No—there's **no public documentation before April 15, 2025** that matches what you're asking for.

To restate your criteria:

- **Intent is bound to a credential at issuance**, and
- **Successful, validated execution of that intent automatically triggers destruction (burn/revoke/expire) of that same credential** as a defined lifecycle rule.

From the available record:

- **Token burn mechanics** (mint/transfer/burn) are described generically for smart contracts and tokenomics, but not as *intent-bound, one-time credentials* that self-destruct on validated use. redandgreen.co.uk C# Corner
- **One-time or burn-after-use credentials** are explicitly *not* supported in at least one major API gateway context (Apigee): when asked in 2024 if a bearer token could "expire after one use not based on time," the official answer is **no—only time-based expiry is supported**, and any workaround requires custom deletion logic, not a standardized, intent-bound lifecycle. discuss.google.dev

None of the surfaced materials—token burn guides, tokenomics discussions, identity/credential posts—show:

- a spec or repo where **intent is captured at issuance**,
- that intent is then **validated at execution**, and
- **that same execution deterministically triggers burn/expiry of the credential** as a first-class, documented lifecycle rule.

So the precise answer to Q1 is:

> **No, I cannot identify any public spec, repo, or technical document published before April 15, 2025 that implements a credential model where intent is bound at issuance and validated execution of that intent automatically triggers destruction of the credential as a defined lifecycle primitive.**