eDelivery Tutorial

How can CEF help you set-up your eDelivery infrastructure?

November 2016

Version Control

Version	Date	Created by	Description
V1.2	November 2016	CEF Project & Architecture Office	Final draft for publication

Table of content

- Introduction
- Introduction to message exchange infrastructures
  - Message Exchange Models
    - Topologies
    - Protocols
    - Integration approach
  - Discovery Models
  - Security Models
    - Trust circles
    - Security controls
- Technical Specifications
- Sample Implementations
- End

Benefits with an impact

10 TOP PRIORITIES OF THE EC

Jobs, growth and investments

Digital Single Market

Energy Union and Climate

Internal market

A deeper and fairer economic and monetary union

A balanced EU-US free trade agreement

Justice and fundamental rights

Migration

A stronger global actor

Democratic change

PROBLEM

- Europeans often face barriers when using online tools and services
- At present, markets are largely domestic in terms of online services
- Only 7% of EU small- and medium-sized businesses sell cross-border

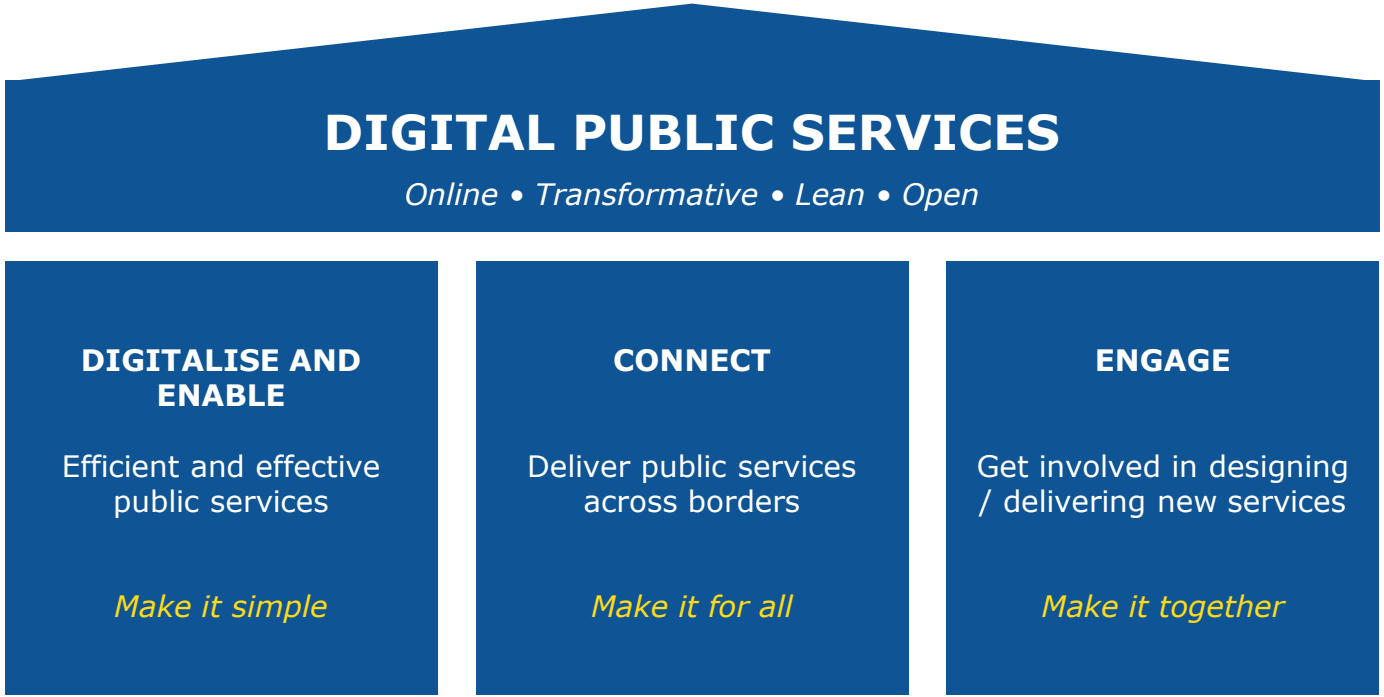
SOLUTION

- This includes common EU data protection, copyright rules, boosting digital skills, accessible online content
- …and **Cross-border Digital Public services** (CEF Digital)

CONSEQUENCE

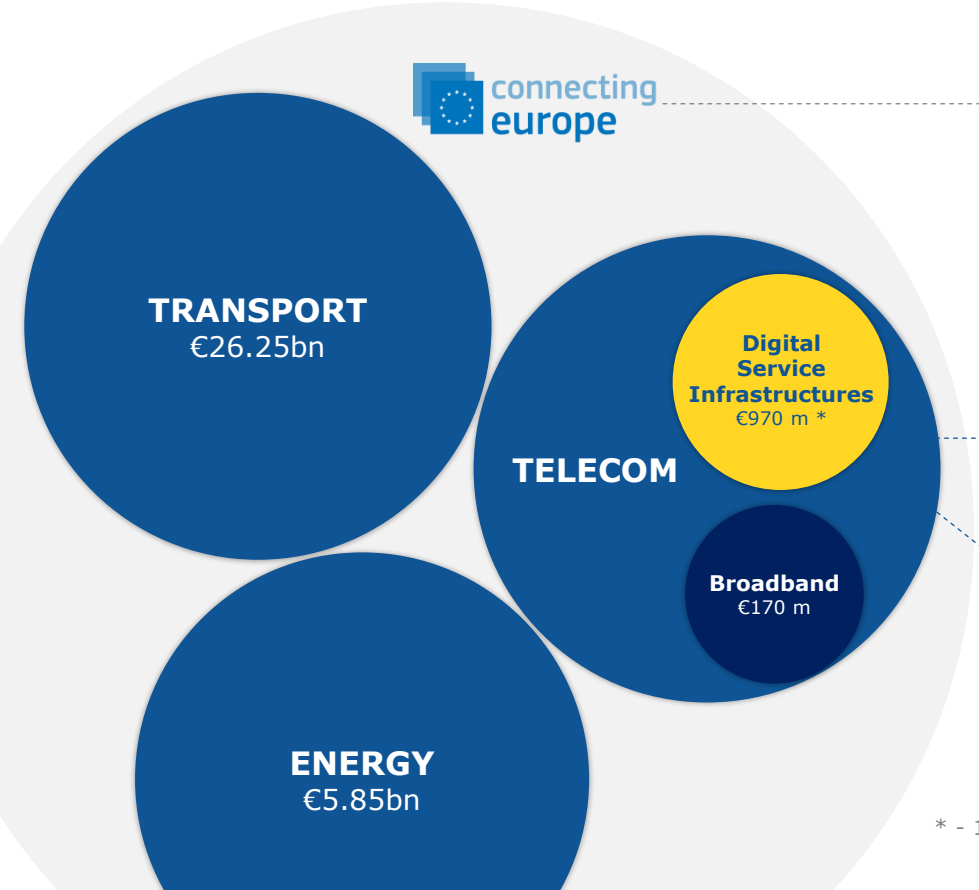
- Maximise economic potential, growth/jobs – anticipated to be 415€ billion to EU economy

Political support in the eGovernment Action Plan 2016 - 2020



ACTION 6: The Commission will use the common building blocks such as CEF DSIs

What is CEF



HOW IS IT REGULATED?

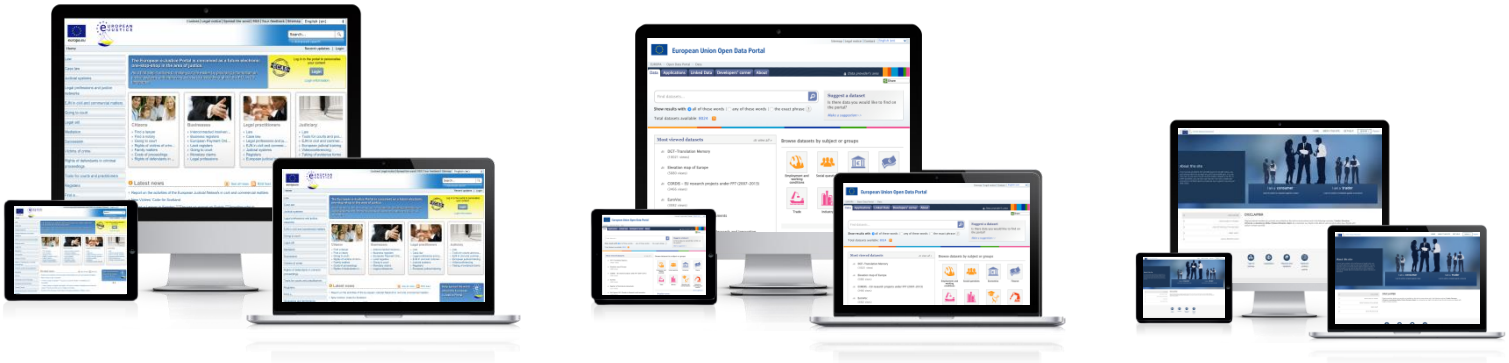
CEF Regulation
The Connecting Europe Facility (CEF) is a regulation that defines how the Commission can finance support for the establishment of trans-European networks to reinforce an interconnected Europe.

CEF Telecom Guidelines
The CEF Telecom guidelines cover the specific objectives and priorities as well as eligibility criteria for funding of broadband networks and Digital Service Infrastructures (DSIs).

CEF Work Programme
Translates the CEF Telecom Guidelines in general objectives and actions planned on a yearly basis.

* - 100 m Juncker Package

CEF Telecom – what does it finance



DIGITAL SERVICE INFRASTRUCTURES (DSIs)

EUROPEAN COMMISSION

MEMBER STATES

CORE SERVICE PLATFORM
(Services offered by the European Commission)

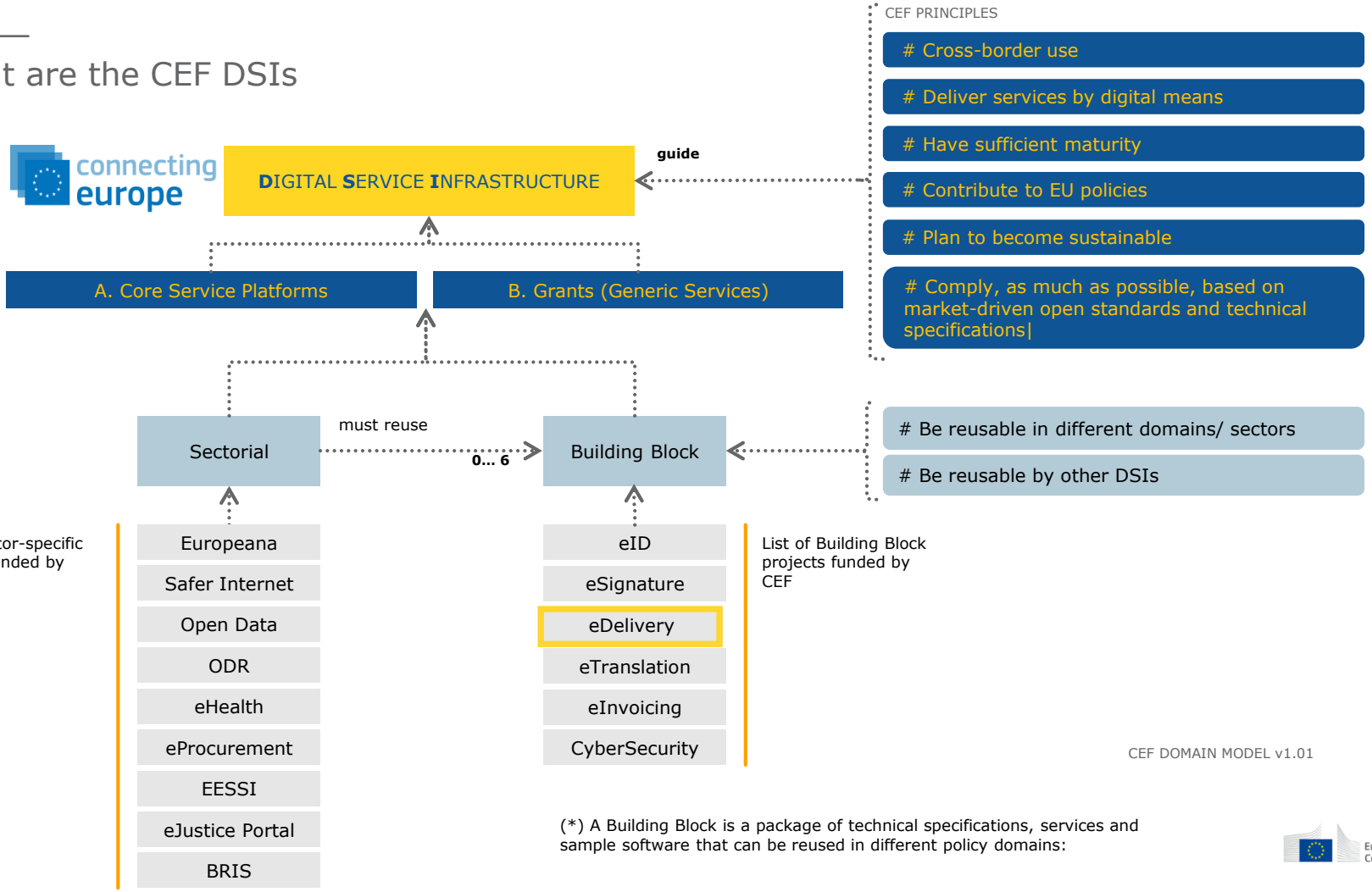
https://ec.europa.eu/cefdigital/wiki/x/QAFfAQ

GENERIC SERVICES
(Grants for projects in the Member States)

https://ec.europa.eu/inea/connecting-europe-facility/cef-telecom

European Commission

What are the CEF DSIs

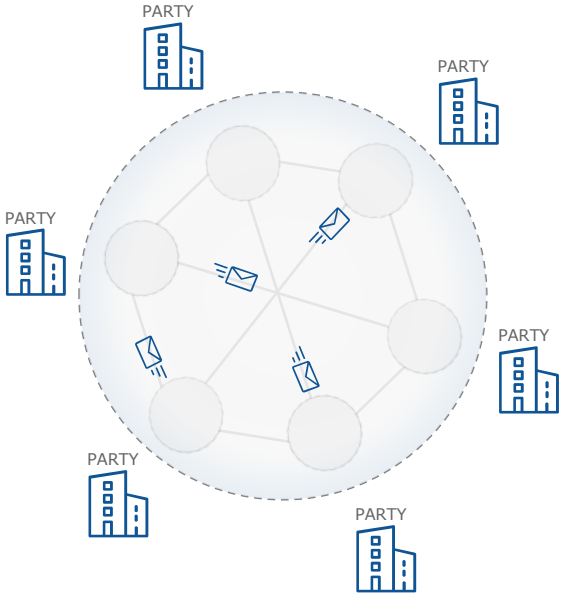


(*) A Building Block is a package of technical specifications, services and sample software that can be reused in different policy domains:

European Commission

What is eDelivery

- eID
- **eDelivery**
- eInvoicing
- eSignature
- eTranslation



eDelivery enables you to securely exchange data and documents

Deploying CEF eDelivery – today's focus

Domain Owner

Participants in eDelivery Messaging Infrastructure

PHASE

ELICIT requirements

DESIGN eDelivery infrastructure

SELECT eDelivery solutions

DEPLOY eDelivery solutions

INTEGRATE with backend(s) / with partners

OPERATE eDelivery solutions

CEF TEAM

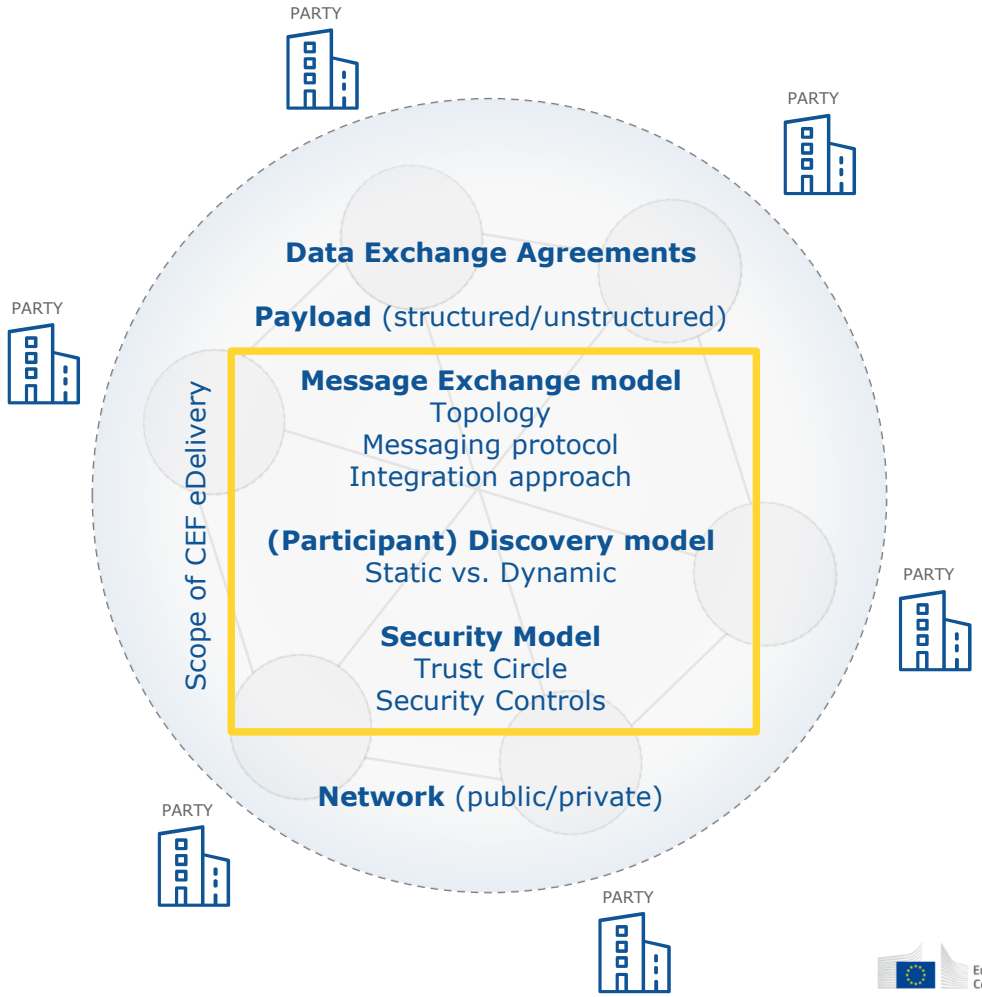
- Technical Specifications
- Onboarding
- Self-Assessment tool
- Documentation (COD, SOD, …)
- List of Software solutions
- SML Service
- PKI Service
- Service Desk
- Training and deployment
- Connectivity Testing
- Service Desk
- CEF eDelivery Community

YOUR TEAM

- Attend workshops • Complete self-assessment tool • Identify business requirements • Carry out feasibility study
- Design message exchange model • Design discovery model • Design security model • Participate in the writing of a SDD
- *Open source*: Assess OSS projects; Customise/ extend solution
- *Commercial solution*: Assess Vendors; Buy solution
- *Custom built*: Build solution
- Deploy components • Configure components
- Integrate with eDelivery Access Point • Perform Integration testing • Perform Pre-production testing
- Participate in Connectivity testing • Perform Pre-production testing
- *Open source*: Hosting • Maintenance
- *Commercial solution*: Hosting • Fees
- *Custom built*: Hosting • Maintenance

A message exchange infrastructure is

A combination of a message exchange model, discovery model and security model on top of the internet, or of a private network, to exchange structured or unstructured information encapsulated in messages.

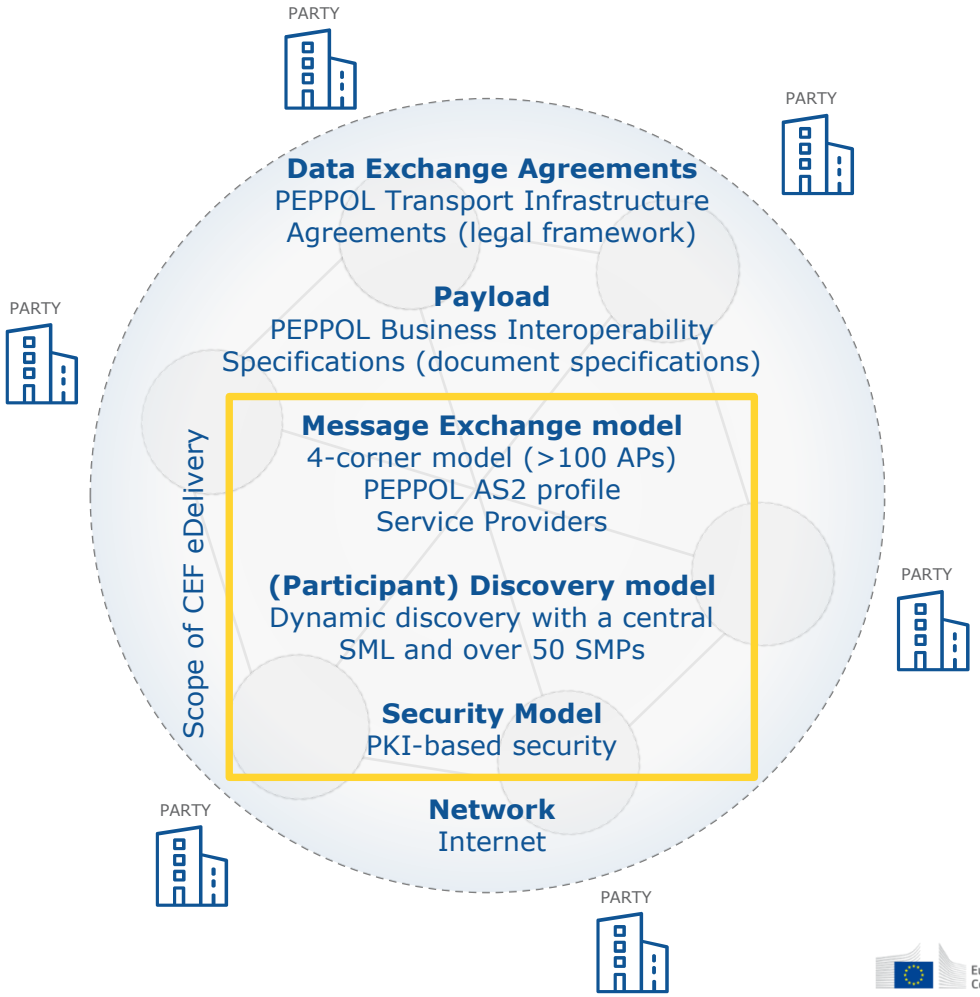


European Commission

The example of OpenPEPPOL

The Pan-European Public Procurement Online, the LSP of eProcurement, now transferred to the non-profit international association OpenPEPPOL.

The purpose of OpenPEPPOL is to enable European businesses to easily deal electronically with any European public sector buyers in their procurement processes, thereby increasing opportunities for greater competition for government contracts and providing better value for tax payers' money.

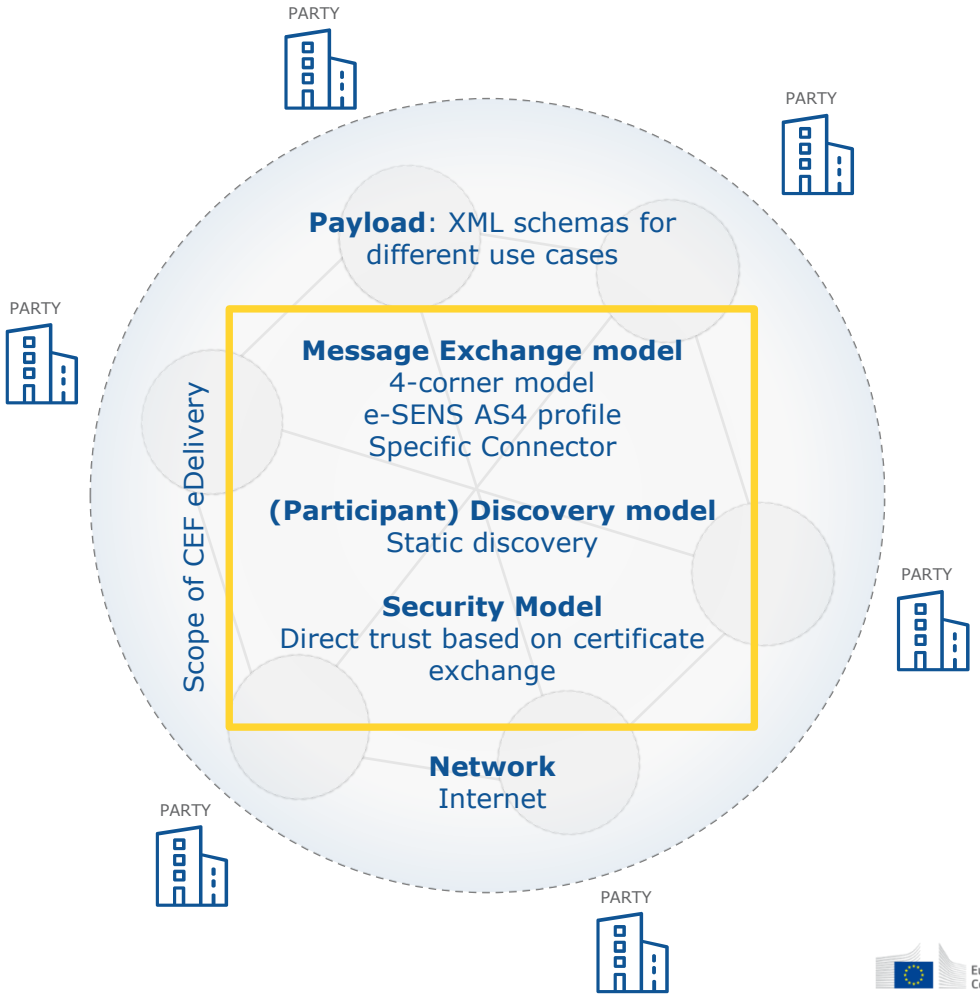


European Commission

The example of e-CODEX

The e-Justice Communication via Online Data Exchange, the LSP of eJustice, running until May 2016.

The e-CODEX project improves the cross-border access of citizens and businesses to legal means in Europe and furthermore creates the interoperability between legal authorities within the EU.



European Commission

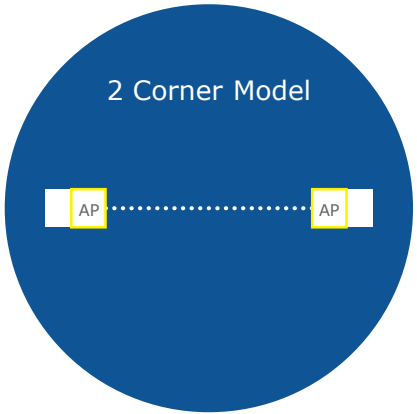
CEF eDelivery is not a one-size fits all solution

SCOPE OF CEF eDELIVERY

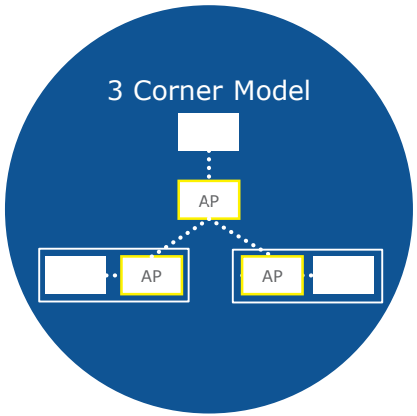
		PEPPOL	e-CODEX	**Your** CEF eDelivery implementation
EXCHANGE MODEL	TOPOLOGY	4-corner model	4-corner model	**Your** choice
	PROTOCOL	PEPPOL AS2 profile	e-SENS AS4 profile	e-SENS AS4 profile
	INTEGRATION APPROACH	Service Providers (Market)	Specific Connector	**Your** choice
DISCOVERY MODEL		Dynamic	Static	**Your** choice
SECURITY MODEL	TRUST CIRCLE	PKI	Mutual trust	**Your** choice
	SECURITY CONTROL	Liberal inner security	Inner security with connector	**Your** choice

- Introduction
- Introduction to message exchange infrastructures
  - Message Exchange Models
    - Topologies
    - Protocols
    - Integration approach
  - Discovery Models
  - Security Models
    - Trust circles
    - Security controls
- Technical Specifications
- Sample Implementations
- End

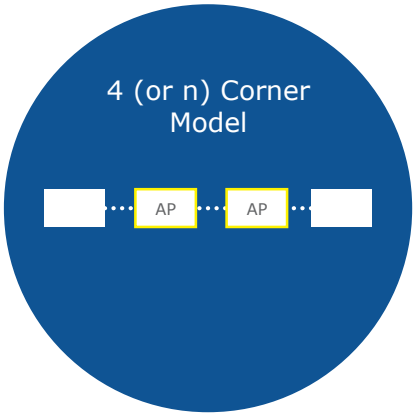
Message exchange topologies: Overview



Backend systems **communicate directly –** acting as Access Points - with each other



Backend systems don’t exchange data directly but are connected to the same **central hub (or Access Point**)



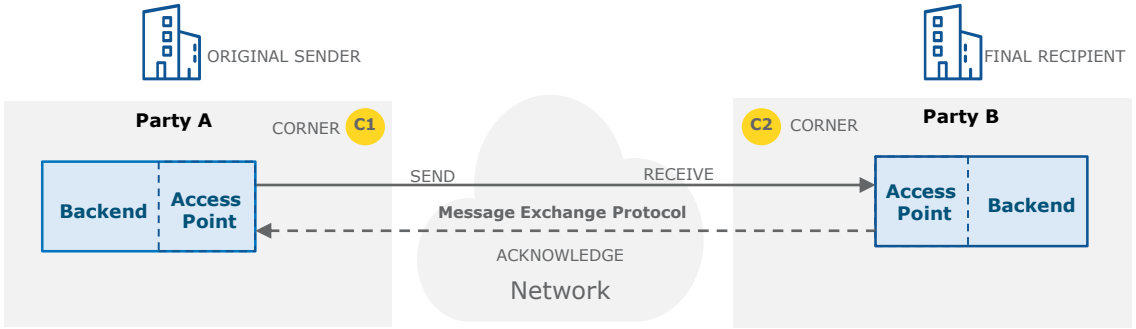
Backend systems don’t exchange data directly but through intermediary nodes (or **Access Points**)

2 Corner model in detail

In the 2 corner model, backend systems communicate directly with each other through a point-to-point connection.

As a result, there is a need to set-up bilateral channels between every participant (when there is no common messaging protocol) or change backend systems to support the common protocol and impact the backends.

This is also known as the **Fully connected network**.



PROS

- \+ Best suited for simple integration with few participants

CONS

- \- Not easily scalable
- \- Heavy impact on Backends

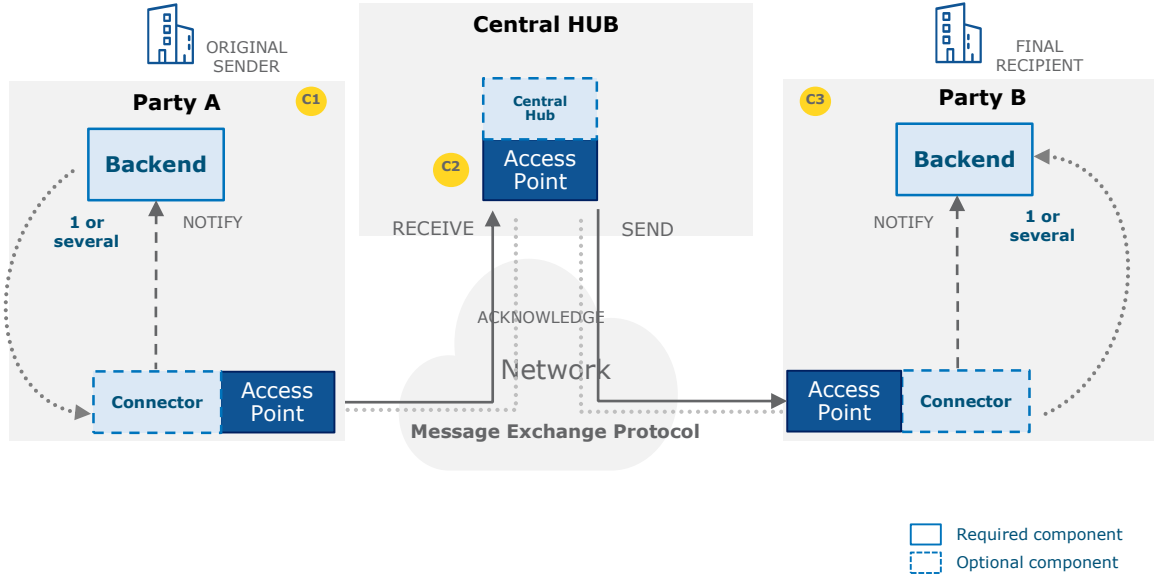
3 Corner model in detail

In the 3 corner model, backend systems communicate with each other through a central hub.

Thanks to the fully centralised approach, parties exchange messages with each other via the central hub in 2 steps:

- Party A exchanges information with the Central Hub
- Central Hub exchanges information with Party B

This is also known as the **Star network.**



PROS

- \+ No need to set up bilateral channels between participants.
- \+ Central management and control of all processes
- \+ Central monitoring processes

CONS

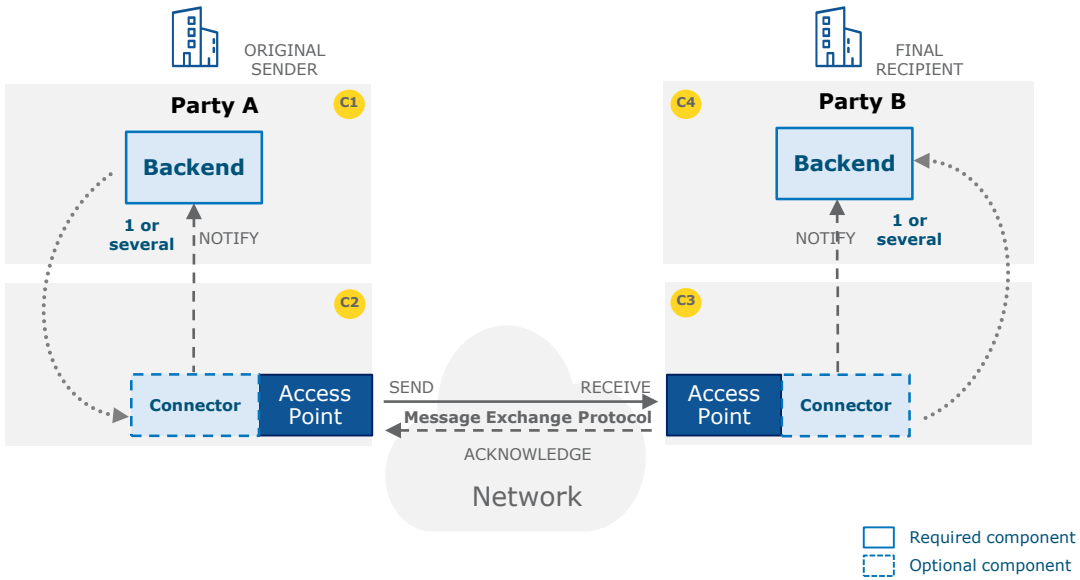
- \- Central Access Point may become a bottleneck/single point of failure in the network.
- \- Risk of service provider lock-in.
- \- Scalability.

4 Corner model in detail

In the 4 corner model, the backend systems of the users don't exchange data directly with each other but do this through Access Points. These Access Points are conformant to the same technical specifications and therefore capable of communicating with each other.

As a result, users can easily and safely exchange data even if their IT systems were developed independently from each other.

This is also known as the **Mesh network**



PROS

- \+ Eliminates risk of single point of failure
- \+ Eliminate risk of service provider lock-in

CONS

- \- Need to enhance security between Access Points
- \- Need to conform to common message exchange protocol

- Introduction
- Introduction to message exchange infrastructures
  - Message Exchange Models
    - Topologies
    - Protocols
    - Integration approach
  - Discovery Models
  - Security Models
    - Trust circles
    - Security controls
- Technical Specifications
- Sample Implementations
- End

Message exchange protocols

Scope of CEF eDelivery

	PREDECESSORS			AS4 based on WS*	RESTFUL
	Many protocols were developed around the concepts in Electronic Data Interchange (EDI) but over the internet, some of which address the needs of specific industries or regions.			WS* refers to a large set of specifications developed for standardizing aspects exchanging information using SOAP-based web services. ebMS3/AS4 is a profile based on WS* standards developed by OASIS.	REST refers to REpresentational State Transfer. It is a software architecture style, as well as a lightweight messaging protocol, for machine-to-machine information exchange directly using the network layer (HTTP).
NETWORK	SMP	HTTP	FTP	HTTP	HTTP
MESSAGING	AS1	AS2	AS3	SOAP 1.2 with attachments	
				ebMS3/AS4 WS-Security	
DATA	TEXT/MIME			XML	XML/JSON

Message exchange protocols: Pros and Cons

CEF eDelivery

	PREDECESSORS	AS4 based on WS*	RESTFUL
PROS	Automated data validation and confirmation of message sent	Additional WS* specifications to enhance security and reliability Payload agnostic	Stateful Performant, scalable and easy to deploy
CONS	Supports "One-way Push" only Many standards and regular revisions causing limited cross-interoperability and lock-in partnerships High set-up cost (direct integration into the business application)	Heavy-weight XML standard	Reliability and security are not standardised Only supports basic messaging patterns: "One-Way Push" and "Two-way Synch"

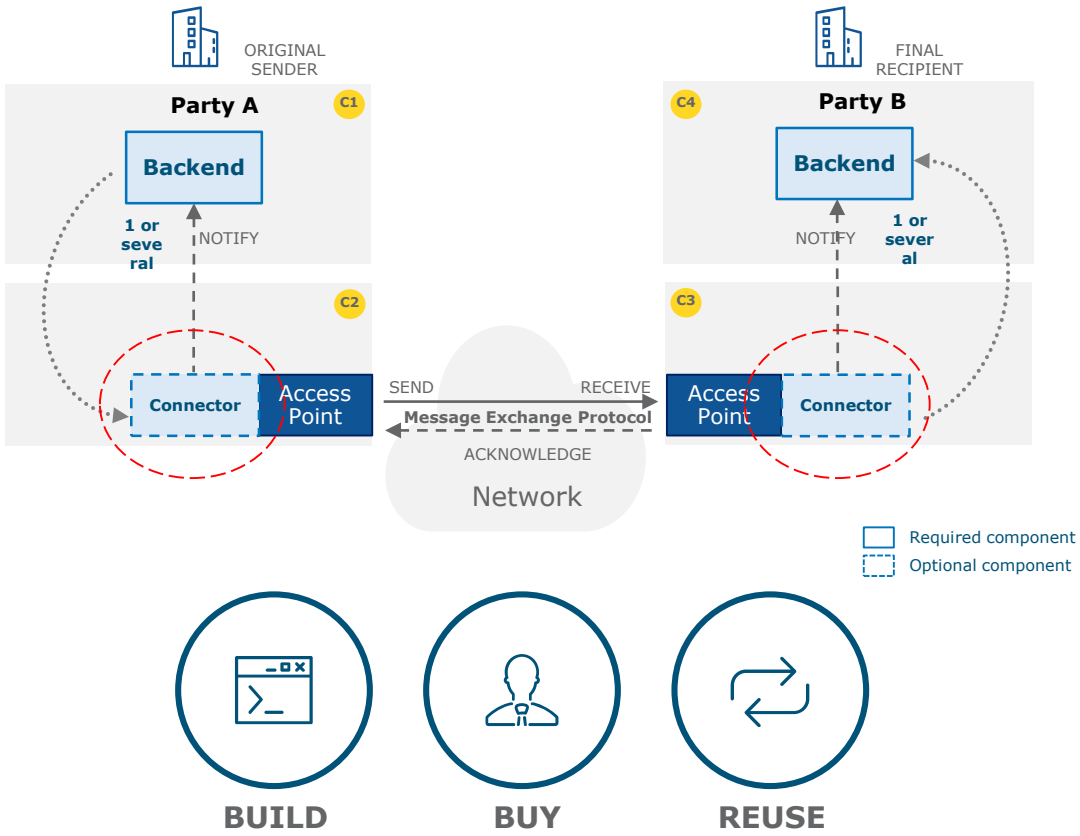
- Introduction
- Introduction to message exchange infrastructures
  - Message Exchange Models
    - Topologies
    - Protocols
    - Integration approach
  - Discovery Models
  - Security Models
    - Trust circles
    - Security controls
- Technical Specifications
- Sample Implementations
- End

Integration approach

It is key to determine how Backends will be integrated with the Access Points. Connectors may be built, bought or reused.

Some Access Point products offer advanced integration possibilities whereas others are purely for messaging purposes.

Services Providers may provide integration added-value services and at the same time operate the Access Point.



- Introduction
- Introduction to message exchange infrastructures
  - Message Exchange Models
    - Topologies
    - Protocols
    - Integration approach
  - Discovery Models
  - Security Models
    - Trust circles
    - Security controls
- Technical Specifications
- Sample Implementations
- End

Discovery models

Static

In a Static Service Location model the IP address and related attributes are static. The IP address of all the Access Points in the network are stored on a central location for the other Access Points to reference. To send a message, the sending Access Point looks a the static list of IP addresses on the networks' Domain Name System (DNS) to locate the Access Point of the receiver.

Dynamic

Dynamic Service Location enables the sending AP to dynamically discover the IP address and capabilities of the receiver. Instead of looking at a static list of IP addresses, the sender consults a **Service Metadata Publisher (SMP)** where information about every participant in the data exchange network is kept up to date. As at any point in time there can be several SMPs, every participant must be given a unique ID that must be published by **the Service Metadata Locator (SML)** on the network's Domain Name System (DNS). By knowing this URL, the sender is able to dynamically locate the right SMP and therefore the right receiver.

PROS & CONS

Static	Dynamic
+ High speed as there is no overhead processing	+ More automated and flexible
- Less flexible, change of irrelevant references	- Slower speed, as some overhead processing is required but

Dynamic discovery in detail

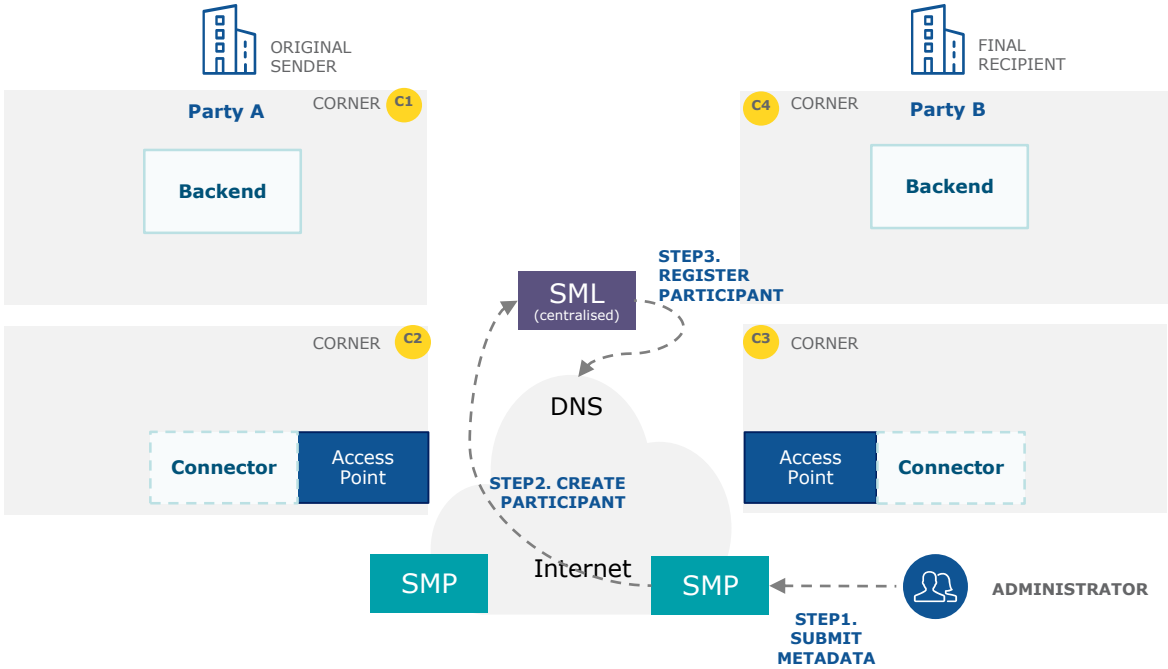
SML

The role of the SML (Service Metadata Locator) is to manage the resource records of the participants and SMPs (Service Metadata Publisher) in the DNS (Domain Name System). The SML is usually a centralised component in an eDelivery Messaging Infrastructure.

SMP

Once the sender discovers the address of the receiver's SMP, it is able to retrieve the needed information (i.e. metadata) about the receiver. With such information, the message can be sent. The SMP is usually a distributed component in an eDelivery Messaging Infrastructure.

Phase 1: Registration



Dynamic discovery in detail

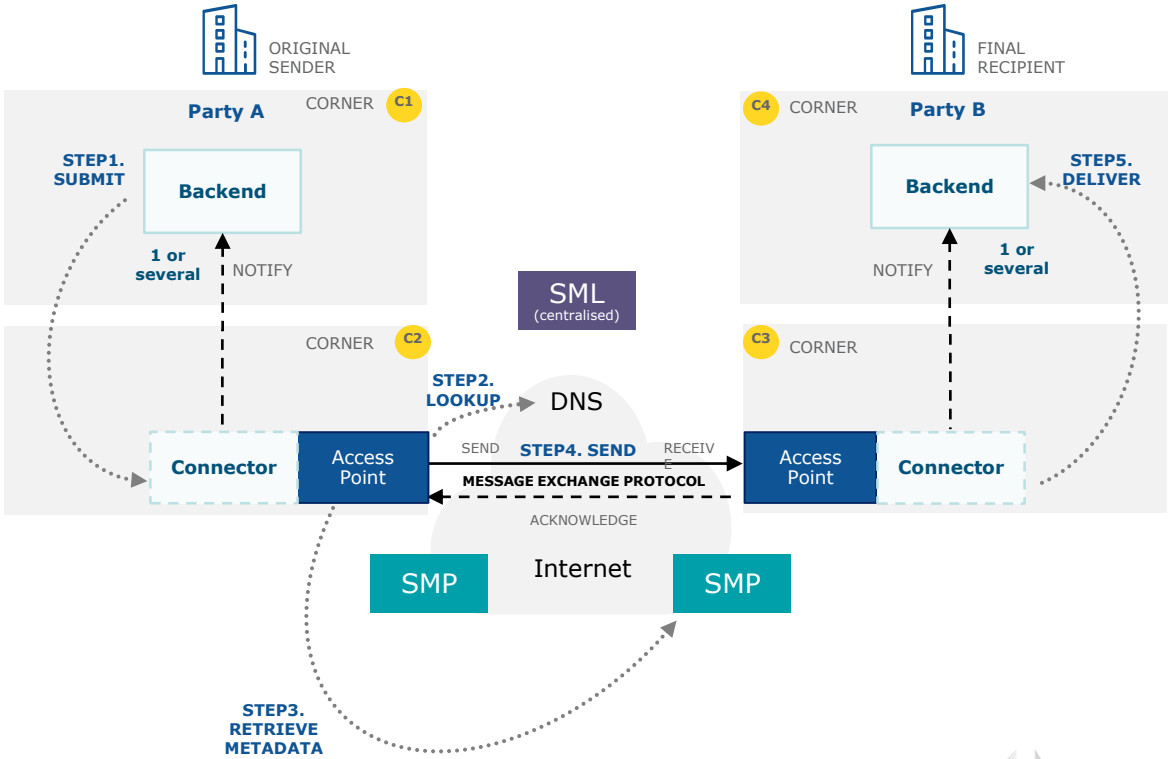
SML

The role of the SML (Service Metadata Locator) is to manage the resource records of the participants and SMPs (Service Metadata Publisher) in the DNS (Domain Name System). The SML is usually a centralised component in an eDelivery Messaging Infrastructure.

SMP

Once the sender discovers the address of the receiver's SMP, it is able to retrieve the needed information (i.e. metadata) about the receiver. With such information, the message can be sent. The SMP is usually a distributed component in an eDelivery Messaging Infrastructure.

Phase 2: Operations



- Introduction
- Introduction to message exchange infrastructures
  - Message Exchange Models
    - Topologies
    - Protocols
    - Integration approach
  - Discovery Models
  - Security Models
    - Trust circles
    - Security controls
- Technical Specifications
- Sample Implementations
- End

Trust circles: overview

Dedicated PKI

This trust architecture assumes that there is a dedicated PKI per policy domain that enables the eDelivery components (APs, SMPs and SML) to trust each other by sharing the common root CA (Certification Authority) certificate as a trust anchor.

To facilitate building of such a trust model, DIGIT provides support for the PKI services by establishing so-called eDelivery CA. The next section explains the architecture of the eDelivery CA.

Mutual exchange of certificates

Local trust store model assumes that each relying party, e.g. AP, SML, SMP, maintains its own repository of PKI certificates it trusts. Creation of a local trust store is the simplest way for relying parties to trust each other's certificates.

Using local trust stores does not require cross-certification between the PKIs that issued different certificates, nor does it require implementing mechanisms for processing complex certification paths, as all CAs in a path can be included in the local trust store.

Domain trusted list

The idea behind domain trusted lists is to enable service providers to use certificates issued by multiple CAs without the need to build complex cross-certification paths. For instance, a service provider who intends to operate APs and SMPs inside a policy domain will be able to use the certificates for these infrastructure components issued by a CA of its choice, as long as they comply with the domain policy.

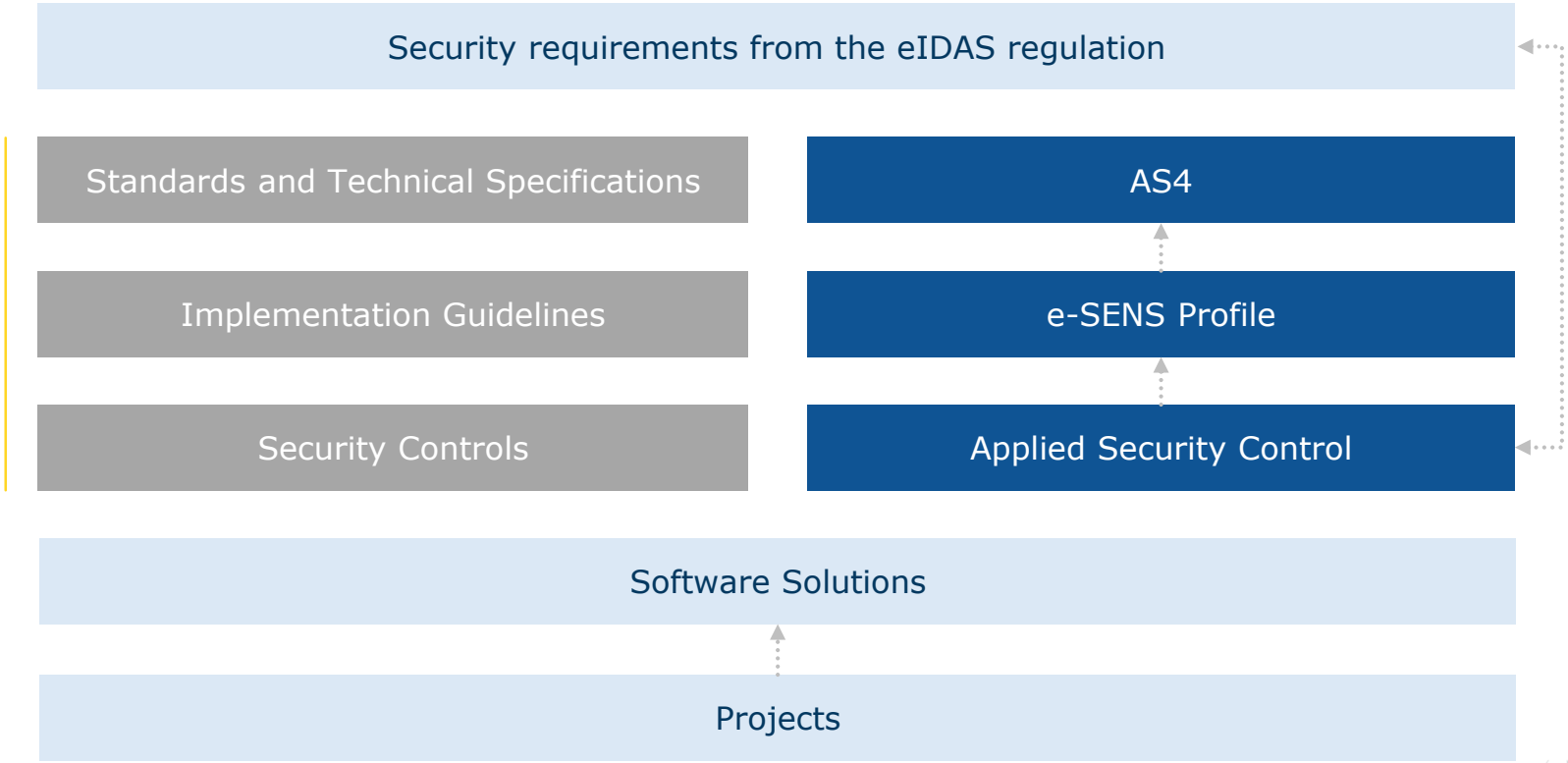
Trust circles: Pros and cons

		Dedicated PKI	Mutual exchange of certificates	Domain trusted list
DIGIT	**SETUP**	Simple configuration as all components share the same CA	Integration of the SML containing all the SMP certificates in the network	Integration of the SML + Not supported by TLS protocol
	MAINTENANCE	Low maintenance as all components share the same CA	Maintain SML trust store and keep it up-to-date	Maintain the certificates of multiple domain trusted list issuers
POLICY DOMAIN	**SCALABILITY**	Easy to add/remove APs/SMPs as the have the same trust root.	All local trust stores need to be updated when a AP/SMP is changed	Adding/removing of AP/SMP can be done in a central place.
	FLEXIBILITY	Full reliance on the root CA certificate	Flexibility in choice of the CA provider + No single point of failure	Flexibility in choice of CAs but full reliance on the domain trusted list
	OPERATIONAL EFFORT	CA provided and managed by DIGIT	Significant effort to maintain the local trust stores	Maintenance of the domain trusted list + distribution of the certificate used to sign the trusted list
	COST	PKI architecture provided by DIGIT	No additional expenses on certificate infrastructure	Additional cost to establish and operate a domain trusted list
	SECURITY	Transparent certificate policy and accurate certificate status info	No direct control over certificate policies and trust store content	Accurate trust info in a domain trusted list

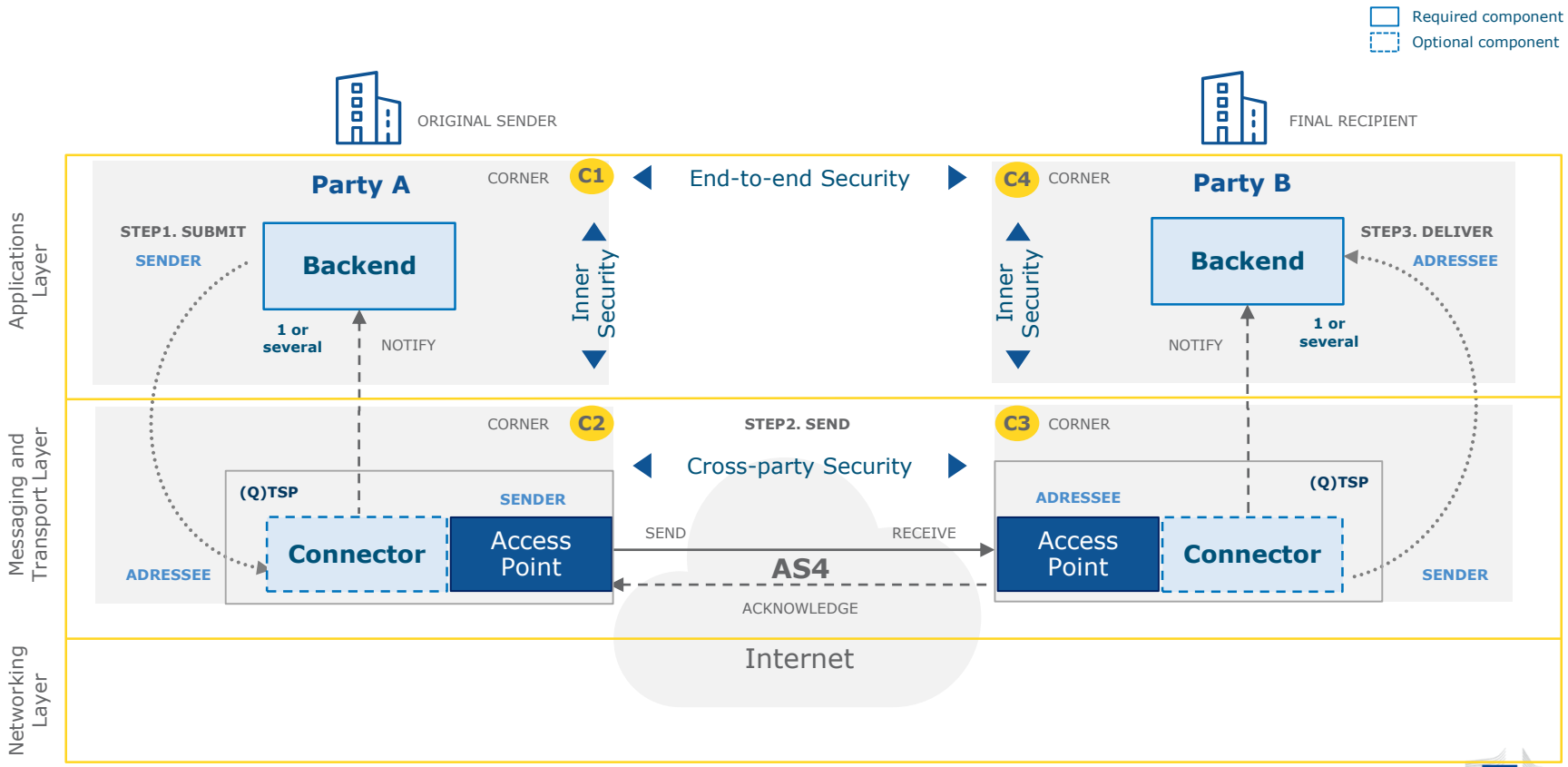
High score
Medium score
Low score

- Introduction
- Introduction to message exchange infrastructures
  - Message Exchange Models
    - Topologies
    - Protocols
    - Integration approach
  - Discovery Models
  - Security Models
    - Trust circles
    - Security controls
- Technical Specifications
- Sample Implementations
- End

Approach to link eDelivery and eIDAS regulation



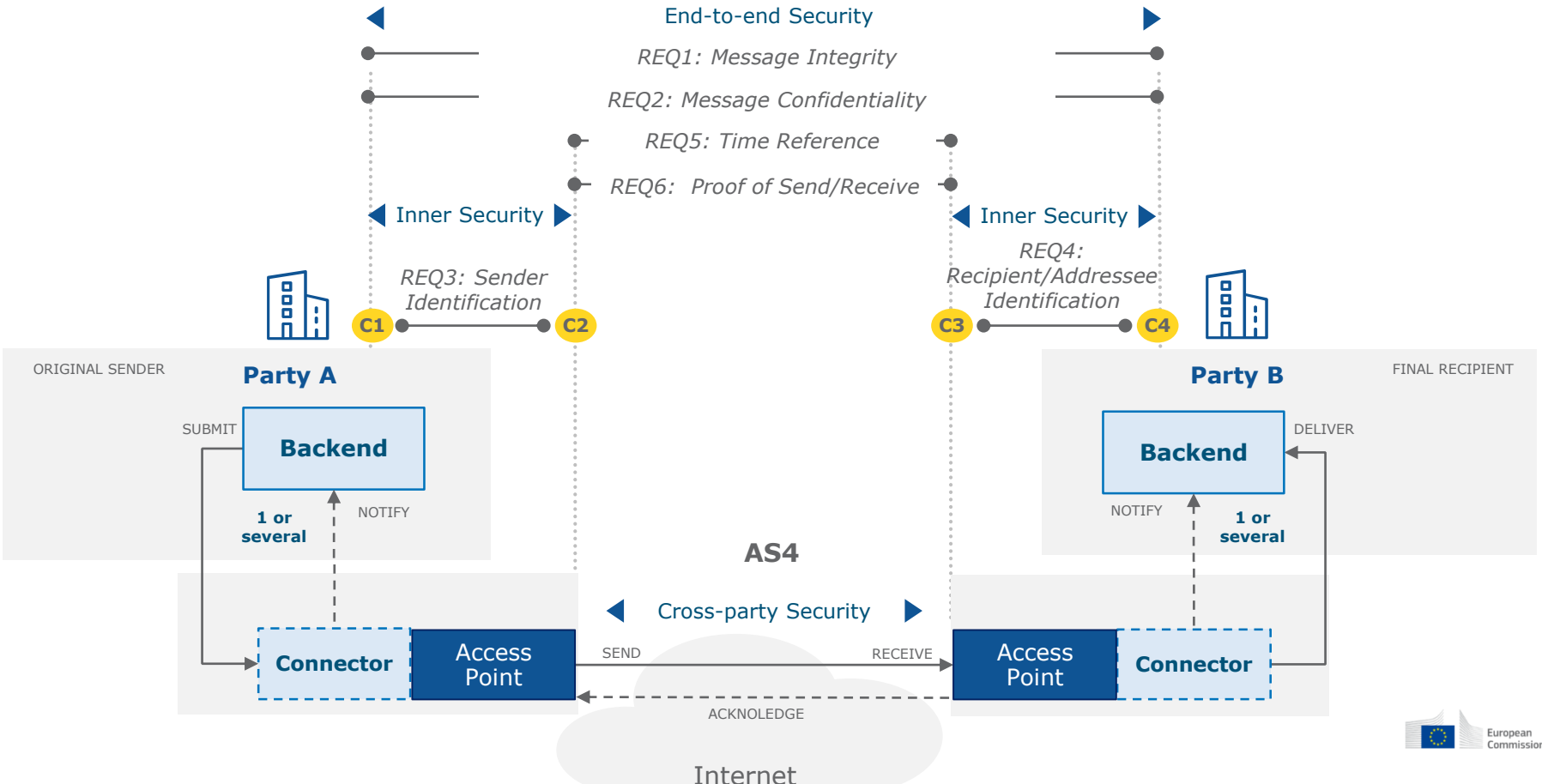
eDelivery Messaging Infrastructure based on the 4-Corner Model



Summary of security requirements from the eIDAS regulation

Requirement	Description	eIDAS reference
REQ1 **Message Integrity**	Messages should be secured against any modification during transmission.	Article 3 (36) Article 19 Article 24 Article 44, (d) 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;
REQ2 **Message Confidentiality**	Messages should be encrypted during transmission	Article 5 Article 19 Article 24
REQ3 **Sender Identification**	The identity of the sender should be verified.	Article 24 Article 44 (b) they ensure with a high level of confidence the identification of the sender;
REQ4 **Recipient / Addressee Identification**	Recipient / addressee Identity should be verified before the delivery of the message.	Article 24 Article 44 (c) they ensure the identification of the addressee before the delivery of the data;
REQ5 **Time-Reference**	The date and time of sending and receiving a message should be indicated via a qualified electronic timestamp.	Article 44 (f) the date and time of sending, receiving and any change of data are indicated by a qualified electronic time stamp.
REQ6 **Proof of Send/Receive**	Sender and receiver of the message should be provided with evidence of message recipient and deliver.	Article 3 (36) "… provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data…"

Mapping of security requirements to the 4-Corner Model

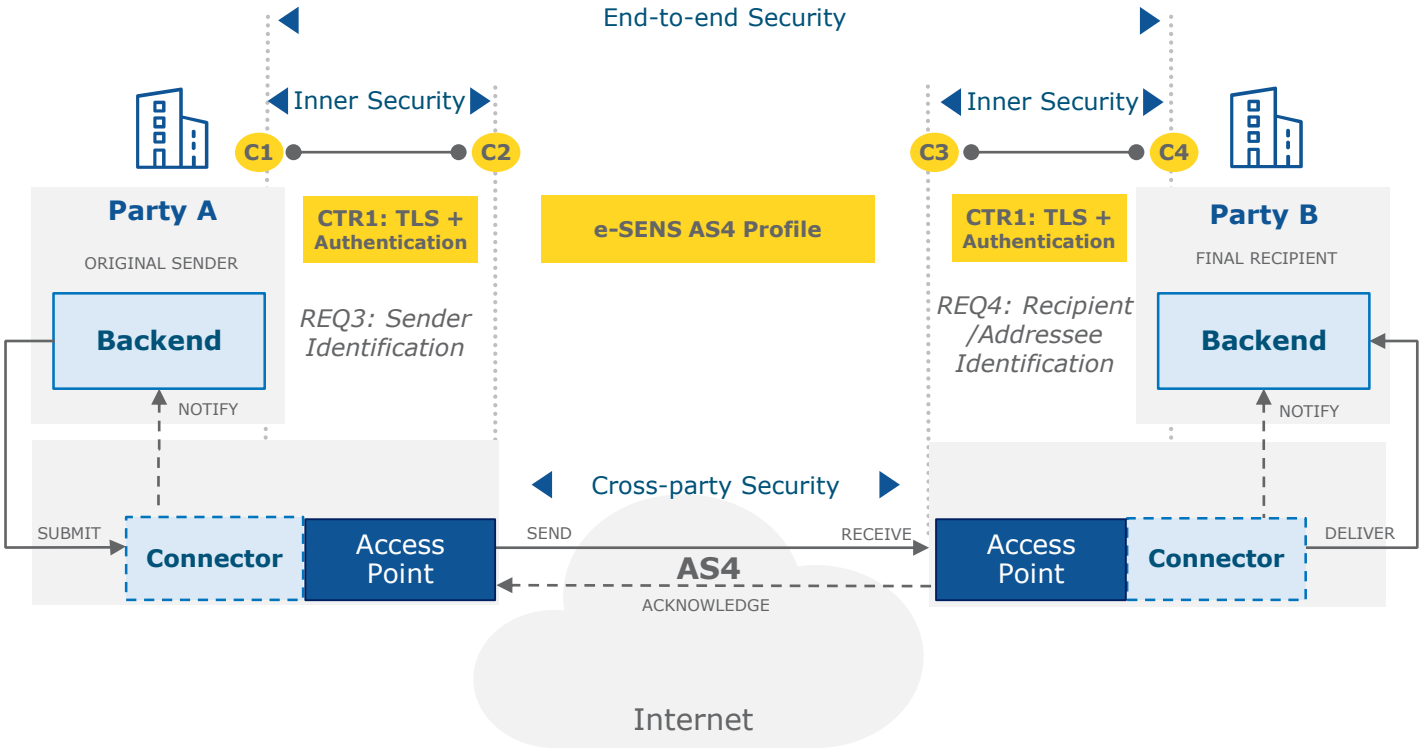


Summary of security controls

(*) Not exhaustive and it is by no means a guarantee that the system will be granted qualified status under the eIDAS regulation. For the process of granting the qualified status, please refer to the national supervisory body in the respective country.

Security control	Legal implications
CTR1 **Transport Layer Security (TLS) + Authentication** TLS protocols ensure authenticity and integrity of the message, by applying host to host cryptographic mechanisms	European General Data Protection Regulation (GDPR), in case of applicability.
CTR2 **Message Encryption** Message encryption ensures confidentiality of the message payload so that only the correct recipient can access it	European General Data Protection Regulation (GDPR), in case of applicability.
CTR3: **Electronic Seal of message** From technical perspective, electronic seal ensures integrity of the message header and payload and authenticity of origin	**Non-qualified**: Ensures integrity and origin of the data, in other words its authentication **Qualified**: eIDAS Regulation, Article 35. "A qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data" **Both**: Non-discrimination in legal proceedings
CTR4: **Electronic Seal of evidence** Provides evidence to the sender C1 that the message was sent, delivered to the final recipient C4 and authenticity of destination	
CTR5: **Electronic Timestamp** Data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time	**Non-qualified:** Ensures date and time of the data. **Qualified:** eIDAS Regulation, Article 41. "A qualified electronic time stamp shall enjoy the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound." **Both:** Non-discrimination in legal proceedings

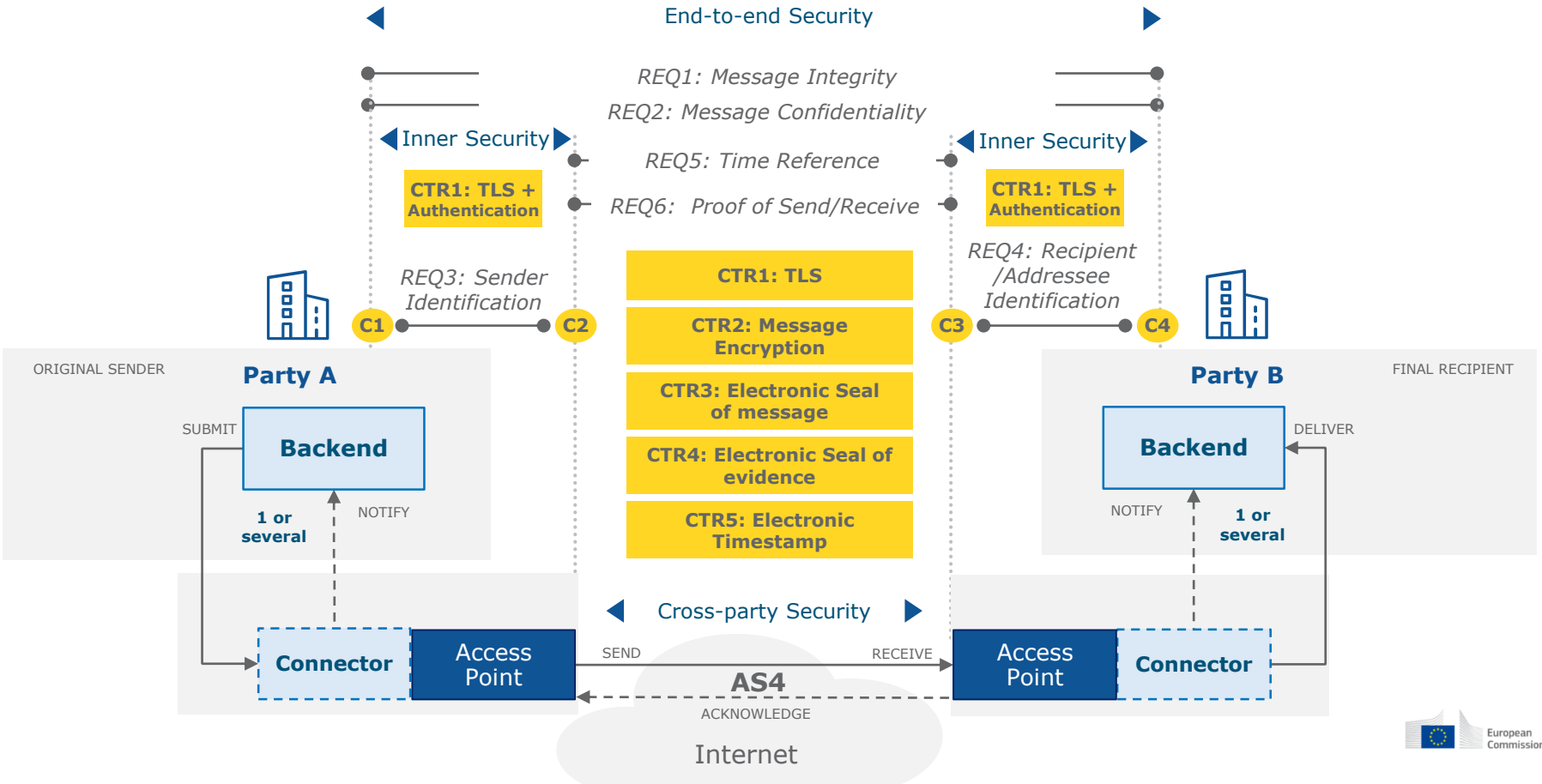
Mapping of security controls to the 4-Corner Model



List of security controls applied to the e-SENS AS4 message protocol

Security control	Description
CTR1 **Transport Layer Security (TLS)**	Transport Layer Security (TLS 1.2 [9]) protocol is used, following ENISA security [7] and BSI [8] guidelines. For the sender identification is provided as follows: • Basic authentication: C2 uses username/password to authenticate to C3. In this case, proper password management, including secure storage, sufficient complexity and regular updates need to be ensured by C2; • Mutual authentication: This is done using the digital certificate of C2, allowing C3 to identify C3.
CTR2 **Message Encryption**	C2 encrypts the payload of the message using AES-GCM with a random secret key, and the random key with the public key of C3 using RSA-OAEP. Message encryption follows WS-Security using W3C XML Encryption The used cipher suite for symmetric encryption is: AES GCM-mode, and for asymmetric: RSA-OAEP. This should follow the ENISA security [7] and BSI [8] guidelines.
CTR3: **Electronic Seal of message**	C2 applies an electronic seal to the message header and payload using its own private key which guarantees integrity protection. The seal is verified by C3 using C2 public key for authenticity and non-repudiation of the message payload and headers. Electronic sealing follows WS-Security with W3C XML Signing. The cipher suite is RSA-SHA256.
CTR4: **Electronic Seal of evidence**	Electronic seal is applied to the receipt. Upon reception and verification of a message from C2, C3 generates an evidence receipt based on message identification information (e.g., message identifier, timestamp, and sender metadata) with a new timestamp and a reference to the received message, applies an electronic seal and returns the sealed evidence to C2. The receipt is sent automatically to C2 as a "signal" message response to the initial message. Electronic sealing follows WS-Security with W3C XML Signing. The used cipher suite is: RSA-SHA256.
CTR5: **Electronic Timestamp**	Timestamp is placed at the WS-Security header, and it is electronically sealed for integrity protection. At this moment, by default, it is not a qualified time stamp and it relies on the system clock.

Mapping of security controls to the 4-Corner Model



- Introduction
- Introduction to message exchange infrastructures
  - Message Exchange Models
    - Topologies
    - Protocols
    - Integration approach
  - Discovery Models
  - Security Models
    - Trust circles
    - Security controls
- **Technical Specifications**
- Sample Implementations
- End

CEF eDelivery specifications

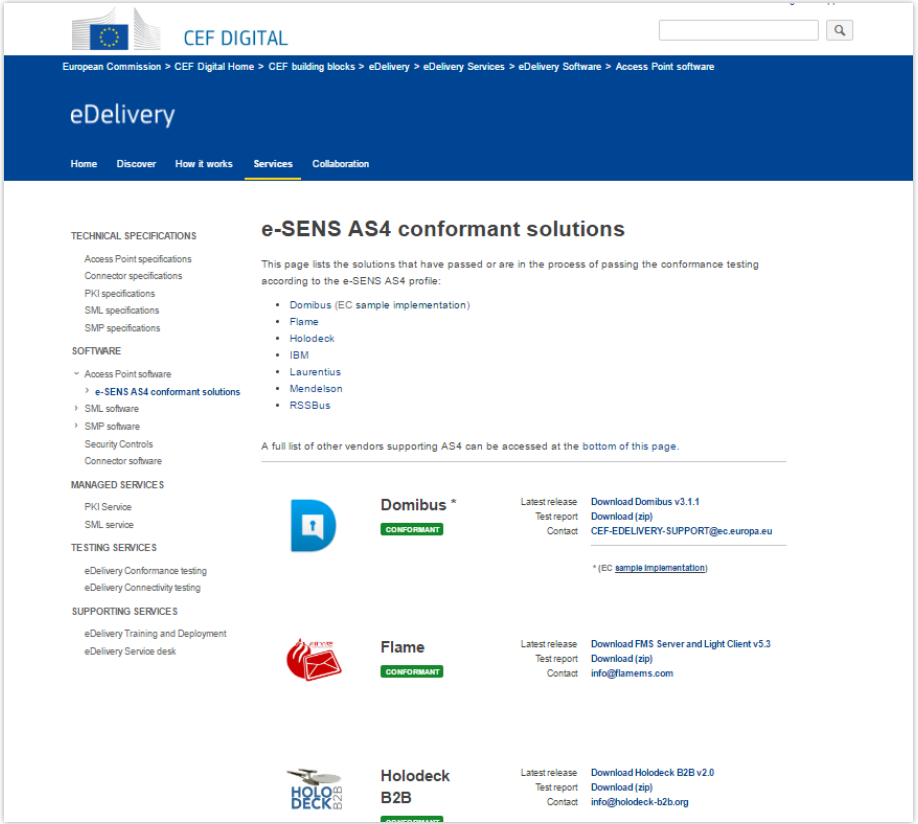
The approach employed by eDelivery is to promote the use of existing technical specifications and standards rather than to define new ones.

The profiling work of e-SENS and PEPPOL on these standards, i.e. constraining configuration choices, is equally taken on board. Even though eDelivery makes software available implementing these specifications, the use of commercial software or other Open Source software projects is also possible.

COMPONENT	KEY SPECIFICATIONS
Access Point	➢ e-SENS AS4 profile of the ebMS3/AS4 OASIS Standards ➢ PEPPOL AS2 profile of AS2 and SBDH (for the eProcurement only)
Digital Certificates	➢ ETSI – Electronic Signatures and Infrastructures profile
Service Metadata Locator (SML)	➢ OASIS BDXL Specification ➢ OASIS ebCore Party ID Type Technical Specification
Service Metadata Publisher (SMP)	➢ OASIS SMP Specification ➢ The original PEPPOL SMP Specification
Connector	➢ ETSI REM for evidences

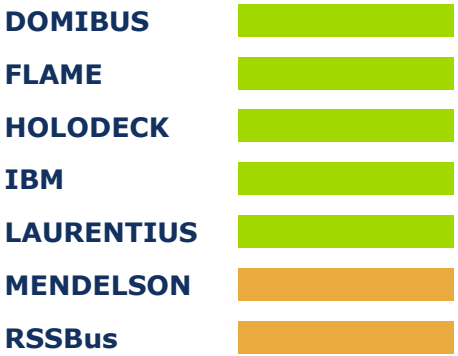
- Introduction
- Introduction to message exchange infrastructures
  - Message Exchange Models
    - Topologies
    - Protocols
    - Integration approach
  - Discovery Models
  - Security Models
    - Trust circles
    - Security controls
- Technical Specifications
- Sample Implementations
- End

e-SENS AS4 conformant solutions



More information on CEF Digital

Conformant Solutions >



Conformant

Ongoing

European Commission

Sample software maintained by the EC

DOMIBUS

Domibus is the European Commission’s sample implementation of an AS4 conformant Access Point, based on the e-SENS AS4 profile.

Through the "Operational Management Board", CEF eDelivery stakeholders define the evolution of these solutions, by suggesting features that are then developed by the CEF's team.

BENEFITS

- Released under an open source license
- Viable solutions for use in production environment
- Fully supported by the European Commission
- Based on market-driven technical specifications

USERS

Software Providers
Service Providers
Policy Domains

STATUS

Service
Documentation

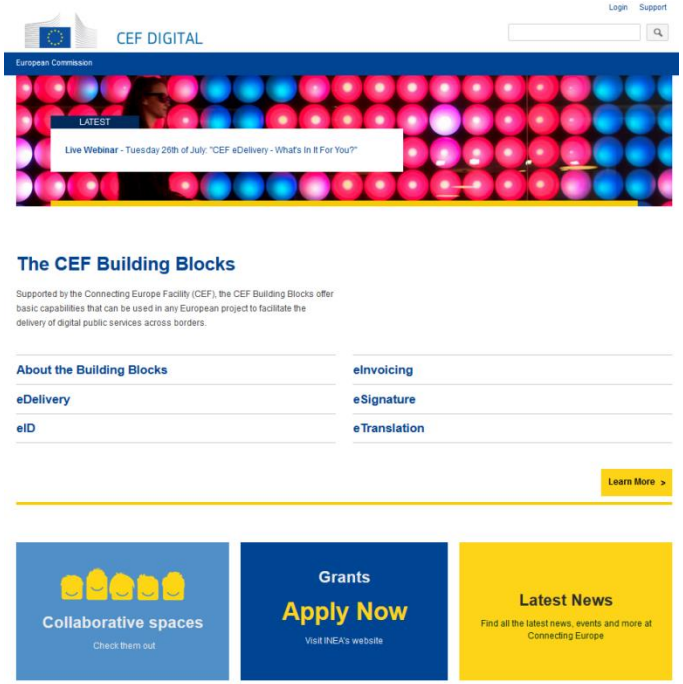
More info

CEF Digital >

Get started

Contact us >

Find out more on CEF Digital



ec.europa.eu/cefdigital

DIGIT
Directorate-General for Informatics

DG CONNECT
Directorate-General for Communications Networks, Content and Technology

Contact us

CEF-BUILDING-BLOCKS@ec.europa.eu