

Dynamic Discovery Webinar

8 June 2023



Reminder



Webinar is recorded



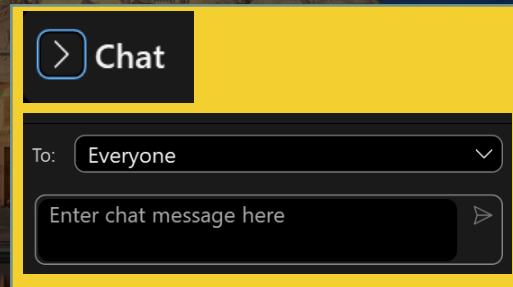
Place your Qs in the chat section



Raise your hand if you want to speak or ask Q



Mute your microphone



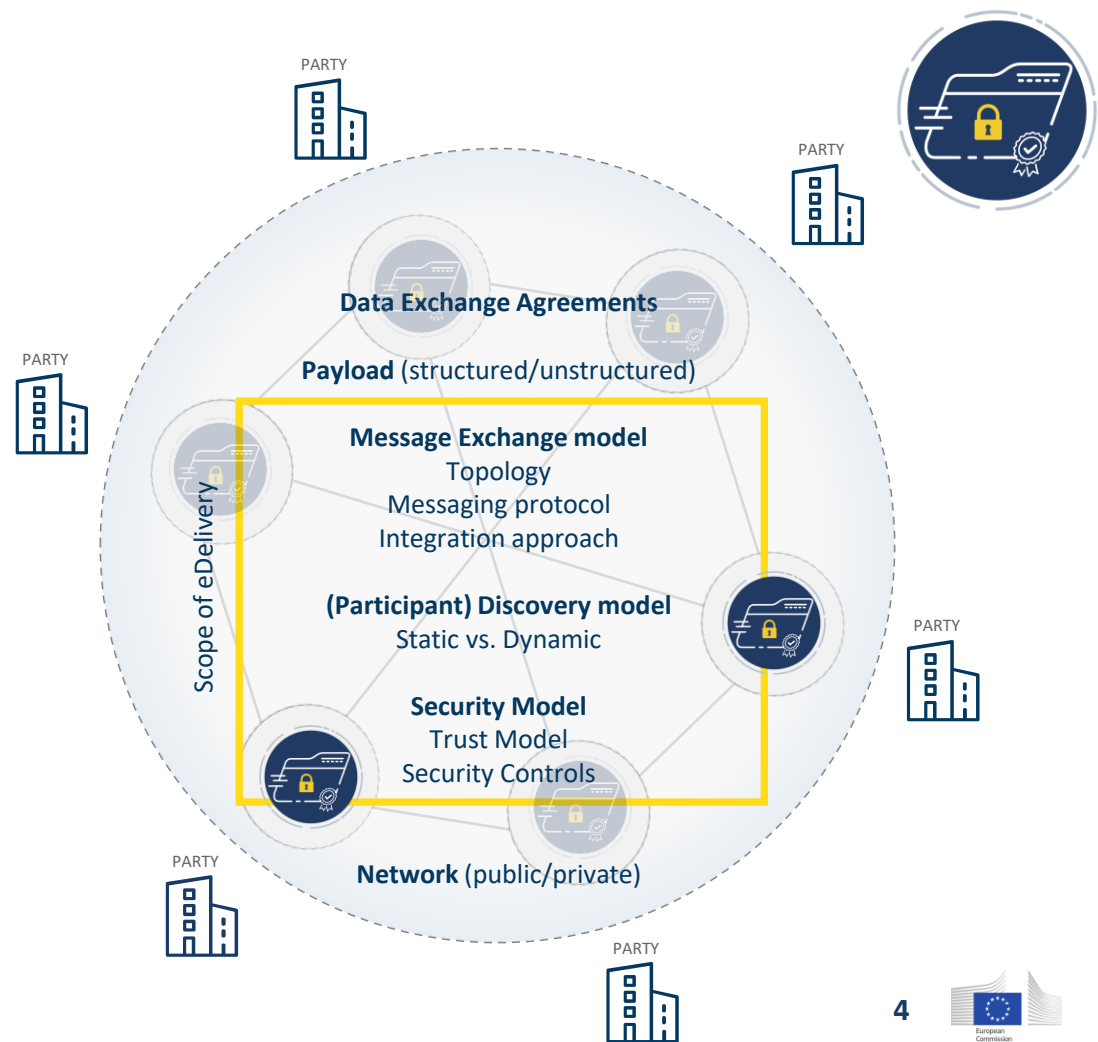
eDelivery Building Block and SMP/SML

Bogdan Dumitriu







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.



eDelivery Service Offering



SOFTWARE	
Sample software maintained by the EC (with documentation)	
Access Point (AP)	 
Service Metadata Publisher (SMP)	
Service Metadata Locator (SML)	

OPERATIONS SERVICES		
Managed services	Testing services	Supporting services
Public Key Infrastructure (PKI)	Connectivity testing	Training & Deployment
Service Metadata Locator (SML)	Conformance testing	Service Desk

STAKEHOLDER MANAGEMENT SERVICES	
Onboarding services (for stakeholders)	Community management services
Self-assessment tool	Developers Community
Onboarding of new stakeholders	Market guide
Cost estimation tool	

TECHNICAL SPECIFICATIONS				
Access point specifications	SMP specifications	SML specifications	Security control guidance	Trust models guidance
			Guidance on digital certificates	

STANDARDS OF SOs
Standards monitoring



Service offering Description (SOD)

All services are described in a SOD describing its purpose, the users for which it is for, its benefits and the process to obtain it



Service Level Arrangements (SLA)

Documents that describe Service Level Targets to be reached when delivering Building Block Services.



eLearning, videos, success stories

Some services feature multimedia such as eLearnings, instructional videos or success stories to help grasp what the service is about

Digital Europe platform

eDelivery service offering, and more about the building block, can be found online

Digital Europe

SMP 1.10 conformant solutions



More information on Digital Europe

[SMP Conformant Solutions >](#)



- **Datainterchange – EPIC**
- **eConnect – Procurement Service Bus (PSB)**
- **Edicom SMP**
- **eefacta server**
- **Galaxy Gateway**
- **Harmony eDelivery Access**
- **ion-SMP**
- **phoss**
- **Qvalia**
- **DomiSMP (EC Sample Software)**



eDelivery SMP 2.0 specification

May 2018



eDelivery SMP 1.10

- Support for OASIS SMP version 2.0
- Allow publishing multiple certificates (signing, encryption, key exchange) for a transport
- Supports eDelivery AS4 1.15 and 2.0

Q3-Q4 2023



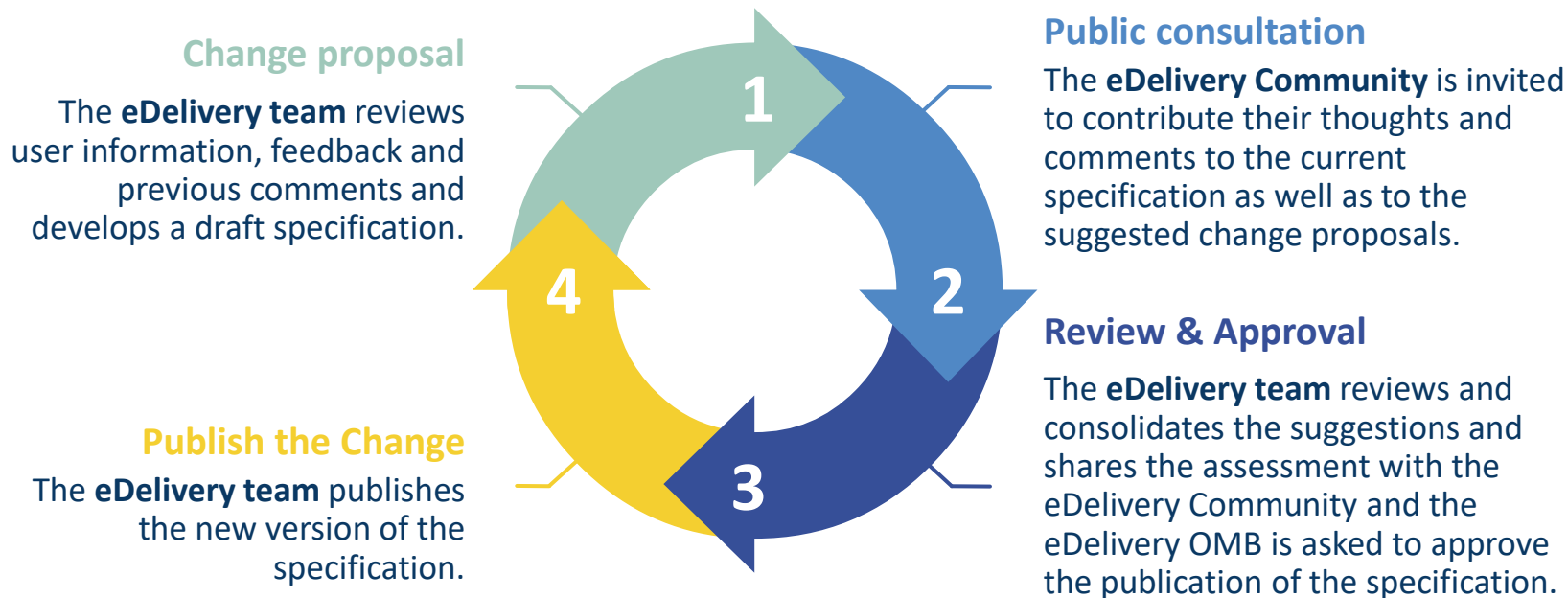
eDelivery SMP 2.0

eDelivery SMP profile 2.0 draft available:
<https://ec.europa.eu/digital-building-blocks/wikis/x/xqfXGw>



eDelivery Specification Change Process

The consultation is part of our change management process to involve the eDelivery community (transparently) in the assessment of change requests and in the creation of community drafts



Projects using eDelivery with SMP/SML



Interconnection of Insolvency Registers (IRI)



Business Registers Interconnection System (BRIS)



European Product Registry for Energy Labelling (EPREL)



Council Information Exchange Platform (CIxP)



DECIDE Decision



European Maritime Single Window environment (EMSWe)



European Database on Medical Devices (EUDAMED)



Beneficial Ownership Registers Interconnection System (BORIS)



Poison Centres Notification System (PCN)



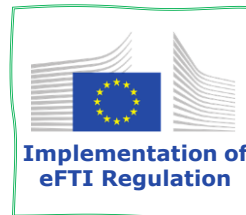
eEvidence Digital Exchange System



European Hull Database (EHDB)



EU Common Entry Gate for Tobacco Reporting (EU-CEG)



Implementation of eFTI Regulation



European Crew Database (ECDB)

Would like to learn more about eDelivery?

Stay in touch!



eDelivery User Community

The eDelivery User Community space enables stakeholders to share experiences and best practices on the exchange of electronic data and documents between public administrations, businesses and citizens. Pan-European projects (re)using eDelivery have their own sub-communities within this space.

Register for personalised eDelivery news

here  <https://europa.eu/!8rtpfj>

More about eDelivery

 @edeliveryBB

 <https://europa.eu/!hwcjvy>

 [eDelivery events \(DEP\) - YouTube](#)



Newsletter



Events



Interoperability Forum



Webinars



Relaunch of the eDelivery Interoperability Forum (part 2 – discussions)



- The Forum is a platform for the eDelivery BB and for solution and services providers to **explore together the technical evolution, market opportunities and market needs around eDelivery**
- Aims to promote knowledge sharing, provide feedback on challenges, needs and preferences, and facilitate the discussion for the way forward
- First post-pandemic edition of the Forum took place on May 3rd (check [here](#) for event details)

Don't miss the **next meeting on 27th June!** Apply to be a point of contact for the Forum [here](#)



2023 Calendar



[eDelivery
Interopera
bility
Forum
27 June](#)

eDelivery



[Archive of
past events](#)



[Webinar
eDelivery value
proposition
28 September
\(TBC\)](#)



[Survey to
collect the
interests
to future
webinars](#)

Publications

Feel free to register here
eDelivery (4x/year)

<https://europa.eu/!v4njKB>

Building Blocks (2x/year)

<https://europa.eu/!jj87JU>



Digital eDelivery Newsletter

Get the latest news about eDelivery, part of the eIDAS enablers Family of Building Blocks

Hello everyone,

We are excited to share with you this first edition of the Digital eDelivery Newsletter. This newsletter will inform you on important news and technical updates for eDelivery, provide an outlook of what we have planned for the coming months, and share information on our upcoming events. Highlights include an invitation to our hands-on webinar on the 13th of July, and news that eDelivery has been proposed as best reusable solution for the Once-Only Technical System (OOTS).

We hope you enjoy this first edition of the Newsletter. If you have a story to tell us about how eDelivery is helping you creating a Digital Europe, just reply to this email and you may be featured in our next newsletter.

Please scroll to the end for information about this newsletter.



Digital Europe Newsletter

Get the latest news about eIDAS enablers Family of Building Blocks.

Hello everyone,

We are excited to welcome you to the very first edition of our DIGITAL Building Blocks Bulletin and want to **warmly thank you for your continued interest in the Building Blocks!**

The beginning of 2022 has marked a new chapter in our collective efforts for creating a truly digital Europe. The work begun under CEF Digital continues under the **Digital Europe Programme (DIGITAL) (2021-2027)**, the EU's new funding programme aiming to bring digital technology to businesses, citizens, and public administrations.



Events



Success stories

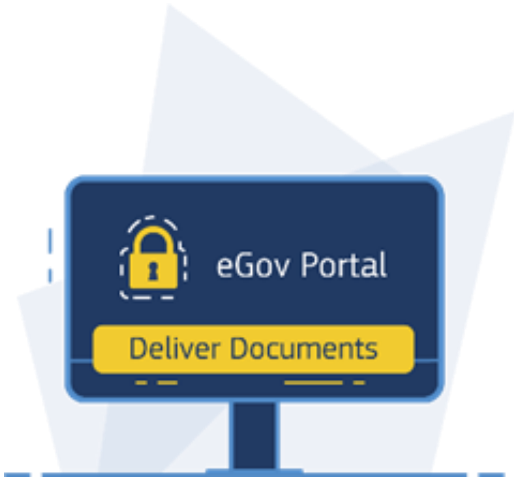


News



Technical Updates

Have a question?



eDelivery

Exchange data and documents
online reliably and securely



Bogdan Dumitriu



To continue the conversation,
contact our team via email

Emails:

EC-digital-building-blocks@ec.europa.eu



EC-eDelivery-support@ec.europa.eu



Thank you

& stay in touch



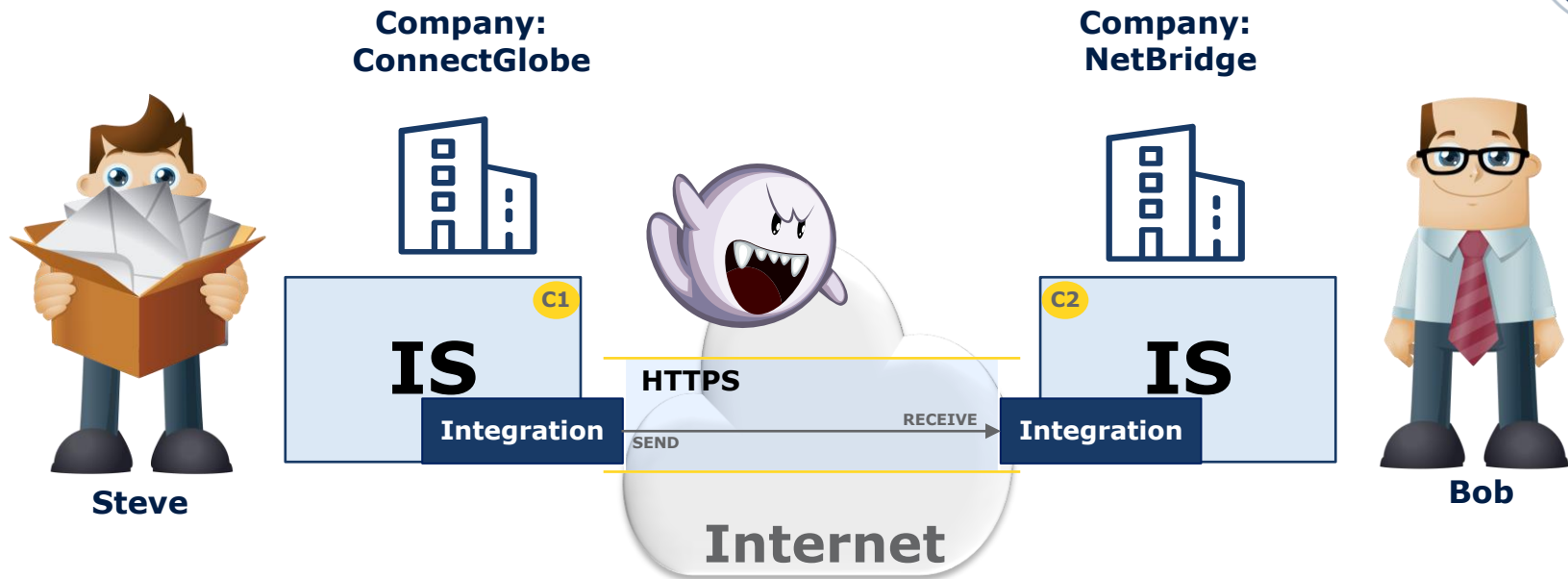
Dynamic Discovery Service

Jože Rihtaršič





Message exchange: Connecting the IS

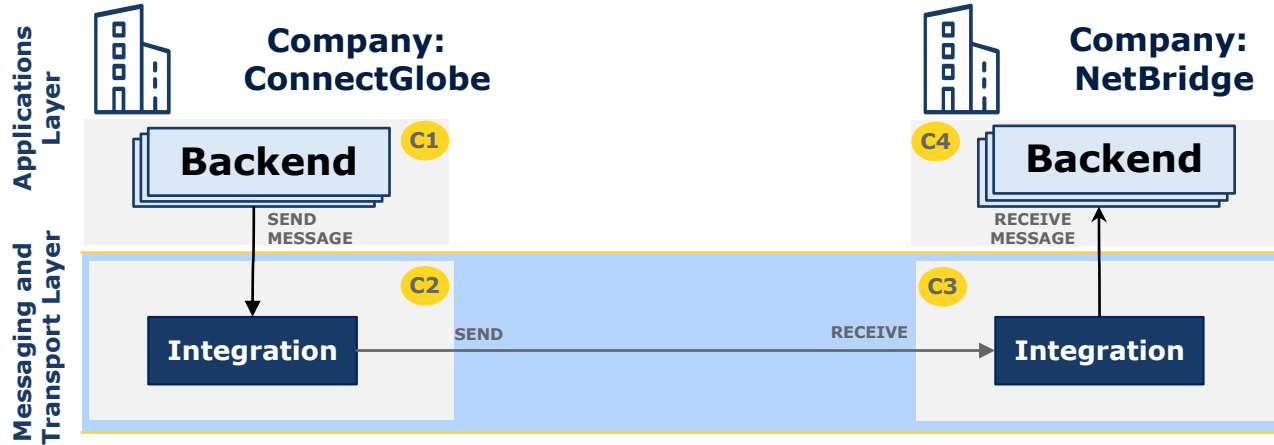


- **URL ADDRESS**
- **HTTPS/TLS Certificate(s)**

Message exchange: Extract integration module



Steve



Bob

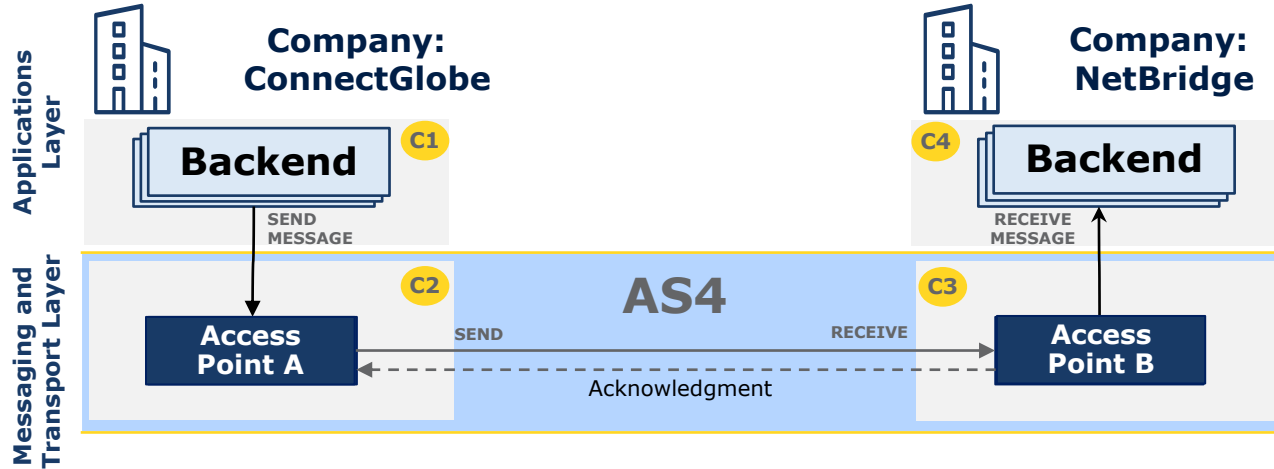
Extracting the integration module into a dedicated component:

- Reuse the component (Reducing development and maintenance costs).
- Loosely coupled components (Easier to maintain and develop).
- Allows different teams to be responsible for integration/messaging service and backend system.
- Allows option to use "Messaging service provider".
- Allows replacement of the messaging service with up-to-date technologies/standards.
-

Message exchange: Enhancement of integration



Steve



Bob

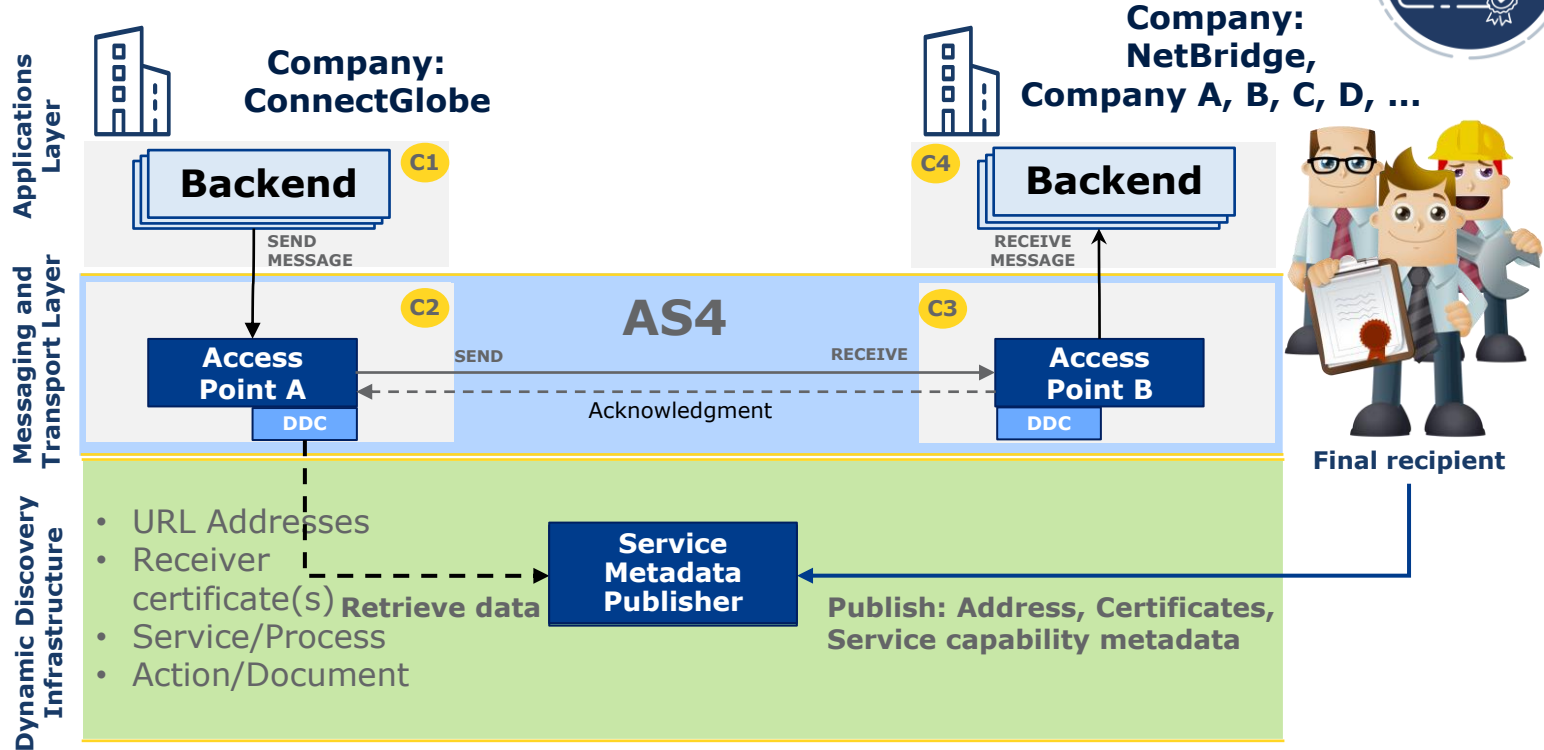
Enhancement of integration:

- Business context: (Transaction/Conversation Id, Service/Process, Action/Document)
 - Message routing,
 - Basic payload or/and message metadata validation.
- Reliability (Acknowledgment/Error Signal messages).
- Message Authenticity (eSignature)

Message exchange: Dynamic Discovery infrastructure



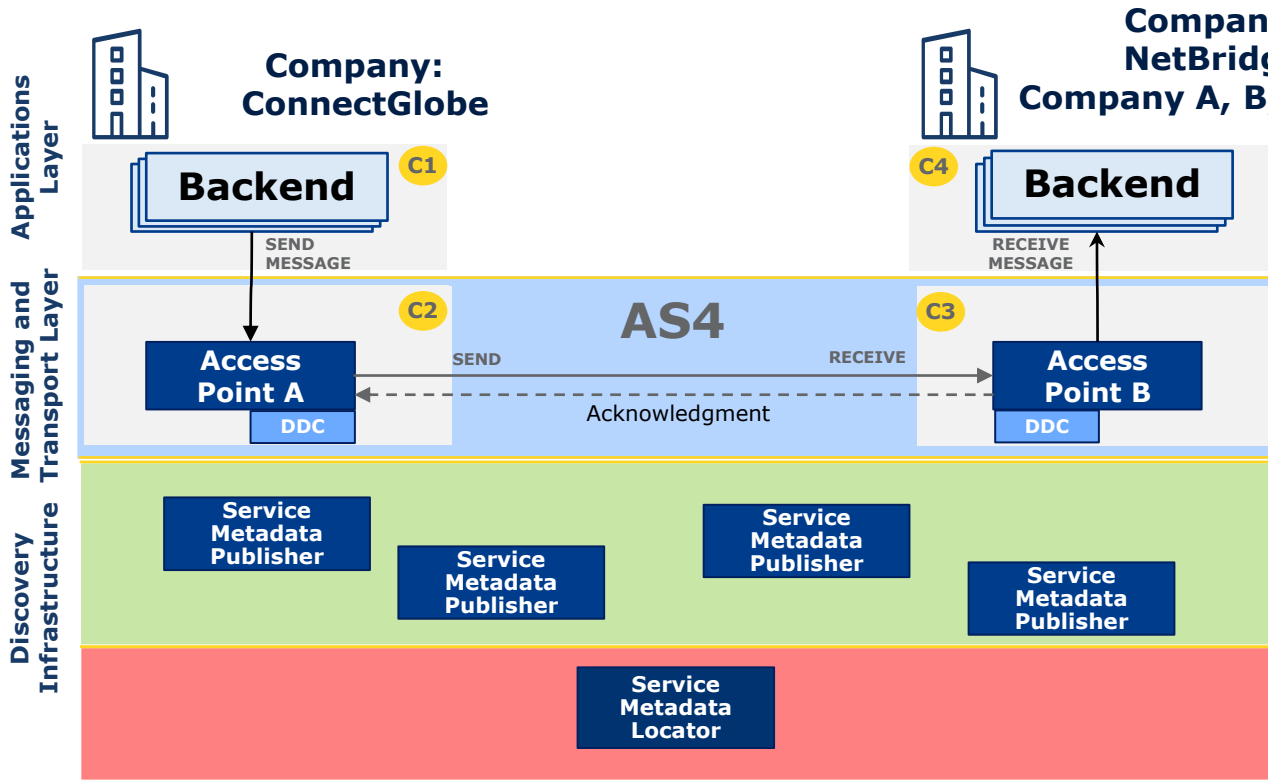
Original sender



Message exchange: Delegated Dynamic Discovery infrastructure



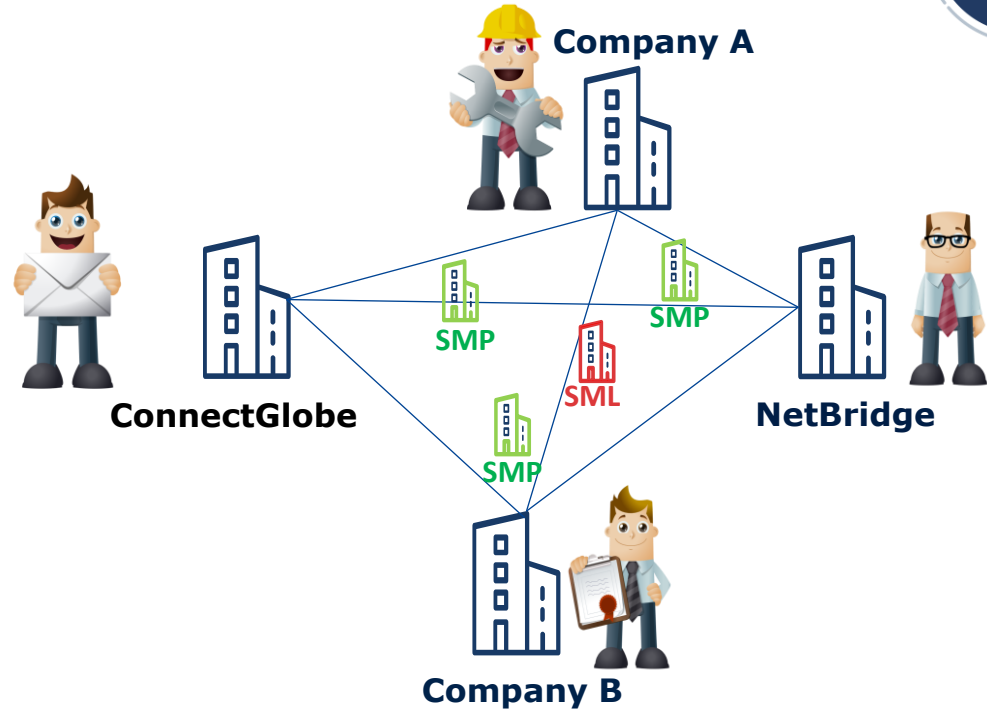
Original sender



Final recipient

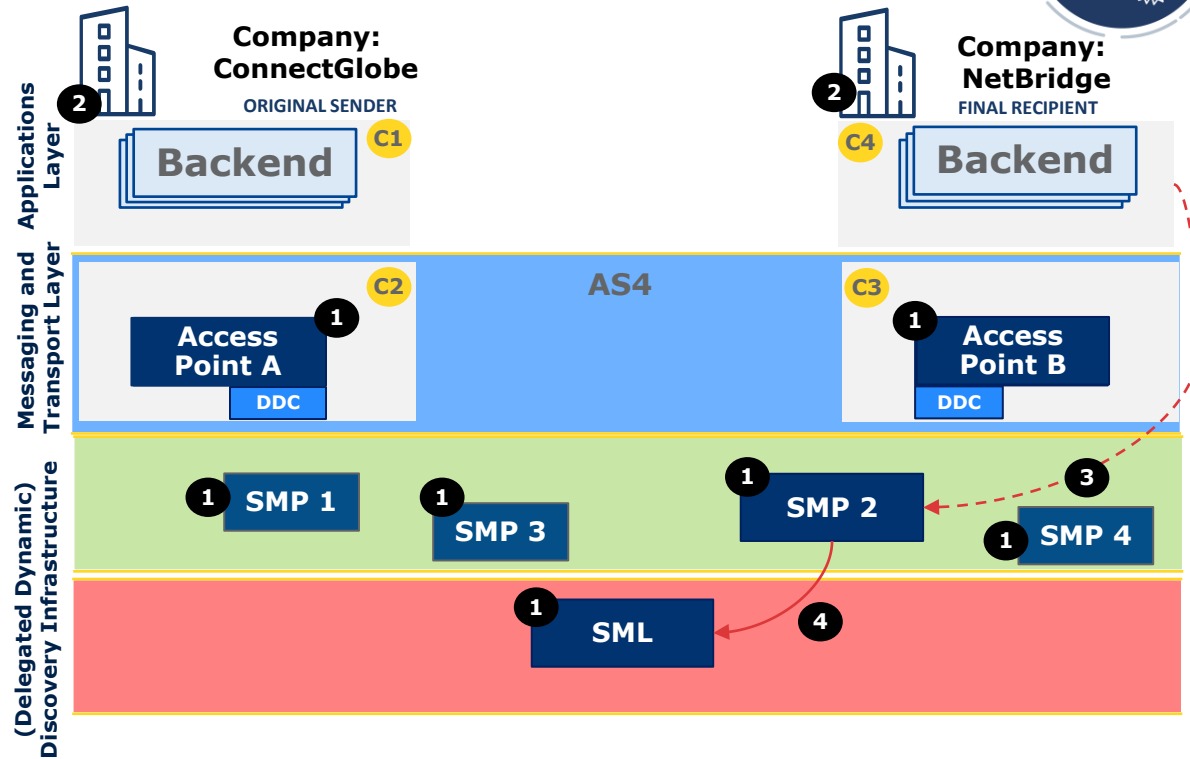
Message exchange: Business domain network of participants

- Business domain owner (Network rules):
 - Document types
 - Participant identifier types and formats
 - Visibility: public/closed
 - Trust model
 - SMP providers
 - SML provider(s)
 - Discovery parameters
 - ...



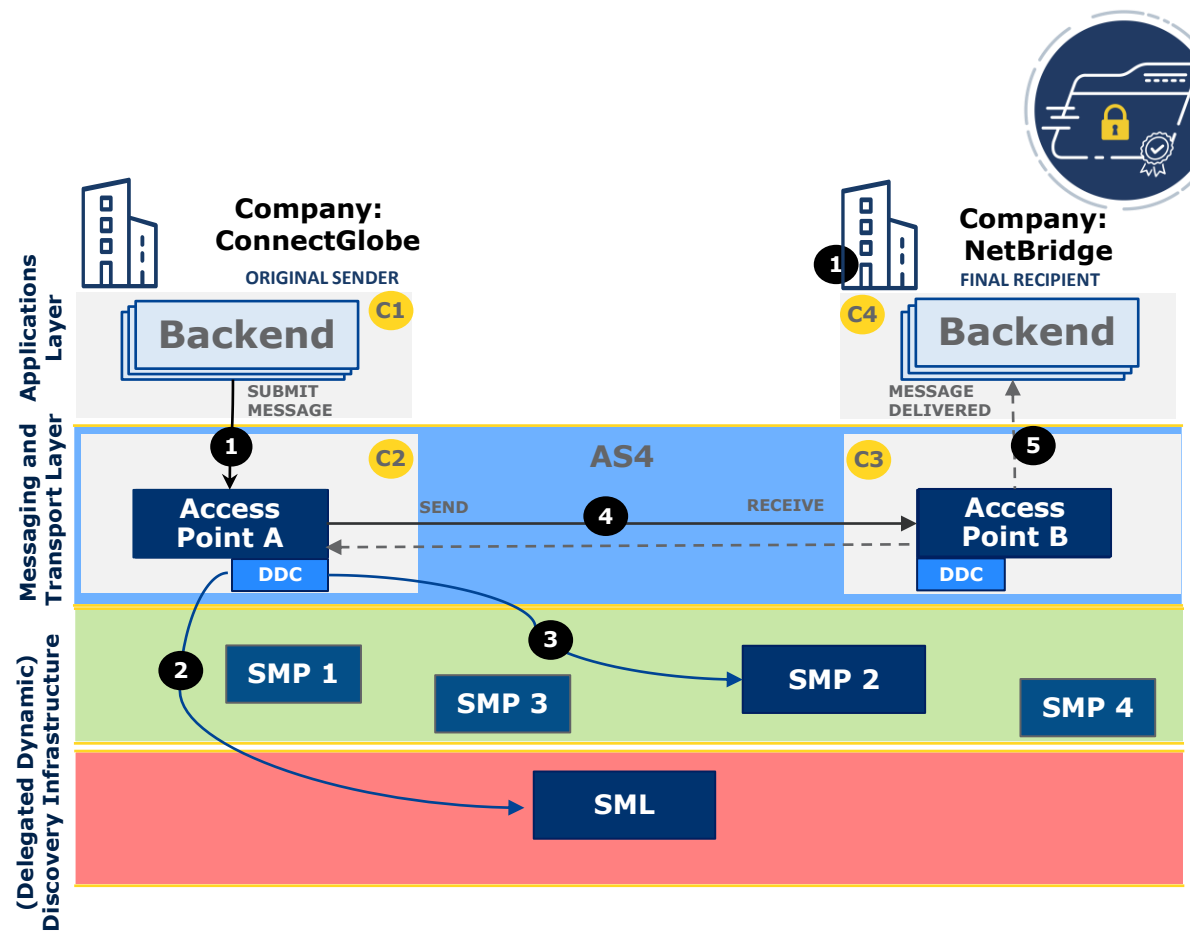
Overview: Dynamic Discovery process: Getting ready

1. Established network trust model (combination of technical solutions and network policies) Example: All network components (APs, SMPs, SMLs) have valid and trusted Certificates.
2. Network participants obtain unique identifiers for the message exchange network.
3. "Final Recipient" publishes the service metadata to chosen SMP.
4. The SMPs registers "Final Recipient" identifier to SML.



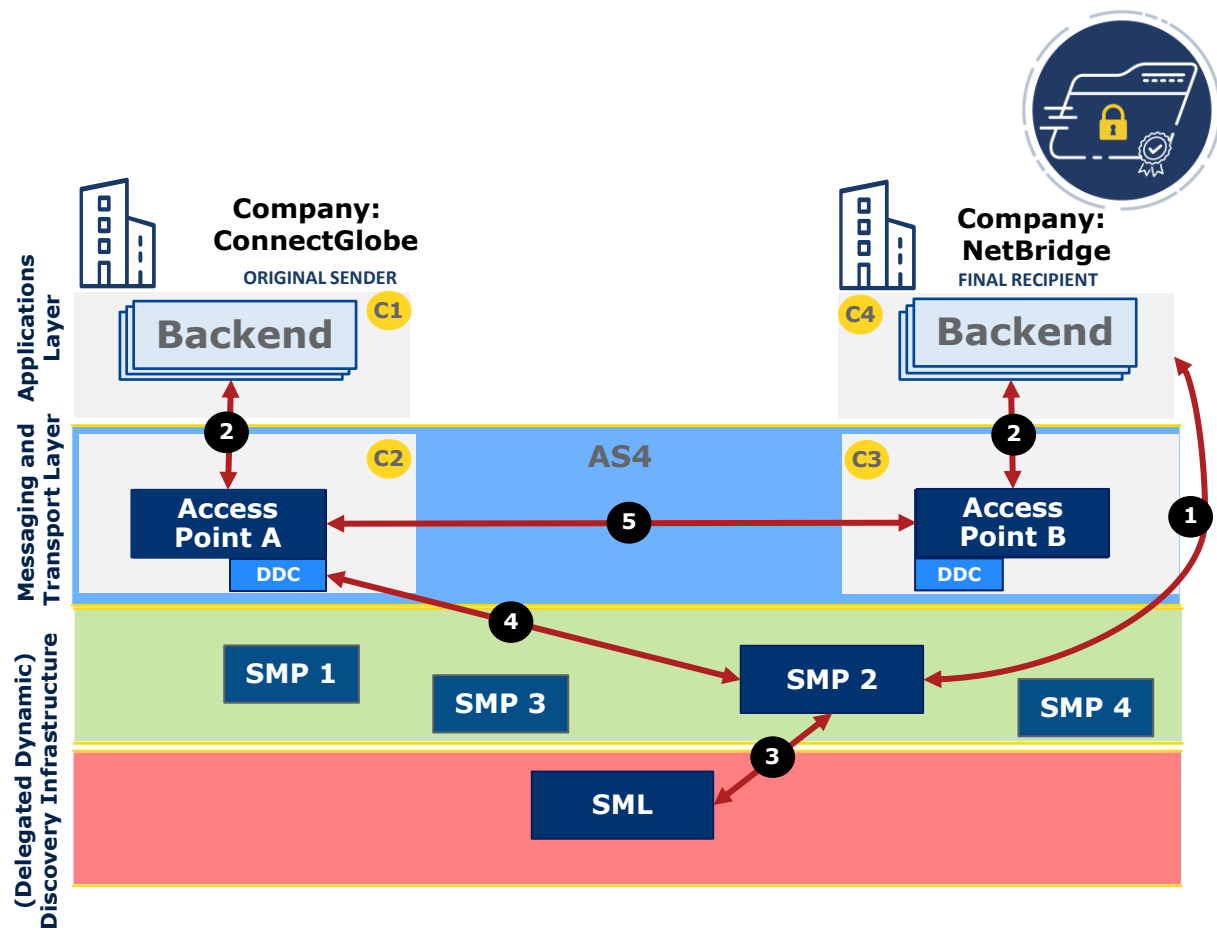
Overview: Dynamic Discovery process: Message delivery

1. Original Sender (ConnectGlobe) submits the message to Access Point A.
2. The Dynamic Discovery Client DDC(A) queries the SML for the URL Address of SMP where the Final Recipient (NetBridge) published service metadata.
3. The DDC(A) retrieves the service metadata from the targeted SMP (SMP 2). DDC(A) validates the integrity and the authenticity of the data received from SMP 2.
4. Access Point A submits the message to discovered Access Point B. The Access Point B validates the message integrity and authenticity.
5. Final recipient (NetBridge) receives the message from the Access Point B.



Establishing the network trust model

- Enables the integrity and authenticity of exchanged data between network components.
- Combination of technical solutions and business domain network policies.
- The trust between components (Integrity and authenticity data validation):
 1. Company/Participant <--> SMP provider
 2. Company/Participant <--> Access point provider
 3. SMP provider <--> SML provider
 4. Access point (DDC) <--> SMP provider
 1. Access point <--> Access point



Trust Model examples: X509 Certificates and trust anchors



Dedicated Domain PKI

In this model, digital certificates are associated with a single trust anchor dedicated to a business domain network. For example, in the eProcurement domain, PEPPOL operates a dedicated PKI.

Validation of trust:

All certificates issued from a dedicated issuer/CA are considered trusted.

Shared Domain PKI

In this model, digital certificates are associated to a single trust anchor which is shared on multiple domains. But the certificates have domain specific constraints which can be validated: subject regular expression, Certificate policies, etc.

Validation of trust:

Certificate is trusted if is issued from a dedicated issuer/CA and matches the domain constraints (subject, certificate policy, etc..).

Domain Trusted List

This model relies on a list containing the trusted certificates and/or trust anchors complying with a domain trust policies.

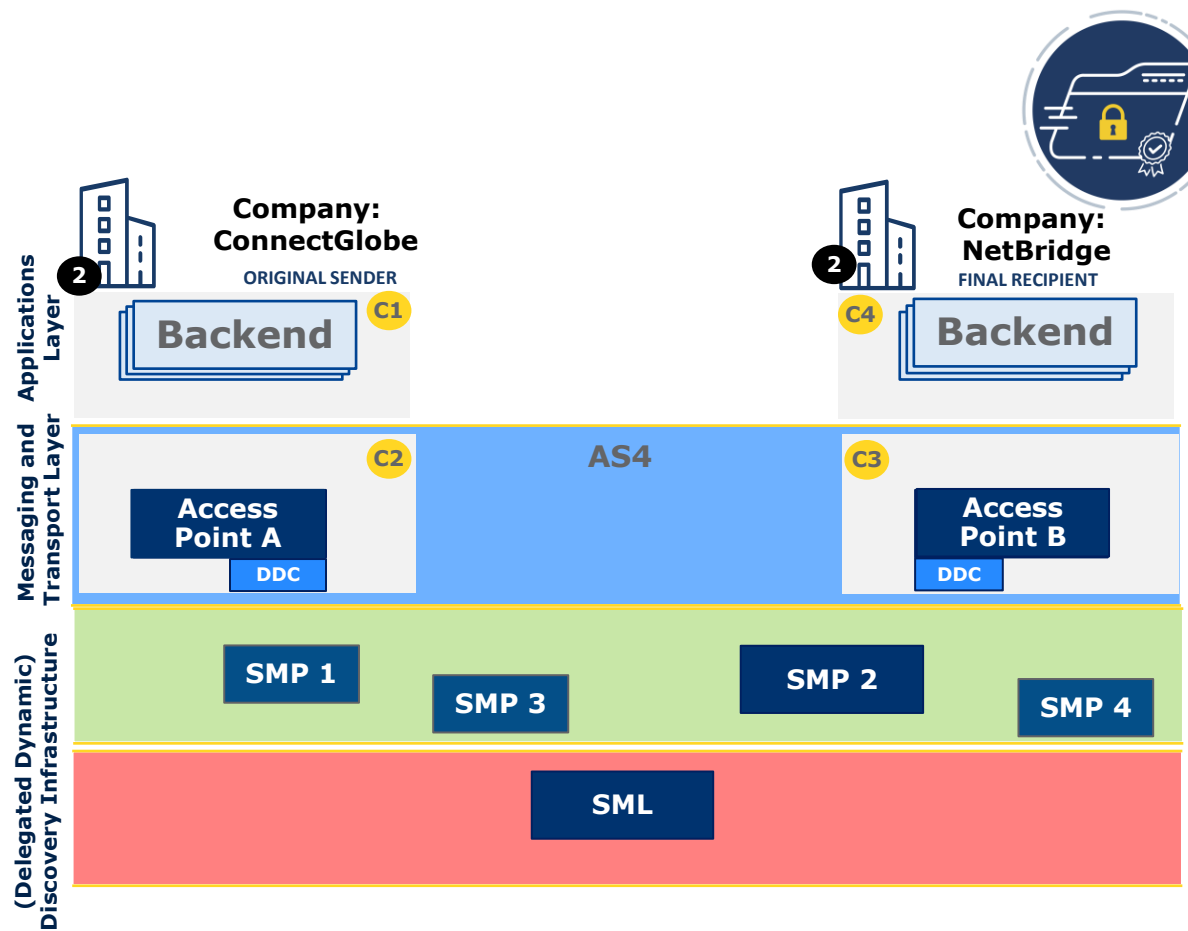
Validation of trust:

Business domain owner provides:

- Dedicated web services for validating Certificates.
- Publish/distribute the truststore.
- Blockchain technology as identity provider map components ID and Certificates in Blockchain ledger (Experimental).

Dynamic Discovery process: Getting ready/registration

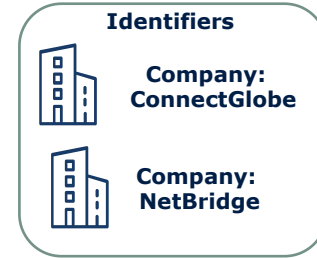
1. Established network trust model (combination of technical solutions and network policies) Example: All network components (APs, SMPs, SMLs) have valid and trusted Certificates.
2. **Network participants obtains a unique identifiers for the message exchange network.**



Participant identifiers



- Participant Identifiers are the input data for:
 - Message addressing (Original Sender, Final Recipient).
 - Creating the SML queries.
 - Retrieving the data from the SMP instance.
- Participant Identifier must belong to only one participant/company in the network.
- Types, Catalogues of participant identifiers:
 - Custom identifier. E.g.: ehealth-participantid-qns::urn:ehealth:eu:ncp-idp
 - National identifiers: VAT numbers, company registration number, ...
 - International identifiers: International catalogues of identifiers: ISO 6523, ISO 9735, ISO 20022, ...

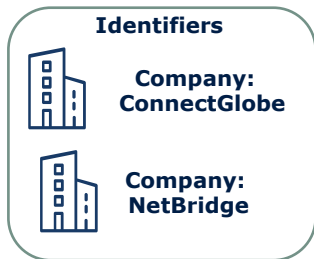




Participant identifiers

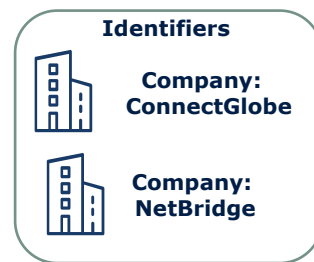
Example

- NetBridge has GLN number: 2203148000007
- Connect Globe: Belgium VAT number: 0465878231
- ISO 6523: international standard/catalogue that defines a structure for uniquely identifying organisations. The identifier consists of two mandatory parts:
 - International Code Designator (ICD), uniquely identifies the authority which issued the code to the organisation, up to 4 digits:
 - The ICD for the GLN number: 0088
 - The ICD for Belgium VAT numbers: 0206
 - Organisation identifier, up to a maximum of 35 characters
- NetBridge: **ISO6523** Registrar with ICD value **0088**: Identifier: **2203148000007**
- Connect Globe: **ISO6523** Registrar with ICD value **0206**: Identifier: **0465878231**



Participant Identifier formatting

The Participant Identifier consists of two parts: a scheme and a value.



Oasis ebCore Party Identifier format:

Example: urn:oasis:names:tc:ebcore:partyid-type:iso6523:0088:220314800007

Template: <urn:oasis:tc:ebcore:partyid-type:[catalog-identifier]:[scheme-in-catalog]>:<[scheme-specific-identifier]>

Scheme: urn:oasis:names:tc:ebcore:partyid-type:iso6523:0088

Value: 220314800007

Peppol Party Identifier format:

Example: iso6523-actorid-upis::0088:220314800007

Template: <peppol-participant-identifier-meta-scheme>::<identifier-value>

Scheme: iso6523-actorid-upis

Value: 0088:220314800007

Example of custom Party Identifier format:

Example: ehealth-participantid-qns::urn:ehealth:eu:ncp-idp

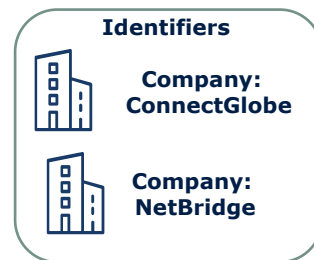
Template: <identifier-scheme>::<identifier-value>

Scheme: ehealth-participantid-qns,

Value: urn:ehealth:eu:ncp-idp

Participant Identifier formatting

Document (XML) notation



Oasis ebCore Party Identifier format:

Scheme: `urn:oasis:names:tc:ebcore:partyid-type:iso6523:0088`, **Value:** `220314800007`

```
<ParticipantIdentifier scheme="urn:oasis:names:tc:ebcore:partyid-type:iso6523:0088">220314800007</ParticipantIdentifier>
```

Note: eDelivery AS4 profile's Dynamic Discovery enhancement does not use **scheme!** (Better fit to Oasis SMP standard)

```
<ParticipantIdentifier>urn:oasis:names:tc:ebcore:partyid-type:iso6523:0088:220314800007</ParticipantIdentifier>
```

Peppol Party Identifier format:

Scheme: `iso6523-actorid-upis`, **Value:** `0088:220314800007`

```
<ParticipantIdentifier scheme="iso6523-actorid-upis">0088:220314800007</ParticipantIdentifier>
```

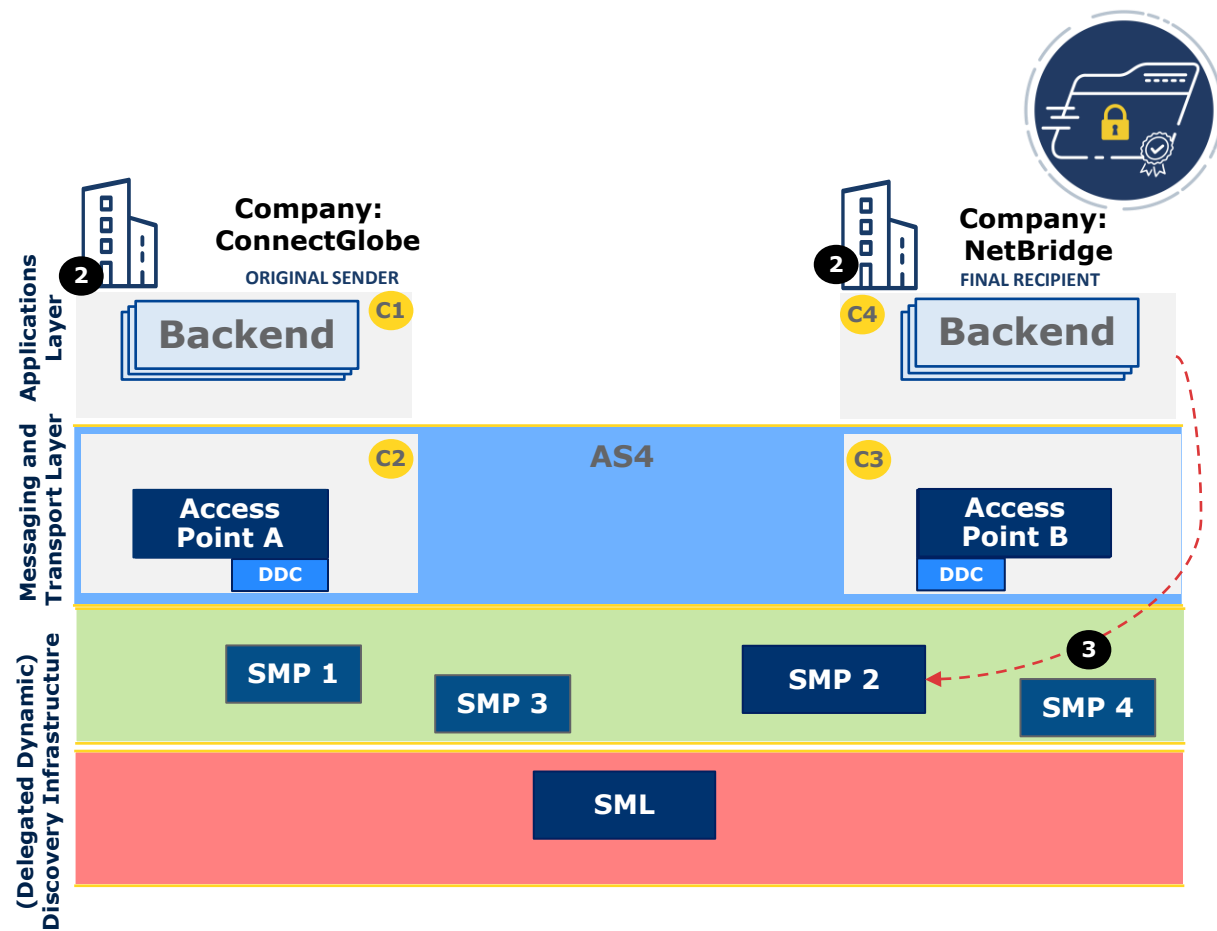
Example of custom Party Identifier format:

Scheme: `ehealth-participantid-qns`, **Value:** `urn:ehealth:eu:ncp-id`

```
<ParticipantIdentifier scheme="ehealth-participantid-qns">urn:ehealth:eu:ncp-id</ParticipantIdentifier>
```

Dynamic Discovery process: Getting ready/Registration

1. Established network trust model (combination of technical solutions and network policies) example: All network components (APs, SMPs, SMLs) have valid and trusted certificates.
2. Network participants obtain unique identifiers for the message exchange network.
3. "Final Recipient" publishes the service metadata to chosen SMP.





Publishing service metadata

- Request SMP provider to create a "placeholder" in the SMP instance with company identifier.

- Example of the URL address of web resource:

[https://smp-provider.eu/\[party-identifier\]](https://smp-provider.eu/[party-identifier])

The URL example

(Note: Identifier is URL encoded):

<https://smp-provider.eu/urn%3Aoasis%3Anames%3Atc%3Aebcore%3Apartyid-type%3Aiso6523%3A0088%3A220314800007>

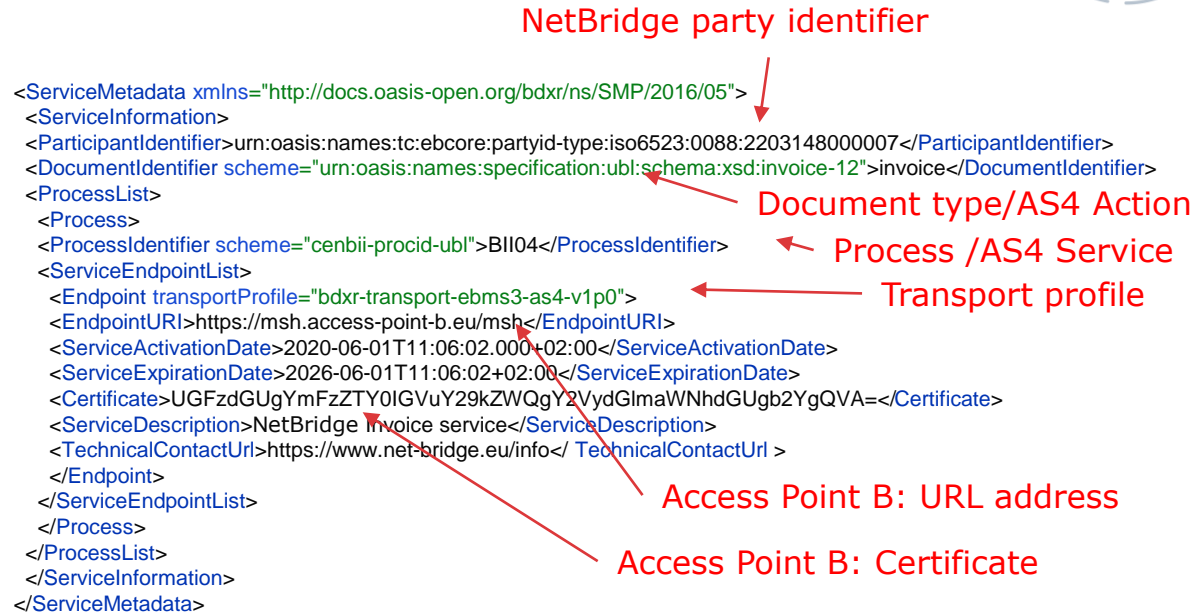
- Web resource document example (Oasis SMP 1.0 Document):

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceGroup xmlns="http://docs.oasis-open.org/bdxr/ns/SMP/2016/05">
  <ParticipantIdentifier>urn:oasis:names:tc:ebcore:partyid-type:iso6523:0088:220314800007</ParticipantIdentifier>
  <ServiceMetadataReferenceCollection />
</ServiceGroup>
```

Publishing service metadata

- Request SMP provider to create a "placeholder" in the SMP instance with company identifier.
- Company "NetBridge" publishes the service metadata.

The registration of the service metadata (Oasis SMP 1.0)





Published document definitions/types

- SMP Document type(s) must be supported by:
 - SMP service provider
 - Access Point/Dynamic Discovery client
- Options:
 - Oasis SMP 1.0
 - Oasis SMP 2.0
 - PEPPOL SMP (technical specification)
 - ...

• Oasis SMP 1.0 ServiceGroup document:

```
<ServiceGroup xmlns="http://docs.oasis-open.org/bdxc/ns/SMP/2016/05">
  <ParticipantIdentifier>urn:oasis:names:tc:ebcore:partyid-type:iso6523:0088:220314800007
</ParticipantIdentifier>
  <ServiceMetadataReferenceCollection>
    <ServiceMetadataReference href="http://service.smp-b.eu/urn..." />
  </ServiceMetadataReferenceCollection>
</ServiceGroup>
```

• Oasis SMP 2.0 ServiceGroup document:

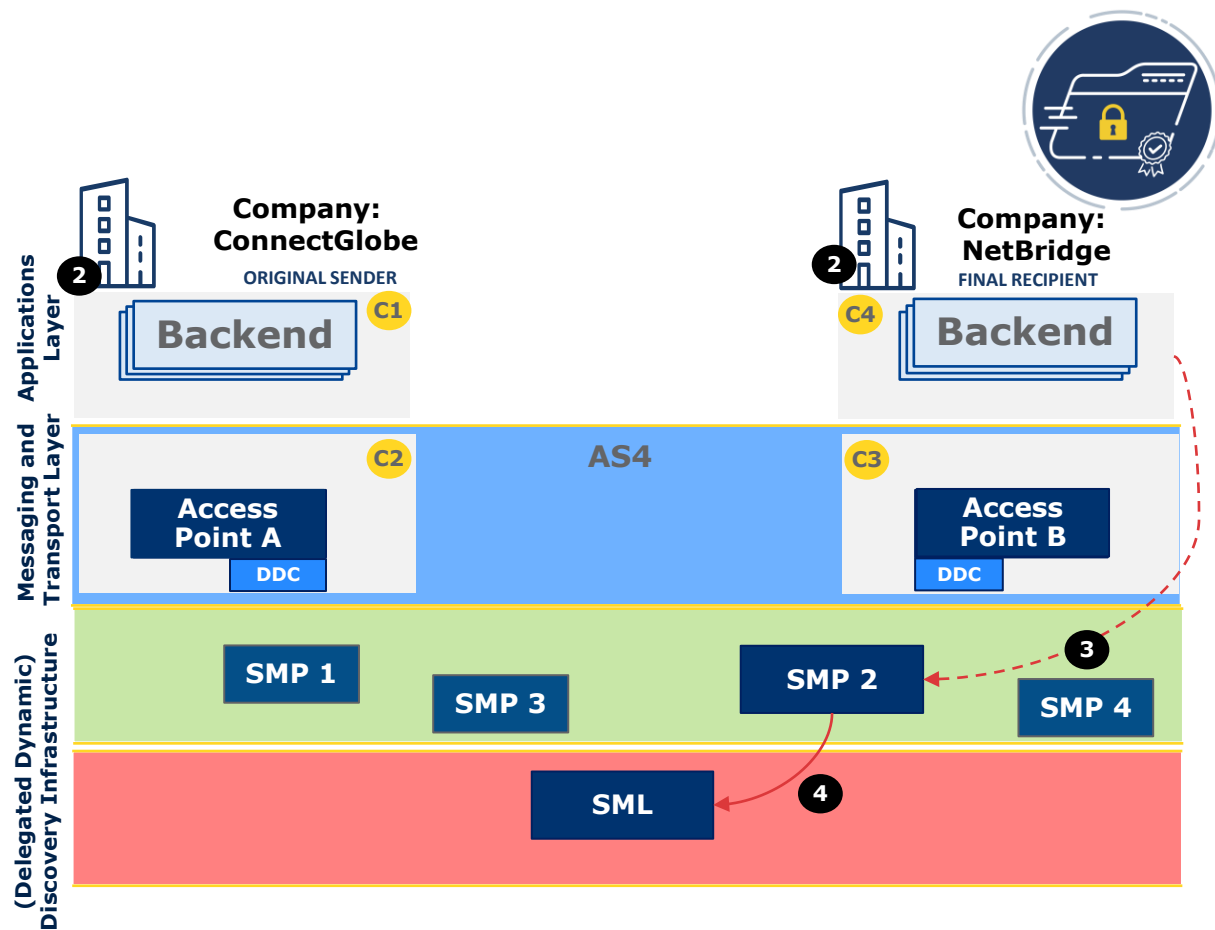
```
<ServiceGroup xmlns="http://docs.oasis-open.org/bdxc/ns/SMP/2/ServiceGroup" xmlns:smb=...>
  <smb:SMPVersionID>2.0</smb:SMPVersionID>
  <smb:ParticipantID>urn:oasis:names:tc:ebcore:partyid-type:iso6523:0088:220314800007
</smb:ParticipantID>
  <sma:ServiceReference>
    <smb:ID schemeID="urn:oasis:names:specification:ubl...">invoice</smb:ID>
    <sma:Process>
      <smb:ID schemeID="cenbii-procid-ubl">BII04</smb:ID>
    </sma:Process>
  </sma:ServiceReference>
</ServiceGroup>
```

• PEPPOL SMP ServiceGroup document:

```
<smp:ServiceGroup
  xmlns:smp="http://busdox.org/serviceMetadata/publishing/1.0/" ...>
  <id:ParticipantIdentifier>urn:oasis:names:tc:ebcore:partyid-type:iso6523:0088:220314800007
</id:ParticipantIdentifier>
  <smp:ServiceMetadataReferenceCollection>
    <smp:ServiceMetadataReference href="http://service.smp-b.eu/urn.." />
  </smp:ServiceMetadataReferenceCollection>
</smp:ServiceGroup>
```

Dynamic discovery process: Getting ready/registration

1. Established network trust model (combination of technical solutions and network policies) example: All network components (APs, SMPs, SMLs) have valid and trusted certificates.
2. Network participants obtain unique identifiers for the message exchange network.
3. "Final Recipient" publishes the service metadata to chosen SMPs.
4. **The SMPs registers "Final Recipient" identifier to SML.**



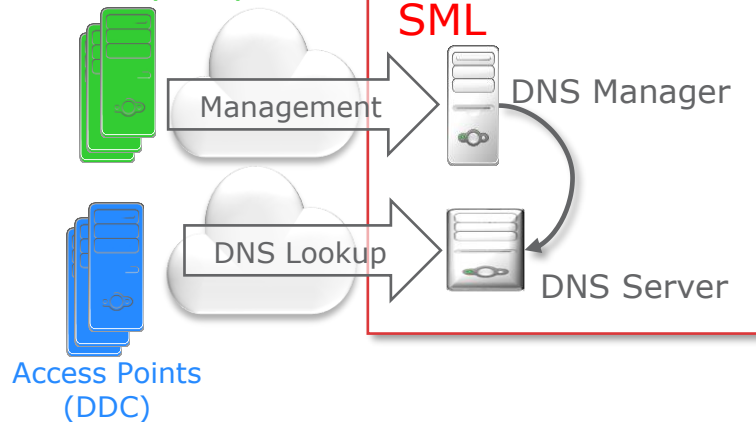
Register party identifier to SML

Two main functions of SML

- Management/registration
- Lookup

- The SML service has two endpoints:
 - **Management endpoint:** Interface used by SMP for participant registration management
 - **Lookup endpoint:** based on Domain Name System (DNS) protocol. (DNS server is the "key-value database" of the internet)

Service Metadata Publishers (SMPs)





SML management interface (HTTP SOAP Operations)

SMP management (ManageServiceMetadataService)	
Operation	Description
Create	Create a Service Metadata Publisher (SMP) metadata record, containing the metadata about the SMP.
Read	Retrieves the SMP record for the service metadata publisher.
Update	Updates the SMP record for the service metadata publisher.
Delete	Deletes the SMP record for the service metadata publisher.



SML Management interface (HTTP SOAP Operations)

Participant Management (ManageBusinessIdentifierService)	
Operation	Description
Create CreateList	Create Participant record(s) in BDMSL and DNS.
Delete DeleteList	Delete Participant record(s) from BDMSL and DNS.
List	List (pages of) Participants.
Migrate PrepareToMigrate	Migrate participant to new SMP.



SML Management interface (HTTP SOAP Operations)

SMP Management	
Operation	Description
ChangeCertificate	This operation allows the SMP owner to change the SMP's authentication certificate.
CreateParticipantIdentifier	This operation has the same behaviour as the Create() operation in the ManageParticipantIdentifier interface with the additional option to define the service name for NAPTR DNS record.
ExistsParticipantIdentifier	This operation allows SMP to verify if participant identifier is already registered.



Register Party identifier to SML

- Registration (SOAP request)
- Create DNS Record(s) to DNS server
 - NAPTR
 - CNAME (eDelivery legacy)

- SMP registers participant identifier to SML

```
<soapenv:Envelope xmlns:soapenv=...>
  <soapenv:Body>
    <ns:CreateParticipantIdentifier>
      <ns:ServiceMetadataPublisherID>smp-b</ns:ServiceMetadataPublisherID>
      <ns1:ParticipantIdentifier>urn:oasis:names:tc:ebcore:partyid-type:iso6523:0088:220314800007
    </ns1:ParticipantIdentifier>
    </ns:CreateParticipantIdentifier>
  </soapenv:Body>
</soapenv:Envelope>
```

- DNS NAPTR record

Q5[...]Q.sml.service.eu. 60 NAPTR "Meta:SMP" "!.*!https://service.smp-b.eu/smp!"

DNS Record
Domain

NAPTR service

DNS Record Type

- DNS CNAME record

B-a5[...]04.sml.service.eu. 60 CNAME service.smp-b.eu.

TTL

DNS Record Value



DNS Domain for NAPTR Records

- SML-zone name
 - Defines the DNS "search" space of network: Ex:
sml-service.eu
my-network.sml-service.eu
 - Owned by the SML service provider.
- ID-scheme (Optional)
 - Scheme part of participant identifier
- Hash value over normalized participant identifier (with or without scheme)
 - Hash SHA256
 - Base32(no padding)
 - Upper case

NAPTR record:

<hash(sha256)-over-identifier>[.<ID-scheme>].<SML-zone-name>

- ebCoreParty Identifier format:

<ParticipantIdentifier>urn:oasis:names:tc:ebcore:partyid-type:iso6523:0088:2203148000007</ParticipantIdentifier>

Q5BGWHKA3TGO5XM2Z6JRXMXEWAP2MAH7LKKFYOGP5Y3546TZATRQ.sml-service.eu

- Peppol identifier format:

<ParticipantIdentifier scheme="iso6523-actorid-upis">0088:2203148000007</ParticipantIdentifier>

4UMAAIZDFWP76HPXFUBIJBN7T7MCE3IAKPSVJBIQSWZAB6YRTXRQ.iso6523-actorid-upis.sml-service.eu



DNS Domain for CNAME

- Hash value over normalized participant identifier (with or without scheme)
 - Hash MD5
 - Hexadecimal encoded
 - Lower case

CNAME record:

B-`<hash(md5)-over-identifier>`[.`<ID-scheme>`].`<SML-zone-name>`

- ebCoreParty identifier format:

`<ParticipantIdentifier>`urn:oasis:names:tc:ebcore:partyid-type:iso6523:0088:220314800007
`</ParticipantIdentifier>`

B-a55572feed1a024bc126e015b4d8bc04.sml-service.eu

- Peppol identifier format

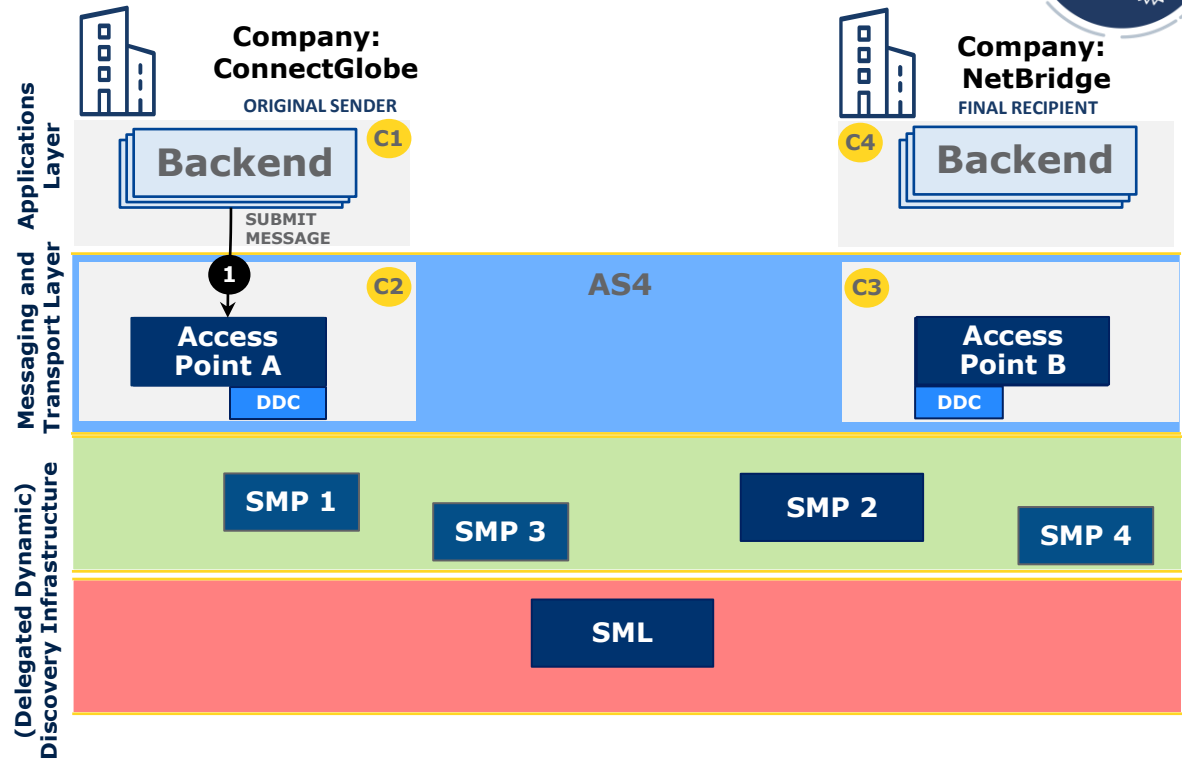
`<ParticipantIdentifier scheme="iso6523-actorid-upis">`0088:220314800007`</ParticipantIdentifier>`

B-4f8bd4366e43ba9180ab9bf9a628f405.iso6523-actorid-upis.sml-service.eu

Dynamic Discovery process: Message delivery



1. Original Sender (ConnectGlobe) submits the message to Access Point A.





1. Company A submits the message to "Access Point A".

```
<soap:Envelope .... >
<soap:Header>
<ns:Messaging>
  <ns:UserMessage>
    <ns:PartyInfo>
      <ns:From>
        <ns:PartyId type="urn:oasis:names:tc:ebcore:partyid-type:unregistered">access-point-a</ns:PartyId>
        <ns:Role>http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/initiator</ns:Role>
      </ns:From>
    </ns:PartyInfo>
    <ns:CollaborationInfo>
      <ns:Service type="cenbii-procid-ubl">BII04</ns:Service>
      <ns:Action>urn:oasis:names:specification:ubl:schema:xsd:invoice-12::invoice</ns:Action>
    </ns:CollaborationInfo>
    <ns:MessageProperties>
      <ns:Property name="originalSender">urn:oasis:names:tc:ebcore:partyid-type:iso6523:0088:999999999999997</ns:Property>
      <ns:Property name="finalRecipient">urn:oasis:names:tc:ebcore:partyid-type:iso6523:0088:2203148000007</ns:Property>
    </ns:MessageProperties>
    <ns:PayloadInfo>
      <ns:PartInfo href="cid:message">
        <ns:PartProperties>
          <ns:Property name="MimeType">text/xml</ns:Property>
        </ns:PartProperties>
      </ns:PartInfo>
    </ns:PayloadInfo>
  </ns:UserMessage>
</ns:Messaging>
</soap:Header>
<soap:Body>
<msg:submitRequest>
  <payload payloadId="cid:message" contentType="text/xml">
    <value>PD94bWwgdmlvbj0iMS4wliBlbmNvZGluz0iVVRGLTgiPz4KPz4KZGhlcGxvPndvcmxkPC9oZWxsYXZ4=</value>
  </payload>
</msg:submitRequest>
</soap:Body>
</soap:Envelope>
```

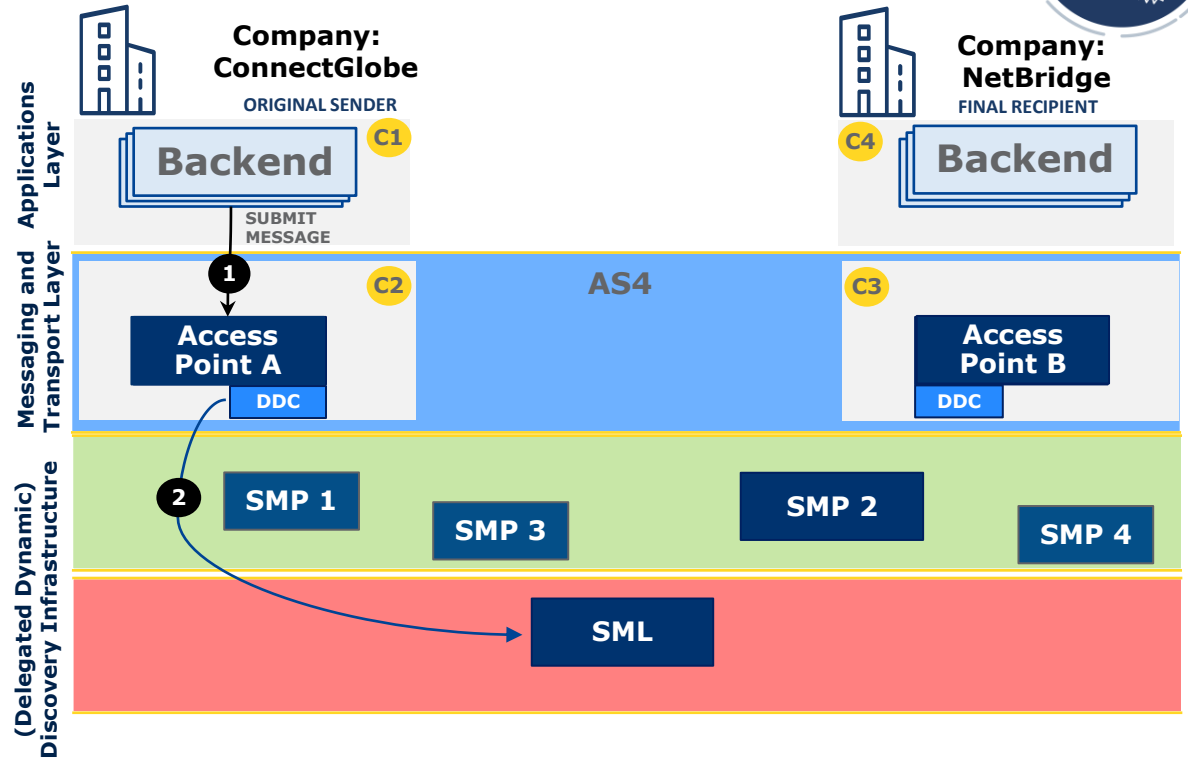
Missing To/PartyId for Access Point B(C3)

Service(Process)/Action(DocumentType) defined in SMP document

Final Recipient Identifier (C4)

Dynamic Discovery process: Message delivery

1. Original sender (ConnectGlobe) submits the message to Access Point A.
2. The DDC(A) queries the SML for the URL address of SMP where the final recipient (NetBridge) published service metadata.





The DDC(A) query the SML for the location of AP of the final recipient

- Generate the DNS query
- Extract/build target SMPs URL.

- Lookup with NAPTR record

- [Q5...RQ.sml.service.eu](https://service.smp-b.eu)

Result: `!.*!https://service.smp-b.eu/smp!`

- Extract value:

`https://service.smp-b.eu/smp`

- Lookup with CNAME (eDelivery Legacy)

- [B-a5...04.sml.service.eu](https://service.smp-b.eu)

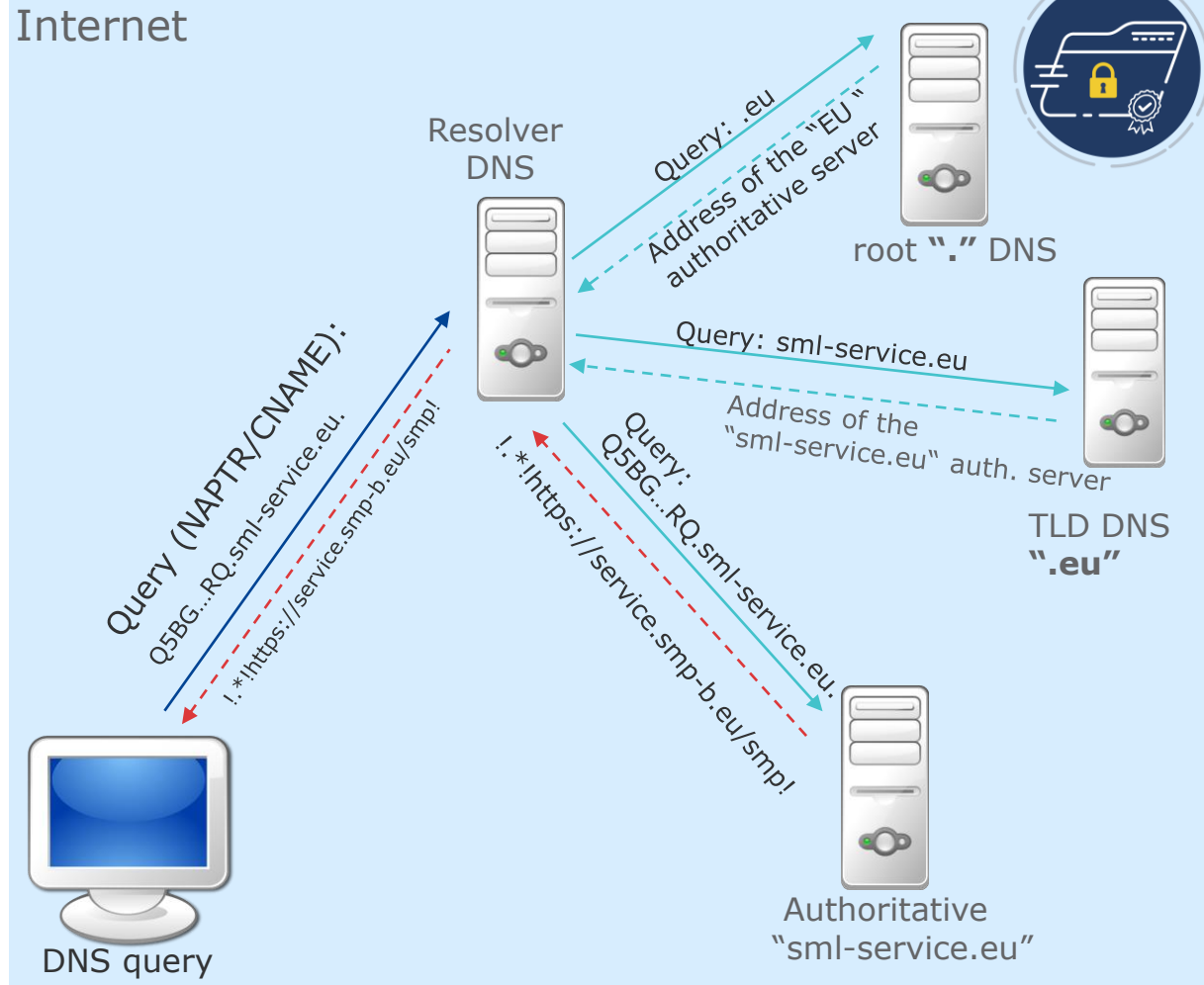
Result: `service.smp-b.eu.`

- Build URL with predefined missing parts defined by business domain network:

`https://service.smp-b.eu/smp`

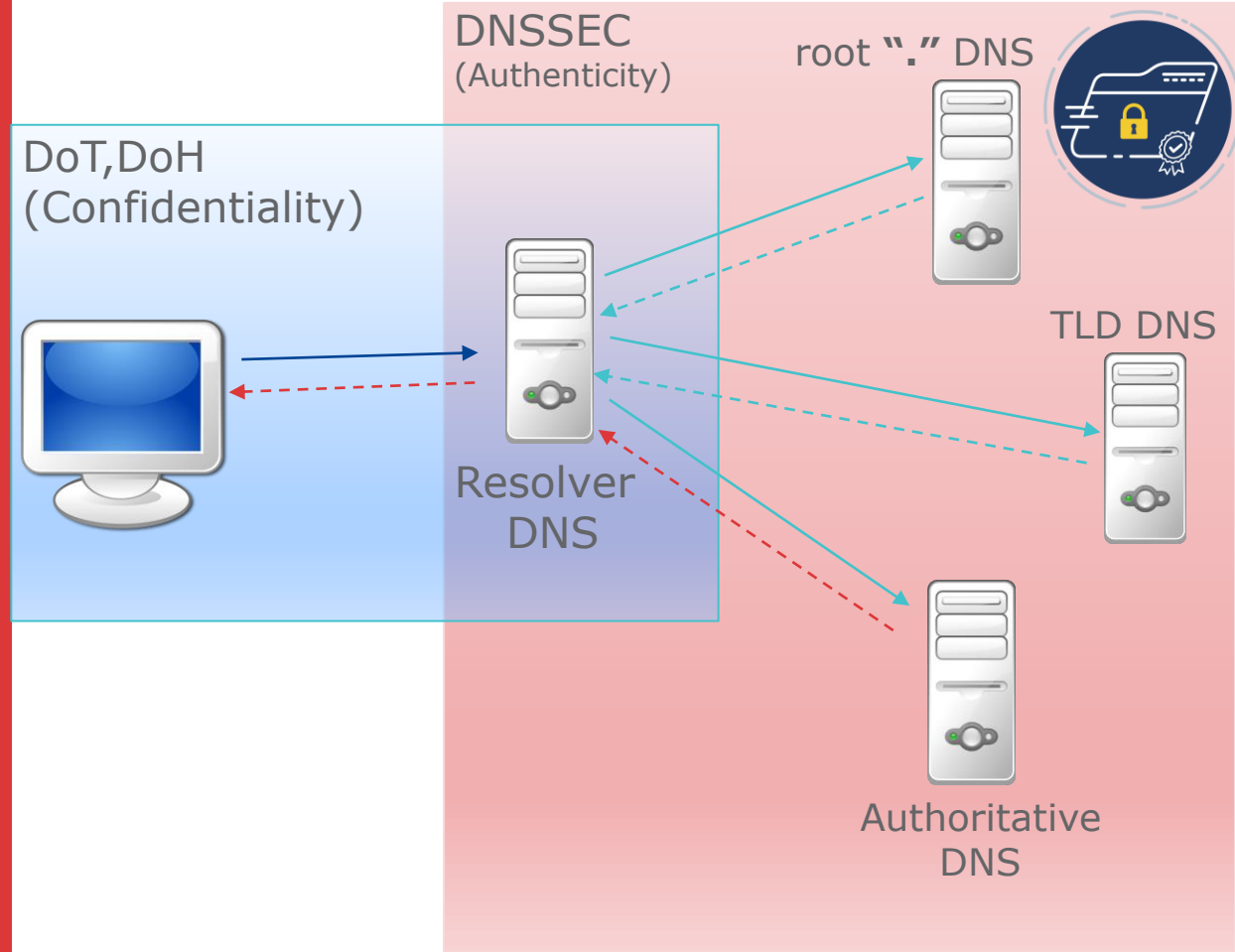
DNS lookup

- Resolver DNS
 - Internet service provider, business enterprise / company network, router, public DNS resolvers (Google: 8.8.8.8, Cloudflare: 1.1.1.1, OpenDNS: 208.67.222.222, ...)
- Root DNS server
- Top level domain (TLD) DNS server
- Authoritative DNS server



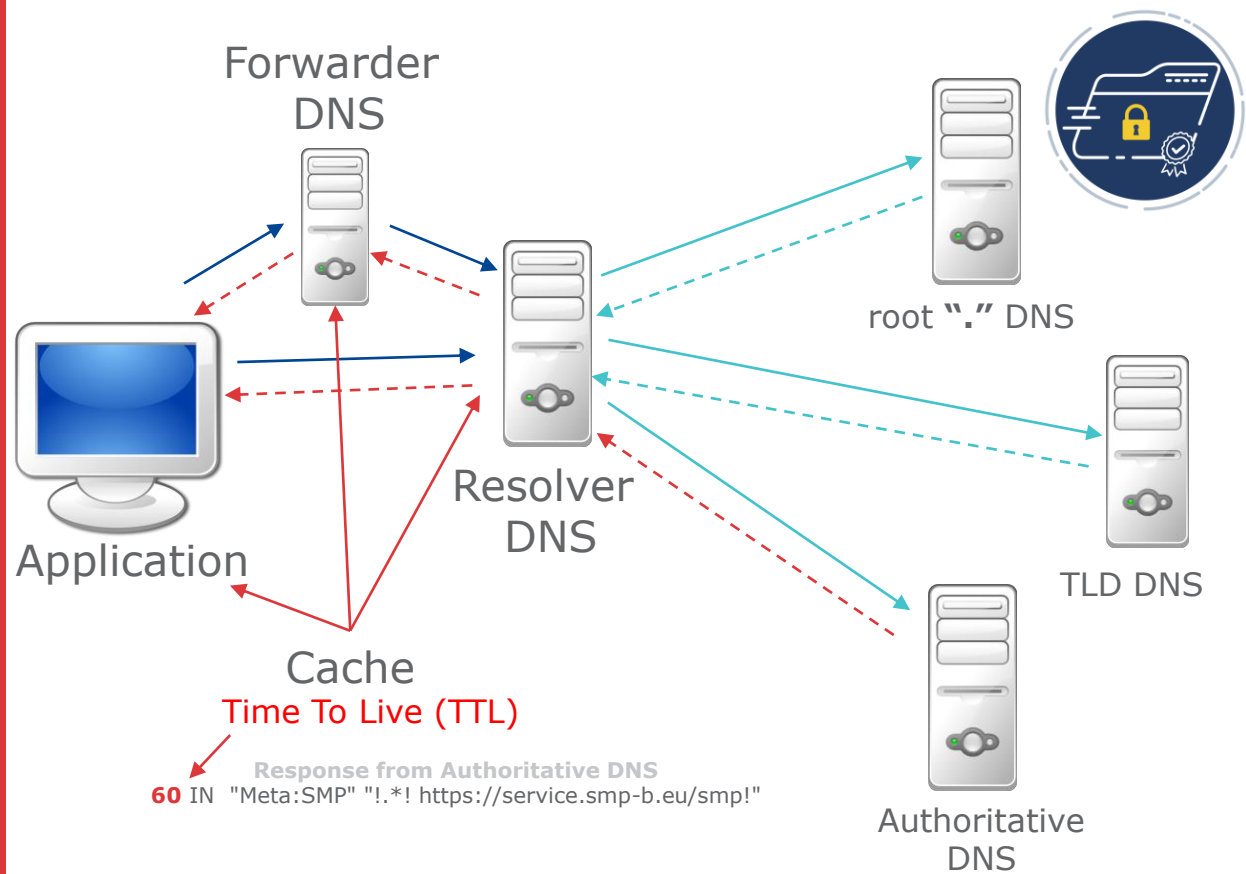
DNS Security

- Domain Name System Security Extensions (DNSSEC)
- Strengthens authenticity of the received data
- DNS over HTTPS (DoH), DNS over TLS (DoT), ...
- Confidentiality



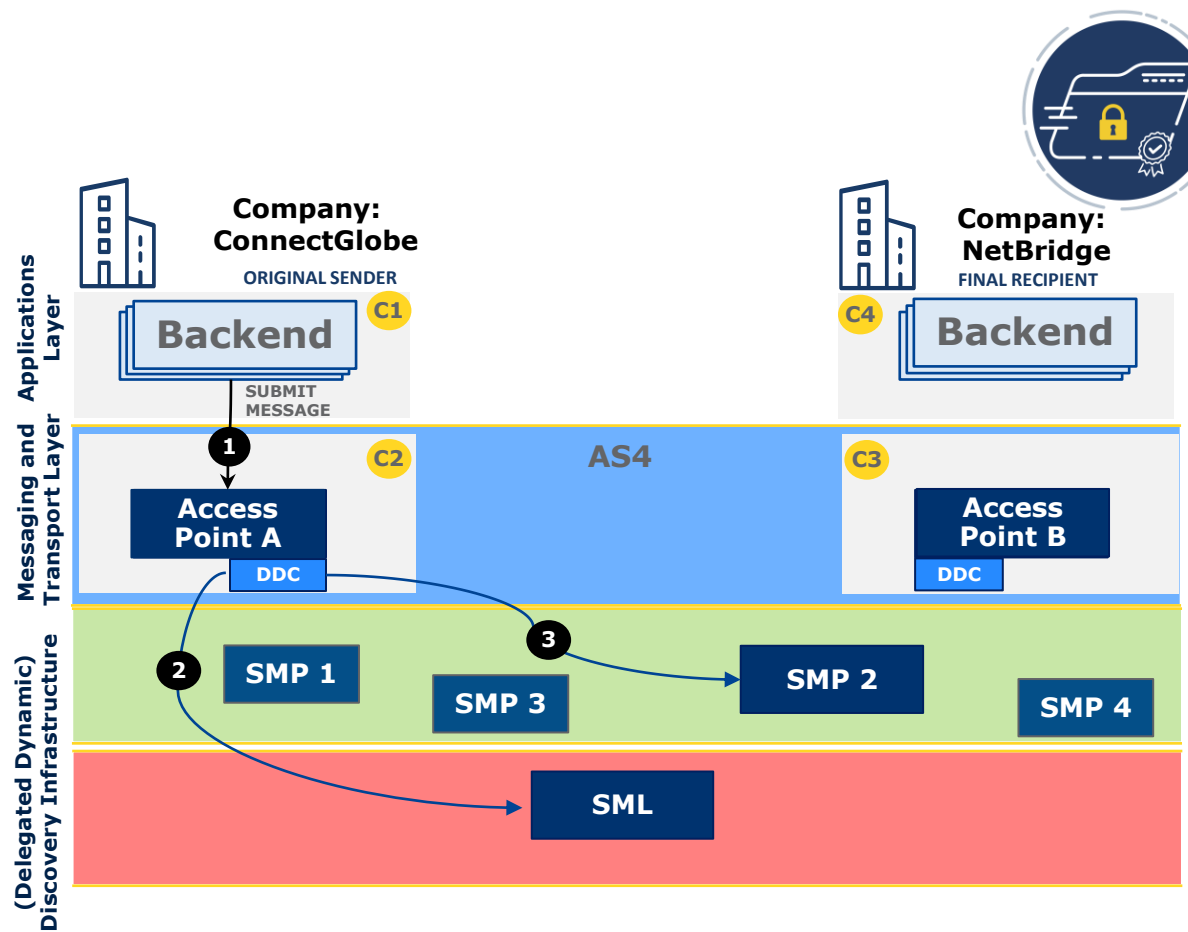
DNS Cache

- Improves performance
- Improves stability / resilience
- Delays the changes
- Where is the Cache?
 - Resolver DNS
 - Forwarder DNS
 - Application level



Dynamic Discovery process: Message delivery

1. Original Sender (ConnectGlobe) submits the message to Access Point A.
2. The DDC(A) queries the SML for the URL address of SMP where the final recipient (NetBridge) published service metadata.
3. **The DDC(A) retrieves the Service metadata from the targeted SMP (SMP 2).**
DDC(A) validates the integrity and the authenticity of the data received from SMP 2.





Dynamic Discovery Client (Access point A)

- Generate the SMP request:
(HTTP GET)
 - SMP Address (DNS
Lookup)
 - Participant Identifier
(Final Recipient)
 - /services/ (constant)
 - Document identifier
(AS4 message: Action)

[SMP address] /**[Participant-Identifier]**/ **services** / **[Document-Identifier]**

[https://service.smp-b.eu/smp/urn:oasis:names:tc:ebcore:partyid-type:iso6523:0088:2203148000007/
services / urn:oasis:names:specification:ubl:schema:xsd:invoice-12::invoice](https://service.smp-b.eu/smp/urn:oasis:names:tc:ebcore:partyid-type:iso6523:0088:2203148000007/services/urn:oasis:names:specification:ubl:schema:xsd:invoice-12::invoice)



The SMP response: service metadata

- Signature
- Missing message data
 - Access point B URL
 - Access point B Certificate(s)
 - Where is the access point identifier (The To/PartyId for Access Point B(C3)?

```
<SignedServiceMetadata xmlns="http://docs.oasis-open.org/bdxml/ns/SMP/2016/05">
  <ServiceMetadata>
    <ServiceInformation>
      <ParticipantIdentifier>urn:oasis:names:tc:ebcore:partyid-type:iso6523:0088:2203148000007</ParticipantIdentifier>
      <DocumentIdentifier scheme="urn:oasis:names:specification:ubl:schema:xsd:invoice-12">invoice</DocumentIdentifier>
      <ProcessList>
        <Process>
          <ProcessIdentifier scheme="cenbii-procid-ubl">BII04</ProcessIdentifier>
          <ServiceEndpointList>
            <Endpoint transportProfile="bdxml-transport-ebms3-as4-v1p0">
              <EndpointURI>https://access-point.company-b.eu</EndpointURI>
              <ServiceActivationDate>2020-06-01T11:06:02.000+02:00</ServiceActivationDate>
              <ServiceExpirationDate>2026-06-01T11:06:02+02:00</ServiceExpirationDate>
              <Certificate>UGFzdGUgYmFzZTY0IGVuY29kZWQgY2VydGlmaWNhdGUgb2YgQVA= </Certificate>
              <ServiceDescription>This is the Invoice service</ServiceDescription>
              <TechnicalInformationUrl>https://www.company-b.eu/info</TechnicalInformationUrl>
            </Endpoint>
          </ServiceEndpointList>
        </Process>
      </ProcessList>
    </ServiceInformation>
  </ServiceMetadata>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>...</SignedInfo>
    <SignatureValue>UCGUg....YZkqsTQ==</SignatureValue>
    <KeyInfo>
      <X509Data>
        <X509SubjectName>CN=SMP_B,OU=SMP-SERVICE,O=SMP-B,C=EU</X509SubjectName>
        <X509Certificate>MIIFY ....fTI=</X509Certificate>
      </X509Data>
    </KeyInfo>
  </Signature>
</SignedServiceMetadata>
```

AP (B) URL address

AP (B) certificate

AP (B) To/PartyId

Signature



The To/PartyId for Receivers Access Point (C3)

- The eDelivey AS4 enhancement
- The Business domain/network technical specifications

Certificate Details for Entry 'access-point-b'

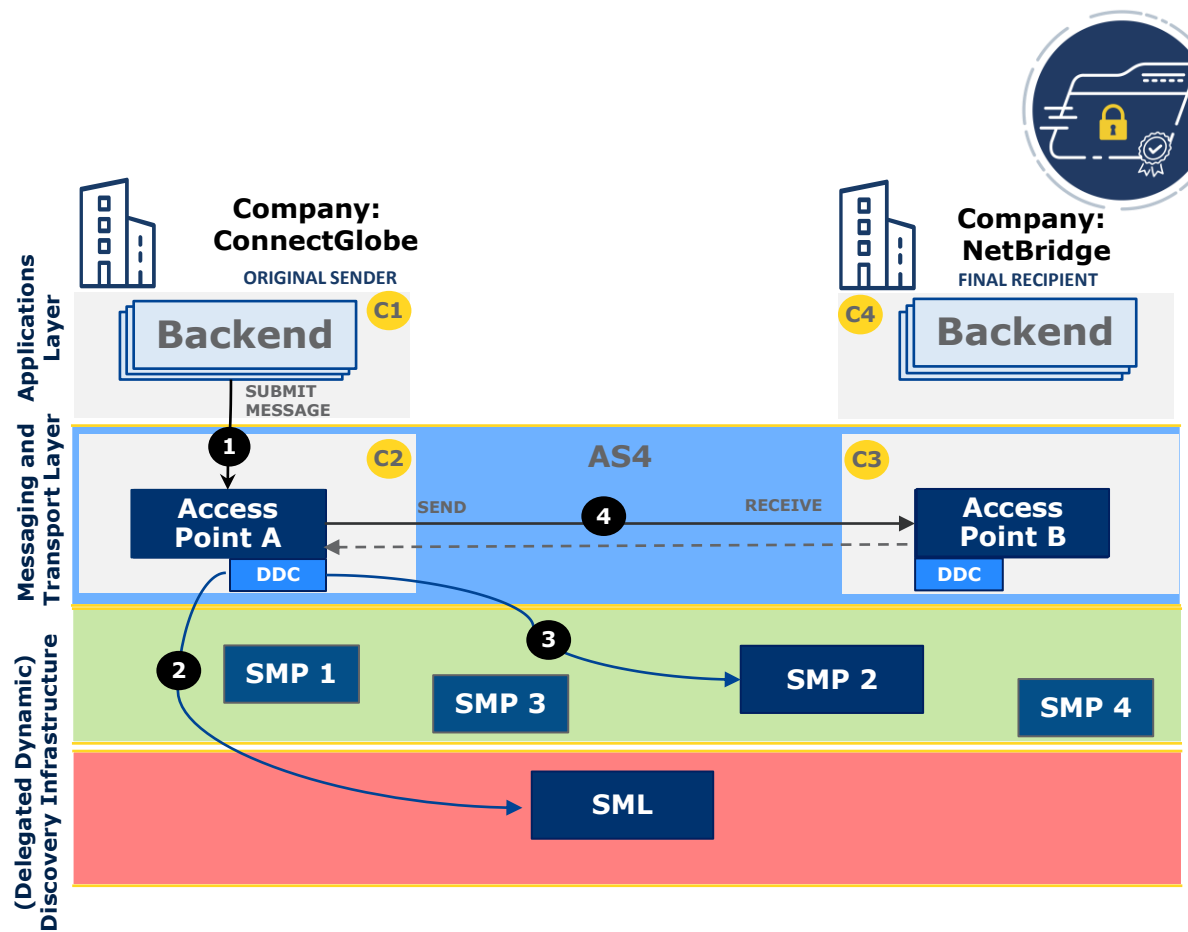
Certificate Hierarchy:	access-point-b
Version:	3
Subject:	CN= <u>access-point-b</u> ,O=company-b,C=eu
Issuer:	CN=access-point-b,O=company-b,C=eu
Serial Number (hex.):	0x64758BFD
Serial Number (dec.):	1685425149

```
<ns:To>  
  <ns:PartyId type="urn:oasis:names:tc:ebcore:partyid-type:unregistered">access-point-b</ns:PartyId>  
  <ns:Role>http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/ns/core/200704/responder</ns:Role>  
</ns:To>
```

Public Key:	RSA 2048 bits
Signature Algorithm:	SHA-256 with RSA
Fingerprint:	SHA-1 46:24:F1:96:CC:50:7B:C8:1D:E8:F6:75:EA:CF:20:62:68:

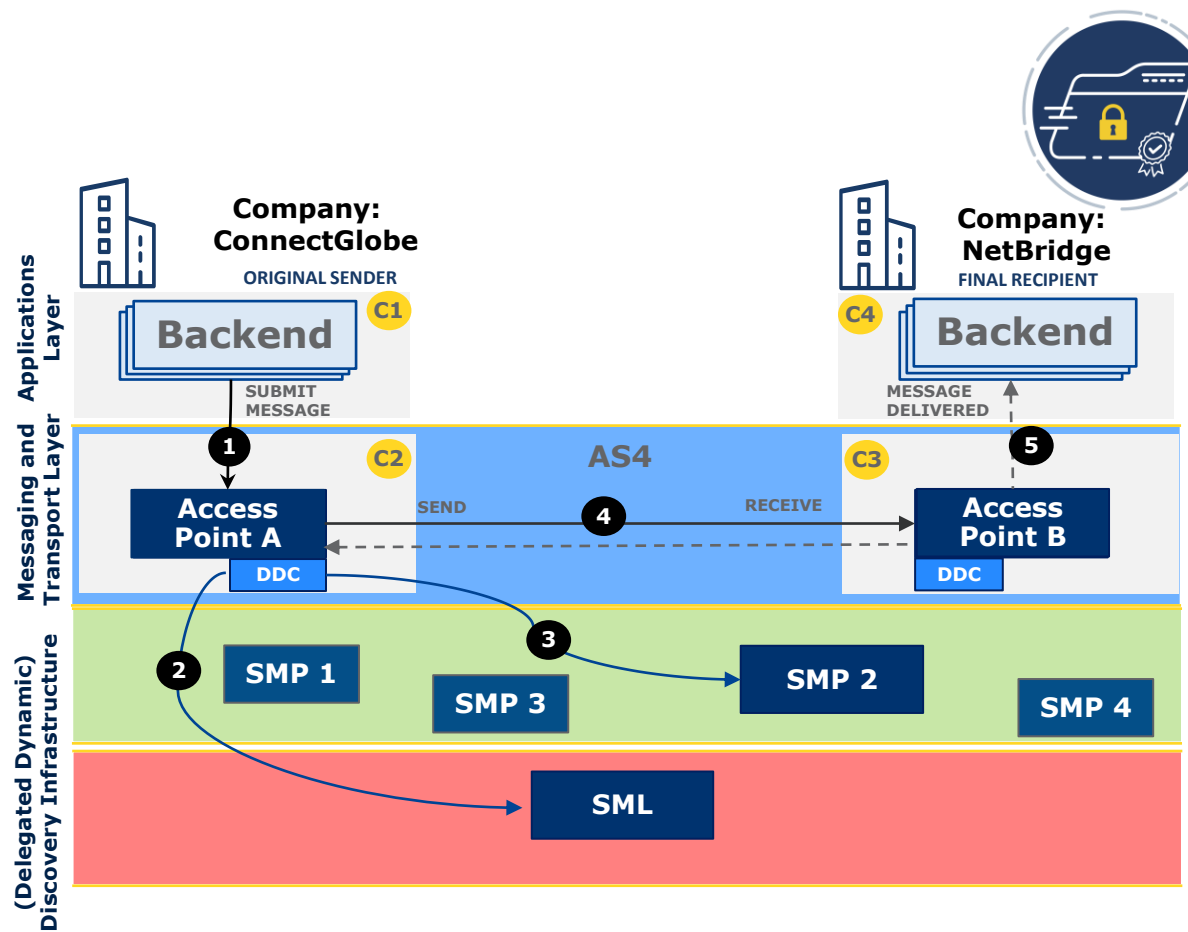
Dynamic Discovery process: Message delivery

1. Original Sender (ConnectGlobe) submits the message to Access Point A.
2. The DDC(A) queries the SML for the URL address of SMP where the final recipient (NetBridge) published service metadata.
3. The DDC(A) retrieves the service metadata from the targeted SMP (SMP 2). DDC(A) validates the integrity and the authenticity of the data received from SMP 2.
4. **Access Point A submits the message to discovered Access Point B. The Access Point B validates the message integrity and authenticity.**



Dynamic Discovery process: Message delivery

1. Original Sender (ConnectGlobe) submits the message to Access Point A.
2. The DDC(A) query the SML for the URL Address of SMP where the Final Recipient (NetBridge) published Service metadata.
3. The DDC(A) retrieves the Service metadata from the targeted SMP (SMP 2). DDC(A) validates the integrity and the authenticity of the data received from SMP 2.
4. Access Point A submits the message to discovered Access Point B. The Access Point B validates the message integrity and authenticity.
5. **Final recipient (NetBridge) receives the message from Access Point B.**





References

SMP references

- eDelivery SMP Version 1.10 (30 May 2018)
<https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eDelivery+SMP+-+1.10>
- Service Metadata Publishing (SMP) Version 1.0 (01 August 2017)
<http://docs.oasis-open.org/bdxb/bdx-smp/v1.0/bdx-smp-v1.0.html>
- Service Metadata Publishing (SMP) Version 2.0 (14 February 2021)
<http://docs.oasis-open.org/bdxb/bdx-smp/v2.0/bdx-smp-v2.0.html>
- Peppol Transport Infrastructure: Service Metadata Publishing (SMP) v1.2.0 (24 February 2021)
<https://docs.peppol.eu/edelivery/smp/PEPPOL-EDN-Service-Metadata-Publishing-1.2.0-2021-02-24.pdf>

SML references

- eDelivery BDXL 1.6
<https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eDelivery+BDXL+1.6>
- Business Document Metadata Service Location Version 1.0
<http://docs.oasis-open.org/bdxb/BDX-Location/v1.0/BDX-Location-v1.0.html>
- PEPPOL Transport Infrastructure - Service Metadata Locator (Description of the SML SOAP API)
https://github.com/OpenPEPPOL/documentation/blob/master/TransportInfrastructure/ICT-Transport-SML_Service_Specification-101.pdf
(Latest (2021-05-13) Changes not supported by eDelivery (Changed "ManageParticipant*" to "ManageBusiness*"))
<https://docs.peppol.eu/edelivery/sml/PEPPOL-EDN-Service-Metadata-Locator-1.2.0-2021-05-13.pdf>



References

Party Identifier

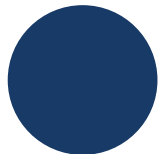
- eDelivery ebCore Party Id v1.4 (30 May 2018)
<https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eDelivery+ebCore+Party+Id+1.4>
- OASIS ebCore Party Id Type Technical Specification v1.0 (28 September 2010)
<http://docs.oasis-open.org/ebcore/PartyIdType/v1.0/PartyIdType-1.0.html>
- Peppol Transport Infrastructure: Policy for use of Identifiers v1.4.0 (11 March 2020)
<https://docs.peppol.eu/edelivery/policies/PEPPOL-EDN-Policy-for-use-of-identifiers-4.1.0-2020-03-11.pdf>

Access point

- eDelivery AS4 profile v1.15 (11 November 2020)
<https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eDelivery+AS4+-+1.15>
- AS4 Profile of ebMS 3.0 v1.0 (23 January 2013)
<http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/AS4-profile-v1.0.html>
- OASIS ebXML Messaging Services Version 3.0: Part 1, Core Features (1 October 2007)
http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/ebms_core-3.0-spec.html



Received questions and expectations



Overview of the mentioned functionality, and its existing implementations.

Business domain definitions / technical specification

- Party identifiers (type and format)
- Definition of exchange messages: Document types/AS4 Actions and Process/AS4 Services
- Trust model

Access points ([AS4 Conformant solutions](#)): liaise with the vendor to check support for dynamic discovery

- DNS Lookup
- SMP Document (Fetch, Validate, Parse)

SMP Component ([Oasis SMP 1.0 conformant solutions](#))

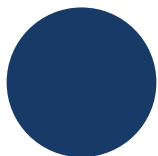
- Publish Oasis SMP documents for the participants
- Update SML records

SML Component (DomiSML)

- DNS server (Bind9, CoreDNS, PowerDNS, ...)



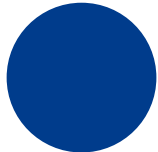
Received questions and expectations



Work together with other vendors, certification process

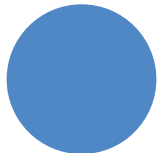
The [conformance testing service](#):

- Oasis SMP 1.0/eDelivery SMP profile
- eDelivery AS4 profile



SMP and SML business aspect with implementation scenarios in other EU member states

Peppol, EESPA, EHDS, OOTS, implementation of eFTI regulation, DIGG, ...

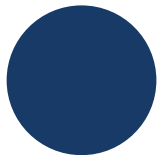


Get familiar with the eDelivery SMP component

In this presentation we present the basics SMP functionalities. But if there is interest, we can organise a “hands on” webinar on eDelivery SMP component (DomiSMP).



Received questions and expectations



It would be great if you would present how to set up the Domibus AP to allow all kinds of messages going in and out without any need to explicitly configure them in the pmode file.

The initial PMode must be present in the Domibus AP.

Using Dynamic Discovery Service eliminates the need to add configuration for new participants.



Received questions and expectations

Domibus PMode:
Dynamic Discovery configuration example

Static participant configuration

```
<process
name="tc1Process" mep="oneway" inding="pu
sh"
initiatorRole="defaultInitiatorRole"
responderRole="defaultResponderRole">
  <initiatorParties>
    <initiatorParty name="senderalias"/>
  </initiatorParties>
  <responderParties>
    <responderParty name="receiveralias"/>
  </responderParties>
  <legs>
    <leg name="pushTestcase1tc1Action"/>
  </legs>
</process>
```

Dynamic receiver configuration I

initiatorParties must not be set

```
<process name="tc1Process" mep="oneway" inding="push"
initiatorRole="defaultInitiatorRole"
responderRole="defaultResponderRole">
  <responderParties>
    <responderParty name="receiveralias"/>
  </responderParties>
  <!-- no initiatorParties element -->
  <legs>
    <leg name="pushTestcase1tc1Action"/>
  </legs>
</process>
```

Dynamic sender configuration I

responderParties must not be set

```
<process name="tc1Process" mep="oneway" inding="push"
initiatorRole="defaultInitiatorRole"
responderRole="defaultResponderRole">
  <initiatorParties>
    <initiatorParty name="senderalias"/>
  </initiatorParties>
  <!-- no responderParties element -->
  <legs>
    <leg name="pushTestcase1tc1Action"/>
  </legs>
</process>
```

PMode examples can be found in Domibus [Administration Guide](#), chapter "Dynamic Discovery of unknow participants"

Q&A



Thank you

& stay in touch



Additional slides





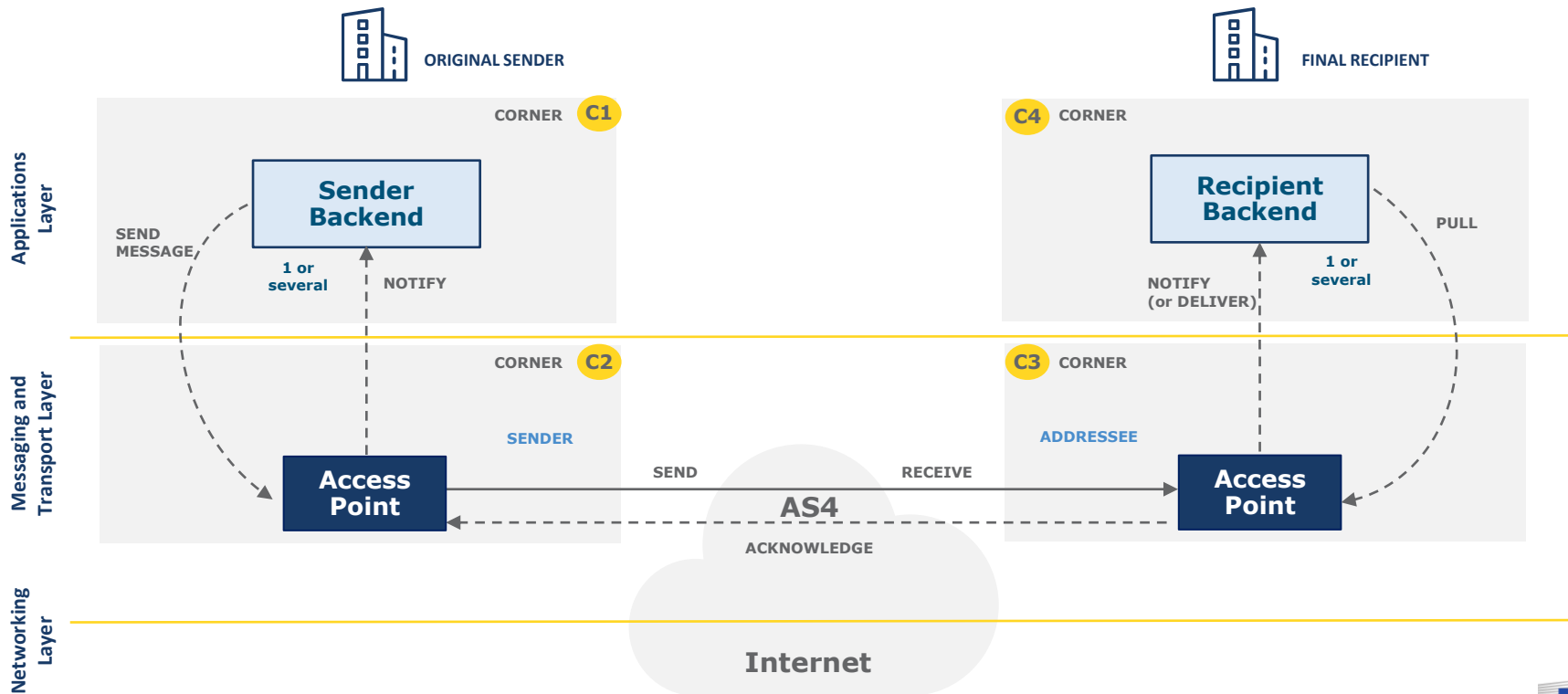
Glossary

Acronym	Meaning
PKI	Public Key Infrastructure (for validating Digital Certificates)
CA	Certificate Authority
SMP	Service Metadata Publisher
SML	Service Metadata Ledger
DDC	Dynamic Discovery Client
IS	Informational System
TLS	Transport Layer Security
AP	Access Point

Acronym	Meaning
PEPPOL	Pan-European Public Procurement Online (Organization)
AS4	Open standard for the secure and payload-agnostic exchange of messages
DNS	Domain Name System
SOAP	(Simple Object Access Protocol) XML based Messaging protocol
NAPTR	(Name Authority Pointer) The type of DNS record
CNAME	(Canonical Name) The type of DNS record

eDelivery Four-Corner Model

Static discovery



eDelivery Message Exchange



1

Submit

Sender sends message to sending AP

2

Send

Sending AP processes message

- Validation and compression of the user message;
- Signing of the compressed message;
- Encryption of the signed compressed message.

3

Receive

Receiving AP processes message

- Receives and decrypts the encrypted message;
- Verifies the sender's signature;
- Decompresses the decrypted message;
- Validates the original user message;
- Sends the acknowledgement to the sending AP;
- Stores the user message for download.

4

Deliver

Recipient receives message from receiving AP

