Data Rights Protocol

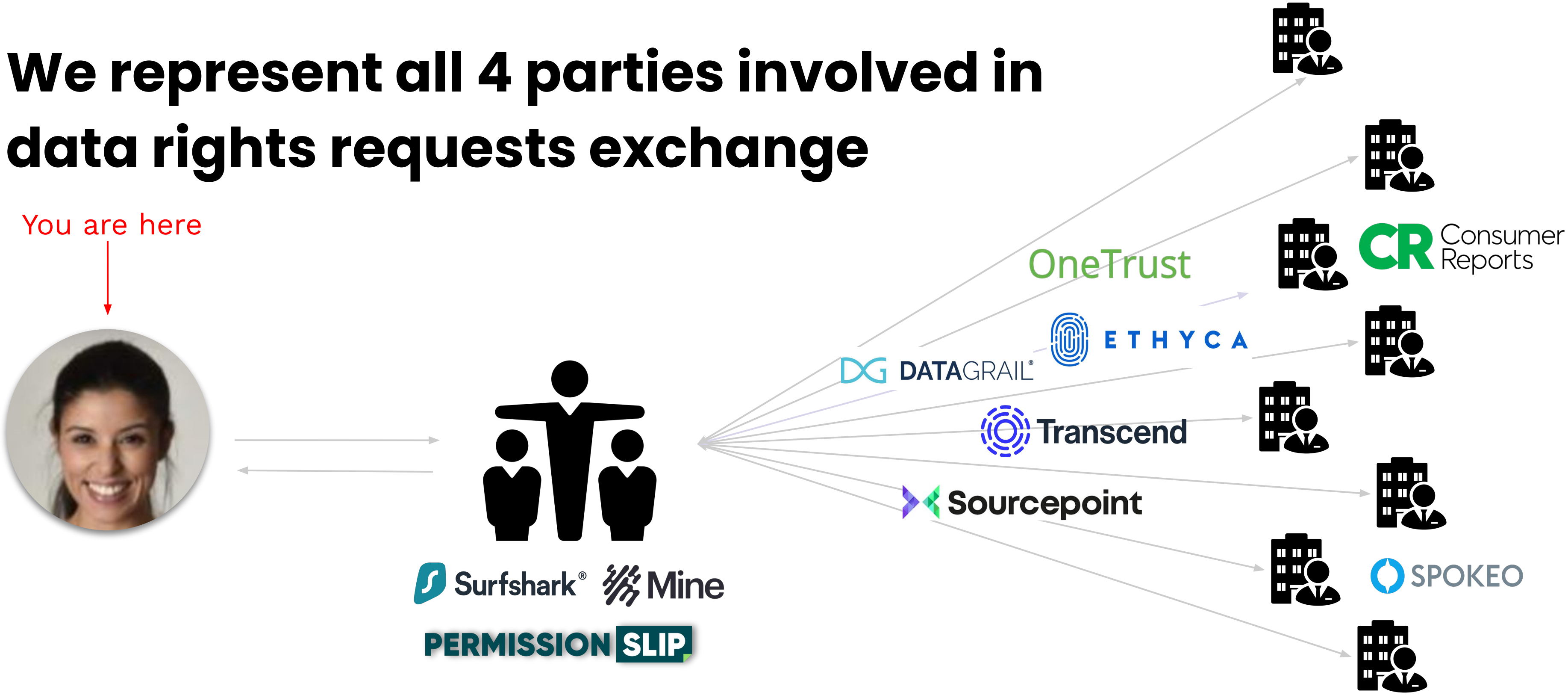
A technical standard for exchanging data rights requests, incubated at Consumer Reports Digital Lab

Consumer Reports®

Consumers have new rights to their data.

There is no standard way to exchange data rights requests under the law.

We represent all 4 parties involved in data rights requests exchange



Consumer authorizes agent

Agent helps consumer submit request

Privacy compliance tech facilitates request

Covered business processes request

We are a consortium of companies that play different roles in the exchange of data rights requests

OneTrust

DATAGRAIL®

SPOKEO

Transcend

Surfshark®

ETHYCA

Sourcepoint

Mine

wirewheel

MIT Connection Science
the technology of innovation

CR Consumer Reports

We're deploying a system and standard to make data rights real.

The goal is to deploy a holistic Data Rights System in three dimensions:

Technical protocol

Participatory network

Operating rules

The goal is to deploy a holistic Data Rights System in three dimensions:

Technical protocol

Technology

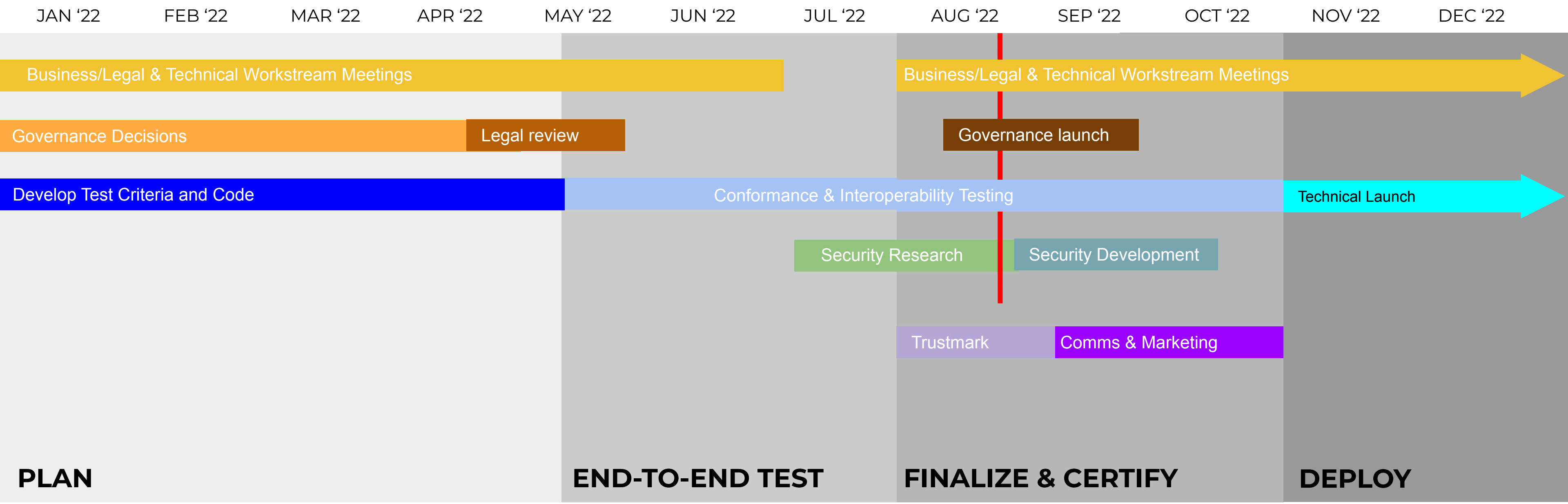
Participatory network

Business

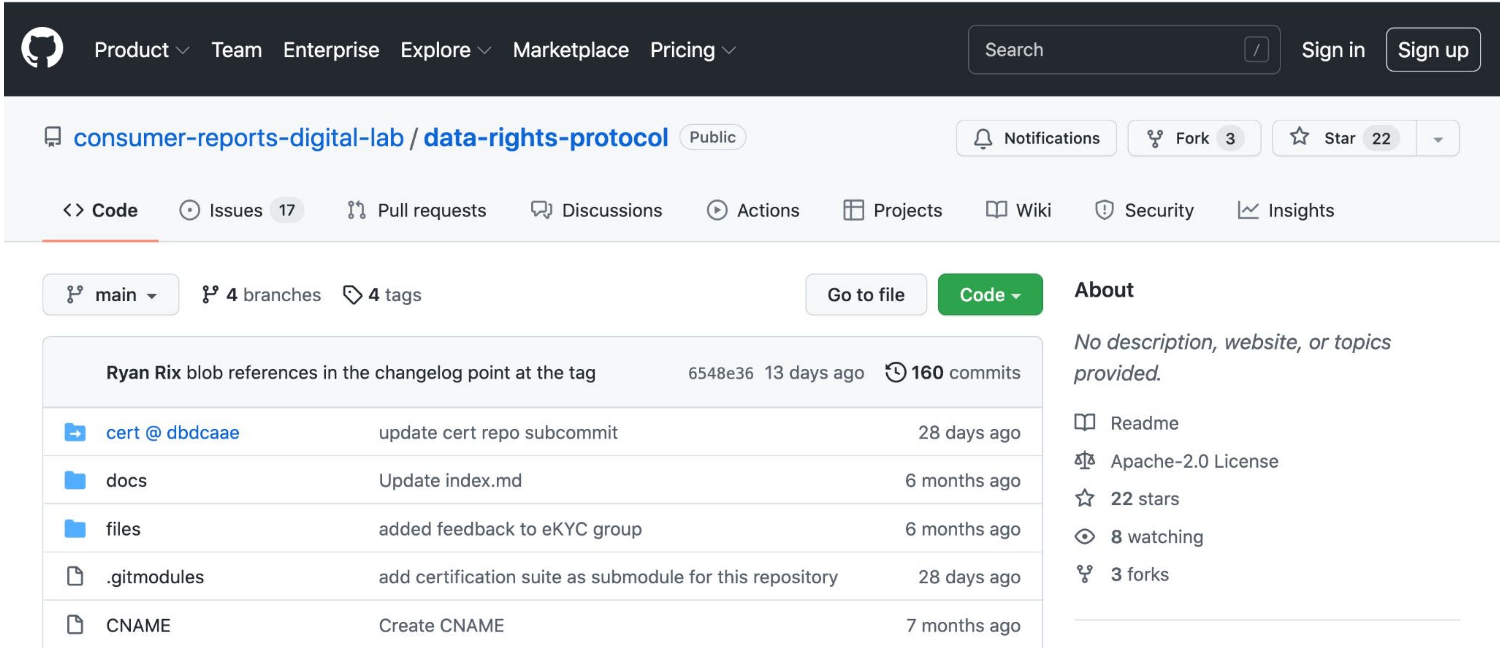
Operating rules

Legal

We facilitate the Business, Legal, & Technical workstreams necessary for deployment



Data Rights Protocol is developed openly on GitHub, with plans to deploy in production later this year



Ryan Rix blob references in the changelog point at the tag 6548e36 13 days ago 160 commits

cert @ dbdcaae	update cert repo subcommit	28 days ago
docs	Update index.md	6 months ago
files	added feedback to eKYC group	6 months ago
.gitmodules	add certification suite as submodule for this repository	28 days ago
CNAME	Create CNAME	7 months ago

About

No description, website, or topics provided.

- Readme
- Apache-2.0 License
- 22 stars
- 8 watching
- 3 forks

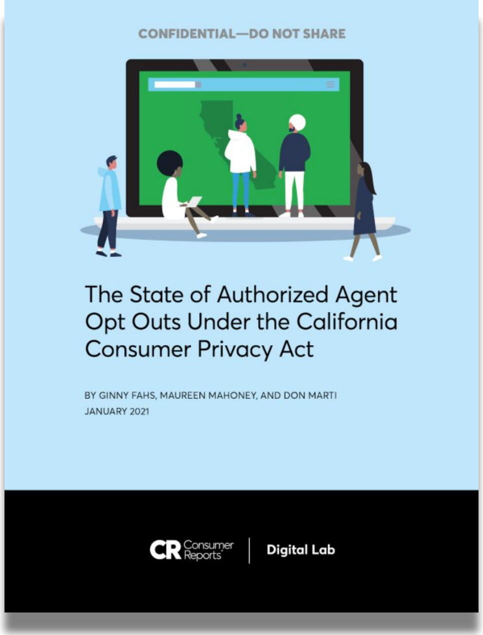
https://github.com/consumer-reports-digital-lab/data-rights-protocol

DRP is one of many initiatives Consumer Reports is backing to make consumer data rights real

California Consumer Privacy Act:
Are Consumers' Digital Rights Protected?

MAUREEN MAHONEY
OCTOBER 1, 2020

CR Consumer Reports | Digital Lab

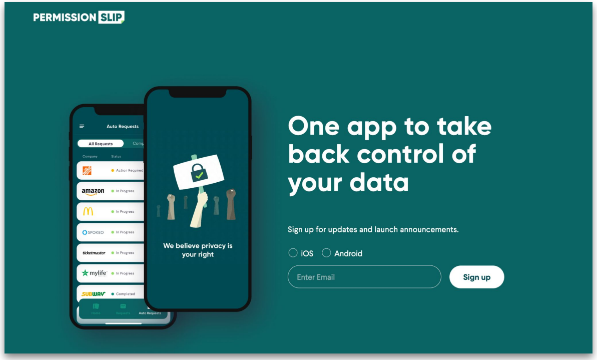


CONFIDENTIAL—DO NOT SHARE

The State of Authorized Agent Opt Outs Under the California Consumer Privacy Act

BY GINNY FAHS, MAUREEN MAHONEY, AND DON MARTI
JANUARY 2021

CR Consumer Reports | Digital Lab



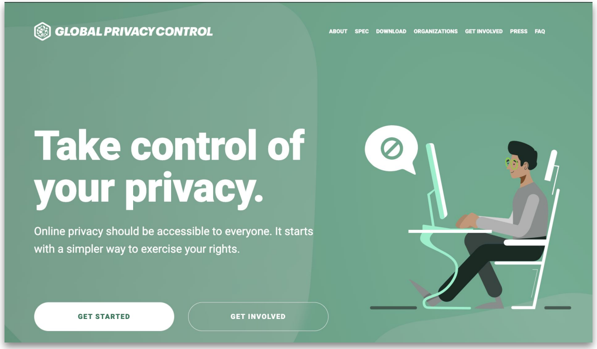
PERMISSION SLIP

One app to take back control of your data

Sign up for updates and launch announcements.

○ iOS ○ Android

Enter Email | Sign up



GLOBAL PRIVACY CONTROL

ABOUT SPEC DOWNLOAD ORGANIZATIONS GET INVOLVED PRESS FAQ

Take control of your privacy.

Online privacy should be accessible to everyone. It starts with a simpler way to exercise your rights.

GET STARTED | GET INVOLVED

PERMISSION SLIP

We bring expertise in law, technology & business

Dazza Greenwood
Protocol Lead
dazza@civics.com

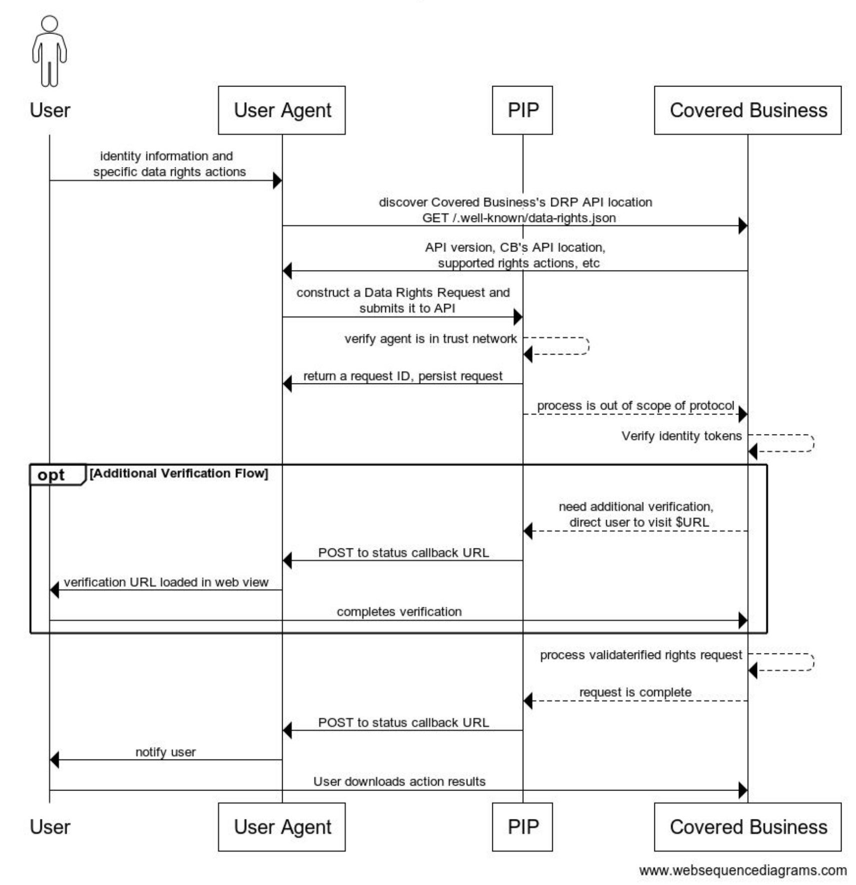
Ryan Rix
Tech Lead
drp@rix.si

Ginny Fahs
Director, Product R&D
ginny.fahs@consumer.org

Note: Nobody here ^ is a security engineer

Data Rights Protocol

- A communication workflow to receive, process, and complete data rights requests in an interoperable fashion.



User

User Agent

PIP

Covered Business

identity information and specific data rights actions

discover Covered Business's DRP API location GET /.well-known/data-rights.json

API version, CB's API location, supported rights actions, etc

construct a Data Rights Request and submits it to API

verify agent is in trust network

return a request ID, persist request

process is out of scope of protocol

Verify identity tokens

opt [Additional Verification Flow]

need additional verification, direct user to visit $URL

POST to status callback URL

verification URL loaded in web view

completes verification

process validaterified rights request

request is complete

POST to status callback URL

notify user

User downloads action results

User

User Agent

PIP

Covered Business

www.websequencediagrams.com

Data Rights Protocol

- A communication workflow to receive, process, and complete data rights requests in an interoperable fashion.

- **A set of simple HTTPS + JSON endpoints**

```
GET  /.well-known/data-rights.json
POST /exercise
GET  /status
POST /revoke
POST status_callback
```

Data Rights Protocol

- A communication workflow to receive, process, and complete data rights requests in an interoperable fashion.
- A set of simple HTTPS + JSON endpoints
- **A data request format**

```
{
  "meta": {
   "version": "0.5"
  },
  "regime": "ccpa",
  "exercise": [
   "sale:opt-out"
  ],
  "identity": <jwt>... ,
  "status_callback": ...
}
```

Data Rights Protocol

- A communication workflow to receive, process, and complete data rights requests in an interoperable fashion.

- A set of simple HTTPS + JSON endpoints

- A data request format

- **An agreement to support JWT identity tokens**

Data Rights Protocol

- A communication workflow to receive, process, and complete data rights requests in an interoperable fashion.
- A set of simple HTTPS + JSON endpoints
- A data request format
- An agreement to support JWT identity tokens
- **A state machine representing the full lifecycle of a Data Rights Request**

Data Rights Protocol

- A communication workflow to receive, process, and complete data rights requests in an interoperable fashion.
- A set of simple HTTPS + JSON endpoints
- A data request format
- An agreement to support JWT identity tokens
- A state machine representing the full lifecycle of a Data Rights Request
- **A process for providing additional information or verification by the User**

Data Rights System in three dimensions:

Technical protocol

Participatory network

Operating rules

We plan to deploy the protocol as a trust network.

B2B trust network

- Authorized Agents and Covered Businesses can enter trust agreements in a network with services (think Visa/Mastercard)
- Authorized Agents can provide identity attestations at levels of assurance which businesses are able to trust
- At the same time, the Authorized Agent is an agent ***<u>of the</u>*** consumer

Decentralized models?

- In a perfect world, individuals could submit their own standard data rights requests

- Without strong self-sovereign identity businesses have no reason to trust submitted identity attributes though!

- But self-sovereign identity isn’t fully baked…

- Of course, centralized models were considered but not appropriate

Externally issued identity model?

- We need first and second parties, not third parties with non-conforming trust models, legal relationships and business roles

- Individuals should not need to submit more data to companies to be able to access their rights (scope creep)

- Considering models by OpenID Connect (OIDC) Foundation, electronic Know Your Customer (eKYC)

B2B trust network!

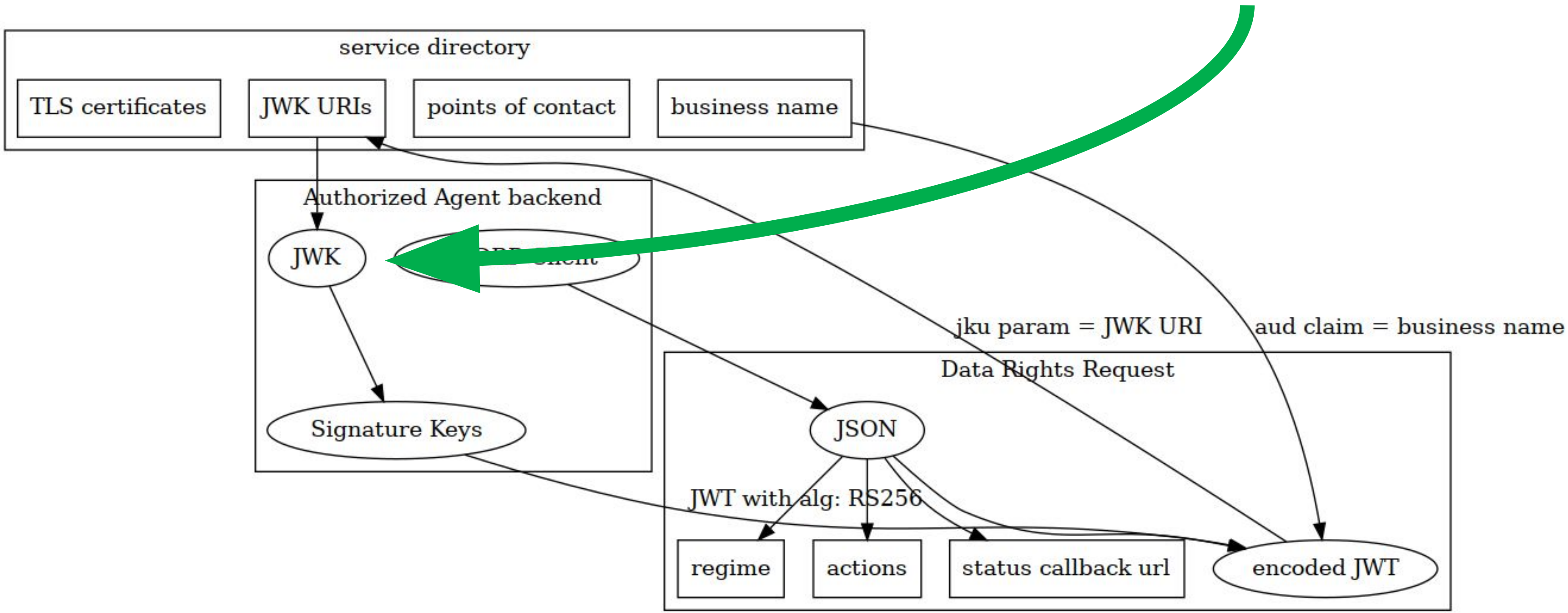
Trust & identity will be the agent’s responsibility

How can trust between Business and Agent be established?

- Businesses need a method to discover trust roots of agents
  - We need: Public keys for JWT signatures, API authentication elements
  - Multiplicative business communications won’t scale if DRP succeeds
- Could a JSON service directory managed by the DRP consortium be the simplest method to solve this?
  - Change process and auditing need to be well-vetted
  - Start with GitHub repo and tight review/merge ACLs
- What other options could we consider?
  - Could JSON directory grow in to a small cloud services application
  - DNS SRV record model?
  - X.500 directory?

Trusting Identity Attributes

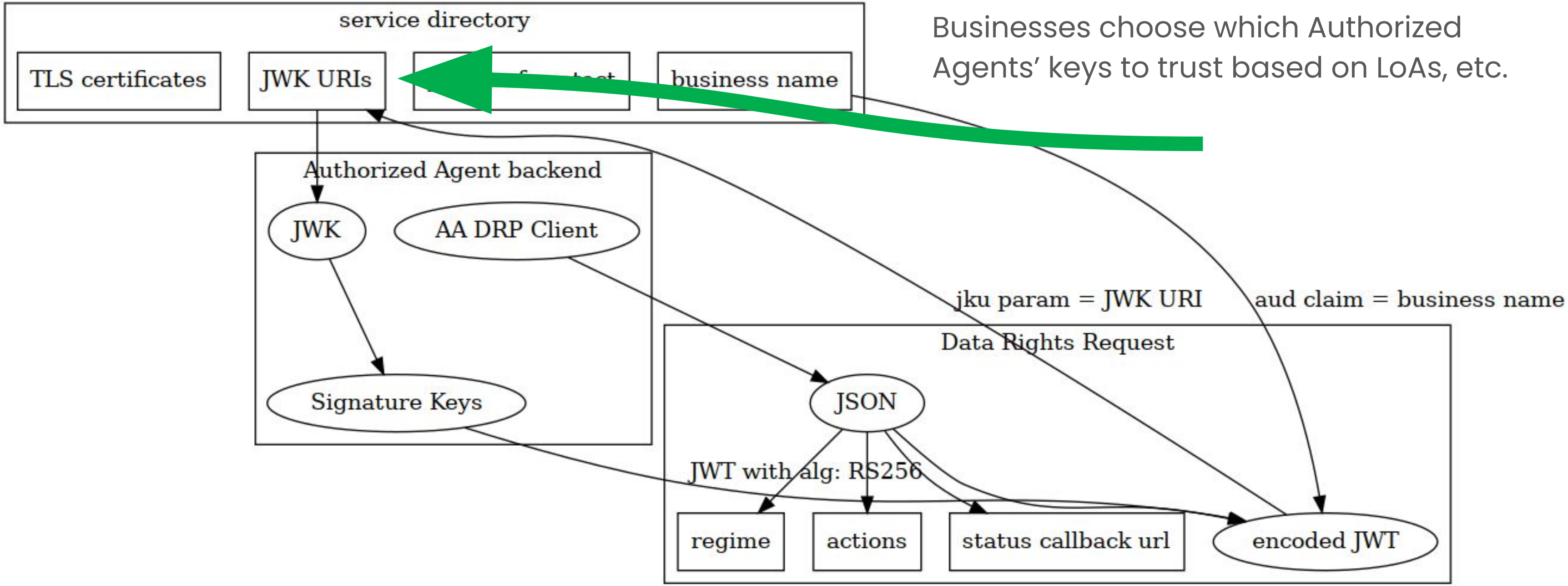
Authorized Agents generate and deploy cryptographic signing key



Trusting Identity Attributes

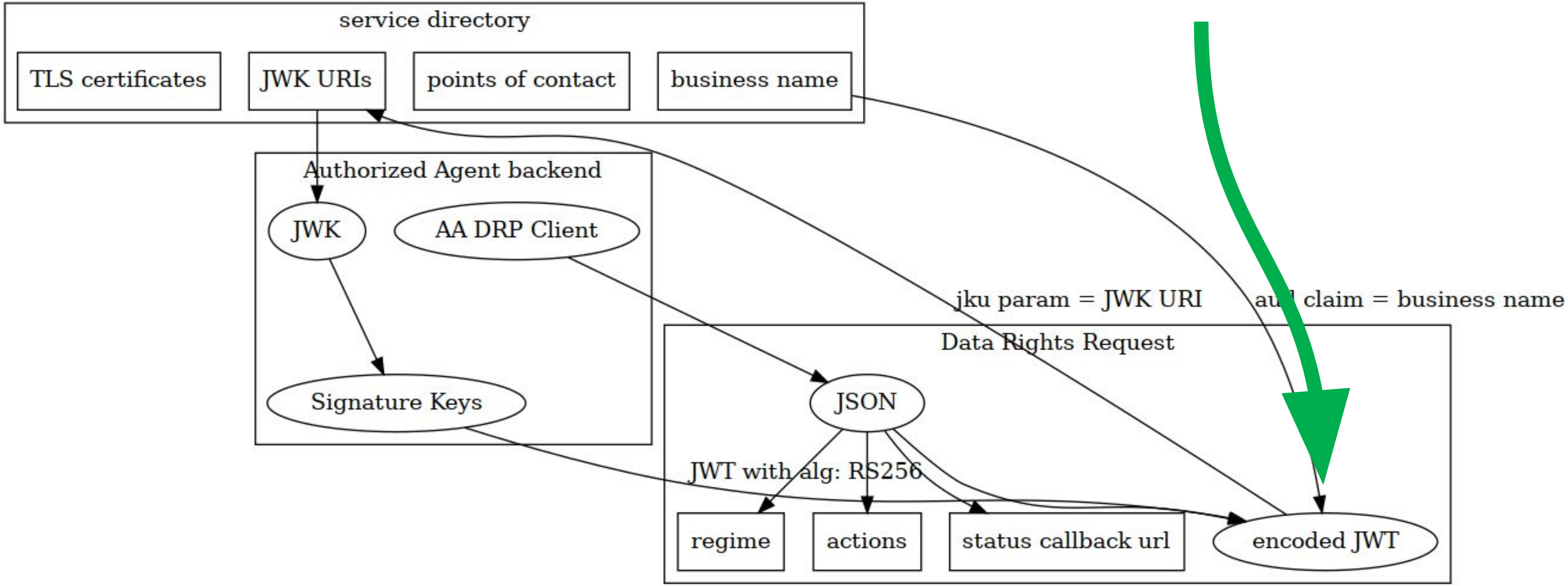
DRP Consortium collects, collates, and presents these signing keys to Businesses and privacy infrastructure providers

Businesses choose which Authorized Agents' keys to trust based on LoAs, etc.



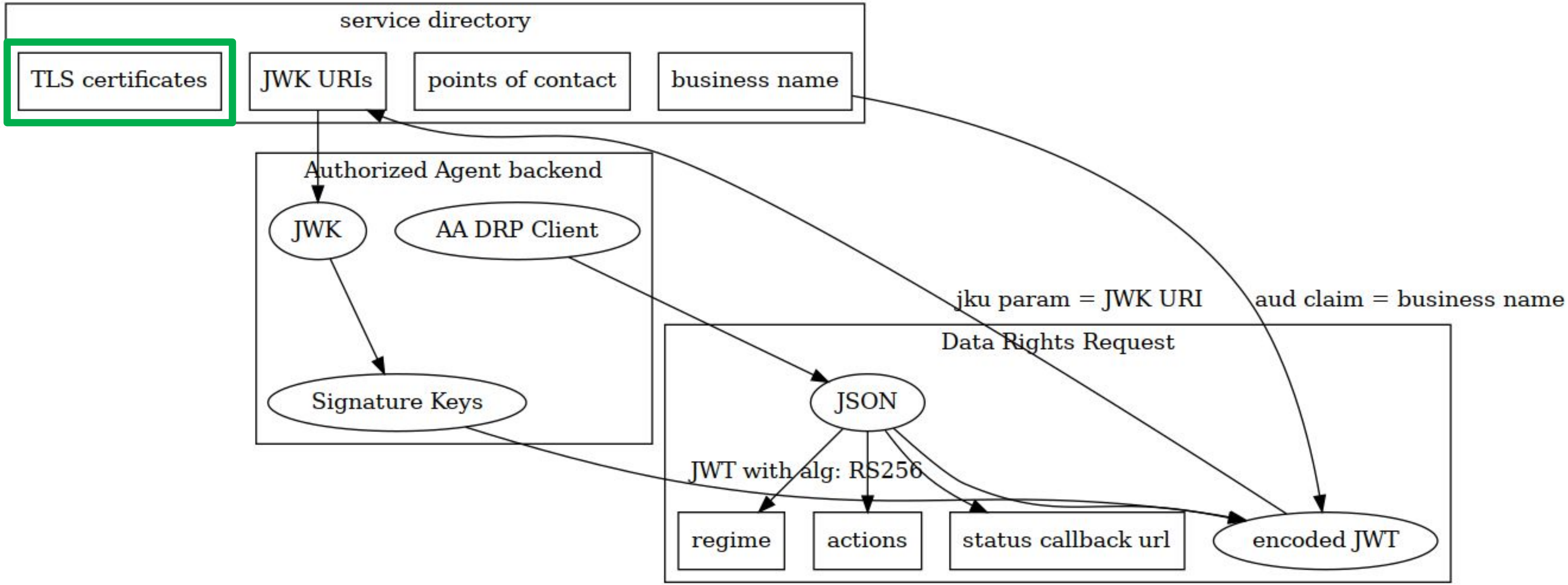
Trusting Identity Attributes

Data Rights Requests have cryptographically verifiable origin within Authorized Agent infrastructure



Mutual TLS *seems* like the frontrunner for API authentication…

Securing the Transport Layer



Mutual TLS

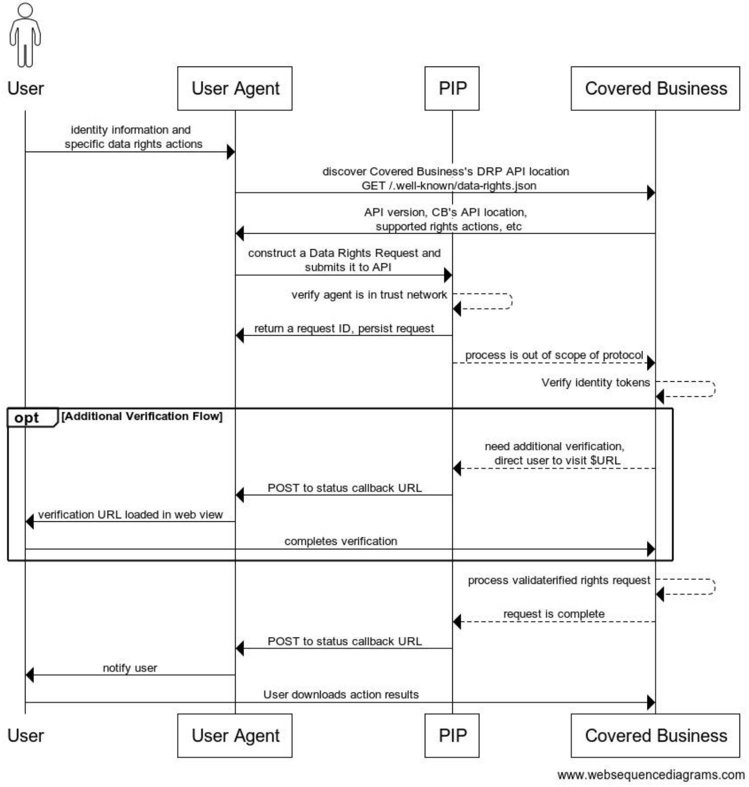
- Open questions between API Security and Identity Attestation
  - Provisos around mTLS implemented directly in application service versus sidecar (are we authenticating the server or the application)
  - Will businesses validate the client certificates?
  - Web PKI or managed registry?
  - Must JWTs be signed, too? (Do we need JWTs?)

Why not OAuth2?

- Seems like a no-brainer on the surface
  - Unreasonable lift for small companies to implement their own APIs
  - DRP could provide security token services to business but this is a significant piece of infrastructure to keep running & attack surface
  - User-initiated flows should not be required for each business

Open questions

- Who are the threat actors?
- What is the threat model?
- What are you worried about?



User

User Agent

PIP

Covered Business

identity information and specific data rights actions

discover Covered Business's DRP API location GET /.well-known/data-rights.json

API version, CB's API location, supported rights actions, etc

construct a Data Rights Request and submits it to API

verify agent is in trust network

return a request ID, persist request

process is out of scope of protocol

Verify identity tokens

opt [Additional Verification Flow]

need additional verification, direct user to visit $URL

POST to status callback URL

verification URL loaded in web view

completes verification

process validaterified rights request

request is complete

POST to status callback URL

notify user

User downloads action results

User

User Agent

PIP

Covered Business

www.websequencediagrams.com

Interested in learning more? Get in touch!

Here's how you join us:

- Hack against the protocol
- Offer feedback on the protocol
- Come find us after this talk!
    - ○ **Accord Boardroom 17:00 - 20:00**

datarightsprotocol.org

Dazza Greenwood
dazza@civics.com

Ryan Rix
drp@rix.si

Ginny Fahs
ginny.fahs@consumer.org