IDEMIA PUBLIC SECURITY

Modernizing Digital Identity for Stablecoin Regulation under the GENIUS Act

Summary of Response to RFI: Request for Information and Comment Related to the Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act

Introduction

The GENIUS Act, together with Executive Order 14178, establishes a comprehensive regulatory framework for U.S. stablecoin issuers, aiming to promote innovation, consumer protection, and national security in digital assets. IDEMIA, a leader in digital identity and biometrics, responded to the U.S. Treasury's request for information by advocating for the adoption of modern, privacy-preserving digital identity solutions—specifically Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs)—to strengthen anti-money laundering (AML) and know your customer (KYC) and customer information program (CIP) controls in the evolving digital asset ecosystem.

IDEMIA's Expertise and Solutions

IDEMIA brings over 40 years of experience in secure identity credentials and 20+ years in document authentication. Its digital identity platform supports issuance, validation, and authentication of both physical and digital IDs, including mDLs and VCs, across government and commercial sectors. With decades of proven experience in biometrics, digital identity, and document authentication, IDEMIA has set the standard for trusted identity verification across a range of high-stakes domains—including border security, law enforcement, and telecommunications.

We are bringing these tested capabilities to address emerging challenges in the financial services and digital asset ecosystem, ensuring both regulatory compliance and consumer privacy to meet core obligations as related to KYC/CIP and embedding modernized digital identity and credential capabilities that strengthen controls against illicit activities and security vulnerabilities in the sector.

Combatting Illicit Digital Activities and Protecting Privacy

Identity as the Foundation of Financial Crimes Compliance

Effective AML and KYC depend on robust identity verification—establishing, authenticating, and authorizing individuals using trusted sources. Innovations in digital identity, such as mDLs and VCs, enhance security, reduce fraud, and protect PII.

Challenges in Digital Asset Services

Traditional KYC methods are inadequate for digital asset providers, especially with non-custodial wallets and anonymous transactions. The rise of AI-driven fraud, data breaches, and privacy coins further complicates compliance. Modern identity solutions must enable privacy-preserving verification, support interoperability, and empower users to control their data.

Addressing Vulnerabilities: Decentralized Identity Technologies

Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) allow individuals to control their digital identities, share only necessary information, and enable secure, cross-jurisdictional KYC. These credentials are cryptographically signed, tamper-proof, and can be bound to biometrics for higher assurance.

The **Issuer-Holder-Verifier model** enables the transition toward a consumer-centric approach to data control. In this model, consumers become the rightful holders of their personal data and establish direct relationships with verifiers. This ensures a secure and transparent process for data verification with the consumer's consent and without compromising privacy—a stark departure from the traditional centralized and intermediary-dependent model. This new model attaches attestable attributes to an individual or entity alongside financial data, account credentials, and other identifiers. It allows bank and payments service providers to validate an individual's verified status without exposing sensitive information.

Enabling VCs in KYC/CIP Flows

Combining biometric authentication, document verification, and VCs provides strong fraud protection and privacy. For example, a passport chip can be ingested by wallet software, creating a tamper-proof credential for account access. This process is secure, fast, and privacy-preserving. DIDs/VCs can be embedded at the time of onboarding, and enable user-centric control in a privacy preserving way. Such capabilities embed KYC/CIP controls for both traditional and web-based financial services applications, interoperability between traditional banking, payments and decentralized services, while ensuring KYC/CIP compliance for institutions covered by such obligations.

Modernizing BSA Enforcement: The Role of Certification

Financial regulators should partner with organizations like the Kantara Initiative, which certifies identity service providers against rigorous standards (e.g., NIST 800-63). Certification ensures that digital credentials meet compliance, security, and privacy requirements, enabling reliance agreements between financial institutions and reducing redundant KYC processes by and between service providers—traditional and web-based. Enabling a consistent and certified assurance framework enables impartial third-party assessment and certification for identity service providers, to support the obligations for KYC/CIP for digital asset services providers (and financial services more broadly).

Key Considerations and Recommendations

1. Evolving Risks in Digital Financial Services

Digital asset services face risks similar to traditional finance—identity theft, account takeover, synthetic identities, and AI-driven threats like deepfakes. These risks are heightened by remote onboarding and the digital nature of transactions. Overreliance on static personally identifiable information (PII) and physical documents increases fraud and privacy risks.

2. The Role of Digital Identities and Verifiable Credentials

Modern digital identity solutions, such as DIDs and VCs, embed privacy and user control by design. Users can share verifiable credentials with explicit permissioning, reducing exposure of sensitive PII. These technologies enable secure, remote onboarding and ongoing KYC compliance, supporting both traditional and decentralized financial services.

3. Mobile Driver's Licenses (mDLs) as a Root of Trust

Mobile driver's licenses (mDLs), issued by state authorities and stored securely on user devices, offer a logical evolution for identity verification. They provide cryptographic security, enable selective data sharing, and are recognized under national standards (e.g., REAL ID, NIST). Secure mDLs on mobile phones enable device-centric, universally applicable identity verification, supported by IDEMIA's hardware and software solutions.

Key Recommendations:

- Treasury and FinCEN should encourage the adoption of DIDs/VCs and mobile identities (such as mobile driver's licenses) as mechanisms that meet the requirements for KYC/CIP obligations. Guidance should affirm that mDLs and verifiable digital credentials issued by competent authorities and meeting aforementioned certification standards to meet regulatory requirements.

- Treasury and FinCEN should work with competent certification bodies, such as Kantara to ensure they been verified pursuant to NIST Identity Assurance Level 2 (IAL2), and such certification promotes a landscape where multiple technologies can thrive, preventing vendor lock-in and strengthening the entire financial system.

Conclusion

As digital assets and web-native financial services expand, modernized identity solutions are critical for security, compliance, and inclusion. DIDs/VCs and mDLs offer privacy, interoperability, and user control, aligning with the GENIUS Act's goals. IDEMIA stands ready to support Treasury and FinCEN in advancing these technologies for a safer, more innovative financial ecosystem.

Further Reading

1. Federal Register Notice on GENIUS Act
2. White House Fact Sheet on Digital Asset Markets
3. FFIEC Mission
4. Kantara Initiative
5. NIST 800-63 Digital Identity Guidelines
6. FATF Guidance
7. National Cyber Security Center of Excellence: Digital Identities – Mobile Driver's License (mDL)
8. W3C Verifiable Credentials Data Model v. 2.0
9. Personal Financial Data Rights Rule