Company name	Security model 1 feedback	Changes in response to feedback 1	Security model 2 feedback	Changes in response to feedback 2
Mine	cut out complexity, lean on standard encryption, standard auth stuff like oauth2; enforce usage of updated versions, minimum ciphers etc. Push some of the security and workflow "best practices" to guidance and not mandatory protocol conformance.	simplified data model, proposing libsodium as both a standard library with also very good cipher &c choices and enforcement		
Transcend	questions regarding API secret/JWT signing, etc; they already have some features in their DSAR tooling to process signed JWTs for consumer identity which could be leveraged if businesses had a method to signal trust of AAs' signing key	built clarity on what work auth & signing mechanisms are doing and how we propose to implement them; improving our communication of them in the docs		
OneTrust	mTLS will be a pain to implement on both sides of the relationship -- Example: onetrust uses Cloudflare for TLS termination, client certificates with arbitrary private CA is enterprise-contract feature; was positive on service discovery mechanism	dropped mTLS		
Surfshark/Incogni	sort of over-engineered, can we make this much more simple HTTPS+authentication header? shared secret to start, move to something like libsodium later	Kevin's revision to the security model is much more concise, simple, and focused than the initial proposal; also proposes a series of small steps to gradually implement rather than doing everything at once		