SML AND SMP EXPLAINED BY BASWARE

Manjeet Yadav
Product Manager, PEPPOL @ Basware

basware
Simplify Operations, Spend Smarter.

OBJECTIVES

Understand functional and technical details with associated benefits of

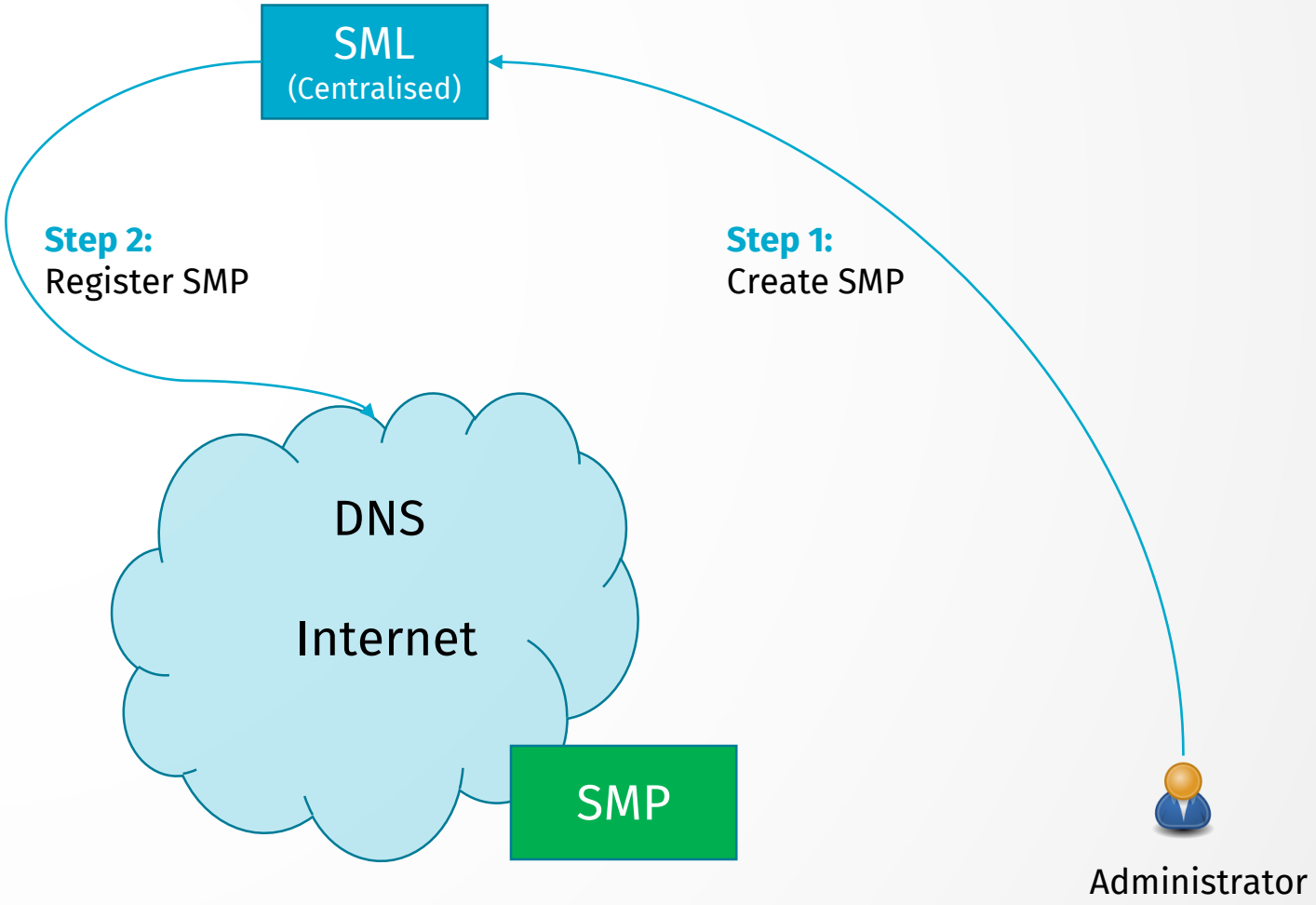
- **Dynamic discovery model**
  - allows the sending access point to query an external service storing up-to-date information about every receiving party in the network.
  - The dynamic discovery involves three components
    - Service Metadata Locator (SML)
      - Central registration system for addressing
    - Domain name system (DNS)
      - a hierarchical decentralized naming system
    - Service Metadata Publisher (SMP)
      - Publish the capabilities of PEPPOL participant
- **Public Key Infrastructure (PKI)**
  - Security and integrity to establish a trusted network

basware

DYNAMIC DISCOVERY MODEL

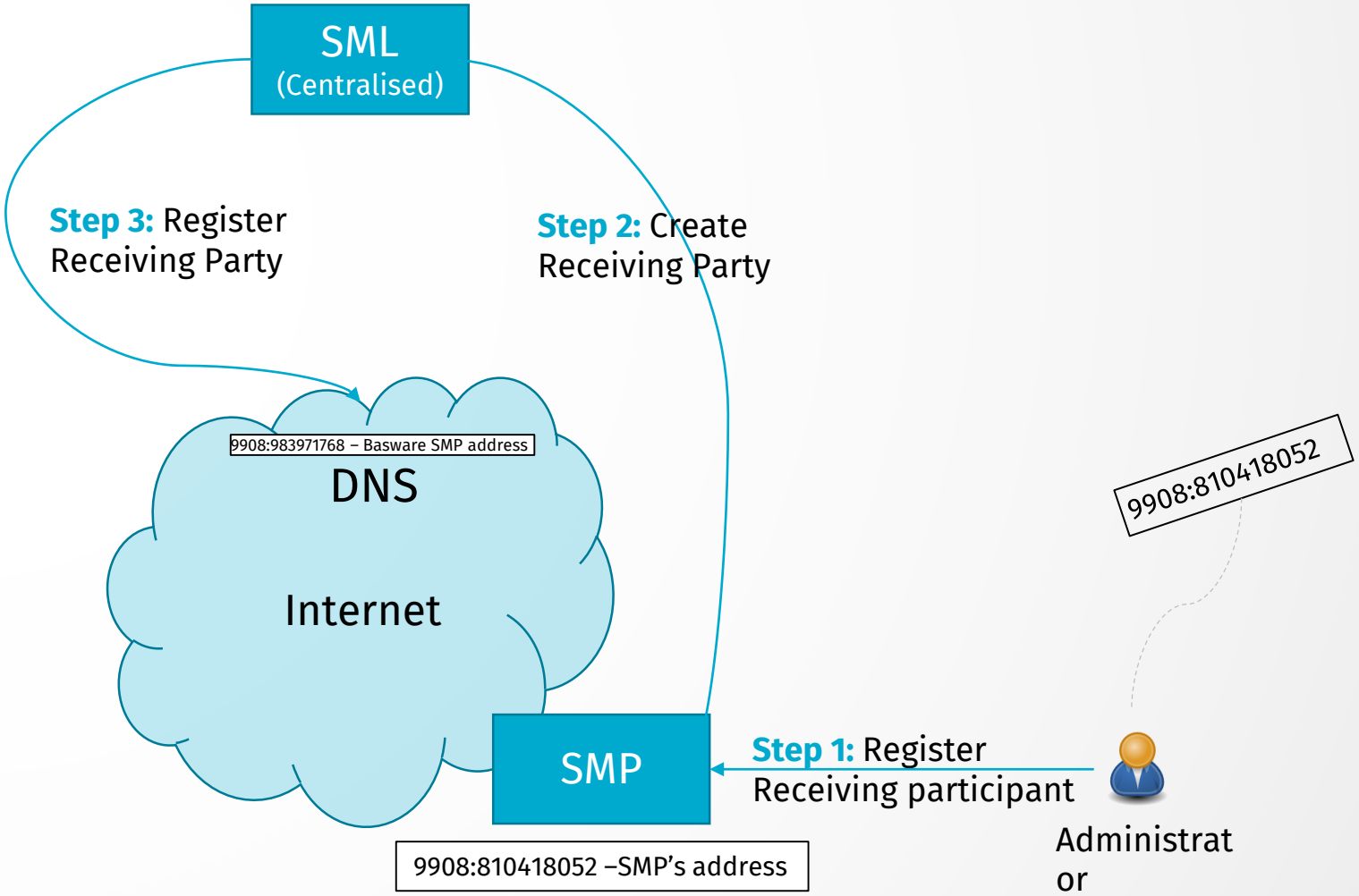
- **Benefits** over extra lookup overhead
  - Automation
  - flexibility
  - Scalability
- **Best suited for**
  - medium to large scale networks (scale)
  - for meshed network (topology)
  - for evolving networks (stability)
  - for sensitive networks (uptime)
  - for distributed administration model.
- The dynamic discovery process is composed of following **two phases**:
  - **Registration**
  - **Operation**

DYNAMIC DISCOVERY: REGISTRATION OF A SMP



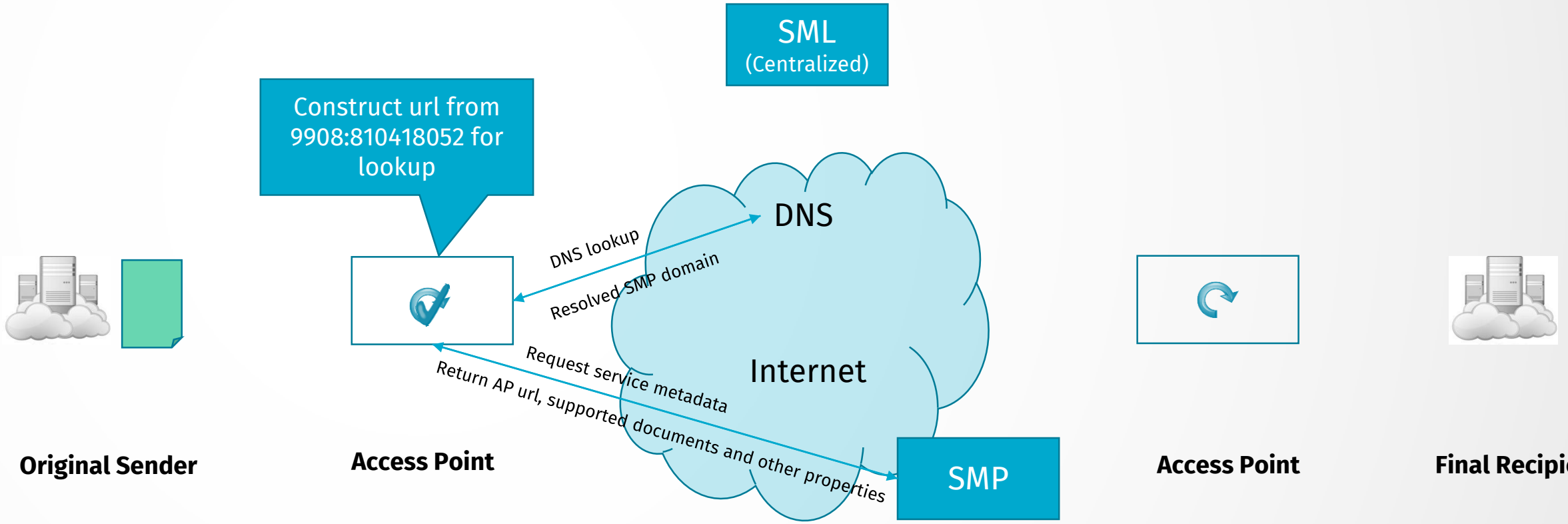
basware

DYNAMIC DISCOVERY: REGISTRATION OF A PARTY



basware

DYNAMIC DISCOVERY: OPERATION PHASE



basware

SERVICE METADATA

- Information necessary for invoking a service
- It is a combination of information on the end entity recipient (such as its *identifier, certificate, supported business documents and processes in which it accepts those documents*) and its associated endpoint/AP (such as the *transport protocol and AP address*)

Participant: BASWARE AS

Edit participant Delete participant

Organization

ICD	NO:ORGNR (9908)
Identifier	923829644
Name	BASWARE AS

Contact person

Name	Fredrik Heimerback
Phone number	+47 90 24 99 13
Email	fredrik.heimerback@basware.com

Endpoint

Endpoint	Basware
Registration date	19.12.2012

Profiles

BIS04 V2 - PEPPOL BIS Invoice 2.0 (Profile 04A)
BIS05 V2 - PEPPOL BIS Billing 2.0 (Profile 05A)
EHF_CREDITNOTE 2.0 - EHF Creditnote 2.0 (Profile XXA)
EHF_INVOICE 2.0 - EHF Invoice 2.0 (Profile 04A)
EHF_INVOICE_CREDITNOTE 2.0 - EHF Invoice and Creditnote 2.0 (Profile 05A)
EHF_XYA_1.0_REMINDER - EHF Reminder 1.X (Profile XYA)

Endpoint: Basware

Edit endpoint Show participants

Description

Description	Basware Access Point
URL (AS2)	https://api.basware.com/peppol/as2

Contact

Rolle	Name	Phone number	Email
Support	-	+47 98 23 64 00	customer.support@basware.com
Administration	Manjeet Yadav	+91 7341144993	Manjeet.Yadav@basware.com
Technical	Arun Kumar	+91 9815295761	Arun.Kumar@basware.com

Certificate

Subject	**O=Basware Corporation,CN=APP_1000000333,C=FI**
Issuer	CN=PEPPOL ACCESS POINT CA,O=NATIONAL IT AND TELECOM AGENCY,C=DK
Valid from	14.08.2017
Valid to	15.08.2019

basware

SERVICE METADATA LOCATOR (SML)

- a centralized component that stores the location of every SMP in the network
- manages the resource records of the participants and SMPs in the DNS Server.
- stores the unique identifier of all receiving parties and SMPs in the DNS Server.
- provides management interface towards SMPs
- provides DNS-based resolve mechanism to locate individual SMPs
- SMP service providers are the administrators of SML, Basware is such a provider.
- only ONE SML per network, PEPPOL is such a network
- hostname for SML is “edelivery.tech.ec.Europa.eu”
- SMK is a SML for test purposes
- hostname for SMK is “acc.edelivery.tech.ec.Europa.eu”
- currently only Belgium is using SMK before onboarding participants on production environment

basware

SML INTERFACES

The Service Metadata Locator service exposes three interfaces:

Service Metadata discovery interface

- This is the lookup interface which enables senders & their AP service providers to discover service metadata about specific target participants

Manage participant identifiers interface

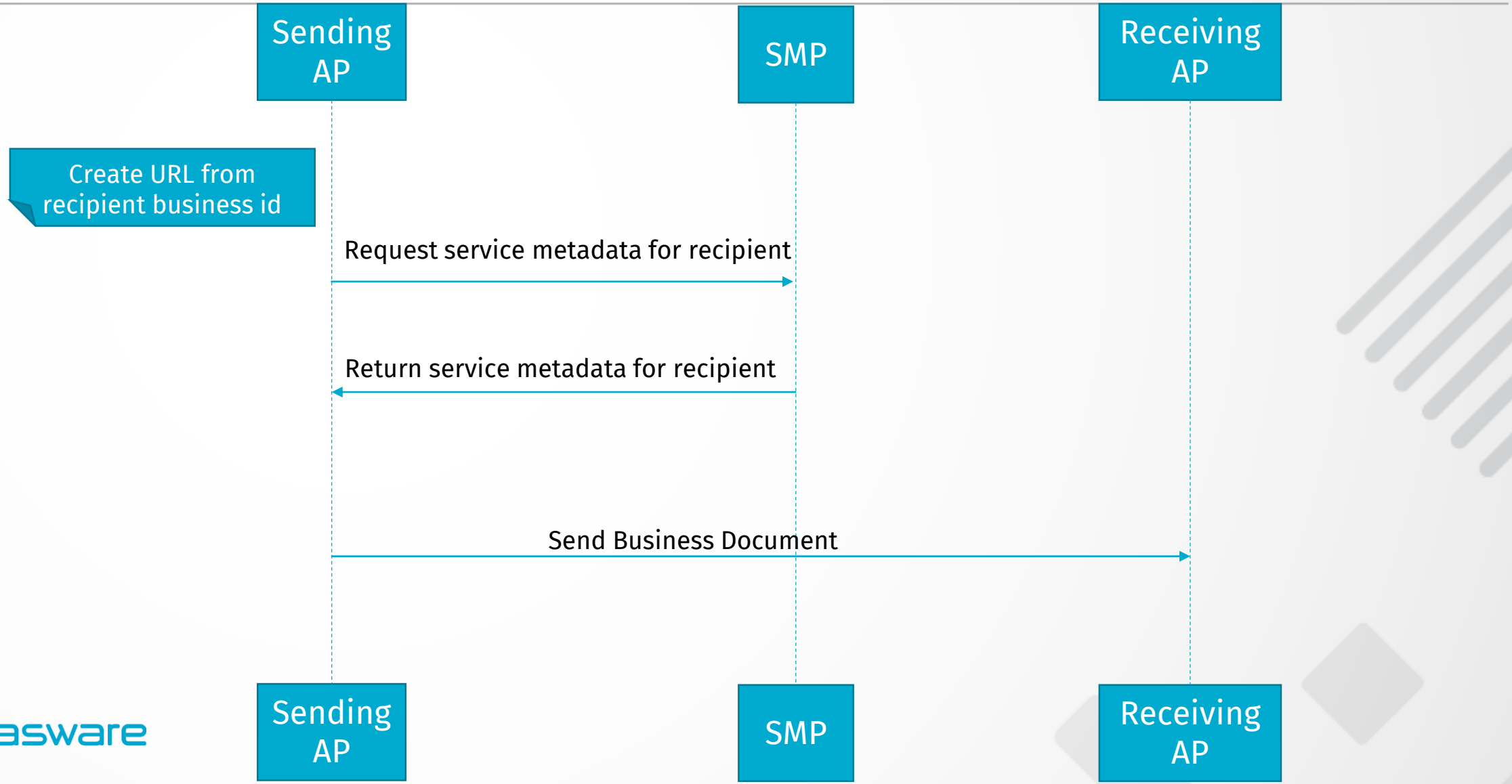
- This is the interface for Service Metadata publishers (SMPs) for managing the metadata relating to specific participant identifiers that they make available

Manage service metadata interface

- This is the interface for Service Metadata publishers (SMPs) for managing the metadata about their services e.g. binding, interface profile and key information.

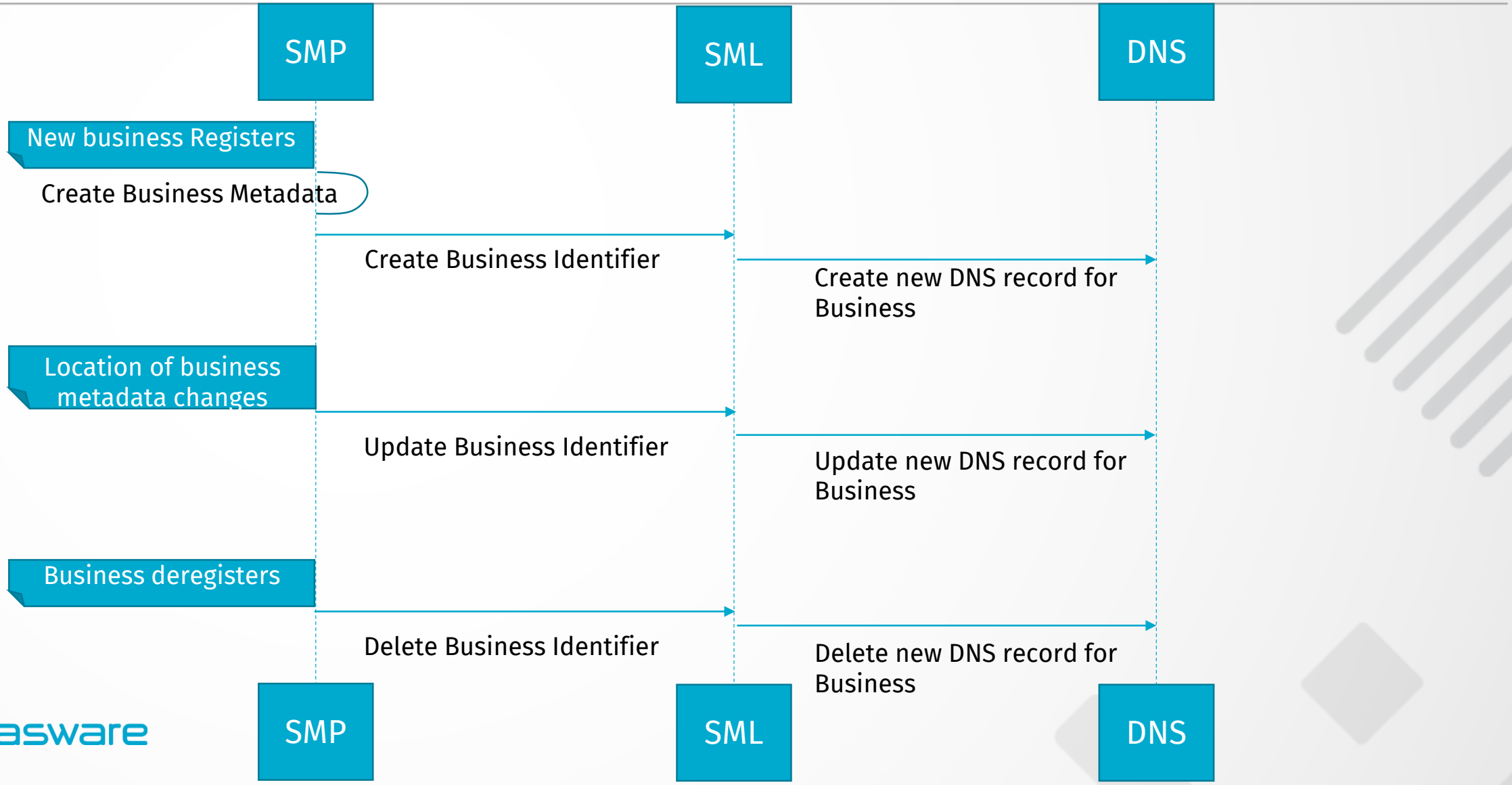
basware

SERVICE METADATA DISCOVERY INTERFACE



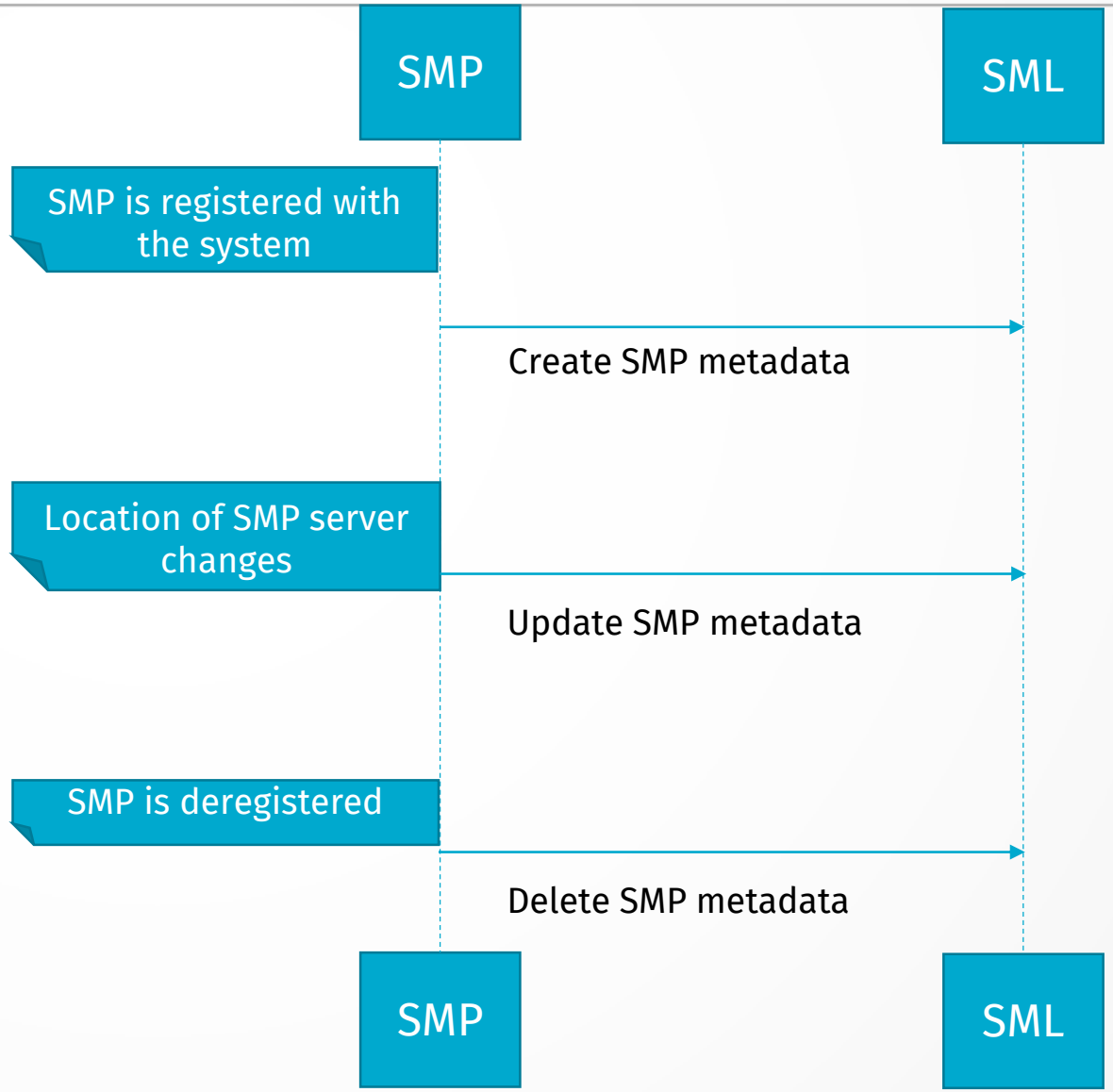
basware

PARTICIPANT IDENTIFIER MANAGEMENT INTERFACE



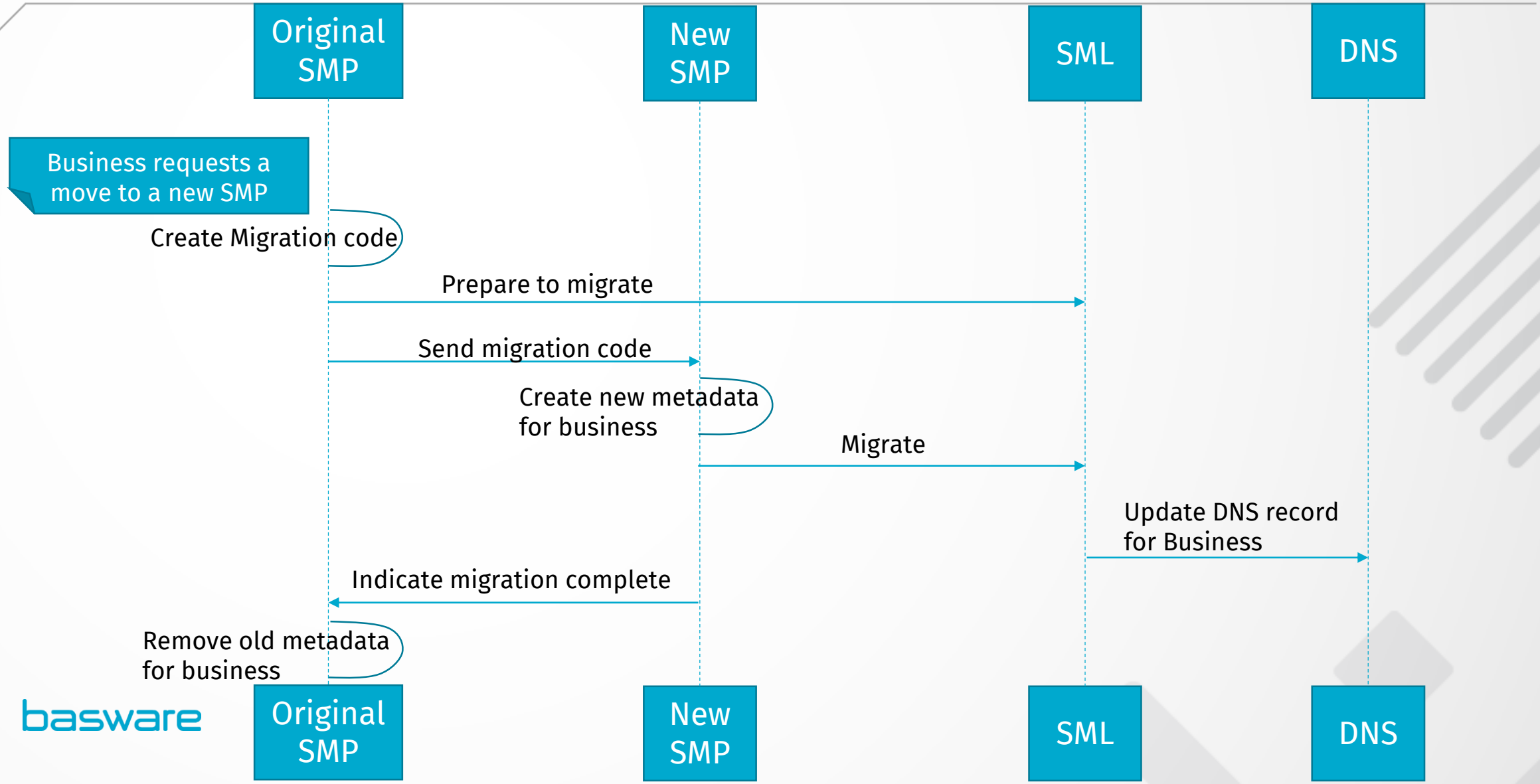
basware

SERVICE METADATA MANAGEMENT INTERFACE



basware

MIGRATING A PARTICIPANT TO A NEW SMP



basware

SML LOGICAL INTERFACES

ManageParticipantIdentifier interface:

This interface requires authentication of the SMP. It can provide the metadata for all participant identifiers belonging to a particular participant identifier scheme with concept of a "wildcard" CNAME record in the DNS: *.<schemeID>.<SML domain> CNAME <SMP domain> . It has the following operations:

- Create
- CreateList
- Delete
- DeleteList
- PrepareToMigrate
- Migrate
- List

ManageServiceMetadata interface:

- This interface requires authentication of the user. This has the following operations:
  - Create
  - Read
  - Update
  - Delete

basware

SML DATA TYPES

- ServiceMetadataPublisher

```
<ServiceMetadataPublisherService>
        <PublisherEndpoint>
                <EndpointAddress/>
        </PublisherEndpoint>
        <ServiceMetadataPublisherID/>
</ServiceMetadataPublisherService>
```

- RecipientParticipantIdentifier

```
<ServiceMetadataPublisherServiceForParticipant>
        <ServiceMetadataPublisherID/>
        <ids:ParticipantIdentifier/>
</ServiceMetadataPublisherServiceForParticipant>


<ids:ParticipantIdentifier scheme=”xs:string”>
        xs:string
</ids:ParticipantIdentifier>
```

basware

SML DATA TYPES CONTINUED…

- ParticipantIdentifierPage

```
<ParticipantIdentifierPage>
        <ServiceMetadataPublisherID/>
        <ParticipantIdentifier/>*
        <NextPageIdentifier/>?
</ParticipantIdentifierPage>
```

- MigrationRecord

```
<MigrationRecord>
        <ServiceMetadataPublisherID/>
        <ParticipantIdentifier/>*
        <MigrationKey/>?
</MigrationRecord>
```

basware

BUSINESS DOCUMENT METADATA SERVICE LOCATION VERSION 1.0

Format of Participant Identifiers logical address:

- http://<hash over recipientID>.<schemeID>.<SMLdomain>/<recipientID>/services/<documentType>
- Real example: http://b-ed82cee0dc0a8e558d570239bb7f3073.iso6523-actorid-upis.edelivery.tech.ec.europa.eu/iso6523-actorid-upis%3A%3A9908%3A923829644/services/busdox-docid-qns%3A%3Aurn%3Aoasis%3Anames%3Aspecification%3Aubl%3Aschema%3Axsd%3AInvoice-2%3A%3AInvoice%23%23urn%3Awww.cenbii.eu%3Atransaction%3Abiitrns010%3Aver2.0%3Aextended%3Aurn%3Awww.peppol.eu%3Abis%3Apeppol5a%3Aver2.0%3A%3A2.1

- Then a U-NAPTR for a DNS query string "B-ed82cee0dc0a8e558d570239bb7f3073.sid.peppol.eu to a SMP metadata service hosted at “serviceprovider.peppol.eu” might be:
- IN NAPTR 100 10 "U" "Meta:SMP" "!^.*$!https://serviceprovider.peppol.eu/e49b223851f6e97cbfce4f72c3402aac/!" .
- Or, utilizing the regexp capability for group extraction from query strings,
- IN NAPTR 100 10 "U" "Meta:SMP" "!^B-(+[0-9a-fA-F]).sid.peppol.eu$!https://serviceprovider.peppol.eu/\\1!" .

basware

SERVICE METADATA PUBLISHER (SMP)

- are responsible for Capability Lookup
- are registers of the message exchange capabilities and location of parties (i.e. service metadata)
- are usually used in a distributed way
- many access point service providers can also provides SMP services to other APs e.g. **Basware**
- once the Access Point of the Sending Party discovered the address of the Receiving Party's SMP (Service Metadata Publisher), it is able to retrieve the required information to interoperate with the Receiving Party (i.e. metadata).
- provides the sending AP with the service metadata of the receiving party which includes the followings:
  - The receiving Access Point lookup information (e.g. IP address, URL, transport protocol)
  - The communication protocol (AS2, AS4)
  - The available and possible business processes
  - The message types supported and required
  - The security setup (e.g. public key used for the encryption of the message)
  - Any information relevant for the message exchange (customizable through extension anchors)

basware

SMP INTERFACE MODEL

- This specification only defines the protocol for retrieving Service Metadata
- It does not specify interfaces for creating, updating, deleting and managing Service Metadata, or any internal data storage formats
- The goal is to allow the interface in this specification to expose data from many different Service Metadata back-ends, which may be based on any suitable technology such as for example RDBMS, LDAP or UDDI

SMP DATA TYPES

The data model comprises the following main data types:

- ServiceGroup
- ServiceMetadata / SignedServiceMetadata

Supporting data types for these main types are:

- ServiceInformation
- ServiceEndpointList
- ParticipantIdentifier
- DocumentIdentifier
- Redirect
- Process
- ProcessList
- Endpoint

basware

SERVICEGROUP

- The ServiceGroup structure represents a set of services associated with a specific participant identifier that is handled by a specific Service Metadata Publisher. The ServiceGroup structure holds a list of references to SignedServiceMetadata resources in the ServiceList structure
- Pseudo-schema for ServiceGroup:

```
<smp:ServiceGroup>
    <ids:ParticipantIdentifier scheme=”xs:string”>
            xs:string
    </ids:ParticipantIdentifier>
    <smp:ServiceMetadataReferenceCollection>
            <smp:ServiceMetadataReference href=”xs:anyURI” />*
    </smp:ServiceMetadataReferenceCollection>
    <smp:Extension>xs:any</smp:Extension>?

</smp:ServiceGroup>
```

basware

SIGNEDSERVICEMETADATA

- The SignedServiceMetadata structure is a ServiceMetadata structure that has been signed by the ServiceMetadataPublisher, according to governance policies that are not covered by this document. Pseudo-schema for this data type:

```
<smp:SignedServiceMetadata>
    <smp:ServiceMetadata />
    <ds:Signature />
</smp:SignedServiceMetadata>
```

- **ServiceMetadata:** The ServiceMetadata element covered by the signature.
- **Signature** represents an enveloped XML signature over the SignedServiceMetadata element

basware

EXAMPLE SMP REGISTRATION

```
<ns3:SignedServiceMetadata>
  <ns3:ServiceMetadata>
    <ns3:ServiceInformation>
      <ParticipantIdentifier scheme="iso6523-actorid-upis">9908:923829644</ParticipantIdentifier>
      <DocumentIdentifier scheme="busdox-docid-qns">
        urn:oasis:names:specification:ubl:schema:xsd:Invoice-2::Invoice##urn:www.cenbii.eu:transaction:biitrns010:ver2.0:extended:urn:www.peppol.eu:bis:peppol5a:ver2.0::2.1
      </DocumentIdentifier>
      <ns3:ProcessList>
        <ns3:Process>
          <ProcessIdentifier scheme="cenbii-procid-ubl">urn:www.cenbii.eu:profile:bii05:ver2.0</ProcessIdentifier>
          <ns3:ServiceEndpointList>
            <ns3:Endpoint transportProfile="busdox-transport-as2-ver1p0">
              <ns2:EndpointReference>
                <ns2:Address>https://api.basware.com/peppol/as2</ns2:Address>
                <ns2:ReferenceParameters/>
                <ns2:Metadata/>
              </ns2:EndpointReference>
              <ns3:RequireBusinessLevelSignature>false</ns3:RequireBusinessLevelSignature>
              <ns3:MinimumAuthenticationLevel>1</ns3:MinimumAuthenticationLevel>
              <ns3:ServiceActivationDate>2017-08-14T02:00:00.000+02:00</ns3:ServiceActivationDate>
              <ns3:ServiceExpirationDate>2019-08-15T01:59:59.000+02:00</ns3:ServiceExpirationDate>
              <ns3:Certificate></ns3:Certificate>
              <ns3:ServiceDescription>Basware Access Point</ns3:ServiceDescription>
              <ns3:TechnicalContactUrl>customer.support@basware.com</ns3:TechnicalContactUrl>
            </ns3:Endpoint>
          </ns3:ServiceEndpointList>
        </ns3:Process>
      </ns3:ProcessList>
    </ns3:ServiceInformation>
  </ns3:ServiceMetadata>
  <Signature>
    <SignedInfo></SignedInfo>
    <SignatureValue></SignatureValue>
    <KeyInfo>
      <X509Data>
        <X509SubjectName></X509SubjectName>
        <X509Certificate></X509Certificate>
      </X509Data>
    </KeyInfo>
  </Signature>
</ns3:SignedServiceMetadata>
```

basware

USE OF EXTENSIONS

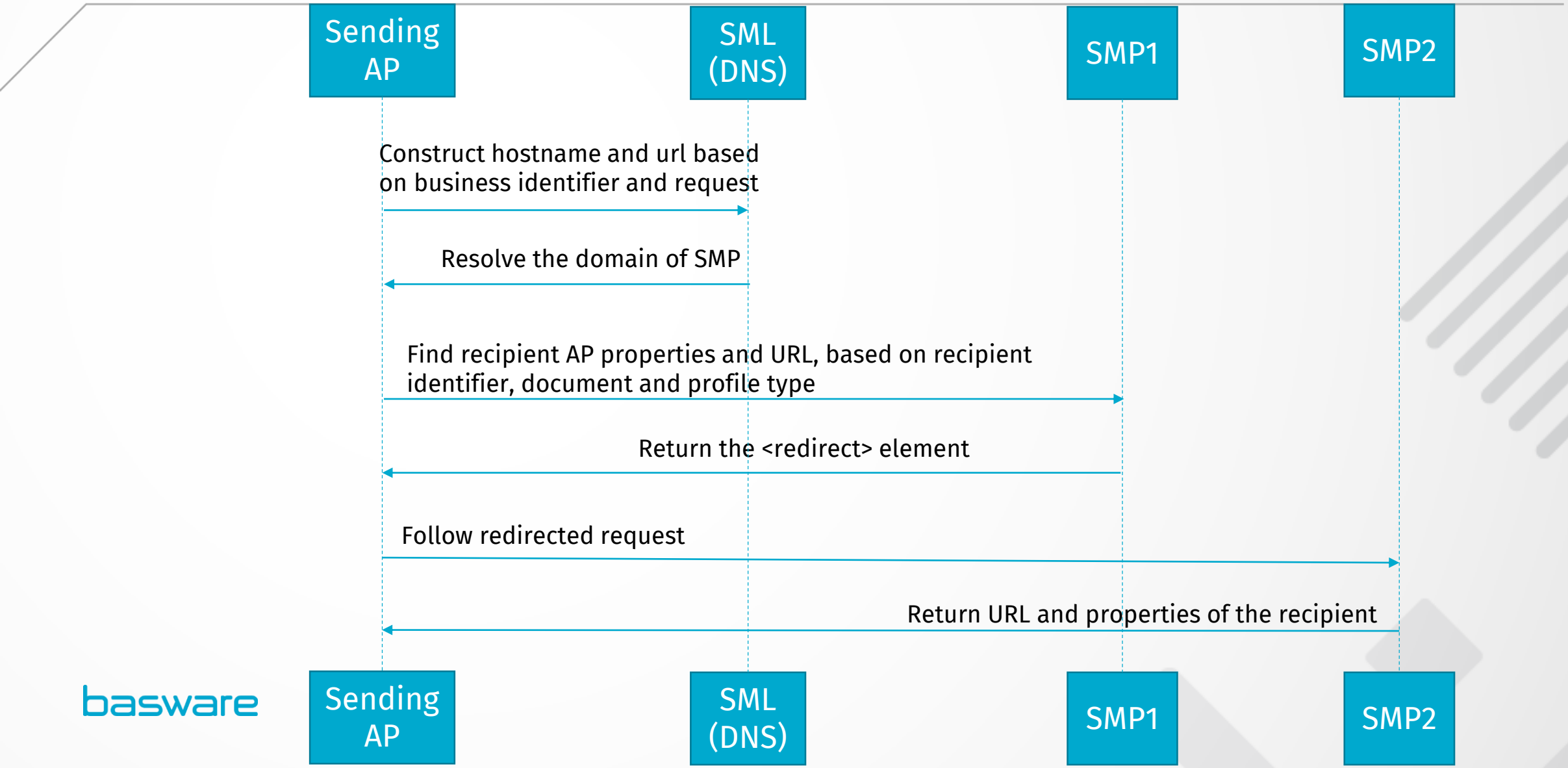
For each major entity, extension points have been added with the optional <Extension> element:

- Cardinality at extension points is by definition unbounded. An SMP publishing service may introduce as many extensions at each extension point as required
- SMP publishing services MUST NOT produce metadata that contain extensions necessary for a Client to understand in order to make use of this metadata. The ability to parse and adjust client behavior based on an extension element MUST NOT be a prerequisite for a client to locate a service, or to make a successful request at the referenced service
- A client MAY ignore any extension element added to specific service metadata resource instances

```
<Extension>
  <ExtensionID>xs:token</ExtensionID>?
  <ExtensionName>xs:string</ExtensionName>?
  <ExtensionAgencyID>xs:string</ExtensionAgencyID>?
  <ExtensionAgencyName>xs:string</ExtensionAgencyName>?
  <ExtensionAgencyURI>xs:anyURI</ExtensionAgencyURI>?
  <ExtensionVersionID>xs:normalizedString</ExtensionVersionID>?
  <ExtensionURI>xs:anyURI</ExtensionURI>?
  <ExtensionReasonCode>xs:token</ExtensionReasonCode>?
  <ExtensionReason>xs:string</ExtensionReason>?
  xs:any
</Extension>
```

basware

USING DIFFERENT SMP FOR DIFFERENT DOCUMENT TYPES



basware

SERVICE BINDINGS & DNSSEC

- Both "manage participant identifier" and “"ManageServiceMetadata"” interfaces are bound to an HTTP SOAP 1.1 transport.
- The service is secured at the transport level with a two-way SSL / TLS connection.
- The requestor must authenticate using a client certificate issued for use in the infrastructure
- For SMP binding a service implementing the REST binding MUST set the HTTP “content-type” header, and give it a value of “text/xml”. A service implementing the REST profile MUST NOT use TLS (Transport Layer Security) or SSL (Secure Sockets Layer).
- The regular lookup of the address of the SMP for a given participant ID is performed using a standard DNS lookup. There is a potential vulnerability of this process if there exists at least one "rogue" certificate
- someone possessing such a rogue certificate could perform a DNS poisoning or a man-in-the-middle attack to fool senders of documents into making a lookup for a specific identifier in a malicious SMP , effectively routing all messages intended for one or more recipients to a malicious access point.
- This attack could be used for disrupting message flow for those recipients, or for gaining access to confidential information in these messages (if the messages were not separately encrypted).
- One mitigation for this kind of attack on the DNS lookup process is to use DNSSEC rather than plain DNS. DNSSEC allow the authenticity of the DNS resolutions to be checked by means of a trust anchor in the domain chain. Therefore, it is recommended that an SML instance uses the DNSSEC infrastructure.

basware

MESSAGE SIGNATURE

- The message returned by the service is signed by the Service Metadata Publisher with XML-Signature according to the standard http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/.
- The signature MUST be an enveloped XML signature represented via an <ds:Signature> element embedded in the <SignedServiceMetadata> element. The <ds:Signature> element MUST be constructed according to the following rules:
- The <Reference> MUST use exactly one Transform being: “http://www.w3.org/2000/09/xmldsig#envelopedsignature”
- The <ds:KeyInfo> element MUST contain an <ds:X509Data> element with an <ds:X509Certificate> sub-element containing the signer’s X.509 certificate as PEM base 64 encoded X509 DER value.
- The canonicalization algorithm MUST be http://www.w3.org/2001/10/xml-exc-c14n#
- The SignatureMethod MUST be http://www.w3.org/2000/09/xmldsig#rsa-sha1
- The DigestMethod MUST be http://www.w3.org/2000/09/xmldsig#sha1

VERIFYING SIGNATURES

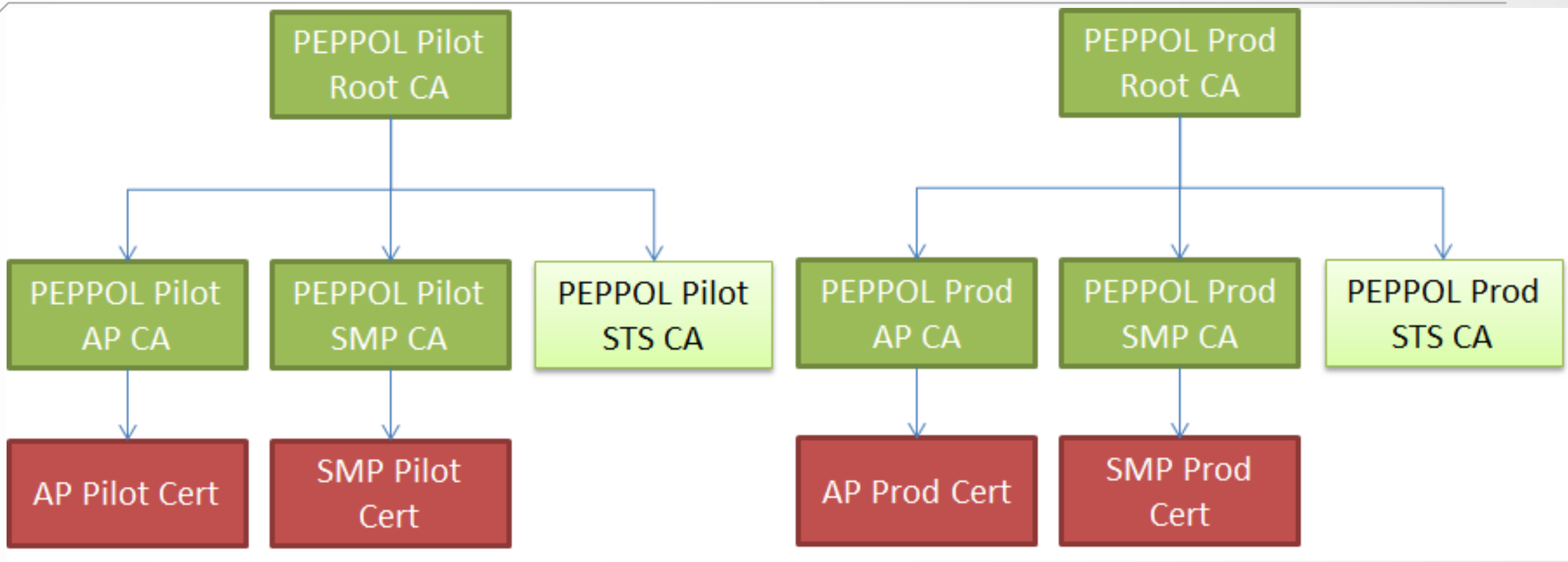
Verifying the signature

- When verifying the signature, the consumer has access to the full certificate as a PEM base 64 encoded X509 DER value within the <Signature> element. The consumer may verify the signature by a) extracting the certificate from the <ds:X509Data> element, b) verify that it has been issued by the trusted root, c) perform a validation of the signature, and d) perform the required certificate validation steps (which might include checking expiration/activation dates and revocation lists).

Verifying the signature of the destination SMP

- For the redirect scheme, the unique identifier of the destination SMP signing certificate is stored at the redirecting SMP. In addition to the regular signature validation performed by the client of the destination SMP resources, the client SHOULD also validate that the identifier of the destination SMP signing certificate corresponds to the unique identifier which the redirecting SMP claims belongs to the destination SMP.

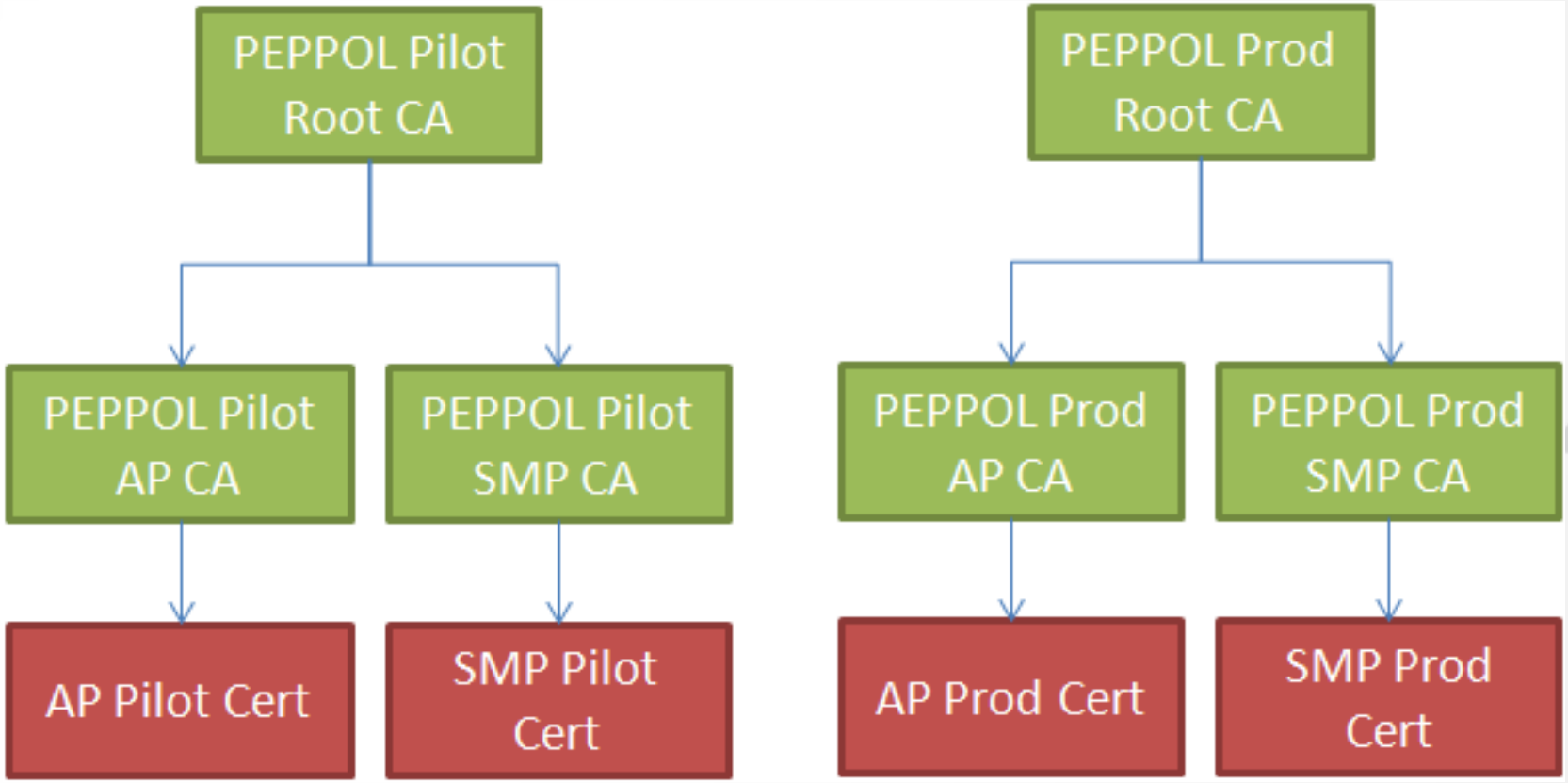
PEPPOL PKI CERTIFICATES V2



The PEPPOL PKI (Public Key Infrastructure) is an integral part of the PEPPOL security model. These are the issuing certificates for the "AP Root" (AccessPoint), the "SMP Root" (Service Metadata Publisher) and the "STS Root" (Secure Token Service - unused!). Each AP and SMP certificate used in practice is based on the respective AP or SMP ROOT certificate

basware

PEPPOL PKI CERTIFICATES V3



During 2018 all PEPPOL certificates must be replaced, because the underlying root certificate is about to expire in January 2020. The new PKI is called "OpenPEPPOL PKI v3" and the root certificates are valid from 2018 to 2028. The structure is very similar to the old one, but the STS CA is not present any more.

basware

DECISION TIME WHETHER TO AVAIL SMP SERVICES OR BUILD YOUR OWN?

basware

LINKS

http://directory.peppol.eu/public

https://vefa.difi.no/smp/

https://peppol.helger.com/public/locale-en_US/menuitem-tools-participant

https://peppol.eu/downloads/peppolimplementations/

https://peppol.eu/

https://peppol.eu/who-is-who/openpeppol-member-list-2/

https://www.basware.com/en-sg/solutions

basware

THANK YOU

Manjeet Yadav | Product Manager - PEPPOL

Manjeet.Yadav@basware.com

+91 7341144993

https://www.linkedin.com/in/ermanjeetyadav/

basware