Securing your weather data with message authentication

We verify radiosonde messages with cryptographically generated Message Authentication Codes (MACs) to prevent tampering or falsification.

Uses HMAC-SHA256, a widely trusted cryptographic standard

RS41-SGM radiosondes encrypt data, for extra security

Other RS41 models prevent tampering with authentication codes but do not encrypt data

1 A secret key is generated for each sounding

2 The key is securely shared with the radiosonde during ground check

3 Radiosonde adds authentication codes to all sent messages

4 The ground station validates messages and discards unauthenticated ones