

Trust Management of Identity Wallets

Wallet Unit Attestation & Global Interoperability

Juliana Cafik | Independent Expert | Standards & Solutions Architect

Identity Wallet Attestation

Cryptographic proof verifying a wallet's integrity, security and authenticity to a Relying Party



CRYPTOGRAPHIC
BINDING



ASSURANCE OF SECURITY



APPLICATION
AUTHENTICITY

Identity Wallet Attestations in an AI Forward World

Shift the security paradigm from analyzing presented data to verifying its cryptographic origin



HARDWARE BOUND
CONTROL PLANE



ACTIVE TRUST



KINETIC PROVENANCE

Identity Wallet Attestations & Relying Parties

Deliver safe, consistent customer experiences & meet rigorous risk & regulatory requirements

Decouple the user-experience of interacting and authenticating from the technical burden of proofs

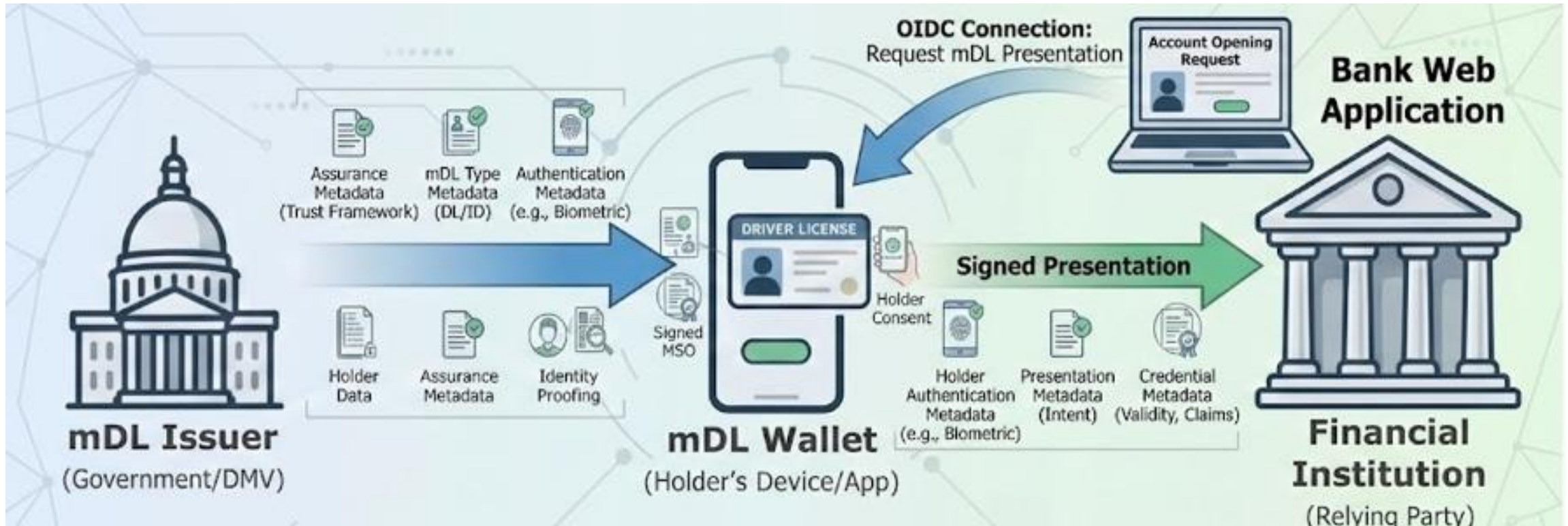
1. Meet their customer where they are, keep them safe and reduce friction:

- Establish intent & corresponding consent
- Invisible Cryptography
- Consistent Journeys
- Privacy First
- Zero Trust

2. Satisfy operational, regulatory & risk requirements

- Cryptographically bound intended action & consent
- Mathematical proofs
- Machine readable evidence
- Standardized claims & values
- Active trust & auditability
- Reduce risk
- Lower Operational Costs

NIST NCCoE mDL (Phase 1) Architecture + KYC Extended Claims and Values Active Trust Model (illustrative)



OIDF KYC & IDA: Protocol, format and jurisdiction-agnostic framework for identity claims to directly support RPs in establishing a defensible “reasonable belief” of customer identity.

Global Interoperability

To achieve global interoperability, Relying Parties need a standardized way to request and verify wallet attestations without building custom APIs for every wallet provider globally.

THANK YOU!