LIVE · ACN 1.1 · READY TO USE

GoGuides Authority Clearing Network

Technical White Paper · September 2026

Create ACN Account | PDF Edition

> **A credential tells a machine what was authorized. ACN tells the machine what remains authorized now.**

1. Executive summary

Autonomous and machine-operated systems increasingly receive authority to perform consequential actions across independent services. The authority may be bounded by money, quantity, capacity, time, quota, inventory, credits, permissions or another finite resource.

Conventional signed authorization answers an important question: was this authority genuinely granted?

It does not necessarily answer a different question: how much of that authority is still available at the instant another independent system is about to act?

The GoGuides Authority Clearing Network addresses that second problem. ACN maintains a shared, durable, current authority state and provides atomic reservations, signed action clearances, live validation, receipts, explicit reconciliation and independently verifiable evidence.

The primitive is called **Current Delegated Authority State**.

2. The problem: valid credentials can describe stale authority

Consider an autonomous purchasing system that has been granted authority to spend 1,000 units.

```
Original authority: 1,000

Request to Service A: 600
Request to Service B: 500
Request to Service C: 300

Combined requested amount: 1,400
```

Each independent service may receive the same authentic signed grant. Each may successfully verify its cryptographic signature. Nothing about that verification alone tells Service B that Service A has already reserved or consumed 600 units.

The authorization credential can therefore be authentic while the authority represented by it is no longer fully available.

This is not primarily an identity problem. It is not solved merely by stronger signatures, better authentication or another copy of the original grant.

It is a shared mutable-state problem.

3. Current Delegated Authority State

ACN maintains an authoritative answer to:

> **How much of this bounded delegated authority remains valid and unused right now?**

A relying system can therefore distinguish between:

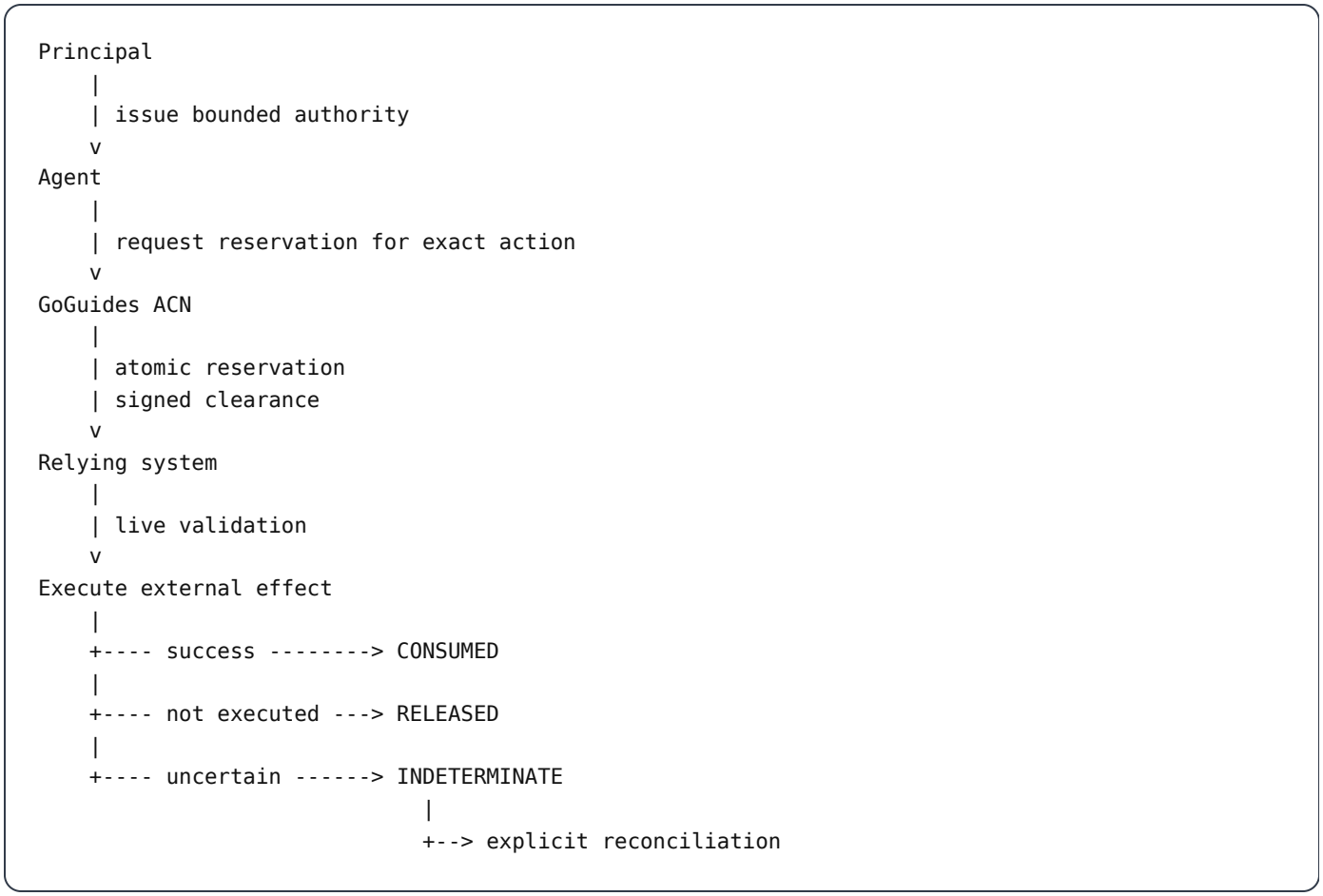
- authority that was once granted, and
- authority that is currently executable.

That distinction becomes important when independent actors operate concurrently.

4. Actors

Actor	Role
Principal / issuer	Creates bounded authority and may later freeze, reactivate or revoke it.
Agent / delegate	Holds authority or delegated authority and proposes an exact action.
GoGuides ACN	Maintains current state, atomically reserves authority and produces signed evidence.
Relying system / executor	Validates the clearance immediately before performing the consequential external action.

5. Core transaction



6. Why reservation must be atomic

Suppose 1,000 units remain and two systems simultaneously request 700 units.

If both systems independently read the same value before either writes a new state, both may conclude sufficient authority exists.

ACN serializes the authoritative state transition. A reservation either succeeds completely or changes nothing.

```
Available: 1,000

Request A: reserve 700
ACN: success

Available: 300

Request B: reserve 700
ACN: insufficient remaining authority
```

The guarantee comes from the shared state transition, not from the original token.

7. Conservation

ACN treats delegated authority as conserved capacity.

Delegation transfers or allocates authority. It does not create an additional copy of the same spendable capacity.

```
Parent authority: 1,000

Delegate to Agent A: 400
Delegate to Agent B: 300

Remaining unallocated parent capacity: 300
```

Concurrent reservation and delegation operations therefore share the same conservation requirement: usable descendant authority cannot exceed the bounded parent authority.

8. Authority and clearance states

Authority states

- **ACTIVE** — available for permitted operations.
- **FROZEN** — temporarily blocked.
- **REVOKED** — no longer usable.

Clearance states

- **RESERVED** — capacity is held for an exact action.
- **CONSUMED** — the external effect occurred.
- **RELEASED** — the action did not consume the reserved capacity.
- **INDETERMINATE** — the external outcome is not yet known safely.

9. The INDETERMINATE state

Distributed systems encounter an especially dangerous failure case: the external action may have happened even though the caller never received confirmation.

For example:

```
1. ACN reserves 400 units.
2. The relying service performs the external action.
3. The network connection fails before the result is recorded.
4. The caller does not know whether the action succeeded.
```

Automatically releasing those 400 units could allow them to be used again even though the first action actually occurred.

Automatically consuming them could also be incorrect if the action did not occur.

ACN therefore preserves the reservation as **INDETERMINATE** until an explicit reconciliation determines whether the result should become CONSUMED or RELEASED.

10. Exact-action binding

A clearance is not intended to be a generic bearer authorization. It is bound to the proposed action and counterparty.

The clearance validation path checks the stored action binding and the signed payload. A clearance for one materially different action cannot simply be replayed for another.

11. Revocation closure

Delegated authority can form a chain. The current state of that chain matters.

If an ancestor authority is frozen, expired or revoked, a descendant cannot be treated as independently current merely because the descendant credential was signed earlier.

ACN evaluates the authority chain as current state.

12. Idempotency and lost responses

Network retries are normal. Double-reserving authority is not.

ACN operations that may be retried use idempotency identifiers. A repeated request with the same idempotency key and same request content returns the original logical result rather than creating another reservation or delegation.

Reuse of the same idempotency key for different request content is rejected.

13. Cryptographic evidence

ACN 1.1 uses Ed25519 signatures for protocol evidence.

The evidence model includes:

- signed authority grants,
- signed action clearances,
- signed action receipts,

- append-only event hashes, and
- signed event checkpoints.

The current verification key is public:

```
GET https://www.goguides.com/api/v1/public-key
```

A relying system does not need to trust an undocumented signing key. The current key identifier and Ed25519 public key are published through the API.

Signing-key lifecycle and compromise status

ACN publishes the signing-key registry through `GET /api/v1/public-keys`. Registry states include **CURRENT**, **RETIRED**, and **COMPROMISED**.

Only the CURRENT signing key is used for newly issued protocol evidence. Retired and compromised public keys remain published so that historical signatures can still be examined cryptographically. A cryptographic match to a key marked COMPROMISED does not by itself establish that the historical object should be trusted; relying systems can also inspect the key status and available compromise metadata.

14. Live validation rule

Possession of a previously valid signed clearance does not necessarily mean the authority remains executable.

Immediately before a consequential action, the relying system should live-validate the clearance against ACN current state.

The underlying authority may have been frozen, revoked, expired or otherwise changed after the clearance was originally created.

15. ACN is live and ready to use

ACN 1.1 operates as a live HTTPS/JSON service.

Users create a dedicated ACN account. The ACN account system is separate from GoGuides webmaster accounts and Bot Radar.

Each ACN account receives its own production API client and API credential. The plaintext key is displayed once. Only its cryptographic hash is retained for authentication.

Customer API activity is account-scoped. One ACN customer cannot read another customer's authorities or evidence through customer-owned resources.

16. Creating an account

Create an ACN account here:

https://www.goguides.com/authority-clearing-network/signup

After signup the dashboard displays the newly generated production API key once.

The dashboard is available at:

https://www.goguides.com/authority-clearing-network/dashboard

Offline account recovery

ACN does not require email delivery for account recovery. At account creation, the user receives a high-entropy offline recovery key that must be stored securely. ACN stores only the recovery-key hash.

Recovery is available at https://www.goguides.com/authority-clearing-network/recover . A successful recovery changes the account password, rotates the recovery key, invalidates earlier login sessions, and invalidates existing API credentials as a security reset.

The replacement recovery key is displayed once. It should be treated as a high-value credential and stored separately from the normal password and API credentials.

17. API authentication

Authenticated calls send:

```
X-GoGuides-API-Key: YOUR_API_KEY
Content-Type: application/json
```

API keys should never be placed in URLs or committed to public source repositories.

18. Five-minute API quick start

Step 1 — network status

```
curl https://www.goguides.com/api/v1/status
```

Step 2 — obtain the public verification key

```
curl https://www.goguides.com/api/v1/public-key
```

Step 3 — issue bounded authority

```
curl -X POST \
  https://www.goguides.com/api/v1/authority/issue \
  -H 'X-GoGuides-API-Key: YOUR_API_KEY' \
  -H 'Content-Type: application/json' \
  --data '{
    "subject":"purchasing-agent-17",
    "authority_type":"spending",
    "unit":"USD",
    "amount":"1000.00000000"
  }'
```

The response supplies an `authority_id`. That identifier represents the current authority record.

Step 4 — reserve authority for an exact action

```
curl -X POST \
  https://www.goguides.com/api/v1/clearance \
  -H 'X-GoGuides-API-Key: YOUR_API_KEY' \
  -H 'Content-Type: application/json' \
  --data '{
    "authority_id":"AUTHORITY_ID",
    "amount":"400.00000000",
    "idempotency_key":"purchase-2026-0001",
    "action":"purchase",
    "counterparty":"vendor.example",
    "ttl_seconds":120
  }'
```

A successful reservation returns a clearance with a signed token and reduces currently available authority.

Step 5 — validate immediately before execution

```
curl -X POST \
  https://www.goguides.com/api/v1/clearance/validate \
  -H 'X-GoGuides-API-Key: YOUR_API_KEY' \
  -H 'Content-Type: application/json' \
  --data '{
    "clearance_id":"CLEARANCE_ID",
    "signed_token":"SIGNED_TOKEN",
    "action":"purchase",
    "counterparty":"vendor.example"
  }'
```

The relying system should execute the consequential action only when the clearance is currently valid for the intended action.

Step 6 — record the outcome

When the effect occurred:

```
curl -X POST \
  https://www.goguides.com/api/v1/clearance/CLEARANCE_ID/receipt \
  -H 'X-GoGuides-API-Key: YOUR_API_KEY' \
  -H 'Content-Type: application/json' \
  --data '{
    "result":"CONSUMED",
    "external_action_id":"vendor-order-92831"
  }'
```

If the action definitely did not occur, report `RELEASED`.

If the outcome cannot safely be determined, report `INDETERMINATE` and reconcile it later.

Step 7 — retrieve evidence

```
curl \
  -H 'X-GoGuides-API-Key: YOUR_API_KEY' \
  https://www.goguides.com/api/v1/evidence/AUTHORITY_ID
```

19. Delegation

Authority may be allocated from a parent authority to a child authority. Delegation consumes part of the parent's unallocated capacity rather than creating another independent copy.

```
POST /api/v1/authority/{authority_id}/delegate
```

The resulting child authority participates in ancestor state checks, including freeze, expiry and revocation.

20. Authority management

```
GET  /api/v1/authority/{authority_id}

POST /api/v1/authority/{authority_id}/freeze
POST /api/v1/authority/{authority_id}/activate
POST /api/v1/authority/{authority_id}/revoke
```

These operations change current executable state. A previously issued credential cannot override the current authority state.

21. Clearance management

```
POST /api/v1/clearance
GET  /api/v1/clearance/{clearance_id}
POST /api/v1/clearance/validate
POST /api/v1/clearance/{clearance_id}/receipt
POST /api/v1/clearance/{clearance_id}/reconcile
```

22. Protocol invariants

Invariant	Required property
Conservation	Delegation and concurrent reservations cannot create more usable authority than the bounded grant permits.
Atomicity	A state-changing reservation succeeds completely or changes nothing.
Idempotency	Retrying the same operation cannot reserve or allocate authority twice.
Monotonicity	Consumed authority does not silently become spendable again.
Revocation closure	A non-current ancestor prevents descendant authority from admitting a new effect.
Uncertain-effect safety	An unresolved external outcome remains reserved until explicit reconciliation.
Exact-action binding	A clearance cannot be reused for a materially different action or counterparty.

23. Customer isolation

ACN customer resources are bound to ACN accounts. Customer authority reads, state management and evidence access are scoped to the owning account.

Unauthorized cross-account resource lookup is not treated as evidence that another customer's resource exists.

24. API rate limiting

Customer accounts have enforced API request limits. The current account limit is visible in the ACN dashboard.

When a limit is exceeded, ACN responds with HTTP 429 and a `Retry-After` header.

25. Customer operational visibility

The ACN dashboard provides real operational telemetry, including:

- API calls over 24 hours, 7 days and 30 days,
- HTTP errors,
- average API latency,
- authorities and active authorities,
- clearances by current state,
- receipts,
- route-level usage,
- recent authority records,
- recent API activity,
- API client state, and
- API-key creation, rotation and revocation history.

26. Credential scopes, rotation and revocation

Each ACN account begins with a default full-access production credential. The dashboard can also create additional credentials with explicit API scopes.

Supported scopes separate authority issuance, authority reads and management, delegation, clearance reservation and reads, validation, receipt submission, reconciliation, and evidence access.

Credentials are managed independently. Rotating the default full-access credential revokes the previous default credential and creates a replacement, but does not revoke separately scoped credentials. A scoped credential can likewise be revoked without disabling the default credential or other active scoped credentials.

Plaintext credentials are displayed only when created or rotated. Only credential hashes are retained for authentication. Account recovery is intentionally different from normal credential rotation: recovery acts as a security reset and invalidates existing API credentials.

27. What ACN guarantees

Within the ACN authority state domain, the design is intended to provide:

- one durable current authority state,
- atomic reservation of bounded authority,
- conservation across delegation,
- idempotent state-changing operations,
- live state validation,
- ancestor-state enforcement,
- explicit handling of uncertain outcomes, and
- cryptographically verifiable protocol evidence.

28. What ACN does not claim to determine

ACN does not determine whether a real-world action is morally, commercially or legally desirable.

It does not determine whether a principal should have granted the authority in the first place.

It does not replace the relying organization's own safety, fraud, identity, compliance or business rules.

Its job is narrower: maintain and prove the current state of bounded delegated authority.

29. Failure semantics

A network failure must not automatically be interpreted as proof that a state-changing operation did not occur.

Applications should use idempotency for replay-safe operations and explicit reconciliation for uncertain external effects.

This avoids a common distributed-systems error: treating lack of a response as proof that no effect happened.

30. Evidence and audit trail

Authority transitions are represented in an append-only event sequence. Events include chained hashes, and ACN creates signed event checkpoints.

Receipts and clearances are signed protocol objects. The public verification key allows independent cryptographic verification.

31. Separation from the GoGuides web-trust system

ACN operates as a distinct state and failure domain.

ACN usage does not alter:

- AI Rank,
- public eligibility,
- crawler observations,
- domain provenance,
- Bot Radar measurements,
- Trust Records, or
- existing GoGuides machine-readable web evidence.

32. Machine discovery

Automated systems can discover the service through:

```
https://www.goguides.com/machine-use.json

https://www.goguides.com/authority-clearing-network/machine-use.json

https://www.goguides.com/authority-clearing-network/openapi.yaml
```

33. Public service endpoints

```
Network status:
https://www.goguides.com/api/v1/status

Current Ed25519 public key:
https://www.goguides.com/api/v1/public-key

Documentation:
https://www.goguides.com/authority-clearing-network/

Signup:
https://www.goguides.com/authority-clearing-network/signup

Login:
https://www.goguides.com/authority-clearing-network/login
```

34. What meaningful adoption looks like

Documentation traffic alone is not meaningful adoption.

The meaningful event occurs when an outside system treats ACN's current-state transition or validation as necessary before a consequential delegated action proceeds.

```
Machine A
   |
   v
GoGuides ACN
   |
   v
Machine B
```

At that point ACN is no longer merely describing authority. It is participating in the control path of the action.

35. Conclusion

Machine authority cannot always be represented safely as an immutable credential.

When bounded authority can be exercised concurrently across independent systems, those systems require shared current state.

The GoGuides Authority Clearing Network provides that state through atomic reservation, live validation, delegation conservation, reconciliation and signed evidence.

> **A signed grant proves what was authorized. Current Delegated Authority State proves what remains executable now.**

Create an ACN Account **OpenAPI Contract**