Executive Summary: Traveler Profile Identifier and Credential Model

This executive summary presents a high-level overview of the Traveler Profile MVP design, focusing on its identifier strategy, flexible credential model, and micro-sharing capabilities.

# 1. Identifier Strategy

- The Traveler Profile is anchored by a UUIDv7, ensuring global uniqueness and compatibility with legacy Hospitality & Travel (H&T) systems.  
- A traveler-controlled Decentralized Identifier (DID) is optionally linked to the profile. This enables SSI-compatible use cases, with the traveler as the DID controller.  
- Legacy systems can continue to use internal IDs by mapping them to the Traveler Profile’s UUIDv7.

# 2. Credential Variation

- The Traveler Profile is passive data, not an active cryptographic entity.  
- Third-party attestations (e.g., physician-issued health or accessibility records) may be signed using the issuer’s DID, and bound to the traveler’s DID, but they are not limited to the Verifiable Credential (VC) format.  
- Supported evidence formats include VC, JWS, COSE, PKCS#7, HL7 FHIR signatures, and others.

# 3. Micro-Sharing

- Travelers or their delegated AI agents can repackage subsets of the profile to respond to travel service queries.  
- These micro-profiles contain only the relevant data, signed by the traveler’s DID or the delegate’s DID.  
- Each micro-profile is ephemeral and purpose-limited, discouraging long-term storage by verifiers.

# 4. Key Benefits

- \*\*Global interoperability\*\*: UUIDv7 works in all systems; DID enables SSI features.  
- \*\*Flexibility\*\*: Evidence can be carried in multiple formats, avoiding lock-in to VCs.  
- \*\*Traveler sovereignty\*\*: The traveler controls their DID and can delegate authority when needed.  
- \*\*Privacy\*\*: Micro-sharing ensures minimal disclosure per transaction.