0PN

AN INTRO TO
DIGITAL IDENTITY TRUST

Introduction: 0PN Interop for Digital Identity and Personal Data Control

Author: Mark Lizar v1 9-2-26

Overview

0PN Interop provides the missing digital public transparency infrastructure layer between Convention 108+ legal requirements, digital identity systems, and AI governance. It enables **privacy-enabling personal data control** through **Transparency by Default (TbD)** architecture—where controller identification disclosure precedes data collection, enabling individuals to make informed trust decisions.

Core Principle: Controller-ID first architecture creates "architecture I choose to trust" rather than "trust us" surveillance-by-default systems.

Strategic Paradigm: Privacy-Enabling vs Privacy-Preserving

Privacy-Preserving (Data Protection)

Top-down, controller-centric approach:

- Organizations implement safeguards (encryption, anonymization, differential privacy)
- Controllers protect data they already collect and control
- Individual remains identified/tracked within controller systems
- Focuses on: "How can we protect the data we collect?"
- Architecture pattern: **"Trust us to protect your data"**

Use cases: Secure data storage, anonymization techniques, federated learning, differential privacy in analytics

Privacy-Enabling (Individual Data Control)

Bottom-up, individual-centric approach:

- Individuals remain anonymous and unlinked until they choose to identify
- Controller discloses identity BEFORE collecting PII
- **Transparency by Default (TbD)** architecture where controller identification record is disclosed first
- Individuals decide whether to authorize after reviewing controller disclosure
- Focuses on: "Can I trust this controller with my data?"
- Architecture pattern: **"Architecture I choose to trust"**

Use cases: ISO/IEC 27560-1 Universal Notice Receipt Profile, Controller Identification Records, Notice Event Logs, portable consent tokens

Complementary Relationship

These paradigms are complementary: Controller transparency (privacy-enabling) enables informed trust decisions BEFORE credential presentation or data sharing. Once an individual chooses to trust a controller, privacy-preserving techniques protect the data within that trusted relationship with architectural contextual integrity that enables secondary consented data.

> **0PN Interop operates in the privacy-enabling paradigm** while supporting integration with privacy-preserving systems.

Digital Consent and Real Choice: Architecture Flow

The Critical Distinction: Consent vs Permission

Consent (Legal Basis — Human-Managed)

Definition: One of six legitimate legal bases for processing personal data under Convention 108+ Article 5

Requirements:

- **Notice First:** Controller identification BEFORE data collection (Article 8.2)
- **Freely given:** No coercion, power imbalance addressed
- **Specific:** Granular purpose disclosure
- **Informed:** Transparent notice enables meaningful choice
- **Unambiguous:** Clear affirmative action required
- **Use of authority:** Individual exercises right to authorize or refuse

Managed by: Humans making informed decisions

Permission (System Control — Agent-Managed)

Definition: Technical access control executed by systems/agents

Characteristics:

- **Post-authorization:** Granted AFTER consent (if consent is the legal basis)
- **Technical enforcement:** What systems allow/deny
- **No legal basis:** Permission ≠ lawful processing justification
- **Automated:** Systems execute permissions, humans grant consent

Managed by: Software agents and system access controls

The Surveillance-by-Default Problem

Current "trust us" pattern:

1. Permission requested BEFORE controller identification disclosed
2. Permission fatigue treated as consent
3. No meaningful choice ("accept all cookies" dark patterns)
4. **Category error:** Permission labeled as "consent"

Result: Surveillance-by-default architecture where individuals cannot make informed trust decisions.

Flow Diagram 1: Surveillance-by-Default vs Transparency by Default

Current Surveillance Pattern (Privacy-Preserving Only)

```
┌────────────────────────────────────────────────────────────
┐
│          SURVEILLANCE-BY-DEFAULT ARCHITECTURE
│
│               ("Trust Us" Pattern)
│
└────────────────────────────────────────────────────────────
┘

    Individual                    System                 Hidd
en Controller
       │                             │
│
       │                             │
│
   [Landing]─────────────────────────▶
│
```

```
       |                            |
|
       |                      [Cookie Banner]
|
       |                     "Accept All"
|
       |                            |
|
       |◄─────[Permission Request]──|
|
       |      (No Controller-ID)    |
|
       |                            |
|
   [Fatigue]                        |
|
   [Click]──────["Accept"]─────────►|
|
       |                            |
|
       |                            |──[Data Collection Start
s]─►
       |                            |
|
       |                            |                     [Unk
nown Identity]
       |                            |                     [Unk
nown Purpose]
       |                            |                     [Unk
nown Legal Basis]
       |                            |
|
       |                     [Tracking Active]
|
       |◄─────────────────[Permissions Granted]───────────────
───|
       │                            │
│
    NO REAL                   Permission ≠                 Su
rveillance
    CHOICE                     Consent                      E
nabled
```

Problems:

- No controller identification before data collection
- Permission fatigue treated as informed consent
- Individual cannot evaluate "Do I trust this controller?"
- Zero transparency = Zero meaningful choice

Transparency by Default Architecture (Privacy-Enabling)

```
┌────────────────────────────────────────────────────────────
─┐
│        TRANSPARENCY BY DEFAULT ARCHITECTURE
│
│          ("Architecture I Choose to Trust")
│
└────────────────────────────────────────────────────────────
─┘

    Individual            Controller                 System
       │                      │                        │
       │                      │                        │
   [Landing]                  │                        │
       │                      │                        │
       │◄─[Controller-ID]─────│                        │
       │  [CIR Disclosure]    │                        │
       │  • Identity          │                        │
       │  • Purpose           │                        │
       │  • Legal Basis       │                        │
       │  • Privacy Access    │                        │
       │                      │                        │
   [Review]                   │                        │
   [Evaluate]                 │                        │
   "Do I trust                │                        │
    this controller?"         │                        │
       │                      │                        │
    ┌──▼───┐                  │                        │
    │CHOICE│                  │                        │
    └──┬───┘                  │                        │
       │                      │                        │
  ┌────┴─────┐               │                        │
  │          │               │                        │
[NO]       [YES]             │                        │
  │          │               │                        │
  │          │               │                        │
  │      [Informed           │                        │
  │       Consent]───────────▶                        │
  │          │               │                        │
  │          │          [Notice Receipt Generated]    │
  │          │               │                        │
  │          │               │──[Bilateral Proof]─────▶
  │          │               │                        │
  │          │               │                 [UNR to Indivi
dual]
  │          │               │                 [Shadow Receip
t Logged]
  │          │               │                        │
  │          │               │──[Permission Granted]──▶
  │          │               │                        │
  │          │◀──────[Notice Token]───────────────────│
  │          │               │                        │
  │      [Portable           │                  [Processing A
uthorized]
```

```
  |       Authorization]     |                        |
  |          |               |                        |
 [Exit]  [Monitored          |                        |
  |      Relationship]        |                        |
  |          |               |                        |
  |     [TPI-R Query]        |                        |
  |     [Rights Exercise]    |                        |
  |     [Withdraw]           |                        |
```

Key Principles:

1. **Controller-ID First:** Identification disclosed BEFORE data collection
2. **Real Choice:** Individual evaluates trust before authorization
3. **Bilateral Proof:** Both parties receive Notice Receipt
4. **Consent → Permission:** Human consent creates system permissions
5. **Portable Authorization:** Notice Tokens enable cross-context control
6. **Continuous Monitoring:** TPI-R queryability and rights exercise

Flow Diagram 2: Digital Consent Sequence

DPTI Solution Sequence

```
┌─────────────────────────────────────────────────────────────
───────┐
│     DIGITAL PUBLIC TRANSPARENCY INFRASTRUCTURE
│
│           Consent → Permission Sequence
│
└─────────────────────────────────────────────────────────────
───────┘


 ┌─────────────────┐
 │   CONTROLLER    │
 │  IDENTIFICATION │
 │                 │
 │  • WHO: Legal   │
 │    Identity     │
 │  • WHERE:       │
 │    Jurisdiction │
 │  • CONTACT:     │
 │    Privacy      │
 │    Access Point │
 └────────┬────────┘
          │
          │ (Disclosed First)
          │
          ▼
 ┌─────────────────┐
 │     NOTICE      │
 │   DISCLOSURE    │
 │                 │
 │  • PURPOSE:     │
 │    Processing   │
 │    intention    │
 │  • LEGAL BASIS: │
 │    Authorization│
 │    type         │
 │  • RETENTION:   │
 │    Duration     │
 └────────┬────────┘
          │
          │ (Transparent Disclosure)
          │
          ▼
 ┌─────────────────┐         ┌──────────────┐
 │     CONSENT     │◄────────│  INDIVIDUAL  │
 │  (Human-Managed)│         │   DECISION   │
 │                 │         │              │
 │  • Freely Given │         │ "Do I choose │
 │  • Specific     │         │  to trust    │
 │  • Informed     │         │  this        │
 │  • Unambiguous  │         │  controller?"│
 └────────┬────────┘         └──────────────┘
          │
          │ (Legal Basis Established)
          │
          ▼
 ┌─────────────────┐
 │   PERMISSION    │
 │ (Agent-Managed) │
 │                 │
 │  • Access       │
 │    Control      │
 │  • System       │
 │    Authorization│
 │  • Technical    │
 │    Enforcement  │
 └────────┬────────┘
          │
          │ (Automated Execution)
          │
          ▼
 ┌─────────────────┐
 │   PROCESSING    │
 │                 │
 │  Authorized     │
 │  with Bilateral │
 │  Proof          │
 │  (Notice Token) │
 └─────────────────┘
```

Critical Rule: Humans manage consent, systems/agents manage permissions. Conflating them enables surveillance.

Flow Diagram 3: Privacy-Enabling vs Privacy-Preserving Integration

Architectural Complementarity

```
┌────────────────────────────────────────────────────────────
──────────┐
│         PRIVACY-ENABLING + PRIVACY-PRESERVING INTEGRATION
│
│                  (Complementary Paradigms)
│
└────────────────────────────────────────────────────────────
──────────┘

                         INDIVIDUAL
                             │
                             │
                    [Anonymous State]
                    [Unlinked State]
                             │
                             │
            ┌────────────────┴────────────────┐
            │                                 │
            │   PRIVACY-ENABLING LAYER        │
            │   (Transparency by Default)     │
            │                                 │
            │   Controller-ID First           │
            │   Architecture                  │
            │                                 │
            │   ┌─────────────────────┐      │
            │   │ Controller          │      │
            │   │ Identification      │      │
            │   │ Record (CIR)        │      │
            │   │                     │      │
            │   │ • Identity          │      │
            │   │ • Purpose           │      │
            │   │ • Legal Basis       │      │
            │   │ • Privacy Access    │      │
            │   └──────────┬──────────┘      │
            │              │                  │
            │              ▼                  │
            │   [Individual Evaluates]        │
            │   "Architecture I choose        │
            │    to trust"                    │
            │              │                  │
            │              ▼                  │
            │   [Informed Decision]           │
            │              │                  │
            └──────────────┼──────────────────┘
                           │
                  ┌────────┴────────┐
                  │                 │
              [Trust]           [No Trust]
                  │                 │
                  │              [Exit]
                  │              [Remain Anonymous]
                  ▼

            ┌─────────────────────────────┐
            │                             │
            │   AUTHORIZED RELATIONSHIP   │
            │   (Consent/Legal Basis)     │
            │                             │
            │   Notice Receipt Generated  │
            │   Bilateral Proof           │
            │                             │
            └──────────────┬──────────────┘
                           │
                           │
            ┌──────────────▼──────────────┐
            │                             │
            │  PRIVACY-PRESERVING LAYER   │
            │  (Data Protection)          │
            │                             │
            │  Within Trusted             │
            │  Relationship               │
            │                             │
            │  ┌─────────────────────┐   │
            │  │ Encryption          │   │
            │  │ Anonymization       │   │
            │  │ Differential Privacy│   │
            │  │ Secure Processing   │   │
            │  │ Access Controls     │   │
            │  └─────────────────────┘   │
            │                             │
            │  "Trust us to protect       │
            │   your data"                │
            │                             │
            └─────────────────────────────┘
                           │
                           ▼
                  [Protected Data]
                  [Secure Processing]
```

Key Insight: Privacy-enabling architecture (Controller-ID first) provides the transparency layer that allows individuals to make informed trust decisions BEFORE entering into relationships where privacy-preserving techniques protect their data.

Integration Pattern:

1. **Privacy-Enabling (First):** Controller transparency enables informed choice
2. **Privacy-Preserving (Second):** Data protection within trusted relationships
3. **Continuous:** TPI-R queryability maintains transparency across relationship lifecycle

Flow Diagram 4: Digital Identity in 0PN Interop

Digital Identification vs Identity

```
┌────────────────────────────────────────────────────────────
──────────┐
│              DIGITAL IDENTIFICATION vs IDENTITY
│
│         (Surveillance vs Sousveillance Paradigms)
│
└────────────────────────────────────────────────────────────
──────────┘


╔════════════════════════════════════════════════════════════
═══════╗
║         DIGITAL IDENTIFICATION (Surveillance)
║
║         Top-Down, Controller-Controlled
║
╚════════════════════════════════════════════════════════════
═══════╝

    Controller
        │
        │ [Assigns Identifier]
        │ [Infers Identity]
        │ [Mandates Credential]
        │
        ▼
    Individual ──▶ [Must Accept]
                   [Controller-Defined ID]
                   [No Choice of Trust]
    Example: Cookie IDs, tracking pixels, device fingerprinti
ng,
             mandatory government IDs presented to untrusted 
parties

    Problem: Individual cannot choose which controllers to tr
ust
             with their identifying information


╔════════════════════════════════════════════════════════════
═══════╗
║         IDENTITY (Sousveillance)
║
║         Bottom-Up, Individual-Controlled
║
╚════════════════════════════════════════════════════════════
═══════╝

    Individual
        │
        │ [Self-Defines Identity]
        │ [Controls Identifiers]
        │ [Chooses Trust]
        │
        ▼
    ┌───────────────────┐
    │ Controller-ID     │
    │ Disclosed First   │
    │                   │
    │ Individual        │
    │ Evaluates         │
    └────────┬──────────┘
             │
        ┌────┴────┐
        │         │
```

```
     [Trust]   [No Trust]
        │         │
        │         └──▶ [Remain Anonymous]
        │
        ▼
    [Individual Chooses]
    [to Bind Identity]
    [to Trusted CIR]

    Example: ISO/IEC 27560-1 Notice Receipts, anchored receip
ts,
             portable consent tokens, individual-controlled D
IDs

    Solution: Individual binds their identity to Controller
              Identification Records they choose to trust


╔════════════════════════════════════════════════════════════
═══════╗
║         0PN INTEROP SOLUTION
║
║         Transparency by Default with Identity Control
║
╚════════════════════════════════════════════════════════════
═══════╝

    STAGE 1: Controller Identification Disclosure
    ┌─────────────────────────────────────┐
    │ Controller Identification Record    │
    │ (CIR)                              │
    │                                    │
    │ • Controller Legal Identity        │
    │ • Jurisdiction                     │
    │ • Purpose                          │
    │ • Legal Basis                      │
    │ • Privacy Access Point             │
    │                                    │
    │ NO pii_principal_id REQUIRED       │
    │ (Individual remains anonymous)     │
    └──────────────┬──────────────────────┘
                   │
                   ▼
    STAGE 2: Individual Evaluation
    ┌─────────────────────────────────────┐
    │ Individual Decision:                │
    │                                     │
    │ "Do I choose to trust this          │
    │  controller with my identity?"      │
    │                                     │
    │ [Architecture I Choose to Trust]    │
    └──────────────┬──────────────────────┘
                   │
              ┌────┴────┐
              │         │
           [YES]      [NO]
              │         │
              │         └──► [Exit Anonymous]
              │
              ▼
    STAGE 3: Identity Binding
    ┌─────────────────────────────────────┐
    │ Individual Self-Identifies          │
    │                                     │
    │ Universal Notice Receipt (UNR)      │
    │ Generated:                          │
    │                                     │
    │ • PII Principal ID (self-defined)   │
    │ • Bound to CIR                      │
    │ • Bilateral Proof                   │
    │ • Portable Authorization            │
    │                                     │
```

```
      │ Notice Token enables cross-context  │
      │ authorization without corporate     │
      │ identification systems              │
      └─────────────────────────────────────┘


    KEY PRINCIPLE:
    "Identity" = What individuals define and control about th
emselves
    "Identification" = What controllers assign, infer, or req
uire

    0PN Interop enables IDENTITY (individual-controlled)
    while providing standardized CONTROLLER IDENTIFICATION
```

0PN Interop Technical Architecture

Core Components

1. Controller Identification Record (CIR)

Machine-readable controller disclosure at `.well-known/notice.txt`:

```
{
  "controller_id": "https://example.com",
  "legal_name": "Example Corp Ltd.",
  "jurisdiction": ["CA", "US"],
  "purpose": ["Service delivery", "Analytics"],
  "legal_basis": ["Consent", "Legitimate Interest"],
  "privacy_access_point": "https://example.com/privacy",
  "data_protection_officer": "dpo@example.com"
}
```

2. Universal Notice Receipt (UNR)

Bilateral proof-of-notice exchanged between controller and individual:

- **Controller receives:** Shadow Receipt (logged in Notice Event Log)
- **Individual receives:** Notice Receipt (stored in personal receipt wallet)
- **Both contain:** Synchronized timestamp, controller_id, purpose, legal_basis, notice_token

3. Notice Event Log

Controller-maintained audit trail of all transparency events:

- Notice issued
- Consent granted/withdrawn
- Purpose changed
- Legal basis updated
- Rights exercised
- Processing stopped

4. Notice Token

Portable authorization credential:

- Legal basis agnostic (works for all 6 Convention 108+ Article 5 bases)
- Cryptographically bound to CIR and UNR
- Enables cross-context authorization without corporate identification systems
- Individual-controlled, portable across services

5. Digital Transparency Risk Assurance (Four Levels)

Level 1 (Self-Assertion): Controller adds notice.txt, CIR, Notice Event Log

Level 2 (Registered Controller): Controller registered with verified CIR, optional UNRs

Level 3 (ANCR and Signaling): Anchored receipts with cryptographic signatures, requires Digital Privacy Risk Officer

Level 4 (Active State High Assurance): Real-time signaling and control, certified notarization

Integration with Digital Identity Standards

OpenID Connect + ISO/IEC 27560-1

Pattern: Controller-ID disclosure BEFORE authentication request

1. Individual visits service
2. Service presents CIR via `.well-known/notice.txt`
3. Individual evaluates controller transparency
4. If trusted, individual initiates OpenID Connect flow
5. UNR generated and exchanged during authentication
6. Notice Token included in authorization token

Verifiable Credentials + Transparency by Default

Pattern: Controller-ID disclosure BEFORE credential presentation request

1. Verifier discloses CIR ("Who am I? Why do I need this credential?")
2. Individual evaluates verifier transparency via TPI-R query
3. If trusted, individual presents verifiable credential
4. UNR generated documenting credential presentation event
5. Notice Token binds authorization to specific controller and purpose

Digital Wallets + Notice Receipt Management

Pattern: Wallet stores Notice Receipts alongside credentials to become a digital consent wallet

- **Privacy-Enabling Layer:** Notice Receipts track which controllers individual has authorized
- **Privacy-Preserving Layer:** Credentials enable selective disclosure to trusted controllers
- **Integration:** Wallet queries TPI-R before credential presentation to verify controller transparency

Use Cases

Use Case 1: Cross-Border Consent

Individual in Canada authorizes EU controller:

1. EU controller discloses CIR with Convention 108+ Article 14 cross-border transfer disclosure
2. Canadian individual evaluates controller via TPI-R
3. Individual grants consent, UNR generated with bilateral proof
4. Notice Token enables portable authorization across jurisdictions
5. Either party can prove consent occurred with synchronized Notice Receipt

Use Case 2: Multi-Service Authorization

Individual authorizes data sharing between trusted controllers:

1. Primary controller (e.g., health provider) discloses CIR
2. Individual consents to share data with secondary controller (e.g., specialist)
3. Primary controller discloses secondary controller's CIR
4. Individual evaluates secondary controller transparency
5. If trusted, Notice Token enables authorized data flow
6. Notice Event Logs at both controllers document transfer with bilateral proof

Use Case 3: Immortal Consent (For UMA Death and the Digital Estate)

See Appendix A for detailed use case

Use Case 4: AI Agent Authorization

Individual authorizes personal AI agent (Priv8AI) to manage data:

1. Individual grants Priv8AI Notice Tokens for authorized controllers
2. Priv8AI monitors Notice Event Logs for transparency changes
3. If controller transparency degrades (TPI-R score drops), Priv8AI alerts individual
4. Individual can withdraw consent, Priv8AI executes withdrawal with Notice Token
5. All actions logged with bilateral proof in Notice Event Logs

Standards Alignment

Convention 108+ Modernised Convention

- **Article 5:** Six legal bases for processing (consent, contract, legal obligation, vital interest, public interest, legitimate interest)
- **Article 8.2:** Transparency requirements—controller identification, purpose, legal basis BEFORE collection
- **Article 9:** Data subject rights (access, rectification, erasure)
- **Article 14:** Cross-border data flows with maintained authorization

ISO/IEC 27560-1 Universal Notice Receipt Profile

- **CIR:** Controller Identification Record structure
- **UNR:** Universal Notice Receipt bilateral proof format
- **NEL:** Notice Event Log audit trail requirements
- **ANCR:** Anchored receipt cryptographic binding
- **Digital Transparency Risk Assurance Levels:** Four-level framework

GDPR Article 13 & EU Regulation 1725 Article 14

- Information to be provided when personal data collected from data subject

- Controller identity, contact details, DPO contact
- Purposes and legal basis for processing
- Right to withdraw consent at any time

Next Steps for Integration

For Digital Identity Standards Bodies

1. **Review Controller-ID First Pattern:** How can existing authentication/authorization protocols incorporate controller disclosure BEFORE credential requests?
2. **TPI-R Integration:** How can digital wallets query controller transparency before credential presentation?
3. **Notice Token Support:** How can authorization tokens include portable consent evidence?

For Privacy-Preserving Technology Developers

1. **Transparency Layer Integration:** How can privacy-preserving systems provide Controller-ID disclosure before data collection?
2. **Bilateral Proof Requirements:** How can selective disclosure protocols generate Notice Receipts for both parties?
3. **Audit Trail Standards:** How can Notice Event Logs integrate with existing compliance frameworks?

For Regulatory Capacity Infrastructure

1. **TPI-R Queryability:** How can regulators assess controller transparency at scale across jurisdictions?
2. **Notice Event Log Inspection:** How can enforcement authorities access bilateral proof for complaint investigation?

3. **Multi-Jurisdictional Coordination:** How can Convention 108+ signatories coordinate enforcement using standardized transparency infrastructure?

Security Benefits and High Assurance Potential

Security Architecture Benefits

1. Reduced Attack Surface

Transparency by Default eliminates surveillance-by-default vulnerabilities:

- **No hidden controllers:** All data processors must disclose identity BEFORE collection, eliminating shadow tracking and unknown third-party data flows
- **Blast radius containment:** When breaches occur, Notice Event Logs provide complete audit trail of which controllers accessed data and when, enabling precise impact assessment
- **Authorization state visibility:** Notice Tokens make authorization explicit and queryable—no hidden permissions or forgotten data sharing agreements

Contrast with surveillance-by-default:

- Current pattern: Unknown controllers collect data → Individual cannot assess risk → Breach reveals unknown exposure
- TbD pattern: Controller-ID disclosed first → Individual evaluates risk → Only trusted controllers receive authorization → Breach impact is known and bounded

2. Proof-of-Notice Protection Against False Claims

Bilateral Notice Receipts create cryptographic evidence:

- **Controller protection:** Shadow Receipt proves notice was provided with specific terms at specific time
- **Individual protection:** Personal Notice Receipt proves what was disclosed and agreed to

- **Dispute resolution:** Synchronized receipts eliminate "they said / we said" conflicts
- **Regulatory evidence:** Both parties can demonstrate compliance with Convention 108+ Article 8.2 notice requirements

Security benefit: Prevents post-hoc claims that notice was inadequate or that consent was broader than actually granted.

3. Authorization Delegation Security

Notice Tokens enable secure cross-context authorization:

- **Cryptographically bound:** Token linked to specific CIR, purpose, and legal basis
- **Portable but constrained:** Individual can delegate authorization without exposing credentials
- **Revocable:** Withdrawal updates token state across all contexts
- **Auditable:** Notice Event Logs track token issuance, use, and revocation

Security benefit: Individual can authorize AI agents (Priv8AI) or third-party services to act on their behalf without sharing passwords or identity credentials.

4. Phishing and Social Engineering Resistance

Controller-ID first architecture creates verification layer:

- **Pre-authorization verification:** Individual can query controller transparency (TPI-R) BEFORE sharing data
- **Controller reputation signals:** Low TPI-R score indicates non-transparent controller—warning signal
- **Consistent CIR structure:** Standardized controller disclosure format makes suspicious patterns detectable
- **Notice Receipt validation:** Individual can verify controller's CIR matches claimed identity

Security benefit: Phishing attacks must either (a) disclose actual malicious identity in CIR, or (b) impersonate legitimate controller, which can be detected via

TPI-R query and CIR validation.

ANCR Exchange Protocol: High Assurance Levels

Anchored Consent Receipt (ANCR) Architecture

Level 3 Digital Transparency Risk Assurance introduces cryptographic anchoring:

```
┌────────────────────────────────────────────────────────────
──┐
│              ANCR EXCHANGE PROTOCOL
│
│         (Level 3 High Assurance Architecture)
│
└────────────────────────────────────────────────────────────
──┘


    Individual                Controller              Trust A
nchor
       │                          │                        │
       │                          │                        │
   [Landing]                      │                        │
       │                          │                        │
       │◄─[CIR + Anchor]──────────│                        │
       │  [Signed Controller      │                        │
       │   Disclosure]            │                        │
       │                          │                        │
   [Verify]                       │                        │
   [CIR Signature]────────────────┼───────────────────────►│
       │                          │                    [Validat
e]
       │◄─────────────────────────┼─────────[Signature Valid]
│
       │                          │                        │
   [Evaluate]                     │                        │
   [Trust Decision]               │                        │
       │                          │                        │
       │──[Informed Consent]─────▶│                        │
       │                          │                        │
       │                     [Generate UNR]                │
       │                     [Create ANCR]                 │
       │                          │                        │
       │                          │──[Blind Notarization]─▶│
       │                          │   [Timestamp]          │
       │                          │   [CIR Hash]           │
       │                          │   [Purpose Hash]       │
       │                          │   [NO PII]             │
       │                          │                        │
       │                          │◀─[Anchor Signature]────│
       │                          │   [Merkle Root]        │
       │                          │                        │
       │◀─[ANCR to Individual]────│                        │
       │  [Controller Shadow]     │                        │
       │  [Individual Receipt]    │                        │
       │  [Both Anchored]         │                        │
       │                          │                        │
    [Verify]                      │                        │
    [Anchor]─────────────────────────────────────────────▶│
       │                          │                  [Validat
ed]
       │                          │                        │
   [Store]                   [Log NEL]                [Archiv
e]
   [Personal Wallet]         [Shadow Receipt]        [Merkle
Tree]
```

ANCR Security Properties

1. Blind Data Notarization

- **Zero-knowledge proof:** Trust anchor timestamps and signs notice WITHOUT accessing PII
- **Privacy preserved:** Only hashes submitted to anchor (CIR hash, purpose hash, timestamp)
- **Cryptographic binding:** Merkle tree links notice to specific controller and time
- **Non-repudiation:** Neither party can later claim notice did not occur or contained different terms

2. Multi-Party Verification

- **Individual verification:** Can validate anchor signature independently
- **Controller verification:** Can prove notice was provided with specific terms
- **Third-party verification:** Regulators/auditors can validate notice without accessing PII
- **Long-term validity:** Merkle tree provides permanent proof even if parties dispute years later

3. Tamper Evidence

- **Immutable timestamp:** Anchor signature fixes time of notice
- **Content binding:** Hash of CIR and purpose locked at time of notice
- **Modification detection:** Any change to terms invalidates anchor signature
- **Audit trail integrity:** Notice Event Log entries can be anchored to prove log was not altered

ANCR Exchange Protocol Benefits

High assurance authorization:

- **Cryptographic proof of consent:** ANCR provides mathematical certainty that notice occurred
- **Cross-jurisdictional recognition:** Anchored receipts recognized across Convention 108+ signatories
- **Regulatory-grade evidence:** Meets highest standards for consent documentation

- **Dispute resolution efficiency:** Cryptographic proof eliminates evidence disputes

Trust minimization:

- **No reliance on controller honesty:** Anchor provides independent verification
- **No reliance on individual memory:** Receipt provides permanent record
- **Distributed trust:** Multiple parties can verify without central authority

---

Authorization and Notice Negotiation

Dynamic Authorization Negotiation Protocol

Transparency by Default enables negotiation BEFORE authorization:

Stage 1: Initial Disclosure

```
Controller → Individual:
{
  "controller_id": "example.com",
  "purpose": ["Service delivery", "Analytics", "Marketing"],
  "legal_basis": ["Consent"],
  "data_requested": ["email", "name", "location", "device_id"],
  "retention": "3 years",
  "third_party_sharing": ["analytics-provider.com", "ad-network.com"]
}
```

Stage 2: Individual Counteroffer

```
Individual → Controller:
{
  "accepted_purpose": ["Service delivery"],
  "rejected_purpose": ["Analytics", "Marketing"],
  "data_consent": ["email", "name"],
  "data_refused": ["location", "device_id"],
  "retention_limit": "1 year",
  "third_party_consent": [],
  "conditions": ["No cross-context tracking", "Quarterly transparency reports"]
}
```

Stage 3: Negotiated Authorization

```
Controller → Individual (Revised Offer):
{
  "controller_id": "example.com",
  "purpose": ["Service delivery", "Anonymous analytics (no PII)"],
  "legal_basis": ["Consent", "Legitimate Interest"],
  "data_collected": ["email", "name"],
  "retention": "1 year active, 1 year archive",
  "third_party_sharing": ["None"],
  "transparency_commitment": "Quarterly TPI-R publication"
}

Individual accepts → UNR generated with agreed terms
```

Negotiation Benefits

1. Granular Authorization Control

- **Purpose-specific consent:** Individual can accept service delivery, reject marketing
- **Data minimization enforcement:** Individual specifies minimum necessary data
- **Retention negotiation:** Individual can demand shorter retention periods
- **Third-party veto:** Individual can refuse specific third-party sharing

2. Market-Driven Transparency Competition

- **Competitive differentiation:** Controllers offering better terms attract privacy-conscious users
- **Race to transparency:** Network effects reward high TPI-R scores
- **Dark pattern elimination:** Negotiation exposes manipulative terms before authorization

3. Regulatory Capacity Efficiency

- **Self-enforcing compliance:** Negotiation creates bilateral record of agreed terms
- **Complaint investigation:** Notice Event Log shows if controller violated negotiated terms
- **Pattern detection:** Regulators can identify controllers who refuse reasonable negotiation

Multi-Level Notice Negotiation

Context-aware authorization across Digital Transparency Risk Assurance levels:

Level	Negotiation Capability	Assurance	Use Case
L1 (Self-Assertion)	Basic purpose selection	Self-certified	Low-risk services, public data
L2 (Registered)	Granular data selection	Registrar verified	Standard web services
L3 (ANCR)	Full negotiation + anchoring	Cryptographic proof	Financial services, health data
L4 (Active State)	Real-time authorization + monitoring	Live signaling	High-risk processing, AI agents

Progressive trust model:

- Individual starts with minimal authorization (L1)
- As trust develops, individual can upgrade to higher assurance levels
- Controller earns access to more data/purposes by maintaining transparency
- Relationship can downgrade if controller transparency degrades (TPI-R drops)

Network Effects and Adoption Potential

Individual Adoption Benefits

1. Portable Authorization Management

- **Single authorization infrastructure:** Notice Tokens work across all compliant controllers
- **Unified rights exercise:** One withdrawal request propagates to all authorized controllers
- **Cross-service visibility:** Personal receipt wallet shows all active authorizations
- **AI agent delegation:** Priv8AI can manage authorizations on individual's behalf

2. Transparency Competition Drives Value

- **TPI-R comparison shopping:** Individuals choose controllers with highest digital transparency and consent (public) reputations
- **Better terms over time:** Network effects reward controllers who negotiate fairly
- **Reduced ~~consent~~ (digital-id) permission fatigue:** Negotiation replaces binary "accept all or nothing" patterns
- **Trust accumulation:** Long-term transparent relationships build valuable reputation

Controller Adoption Benefits

1. Liability Protection

- **Bilateral proof protects against false claims:** Shadow Receipts document exactly what was disclosed
- **Breach impact containment:** Notice Event Logs prove which data was authorized vs unauthorized collection
- **Regulatory safe harbor:** ANCR compliance demonstrates good-faith transparency efforts

- **Insurance premium reduction:** High TPI-R scores indicate lower regulatory risk
- AI Insurance: AI Knowledge System Assurance for Digital Estates

2. Competitive Differentiation

- **Privacy-conscious market access:** High transparency attracts users who reject surveillance-by-default
- **Trust premium pricing:** Controllers with high TPI-R can charge premium for verified privacy
- **Cross-border interoperability:** Convention 108+ alignment enables multi-jurisdictional operations
- **Partnership opportunities:** Transparent controllers preferred for data-sharing agreements

3. Operational Efficiency

- **Automated compliance:** ISO/IEC 27560-1 infrastructure replaces manual privacy policy management
- **Reduced support burden:** Notice Receipts answer "what did I agree to?" queries
- **Streamlined audits:** Notice Event Logs provide ready-made audit trail
- **Rights exercise automation:** Notice Tokens enable programmatic consent withdrawal

Regulatory Adoption Benefits

1. Enforcement at Scale

- **TPI-R queryability:** Assess controller transparency across entire jurisdiction
- **Automated monitoring:** Notice Event Log inspection via API
- **Cross-border coordination:** Shared transparency infrastructure enables multi-lateral enforcement
- **Pattern detection:** Identify systemic non-compliance across controller populations

2. Complaint Investigation Efficiency

- **Bilateral evidence:** Both parties provide Notice Receipts for investigation
- **Tamper-proof audit trail:** ANCR ensures evidence integrity
- **Clear violation detection:** Notice Event Log shows if processing exceeded authorization
- **Proportionate penalties:** Transparency compliance history informs enforcement decisions

3. Policy Development Intelligence

- **Real-world negotiation data:** See which terms individuals accept vs reject
- **Market transparency trends:** TPI-R distribution shows regulatory impact
- **Cross-jurisdictional learning:** Convention 108+ network shares transparency metrics
- **Evidence-based regulation:** Notice Event Logs provide empirical policy foundation

Ecosystem Network Effects

Positive feedback loops:

1. **More adopters → Better tools:** Wallet providers build better interfaces for Notice Receipt management
2. **More controllers → Higher standards:** Transparency competition drives TPI-R scores upward
3. **More regulators → Stronger enforcement:** Multi-lateral coordination increases compliance incentives
4. **More data → Better AI agents:** Priv8AI learns negotiation strategies from ecosystem patterns
5. **Higher transparency → Lower costs:** Automated compliance infrastructure scales with adoption

Tipping point dynamics:

- **Critical mass:** Once 15-20% of market adopts, non-adoption becomes competitive disadvantage
- **Regulatory forcing function:** Convention 108+ Article 8.2 enforcement accelerates adoption
- **Technology integration:** Digital identity standards incorporating Controller-ID first patterns
- **Consumer awareness:** TPI-R scoring creates legible transparency signal

Future Potential: Active State High Assurance (Level 4)

Real-Time Authorization and Notice Signaling

Level 4 enables dynamic authorization management:

HABNI Protocol (Human-Agent Bilateral Notice Interface) for high assurance network broadcasting

```
┌────────────────────────────────────────────────────────────
──┐
│           LEVEL 4 ACTIVE STATE ARCHITECTURE
│
│     (Real-Time Authorization + Continuous Monitoring)
│
└────────────────────────────────────────────────────────────
──┘

    Individual              0PN-AI              Priv8AI
    (Smartopian)         (Controller-side)   (Individual-sid
e)
       │                      │                      │
       │                      │                      │
   [Grants]                   │                      │
   [Notice Token]─────────────┼─────────────────────▶│
       │                      │                 [Monitors]
```

```
         │                      │                     │
         │                [Processing              [Query]
         │                 Active]                  │
         │                      │                     │
         │                      │◄────[TPI-R Query]───│
         │                      │                     │
         │                      │──[TPI-R Score]─────►│
         │                      │   [NEL Summary]     │
         │                      │                     │
         │                      │               [Evaluates]
         │                      │               [Transparency]
         │                      │                     │
         │                [Purpose             [Alert Trigger]
         │                 Change]                    │
         │                      │                     │
         │                      │──[Notice Event]──►│
         │                      │   "Purpose Changed" │
         │                      │                     │
         │                      │              [Notify]
         │◄─────────────────────┼─────────────────────│
         │  [Alert: "Controller changed purpose      │
         │   from 'Analytics' to 'Marketing'."]      │
         │  [Action: Review / Withdraw / Accept]      │
         │                      │                     │
     [Review]                   │                     │
     [Decides:                  │                     │
      Withdraw]                 │                     │
         │                      │                     │
         │──[Withdraw Command]──┼────────────────────►│
         │                      │                     │
         │                      │◄──[Execute Withdrawal]─│
         │                      │   [Notice Token        │
         │                      │    Revocation]         │
         │                      │                        │
         │                 [Processing                   │
         │                  Stopped]                     │
```

```
│                      │                        │
│                 [NEL Updated:                 │
│                  "Authorization               │
│                   Withdrawn"]                 │
│                      │                        │
│                      │──[Confirmation]───────▶│
│                      │                        │
│◀─────────────────────┼────────────────────────│
│  [Confirmed: Authorization withdrawn,         │
│   processing stopped, data deletion           │
│   scheduled per retention policy]             │
```

Level 4 Capabilities

1. Real-Time Transparency Monitoring

- **Continuous TPI-R assessment:** Priv8AI queries controller transparency on schedule
- **Anomaly detection:** Sudden TPI-R drops trigger individual alerts
- **Purpose drift detection:** Notice Event Log changes monitored for unauthorized scope expansion
- **Third-party sharing alerts:** Individual notified when new data sharing relationships added

2. Automated Rights Exercise

- **Programmatic withdrawal:** Priv8AI executes consent withdrawal with Notice Token
- **Data portability automation:** Automated export requests on defined schedule
- **Rectification management:** Priv8AI monitors for data quality issues and requests corrections
- **Objection handling:** Automated objection to processing based on individual-defined rules

3. Dynamic Authorization Adjustment

- **Context-aware permissions:** Authorization level adjusts based on current risk assessment
- **Temporary authorization:** Time-limited Notice Tokens for one-time or limited-duration processing
- **Conditional processing:** "Process data only if TPI-R remains above threshold"
- **Graduated revocation:** Reduce authorization scope rather than binary withdrawal

4. Multi-Party Coordination

- **Data sharing orchestration:** Priv8AI manages authorization across controller networks
- **Consolidated reporting:** Single dashboard shows all authorizations across all controllers
- **Collective bargaining:** Groups of individuals negotiate common transparency terms
- **Federation management:** Individual authorizes controller federations with unified governance

High Assurance Use Cases

Healthcare data sharing:

- Patient authorizes primary physician with L3 ANCR
- Physician requests specialist consultation → Patient receives notice
- Patient evaluates specialist's TPI-R → Approves temporary L4 authorization
- Priv8AI monitors both controllers → Alerts if data used beyond authorized purpose
- Post-consultation: Authorization automatically expires, data deletion verified

Financial services with AI agents:

- Individual authorizes bank with L4 active state monitoring
- Priv8AI continuously queries bank's TPI-R and Notice Event Log
- Bank introduces new analytics purpose → Notice Event generated

- Priv8AI evaluates purpose against individual's privacy rules → Auto-rejects
- Bank must negotiate revised terms to maintain full authorization

Cross-border research participation:

- Researcher discloses CIR with multi-jurisdictional processing disclosure
- Individual grants L3 ANCR consent for specific research purpose
- Data transfer to collaborating institution → Individual receives notice
- Individual evaluates collaborator TPI-R → Approves with monitoring
- Priv8AI tracks research outputs → Verifies data used only for authorized purpose
- Study completion → Automated data deletion verification via Notice Event Log

---

Strategic Advantages Summary

Security Architecture

- ✅ Reduced attack surface via controller transparency
- ✅ Bilateral proof protection against false claims
- ✅ Phishing resistance through pre-authorization verification
- ✅ Authorization delegation security with Notice Tokens

High Assurance Infrastructure

- ✅ ANCR blind notarization preserves privacy
- ✅ Cryptographic non-repudiation for dispute resolution
- ✅ Multi-party verification without central authority
- ✅ Long-term tamper-evident audit trails

Authorization Negotiation

- ✅ Granular purpose and data selection
- ✅ Market-driven transparency competition

- ✅ Progressive trust across four assurance levels
- ✅ Self-enforcing compliance through bilateral records

Network Effects

- ✅ Portable authorization across services and jurisdictions
- ✅ Regulatory enforcement at scale via TPI-R queryability
- ✅ Ecosystem positive feedback loops
- ✅ Tipping point dynamics favor transparency

Future Potential

- ✅ Real-time authorization with HABNI protocol
- ✅ AI agent automation (0PN-AI + Priv8AI)
- ✅ Dynamic authorization adjustment
- ✅ Multi-party coordination infrastructure

Core Innovation: 0PN Interop transforms transparency from compliance burden into **security infrastructure, competitive advantage, and regulatory capacity enabler**.

Summary: 0PN Interop Value Proposition

For Individuals:

- Real choice: "Architecture I choose to trust"
- Portable authorization across services and jurisdictions
- TPI-R transparency scoring before data sharing
- Rights exercise with bilateral proof

For Controllers:

- Standardized transparency disclosure (ISO/IEC 27560-1)
- Bilateral proof of notice protects against false claims

- Reduced compliance cost through infrastructure automation
- Cross-border interoperability via Convention 108+ alignment

For Regulators:

- Enforcement at scale via TPI-R queryability
- Multi-jurisdictional coordination with standardized transparency infrastructure
- Notice Event Log inspection for complaint investigation
- Regulatory capacity infrastructure reduces manual assessment burden

For Digital Identity Ecosystem:

- Controller-ID first creates trust layer before credential exchange
- Privacy-enabling + privacy-preserving complementary integration
- Notice Tokens enable portable authorization without corporate identification systems
- Transparency by Default supports informed trust decisions

Tagline: *"It's not fair or trustworthy, if it's not Transparent First."*

License & Attribution

Technical Specifications Referenced: The technical specifications described in this document (ISO/IEC 27560-1 Universal Notice Receipt Profile, Controller Identification Record schema, ANCR protocol) are subject to separate licensing terms:

- **ISO/IEC 27560-1 Profile:** OPN-RF-RAND (Royalty-Free with RAND opt-out)
- **Implementation conformance:** Patent grant for Essential Claims under OPN IPR Agreement

Attribution: 0PN Lab (lab.0pn.org) | Digital Transparency Lab (transparencylab.ca)

Citation Format:

Lizar, M. (2026). *Introduction: 0PN Interop for Digital Identity and Personal Data Control*. 0PN Lab. Retrieved from [URL]

Version: 1.0 | February 9, 2026

Contact: Mark Lizar, ISO/IEC 27560-1 Profile Editor | mark@transparencylab.ca

Resources:

- ISO/IEC 27560-1 Universal Notice Receipt Profile
- Convention 108+ Modernised Convention
- 0PN Lab Standards Hub
- Digital Transparency Infrastructure Market Analysis

Appendix A: Use Case 3 — Immortal Consent (Digital Estate & UMA Post-Mortem Authorization)

Problem Statement

When an individual dies, their digital authorizations typically die with them. Service providers lock accounts, authorization servers revoke tokens, and families cannot access critical data (photos, financial records, health information) despite legitimate interest. Current identity protocols have no mechanism for authorization transfer or inheritance.

UMA 2.0 Challenge: UMA enables user-managed authorization during life, but provides no path for authorization management after death. The "user" in "user-managed" becomes undefined.

0PN Interop Solution: Immortal Consent via Notice Receipt Inheritance

Architecture: Authorization Transfer Protocol

Pre-Death Setup:

1. **Individual Creates Digital Estate Plan:**
    - Individual designates trusted executor(s) in Notice Receipt wallet
    - Specifies inheritance rules for Notice Tokens per controller
    - Defines data access levels for different beneficiaries
    - Anchors estate plan with L3 ANCR for non-repudiation
2. **Controllers Publish Estate-Aware CIRs:**

```
{
  "controller_id": "service-provider.com",
  "digital_estate_support": true,
  "post_mortem_authorization": {
    "supports_notice_token_transfer": true,
    "executor_verification_required": true,
    "beneficiary_authorization_types": [
      "data_access",
      "data_portability",
      "account_closure"
    ],
    "retention_post_mortem": "Until executor requests deletion"
  },
  "legal_basis_post_mortem": ["Legitimate Interest", "Legal Obligation"]
}
```

1. **Notice Receipts Include Inheritance Metadata:**

```
{
  "notice_token": "nt_immortal_xyz789",
  "pii_principal_id": "did:example:deceased",
  "estate_planning": {
    "executor_did": "did:example:executor",
    "transfer_rules": {
      "full_access": ["executor_did"],
      "limited_access": ["beneficiary_1", "beneficiary_2"],
      "data_types": {
        "photos": "transferable",
        "financial_records": "executor_only",
        "health_data": "restricted"
      }
    },
    "activation_trigger": "verified_death_certificate",
    "anchored_signature": "ANCR_estate_plan_signature"
  }
}
```

Post-Death Authorization Transfer Flow

```
┌────────────────────────────────────────────────────────────
──┐
│         IMMORTAL CONSENT: AUTHORIZATION TRANSFER
│
│            (Post-Mortem Notice Token Inheritance)
│
└────────────────────────────────────────────────────────────
──┘


  Executor            Controller            Trust Anchor       Be
neficiary
     │                   │                     │
│
     │                   │                     │
│
[Death                   │                     │
│
 Certificate]            │                     │
```

```
|
     |                   |                     |
|
     |──[Submit Death Certificate + Executor Proof]──────────
───►|
     |                   |                     |
|
     |                   |                [Verify Death]
|
     |                   |                [Verify Executor]
|
     |                   |                     |
|
     |◄──────────────────────────────────[Authorization Grant]
───|
     |   [Executor Status Token]       |
|
     |                   |                     |
|
 [Access                |                     |
|
  Deceased's            |                     |
|
  Receipts]             |                     |
|
     |                   |                     |
|
     |──[GET /.well-known/notice.txt]────────►|
|
     |                   |                     |
|
     |◄─[CIR: Estate Support Confirmed]───────|
|
     |                   |                     |
|
 [Review               |                     |
|
  Estate Plan]          │                     │
|
     │                   │                     │
|
     │──[Request Authorization Transfer]───────►│
|
     │   {deceased_notice_token,       │
|
     │    executor_status_token,       │
|
     │    estate_plan_ancr}            │
|
     │                   │                     │
|
     │              [Validate:]                │
|
     │              - Death certificate        │
|
     │              - Executor authorization   │
|
     │              - Estate plan ANCR         │
|
     │              - Notice Token binding     │
|
     │                   │                     │
|
     │              [Generate Inherited        │
|
     │               Notice Token]             │
|
     │                   │                     │
|
     │◄─[Transfer UNR]──│                     │
|
     │   {inherited_notice_token,              │
```

```
|
     |    original_notice_token_ref,           |
|
     |    executor_authorization,              |
|
     |    beneficiary_access_rules}            |
|
     |                   |                     |
|
     |              [Log NEL:]                 |
|
     |              "Authorization transferred |
|
     |               to executor per estate    |
|
     |               plan ANCR"                |
|
     |                   |                     |
|
[Delegate               |                     |
|
 to Beneficiary]         |                     |
|
     |                   |                     |
|
     |──[Create Beneficiary Notice Token]────────────────────
──▶|
     |   {inherited_token: "nt_beneficiary_abc",
|
     |    access_scope: "photos_only",
|
     |    valid_until: "2027-12-31"}
|
     |                   |                     |
|
     |                   |                     |
[Access]
     |                   |                     |
[Photos]
     |                   |                     |
|
     |                   |◄────[Present Beneficiary Token]───
───|
     |                   |                     |
|
     |              [Validate Token]           |
|
     |              [Check Scope]              |
|
     |                   |                     |
|
     |                   |──[Grant Limited Access]───────────
──►|
     |                   |   (Photos only, no deletion right
s)  |
     |                   |                     |
|
     |              [Log NEL:]                 |
|
     |              "Beneficiary access granted|
|
     |               per executor delegation"  |
|
```

Key Innovation: "Immortal Consent"

1. Authorization Survives Death

- Notice Tokens include estate planning metadata
- Authorization transfer rules encoded in ANCR
- Bilateral proof persists beyond individual's death

- Controllers honor inherited Notice Tokens

2. Executor as Authorization Manager

- Executor inherits Notice Receipt wallet
- Can query TPI-R on behalf of estate
- Can exercise rights (access, portability, deletion)
- Can delegate limited access to beneficiaries
- Actions logged in Notice Event Log with executor attribution

3. Granular Beneficiary Control

- Executor creates derivative Notice Tokens for beneficiaries
- Each beneficiary receives scope-limited access
- Example: Child gets photo access, accountant gets financial records access, no one gets health data
- Time-limited authorizations (e.g., 1 year to download photos)

4. Cryptographic Non-Repudiation

- L3 ANCR on estate plan prevents disputes
- Death certificate + executor proof required for transfer
- Controllers cannot arbitrarily deny access
- Beneficiaries cannot claim broader access than granted

UMA 2.0 Integration

Traditional UMA Problem:

- Authorization Server (AS) manages policies during life
- Individual dies → policies become orphaned
- No mechanism to transfer policy control
- Resource Server (RS) locks access

0PN Interop Enhancement:

1. Estate-Aware Authorization Server:

```
{
  "authorization_server": "https://uma-as.example.com",
  "estate_planning_endpoint": "https://uma-as.example.com/estate-plan",
  "supports_notice_token_inheritance": true,
  "executor_authorization_flow": "uma-executor-grant"
}
```

2. Executor Authorization Grant Flow:

```
1. Executor presents:
   - Death certificate (verified by Trust Anchor)
   - Executor status token
   - Deceased's Notice Receipt with estate plan

2. Authorization Server validates:
   - Death certificate authenticity
   - Executor legal authority
   - Estate plan ANCR signature
   - Notice Token binding to deceased

3. Authorization Server issues:
   - Executor authorization token (inherited from deceased's policies)
   - Scoped to estate plan rules
   - Logged in Notice Event Log

4. Executor can now:
   - Request resources on behalf of estate
   - Delegate limited access to beneficiaries
   - Exercise data subject rights
   - Close accounts per estate plan
```

3. Resource Server Estate Policies:

```
{
  "resource_server": "https://photos.example.com",
  "estate_access_policy": {
    "accepts_inherited_tokens": true,
    "executor_permissions": ["read", "download", "delete"],
    "beneficiary_permissions": ["read", "download"],
    "verification_required": "L3-ANCR",
    "retention_post_transfer": "90 days after executor notifi
cation"
  }
}
```

Regulatory Alignment

Convention 108+ Article 9 (Data Subject Rights):

- Rights exercisable by legal representatives post-mortem
- Notice Receipt inheritance enables representative action
- Bilateral proof protects estate from controller denial

GDPR Recital 27:

- Regulation does not apply to deceased persons
- BUT member states may provide rules for post-mortem data processing
- Notice Token inheritance provides technical mechanism for such rules

Succession Laws (Jurisdiction-Specific):

- Executor legal authority varies by jurisdiction
- Notice Receipt estate plan references applicable law
- Controllers verify executor authority via jurisdiction-specific proofs

Implementation Example: Digital Photo Estate

Scenario: Individual has 20 years of family photos on cloud service, wants children to inherit access after death.

During Life:

1. Individual creates estate plan in Notice Receipt wallet:

```
{
  "estate_plan_id": "estate_plan_photos_2026",
  "controller": "cloud-photos.example.com",
  "executor": "did:example:spouse",
  "beneficiaries": [
    {"did": "did:example:child1", "access": "full_photos"},
    {"did": "did:example:child2", "access": "full_photos"}
  ],
  "actions_authorized": ["view", "download", "share"],
  "actions_prohibited": ["delete", "modify", "upload_new"],
  "expiration": "2030-12-31",
  "ancr_signature": "anchored_2026-02-09"
}
```

1. Cloud service publishes estate-aware CIR
2. Individual's Notice Receipt includes estate plan reference
3. L3 ANCR anchors estate plan (non-repudiable)

After Death:

1. **Executor Actions:**
    - Submits death certificate to Trust Anchor
    - Receives executor status token
    - Presents inherited Notice Token to cloud service
    - Cloud service validates via estate plan ANCR
    - Executor granted access to photos
2. **Beneficiary Delegation:**
    - Executor creates derivative Notice Tokens for children
    - Child 1 receives: `nt_beneficiary_child1_photos`

    - Child 2 receives: `nt_beneficiary_child2_photos`
    - Both tokens scoped to: view + download only, no deletion
    - Tokens valid until 2030-12-31
3. **Access Flow:**
    - Child 1 presents beneficiary token to cloud service
    - Cloud service validates token lineage: deceased → executor → child1
    - Cloud service verifies scope: photos only, no delete
    - Access granted for 90 days to download all photos
    - Notice Event Log records: "Beneficiary access per estate plan"
4. **Closure:**
    - After beneficiaries download photos (or expiration date)
    - Executor exercises deletion right via inherited Notice Token
    - Cloud service deletes account per estate plan
    - Final Notice Event Log entry: "Account closed per executor request, estate plan fulfilled"

Security Properties

1. Prevents Unauthorized Access:

- Death certificate verification required
- Executor authority validated
- Estate plan ANCR signature checked
- Cannot forge inheritance without all three proofs

2. Protects Against Executor Abuse:

- Estate plan ANCR limits executor powers
- Executor cannot exceed scope defined by deceased
- Notice Event Log tracks all executor actions
- Beneficiaries can audit executor activities

3. Prevents Controller Overreach:

- Controller cannot arbitrarily deny estate access
- Bilateral proof (inherited Notice Receipt) is evidence
- Regulator can verify controller honored estate plan
- TPI-R includes estate support transparency

4. Time-Limited Access:

- Beneficiary tokens have expiration dates
- Prevents indefinite access to deceased's data
- Aligns with data minimization principles
- Controller can enforce retention limits

Comparison: Current State vs Immortal Consent

Current State (Surveillance-by-Default):

- Individual dies → accounts locked automatically
- Family must navigate each service's unique "deceased user" policy
- Requires death certificates, legal documents per service
- No standardized process
- Access often denied even with legal authority
- No audit trail of post-mortem data access
- No bilateral proof of deceased's wishes

Immortal Consent (Transparency-by-Default):

- Individual pre-authorizes estate access via Notice Receipt
- Standardized transfer protocol across all controllers
- Single executor status token works everywhere
- Controllers honor inherited Notice Tokens
- Complete audit trail in Notice Event Logs

- Bilateral proof: deceased's estate plan ANCR + executor's inherited token
- Granular beneficiary control per deceased's wishes

Business Value

For Individuals:

- Peace of mind: digital estate plan will be honored
- Granular control: specify exactly who gets what access
- Portable: one estate plan works across all compliant services
- Verifiable: L3 ANCR provides cryptographic proof of intent

For Families/Executors:

- Simplified access: single protocol across services
- Legal protection: bilateral proof supports estate administration
- Reduced friction: no per-service death certificate submissions
- Audit trail: Notice Event Logs document all actions

For Controllers:

- Reduced support burden: automated estate authorization flow
- Legal protection: ANCR proves deceased's consent to data transfer
- Compliance: demonstrates respect for data subject rights post-mortem
- Competitive advantage: "digital estate planning support" feature

For Regulators:

- Standardized oversight: TPI-R includes estate support transparency
- Evidence-based enforcement: Notice Event Logs show estate plan compliance
- Cross-border coordination: Convention 108+ enables mutual recognition
- Policy development: Notice Event Logs provide empirical data on post-mortem data practices

Future Extensions: Advanced Estate Scenarios

1. Conditional Access Triggers:

```
{
  "conditional_release": {
    "trigger": "child_turns_18",
    "beneficiary": "did:example:minor_child",
    "release_date": "2035-06-15",
    "data_types": ["family_photos", "letters_to_child"],
    "notification": "automated_on_trigger_date"
  }
}
```

2. Multi-Sig Estate Plans:

- Requires multiple executors to approve access
- Prevents single executor abuse
- Useful for high-value digital assets

3. Progressive Disclosure:

- Staged access over time
- Example: Beneficiary gets financial summary immediately, detailed records after 6 months
- Reduces information overload for grieving families

4. Digital Asset Marketplace:

- Inherited Notice Tokens enable digital asset transfer
- NFTs, cryptocurrency wallets, domain names
- Estate plan specifies transfer or liquidation

Core Innovation

0PN Interop's Immortal Consent transforms "user-managed authorization" into **"human-managed authorization that transcends mortality"**—ensuring individuals' data control wishes extend beyond death through cryptographically-anchored, bilaterally-proven, standardized authorization inheritance.