WeatherXM Specifications for Third-Party Weather Station Manufacturers

This document outlines the standards, protocols, and hardware specifications that third-party manufacturers must follow to build weather stations compatible with the WeatherXM decentralized network. By adhering to these guidelines, manufacturers ensure their weather stations meet the quality and operational requirements needed to deliver weather data within the WeatherXM network. The goal is to create specs and guidelines that enable different manufacturers to join and contribute to the WeatherXM network.

How WeatherXM works

Overview

WeatherXM is a decentralized network that leverages community-operated weather stations to collect and share hyper-local weather data.. In return for providing high-quality weather data, station owners are rewarded with $WXM tokens, creating an economic incentive for participation. This data is then utilized to provide consumers access to accurate, hyper-local weather services.

Key components

The following are key components of the network. More information can be found on the WeatherXM Network and WeatherXM docs websites.

- **Data Collection and Storage**: Each weather station is uniquely identified within the network and transmits cryptographically signed data securely to WeatherXM's infrastructure from where it is forwarded to decentralized storage. This ensures data integrity and transparency, as all data is authenticated and stored in a tamper-proof manner.
- **Weather Data and Station Verification**: The **Quality of Data (QoD)** mechanism evaluates the accuracy and reliability of the incoming weather data, ensuring that only valid information is rewarded. Data is also accompanied by cryptographic proof of origin, to confirm its authenticity.
- **Location Verification**: Weather station location is verified via a **Proof of Location (PoL)** mechanism using GNSS (Global Navigation Satellite Systems) data (such as GPS, GLONASS etc.) provided by the weather station. This ensures that data is collected at the claimed location.

- **Rewarding**: Stations that provide valid and verified data receive $WXM tokens. If the data, including location, is deemed invalid, penalties may be applied. The reward mechanism encourages reliable data contribution and penalizes manipulative behavior.

Weather Station types

There are two primary types of weather stations, each tailored for different operational environments and communication needs.

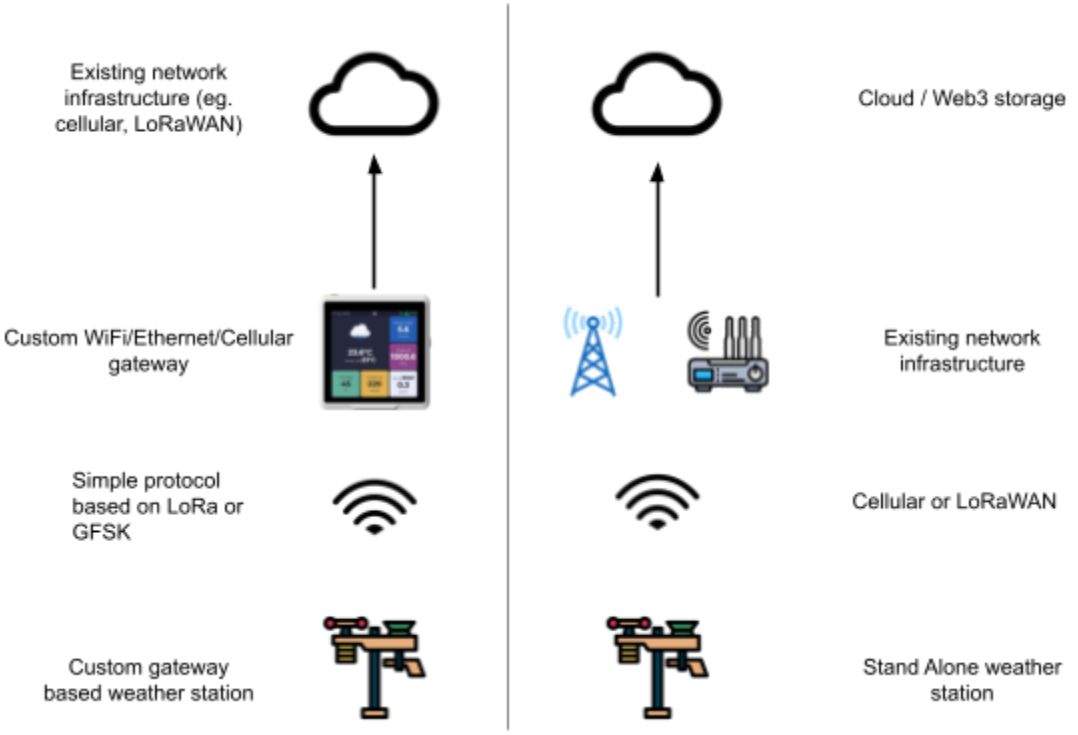
1. **Standalone Weather Stations**

   Standalone weather stations are designed to operate independently by directly connecting to existing network infrastructures such as **LoRaWAN** (e.g., Helium network) or **cellular networks** (e.g., GPRS, HSPA, LTE, NB-IoT etc.). These stations are typically equipped with all the necessary hardware to manage data transmission within the device itself without needing additional external components, Additionally stand-alone weather stations possess the necessary functionality to store, aggregate and execute all the required transformations on the data before sending it to the network.

2. **Gateway-Based Weather Stations**

   Gateway-based stations communicate with a gateway unit using simpler, low-power non-standard protocols based on GFSK or LoRa. The gateway acts as an intermediary, receiving the weather data from the station and forwarding it to the WeatherXM network via a more robust and stable network, such as Wi-Fi or Ethernet. In this setup, the gateway is usually responsible for collecting, storing and applying any possible transformations that may be required on the data, before submitting it to the network, while the station acts as a somewhat-simple data sensor and transmitter with limited capabilities.

   Gateways usually also offer additional features such an LCD display which provides real-time weather data from the connected station as well as other user friendly features.



Custom-gateway based weather station **vs** Standalone weather station

Weather Station specifications

This section describes the core requirements for third-party weather stations, ensuring they meet the operational standards of the WeatherXM network.

Communications

Weather stations must support global operation by accommodating various communication technologies and frequency bands.

Standalone stations come with integrated communication capabilities and as they do not rely on a gateway for relaying their data, they must leverage existing network infrastructure directly, such as cellular, LoRaWAN (eg. Helium), WiFi or others.

Stations utilizing protocols on ISM bands such as LoRaWAN, LoRa, GFSK or other types of radio, should be able to operate across multiple regional frequency bands **configurable within the same unit**, eliminating the need for different hardware versions for different regions. Supported bands should include EU868, US915, AU915, AS923, IN865, RU864, and EU433.

Stations using cellular connectivity must support a range of global cellular technologies such as GPRS, HSPA, LTE, NB-IoT, 5G and others to ensure compatibility with cellular networks worldwide, allowing for data transmission regardless of the station's location.

Weather Data

Weather data must be acquired from the weather station's sensors at intervals **less than 1 minute** to capture accurate, real-time weather conditions, appropriate for each specific parameter. The raw sensor data should be processed and aggregated appropriately (such as through averaging or summing) depending on the nature of the parameter. Data should then be transmitted at intervals **less than 10 minutes**, depending on hardware limitations and protocol used.

Sensors

The following is a list of sensors a weather station must possess along with their minimum specifications. A station is required to meet or exceed these standards.

Parameter	**Range**	**Tolerance**	**Resolution**	**Aggregation method**
Temperature	-40 °C - 60 °C	± 0.5 %	0.1 °C	Average
Relative Humidity	1 % - 99 %	± 0.1 %	3 %	Average
Pressure	300 ~ 1100 hPa	±1 hPa	0.1 hPa	Average
Wind Speed	0 - 50 m/s	5 %	0.1 m/s	Average
Wind Gust	0 - 50 m/s	5 %	0.1 m/s	Max
Wind direction	0 - 359 deg	± 5 deg	1 deg	Vector average
Precipitation (cumulative)	-	± 0.254 mm	0.254 mm	Latest
Illuminance	0 - 200000 lux	± 1 lux	1 lux	Average

Metadata

Weather stations must generate and transmit essential metadata to enable identification, diagnostics, maintenance, and enhance user experience:

- **Unique Identification**: A unique identifier, such as a public key or serial number, serving as the station's identity within the WeatherXM network.
- **Hardware Version**: Identifies the specific hardware model and revision, aiding in support and backwards compatibility.
- **Firmware Version**: Firmware version running in the station, important for updates and troubleshooting.
- **Battery Status**: Battery level to warn user for upcoming maintenance.
- **Cryptographic proof:** Station sensor data should be accompanied by cryptographic proof of its authenticity and integrity.

GNSS capabilities

As weather data is location-sensitive, weather stations must regularly acquire and transmit GNSS coordinates. Ideally, the station should support multiple GNSS constellations (e.g., GPS, GLONASS, Galileo) to improve the reliability and accuracy of positioning.

Power

Stations should be power autonomous, meaning they should operate with minimal user intervention and without having to plug them into mains power. This can be achieved by using rechargeable batteries and solar panels, ensuring continuous operation without frequent maintenance.
Alternatively, if non-rechargeable power sources are used, the station should be capable of operating for **at least one year** before the batteries require replacement. In this case, a solar panel can also be used as an enhancing element to reduce power consumption during sunny days.

Security - cryptographic proofs

The trustless nature of web3 means that all participants of the network must be able to verify the authenticity and integrity of the data. This means confirming that the data originates from a specific weather station at a particular location ensuring data has not been tampered with.

To achieve this, each weather station must possess a unique cryptographic identity and provide verifiable proof that transmitted data whether its weather measurements, GNSS coordinates, or metadata, originates from that specific station. This ensures that the network remains resilient against attempts to game the rewards system. To enable the above, a weather station must implement a number of minimum security measures.

- **Secure Boot Mechanism**: Stations must implement a secure boot process that prevents unauthorized firmware from running on the device.
- **Hardware-Based Secure Element**: Each station should contain a secure element tightly integrated with the microcontroller unit (MCU) in a two-way binding. This means the

secure element operates exclusively with the designated MCU and its signed firmware. Alternatively, an MCU with an integrated secure element can be used.

- **Cryptographic Key Provisioning**: Weather stations must be pre-provisioned during manufacturing with a cryptographic key pair (ECDSA or EdDSA). The public key (or its fingerprint), serves as the station's unique identifier within the WeatherXM network and is made available to WeatherXM to be used during the onboarding process. The private key must be generated and stored securely within the secure element in such a way that it is inaccessible to manufacturers, WeatherXM, or any third parties.
- **Data Authentication**: All data acquired by the weather station, including weather measurements, GNSS coordinates, and metadata must be cryptographically signed using the station's private key. This provides a verifiable proof of origin, ensuring that the data has not been altered and comes from the claimed station.
- **Tamper-proof communication lines**: Sensitive communication channels such as those between the GPS receiver and the MCU, or the secure element and the MCU must be tamper proof. This requires selecting components with appropriate security features to ensure these channels are protected effectively.
- **Ability for over the air firmware upgrades** to ensure bugs and security issues can be addressed by the manufacturer when they arise.

Mechanical specifications

- **IP Rating**: Stations should have a minimum Ingress Protection (IP) rating of IP55 to protect against dust and low-pressure water jets from any direction. Higher ratings are encouraged for improved durability.
- **Operating Temperature:** Components must function correctly within the temperature ranges specified for the sensors, from -40°C to +60°C, to ensure accurate data measurements.

Certifications

The weather station will comply with CE, FCC, RoHS, and any other locally required certifications, ensuring it meets global and regional standards for safety, electromagnetic compatibility, and environmental protection. These certifications guarantee that the device is suitable for deployment in various regions worldwide.

Installation and Maintenance

- **Visible Identification:** The station's unique identifier (e.g, public key fingerprint or serial number) must be displayed on the device in both plain text and QR code formats. This facilitates quick identification and streamlines the onboarding process.
- **Accessible Controls:** Stations should feature hardware buttons or interfaces that allow users to perform essential functions (such as power cycling, factory reset) with minimal effort, considering that weather stations are typically installed in hard-to-reach areas.

- **Installation Aids**: Stations should be equipped with leveling and directional indicators to assist during installation. These features help ensure that users install the station properly, and ensure that collected data is accurate.
- **Repairability:** Sensors susceptible to wear, such as wind vanes, wind cups and other mechanical parts, as well as sensors vulnerable to EMF damage (eg. lightning) should be designed for easy user replacement.

Glossary

The following is a table of terms used throughout this document.

Stand-alone station	A weather station with integrated communications (eg. LoRaWAN, Cellular), computation and storage capabilities, reporting data directly to the network via existing infrastructure (WiFi, Cellular, LoRaWAN etc), not relying on a custom gateway. (for example WeatherXM H2)
Custom Gateway based station	A station with limited, proprietary communication (eg. LoRa), computation and storage capabilities, relying on a bundled gateway to store, possibly transform and relay its data to the network. Sometimes referred to as “console” or “receiver”. (for example WeatherXM D1)

Configuration interface

Weather stations should offer configurable settings to accommodate various requirements and usage contexts. At a minimum the following parameters must be adjustable:

- **Frequency Region**: Allows users to select the appropriate regional frequency band.
- **Data Transmission Interval (gateway-based stations)**: Enables adjustment of how frequently the station transmits its measurements, allowing the gateway to balance between data resolution and power consumption.

These configurations should be accessible through the communication protocol with the gateway for gateway-based stations. For stations equipped with Bluetooth connectivity, an appropriate command interface should be provided for integration with the WeatherXM or other apps.