

LEISTUNGSBESCHREIBUNG

Aufbau und Betrieb eines LoRaWAN-Netzes

Smart City / Kommunale Infrastruktur

Auftraggeber	Magistrat Büdingen smarte Region Hessen
Vergabenummer	02/2026/EU
Projektlaufzeit	01.10.2025 – 01.06.2027
Dokumentenversion	1.0
Stand	09.10.2026

Dieses Dokument ist vertraulich und ausschließlich für den Empfänger bestimmt.

Inhaltsverzeichnis

1. Allgemeine Angaben

Diese Leistungsbeschreibung beschreibt die Anforderungen für die Planung, Lieferung, Installation und den Betrieb eines LoRaWAN-Netzwerks (Long Range Wide Area Network) im Rahmen der Smart-City-Strategie der Kommune. Die Leistungen umfassen die Bereiche Planung & Konzeption, Hardware (Gateways und Sensoren) sowie Netzwerk-Backend und Server-Infrastruktur.

1.1 Auftraggeber

Organisation	Magistrat Büdingen
Fachbereich	Hauptamt
Ansprechpartner	Aylin Aydin, stellv. Amtsleitung Haupt- und Organisationsamt Manuel Hasific, Wirtschaftsförderung
Anschrift	Eberhard-Bauner-Alle 16, 63654 Büdingen

1.2 Hintergrund und Motivation

Förderprojekt: Starke Heimat Hessen“ – Förderung smarter Kommunen und Regionen (Förderlinie 2)

Die Kommune verfolgt das Ziel, durch den Aufbau einer skalierbaren IoT-Infrastruktur verschiedene kommunale Dienste zu digitalisieren und datengestützte Entscheidungen zu ermöglichen. LoRaWAN bietet hierfür eine energieeffiziente, weitreichende und kostengünstige Funktechnologie, die sich für den flächendeckenden Einsatz in städtischen und ländlichen Gebieten besonders eignet.

Geplante Anwendungsfälle umfassen unter anderem:

- Passanten- und Verkehrsfrequenzmessung
- Klimadaten und Katastrophenschutz
- Dynamisches Parkleitsystem
- Abfallmanagement

2. Rahmenbedingungen und Ausgangslage

2.1 Geografische und infrastrukturelle Situation

Das zu versorgenden Gebiet umfasst:

Gesamtfläche	122,9 km ²
Einwohner	Ca. 23.000
Bebauungsstruktur	Die Stadt Büdingen umfasst rund 123 km² und besteht aus der Kernstadt sowie 16 Stadtteilen. Die 16 Ortsteile zzgl. der durch Straßen bebauten Fläche haben insgesamt eine Fläche von rund 24 km². Hinzu kommen rund 48 km² landwirtschaftliche Fläche, 48 km² Forst und 3 km² Gewässer.
Besonderheiten	Die Siedlungsstruktur ist heterogen und reicht von einer verdichteten, historisch geprägten Innenstadt über Wohn- und Mischgebiete sowie Gewerbeflächen bis zu ländlich geprägten, räumlich verteilten Ortsteilen. Die Ortsteile sind überwiegend dörflich und durch aufgelockerte Bebauung, landwirtschaftliche Flächen sowie größere Entfernungen zwischen den Ortslagen geprägt. Für den LoRaWAN-Ausbau ist deshalb eine bedarfsgerechte, skalierbare Netzplanung erforderlich, die sowohl die dicht bebaute Kernstadt als auch die ländlichen Ortsteile zuverlässig versorgt.

Der Auftragnehmer hat die örtlichen Gegebenheiten im Rahmen einer Standortanalyse zu erfassen und die Netzplanung darauf abzustimmen. Besondere Aufmerksamkeit ist auf potenzielle Funkhindernisse (Bebauungsdichte, Topografie, Metallfassaden) sowie auf regulatorische Aspekte (Dachstandorte, Straßenlaternenmontage, Baugenehmigungen) zu richten.

2.2 Bestehende IT-Infrastruktur

Folgende relevante Infrastrukturkomponenten sind bereits vorhanden und müssen bei der Planung berücksichtigt werden:

- Netzwerk: teilweise kommunales Glasfasernetz, Stadtverwaltung besitzt drei WAN-Konnektoren zwei davon gehen ins Landesnetz einer geht ins freie Netzwerk
- Rechenzentrumsbetrieb: eigenes kommunales RZ ohne DMZ, daher ist der Betrieb des LoRaWan-Servers innerhalb des RZ nicht möglich
- Bestehende IoT-Systeme: keine
- Georeferenzsystem: Ingrada, GeoAss, Vialytics

2.3 Technische Vorgaben und Standards

Der Auftragnehmer hat folgende technische Standards und Vorgaben zwingend einzuhalten:

- LoRaWAN-Spezifikation Version 1.1
- Frequenzband: EU868 (863–870 MHz) gemäß ETSI EN 300 220
- DSGVO-konforme Datenverarbeitung; keine personenbezogenen Daten ohne Einwilligung
- BSI IT-Grundschutz (Mindest-Absicherung) für die Backend-Infrastruktur
- Open-Source-Offenheit für Netzwerkserver-Software (z.B. ChirpStack)

3. Leistungsumfang

3.1 Leistungsbereich A: Planung und Konzeption

Grundlage für alle weiteren Leistungsbereiche ist eine fundierte technische Planung, die alle relevanten Aspekte des LoRaWAN-Netzaufbaus systematisch erfasst und dokumentiert.

3.1.1 Bestandsaufnahme und Anforderungsanalyse

Der Auftragnehmer führt zu Projektbeginn eine strukturierte Anforderungsanalyse durch:

1. Erhebung und Dokumentation aller Anwendungsfälle (Use Cases) mit Priorisierung
2. Analyse bestehender Infrastruktur (Netzwerk, Stromversorgung, Dachstandorte)
3. Begehung der Schlüsselstandorte für Gateway-Platzierung. Die Standorte sind idealerweise auf/an Gebäuden der Stadt vorzusehen.
4. Erstellung eines Anforderungsdokuments (Lasten-/Pflichtenheft-Abschnitt) zur AG-Freigabe

3.1.3 Netzwerkarchitektur und Systemkonzept

Der Auftragnehmer erstellt ein vollständiges Systemkonzept mit:

- Netzwerktopologie-Diagramm (Gateway-Placement, Backhaul-Anbindung, Backend-Architektur)
- Konzept für die Backhaul-Anbindung der Gateways (LTE/4G/5G, Ethernet/Glasfaser – je nach Standort)
- LoRaWAN Network Server (LNS) Architektur: Auswahl und Begründung des LNS (präferiert: ChirpStack oder TTN/TTS)
- Application Server und Datenfluss-Konzept (Anbindung an kommunale Fachanwendungen via MQTT, HTTP-Webhooks, REST-API)
- Sicherheitskonzept (Netzwerksegmentierung, VPN, Zugriffskontrolle, Schlüsselverwaltung)
- Skalierungskonzept: Erweiterbarkeit auf [X] Gateways und [X].000 Endgeräte
- Energiekonzept: Stromversorgung, USV-Anforderungen, ggf. Solar-/Batteriebetrieb für autarke Standorte

3.1.4 Projektplan und Meilensteinplanung

Vorzulegen sind:

- Detaillierter Projektplan (Gantt-Chart) mit allen Phasen und Meilensteinen
- Ressourcenplanung (Rollen, Qualifikationen, Einsatzzeitraum)
- Risikoregister mit Maßnahmen zur Risikovermeidung/-minderung
- Kommunikations- und Eskalationsplan

3.2 Leistungsbereich B: Hardware – Gateways und Sensoren

Der Auftragnehmer liefert, installiert und nimmt alle Hardwarekomponenten in Betrieb. Alle Geräte müssen CE-zertifiziert sein.

3.2.1 LoRaWAN-Gateways – Anforderungen

Für den Außeneinsatz (Outdoor-Gateways) gelten mindestens folgende technische Mindestanforderungen:

- Backhaul: LTE Cat-M1/NB-IoT (Dual-SIM) als Standard; optional Ethernet/SFP
- Zertifizierung: IP67 oder besser, IK10 (Vandalismusschutz), Betriebstemperatur – 40°C bis +70°C
- Antennengewinn: mindestens 3 dBi Rundstrahlantenne, extern austauschbar
- Montage nach DIN EN 60728-11 (VDE 0855-1) bzw E DIN VDE 0855-300 und DIN VDE 0185-305
- GPS/GNSS-Modul für Zeitstempel-Synchronisation (Fine Timestamp für TDOA)
- Fernwartung: HTTPS/SSH-Zugang, automatische Firmware-Updates (OTA)
- Montageoptionen: Mastmontage (inkl. Montageschellen) und Wandmontage
- Stromversorgung: 12V DC extern; optional: PoE+ (802.3at); USV-Anbindung möglich
- MTBF: ≥ 100.000 Stunden

Hinweis: Gleichwertige Produkte sind zugelassen, sofern alle Mindestanforderungen nachweislich erfüllt werden. Referenzprodukt: z.B. Kerlink Wirnet iBTS Compact, RAK Wireless RAK7289, Dragino DLOS8N oder gleichwertig.

3.2.2 Sensoren und Endgeräte

Die folgenden Sensortypen sind voraussichtlich nach Projektabschluss zu integrieren und zu installieren. Alle Endgeräte müssen LoRaWAN Device Klasse A unterstützen; Klasse C für Anwendungen mit hohen Latenzanforderungen:

Sensortyp	Anwendungsfall	Anzahl	Device-Klasse	Schutzklasse
Füllstandssensor (Ultraschall)	Abfallbehälter-Monitoring	[X]	A	IP68
Parkplatzsensor (Magnetisch)	Parkraummanagement	[X]	A	IP68
Umweltsensor (CO ₂ , NO ₂ , PM2.5)	Luftqualitätsmessung	[X]	A	IP65
Lärmpegelmessgerät	Lärm-Monitoring (dB(A))	[X]	A	IP65
Pegelstandssensor	Gewässer- / Kanal-Monitoring	[X]	A	IP68
Temperatursensor / Feuchte	Stadtklima-Monitoring	[X]	A	IP65
Zählsensor (PIR / Radar)	Fußgänger- / Fahrradfrequenz	[X]	A	IP65

Für alle Sensoren gelten zusätzlich:

- Datenformat: strukturiert (Cayenne LPP oder hersteller-spezifisch mit offenem Codec)
- Gehäuse witterungsbeständig (UV-stabilisiert), geeignet für Außen-Dauerbetrieb
- Zertifizierung: IP65 oder besser, eventuell IK10 (Vandalismusschutz), Betriebstemperatur –40°C bis +70°C
- Einfache Montage und Austausch ohne Spezialwerkzeug
- LoRaWAN-Aktivierung: OTAA (Over-The-Air Activation) präferiert
- Konfigurations- und Firmware-Updates per LoRaWAN Firmware Update (FUOTA) oder Bluetooth

3.2.3 Installation und Inbetriebnahme Hardware

Umfang der Installationsleistungen:

1. Koordination der Standortgenehmigungen mit Behörden, Eigentümern und Netzbetreibern
2. Montage der Gateways inklusive Antennen, Kabelführung und Erdung
3. Anbindung an Backhaul (SIM-Karten-Einbau und -konfiguration, LAN-Anbindung)
4. Konfiguration aller Gateways im LNS (EUI, Frequenzplan, Verbindungsparameter)
5. Erstellung von Installations- und Abnahmeprotokollen je Standort
6. Übergabe-Dokumentation mit Fotos, GPS-Koordinaten und technischen Daten

3.3 Leistungsbereich C: Netzwerk-Backend und Server-Infrastruktur

Das LoRaWAN-Backend bildet das digitale Rückgrat des Netzes. Es besteht aus dem LoRaWAN Network Server (LNS), dem Application Server, Datenspeicherung, Visualisierung und API-Schnittstellen.

3.3.1 LoRaWAN Network Server (LNS)

Anforderungen an den LoRaWAN Network Server:

- Unterstützung von LoRaWAN 1.1.x (Dual-Stack)
- Open-Source-Lösung präferiert: ChirpStack v4 oder The Things Stack Community / Enterprise oder Cloud Hosted TNN
- Optional: Multi-Tenant-Fähigkeit: Mandantentrennung für verschiedene Fachämter
- Unterstützung aller Geräteklassen: A, B und C
- Adaptive Data Rate (ADR) muss serverseitig implementiert sein
- Geolokalisierung: Unterstützung von TDOA (Time Difference of Arrival) und RSSI-basierter Positionsbestimmung
- Device Management: Massenregistrierung per CSV/API, FUOTA-Unterstützung
- Audit-Log: alle sicherheitsrelevanten Ereignisse lückenlos protokolliert
- Hochverfügbarkeit: Redundanter Betrieb (Active/Passive oder Active/Active Cluster)
- API: vollständige REST-API und gRPC-API für alle Verwaltungsfunktionen

3.3.2 Application Server und Datenverarbeitung

Datenfluss und Verarbeitung:

- Echtzeit-Datenstrom via MQTT-Broker (z.B. EMQX, Mosquitto) mit TLS-Verschlüsselung
- Payload-Decoder: individuelle Decoder je Geräteprofil (JavaScript-basiert im LNS)
- Datenspeicherung: Zeitreihendatenbank (z.B. InfluxDB, TimescaleDB) für Sensor-Rohdaten
- Schwellwertüberwachung: konfigurierbare Regeln je Sensor/Anwendung
- Datenexport: standardisierte Schnittstellen (REST-API, MQTT, OGC SensorThings API)
- Integration kommunaler Datenbank-Server zur Sicherung
- Datenaufbewahrung erfolgt nach gemeinsamer Abstimmung, mindestens 2 Jahre für Rohdaten

3.3.3 Visualisierung und Dashboard

Anforderungen an das Monitoring-Dashboard:

- Web-basiertes Dashboard ohne Client-Installation (Browser-basiert)
- Kartenbasierte Ansicht aller Gateways und Sensoren (Leaflet/OpenLayers/thethingsnetwork)
- Echtzeit-Anzeige von Gerätestatus (online/offline), Signalqualität (RSSI, SNR, SF)
- Zeitreihendarstellung von Messwerten mit konfigurierbaren Zeiträumen
- Alarmierungs-Dashboard mit Quittierungsfunktion
- Rollenbasierte Zugriffssteuerung (RBAC): Lese- und Schreibrechte je Fachamt

Anforderungen an das Bürger*inneninformations-Dashboard:

- Web-basiertes Dashboard ohne Client-Installation (Browser-basiert) |
- Kachelbasierte Übersicht verschiedener aufbereiteter Sensormesswerte und allgemeinen Informationen
- Konfiguration, Auswahl und Anordnung der Kacheln soll durch Mitarbeitende des Stadtmarketings erfolgen können
- Echtzeit-Anzeige von Gerätestatus (online/offline) und freigegebenen Messwerten
- Zeitreihendarstellung von Messwerten mit konfigurierbaren Zeiträumen
- Live-Daten Aktualisierung

3.3.4 Infrastruktur und Hosting

Technische Infrastrukturanforderungen:

- Hosting: ISO 27000:1 zertifiziertes RZ + Standort in Deutschland oder kommunales Rechenzentrum
- Netzwerksicherheit: Firewall, VPN-Zugang für Administration, kein direkter Internetzugang der Datenbank-Server
- Backup: tägliche Sicherung aller Konfigurationsdaten und Datenbanken, georedundant
- Monitoring: Infrastruktur-Monitoring (z.B. Prometheus/Grafana, Zabbix) mit Alerting

3.3.5 Sicherheit und Schlüsselverwaltung

Für die LoRaWAN-Sicherheitsarchitektur gelten:

- Join Server: separater, sicherer Join Server (z.B. in LNS integriert oder HSM-basiert)
- Schlüsselverwaltung: AppKey und NwkKey ausschließlich verschlüsselt gespeichert
- Keine Wiederverwendung von DevEUI oder Session Keys über verschiedene Netzwerkinstanzen
- TLS 1.2 / 1.3 für alle Backhaul- und API-Verbindungen
- Regelmäßige Security-Patches: kritische Patches innerhalb von 72h einzuspielen
- Penetrationstest: einmalig nach Inbetriebnahme durch zertifizierten Dritten (BSI IT-Grundschutz)

Qualität, Abnahme und Service Level Agreements

4.1 Abnahme und Abnahmekriterien + EVB-IT Verträge

Die Abnahme erfolgt in zwei Stufen:

- Teilabnahme: nach Abschluss jedes definierten Meilensteins (z.B. nach Planungsphase, nach Hardware-Installation)
- Gesamtabnahme: nach vollständiger Inbetriebnahme und erfolgreichem Abnahmetest

Abnahmetest-Kriterien (Mindestanforderungen):

1. Coverage-Nachweis: Messung RSSI/SNR an [X] repräsentativen Standorten, Unterschreitung von -120 dBm an max. [X]% zulässig
5. Paketverlustrate: $< 2\%$ bei SF7 unter normalen Umgebungsbedingungen
6. Gateway-Verfügbarkeit: $> 99\%$ über 7-tägigen Testbetrieb
7. End-to-End-Latenz: Datenübertragung Sensor $\rightarrow$ Dashboard < 30 Sekunden (p95)
8. LNS-Funktionstest: alle Geräteklassen, OTAA-Join, ADR, Downlink, FUOTA
9. Sicherheitstest: kein unautorisierter Netzwerkzugang, TLS-Verifikation
10. Funktionstest: alle Sensortypen korrekt angebunden, Alarmer ausgelöst

4.2 Service Level Agreements (SLA) – Betriebsphase

Parameter	Anforderung (Minimum)	Zielwert	Messmethode
Netz-Verfügbarkeit (Gateways gesamt)	$\geq 98,5\%$ p.Monat	$\geq 99,5\%$ p.M.	Automatisches Monitoring
Einzelgateway-Verfügbarkeit	$\geq 95\%$ p.Monat	$\geq 99\%$ p.M.	Heartbeat alle 5 Min.
LNS-Verfügbarkeit (Backend)	$\geq 99,5\%$ p.Monat	$\geq 99,9\%$ p.M.	Uptime-Monitoring
Störungsmeldung Kritisch (P1)	Innerhalb 1 Stunde	Innerhalb 30 Min.	Ticketsystem
Störungsbehebung Kritisch (P1)	≤ 4 Stunden	≤ 2 Stunden	Ticketsystem
Störungsmeldung Normal (P2)	Innerhalb 4 Stunden	Innerhalb 2 Stunden	Ticketsystem
Störungsbehebung Normal (P2)	≤ 2 Werktage	≤ 1 Werktag	Ticketsystem
Sicherheits-Patches (kritisch)	≤ 72 Stunden	≤ 24 Stunden	Patch-Protokoll

Parameter	Anforderung (Minimum)	Zielwert	Messmethode
Geplante Wartungsfenster	Max. 4h/Monat, Ankündigung 48h vorher	Max. 2h/Monat	Change-Protokoll
Paketverlustrate (Netz gesamt)	< 3% im Monatsmittel	< 1%	LNS-Statistiken

Bei Unterschreitung bzw. Nichteinhaltung der vereinbarten Mindest-SLAs gelten folgende Pönale (Service Credits):

- Unterschreitung der LNS-Verfügbarkeit um 0,5 bis 1,0 Prozentpunkte: 5 % der monatlichen Betriebspauschale
- Unterschreitung der LNS-Verfügbarkeit um mehr als 1,0 Prozentpunkt: 15 % der monatlichen Betriebspauschale
- Nichteinhaltung der P1-Reaktionszeit: 10 % der monatlichen Betriebspauschale je Ereignis
- Nichteinhaltung der P2-Reaktionszeit: 2 % der monatlichen Betriebspauschale je Ereignis

Die Einhaltung der Mindest-SLAs wird quartalsweise geprüft. Die Service Credits für sämtliche innerhalb eines Quartals festgestellten SLA-Verstöße werden kumuliert und sind insgesamt auf maximal 70 % der für das jeweilige Quartal anfallenden Betriebspauschale begrenzt.

5. Schulung, Wissenstransfer und Dokumentation

5.1 Schulungsleistungen

Der Auftragnehmer führt nach Inbetriebnahme Schulungen durch, die einen Betrieb des LoRaWan-Netzwerkes durch Mitarbeiter der Stadtverwaltung gewährleisten können.

Schulungsunterlagen sind in deutscher Sprache als PDF und bearbeitbare Quelldatei zu liefern.

5.2 Dokumentationsanforderungen

Folgende Dokumente sind spätestens zur Gesamtabnahme vollständig vorzulegen:

- Technische Dokumentation: Systemarchitektur, Netzwerkplan, Konfigurationsübersicht (Gateway- und Sensor-EUIs, DevAddr, Frequenzpläne)
- Betriebshandbuch: Betrieb, Überwachung, Update-Prozesse, Backup/Restore-Verfahren

- Störungshandbuch: häufige Fehlermeldungen und deren Behebung (Troubleshooting Guide)
- Sicherheitskonzept und Schlüsselmanagement-Dokumentation
- Installationsprotokolle aller Gateways und Sensoren (inkl. Fotos, GPS-Koordinaten)
- API-Dokumentation (Swagger/OpenAPI oder gleichwertig)
- Abnahmetest-Protokolle

Alle Dokumente werden im Auftraggeber-Repository (z.B. SharePoint / Git) hinterlegt.

– Ende des Leistungsverzeichnisses –

Version 1.0 | Entwurf | Vertraulich

Informatorisch