Template RFP for IoT Connectivity

Developed by
Beecham Research for the IoT M2M Council
Updated September 2020

Template RFP for IoT Connectivity

There has been an explosion of IoT software platforms and IoT Connectivity types on the market which has created confusion in the marketplace for enterprise users and OEMs. Buyers are looking for hands-on tools to help in procurement. A recent IoT M2M Council (IMC) survey of over 100 IoT buyers shows that...

- **100% of IoT buyers would find template RFP documents useful in their procurement process.**
- **83% of buyers would find 3rd-party reports of vendor compliance (to those RFPs) useful.**

In answer to this market need, the IMC has developed this template RFP for IoT Connectivity which goes together with RFP Connectivity Guidelines and the template RFP for IoT software platforms. The RFP Connectivity Guidelines indicate which connectivity types are recommended for 80+ different use cases across 9 different sectors – Buildings, Consumer & Home, Energy, Health & Life Science, Industrial & Agriculture, Retail, Security & Public Safety, Smart City, Transportation & Logistics.

About the IoT M2M Council

The IMC is the largest and fastest-growing trade organization in the IoT/M2M sector, with over 25,000 OEMs, enterprise users, and apps developers as members, and an average of 300 new members joining weekly. The IMC brings a new approach – it will increase deployments of IoT/M2M solutions by proving the business case of the technology to those that would adopt it. It will stand for connectivity as its own global industry, and will not see IoT/M2M technology through the narrow lens of technical standards or a single vertical industry. For more information, please visit www.iotm2mcouncil.org.

Beecham Research

Beecham Research is a leading market analyst and consulting firm that has specialized in the development of the rapidly-growing M2M/IoT market worldwide for the last 16 years, since 2001. Based in London UK, and in Boston US, we are internationally recognized as thought leaders in this market and have deep knowledge of the market dynamics at every level in the value chain. We are experts in M2M/IoT services, platforms and IoT solution security. Our clients come from right across the value chain, from components through to connectivity, gateway and platform suppliers, system integrators, service providers and with an increasing focus on enterprise users in all major sectors. For more information, please visit www.beechamresearch.com

Contents

Confidentiality Notice

In Sections 1.0 and 2.0 an adopter/potential adopter (<u>'The Company'</u>) is describing their business. Although much of the information offered is in the public domain, some concerns strategy and specific plans relating to the RFP. With this in mind, a statement along the lines of the following should precede the RFP…

<u>This document is confidential to *The Company* and may be used only by organisations responding to this Request for Proposal</u>

Information provided in this document, its annexes and/or enclosed are the proprietary of <u>*The Company*</u> and must not, at any time and/or under any circumstanced, be disclosed, imbedded, transmitted, used in any shape or form without written permission from <u>*The Company*</u> or its designated authority and only for the purpose it is intended for.

This document (which is designated as an RFP – Request for Proposal) illustrates the business and technical requirement for the supply, delivery, installation and commissioning of goods and/or services required for the purpose described below, and it DOES NOT in any shape or form replace <u>*The Company*</u> purchasing contract which the bidder must comply to at all the times.

1.0 Executive Summary

1.1 Company Background

Who are we? What business are we in? How are we doing?

Description of business operations

- Products and services offered
- Markets served.
- Financial profile:
  - Reference published reports for last FY
  - Trend financials over past 5 years
  - Number of employees
- Geographic reach
- Company vison/Mission Statement

1.2 Summary of Requirements

Why are we looking for an IoT connectivity service?

- Outline of Short and Long term strategy
- How strategy fits with this project and issuing of RFP
  - Develop new revenue streams
  - Control and reduce costs (Operational, manufacturing, development)
  - Asset management
  - Part of an existing product or service development
  - Enhancement to existing product/service

What is the nature of our project?

- Description of project referencing 'Why?'
- Expected outcomes from implementation of this project
- Expected timescales

1.3 Expectations from this RFP

How will we go about this project? (Information needed from suppliers, evaluation criteria, award of contract criteria)

We are inviting potential suppliers to respond to this RFP, proposing an IoT connectivity solution. The evaluation of suppliers will be based on:

- The IMC validation process *(should we include this?...any/all of following?)*
- Case studies of relevant applications
- Geographic reach of the service
- Demonstrable track record of integrating customer specific software and working with 3rd party OEMs
- Pricing options for different levels of service

1.4 RFP Criteria and Timescales

Award of Contract criteria:

- As detailed in 6.0 'Selection Criteria'
- Compliance with timescales
- Post implementation flexibility to respond to changes in requirements
- Total contract price

When? Selection process timescales and deadlines.

List of Key contacts:

Name	Job Title	Contact Details

2.0 Statement of Purpose

2.1 Objective of the RFP

- Expected outcomes resulting from the response to the RFP
- How these relate to strategic objectives

2.2 Business Case Supporting this RFP

- Level of support for this project (Board, C-Level, Result of M&A activity, External Investor etc.)
- Operational support
- Cost and Schedule confidence levels (Budget Approval)
- KPIs of supporting Business Case
    - ○ ROI, NPV of investment
    - ○ Market share targets
    - ○ Revenue per customer/revenue per unit sale

2.3 Schedule of Service Rollout

- By Geography
- By Country
- By Product/Service type

2.4 Forecasts

- Markets to be served
- Market forecasts underpinning the business case.
- Effect of variations in market forecasts on business case.

2.5 Technical Requirements

- Type of project; e.g. Monitoring, Command & Control, Data Acquisition, Asset Tracking etc.
- Project consultancy
- Expectations of connectivity type; e.g Wifi, Cellular, fixed, LPWA, Satellite.
- Application requirements, e.g. Data rate required by application, expected data volumes required by application latency, in-building penetration, autonomy when battery powered, mobility etc.
- Market specific hardware interface requirements – depending on technology choice.

2.6 Device Connectivity details

With reference to the IMC Connectivity Guidelines.

These questions will help determine the range of devices required to be connected. There may be only one type with a single set of requirements for data rate, latency and cost for example. Or there may be more than one type of device to be connected, consequently more than one set of connectivity requirement.

- Standard SIM or eSIM for cellular connectivity
- Low Power (NBIoT) SIM, cellular.
- Low Power Non-cellular network, e.g. LPWA.
- Satellite (LEO or GEO)
- Multi-network gateway e.g. MESH to cellular gateway, Cellular to LPWA

2.7 Environmental requirements

What kind of environment does the end-point device operate in? e.g. temperature, humidity, dust, vibration. *This question does not directly effect the connectivity technology used but it will influence the choice of communications hardware. The availability of communications hardware varies between connectivity technologies, see* **IMC Connectivity Hardware RFP.**

3.0 Supplier (Bidder) Profile

Who are you?

3.1 History and Market experience

- Overview of the bidder, including location of headquarters, scale of operations and geographies covered.
- History of the bidder and experience in the relevant business.
    - Length of time in the M2M/IoT connectivity market
    - Case studies (anonymous)
    - Relevant industry events attended
    - Evidence of achievements and recognition in the industry

3.2 Relative Financials

Public company records will be accessed in the normal way. Private companies are expected to say more in the RFP to give some assurances to the buyer of financial stability.

- Years since formation, revenue growth rates.
- Percentage of revenues from M2M/IoT services.

In the context of a long- term supplier relationship

3.3 Supplier Five Year Roadmap to 20xx (year)

- Supplier to share expected developments of their business and relevant services.
- Supplier will provide a credible Business Continuity Plan (BCP) to ensure *connectivity* service delivery for a period of xx years.

3.4 Professional Services Support

- What services are provided to help/guide the IoT connectivity implementation?
- What pre and post sales training and support are available for our staff?
- What experience, with case studies, can you bring to our organisation on how the implementation of an IoT solution affects other aspects of our business, strategy, go to market and revenue models?

4.0 Connectivity Supplier Service Offerings

Tell us what you are offering and how you will meet our requirements

IoT Connectivity Capabilities required as follows:

- 4.1 Technology
- 4.2 Services
- 4.3 Commercial
- 4.4 Security

4.1 Technology

Please provide detailed descriptions on the technical functionality of the network underpinning your connectivity services, these to include the following Evaluation Criteria as guidance but the responder is invited to include additional information as appropriate.

Evaluation Criteria	Response Prompts
Connectivity Service description.	Does the connectivity service run on your own network? What elements of the end to end network do you own – wide area radio access, local loop, local area radio access, satellite? If all or part of the connectivity service does not run on your own network (Virtual Network Operator) please describe how this work, the relationships you have with network infrastructure providers and the level of integration your service has with the Connectivity Management Platform (CMP). Do you run your own CMP or use a third party?
Service Coverage	Please describe the geographic coverage offered at the global, regional and local levels. Is coverage achieved by roaming agreements? Multi-IMSI SIMs?
Service Delivery	How is connectivity hardware delivered, physical SIM from Carrier/MNO, eUICC, own SIM, muti-IMSI? How are services delivered, Via the Internet, Site to Site VPN, Client Access VPN, Direct Connectivity to mobile network?
Technology Options	What connectivity technologies do you offer on your network? Licensed cellular wireless: 2G, 3G, 4G, NBIoT (any variations of these?) Are ruggedized SIMs available to cope with a variation of environments? Non Cellular wireless: LoRa, Sigfox, Other unlicensed LAN/Mesh: Wifi, Zigbe, EEE 802.11g Landline: xDSL, leased line, VPN Satellite: LEO, GEO. Explain how these are presented for connection to the network: SIM, Transceiver, other hardware.
Available Data Rates	Given the technologies running on your network, what uplink and downlink data rates do you expect for each technology type. It is understood that there are a number of factors affecting data rates but

	please provide some typical data rates for each technology type you offer.
Latency	Some IoT applications have varying sensitivity to latency in the network. Even within the same technology type there are variations. Please provide typical latency data for each technology type you offer.
Payload	What payload sizes are supported for each technology type
In Building/In Ground Capability	Some technologies work better than other for applications where the IoT device is inside a building, in a basement or under the ground. Please provide case studies with your recommended connectivity technology together with technical data showing this capability
Scalability	How scalable is your connectivity service in terms of number of connections in one geographic location. What device density is supported and is this dependent on cell capacity or some other factor. In the event of needing to increase number of connections in a given area is it possible to 'scale up' to accommodate?
Communications Hardware Integration	Describe any packaged options offered with the connectivity service.
IP Addressing Mechanisms and Access Point Name - APN (private and public) provisioning	Are both static and dynamic IP, public and private addressing offered? Can contiguous static IP addresses be provided within a private APN? Are both public and private APN provisioning offered? Describe how naming is implemented for new connections or changed for existing connections. How is billing data collected? How is rating and charging managed?
Connectivity Analytics	What type of metrics are used to assess network conditions and behaviour? Is it possible to run predictive analytics on the conditions of the network?
Development Process	What development process do you use? E.g. DevOps, Agile, Waterfall
Network Resilience	What provisions are in place for network resilience/redundancy?

4.2 Services

Please provide detailed descriptions on the functionality of the network services being offered, these to include the following Evaluation Criteria as guidance but the responder is invited to include additional information as appropriate.

Evaluation Criteria	Response Prompts
Order Provisioning Management	How are orders placed, processed and provisioned on the network? What is the typical time between placing the order and the asset being connected? Can the platform support integration with 3rd Party Order/Management systems? Can the connected estate be managed via a portal? What hardware and software are required for access to the platform? How are additional connected ordered? Existing subscriptions changed? SIM activated/deactivated?
Subscriptions Management.	How are subscriptions managed, new connections added, data plans changed? Is there an upper limit on the number of subscriptions supported on one account? Which profiles are supported (eSIM, multi IMSI SIM)?

	Do you provide regulatory certification for the connected device?
Over the Air (OTA) Provisioning.	Are OTA provisioning and upgrades offered?
SLA/QOS	What service metrics are monitored and offered as part of an SLA? Are commitments made to service availability, e.g. 99.x% uptime? List other quality and service levels you commit to and measure. Are SLAs on the performance of the service offered? How are SLAs measured and reported? What are the criteria for SLAs met/not met? What QoS metrics are used to monitor SLAs? How are these reported? Are other services such as VPNs, APIs and the CMP portal covered by SLAs?
Loss of Service - Fault management procedures, Help Desk and SLA criteria	Describe the reporting procedure for loss of one or more connections. Describe the rectification of faults and notification processes relating to loss of connection or loss of services. Is a 24x7 help desk offered? Please outline the administrative capabilities such as service desk capabilities, disaster recovery management and etc.
Deployment Templates	Does the network service support both single and batch deployment?
Connectivity Management Platform (CMP). *(Ref IMC Template RFP for IoT Software Platforms)*	Is there a portal interface to view and manage the entire connected estate of devices? Does it have reporting capabilities? Can the CMP be white labelled? Does it support MVNE capabilities? Please describe its function and capabilities. This capability will be explored further in an IoT Software Platforms RFP
Billing, tariff, and usage management	How is the bill presented? What options are available on the billing system. Are real time rating and billing supported? What tariff options/bands are available? Is data pooling of SIMs an option? Describe volume discounting policy. Are both manual and automatic usage monitoring options available? Is subscription based billing of resellers/distributors supported.
Service Quality	What quality measurement system is in place? Describe your QA process – measurement, system tools. Which KPIs do you use to express the stability of the network?

4.3 Commercial

Business Service Offerings	Are monetized services provided? For specific verticals?
Pricing Models	Please describe the pricing options available: - SIM + Data - Data Pools - Aggregate pricing - Lifetime pricing Is pricing based on technology used, data volume, number of message per day? Or other factors? What additional charges are there for Roaming, VPNs, Private APNs, API access and use, security features, location services and other services? Is there a charge for activation/deactivation Do higher SLA and QOS agreements carry premium pricing, e.g 'Bronze, Silver, Gold'
Partnering/Ecosystem	Please describe your partner ecosystem and how you see that enhancing your services: - Hardware - Connectivity Management Platforms - Applications Development Platforms - Device and Data Management platforms
IoT Vertical/Industry Sector	Do you consider your connectivity services are optimised for any particular industry sector? E.g. those requiring high density deployment, those requiring global coverage in remote locations etc.
Joint Go-to-market models	Are there existing GTM examples you can reference or describe possible GTM propositions achievable within the service offerings of your network and/or in conjunction with your ecosystem partners.
Other Considerations	Please describe any other aspects of your connectivity offering, business-related or of a technical nature, not covered by the above questions.

4.4 Security Provisions

The Connectivity solution must address 2 basic requirements

4.4.1   Align with our current IT infrastructure boundaries:
- Networks
- End-points, including IoT devices
- Users and applications

4.7.2   Align with our current and evolving security strategy around the 5 security objectives:
- Prevent breach of IT infrastructure boundaries
- Detect threats in the IoT systems, through integration with SIEM platforms
- Respond and remediate incidents
- Continuously improve security posture through a holistic security strategy
- Comply with required audits and legislative reporting

Functionality	Response Prompts
Network / Security of connection & Security of transmission	Describe the systems and processes in place to ensure security of transmission. Eg: what is the encryption to enable secure transmission (SSL/SSH/TSL) between networks (on-premise, public, private and hybrid clouds), endpoints, and users & applications Describe the systems and processes in place to ensure security of connection. Eg: Are you relying on the inherent security from standardised cellular connectivity such as those from 3GPP?
End points – Considerations for the IoT Application and device design	How do you secure • Access authorisation and authentication of IoT devices • Secure edge gateway management • Network access control (discovery, operation and management) • Encryption (KPI, digital signatures, SSH, SSL) • Rule-based access & audit trails

Users & Application	How do you ensure secure:
	• Identity access management
	• User/application based policy & audit trails
	• API security
	  o Mobile application security
	  o Patch management
	  o Secure coding
	  o OT application security

General functionality	How does the network support adopters' overall security objectives? Eg. How does the network provide real time visibility and awareness of the IoT system to the adopters' overall security tools, controls and processes? • Is a secluded network layer available? • Which IoT Security Framework(s) does your network adhere to? • Describe you subscription management procedures • Does your network allow IoT endpoint device blacklisting? • Is analytics based security offered? • With which security specialist(s) are you currently working together on the network, end points, and users & applications side? • Is continuous threat monitoring in place? • What security services are provided beyond the usual encryption/VPN?
Risk Management Plan	Describe your risk management plan, to include: - Disaster recovery plan? - Data Security - Data Privacy - GDPR Compliance

5.0 **Proposal Submission Guidelines**

5.1 General Instructions.

- Expected responses to this RFP: One document OR more than one, e.g. Technical & Commercial.
- A non-disclosure agreement to be signed in relation to the contents of this RFP and the responses to it.
- References made to the "project" in this RFP refer to the deployment, testing and acceptance of the connectivity services provided, all related project management, training, and pre-launch activities
- When a reference is made to the "supplier" or "bidder" in this RFP, this refers to the vendor who is participating in this procedure through the submission of an offer for this project

5.2 Presentation of Responses

5.2.1 Technical Responses

- Service capabilities
- Service metrics

5.2.2 Commercial Responses

5.2.3 Project Plan to Implementatio

6.0 Selection Criteria

6.1 Evaluation Process

6.1.1 Technical

Criteria	Details	Assigned Weight
Standard Features	Basic connectivity on the network	xx %
Additional features	Packaged hardware, Connectivity management platform	xx%
Connectivity Service Wrap	Help desk, Self-provisioning,	Xx%
Project Specific Features	Customised platform capability e.g. Bulk on-boarding.	xx%
QOS Offered	Commitments to service metrics e.g. network availability, response times to LOS. Outage notifications	xx%
Compliances	IIC Test bed compliances ?	xx%

	IMC Validation ? *Will these apply for connectivity?*	

6.1.2 Financial

Criteria	Details	Assigned Weight
Basic Pricing – Network usage, data plans, application based pricing options	To be given in $/€/£ etc. Per connection, per Mb/month. Data pool pricing where appropriate e.g. shared across SIMs	xx %
Additional services pricing	Differentiated service wrap chargeables	Xx%
Communications hardware	Additional pricing for packaged hardware with CAPEX and OPEX options	Xx%
Project specific services – Breakdown of costs to develop and test	For Development For Testing For Project Management Activities	xx%

7.0 General Terms and Conditions

7.1 Payments, Incentives and Penalties

7.2 Contractual Terms and Conditions

- Confidentiality
- Non-disclosure
- Right of rejection
- Cost of responses
- Public Statements
- Cancellation
- Law and Regulation
- Ownership

7.3 Process Schedule

- Decision date on responses
- Awarding of contracts
- Commencement of work
- Completion of development work
- Completion of compliance testing
- Completion of alpha testing (live)
- Completion of beta testing (controlled rollout)

- Full Service Launch

Addendum & Referenced Documents

Connectivity Look-up table

For more details on the available types of connectivity technologies see *IMC Connectivity Guidelines.* The following table is a quick reference to match application needs with suitable technologies, Services and Hardware.

My Application Needs	Technology
High speed (data transfer rate), low network latency	4G/LTE Cat 4 and above.
Good in-building or in-ground penetration	NB1, LoRa, Sigfox
Autonomy from electrical supply – where end device and/or other hardware is battery powered.	LTE NB1, Cat M1, LoRa, Sigfox
Global coverage – Remote areas or at sea typically out of cellular range	Satellite LEO or GEO
High levels of device density in one area i.e. urban deployments	NB1, Cat M1
Roaming capabilities	2G/3G/4G.
	Services
An order fulfilment process with contractual commitments to rapid processing of orders for device on-boarding.	For vendor response
Message delivery acknowledgement, high availability	For vendor response
24 x 7 Telephone support	For vendor response
Flexible pricing based on number of messages/data volume/connection volumes	For vendor response

Contract option of SLAs with QOS measurements as KPIs for compliance.	For vendor response
A Fault reporting and resolution process with contractual commitments to rapid resolution and minimised LOS	For vendor response
Network based geolocation services	For vendor response
	Hardware
The communications hardware built into our device	Cellular module, Transceiver
The communications hardware separate from our device	Modem, Router, Gateway
The communications hardware ruggedized for temperature, vibration, outdoor use	For Vendor response
The communications hardware capable of edge processing	Gateway (for vendor response)
The communications hardware equipped with dual radio capability for redundancy	Router, Gateway (for vendor response)

Points of Contact for Future Correspondence.

Format guidelines for RFP responses

References to IMC Platforms RFP

References to IMC Connectivity Hardware RFP

Referenced Documents

'GSMA IoT Security Guidelines, Official Document CLP.14 - IoT Security Guidelines for Network Operators' 31st October 2017