Syniverse is the world's most connected company, revolutionizing how businesses connect, engage, and communicate with their customers. For decades, Syniverse has delivered innovative software and services that has transformed the experiences of its clients. Our secure global network reaches almost every person and device on Earth. Our communications platform is industry-recognized as the best of its kind. And each year, we process over $35 billion in transactions, revolutionizing how goods and services are exchanged. We are proud to be the most recognizable brands—nearly every mobile communications provider, the largest global banks, the world's biggest tech companies, and thousands more—rely on us to shape their future.

Syniverse has a long history of providing SIM and IMSI-based services ensuring humans and machines properly and efficiently communicate anywhere on the planet. These services can require the use and the provisioning of IMSIs via Over-the-Air (OTA) methods. Our management and delivery of these services affords customers flexibility to provision their solutions via physical SIMs running embedded applets and via eSIMs. Thus, Syniverse has a strong familiarity with the use of Subscriber Manager – Data Prep (SM-DP) and Subscriber Manager – Secure Routing (SM-SR) tools and associated platforms. Further, our global relationships to cellular operators and IoT service providers, offers an understanding for how these services must be applied for successful use.

Syniverse is honored to provide initial submission to TRAI's Consultation paper. We would be further honored to continue detailed discussion, offer commentary and further inputs as TRAI begin to formulate commercial and operational policy around this subject.

Thank you.

(c) Syniverse Technologies
syniverse.com

Q1. Whether the TRAI recommended timeline, about the foreign eUICC fitted devices to be on roaming with Indian TSP's network for a maximum period of three years only, needs a review? If yes, what should be the timeline after which the eUICC should mandatorily be configured with Indian TSP's profile?

Answer : Yes. Every partner in the ecosystem has different business needs, views and customer deliverables. While the stated three-year period is a starting point, it should be reviewed, possibly in favor of no stated period. TSPs should be permitted to review and set their rules based on their actual business case for services launched and supported in India. This approach would permit market forces to define the period policy and create a healthier competitive environment.

Q2. Whether there is a need to change the controlling SM-SR from foreign TSP to Indian TSP in case of foreign eUICC fitted devices operating in India? If yes, what should be the methodology and time period within which it should be done?

Answer: No. Firstly, the SM-SR is the critical interface point for communication between eUICC and SM-DP, and a key component for the provisioning and ongoing service management of eUICC-fitted device routing. From a business perspective, generally, the business responsible for the delivery and performance of the eUICC-fitted device would want to retain control of the SM-SR function and not be forced to change or swap it to a new TSP. Secondly, a number of IoT use cases (and devices) are dynamic in nature. Change of the controlling SM-SR in cases where the device moves from one geography is not a current policy for global IoT services and not advocated.

Q3. Whether there is a need for the SM-SR of each TSP to be integrated with the SM-DP of each other TSP? If yes, what should be the methodology for integration? Please specify the timelines also.

Answer: No. For business reasons and, if not a special case, the SM-SR and an associated SM-DP is typically owned and operated by the provider TSP. As in Question 2, the business has a vested interest in the end-to-end success of service delivery and would not readily seed control of key delivery elements. Further, while requested here, integrated or interconnected SM-DPs might prove challenging without carefully pre-defined rules or standards for interconnecting, storing data, moving data, securing data, etc. Such standards must identify a secure and reliable method for communications like the use of IPX networks and associated standards for the handling of roaming traffic and settlement/clearing records.

Q4. Whether there is a need to prescribe SM-SR swapping among the Indian TSPs? If yes, what should be the modalities and procedure for such swap?

Answer: No. The owner of the SM-SR will commonly be the initial provider TSP and is responsible for the successful deployment of the eUICC-fitted device solution. While the swapping concept presented here might potentially encourage competition and offer a level of redundant services, from a business perspective, seeding control to another business entity would introduce risk to the overall performance of service to the customer.

Q5. Whether the profile switchover, from one TSP to another, is driven by the user or OEM?

If yes, what methods can be deployed to execute such switchover?

Answer: From a technical perspective, profile switchover can consider and possibly apply an Over-the-Air (OTA) process like known and proven IMSI profile switching. However, in the end it largely depends on how the terms of service and business relationship are defined in any service agreement between the initial TSP and the OEM and the user. An agreement permitting a profile switch to another TSP, whether initiated by the OEM or a user, must also be aligned to technical abilities, clear methodology and legal relationships between the parties.

Q6. Whether non-TSP entities, such as OEMs and M2M Service Providers, should be permitted to own SM-SR and manage the subscribed profiles for their devices? If yes, what should be methodology and procedure?

Answer: Technically, the SM-SR (e.g. the platform) is owned by the TSP and it can be considered a necessary conduit for service. However, the ownership of the profile and the associated management of that profile is with the OEM or M2M Service Provider. Service agreements signed between the TSP and OEM/M2M Service Provider could offer clear policy to differentiate ownership, management and service delivery of subscribed profiles. Associated charging models would be based on task.

Q7. Whether the use of ITU allocated shared Mobile Country Code 901.XX (Global IMSI) be permitted in India for M2M Communication? If yes, what should be the methodology and procedure? If not, what are the reasons and challenges in implementation of Global IMSI? Please elaborate.

Answer: Yes. The 901.xx range is assigned by ITU specially for global IoT services. In future, the IoT devices and services will be dynamic in nature, agnostic to geographical boundaries. The use of 901 IMSIs requires a direct relationship with a TSP to support IMSI access via IR.21. In our opinion, a range of 901 IMSIs may be permitted by the TSP but also restricted in their use based on a negotiated relationship with M2M providers. This restriction, for example, could be to permit permanent roaming while used in India – with no roaming permitted outside India.

Q8. Is there any issue, pertaining to the Consumer eSIM, that needs to be addressed? Please highlight the issue and suggest mechanism to address it with justification.

Answer: No. The solution choice of eUICC (OTA) deployment or consumer-driven deployment is one of use case. Functionally, they are provisioned and governed in a similar manner.

Q9. Give your comments on any related matter that is not covered in this Consultation Paper.

Answer: No further comments at this time.