Initial Email

Hello eKYC WG,

I'm part of a consortium of privacy infrastructure and technology businesses working to create an open standard for Data Subject Rights (DSR) Requests for businesses under the jurisdiction of the CCPA. You can read a little bit more about the protocol here: http://datarightsprotocol.org

"This specification defines a web protocol encoding a set of standardized request/response data flows such that End-Users can exercise Personal Data Rights provided under regulations like the California Consumer Privacy Act, General Data Protection Regulation, and other regulatory or voluntary bases, and receive affirmative responses in standardized formats.

We aim to make the data rights protocol integrable with an ecosystem of data rights middlewares, agent services, automation tool kits, and privacy-respecting businesses which empower and build trust with consumers while driving the cost of compliance towards zero."

We believe that the eKYC extension to OIDC would be a good fit for our use case. I will lay out the scenario below

These are the relevant entities:

- a **data subject**: A natural person about whom a controller holds personal data and who can be identified, directly or indirectly, by reference to that personal data
- an **authorized agent**: A third party designated by a Consumer to perform Data Subject Requests on their behalf. This would be like a user agent/app.
- a **Privacy Infrastructure Provider (PIP)**: a technology solution that can orchestrate a DSR request for a business.
- **a covered business**: A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data and is subject to the CCPA.

A data subject will initiate one or more data subject requests through an authorized agent. The authorized agent will create these requests with one or more covered businesses. The covered business will have certain requirements in place for establishing the identity of the data subject. Once the requirements are met, the businesses will process the rights requests (for erasure, access, etc) based on their internal processes, or the PIP will do so on behalf of the covered business. Upon completion of the internal processes, the results of the rights request will be returned to the authorized agent for delivery to the data subject.

We're trying to answer the following questions:

1. Identity claims could be supplied by the authorized agent or the PIP/covered business. What is the proper trust model and how can we establish confidence in the claims?

2. The PIP/covered business may need to get identity claims that the authorized agent does not yet have (for instance, if the covered business is an ecommerce company it may want to know the date of the last order placed by the data subject). What is the right model for us to establish such claims?
3. Presumably, for the API authorization that would go along with the identity claims, we would be able to use the standard OIDC flow with the PIP/covered business acting as the authorization server and the authorized agent acting as a user agent, correct?
4. Do you have any concerns or other questions as we figure out how to meet our DSR use cases with OIDC?

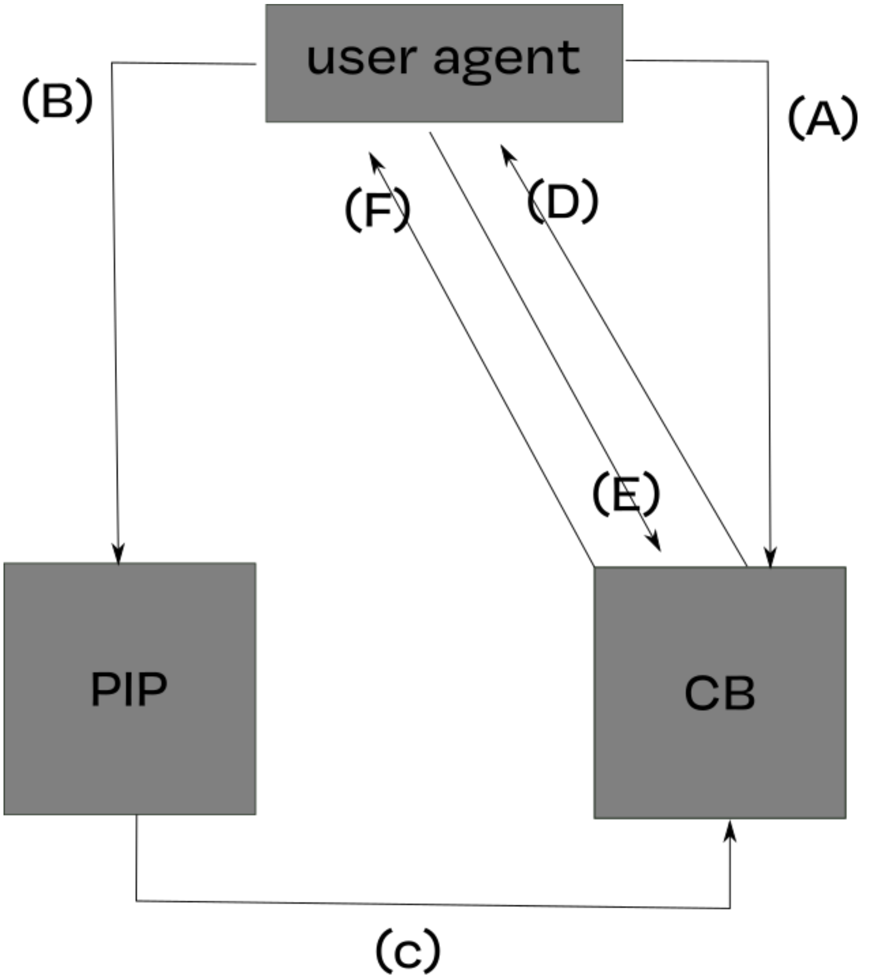
We've put together a few explanatory diagrams in this document for further explanation.

We're looking forward to your input! I will be unavailable via email for the next week, but will respond to comments upon my return.

Cheers,
John

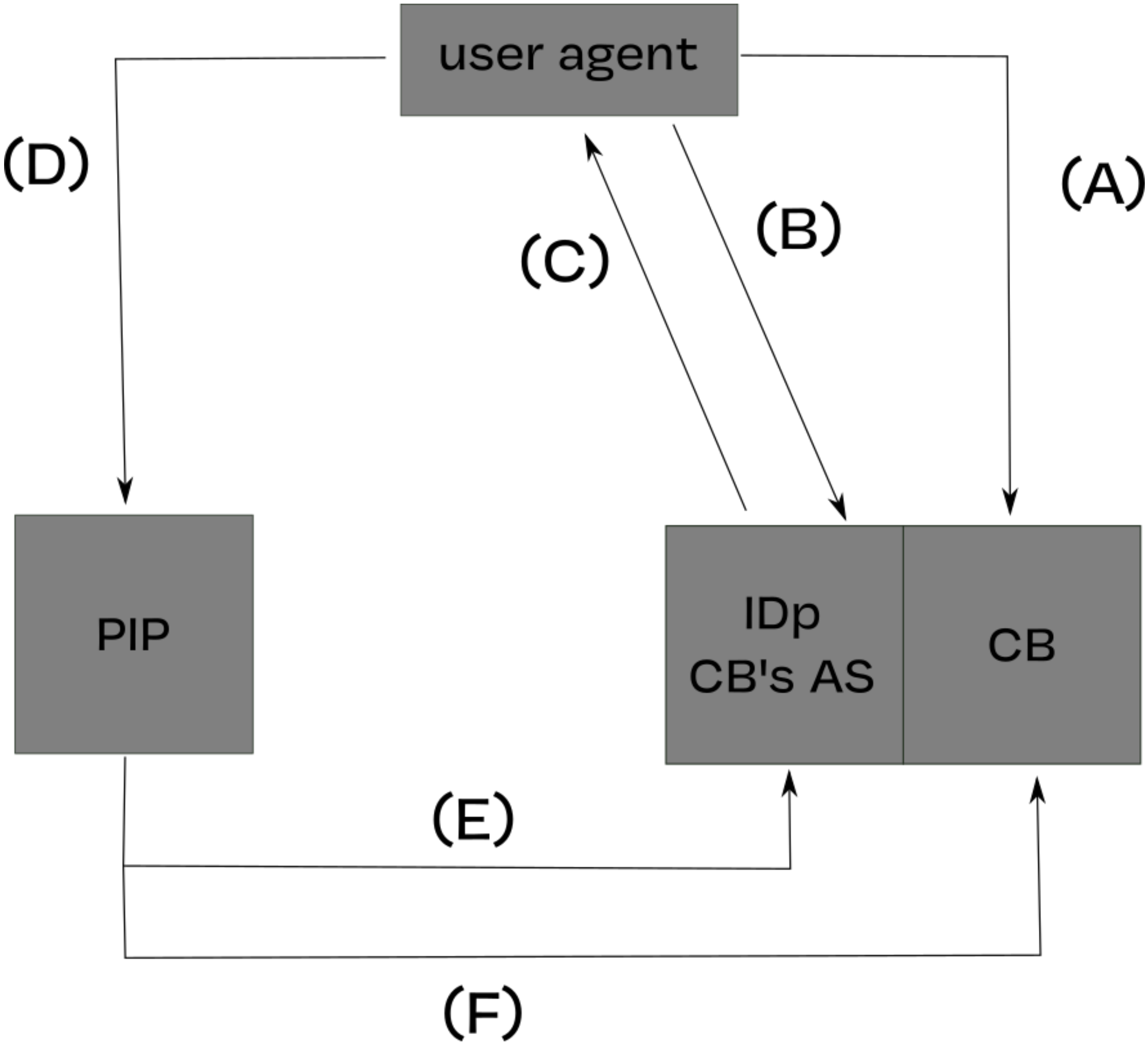
Appendix A: design flow from unsigned-JWTs to eKYC

Un-attested flow relies on “out of band” verification



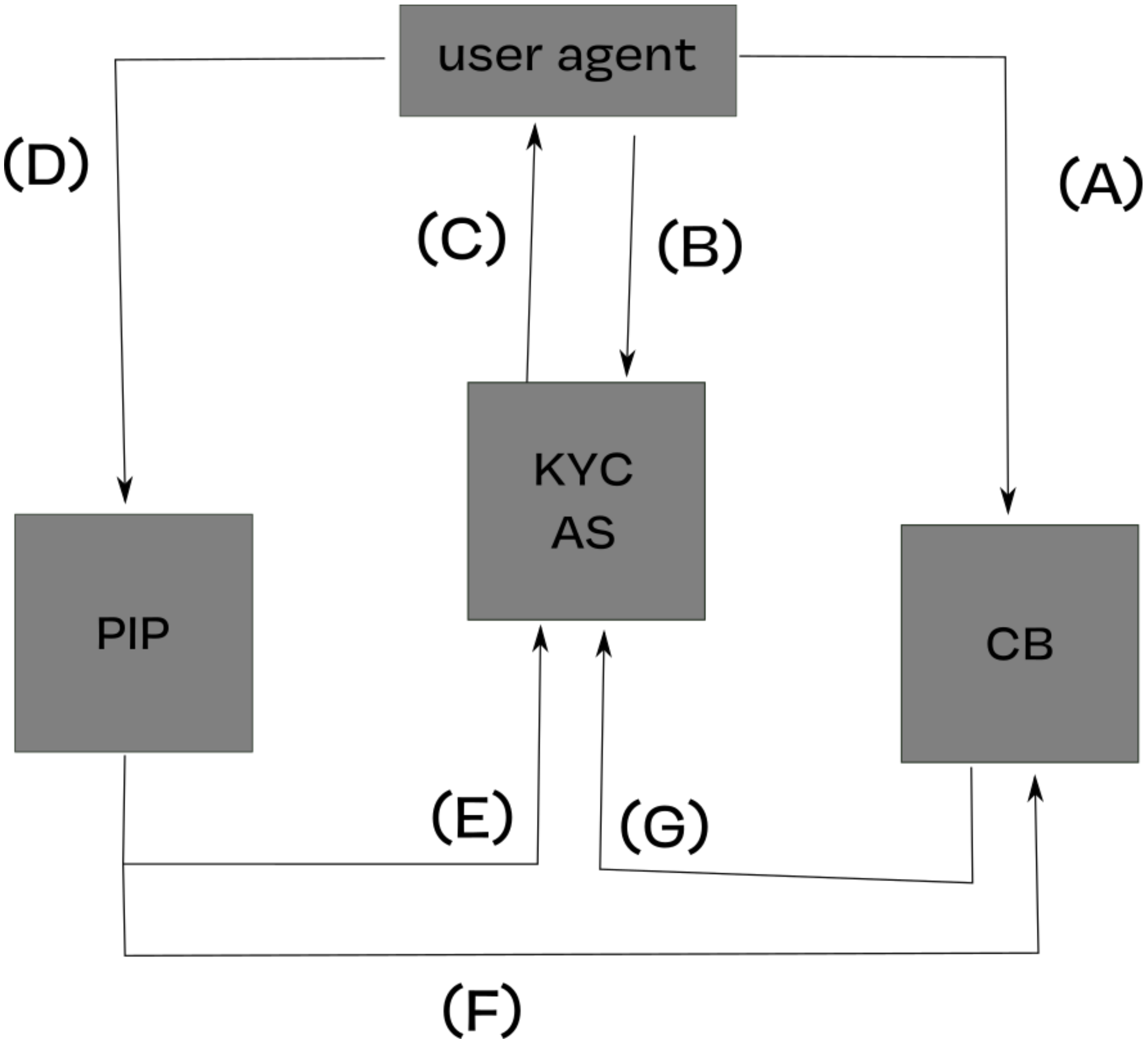
A. GET /.well-known/data-rights.json signals no ID flow; assuming interactive verification
B. Data rights request sent from UA to PIP with un-attested claims in JWT
C. PIP sends unverified claims for matching to account-holder
D. Data rights request enters need_user_verification status
E. User loads verification URL and completes requirements inside UA
F. CB redirects back to UA app on success, ID process completed

OIDC using business’s or their IDp’s AS



A. GET /.well-known/openid-configuration and /.well-known/data-rights.json to look for an AS to use
B. AS found, auth against it in the web
C. AS returns a signed JWT which CB can match against.
D. User Agent constructs a JWT with the AS’s JWT embedded in it, maybe unattested claims too?
E. PIP verifies the JWT is valid against the AS’s JWKs (implicit: ask same well-knowns to find it, or CB provides list of “trusted” AS directly to PIP)
F. PIP forwards validated, subject-matched request to CB

eKYC flow with trusted intermediary AS



A. User Agent queries data-rights.json for eKYC support
B. UA sends a JWT with unattested claims, eKYC AS provides attestation framework for user
C. AS returns a JWT with those claims attested, signed.
D. UA sends data rights request with attested JWT
E. PIP validates signature
F. PIP forwards request to CB
G. CB validates signatures, approves request

Note: PIP is Privacy Infrastructure Provider, aka DSR Provider CB is "Covered Business".

Note: Future implementations may support some use cases where Authorized Agent provides auth server (IdP) service for consumers (aka users/subjects).