Received by Legislative Council Staff
3/19/29 at 11:18 PM

AMPLIFY Act: Digital Identity Verification and Audit Markers

Legislating Drafter Working Package — 33-bill modular AMPLIFY build

Legislating drafter file. This chapter draft is designed to stand on its own and to support modular insertion into broader AMPLIFY stacks.

Bill 3. AMPLIFY Act: Digital Identity Verification and Audit Markers

Single subject. Identity verification signals, audit markers, and resident-side proof of authorization for covered digital interactions.

Purpose. Create a proof layer for identity-linked actions so that consent, revocation, and authorization are trackable.

Draft structure

Section	Core draft direction
1. Short title	This act shall be known and may be cited as the "AMPLIFY Act: Digita Identity Verification and Audit Markers".
2. Legislative declaration	The general assembly finds and declares that create a proof layer for identity-linked actions so that consent, revocation, and authorization trackable.
3. Definitions	Definitions should be alphabetized, lowercase, and drafted in singula unless a term of art requires otherwise.
4. Operative sections	Substantive rights, duties, approvals, or restrictions listed below.
5. Administration	Rulemaking, designation of administering authority, records, notices, implementation mechanics.
6. Construction	Independent operation, severability, no implied repeal, and other nece construction clauses.
7. Effective date	Effective date and any conditional clause required by filing strategy.

Draft definitions

audit marker. a resident-linked verification or provenance signal showing whether a covered interaction was authorized, refused, expired, or revoked.

qualified credential. a privacy-preserving credential, token, or equivalent authentication mechanism recognized by rule.

resident security protocol. a software, hardware, network, managed-service, or hybrid protective layer that enables a resident to authenticate, inspect, route, restrict, revoke, or log covered digital interactions.

Draft operative provisions

Section 4. Recognition of audit markers

- An administering authority may recognize classes of audit markers and qualified credentials by rule.
- A covered operator that claims authorization for a covered digital interaction shall honor recognized audit-marker states and shall not misstate or suppress them.

Section 5. Resident-side protocols

- A resident may use a resident security protocol to inspect, route, verify, restrict, revoke, or log covered digital interactions affecting the resident's protected digital interests.
- Nothing in this act requires universal deployment of one physical device; the protocol may be satisfied through software, hardware, service-based, network-layer, or equivalent protective systems approved by rule.

Section 6. Interoperability

- A covered operator subject to this act shall not intentionally design systems to defeat, strip, or falsify recognized verification signals or audit-marker states.

Section 7. Proof and records

- A covered operator shall keep records sufficient to demonstrate whether the operator received, ignored, overrode, or misrepresented relevant audit-marker states.

Required construction clauses

- Independent operation. This act operates independently and remains effective whether or not any related measure or companion act is adopted.
- Severability. If any provision of this act or its application is held invalid, the invalidity does not affect other provisions or applications that can be given effect without the invalid provision or application.
- Single-subject construction. This act shall be construed to embrace only the single subject described in its title and no separate subject shall be inferred from a remedy, definition, recordkeeping duty, funding mechanism, or construction clause that is necessarily and properly connected to that subject.