must be redundant between VNFs and EM/VNFM.

Answer

Q66 THE SUPPLIER shall detail all features for the NMS system.

Answer

Q67 THE SUPPLIER shall provide Roadmap by mentioning the required release to manage each new SDM release.

Answer

3.13.2. Network Management System

R114 As part of their proposal, THE SUPPLIER is expected to include an NMS that has been dimensioned to meet Customer ’s needs.

Compliancy

Q68 A detailed description of the configuration of all NMS elements: NMS VNFs (VNF components, vCPUs, RAM memory, VM image size, ephemeral and persistent storage, vNICs interfaces), NMS Clients, Other equipment (Backup server and robot, external disks arrays,...).

Redundancy must be provided for all critical elements.

Answer

Q69 THE SUPPLIER will indicate the dimensioned performances of its NMS. As a minimum, performance should be specified in terms of the maximum number of faults, alarms, statistical counters and commands that may be processed per second, the maximum number of users simultaneously connected to NMS globally and per application (HLR, IMS, EIR). THE SUPPLIER is at liberty to extend this definition of performance should they feel it helpful.

Answer

Q70 THE SUPPLIER shall be able to provide the following types of access to the SDM system:

a. Connection to the Customer centralized NMC using: SNMP, CORBA, ASCII over TCP, SQL protocols. SNMP is mandatory

b. Secure remote connexion to the system to be used by the Supplier in emergency cases

c. Local operation and maintenance terminal

d. Local alarm management terminal or panel

Answer

R115 The system shall be managed locally and centralized. All the functions offered in the local mode shall be available in centralized mode.

Answer

R116 The proposed SDM shall support the following data configuration management:

a. Easy-to-use MML interface

b. Predictive text input function

c. GUI based command input mode

d. Command line mode

e. Possibility to run MML macro commands or scripts.

f. History command list

g. Online data modification and loading with immediate affecting of services

Answer

R117 The proposed SDM shall support the following subscriber data management:

a. Easy-to-use MML operation interface with predictive text input function.

b. GUI based command input mode

c. Convenient service addition, modification, and deletion functions.

d. Operation log function that provides detailed operation history.

e. Interfaces to business office such as the provisioning system.

Answer

Q71 THE SUPPLIER will indicate which secured protocols are supported by the NMS.

The NMS must have an interface to connect user terminals. THE SUPPLIER will indicate which application(s) will allow access to the NMS via a remote connection.

Answer

Q72 THE SUPPLIER will explain how it will be possible to use individual logins to manage fully each of the platforms provided as part of the SDM solution without any requirement either to use generic usernames or to swap between usernames for individual tasks.

Answer

Q73 Explain what management facilities (examples include NIS or Kerberos) are available for tasks such as creating user logins Customer then distributing them for use across all deployed nodes.

Answer

Q74 Detail the access profile levels that can be applied to individual users, and how these are used to allow or restrict access to management tasks (e.g. backup, restore, platform shutdown, ...)

Answer

R118 The offered system should have the option to redirect alarms and KPIs reports to email and/or external server by ftp/sftp.

Compliancy

R119 The proposed SDM shall support the following alarm management:

a. Collect alarm information upon alarm occurrence or alarm clearance.
b. Classify alarm information and send them to the alarm system according to their priority levels.
c. Display detailed descriptions and removal suggestions of alarms on graphical interfaces through the alarm console.
d. Acknowledge and comment alarm mechanism
e. Configurable alarm severity mechanism
f. Detailed or quantity alarm display
g. Friendly GUI alarm display
h. Extensive alarm log for a long period of time (months)
i. Redirection mechanism to an external backup server of alarm log files

Answer

Q75 THE SUPPLIER shall detail any mechanisms in place to prevent O&M Alarms Storms in the case of mass failures/outages.

Answer

Q76 In case of O&M Alarm congestion, THE SUPPLIER shall detail any mechanisms in place on Agent and/or Element Management System to prioritize the flows.

Answer

Q77 Detail how the data repository can be queried by external IT systems. Explain whether it is possible to perform data repository's listing based on criteria.

Answer

3.13.3. Statistics and performance

R120 The proposed SDM shall support customized measurement reports entity regarding the following aspects: telecom and subscriber data base.

Answer

R121 Number of subscribers, calls and traffic, operator defined KPIs and default KPIs shall be scanned and measured on a real-time basis.

Answer

R122 The proposed SDM shall support measurement time-segment (including the day time segment, week time segment and month time segment) and measurement cycle ranging from 1 minute to 24 hours.

Answer

R123 Standard and open output format, with printing function available.

Answer

R124 Automated KPIs tasks configurable by operator with exported results in a standard format (e.g. xls, csv, txt).

Answer

R125 Substantial space required for counter data storage for at least 1 year.

Answer

R126 Possibility to retrieve KPIs within 6-12 months with a set by operator granularity of 5min/15min/30min/60min/day/week.

Answer

R127 Counters stream redirecting to an external server and external email server in raw data or other Supplier specified format.

Answer

3.13.4. Network Crisis

The network can be in crisis. In that situation, a peak of messages is possible (all kinds of messages: alarms, faults, measurements).

R128 The NMS shall not lose any messages and shall log all the messages.

Answer

R129 All the basic functions (fault, configuration, performance and security management) shall remain operational.

Answer

R130 The NMS shall give different priorities to the messages in order to process the most important alarms and to store the minor ones.

Answer

R131 The NMS shall come back to the optimal and daily usage mode in maximum one hour after the end of the network crisis.

Answer

3.14. Provisioning

3.14.1. Provisioning interface

On-line interface shall be synchronous: one direct and on-line answer on each request sent by the provisioning system. The interface should be based on well-known and open standards, ensure high reliability and automatic recovery in case of communication problems. The

preferred on-line interface is based on SOAP, the xml web-service based like services, through https-soap.

The provisioning interface (batch & online) shall support the following provisioning use cases:

- Creation of a SDM user
- Deletion of a SDM user
- Activation of services to the SDM user, with all needed parameters/features
- Deactivation of services
- Suspend/resume of services
- Update of services: Add/Remove/Update services parameters/features (barring, vm, call forward, …
- Query of detailed info on service based on SDM user key identity (ex MSISDN, IMSI, GPSI, SUPI…)
- Simplified provisioning with templates

In case of update of an existing SDM user, the SDM will allow to just send the concerned changes and NOT the full service description

All requested functional requirements shall need to be covered through the SDM provisioning API. The SDM allows that all those services are provisioned through the same connector. So this is seen as one global API.

R132 THE SUPPLIER shall provide a full description of its solution for provisioning of all requested service (including WSDL files per network function). Compliance with above listed requirements shall be included. The description should also highlight whether the SDM will provide a unique interface to the IT or a direct access to each of its elements. THE SUPPLIER shall detail the provisioning flows per HLR, IMS-HSS, EPC-HSS and EIR (if provisioning is separated per HLR, IMS-HSS, EPC-HSS, EIR the interdependencies of provisioning flows in case of multi-application platforms, etc.).

Compliancy

Q78 THE SUPPLIER shall provide a description of the interfaces available for the provisioning of the SDM. The following details should be provided for each interface:

- type (real time, batch, API, GUI,…)
- technology (web services, SOAP/XML-RPC, CORBA, JMS,…)
- synchronous or asynchronous
- ASCII or binary
- response times (during typical daily use of SDM)
- data elements supported
- transactions / commands
- status codes, error codes
- typical response times for the commands (e.g. subscriber query, create, update, etc)

Answer

Q79 The interface with the provisioning system should allow parallel provisioning. THE SUPPLIER shall describe how parallelism is supported and describe any limitations. What

will be the behaviour of the SDM if several provisioning requests for the same subscriber are sent at the same time to the SDM?

Answer

R133 The SDM shall support change of MSISDN, change of IMSI, and provide the corresponding provisioning interfaces

Compliancy

R134 The interface with the provisioning system should allow querying any kind of permanent or dynamic data on a per subscriber basis.

Compliancy

R135 The interface with the provisioning system should the definition of subscriber profiles (templates) to provision.

Compliancy

Q80 After provisioning, is the subscriber still linked to the profile, in a way that a change to the profile impacts the user? How changes on one parameter outside the profile are done?

Answer

For each command sent by the IT system to the SDM, the SDM must answer with one and only one response (successful or erroneous), including an pre-defined error code allowing the IT system to interpret this error and to take the correct action. The answer means also that the command is fully executed at the SDM side – no more background treatment are done by the SDM.

The exhaustive list of error codes & descriptions will be made available to Customer .
A clear distinction will be made between successful cases, technical errors cases and functional errors cases.

The different applications that use this SDM API will implement timeouts mechanisms. So it's possible that at the time SDM wants to answer, that the connection has been closed by the application that has sent the request. And this may not generate issues at the SDM side.

In case if SDM receive a set of commands in the same time related to the same profile which require modifications on external network elements then these modification will be executed synchronous in the order received from provisioning system.

R136 THE SUPPLIER shall clarify compliance with above listed requirements on SDM provisioning response behaviour.

Compliancy

Q81 What will be the behavior of the SDM with respect to the IT provisioning system in case of unavailability of one of its elements (Front-End, Back-End)?

Answer

The SDM will allow to use or not encrypted data (as for KI values) in the provisioning commands, based on the system/applications sending the request. The fact that it's encrypted or not will depend of the system/application that sends the requests to the SDM.

R137 THE SUPPLIER shall clarify compliance with above listed requirements on secured provisioning.

Compliancy

R138 A query of authentication data shall return if an entry is present, not the data itself.

Compliancy

Q82 In order to provision more easily some services (like GPRS) SDM should allow defining specific profiles (like GPRS profile) that will be linked to subscriber.

Answer

Q83 Is it possible to prioritize the provisioning commands – e.g. make query commands a lower priority to create or update commands?

Answer

3.14.2. Bulk provisioning

Aside from the on-line IT provisioning interface, a batch provisioning mechanism should be possible. This batch provisioning should allow us to perform bulk user data manipulation such as mass changes of SK, GT, Camel marks,…. Also the pre-provisioning of KI directly on the AUC should be possible through the batch provisioning interface.

Q84 THE SUPPLIER shall confirm availability of a bulk/batch provisioning interface. The provided information shall list any restrictions on the data which can be updated through the batch interface and shall contain a description of the way the batch file is created and executed.

Answer

R139 The interface with the provisioning system should allow the mass provision (creation and modification) of all or a subset of subscriber data. The definition of a subscriber subset shall support at least, selection by IMSI range, selection by MSISDN range, selection by PVI range, selection by PUI range, selection based on values of any subscriber data item within the SDM. The supplier will describe the different subscribers' criteria/parameters that can be used to apply massive changes.

Compliancy

R140 The mass provisioning response must include one status/return code per unitary request contained in the mass provisioning request

Compliancy

Q85 For both individual and mass provisioning, is it possible to select an IMS subscriber by IMPI range, or by IMPU range?

Answer

R141 It shall be possible to query the current number of subscribers on an SDM element through the real time interface

Compliancy

Q86 THE SUPPLIER shall provide for each provisioning action, a template of the batch file to execute.

Answer

Since batch provisioning could run in parallel to the on-line IT provisioning interface, precautions should be taken to avoid impacting the on-line provisioning, while running batch files. Priority should always be given to the on-line provisioning flow.

Q87 THE SUPPLIER shall explain if and how priority can be given to on-line provisioning, avoiding performance impact on on-line provisioning if running batch provisioning in parallel.

Answer

3.14.3. Bulk SIM cards pre-provisioning and de-provisioning

There are 2 possibilities that SIM cards to be declared:

- in bulk mode as part of the SIM ordering process
- on-the-fly (one command a time)

It is therefore not inconsistent that questions related to bulk and non-bulk SIM activation are present in this document; the Supplier will answer questions related to both approaches.

This chapter covers all bulk/on-the-fly SIM loading/deleting needs;

- at SIM ordering time
- for the initial setup of the HLR
- for operational maintenance

Item	at SIM ordering	Initial setup	Operational maintenance
Ki pre-provisioning of new SIMs	Yes	No	Yes
Ki provisioning of existing SIMs	No	Yes	No
Ki de-provisioning	No	No	Yes

3.14.3.1. KIs pre-provisioning of new SIMs

At each SIMs order (batch of up to 30000 SIMs), a file would be provided to HLR operations, and would be loaded into AUC through Customer provisioning system.

Q88 THE SUPPLIER shall:

- Clarify what native interface it provides to perform such a bulk load as well as on-the-fly
- List the card parameters that must be provided if they differ from the IMSI + the KI key + an algorithm identifier
- Provide an sample (demo) file for a small number of SIM cards
- Clarify what performance it can guarantee for this loading
- Explain the security features of this interface to prevent disclosure of KI key values (for instance, encrypting of the whole file or of the KI value in the file).

Answer

3.14.3.2. KIs pre-provisioning existing SIMs

Today approximately 15 million SIMs are declared on HLR/AUCs.

Q89 THE SUPPLIER shall explain how the SIMs information will be copied from existing SDM to the new SDM.

Answer

3.14.3.3. KIs de-provisioning

Customer performs process on regular bases for identifying SIM cards that should be deleted. SIMs identifying is based on some particular patterns, for example subscribers that had no activity in a certain time frame.

Q90 THE SUPPLIER shall indicate if it can provide a tool or feature that shall be used for querying all the subscribers that did not have activity in a specified time frame. THE SUPPLIER shall quote of such feature or tool if not included into basic package.

Answer

3.14.4. Provisioning interface performances

Customer requires a minimum rate of provisioning of 200 commands/sec distributed over at least 60 simultaneous sessions.

Number of commands per second	> 200
Number of simultaneous opened sessions	> 60

R142 No delay between openings of at least 60 simultaneous sessions should be provided. All sessions shall be opened at the same time.

Compliancy

Q91 THE SUPPLIER shall explain all hardware and software modification for provisioning in case of SDM capacity expansion (database and/or real time applications). The answer will also detail all functional changes of provisioning in these cases.

Answer

Q92 THE SUPPLIER shall explain any constraints and limitations of provisioning methods related to subscriber partitions. For example when changing the IMSI or adding a data subscription to a subscriber if any relocation of subscriber profile on other partition or internal data group is mandatory this should be done automatically by the system. Please describe it for HLR, EPC, IMS and EIR applications.

Answer

Q93 THE SUPPLIER shall explain if the system offers any scripting capability on top of basic/standard methods exposed over the provisioning interface. A script is a custom (developed/modified by the Customer) group of standard methods that can be invoked with input parameters, execute certain logic and issue some basic commands on the platform. The "script" can be also referred as a "macro-command" -> a group of standard commands following certain logic.

In case the platform has such functionality, please detail:

- instructions that can be used in the macro-command (decisional structures, looping structures, lookup methods; ex. IF, SWITCH, WHILE, SELECT)
- if it is possible to use the current value of certain attributes of the subscriber in the decisional process.

Answer

Q94 THE SUPPLIER shall indicate the average number of commands used for performing a task (display a subscriber profile, adding/removing services on a subscriber profile, create/modify/delete a subscriber, etc) on SDM. THE SUPPLIER shall provide some example of real commands used for such tasks.

Answer

Q95 THE SUPPLIER shall explain if an external key can be added to all or a part of subscriber profiles. The key should be unique for one subscriber and should be visible in subscriber profile display and database export files. This user id (key) may be used for synchronization process with other external tools. The supplier will quote as optional if not included in the basic package.

Answer

Q96 THE SUPPLIER shall explain the load balancing mechanism for provisioning system.

Answer

3.14.5. Coherence check

Customer uses a dedicated tool for coherence check of real HLR, EPC, IMS database with Customer Care System database. Once a week all database is loaded into the tool and analysed using different criteria. The tool allows querying the databases using filters (simple or complex, for example query all subscribers that have in profile OSS12 AND call forward on busy to +40744945555, etc). The query shall be possible for any subscriber profile parameter filters. The result is exported to an output file that is further used in the coherence check process. The filters shall also be possible for output result. The output result filters might be different then query filters.
The coherence check process in done without stopping of the provisioning.

Q97 THE SUPPLIER shall state if such coherence check feature is available on SDM or must be developed. THE SUPPLIER can provide another approach to deal with this demand. THE SUPPLIER shall provide complete description and provide such pricing.

Answer

3.14.6. Provisioning interface limits

Q98 THE SUPPLIER shall describe the limits that exist on the various provisioning interfaces. These limits could be:

- Maximum number of arguments in a command
- Maximum size of a command
- Maximum execution time for a bulk command (it is possible that the system refuses to process a large job for longer than a certain time)
- Maximum number of concurrent connections to the interface
- Any other… (to be clarified if any)

Answer

3.14.7. Provisioning interface tracing

It must be possible to activate a tracing mode where all messages exchanged with the provisioning application are recorded in a file or pushed to a logging application.
Additionally:

- The messages (or events) must be recorded with a timestamp.
- If the logging file/application collects events from several sources (not only the provisioning interface), it must be easy to distinguish the interface-originated messages from the others (thanks to a 1 line regular expression for instance)
- It must be possible for an Customer operator to activate / deactivate this tracing mode (without intervention of the Supplier)
    - Changing the tracing mode should either
    - Not require to stop the provisioning interface at the SDM side
    - Or the stop + change mode + restart duration must be less than 5 minutes.

Q99 THE SUPPLIER shall describe the tracing capabilities of the provisioning interface.

Answer

Q100 THE SUPPLIER shall clarify:

- The performance impact on the provisioning interface and the rest of the SDM functions of this trace mode is activated.
- The size of the logged data for 100 creations of the subscriber profile.

- If possible, the Supplier will provide a sample of such a trace.

Answer

3.14.8. Provisioning interface statistics

The SDM provisioning interface should provide some statistics about operations performed by the client interface.
The needed statistics are:

- Number of commands per hour (split per type of command)
- Average processing time (per type of command)
- Number and % of failed commands (per day)
- …

Alternatively, the interface can provide raw "access logs" that would be loaded into a statistics package by Customer to generate the reports. Such access logs would consist in 1 record per command executed and report at least the command, timestamp, duration and return code.

Q101 THE SUPPLIER shall explain if these statistics/access logs can be enabled or disabled, and the impact on the performance of provisioning interface (Customer will probably want these always enabled).

Answer

3.14.9. Provisioning interface redundancy

Q102 THE SUPPLIER shall describe the redundancy mechanism of the provisioning interface (cluster, active/standby). Customer expects this mechanism will be transparent for the client provisioning application.

Answer

3.14.10. Mediation to interface with legacy SDM

Customer would like that an intermediate provisioning layer (device) during migration exists. The adaptation of Customer provisioning system to the new requirements of SDM will be done prior migration.
The mediation layer should expose towards Customer provisioning system only the new SDM interface, while on the other end should be able to integrate with both new SDM and legacy SDM.
The interface exposed towards ORO provisioning system should be the same with the one exposed by the new SDM system, so no other functional modification will be required after the entire subscribers base will be migration on new SDM, and this intermediate layer will be removed from the provisioning chain.

The behaviour required for the mediation layer is that when receiving a command in new SDM format it is able to internally determine the HLR/AUC/IMS the subscriber resides (either new SDM or legacy SDM). Based on this information it selects the SDM to run the command, makes necessary adaptation (if it is legacy SDM it should translate the command to legacy format) and then sends the command to selected SDM. The selection of SDM where command should run is made based on IMSI (MSIN) range when IMSI is provided as command parameter. If IMSI is not provided the one possible way to make the selection is to mark the MSISDN (SN) with a prefix.
The mediation layer will be deactivated after legacy SDM database is migrated.
Capacity of the mediation layer should not be smaller than 40 cmds/sec.(if the mediation will be used only for the migration period, or the requested capacity of 200 cmds/sec and at least 60 simultaneous opened sessions if the system will remain as a permanent interface).

Q103 THE SUPPLIER shall analyse the possibility to provide the required mediation layer (device). THE SUPPLIER shall quote such feature/tool if not included into the basic package.

Answer

3.14.11. GUI access to user data

Access to user data will be needed, not only through a direct maintenance client access for the engineers designing or operating the SDM platforms, but also for customer care agents, who need the ability to interrogate and modify user information through a Web based GUI.

Q104 THE SUPPLIER shall explain the possible ways and available tools for different kind of operators to get access to user data, related to all configured functions (as listed in the functional requirements chapter). The available tools shall allow interrogation of user data, as well as updates to user data. Any restrictions on the scope of this interrogation / modification shall be listed.

Answer

The provided tools for data interrogation will also be used to extract a full or filtered dump of the provisioned data of all users, for external use (reporting, batch file creation,..).

Q105 THE SUPPLIER shall confirm ability to obtain full or filtered dump of the stored data of all or a subset of the provisioned users. A description of the possible filters / criteria for data extraction shall be provided, as well as the possible output formats of the extracted data files.

Answer

3.15. Security requirement

3.15.1. Security of the solution

R143 The architecture of the application / solution must guarantee high availability of the service with redundant infrastructure, nodes and equipment. THE SUPPLIER shall describe and document the proposed solution for high availability.

Answer

Q106 THE SUPPLIER shall confirm ability to generate access and activities logs which could be push by FTP or SFTP on Customer dedicated server.

Answer

Q107 And allow “cold” analysis of any access and any unauthorized operation on the system.

Answer

R144 Operators’ access shall be based on an authentication system guarantees, authorization, traceability and accountability.

Answer

R145 User authentication

a) Prior to accessing the application a user must enter a valid user-id and password.

b) All users must have unique user-ids.

c) No hard coded passwords.

d) Passwords must not be displayed on input.

e) Encrypt authentication credentials (user-id and password) between the application client and the application server.

f) Display a security, terms & conditions warning banner straight after the user has been successfully authenticated.

g) Display details of the last successful login to the user after they login.

h) Restrict the number unsuccessful logins to 3 logon attempts.

i) The logon procedure must validate the user only after the password is input.

j) The application must not identify which of the user-id, password or other authentication credential is incorrect.

k) Force the user to change their password on their 1st logon.

l) Force the user to provide a quality password:

- Expire every 60 days;
- At least 8 characters;
- At least 6 different passwords must be used before re-issue is permitted. For administrators this must be at least 13 different passwords to prevent annual cycles;
- For administrative accounts, 4 types of characters should be used: alpha numeric, upper case, lower case, special ones;
- For non-administrator accounts, 3 types of characters are acceptable;

Answer

R146 User access control

a) The application must allow user profiles to be created, which can then be attributed to more than one user.

b) All users must belong to a user profile.

c) Rights to all application data and objects must be delegated to a user profile – not a user.

d) User profiles must have the capability of restricting access to data, this being either:

- Full read/write access;
- Read only access;
- No Access

e) User profiles must have the capability of restricting access per command, this being either:

- Full read/write access;
- Read only access;
- No Access

f) Users must not be able to access administrator level functions.

g) Perform administration functions over SSL for browser based applications

h) The application must support simultaneous multiple user logons.

i) Encrypt sensitive data when transferred between internal and external systems. Use sFTP and/or SCP for file transfers – FTP is not permitted.

j) Secret, Confidential, Personal and security data must be encrypted between the application client and the application server using either a VPN or SSL.

k) The application must be able to timeout or disestablish the session between the client and the application server after a period of inactivity.

l) The system administrator must be able to terminate a user's session.

m) A user must be able to log-out of an application.

n) The application must not leave residual data on the application client system after the user logs out.

o) For web applications:

- Implement anti-browser caching.
- Cookies must not include sensitive data - specifically authentication or any other security that may lead to the compromise of the application.

p) It must be possible for the administrator to control access to the application.

q) A user-id must not be able to be re-used.

r) Provide an Information Classification on all data produced by the application (E.g. reports). For example, Secret, Confidential, Restricted, Unrestricted.

Answer

R147 Audit and Logging

a) Log all attempts to access the application.

b) Log the device and the path that the user has used to access the application

c) Log all security related activity.

d) Detect all unauthorised activity.

e) Logs should include:

- User ID
- dates, times, and details of key events, e.g. log-on and log-off;

- terminal identity or location if possible
- records of affected records, successful and rejected data and other resource access attempts;
- changes to system configuration;
- files and databases accessed, the operation code (type) and the kind of access;

f) Keep transaction logs and audit trails for a minimum of 3 months.

g) Time-stamp the insertion of new and update of existing database records

h) Display that the data has been recorded accurately when a user has completed a transaction successfully

i) Log all system administrator activity.

j) Provide facility to filter logs based on any combination of:

- User-id
- Command/Action performed
- Date/time
- Means of access

k) Archive audit logs on a regular basis.

l) Where there are multiple audit logs, provide a facility to produce a single report from multiple logs based on:

- User-id
- Command
- Date
- Time

Answer

R148 Third Party Connections

a) 3rd parties shall not use generic user ID

b) Use two part authentication for all 3rd party connections

c) All 3rd party connections are through an approved Customer security gateway

d) Encrypt sensitive data between Customer and 3rd party user using a VPN, SSL or a file level encryption tools. Sensitive data includes:

- Secret or Confidential information
- Personal data as defined by the Data Protection legislation
- System security events such as authentications session
- System Administrator activity

e) Use SSH v2 for maintenance and support activity – Telnet is not permitted

Answer

Q108 Depending on the OS type and Database, a description of the configuration must be provided. This document must contain the information on user profiles, services and enabled ports. All unused network services should be disabled on each equipment.

Answer

Q109 If THE SUPPLIER has a disaster recovery plan strategy on the solution, it is invited to present it.

Answer

3.15.2. Operations & Maintenance

R149 Live and testing environments must be separated by at least logical mechanisms to prevent unauthorized connections between these 2 environments.

Answer

Q110 THE SUPPLIER shall provide a detailed description of the logs generated by the solution (type, location, content, ...)

Answer

R150 The solution must not generate logs containing user passwords.

Answer

Q111 THE SUPPLIER shall confirm the ability to generate logs for following actions:

- all access to administrative facilities (source, date, time, login, IP)
- all access to applications (source, date, time, login, IP)
- all successful and unsuccessful access and operation (source, date, time, login, IP, type of operation)

Answer

Q112 THE SUPPLIER shall confirm the ability to generate logs for anomalies.

Answer

Q113 THE SUPPLIER shall confirm the ability to generate complete user operation logs and applications running logs.

a. User access log: success access or failed access to servers with detailed information
b. Functional log for SW aspects e.g. system, security, operation, provisioning logs
c. Provisioning logs should be retrieved and queried directly from SDM interface with configurable filtering criteria e.g. MSISDN, IMSI, PUI, PVI, user name, error code, command code, etc, over minimum 24 hours timeframe.
d. Logs redirecting mechanism to an external server over ftp/sftp in a readable format
e. Friendly and easy-to-use output interfaces for logs, with detailed online help

f. Viewable log information regarding user operations
g. Explanation and analysis for non-viewable information.
h. Filtering of test and debug information in the logs to help maintenance engineers locate faults based on the log information.
i. Searching criteria mechanism.

Answer

R151 The logs must be retained and available for online review for a minimum of three months.

Answer

Q114 All machines and equipment used in the project must be synchronized with Customer NTP server (Network Time Protocol).

Answer

R152 The proposed SDM shall support the following maintenance functions:

a. Monitoring the status of a link or a functional unit
b. Tracing messages over the standard interfaces of the system
c. Remote maintenance

Answer

R153 The proposed SDM shall support the following secure and convenient remote maintenance functions.

a. Query the versions and status of subsystems and each module。
b. Monitor and isolate system faults.
c. Query alarm information.
d. Obtain real-time operation information.

Answer

R154 The proposed SDM shall support the following secure and convenient remote maintenance functions.

a. Query the versions and status of subsystems and each module。
b. Monitor and isolate system faults.
c. Query alarm information.
d. Obtain real-time operation information.

Answer

3.15.3. Tracing

R155 The proposed system shall deliver powerful subscriber and signalling tracing functions that can be fulfilled without any additional signalling test device. Subscriber and signalling tracing help locate faults.

Answer

Q115 THE SUPPLIER shall describe the mechanism of the traced subscriber messages.

Answer

R156 The proposed system shall be able to trace the messages on the standard interfaces, for all applications (HLR, AUC, EPC, IMS, EIR, etc), storage of the traced messages. The trace function shall support multi-user. The trace messages shall be exported to file such as txt, csv, wireshark formats.

Answer

R157 THE SUPPLIER shall provide some sample of the traced messages on the standard interfaces.

Answer

R158 The system shall support configurable tracing criteria (e.g. MSISDN, IMSI, PUI, PVI) depending on application and interface. The filter should allow use of wildcard, ranges and prefixes.

Answer

R159 The system should support tracing for internal messages on modules/functional units/internal interfaces used for debugging.

Answer

3.15.4. Software upgrades

Q116 THE SUPPLIER shall describe the software upgrade procedure for real time applications (HLR, EPC-HSS, IMS-HSS, EIR), database and other software components if applicable.

Answer

Q117 Considering that the system is distributed over several sites, THE SUPPLIER shall describe how the software upgrade is performed:

a. All or part of equipment (FE, BE, etc) on one site in one maintenance window, then roll-out on the other sites on other maintenance windows (one per site)? Please detail.

b. All the same type equipment (e.g. FEs) on one site in one maintenance window, then roll-out on the other sites on other maintenance windows (one per site) for the same type of equipment (FEs)? Please detail.

c. All the same type equipment (e.g. FEs) on all sites in one maintenance window, then all other same type equipment (e.g. BE) on all sites in other maintenance window, and so on for all equipment types? Please detail.

d. All system components (FE, BE, other servers) on all sites during the same maintenance window? Please detail.

e. None of the above. Please detail.

Answer

Q118 THE SUPPLIER shall specify the average roll-out duration for one site and indicate if the roll-out will be done on the roll-out site or remotely.

Answer

Q119 THE SUPPLIER shall specify if a node re-start is necessary during software rollout, causing loss of service.

Answer

Q120 THE SUPPLIER shall specify whether redundancy/resilience is compromised during software rollout. If so, detail how it is compromised, and any steps that will be taken to mitigate risk.

Answer

Q121 THE SUPPLIER shall specify how a “roll back” will be performed in the event of an unsuccessful upgrade.

Answer

Q122 Questions Q117 to Q122 refer to software upgrades. THE SUPPLIER shall answer to the same questions in case of software updates.

Answer

4. Project plan and scope

4.1. Section overview

This section provides to THE SUPPLIER the planning constraints and the scope of the requirements for the management of this project. It will allow THE SUPPLIER to quote accordingly the different Professional services.

4.2. Project Planning

R160 The availability for Customer of the Cloud SDM for 5G commercial launch in standalone architecture is expected for Q4 2021. THE SUPPLIER shall precise the nearest date of Cloud SDM delivery and other related elements in Customer .

Customer wishes finishing the swap of all legacy SDM subscribers towards Cloud SDM including the support of all existing functions (HLR/AUC, EPC-HSS, IMS-HSS, MNP, EIR, HSM) and new 5G functions (UDM, AUSF, UDR, UDSF, 5G EIR) before Q4 2023.

THE SUPPLIER may propose, describe and quote alternative solutions and steps to smoothly introduce all required 5G functions as long as Customer deadlines are respected. It will make sure that the following requirements are considered until migration is finished (to be described in SUPPLIER answer):

- Interworking and service continuity between 5G and existing networks (2G, 3G, 4G, IMS and non 3GPP) without customer impact.
- Provisioning management optimized to reach either legacy or Cloud SDM.
- Signalling (MAP/DIAMETER/HTTP) routing optimized to reach either legacy or Cloud SDM.

Compliancy

R161 Customer is interested by another scenario where the legacy front end applications (HLR/AUC, EPC-HSS, IMS-HSS, EIR) are still exclusively covered by incumbent SUPPLIER. In detail, the following steps will be considered:

1) Introduction of Cloud SDM 5G, meaning UDM, AUSF and UDR (UDSF), and integration of UDM with Legacy HSS via UDICOM interface before Q4 2021.

2) Evolution of the Legacy SDM by Incumbent SUPPLIER: Virtualization of the SDM (Cloud) front end applications (HLR/AUC, HSS, EIR and evolution to 5G EIR) before Q4 2024.

3) Migration of the 2G/3G/4G profiles from Legacy SDM to UDR and integration of Cloud front end applications (HLR, HSS, EIR) from Incumbent supplier to the UDR before Q4 2024. As a first step, the UDR data model will be extended / adapted to support 2G/3G/4G profiles and data schema of Incumbent supplier Cloud front end applications.

The SUPPLIER will detail how the interactions with HSM are managed.

For this scenario it is assumed that incumbent SUPPLIER will only quote necessary product and services related to Legacy SDM evolutions among the three steps.

Compliancy

R162 If not possible to respect the deadlines, THE SUPPLIER should propose and commit on the most optimistic project plan.

Compliancy

R163 THE SUPPLIER shall attach to this document the detailed project plan for the Cloud SDM swap of Customer network

Compliancy

4.3. Testbed

R164 THE SUPPLIERs shall provide the testbed equipment listed below free of charge:

- Data storage and network functions replicating the configuration in commercial network in terms of features/resilience/geo-redundancy configuration. Minimal processing capacity is needed for this configuration. Minimum capacity: 50k provisioned and active SIM cards.
- Provisioning gateway

Compliancy

4.4. Installation and Commissioning

R165 THE SUPPLIER shall quote all Cloud SDM Installation and Commissioning services on the basis of equipment proposed for defined network overview.

Compliancy

R166 It is a requirement of THE SUPPLIER to provide Customer with the following services for deployment of the Cloud SDM solution (see also On-boarding & Installation services requirements as part of the RFP):

- All equipment specification documentation, including rack schematics
- All installation specific documentation
- Site Surveys
- Physical installation of equipment to Customer standards
- All configuration specific documentation
- Configuration of equipment to Customer designs (HLD, LLD)
- Integration and commissioning of equipment in Customer network
- End to End Functional Testing
- Acceptance Testing
- Communication clarity between Customer and the vendor delivery team
- Forecast and delivery timescales for equipment
- Etc …

Compliancy

For Scenario #V and HSM (if applicable) where Hardware is supplied, the following requirements are expected:

R167 THE SUPPLIER will provide its requirement in terms of space availability, site access, power etc.

Compliancy

R168 It is a requirement of THE SUPPLIER to support bottom up cable management within their SDM technology.

Compliancy

R169 It is a requirement of THE SUPPLIER to state that their SDM solution incorporates suitable cable management for all inter-rack cabling so that cooling and maintenance access are not compromised.

Compliancy

R170 It is a requirement that THE SUPPLIER supports site surveys with Customer staff and possible returns to site in supporting second surveys and/or ongoing support during the deployment activities.

Compliancy

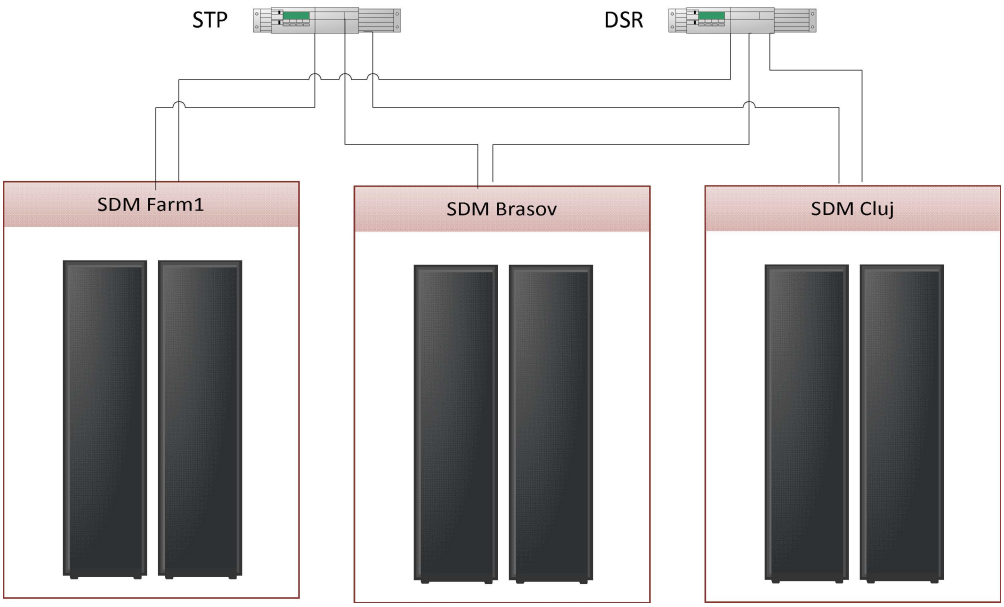
In order to provide effective asset management of both hardware and software Customer needs to identify the hardware and software build including the unique part and serial numbers of all traceable equipment to plug in unit level. This information is to be available in an electronic format and by remote access into the node or equipment.

4.5. Migration

4.5.1. Preliminary

Customer has currently 2+1 STPs and 2 DSRs in its network. All MAP Request to HLR are routed through the STPs and all DIAMETER requests to HSS are routed through the DSRs.

Routing to correct FE is performed by the STP/DSR, based on MSISDN ranges and/or IMSI ranges.



Mobile number portability feature is deployed in STPs.

At STP/DSR level, the SDM shall be defined as an independent supplementary HLR/HSS with:

- One specific GT
- One specific PC,
- Specific IMSI Ranges (XYs)
- Specific MSISDN ranges (PQs)
- One specific hostname/realm

4.5.2. Initial situation

R171 The Cloud SDM shall be considered as a new SDM in the network.

Population of new SIM & MSISDN using the SDM PQ and XY ranges shall be possible before any migration of data from legacy SDM is performed. This shall allow the usage of the SDM even if NO migration takes place.

Compliancy

4.5.3. Migration of full subscribers base

R172 THE SUPPLIER shall be responsible for SDM subscriber migration process and implementation. The SDM subscriber migration services shall be included in the solution quotation. The service quotation shall include all tools, resources and any adaptation or changes necessary for complete implementation of the process.

Compliancy

R173 THE SUPPLIER shall manage dumping of subscriber data from legacy SDM, map the binary output into its data base schema. Customer role will be to facilitate getting the

subscribers binary dump, all steps later to have the subscribers working on the new solution are responsibility of THE SUPPLIER.

Compliancy

R174 Migrations shall be performed by night in maintenance windows (12:00 to 06:00 AM).

Compliancy

R175 A period of observation of 4 weeks shall be observed after the original SDM is migrated. Eventual Fall-back is done by provisioning system to old XY & PQ. Potential data already populated on the SDM have to be properly cleaned-up.

Compliancy

Q123 THE SUPPLIER will describe in detail the proposed migration procedure (network routing, data repository copying,) and provide an indicative planning. THE SUPPLIER shall describe the expected impact of this procedure (e.g. loc update side effect…). Also a fall-back procedure must be described in detail. THE SUPPLIER will split the migration procedure into two parts:

- Migration of mobile HLR, EPC-HSS, IMS-HSS subscribers
- Migration of fixed IMS-HSS subscribers

This is needed in case Customer will decide to migrate independently the fixed and mobile subscribers.

Answer

R176 Customer will decide the granularity of ranges of subscribers (e.g. number of subscribers, IMSI ranges and number of IMSI ranges, MSISDN ranges and number of MSISDN ranges) that will be migrated in one night.

Compliancy

4.5.4. Migration experience

R177 For the solution proposed, THE SUPPLIER shall describe experience in deploying such solution in other networks.

Compliancy

4.6. Technical support

R178 On-site technical support for babysitting of the Cloud SDM platform shall be provided after live traffic launch of the Cloud SDM and after the different migrations steps. This technical support will stop 4 weeks after the end of migration.

Compliancy

4.7. Training

R179 THE SUPPLIER shall quote the training services for each network element proposed for Cloud SDM domain.

The trainings shall cover the following category:

- Technical Overview
- Network Design
- I&C & 1st maintenance level
- 2nd Maintenance Level

Compliancy

R180 THE SUPPLIER will provide the list of training courses, based on the requirements mentioned above.

Compliancy

R181 THE SUPPLIER will provide the overall training period.

Compliancy

R182 The training shall be carried out in Customer and shall be provided in 2 sessions of 10 persons.

Compliancy

R183 THE SUPPLIER is invited to detail in an Annex the cost of each training session.

Compliancy

4.8. Maintenance

4.8.1. Technical Support Services

R184 THE SUPPLIER shall quote the Fault Report Handling service for all SDM related equipment on the basis of equipment proposed for defined network overview and per quarter. Service Level GOLD will be taken into account for this quotation.

Compliancy

R185 THE SUPPLIER shall quote the Software and Hardware Update Services for all SDM related equipment on the basis of equipment proposed for defined network overview and per quarter/year.

Compliancy

4.8.2. Hardware Services

R186 THE SUPPLIERs is requested to quote Repair/Replacement Services for all SDM related equipment on the basis of equipment proposed for defined network overview and per quarter within the following TAT Customer require Option 1 as preference

- Option 1 : 30 calendar days
- Option 2 : 45 calendar days
- Option 3 : 60 calendar days

This includes time for incoming logistic.

Compliancy

R187 Spare Part Management Services (SPMS) enable Customer affiliate or 3rd party entity to access spare parts 24 hours / 7 days a week / 365 days a year.

If the service is available, THE SUPPLIER is requested to deliver spare part to site where the Replaceable Unit is needed, agreed hand-over point, or agreed drop-off point with courier services within following delivery time:
THE SUPPLIERs is requested to quote SPMS service with the following TAT:

- Option 1 : 4 hours
- Option 2 : 24 hours

Compliancy

4.9. Software upgrades

R188 THE SUPPLIER is requested to quote annual fee for all SDM related equipment on the basis of equipment proposed for defined network independent on the amount of software update/upgrade. It will cover both pre-production and production environment. Moreover, THE SUPPLIER will take into account for their planning and for quotation, the requirements of one engineer either on-site or in supervision centre, full time for each software upgrade.

Compliancy

Q124 THE SUPPLIER shall specify the average roll-out duration for one site and indicate if the roll-out will be done on the roll-out site or remotely.

Answer

Q125 THE SUPPLIER shall specify if a node re-start is necessary during software rollout, causing loss of service.

Answer

Q126 THE SUPPLIER shall specify whether redundancy/resilience is compromised during software rollout. If so, detail how it is compromised, and any steps that will be taken to mitigate risk.

Answer

Q127 THE SUPPLIER shall specify how a “roll back” will be performed in the event of an unsuccessful upgrade.

Answer

4.10. Documentation

Q128 THE SUPPLIER will describe the list of technical documentation of their product made available to Customer . Examples of these include but are not limited to: interface specifications, standard compliance statements, alarm codes for the various interfaces, functionality of specific features, provisioning commands handling, etc.

Answer

R189 It is a requirement of THE SUPPLIER to supply a complete set of standard technical documents at least 4 weeks prior to the start of Installation and Commissioning of the platform.

This set of documents shall include (but not be limited to – see also On-boarding & Installation documentation requirements as part of the RFP):

- Hardware qualifications documentation
- Environmental characteristics documentation
- Functional and sizing specifications
- Product specifications
- Technical requirement specifications
- Configuration templates and guidelines
- SOC, Statements of Compliance with all 3GPP and other if applicable (e.g. ITU) standards relevant for the node
- Full set of Customer Documentation and User Guides
- Supplier test plans for all features and hardware selected for test by Customer in the final project scope of work (including test data sheets, test cases, test results and problem data sheets)
- Acceptance test sheets for each deliverable, vendor provides a list of potential restrictions and problems
- Platform configuration and software release notes

Compliancy

4.11. Project commitments

This section describes the generic project control organisation and working practices that should be adopted during the project.

R190 It is a requirement of THE SUPPLIER to support regular face to face meetings at each of the following levels and that the frequency of these meetings be held at least every 2 weeks at the following levels:

- Contract Review Meeting (CRM)
- Local Contract Steering Group (CSG)
- Technical Working Group (TWG)
- Operations Working Group (OWG)
- Deployment Working Group (DWG)

Compliancy

R191 THE SUPPLIER is required to provide staff based in an office local to Customer premises to allow additional ad-hoc meetings, technical discussions and workshops to take place as required.

Compliancy

R192 It is a requirement of THE SUPPLIER to have a local presence in , all along the project but also after in a permanent mode, to support a high level of engagement with Customer program team.

Compliancy

R193 It is a requirement of THE SUPPLIER to provide regular weekly written progress reports covering:

- Installation and commissioning status
- Testing & Acceptance status
- Migration status
- Software delivery status
- Product roadmap updates

Compliancy

5. Pricing

R194 THE SUPPLIER shall provide detailed quotation by filling the Buyin template, included with this RFQ.

If different SDM configurations or products are proposed to Customer , THE SUPPLIER will give several quotations.

Compliancy

The Supplier will quote as optional the following specific items

Coherence check tool: details in paragraph 1.4 in “SDM_Provisioning.doc” document. The Supplier will quote the development of an application or web interface able to perform the same function.

Intermediate provisioning layer: details paragraph 1.10 in “SDM_Provisioning.doc” document. The Supplier will provide the quotation of a mediation gateway able to interface its SDM system and Customer provisioning system.

Any specific development required to full-fill Customer interoperability, integration in Customer environment and functional requirements.