Roles, Principles, and Ecosystem Version 1.0

Committee Specification Draft 02 / Public Review Draft 01

13 October 2016

Specification URIs

This version:

http://docs.oasis-open.org/coel/RPE/v1.0/csprd01/RPE-v1.0-csprd01.docx (Authoritative)
http://docs.oasis-open.org/coel/RPE/v1.0/csprd01/RPE-v1.0-csprd01.html
http://docs.oasis-open.org/coel/RPE/v1.0/csprd01/RPE-v1.0-csprd01.pdf

Previous version:

http://docs.oasis-open.org/coel/RPE/v1.0/csd01/RPE-v1.0-csd01.docx (Authoritative)
http://docs.oasis-open.org/coel/RPE/v1.0/csd01/RPE-v1.0-csd01.html
http://docs.oasis-open.org/coel/RPE/v1.0/csd01/RPE-v1.0-csd01.pdf

Latest version:

http://docs.oasis-open.org/coel/RPE/v1.0/RPE-v1.0.docx (Authoritative)
http://docs.oasis-open.org/coel/RPE/v1.0/RPE-v1.0.html
http://docs.oasis-open.org/coel/RPE/v1.0/RPE-v1.0.pdf

Technical Committee:

OASIS Classification of Everyday Living (COEL) TC

Chairs:

David Snelling (David.Snelling@UK.Fujitsu.com), Fujitsu Limited
Joss Langford (joss@activinsights.co.uk), Activinsights Ltd

Editor:

Matthew Reed (matt@coelition.org), Coelition

Related work:

This specification is related to:

- *Classification of Everyday Living Version 1.0.* Edited by Joss Langford. Latest version: http://docs.oasis-open.org/coel/COEL/v1.0/COEL-v1.0.html.
- *Behavioural Atom Protocol Version 1.0*. Edited by Joss Langford. Latest version: http://docs.oasis-open.org/coel/BAP/v1.0/BAP-v1.0.html.
- *Minimal Management Interface Version 1.0*. Edited by David Snelling. Latest version: http://docs.oasis-open.org/coel/MMI/v1.0/MMI-v1.0.html.
- *Identity Authority Interface Version 1.0*. Edited by Paul Bruton. Latest version: http://docs.oasis-open.org/coel/IDA/v1.0/IDA-v1.0.html.
- *Public Query Interface Version 1.0.* Edited by David Snelling. Latest version: http://docs.oasis-open.org/coel/PQI/v1.0/PQI-v1.0.html.

Abstract:

This document defines and describes roles of the various actors and principles of a COEL ecosystem, within the framework of the COEL Model.

Status:

This document was last revised or approved by the OASIS Classification of Everyday Living (COEL) TC on the above date. The level of approval is also listed above. Check the "Latest version" location noted above for possible later revisions of this document. Any other numbered Versions and other technical work produced by the Technical Committee (TC) are listed at https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=coel#technical.

TC members should send comments on this specification to the TC's email list. Others should send comments to the TC's public comment list, after subscribing to it by following the instructions at the "Send A Comment button on the TC's web page at https://www.oasis-open.org/committees/coel/.

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the TC's web page (https://www.oasis-open.org/committees/coel/ipr.php).

Citation format:

When referencing this specification the following citation format should be used:

[COEL-RPE-v1.0]

Roles, Principles, and Ecosystem Version 1.0. Edited by Matthew Reed. 13 October 2016. OASIS Committee Specification Draft 02 / Public Review Draft 01. http://docs.oasis-open.org/coel/RPE/v1.0/csprd01/RPE-v1.0-csprd01.html. Latest version: http://docs.oasis-open.org/coel/RPE/v1.0/RPE-v1.0.html.

Notices

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The name "OASIS" is a trademark of OASIS, the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see https://www.oasis-open.org/policies-guidelines/trademark for above guidance.

Table of Contents

1 Introduction

This document describes in detail the comprehensive set of ACTORS that take part in a COEL compliant ecosystem. For each of the ACTORS a description of their possible activities is given, all referenced to a set of seven normative principles. A number of specific, but jurisdiction agnostic, definitions are given to support the role descriptions and principles.

1.1 Terminology

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in **[RFC2119]**.

1.2 Normative References

[RFC2119] Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels”, BCP 14, RFC 2119, March 1997. http://www.ietf.org/rfc/rfc2119.txt.

[RFC5246] Dierks, T., Rescorla, E., “The Transport Layer Security (TLS) Protocol Version 1.2” RFC 5246, August 2008 http://www.ietf.org/rfc/rfc5246.txt .

[COEL_COEL-1.0] *Classification of Everyday Living Version 1.0.* Latest version: http://docs.oasis-open.org/coel/COEL/v1.0/COEL-v1.0.docx

1.3 Non-Normative References

[Data to Life] Reed, M. & Langford, J. (2013). Data to Life. Coelition, London. ISBN 978-0957609402

2 Roles

2.1 Summary of Roles

The **Identity Authority** (IDA) oversees the effective, open running of the eco-system and administers the operation of the IDA service. The IDA service issues and checks unique Pseudonymous Keys that provide security and ensure the interoperability and universality of the ecosystem.

Data Engines receive, store and process Behavioural Atoms. Data Engines provide business-to-business services to Service Providers and other organisations in the form of queries that create Report Data.

Service Providers are the primary link between a Consumer and a Data Engine. They are able to query the atoms held by a Data Engine to develop personalised services for Consumers based on their everyday behaviours. Service Providers will often be consumer facing brands.

Operators administer contact with the Consumer and hold the directly-identifying personal information (DIPI) needed to engage with the Consumer. An Operator might be an independent app, exist within a Service Provider or be an independent organisation. Operators only receive information from their Consumers and their Service Provider.

The **Consumer** is the generic reference to any individual registered with the eco-system. They might be patients in a healthcare setting, subjects in a trial as well as consumers of a commercial digital service. A Consumer's primary relationship might be with a Service Provider via a near-invisible Operator or with clearly recognisable Operator that is supported by a Service Provider in the background.

Technical Service Developers create tools, infrastructure and software for managing data or services within the ecosystem, who do not handle Coelition services or personal data. These include: app developers for Service Providers, development agencies that create Service Provider or Data Engine or Coelition infrastructure. It could be that a Data Engine acts as a Technical Service Developer to create software infrastructure that is then run by one of their Service Providers. Technical Service Developers may be members of Coelition if they wish to use the trademarks to display that they conversant with the Coelition ecosystem and the development of software within it.

Hardware Developers are developers of hardware (such as Internet of Things devices) which are compliant with COEL protocols for use by Service Providers and Operators.

These roles will be performed by a number of actors that create the ecosystem. Actors may have multiple roles but certain combinations are not permissible as described in the Technical Requirements and the table below. The table shows all the possible role pairs; an actor may have more than two roles but every paring must be permitted.

		Role 2						
		IDA	Data Engine	Service Provider	Operator	Consumer	Technical Service Developer	Hardware Developer
Role 1	IDA		✘	✘	✘	✘	✘	✘
	Data Engine	✘		✘	✘	✘	✓	✓
	Service Provider	✘	✘		✓	✘	✓	✓
	Operator	✘	✘	✓		✘	✓	✓
	Consumer	✘	✘	✘	✘		✓	✓
	Technical Service Developer	✘	✓	✓	✓	✓		✓
	Hardware Developer	✘	✓	✓	✓	✓	✓	

2.2 Identity Authority

Technical requirement		**Guiding principles & notes**
SHALL	Maintain an always-on IDA service that will generate or validate unique Pseudonymous Keys for Data Engine, Service Provider & Operator	P4
	Be a non-profit legal entity	P5
	Provide its services on a fair, reasonable and non-discriminatory basis	P5
	Provide Consumers with information about the operation of the eco-system free of charge	P5 & P7
SHALL NOT	Act as a Data Engine or Service Provider (other than for the purposes of providing a limited ‘sandbox’ test environment)	P4 & P5
	Store Behavioural Atoms	P4 & P5

	Hold any Consumer's directly identifying personal information (DIPI)	P5
MAY	Request Data Engine support to deliver population-level insights for public information and the purposes of marketing the specification	P6
	Make a query on Data Engines to ensure a specific ConsumerID has been forgotten	P7 This allows the Identity Authority to audit the forgetting process.
	Provide Consumers with information about their status within the eco-system, i.e. 'known' or 'forgotten' and only by ConsumerID and not DIPI.	P5 & P7
	Provide audit services to Data Engine, Service Provider, Operator and regulators	P6

2.3 Data Engine

Technical requirement		**Guiding principles & notes**
SHALL	Provide secure storage of Behavioural Atoms for a period to be agreed with the Service Provider in line with the Consumer consent	P2 & P3
	Provide minimal interface services for Service Providers to process joiners, movers, and leavers (e.g. Operator & Consumer trees, registration, ID re-allocation, forgetting)	P4
	Provide minimal interface services for querying Behavioural Atoms by registered Service Providers	P1
	Maintain an always-on, single entry point for uploading Behavioural Atoms to the Data Engine	P4
	Receive Behavioural Atoms from Consumers or Devices registered with their Operators that conform to the specification free of charge	Receiving data is a minimal requirement for a Data Engine; commercial services apply to the use and processing of data.
	Provide information to the Service Provider about the location and security of the infrastructure used in the delivery of services	P7
SHALL NOT	Link Behavioural Atom data to directly-identifying personal information (DIPI) from external sources	P1
	Link Behavioural Atom data directly to external data storage if such link might directly identify Consumers	P1

	Hold any Consumer's directly identifying personal information (DIPI)	P1
	Act as a Service Provider or Operator itself	P1 & P4
	Request more than the Segment Data as defined in the specification (gender, year of birth, time zone & latitude to 0 decimal points) on registration of a Consumer	P1
	Knowingly receive DIPI	P1
	Levy unreasonably punitive charges for the complete download of stored Behavioural Atoms	Supports EU data protection and an open, competitive eco-system.
	Utilise IDA unique Pseudonymous Keys outside of the ecosystem	P1
MAY	Add non-personal data to the atom store to deliver enhanced services (e.g. local weather data)	P1 While Behavioural Atoms cannot be linked out, additional information can be linked in.
	Use suitable aggregation techniques rendering the data non-personal to provide indirect services to parties other than contracted Service Providers	P1 & P6
	Host multiple Service Providers	

2.4 Service Provider

Technical requirement		**Guiding principles & notes**
SHALL	Ensure that their Operators have the minimum standard consent from Consumers	P3
	Secure additional consent from Consumers when sending personal information outside the eco-system	P3 & P6
	When sending Behavioural Atom information outside the eco-system, remove the ConsumerID and replace with DIPI	P6 This ensures that information that has left the eco-system can be clearly identified.
	Ensure that their Operators follow the specification	P6
	For any one purpose and at any one time, have only one Data Engine	Avoids potential data loss for the consumer and ensures the complete audit map of the eco-system.
	On a request from a Consumer, supply (or require associated Operator to do	P2 Basic tenet of EU data protection.

	so) all DIPI, Segment Data, Behavioural Atoms and any stored Report Data	
	On a request from a Consumer to be forgotten, remove or render DIPI to be non-personal	Basic tenet of EU data protection.
	On a request from a Consumer to be forgotten, instruct their Data Engine to remove or render data to be non-personal	P2 & P3
	On a request from an Operator or Consumer, provide the identity of the Data Engine	P7
	Notify Consumers (via Operators) of any mergers and acquisitions or other changes that would result in a change of control over the Consumers' data	P7
	Check the credentials of an Operator every time a request is made to release data for a ConsumerID	Security.
	Ensure that all Operators within a specific embodiment are working under equivalent terms (e.g. consent, purpose, retention periods etc.).	P7
	Use different passwords to interact with different actors in the ecosystem (within the same service embodiment).	Security.
	Use a different ServiceProviderID for every instance of a service embodiment in which they are an actor	Security.
	Hold ConsumerID Pseudonymous Keys with the same security level as DIPI.	Security.
	Provide a secure interface to Operators such that communication is done in an appropriate manner with basic authentication as a minimum.	Security.
SHALL NOT	Receive Behavioural Atoms directly	P1
	Send DIPI to a Data Engine	P1
	Share DIPI with another Service Provider without additional consent from the Consumer	P3
MAY	Transfer its operations between Data Engines	Supports open, competitive eco-system.
	Host multiple Operators	

An **Associated Service Provider** is a Service Provider that gains access to data collected by another service provider to provide a service to a Consumer. To do so, the Consumer MUST give consent to the Associated Service Provider to access the data collected by the original Service Provider. An Associated Service Provider has no right to grant a third-party any access to the data held by the original Service Provider. All of the technical requirements on a Service Provider above will apply to an Associated Service Provider except for Consumer requests to access or modify data held by the Data Engine which MUST be passed to the original Service Provider that collected the data.

2.5 Operator

Technical requirement		**Guiding principles & notes**
SHALL	Provide a mechanism for the consumer to access their ConsumerID.	P7 This allows the Identity Authority to audit the 'forgetting' process.
	Ensure that the minimum standard consent is given by Consumers - freely, specific & informed	P3
	For any one purpose and at any one time, have only one Service Provider	Avoids potential data loss for the consumer and ensure the complete audit map of the eco-system.
	Clearly identify the Service Provider to the Consumer	P7
	Notify Consumers of any mergers and acquisitions or other changes that would result in a change of control over the Consumers' data	P7
	Hold ConsumerID Pseudonymous Keys with the same security level as DIPI	Security
	Use different passwords to interact with different actors in the ecosystem (within the same service embodiment).	Security.
	Use a different OperatorID for every instance of a service embodiment in which they are an actor	Security.
SHALL NOT	Store Behavioural Atoms other than for the purposes of transmission to the Data Engine.	P1
	Send DIPI to a Data Engine	P1
	Share DIPI with another Operator or Service Provider without additional consent from the Consumer	P3
	Utilise IDA unique Pseudonymous Keys outside of the ecosystem	P1
MAY	Host multiple Consumers	

2.6 Consumer

Technical requirement		Guiding principles & notes
MAY	Request to be ‘forgotten’ in the eco-system	Basic tenet of EU data protection.
	Request the Identity Authority to audit their status in the eco-system	P5 & P7
	Request the Service Provider to supply their DIPI, demographic information and all Behavioural Atoms	Basic tenet of EU data protection.

3 Normative principles of the Operation of COEL ecosystem

3.1 Data Separation Principle (P1)

The specification implements a separation of data types: Data Engines keep data on *what* Consumers do (Behavioural Atoms) and the Service Provider/Operator keeps data on *who* Consumers are (DIPI). No single organisation holds both sets of data together. This means that it would need a double accidental or malicious disclosure for connected information to be released.

3.2 Data Atomisation Principle (P2)

Data is deliberately broken down into small chunks of information by the Operator and coded with the Consumer's ConsumerID (which implies their atomised consent), thus each separate Behavioural Atom has a very low privacy risk. Neither the Operator/Service Provider sees these atoms as raw atoms and can only see composite data from Data Engine under the terms of the specification.

3.3 Atomised Consent Principle (P3)

Consumer gives informed consent to the Operator under guideline terms set by the specification. Consent allows the Operator to sign up the consumer with a ConsumerID. This ConsumerID is the indicator to Identity Authority and other eco-system actors that the consumer has given appropriate consent. Because each and every Behavioural Atom has the ConsumerID, each atom has that consumer's consent written into the structure of the data. Removing the ConsumerID from a Behavioural Atom is removing the consent of that individual so the data can no longer be used by either the Operator or Service Provider who signed them up. The time stamp uniquely associated with each Behavioural Atom allows full auditing of this principle.

3.4 Separation of Competence Principle (P4)

Data Engines are expert data handlers. They know how to run robust, secure and always on cloud based data services; they handle Behavioural Atoms NOT Consumers. Service Providers / Operators are experts at Consumer facing / relevant services and handling DIPI; they handle Consumers NOT Behavioural Atoms. The Identity Authority is expert at overseeing the ecosystem.

3.5 No Conflict of Interest Principle (P5)

Consumers need to see that there are no conflicts around their data. To ensure this, the Identity Authority acts on behalf of the Consumer in partnership with Operator/Service Provider, Data Engine and regulators.

3.6 Active Support Principle (P6)

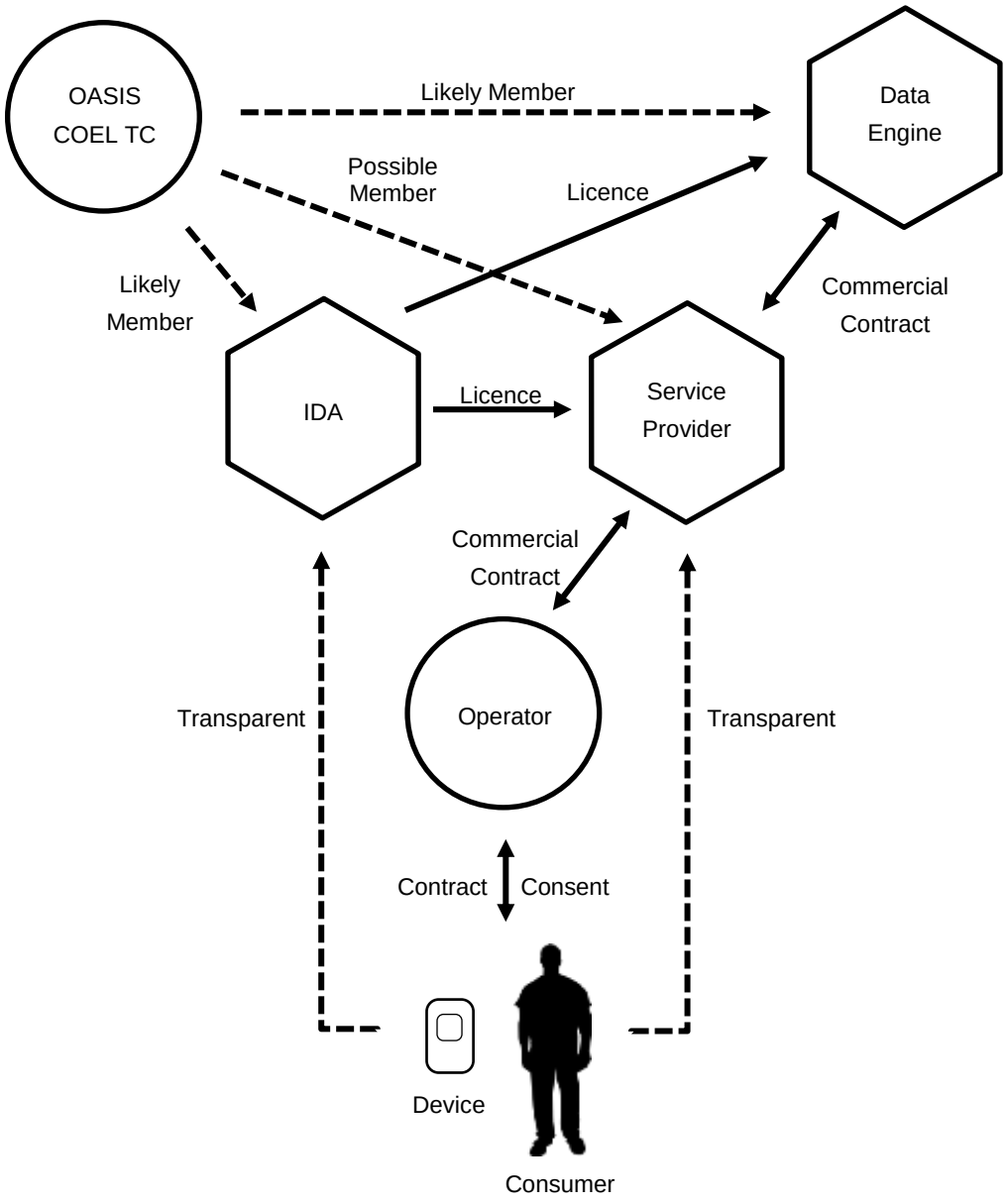
All actors will actively promote the principles of the specification, safeguard the structure of the eco-system and support good data practice for both consumers and enterprise.

3.7 Transparency Principle (P7)

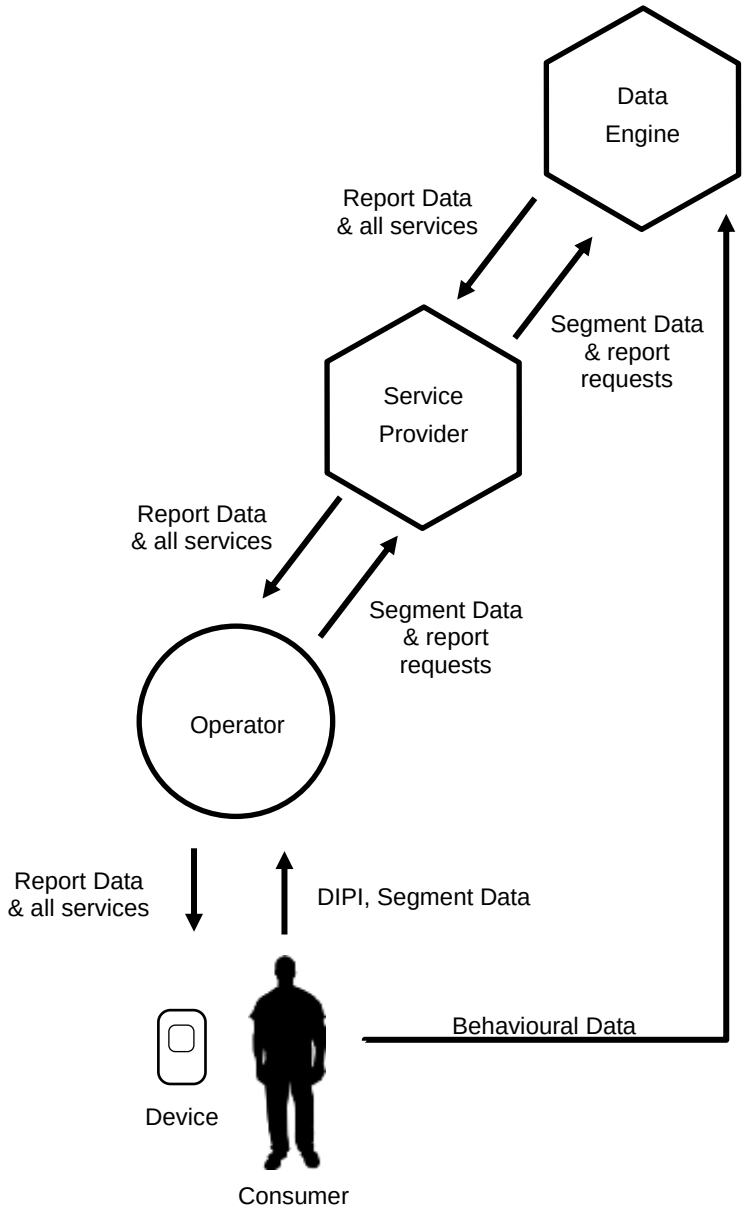
The roles and identities of all the actors in the eco-system who are working together on behalf of a Consumer will be clear and visible to that Consumer.

4 Ecosystem

4.1 General diagram of key relationships between actors



4.2 Data Flows



The 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.

The illustration shows the Segment Data delivered through the Service Provider, this is accurate when the data is recalled but the Operator sends this directly to the Data Engine when the Consumer is first registered.

4.3 Security Considerations

4.3.1 General technical principles:

4.3.1.1 Internet

SSL/TLS **[RFC5246]** SHALL be used 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/TLS certificates.

4.3.1.2 Authentication

Single factor authentication (userid and password) SHALL be used for all Data Engine and IDA calls with the exception of: [a] submitting atoms which can be done anonymously [b] an Operator registering consumers or assigning devices with the DE.

4.3.1.3 Pseudonymous Keys

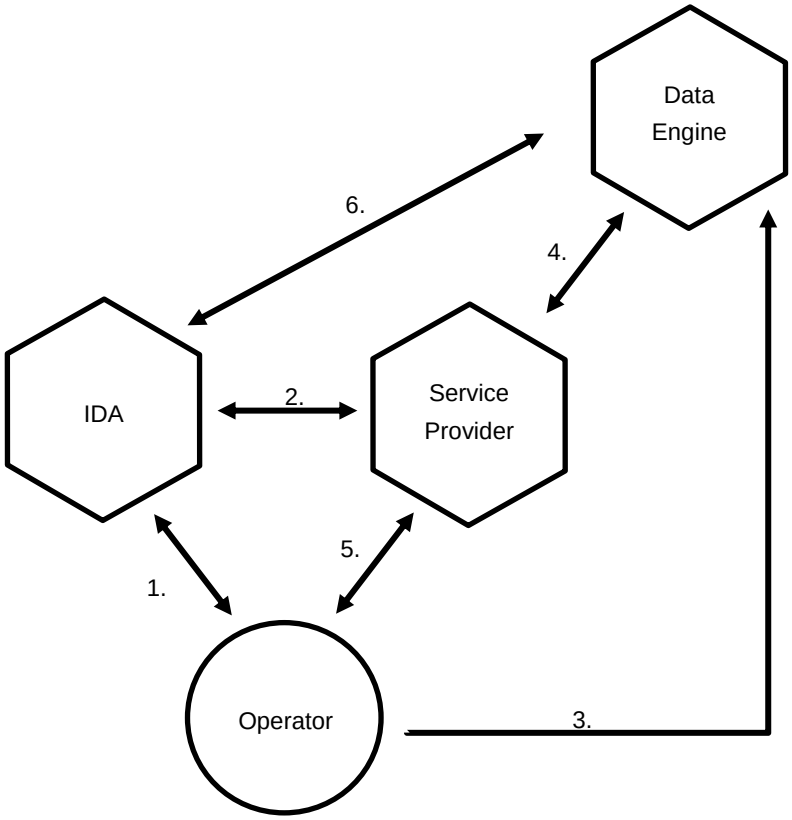
IDA generated Pseudonymous Keys SHALL be used as the userids for actors in the ecosystem. These are devoid of DIPI and unique across the ecosystem.

Pseudonymous Keys used as Consumer IDs need to be handled carefully since they could be mis-used to pollute the atom collection in a data engine, or to retrieve data about a consumer if a service providers credentials are divulged.

4.3.1.4 Userids and passwords

Different userids MAY be used and different passwords SHALL be used for each embodiment (e.g. for Operator with IDA, Operator with Data Engine, Service Provider with different Data Engines). These SHALL be stored in an encrypted format.

4.3.2 Ecosystem security diagram and analysis



With reference to above diagram, the following is a summary of the specific requirements for the use or otherwise of secure communication:

1. Operator / IDA: The IDA SHALL require single factor authentication with userid and password for an Operator to access the IDA API.

2. Service Provider / IDA: The Service Provider does not have a role in the IDA API. The IDA MAY provide a mechanism to allow a Service Provider to register new Operators and this mechanism MUST be protected through single factor authentication, at least, with userid and password. The IDA SHALL NOT keep any DIPI for Operators.

3. Operator / Data Engine: The Data Engine SHALL NOT require a password from an Operator when registering a new Consumer or when assigning a new Device to a Consumer.

4. Service Provider / Data Engine:

    a. The Data Engine SHALL require single factor authentication with userid and password for a Service Provider to access the Management Interface (MI) and Query Interface (QI)
    b. Separate credentials SHOULD be used to access the Management Interface (MI) and Query Interface (QI), reducing the likelihood of getting access to both and retrieving Atoms for all of the Service Provider's Consumers.

c. The data engine MUST use a secondary method to assert the identity of the Service Provider prior to processing a ‘forget’ request for a Consumer since these requests are not reversible.

5. 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 and contain no DIPI. Where the Operator is a separate entity their communication MUST use single factor authentication with userid and password.

6. Data Engine / IDA: The IDA SHALL require single factor authentication with userid and password for a Data Engine to access the IDA API.

5 Glossary and Nomenclature

For the purposes of this specification and the COEL ecosystem the following are defined.

5.1 Behavioural Atom

The fundamental data type defined and used extensively throughout the COEL ecosystem is Behavioural Atom (Atom). An Atom is a digital representation of an observable event in an individual's life. It is a small block of self-describing, micro-structured data. Any type of life event can be coded into a Behavioural Atom using the Classification of Everyday Living, a hierarchical taxonomy of decreasing granularity. The individual's identity is pseudonymised with the directly identifying personal information (DIPI) segregated from the Behavioural Atoms in both storage and transmission. The Behavioural Atoms also code the time and duration of events, how they were observed and where they occurred. The Atom types are described by the Classification of Everyday Living Version 1.0, one of this collection's specifications.

5.2 Ecosystem

The Ecosystem is defined as 'the extended set of corporate and individual actors who interact for their mutual benefit via the medium of the specification and under appropriate voluntarily entered into legal agreements'.

5.3 Pseudonymous Key

The unique Pseudonymous Keys are generated by the IDA for use with the ecosystem to provide unique codes for the data and transaction of Consumers, Devices, Operators and Service Providers.

5.4 Directly Identifying Personal Information (DIPI)

Static or slow-changing data needed to provide services to a Consumer including, for example: name, date of birth, contact information, medical/insurance numbers, payment details, etc. DIPI specifically excludes all event-based information (Behavioural Data / Atoms). DIPI is information that would be generally known as PII in a USA context.

5.5 Segment Data

Year of birth, gender, home time zone (GMT+/-x) and home latitude to single degree resolution.

5.6 Behavioural Data

Data that is coded according to the COEL TC protocols with, as a minimum, a Classification of Everyday Living code, a unique ConsumerID and a timestamp. A single instance is known as a Behavioural Atom or Atom.

5.7 Report Data

Data developed from the analysis of Behavioural Data (Atoms) for the purposes of developing insight and information for the provision of value-add services.

5.8 Aggregated and anonymised summary data

Data developed from the analysis of Behavioural Data (Atoms) for the purposes of comparison with Report Data and to deliver business to business services outside a COEL ecosystem.

5.9 ConsumerID

An IDA unique Pseudonymous Key for a particular Consumer.

5.10 ServiceProviderID

An IDA unique Pseudonymous Key for a particular Service Provider.

5.11 OperatorID

An IDA unique Pseudonymous Key for a particular Operator.

5.12 DeviceID

An IDA unique Pseudonymous Key for a particular consumer device.

6 Conformance

An **Identity Authority** (IDA) conforms if it meets the technical requirements set out in Section 2.2 and the security requirements of Section 4.3.

A **Data Engine** conforms if it meets the technical requirements set out in Section 2.3 and the security requirements of Section 4.3.

A **Service Provider** conforms if it meets the technical requirements set out in Section 2.4 and the security requirements of Section 4.3.

An **Operator** conforms if it meets the technical requirements set out in Section 2.5 and the security requirements of Section 4.3.

A **Consumer** of a COEL compliant service conforms if they meet the conditions set out in Section 2.6.

Appendix A. Acknowledgments

The following individuals have participated in the creation of this specification and are gratefully acknowledged:

Participants:

Paul Bruton, Individual Member
Joss Langford, Activinsights
Matthew Reed, Coelition
David Snelling, Fujitsu

Appendix B. Revision History

Revision	Date	Editor	Changes Made
1	22/9/2015	Matthew Reed	First full version
2	26/9/2015	Joss Langford	Updated with all latest definitions.
3	05/10/2015	Paul Bruton	Minor corrections and review comments.
4	13/10/2015	Matthew Reed	Added definition of Associated Service Provider in Section 2.1.
5	19/10/2015	David Snelling	Major review from DE perspective.
6	20/10/2015	Joss Langford	COEL – 24, 35, 36, 37, 38 all fixed. Some defined terms updated.
7	23/10/2015	Paul Bruton	Minor style updates, placeholder for definition of Hardware Developer, Rephrased security requirements.
8	27/10/2015	Joss Langford	Hardware Developer defined, changes agreed and conformance modified to include all security requirements.
9	31/10/2015	Joss Langford	Accept all changes, track changes off, check references and style consistency.
10	02/11/2015	David Snelling	Final date change
11	25/11/2015	Joss Langford	Fix issue COEL-46, first ‘SHALL’ in 4.3.1.4 changed to ‘MAY’.
12	25/11/2015	David Snelling	Set date for CD publication.
13	07/01/2016	David Snelling	Update to WD02.
14	16/08/2016	Paul Bruton	Accepted changes from revision 13 and added comments from work on COEL-53 related to security.
15	17/08/2016	Paul Bruton	Removed comments relating to security and created COEL-74 and COEL-75. Comment relating to COEL-61 remains as a reminder of an inconsistency
16	24/08/2016	Paul Bruton	Applying COEL-75 and COEL-76: Security of the Consumer ID and use of passwords.
17	26/08/2016	Paul Bruton	Accepted changed from COEL-75 and COEL-76. Also corrected references to operators using passwords for DE from COEL-61
18	02/09/2016	Paul Bruton	Fixed misformatting, no content change
19	22/09/2016	Joss Langford	COEL-80: added clarification for roles & actors and moved Associated Service Providers description to a lower level note.

20	25/09/2016	Joss Langford	Roles table clarified.
21	30/09/2016	Paul Bruton	Reviewed and changes accepted.