



M2M Device Guide

22 July 2015

Device development

M2M and the Internet of Things promote the introduction of a wide range of device designs. You may choose to use semiconductor devices deeply embedded in a custom design, or adopt pre-fabricated modules from specialist vendors to alleviate the complexity of design and development. To reduce problematic behaviour on our mobile network, we've assessed a range of these prefabricated modules and maintain a list of preferred solutions.

If you choose to pursue highly custom development, we'll seek to understand the proposed network activity prior to commercial contract, and will recommend testing with an accredited facility before market launch.

Considerations around device behaviour

M2M devices can be problematic because they're often programmed *once* to run forever, without user intervention. A wireless network may deny a service request for any number of reasons, including:

- the network is under maintenance
- the SIM is blocked because the user hasn't paid the bill
- certain network nodes are overwhelmed with service requests
- the user hasn't subscribed for a particular service

When a service request is denied, the device doesn't analyse *why*. Instead, it continues retrying. This behaviour could cause multi-dimensional issues on the network, in terms of capacity, performance, outages, and processing. This ultimately impacts your application performance. Aggressive behaviour can occur when the service request is made or after service is granted. Typical examples include:

Before service begins:

- a device which is GSM-barred on the network is trying to perform GSM registration
- a device which is GPRS-barred on the network is trying to attach to GPRS data service
- a device is in a barred location of the network trying to perform GSM or GPRS registration
- a device is trying to register to a wireless network against the recommended PLMN order on the SIM

After service begins:

- a device that sets up and tears down a session very frequently
- synchronized activity – a large number of devices programmed to generate traffic at the same time.
- devices that send bursts of MO SMS in a short period of time
- short, uneven bursts of IP traffic
- the device application is trying to steer the traffic against the network preference

Other considerations associated with device behaviour include:

- device wake-up procedures to initiate information transfer
- ability to process SMS queues, given that mobile networks (and potentially spammers) also use this service to provide updates and notifications
- power down scenarios and procedures to ensure a clean network and device state

We recommend you consider these scenarios when designing your device – optimising its performance and avoiding problems once deployed.

Working with SIM products

We commission and test SIM cards to meet the requirements of our customers. With the rise of Machine-to-Machine (M2M) devices and applications, SIM card requirements have become increasingly demanding. By working closely with our SIM vendors, we're able to provide SIM cards to meet these demands and comply with the following GSMA and 3GPP Release 8 standards:

- 3GPP TS 03.48 v8.9.0
- 3GPP TS 31.103 V8.6.0
- 3GPP TS 51.011 V4.15.0
- 3GPP TS 31.102 V8.17.0
- 3GPP TS 33.220 V8.9.0

To ensure your devices operate correctly, we require that they comply with interfaces and procedures contained within the above when interacting with EE SIM cards.

It's your responsibility to ensure SIM cards are used in accordance with the manufacturer guidelines and that devices operate correctly with the services provided by EE.

For further information contact our sales team on **0800 079 0873** or emailing **m2m@ee.co.uk**.