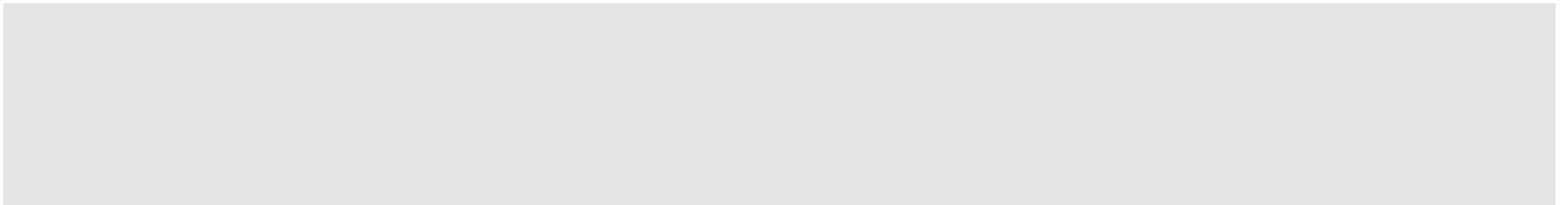


RUBIX DID— Own Your
Identity



Self-Signed Identity



Existence — Users have independent existence.



Control — Users control their identities.



Access — Users have access to their own data & control who else can access them



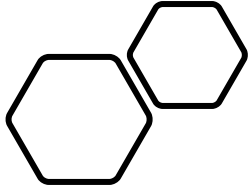
Portability — Information and services about identity are transportable



Consent — Users must agree to the use of their identity.



Minimization — Users can disclose only selected information



Register self-owned identities

Create

- Create Unique IDentity (UID) and derive shares using Non-Linear Secret Sharing (NLSS)

Map

- Map any digital information to UID

Prove

- Prove ownership of UID by proving ownership of secret share (ZK proofs)

Verifiable Claims



Get signed by verifiers by submitting [verifiable presentations](#)



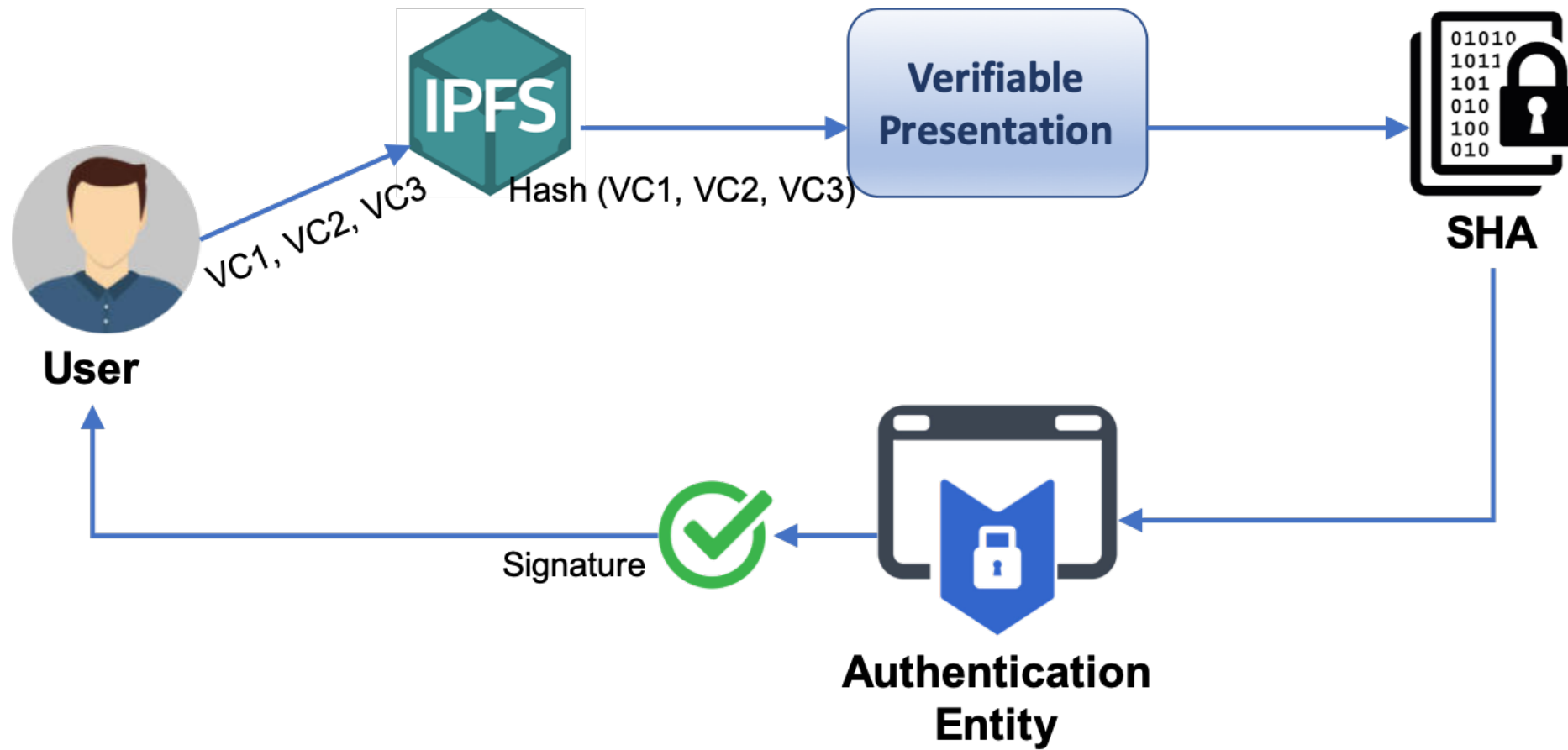
Can get multiple verifications for same [verifiable credentials](#)

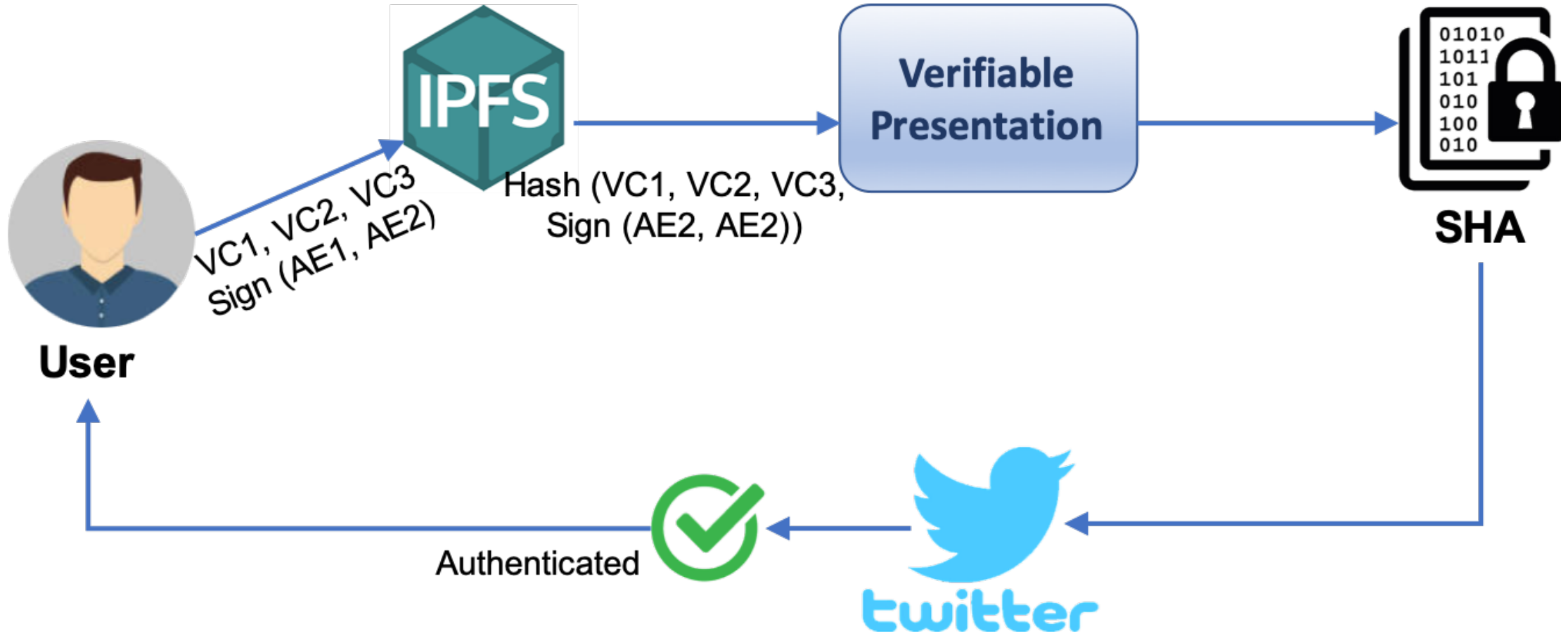


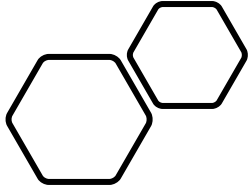
Uses NLSS based Challenge – Response to achieve [selective disclosure](#)



Verifiable credentials in JSON/XML Form







Privacy and Security Features



ULTRA-SCALABLE - < 100MS FOR
VERIFICATION (MILLIONS OF
ASYNCHRONOUSLY PARALLEL
VERIFICATIONS)



PRIVACY & FAIRNESS – SELECTIVE
DISCLOSURE WITH TAMPER-PROOF ,
IRREFUTABLE SIGNATURES



KEY RECOVERY BY NLSS SCHEMA



KEY DERIVATION & RECOVERY USING
BIOMETRICS FOR ADDED SECURITY

Interoperability and Open Standards

