Key relationships

Data

Engine

Coelition

Service

Provider

OASIS

COEL TC

Operator

Likely Member

Member

Licence

Licence

Commercial

Contract

Commercial

Contract

Contract Consent

Possible Member

Consumer

Device

Data flows

Data

Engine

Service

Provider

Operator

Report Data & all services

Consumer

Device

DIPI, Segment Data

Behavioural Data

Segment Data & report requests

Segment Data & report requests

Report Data & all services

Report Data & all services

The Coelition IDA issues a unique pseudonymous key to the Operator when the Consumer joins the ecosystem. Once this has been registered with the Data Engine it becomes the ConsumerID and replaces the DIPI in all transactions other than those between the Operator and Consumer.

In normal operation the Behavioural Data will stay with the Data Engine unless the Service Provider needs to provide non-standard services or the Consumer makes a specific data request.

Security considerations

Data

Engine

Coelition

Service

Provider

Operator

2.

1.

3.

4.

5.

General technical principles:

* Use SSL for all internet communications within the ecosystem. This creates an encrypted channel for the data (Behavioural Atoms, Report data and Pseudonymous Keys – no DIPI) and prevents a third party from reading it in transit. It means that servers like the IDA, Data Engine and any Service Provider/ or Operator systems must have SSL certificates (between £100 and £300 pa cost or see https://letsencrypt.org/).
* Use single factor authentication (user-id and password) for all Data Engine and IDA calls with the exception of: [a] submitting atoms which can be done anonymously [b] an Operator registering consumers with the DE (see below for why)
* Use IDA generated pseudonymous keys as the user-ids for actors in the ecosystem. These are devoid of DIPI and unique across the ecosystem.
* Use different user-ids AND different passwords for each embodiment (e.g. for Operator with IDA, Operator with DE, Service Provider with different DEs etc)

Systems interaction threat analysis:

1. Operator / IDA: Disclosure of M2M credentials would allow an attacker to generate Pseudonymous Keys on behalf of an operator. There is no possibility of disclosure of DIPI or behavioural data. Risk is low.
2. Service Provider / IDA. Disclosure of SP interactive login would allow attacker allocate new OperatorIDs or disable existing OperatorIDs. The IDA will not keep any DIPI for operators and their IDA passwords are stored encrypted so there is no risk of these being disclosed. If an attacker gains access then the Service Provider will need to change their password and re-register its operators.
3. Operator / Data Engine: Disclosure of operator credentials would allow an attacker only to register Consumers as the Operator has no other role with the Data Engine. There is therefore no need for an operator password when registering a consumer with the Data Engine. Registering is similar to submitting a Behavioural Atom.
4. Service Provider / Data Engine: This is the area of highest threat. Disclosure of credentials that gave access to the Data Engine Management Interface (MI) and Query Interface (QI) would open up two possible attacks:
	1. An attacker can query the tree of operators and consumers (via MI) and then retrieve all Behavioural Atoms for all consumers for the Service Provider (via QI).
	2. An attacker can use the MI to issue forget requests for consumers. This would result in either deleting all the atoms, or disconnecting the atoms from their original ConsumerID. It would render the atoms useless to the Service Provider because by definition forgetting is not reversible.

To reduce the likelihood of [a], we should mandate that separate credentials be used to access the MI and QI, reducing the likelihood of getting both.

To reduce the likelihood of [b], the data engine must use a secondary method to assert the identity of the Service Provider. Forgetting is a rare event and insisting that there be a human in the loop will make it more secure. We can mandate that the Data Engine send an authorisation email to the Service Provider asking it to confirm the forget request. (Unlikely attacker has access to this mailbox). Or the Data Engine can mandate a second factor of authentication for forget requests such as a handheld RSA key

1. Operator / Service Provider: Where the operator is a separate entity), it will request reports on consumers from the Service Provider, but these reports are pseudonymised so contain no more information than the query returned from the DE. The operator adds in the DIPI itself. Low risk.