A L E T H I A

Citizen Credential Specification

How citizenship is proven without being revealed

> *Citizenship is a fact about a person. The credential proves the fact without disclosing the person.*

Introduction

This document specifies the Alethian Citizen Credential — the cryptographic proof that a given holder is a verified citizen of Alethia. It is a companion document to the Technical Specification, focused specifically on the credential system that underpins every interaction within the nation.

The credential is the single most important technical artefact in Alethia. It is what makes everything else possible. It is the mechanism by which citizens prove their standing without surrendering their privacy, by which Alethia knows who its citizens are without tracking what they do, and by which the Charter's promise of dignity is made technically real.

This specification is written in two registers. The main body explains what the credential is, what it contains, and how it works in language any citizen can understand. The technical appendix at the end provides the implementation-level detail that builders will need.

This document is part of the founding library of Alethia. Companion documents include the Charter (the constitution), the Technical Specification (the broader architecture), the Founding Pathway (how Alethia comes into being), and the Visual Identity Guide (the Mark, the eight pillars, and design standards). All are available in the Library of Alethia, the public record of the nation, open to citizens and non-citizens alike.

Part I — What the Credential Is

The Alethian Citizen Credential is a piece of mathematical proof. When a candidate passes the Entrance Examination, the credential is issued to them. From that moment, they can use it to prove to any Alethian service that they are a valid citizen — without revealing which citizen they are.

The credential is not a card. It is not a username and password. It is not a key in the traditional sense. It is closer to a passport that the bearer can show without the inspector ever seeing the name inside it.

The technique that makes this possible is called a zero-knowledge proof. A zero-knowledge proof is a mathematical procedure by which one party can prove to another that a statement is true, without revealing any information beyond the truth of the statement itself. In plain language: the credential can prove "I am a citizen" without proving "I am specifically this citizen."

Why This Matters

Traditional digital identity systems — accounts, logins, profiles — work by linking every action a person takes to a persistent identifier. The platform knows who you are at every moment, even when other parties do not. This is the architecture of surveillance, dressed up as convenience.

Alethia rejects this architecture. The credential is designed so that even Alethia itself cannot trace a citizen's activity back to a real-world identity. The system is not asking citizens to trust it not to misuse their data — it is built so that no such trust is necessary.

> *A privacy promise that requires trust is a promise that can be broken. A privacy guarantee that requires no trust cannot be.*

Part II — What the Credential Contains

The credential is a small data object. What it contains is as important as what it deliberately does not contain.

What is Included

- A cryptographic public key — a unique mathematical value that identifies the credential without identifying the holder.
- The Arbiter's signature on that public key — proof that this credential was issued by Alethia, not forged by an outside party.
- The year of issuance — useful for understanding how long the credential has been valid, but never the exact date or time.

- The credential's validity status — confirmation that the credential has not been revoked.

What is Deliberately Excluded

- No real-world name.
- No email address, phone number, or other contact information.
- No date of birth, country of residence, or any demographic data.
- No photograph, biometric data, or physical descriptor.
- No examination score, examination session identifier, or any reference to how the credential was earned.
- No record of which Alethian services the credential has been used to access.
- No internet address, device identifier, or hardware information.

This list is exhaustive. There is no hidden field, no metadata layer, no internal log entry that contains any of these items. They are not stored encrypted; they are not stored at all.

Part III — Issuance

The moment a candidate passes the Entrance Examination, the credential is generated and issued. The process is deliberately one-way: no record is preserved that links the credential back to the examination session that produced it.

The Issuance Sequence

When a candidate completes the examination:

- The examination session generates a fresh cryptographic keypair on the candidate's own device. The private half of this keypair never leaves the candidate's control. The public half is sent to the Arbiter.
- The Arbiter signs the public key with its own credential authority key. This signature is what makes the credential valid — it proves that Alethia, and only Alethia, issued it.
- The signed credential is returned to the candidate's device.
- The examination session itself is destroyed. The questions answered, the time taken, the order of selections, the network connection used — all of this is deleted. No archive is kept.

- The Arbiter records only that one more credential has been issued. It does not record to whom, when within a given day, or in association with what session.

From the moment of issuance, the credential exists only on the candidate's device, with their private key. Alethia retains no copy. The Arbiter cannot recover the credential, cannot regenerate it, and cannot read it. This is not a limitation of the system. It is the system's core protection.

Part IV — Storage and Custody

The credential is stored entirely on the citizen's own devices. The Alethian client — desktop or mobile — holds the credential in a secure local store, encrypted with a key derived from the citizen's chosen unlock mechanism (a password, a biometric, or a hardware key).

Citizens may copy their credential between their own devices using a secure transfer procedure built into the client. They may also export it to a secure backup of their choosing — a hardware security module, an encrypted file, a printed cryptographic representation. The choice is theirs. The responsibility is theirs.

Multi-Device Use

A citizen may hold their credential on multiple devices simultaneously — for example, a desktop computer and a phone. Each device presents the same underlying credential. This is treated by Alethia as a single citizen with multiple access points, not as multiple citizens.

Loss of Credential

If a citizen loses their credential — through device failure, accidental deletion, or any other cause — they cannot simply request a new one. The recovery process is defined in Part VII of this document, and exists to balance the protection against impersonation with the practical needs of citizens who have genuinely lost access.

Part V — Presentation and Use

Citizens use their credential every time they interact with Alethia, but the credential itself never travels across the network. What travels is a freshly generated proof — a one-time mathematical statement asserting that the citizen holds a valid credential, without revealing which credential.

The Presentation Sequence

When a citizen accesses any Alethian service:

- The Alethian client generates a fresh zero-knowledge proof on the citizen's device. The proof asserts: "The holder of this proof possesses a valid Alethian credential that has not been revoked."
- The proof is sent to the service the citizen is accessing. The service verifies the proof mathematically. If the verification succeeds, the citizen is granted access.
- The service learns nothing other than that a valid citizen is present. It does not learn which citizen, what other services they have used, when they last accessed something, or anything else. The proof is mathematically incapable of revealing this information.

Each proof is unique. The proof generated to access the Commons at noon is mathematically unrelated to the proof generated to access the Market five minutes later. Alethia cannot correlate two proofs to infer that they came from the same citizen, because the proofs themselves contain no information that would permit such correlation.

The Pseudonymous Handle

To participate in social activity — posting in the Commons, sending messages, trading in the Market — citizens choose a pseudonymous handle. This handle is what other citizens see and interact with. The handle is linked to the credential cryptographically, but the linkage is opaque to Alethia. The handle persists across a citizen's activity within their chosen context; what does not persist is any external identity attached to it.

A citizen may use one handle for everything they do in Alethia, or they may choose to maintain different handles for different contexts. The choice is theirs.

Part VI — Revocation

Citizenship can be revoked. This happens in two circumstances: when a citizen chooses to leave Alethia voluntarily, or when a Citizen Tribunal issues a Fourth-Level sanction under the Charter for the most serious violations.

How Revocation Works Technically

When a credential is revoked, its identifier is added to a public revocation list maintained by the Arbiter. The revocation list is checked as part of every credential verification. Any credential whose identifier appears on the list will fail verification, regardless of what other proofs the citizen attempts to present.

The revocation list is public. Any citizen, and any external party, may read it to verify that the system is operating honestly. What the list contains is the cryptographic identifiers of revoked credentials — not the identities of the citizens those credentials belonged to.

Voluntary Departure

When a citizen chooses to leave Alethia, their credential is added to the revocation list as a departed status. Departed credentials are distinguished from revoked credentials in the public record — Alethia does not stigmatise citizens who leave by choice. A departed citizen may always return; they will need to pass the Entrance Examination again, but their record of voluntary departure carries no penalty.

Tribunal-Imposed Revocation

Revocation as a sanction is the most severe punishment Alethia can impose. It requires a unanimous verdict from a Citizen Tribunal, may be appealed once before a fresh tribunal panel, and is recorded with full transparency in the public archive — though the identity of the revoked citizen is recorded only by their handle, never by any real-world identifier.

Even revoked citizens retain the absolute right of data export defined in Article VII of the Charter. They lose access to Alethia. They do not lose access to what was theirs.

Part VII — Recovery

The privacy guarantees of the credential system have an unavoidable cost: if a citizen loses their credential, Alethia cannot simply look them up and reissue it. There is no record to look up. There is no list of citizens. There is only the cryptographic fact of validity, which lives on the citizen's own device.

Alethia does not pretend this is a small problem. It is a real cost, paid in exchange for real protection. The recovery process is designed to be as humane as possible while preserving the protections that make Alethia what it is.

The Standard Recovery Path

A citizen who has lost their credential must retake the Entrance Examination. Upon passing, a fresh credential is issued through the standard issuance process. The new credential is mathematically independent of the lost one — the recovering citizen begins with a clean cryptographic identity. Their previous handle, their previous Eranos balance, and their previous activity are not transferred. Recovery is, technically speaking, indistinguishable from new citizenship.

This is harsh by design. Easy recovery is incompatible with the privacy guarantees of the credential system. A system that allowed Alethia to restore your credential by checking your identity would be a system that knew your identity. Alethia is not that system.

The Recovery Beacon (Optional)

Citizens who wish to make recovery easier may choose to set up a Recovery Beacon at the time their credential is issued. A Recovery Beacon is a small, encrypted, citizen-controlled document containing recovery hints — typically a passphrase, a list of trusted contacts, or a hardware key reference — stored entirely on the citizen's own infrastructure (a USB drive, a printed sheet in a safe, a trusted family member's device).

If the citizen loses their primary credential but retains their Recovery Beacon, the beacon can be used to re-derive their previous credential, preserving handle, balance, and activity. The beacon never touches Alethia's infrastructure and cannot be requested by Alethia. It is the citizen's own backup, by their own design.

Use of a Recovery Beacon is entirely optional. Many citizens will prefer the simpler model of accepting that loss of credential means starting fresh. Both choices are equally valid.

Part VIII — What the Credential Cannot Do

Honesty about the boundaries of the credential system is essential. The credential is powerful within its domain and limited outside it. The following list is a deliberate, public statement of what the credential is not designed to do.

The Credential Cannot Identify You

The credential proves citizenship. It does not prove who you are in the physical world. Alethia knows nothing about your real identity, your location, your nationality, your appearance, or your history. The credential is incapable of being read back into that information.

The Credential Cannot Be Forged

Without the Arbiter's signing key, no one can issue a valid credential. The Arbiter's key is itself protected by constitutional safeguards and held under threshold control — no single component, human or otherwise, can sign credentials alone. A forged credential cannot pass verification.

The Credential Cannot Be Transferred

The credential is bound to a private key held by the citizen. Without the private key, the credential cannot be used by anyone else. Even if a citizen gave their credential file to another person, that person could not present valid proofs without also possessing the private key, which exists only on the original citizen's authenticated device. Citizens are bound by the Charter not to share their credentials, and the system makes such sharing technically pointless.

The Credential Cannot Track You

Because each presentation generates a fresh proof unrelated to any previous one, Alethia cannot correlate a citizen's activity across services or across time. The credential is mathematically incapable of leaving a trail.

The Credential Cannot Replace Your Legal Identity

Alethian citizenship is a status within Alethia. It does not exist in the physical world's legal systems. The credential cannot be used to vote in physical elections, to access government services in any country, to open bank accounts, or to verify any aspect of your real-world

existence. Citizens of Alethia remain subject to the laws and identity systems of the countries they physically live in, exactly as the Charter's Section 19 specifies.

The Credential Does Not Make You Anonymous to Other Citizens

Within Alethia, your handle is visible to other citizens you interact with. They will see what you post, what you trade, what you say. The credential protects you from Alethia learning your real identity; it does not protect you from the social consequences of your conduct as a citizen. The Code of Civic Conduct still applies. Citizen Tribunals can still sanction citizens for harmful behaviour under their handles.

The Credential Cannot Prevent Its Own Theft

If a citizen's private key is stolen, the thief possesses a mathematically valid credential. Alethia cannot detect the theft through observation alone, because doing so would require the kind of continuous monitoring that the privacy architecture is designed to prevent. The mitigations — citizen-initiated revocation, key rotation, heuristic alerts, and Recovery Beacons — significantly reduce the risk and the window of exposure. But they do not eliminate it. This limitation is stated honestly in Part IX, together with the full response framework.

Appendix: Implementation Detail for Builders

The following appendix contains technical detail relevant to citizens implementing or auditing the credential system. Other citizens may skip it without missing anything essential.

APPENDIX A — CRYPTOGRAPHIC PRIMITIVES

The credential system is built on well-established cryptographic primitives, each chosen for maturity, broad analysis, and the existence of audited open-source implementations.

- Signature scheme: EdDSA (Ed25519) for the Arbiter's credential signing key, chosen for its small key size, fast verification, and resistance to side-channel attacks.

- Zero-knowledge proof system: Groth16 with BN254 curve in the founding implementation, with planned migration to a post-quantum alternative (likely a STARK-based system) as the technology matures.
- Symmetric encryption: AES-256-GCM for local credential storage.
- Key derivation: Argon2id for password-based key derivation, configured for current best-practice parameters.
- Hash function: SHA-3 (Keccak) for all credential-related hashing operations.

These choices are not permanent. The Arbiter's credential signing scheme, in particular, may need to migrate as cryptographic best practice evolves. Any such migration is itself a citizen referendum matter under the Charter's constitutional amendment process.

APPENDIX B — CREDENTIAL DATA STRUCTURE

A credential, in its serialised form, is a small JSON-like data structure of the following shape:

```
{   "credential_version": 1,   "public_key": "<32-byte Ed25519 public
key, base64-encoded>",   "issuance_year": 2026,   "arbiter_signature":
"<64-byte Ed25519 signature, base64-encoded>",
"revocation_check_endpoint": "<URL of public revocation list>" }
```

Note that the credential does not contain a unique identifier. The public key serves both as the identity of the credential and as the cryptographic anchor for verification. The credential is signed by the Arbiter's known credential authority key. Any verifier who has the Arbiter's public key — which is itself published openly and never changes without constitutional referendum — can verify the credential's authenticity offline.

APPENDIX C — PROOF GENERATION

When a citizen accesses a service, the client generates a zero-knowledge proof. The proof is structured to assert the following statement:

```
STATEMENT:   "I possess a private key whose corresponding public key
is signed by the Arbiter's credential authority,    and whose public
key does not appear on the current    revocation list."  WITNESSES
(kept private):   - The citizen's private key   - The citizen's public
key   - The Arbiter's signature on the public key  PUBLIC INPUTS:   -
The Arbiter's credential authority public key   - The Merkle root of
the current revocation list   - A fresh challenge string from the
verifying service
```

The proof reveals only that the statement is true. It does not reveal the witnesses, which means the citizen's public key, private key, and signature remain unknown to the verifier.

APPENDIX D — THE REVOCATION LIST

The revocation list is implemented as a sparse Merkle tree, allowing both efficient membership proofs ("yes, this credential is revoked") and efficient non-membership proofs ("no, this credential is not revoked"). The Merkle root of the revocation list is published with every Arbiter update and forms a public input to all credential presentation proofs.

Citizens, services, and external auditors may all maintain their own copies of the revocation list. Disagreement between copies is resolvable by reference to the Arbiter's signed root.

APPENDIX E — THE ARBITER'S SIGNING KEY

The Arbiter's credential authority signing key is the single most sensitive technical asset in Alethia. Its compromise would allow forged credentials. Its protection is governed by the following measures:

- Threshold cryptography: the signing key is split into shares held by independent infrastructure components, requiring multiple shares to combine for any signing operation.
- Hardware isolation: signing operations occur within hardware security modules with no general-purpose computation capability.
- Multi-party authorisation: every credential issuance requires authorisation from both the Arbiter's rule engine and the constitutional guardrail layer.
- Public key publication: the corresponding public key is published openly in the Library of Alethia and on every node's public information page, with any change to the public key requiring constitutional referendum.
- Key rotation: the signing key is rotated on a regular schedule defined by citizen poll. Old credentials remain valid through documented transition periods.

APPENDIX F — CLIENT IMPLEMENTATION REQUIREMENTS

Any Alethian client implementation that handles credentials must satisfy the following minimum requirements to be certified for use:

- Open source: the full source code must be published under an OSI-approved licence.
- Reproducible builds: any citizen must be able to verify that the binary they are using was built from the published source.

- Local key custody: the private key must never leave the client device in unencrypted form.
- No telemetry: the client must not transmit any data about its operation to Alethia or any third party beyond what is strictly necessary for service interaction.
- Auditable cryptography: the client must use cryptographic libraries that are independently audited and broadly trusted.
- Citizen-controlled storage: the citizen must have full control over where their credential is stored, including the ability to back it up, transfer it between devices, and delete it.

Clients that fail any of these requirements may not be promoted as Alethian clients. Citizens are free to use any client they choose, but the warning attached to non-certified clients is explicit and unavoidable.

Part IX — Credential Compromise and Response

The credential system is designed to prevent unauthorised issuance. It cannot prevent the theft of a credential that already exists. If a citizen's private key is stolen — through malware, physical device compromise, phishing, or a leaked backup — the thief holds a mathematically valid credential and can present it as the real citizen. Alethia cannot distinguish between a legitimate presentation and a stolen one, because distinguishing them would require surveillance capabilities that Alethia deliberately does not have.

This is a genuine limitation, and this specification states it plainly rather than obscuring it. The mitigations below significantly reduce the window of exposure and the practical risk — but they do not eliminate the threat entirely. No cryptographic credential system does.

Section 9.1: Citizen-Initiated Emergency Revocation

Any citizen who believes their credential has been compromised may initiate an emergency revocation at any time, without waiting for a tribunal, without requiring any authority's approval. This is a unilateral right, exercisable instantly.

Emergency revocation is triggered through the Alethian client on any device where the credential is still held. The revocation transaction is signed by the citizen's own private key — proving that the legitimate holder initiated it — and is propagated immediately to all

Alethian nodes. Once the revocation is confirmed across the network, the credential is invalid everywhere, for everyone, within minutes.

The complication: if an attacker has stolen the private key and the citizen no longer has access to any device holding the credential, the citizen cannot self-revoke, because they cannot sign the revocation transaction. In this case, the citizen must contact the Citizens' Council, present whatever evidence they can of the compromise, and request an assisted revocation. The Council reviews the request and, if satisfied, issues a revocation directly. This process is treated as urgent and has a target resolution time of twenty-four hours.

Section 9.2: Key Rotation

Citizens may voluntarily rotate their credential at any time. Rotation generates a new keypair, has the Arbiter re-sign the new public key, and revokes the old credential. The new credential is mathematically independent of the old one — it cannot be connected to it by any observer — but it remains linked to the same pseudonymous handle and Eranos balance through a citizen-initiated transition record.

Regular key rotation is strongly recommended as a security habit. A citizen who rotates their key quarterly limits the period during which a silently stolen key could be exploited to approximately three months at most. The Alethian client prompts citizens to consider rotation on a schedule they define, but never forces it.

Section 9.3: Recovery from Compromise (Not Loss)

Recovery from compromise is different from recovery from loss. A citizen who has lost their credential no longer has it. A citizen whose credential has been stolen still has it — they simply share it with an attacker.

If a citizen still holds their private key and can sign transactions, the compromise recovery process is key rotation: revoke the old credential, issue a new one, and preserve the handle and balance through the transition. The attacker's stolen copy of the old credential is invalidated the moment the rotation completes.

If the citizen has lost their private key to an attacker and no longer holds a copy themselves, the citizen must request assisted revocation from the Citizens' Council (Section 9.1), then begin the standard recovery process described in Part VII — retaking the examination or using a Recovery Beacon to re-derive their credential. This is the worst case, but the resolution path is defined.

Section 9.4: Suspicious Activity Detection

Alethia is not a surveillance system. But it is also not indifferent to signs that a citizen's credential may have been compromised. The Arbiter maintains a narrow, publicly documented set of heuristics that may flag a credential for review. These heuristics are designed to detect abuse, not to monitor behaviour.

The complete list of heuristics is as follows, published here and updated only by citizen referendum:

- Simultaneous presentation: the same credential used to generate valid proofs on two geographically distinct network endpoints within a time window that makes the same physical device impossible — for example, proofs from two different continents within five minutes of each other.
- Mass Eranos transfer: a transfer of the citizen's entire Eranos balance to an unknown handle in a single transaction, with no prior trading relationship between the handles.
- Poll vote reversal: a vote cast and then immediately reversed in a manner inconsistent with the citizen's established civic participation patterns, particularly during a contested referendum.

When a heuristic fires, the Arbiter does not automatically act. It sends an alert to the citizen through their registered notification channel asking them to confirm their recent activity. The citizen may confirm it (heuristic dismissed, no further action), deny it (emergency revocation process begins automatically), or ignore it (the credential is temporarily suspended after a defined timeout and the Citizens' Council is notified).

Every heuristic firing, every alert sent, and every citizen response is logged in the public audit record — with handle only, never with any real-world identifier. Any citizen may review the aggregate statistics of heuristic firings at any time. The system is not secret. Citizens can see whether it is working proportionately, and they can challenge any heuristic that seems to be triggering unfairly through the citizen referendum process.

Section 9.5: What Cannot Be Fully Prevented

An attacker who obtains a citizen's private key, uses it infrequently, mimics the citizen's normal patterns, and avoids triggering any of the documented heuristics will not be detected by Alethia. The system cannot close this gap without becoming a surveillance system, and Alethia will not become a surveillance system to catch edge-case attackers.

The practical mitigations for this threat sit primarily with the citizen rather than with Alethia: keeping devices secure, using strong encryption on credential storage, performing regular key rotation, setting up a Recovery Beacon, and reporting suspected compromise quickly. Alethia can educate, warn, and respond. It cannot watch on citizens' behalf without becoming the thing it was built to resist.

This is consistent with the Charter's first principle: citizens are not products to be protected by surveillance. They are sovereign individuals who accept some responsibility for their own security in exchange for genuine privacy. Alethia provides the tools. Citizens use them.

In Closing

The credential system is not glamorous. Most citizens will never see it operating. They will install their Alethian client, pass the examination, and from that moment, the credential will quietly do its work in the background — proving without revealing, verifying without watching.

That quiet competence is the point. Privacy that demands attention is a burden. Privacy that simply works, every time, without the citizen having to think about it, is freedom.

> *The best protection is the one you never have to remember is there.*

A L E T H I A

Truth. Reason. Dignity.