Traveler Profile Identifier and Variation on Verifiable Credential

This document outlines the proposed identifier strategy for the Traveler Profile, and a variation on the Verifiable Credential (VC) model suitable for the Hospitality & Travel (H&T) domain. It emphasizes practical interoperability with both SSI and non-SSI stacks, while supporting privacy-preserving micro-sharing.

# 1. Identifier Strategy

For the MVP release, the Traveler Profile will use a UUIDv7 as the primary identifier. This ensures globally unique, sortable identifiers that are well supported across legacy systems. In addition, a DID (Decentralized Identifier) may be associated with the profile to enable SSI use cases. The controller of this DID is the traveler themselves, representing their authority as the holder.

This dual approach allows the profile to be recognized by legacy systems using UUIDs while also enabling SSI-compatible systems to verify the profile through the traveler's DID. The UUIDv7 is immutable, while the DID provides a flexible anchor for cryptographic proofs and key rotation.

# 2. Variation on the Verifiable Credential

Unlike conventional approaches where any third-party issued data is assumed to be a Verifiable Credential (VC), this model treats the Traveler Profile as a passive data object that can optionally be accompanied by signed evidence. The evidence may be in the form of a VC, but it may also take other standardized formats such as JWS, COSE, CMS/PKCS#7, or HL7 FHIR signatures. The traveler, using their holder DID, acts as the binding point for these proofs, ensuring that the evidence applies to them.

This approach allows health, accessibility, or other sensitive records to be signed by an issuer (e.g., a physician using their controller DID) and bound to the traveler’s DID without forcing all such data into the VC model. The Traveler Profile can thus be viewed as an extension or container for VC-like data, without being limited to the VC data model.

# 3. Micro-Sharing and Repackaging

The Traveler Profile supports micro-sharing: the ability to selectively disclose only the minimal subset of profile data relevant to a specific travel service query. This prevents over-disclosure and aligns with privacy best practices.

Travelers, or their delegated AI agents, may repackage sub-sets of the profile data in response to service provider requests. This packaging process may include trimming irrelevant fields, annotating fields with purpose-specific constraints, and signing the result. The signing can be done directly by the traveler (using their holder DID) or via delegation to an AI agent authorized to sign on their behalf.

The result is a signed micro-profile: a transient, purpose-limited data package that can be presented to a verifier. These micro-profiles should have explicit expiration times and should discourage long-term storage by verifiers.

# 4. Governance Implications

This identifier and credential variation model has several governance implications:

- Travelers retain sovereignty: they control their DID and can rotate keys without invalidating the profile.  
- Legacy systems remain compatible: UUIDv7 provides a stable anchor for mapping existing internal identifiers.  
- Evidence is flexible: third-party assertions can be carried in multiple formats, not just VC, supporting diverse domains such as healthcare.  
- Privacy is preserved: micro-sharing ensures that only the necessary data is disclosed per transaction, reducing risk of correlation or surveillance.

# 5. Summary

The MVP Traveler Profile model combines a UUIDv7 identifier with an optional traveler-controlled DID, and allows evidence to be attached in multiple signed formats. It supports micro-sharing and delegated signing, enabling travelers and their AI agents to safely interact with both SSI and non-SSI Hospitality & Travel stacks. This approach ensures both global uniqueness and forward compatibility with SSI ecosystems.