Keith’s Comment:

General Comment

When I introduced ONE Record shared data concept to other, the first question they ask is security control and how we can trust that the data is secured

From last year PoC, I see i-share provided trust worth and advanced API security control between AC-SP.

If we simplify the handshaking by adding a proxy GSP, will GSP become a vulnerable point or a less secure solution? Pure technical question, as more global/enterprise companies concern about security on digital solution (e.g. cloud, shared data…)

If we try to maintain the same i-share security concept in GSP, do we need to setup the same handshaking between GSP-SC, GSP-SP and make it more complex? e.g. more token/cert exchange.

Comments on raised challenges

Challenge 1. How SC know the resource of SP identity (public cert) & URI of API?

Long term idea: Stored in central inventory or pool of authorized providers and query through central directory query (like DNS). But I guess it’s not available in the market, will some industrial organization (e.g. IATA) setup a member lookup API to provide such resource for each registered member? Or any public service providing similar service?

Short term idea: Do it in traditional way, similar to e-AWB agreement, forwarder and airline signed up e-AWB agreement, both parties will also exchange IT setup contact and method (or selected CCS vendor). Can GSP be the IT provider role to store the setup in this case?

Challenge 2. How we hide the AR complexity from SC, SP. & Challenge 3. Policy checking in (G)SP instead of AR

Areas of checking in traditional solution:

- Checking in current practice (in CCS network)
    1. Check whether Consumer (SC)’s identity (PIMA) is allowed to perform transaction with data provider (SP). e.g. Registered forwarder, airline. Invalid identity will be rejected.
       I guess policy define in AR can cover this part.
    2. Check the allowed msg. type (e.g. FWB, FHL, FSR) from SC, if not allowed, reject the transaction.
       Seems (G)SP can keep the data set (AWB, HAWB, Status) to ONE Record data fields grouping so as to simplified the API provided to SC and AR policy.
    3. Check Consumer’s access right on the required data (e.g. Airline system check whether the AWB belongs to this forwarder). If request is not allowed, reject the request. Currently this checking is mainly perform in stakeholder’s in-house system, I think this kind of business checking can check by (G)SP rather than AR.

Additional check not cover by current practice:

- Delegation of data access (e.g. Forwarder delegate access to trucker, Airline delegate the access to GHA, shipper/forwarder/airline delegate the access to Origin/Destination Customs…)

  Need further discussion how to define AR policy on this.