Connecting Europe Facility

Primer on eDelivery

FIWARE Summit
13 – 15 December 2016

Agenda

1 **Introduction to CEF**
Joao Rodrigues Frade

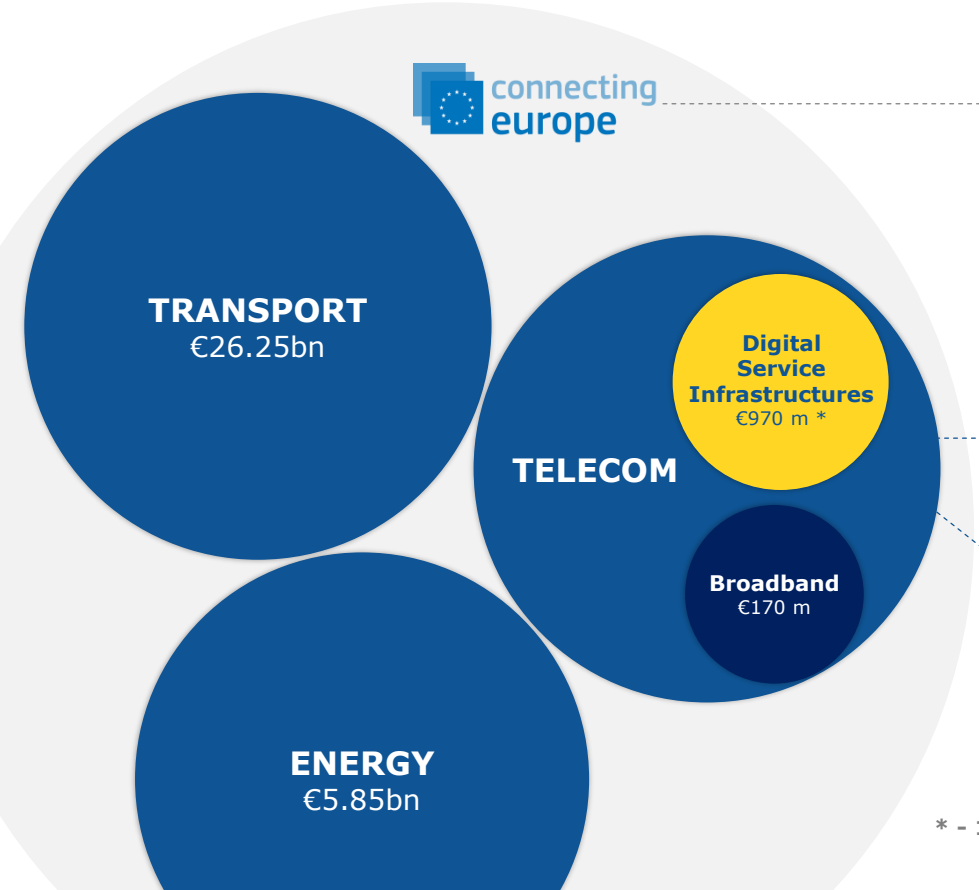
2 **Introduction to eDelivery**
Britt Joosten

3 **Demo**
Ioana Dragusanu

Introduction to CEF

Joao Rodrigues-Frade

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**

CHALLENGES IN CURRENT CONTEST

Only 59% of Europeans can **access 4G** networks

90% of jobs will soon require **digital skills**

+ **€11 billion** in **savings** for consumers when **shopping online**

THE DIGITAL CITIZEN OF THE FUTURE

- IDENTIFY *with* **eID**
- TRANSLATE *with* **eTranslation**
- INVOICE *with* **eInvoicing**
- SIGN *with* **eSignature**
- EXCHANGE *with* **eDelivery**

CHALLENGES IN CURRENT CONTEST

Small businesses could save €9.000 per market on legal and translation fees thanks to harmonised national laws in the EU

52% of cross-border **purchases** are **blocked**

THE DIGITAL ENTERPRISE OF THE FUTURE

- IDENTIFY *with* **eID**
- TRANSLATE *with* **eTranslation**
- INVOICE *with* **eInvoicing**
- SIGN *with* **eSignature**
- EXCHANGE *with* **eDelivery**

What does CEF Digital finance?

DIGITAL SERVICE INFRASTRUCTURES (DSIs)

Funding for the
EUROPEAN COMMISSION

Funding for the
MEMBER STATES

CORE SERVICE PLATFORM
Services offered by the European Commission

SECTORIAL

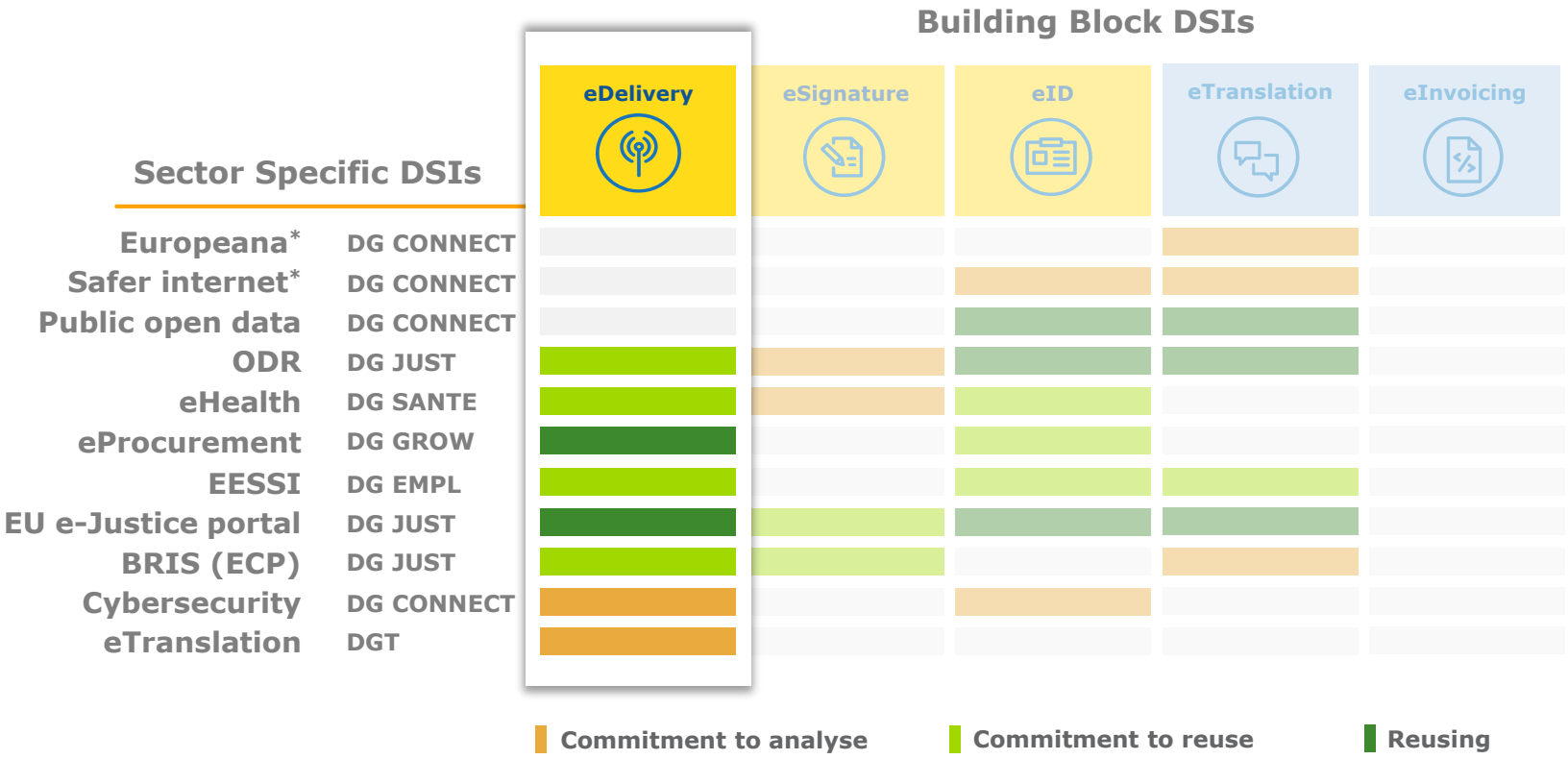
eJustice Portal
EU Open Data Portal
...

BUILDING BLOCKS

- eInvoicing
- eSignature
- eDelivery
- eID
- eTranslation

GRANTS
Projects in the Member States

Reuse of eDelivery by CEF's sectorial projects



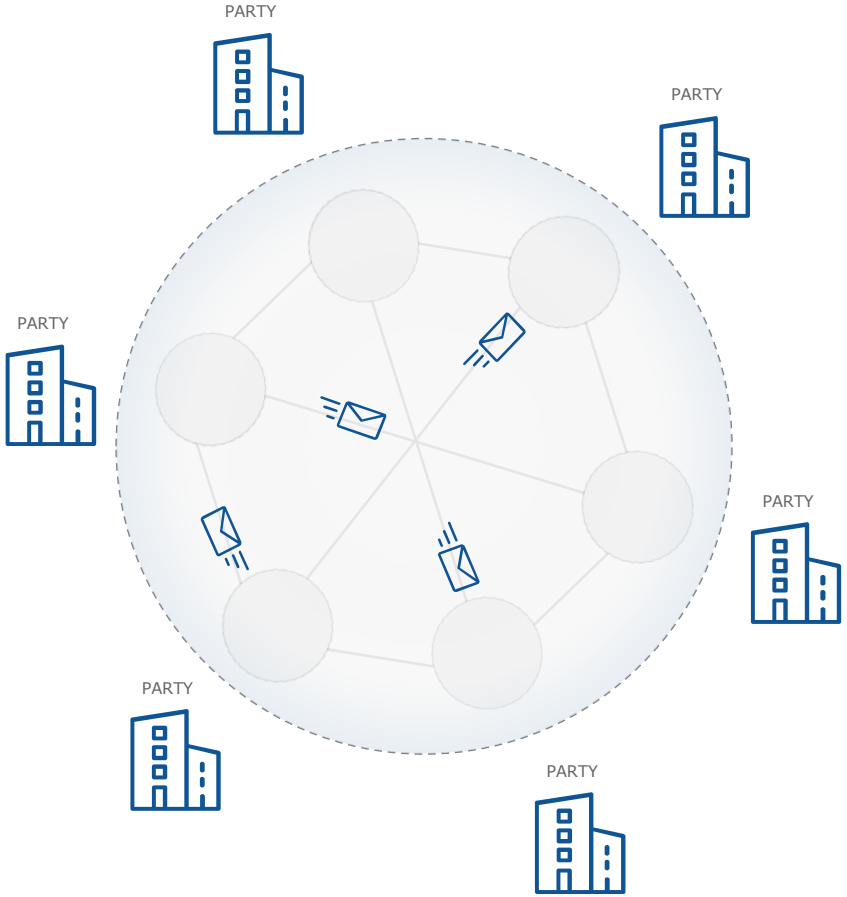
Introduction to eDelivery

Britt Joosten

What is eDelivery

The eDelivery Building Block enables you to **exchange electronic data and documents** in an interoperable, secure, reliable and trusted way.

- Distributed (“4-corner model”)
- Payload agnostic



European Commission

Online Dispute Resolution (ODR)

eDelivery re-use case study

- **Online platform** to help online traders and consumers resolve disputes.
- A simple and low-cost out-of court solution to disputes using **alternative dispute resolution (ADR) entities**.

"Boost confidence in (cross-border) e-commerce"

THE CHALLENGE

In order to effectively bring traders, consumers and dispute resolution entities together to resolve disputes online, **electronic documents needed to be sent** between parties **quickly** and **securely.**

eDelivery

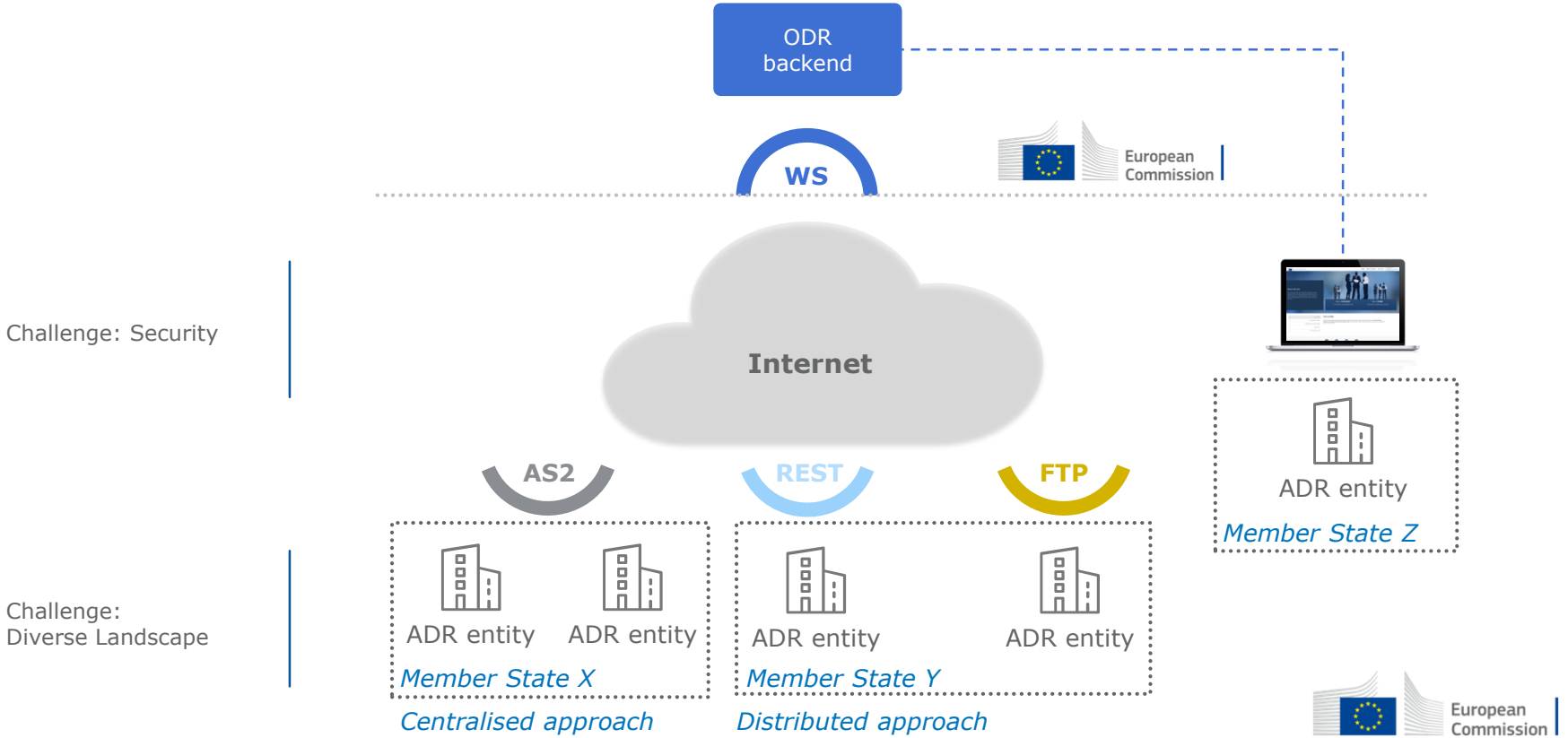
Online Dispute Resolution (ODR)

eDelivery re-use case study

OASIS AS4*

Any Protocol

* According to CEF's implementation guidelines



Online Dispute Resolution (ODR)

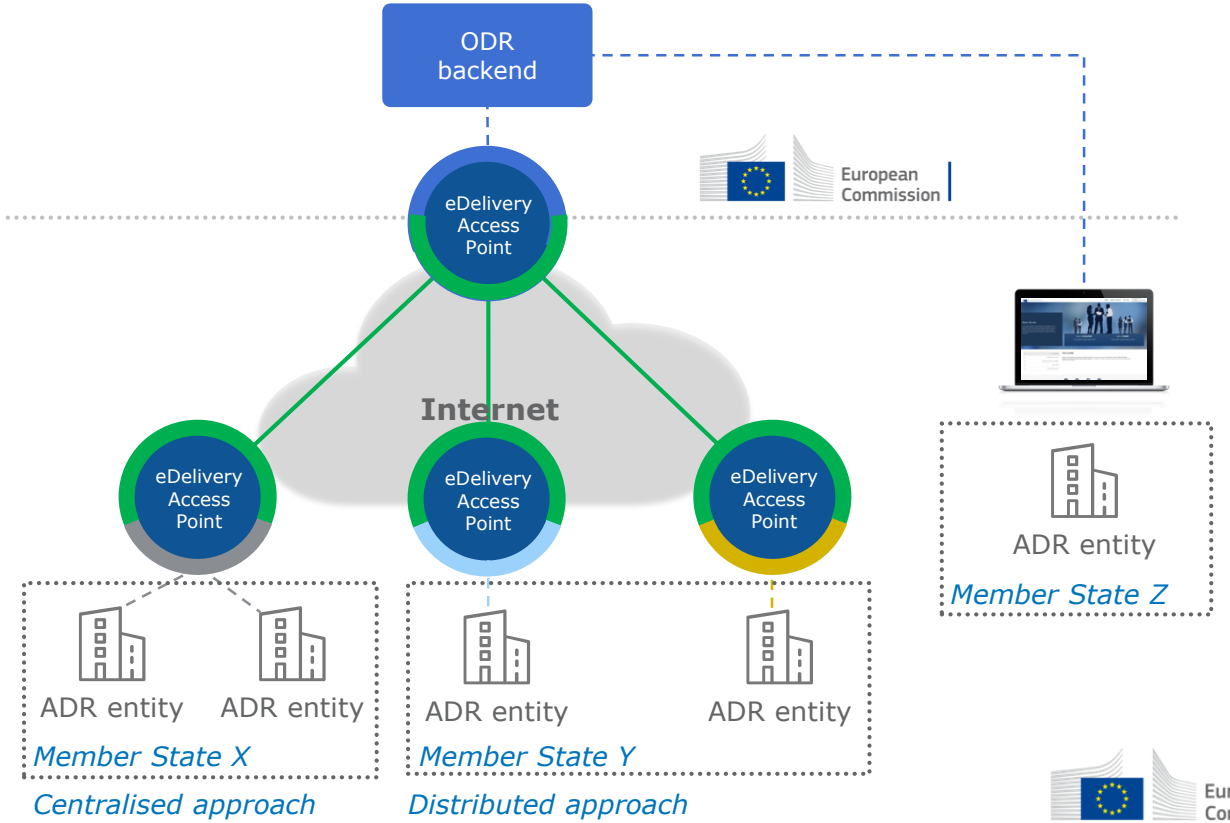
eDelivery re-use case study

OASIS AS4*

Any Protocol

* According to CEF's implementation guidelines

- Message Integrity
- Message Confidentiality
- Message Filtering
- Message Correlation
- Proof of Send/Receive



Online Dispute Resolution (ODR)

eDelivery re-use case study

OASIS AS4*

Any Protocol

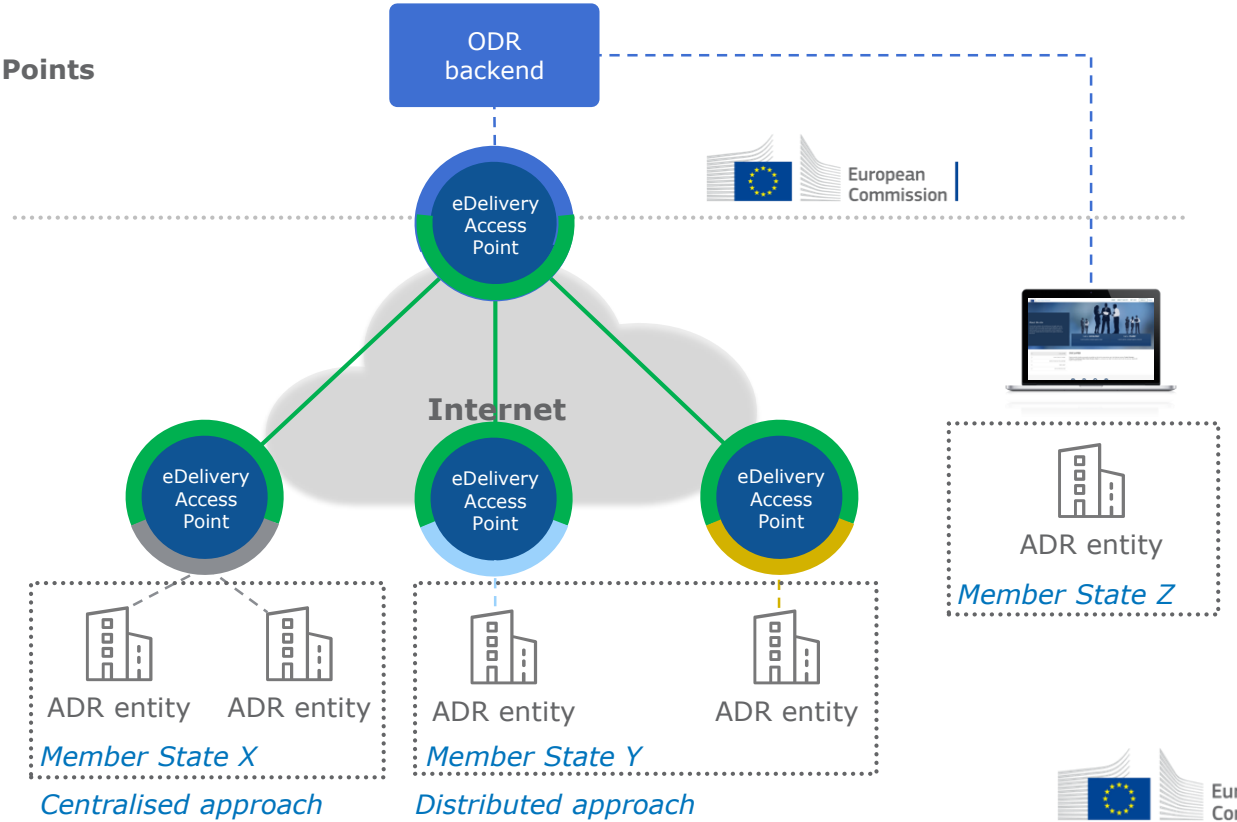
* According to CEF's implementation guidelines

eDelivery Conformant Access Points

- DOMIBUS
- FLAME
- HOLODECK
- IBM
- LAURENTIUS
- MENDELSON
- RSSBus

More information

Conformant Solutions >



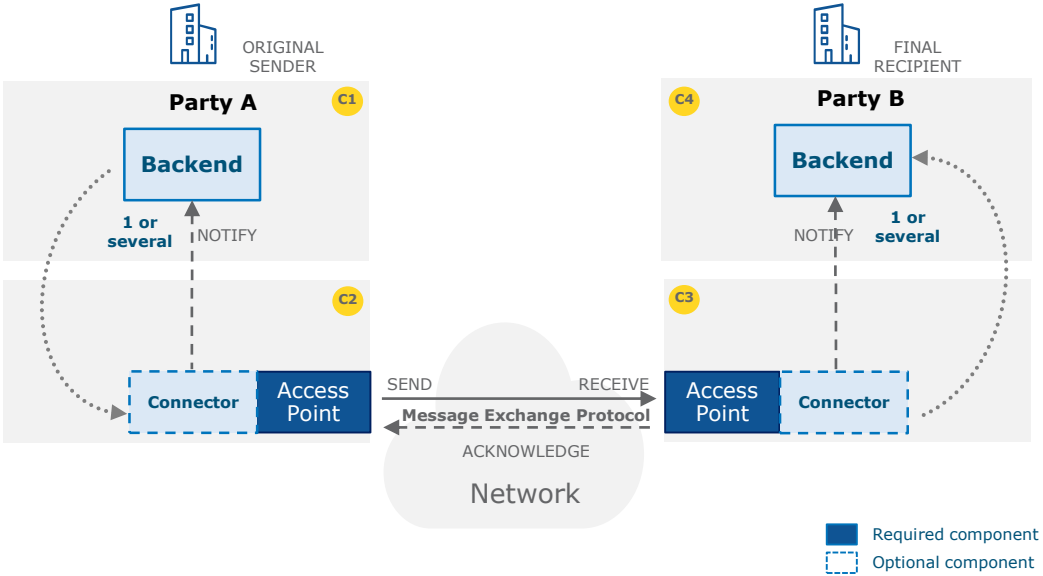
European Commission

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**

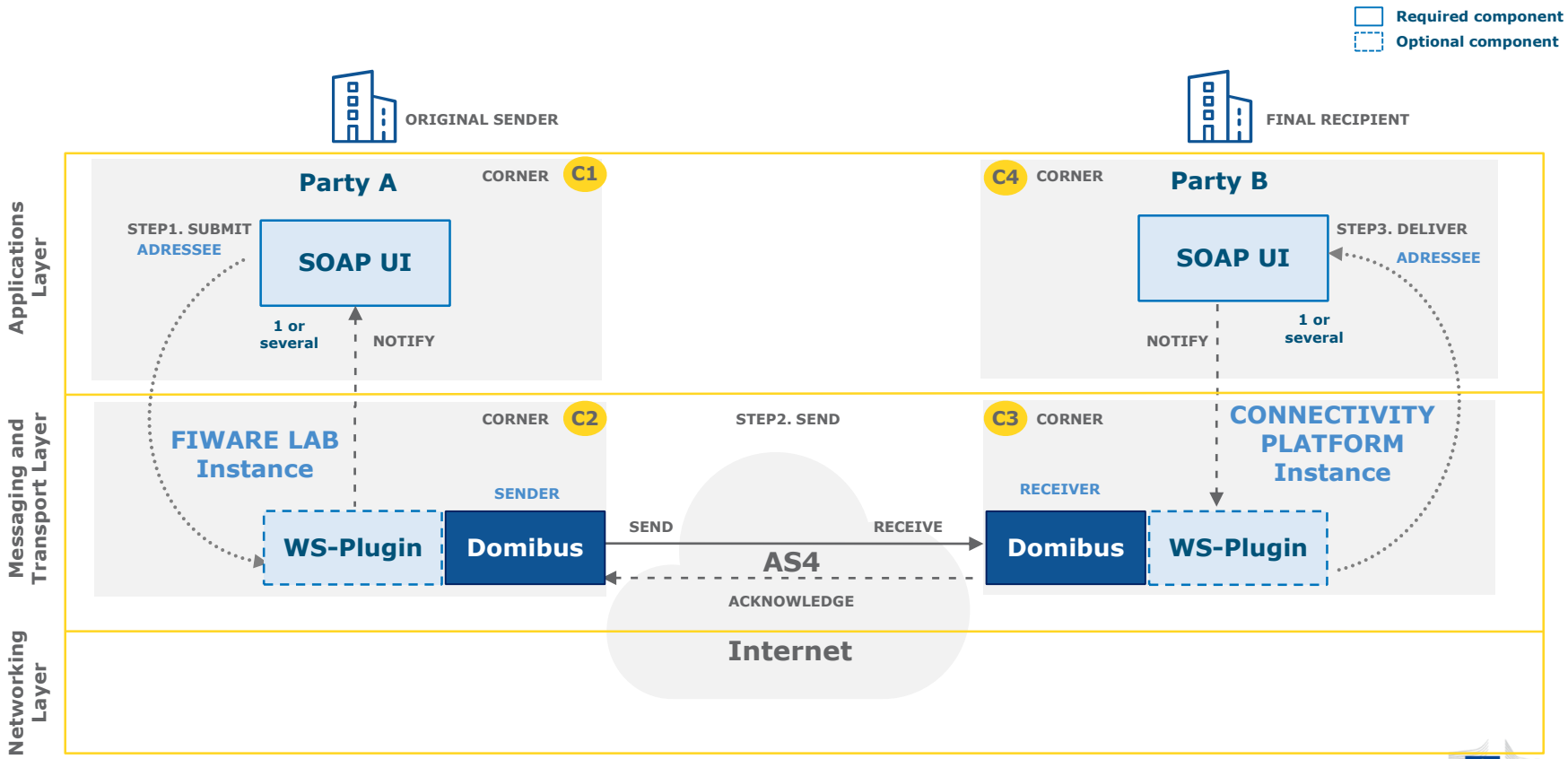
CONS

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

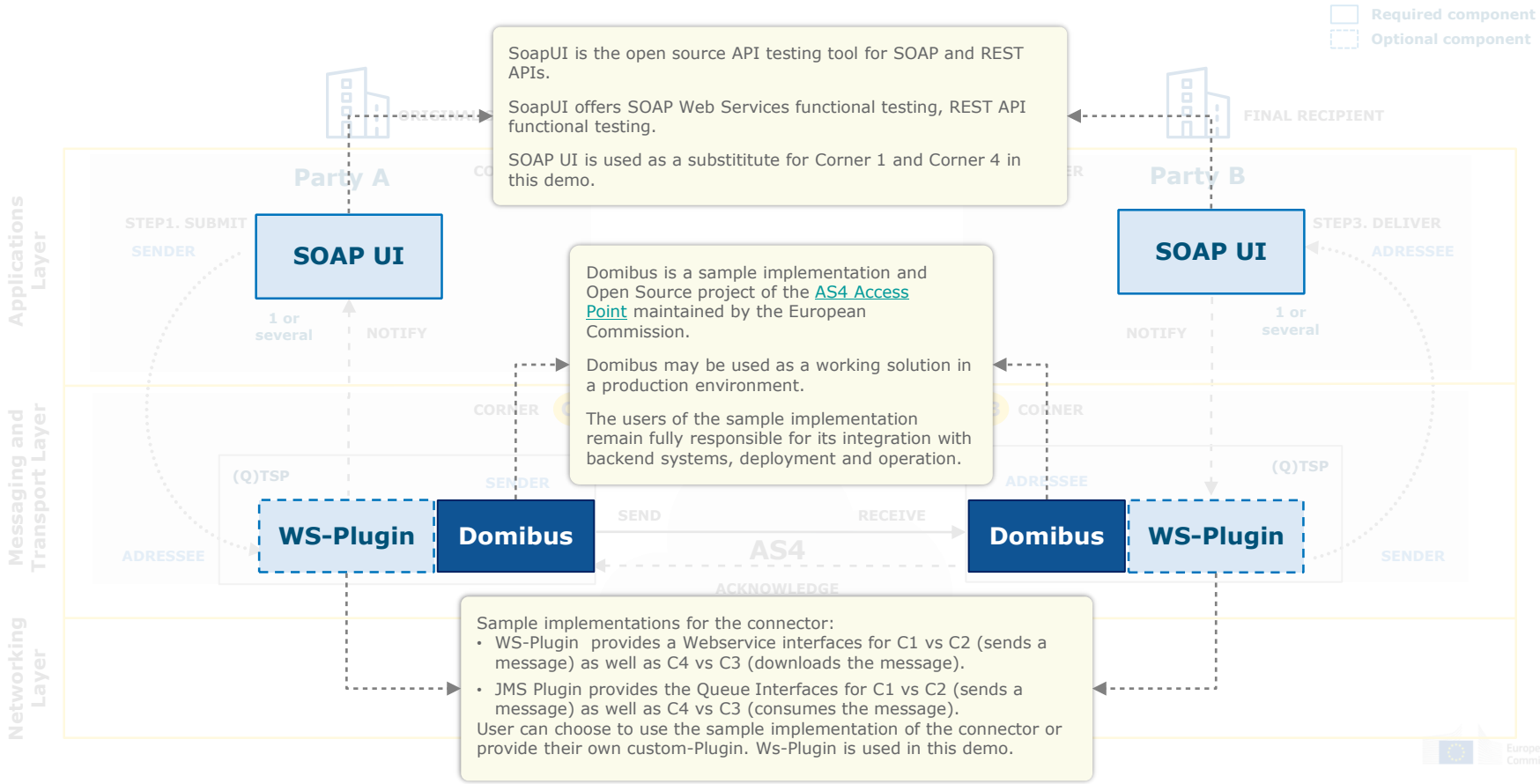
Demo

Ioana Dragusanu

Demo in detail



Demo scenario



Demo Steps

DEMO TIME

Launch instance

a) FIWARE LAB Instance
   - Launch an instance based on a public VM image on the FIWARE lab.

b) Docker image
   - Launch an instance based on a docker image published on the Docker Hub under "fiware" account.

DEMO TIME

Configuration *(pre-configured)*

a) PMode File
   - Configure the parties, endpoint URLs for the sending and receiving Access Points
   - Configure compression, number of retries, etc.

b) Security File
   - Configure the location and password for the Keystore and Truststore

DEMO TIME

Runtime Scenario

a) Backend C1 sends the message to Access Point C2

b) The Message is sent from sender Access Point C2 to receiving Access Point C3

c) An acknowledgement is sent from C3 to C2

d) C4 downloads the message from C3

I. Launch instance

a. Launch instance on Fiware Lab

Image: domibus3.2_r5.4

b. Launch instance using docker container

Image: https://hub.docker.com/r/fiware/domibus-tomcat/

II. Configuration

a. PMode Configuration

Configure Parties container

PMode[1].businessProcesses.parties.party: This parameter Contains the name of the partner Access Points and the address (endpoint URL) of the Receiver MSH to which User Messages under this PMode are to be sent.

PMode[1].businessProcesses.parties.party.Identifier: This Parameter contains the name of the clients' backend associated to the parent Access Point.

```
<party name="red_gw"
         endpoint="http://40.118.20.112:8080/domibus/services/msh"
         allowChunking="false">
         <identifier partyId="domibus-red" partyIdType="partyTypeUrn"/>
</party>
<party name="blue_gw"
         endpoint="http://domibus.lab.fiware.org:8080/domibus/services/msh"
         allowChunking="false">
         <identifier partyId="domibus-blue" partyIdType="partyTypeUrn"/>
</party>
```

b. Security File Configuration

Configure Security File details

```
<util:properties id="keystoreProperties">
     <!-- The crypto provider to be used -->
     <prop key="org.apache.ws.security.crypto.provider">
          org.apache.wss4j.common.crypto.Merlin
      </prop>
      <!-- Type of the used keystore -->
      <prop key="org.apache.ws.security.crypto.merlin.keystore.type">jks
      </prop>
      <!-- The password used to load the keystore -->
      <prop key="org.apache.ws.security.crypto.merlin.keystore.password">
         test123
      </prop>
      <!-- The keystore alias to use for decryption and signing. -->
      <prop key="org.apache.ws.security.crypto.merlin.keystore.alias">
         blue_gw
      </prop>
      <!-- The location of the keystore -->
      <prop key="org.apache.ws.security.crypto.merlin.file">
         ${domibus.config.location}/keystores/gateway_keystore.jks
      </prop>
</util:properties>
```

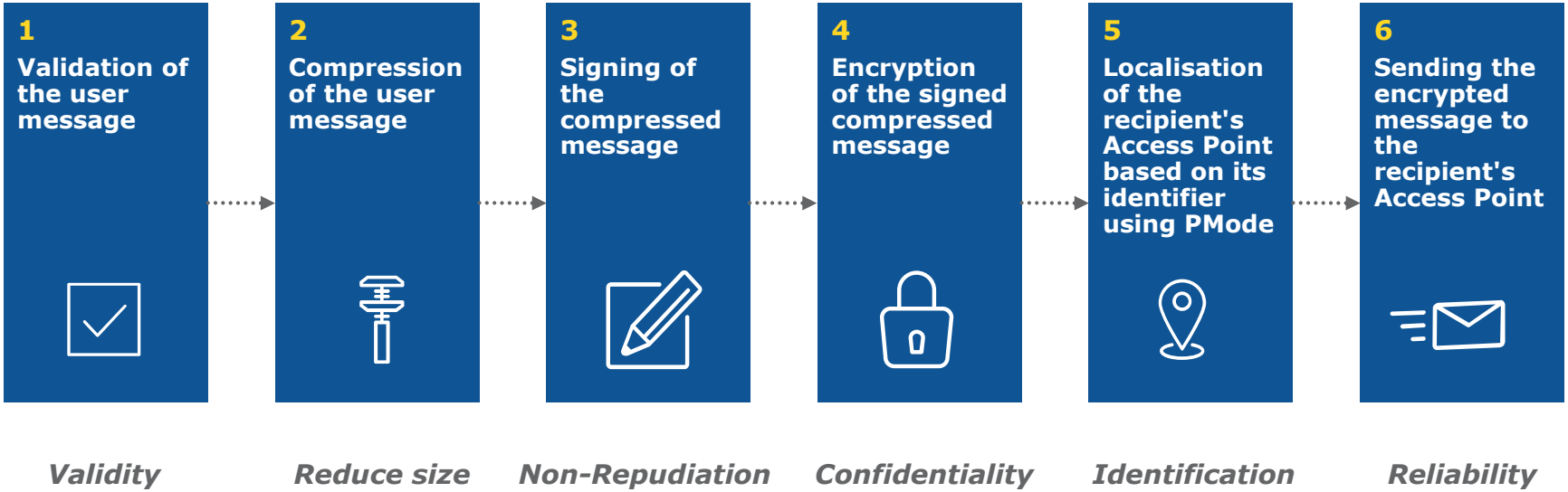
III. Run-time process

Connecting Europe Facility

Primer on eDelivery

- FIWARE Summit
- 13 – 15 December 2016

SEND: Processing at C2.



RECEIVE: Process at C3

1 Receives the encrypted message

Duplicates detection

2 Decrypts the encrypted message

Confidentiality

3 Verifies the sender's signature

Non-Repudiation

4 Decompresses the decrypted message

Original size

5 Validates the original user message

Validity

6 Sends the acknowledgement to the sender Access Point C2

Reliability

7 Archives the user message

Retention

Release 3.2

Specifications

- e-SENS AS4 Profile
- OASIS AS4 Profile
- ebMS3 Core

App serves

- Tomcat 8, WebLogic 12, Wildly 9

Databases

- MySQL, Oracle

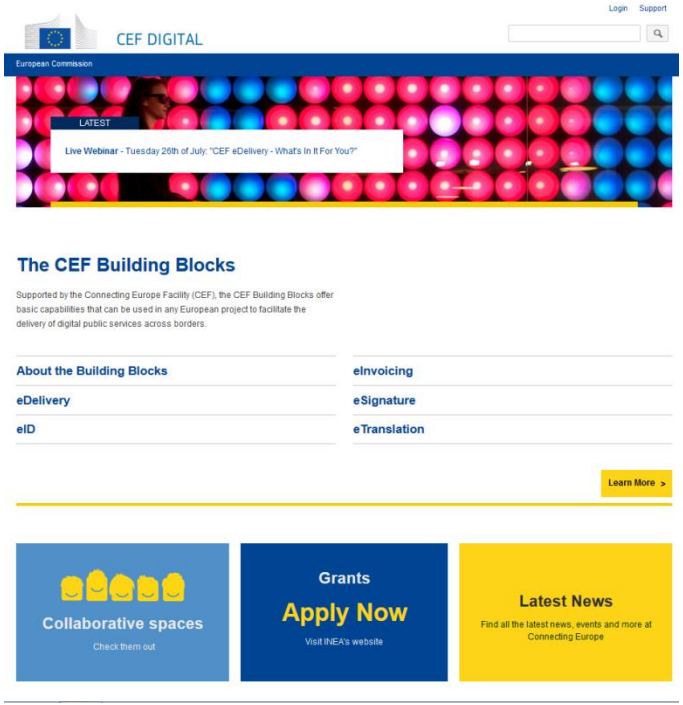
Technologies

- SOAP 1.2 *with attachments*
- Apache CXF
- Apache WSS4J
    - WS-Security: *WSSSMA, WSSX509, WSSSWA,*
    - *WS-Policy: rsa-sha256, aes128-gcm, rsa-oaep, mgf1sha256*
- GZIP
- WS and JMS plugins

Anatomy of a message

```
<?xml version="1.0" encoding="utf-8"?>
<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope">
      <env:Header>
            <eb:Messaging xmlns:eb="http://docs.oasis-open.org/ebxml-msg
      <eb:UserMessage mpc="http://docs.oasis-open.org/ebxml-msg                                    ...
                </eb:UserMessage>
            </eb:Messaging>
            <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss
                <xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001
                        <xenc:EncryptionMethod Algorithm="http://www.w3.
                        ...
                </xenc:EncryptedKey>
                <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001
                    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2009/xmlenc11#aes128-gcm"/>
                        ...
                </xenc:EncryptedData>
                <ds:Signature xmlns:ds=""http://www.w3.org/2000/09/xmldsig#"
                        ...
                </ds:Signature>
            </wsse:Security>
      </env:Header>
   <env:Body/>
</env:Envelope>
```

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