

**CONSUMER PROTECTION ASSOCIATION  
HIMMATNAGAR  
DIST. : SABARKANTHA  
GUJARAT**



**Comments  
On  
Embedded SIM for M2M Communications**

**INTRODUCTION :**

IoT generally, and M2M more specifically, are inherently global business and operations models which require norms, standards and regulatory policies that reflect this unique requirement. In particular, policies must recognize and facilitate cross border data flows and permanent M2M roaming and should not impose norms which are at variance with international best practices. Global best practices should be considered to undermine development with regards to proliferation, operational aspects, and investment opportunities where the M2M and IoT sectors are concerned.

TRAI should have a longstanding approach to encouraging innovators in new technologies, while taking steps to address policy matters. The authority and DoT should approach emerging market trends and technologies with restraint and an eye toward allowing new entrants room to experiment and mature before they encounter significant government intervention.

## ISSUES FOR CONSULTATION :

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?

Comments : Yes.

The timeline about the foreign eUICC fitted devices to be on roaming with Indian TSP's network should be maximum period of 6 months to 12 months.

1. All IoT device manufacturers need a global connectivity solution. The choice comes down to a provider who can ensure data connection across the globe. Currently, cellular technology ticks all the boxes because of its maturity and being the only solution that is both mobile and global.
2. A list of countries with the strictest permanent roaming restrictions:
  - **Brazil** – Permanent roaming is prohibited and the local carriers need to make sure that there are no such devices connected to their networks.
  - **The US and Canada** – No official regulations, but MNOs usually want to prevent permanent roaming by implementing strict restrictions on incoming roaming connections.
  - **India** – Obligation to comply with local Know Your Customer rules in addition to general permanent roaming restrictions.

- **Turkey** – Using roaming services on the same device for over 120 days is prohibited.
- **Middle East** – No official regulations, but the connection services must be provided by a licensed local operator.
- **China** – Permanent roaming is prohibited and companies need a license to provide communication services in China.
- **Australia** – No official regulations, but MNOs prohibit using roaming services for over 6 months.

3. Enable permanent roaming at a wholesale level for IoT application providers:

For the new generation of industrial mobile applications based on country wide roaming for certain vertical sectors (e.g. car industry, aerospace, logistics, etc) the specialized service providers need long term wholesale access. Effectively that requires permanent roaming agreements, usually at wholesale level.

4. **Permanent Roaming for Machine-to-Machine Communications – *BEREC Study***:

MNOs and specialized MVNOs are keen on opening the M2M market segment for major Indian vertical industrial users (e.g. automotive, aerospace, logistics, etc). M2M traffic is typically of low data volume, dominated by signaling for process or machine states. This is likely to demand highly reliable infrastructure, with high quality, and perhaps low and standardized latency.

BEREC (2016) assessed permanent roaming in relation to the IoT and specifically for M2M and found that a majority of MNOs do not apply specific prices or conditions for M2M traffic at a wholesale level, i.e. the IoT segment is treated much the same as all other data in wholesale

contract financial conditions. Some MNOs expressed their concerns to BEREC that since national networks were dimensioned for domestic SIM cards, a large increase in foreign SIM cards for M2M, on a permanent basis, might produce capacity problems with possible network congestion in visited networks without a fair use policy (FUP). However, whether this is a real issue is open to question because, typically, M2M networks exploit low volume, burst data communications for signaling, rarely measured in GB per session, but perhaps low Roaming: One Year After Implementation PE 626.090 23 kb per signal, for commands or monitoring messages often at slow speed (kbps to Mbps range). Hence, only a small minority of MNOs have special conditions and rates for M2M traffic, e.g. exclusion from discounts. Interestingly, no MNOs with M2M agreements were found to employ an exclusivity of carriage clause for their network, perhaps because that may not be favorable to the M2M segment. Such applications need to select the best network available at any given time (BEREC, 2016). The reliability and mean time before failure (MTBF)/mean time to repair (MTTR) of commercial mobile cellular networks do not always meet the requirements of M2M users and so multiple MNOs are preferred, for failover.

### **Constraints for Permanent Roaming :**

According to BEREC in its March 2018 report, the majority of responding MNOs had not yet implemented any measures to discourage permanent roaming in their wholesale roaming agreements as fair use policies (FUPs) were ignored. Some explained it as unnecessary, as all usage was charged for. Others even encourage usage through volume or revenue commitments. Only about 20% of responding MNOs had some kind of mechanism in their wholesale roaming agreement to discourage permanent roaming. Also, certain MNOs, may exclude permanent roaming from discounts. Mobile originated calls to countries outside the

EEA are excluded from discount rates. This is a concern for large business users that try to negotiate wholesale deals (Beltug, 2018). In essence, the difference between discounted and non-discounted wholesale rates has emerged as a key element for MNOs to control permanent roaming. On wholesale resale of capacity, a majority of the MNOs responding to BEREC surveys had not yet implemented measures to discourage permanent wholesale roaming by their MVNO and reseller customers (rather than consumer and business users). Some MNOs did not feel the necessity, as all is charged for. Other MNOs actually encourage wholesaler traffic, via volume commitments and revenue commitments in wholesaler contracts. Few MNOs replied with explicit consumption limits.

5. Considering the unpredictable data volume, varieties, and usage patterns of IoT devices, it is quite clear that IoT data roaming is very different from consumer roaming in that the management of data traffic is crucial and connectivity is essential to be able to monitor, measure and monetize the traffic.

**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?**

**Comments :**

1. Cellular connectivity for IoT projects has until today been provided by operators and mobile virtual network operators. There will be a significant increase in the number of players who support this sector over the next five years, with many needing specialist support in areas such as device, routing and application management. These new players will include enterprises seeking to

control and provide consistent service across large global deployments. Automotive is expected to lead the charge, followed by global enterprises in several other sectors, who will each have extremely diverse requirements and service needs.

2. Whether enterprise or operator, these new players in the IoT roaming space are likely to adopt a mobile virtual network operator-like model so that they can cut time to market and lower upfront capital investment: crucial for IoT traction and success. A service provider that can provide reliable global cellular connectivity in an agile manner, giving them autonomy and control, is an essential partner for their success.
3. Many IoT networks will deploy IoT-devices that will cross countries' borders. For this reason, roaming and roaming steering is absolutely crucial, as the price for data is a massive cost factor, especially for large-scale environments with hundreds or thousands of IoT-enabled devices.
4. Highly reliable, secure virtualized network infrastructure that supports dynamic, multi-country service provisioning, alongside the ability to offer flexible pricing models.
5. The IoT at scale business model is fundamentally dependent on ROI, which is enhanced by eliminating complexity, increasing operational insights or cross-/upselling services. Cellular connectivity and roaming service providers addressing this market must be able to provide reduced complexity at lower costs, and transparent business models to enterprises. Whether it is a price per-unit, a flat rate or local breakout, there is a range of business models that can be used and tailored to meet specific business requirements.

**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.**

**Comments :**

A sustainable and easy-to-use IoT roaming business model is a prerequisite for the success of large global IoT deployments, and we can expect significant innovation in business models, value-added services and more in the coming years. By partnering with an IoT roaming specialist like BICS, both operators and enterprises can reap the benefits of transparency in pricing, wholesale business models and advanced analytics tools.

**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?**

**Comments :** No Comments.

**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?**

**Comments :** No Comments.

**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?**

**Comments :** No Comments.

**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.**

**Comments :** No Comments.

**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.**

**Comments :**

1. There should be highly reliable, secure virtualized network infrastructure that supports dynamic, multi-country service provisioning, alongside the ability to offer flexible pricing models.
2. The Internet of Things (IoT) is growing exponentially, but security for IoT projects and deployments remains an obstacle. One fundamental IoT security component is making sure devices and services have trusted identities that can interact within secure ecosystems.
3. Simple certificates cannot address the multiple levels of authorizations, roles, and information these complex environments need.
4. eSIM, being integrated into the device itself, can cause some serious privacy issues when used in consumer mobile devices. The end-user is left with complete control of the device with the manufacturer and the service providers. Automatic configuration and updating can cause an infringement of privacy and security of the devices as well as users. The



privacy and security of IoT devices with eSIM cannot be guaranteed until the specification is universally adopted all around the world.

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

**Comments :**                      **No comments.**

**Yours faithfully,**

**( Dr. Kashyapnth )  
President**