

A Collaborative IT Network for Three Adriatic Maritime Ports

Stefanos Petsios and Chrysostomos Stylios

Department of Computer Engineering,
Technological Educational Institute (T.E.I.) of Epirus,
47100 Kostakioi Arta, Greece
stefanos@kic.teiep.gr, stylios@teiep.gr

Abstract. Collaborative IT networks are suitable to model and represent the interconnected maritime ports that in nowadays globalized world are poised for tremendous growth. Actually, there are already such strongly connected collaborative networks mainly serving national purposes. Although, there are almost no collaborative networks for maritime port B2B platforms for cross border services. Here, we present a pilot collaborative network that was built to serve in Adriatic Sea among three heterogeneous and autonomous maritime port community systems (PCS). Their integration was based on a cross border platform that dealt with several challenges and met all the key requirements set by the stakeholders. In this paper we present the design details of this innovative platform, the experimental results of the prototype and the potential for wide use.

Keywords: Maritime Ports, data exchange, web services, business2business, cross border IT, port stakeholders, EDI exchange, port community systems.

1 Introduction

European Union has effectively undertaken actions in the field of maritime security and transportation services that led European ports to work towards creating cross border alliances. This is the case of a project named Adriatic Port Community (APC) [1] aiming to enhance the collaboration of port process of the participating ports (Venice, Igoumenitsa and Ploče) through the establishment of a common information interchange electronic platform. Almost all modern ports have developed Port Community Systems (PCS exploiting Information Technology to provide better passenger and maritime services. Interactions, exchanging, and collaborations among PCS are fast becoming a necessity in today's international freighting and transportation industries. Sophisticated logistics chains require an accurate flow of information for tracking, planning and control. Many sectors of the shipping and containerization industries already used Electronic Data Interchange (EDI) [2] as a natural technology for the communication of much of this vital information. Since the first efforts for data interchange in international trade the contributions of such applications, to governments and corporations, are primarily to provide models of

successful applications to existing international processes, such as transportation and trade [3]. Port Community Systems have played a major role in facilitating and increasing the efficiency in movement of goods and passengers while allowing Customs and all the other interesting government departments to organize effective inspections [4]. This study revealed a great variety of existing port community systems in terms of features and implementations. While the needs of different ports vary, also PCSs usually differ quite a lot from each other. There is no golden rule or guidelines between them except the wide use of EDI for the paperwork similar to the IMO FAL forms [5].

Today's trend is Single Window for implementation of modern PCS that significantly help to organize and improve the efficiency of a collaborative network of PCSs. Admissible European directives and development frameworks and methodologies were examined [6] towards the efficient implementation of cross border service models. The APC project successfully recorded and described all the in-port stakeholder's needs but also the "cross border needs" to achieve quality of travelling services for passengers, security and goods transportation. In this paper we present the main outputs regarding the APC collaborative network named hereafter Global Single Window (GSW). Key points of the paper refers to the approaches regarding data restriction, data sharing, and user moderation.

2 The Needs and Requirements of a Cross Border Collaborative Network for PCSs

In Port Community Systems the required IT services are usually maintained and handled by the local port authorities covering all the needs and features that ensure a smooth working environment between the port stakeholders. Any PCS has to be aligned with all the national laws, European directives and obligations. Within APC project we expanded their functionality by creating special supplementary modules to the PCS to implement data exchange interfaces. The aim was to strengthen the relationship between ports, to make the procedures more efficient, harmonized and to reduce the time for administrative procedures linked to ship's arrival and departure. The analysis of the main process among the three port authorities, identified the key actors, the cases and the existing port procedures that could benefit from cross border data. In early stages of the analysis it was mandatory to create a new common web platform, based on the principle of "single window", for all the stakeholders and cross border processes. Each PCS had only to create a new software module for data exchange and there was not acceptable to perform significant modifications to the existing processes and data handling. There was identified a set of practical and useful processes, a universal communication protocol, the exchanged data format, a pairing of terms in four languages and an innovative process to moderate and handle the users and the data in the proposed collaborative network of port community systems.

3 Innovation / Contribution

3.1 Actor Identification

The port community processes and the role of port authorities have a direct impact in the way port communities are using ICT technologies. Consequently it is worth to enlist the main roles of all actors being part of a port community system that were identified for the APC ports: shipping agent, forwarding agent, port authority, harbor master, mooring services, terminal operator, waste treatment, vessel supplies, customs brokers, customs authority, police, security of port area, inspection services, fire department, gate control and haulers.

At the next stage we narrowed them down the roles that were interested and allowed to access cross border maritime port data: 1) Shipping agent, 2) Port authority, 3) Coast Guard, 4) Police, 5) Security of port area, 6) Customs Authority. There was also identified two global moderated roles named: 7) global administrator and 8) local port moderator. The global administrator was a special role to be used only for moderating the users with local port moderator, no other permission was allowed. Global administrator had no authority to perform moderation on attributes and parameters handled by the local authorities. Such actions were performed only by the local port moderators.

3.2 Data Sharing and Collaborative Operations in Maritime Ports

The inspiration to create collaboration network between maritime ports was born from four key areas. These key areas mainly use the data collected in the local port community systems which can be improved by enriching ship data retrieved from the other participating ports of the collaborative network.

For example a ship, carrying dangerous goods, which left from Venice with direction to Igoumenitsa must be declared at the departure in Venice (IMO FAL document 7). This information (data at Venice) may be used in Igoumenitsa (as extra input to OLIG PCS) in order to perform on time activities to handle safer and better the expected to ship's arrival dangerous goods.

First key area was related to the ship arrival and departure management. This manages port processes related to a ship's arrival and departure in/from the port up to the announcement, up to obtainment of the inward/outward clearance. It coordinates the exchange of documents, port information and decisions between the different public and private parties that interact with a member of the port community.

The second area was related to custom export clearance applications. This represents an up-to-date tool capable to provide the customs clearing readiness for export goods functionality and to set up the departure cargo manifest.

The third area was custom import clearance applications. This activity was designed to reinforce and speed up the import of cargo customs clearing operations at the port premises as early as possible. To achieve the expected result the implemented modules allowed to prepare the statement of incoming cargo manifest when it was certain that the ship called at the port of reference for the arrival, even when the ship was still be under way.

Last area was the parking space booking and in port traffic. The collaborative network can deliver extra information to help in port traffic and parking space automated estimators to perform better on congestion avoidance in port facilities and services. For example we the PCS can predict to have more personnel at the gates when a passenger ship unloads and loads thousands passengers and vehicles in a short period of time.

During the implementation step, APC created a set of on demand operations where port community users could fetch data from foreign port authorities on the collaborative network. Thus, the system provided authorized and analytical communication information among all the participating ports. The exchanged messaging and data was in XML format as described in [7] and the data was a superset of information based on IMO FAL documents and stakeholder requirement analysis.

3.3 Data Restriction and User Management of the Collaborative Network

The user authentication, role management and user profiling was based on the commonly used Lightweight Directory Access Protocol (LDAP) services. Each user in order to use the GSW should be authenticated based on the profile stored to the APC LDAP service. Moreover each participating port can dynamically moderate the privileges assigned to the roles of other collaborative ports based on the location of the user and the role. For example a port moderator of port A can restrict or permit the shipping agents of port B to access a subset of data belonging to port A. These set of privileges were also included accordingly to the LDAP schema.

The data restriction was a process triggered whenever a user tried to start a data retrieval operation. This restriction performed in two logical authentication levels.

- The first level of authentication takes place on the GSW platform and does not allow the user to create any data retrieval to the port.
- The second level of authentication was handled by the new implemented module in the local port community system. In this case the PCS through the module performs the second restriction data according to the parameters provided from the GSW and restrictions stored to the local PCS. With this feature the port authorities have the option to know who the recipient of the requested data is and perform extra restrictions actions accordingly.

The main objective for this innovative approach was to create cross border “teams”. It was asked, by the stakeholders, to design an extra feature that the data submitted from a shipping agent user to a PCS A can be restricted and be available only to shipping agent users belonging to the same working company in port B. Without this extra feature it was possible, unintentionally to permit competitors to reach sensitive company data. With the second authentication level now we could separate the shipping agent roles based on their companies and create any motif of cross border – multinational trusted teams.

Summarizing all the above we present the two level of authentication in a short example of how we can have a cross border team between the user X@ppa (user from Ploce Port Authority) and user Y@vpa (user from Venice Port Authority).

- step1: The user X@ppa will use the GSW to search for dangerous goods in a ship that comes from Venice.
- step2: The GSW will use the PPA's role/privileges matrix to see if the dangerous goods service at VPA is available for the shipping agents of PPA.
- step3: If step2 permits the access the GSW starts the appropriate service of VPA including all the details related to the profile X@ppa (team tag, team members etc.).
- step4: the PCS module of VPA PCS will evaluate the team parameter and accordingly it decides if the related data was submitted from a user (in VPA) of the same team.
- step5: Accordingly the returned data are plotted to the screen of user X@ppa.

Implementing the First Level of Authentication the GSW LDAP service stores a logical two dimensional matrix for each port where the operations of the prototype were correlated with the eight (8) different user types as were described in paragraph 3.1. According to the privileges given on this matrix the GSW platform enable's or disable's for each user the available operations.

The flow of processes related to the second level of authentication includes a matching mechanism, by port authority, in order to map the teams with users on the local port community system. This functionality was applicable only for local port community systems where the submitted data were linked with GSW users or with the cross border "teams".

3.4 The Architecture of the Collaborative Network

The architecture was a web based platform enabling intelligent and secure exchange of information between port stakeholders of the three Adriatic port community systems. The architecture challenges were set to be able to update information and maintenance system that supports per year more than 10000 sea going ship calls, create innovative efforts for safely and trusted data, increase productivity and quality for maritime services, semi-automated acquisition of master data, single window implementation. In Figure 1 the most important modules were depicted in order to create a representation of the used approach. The GSW platform consists of: GSW Application Services, GSW Web Service (client), GSW Application, GSW Web Interface, GSW Application layer, Open LDAP (server) and a Database Server. The three participating PCS implemented a web service that followed the APC protocol. A thorough description of the communication protocols, LDAP and database schemas can be found at [1].

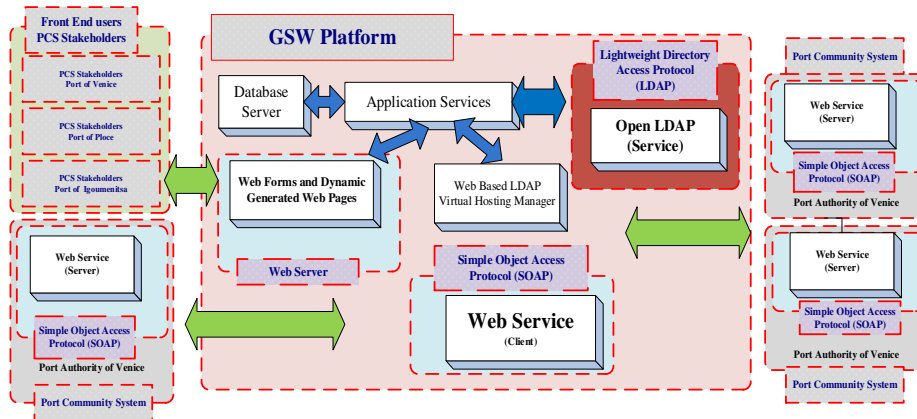


Fig. 1. The overall architecture of the collaborative maritime network

4 Experimental Results of the Collaborative Network

The most common communication method for daily port processes were, as anticipated, the port community system, telephone and fax, as well as e-mail. For the shipping companies the main volume of data exchange and internal communication was served via their corporate information systems. In very rare occasions for port to port communications were performed by formal communication procedures. Such processes usually involved other public sector services like customs authorities. Within APC prototype was performed quantitative and qualitative evaluation. The quantitative evaluation benchmarked the prototype under low and high stress. The qualitative analysis was based on evaluating questionnaires filled by the port stakeholders.

4.1 The Quantitative Analysis of the Collaborative Network

To generate test cases the methodology was based on a three-step procedure from a fully detailed use case. The first phase created a set of use case scenarios randomly generated by identifying combinations of main and alternate flows on the basis of the use case description. Once the full sets of scenarios were identified, the next step was to describe test cases with a variety of conditions and data elements required to run the scenarios. Since all test cases were identified, there were reviewed and validated thoroughly to ensure accuracy and search for redundant or missing test cases. Once they were approved by the stakeholders, the final step was to substitute actual data values. However, some of the interactions with the system did not included data input, but user actions such as clicking with the mouse in a specific area of the screen or scrolling. The test bed was based on a tool named SOAPUI and we run a complete set of tests to each participating PCS. The stress test was performed as a debug tool and as evaluation tool to estimate the traffic and limitations of the different implementations. Moreover the stress test was an indicator of the scalability of the

system. Details of the results are out of the scope of this paper and can be found at [1] but the potential of generalization was based on these tests.

4.2 The Qualitative Analysis

Local stakeholders evaluated the system. Evaluation procedure included presentations and training of the GSW during bilateral meetings between APC team members and port-related stakeholders. During demonstrations there was presented the usage of both systems to stakeholders, and they had the opportunity to discuss about related issues and to suggest changes and future improvements. The developed GSW system would be used every day by the customs and harbor master officers, but only in special occasions by the shipping companies. The overall assessment of the Global Single Window application, based on the demonstration and discussion sessions with the representatives of each stakeholder, led to the following output that:

- 20% certain modifications required to be made
- 50% suitable for their needs as is
- 30% minor improvements were required

Overall, the GSW application was positively evaluated with the following key benefits for the customs operations:

- Faster and more reliable exchange of information.
- Estimation of anticipated workloads.
- Redundant channel of updating delays in ship arrivals.
- Statistical record of arrivals/departures for ships, trucks, private vehicles.
- Complementary tool to the existing one.

Custom officers stressed that documents exchange and communication from and towards the customs authority is legally restricted and usually confidential. Due to this attribute, the customs employees will normally be able to receive and utilize the information from the GSW system, but only provide limited amount of data to other users only through the port community system. The Coast Guard representatives were highly positive about the functionalities of the features presented, because they would have fast and systematic access to well-structured data allowing them to crosscheck passenger or vehicle movements and to improve other everyday operations.

5 Potential Generalization and Conclusions

The success of the developed IT collaboration network was multidimensional. The project consortium successfully identified all the necessary non-functional requirements for designing and implementing the cross border data exchange system. The test of the developed system proved that the data, related to departure of a ship, stored in a maritime port community system is very useful to the destination port. In order to implement this collaborative network, there were a lot of difficulties such as different interpretation of data, national laws, added effort and requirements to the

existing port community systems. The qualitative and quantitative evaluation of the prototype showed that between two ports with direct ship transportations connections should perform direct or in-direct data exchange and so to raise the provided port services and reduce their load. The benchmarking tests of the pilot showed that the scalability of the network was quite impressive and even a network of 100 ports could be handled by the proposed collaborative architecture. The feedback gathered, from the three PCS, showed that all port authorities with often direct ship connections, either at national level or international level, should make efforts on establish PCS data exchange.

Results of the pilot suggest the following improvements for similar applications: Existing port community systems should create more complex data sharing modules in order to enrich their available data presented to the stakeholders. Certified users could use directly the port community system user interface to access cross border available port data. Secondly the directory services that were handled by the GSW LDAP server and the proposed two levels of authentication were highly connected to the efficiency of the modules implemented by the port community systems. For future implementations, it is suggested to create a distributed LDAP service over the centralized one, used in APC collaborative network, which would offer better flexibility and data control.

Acknowledgement. This work was co-supported by the APC Project, part of the Adriatic IPA Cross Border Cooperation Program and by the E.U. FP7-People-IAPP-2009, Grant Agreement No 251589, Acronym:SAIL

References

1. Adriatic Port Community, <http://www.apcwindow.eu>
2. Garstone, S.: Electronic data interchange (EDI) in port operations. *Logistics Information Management* 8(2), 30–33 (1995)
3. Wrigley, C.D., Wagenaar, R.W., Clarke, R.A.: Electronic data interchange in international trade: frameworks for the strategic analysis of ocean port communities. *The Journal of Strategic Information Systems* 3(3), 211–234 (1994)
4. Long, A.: Port community systems. *World Customs Journal* 3(1), 63–67 (2009)
5. Burmester, C.: International Ship and Port Facility Security (ISPS) Code: the perceptions and reality of shore-based and sea-going staff. *Maritime Security and MET*, 185–194 (2005)
6. Fjortoft, K.E., Hagaseth, M., Lambrou, M.A., Baltzersen, P., Papachristos, D., Nikitakos, N.: Maritime transport single windows: issues and prospects. In: *Proceedings of the 9th International Symposium on Marine Navigation and Safety of Sea Transportation—TransNav* (2011)
7. Petsios, S., Stylios, C.: A platform and exchange protocol for cross border application in maritime ports. In: *Proceedings of the TEN ECOPORT 1st International Conference on “Sustainable Development of the Sea-Corridors and Coastal Waters”* (2014)