Executive Summary Prepared December 19, 2025

GBBC GSMI 6.0

DIGITAL IDENTITY & PRIVACY

KEY TAKEAWAYS

UNPACKING DIGITAL IDENTITY

Digital identity has become critical for accessing finance, government services, healthcare, and cross-border digital interactions. At the same time, rising privacy concerns, cyber risks, and regulatory requirements (e.g., data minimization, consent, transparency) make stronger, privacy-preserving approaches essential

THE CHALLENGE

As digital services scale globally, identity frameworks must balance trust, security, interoperability, and user control, while protecting people from misuse and over-collection of personal data. Traditional identity models often create fragmentation, excessive exposure, and dependence on centralized intermediaries

THE WEB3 ECOSYSTEM

Digital identity and privacy are foundational components of digital ecosystems. Decentralized identity, verifiable credentials, and privacy-enhancing technologies can enable secure, user-centric interactions across sectors

LANDSCAPE OF PRIVACY-PRESERVING SOLUTIONS

TOOLS

- Attribute-Based Encryption (ABE)
- Biometric Template Protection
- Commitment Schemes
- Differential Privacy Libraries
- Digital Signature Schemes
- Fully Homomorphic Encryption (FHE)
- Hardware Security Module (HSM)
- Hash Functions
- Multi Party Computation (MPC)
- Pseudonymization Engines
- Public-Key Encryption
- Ring Signature Schemes
- Symmetric Encryption
- Tokenization Engines
- Trusted Execution Environment (TEE)
- Zero-Knowledge Proofs (ZKPs)

PROTOCOLS

- Anonymous Credential Protocols (Idemix)
- Confidential Transaction Protocols (CT)
- Data Marketplaces: Privacy-Preserving Data Market Protocols
- Decentralized Identifier (DID) Protocols
- Federated Learning with MPC/DP
- Mixing/ Tumbling Protocols (CoinJoin)
- Privacy Pools Protocol
- MPC Key Management/Sig & Multi-Sig Protocols
- Privacy-Preserving Smart Contract Protocols
- Privacy Tokens
- Remote Attestation Protocols (TEE/ TPM)
- Shielded Transfer Protocols (Zcash, etc.)
- SSI Protocols
- Verifiable Credential (VC) Protocols

TECHNIQUES

- Anonymity Set Enlargement (Mixing/Pools)
- Association Set Compliance
- Biometric Template Protection Techniques
- Compute-on-Encrypted-Data
- Data Minimization by Design
- Differential Privacy
- Pseudonymization
- Selective Disclosure
- Tokenization
- Unlinkability

ACCESS THE FULL REPORT

GBBC.IO/GSMI