Comments from IDEMIA, on Consultation Paper on the Issues Related to Critical Services in the M2M Sector, and Transfer of Ownership of M2M SIMs

Chapter	Questions		Remarks on Questions	Additional Remarks
	Q1	Whether there is a need for a broad guiding framework for defining a service as critical M2M/ IoT service? If yes, what should be the guiding framework? Please provide a detailed response with justifications.	**Guiding framework for Endpoint Security -** 1. M2M device - Security Assurance requirement based on "TEC TR Security by Design for IoT/M2M manufacturers" Implementation. 2. Security certified devices based on DoT NCCS ITSAR for respective equipment. 3. SIM/eSIM - MTCTE certificate based on TEC ER and Security Certificate using DoT NCCS UICC and eUICC ITSAR **Connectivity Platform -** 1. Compliance with OneM2M standards 2. OTA Services to for MNO/TSP profile assets shall be controlled under TSP/MNO and audited by Regulatory. 3. eSIM RSP platform certified with GSMA SAS and shall be under Trusted framework 4. Certified Physical and logical security **M2MSP -** Reseller of TSPs IMSI and consuming the TSP network to provide the critical services, must be under the same category of Licensee.	We should be sensitive to the evolution of M2M/IoT which is likely to impact every domain and shall be omni-directionally inclusive & intrusive in every sphere of Human, Machine, Industry, Services, Utilities, Agriculture, Energy, Mobility etc. Hence, with the consideration and view, our objective should be to ask the question contrarily; **Which are the M2M/IoT services which can be accredited as NON-CRITICAL?** With high acceleration and penetration of M2M/IoT, it is likely to intrude into every aspect of human and objects and possibly will become the critical back bone of any individual, object, industry, machine or service with cross geographical cyber impacts; few examples are; Metering, Automotive, Health, Energy, Infrastructure, ITMS (Smart City), Any Nationally Critical Systems, Home Automation Manufacturing 4.0, Access Control and many more The technological advancement and peripheral use cases will continue to attract implementations and adaptations, therefore the focus should be to regulate, standardise and securitise it from the beginning and continue to innovate and upgrade such measures to

Chapter 2 Page 17	**Q2**	Through the recommendation No. 5.1(g) of the TRAI's recommendations on 'Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications' dated 05.09.2017, TRAI had recommended that critical services in the M2M sector should be mandated to be provided only by connectivity providers using licensed spectrum. Whether this recommendation requires a review? Specifically, whether critical services in the M2M sector should be permitted to be provided by using unlicensed spectrum as well? Please provide a detailed response with justifications.	Agreeing with TRAI recommendation and even the services under unlicensed should be also in same category. The vulnerability in unlicensed network can penetrate the licensed network and vice versa, which may cause a security challenge too . if unlicensed network can not be under licensed framework then below should be implemented 1. Regulatory has to create guidelines and protocols to connect two or more captive network without accessing public network. 2. if they access the public network then Gateway and firewall shall be certified by recognized agencies may be STQC	Basis above submission, it is highly recommended that not only critical components/ products/ services, but even M2MSP framework itself should be Regulated through License and Trusted ecosystem. Beside we agree with TRAI recommendation ..... That all services should be based on licensed spectrum, but may be allowed to rely on CNPN based models for captive or non critical use cases, which will still be relying on licensed spectrum and regulated entities with vigilant and secure implementation design and architecture.
	Q3	Whether there is a need to bring M2M devices under the Trusted Source/ Trusted Product framework? If yes, which of the following devices should be brought under the Trusted Source/ Trusted Product framework: (a) All M2M devices to be used in India; or (b) All M2M devices to be used for critical IoT/ M2M services in India; or (c) Any other (please specify)? Please provide a detailed response with justifications.	M2M SP, Products and Services as well as all M2M devices must be under Trusted Source. The devices used in critical places are required to securitize (a) All M2M devices under Level 3 of security Assurance as defined in "TEC TR Security by Design for IoT/M2M manufacturer". Need to initiate the the certificate scheme based on "TEC TR "Security by Design for IoT/M2M manufacturers" for the IoT/M2M device for their Security Assurance Level.	Although there are captive environments available, but as per our understanding there is no standardised scheme, currently available in India, to certify the devices for their use cases, neither for critical services nor for non-critical services. Therefore, this is required to initiate the certificate scheme for the IoT/M2M devices based on TEC TR "Security by design for IoT/M2M manufacturers"

	Q4	Whether there is a need for establishing a regulatory framework for the transfer of ownership of M2M SIMs among M2MSPs? If yes,- (a) What should be the saliant features of such a framework? (b) In which scenarios, the transfer of ownership of M2M SIMs should be permitted? (c) What measures should be taken to avoid any misuse of this facility? (d) What flexibility should be given to the new M2MSP for providing connectivity to the existing customers? Please provide a detailed response with justifications.	Yes (It should be mandated) (a)(c) As the licensees TSP/MNO having the framework for Transfer ownership. (b) At the time OEM sold/ handover to other the custodian digital KYC this is should be done by OEM with M2M SP. (d) For the ease of business some Tax benefit up to 3 yrs. for sure they should be under licenses category and under Trusted framework	M2MSP and entire ecosystem relying on connected and cyber layers should be under Trusted and Security compliant environment. A Trusted & localised value chain wiill not only help economic acceleration through manufacturing and skill development, employment generation but will greatly contribute towards a better Privacy and Security by design. In our opinion, M2m/IoT should be not only under Trusted but also requires a licensed (not registered) category with robust regulations and standardisation., which may address all relevant concerns related to security and trust.
	Q5	Whether there are any other relevant issues relating to M2M/ IoT services sector which require to be addressed at this stage? Please provide a detailed response with justifications.	1. Cyber security compliance to ETST EN 303 645 2. In Automotive Cyber security implementation ISO 21434 Except for Device Firmware updates (through Trusted mechanism only) any other OTA or Remote Subscription management should be either managed by Licensed TSP or Specific Service Provider for such services, for which the framework may be defined	1. M2MSP should be under licensee category 2. M2MSP should be under Trusted framework 3. OTA services shall be under control of TSP/MNO if it is under third party or with M2MSP, shall be regulated and audited by authority. 4. RSP platform should be GSMA SAS SM certified 5. SIM/eSIM manufactures should follow SIM SOP and UICC and eUICC ITSAR compliance and MTCTE certified. 6. Unlicensed network should be under licensed category or required to create security guidelines for the connectivity between captive networks and certified Gateway Firewall framework in case captive network land in public network

Chapter 3 Page 37	**Q1**	Whether there is a need for a broad guiding framework for defining a service as critical M2M/ IoT service? If yes, what should be the guiding framework? Please provide a detailed response with justifications.	(1) M2MSP be kept under licensee as TSP and MNO (2) TSP/MNO , Owner of IMSI , should be responsible for misusage of it the data generated for corresponding to these Assets (IMSI).	
	Q2	Through the recommendation No. 5.1(g) of the TRAI's recommendations on 'Spectrum, Roaming and QoS related requirements in Machine-to-Machine (M2M) Communications' dated 05.09.2017, TRAI had recommended that critical services in the M2M sector should be mandated to be provided only by connectivity providers using licensed spectrum. Whether this recommendation requires a review? Specifically, whether critical services in the M2M sector should be permitted to be provided by using unlicensed spectrum as well? Please provide a detailed response with justifications.	As the connectivity penetration is increases rapidly , M2M services can not be limited to critical and non critical services. That's the reason M2M should be under licensees category and also in trusted framework.	
	Q3	Whether there is a need to bring M2M devices under the Trusted Source/ Trusted Product framework? If yes, which of the following devices should be brought under the Trusted Source/ Trusted Product framework: (a) All M2M devices to be used in India; or (b) All M2M devices to be used for critical IoT/ M2M services in India; or (c) Any other (please specify)? Please provide a detailed response with justifications.	Same as Q3 of chapter 2 (see above)	

	Q4	Whether there is a need for establishing a regulatory framework for the transfer of ownership of M2M SIMs among M2MSPs? If yes,- (a) What should be the saliant features of such a framework? (b) In which scenarios, the transfer of ownership of M2M SIMs should be permitted? (c) What measures should be taken to avoid any misuse of this facility? (d) What flexibility should be given to a new M2MSP for providing connectivity to the existing customers?	Same as Q4 of chapter 2 (see above)	
	Q5	Whether there are any other relevant issues relating to M2M/ IoT services sector which require to be addressed at this stage? Please provide a detailed response with justifications.	Same as Q5 in chapter 2	