

How UMA Enables Licensing Access to Digital Assets

Eve Maler | UMA WG Chair | eve@xmlgrri.com

Tim Reiniger | UMA WG Legal Editor | tsreiniger@gmail.com

21 August 2018



User-Managed Access is a set of specifications from Kantara Initiative

- The specifications are currently at Version 2.0
- Multiple implementations exist (products and open source)
- The Work Group operates under the Kantara IPR policy “Option Patent & Copyright: Reciprocal Royalty Free with Opt-Out to Reasonable And Non discriminatory (RAND)”
- See the group’s wiki home page for relevant details:
<https://kantarainitiative.org/confluence/display/uma/Home>

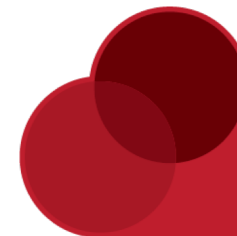
UMA is designed to give an individual a unified control point for authorizing who and what can access a wide variety of digital assets, at their desired “grain”

Some use cases:


- For financial consumers
 - Discovering and aggregating UK pension accounts and sharing access to financial advisors
- In industrial and consumer IoT
 - For proactively or dynamically sharing smart device control or data with others
- Healthcare
 - Health Relationship Trust (HEART) WG: patient-controlled health data exchange
 - Part of the new OpenMedReady framework for trustworthy remote care




Alongside Open APIs, **UMA would enable consumers to have full control of who can access their data and for how long** – granting access for example, to their **financial adviser** or the Single Financial Guidance Body – as well as the ability to revoke access and for security to be in place to prove who is accessing the data. The UMA approach to security and consent is also well aligned with the requirements of GDPR (General Data Protection Regulations).






Grocery store portal

 Sharing

 Activity

Sharing
Manage your shared resources.

- Personal Info
- Sign-in & Security
- Preferences
- Trusted Devices
- Authorized Apps
- Privacy & Consent
- Sharing**
- Activity
- Account Controls


	Party Food Shopping List	Shared with 2 people
	Shopping List	Not shared
	Oliver's Bday Wish List	Shared with 2 people

Share



Shared with 2 people.

People


Permissions


 LIST

Oliver's Bday Wish List

 ed.enduser@example.com	<input type="button" value="View"/> <input type="button" value="Share"/> <input type="button" value="Edit"/>	<input type="button" value="Unshare"/>
 edna.enduser@example.com	<input type="button" value="View"/>	<input type="button" value="Unshare"/>

Grocery store portal





 Sharing

 Activity

- Personal Info
- Sign-in & Security
- Preferences
- Trusted Devices
- Authorized Apps
- Privacy & Consent
- Sharing
- Activity**
- Account Controls

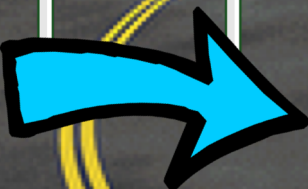
Activity

Account actions you've taken in the last 28 days.

	Party Food Shopping List You updated sharing	9 hours ago
	Party Food Shopping List ed.enduser@example.com viewed	1 day ago
	Oliver's Bday Wishlist You allowed access to ed.enduser@example.com	1 day ago
	Oliver's Bday Wishlist edna.enduser@example.com shared	July 2, 2017



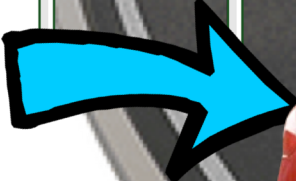
Coordinate with smart city



Let renters use for \$\$



Pick up dry cleaning



\$ from correct operator



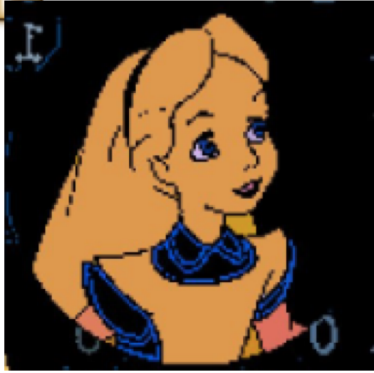
Connected car

Health IoT

Sharing pulse oximeter data in a trusted and consented way with third parties through loosely coupled cloud services



2



Strongly authenticated user identity

3



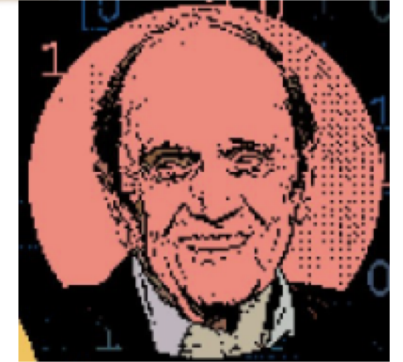
User/device association

4

Consented device data sharing with others



5



Strongly authenticated third-party identity

1



Certified device identity

5



Cryptographic auditability

Standards

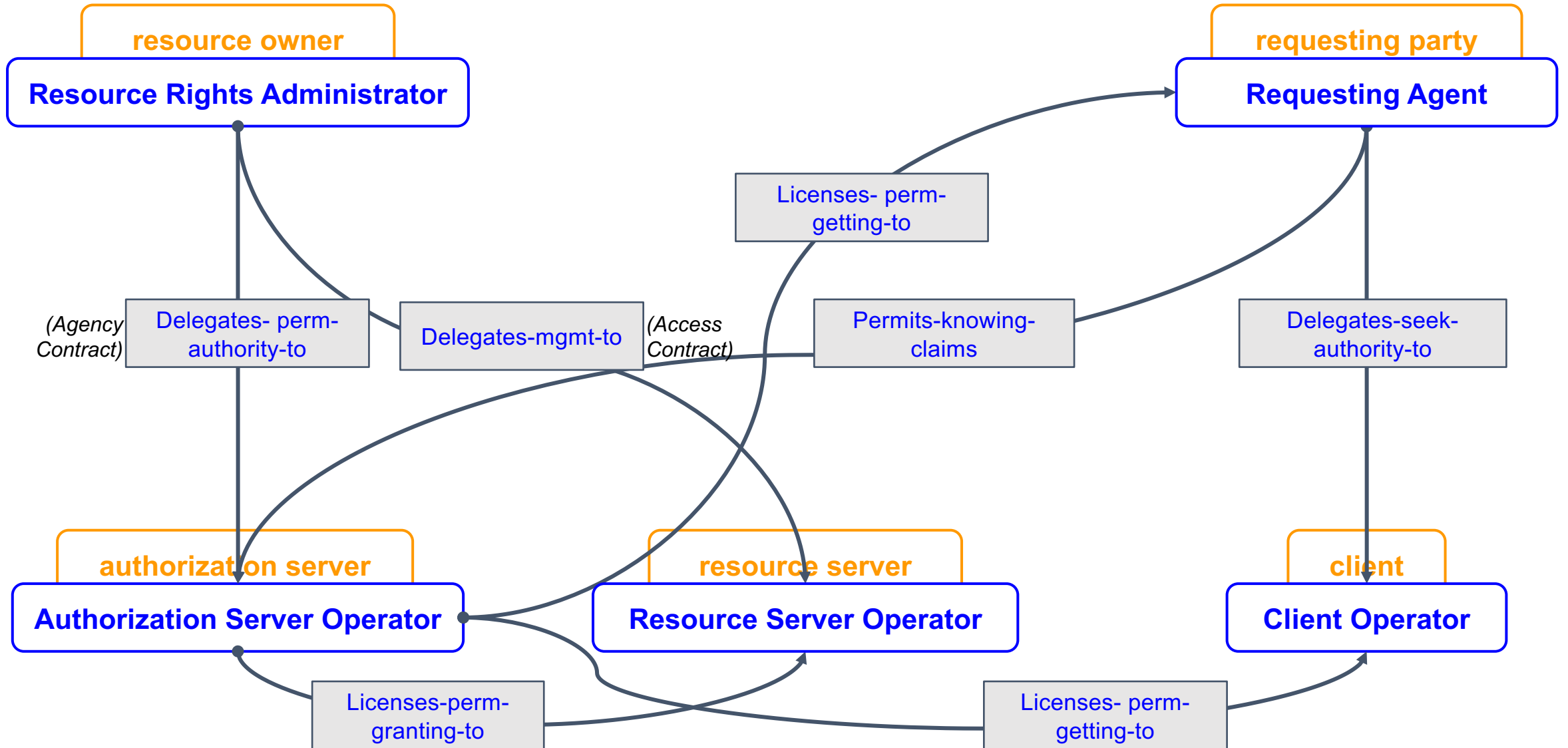


Where the UMA work is heading: a business model

- Model real-life relationships in, say, a graph database
- Implement lifecycle stages needing “sharing controls” in UMA
- We have been mapping legal devices to technical artifacts: OAuth/UMA token, policies, etc.
 - These artifacts are auditable
 - UMA assists in unique properties for compliance and user trust
- When a relationship changes, the artifacts can be torn down and new ones can be built up
 - These changes themselves can be made auditable
 - Much like “right to erasure” workflows, they can be hardened

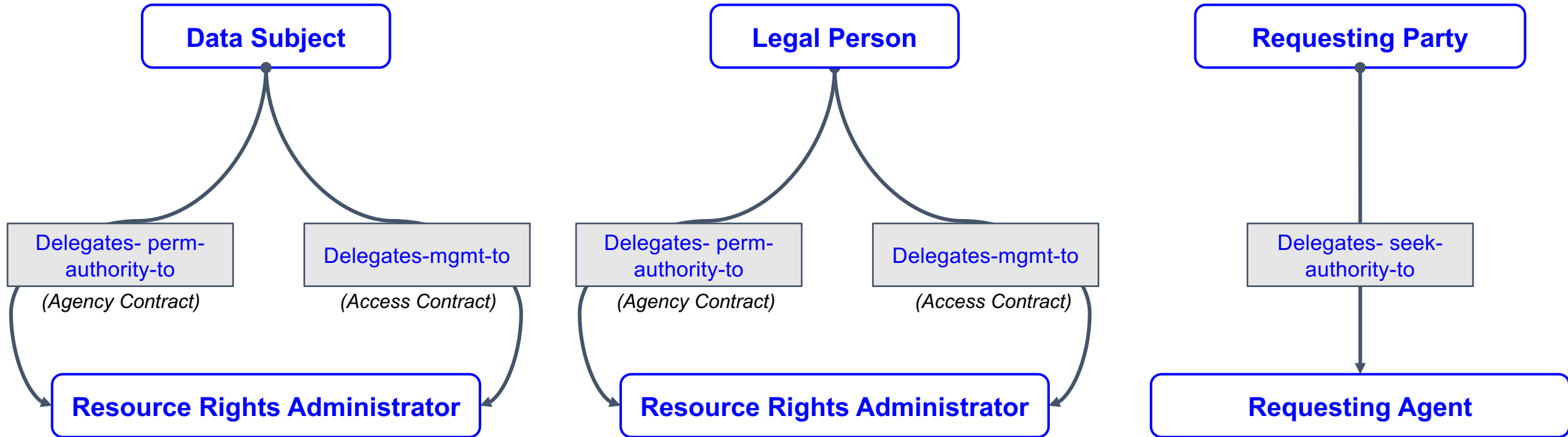
Legal relationships: “Endpoint to endpoint”

Intra-protocol relationships among parties in legal roles, illustrated



Legal relationships: “Extending the ends”

How “offline” types of parties may play delegation roles, illustrated



A Data Subject may not wish to, or be capable of being, his/her own Resource Rights Administrator (for example, wishing to give power of attorney to someone else) and delegates permissions and resource management.

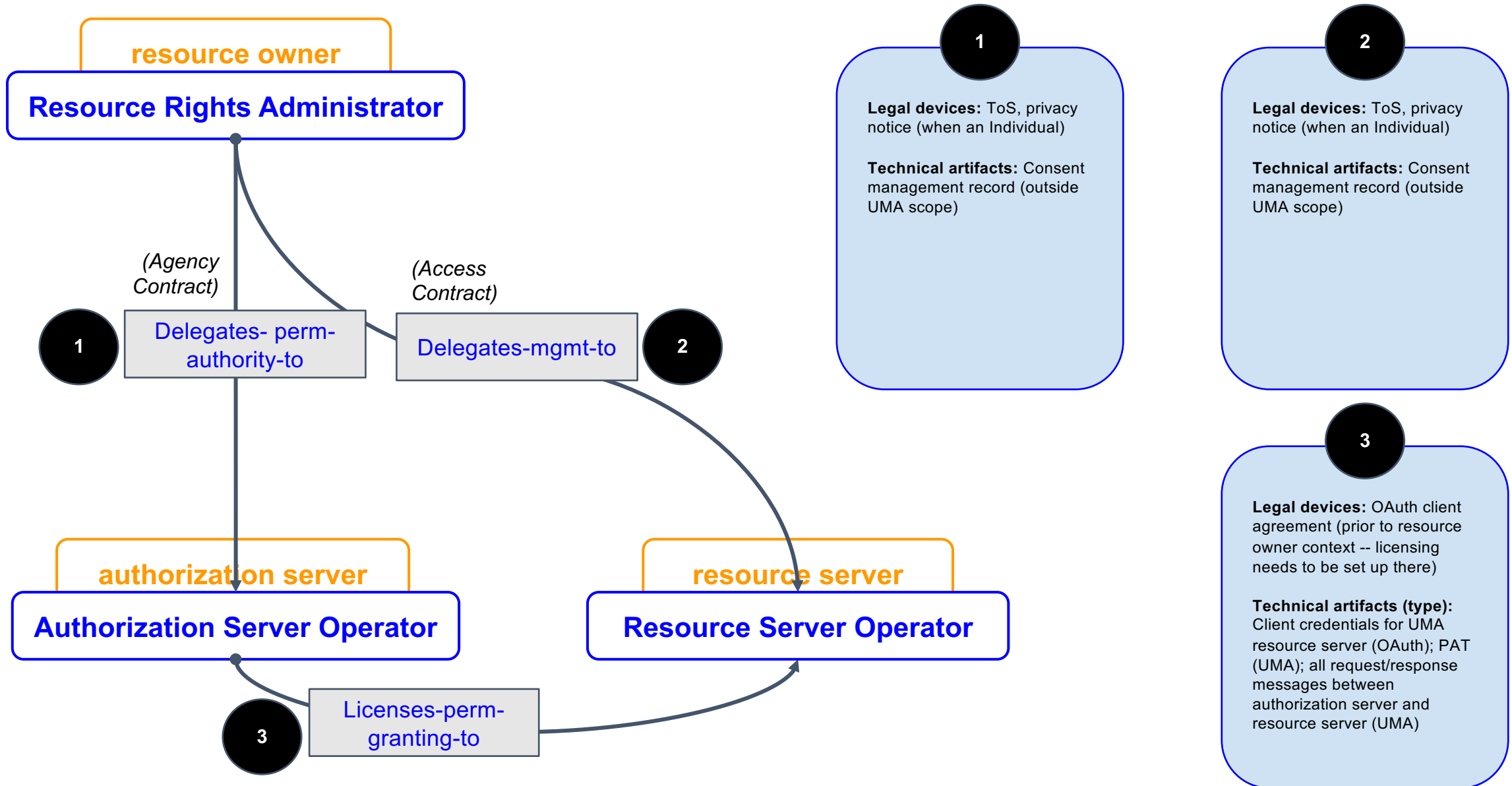
A Legal Person may delegate manual permissions and resource management to an administrator (for example, an employee as an Individual RRA).

A Requesting Party may be an Individual or a Legal Person, and a Requesting Agent may also be an Individual or a Legal Person. The former may not wish to be, or be capable of being, its own Agent.

In that case, a Requesting Party may delegate access-seeking authority to another party on its behalf (for example, in the case of a hospital having a specific clinician seek access as its employee, an Individual RqPA).

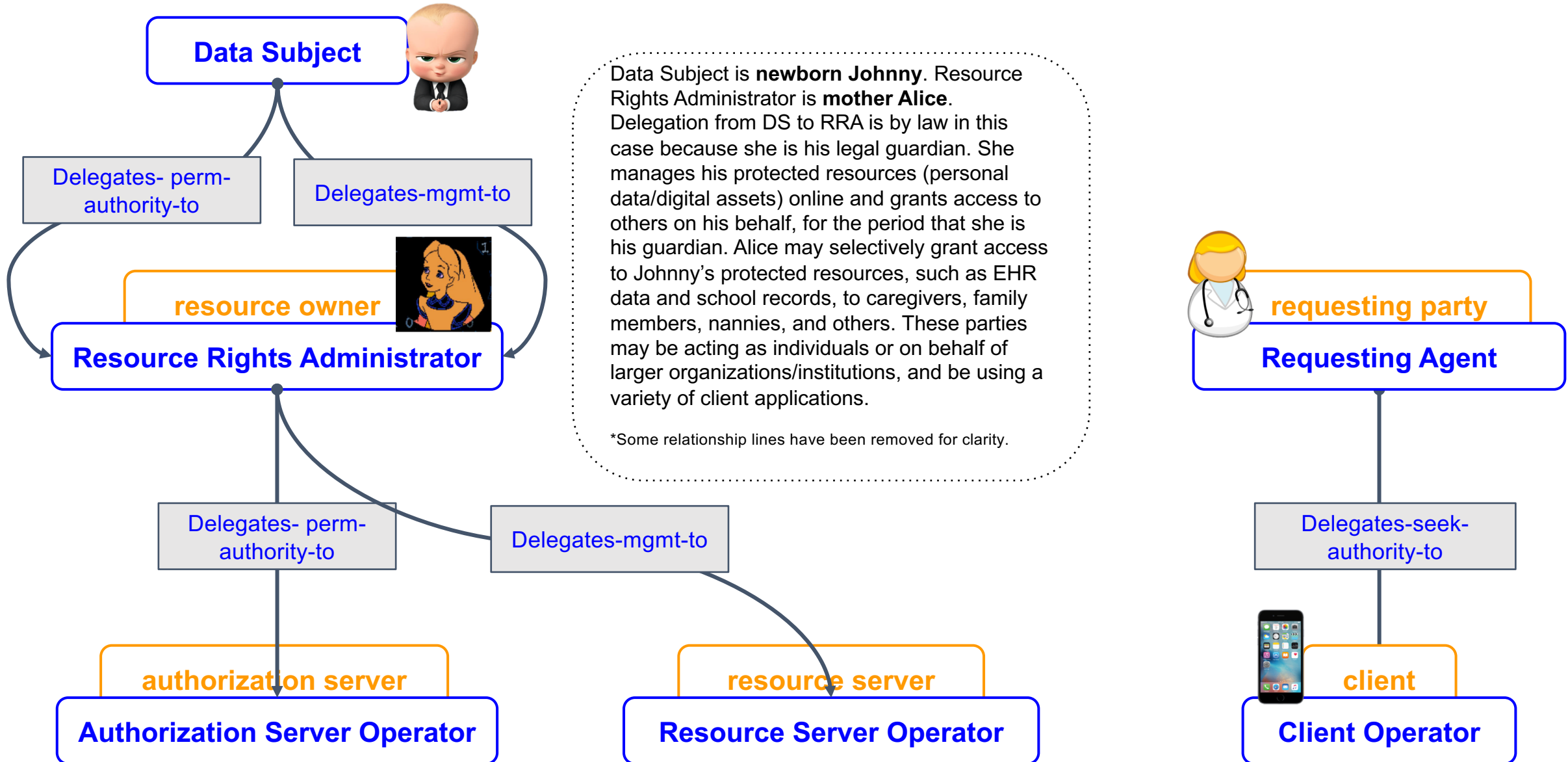
Legal relationships: Devices and artifacts

Making relationships and their changes auditable and machine-readable



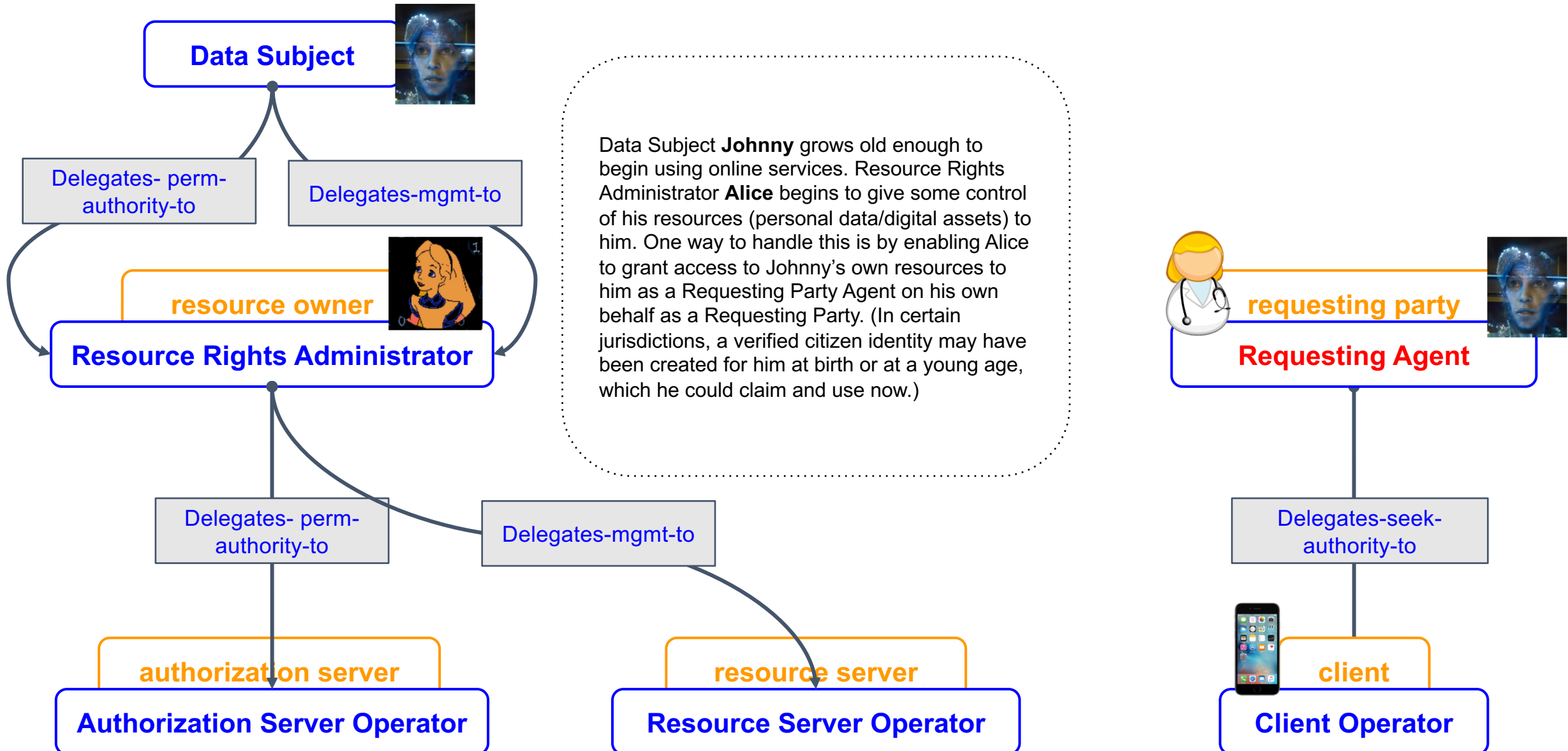
Scenario: Cradle-to-grave

1. Data Subject is too young to use digital assets



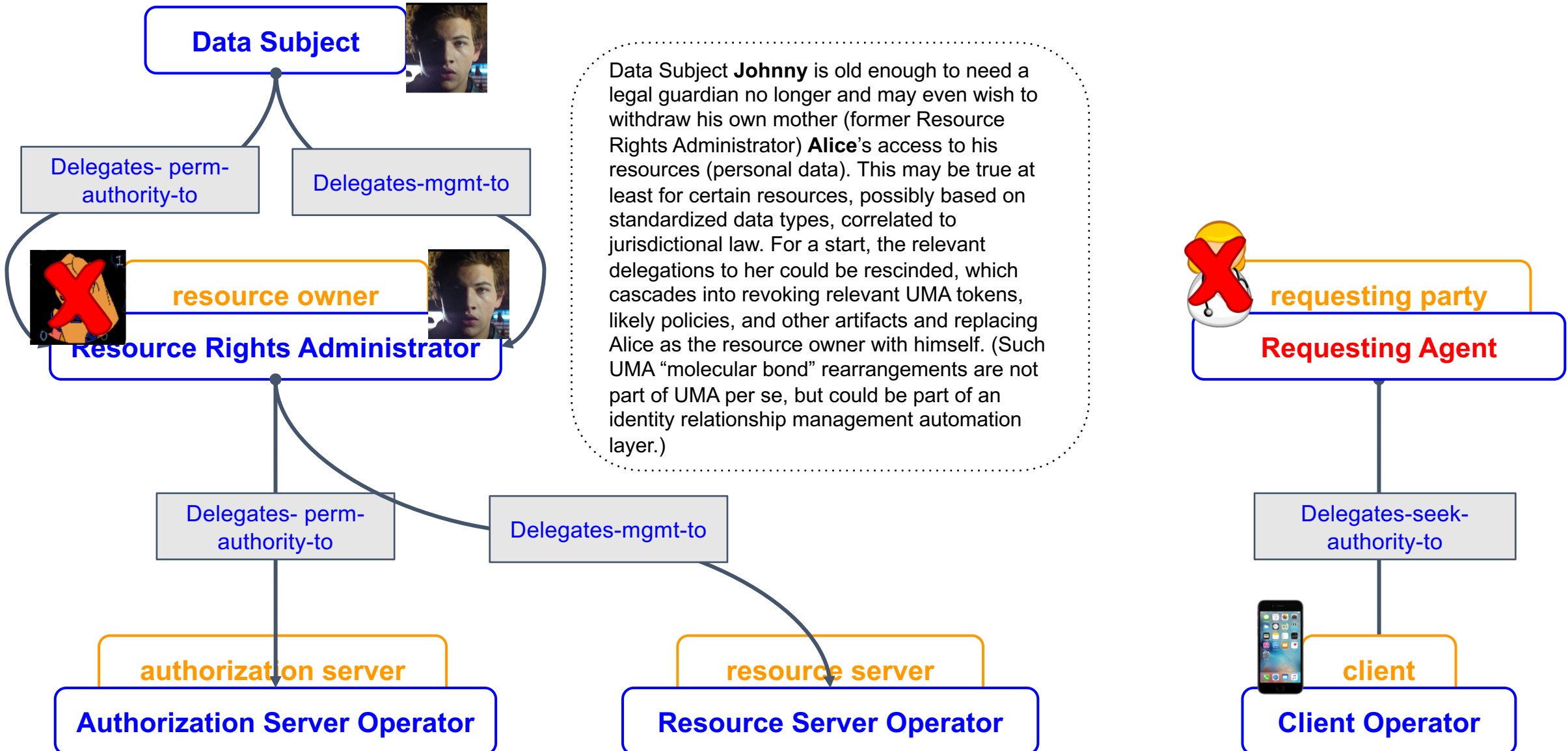
Scenario: Cradle-to-grave

2. Data Subject is old enough to use assets but too young to consent to their use



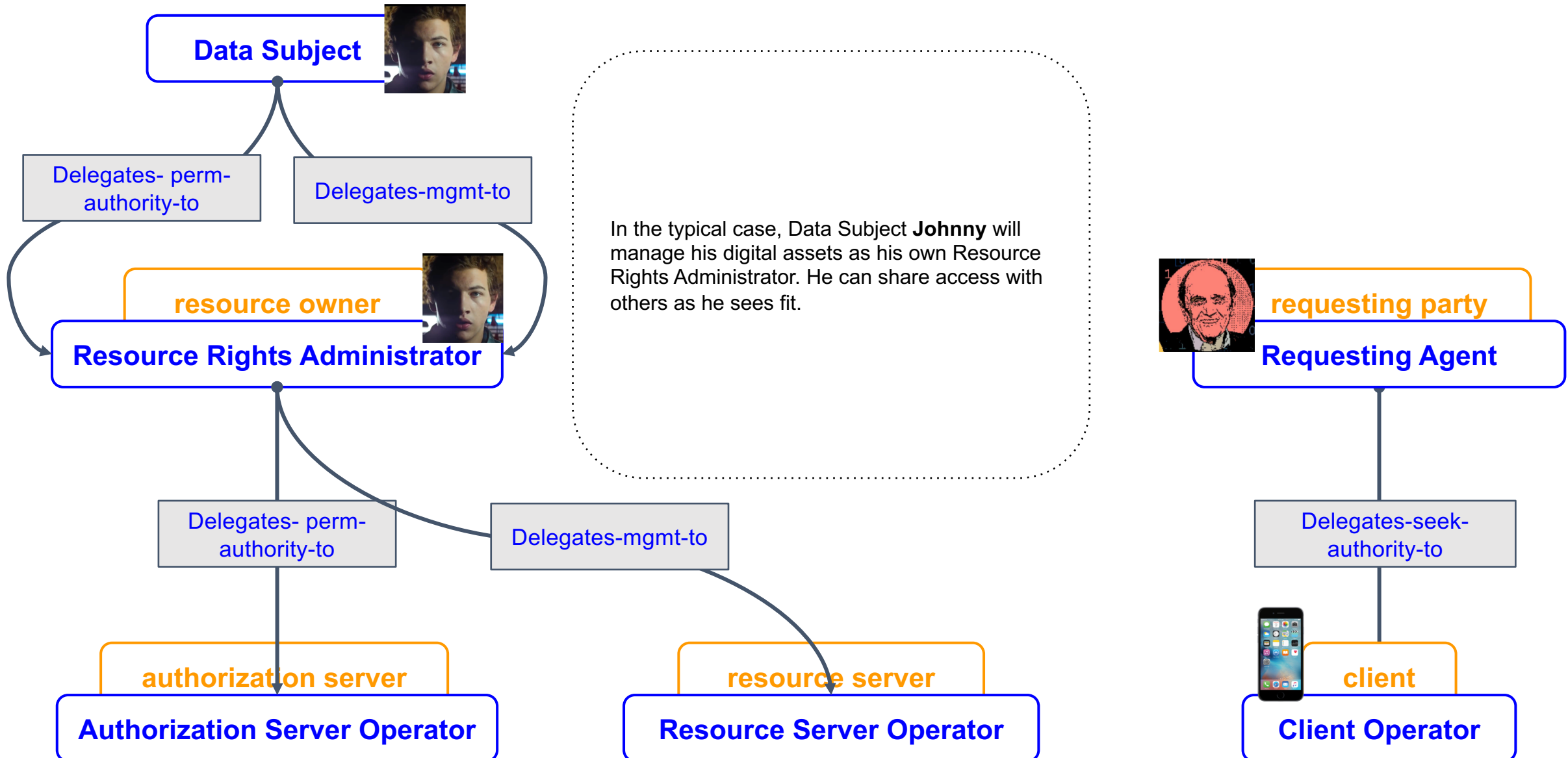
Scenario: Cradle-to-grave

3. Data Subject is old enough to consent to their use and manages digital assets themselves



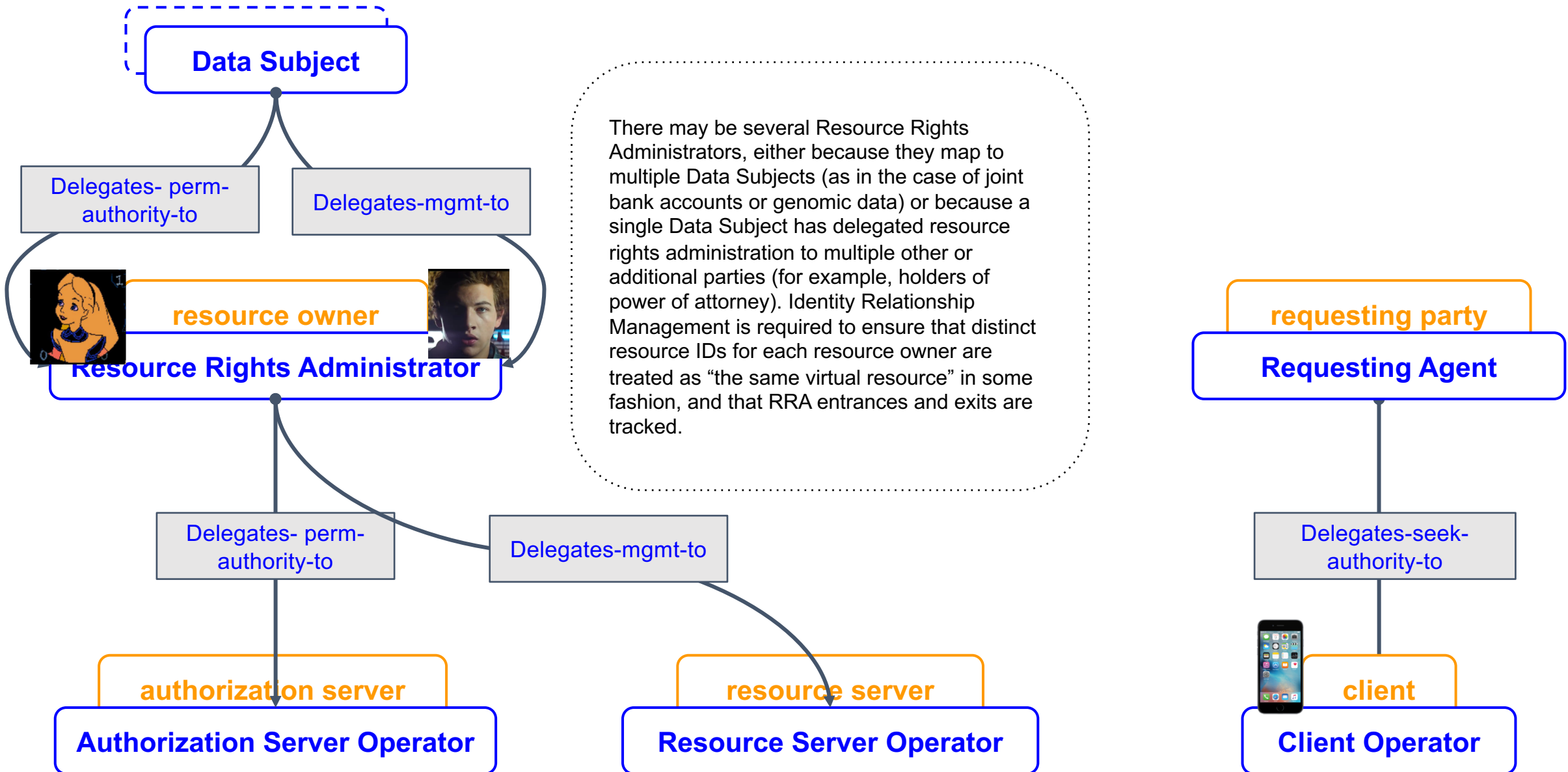
Scenario: Cradle-to-grave

3a. Steady state: Data Subject manages their own digital assets



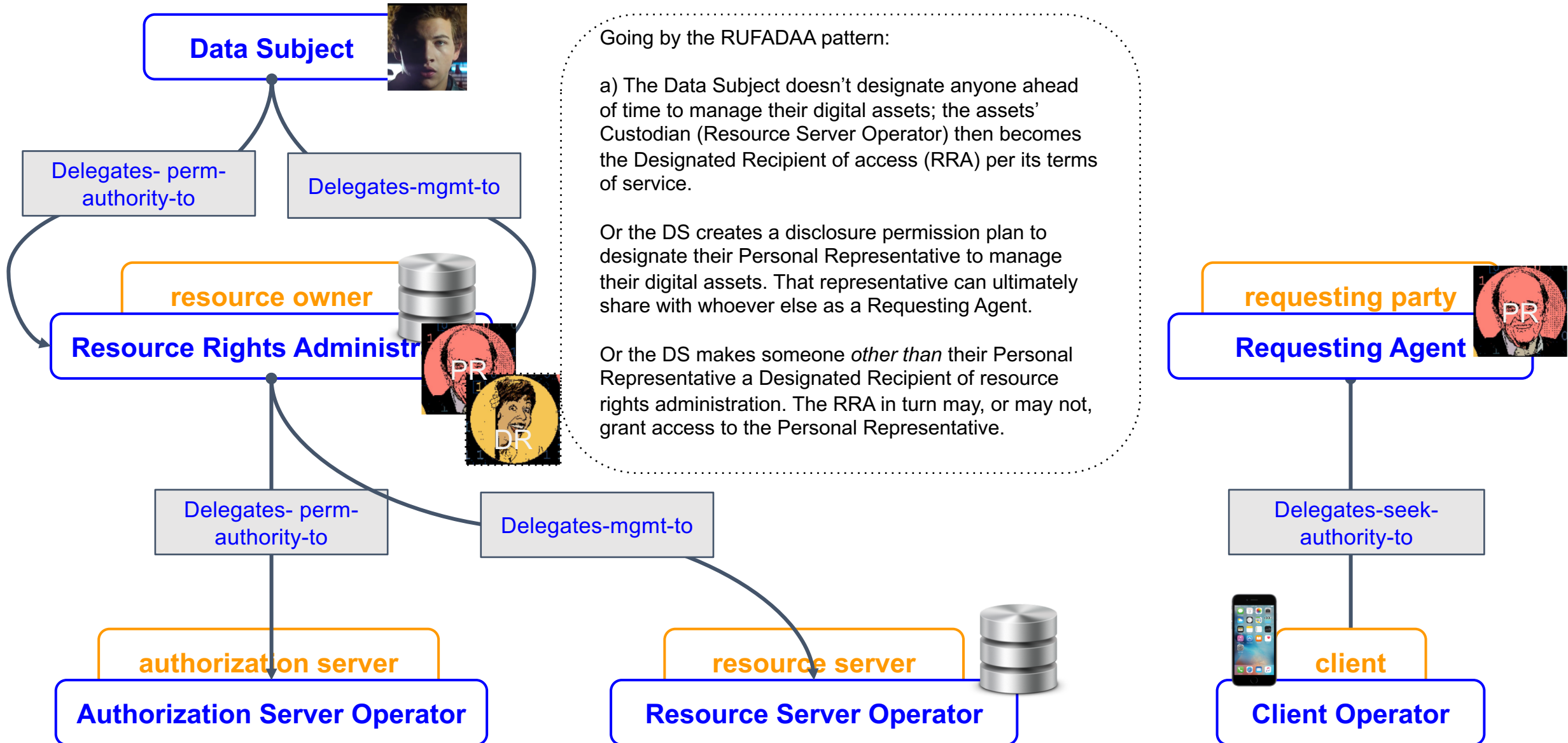
Scenario: Cradle-to-grave

4. There are multiple administrators of resource rights



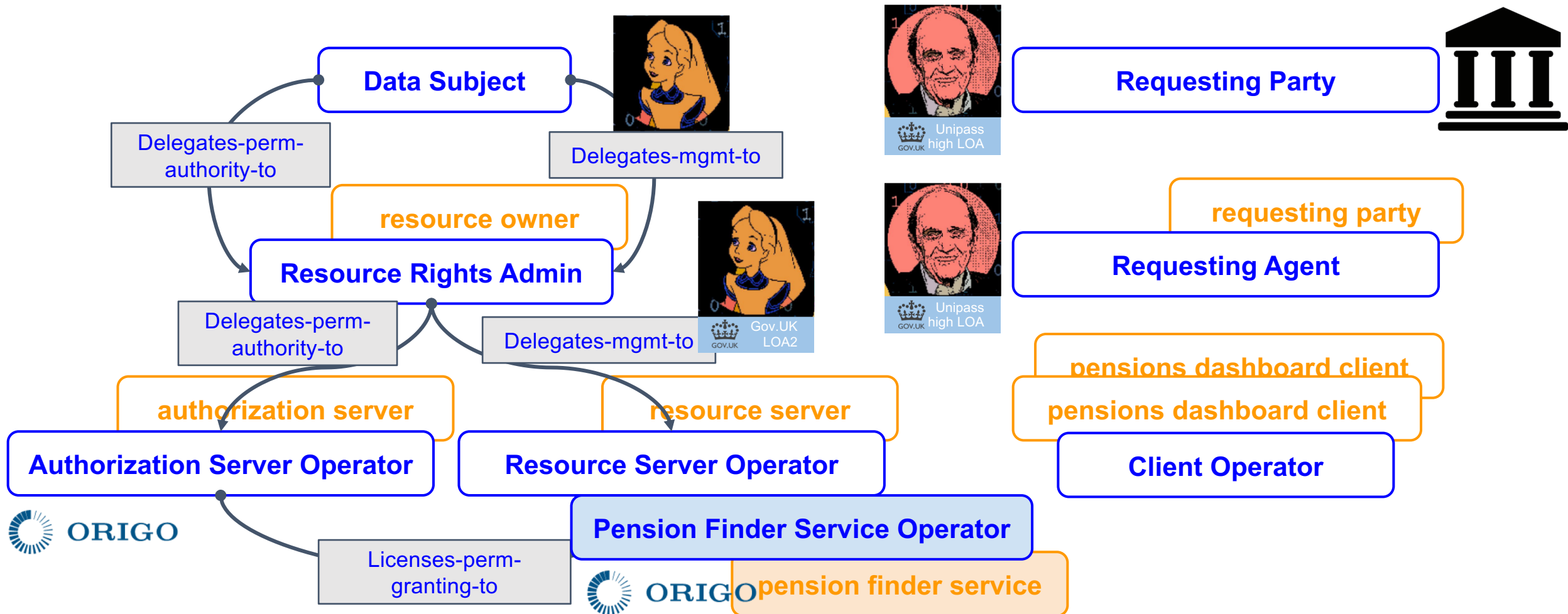
Scenario: Cradle-to-grave

5. Data Subject becomes mentally incapacitated or dies



Scenario: UK Pensions Dashboard

Step 2



Alice, now in her shared-with role as "Big Alice", can now selectively share pension account information to financial advisors from a resource server run by the government that was sourced from the Pension Finder Service.
Guessing about the relationships between the services.

Through the Unipass IdP run by Origo for financial advisors, Bob provides high-LOA claims to get access. He may work for himself or a larger firm. **Guessing about varying RqP/RqPA relationships.**