

Nasjonal referansearkitektur for meldingsutveksling

Forslag



Intro

The following is a printable (pdf) version of the Reference Architecture for eDelivery (eMelding).

The technical part, the reference architecture, is created as a Wiki available here:


<https://difidrift.sharepoint.com/sites/Arkitekturbibliotek/Referansearkitekturer/Hjemmeside.aspx>

(note that at the moment, access requires a Microsoft account)

This printable (pdf) version is the set of all pages in the wiki, that relates to the eDelivery Reference Architecture:

01. Arkitekturbibliotek – Hjemmeside
02. Arkitekturbibliotek - SAT-eDelivery
03. Arkitekturbibliotek - SAT-eDelivery_Requirements
04. Arkitekturbibliotek - ABB-eIDAS_Regulation
05. Arkitekturbibliotek - ABB-eDelivery_Interoperability_Agreement
06. Arkitekturbibliotek - ABB-Business_Process_Choreography
07. Arkitekturbibliotek - ABB-eDocument
08. Arkitekturbibliotek - ABB-Access_Point
09. Arkitekturbibliotek - ABB-Backend_Integration
10. Arkitekturbibliotek - ABB-Message_Exchange
11. Arkitekturbibliotek - ABB-Capability_LookUp
12. Arkitekturbibliotek - ABB-eDelivery_Trust

Reference Architectures

- *eInformation (Informasjonsutveksling)*
 - Reference Architecture
 - Work-in-Progress
- **eDelivery (eMelding) (in Review)**
 - **Strategy:**  **17-01407-2 Forslag - Nasjonal referansearkitektur og strategi for meldingsutveksling 526865_2_0-v1_1.pdf**
 - **Reference Architecture: SAT-eDelivery**
 - **Soution architectures:**
 - BRIS: <https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageld=46992657>
 - EESSI: <http://ec.europa.eu/social/main.jsp?catId=869>
 - EHF: <https://www.anskaffelser.no/digitalisering/verktoykasse-systemleverandorer/formater-ehf-bis>
 - PEPPOL: <https://peppol.eu/what-is-peppol/>
 - ISO20022: <https://vefa.difi.no/iso20022/>
 - eFormidling: <https://samarbeid.difi.no/eformidling>
- **eInteraction (eOppslag)**
 - Strategy: (Work-in-Progress)
 - Reference Architecture: (Work-in-Progress)
- **eNotification (eNotifikasjon)**
 - Strategy: (Work-in-Progress)
 - Reference Architecture: (Work-in-Progress)

Reference Architectures SAT-eDelivery

What is Reference Architecture

Has various definitions and meanings dependent on context and domain area. In the context of Norwegian Interoperability Framework, the generic definition from wikipedia is used:

"A reference architecture provides a template, often based on the generalization of a set of solutions. These solutions may have been generalized and structured for the depiction of one or more architecture structures based on the harvesting of a set of patterns that have been observed in a number of successful implementations. Further it shows how to compose these parts together into a solution. Reference Architectures will be instantiated for a particular domain or for specific projects."

https://en.wikipedia.org/wiki/Reference_architecture

The Norwegian Interoperability Framework takes a business value approach to reference architecture by focusing on the requirements of "digital by default" and "Once only" set by Norwegian Digital Agenda, thereby supporting national and international seamless service provision to citizens and businesses from the Norwegian public sector.

Norwegian Interoperability Reference Architectures can be at various EIF (link) (model?) layers and also cover more EIF (model?) layers i.e. legal, organisational, semantic and/or technical layers. The Reference Architectures are best practice architectures for generic legal, business, semantic and technical requirements and are based on the Norwegian Interoperability Architecture Framework principles (link).

The Reference Architectures are templates for Solutions, expressed by detailing and combining Building Blocks in (Norwegian profile of) the European Interoperability Reference Architecture into SATs (Solution Architecture Templates).

Why use Reference Architecture

Reference architectures provide a national harmonisation of interoperability architectures through common vocabulary, reusable designs and best practices.

Speed: Provides a mature starting point for your architectural work, so you don't have to reinvent the wheel.

Quality: Since a Reference Architecture is proven best practice.

Reuse: Easier to create Building Blocks that are reusable across the Norwegian Public sector.

Harmonisation and interoperability: Harmonises the different views on interoperability and offers interconnection specifications for interoperability in a distributed Norwegian Public Sector.

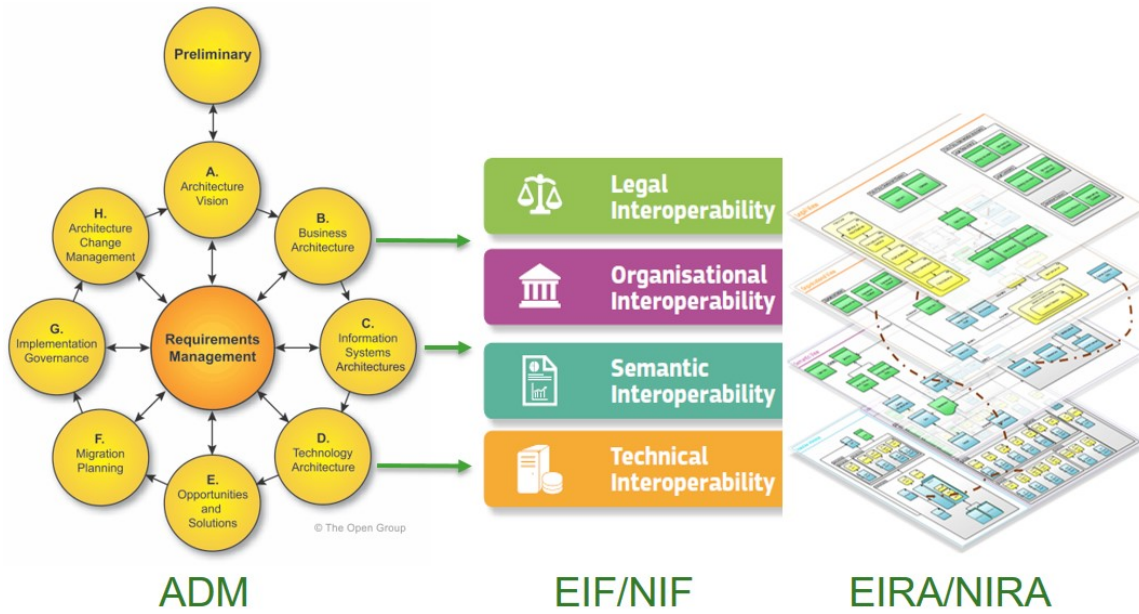
Cross organisational cooperation: through a common vocabulary, models and architectures, the architectural cooperation can be effective on knowledge sharing and joint maturation on interoperability.

Benchmarking: Easier benchmarking, thereby giving a transparent view on the Norwegian Architectural Landscape e.g. identifying gaps and support prioritisation.

Legal compliance: A Reference Architectures can incorporate legal requirements and through test and reviews secure that these requirements are met, this secures an overall translation of legal rules to architecture.

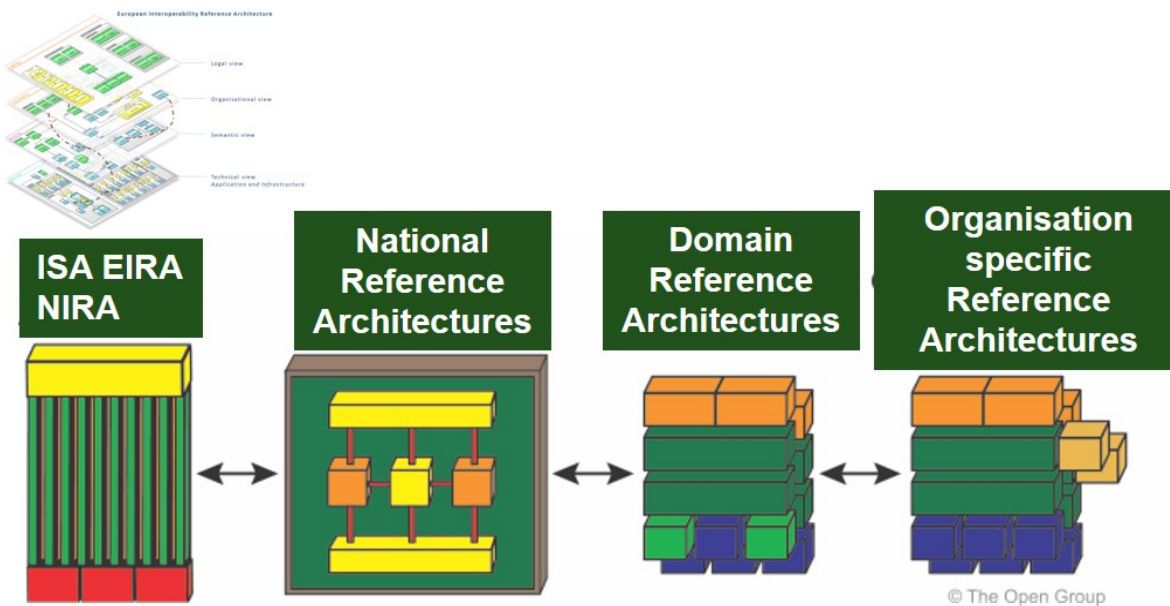
How to use reference architectures?

Reference Architectures are tightly coupled to the method for creating a Solution Interoperability Architecture. The TOGAF ADM is recommended through the Norwegian Interoperability Architecture. The phases B-Business Architecture, C-Information Systems Architecture (data and application) and D-Technology Architecture uses Reference material e.g. Reference Architectures, as the foundation for the Architectural work.



According to TOGAF this material is found in the Architecture Repository, classified and structured according to the TOGAF Continuum (<http://pubs.opengroup.org/architecture/togaf9-doc/arch/ch.39>). In addition, the Norwegian Architecture Repository uses the EIF layers and the EIRA/NIRA to structure the Reference Architectures for quick accessibility.

The Norwegian Interoperability Framework profile of the Architecture Continuum is shown in this figure:



Version: 0.9.0	EIF layer: Legal, Organisational, Semantic, Technical
Type: Solution Architecture Template SAT (Referanse Arkitektur)	Continuum Generic <-----+----> Solution

Home/Hjem: [Hjemmeside](#)

[SAT for eDelivery](#)

[SAT-eDelivery](#)

[SAT-eDelivery_Requirements](#)

[ABBs for eDelivery](#)

Legal level

[ABB-eIDAS_Regulation](#)

Organizational level

[ABB-](#)

[eDelivery_Interoperability_Agreement](#)

[ABB-Business_Process_Choreography](#)

Semantic level

[ABB-eDocument](#)

Technical level

[ABB-Backend_Integration](#)

[ABB-Access_Point](#)

[ABB-Message_Exchange](#)

[ABB-Capability_LookUp](#)

[ABB-eDelivery_Trust](#)

TBD - Work in Progress

[Adress_LookUp](#)

[Addressing_Entities](#)

[Non_Repudiation](#)

EIF Classification:

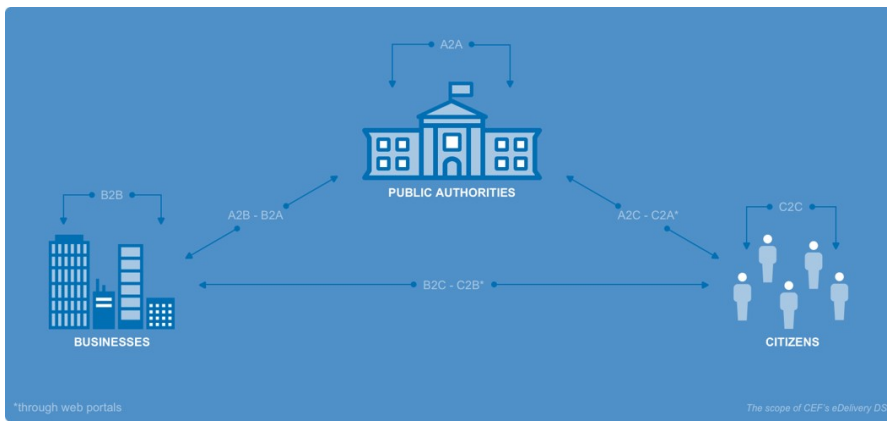


Figure 1: EIF scope

- A2A – Fully with flexible ways of interconnectivity
- A2B – Fully with flexible ways of interconnectivity
- B2B - Fully with flexible ways of interconnectivity
- A2C – Partial with Citizens interconnectivity through a private- or public service provider e.g. portals
- C2C – Partial with Citizens interconnectivity through a private- or public service provider e.g. portals

Non technical description

The reference architecture supports cross enterprise business processes, where two enterprises participate in a distributed Business Process in a choreography manner. Where the Business Process crosses the Enterprise border to another Enterprise, the sending enterprise makes an event notification and hands over necessary information to a receiving Enterprise to invoke the corresponding business process.

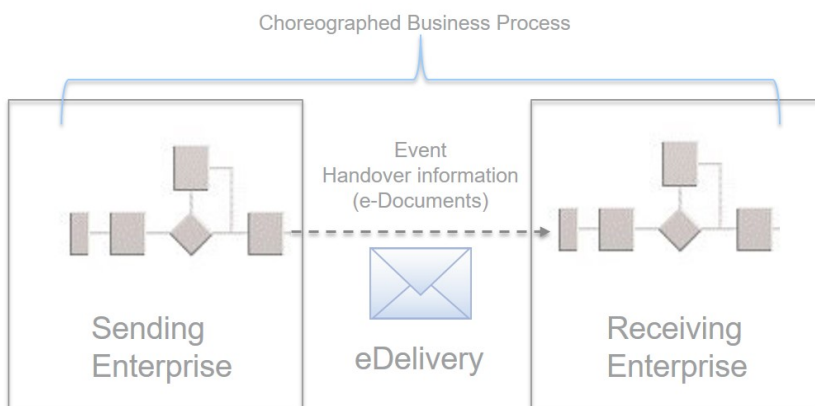


Figure 2: eDelivery context

An enterprise conducting a Business process, where the Business Process needs to invoke a Business Process in another Enterprise can use the Reference architecture for Norwegian e-Delivery to send an event notification and the required information (eDocuments) to the other Enterprise to invoke and thereby proceed the continued Business Process.

The Term Enterprise can be extended to Citizens, where a citizen can either be sending i.e. trigger the process of a receiving Enterprise or be receiving, thereby start a "citizen process" e.g. fill in tax return.

Definition

eDelivery is electronically pushing Event notification and eDocuments (Set of interrelated structured or semistructured information) between two Enterprises i.e. from a sending Back-end system (or Citizen) to another receiving Back-end System (or Citizen).

eDelivery supports public Public administrations, Businesses and Citizens to engage in shared Business processes in an electronic way by exchanging event-notifications and eDocuments with other Public administrations, Businesses and citizens, in a flexible interoperable, secure, reliable and trusted way.

Requirements

Electronic Delivery Service

Norwegian eDelivery basic requirements: [SAT-eDelivery_Requirements](#)

Electronic Registered Delivery Service

A service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations

eIDAS (reference) compliant requirements: [ABB-eIDAS_Regulation](#)

Description of Architecture

The Architecture is in compliance with the SOA principles, EIF principles and the Norwegian IT-principles for public sector (see "Nasjonal strategi for meldingsutveksling")

The Business Exchange Pattern used is Asynchronous-Push, meaning that the Sending Enterprise can send event notifications and eDocuments in a reliable and secure way, without knowing when the receiving Enterprise is ready to consume the event notification and eDocuments.

It should be noted that here the term eDelivery is not fully consistent with the CEF eDelivery term eDelivery. The definition and architecture of eDelivery spans all of the EIF layers, whereas CEF eDelivery uses the term for the technical part, here defined as Technical eDelivery.

The Solution Architecture Templates contributes to eDelivery in the following areas:

Legal	EU eIDAS regulation to set additional requirements to eDelivery: ABB-eIDAS_Regulation
Organisational	Interoperability Agreement to set up an eDelivery community: ABB-eDelivery_Interoperability_Agreement

	<p>Business Process Choreography to define the interaction relationship between two or more enterprises in performing a joint Business Process:</p> <p>ABB-Business_Process_Choreography</p>
Semantic	<p>eDocument to define the Event notification and the accompanying information:</p> <p>ABB-eDocument</p>
Technical	<p>A detailed flexible, scalable, reliable and secure architecture for the exchange of eDocuments in compliance with the defined Business Process Choreography, within an eDelivery community in accordance with eIDAS regulations:</p> <p>See below</p>

Technical eDelivery Architecture

Technical eDelivery architecture is based on a distributed model, allowing communication (one Back-end system to send eDocument(s) to another Back-end system) between participants without the need to set up bilateral agreements and technical channels.

For Flexibility and Scalability the Architecture is based on a 4 Corner model with Location- and Capability LookUp:

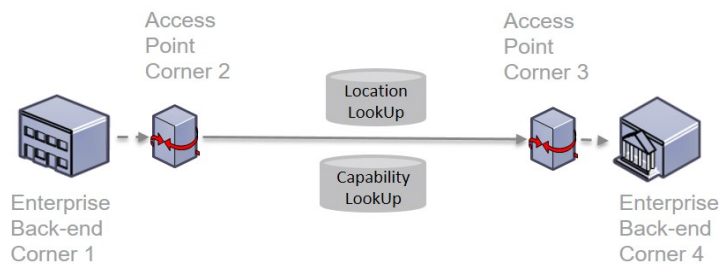


Figure 3: Four Corner Model with Location- and Capability LookUp

Corner 1 represents a Back-end system (within the legal responsibility of the sending organization), that needs to send eDocument(s) to another Back-end system (Corner 4). This is done by interacting with

Corner 2 (Sending Access Point). The address and the receiving capabilities (legal, organisational, semantic and technical) of the receiver is established through the Location LookUp and the Capability LookUp. With the technical capability to send the event notification and related eDocuments(s) in a reliable and secure way to the correct receiving

Corner 3 (Receiving Access Point). The Receiving Access Point has technical capability to receive the eDocuments(s) in a reliable and secure way and interact with

Corner 4, the receiving Back-end system (within the legal responsibility of the receiving organization) to deliver the eDocuments.

In this 4-Corner Store-and-Forward model, every eDelivery Access Point becomes a node in a trusted interoperability community.

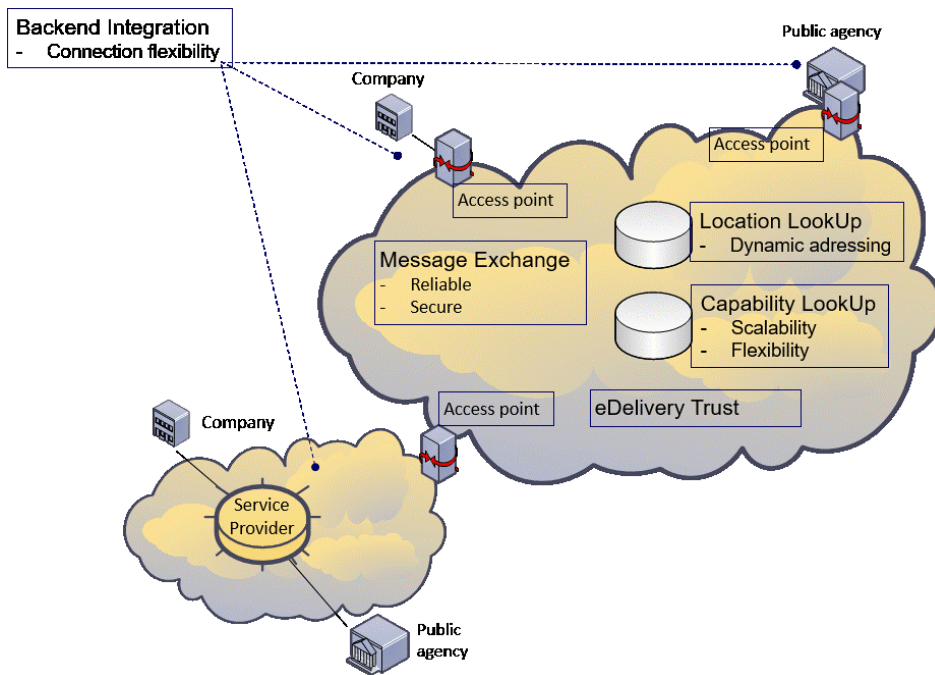


Figure 4: Example of eDelivery community

Figure 4 shows the different Architectural Building Blocks (ABB) of the Technical eDelivery Architecture.

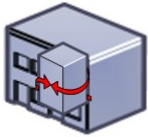
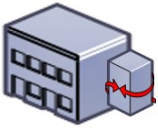
Each Architectura Building Block will be described below with a more detailed description and specification in a seperate page. Order of description:

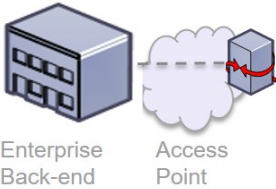
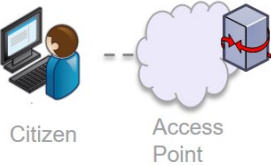
- Backend Integration (detailed ABB description and specification: [ABB-Backend_Integration](#))
- Access Point (detailed ABB description and specification: [ABB-Access_Point](#))
- Message Exchange (detailed ABB description and specification: [ABB-Message_Exchange](#))
- Location LookUp (TBD if it belongs in the Norwegian SAT)
- Capability LookUp (detailed ABB description and specification: [ABB-Capability_LookUp](#))
- eDelivery Trust (detailed ABB description and specification: [ABB-eDelivery_Trust](#))

Backend Integration

[ABB-Backend_Integration](#)

The Architecture is flexible on the integration between Access Points and Back-end systems:

 <p>Enterprise Back-end Access Point</p>	<p>Tightly Coupling</p> <p>Back-end system and Access Point is tightly coupled i.e. The Back-end system has integrated the Access Point into the Back-end system. One Access Point handles the eDelivery of one Back-end System.</p>
 <p>Enterprise Back-end Access Point</p>	<p>Semi-Tightly Coupling</p> <p>Back-end system and Access Point is semi-tightly coupled i.e. The Back-end system and the Access Point is internally loosely coupled, but part of the same internal IT-Architecture and IT-Infrastructure or the Access Point is an Internal Cloud solution.</p>

	One Access Point can handle the eDelivery of several Back-end Systems.
 <p>Enterprise Back-end Access Point</p>	<p>Loose Coupling Coupling</p> <p>The Back-end system and the Access Point is loosely coupled and not part of the same internal IT-Architecture and IT-Infrastructure. One Access Point can handle the eDelivery of many Back-end Systems from many Enterprises. This model accomodate the use of Service-/Cloud providers, where the interaction between the Back-end system and the Cloud is determined by the Architecture and Infrastructure of the Service/Cloud provider.</p>
 <p>Citizen Access Point</p>	<p>Loose Coupling Coupling (Citizen)</p> <p>The Citizen can send and receive eDocuments through the use of Service-/Cloud providers, where the interaction between the Citizen and the Service-/Cloud provider is determined by the setup of the architecture and infrastructure of the Service/Cloud provider.</p>

The above means that in a specific instance of an eDelivery transfer of Event notification and eDocuments, the actual number of corners can be 1, 2, 3, or 4.

Access Point

[ABB-Access_Point](#)

The Access Point is at the core of the Architecture and its role is illustrated with this animation:

 [RA-SAT-eDelivery-Additional1.pptx](#)

Message Exchange

[ABB-Message_Exchange](#)

The Message Exchange performs the Secure and Reliable transfer of the message from Corner3 to Corner4.

Capability LookUp

[ABB-Capability_LookUp](#)

The Capability LookUp publish the Receiver (Corner4) Legal, Organisational and Semantic Capabilities i.e. Legal constraints, Business Processes supported and eDocuments supported. It also publishes the Receiver (Corner4) Technical Capabilities i.e. choice of Message Exchange protocol, version and configuration.

eDelivery Trust

[ABB-eDelivery_Trust](#)

eDelivery Trust defines the overall Trust circle between Sending Enterprise and Receiving Enterprise. It also specifies how the implementation of a virtual eDelivery community.

Location LookUp

(TBD)

The Location LookUp enables the Sending Access Point to dynamically discover the IP address of the Capability LookUp for the Receiving Enterprise. The Internet's Domain Name System (DNS) is used for this purpose.

Addressing Entities

(TBD)

Unique identification of an Enterprise as a logical electronic address.

Non Repudiation

(TBD)

The PEPPOL-extended addresses this feature of end-to-end non-repudiation.

References

1. [EIF3]: European Interoperability Framework (EIF), ISA² COMMITTEE 2016-03-02 DOC 9 (DRAFT)
2. [EIRA]: EIRA Description: Joinup, <https://joinup.ec.europa.eu/asset/eia/description>
3. [DIFI2013:13]: Meldingsutveksling internt i forvaltningen Rapport 2013:13, ISSN: 1890-6583
4. [DIFI2015:3]: Løsning for meldingsutveksling i offentlig sector, Rapport 2015:3, ISSN: 1890-6583
5. [e-SENS] e-SENS SAT e-Delivery: <http://wiki.ds.unipi.gr/display/ESENS/SAT+-+eDelivery>
6. [CEF eDel] CEF e-Delivery: <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery>
7. [ISA eDel] ISA EIRA SAT: e-Delivery: https://joinup.ec.europa.eu/asset/eia/asset_release/edelivery-sat-v101-beta

Work-in-progress

-

Log

Date	Version	Author	Remarks
01.12.2017	0.90	Klaus Vilstrup Pedersen	First version

Home/Hjem: [Hjemmeside](#)

[SAT for eDelivery](#)

[SAT-eDelivery](#)

[SAT-eDelivery_Requirements](#)

[ABBs for eDelivery](#)

Legal level

[ABB-eIDAS_Regulation](#)

Organizational level

[ABB-](#)

[eDelivery_Interoperability_Agreement](#)

[ABB-Business_Process_Choreography](#)

Semantic level

[ABB-eDocument](#)

Technical level

[ABB-Backend_Integration](#)

[ABB-Access_Point](#)

[ABB-Message_Exchange](#)

[ABB-Capability_LookUp](#)

[ABB-eDelivery_Trust](#)

TBD - Work in Progress

[Adress_LookUp](#)

[Addressing_Entities](#)

[Non_Repudiation](#)

Version: 0.9.0	EIF layer: Legal, Organisational, Semantic, Technical
Status: Requirements (Krav)	Continuum Generic<-----+---->Solution

Requirements for Norwegian eDelivery (Meldingsutveksling)

Note that an additional set of requirements related to eIDAS: <https://ec.europa.eu/digital-single-market/en/trust-services-and-eid> e.g. end-to-end non-repudiation and additional security for transmission of sensitive data, is available in [ABB-eIDAS_Regulation](#)

The description of Requirements is organized with the following attributes:

"Id" is the unique Id of the Requirement in the Requirement Catalogue (Krav kataloget):

- Context shortname:
 - "Gen" for general
 - "InfEx" for Information Exchange
 - "eDel" for eDelivery
- EIF level, where the requirement is initiated:
 - "Leg" for Legal
 - "Org" for organizational
 - "Sem" for semantic
 - "Tec" for technical
- Number

"Requirement" is a short statement of the requirement. The formulation of each Requirement contains a strength of the requirement:

- "Must" - the Reference Architecture accommodates this requirement and solution architectures must fulfill this requirement
- "Should" - the Reference Architecture accommodates this requirement and for the solution architectures it is a recommendation to fulfill this requirement. If not, an explanation must be given.
- "Can" - the reference architecture accommodates this requirement and for the solution architectures it is a recommendation to fulfill this requirement if needed.

Description is an explanation of the Requirements and can contain:

- Describing the Requirement in more detail
- References to similar requirements (requirement overlap)
- References to the source of the requirement

The below requirements below was to a large degree defined in the EC PEPPOL project <http://peppol.eu/> (2008-2012), consolidated in the EC eSENS project <https://www.esens.eu/> (2013-2017) and the EC CEF eDelivery programme <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery> (2015-2020). In the Spring of 2017, the requirements was further consolidated and profiled by Difi to match Norwegian needs and requirements.

Id	Requirement	Description
Gen-Leg01	Must follow the Norwegian Interoperability principles and the EIF principles	Norwegian Interoperability Principles (Norske Samhandlings Prinsipper) (Link) European Interoperability Framework Principles https://ec.europa.eu/isa2/eif_en
Gen-Leg02	Should follow the eIDAS regulations	https://ec.europa.eu/digital-single-market/en/policies/trust-services-and-eidentification
eDel-Leg01	Must follow the set of principles set in the Norwegian eDelivery Strategy (Strategi for Norsk meldingsutveksling)	Norwegian Strategy on eDelivery (Norsk strategi for meldingsutveksling) (Link)
InfEx-	Must be easy accessible by	This requirement can be restated as "use of Internet and

Org01	Participants	Internet technologies" at the Technical level.
eDel- Org01	Must encapsulate a eDelivery community.	That only participants cleared for the community is able to send and receive event notifications and eDocuments. With eDEL-Org01, this requires other measures than physical division of communities e.g. by use of certificates.
eDel- Org02	An eDelivery community must share one interoperability agreement	The Interoperability agreement defines the eDelivery community, those participants signing the agreement are members of the community. Avoiding bilateral interoperability agreements.
eDEL- Org03	Must be possible to participate in multiple eDelivery communities with own interoperability agreements.	A participant can be part of several interoperability agreements e.g. eProcurement, eHealth, through a virtual segmentation of the eDelivery Infrastructure.
eDEL- Org04	Transmission of Event notifications and eDocuments should be reliable.	An Event notifications and eDocuments is delivered to the receiver once and only once. Level of reliability must be addressed in the Interoperability agreement. For additional reliability see ABB-eIDAS_Regulation
eDEL- Org05	Transmission of Event notifications and eDocuments should be Secret.	In some cases Secrecy is not a requirement, whereas in other cases Secrecy is a "must" requirement. Level of Secrecy must be addressed in the Interoperability agreement. For additional Secrecy see ABB-eIDAS_Regulation
eDEL- Org06	Transmission of Event notifications and eDocuments should have Authenticity of sender.	In some cases Authenticity is not a strong requirement, belonging to the eDelivery community is enough, whereas in other cases Authenticity is a "must" requirement. Level of Authenticity must be addressed in the Interoperability agreement. For additional Authenticity see ABB-eIDAS_Regulation
eDEL- Org07	Transmission of Event notifications and eDocuments should be with Integrity.	In some cases eDocuments will be transformed e.g. from one format to another, whereas in other cases Integrity is a "must" requirement. Level of Integrity and possibilities for transformation must be addressed in the Interoperability agreement. For additional Integrity see ABB-eIDAS_Regulation
eDEL- Org08	Transmission of Event notifications and eDocuments can be Non-reputable.	Non-repudiation is the creation of a digital Notification and eDocument original e.g. neither parties can dispute the sending and reception incl. the content. In some cases Non-repudiation is not a requirement, trust in the eDelivery community and the receiver is enough, whereas in other cases, with high importance Business Processes, Non-repudiation is a "must" requirement. Use of Non-repudiation must be addressed in the Interoperability agreement. For Non-repudiation see ABB-eIDAS_Regulation
eDEL- Org09	eDelivery must be flexible – allow and handle participants with different Business Process interoperability maturity.	Difference between participants in what business processes are digitalized and what parts of a business process is digitized.
eDEL-	eDelivery must be flexible –	Valid Business Processes, Notifications and

Org10	allow and handle Business processes and eDocuments with different requirements.	eDocuments must be addressed in the Interoperability agreement. See eDEL-Org04, eDEL-Org05, eDEL-Org06, eDEL-Org07, eDEL-Org08
eDEL-Org11	eDelivery must be scalable – number of participants	An eDelivery community must be able to scale i.e. inherent in the architecture is possibilities to make solutions that doesn't put up barriers for scalability
eDEL-Org12	eDelivery must be scalable – number of transactions	An eDelivery community must be able to scale i.e. inherent in the architecture is possibilities to make solutions that doesn't put up barriers for scalability
eDel-Sem01	Must be possible to send multiple eDocuments with an Event Notification.	An Event notification can be followed by multiple eDocuments, that are relevant to initiate (and fulfill) a Business Process on the receiving side.
eDel-Sem02	Must be eDocument agnostic.	Any type of Documents are supported e.g. XML, pdf, Doc.
eDel-Sem03	Must be able to exchange eDocuments at a size < 2GB	Current technical constraint. Se prinsip for at data anvendes fra Deres plasering.
eDel-Tec01	Must be based on Open standards with high traction.	Building the technical eDelivery (Meldingsformidling) on Open standards that are
eDel-Tec02	Must have flexible Change Management	Possibility to change Building Blocks or versions in an easy and flexible way e.g. «long» phase-in and phase-out of technologies.
eDel-Tec013	Must accomodate competition on solutions and service provision	Building the technical eDelivery (Meldingsformidling) architecture on Open standards that are widely used (traction) Building the technical eDelivery (Meldingsformidling) architecture such that it offers a wide variety of choices of participating e.g. directly or through service providers (cloud based).

Work-in-progress

-

Log

Date	Version	Author	Remarks
01.12.2017	0.90	Klaus Vilstrup Pedersen	First version

Version: 0.9.0	EIF layer: Legal
Type: Requirements (Krav)	Continuum Generic<-----+---->Solution

Description

Sets requirements for Information Exchange (Informasjonsutveksling)

Electronic identification (eID) and electronic Trust Services (eTS) are key enablers for secure cross-border electronic transactions and central building blocks of the Digital Single Market.

The Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) adopted by the co-legislators on 23 July 2014 is a milestone to provide a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities.

<https://ec.europa.eu/digital-single-market/en/policies/trust-services-and-eidentification>

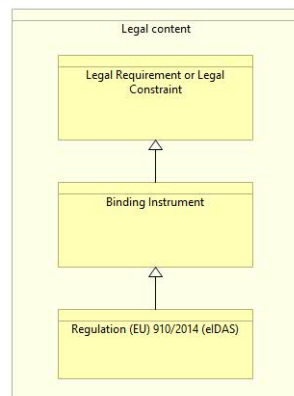
Requirements

[SAT-eDelivery_Requirements](#)

Gen-Leg01

Specification

The eIDAS Regulation Trust is a specialization of the EIRA 2.0 Building Blocks "Legal Requirement or Legal Constraint", "Binding Instrument".



See <https://joinup.ec.europa.eu/release/eira/v200> for definitions of Architectural Building Blocks in EIRA 2.0.

eDelivery definition (specialization of the EIRA 2.0 definition) of:

Public Policy Formulation and Implementation Instrument

Public Policy Formulation Instrument: Technique or means for the development of pertinent and acceptable proposed courses of action for dealing with public problems.

Public Policy Implementation Instrument: Technique or means for the carrying out of a policy decision

Based on NCPI and OECD definitions.

https://web.stanford.edu/group/ncpi/unspeficied/assessment_states/framework.html

<https://www.oecd.org/edu/cei/The%20Nature%20of%20Policy%20Change%20and%20Implementation.pdf>

DECISION (EU) 2015/2240 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015 establishing a programme on interoperability solutions and common frameworks for European public administrations, businesses and citizens (ISA2 programme) as a means for modernising the public sector.

Legal Requirement or Legal Constraint

Legal requirements: Any legal demands, constraints, needs to be met.

Legal constraint: Legal limitation.

Home/Hjem: [Hjemmeside](#)

[SAT for eDelivery](#)

[SAT-eDelivery](#)

[SAT-eDelivery_Requirements](#)

[ABBs for eDelivery](#)

Legal level

[ABB-eIDAS_Regulation](#)

Organizational level

[ABB-](#)

[eDelivery_Interoperability_Agreement](#)

[ABB-Business_Process_Choreography](#)

Semantic level

[ABB-eDocument](#)

Technical level

[ABB-Backend_Integration](#)

[ABB-Access_Point](#)

[ABB-Message_Exchange](#)

[ABB-Capability_LookUp](#)

[ABB-eDelivery_Trust](#)

TBD - Work in Progress

[Adress_LookUp](#)

[Addressing_Entities](#)

[Non_Repudiation](#)

Based on the Black's law dictionary:

<http://thelawdictionary.org/requirements/>

<http://thelawdictionary.org/constraint/>

Binding Instrument

Legal means, involving an obligation, which are available to the European institutions to carry out their tasks. The European binding instruments listed in Article 288 of the Treaty on the Functioning of the European Union are:

- regulations: these are binding in their entirety and directly applicable in all EU countries;
- directives: these bind the EU countries as to the results to be achieved; they have to be transposed into the national legal framework and thus leave margin for manoeuvre as to the form and means of implementation;
- decisions: these are fully binding on those to whom they are addressed.

Based on EUR-Lex

http://eur-lex.europa.eu/summary/glossary/community_legal_instruments.html

Regulation (EU) 910/2014 (eIDAS)

<https://ec.europa.eu/digital-single-market/en/policies/trust-services-and-eidentification>.

This is translated into a set of Requirements for eDelivery.

The description of Requirements is organized with the following attributes:

"Id" is the unique Id of the Requirement in the Requirement Catalogue (Krav kataloget):

- Context shortname:
 - "InfEx" for Information Exchange
- EIF level, where the requirement is initiated:
 - "Leg" for Legal
- Number

"Requirement" is a short statement of the requirement. The formulation of each Requirement contains a strength of the requirement:

- "Must" - the Reference Architecture accommodates this requirement and solution architectures must fulfill this requirement
- "Should" - the Reference Architecture accommodates this requirement and for the solution architectures it is a recommendation to fulfill this requirement. If not, an explanation must be given.
- "Can" - the reference architecture accommodates this requirement and for the solution architectures it is a recommendation to fulfill this requirement if needed.

Description is an explanation of the Requirements and can contain:

- Describing the Requirement in more detail
- References to similar requirements (requirement overlap)
- References to the source of the requirement

The below Requirements is derived from the eIDAS regulations.

Id	Requirement	Description
InfEx-Leg01	Message integrity: Messages should be secured against any modification during transmission.	The sending and receiving of data is secured by an advanced electronic signature or an advanced electronic seal of a qualified trust service provider in such a manner as to preclude the possibility of the data being changed undetectably. Artikel 3 (36), 19, 24,44
InfEx-Leg02	Message Confidentiality: Messages should be encrypted during transmission.	Artikel 5,19,24
InfEx-Leg03	Sender authenticity: The identity of the sender should be verified. Ensure with a high level of confidence the identification of the sender.	Artikel 24, 44
InfEx-Leg04	Recipient authenticity: Recipient / addressee Identity should be verified before the delivery of the message.	Ensure the identification of the addressee before the delivery of the data. Artikel 24, 44

InfEx-Leg05	Non repudiation: The date and time of sending and receiving a message should be indicated via a qualified electronic timestamp.	The date and time of sending, receiving and any change of data are indicated by a qualified electronic time stamp.Artikkel 44
InfEx-Leg06	Non repudiation: Sender and receiver of the message should be provided with evidence of message recipient and deliver.	Provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data.Artikkel 3
InfEx-Leg07	Trusted providers: Qualified and non-qualified trust service providers shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide.	Having regard to the latest technological developments, those measures shall ensure that the level of security is commensurate to the degree of risk. In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of the adverse effects of any such incidents.Artikkel 19
InfEx-Leg08	Qualified and non-qualified trust service providers shall, without undue delay but in any event within 24 hours after having become aware of it, notify the supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority, of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein.	Artikkel 19
InfEx-Leg09	Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the trust service provider shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay.	Artikkel 19
InfEx-Leg10	Where appropriate, in particular if a breach of security or loss of integrity concerns two or more Member States, the notified supervisory body shall inform the supervisory bodies in other Member States concerned and ENISA.	Artikkel 19
InfEx-Leg11	The notified supervisory body shall inform the public or require the trust service provider to do so, where it determines that disclosure of the breach of security or loss of integrity is in the public interest.	Artikkel 19
InfEx-Leg12	Trusted providers: The supervisory body shall provide ENISA once a year with a summary of notifications of breach of security and loss of integrity received from trust service providers.	Artikkel 19
InfEx-Leg13	Trust service providers: They are provided by one or more qualified trust service provider(s).	Artikkel 44
InfEx-Leg14	Integrity: Any change of the data needed for the purpose of sending or receiving the data is clearly indicated to the sender and addressee of the data.	Artikkel 44
InfEx-	Non-repudiation: Data sent and received using an	Artikkel 43

Leg15	electronic registered delivery service shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic registered delivery service.	
InfEx-Leg16	Integrity: Data sent and received using a qualified electronic registered delivery service shall enjoy the presumption of the integrity of the data, the sending of that data by the identified sender, its receipt by the identified addressee and the accuracy of the date and time of sending and receipt indicated by the qualified electronic registered delivery service.	Artikkel 43
InfEx-Leg17	Legal effect: An electronic document shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form.	Artikkel 46
InfEx-Leg18	Data processing and protection: Processing of personal data shall be carried out in accordance with Directive 95/46/EC	Artikkel 5
InfEx-Leg19	Data processing and protection: Without prejudice to the legal effect given to pseudonyms under national law, the use of pseudonyms in electronic transactions shall not be prohibited.	Artikkel 5

Standards/profiles

Profile	Link	Standard	Description	Status
eIDAS Regulations	https://ec.europa.eu/digital-single-market/en/policies/trust-services-and-eidentification	-	-	Production

Recommendations

-

Work-in-progress

-

Log

Date	Version	Author	Remarks
01.12.2017	0.90	Klaus Vilstrup Pedersen	First version

ABB-eDelivery_Interoperability_Agreement

Home/Hjem: [Hjemmeside](#)

Version: 0.9.0	EIF layer: Organisational
Type: Architectural Building Block ABB (Arkitekturkomponent)	Continuum Generic <-----+-----> Solution

[SAT for eDelivery](#)

[SAT-eDelivery](#)

[SAT-eDelivery_Requirements](#)

[ABBs for eDelivery](#)

Legal level

[ABB-eIDAS_Regulation](#)

Organizational level

[ABB-eDelivery_Interoperability_Agreement](#)
[ABB-Business_Process_Choreography](#)

Semantic level

[ABB-eDocument](#)

Technical level

[ABB-Backend_Integration](#)

[ABB-Access_Point](#)

[ABB-Message_Exchange](#)

[ABB-Capability_LookUp](#)

[ABB-eDelivery_Trust](#)

TBD - Work in Progress

[Adress_LookUp](#)

[Addressing_Entities](#)

[Non_Repudiation](#)

Description

The Interoperability Agreement is setting the overall terms/conditions for the exchanging of information in an eDelivery community.

The Interoperability Agreement is what defines an eDelivery community, that is separated from the general Internet (Virtual Community) and other eDelivery communities. Only participants that has signed the Interoperability Agreement is a direct member of the specific eDelivery community. In the case of Service Providers, they are seen as proxies for their customers and therefore signs the Interoperability Agreement on their behalf and indirectly through their services, gives access to the eDelivery community.

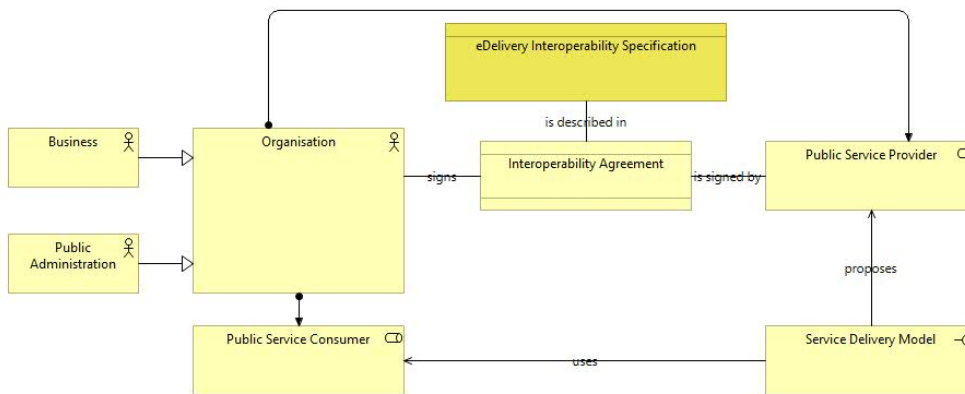
Requirements

[SAT-eDelivery_Requirements:](#)

InfEx-Org01, eDel-Org01, eDel-Org02, eDEL-Org03

Specification

The eDelivery Interoperability Agreement is a specialization of the EIRA 2.0 Building Block "Interoperability Agreement"



See <https://joinup.ec.europa.eu/release/eira/v200> for definitions of Architectural Building Blocks in EIRA 2.0.

eDelivery definition (specialization of the EIRA 2.0 definition) of:

Interoperability Agreement

Concrete and binding documents which set out the precise obligations of two parties cooperating to achieve interoperability.

This ABB is a key interoperability enabler for assessing the TERMS/CONDITIONS for EXCHANGING information.

An Interoperability Agreement is the means through which organisations (public administrations, or businesses) formalises the cooperation with one another. These agreements aim at the development of interoperability solutions, which meets the functional / technical requirements and needs of one another.

The agreement should include purposes and goals, terms and conditions, governance, and the description of the channel(s).

The EIRA differentiates the following Interoperability Agreements:

- Interoperability Service Agreement (between Public Service Consumers and Public Service Providers;
- Interoperability Collaboration Agreement (between Organisations); or
- Interoperability Provider Agreement (between Public Service Providers).

With the eDelivery Interoperability Agreement being an Interoperability Collaboration Agreement

eDelivery Interoperability Agreement

Concrete and binding documents which set out the precise obligations of two or more parties cooperating to achieve interoperability.

Standards/profiles

Profile	Link	Standard	Description	Status
-	-	-	-	-

Recommendations

As a starting point the following (Solution) Architecture Block should be used:

- The Transport Infrastructure Agreement (TIA) produced openPEPPOL (<https://peppol.eu/>) and DIFI ANS:
 - https://www.anskaffelser.no/sites/anskaffelser/files/peppolaprovideragreement_v3p0-no_20121102_0.pdf
 - <https://www.anskaffelser.no/verktoy/avtaler-mellom-difi-og-aksesspunkt>

Work-in-progress

-

Log

Date	Version	Author	Remarks
01.12.2017	0.90	Klaus Vilstrup Pedersen	First version

Version: 0.9.0	EIF layer: Organisational
Type: Architectural Building Block ABB (Arkitektur komponent)	Continuum Generic<-----+----->Solution

Description

Business Process can be defined as:

“a series or network of value-added activities, performed by their relevant roles or collaborators, to purposefully achieve the common business goal.”

Ryan K. L. Ko: A Computer Scientist's Introductory Guide to Business Process Management (BPM), www.acm.org/crossroads Summer 2009/Vol. 15, No. 4

This means that any kombination of humans, technology, materials, methods that is used to produce a deliverable (the Business goal: goods, service, result, experience etc.) can be seen as a Business Process.

A Business Process can be Structured, Semi-structured and Unstructured, meaning that it covers any kind of work in any kind and form in any organizations e.g. commercial-, non-for-profit- and public organisations. It also covers different types of processes i.e. management-, core- and support processes.

In order to create Digitalised Business Processes that are shared between and crosses multiple organizations, the Business Collaboration between the Organisations needs to be established. In this context, the **Business Process Choreography** is the formal description of the Business Collaboration and includes:

- Goal - the overall goal of the Business Process - sets the context of the Choreography
- Roles - what roles are involved in the Business Process i.e. who has which responsibilities in order reach the overall Business goal.
- Organisations - Who is responsible for performing the role
- Sequence/flow - in what order is transactions between the roles performed
- Documents - Information transferred in a transaction in terms of the Notification (start a specific process) and Information contained in one or more Documents (needed to initiate the Business Process at the receiver side)

Example:

Business Goal: Public entity acquiring services or goods

Roles: Contracting Authority (Buyer), Economic Operator (Supplier)

Organisations: TBD

Sequence/flow:

Home/Hjem: [Hjemmeside](#)

[SAT for eDelivery](#)

[SAT-eDelivery](#)

[SAT-eDelivery_Requirements](#)

[ABBs for eDelivery](#)

Legal level

[ABB-eIDAS_Regulation](#)

Organizational level

[ABB-](#)

[eDelivery_Interoperability_Agreement](#)

[ABB-Business_Process_Choreography](#)

Semantic level

[ABB-eDocument](#)

Technical level

[ABB-Backend_Integration](#)

[ABB-Access_Point](#)

[ABB-Message_Exchange](#)

[ABB-Capability_LookUp](#)

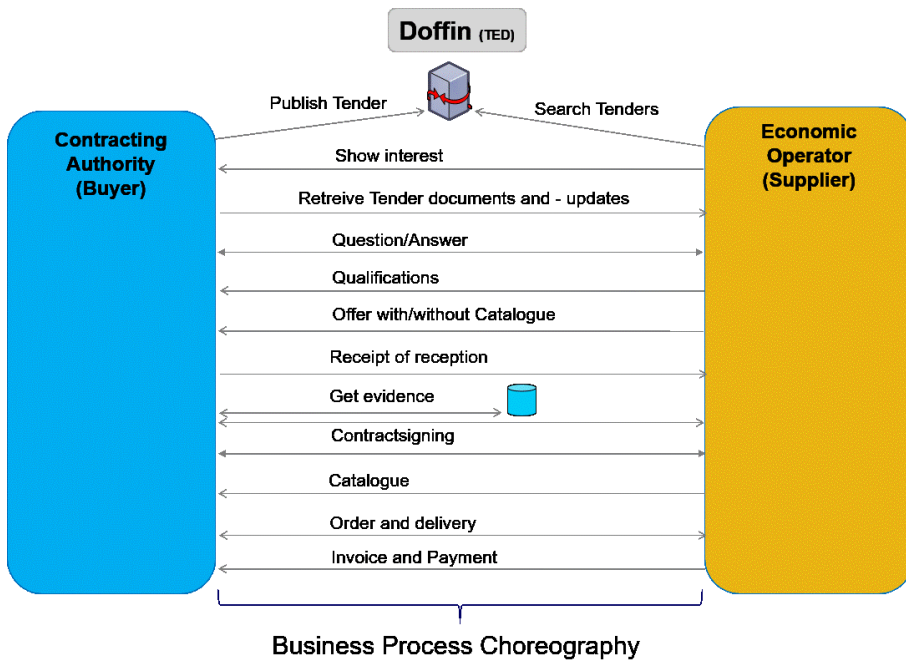
[ABB-eDelivery_Trust](#)

TBD - Work in Progress

[Adress_LookUp](#)

[Addressing_Entities](#)

[Non_Repudiation](#)



Messages: Definition of Documents: Publish Tender,..., Qualifications,..., Order, invoice and Payment

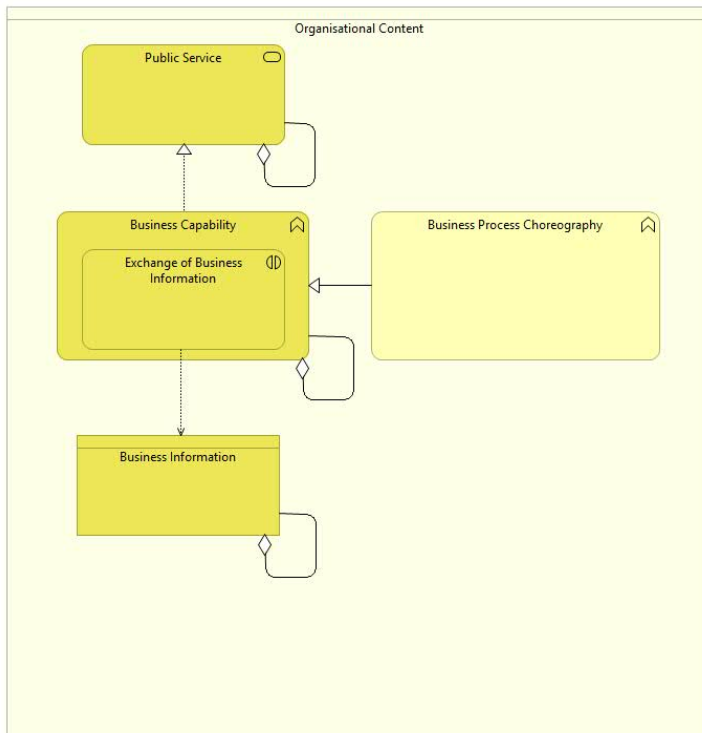
Requirements

SAT-eDelivery_Requirements:

eDEL-Org04, eDEL-Org05, eDEL-Org06, eDEL-Org07, eDEL-Org08,

Specification

The eDelivery Interoperability Agreement is a specialization of the EIRA 2.0 Building Block "Business Capability", "Exchange of Business Information"



See <https://joinup.ec.europa.eu/release/eira/v200> for definitions of Architectural Building Blocks in EIRA 2.0.

Definition (specialization of the EIRA 2.0 definition) of

Business Capability

A particular ability or capacity that an organisation may possess or exchange to achieve a specific purpose or outcome.

Defining a business capability involves identifying and describing what needs to be done by the business in support of its overall mission.

Business capabilities provide an abstraction of the business reality in a way that helps to simplify conversations between interested stakeholders.

Based on TOGAF definition and description of business capability.

<https://www2.opengroup.org/ogsys/catalog/g161>

Exchange of Business Information

Communication of business information by a business capability.

This ABB is a key interoperability enabler (*) for assessing the compatibility of interaction in exchanged information.

Based on TOGAF definitions.

<https://www2.opengroup.org/ogsys/catalog/g161>

<http://pubs.opengroup.org/architecture/togaf9-doc/arch/>

(*)DECISION (EU) 2015/2240 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015 establishing a programme on interoperability solutions and common frameworks for European public administrations, businesses and citizens (ISA2 programme) as a means for modernising the public sector.

Business Process Choreography

Interaction between 2 or more autonomous Enterprises participating in a Business Process. Set and order of transactions each with Event Notification and relevant Business Information.

Standards/profiles

Profile	Link	Standard	Description	Status
-	-	-	-	-

Recommendations

BPMN (<http://www.bpmn.org/>) can be used for the design of a Choreography.

The design of a Choreography must contain the roles participating in the Digitalized Choreography.

The design of a Choreography must contain references to Notifications and eDocuments (Semantic level) involved in the Choreography.

The design of a Choreography must contain the normal flow of the Digitalized Choreography:

- The overall goal of the full Business Process is reached
- All exchange of information is digitalized (Digital by Default)

The design of a Choreography should contain exception flows of the Digitalized Choreography:

- The overall goal of the full Business Process is not directly reached (exception to normal flow) e.g. Invoice with errors leading to the Business process goal through a dispute and resolution exception Process.
- Exchange of (part-of) information is not digitalized (exception to Digital by Default) e.g. Citizens handing in a tax return on paper.

The design of a Choreography can contain error flows of the Digitalized Choreography:

- The Service Level Agreement of the Business Process is violated e.g. handling of a case takes more time than promised, the citizen involved is informed of the situation and his or her rights.

- Human and/or System failures e.g. how to recover (at the Business level) from an IT system breakdown

The design of a Choreography should contain business level SLAs.

Work-in-progress

Align with CEN TC440 work

Log

Date	Version	Author	Remarks
01.12.2017	0.90	Klaus Vilstrup Pedersen	First version

Version: 0.9.0	EIF layer: Semantic
Type: Architectural Building Block ABB (Arkitektur komponent)	Continuum Generic <-----+-----> Solution

Description

An **e-Document** is any electronic document, structured or unstructured, which supports various formats and it is support functionality that fulfils a set of generic, domain or use case specific requirements.

Thus an e-Document carries information as payload and supports functions to be used in processing.

There are two parties or roles involved in an e-Document transaction, an e-Document producer and an e-Document consumer.

The **producer** is responsible for creating and maintaining an e-Document. Different actors can be associated with the producer's role, such as the authors, contributors or document signers.

The e-Document **consumer** is acting on the e-Document with the purpose of processing it accordingly to needs. A consumer may be a computer system that automatically processes the e-Document as well as an end-user.

To guarantee the interoperability, the data protection and data privacy, a binding specification must exist between the producer and the consumer. By specification the two parties are agreeing upon the e-Document exchange semantics and format.

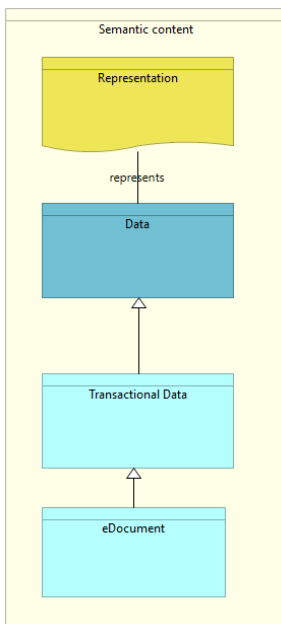
Requirements

SAT-eDelivery_Requirements:

eDel-Org01, eDel-Org03, eDel-Org06

Specification

The eDocument is a specialization of the EIRA 2.0 Building Block "Representation". "Data", "Transactional Data"



See <https://joinup.ec.europa.eu/release/eira/v200> for definitions of Architectural Building Blocks in EIRA 2.0.

eDelivery definition (specialization of the EIRA 2.0 definition) of :

Representation

The perceptible form of the information carried by a business object. If relevant, representations can be classified in various ways; for example, in terms of medium (electronic, paper, audio, etc.) or format (HTML, ASCII, PDF, RTF, etc.).

This ABB is a key interoperability enabler(*) for assessing compatible interpretations of Data.

Source: ArchiMate® v3

<http://pubs.opengroup.org/architecture/archimate3-doc/chap08.html>

(*)DECISION (EU) 2015/2240 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015 establishing a programme on interoperability solutions and common frameworks for European public administrations, businesses and citizens (ISA2 programme) as a means for modernising the public sector

Data

Home/Hjem: [Hjemmeside](#)

[SAT for eDelivery](#)

[SAT-eDelivery](#)

[SAT-eDelivery_Requirements](#)

[ABBs for eDelivery](#)

Legal level

[ABB-eIDAS_Regulation](#)

Organizational level

[ABB-](#)

[eDelivery_Interoperability_Agreemen](#)

[ABB-Business_Process_Choreograph](#)

Semantic level

[ABB-eDocument](#)

Technical level

[ABB-Backend_Integration](#)

[ABB-Access_Point](#)

[ABB-Message_Exchange](#)

[ABB-Capability_LookUp](#)

[ABB-eDelivery_Trust](#)

TBD - Work in Progress

[Adress_LookUp](#)

[Addressing_Entities](#)

[Non_Repudiation](#)

Data is facts represented as text, numbers, graphics, images, sound, or video. Data is the raw material used to represent information, or from which information can be derived.

This ABB is a key interoperability enabler (*) enabling for sharing/PROVISIONING and reusing/CONSUMING Data.

Based on Data Management Body Of Knowledge (DAMA DM_BOK) First edition

<http://www.dama.org>

(*)DECISION (EU) 2015/2240 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015 establishing a programme on interoperability solutions and common frameworks for European public administrations, businesses and citizens (ISA2 programme) as a means for modernising the public sector

Transactional Data

Data that covers the business information related to business transactions and information exchanges .

Based on DAMA DM_BOK

<http://www.dama.org>

eDocument

An electronic document, structured or unstructured, which supports various formats and it is support functionality that fulfils a set of generic, domain or use case specific requirements.

Standards/profiles

Profile	Link	Standard	Description	Status
OpenPEPPOL-SBDH	https://github.com/OpenPEPPOL/documentation/blob/master/TransportInfrastructure/ICT-Transport-OpenPEPPOL-Envelope_Specification-100_2014-01-15.pdf	UN/CEFACT SBDH		
ASIC				

Recommendations

A best practice of the specification of eDocuments can be found at TC----

Work-in-progress

Upcoming new standard UNCEFACT/OASIS XHE on Envelope header, based on UN/CEFACT SBDH and OASIS BDE. Finalization and publication date unknown.

References

eSENS eDocument: <http://wiki.ds.unipi.gr/display/ESENS/SAT+++eDocument++0.6.0>

GS1 resources: <https://www.gs1.org/standard-business-document-header-sbdh>

OpenPEPPOL SBDH profile: <https://vefa.difi.no/bb/standard/sbdh/>

eSENS SBDH profile: <http://wiki.ds.unipi.gr/display/ESENS/PR+++SBDH>

eSENS ASIC profile: <http://wiki.ds.unipi.gr/display/ESENS/PR+++eSENS+Container>

Log

Date	Version	Author	Remarks
01.12.2017	0.90	Klaus Vilstrup Pedersen	First version

Version: 0.9.0	EIF layer: Technical
Type: Architectural Building Block ABB (Arkitektur komponent)	Continuum Generic<-----+---->Solution

Description

The eDelivery Access Point (AP) implements the participation in one or more eDelivery virtual Communities. The Access Point can have one of two roles in a Business transaction: Sender or Receiver.

As a Sender it uses the "Location LookUp" (TBD) to find the IP adress of the "Capability LookUp".

The Sender then uses the "Capability LookUp" ([ABB-Capability_LookUp](#)) to check Receivers Legal, Organizational, Semantic and Technical Capabilities for the Transaction and uses the Technical Capabilities to configure the Message Exchange and the IP adress of the Receiver.

The Certificate of the Virtual Community Trust ([ABB-eDelivery_Trust](#)) is added to the Message and a Message Exchange ([ABB-Message_Exchange](#)) with a Receiver is performed.

As a Receiver the receives the Message through the Message Exchange ([ABB-Message_Exchange](#)) and the Certificate of the Virtual Community Trust ([ABB-eDelivery_Trust](#)) is verified.

Requirements

SAT-eDelivery_Requirements

Se individual ABBs:

Specification

The Access Point is a specialization of the EIRA 2.0 Building Block "Application Service" in the Technical Application layer:

Home/Hjem: [Hjemmeside](#)

SAT for eDelivery

[SAT-eDelivery](#)

[SAT-eDelivery_Requirements](#)

ABBs for eDelivery

Legal level

[ABB-eIDAS_Regulation](#)

Organizational level

[ABB-eDelivery_Interoperability_Agreement](#)
[ABB-Business_Process_Choreography](#)

Semantic level

[ABB-eDocument](#)

Technical level

[ABB-Backend_Integration](#)

[ABB-Access_Point](#)

[ABB-Message_Exchange](#)

[ABB-Capability_LookUp](#)

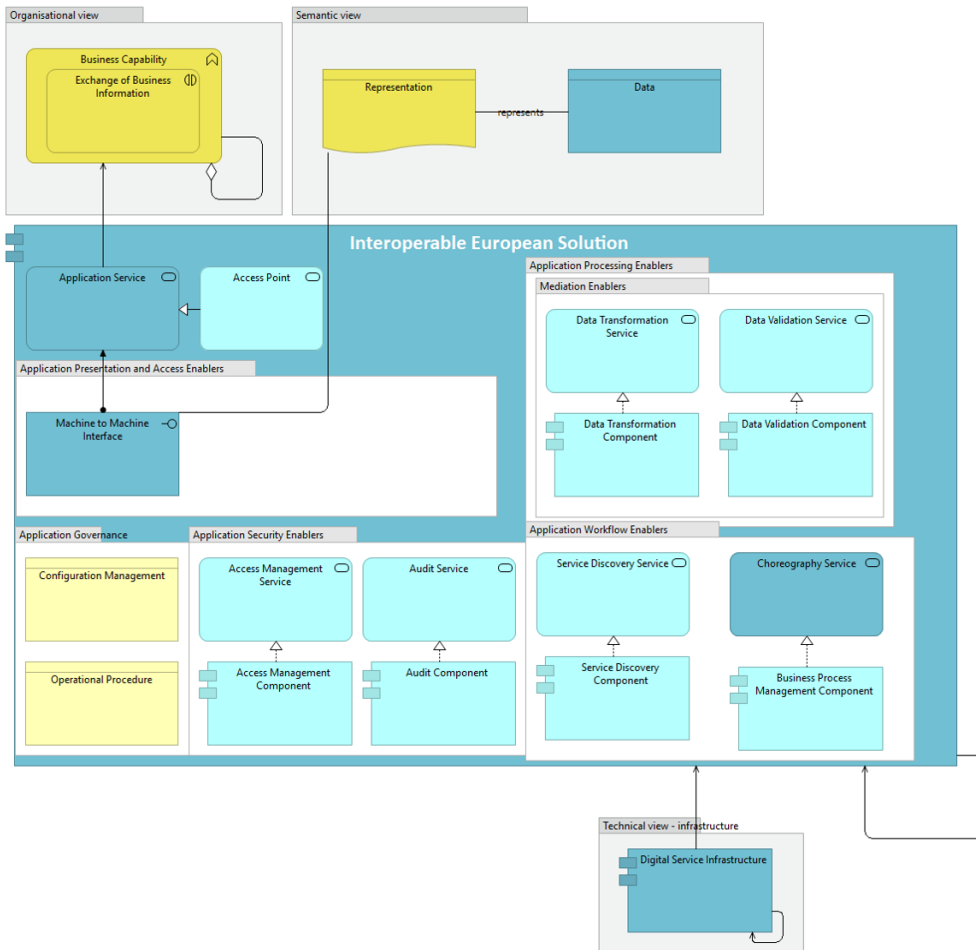
[ABB-eDelivery_Trust](#)

TBD - Work in Progress

[Adress_LookUp](#)

[Addressing_Entities](#)

[Non_Repudiation](#)



See <https://joinup.ec.europa.eu/release/eira/v200> for definitions of Architectural Building Blocks in EIRA 2.0.

eDelivery definition (specialization of the EIRA 2.0 definition) of:

Application Service

Represents an explicitly defined shared application behavior.

Based on ArchiMate v3

<http://pubs.opengroup.org/architecture/archimate3-doc/chap09.html>

Access Point

An access point is an application that can incorporate Mediation enablers, Application Governance, Application Security enablers and Application Workflow enablers.

The Access Point can play two roles in an eDelivery exchange: Sender or Receiver.

As a sender:

1. The message is received from the Backend system through the Backend integration [ABB-Backend_Integration](#)
2. The message can be transformed and validated through Mediation enablers
3. Package the message as an eDocument [ABB-eDocument](#)
4. Then uses the "Capability LookUp" ([ABB-Capability_LookUp](#)) to check Receivers Legal, Organizational, Semantic and Technical Capabilities for the Transaction and uses the Technical Capabilities to configure the Message Exchange and the IP adress of the Receiver.
5. Adds the Virtual Community Trust ([ABB-eDelivery_Trust](#)) to the eDocument
6. Sends the eDocument through the "Message Exchange" [ABB-Message_Exchange](#) to the Receiver

As a Receiver

1. Receives an eDocument from the [ABB-Message_Exchange](#)
2. Verifies the Virtual Community Trust ([ABB-eDelivery_Trust](#)) to the eDocument

3. The message can be transformed and validated through Mediation enablers
4. Act as store until Backend system is ready to consume the eDocument through the Backend integration [ABB-Backend_Integration](#)

Standards/profiles

Profile	Link	Standard	Description	Status
-				

[Recommendations](#)

Currently Access Points is available both as Open Source and Commercial Vendor implementations - check at DIFI for solutions that fulfill your requirements.

[Work-in-progress](#)

-

[Log](#)

Date	Version	Author	Remarks
01.12.2017	0.90	Klaus Vilstrup Pedersen	First version

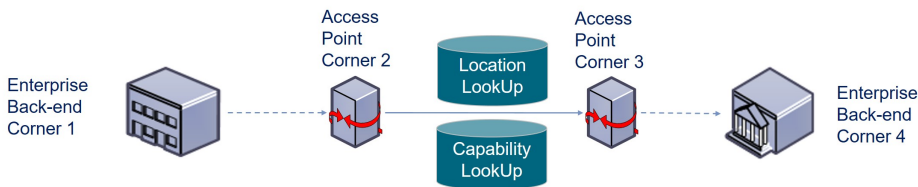
ABB-Backend_Integration

Home/Hjem: [Hjemmeside](#)

Version: 0.9.0	EIF layer: Technical
Type: Architectural Building Block ABB (Arkitektur komponent)	Continuum Generic<-----+----->Solution

Description

This ABB relates to the eDelivery 4-corner model and addresses the Communication/Integration of Corner1-Corner2/Corner3-Corner4.



The 4-corner model creates a very flexible architecture, where the enterprises can make their own decisions on how to integrate the external Business Process Choreography component into their own IT-architecture orientation.

From the backend perspective there is 4 ways of integration of Corner1-Corner2/Corner3-Corner4

<p>Enterprise Back-end Access Point</p>	<p>Tightly Coupling</p> <p>Back-end system and Access Point is tightly coupled i.e. The Back-end system has integrated the Access Point into the Back-end system. One Access Point handles the eDelivery of one Back-end System.</p>
<p>Enterprise Back-end Access Point</p>	<p>Semi-Tightly Coupling</p> <p>Back-end system and Access Point is semi-tightly coupled i.e. The Back-end system and the Access Point is internally loosely coupled, but part of the same internal IT-Architecture and IT-Infrastructure or the Access Point is an Internal Cloud solution. One Access Point can handle the eDelivery of several Back-end Systems.</p>
	<p>Loose Coupling Coupling</p> <p>The Back-end system and the Access Point is loosely coupled and not part of the same internal</p>

[SAT for eDelivery](#)

[SAT-eDelivery](#)

[SAT-eDelivery_Requirements](#)

[ABBs for eDelivery](#)

Legal level

[ABB-eIDAS_Regulation](#)

Organizational level

[ABB-](#)

[eDelivery_Interoperability_Agreement](#)

[ABB-Business_Process_Choreography](#)

Semantic level

[ABB-eDocument](#)

Technical level

[ABB-Backend_Integration](#)

[ABB-Access_Point](#)

[ABB-Message_Exchange](#)

[ABB-Capability_LookUp](#)

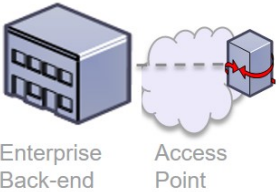
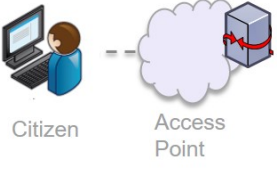
[ABB-eDelivery_Trust](#)

TBD - Work in Progress

[Adress_LookUp](#)

[Addressing_Entities](#)

[Non_Repudiation](#)

 <p>Enterprise Back-end Access Point</p>	<p>IT-Architecture and IT-Infrastructure. One Access Point can handle the eDelivery of many Back-end Systems from many Enterprises. This model accomodate the use of Service-/Cloud providers, where the interaction between the Back-end system and the Cloud is determined by the Architecture and Infrastructure of the Service/Cloud provider.</p>
 <p>Citizen Access Point</p>	<p>Loose Coupling (Citizen)</p> <p>The Citizen can send and receive eDocuments through the use of Service-/Cloud providers, where the interaction between the Citizen and the Service-/Cloud provider is determined by the setup of the architecture and infrastructure of the Service/Cloud provider.</p>

In the case of Loose Coupling, there's special issues related to Corner1/Corner4 when dealing with Non-repudiation, since this is End-to-End. Corner1 must pack and encrypt the original message and only Corner4 can reply with an encrypted message. Corner 2 and Corner 3 is not allowed to repack, delete or add to the message, only act as a routing mechanism.

Requirements

SAT-eDelivery_Requirements:

InfEx-Org01, eDEL-Org04, eDEL-Org08, eDEL-Org09, eDEL-Org010, eDEL-Org11, eDEL-Org12, eDel-Tec013

Specification

None

Standards/profiles

Profile	Link	Standard	Description	Status
-	-	-	-	-

Recommendations

In a SOA-oriented or API-oriented IT-architecture, the Access point can be seen as an External Business Process Choreography Service on the Task/Entity-layer or System-layer:

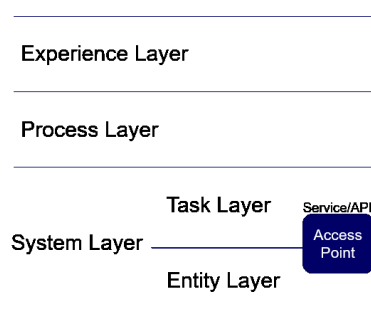
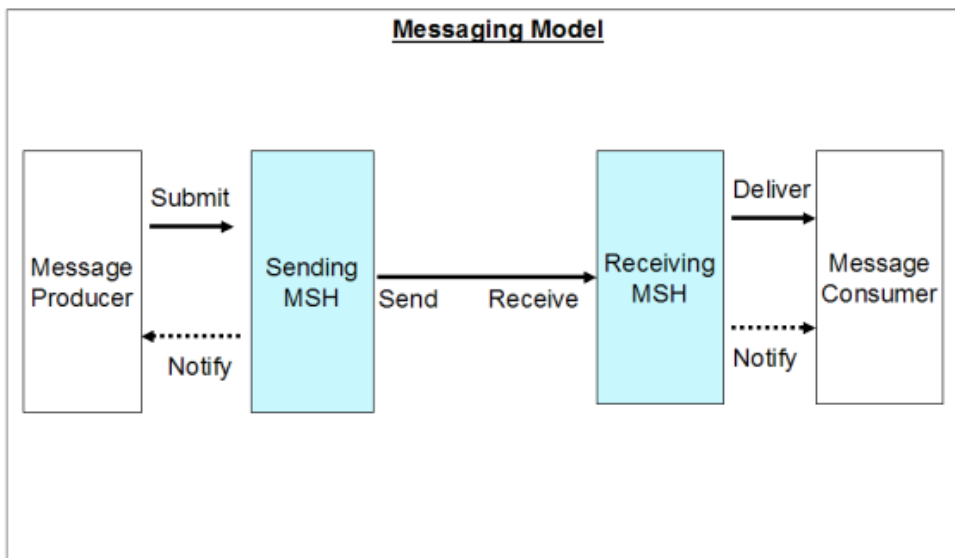


ABB-Message_Exchange

Version: 0.9.0	EIF layer: Technical
Type: Architectural Building Block ABB (Arkitektur komponent)	Continuum Generic<----->Solution

Description

The Message Exchange provides secure and reliable exchange of single or groups of payloads in any structured or unstructured format. It is designed to support both One Way and Two Way (Request-Response) exchanges. The ABB can be used in four-corner topologies or in point-to-point exchanges. In four-corner topologies, only the interconnect hop (Corner2 to Corner3) is in scope as the edge hops may use other message protocols.



Requirements

SAT-eDelivery_Requirements

eDel-Org04, eDel-Org05, eDel-Org06, eDEL-Org07, eDEL-Org08, eDel-Sem01, eDel-Sem02, eDel-Sem03, eDel-Tec01, eDel-Tec013

Specification

The "Message Exchange Service" is a specialization of the EIRA 2.0 Building Blocks "Data Exchange Service".

Home/Hjem: [Hjemmeside](#)

[SAT for eDelivery](#)

[SAT-eDelivery](#)

[SAT-eDelivery_Requirements](#)

[ABBs for eDelivery](#)

Legal level

[ABB-eIDAS_Regulation](#)

Organizational level

[ABB-](#)

[eDelivery_Interoperability_Agreement](#)

[ABB-Business_Process_Choreography](#)

Semantic level

[ABB-eDocument](#)

Technical level

[ABB-Backend_Integration](#)

[ABB-Access_Point](#)

[ABB-Message_Exchange](#)

[ABB-Capability_LookUp](#)

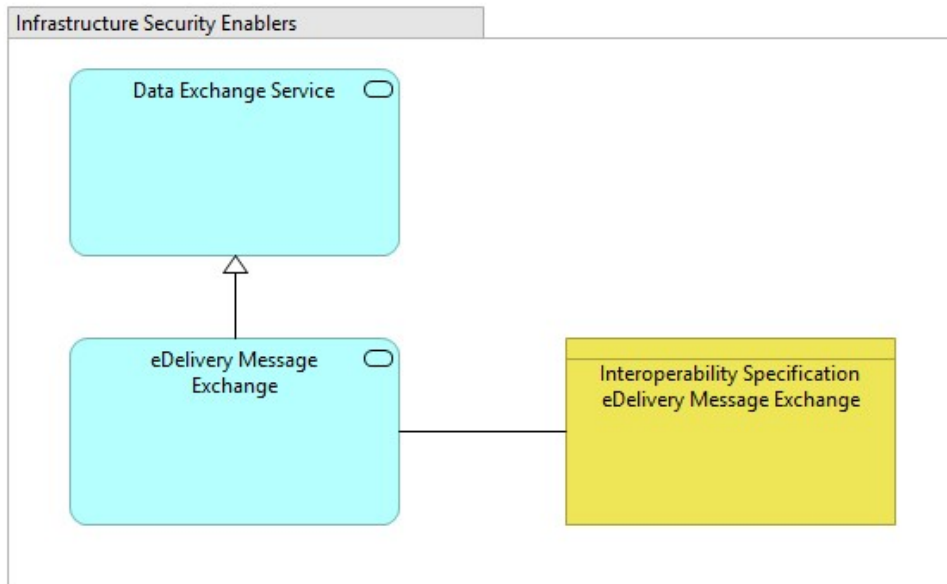
[ABB-eDelivery_Trust](#)

TBD - Work in Progress

[Adress_LookUp](#)

[Addressing_Entities](#)

[Non_Repudiation](#)



See <https://joinup.ec.europa.eu/release/eira/v200> for definitions of Architectural Building Blocks in EIRA 2.0.

eDelivery definition (specialization of the EIRA 2.0 definition) of:

Data Exchange Service

Shares the functionality that enables the secure exchange of messages, records, forms and other kinds of data between different ICT systems. This includes data routing, except endpoint discovery.

Based on EIFv2

http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf

eDelivery Message Exchange Service

Shares the functionality that enables the secure exchange of messages between two Access Points.

The standard(s) or profiles of standard(s) is compliant with CEF eDelivery recommendations (<https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/All+CEF+eDelivery+services>)

eDelivery Message Exchange Interoperability Specification

Specifies the functionality that enables the secure exchange of messages between two Access Points.

The standard(s) or profiles of standard(s) is compliant with CEF eDelivery recommendations (<https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/All+CEF+eDelivery+services>)

Standards/profiles (eDelivery)

Profile	Link	Standard	Description	Status
OpenPEPPOL AS2 profile	https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Access+Point+specifications	IETF AS2		Production
eSENS AS4	https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Access+Point+specifications	OASIS AS4 (OASIS ebMS 3.0)	OASIS AS4 is a profile of OASIS ebMS 3.0	Phase-in

Recommendations

-

Work-in-progress

-

Log

Date	Version	Author	Remarks

01.12.2017	0.90	Klaus Vilstrup Pedersen	First version

Version: 0.9.0	EIF layer: Technical
Type: Architectural Building Block ABB (Arkitektur komponent)	Continuum Generic<-----+---->Solution

Description

Capability Lookup is a technical service to accommodate a dynamic and flexible interoperability community. A capability lookup can provide metadata on the What, How and Where. What are the communication partner's interoperability capabilities, How are these Capabilities implemented through Service features and Where are the Service to be found. The metadata can be used to dynamically set interoperability parameters and ambitions between the sender and receiver.

A Capability Lookup service is owned by the communication receiver and it expresses the receiver's interoperability capabilities::

Legal Capability

- What are the legal restrictions on the specific digital interoperability

Organisational Capability

- What Digitalized Business choreographies can the receiver participate in.
- What is the Business role of the receiver

Semantic Capability and Feature

- What is the semantics and formats of the information transferred in a Business transaction of a the Business Choreography

Technical Capability and Features

- What are the options and How should the Service be accessed, when it comes to Security, Evidence, Trust, Protocols
- Where is the Service to be found (Location)

In the context of setting up an interoperability connection with a Business partner, the sender needs to dynamically resolve the settings e.g. Legal, Organizational, Semantic and Technical capabilities and constraints. The recipient published the Receiving Capabilities in the Capability_LookUp service and by requesting the meta data, the sender can adopt and choose the most optimal settings and Capabilities.

Requirements

[SAT-eDelivery_Requirements:](#)

eDel-Org09, eDel-Org10, eDel-Org11, eDel-Tec02

Specification

The Capability LookUp is a specialization of the EIRA 2.0 Building Block "Metadata Management Service", "Metadata Management Component" in the Technical Infrastructure layer:

Home/Hjem: [Hjemmeside](#)

[SAT for eDelivery](#)

[SAT-eDelivery](#)

[SAT-eDelivery_Requirements](#)

[ABBs for eDelivery](#)

Legal level

[ABB-eIDAS_Regulation](#)

Organizational level

[ABB-](#)

[eDelivery_Interoperability_Agreement](#)

[ABB-Business_Process_Choreography](#)

Semantic level

[ABB-eDocument](#)

Technical level

[ABB-Backend_Integration](#)

[ABB-Access_Point](#)

[ABB-Message_Exchange](#)

[ABB-Capability_LookUp](#)

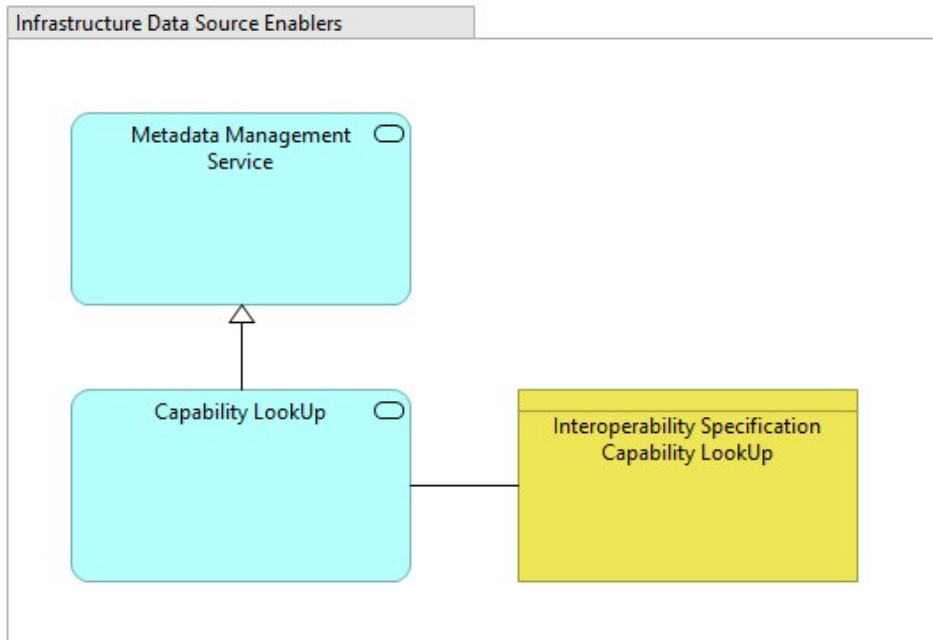
[ABB-eDelivery_Trust](#)

TBD - Work in Progress

[Adress_LookUp](#)

[Addressing_Entities](#)

[Non_Repudiation](#)



See <https://joinup.ec.europa.eu/release/eira/v200> for definitions of Architectural Building Blocks in EIRA 2.0.

eDelivery definition (specialization of the EIRA 2.0 definition) of:

Metadata Management Service

Shares the functionalities for the i) creation, ii) storage, iii) categorisation and iv) retrieval of metadata.

Based on DAMA <http://www.dama.org/>

Capability LookUp

Shares the functionalities for the i) creation, ii) storage, iii) categorisation and iv) retrieval of metadata for a Service on Legal, Organisational, Semantic and Technical Capabilities

Capability LookUp Interoperability Specification

Specifies the functionality for Capability LookUp.

The standard(s) or profiles of standard(s) is compliant with CEF eDelivery recommendations (<https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/All+CEF+eDelivery+services>)

Standards/profiles

The standard(s) or profiles of standard(s) is compliant with CEF eDelivery recommendations (<https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/All+CEF+eDelivery+services>)

Profile	Link	Standard	Description	Status
SMP	http://docs.oasis-open.org/bdx/bdx-smp/v1.0/os/bdx-smp-v1.0-os.html	OASIS SMP		

Recommendations

-

Work-in-progress

-

References

-

Log

Date	Version	Author	Remarks
01.12.2017	0.90	Klaus Vilstrup Pedersen	First version

Version: 0.9.0	EIF layer: Technical
Type: Architectural Building Block ABB (Arkitektur komponent)	Continuum Generic<-----+---->Solution

Description

The eDelivery Trust is what holds an eDelivery community together. A PKI serves as the "ticket" for the participants belonging to a specific eDelivery. When sending a message to another participant in the eDelivery community, the PKI must accompany the message as proof that this message was from a participant in the eDelivery community.

This Trust Establishment Model is based on using a single PKI issuing Certificates for all members of a Trust Domain (TD). The PKI may be a hierarchical one, having different sub CAs for different types of Trust Services Providers (TSPs) allocated to the Trust Domain.

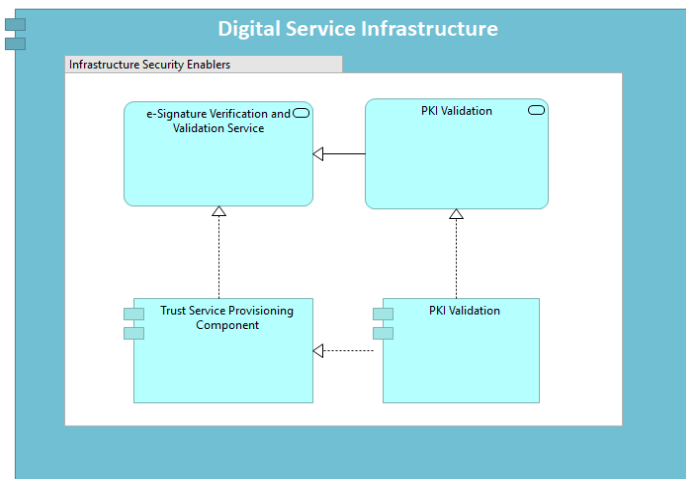
Requirements

SAT-eDelivery_Requirements:

eDel-Org01, eDel-Org03, eDel-Org06

Specification

The eDelivery Trust is created through a PKI infrastructure, where the PKI validation service, that is a specialization of the EIRA 2.0 Building Block "e-Signature Verification and Validation Service" implemented as a PKI validation component, that is a specialization of "Trust Service Provisioning Component" in the Technical Infrastructure layer:



See <https://joinup.ec.europa.eu/release/eira/v200> for definitions of Architectural Building Blocks in EIRA 2.0.

eDelivery definition (specialization of the EIRA 2.0 definition) of:

e-Signature Verification and Validation Service

Shares the functionality of the verification of documents that are signed electronically.

An 'electronic signature' means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.

'validation' means the process of verifying and confirming that an electronic signature or a seal is valid.

Based on eIDAS - REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

Trust Service Provisioning Component

Implements the functionalities encapsulating the trust services functionalities.

A 'trust service' means an electronic service normally provided for remuneration which consists of these functionalities:

- the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or
- the creation, verification and validation of certificates for website authentication; or
- the preservation of electronic signatures, seals or certificates related to those services.

Based on eIDAS - REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

The standard(s) or profiles of standard(s) is compliant with CEF eDelivery recommendations (<https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/All+CEF+eDelivery+services>)

[Home/Hjem: Hjemmeside](#)

[SAT for eDelivery](#)

[SAT-eDelivery](#)

[SAT-eDelivery_Requirements](#)

[ABBs for eDelivery](#)

Legal level

[ABB-eIDAS_Regulation](#)

Organizational level

[ABB-](#)

[eDelivery_Interoperability_Agreement](#)

[ABB-Business_Process_Choreography](#)

Semantic level

[ABB-eDocument](#)

Technical level

[ABB-Backend_Integration](#)

[ABB-Access_Point](#)

[ABB-Message_Exchange](#)

[ABB-Capability_LookUp](#)

[ABB-eDelivery_Trust](#)

TBD - Work in Progress

[Adress_LookUp](#)

[Addressing_Entities](#)

[Non_Repudiation](#)

Standards/profiles

The standard(s) or profiles of standard(s) is compliant with CEF eDelivery recommendations
(<https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/All+CEF+eDelivery+services>)

Profile	Link	Standard	Description	Status
PKI	https://github.com/OpenPEPPOL/documentation/blob/master/TransportInfrastructure/ICT-Transport-Trust_Network_Certificate_Policy-2.00.pdf			

Recommendations

-

Work-in-progress

-

References

PKI explained: <https://peppol.helger.com/public/menuitem-docs-peppol-pki>

Log

Date	Version	Author	Remarks
01.12.2017	0.90	Klaus Vilstrup Pedersen	First version