

Executive Summary (Concise Version)

Bidkee DID Method Enhancement Proposal v1.6 introduces a blockchain-agnostic, dual-signature-based DID method designed for secure and compliant endpoint identification across IoT (e.g., drones), financial (e.g., bank cards), supply chain, and identity certification (e.g., national ID cards).

By separating **issuer authorization** (`superordinateSignature`) from **holder proof** (`signatureMessage`), the proposal enables both regulatory legitimacy and real-time possession verification. Version 1.6 expands use cases (notably identity cards), refines terminology, and enhances compatibility with protocols such as FAA Remote ID. The method remains lightweight and aligns with W3C DID Core 1.0. We welcome community feedback and participation in testing and prototyping.

Compliance Report (with Checklist)

Bidkee DID Method Enhancement — W3C Compatibility Checklist

Compliance Area	Description	Status
W3C DID Core v1.0 Compatibility	Built on standard DID Document JSON-LD structure	✓ Compliant
DID Method Syntax Defined	Uses <code>did:bidkee:[chain]:[identifier]</code> format	✓ Defined
Unique Identifier Support	Ensures uniqueness via blockchain prefix and address	✓ Supported
Controller Declaration	controller field explicitly defines DID control	✓ Provided
Authentication Mechanism	Uses Ed25519 keys and recognized verification methods	✓ Valid
Extension Fields	Adds <code>equipmentID</code> , <code>dynamicData</code> without altering core DID spec	✓ Reasonable
Security Design	Employs dual signatures, SHA-256 hashing, JCS normalization	✓ Secure

Compliance Area	Description	Status
Privacy Considerations	Supports ECDH key exchange and AES encryption	✓ Addressed
Blockchain Agnosticism	Supports any chain with cryptographic signatures (e.g., Kaspas, Polygon)	✓ Compliant
CRUD Operations Defined	Includes clear flows for Create, Resolve, Update, Deactivate	✓ Documented
Use Case Coverage	Applies to drones, payments, logistics, identity verification	✓ Broad
Intellectual Property	Disclosed under W3C CLA, with relevant patent details provided	✓ Transparent
Open Specification	Available for public review, testing, and contribution	✓ Open Source Intent

✓ **Conclusion:** This proposal meets the fundamental requirements of a W3C-compliant DID method. It is ready for community discussion, experimental implementation, and candidate registration consideration.

GitHub: <https://github.com/bidkee>