Secure Document Exchange in the Greek Public Sector via eDelivery

Antonios Stasis(✉) and Loukia Demiri(✉)

Hellenic Ministry of Administrative Reconstruction, 15, Vas. Sofias Avenue, Athens, Greece
{a.stasis,l.demiri}@ydmed.gov.gr

Abstract. This paper describes how eDelivery specifications and technologies can be implemented in order to show how Document Management Systems used by the Greek Public Authorities can be connected in a common interoperability infrastructure for establishing communication with stakeholders (namely national and cross-Border Public Authorities, citizens and businesses) in a structured, secure, legal binding and accountable way. The action is conducted by the Hellenic Ministry of Administrative Reconstruction and it takes into account the eIDAS regulation's provisions on Electronic Registered Delivery Systems and on Trust Establishment and the Connecting Europe Facility (CEF) eDelivery specifications. The action includes the establishment of interoperability nodes (Access Points) and of infrastructure for discovery of the recipients (Service Metadata Publisher), the development of connectors for the integration of the backend Document Management Systems, the generation and exchange of evidences for ensuring authenticity and non-repudiation and the establishment of trust between the communicating points by using digital certificates. As communication is necessary not only at national but also at cross-border level, the Ministry has cooperated with Greek and European Public and Private Bodies, in order to ensure fulfillment of all requirements and integration with all possible stakeholders. The connection of the Document Management System used by the Hellenic Ministry of Administrative Reconstruction serves as a proof-of-concept.

Keywords: Secure Document Exchange · eDelivery · Access Points · Document Management Systems · Cross-border message exchange · Exchange of evidences · Non-repudiation · Back end system integration

1 Introduction

With the introduction of Law 4440/2016 [1], Greece aspires to move towards a new era of communication of the Greek Public Authorities with each other and with citizens and businesses at both national and cross-border level. The law foresees the obligatory use of electronic communication by all Public Bodies for all document exchanges, in order to be able to offer quicker and simpler services and to reduce bureaucracy and costs. For the realization of this, it is however necessary to ensure that all communications are safe and trusted and that transaction evidences are produced and can be accessed at any time. Moreover, electronic document exchange falls under the Greek Administrative Procedure Code i.e. law 2690/1999 (OG A 45), which means that it must also comply with

S.K. Katsikas and V. Zorkadis (Eds.): E-Democracy 2017, CCIS 792, pp. 213–227, 2017.
https://doi.org/10.1007/978-3-319-71117-1_15

its provisions as far as legal validity and proof of transactions goes. Finally, the eIDAS regulation, i.e. the European regulation on Electronic Identification and Trusted Services [2], has provisions for data exchange via Electronic Registered Delivery Services, whereas the Connecting Europe Facility (CEF) European Mechanism [3], sets technical standards and provides sample implementation for eDelivery [4] and funds related actions aiming at ensuring cross-border trusted communication. However, there are still issues that remain unclear at both technical and legal level. Determination of "Qualified ERDS", signing of exchanged documents and/or messages, establishment of trust, are only examples of the issues that still remain at "grey" zone. This becomes more obvious when coming to cross border data exchange. However, even at national level it is not always easy to design and implement electronic document exchange. The Hellenic Ministry of Administrative Reconstruction has started electronic document exchange using a simple e-mail service in 2012. In 2013 the Ministry adopted the use of a document management system (DMS) that used a specific xml format for document exchange that was developed in collaboration with DMS vendors that offer services in Greece[1]. The discussion on electronic document exchange in Public Administration has revealed a number of issues given that (a) different systems provided by various vendors are used by the Greek Public Bodies, (b) the specifications about protocols and exchanged documents are not always clear or globally implemented and (c) the existing technical and legal framework (national and EU) is still uncomplete as mentioned before.

In this context it is worthwhile to investigate how the Document Management Systems (DMS) used by the different GR Public Authorities can be interconnected by implementing eDelivery specifications and solutions with minimal, or even no, interference with the existing systems and how the unspecified technical issues can be tackled in a generic way, applicable to other MS as well. In parallel it is interesting to examine how the eIDAS regulation and the Greek Administrative Procedure Code (along with all related administrative decisions) can be combined and which issues still remain unregulated in order to ensure that all exchange is conducted in a legal binding, secure, trusted and evidence accompanied way at both national and cross-border level. The connection of the Hellenic Ministry of Administrative Reconstruction (HMAR) DMS will serve as a proof-of-concept.

The structure of this article has four (4) sections as following:

1. EU Existing Framework
2. The "Electronic Document Exchange" Greek Action
3. Implementation and Issues Tackled
4. Results and next steps

[1] See press releases for the evolution of Electronic Document Exchange in Hellenic Ministry of Administrative reconstruction http://www.minadmin.gov.gr/?cat=99.

2 EU Legal and Technical Framework

2.1 eIDAS Electronic Registered Delivery Services

Regulation (EU) N°910/2014 "on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC" (eIDAS Regulation aims to raise the trust between the stakeholders of cross-border interoperable services setting the legal framework for valid and trusted electronic communication.

According to the regulation a "qualified trusted service" is a service offered by an accredited provider who is registered in at least one trusted list created and maintained by the supervisory body of a Member State (MS) i.e. the body that has been designate by the MS for this role. By introducing the EU trust mark, the regulation also gives to qualified service providers the opportunity to indicate in a simple and recognisable manner that they are registered in a trusted list and thus offer qualified trusted electronic services.

Electronic signatures, electronic seals, electronic timestamps are all considered as "qualified services". Electronic Registered Delivery Services (ERDS) are also qualified services, defined in art.3(36) of the regulation as a *service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations*.

The legal validity of Electronic Registered Delivery Services are defined in art.43 of the regulation. According to art.43 all data sent and received via an ERDS, cannot be denied their legal validity and must be accepted as evidences, even if the ERDS is not qualified. Moreover, if the ERDS is qualified, then the data transmitted are also to be considered as having data integrity, identified sender and recipient and accuracy of date and time indicated by the service.

In addition art.44 defines the requirements that an ERDS needs to meet in order to be recognised as qualified. Given the complexity in interpreting the requirements, the article also provides for the authorization to the European Commission to introduce implementing acts for the definition of standards for sending and receiving procedures, which must be followed in order for the requirements to be fulfilled; the same authorisation is granted by the regulation to the Commission in order to also issue specific implementing acts for other fields, such as electronic identification, EU trust mark, trusted lists, etc.

Until now, a number of implementing acts has been published, on electronic identification and on electronic trusted services [5]. However, no implementing act has been yet issued for ERDS, leaving the standards for qualified ERDS still unclear.

2.2 Proposal on a Single Digital Gateway Regulation [6]

The EC's proposal for an EU Regulation on *establishing a single digital gateway to provide information, procedures, assistance and problem solving services and amending Regulation (EU) No 1024/2012*, is an initiative aiming at boosting the

European Digital Single Market by making national electronic services and the related legal framework transparent and easy to reach by all potential users across Europe. The regulation sets a number of provisions for the creation of a central digital window through which national online administrative procedures, assistance services and related legislation available to domestic users, will be made available to all EU citizens and businesses. At the beginning the Member States will be obliged to offer fully online services for 13 key procedures, including services addressing various citizen and business lifecycle events such as birth, studying, working, moving, retiring, starting a business and doing business.

In order to ensure the quality of the offered information and services, all available procedures that will be through the Gateway will be subjected to specific quality criteria indicated by the regulation. Article 12 in particular, provides for the cross-border exchange of evidence between the competent authorities. More specifically the Article states that evidences for each transaction between competent Authorities must be generated whenever there is an explicit request of the online procedure's user (i.e. citizen or business).

Evidences will be generated by the competent authorities, but requested and exchanged via *a technical system established by the Commission in cooperation with the Member States*. However this is not applied for procedures *established at Union level which provide for different mechanisms for the exchange of evidence, unless they are integrated into those procedures*. From that point of view seems that the use of e-delivery may also be extended to other on line services just to ensure the creation and exchange of the appropriate evidence for each service, therefore the e-delivery is a prominent solution that can have many different types of use depending on the business requirement.

2.3 CEF eDelivery Building Block

The European Mechanism "Connecting Europe Facility" (CEF) is a funding instrument created to enhance the Digital Single Market and to promote interoperability between the different Member States in three areas: Transport, Energy and Telecom. CEF Telecom supports the connection between electronic services available in the different Member States for the communication between EU Public Administrations, Citizens and Businesses. In order to assist the Member States and to ensure technical consistency, CEF Telecom [7] has defined five Digital Service Infrastructures (DSIs): eID, eSignature, eTranslation, eInvoicing and eDelivery [8]. Each DSI, also referred to as Building Block (BB), provides the Member States with technical specifications and standards, implementation guidelines, sample implementation software, assistance services and test platforms to verify the implemented solutions' compliance to the specified rules.

eDelivery DSI refers to the electronic exchange of information (data) and it is based on a 4-corner model: corner 1 represents the sender's service/system (backend system), corner 2 the sending interoperability node, corner 3 the receiving node and corner 4 the recipient's system/service. eDelivery interoperability nodes are called Access Points (AP), they are all implemented according to the same (CEF) specifications and they handle the communication between the sender's and the recipient's systems, according

to the defined by CEF message exchange protocol. Access Points are implemented at Member State level and may run under the supervision of a public or a private body. Recipients' addresses, the related Access Points as well as conditions of accessing (ex. accepted document types) are registered in a Service Metadata Publisher (SMP); one or more SMPs may run in a Member State. The discovery of the location of the correct SMP to consult during a message exchange is done by a Service Metadata Locator (SML). Messages sent via eDelivery, are "content agnostic", in the sense that the same mechanism is used no matter the type and/or the format of the original information. Messages are "enveloped" in a pre-defined schema, commonly agreed between the communicating parties (including the APs) and followed by a set of metadata which are used for its routing. Backend integration may be achieved via the implementation of a connector. Commonly agreed evidences are produced at key route points and exchanged between the involved parties, in order to ensure legal assurance and accountability. Trust between the 4-corners is established via digital certificates (Fig. 1).

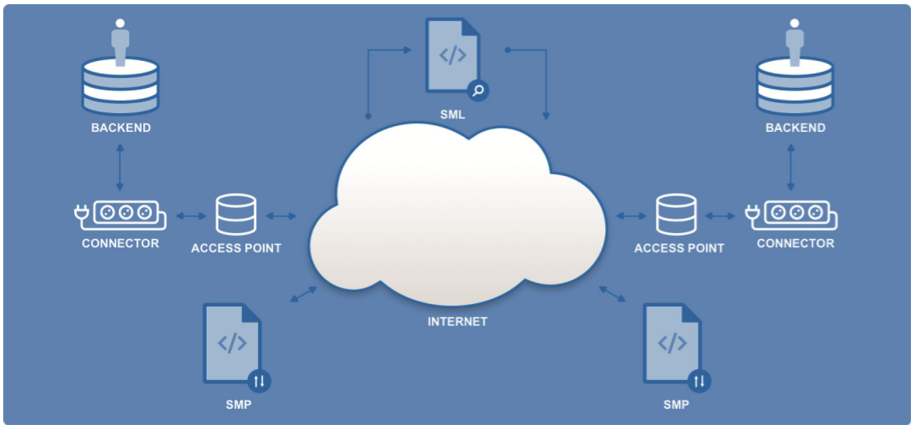

Fig. 1. The generic 4-corner eDelivery model

The generic topology of an eDelivery network as specified by CEF is the following [9]:

For the implementation of an Access Point, CEF specifies as standards the open-PEPPOL AS2 [10] (used in e-Procurement) and the e-SENS AS4 profiles [11]. The e-SENS AS4 profile is the outcome of the work on eDelivery in the context of the e-SENS project [12] and it is a profile of the ebMS3 [13] and AS4 [14] OASIS Standards, based on ENTSOG (the European Network of Transmission System Operators (TSO) for Gas [15]) AS4 profile for TSOs and on e-CODEX [16] specifications. CEF proposes a number of open- and close-Source software products that can be used for the implementation of APs by the Member States [17].

In order to ensure authenticity, integrity and trust, all messages and evidences are digitally signed by the APs. Digital certificates can either be mutually exchanged or be registered in a commonly accessed trusted list (PKI model). In the context of eIDAS this list is the one defined in the implementing act (EU) 2015/1505. eIDAS specifications

are applicable for the security controls [18]. The ETSI Electronic Signature and Infrastructure [19] standard is applied for the signature of the messages and the evidences.

For the location of data (SML) and the capability lookup (SMP), CEF specifies the e-SENS profile of the OASIS BDXL standard [20] and the e-SENS profile of the OASIS SMP standard [21] respectively. For both the SML and the SMP, CEF also offers a reference implementation software [22, 23].

The implementation of a connector for the integration of the backend systems is not obligatory but it is strongly suggested by CEF, since it offers added value functionality, such as monitoring and evidences [24]. The e-SENS REM profile is the proposed standard for evidences generation [25], implementing the REM Evidence standard.

3 The "Secure Electronic Document Exchange Action" in Greece

As mentioned in the introduction, Greece is currently working on the establishment of a network for the secure electronic communication and document exchange of the Public Authorities (a) with each other (b) with citizens and businesses and (c) with cross-border Authorities and/or citizens and businesses [26]. Until now this communication is done by using traditional post services, or in best cases, simple email services; the first solution leads to the waste of tons of paper and printing supplies, whereas the second one lacks of security and proof-of-communication. This is why eDelivery has been considered as the suitable solution to establish secure and trusted message exchange, ensuring at the same time non-repudiation of communication by either part (sender or receiver).

Even though the framework for technical specifications is already defined by CEF, the implementation of eDelivery for message exchange in the Public Administration, requires for a number of additional agreements and requirements at national, or per case also at cross-border, level. This is necessary in order to ensure the suitability of the implemented solution not only from technical aspect, but also from administrative, operational and legal point of view. Taking this under consideration, the description of metadata and the generation of the appropriate evidences are two of the most important issues to tackle. Moreover, it is necessary to define accountability at each step of the message transaction in order to be able to attribute responsibility in case of discrepancies. The definition of different degrees of confidentiality may also be needed, in order to ensure integrity and security of the transferred information. Finally, it is necessary to minimize any changes to the existing services and/or the way the users interact with them, so that the release in production of the new functionality is done in a smooth and easy way. In all cases, it is also important that all the eIDAS requirements for ERDS are fulfilled and all CEF specifications implemented, and to ensure that all decisions are accepted by cross-border partners.

The decisions about all the aforementioned issues, are generic and applicable to all services connected to the Hellenic eDelivery infrastructure. This considered, the initial phase of the action includes the development of a connector for the Document Management System used by HMAR, and the interconnection of the Ministry and of at least one other Public Authority using the same DMS, as an initial proof-of-concept [27]. It is worth mentioning that the HMAR DMS is one of the more commonly used in the

Greek Public Sector. At a second phase the connector for another widely used DMS and the connection for more than 20 other Public Authorities of the Central and the Local Government, using either one of the two, will also take place.

Given the number of different backend systems that need to be connected, four (4) access points have or will be developed initially in Greece: AP1 for the connection of the DMS of Public Authorities of the Central Government, AP2 for Cross-border communication, AP3 for the connection of services addressed to citizens and businesses and AP4 for the needs of the Local Government. AP3 will be implemented and be operated by Hellenic Post SA, whereas the rest three are currently under the responsibility of HMAR.

Before the beginning of the action one Access Point has been implemented for pilot purposes in Greece as a result of a joint action between Germany, France, Austria and, at a later stage, Slovenia and Greece in the context of the e-SENS "Business Lifecycle" WP5.4 domain [28]. The results of e-SENS were delivered to CEF. The results of this work are being evolved in the CEF funded project "NO Barriers in eDelivery (NOBLE)" [29]. Through NOBLE Greece, Germany, France and Slovenia continue to cooperate in order to address implementation problems that remain open and to move things forward. Issues, such as advanced evidence generation and exchange, use of SMP and establishment of trusted lists will be tackled by NOBLE partners. The main target is to make the eDelivery network developed in e-SENS fully operational at production level. The project intends also to extend at cross-border level the use the existing ERDS, especially those offered by Postal Services. This way more ground for communication and business transactions with other Member States will be offered enhancing the Digital Single Market.

The development of AP1, AP2 and AP3, the connection of a service addressed to citizens/businesses (to show communication with end users via the Hellenic Post SA services) and the communication with foreign ERDS all fall in the context of the NOBLE action. The same goes for the connector of HMAR's DMS, which means that the specifications definition, will also take into account all decisions taken at NOBLE level for cross-border communication.

The connector for the second DMS and the connection of the other Public Bodies are the purpose of the, also funded by CEF, project "Secure Document Exchange with eDelivery in Greece". This action is complementary to the NOBLE one and will re-use and extend its results for the needs of the Local GR Government.

In order for the whole action to be successful, the aforementioned technical activities, will be accompanied with administrative acts and, if necessary, legal provisions. In all cases it is important to ensure that the system created will be functional not only at technical but also at operational level.

4 Implementation and Issues Tackled

The implementation of the HMAR DMS connector [30] followed the implementation of AP1 (for the connection of Central Government Public Bodies) and of the SMP. The AP and the SMP follow the CEF specifications and the implementation details decided

by NOBLE partners. The AP implemented the Holodeck AS4 software solution [31], which is an open source product that offers basic AP functionality fully compatible with the AS4 standard. Given that extra functionality is required to support the evidence required by the Administrative Procedure Code a connector in front of the AP is also being implemented. The SMP currently is based on Philip Helgers' PEPPOL SMP server. The additional support for the trusted list is being examined and alteration in the current version will be required.

For the implementation of the DMS connector two major factors had to be combined: cross-border (namely CEF and NOBLE) specifications (given that the exchange of messages isn't limited at national level) and national legal and administrative requirements. Message envelope format and core metadata are defined at cross-border level. However it may be needed that additional metadata are defined at national level; they will also be transmitted cross-borderly but they will not be used at the destination country. The same goes for evidences: core evidence information as defined for cross-border communication must be generated at all cases. Any extra information required for national communication is acceptable even though not necessarily processed in the destination country. Minimum metadata and evidences exchanged at cross-border level are a matter of bi- or multi- country negotiation and it is important. However it is not always easy or feasible, to find a compromise that address each country's minimum requirements. As mentioned earlier in the paper, message exchanged are content agnostic. Nevertheless, given the Hellenic Administrative Procedure Code, it was necessary to define the basic categories of documents to be transmitted and some specific metadata for each one. For the fulfillment of the special national needs, the extended part of the AS4 and REM messages will also be used.

4.1 Message Creation and Routing

According to the existing legal framework and defined procedures, in the Greek Public Administration "conventional document exchange" is done via each Public Authority's DMS. For communication with another public authority or with a business, the sender defines the recipient's organization and the address (postal and/or email) and optionally the final recipient's name and address (if different than the one of the organization). When coming to communication with citizens, the sender defines the final recipient's name and (postal and/or email) address. The sender also defines a set of metadata (such as subject of document, type, keywords, etc.), is then forwarded via the DMS to the (sender) Authority's DMS and then sent to the destination Authority/business/citizen via post and/or email.

In the HMAR's DMS "conventional routing" is done through a screen in which the user uploads the document(s) to be transmitted and adds a set of mandatory and optional metadata. The name, subject and date are mandatory, whereas other information such as remarks, keywords, etc. are optional. The address of the recipient is already registered in the DMS system, since the recipient(s) are chosen by a predefined list. Before the sending of the document the system adds automatically some extra information, namely document unique identification number, year and date.

Given that the generic legal and procedure framework must still be followed, routing via eDelivery will be done in the same way, with the addition of a new "eDelivery address" field to the recipients' predefined list. The user will be able to select the recipient's (no matter if it is a Public Authority, a business or a citizen) eDelivery address instead of the "conventional" one. The system will recognize the type of the address and will automatically make all necessary adjustments to route the message via the eDelivery network (see Fig. 2 below). Almost no changes are necessary in the current user-interface in order for eDelivery document exchange. All the added functionality is achieved via the connector implemented.

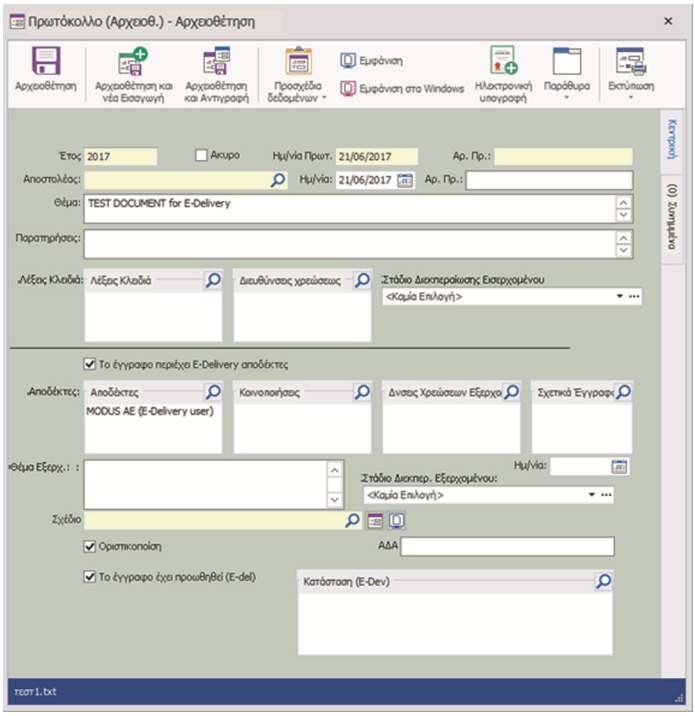

Fig. 2. eDelivery message metadata in the HMAR DMS

The (eDelivery) addressing schema has been agreed in the context of the e-SENS WP5.4 action and it is an email like address where the recipient's domain is included. The domain, deriving from the address, is sent as an additional metadata, so that the related AP can be discovered via the SMP/SML.

Following the provisions of the existing legal framework and in order to maintain the existing granularity schema, the addresses of the Public Bodies will be assigned to each instance of the DMS used by the recipient Public Body. For instance for HMAR where four different DMS instances are used (Generic, Confidential, Secretary Generals and Ministers' DMS instance) four distinct eDelivery addresses will be defined.

The connector developed runs in front of the DMS system and connects it with the AP connector. In the topology, depicted in Fig. 3, Corner 1 includes the DMS connector ("Papyros Bridge") and the Public Body DMS in the right, Corner 2 the right Access Point and Connector, Corner 3 the left Access Point and Connector and Corner 4 the left (unnamed) system:

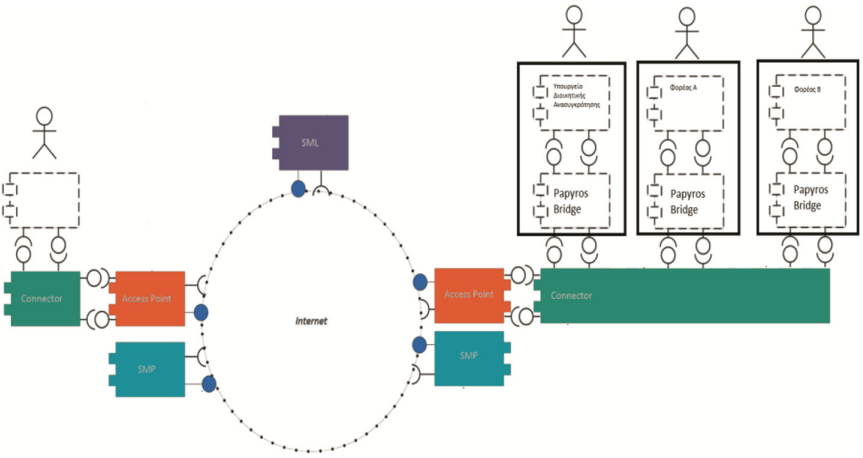

Fig. 3. Connecting GR Public Authorities via eDelivery Topology

The message format is the one defined in the context of the e-SENS project, re-used in NOBLE and it is a standard SBD/SBDH document. The message's header contains the appropriate routing metadata according to the e-SENS SBDH profiling [32]. The document and its metadata are included in the body. The document to be exchanged and any attachments are included in the body's message as an "Attachment Type" element.

Additionally to the metadata described by the SBDH profile, for the documents exchange in Greece more metadata need also to be transmitted. The extra metadata derive by the core document attributes defined in the context of the Greek eDocument Interoperability Framework [33]. The type of the document for which a pre-defined list will be described, the protocol date, remarks, other recipients and/or notifications and document issuer may be included as metadata. Other fields may also be defined at a later stage.

For the transmission of the message between the four corners a REM-Dispatch message is created and signed by the connector, namely the DMS (Corner 1). The message is sent to the connector of Corner 2. For cross-border communication it has been commonly agreed that no evidences are needed by Corner 2. For national message exchange a REMevidence Acceptance/RejectiononSubmission is generated at Corner 2.

Corner 2 evaluates the recipient's address against the SMP in order to discover the recipient AP (Corner 3). Once the message is received by Corner 3 a DeliveryNonDelivery evidence is generated. According to the current implementation the message is not sent back until Corner 4 (i.e. the recipient) accesses its mailbox. However since

responsibility ambiguities may occur, this may change so that the Delivery/NonDelivery evidence is signed by Corner 3 and sent back to Corner 2 immediately.

When the message arrives at Corner 4 two more evidences AcceptanceRejection-ByRecipient is generated by Corner 4. The evidences are signed by Corner 4, sent back to Corner 1 (i.e. the Sender) and it is displayed as a flag of the related message at the DMS system.

4.2 Open Implementation Issues

Evidences Generalisation

As it is described in the previous paragraph three types of evidences are currently generated for national and cross-border communication needs: DeliveryNonDelivery by Corner 3, RetrievalNonRetrieval and AcceptanceRejection by Corner 4. These represent the minimum set of evidences agreed among the NOBLE partners in order to ensure liability at cross-border level.

However, it is possible that at a second stage more detailed evidences are required at national level for administrative and legal purposes, especially when it comes to documents exchanged between Public Authorities and citizens/businesses. The implementation of such functionality may require either the generation of other type of evidences, such exchange of evidences between Corner 1 and Corner 2 or the addition of more information in the existing ones. In all cases, this will not affect the cross-border communication since any extra information will simply be ignored by the receiving systems.

Moreover, the proposed EU Digital Single Gateway regulation provides for the generation of evidences for Public Authorities communication upon request of the final (citizen or business) user and exchange via a central technical system. Once the regulation is accepted and put into force, it may have impact on the way or the type of evidences generated and the way they are exchanged.

Trust Establishment

Trust Establishment is an issue that still remains open for both domestic and cross-border message exchanges. Mutual exchange of certificates, which was initially used, is suitable only for a limited number of services/APs.

Moving towards the connection of multiple services/APs calls for the use of something more generic and less cumbersome. Trust lists (TL), where the APs' and possibly the SMPs' certificates are registered are definitely a good solution. However it seems to be rather complicated and difficult to maintain TLs within the scope of the current action (including the NOBLE project). In this view, it has been decided to use an intermediary solution for proof-of-concept reasons. The CEF PKI service [34] has been used for the issuance of certificates for all the implemented APs and SMP; these certificates will be registered in a shared key store created for the needs of the project and will serve as a mockup of a trusted list. Once maintenance and governance issues are solved, TL will be used in production environment.

Messages Signature
Messages and evidences are signed by the sending corners before their transmission. Currently the XML Signature generated by the SPOCS (XMLDsig) [35] components is used. This is ETSI REM compliant but it is not conformant to the eIDAS specifications for Advanced Electronic Signatures (AdES). Taking this into account, the signature service will be upgraded to at least XAdES-B [36] in order to meet the Advanced e-Signature standards.

Integration of SMP with the existing AS4 implementation
SMP has been implemented and it is being used for capability lookup. However the Holodeck AS4 software solution doesn't offer as open source software any functionality for the connection of the AP to the SMP. This means that extra implementation is required either in-house or by an external vendor. Since this is an ad-hoc solution, maintenance and update cost can raise dramatically.

On the other hand, other AS4 compliant software solutions are also proposed by CEF. Some of them (ex. Domibus i.e. the CEF sample implementation [37]) do offer SMP connection functionality but they have to be examined in details in order to decide whether or not they fit the generic GR DMS connection requirements. An impact and cost analysis for each one is needed in order to estimate how difficult it is to move towards another solution and whether the benefits of choosing a commercial product (ex. IBM solution [38], FLAME [39]) outweighs its acquisition and maintenance cost.

5 Conclusions - Next Steps

In order to pass from paper to electronic document exchange it is necessary to ensure that electronic communication is done in a secure, trusted and evidence emitting manner. No room for legal ambiguities, administrative failures and/or organizational gaps should be left. The implementation of the EU specifications and standards for eDelivery along with the eIDAS regulation provisions for ERDS are key elements for the achievement of the aforementioned goal. Through the connection of the DMS used by HMAR, it has been showed that secure and trusted electronic communication with Public Bodies using the same DMS is possible. Moreover via the e-SENS and NOBLE projects the Hellenic ERDS connected in the domestic eDelivery system will be able to also communicate with other ERDS originating from the other partner's countries, setting the grounds for a more wide EU cross-border message exchange.

The national next steps include the establishment of communication with end users, which will be achieved via the connection to the existing AP of a number of ministry's services addressed to citizens and businesses. The implementation of the AP held by Hellenic Post and the connection of their services will complete the network. Administrative documents and acts will be sent by HMAR to Hellenic Post (via AP1 and AP3) and then routed by the Hellenic Post backend system to the address declared by the citizen/business (which may be an eDelivery, an e-mail or a postal address). In this case, a mixed model of communication will be used: eDelivery to eDelivery, eDelivery to email and eDelivery to paper. For the routing of the initial message the connector will

be programmed to set as recipient address in the SBDH the eDelivery address of the Hellenic Post, keeping the final recipient address as part of the message's metadata.

Implementation of cross-border communication will continue via the NOBLE project. The work already achieved and the fact that there are issues that still remain open and need to be negotiated, show that there is a number of more specific technical guidelines and of administrative decisions that need to be taken. In some cases these are policy decisions and they exceed the limits of the project. Issue like minimum required evidences and corner of generalisation for cross-border communication, governance and maintenance of central trusted lists, standards for the signing of messages and evidences are some core issues that should be resolved at EU level. In the context of the NOBLE project some agreement can be made between the partners, but the extension of the functionality to other countries demands for more central decisions.

Moreover there is still lack of specific standards for qualified ERDS, which gives room to interpretations and diversity in the offered services. When it comes to cross-border communication this may cause security and trust discrepancies. At this stage and in order to achieve the desired level of quality and assurance, one or more eIDAS implementing acts on qualified ERDS are necessary to set the appropriate standards. The definition of an eIDAS cooperation network so as to permit to all the MS to cooperate and the drafting of a related proposal could be a first step towards this direction. The connection of a new ERDS system to an AP causes some additional implications that have to be tacked regarding the management of the SMP i.e. how the new ERDS will be registered to the SMP. The registration can either be centralized or decentralized providing the connector the possibility to add new systems to the AP and do the appropriate registration to the SMP. Last but not least the notification of the existing ERDS systems regarding the changes in the SMP is still an ongoing issue, since the existing available EC sample implementation does not provide such functionalities. It is crucial for the end user of a document management system to be aware for the ERDS systems that are being connected to the trust realm of the document exchange domain. For these issues further work is required.

More specifically in Greece the action will also continue with the implementation of the AP for Local Government, the connection of another widely used DMS and the participation in the eDelivery system of more than 20 additional Public Authorities. In order to ensure interoperability, the requirements and specifications defined for the connection of the HMAR DMS will be implemented. It is obvious that each time a new DMS or service joins the Hellenic eDelivery network, a new connector must be developed. For the integrity of the system, it is necessary that all new connectors comply with the same rules and follow the same standards. As long as the legal framework remains the same, the basic required functionality shouldn't differentiate from one system to another.

References

1. Law no 4440/2016 (Government Gazette Part A, no 224) on "Regulatory Governance: Principles, Processes and Means of Better Regulation"
2. eIDAS regulation. http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&from=EN

3. Connecting Europe Facility (CEF). https://ec.europa.eu/inea/en/connecting-europe-facility
4. CEF Digital eDelivery. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eDelivery
5. EU eIDAS observatory. https://ec.europa.eu/futurium/en/content/eidas-implementing-acts
6. Proposal for a Regulation on Digital Single Gateway. https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-256-0_en
7. European Commission Strategy on Digital Single Market. https://ec.europa.eu/digital-single-market/connecting-europe-facility
8. CEF Digital Home. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/CEF+Digital+Home
9. CEF Digital eDelivery overiew. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/How+does+eDelivery+work+-+Overview
10. Peppol Homepage. http://peppol.eu/
11. eSENS Generic Architecture Repository AS4. http://wiki.ds.unipi.gr/display/ESENS/PR+-+AS4
12. eSENS homepage. https://www.esens.eu/
13. OASIS open document on ebms3. http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/os/ebms_core-3.0-spec-os.pdf
14. OASIS open document on AS4. http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/profiles/AS4-profile/v1.0/os/AS4-profile-v1.0-os.html
15. ENTSOG homepage. https://www.entsog.eu/
16. e-CODEX Homepage. https://www.e-codex.eu
17. CEF Access Point Software. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/e-SENS+AS4+conformant+solutions
18. CEF Security Control Guidance. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Security+Controls+guidance
19. ETSI Electronic Signature and Infrastructure. https://portal.etsi.org/esi/el-sign.asp
20. eSENS Generic Architecture Repository DBXL. http://wiki.ds.unipi.gr/display/ESENS/PR+-+BDXL+1.3.0
21. eSENS Generic Architecture Repository SMP. http://wiki.ds.unipi.gr/display/ESENS/PR+-+SMP_home
22. CEF SML Software. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/SML+software
23. CEF SMP Software. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/SMP+software
24. CEF Backend Integration. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/How+does+eDelivery+work+-+Backend+Integration
25. eSENS Generic Architecture Repository REM. http://wiki.ds.unipi.gr/display/ESENS/PR+-+REM
26. Press release for implementation of eDelivery. http://www.aftodioikisi.gr/ipourgeia/dimosio-ilektronika-i-diakinisi-engrafon-apo-fthinoporo-oi-protoi-foreis-lista/
27. Hellenic Ministry of Administrative Reconstruction Call for Connecting the Document Management System to eDELIVERY. http://www.minadmin.gov.gr/?p=20938
28. e-SENS Business Lifecycle eDELIVERY. http://wiki.ds.unipi.gr/display/ESENSPILOTS/5.4.2+-+Architecture+and+BB+Implementation+-+eDelivery. last updated
29. NOBLE Press Release. https://www.governikus.de/fileadmin/user_upload/Pressemitteilungen_PDF/PressRelease_GovernikusKG_CEF-NOBLE_Feb2017_english.pdf
30. Hellenic Ministry of Administrative Reconstruction and MODUS S.A., Contract for the Connection of the Hellenic Ministry's of Administrative Reconstruction Document Management System to eDELIVERY, Athens, April 2017
31. Holodeck homepage. http://holodeck-b2b.org/

32. e-SENS SBDH profile. http://wiki.ds.unipi.gr/display/ESENSPILOTS/5.4.2+-+Architecture+and+BB+Implementation+-+eDelivery?preview=/29921991/33587213/Business%20Lifecycle%20SDBH%20Profile%20v0.5.pdf#id-5.4.2-ArchitectureandBBImplementation-eDelivery-BusinessLifecycleSDBHProfile
33. Greek e-Government Interoperability Framework homepage. http://www.e-gif.gov.gr/portal/page/portal/egif
34. CEF PKI Service. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/PKI+Service
35. SPOCS Homepage. https://www.eu-spocs.eu/
36. XADES xml signature. https://joinup.ec.europa.eu/sd-dss/webapp-demo/doc/dss-documentation.html#_the_xml_signature_xades
37. CEF Digital Domibus Access Point Software. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Domibus
38. IMB Electronic Data Interchange (EDI) Services. http://www-05.ibm.com/services/dk/ecommerce/index.html?ca=ecommerce&me=w&met=dk_hp_tab2
39. Flame Messaging Solutions. http://flame.co.za/