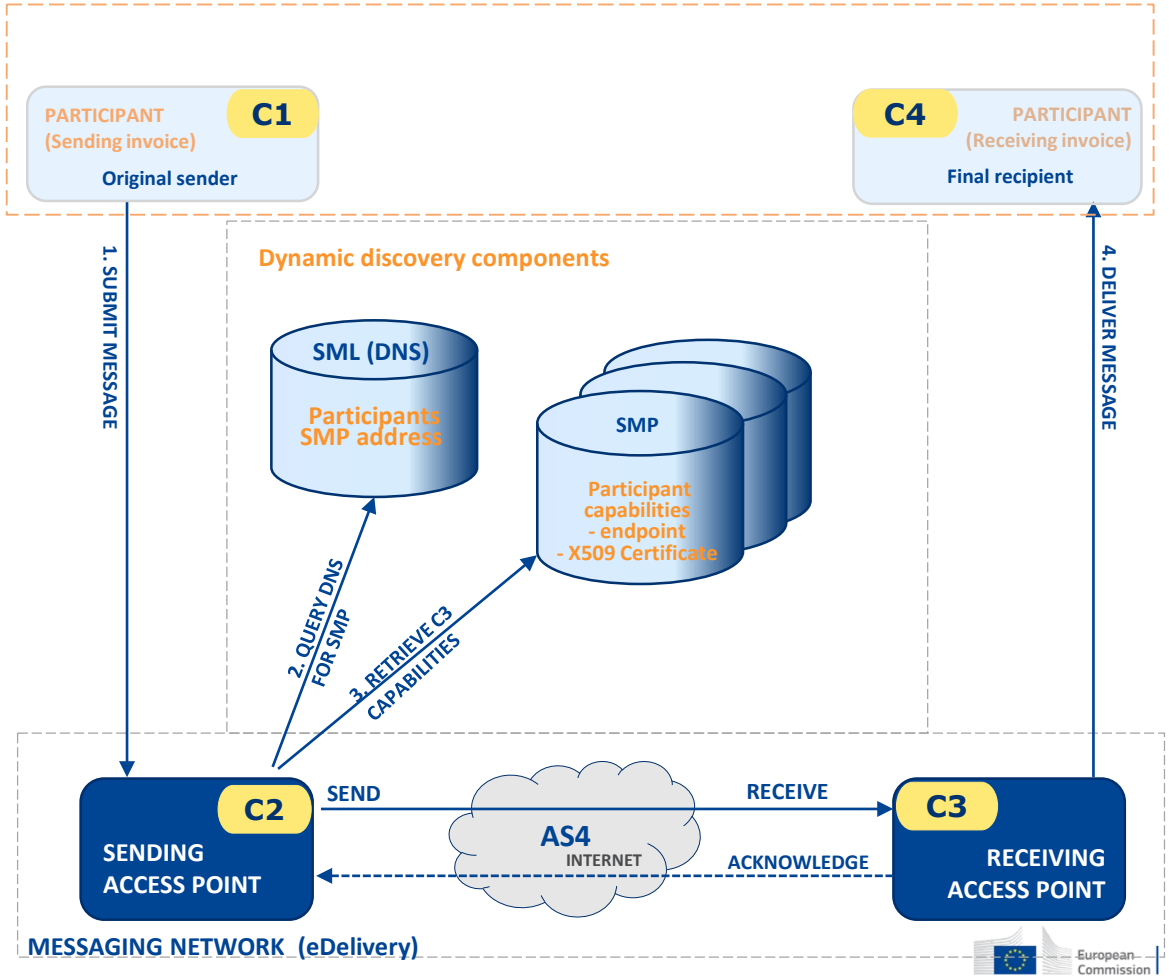
eDelivery SML presentation to OpenPEPPOL community

16 October 2019

Maarten Daniels, Joze Rihtarsic
(CEF eDelivery team)

SML in Dynamic Discovery process

- **C1:** Create message and submit to C2
- C2: Create DNS query for participant
- C2 Process DNS result
- C2: Query SMP for participant capabilities (endpoint URL, X509 Certificate, ..)
- C2 Submit message to receiving Access Point (C3)
- …



eDelivery SML implementation: BDMSL

- Stable version 4.0.1
- No new release is planned
- Request EDELGOV-65: 'retrieving all participant identifiers' is in analysis stage

BDMSL ROADMAP AND RELEASES		
Date	**Version**	**Highlights**
02.10.2019 (current)	v4.0.1	Security patch
17.06.2019	v4.0.0	New administration tools and security enhancements
06.08.2018	v3.1.3	Minor upgrades
07.02.2018	v3.1.2	Minor upgrades
01.10.2017	v3.1.1	Inconsistency report, support for multiple PKI's, …
10.05.2017	v3.0.1	Support for non PKI Certificates, multiple domains, support NAPTR records, …
…	…	…

BDMSL Operations (PEPPOL specification)

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.

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

BDMSL specific operations

SMP Management (BDMSL Service)	
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.
isAlive	Test all components of BDMSL: Weblogic nodes, Database connection and DNS connection.

BDMSL Administration operations

SMP Management (BDMSL Service)	
Operation	**Description**
ChangeCertificate	Operation allows the Administrator to change the SMP's authentication (expired) certificate.
ClearCache	For performance optimization, BDMLS caches configuration values. Operation clears cached values.
Manage Configuration (set, read, update)	Operations are used for BDMSL configuration management, as: proxy settings, keystore management, DNS integration data, SMP DNS authentication regular expression for Certificate DN validation, ... (All system property changes are audited).
Manage SubDomains	Operation(s) enables Administrator to add, remove, update and list BDMSL domains.

BDMSL Administration operations

SMP Management (BDMSL Service)	
Operation	**Description**
Manage DomainCertificates	Operation(s) enable Administrator to add, remove Root PKI(s) certificates or non PKI certificates for the domains.
Manage DNS custom records (A, NAPTR, CNAME)	Operation(s) enable Administrator to add, remove custom DNS record for types: A, NAPTR and CNAME.
CreateInconsistencyReport	Operation creates Inconsistency data report between Database and DNS server.

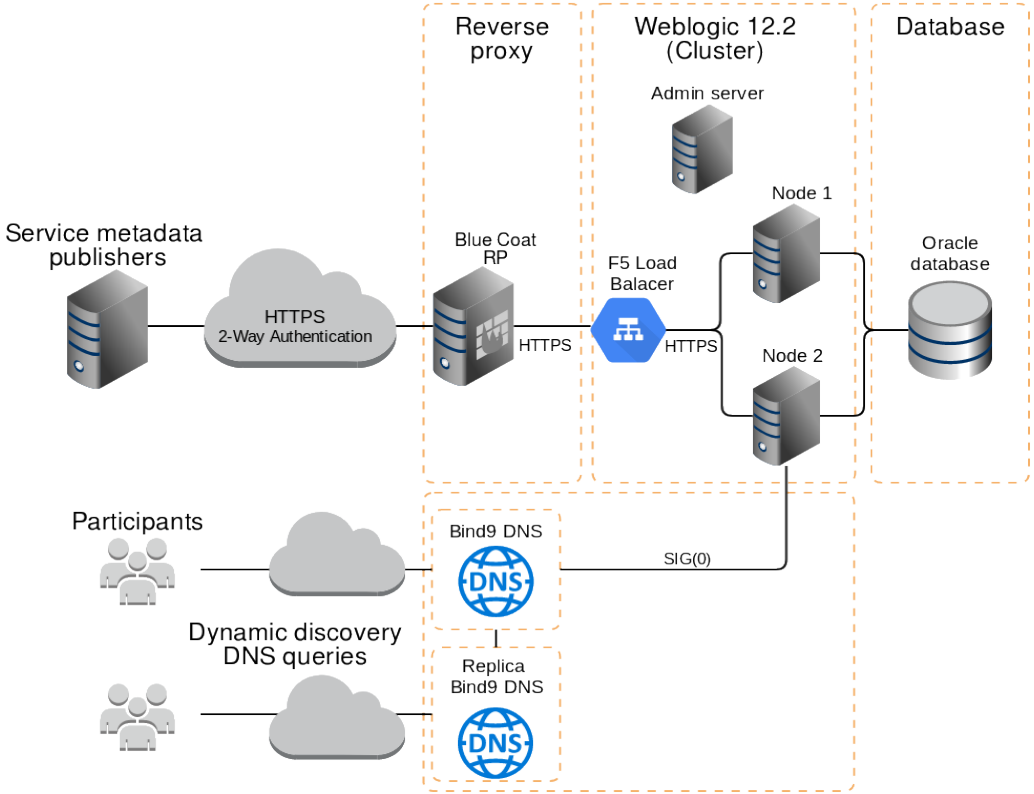
BDMSL architecture

Reliability

- Weblogic 12.2 cluster with 2 nodes (can be increased)
- DNS Server duplication

- 24 / 7 monitoring of all Weblogic nodes
- 24 / 7 monitoring and service for DNS servers
- User support during EC working hours

- Data duplication: DNS entries data are also in database
- Daily DNS consistency validation reporting



BDMSL Security

- HTTPS 2-way authentication for API access
- All accesses are logged
- Signed webservice responses
- Database audit (who, when, what)
- Internal component communication over HTTPS
- DNS update authentication with SIG(0)
- DNSSEC (in progress) for authenticated denial of existence and data integrity, but not for confidentiality

Security maintenance

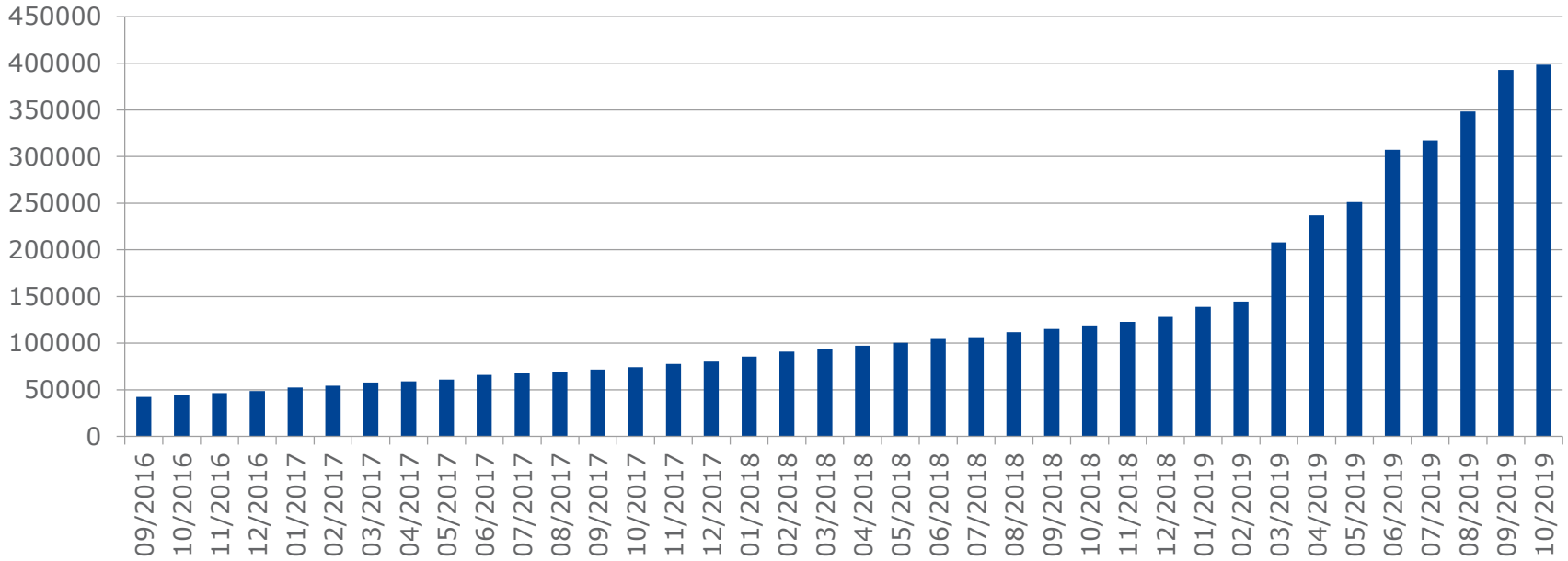
- Upgrade HTTPS to the latest TLS Cipher suites
  (keep SML in ssllabs grade: A)
- Continuous security patches on all levels (OS, application servers, ..)
- Weekly OWASP library checks for BDMSL
- Security validation by EC DIGIT Security Assessment team on major releases

User support tasks

Task	Occurrence
Change expired certificate for SMP owners	Common
Inform users about upgrades and security patches	Common
Network issues (Service metadata publishers cannot access SML)	Rarely
Help on setting up SMP/SML integration	Rarely

Growing participant count challenge

- DNS scalability is identified as threat (taking in to account the current exponential increase)
- Preparing load test for DNS with 2 million entries with DNSSEC enabled



Growing participant count challenge options

- Change configuration setup of Bind9 server
- Change DNS server implementation
- Proposal to change the specifications with an option to add domain additional parts like: country code, participant identifier provider, etc.