NORTH

IoT Services

G-Cloud 15 Service Description

Date: Jan 2026

Stronger networks, smarter places

NORTH

Contents

1. Introduction 4
2. Service Overview 4
2.1. Standard Services 4
2.2. Additional Services 5
3. IoT Solution Components 6
3.1. Connectivity 6
3.2. Sensors (Devices) 7
3.3. Sensor Management (Service Levels) & Data Processing 8
3.4. Data Presentation Platform – North SmartPlaces 9
3.5. Third-party Analytics Platforms 9
4. IoT Services Scope 10
4.1. Standard Service Components 10
4.1.1. Connection of Sensors 10
4.1.2. Device Authentication and Onboarding 10
4.1.3. Device Management 11
4.1.4. Data routing and delivery to application platforms 11
4.1.5. IoT Device Supply Service 11
4.1.6. Operational Support and Service Desk 12
4.2. Additional Service Components 12

4.2.1. Design of IoT network and coverage 12
4.2.2. Enhanced Connectivity Services 13
4.2.3. IoT Private Network Build & Management 13
4.2.4. Use case specific operational services 13
4.2.5. Bespoke Integration services 14
5. Service Benefits 14
6. Security and Information Assurance 14
7. Service Levels and Constraints 14
8. Compliance and Standards 15
9. North in Defence 16
10. Contact Details 16

1. Introduction

The Internet of Things (IoT) is one of the most exciting enablers for change within defence, critical national infrastructure and the wider public sector. While the concept of IoT is not new, advances in technology means that IoT has now reached the maturity where it can drive real improvements, delivering new methods of interaction and data capture. IoT solutions help unlock the rich data available across an organisation to provide real-time insights, enable better informed business decisions, increase efficiencies, reduce costs and improve operational outcomes.

North specialises in building stronger, more reliable networks and creating smarter, more sustainable places. We provide intelligent technology solutions and robust network infrastructures that transform the way people, places, and organisations work. North excels in complex environments where multiple layers of connectivity are required to support a range of applications. Our in-depth knowledge of network architecture, integration expertise and Secure-by-Design capability has allowed North to become the driving forces behind numerous Smart Base, Smart City and Smart Campus projects.

North's Smart Solutions portfolio includes surveillance, control room systems, automated access control, public address, asset tracking and building management integration. North provides design and development, network auditing, cyber-security, configuration, installation, integration, project management, service delivery management, contract management, subcontractor management and full managed services.

This G-Cloud IoT Service aims to help clients capitalise on the opportunities offered by IoT.

2. Service Overview

The IoT Service provides the design, operation and ongoing management of a site-wide IoT network for the intended use of connecting sensors (devices), securely transporting data and delivering this to an application or database. This service description applies to the provision and operation of the network and data handoff. This data will be either handed off to another application provided by North or to a Third Party service. This service description does not cover these components.

2.1. Standard Services

The standard set of IoT services includes:

- IoT sensor connectivity
- Standard data routing and forwarding

Where required, the service can be deployed incrementally, allowing customers to begin with pilot projects before expanding to wider estate adoption.

2.2. Additional Services

North also offers a range of additional services that are tailored for each customer requirement. These include:

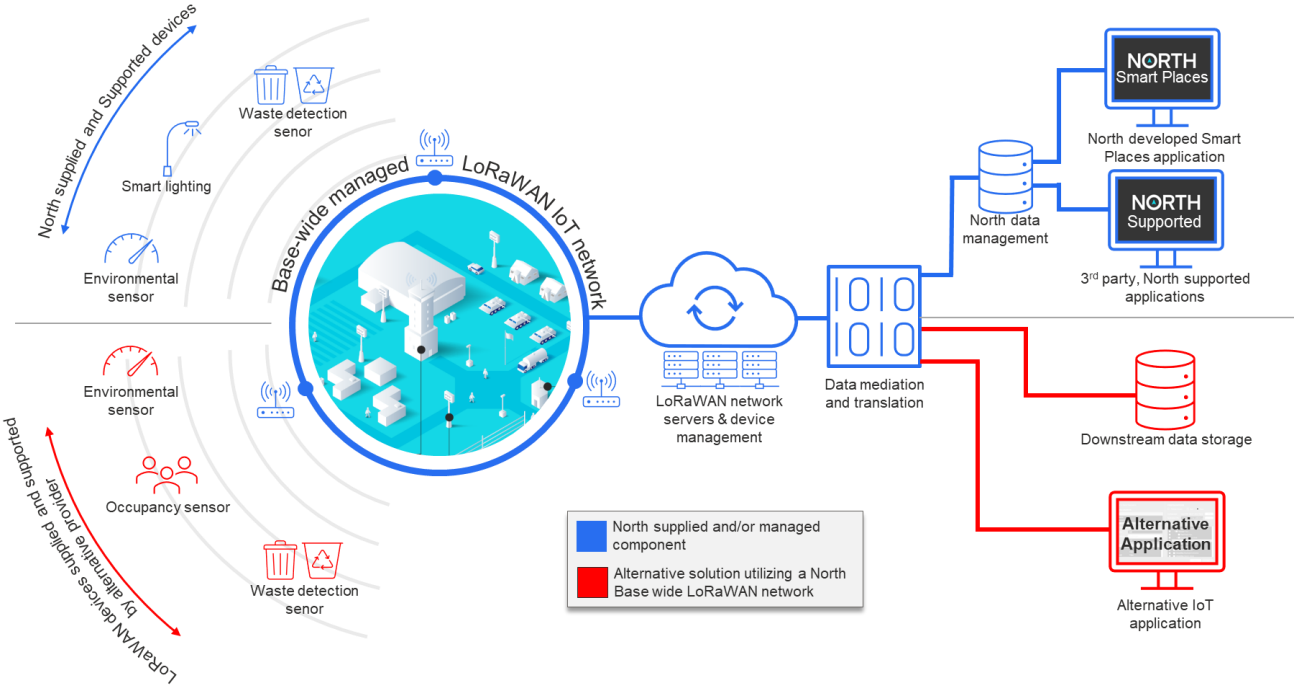
- IoT professional services
- IoT sensor operational support
- Extended data routing and forwarding
- IoT Private network Build & Management
- Supply of approved and tested sensors

Further details of the scope of these services are provided in section 4.

3. IoT Solution Components

An IoT solution consists of the following components which are explained in the below sections and include:

- Gateways
- Sensors
- Management and Data Processing Platform
- Data Presentation Platform / Analytics



3.1. Connectivity

The first stage of an IoT deployment is to establish an umbrella of coverage across a site. This is provided by a network of interconnected IoT gateways. In some scenarios there will be an existing network that can be used, either provided by North or one of our connectivity providers. In this Service Description these are referred to as Public Networks. Where one of these doesn't exist then North can either design and provision a series of Gateways that are registered on their existing shared IoT Platform or they can build an entirely dedicated network including the centralised server infrastructure.

In these instances, North will survey, specify and install the appropriate number of gateways to provide resilient coverage to all indoor and outdoor areas of the site. The IoT network that North provides is based on a secure technology called Long Range Wide Area Network (LoRaWAN). LoRaWAN is a low-power, long-range wireless communication standard designed to securely connect large numbers of IoT devices over wide areas, such as university campuses and military bases.

It uses end-to-end AES encryption, meaning data is encrypted at the sensor and remains protected until it reaches the application, preventing North or third parties from accessing payload data until it reaches its intended destination. Devices are uniquely authenticated before joining the network, with separate network and application security keys to reduce risk if one layer is compromised. This architecture makes LoRaWAN particularly well suited for critical infrastructure and public-sector deployments where data integrity, privacy and resilience are essential.

The external LoRaWAN Gateways are mounted in elevated positions around the intended location to ensure good coverage and an ability for all sensors deployed to communicate with at least two gateways for resilience.

All North LoRaWAN gateways are carrier-grade and can support a large number of mission-critical sensors. The gateways are secure-by-design and optimised by the team at North to provide excellent interference mitigation and enhanced radio performance.

If selected, the North network is fully managed and monitored by the North Network Operations Centre (NOC).

Where required a private instance of the central infrastructure can be provisioned and the gateways will connect either using segregated connectivity over a customer-verified secure LAN environment, where the sensor data will be securely tunnelled across the network and forwarded to the North private IoT platform servers which should be located in diverse data centres within the security perimeter of the customer secure network. This ensures the data does not leave the safe environment of the supported network.

Please note that if a Third Party IoT application provider's service is cloud-based then the data can be forwarded to external locations when requested. In these instances, the nature of the data and application will require assessment and approval from North and the customer in adherence with the principals of Secure-by-Design.

Where North are operating either on their public or private networks to provide the service then customers and permitted partners/suppliers will be able to onboard their sensors for an annual per-sensor licence fee. North can also provide a complete range of end-to-end IoT solutions that include a sensor and associated platform. Information on these is supplied separately.

3.2. Sensors (Devices)

The IoT network supports the deployment of low cost sensors capable of transmitting data over distances up to 15km (in ideal outdoor conditions) whilst running on batteries for 5-10 years. A huge range of sensor types are available; for example sensors to capture and transmit data on energy, environmental, occupancy, air quality, gas or chemical presence, motion, proximity or pressure. LoRaWAN technology delivers the following benefits:

- **Open Standard based technology** – Wide range of low cost sensors capable of measuring myriad things.
- **Long Range** – Sensors are capable of transmitting data over distances of up to 15km line of sight.
- **Deep indoor penetration** – The IoT network is able to communicate with sensors deployed within buildings and even underground.
- **Low Power** – Sensor batteries can last for 5-10 years.
- **Cost effective** – Low cost per sensor annual licence.
- **Strong Security** – Sensor data is encrypted (AES 128) end to end preventing third parties from accessing payload data.

LoRaWAN sensors are manufactured by many organisations meaning that there is a wide range of different sensors catering for various applications. The IoT network is intended to work with any sensor that adheres to the LoRaWAN standard. This means that different organisations operating on customer sites can add sensors to the IoT network using one of the following operating models:

- **Third-party provided sensor**, **not managed by North** – North will required sensor identifiers but will not need to test if the sensor adheres to the LoRaWAN standard. (Public or Private connectivity charges will apply)

- **Third-party provided sensor, managed by North** – For any sensor not provided by North but where there is a requirement for North to manage will need to be taken through testing to understand normal behaviour and constitutes a deviation from this. (Public or Private connectivity charges will apply alongside the selected management level)
- **North provided Sensor** – North only provide pre-tested sensors from reputable manufacturers based in the UK, EU or United States. North will regularly provide an updated catalogue showing all current tested devices that they can provide Public or Private connectivity charges will apply alongside the selected management level)
- **North Provided full solution** – For any North solution where they are providing the sensor, managing the connectivity and supplying the operational platform then the sensors are always tested and sourced from approved providers. Public or Private connectivity charges will apply alongside the selected management level)

3.3. Sensor Management (Service Levels) & Data Processing

Data collected by sensors is transmitted over the IoT network to a central data management platform.

This comprises Connectivity Management components and a Device Management layer to deliver a highly-reliable, highly-scalable and secure method of ingesting data from remote sensors. The North data management platform can decode the raw sensor data if required and add contextual metadata before re-encryption and forwarding to the North database and data presentation platform, SmartPlaces. Sensor data can also be forwarded to third-party platforms on request and under the relevant approval in adherence with the Secure-by-Design process.

The IoT platform, either private or public also supports direct data pass-through where certain solutions will require complete end-to-end encryption and either the application and/or sensor are not provided by North.

3.4. Data Presentation Platform – North SmartPlaces

The contextualised data from the Management and & Data processing platform can be visually presented on either North's own IoT dashboard application using standard operational modules that are use-case specific or through custom modules which are specifically designed for scenarios at request of customers. The North internal application system is referred to as North SmartPlaces.

Data can also be visually represented in an alternative third party platform or through a real-time Video Management system facilitating expanded situational awareness through a variety of additional sensor feeds. For this the data will be routed to the specified application using one of the methods in the pricing document,

For example, data from a tamper-detection sensor on a perimeter fence could be transmitted to the Video Management System, creating an alert in the control room and cueing the CCTV camera to the sensor location.

3.5. Third-party Analytics Platforms

As well as facilitating the transport of data to alternative operational systems, data can also be presented to systems for customer-side processing and analysis in systems such as Microsoft Power BI or customer specific analytics platforms. North can support the customer analysts to introduce new data sources to provide improved information for decision makers.

4. IoT Services Scope

This section sets out the catalogue of available services and the scope of each service.

- Section 4.1 outlines the standard services that will be required for most typical IOT deployments.
- Section 4.2 outlines additional services that may be required for more-specialised customers.

4.1. Standard Service Components

4.1.1. Connection of Sensors

Purpose

Connection of approved sensors and installation onto the IoT network.

Scope

Connection of sensors will be managed by North regardless of whether the sensor is sourced by North or supplied by a Third Party. The following are required for a device to be added to the network successfully;

(a) Sensors should adhere to the LoRaWAN standard unless agreed otherwise.

(b) North will need to be supplied with details of the sensor as follows:

a. Device EUI
b. Assigned device name or title
c. Device JoinKey/AppID
d. Device AppKey
e. LoRaWAN version
f. Any changes to standard data handling
g. Expected device data interval

4.1.2. Device Authentication and Onboarding

Purpose

This is the critical process of verifying the identity of sensors before they can connect to a network, ensuring only trusted, authorized devices exchange data. It protects against unauthorized access, spoofing, and botnet attacks.

Scope

(a) **Device Enrolment** – The North Data Management Platform will handle the enrolment of devices automatically once the details outlined in section 4.1.1 have been supplied. Device registration and activation is delivered via Over-the-air activation (OTAA).

(b) **Connection Management** – The North Data Management Platform will manage all aspects of device connectivity such as managing MAC layer functions, handling the adaptive data rate (ADR), managing message deduplication across the gateway estate and enforcing duty cycle regulations.

(c) **Device Management** – This includes the management of server-side device profiles and configurations, and device status monitoring.

(d) **Device Decommissioning** – The ceasing and decommissioning of devices

4.1.3. Device Management

The IoT Device Management Service provides the tools and processes required to manage IoT devices throughout their lifecycle. This includes device onboarding and registration, configuration management, status monitoring, and the ability to suspend, reactivate, or retire devices as required. The service supports visibility of device connectivity and basic operational health, enabling effective fleet management at scale. Device management does not include physical maintenance or repair of devices unless expressly agreed or as part of a North full end-to-end solution.

4.1.4. Data routing and delivery to application platforms

Purpose

Routing of sensor data to data presentation application software. This could be North's SmartPlaces or a Third Party application.

Scope

North's service includes 3 standard data integration methods depending on how the data is to be visualised. These are all subject to security assessment and approvals:

(a) **HTTP(S) integration -** Enables secure forwarding of IoT device data from the network server to external applications or platforms via standard HTTPS endpoints for downstream processing and storage.

(b) **MQTT (Message Queuing Telemetry Transport) –** MQTT is a lightweight, publish-subscribe network protocol designed for machine-to-machine communication in IoT and resource-constrained environments. It enables efficient, low-bandwidth data transmission, ideal for austere networks.

(c) **Webhooks -** Automatically push IoT device data or events in real time to customer-defined URLs, enabling immediate integration with external systems and workflows.

The above can all be configured to forward the data without any prior decoding to maintain message integrity and security.

4.1.5. IoT Device Supply Service

Purpose

The IoT Device Supply Service provisions compatible and tested IoT sensors to support agreed use-cases.

Scope

- Sourcing approved devices from established manufacturers
- Ensuring compatibility with the IoT network
- Managing ordering, logistics and delivery

4.1.6. Operational Support and Service Desk

Purpose

To provide in-life support of the IoT network

Scope

North's Service Desk provides a single point of contact for the logging and management of faults and support requests. The service desk can be used to support the following actions:

- Incident and Fault Reporting
- Information Requests
- Technical Support Queries
- Change Requests/New Work Requests
- Problems
- Escalations
- Certain end-user applications will also have their own dedicated support pages

Specific service levels, hours of availability and KPIs will be agreed on a case-by-case basis, subject to customer requirements.

4.2. Additional Service Components

4.2.1. Design of IoT network and coverage

Purpose

To design a LoRaWAN network that complies with appropriate security requirements and provides site-wide coverage for a range of connected sensors.

Scope

- Survey site
- Determine number and locations of LoRaWAN Gateways required
- Determine how the LoRaWAN Gateways will connect with the existing site secure IP network, for example, DBI for defence sites.

- Determine LoRaWAN Gateways mounting requirements. New poles/masts to be installed in accordance with current standards and have suitable lightning protection.
- Determine requirements for cabling, containment, power and active equipment
- Produce design documentation. For MoD sites this will be in the form of ECR2 submitted to SCIDA.

4.2.2. Enhanced Connectivity Services

North's standard service is intended to provide exceptional coverage on the majority of sites. On certain occasions specialist measures may be required, such as:

(a) Certain indoor or exceptionally hard to reach locations

(b) Temporary or event-based deployments

(c) Extended outdoor coverage

(d) Segregated connectivity services

(e) Heightened EMC activity

North's expertise in coverage modelling enables us to recommend temporary or permanent solutions in the majority of cases.

4.2.3. IoT Private Network Build & Management

Purpose

Installation and configuration of central servers and storage devices, data management and presentation software (typically North SmartPlaces). North's centralised IoT stack is highly resilient and secure. It is responsible from managing the gateways, controlling the connected sensors and managing data flows.

Scope

- Install and configure physical hardware
- Install and configure software
- Implement security controls as recommended by Secure by Design process

4.2.4. Use case specific operational services

North can provide and variety of IoT Application Services used to visualise, manage, and interpret data generated by connected IoT devices. This includes user access to dashboards, alerts, reporting, and configurable rules relevant to the agreed use cases. The application enables users to monitor assets, environments, or processes through a secure web-based interface and supports integration with third-party systems where required. The service focuses on data presentation and operational insight and does not include changes to underlying connectivity or device hardware unless explicitly stated. Separate documentation covers the operation of these platforms.

4.2.5. Bespoke Integration services

Bespoke Integration Services provide the design and development of tailored integrations between the IoT platform and customer or third-party systems. This may include custom APIs, data transformations, workflow automation, or secure data exchange with systems such as BMS, CAFM, ERP, or analytics platforms. Integrations are developed to meet specific operational requirements and are delivered as scoped professional services, with ongoing support and maintenance subject to separate agreement.

5. Service Benefits

The benefits of North's IoT Service are:

- Deployment blueprints reduce implementation timescales
- Multiple organisations can share the IoT network on a single site increasing return on investment
- Data can captured once and used multiple times
- North’s Secure-by-Design know-how reduces the risk of cyber-attack
- Investment costs can be spread over multiple use cases
- Simplified adoption of new use-cases
- Rapid onboarding of new sensors and IoT devices

6. Security and Information Assurance

North is Cyber Essentials Plus+ certified. Employees delivering this service are cleared to a minimum of SC. All staff undertake mandatory annual security training and have experience (in most cases significant) of working in secure MoD and HMG environments. North has a security team to maintain accreditation and clearances.

7. Service Levels and Constraints

The IoT network requires connectivity to the site’s secure IP network where the sensor data will be securely tunnelled across the network to the Data Management Platform. On MOD sites this is typically provided by the BT operated Defence Business Internet service (DBI). For non-MoD sites, an equivalent service will be required.

The services can be provided throughout the UK during normal business days and working hours. Travel and subsistence may be payable outside of the normal daily rate. More information is available upon request.

8. Compliance and Standards

North has the following accreditations

ISO 9001: 2015	Quality Management System
ISO 14001:2015	Environmental Management System
ISO 27001:2013	Information Security Management System
ISO 45001:2018	Occupational Health and Safety Management System

North is also a signatory to the Armed Forces Covenant.

9. North in Defence

Invaluable sector experience

Over the past 20 years we've built a formidable and trusted reputation working 'behind the wire' in highly specialised live environments – delivering tried and tested, reliable, secure and compliant solutions for front-line commands, digital defence, nuclear and more. Our expertise in defence & justice networks makes us a safe pair of hands for complex and demanding projects and our reliable delivery model enables us to scale at pace.

10. Contact Details

Please direct all initial questions or queries back to Chris and they will ensure that the most appropriate person responds.

Name	Job Title	Contact No.	Email
Chris Laing	Smarter Bases BDM	07989 737283	Chris.Laing@north.tech

Stronger networks, smarter places

north.tech

NORTH