

***DELIVERABLE***

**D19 – iWebCare Platform Overall  
Assessment Report**



**iWebCare : Integrated Web  
Services Platform for the  
Facilitation of Fraud Detection in  
Health Care**

Project reference number **IST-2005-028055**

## Deliverable Number D17

Project Number:	IST-2005-028055
Project Title:	iWebCare
Deliverable Type: (PU/PP/RE/CO)*	PU

Deliverable Number:	D19
Date of Delivery:	10/12/2008
Title of Deliverable:	iWebCare Platform Overall Assessment Report
Work-Package contributing to Deliverable:	WP7
Nature of the Deliverable: (R,P,D,O)**	R
Author(s):	Costas Ballas
Author's org. short name	INTRA

### **Abstract:**

This report provides the overall assessment and evaluation of the iWebCare integrated web services platform and of the two pilot applications.

### **Keywords List:**

Healthcare, e-health, e-gov, fraud, RBH, NHS, TSAY, dataset, pilot application

**\*Type: PU-public, PP-Restricted to other programme participants (including Commission Services), RE-restricted to a group specified by the consortium (including Commission Services), CO-confidential, only for members of the consortium (including Commission Services)**

**\*\*Nature: R-report, P-prototype, D-Demonstrator, O-other**

## Table of Contents

Executive Summary .....	6
1. Introduction.....	7
2. Scope and purpose of pilots .....	9
2.1. Introduction .....	9
2.2. Evaluation objectives .....	9
3. Pilot methodology .....	12
3.1. Introduction .....	12
3.2. Approach used.....	12
3.3. Key activities .....	13
3.4. Evaluation tools.....	14
4. Pilot context.....	16
4.1. Introduction .....	16
4.2. Data used for pilot.....	16
4.3. Description of fraud to be identified by iWebCare platform.....	17
4.4. Description of users involved in pilot .....	17
5. Results .....	19
5.1. Analysis of findings from user diaries and critical incident reports .....	19
5.2. Analysis of findings from statistical data generated from iWebCare platform.....	20
5.3. Analysis of findings from questionnaire survey.....	23
5.4. Deviations from planned and actual pilot.....	29
6. External Experts Evaluation Report .....	31
7. Overall Conclusions.....	33
8. Annex .....	35

## Revision History

<b>Date</b>	<b>Version</b>	<b>Description</b>	<b>Author</b>
10/12/2008	0.1	Initial draft	Costas Ballas
09/02/2009	0.2	2 <sup>nd</sup> draft version	Costas Ballas
13/02/2009	0.5	3 <sup>rd</sup> draft version	Costas Ballas
19/2/2009	1.0	Final Version	Costas Ballas

## Abbreviations

Agilis	Agilis SA, Greece
EU	European Union
FhG	Fraunhofer Institute for Autonomous Intelligent Systems, Germany
ICCS	Institute of Communication and Computer Systems, Greece
IntraInt	Intrasoft International SA, Belgium
IST	Information Society Technologies
RMH	Royal Marsden NHS Foundation Trust
NHS	National Health Service, England
RBH	Royal Brompton and Harefield NHS Trust
TSAY	Social Security Body of Health Care Professionals, Greece
WP	Work Package
VAT	Value Added Tax
XML	eXtensible Markup Language

## Executive Summary

The purpose of this deliverable is to describe the overall assessment and evaluation from the pilot applications of the iWebCare integrated web services platform. The pilot activities in both sites were important because they provided an opportunity to use the platform with real data in a real environment. In addition, the pilot brought together users and technical partners to work together to solve problems and further develop the platform, as well as identifying useful future developments to improve the functionality, usability, reliability, efficiency and satisfaction with the platform. Both pilot applications were successful because they achieved their key objectives to conduct trials in order to validate the iWebCare service from the viewpoint of end-users.

The report begins in Section 1 by summarising the aims and goals of this phase of the project. Section 2 describes the characteristics of the iWebCare platform which were evaluated and validated during the pilot and which fall into two dimensions:

- the technical dimension, which considered performance and quality, including usability, reliability, efficiency, functionality and user satisfaction, and
- the business dimension, which considered the benefits to the organisation of using the iWebCare platform to detect potential fraud

Section 3 describes the activities which users were required to carry out as part of the pilot in each site and the range of evaluation tools used to gather data and triangulate the results: a user diary, critical incident report, statistical data from the platform and a questionnaire survey together with interviews with key stakeholders.

Section 4 describes how the pilot focused on procurement fraud. It also outlines the data used for the pilot applications for both sites.

The results of both pilots for each of the research tools used are fully explored in Section 5, followed by a summary of the way in which the pilots deviated from the pilot plan.

Section 6 describes the external experts' evaluation reports about the applicability of the iWebCare integrated web services platform to the domains where they have their main expertise.

The report ends with the overall conclusions in Section 7.

## 1. Introduction

The aim of Work Package 7 was to pilot the iWebCare platform and evaluate the results of the project from the user point of view at the two end-user sites – TSAY and RBH/NHS. The present deliverable is the outcome of the Task 7.3 “Evaluation and assessment of project results” where an overall assessment and evaluation of the iWebCare integrated web services platform and of the two pilot applications is provided. Additionally the iWebCare integrated web services platform has been presented to three external experts and their evaluation reports about the applicability of the platform to the domains of their expertise is provided.

This deliverable aims to provide information to:

- The EU’s team of reviewers which will undertake an overall assessment of the iWebCare project
- The iWebCare consortium members as a whole to ensure that all the partners have an understanding of the activities carried out as a result of the pilot and the overall conclusions reached from piloting the platform
- Members of the technical team to ensure that they have an understanding of any technical issues identified as a result of the pilot and recommendations for improvement
- Those users who participated in the project
- Other parties which might be interested in the results of the project

During the pilot, users at both pilot sites (RBH/NHS and TSAY), with the help of the technology integrators and software development team, evaluated the range of services offered by the integrated iWebCare web services platform as well as the functionalities offered by each of the main modules<sup>1</sup> in the context of either procurement and potential conflict of interest or fraud detection on electronic prescriptions.

The main goals of this phase of the project were to:

- use and validate the web services offered by the integrated iWebCare platform
- test out the methods for user authentication and authorization
- create, update and delete rules stored in the rules repository
- upload and submit datasets
- preview the results of the validation process and create meaningful reports
- assess the effectiveness of the self-learning module
- apply rules using the validation engine’s services

---

<sup>1</sup> iWebCare modules:

- iWebCare Web Service module which interfaces with e-gov applications which are responsible for submitting the datasets (eg prescriptions) to be checked for fraud
- Self-learning module which will provide a facility to ‘learn’ from the submission of data sets and creates/updates rules in the rules repository
- Health care ontology module which is responsible for mapping domain concepts with datasets and with variables and rules in the rules repository
- Fraud detection (validation) engine module which will use domain specific rules in order to validate an incoming dataset and produce reports
- Rules repository module which will store available rules and rule sets

- identify different types of users who would need to access and use the iWebCare platform, e.g. to maintain user accounts and rule profiles, to submit data for validation, to view rules and reports identifying potential fraud or to view rules and fraud cases of other agencies to compare with their own.

In the case of TSAY pilot an additional goal was identified since an additional step was required from the users for the proper execution of the workflow. This step included the creation of datasets by converting paper based prescriptions to electronic format.

## 2. Scope and purpose of pilots

### 2.1. Introduction

The overall aim of the iWebCare project is “to design and develop a flexible fraud detection web services platform, which will be able to serve e-government processes of fraud detection and prevention, in order to ensure quality and accuracy and minimise loss of health care funds (iWebCare Technical Annex, 2005).

According to the deliverables D17 and D18, which describe the outcomes of the pilots for RBH/NHS and TSAY respectively, a series of evaluation objectives have been defined against which the iWebCare platform has been evaluated. The evaluation objectives have been categorized in two categories. The first category covers the performance and quality of the iWebCare platform (usability, reliability, efficiency, functionality, satisfaction) whilst the second category covers the business dimensions.

Both pilot evaluation reports have been based on the same sets of evaluation objectives for both categories. This decision makes suitable for this overall evaluation report to conclude the assessment and evaluation of the iWebCare integrated web services platform and of the two pilot applications by comparing the results of the two evaluation reports.

In the following section we present the evaluation objectives as have been presented in the respective evaluation reports for TSAY and RBH/NHS pilot applications.

### 2.2. Evaluation objectives

The pilot evaluated the iWebCare platform in two dimensions: performance and quality (the technical dimension) and the business dimension which focused on the benefits of using the platform for the organization.

#### 2.2.1 Performance and quality (technical dimension)

The following characteristics of the iWebCare platform were evaluated and validated during the pilot:

##### *Usability*

This characteristic refers to ease of use and user-friendliness, ie how easy it is for users to learn how to use the system and remember how to use it, the ability of the platform to be operated easily, intuitively and consistently, the accuracy and completeness with which users achieve specific goals, ease of producing reports, ability to export information into other formats (eg Excel spreadsheets), ease of interpretation of validation results, ability to prioritise results for further investigation (eg by being able to identify high, medium and low risk cases or high, medium and low probability cases). This characteristic also considered the ability of users to control access and ensure security and confidentiality of data held on the platform.

##### *Reliability*

The user should be able to rely on the way the system works and to count on its timeliness and predictability. This characteristic defines the capability of the platform to maintain its service provision, and covers frequency of failure and ability of system to recover and be brought to full operation in case of failure.

#### *Efficiency*

This characteristic is concerned with the system resources used when providing the required functionality, including robustness of the system, response times for a given input and resources used, eg time effort and technical resources, and ease of navigation.

#### *Functionality*

Functionality is a key quality characteristic of the iWebCare platform and represents the totality of essential functions that the service provides, broken down into the following sub-characteristics:

- Relevance, ie validity of the rules used to detect irregularities and errors which may represent fraud, and degree of accuracy of the results obtained
- Suitability, ie appropriateness of the platform functions to the specification which was to:
  - detect fraud by validating the contents of e-documents against a predefined set of rules
  - use data mining to discover both unsuspected relations among variables as well as dissimilarities among patterns that cannot be deduced in a straightforward way from any query to databases in order to detect new types and patterns of fraud (iWebCare, D10)
- Interoperability with legacy systems (manual as well as electronic systems), how the platform fits with existing procedures and processes and what adaptations would be required in order to use the iWebCare platform on an ongoing basis.
- Additional features, eg on-line and off-line support

#### *Satisfaction*

This characteristic is concerned with the user's attitude towards the use of the platform broken down into the following sub-characteristics:

- Overall performance and user satisfaction with overall performance
- Performance of specific functions, ie extent of user's satisfaction for all specific functions
- Willingness of users to use the service

### 2.2.2 Business dimension

This dimension considered the benefits to the organisation of using the iWebCare platform to detect potential fraud and looked at how much potential fraud the platform was able to identify, the worth of the potential fraud and the impact of the platform financially, technologically and organizationally. Feedback gathered from users during the pilot included:

- the effectiveness of the platform in identifying potential fraud
- whether users have identified any additional data which might enhance the usefulness of the platform
- whether the platform is able to deliver benefits such as:
  - improved data flow and information exchange between internal departments

- improved data flow and information exchange with external agencies
- improved inter-agency co-operation
- faster and more efficient operations
- reduced administrative costs to support current processes and improved effectiveness by automating tasks to deal with large volumes of data which would be difficult to process without the use of such systems
- potential barriers and critical success factors to implementing the platform on a wider scale
- what organisations might be prepared to pay for access to the platform and pricing models.

### 3. Pilot methodology

#### 3.1. Introduction

In this section we are going to investigate and compare the pilot methodology that was followed by each pilot application. The methodologies in both cases are composed by the approaches used, the key activities that were carried out during the pilot and the evaluation tools that were used. A comparison of the methodology used in each pilot site will help us to identify any differences on the overall methodology and it will guide us to appropriate structure of this overall evaluation deliverable.

#### 3.2. Approach used

In the following table we summarize the activities required from the users during the pilot period for both pilot sites as documented in the respective deliverables.

<b>RBH/NHS pilot site</b>	<b>TSAY pilot site</b>
<ul style="list-style-type: none"><li>• prepare data for inputting onto the platform</li><li>• convert data to XML format</li><li>• upload and submit datasets</li><li>• test out the methods for user authentication and authorization</li><li>• create, update and delete rules stored in the rules repository and modify rules according to weighting</li><li>• apply rules using the validation engine's services</li><li>• preview the results of the validation process and create meaningful reports</li><li>• use the self learning engine to generate new rules and then ask experts whether these new rules are useful in identifying potential fraud to assess the effectiveness of the self-learning module</li><li>• assess whether or not cases of potential fraud are worth further investigation</li><li>• contribute to the evaluation of the pilot by completing diaries and questionnaires and participating in interviews if required</li></ul>	<ul style="list-style-type: none"><li>• prepare data for inputting onto the platform</li><li>• establish links between platform and other data management systems (eg providing information on doctors' specialties and contact details)</li><li>• convert data to XML format</li><li>• test out the methods for user authentication and authorization</li><li>• create, update and delete rules stored in the rules repository and modify rules according to weighting</li><li>• upload and submit datasets</li><li>• apply rules using the validation engine's services</li><li>• preview the results of the validation process and create meaningful reports</li><li>• use the self learning engine to generate new rules and then ask experts whether these new rules are useful in identifying potential fraud to assess the effectiveness of the self-learning module</li><li>• assess whether or not cases of potential fraud are worth further investigation</li><li>• contribute to the evaluation of the pilot by completing diaries and questionnaires and participating in interviews if required</li></ul>

The previous table indicates that the majority of the activities that took place by the involved users during the pilot period are the same for both pilots with a small difference for the case of TSAY's pilot. TSAY users were required to additionally establish the links between the platform results and their data management systems in order to retrieve additional information regarding the doctors and pharmacists.

### 3.3. Key activities

During the preparation of the pilot plan a sequence of activities were set out in order to ensure the proper execution of the pilots. A summary of the key activities is set out in the table below along with any deviation occurred.

Task	Description	Timescale	Actual Timescale	Reasons for delay (if appropriate)
Platform integration	Integration of platform components/modules	M25-28	M25-28	
Testing of platform	Testing and user acceptance test at RBH and TSAY sites	M26-28	M26-33	Bugs and necessary fixes delayed the release of the final prototype.
Helpdesk	Set up Helpdesk arrangements (and see 4.3 below) and provide ongoing Helpdesk support to ensure the pilot is completed effectively	M27-33	M27-35	Pilot extended to M35 due to delayed launch as well as not clear value of data mining results for the TSAY pilot
Access arrangements	Organise access to platform for users involved in pilot	M28	M28 and M31	During the TSAY pilot the M28 goal was meet but RBH/NHS pilot due to problems with the connectivity to the site the goal was meet in M31.
Fine tuning	Fine tuning and bug fixes	M28-29	M28-35	Fine tuning and bug fixed continued throughout pilot.
Data Preparation	Select an adequate sample of handwritten prescriptions to be digitised and used for the pilot	M28-M29	M28-29 and M35	
Training	Training for pilot users	M29-30	M31	Training delayed due to extension of testing and bug fixes.

Task	Description	Timescale	Actual Timescale	Reasons for delay (if appropriate)
User manual	Development of user instructions		M28-33	User manual revised in light of comments received from users.
D30	Finalise and submit final version of D30	M29	M29	
Launch pilot	Meetings with RBH/NHS and TSAY representatives to launch the pilot phase	M30	M25 and M31-33	Meetings delayed due to initial technical problems with platform.
Pilot	Users pilot the system	M30-33	M31-36	Start of pilot delayed due to extension of testing and bug fixes. A two-phase pilot run took place at TSAY in order to get more useful results and rules from the Data mining module. End of pilot delayed due to late start and introduction of 2nd pilot phase (data mining rules).
Evaluation of pilot results	Collation and analysis of results of pilot	M31-33		
D17/D18	Preparation and submission of reports on pilot application at RBH/NHS (D17) and TSAY (D18)	M31-33	M34-36	Delayed due to delay in carrying out pilot activities.
D19	Consolidation of reports – evaluation and assessment	M33-34	M34-36	Delayed due to delay in carrying out pilot activities.
Dissemination	Workshop to share results of pilot with user organisations	M35	M37-M38	Dissemination event delayed until results of pilot available.

### 3.4. Evaluation tools

During the pilot preparation a range of evaluation tools were specified for both pilot applications. The set of the evaluation tools included a user diary, critical incident report, statistical data from the iWebCare platform itself, a questionnaire survey and interviews with key personnel. These evaluation tools used to gather data during both pilot applications. The user diary and critical incident report were structured in such a way as to provide data on

specific areas of the iWebCare platform that needed improvement. These results were immediately reported back to partners involved in the technical design and implementation, so that the iWebCare platform could be modified and improved on an ongoing basis throughout the pilot.

1. User diary and critical incident report

A user diary and critical incident report was provided for users. Each user was required to complete an entry every time they accessed the platform in order to provide a record of usage and a record of how well the platform performed and to help users when they completed the end of pilot questionnaire. The user diary included a critical incident report to be filled in every time they encountered a problem or 'technical bug' when accessing and using the platform in order to provide detailed information on what the fault was, who the problem was escalated to for resolution and how the fault was resolved. The data gathered through use of this research instrument provided information for the evaluation of the technical dimensions of the platform.

2. Critical incident report

A critical incident report was also used by members of RBH/NHS, TSAY and Agilis who were dealing with technical issues/problems encountered either when setting up access to the platform or those reported by users. This research instrument provided information for the evaluation of the technical dimensions of the platform.

3. Statistical data

Statistical data from the iWebCare platform was produced by Agilis to provide information on usage levels and platform performance. These results provided data for the evaluation of the technical dimensions of the platform.

4. Questionnaire survey

Based on the evaluation characteristics defined in Section 2, a pilot questionnaire was prepared to be completed by users to measure the level of the selected evaluation characteristics and to test out some of the business dimensions of the platform and questions raised in the technology implementation plan (iWebCare, D23).

In order to test reliability, usability, efficiency and satisfaction, the questionnaire included a section asking respondents to specify their level of agreement to a range of questions using a five-point likert scale. A range of additional questions were also included to obtain more qualitative information on these characteristics and to explore issues relating to data security and the potential impact of the platform in identifying fraud as well as some of the issues to be covered in the technical implementation plan, such as pricing models.

5. Interviews

The findings from the pilot were further explored through open interviews with users involved in the pilot activities and a small number of experts in the field of finance, audit and counter fraud. The interviews were designed to explore in depth some of the findings from the questionnaire survey and to provide further validation of the findings from the pilot.

## 4. Pilot context

### 4.1. Introduction

In the pilot context section we are going to compare both pilots' contexts as presented in the D17 and D18 deliverables. More particular the context of each pilot can be divided on information regarding the data that was used during the pilots, the description of fraud that was identified with the use of the iWebCare platform and the description of the users involved. The pilot at RBH/NHS user site validated the services of the integrated iWebCare platform in the context of procurement and potential conflict of interest while the pilot at TSAY user site validated the services of the integrated iWebCare platform in the context of potential fraud in medical prescriptions.

### 4.2. Data used for pilot

The data that was collected and used for both pilot applications were specified in the iWebCare D01 deliverable while a full description of the data set can be found in iWebCare D05 deliverable.

In more detail for the RBH/NHS pilot site the data used in the iWebCare platform was extracted from two systems:

- Payroll systems (including employee name, surname, address, date started in employment, date left, number of hours worked) (between 2,000 and 5,000 staff members per Trust)
- Finance systems – creditors' payment history and standing data (including creditor name, address, VAT registration number, invoice numbers, invoice dates, payment amounts) (up to 35,000 creditors per Trust)

For the TSAY pilot application the data used consisted by:

- 60.000 e-prescriptions (including Prescription ID, Insured Person ID, Membership type, Sex, Diagnosis Code, Year of birth, Various Costs, Dates (Issuance, Dispensing), Doctor ID, Pharmacy ID, Drug Details), from years 2005-06
- 700 hand-written prescriptions that were converted to the electronic format (XML language) used by the platform.

In both cases two different dataset converters were implemented in order to transform the initial data source to a format acceptable by the platform. The large numbers of data sources used for the pilots demonstrates the scalability of the platform which indicates its ability to handle growing amounts of work in a graceful manner.

The privacy issues concerning the confidential data included in the datasets were handled by the platform in a respectful way. The access to the platform was restricted and only authenticated users was able to access it. A complete user management system was integrated to the platform from which user privileges for access was managed. Moreover any data provided to the platform was automatically encoded before storage in the platform in order to ensure any misuse of data stored in the platform's database.

### **4.3. Description of fraud to be identified by iWebCare platform**

The architecture of the platform from the early stages was designed with extensibility as a baseline. The different modules and the interfaces connecting them provide the possibility to use the platform for the identification of different type of fraud. An initial aspect of the extensibility properties of the platform was shown in the previous section (4.2) where different types of data can be submitted to the platform. In this section the description of fraud that the platform identifies for each pilot case confirms the extensibility properties of the platform.

More specific for the RBH/NHS pilot case the iWebCare platform was used to identify three types of potential fraud. Two types of fraud relating to procurement and one relating to payroll:

- fraud specifically relating to conflict of interest (failure to disclose inappropriate relationships between an employee and a creditor), for example an employee shares the same address as the creditor and may be involved in price fixing and cartels
- fraud carried out by creditors not relating to conflict of interest (external false representation), for example if the supplier is using an invalid VAT number
- potential payroll fraud (misappropriation of funds) (eg an employee is fraudulently working for one organisation while on paid leave from another).

The TSAY pilot case focused in different types of fraud than the above mentioned. The two types of potential fraud that the iWebCare platform tried to identify was:

- Auditorial fraud cases. In this case rules try to detect incomplete prescriptions and invalid or miscalculated data.
- Medical fraud cases. In this case rules try to detect prescriptions in which the data are inconsistent from a medical point of view. It turned out that the medical rules are very difficult to be expressed and validated in a scientifically accepted manner, mainly because of lack of available codifications and taxonomies that should be used in an e-prescription system. As TSAY does not have such a system (work is done with paper based prescriptions) it was almost impossible to validate the use of such rules.

The different types of fraud that the iWebCare platform was able to identify (except the medical fraud cases from TSAY for the reasons explained previously) highlighted the capabilities and potentials of the platform to provide flexible fraud detection services, not only to ensure quality, accuracy and minimise of loss in health care funds but to serve a variety of e-government processes for fraud detection and prevention.

### **4.4. Description of users involved in pilot**

The pilot application of the iWebCare platform was supported by 12 users from both RBH/NHS and TSAY. These users executed in the required activities, submitted the questionnaires, the user diaries and the critical incident reports. During the RBH/NHS pilot seven users participated in the pilot activities as follows:

<b>RBH/NHS Trust</b>	<b>Number of users</b>	<b>Role</b>
RBH, RMH, Mayday and E&StH	2	Counter fraud and security
RBH	3	Members of project team and Procurement representative from Finance Department
RMH	2	Finance and procurement

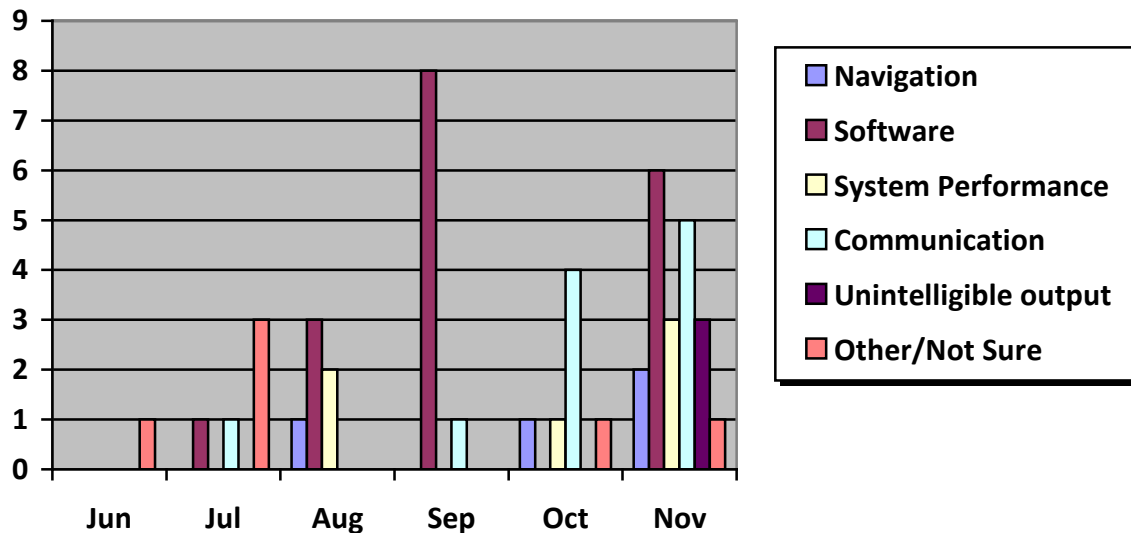
For the TSAY pilot five users participated in the pilot activities as follows:

<b>Specialty</b>	<b>Number of users</b>	<b>Role</b>
IT systems	1	Administer the technical perspective of the pilot and provide help for simple issues to TSAY users
Doctor	1	Counsel Prescriptions Auditing personnel and evaluate results of data mining
Pharmacist	1	Counsel Prescriptions Auditing personnel and evaluate results of data mining
Prescriptions Auditing	2	Select, evaluate and enter data of hand-written prescriptions, evaluate results of data mining

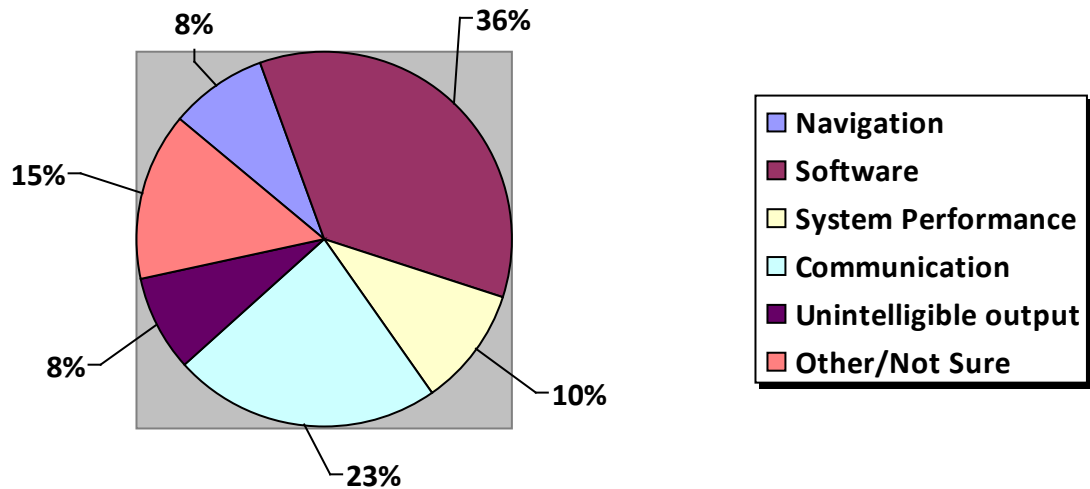
## 5. Results

### 5.1. Analysis of findings from user diaries and critical incident reports

The data gathered from the user diaries and critical incident reports provided information on the technical dimension only. A detailed summary of usage and of critical incidents which occurred during each pilot application can be found in the deliverables D17 and D18. The platform was accessed in total 50 occasions between 18 June and 15 December 2008 and 32 critical event logs were submitted. In each critical event log one or more problems regarding the platform was submitted to the technical partners.



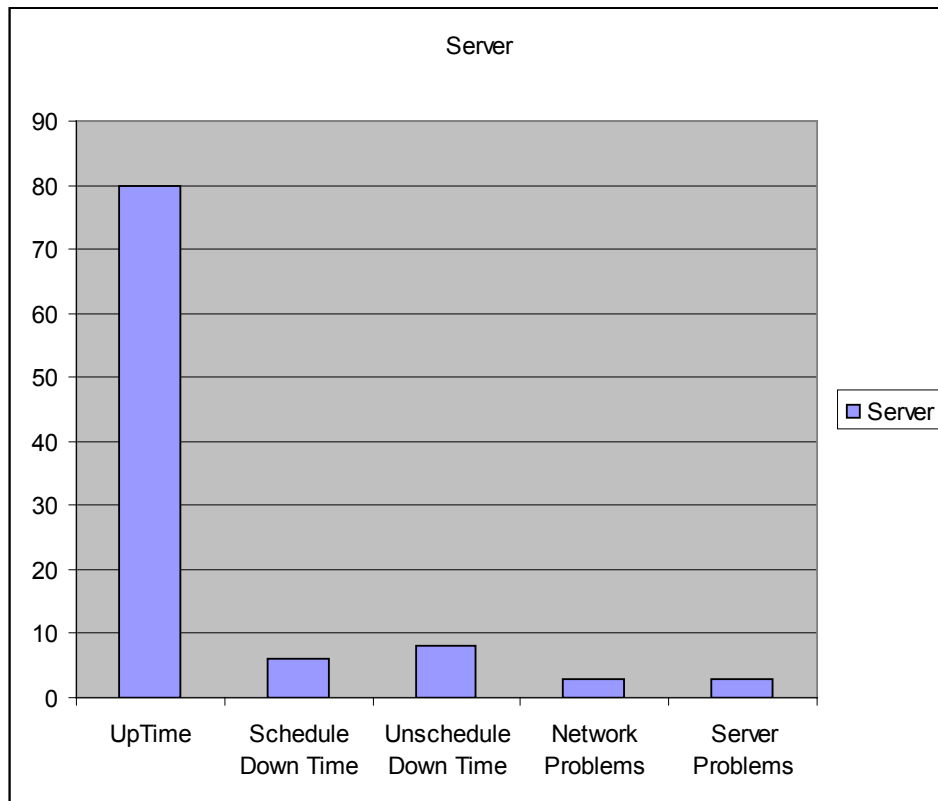
The majority of the faults reported (36%) related to software problems. 23% of faults reported related to communication problems (eg difficulties in accessing the platform). Only 10% of faults related to system performance, 8% to unintelligible output and 8% to problems with navigating around the platform. 15% of faults identified were difficult to categorize to any of the above categories.



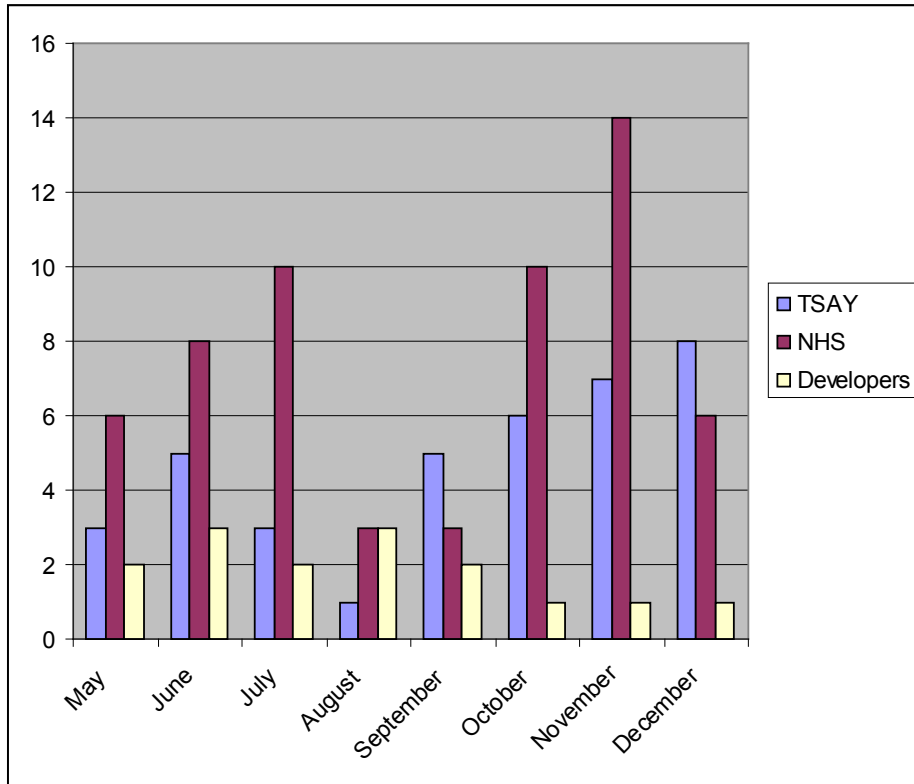
Type of fault		Number of times fault reported	% of total
1	Navigation (moving around platform between modules)	4	8%
2	Software (eg problems uploading or extracting data)	17	36%
3	System performance (eg very slow or platform crashing)	5	10%
4	Communication (eg problems with accessing platform)	11	23%
5	Unintelligible output (eg user is able to use platform and view output but does not understand meaning of results, eg complex rules in rule language or with additional output from self learning engine)	4	8%
6	Other/Not sure	7	15%
TOTAL		48	100%

## 5.2. Analysis of findings from statistical data generated from iWebCare platform

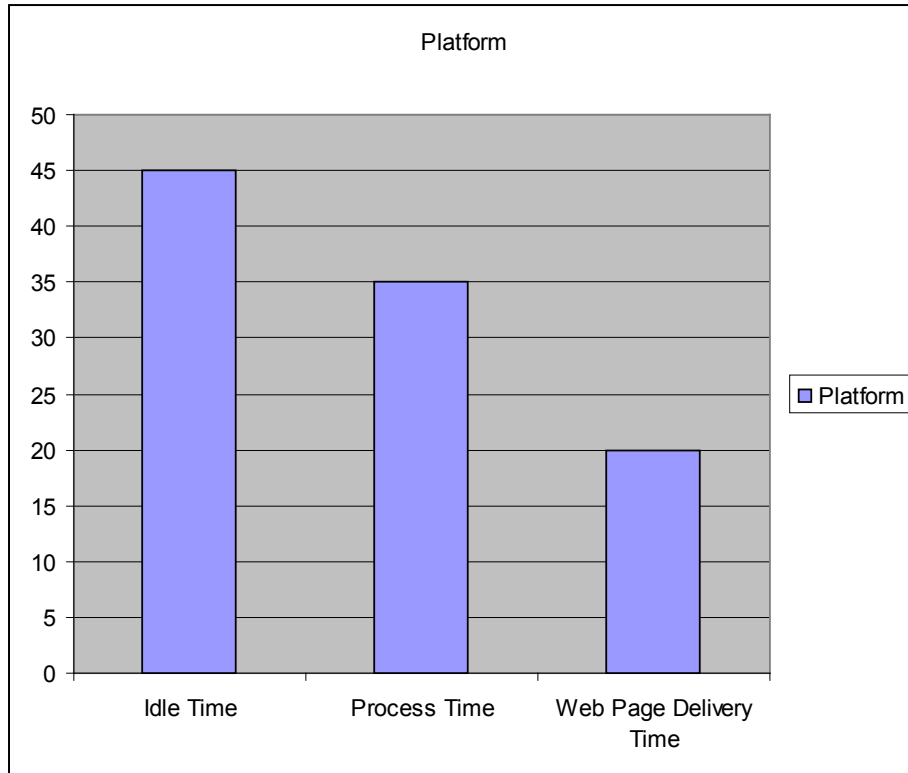
Data on frequency of use, purpose of use and errors which occurred when using the platform was provided by Agilis and is summarized below. This information covers usage during both RBH/NHS and TSAY pilot applications. Based on this information, we can see that the server was performing well 80% of the time, with only 14% downtime (from which 6% was scheduled and the remaining 6% of the time facing network and other server problems).



With regards to usage of the platform by TSAY, RBH/NHS and the developers, we can observe that RBH/NHS used the platform more often and for more hours during the May to December period. The maximum usage for RBH/NHS was in November (14 hours) and the minimum in August and September (3 hours). The corresponding figures for TSAY are 8 hours on December and 1 hour in August, while as would be expected, the Developers made the maximum usage of the platform in June and August with 3 hours and the minimum on October, November, December (1 hour).



Finally, the statistical data shows that the platform was idle for 45% of the time, 35% was taken up with Process Time and the remaining 20% was taken up with Web Page Delivery Time.

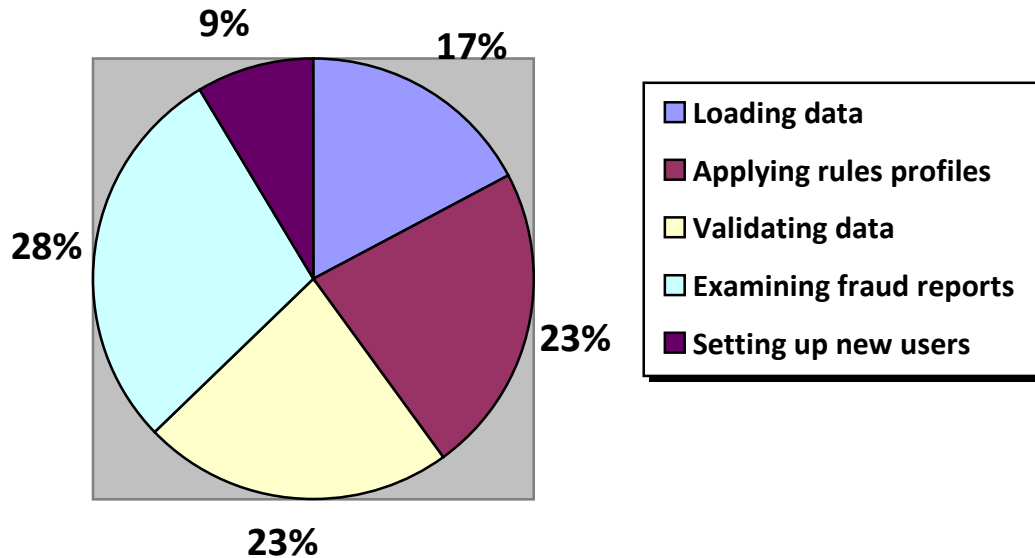


### 5.3. Analysis of findings from questionnaire survey

#### 5.3.1 Performance and quality (technical dimensions)

When asked to comment on the types of activities which the platform was used for the following responses were received:

- Loading data (6)
- Applying rules profiles (8)
- Validating data (8)
- Examining fraud reports (10)
- Setting up new users (3)



### Usability

- 90% of the respondents found it very easy to learn to move from one part of a task to another, 73% found that they got what they expected when they clicked on various parts of the website and that the organization of the menus or information lists seemed quite logical and 81% found that they could easily locate what they want on the site. Only 8% indicated that there are too many steps required in order to get something to work.
- 81% of responses reported that tasks were able to be performed in a straightforward manner and 73% of the responses reported that the site helped them to find what they were looking for. Only 10% of the respondents had problems to remember in which step of the procedure and the respectively page on the site they are.
- 81% of the respondents found that the organization of the menus or information lists seem quite logical.
- 81% of respondents found that the use of the platform will result in an improved data flow and information exchange between internal departments and 73% with external agencies.
- 100% of responses found it easy to apply rules, validate data and produce reports and 90% found it easy to manage the user accounts.
- Finally 62% of the respondents believe that the use of the platform on a regular basis would reduce administrative costs to support current processes and improved effectiveness by automating tasks to deal with large volumes of data which would be difficult to process without the use of such systems.

By the statistics analysis is clear the positive approach of the iWebCare platform from the users. The positive approach was also verified by the answers to the question about what they liked most about the platform. In RBH/NHS pilot the users responded that they liked the most the easy and quick way to validate data and the easy and quick way to produce reports. At the same time the users in TSAY we accepted the

platform because they understand that the services provided could replace the manual, until now, procedure for identifying potential fraud cases.

However a high proportion of responses (73%) also commented that the web site needed more introductory explanations and that they did not find that the help information given on the platform is very useful. Only 27% of responses confirmed that they found the instructions and prompts helpful, with 27% of responses commenting that they way that system information is presented is clear and understandable and only 19% confirming that they find everyone on the website easy to understand.

In both pilot sites the users were not involved in the editing of the rules since, as the technical team agreed, since a higher level of technical skills person was required for this activity. This is because the rules are expressed in a script format that the pilot users were not familiar with and it would be difficult for them to understand the format of the scripts. Due to this fact there were no responses whether users had any comments about the rules repository and use of the rules to validate data.

Differences between the two pilots were observed on the responses regarding the data protection and data confidentiality issues. The users in TSAY pilot had no concerns about data protection and data confidentiality issues, since the platform uses only ID's and not the real names of patients, doctors and pharmacies. In order to link an ID with a name further access to the data management system of the organization was needed. The users in RBH/NHS pilot had clearly pointed out their concerns by responding in the question whether users had encountered any issues relating to access and/or security, with the following answers:

- I am concerned about data protection aspects
- I have major concerns about data confidentiality, particularly the payroll data
- I am worried about the fact that the project team may have access to this data
- We had to write to all staff to advise them we were using their data

In answer to a question about what other information users would have liked to have seen on the platform, the responses in both cases were twofold. The first aspect that the users would like to get more information was the instructions about how to use and move around the platform, while the second aspect was focused upon additional information that currently can be found on their information systems and they feel that if the iWebCare platform could include this information it would make its use more productive. For example for RBH/NHS pilot users would like to see:

- Directors' names and addresses from Companies House
- Links on payroll to maiden names and partner family names

TSAY users requested:

- Data about the specialty of the Physician who wrote the prescription
- Information about the drugs prescribed and how they relate to the prescription's diagnosis

The two main problems identified by the users during the pilot period. RBH/NHS users pointed out the difficulty they encountered during the conversion and uploading of the data to the platform. They found very time consuming the splitting of their data to smaller pieces in order to be able to be uploaded to the iWebCare platform. TSAY users were not so satisfied with the results of the self learning module. During the

several meetings for the enhancement of the self learning module it was clarified that the users expected more than statistical rules from the data mining procedure.

The following responses were received to a question about what users liked the least about the platform:

- Need to split data into smaller subsets (7)
- Not enough information on what the reports mean (5)
- Don't understand how to create new rules/Seems difficult to create new rules (3)
- Not sure how to add other types of data (1)
- Not clear what data is being validated when you press validation button (1)
- Difficult to create new rules profile (1)

### *Reliability*

Regarding the reliability of the platform in total for both pilot 33% of the users reported that the platform had at some time stopped or crashed unexpectedly but no one reported any problems in restarting the platform if it had stopped/crashed. There were some periods when the platform was not available for maintenance reasons as stated in the section regarding statistical data generated from iWebCare platform, but in every case they had a short notice for that.

### *Efficiency*

The results collected by the questionnaires regarding the efficiency of the platform was confusing since for the RBH/NHS pilot a high proportion of the users (86%) found the website too slow, and suggested that they would not like to use this software every day whilst none of the TSAY users had the same belief. An explanation for these results can be given since the RBH/NHS users had to upload larger datasets to the platform than the TSAY users. Moreover the same web server that was used for both pilots was located in Greece, maximizing the network bandwidth requirements for RBH/NHS pilot.

### *Functionality*

- 81% of responses confirmed that the rules were helpful in helping to identify potential fraud
- 62% of responses suggested that use of the platform on a regular basis would reduce administrative costs to support current processes and improved effectiveness by automating tasks to deal with large volumes of data which would be difficult to process without the use of such systems
- The majority of responses appeared to be satisfied with the training and Helpdesk support, with only 17% having to look for assistance most of the time when they used the software, and 83% commenting that if they had a problem, the Helpdesk support team dealt with it promptly and efficiently
- There did, however, appear to be a problem with the reports, with just 29% confirming that reports were well structured, that they provided the information they required and 50% that use of the platform would result in faster and more efficient operations.

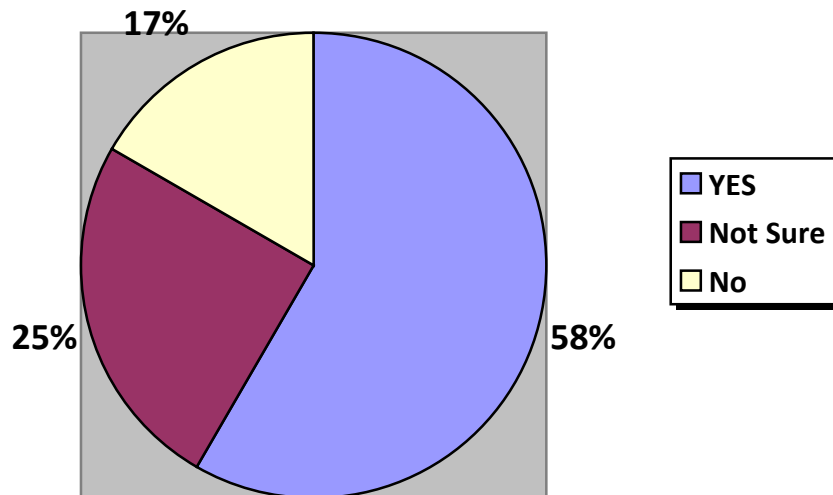
- None of the responses confirmed that the reports were easy to download into other software, eg Microsoft Excel, in order to reformat the reports and add information as required, as this facility was not available when they piloted the platform.

In answer to a question about how often they would use this service if it was available to them in the future, the users responded that with some additional modifications, like an easy way to create rules and the use of an enhanced data set, they could use the platform periodically for fraud detection.

In answer to a question about critical success factors to support implementation of the platform, the RBH/NHS respondents suggested that there should be a “training module with test data and information on how to interpret results”, and the TSAY respondents suggested that the “Civil service bureaucracy” factor could be a problem and suggested “Certain improvements on the platform”. Finally the integration of the platform with existing systems in order to feed the iWebCare platform with data, and thus sidestepping the digitization/conversion and upload procedures, would be an important factor for the success of the platform.

*Satisfaction*

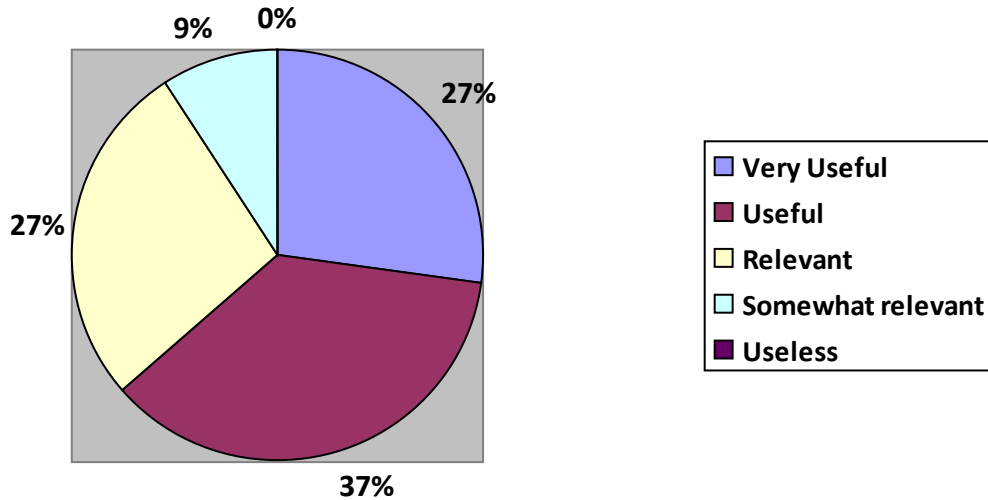
- No respondents felt that using the website was a waste of time and 56% of responses commented that the website had much that was of interest to them. Only 38% of responses suggested that it was difficult to tell if the website had what they wanted and that the website had some annoying features.
- However only 38% of responses appeared to enjoy using the website, felt efficient when using the website and 27% found the pages of the website very attractive
- 58% of respondents confirmed that they would recommend the platform to their colleagues, 25% were not sure and only 17% gave a negative response.



- Examples of colleagues included:
  - Counter fraud team (7)
  - Procurement department (2)

- Finance department (2)
- Anyone in public or private sector (1)

The responses regarding the quality of the information provided by the platform the 64% of responses found the information provided 'useful' or 'very useful'. A further 27% found the information 'relevant'. Only 9% found the platform 'somewhat relevant' and no users found the platform 'useless'.



### 5.3.2 Business dimension

Reports produced from the iWebCare identified the following cases of potential fraud for each pilot:

<b>RBH/NHS pilot application</b>		
	<b>RBH</b>	<b>RMH</b>
Multiple national insurance numbers (ie more than one employee having the same n.i. number)	13	11
Employees with invalid national insurance number	12	11
Employees working in more than one Trust	0	11
Suppliers with invalid VAT numbers	All*	All*
Potential conflict of interest (employee and supplier have same address):		
• Includes names of individuals (NB could be expense claims for employees)	4	41
• Company names only	0	0
Potential conflict of interest (employee and supplier have same postcode)		
• Includes names of individuals (NB could be expense claims for employees)	62	107
• Company names only	5	5
Results from self learning module for one sub group of data only which are worthy of further investigation	1	0

\*Error in report is bringing up all suppliers with invalid VAT number

<b>TSAY pilot application</b>	
<b>Rule</b>	<b>No of Cases</b>
Violation of the 5-day execution period	48
Prescription issuance date should not overlap execution date	35
The prescribed drugs are overpriced	126
Too high treatment cost	95

All the respondents in both pilot applications confirmed that the platform had helped identify potential fraud. The majority of the of responders (81%) felt that use of the platform would result in improved data flow and information exchange between internal departments, a slightly lower proportion (73%) felt that use of the platform would result in improved data flow and information exchange with external agencies and only 48% suggested that use of the platform would result in improved inter-agency co-operation

The responses given to the question about how much their service might be willing to pay for the service pointed out different payment schemes. From the TSAY users a scalable value was provided which is associated with the presences of the improvements on the certain issues that rose during the pilot. An estimation of was provided as below:

- Up to 20.000€ if certain improvements were made (50%)
- Up to 25.000€ if certain improvements were made (25%)
- Up to 30.000€ if certain improvements were made (25%)

RBH/NHS users provided a variety of possible payments schemas like:

- % of non pay spend
- £5,000 for service, ie annual fee
- £20,000 on off fee plus ongoing support
- Flat fee for service is preferred payment model -with service provider uploading data and doing reports
- Fee per transaction would be too costly
- Fee per value of fraud detected could result in problems

The general remark regarding the service payment was that the users were really interested in the iWebCare platform and they were willing to accept it in their business if a certain amount of improvements were made.

#### **5.4. Deviations from planned and actual pilot**

Four was the major deviations between the planned and the actual pilot application:

- The pilot did not require users to test out the facility to modify rules or develop new rules as it was agreed that users did not have the technical knowledge and skills to be able to write the appropriate script language.

- The pilot did not require users to operate the self learning engine due to the complexity and length of time. Instead, users/experts were asked whether the results produced by the self learning module were useful in generating potential fraud.
- The platform did not offer the facility to download reports into other software, eg Excel, in order to reformat the reports and add information as required
- The pilot activities time plan was changed in both pilot sites due to different reasons:
  - The RBH/NHS pilot was delayed due to improvements on the platform regarding the reporting module. Also the changing priorities of RBH/NHS Trusts and changes in staffing contributed to problems in maintaining the commitment of Trusts to be involved in the project, particularly during the pilot phase. In detail, one key project champion working in the counter fraud service at RBH moved on to a new job outside the Trust towards the end of the second year of the project, and from this time onwards it was difficult to get a high level of input and feedback on the pilot.
  - The TSAY pilot was expanded due to problems encountered during the evaluation results for the data mining procedure by TSAY experts, who were not sure about their effectiveness in identifying potential fraud in the results of the self learning module. After several technical meetings and discussions with the data mining team (FhG), a second run of the procedure was decided. On the second run of the procedure, FhG encapsulated the suggestion of TSAY experts by adding the following experiments:
    - Searches for doctors who prescribe expensive drugs for a specific diagnosis.
    - Searches for the doctors who make lots of expensive prescriptions bought in a certain pharmacy.
    - Searches for elderly people with a high number of different diagnosis.
    - Searches for combinations of diagnosis and age having a high total cost.
    - Searches for combinations of diagnosis and sex having a high total cost.

Finally the change of TSAY's legal status was another cause that introduced delays during the pilot.

## 6. External Experts Evaluation Report

During the pilot application of the iWebCare services in RBH/NHS and TSAY as separate parallel activity took place. The consortium approached external experts from other (not healthcare) business areas related to public authorities and e-government, informed them about the iWebCare project, provided the necessary material for review, demonstrated the iWebCare platform and requested an evaluation report on their behalf regarding the applicability of the iWebCare platform to the domains of their expertise.

The experts participated in this evaluation were:

- Heinz Münzenberger, Dipl. Inform
- Alexander Berler, Electrical & Biomedical Engineer, MSC
- European Technology and Innovation Ltd.

Two evaluation reports were collected from this procedure. In the first report the first two external experts worked together in this evaluation and in their report they presented six different preliminary scenarios of anti-fraud systems which will prevent frauds in eProcurement, Registrar's offices, Public Transportation, Revenue Authorities, Customs Authorities and Insurances. All scenarios were reviewed and discussed between the two experts. Thought Mr. Berler was responsible for the eProcurement, Registrar's offices, Revenue Authorities and Customs Authorities sections, while Mr. Münzenberger was responsible for the Public Transportation and Insurances sections.

Each scenario description is structured as follows:

- Fraud(s) encountered in the specific domain
- Solution description
- Requirements
- Examples of Auditing Rules that could be applied

The second report was composed by European Technology and Innovation Ltd, a company located in London, UK which is active in innovation consulting in both private and public owned institutions. The areas at which it has a specific expertise include:

- e-Health applications
- e-Government systems
- e-Commerce

In this report ETI Ltd. was focused on the applicability of the iWebCare platform in the domain of custom offices. Both evaluation reports along with the curriculum vitas of the involved experts of the first report and the company profile for the second report can be found in the Annex.

All experts agreed that the platform has the potentials to be used in other domains. They found that the architecture and the technologies used for the iWebCare platform could easily support the needed modifications in order for the system to be efficient in the other domains. Specific modifications suggested in both reports include the modification on the ontology module in order to support the respective ontologies from the other domains and on the rule

repository in order to be populated with the respective rules. Moreover comments were made regarding the user interface were small modifications could make it more user friendly. Finally comments were provided regarding the self learning module. Experts found interesting the approach of data mining for the enhancement of the rule repository but also stated their concerns regarding the efficiency of the rules generated.

## 7. Overall Conclusions

The pilot applications were important because they provided an opportunity to use the platform with real data in a real environment. In addition, the pilot brought together users and technical partners to work together to solve problems and further develop the platform, as well as identifying useful future developments to improve the functionality, usability, reliability, efficiency and satisfaction with the platform.

The pilot was successful overall because it achieved its key objectives to conduct trials in order to validate the iWebCare service from the viewpoint of end-users. Users found the platform easy to use and the platform identified cases of potential fraud. The results of the self learning module were also welcomed.

Among the full set of positives impressions, the users highlighted the usability of the platform for the identification of cases of potential fraud, the expected improvements in the data flow and information exchange between either internal departments or external agencies and the useful information provided by the platform.

Additionally the users highlighted their belief that the use of the platform on a regular basis would reduce administrative costs to support current processes and improved effectiveness by automating tasks to deal with large volumes of data which would be difficult to process without the use of the platform. Their belief was confirmed with their willing to recommend the platform to their colleagues.

The positive attitude of the users was also confirmed by the group of the external experts who verified in a large scale the positive comments of the users. Moreover additional positive comments were collected by the experts regarding the architecture and technologies used from the platform. The design of the system and the selected technologies make the platform easily configurable in order to be applied in other domains than the healthcare domain.

Although potential fraud has been identified through use of the iWebCare platform, further investigation is required from the fraud experts before fraud can be confirmed. Apart from the positive comments collected during this pilot application the users and the experts identified useful future developments that could help and enhance the platform in many aspects:

- Upgrading the interoperability properties of the platform in order to access the current operating data management systems could minimize the complexity for the end users for preparing and uploading the data while the currently generated reports could be linked to more information that could be very useful to the end user for the judgement of each case separately.
- Providing a more attractive way to represent the auditing rules could help the end users to easily experiment with the creation and editing of the rules and would help on the population of the rule repository with more rules that could maximize the expected results.
- Considerations have been also stated regarding the functionality of the self learning module. Every person involved in the evaluation of the platform welcomed the results of the self learning module but each one had his concerns about the effectiveness of the module. TSAY's expectations, in particular, seemed to be higher than could be archived during the first run of the procedure. TSAY experts were not sure that the

outcome of the first run of the self learning module would help in identifying potential fraud. Thus, as described in the respective deliverable, a second run of the procedure was carried out, producing a set of rules that TSAY experts judged as useful.

The overall evaluation and assessment of the iWebCare integrated web services platform have shown us that the platform is a very useful platform for detecting and fighting frauds not only for the healthcare domain but for any government and business domain.

## **8. Annex**

In the following sections the evaluation reports from the established group of experts are presented.

# iWebCare

**Possible use of the platform in OTHER (not healthcare) business areas related to public authorities and e-government**

## Authors

**Heinz Münzenberger, Dipl. Inform  
Alexander Berler, Electrical & Biomedical Engineer, MSC**

**December 2008**

## Table of Contents

1. Curriculum Vitae .....	38
2. Introduction.....	52
3. Governmental Procurement Procedures.....	53
3.1. Possible frauds .....	55
3.2. Requirements .....	57
3.3. Auditing Rules.....	58
4. Civil Registration.....	59
4.1. Possible frauds .....	60
4.2. Requirements .....	64
4.3. (Examples of) Auditing Rules .....	64
5. Public Transportation.....	65
5.1. Possible Frauds .....	68
5.2. Employees payment fraud .....	68
5.3. Requirements .....	68
5.4. (Examples of) Auditing Rules.....	68
6. eTicketing frauds .....	70
6.1. Requirements .....	70
6.2. (Examples of) Auditing Rules.....	71
7. Revenue authorities.....	72
7.1. Fraud .....	74
7.2. Solution description.....	74
7.3. Requirements .....	74
7.4. (Examples of) Auditing Rules.....	75
7.5. (Examples of) Additional rules for companies .....	76
8. Customs .....	76
8.1. Fraud .....	77
8.2. Solution description.....	78
8.3. Requirements .....	78
8.4. Auditing Rules.....	78
9. Insurances.....	79
9.1. Fraud .....	81
9.2. Solution description.....	81
9.3. Requirements .....	81
9.4. (Examples of) Auditing Rules.....	81
10. Review.....	83
11. Bibliography.....	88

## 1. Curriculum Vitae

### Alexander Berler

1. **Family name:** BERLER
2. **First names:** ALEXANDER
3. **Date of birth:** 6 NOVEMBER 1969
4. **Nationality:** GREEK
5. **Civil status:** MARRIED
6. **Education:**

Institution [ Date from - Date to ]	Degree(s) or Diploma(s) obtained:
present	<b>PhD</b> Candidate in Biomedical Engineering (BME) at the Joint Postgraduate Course on BME of the National Technical University of Athens (schools of electrical and mechanical engineering) and the Medical School of the University of Patras
1995-1997	<b>MSc</b> in Biomedical Engineering at the Joint Postgraduate Course on BME of the National Technical University of Athens (schools of electrical and mechanical engineering) and the Medical School of the University of Patras (score 8,89 out of 10)
1989-1995	<b>MSc</b> in Electrical Engineering at the Polytechnic School of the Aristotle University of Thessalonica, Greece (score of 7,20 out of 10)
1978-1987	<b>Baccalauréat</b> at the Hellenic- French School of Agia-Paraskevi (joint programme of the Hellenic and French Governments)

7. **Language skills:** Indicate competence on a scale of 1 to 5 (1 - excellent; 5 - basic)

Language	Reading	Speaking	Writing
FRENCH (Baccalauréat)	1	1	1
ENGLISH	1	1	1
SPANISH	3	4	4
ITALIAN (Diploma)	3	4	4

**8. Membership of professional bodies:**

- Member of PMI – Project Management Institute since 2006
- Member of HIMSS – Healthcare Information Management Systems Society since 2006
- Member of the Board of Directors of the Greek affiliate of HL7, "HL7 Hellas" since September 2003, Founding member of the Greek HL7 Affiliate
- Member of IEEE Computer and Engineering in Medicine and Biology Societies since 1998
- Member of ESEM - European Society on Engineering in Medicine since 1998
- Member of ACM (Association for Computer Machinery) since 1998
- Member of Hellenic Hospital Association since 1998
- Member of the Pan-Hellenic Association of Electrical and Mechanical Engineers since 1995
- Member of Technical Chamber of Greece (T.E.E.) since 28/06/1995
- Member of Greek Society of Biomedical Engineering (ELEBIT) since 1996

**9. Other skills:** (e.g. Computer literacy, etc.)

**Seminars:**

2006 «The PMI's Science of Project Management & the PMP Exam» - PMI

2003: «The Art of project management in IT/IS Projects»  
Hellenic – American Union

2000: «Anti-Hacking Training and Security solutions»,  
INTERFACE SA

**Computer Literacy:**

- MS Word, Excel, PowerPoint Access, Project, Outlook, Visio
- Data modeling (Rational Rose, UML)
- Database management, SQL, XML, SOA
- Programming in C++, Delphi, Visual Basic

**Teaching Experience**

1996 - Present: Lectures on Project Management, Healthcare Information Systems, Interoperability Standards in the Healthcare domain, Telemedicine, Computer Patient Records, on behalf of the National Technical University of Athens and HL7 Hellas in Greek Public Hospitals in Athens, Thessaloniki and other regions of Greece.

**10. Present position: GNOMON INFORMATICS SA**

**11. Years within the firm: >2 YEARS (from September 2006)**

**12. Key qualifications:** (Relevant to the project)

10 YEARS EXPERIENCE AND EXPERTISE IN THE EGOVERNMENT SECTORS (SYSTEM MODELLING, BUSINESS ANALYSIS)

PROJECT MANAGEMENT

DATA MODELLING – BUSINESS MODELLING

INTEROPERABILITY INFORMATION SYSTEMS

USER REQUIREMENT ANALYSIS

EU FUNDED PROGRAMME UNDER THE 4<sup>th</sup> CSF: DIGITAL CONVERGENCE PROGRAMME (2007 – 2013), USER REQUIREMENTS, IMPLEMENTATION STRATEGY, SYSTEM MODELLING, PROGRAMME MANAGEMENT

EU FUNDED PROGRAMME UNDER THE 3<sup>RD</sup> CSF: INFORMATION SOCIETY PROGRAMME (2000 – 2006), USER REQUIREMENTS, IMPLEMENTATION STRATEGY, SYSTEM MODELLING, PROGRAMME MANAGEMENT

MANAGEMENT OF EU FUNDED RESEARCH PROGRAMMES:

- TOPCARE (IST-2000-25068) – 2002
- VITAL-HOME (EU-ISIS/SPRITE-S2 -1999-2000
- EMERGENCY 112 (EU-TELEMATICS -1998-2000
- THESIS (EU-ESPRIT) - 1997- 1999
- AMBULANCE (EU-TELEMATICS) - 1997-1998
- RISE (EU-TIDE) - 1997

- *BIOTECHNET II (EKBAN 153) -1996- 1997*

### 13. Professional experience

Date from - Date to	Location	Company	Position	Description
May 2006 - present	Athens Greece	Free Lancer	eGOv Expert	Responsible for IT Consulting services and the implementation of complex IT project in the eGovernment sector Responsible or member of project teams in: <ul style="list-style-type: none"> <li>• E-learning project and information portal of the Greek Pedagogical institute</li> <li>• E-learning platform design for the School of Employee of the Greek Ministry of Finance</li> <li>• Design and functional specifications of the National Registrar Office in Greece</li> <li>• Design and implementation of an e-procurement platform for the 4<sup>th</sup> regional healthcare authority of Macedonia-Thrace</li> <li>• Greek Ehealth status report</li> </ul>

May 2006 - present	Athens Greece	GNOMON INFORMATICS	Head of IT Consulting Services	Responsible for delivering IT Consulting Services and Technical Assistance (Project Director) in various business sectors including egovernment, eprocurement, academic education, healthcare, social security and insurance industry. Responsible in projects for the: <ul style="list-style-type: none"> <li>○ University of Patras</li> <li>○ University of Pireaus</li> <li>○ Ministry of Transport</li> <li>○ Ministry of Finance</li> <li>○ Ministry of Interior</li> <li>○ Ministry of Defence</li> <li>○ Institute for Social Protection and Solidarity (disabled people)</li> <li>○ The Greek Ministry of Healthcare and Social Solidarity</li> <li>○ AEMY SA (Primary Care Centers)</li> <li>○ Hellenic Foreign Trade Board</li> </ul>
Feb 2002 - Apr 2006	Athens Greece	INFORMATION SOCIETY SA	Project Director	Project Director (manager of project managers) of 20 EU Funded Projects under the 3 <sup>rd</sup> CSF. (Total budget about 70 M€). all projects are related to the development of regional healthcare information systems in Greece. Responsible for the National design of the HIS currently under development in the above mentioned projects.
Oct 1999 - Oct 2001	Athens Greece	DATAMED SA Healthcare Integrator	Business Development Manager	Project manager in ICT projects for hospitals in Greece Project manager in EU funded research programmes Business Development and Presales for the hospital information system product of the company (VAR of medico//s™, Siemens)

Apr 1999 – Sept 1999	Patras Greece	Institute of Biomedical Engineering	Biomedical Engineer	Member of the task force for the Y2K issue in medical devices
Sept 1996 – March 1999	Athens Greece	Biomedical Engineering Laboratory, School of Electrical and computer Engineering, National Technical University of Athens	Research Fellow, Research Project Manager and Coordinator	Project Manager and Member of implementation teams in EU funded and National Research Programmes in the regions of biomedical engineering, telemedicine, electronic medical record, business modelling in healthcare, etc.

#### 14. Other relevant information (eg, Publications)

##### **Publications**

“Key Performance, Indicators and Information Flow: The Cornerstones of Effective Knowledge Management for Managed Care”, A. Berler, S. Pavlopoulos, D. Koutsouris, to be published in “Knowledge Management: Concepts, Methodologies, Tools, and Applications”, Murray E. Jennex, San Diego State University, Information Science Reference Editions, Chapter 6.25, pp 2808 – 2828, 2008.

“Risk Assessment in Integrated Regional Healthcare Networks”, Alexander Berler, Stergiani Spyrou, Evaggelos Monochristou, Yannis A. Toliás, George Konnis, Nikolaos Magglaveras, Dimitris Koutsouris, eJETA.org Special Issue “Interoperability & Security in Medical Information Systems”, Vol. 2, Issue 2, May 2007, available online at:

<http://minbar.cs.dartmouth.edu/greecom/ejeta/specialMay07-issue/ejeta-special-07may-1.pdf>

“A roadmap towards healthcare information systems interoperability in Greece”, A. Berler, A. Tagaris, P. Angelidis, D. Koutsouris, *Journal of Telecommunication and Information Technology*, No. 2, pp 59-73, 2006

“ Quality of Medical Data with the use of Electronic Records ”, a. Berler, S. Pavlopoulos, D. Koutsouris, *Health Review*, Vol 17, Issue No 100, pp 32-37, 2006 [In Greek].

“The Use of HL7 as an Interoperability Framework in a Regional Healthcare System in Greece”, A. Berler, P.A. Angelidis, D. Koutsouris, *Journal of Telecommunication and Information Technology*, No. 4, pp 18-25, 2005

“Using Key Performance Indicators as Knowledge-Management Tools at a Regional Health-Care Authority Level”, A. Berler, S. Pavlopoulos, and D. Koutsouris, *IEEE Trans. Inform. Tech. Biomed.* Vol9, No 2, pp 184-192, 2005

“Medical Codifications and Healthcare Information systems”, A. Berler, S. Pavlopoulos, Chapter 4, in “Issues of Information Systems Management in Healthcare Facilities”, J Apostolakis, pp 67-78, Mediforce, 2005 [In Greek]

“Issues of Interoperability of Information Systems in Healthcare Facilities”, S. Pavlopoulos, A. Berler, Chapter 5, in “Issues of Information Systems Management in Healthcare Facilities”, J Apostolakis, pp 79-97, Mediforce, 2005 [In Greek]

“Key Performance, Indicators and Information Flow: The Cornerstones of Effective Knowledge Management for Managed Care”, A. Berler, S. Pavlopoulos, D. Koutsouris, published in “Clinical Knowledge Management, Opportunities and Challenges”, Rajeev K. Bali, Chapter VII, pp 116-138, Idea Publishing 2005

«*Medical Codifications: an Indispensable Tool for the Health Monitoring of Citizens*», A Berler, Imerissia, Special Issue «Healthcare», April 2005 [In Greek].

“*Integration Of Healthcare Information Systems: Steps Towards Common Clinical Documents*”, S. Spryrou, A. Berler, P. Angelidis, *Proceeding of the*

2<sup>nd</sup> ICICTH, 8-10 July 2004, Samos Island, Greece, published in special issues of the Journal for the Quality of Life Research (JQLR), 2004.

«Multi-purpose HealthCare Telemedicine Systems with mobile communication link support», E Kyriacou, S Pavlopoulos, A Berler, M Neophytou, A Bourka, A Georgoulas, A Anagnostaki, D Karayiannis, C Schizas, C Pattichis, A Andreou and D Koutsouris, *BioMedical Engineering OnLine* 2003 2:7, <http://www.biomedical-engineering-online.com/content/2/1/7>.

«The new horizons of Regional Healthcare Authorities in the framework of information and communication technologies», A Berler, Imerissia, Special Issue «ΥΓΕΙΑ», November 2002 [In Greek].

«The Introduction of HL7 in Greece», A Berler, Imerissia, Special Issue «Healthcare», November 2002 [In Greek].

«New technologies at the service of Medical Practitioners» A Berler, Imerissia, Special Issue « Healthcare », February 2002 [In Greek].

“Electronic Medical Record: One step towards better quality of care”, A Berler, Imerissia, Special Issue « Healthcare », March 2001 [In Greek].

“A Novel Emergency Telemedicine System Based on Wireless Communication Technology -“Ambulance”, S. Pavlopoulos, E. Kyriacou, A. Berler, S. Dembeyiotis, D. Koutsouris, *IEEE Trans. Inform. Tech. Biomed.* - Special Issue on Emerging Health Telematics Applications in Europe, Vol 2, No 4, pp 261-267, 1998.

“Design and development of a multimedia database for emergency telemedicine.”, S. Pavlopoulos, A. Berler, E Kyriacou, D. Koutsouris, *Technology and Health Care*, ECEM '97 Special Edition, (6) pp 101-110, IOS Press, 1998.

## **Conferences**

“A roadmap towards healthcare information systems interoperability in Greece”, A. Berler, A. Tagaris, P. Angelidis, D. Koutsouris, 6th Nordic Conference on eHealth and Telemedicine, Helsinki, Finland, 31 August – 1 September 2006

"Quality of Medical Data with the use of Electronic Records", A. Berler, S. Pavlopoulos, D Koutsouris, 7<sup>th</sup> Pan-Hellenic Conference on Management of Healthcare Services, Porto Heli, Greece, 5-7 October 2005.

*"Interoperability of Information Systems in Healthcare and the Effect on the Medical Practice from the Implementation of Integrated Healthcare Information Systems"*, A. Berler, 31<sup>st</sup> Pan-Hellenic Medical Conference, Athens, Greece, 17-19 May 2005.

"Medical Codifications and Healthcare Information systems", A. Berler, S. Pavlopoulos, 6<sup>th</sup> Pan-Hellenic Conference on Management of Healthcare Services, Alexandroupolis, Greece, 7-9 October 2004.

«*Interoperability Issues in a Regional Healthcare Information System: The Case of Greece and the Use of HL7*», Berler A., Angelidis P., Koutsouris D., HL7 Roadshow, International Joint Meeting EuroMISE 2004, Prague, Czech Republic, 16 April 2004, <http://www.euromise2004.org/about/hl7.html>

«*A Novel Virtual Patient Record Architecture Based On XML Technology*», G. Konnis, A. Berler, S. Pavlopoulos, G. Karkalis, E. Sakka, D. Koutsouris, proceedings of the 1<sup>st</sup> ICICTH, Samos, Greece, 11-13 July 2003.

*"Information System Interoperability in a Regional Health Care System Infrastructure: a pilot study using Health Care Information Standards"*, Stergiani S. Spyrou, Alexander A. Berler, Panagiotis D. Bamidis' proceedings of MIE 2003, St Malo, France, 4-7 May 2003.

*"Use Of XML Technology In A Virtual Patient Record Infrastructure"*, A. Berler, S. Pavlopoulos, G. Karkalis, E. Sakka, G. Konnis, D. Koutsouris, proceedings of the IEEE EMBS Fourth International Conference on Information Technology Applications in Biomedicine (ITAB 2003), Birmingham, United Kingdom, April 24-26, 2003.

*"Implementation of virtual patient record architecture use case scenarios"*, A. Berler, S. Pavlopoulos, G. Karkalis, E. Sakka, G. Konnis, D. Koutsouris, Proceedings of Mednet 2002, Amsterdam, The Netherlands, 4-7 December 2002

*"Implementation of a novel virtual patient record architecture"*, A. Berler, S. Pavlopoulos, G. Karkalis, E. Sakka, G. Konnis, D. Koutsouris, proceedings of the 2nd Joint Conference of the IEEE Engineering in Medicine and Biology Society and the Biomedical Engineering Society, Houston, TX, USA, 23-26 October, 2002

*"An XML based Electronic Health Care Record Architecture"*, A. Berler, S. Pavlopoulos, D. Koutsouris, proceedings of the Second symposium of

medical physics and biomedical engineering, Patras, Greece, 6-8-October 2000.

*"An XML based Electronic Health Care Record Architecture"*, S.

Pavlopoulos, A. Berler, D. Koutsouris, proceedings of the World Congress on medical physics and biomedical engineering, Chicago 2000, Chicago, USA, 23-28 July 2000.

«*Integrated Telemedicine System for remote surveillance and patient treatment*», E Kyriacou, S Pavlopoulos, A Berler, A Bourka, A Georgoulas, M Neophytou, D. Koutsouris, proceedings of the 2nd Pan-Hellenic Conference of Nursing Students, Athens, Greece, 2000

*" Integrated Telemedicine System for emergency telemedicine"*, E Kyriacou, S Pavlopoulos, A Berler, A Bourka, A Georgoulas, M Neophytou, D. Koutsouris, proceedings of the 2nd Pan-Hellenic Conference on Biomedical Engineering, Athens, 5-6 November 1999

*" Integrated Information System of an emergency telemedicine centre"*, A Georgoulas, P. Spanos A Berler, E Kyriacou, S Pavlopoulos, A Bourka, D. Koutsouris, proceedings of the 2nd Pan-Hellenic Conference on Biomedical Engineering, Athens, 5-6 November 1999

*"Telemedicine in emergency care"*, E Kyriakou, S. Pavlopoulos, A. Bourka, A. Berler, D. Koutsouris, *Proceedings of the VI International Conference on Medical Physics, Patras '99*, Patra, Greece, September 1999.

*"Design and Development of a Web-Based Hospital Information System,"* S. Pavlopoulos, T. Tagaris, A. Berler, D. Koutsouris, *Proceedings of the 20th Annual International Conference IEEE/EMBS*, pp. 1188-1191, Hong Kong, 1998.

*"A GSM-based mobile system for emergency telemedicine -"ambulance"*, S. Pavlopoulos, E. Kyriacou, A. Berler, D. Koutsouris,. VIII Mediterranean Conference on Medical and Biological Engineering and Computing, MEDICON '98, Lemesos, Cyprus, June 14-17, 1998, Proceedings of the VIII Mediterranean Conference on Medical and Biological Engineering and Computing, p113, 1998.

*"Design and development of an Intranet Hospital Information System"* S. Pavlopoulos, T. Tagaris, A. Berler, D. Koutsouris, VIII Mediterranean Conference on Medical and Biological Engineering and Computing, MEDICON '98, Lemesos, Cyprus, June 14-17, 1998, Proceedings of the VIII

Mediterranean Conference on Medical and Biological Engineering and Computing, p193, 1998.

*"A mobile system for emergency Health Care Provision via Telematic Support - AMBULANCE"* S. Pavlopoulos, E. Kyriacou, A. Berler, D.

Koutsouris, in *Proceedings of the 1998 IEEE International Conference on Information Technology Applications in Biomedicine, ITAB '98, Washington DC, USA, May 1998.*

*"Design and development of a medical multimedia database for an emergency telemedicine system"*, A Berler, S Pavlopoulos, D. Koutsouris, E Kyriacou, proceedings of the 1<sup>st</sup> Pan-Hellenic Conference on Biomedical Engineering, Athens, 20-21 March 1998.

*"Emergency Telemedicine Application Using Mobile and Internet Communication Links - The AMBULANCE Project"*,. S. Pavlopoulos, E. Kyriacou, A. Berler, D. Koutsouris, in *Proceedings of EURO-MED NET 98 Conference, Nicosia, Cyprus, pp. 281-282, 4-7 March 1998.*

*"Design and development of a multimedia database for emergency telemedicine"* A. Berler, S. Pavlopoulos, D. Koutsouris, 4<sup>th</sup> European Conference on Engineering and Medicine, Warsaw, Poland, May 1997, *Proceedings of the 4<sup>th</sup> European Conference on Engineering and Medicine* (Eds. Pierre Rabischong, Jacques Melin, Maciej Nalecz), p.221, 1997.

## **Heinz Münzenberger**

### **Curriculum Vitae**

**Dipl.-Inform. Heinz Münzenberger** \* 1949 in Esslingen

#### **Curriculum Vitae:**

<b>1970 – 1976</b>	Studying computer science and economics in Stuttgart and Bonn University Degree: Dipl. Inform.
<b>1976 – 1979</b>	Member of the research staff of GMD (research institute for mathematics and computer science) in St. Augustin
<b>1980 – 1981</b>	Management Consultant (company ADV/ORGA, Wilhelmshaven)
<b>1981 – 1989</b>	Acting Partner of GTI GmbH, Kürten
<b>1990 – 1993</b>	General Manager Information Engineering

(Deutsche Lufthansa AG)

**1993**

Member of the board of directors of GTI AG  
(Public and Private Insurances)  
Consulting German Government  
(Gematik,Knappschaft)  
Reforms of the Public Insurances

**Main focus Relevant to the Project:**

- Management Consulting since 1982 (main focuses: IT process models (e.g. VM-XT (certificate in 2008)), analysis and design methods)
- IT Project Management (corporate PM concepts, project leadership, PM coaching, setup and running project offices (project oriented and organisation wide))
- IT Quality Management (corporate IT-QM concepts, constructive and analytical quality assurance in IT projects)
- Analysis, assessment and improvement of IT process
- Excellent Knowledge of the Public Transport Sector
- Excellent Knowledge of the Insurance Sector
- Knowledge of German Egovernment needs (worked for Gematik, Fiscus, Bundesamt für den zivilienst, etc)

**Methods and Tools:**

- VM-XT (certificate since 2008), V-Model ,97 (D) / Hermes (CH), instep, Rochade
- various client specific process modells (development and customization)
- Project Management (PMI and enhancements, DIN 69901, ORGWARE-PM), MS Project, instep
- Agile Development (especially feature driven

approach)

- UML / RUP / Rational Rose
- event-driven process modelling, ARIS, Adonis, VISIO
- Assessment Methods (CMM, CMMI, SPICE)
- Strategic Information Planning (ISP)
- Requirements Engineering / Management
- Entity Relationship Modelling / data modelling, ERWIN
- Object Oriented Analysis (OOA), Rational Rose
- Metadata Management, Rochade
- SW Configuration Management (IEEE/SEI), CM Synergy
- Change Management, Change Synergy
- Structured Analysis / Design, GUIDE
- ITIL
- Problem Management, JIRA
- Test- und QS-Methods, Testdirector
- Presentation and Communication Techniques

**Lectures and Publications** **Strategische Informationsplanung** in  
,Fachliche  
Modellierung von Informationssystemen',  
Addison  
Wesley 1993

**Eine pragmatische Vorgehensweise zur  
Datenmodellierung**  
in ,Effektives Datendesign', R. Müller Verlag  
1989

Various lectures about the Experience with IT  
Process Models, Agile Software Development,  
Information Strategy Planning, Data Management  
and Data Modelling at national and international  
conferences.

**Memberships:** Member of the German Computing Society, PMI

**Projects (extract)**

**Client:** Employers' liability insurance association (printing and paper industry), Wiesbaden

**Project:** **Merge of two employers' liability associations**

**Client:** Sparkassen Informatik, Frankfurt

**Project:** **Portal based loan processing of business clients**

**Client:** gematik, Berlin

**Project:** **PM-Policy**

**Client:** gematik, Berlin

**Project:** **IT-Process Analysis**

**Client:** Bundesamt für den Zivildienst, Köln

**Project:** **Web-based development and implementation of the electronic individual files**

**Client:** fiscus GmbH, Bonn

**Project:** **Redefinition of several IT-processes**

**Client:** fiscus GmbH, Bonn

**Projects:** various system development projects (property acquisition tax, master data migration, tax collection)

**Client:** Deutsche Bank Bauspar AG, Frankfurt

**Project:** Information Strategy Planning and implementation

**Additional  
Projects before  
07 / 1998  
(extract)  
Tasks**

### **Various Clients**

- Development of an overall IT-QM concept for public services Düsseldorf
- Development of the IT Masterplan for the GfD company, Wermelskirchen
- Development of an IT strategy as part of the merging strategy of Sanacorp eG, München with an Austrian pharma wholesale company
- Development of an overall software development concept for Sanacorp eG, München
- Development and implementation of a company specific IT process model for Data General, Frankfurt
- Introduction of data modelling methods as well as developing various application specific and

department or corporate wide data models for the following companies: Deutsche Lufthansa AG, Heidelberger Druckmaschinen AG, Bayerische Vereinsbank, GEK Schwäbisch Gmünder Ersatzkasse, DASA, Landwirtschaftliche Sozialversicherungen, Victoria Versicherungen

- Development of an overall information engineering concept for a federal home savings and loan association bank
- Project Management concept and PM training for a German federal state bank
- Management consulting and project controlling for the development of an overall information system of the rural social security agency in Germany.

## **2. Introduction**

The consumer policy strategy (2007-2013) seeks to establish comparable levels of security and protection throughout the European Union (EU), as well as a more integrated internal market, through the following objectives:

- empowering consumers by creating a more transparent market that offers consumers real choice, for example in terms of price and quality.
- enhancing consumers' welfare in terms of price, quality, diversity, affordability, safety, etc.
- protecting consumers from serious risks and threats.

This policy focuses on five priority areas:

- better monitoring consumer markets and national consumer policies
- better consumer protection regulation
- enhancing product safety through the development of market monitoring tools
- putting consumers at the heart of other EU policies

- better informed and educated consumers, for example through strengthening the role of the European Consumer Centres.

In this paper, we present six different preliminary scenarios of anti-fraud systems which will prevent frauds in eProcurement, Registrar's offices, Public Transportation, Revenue Authorities, Customs Authorities and Insurances. All sections were reviewed and discussed between the two experts. Thought Mr Berler was responsible for the eProcurement, Registrar's offices, Revenue Authorities and Customs Authorities sections, while Mr Münzenberger was responsible for the Public Transportation and Insurances sections.

Each scenario description is structured as follows:

- Fraud(s)
- Solution description
- Requirements
- Examples of Auditing Rules

Fraud system detection will be very useful for unifying and achieving the goals of EU and as a result National members of EU, companies and civilians will be more protected.

In order to assess the existing iWebCare platform the experts reviewed the existing platform, read all available relevant documents and allocated possibilities of using this platform in other domains.

### **3. Governmental Procurement Procedures**

European governments buy goods and services worth up to one-fifth of their collective gross domestic product (GDP). Most of this expenditure is made through public tenders. Targeted correctly, this spending can make a significant contribution to stimulating economic growth and creating more jobs. eProcurement can help do this, create free and fair competition, promote access to all and cut costs as well.

European governments collect some 45% of their collective GDP in the form of taxes and other revenues and are responsible for spending about 15-20% of GDP – around €1.5-2 trillion – on goods and services.

It is estimated that electronic procurement and invoicing could reduce total procurement costs by around 5% and lower transaction costs by 10% or more, saving governments – and therefore taxpayers – tens of billions of euros annually.

The benefits of eProcurement do not stop at saving money. Traditional procurement systems can be difficult for potential bidders to access, while many may simply be unaware of existing tendering opportunities. This lack of information and knowledge is particularly the case with SMEs, which often lack the manpower to monitor the market.

In addition, despite EU-wide publication of higher-value calls for tender, public procurement still operates mainly at national level, with potential bidders from other countries unaware of opportunities and lacking the

resources to bid. Opening procurement up to wider competition across the EU would help to ensure that governments achieve the best price-quality balance for their taxpayers' money. In addition, governments can carefully target their public spending to stimulate innovation and create jobs.

Moreover, once a contract has been awarded following a tender, Information and Communication Technologies can continue to reduce administration costs and improve efficiency. Electronic ordering and invoicing systems have shown significant potential for cost savings in public administrations.

### **Road map for eProcurement**

Given the benefits of eProcurement, European governments have committed themselves to an ambitious road map for its rollout. Member States are committed to giving all public administrations across Europe the capability of carrying out 100% of their procurement electronically by 2010 and have set a minimum target of 50% for the actual use of electronic procurement.

In order to achieve this, Member States have signed up to a specific eProcurement action plan covering the period 2006-10. The Commission is launching a pilot project with support from the ICT Policy Support Programme to demonstrate an EU wide eProcurement system. The aim is to show that companies, particularly SMEs, will benefit from such a system, that it reduces their costs and simplifies the processes they need to follow to bid for public contracts outside their home Member State.

### **E-procurement in Europe**

The European Union adopted common rules for public contracts with directives 1993/36 (supplies), 1993/37 (public works), 1992/50 (services), 1993/38 (water, energy, transportation, and telecommunications). These directives did not include specific norms for the use of ICT in public administration procurement processes. In order to harmonize, simplify, and modernize these processes the EU adopted two new directives: directive 2004/18, which consolidates and updates the norms on tenders for public works, supplies, and services, and directive 2004/17, which updates these norms for the water, energy, transportation, and postal services sectors. The final term for the adoption of these two directives on the part of member states was January 31, 2006. The use of common standards in the regulation of public contracts is seen as a further step to perfect the European single market, which suffers in this field from barriers on private transactions and the lack of homogeneity in the norms adopted by the single countries.

### **Notes on the contents of the new directives**

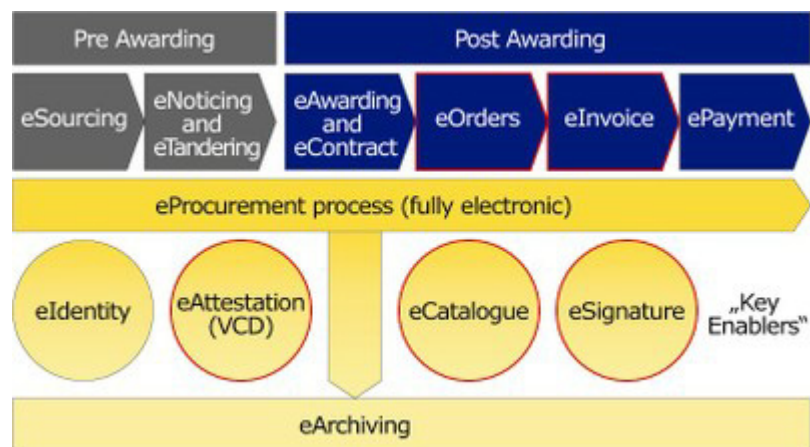
With regards to goods, services, and public works, community norms are applicable for purchases that exceed a given amount, which is updated by the Commission every two years. Certain types of contracts are excluded, in particular secret ones and those that have to do with a country's fundamental interests. In order to guarantee the transparency of procedures, several types of publicity are envisaged. Some are facultative (pre-information announcement and announcement of the publication of the tenders) while others are compulsive (public call for tenders,

announcement on the contracts that have been awarded and on the results of the call for tenders). The templates for these documents are prepared by the Commission.

The Pan European Pilot: PEPPOL

The objective of the PEPPOL (Pan-European Public eProcurement On-Line) project is to set up a pan-European pilot solution that, conjointly with existing national solutions, facilitates EU-wide interoperable public eProcurement. The vision of the PEPPOL project is that any company and in particular SMEs in the EU can communicate electronically with any European governmental institution for the entire procurement process.

The final outcome of PEPPOL will be an interoperational environment build upon national systems and infrastructures supporting the full cycle of eProcurement activities.



The pilots that will be developed in PEPPOL will support any economic operator in the EU and the European Economic Area (EEA) to respond to any published public tender notice electronically and to govern the entire procurement process from their own national infrastructure to any another national infrastructure. Thereby PEPPOL will focus on the engagement and participation of SME companies to public eProcurement.

**After Analyzing the existing and developed platform for the iWebCare project it is possible to use iWebCare in order to track possible fraud in Public Procurement and eProcurement solutions. Most of the existing rule concerning Healthcare procurement can be applied to any other Governmental setting outside the healthcare sector. We propose to use iWebCare as an automated add on to the PEPPOL project under development under the ICT-PSP program.**

### 3.1. Possible frauds

Participation of economic operators to public contracts is subject to verification of their eligibility, based on criteria related to economic and financial capabilities, as well as professional and technical knowledge and skills; furthermore, there are criteria to exclude economic operators that are a risk in terms of fraud and corruption (ongoing competition procedures, convictions for crimes that have to do with professional

morality, instances of fiscal evasion). So, in addition to already defined fraud scenarios we could complementary add:

1. identity theft: one economic operator is using the ID of another operator in order to participate in an eprocurement process
2. the economic operator (bidder) does not have the right to participate in a tender: some of the EU directive rules are not met
3. Invoicing frauds: use of false fiscal details
4. False invoices: invoices are issued but there is no money transfer in accordance to the invoice
5. VAT issues
6. Misrepresentations: It is illegal for a vendor to intentionally misrepresent an important fact in connection with a government contract. The misrepresentation need not be in writing and need not be in a certification. Any material misrepresentation will violate the law. Moreover, it is illegal to make such a misrepresentation during any part of the negotiation, bid, award or administration of the contract.
7. False Claims: It is illegal for a vendor to knowingly make a false claim for payment in connection with a government contract.
8. Price Fixing: Competitors may not agree to raise, stabilize or otherwise affect the prices at which they will sell goods or services. Such agreements are illegal whether or not they set specific prices - any agreement among competitors affecting price levels is illegal.
9. Vertical Price Fixing: An agreement between a seller of a product and the buyer as to what price the buyer will resell the product is illegal.
10. Bid-rigging: Competitors may not agree in any way to affect the outcome of a competitive bid process. They may not agree on who will win the bid, what bids each competitor will submit, that a bidder will not submit a bid or to rotate who will win particular contracts.
11. Bribery: A vendor may not offer or give any benefit to a public official in exchange for an official act or an act that violates the public official's duty. Similarly, a public official may not solicit or take any

benefit from a vendor in exchange for an official act or a violation of his/her duty. "Benefit" includes anything regarded by the recipient as a gain or advantage to him/herself or to a person or entity in whose welfare he/she is interested.

12. **Gratuity:** A vendor may not offer or give any benefit to a public official because of official acts by the public official or because the public official properly or improperly assisted the vendor. Similarly, a public official may not solicit or take such benefits.
13. **Gifts:** A public official may not solicit or take any benefit from a vendor that is not permitted by law. In other words, a public official should be sure that there is legal authority to accept any benefit from a vendor or potential vendor.
14. **Conflict of Interest:** A public official may not transact business on behalf of the government with any business in which the official or any member of his/her family has a financial interest. Further, a public official may not receive any benefit directly or indirectly from any contract for goods or services to be provided to the governmental entity where he/she works.

### **3.2. Requirements**

Government Procurement officials are responsible for the expenditure of taxpayer funds for the purchase of goods and services. Fraud and corruption of the procurement process impacts upon the ability to effectively obtain the goods and services needed at the lowest competitive price and in a timely fashion. Further, the practices which undermine the public perception of integrity of the procurement process impair the ability of all governmental entities to garner support of their legitimate procurement needs. Taxpayers have rightfully demanded that government spend tax money wisely and effectively. Preserving competition and ensuring the integrity of the procurement process provides government purchasing officials with the ability to obtain goods and services at the lowest possible cost and builds public confidence that taxpayer funds are being spent wisely.

The kind of evidences requested and the authorities that shall provide them differ from time to time and Member State to Member State. Thus a major challenge of the VCD work package will be to integrate various stakeholders in the design project process and to set up an IT system which supports a common set of evidences based on electronic business certificates and qualification documents that are most frequently

required. Typical evidences required are mentioned by the directive 2004/18/EC, for example evidences about:

- absence of conviction, e.g. criminal records
- non-bankruptcy and financial status, e.g. certificate or statement about nonbankruptcy
- compliance with fiscal and social obligations, e.g. tax clearance certificate
- suitability to pursue a professional activity, e.g. certificate of registration from the commercial register
- economic and financial standing, e.g. annual accounts,
- technical and professional ability of candidates, e.g. certificates of satisfactory execution of past works
- compliance to quality assurance standards and environmental standards, e.g. ISO certificates

In addition to the above legal requirements that iWebCare should setup rules to monitor, iWebCare should work as an auditing system to what PEPPOL is proposing.

### **3.3. Auditing Rules**

- Rule #1: Bidder ID. iWebCare will check the bidder ID from any existing Identity management system and confront it with details placed into invoices, e-auctions, bidding documents, etc.
- Rule #2. Check Offer Validity: Each offer of bid is following specific rules either stated in the EU Directive or in the RFP/FRI/FRQ documents. In that case iWebCare could check if all mandatory requirements were met for each participant. If a contractor won a tender without having fulfilled all mandatory rules during the tender, this a possible case for fraud or contractor mis-selection.
- Rule #3 Check eAuctions rules: iWebCare could check all the eAuctions rules that are setup and check if the bidder are participating with equal right the each bidding process

- Rule #4 check invoice validity: check that noted fiscal details are valid are a binded with an existing economic operator.
- Rule #5 check the eligibility of a bidder/contractor: at each step on the public procurement process, some rule must be met by the bidder/contractor
- Rule #6 Check payment alignment to invoices: each invoice should fit wit a payment (cash, electronic, bank transfer, etc). If a payment is not related to invoices there is a possibility of fraud (money laundering)
- Rule #7 check the validity of invoices: each invoice should fit with an existing contracting authority, an existing economic operator and a payment
- Rule #8 check if VAT or any other fiscal rule has been fulfilled. Each state has a different VAT percentage and there are European rules for VAT between EU member states. iWebCare should apply those rules to any transaction related to public procurement.

#### 4. Civil Registration

Civil registration is the system with which a government records the vital events of its citizens. The primary purpose of civil registration is to create legal documents that are used to establish and protect the civil rights of individuals. A secondary purpose is to create a data source for the compilation of vital statistics.

The United Nations defines civil registration as "the continuous, permanent, compulsory and universal recording of the occurrence and characteristics of vital events pertaining to the population as provided through decree or regulation in accordance with the legal requirements of a country. Civil registration is carried out primarily for the purpose of establishing the legal documents provided by the law. These records are also a main source of vital statistics. Complete coverage, accuracy and timeliness of civil registration are essential for quality vital statistics.

Vital events that are typically recorded include live birth, death, foetal death, marriage, divorce, annulment of marriage, judicial separation of marriage, adoption, legitimization and recognition. Among the legal documents that are derived from civil registration are birth certificates, death certificates, and marriage certificates.

According the British Register office, dated since 1837, the administration of individual registration districts is the responsibility of registrars in the relevant local authority. There is also a national body for

each jurisdiction. The local offices are generally responsible both for maintaining the original registers and for providing copies to the national body for central retention. A superintendent registrar facilitates the legal preliminaries to marriage, conducts civil marriage ceremonies and retains in his/her custody all completed birth, death and marriage registers for the district. The office of the superintendent registrar is the district Register office, often referred to (wrongly) in the media as the "Registry office".

#### **4.1. Possible frauds**

Identity fraud, of which Impersonation of the Deceased (IOD) fraud is a type, costs the UK economy, for example, over £1 billion a year. The Registrars General can disclose death registration information to assist in the prevention, detection, investigation, and prosecution of offences. Timely disclosure of death registration information will assist the police, other law enforcement bodies and public and private sector organizations to deal with offences and identify cases of attempted fraud by criminals using the personal details of the deceased. This will not only help to combat IOD fraud but will also reduce the impact on relatives of the deceased who have to deal with the consequences of the identity of their loved ones being stolen.

Since the introduction of civil registration in the mid 19th century, society has changed dramatically. GROs across Europe are currently engaged in a programme of modernisation to enhance service delivery by investing in modern IT systems and, where necessary, bringing forward changes in legislation.

Legislation confers powers on the Registrars General to supply bulk information contained in any register of deaths to the police and other organisations in a timely manner for use in the prevention, detection, investigation or prosecution of offences.

Identity fraud is widely recognised as a significant problem that can partly be addressed by wider sharing of information across government and the private sector. In particular, helping to address IOD fraud, a variant of identity fraud, has become an important policy objective.

Criminals can commit IOD fraud by using the obituaries column of a local newspaper, or other means, to identify someone who has recently died and obtaining more information about the deceased to build up an identity. This identity is used to access existing bank, building society or credit accounts or to apply for new financial services in the name of the deceased person.

In Europe, every death must be registered within five days or in the case of Scotland eight days. The Registrars General are required to provide an index of all the records they hold. Death registration information is therefore already in the public domain as soon as a death is registered.

While the fraudster is obtaining sufficient information to impersonate the deceased, organizations with which the deceased had financial dealings may be unaware of the death. Sharing death information more widely in a secure manner, shortly after a death is registered, will significantly reduce the opportunity for fraud.

According to the non-profit Identity Theft Resource Center, and other sources identity theft is sub-divided into five categories:

- business/commercial identity theft (using another's business name to obtain credit)
- criminal identity theft (posing as another when apprehended for a crime)
- financial identity theft (using another's identity to obtain goods and services)
- identity cloning (using another's information to assume his or her identity in daily life)
- medical identity theft (using another's information to obtain medical care or drugs)

Identity theft may be used to facilitate crimes including illegal immigration, terrorism, and espionage. Identity theft may also be a means of blackmail. There are also cases of identity cloning to attack payment systems, including online credit card processing and medical insurance.

Some individuals may impersonate others for non-financial reasons - for instance, to receive praise or attention for the victim's achievements. This is sometimes referred to as identity theft in the media.

### **Financial identity theft**

A classic example of credit-dependent financial crime (bank fraud) occurs when a criminal obtains a loan from a financial institution by impersonating someone else. The criminal pretends to be the victim by presenting an accurate name, address, birth date, or other information that the lender requires as a means of establishing identity. Even if this information is checked against the data at a national consumer reporting agency, the lender will encounter no concerns, as all of the victim's information matches the records. The lender has no easy way to discover that the person is pretending to be the victim, especially if an original, government-issued id can't be verified (as is the case in online, mail, telephone, and fax-based transactions). This kind of crime is considered non-self-revealing, although authorities may be able to track down the criminal if the funds for the loan were mailed to them. The criminal keeps the money from the loan, the financial institution is never repaid, and the victim is wrongly blamed for defaulting on a loan he/she never authorized. In most cases the financial identity theft will be reported to the national Consumer credit reporting agency or Credit bureaus ( in the U.S.) as a collection or bad loan under the impersonated person's record. The victim may discover the incident by being denied a loan, by seeing the accounts or complaints when they view their own credit history, or by being contacted by creditors or collection agencies. The victim's credit score, which affects one's ability to acquire new loans or credit lines, will be

adversely affected until they are able to successfully dispute the fraudulent accounts and have them removed from their record.

Other forms of bank fraud associated with identity theft include "account takeovers", passing bad checks, and "busting out" a checking or credit account with bad checks, counterfeit money orders, or empty ATM envelope deposits. If withdrawals or checks are made against the impersonated person's real accounts, that person may need to convince the bank that the withdrawal was fraudulent or file a court case in order to retrieve lost funds. If checks are written against fraudulently opened checking accounts, the person receiving the checks will suffer the financial loss. However, the recipient might attempt to retrieve money from the impersonated person by using a collection agency. This action would appear in the victim's credit history until it was shown to be fraud.

### **Identity cloning and concealment**

In this situation, a criminal acquires personal identifiers, and then impersonates someone for the purpose of concealment from authorities. This may be done by a person who wants to avoid arrest for crimes, by a person who is working illegally in a foreign country, or by a person who is hiding from creditors or other individuals. Unlike credit-dependent financial crimes, concealment can continue for an indeterminate amount of time without ever being detected. Additionally, the criminal might attempt to obtain fraudulent documents or IDs consistent with the cloned identity to make the impersonation even more convincing and concealed.

### **Criminal identity theft**

When a criminal identifies himself to police as another individual it is sometimes referred to as "Criminal Identity Theft." In some cases the criminal will obtain a state issued ID using stolen documents or personal information belonging to another person, or they might simply use a fake ID. When the criminal is arrested for a crime, they present the ID to authorities, who place charges under the identity theft victim's name and release the criminal. When the criminal fails to appear for his court hearing, a warrant would be issued under the assumed name. The victim might learn of the incident if the state suspends their own drivers license, or through a background check performed for employment or other purposes, or in rare cases could be arrested when stopped for a minor traffic violation.

It can be difficult for a criminal identity theft victim to clear their record. The steps required to clear the victim's incorrect criminal record depend on what jurisdiction the crime occurred in and whether the true identity of the criminal can be determined. The victim might need to locate the original arresting officers, or be fingerprinted to prove their own identity, and may need to go to a court hearing to be cleared of the charges. Obtaining an expungement of court records may also be required. Authorities might permanently maintain the victim's name as an alias for the criminal's true identity in their criminal records databases. One problem that victims of criminal identity theft may encounter is that various data aggregators might still have the incorrect criminal records in their databases even after court and police records are corrected. Thus it

is possible that a future background check will return the incorrect criminal records.

### **Synthetic identity theft**

A variation of identity theft which has recently become more common is synthetic identity theft, in which identities are completely or partially fabricated. The most common technique is combining a real social security number with a name and birth date other than the ones associated with the number. Synthetic identity theft is more difficult to track, as it doesn't show on either person's credit report directly, but may appear as an entirely new file in the credit bureau or as a subfile on one of the victim's credit reports. Synthetic identity theft primarily harms the creditors that unwittingly grant the fraudsters credit. Consumers can be affected if their names become confused with the synthetic identities, or if negative information in their subfiles impacts their credit.

### **Medical identity theft**

Medical identity theft occurs when someone uses a person's name and sometimes other parts of their identity -- such as insurance information -- without the person's knowledge or consent to obtain medical services or goods, or uses the person's identity information to make false claims for medical services or goods. Medical identity theft frequently results in erroneous entries being put into existing medical records, and can involve the creation of fictitious medical records in the victim's name.

iWebCare could assist the General registrars in their daily jobs and extract possible frauds. iWebCare could check for:

- Delayed registration of birth
- Delayed registration of death
- Delayed registration of marriage
- Delayed registration of divorce
- Change of name
- Family history forgery
- Heritage frauds
- Heritage tax avoidance
- Social allowances forgery
- Immigrant and emigrant name forgery or complexity

## 4.2. Requirements

iWebCare must interoperate with general register software in order to access to existing rules and details.

## 4.3. (Examples of) Auditing Rules

iWebCare will check for the following rules:

- Rule #1 Spell check: it is possible that an individual is recorded twice not as a consequence of fraud but as a consequence of a spell check error. This could lead to fraud if someone knows that he are more that one registered ID (for example, other name on the ID card, other on the Driving license, etc). Normally, Local or central authorities should check with the general registrar for birth registration in order to avoid double entries
- Rule #2 Complexity of names: it is often especially for immigrants that their naming convention is not familiar to the civil registry of the hosting country thus creating confusions
- Rule #3 Correction of entries: during the correction of an entry (wrong name or spelling, change of marital status, etc) it is common that partial information are hidden from the registrar for financial and d social allowances reasons
- Rule #4 Checks with social security frauds: it is common that a social change, the death of a relative is often hidden or delayed in its announcement in order to continue to have financial benefits from social security
- Rule #5Check for child abuse: unfortunately it is common that child adoption information is not recorded
- Rule #6 Checks for child trafficking: unfortunately some births are registered as unexpected death to allow child trafficking
- Rule #7 Checks for false pensions: it is common that a social change, the death of a relative is often hidden or delayed in its announcement in order to continue to have financial benefits from retirement pensions

- Rule #8 Check of single identity validity: this is mostly commonly known as identity fraud causing social and financial issues to Governments

## 5. Public Transportation

Busses, trains, subways and trams are part of the public transportation system of Europe.

Several major challenges have to be overcome for Europe's transport system to play its full role in satisfying the mobility needs of the European economy and society:

- Road traffic congestion is estimated to affect 10 % of the road network, and yearly costs amount to 0.9-1.5 % of the EU GDP.
- Road transport accounts for 72 % of all transport-related CO2 emissions, which increased by 32 % (1990-2005).
- Whilst road fatalities are in regression (-24 % since 2000 in EU27) their number (42 953 fatalities in 2006) is still 6 000 above the intended target of a 50 % reduction in fatalities in the period 2001-2010.

These challenges are even more pressing with forecasted growth rates of 50 % for freight transport and 35 % for passenger transport in the period from 2000 to 2020. The main policy objectives arising from these challenges are for transport and travel to become:

- cleaner,
- more efficient, including energy efficient,
- safer and more secure.

Public transport (or public transportation, public transit or mass transit) comprises passenger transportation services which are available for use by the general public, as opposed to modes for private use such as automobiles or vehicles for hire. Some services are free though most of them charge some sort of fare.

Public transportation can consist of buses, subways, trolleys and light rail, commuter trains, van pool services, paratransit services for senior citizens and people with disabilities, ferries, water taxis, or monorails.

Public transport is provided by a company or authority that operates a fleet of vehicles. They may or may not be regulated or subsidized by authorities. The infrastructure used may be exclusive, or shared with private vehicles. Higher public transport ridership is generally seen in urban areas, and less in North America and Australia. The environmental impact of public transport is lower than private due to less use of land area and energy, at the same time reducing urban sprawl. Public

transportation systems are also significantly safer than private road systems.

## **Infrastructure**

All public transport runs on infrastructure, either on roads, rails, airways or seaways; all consists of interchanges and ways. The infrastructure can be shared with other modes of transport, freight and private transport, or it can be dedicated to public transport. The latter is especially true in cases where there are capacity problems for private transport. Investments in infrastructure are high, and make up a substantial part of the total costs in systems that are expanding. Once built, the infrastructure will further require operating and maintenance costs, adding to the total costs of public transport. Sometimes governments subsidize the infrastructure by providing it free of charge, just like roads for automobiles.

## **Financing**

The main sources of financing are ticket revenue, government subsidies and advertisement. The percentage of revenue from passenger charges is known as the fare box recovery ratio. A limited amount of income may come from land development and rental income from stores and vendors, parking fees, and leasing tunnels and rights-of-way to carry fiber optic communication lines.

## ***Fare and ticketing***



A contactless ticket validator used in Oslo, Norway.

Most—but not all—public transport required the purchase of a ticket to generate revenue for the operators. Tickets may either be bought in advance, at the time of the ride, or the carrier may allow both methods. Passengers may be issued with a paper ticket, metal or plastic token, or an **electronic card**. Tickets may be valid for a single (or return) trip or may be valid within a certain area for a period of time. The fare is based on the travel class, either as a function of the traveled distance, or based on a zone pricing.

The tickets may have to be shown or checked automatically at the station platform or when boarding, or during the ride by a conductor. Operators may choose to control all riders, allowing sale of the ticket at

the time of ride. Alternatively, a proof-of-payment system allows riders to enter the vehicles without showing the ticket, but riders may or may not be controlled by a ticket controller; if the rider fails to show proof of payment, the operator may fine the rider at the magnitude of the fare.

Multi-use tickets allow travel more than once. In addition to return tickets, this includes period cards allowing travel within a certain area (for instance monthly cards), or during a given number of days that can be chosen within a longer period of time (for instance eight days within a month). Passes for tourists, allowing free or discounted entry at many tourist attractions, typically include free public transport within the city. Period tickets may be valid for a particular route (in both directions), or for a whole network. A free travel pass allowing free and unlimited travel within a system is sometimes granted to groups including students, elderly people, children, employees (*job ticket*) and the physical or mentally disabled people.

Free or zero-fare public transport services are totally funded by means other than collecting a fare from passengers, normally through extensive subsidies or commercial sponsorship by businesses. Several mid-size European cities and many smaller towns around the world have converted their entire bus networks to zero-fare. Local zero-fare shuttles or inner-city loops are far more common than city-wide systems.

## **Greening of transport**

Integrated Transport System (ITS) applications will play an essential role in the greening of transport. Differentiated charging of vehicles by Electronic Toll Collection systems for circulating on certain routes is a way to influence traffic demand ITS applications for journey planning, dynamic in-vehicle navigation and eco-driving support also contribute to congestion relief, to greener mobility and to less energy consumption.

The "Green transport corridors" are an EU initiative to promote the concept of integrated freight transport, with transport modes complementing each other to enable more environmentally friendly alternatives for long-distance transport between logistics hubs. Reliance on advanced ITS technology is essential for achieving this goal.

An eTicketing system could be used for public transportation. Using an eTicketing system based on smartcards, Governments could reduce paper costs and become more environmentally friendly. Another advantage of eTicketing is that smartcards (tickets) can be used in all public transportations.

Passengers will be able to serve their needs quicker. Passengers could add money to their smartcard via ATM, Credit Card and Cashiers. They could also check their public transportation usage and the routes they took via internet. The last feature should be very useful for companies, because they could check where outdoor employees (salesmen etc) have been.

Another advantage is that a conductor can use a portable smartcard reader, which will be connected to the Smartcard database, to check the passengers. If a passenger doesn't have a valid smartcard (ticket) the employee will charge his smartcard with the defined money penalty.

However, the most important advantage of eTicketing is that the public transportation organization can control incoming money faster and more accurate.

## **5.1. Possible Frauds**

There are two main possible frauds in public transportation system:

1. Employees payment fraud
2. eTicketing fraud

## **5.2. Employees payment fraud**

Employees are paid based on the hours they have worked on night or day shifts. Employees' payment fraud is possible. Sometimes employees seem to work double shifts or can check another's employee working card. As a result employees are paid more money than they should.

## **5.3. Requirements**

Governments can avoid this kind of fraud using iWebCare. In order to achieve this result, the IT system of public transportation should include the following integrated systems:

1. Central Human Resources Database where employee's demographic data, working hours (planned and actual), working shifts (planned and actual) and schedule are stored.
2. Smart cards which should be unique for every employee. Smart cards should contain the following employee's data: unique id, name, surname and photo.
3. Smart card readers connected to the Central Human Resources Database. Employees should check their personal smart card under the following situations: start of working shift, start of break, end of break, end of working shift.
4. iWebCare platform which will detect payment frauds based on rules and data exported from the Central Human Resources Database.

## **5.4. (Examples of) Auditing Rules**

iWebCare will check for the following rules:

- Rule #1: Employee exists. iWebCare will check the employee's unique ID, name and surname if it is registered in the Central Human Resources Database.
- Rule #2: Employee is on training. iWebCare will check if the employee is on training which means that he is paid but he is not available for working.
- Rule #3: Employee has retired or employee has moved to another place/department. iWebCare will check if the employee has retired which means that he is not available for working and payment or if the employee has moved to another place/department which means that his data must be transferred to another's department IT system.
- Rule #4: Employee was on vacation or ill. iWebCare will check if the employee was on vacation and it will calculate his payment or if the employee was ill for some days and it will calculate his payment for the days he wasn't in working schedule.
- Rule #5: Employee's insurance. iWebCare will check employee's insurance and it will calculate the amount of money that the company has to pay to the insurance.
- Rule #6: Employee is fired. iWebCare will check if the employee has been fired and as a result he is not getting payment any more. Additionally, he is not available for the working schedule.
- Rule #7: Employee's working shifts. iWebCare will check if an employee is registered for double shift and if it is possible depending on the working schedule, which will be stored in Central Human Resources Database.
- Rule #8: Employee's working days. iWebCare will check the working days of the employee against a working days limit and the working schedule.
- Rule #9: Employee's working hours. iWebCare will check the working hours of the employee against a working hour's limit and the working schedule.

- Rule #10: Total employees worked. iWebCare will check the total employees worked against a total employees worked limit that the working schedule will depend on. We assume that more statistics are helpful to evaluate the past (e.g. last month, last year) and answer “what if questions” if future changes are considered (total employees needed, average age of employees, sex of employees (males/females), educational status of employees, number of employees needed per route/station/transportation mean, optimization of administration).
- Rule #11: Check shift changes between employees. IWebCare will check for shift programs so that no employee can cover at the same time two shifts in different places.

## 6. eTicketing frauds

A possible eTicketing fraud may happen if someone tries to replicate the passenger’s smartcard, overcharge the passenger’s smartcard or add money to the passenger’s smartcard. Another possible fraud is when a conductor takes the penalty money for himself.

### 6.1. Requirements

In order to have a fully functional eTicketing system, the IT system architecture of a public transportation should include the following integrated systems components:

1. Routes Database. It will include the routes of all public transportation means, their time schedule and pricelist and money penalties for those who don’t have a valid smartcard (ticket).
2. Smartcard Database. It will include the unique ID of the smartcard, username and password (for internet access), money balance, charges and deposits of smartcard.
3. Smartcard readers. Smartcard readers should be placed in every public transportation station and they will be connected to the Routes and Smartcard databases.

4. Passenger's Smartcard. Every passenger must have a unique Smartcard in order to use the public transportation. This smartcard will include the unique ID of the smartcard and money balance.
5. iWebCare platform. It will detect frauds based on rules and exported data from Routes and Smartcard Databases.

## **6.2. (Examples of) Auditing Rules**

iWebCare will check for the following rules:

- Rule #1: Check the smartcard unique ID. This rule will check if a smartcard is original or a fake by comparing its unique ID with those registered in Smartcard database.
- Rule #2: Check the transportation station. It checks if the smartcard reader is a valid smartcard reader by checking its position stored in the Routes database.
- Rule #3: Check the smartcard money balance. When a passenger tries to check for a ticket the smartcard reader reads the money balance and compares it with the money balance stored in the Smartcard database.
- Rule #4: Check the charge. If Rule #3 returns that the balance is equal, the system checks the price for the ticket based on the pricelist stored in the Routes database.
- Rule #5: Check the source of deposit. When a passenger makes a deposit for his smartcard, the system checks if the source of deposit is valid. Valid sources are considered ATMs, Credit Cards and Cashiers.
- Rule #6: Check for valid or invalid tickets. When a conductor validates a passenger's ticket, the system compares the current date and time with the last charge of the smartcard. If the time period is within limits (for example the validation took place after 1 hour), the ticket is valid otherwise the ticket is invalid.
- Rule #7: Money penalty. If a passenger has an invalid ticket the system checks the Routes database for money penalties referring to

the mean of transportation the passenger uses and charges his smartcard.

- Rule #8: Statistics. iWebCare will export statistics for transportation such as passengers per route, frequency of usage per route, hours of usage per route. These statistics will help to optimize the transportation system, working schedule and investments.

## 7. Revenue authorities

In May 2006 the Commission presented a Communication with a view to launching - at EU level - a profound debate on the need for a coordinated approach in the fight against fiscal fraud in the internal market. Intense and fruitful discussions followed within the different European institutions, with Member States and business representatives.

The Commission's Communication of 23 November 2007 concerning some key elements contributing to the establishment of the anti-fraud strategy within the EU and the accompanying report on the state of play of the discussions within the Anti Tax Fraud Strategy (ATFS) expert group provide a good overview of the follow-up that has been given until then to the 2006 Communication. These documents served as the basis for the Council conclusions of 4 December 2007.

In February 2008 the Commission presented a Communication on its analysis of two more '*far reaching*' measures to change the VAT system in order to fight frauds, namely a system of taxation of intra-Community transactions and a general reverse charge system. The Commission also demonstrated its willingness, under certain conditions, to work out a pilot project in order to establish whether a reverse charge could be an appropriate response to tackle VAT fraud or not.

The following ECOFIN Council could, however, not agree on Conclusions as regards the issues raised in this Communication. In the absence of a political agreement on the more '*far reaching*' measures, the Commission has decided to concentrate its efforts exclusively on the so-called '*conventional*' measures to enhance the traditional methods in the fight against tax fraud.

The objective of the present Communication is to set out a coherent short term action plan and a time schedule for the envisaged actions. This Communication intends also to initiate a reflection on a longer term scale notably about the relation between taxpayers and Tax Administrations and the opportunities offered by IT in that context. It should be recalled that in 2006 the Communication presented an IT system that covered all taxes.

Subsequent discussions however made it very clear that absolute priority needs to be given to VAT fraud. This Communication therefore only relates to VAT and the recovery of taxes. This does not mean that no actions will be undertaken in other areas; in particular the Commission will present shortly a proposal in view of strengthening the administrative

co-operation arrangements for taxes other than VAT and the harmonised excises.

### **NECESSARY COMMUNITY APPROACH**

The need to establish an anti-fraud strategy to combat tax fraud at Community level to complement and support national efforts has been recognized by the Council in its conclusions of November 2006 and June 2007. The European Parliament has also expressed its support for an EU fiscal fraud strategy.

An efficient fight against VAT fraud within an internal market requires a common approach both in the legislative field and also on certain aspects of the operational management of the VAT system which - until now- have been left exclusively to the Member States.

Indeed, operational differences between Member States can provide fraudsters the opportunity to undermine the efficiency of the underlying Community legislative measures by shifting their operations to those Member States that have not implemented these measures in an effective way. Differences in national procedures are also amplifying considerably business compliance costs. The national procedures put in place for the fulfillment of VAT obligations by electronic means is a good example of this. When elaborating legislative proposals the Commission carefully balances the need for a Community approach and the respect of national structures and the practices of Tax Administrations. It is essential for the efficiency of the measures proposed that this carefully defined balance is respected and maintained during the whole negotiation process within the institutions.

The reports already presented by the Commission on the state of play of the discussions within the Anti Tax Fraud Strategy (ATFS) expert group gave an overview of the different measures that have been analyzed.

Guiding principles have been:

- the need of Tax Administrations for quick and accurate information
- optimising the use that Tax Administrations can make of this information
- enhancing the possibilities to act against fraudsters
- respecting the needs and expectations of legitimate businesses, in particular not to be exposed to unnecessary administrative burdens leading to additional compliance costs and to have legal certainty guaranteed.

A number of suggested measures have been abandoned because they did not respect these guiding principles.

## 7.1. Fraud

A possible fraud with the current revenue bill system may occur when:

- a company completes a project for the end user (B2C)
- a company completes a project for another company ( B2B)

## 7.2. Solution description

In order to avoid this kind of fraud, revenue authorities could use a new IT system which will protect the end users and companies from being cheated. Companies won't have monthly books for billing control but they will use software which will send a report at the end of the month to the Internal Revenue Service. Additionally, the software that companies will use must have a database for storing offers, orders and customers information. These three components will be necessary for invoices.

The main advantage of this system is that National government will be able to control the companies easier, reduce its paper costs and become more environmentally friendly. The National government will be able to protect the end users and companies in the best way. Finally, it will be able to collect taxes easier and safer.

## 7.3. Requirements

1. Software and Database in company. Software and a database that will store data about customers, offers, orders and invoices. It will also store the entire database about the taxations, tax-payment, employees and operating cost-rules.
2. Tax advisor Software. Using the software consultancies can reduce their workload of daily administrative tasks and consequently implement processes that save time and money. In addition, consultants increase the operational efficiency of their consultancy by increasingly motivating employees resulting in more efficient working methods. The software will automatically send a report to the Internal Revenue Service every month. It will also help to do the accountant administration from the tax-advisor better and faster. This gives more accurate view of the administration to the tax advisor and the tax authority.
3. Internal Revenue Service Database. This database will be used by the Internal Revenue Service for storing information sent by companies. It

will also contain demographical and economical information about companies (B2B) and civilians (B2C).

4. Internal Revenue Service Software. Software that will be used by the Internal Revenue Service for exporting information and reports from the Internal Revenue Service Database.
5. iWebCare platform. It will detect frauds based on rules and exported data from the Tax Advisor Software to the Internal Revenue Service Database.

#### **7.4. (Examples of) Auditing Rules**

iWebCare will check for the following rules:

- Rule #1: Company's TAX ID exists. It checks if the company's TAX ID is registered as national and international.
- Rule #2: End user's TAX ID exists. It checks if the end user's TAX ID is registered as national and international.
- Rule #3: Offer's ID. It checks if the offer's ID is valid and registered.
- Rule #4: Offer accepted or refused. It checks if an offer is accepted or rejected. If it is accepted, it must be associated with order IDs.
- Rule #5: Order's ID. It checks if the order's ID is valid and registered.
- Rule #6: Order's association. It checks if the order is associated with an offer and invoices.
- Rule #7: Invoice's ID. It checks if an invoice's ID is registered and associated with orders and an offer.
- Rule #8: Offer association with end user or company. It checks the TAX ID of the offer and associates it with the end user or company.
- Rule #9: Invoice association with end user or company. It checks the TAX ID of the invoice and associates it with the end user or company.

## 7.5. (Examples of) Additional rules for companies

- Rule #10: Income taxes. It checks the income tax class and category of the company's services and calculates the taxation.
- Rule #11: Expenses taxes. It checks the expenses tax class and category and the system calculates the tax.
- Rule #12: Insurance. This rule checks the company's insurance and calculates the insurance tax. The tax depends of these features: private Health, public health, Pension.
- Rule #13: Household and Vehicle insurance. It checks the company's household and vehicle(s) insurance and calculates the insurance tax. The tax depends of these features: liability insurance, public liability insurance, third party insurance, vehicle insurance.
- Rule #14: Validation of monthly report source. It checks the source of the monthly report sent by the Tax Advisor software if it is trusted and authorized. This rule is important for the stability of the whole system.

## 8. Customs

Customs duties and consumer taxes have been levied in all eras and cultures for more than 5,000 years, providing a means of securing state revenues and controlling the flow of goods. In Germany, the first historical evidence of customs officers goes back to the time of the Roman Empire and can be proved continuously from the reign of Charlemagne the Great onwards at many important trade routes and markets.

The Customs Administration in the Federal Republic of Germany or in other Countries can now look back on a 50-year history since the end of the Second World War. Despite the fact that this period is relatively short in comparison to the entire history of customs, numerous developments of great importance to citizens, the economy and politics have taken place in it.

This period saw the founding of the European Customs Union, the realization of the single European market with the abolishment of inner-European border controls, the application of a Community customs code, The Customs Administration has always adapted to new political and economic developments in a quick and flexible manner. But which role does the Customs Administration play on the single European market nowadays? What is its place in the modern administration of each government, within the context of Europe and in the progressive

globalization of economic, political and social processes? What responsibilities do Customs fulfill today and why does its work remain important for the citizens of Europe?

Competent administration that not only fulfills its classic responsibilities of securing national and European community revenues, but has become a governmental service provider for a future-proof economy, offering more security for citizens and businesses.

In their objectives, tasks and responsibility to the European community, the state and the administration must do justice to changing social, economic and political framework conditions. Its goals and its range of tasks extend far beyond border-related activities:

- *Customs uses modern practices and methods to promote trade and the economy and thus in the EU as locations for industry.*
- *Customs ensures the government's ability to function by means of efficient collection of duties.*
- *Customs protects citizens and the economy.*
- *Customs fights international organized crime – from the drug trade, product piracy and smuggling all the way to money laundering and illegal cash flows, as well as violations of international species protection acts.*
- *Customs is constantly improving its range of services in cooperation with citizens and the economy.*
- *Committed employees identify with the tasks and goals of the administration and continually strive for customer satisfaction and optimal quality service.*

Today's Customs Administration is a customer-oriented, multi-faceted tax and economic authority which simultaneously functions as a guarantor of the internal security of our state. It is indispensable in the promotion of our country as a location for industry and in protecting citizens and business from crime and frauds. The discharging of these duties requires extensive and global collaboration, as well as intensive cooperation in European and international bodies and constant contact to the economy.

Customs performs tasks that serve to protect citizens, promote the economy and ensure the ability of our community to function by means of fair collection of taxes.

## **8.1. Fraud**

A possible fraud with the current customs system may occur when a tax officer doesn't complete the category and tax class of an imported product correctly and as a result National government loses money.

## 8.2. Solution description

In order to avoid fraud and corruption in a customs system, we suggest an IT system that will be able to control tax officers and check imported products in a better way. Another benefit for the National government is that tax officers will be more productive and trustable. As a result more products could be imported.

## 8.3. Requirements

1. Customs Database. Database that will contain information about products (categories, tax classes), tax officers (name, surname, unique ID, demographical information) and imported products.
2. Customs Software. This software will be used by the tax officer to complete the procedure of importing products. Data produced by the customs software will be stored in a customs database.
3. Tax authorities Database. This database will be located within the Internal Revenue Service and customs software will be connected to it in order to associate imported products with invoices, companies, civilians and other economical information.
4. iWebCare platform. It will detect frauds based on rules and exported data from the Customs and Tax Authorities Database.

## 8.4. Auditing Rules

iWebCare will check for the following rules:

- Rule #1: Tax officer authorization. It checks the unique id of a tax officer, his or her name and surname in order to guarantee a legitimate use of the Customs Software.
- Rule #2: Validation of product code. It checks the correctness of a product code and its registration in the Customs Database.
- Rule #3: Product's origin. It checks if the origin of the product is an EU member country or a NON-EU member country.
- Rule #4: Product's category. The Customs Database will be searched for the appropriate category of the product.

- Rule #5: Tax class of product. The Customs Database will be searched for the appropriate tax class of the product.
- Rule #6: Product association with invoices. It checks the Tax Authorities Database for associated invoices.
- Rule #7: Calculation of import duty. It calculates the import duty of the product based on the results of rules #2, #3, #4, #5 and #6.
- Rule #8: Company's TAX ID exists. It checks whether the company's TAX ID is registered as national and international.
- Rule #9: End user's TAX ID exists. It checks if the end user's TAX ID is registered as national and international.
- Rule #10: Invoice IDs. It checks if invoice IDs are registered and associated with a product import ID.
- Rule #11: Product Import accepted or rejected. It checks if a product import is accepted or rejected based on its origin, category, tax class, TAX IDs and invoice IDs. If it is accepted, it must be associated with an invoice and a tax officer.
- Rule #12: Statistics. iWebCare will provide statistics for imported and exported products such as:
  - a. imported/exported amount of products based on code, category, tax class, date
  - b. customs frequency usage
  - c. amount of accepted and rejected products imported/exported
  - d. number of rejected accesses to the system (e.g. wrong tax officer ID)
  - e. number and category of illegal products which were tried to be imported/exported (within a given period)

## **9. Insurances**

Through compulsory liability insurance for attorneys and other professionals, clients' trust in the legal profession is guaranteed because one can remain confident that financial losses caused by any error or mistake will be covered by an insurance policy. Insurance terms, risk

assessment and pricing are, to a large extent, left for the free insurance market to determine.

This type of insurance can be offered in many other areas. Compulsory liability insurance will also help support confidence in the efforts to privatize public tasks with regulatory or advisory functions.

The practice of many professions entails a risk that errors and omissions may cause other people to suffer financial losses. Consequently, professionals take out insurance covering their liability for such losses – advisory insurance or professional liability insurance. For specific professions where it is of material importance to society at large that people have full confidence that the professionals perform their work correctly, such liability insurance is now compulsory. For example, attorneys and accountants need to take out professional liability insurance in order to be able to practice their profession. The statutory requirement for liability insurance enables clients to trust an attorney as they can remain absolutely sure that any loss caused by any error or omission made by the attorney will be covered by a policy.

Compulsory liability insurance is offered on market terms in open competition between the individual insurance companies. As a result of the typically limited number of policyholders, professional liability insurance is often taken out with one or two companies, and frequently group schemes are taken out by the members of the individual professional organization, for example through the Danish Bar and Law Association. Legislation does not necessarily stipulate any detailed requirements for such insurance as the individual professional groups have a considerable self-interest in upholding trust in the profession in question and therefore see to it that liability insurance provides adequate cover.

From an insurance point of view, it is necessary for the individual policyholder to keep the incentive to avoid errors and omissions even though a liability insurance policy has been taken out. As a result, such policies often carry a rather large deductible, meaning that the policyholder himself must pay a substantial part of any amount to be paid in compensation.

Similarly, the policyholder knows that any license to practice the relevant profession will be revoked at no notice if the insurance company decides to cancel the policy.

In line with the general increase in welfare, the extent of losses inflicted on other parties by an advisor will increase, and society thus has a growing interest in securing confidence in the practice of more liberal professions than today.

Just as compulsory liability insurance can be used to inspire confidence in connection with legislation protecting consumers as in the case of compulsory liability insurance for licensed surveyors, such insurance can be used to inspire confidence in the privatization of public tasks – such as the work performed by the Danish Motor Vehicle Inspection Office.

Compulsory professional liability insurance could be a tool for safeguarding the interests of citizens and society in more professional areas than is currently the case with no tax funding, no setup of any guarantee fund and no establishment of administratively cumbersome

guarantee schemes, etc. However, as mentioned above, efforts should be made to ensure that:

- Insurance terms, risk assessment and pricing are left for the free insurance market to determine to the greatest extent possible.
- Policyholders' incentive to avoid errors and omissions is kept at its present level or increased and
- The number of policyholders is sufficiently large to ensure the required spreading of risk.

## 9.1. Fraud

An insured person may claim money for a fake reported incident.

## 9.2. Solution description

In order to avoid frauds in insurances, we suggest a complete IT system for insurance companies that will check the insurance's policy against the reported incident based on an appropriate set of rules.

Additionally, all companies and businessmen must be insured for Facilities and Goods protection in order to get operational permission from the National government. As a result, National government will not have to pay for companies' vandalisms using money from taxes collected for other purposes.

Bank organization may also require a household insurance in order to offer a loan contract to any civilian.

The last two scenarios are commonly used in Germany and other EU member countries.

## 9.3. Requirements

1. Insurance Database. The Database should contain information about insurance's clients, contact information, insurance's agencies, reported claims, incidents information and insurance pricelists and policies.
2. Insurance Software. This software will be used by the insurance's administrations in order to register clients, provide claim reports and incident reports. The data produced by the insurance software will be stored in an insurance database.
3. iWebCare platform. It will detect frauds based on rules and exported data from the Insurance Database.

## 9.4. (Examples of) Auditing Rules

iWebCare will check for the following rules:

- Rule #1: Insured Client's ID. It checks the unique id of a client, his name and surname if registered.
- Rule #2: Contract ID exists and insurance's agency. It checks if the client has a contract ID and which insurance agency registered the contract (and when).
- Rule #3: Contract validation. It checks if a contract is valid (which means that an insurance is guaranteed for the client) or has expired.
- Rule #4: Insured Client's Payments. It checks if the client has completely paid his insurance so far in order to have the right to claim money for an incident.
- Rule #5: Date of Claim Report and Incident Report. It checks the date that the client claimed the money against the date at which the incident was reported. The claim report must be reported at most five days after the incident report.
- Rule #7: Client's Claim Reports History. It checks the client's claim reports history for similar or duplicated claim reports. If a match occurs the last claim report is rejected or has to be investigated in more detail.
- Rule #8: Client's Insurance Categories. It checks the categories for which the client is insured. These categories are the following:
  - a. Healthcare insurance
  - b. Private liability insurance
  - c. Household insurance
  - d. Accident insurance
  - e. Insurance for legal protection
  - f. Life insurance
- Rule #9: Client's insurance is company or individual. It checks if a client is a company or an individual and returns the associated pricelist.
- Rule #10: Cause of incident. It checks the cause(s) of the incident reported based on reports of police, fire brigade and other trusted sources. The result could be one of the following:

- a. Act of God (earthquake, flood, fire etc)
  - b. Vandalism
  - c. Theft
  - d. Inattention
  - e. Third person inattention/unawareness
- Rule #11: Cause of incident and insurance's category association. It checks the cause(s) of an incident and associates it with the insurance's category where client is insured. If there is no match, the claim report is rejected. Otherwise, the claim report is accepted.
  - Rule #12: Payment for accepted claim report. It checks if a claim report is flagged as Accepted and calculates the money that the client will get. The payment is calculated according to the insurance's pricelist.
  - Rule #13: Completeness of payment in time period. It checks if the payment for an accepted claim report has completed within the time period limit (for example 60 days from claim report acceptance).
  - Rule #14: Statistics. Statistics such as the number and reason of non-accepted claim reports (within a certain period), number of delayed payments (e.g. after 60 days), categories of incidents, frequency of incidents etc.

## 10. Review

The iWebCare platform is an integrated system for detecting possible frauds on data submission. It is developed with Open Source Software and it supports Open Standards (such as ebXML, XML, etc.). The detection of frauds depends on configurable rules and data mining algorithms.

The iWebCare fraud detection tool is the core element of the iWebCare integrated web services platform. Separate and interface independent modules comprise the fraud detection tool. These modules interact via clear (mostly SOAP) interfaces. The tool consists of the following main modules:

1. e-gov application (WS Client)
2. iWebCare Web Service (IWS)
3. Self Learning Module Web Service (SLWS)
4. Health Care Ontology (HCO)
5. Fraud detection – validation engine (FDE)
6. Rules Repository (RR)

A management module lies in a separate layer above these modules. It is responsible for the overall management of the tool. It is a web interface tool by which registered users can login and manage the platform. A very important characteristic of the management tools is that each user has his specific profile. User profiles and roles can be defined by the super administrator only.

The iWebCare platform advantage is that it is built as a Web Service which is accessible any time and from any registered domain (Healthcare, Revenue Authorities etc). Although the platform was primarily developed for the HC domain, it can also be used **by other domains** too because it is easily configurable and it supports Open Standards (ebXML, XML etc). As we can see in Table: Technologies, domains are using the same technologies and the only characteristic that changes is the Ontology and Rules Repository which is easily configurable by the iWebCare administrator. In the following table (Table: Rules) we can see that rules for every domain presented is almost the same type.



**Table: Rules 1**

Healthcare		Government Procurement		Civil Registration	
ID	Rule	ID	Rule	ID	Rule
1	Missing diagnosis	1	Bidder ID	1	Spell Check
2	Maximum 3 diagnoses	2	Check offer Validity	2	Complexity of names
3	Maximum 3 prescribed drugs	3	Check eAuctions Rules	3	Correction of entries
4	Missing doctor's or patient's or pharmacist's member number	4	Check invoice Validity	4	Check with social security frauds
5	The patient, the doctor or the pharmacist is not TSAY's member	5	Check the eligibility of a bidder / contractor	5	Check for child abuse
6	The prescribed drugs are not reimbursable	6	Check payment alignment to invoices	6	Check for child trafficking
7	Violation of the 5-day execution period	7	Check the validity of invoices	7	Check for false pensions
8	Prescription issuance date should not overlap execution date	8	check if VAT or any other fiscal rule has been fulfilled	8	Check for single identity validity
9	A drug is characterized as hospital or governmental drug and it needs special documentation				
10	Mismatch between diagnosis and participation				
11	The prescribed drugs are overpriced				
12	Mismatch between diagnosis and drugs				
13	Mismatch between diagnosis and medical specialty				
14	Violation of the maximum dosage per drug				
15	Excessive violation of the recommended dosage per drug				
16	Improper prescribed drugs				
17	Too high treatment cost				

**Table: Rules 2**

Technology	Domain						
	Healthcare	Public Transportation	Revenue Authorities	Customs	Insurances	Government Procurement	Civil Registration
Web Service	x	x	x	x	x	x	x
Use of Open Standards	x	x	x	x	x	x	x
Privacy & Protection of Personal Data	x	x	x	x	x	x	x
Ontology Specifics	Domain Specific	Domain Specific	Domain Specific	Domain Specific	Domain Specific	Domain Specific	Domain Specific
Rules Repository	Relative to Ontology	Relative to Ontology	Relative to Ontology	Relative to Ontology	Relative to Ontology	Relative to Ontology	Relative to Ontology
Security	x	x	x	x	x	x	x

**Table: Technologies 1**

However, the web interface of the platform should be more user friendly. It could be developed with better and cleaner fonts, more attractive icons and colours.

Another interesting feature of the iWebCare platform is the Self-learning module. The self-learning module's purpose is to create or update rules for a certain domain. This is achieved using data mining algorithms and learning from error-free and fraudulent datasets. But is it safe to let the system create or update rules by its own? In my opinion, in the future, the platform may take wrong decisions and fraud analysis because of that module.

Finally, the iWebCare platform is a very useful platform for detecting and fighting frauds for any government and business domain. Although it is easy to use, it is very powerful because of its configuration and development. We believe that iWebCare should be tested for a period of time as a pilot application. We believe that the results will be the expected. After that, the iWebCare platform will be ready to become a fully business market product.

## 11. Bibliography

1. [Identity Theft Resource Center website](#)
2. [http://www.worldprivacyforum.org/medidtheft\\_consumertips.html](http://www.worldprivacyforum.org/medidtheft_consumertips.html)  
world privacy forum
3. <http://www.privacyrights.org/fs/fs17g-CrimIdTheft.htm> Privacy Rights Clearinghouse
4. McFadden, Leslie (2007-05-16). "[Detecting synthetic identity fraud](#)". *Bankrate.com* 1-2.
5. <http://www.fightidentitytheft.com/blog/medical-identity-theft-protect-yourself>
6. [Identity Theft Resource Center Fact Sheet 117 Identity Theft and the Deceased - Prevention and Victim Tips](#)
7. [Identity Theft Protection Services](#) retrieved on 2008-12-16
8. [Identity-Theft Protection: What Services Can You Trust?](#) PC World.com, retrieved on 2008-12-16
9. [http://unstats.un.org/unsd/publication/SeriesF/SeriesF\\_84E.pdf](http://unstats.un.org/unsd/publication/SeriesF/SeriesF_84E.pdf)
10. <http://unstats.un.org/UNSD/demographic/sources/civilreg/default.htm>
11. [http://ec.europa.eu/information\\_society/activities/egovernment/policy/impact/eproc/index\\_en.htm](http://ec.europa.eu/information_society/activities/egovernment/policy/impact/eproc/index_en.htm)

12. [http://ec.europa.eu/internal\\_market/publicprocurement/docs/eprocurement/actionplan/actionplan\\_en.pdf](http://ec.europa.eu/internal_market/publicprocurement/docs/eprocurement/actionplan/actionplan_en.pdf)
13. <http://www.peppol.eu/>
14. <http://ec.europa.eu/idabc/en/document/4720/5874>
15. [http://ec.europa.eu/enterprise/international\\_relations/index\\_en.htm](http://ec.europa.eu/enterprise/international_relations/index_en.htm)
16. [http://ec.europa.eu/taxation\\_customs/taxation/index\\_en.htm](http://ec.europa.eu/taxation_customs/taxation/index_en.htm)
17. <http://www.europarl.europa.eu/activities/committees/homeCom.do?body=ECON&language=EN>
18. [http://www.consilium.europa.eu/cms3\\_applications/applications/newsRoom/loadBook.asp?BID=93&LANG=1&cmsid=350](http://www.consilium.europa.eu/cms3_applications/applications/newsRoom/loadBook.asp?BID=93&LANG=1&cmsid=350)
19. [http://ec.europa.eu/publications/booklets/move/17/txt\\_en.pdf](http://ec.europa.eu/publications/booklets/move/17/txt_en.pdf)
20. [http://europa.eu/pol/trans/index\\_en.htm](http://europa.eu/pol/trans/index_en.htm)
21. [http://ec.europa.eu/transport/its/road/deployment\\_en.htm](http://ec.europa.eu/transport/its/road/deployment_en.htm)
22. [http://ec.europa.eu/transport/its/road/initiatives\\_en.htm](http://ec.europa.eu/transport/its/road/initiatives_en.htm)
23. [http://ec.europa.eu/transport/its/road/useful\\_links\\_en.htm](http://ec.europa.eu/transport/its/road/useful_links_en.htm)
24. <http://www.bundesrechnungshof.de>
25. [http://ec.europa.eu/taxation\\_customs/resources/documents/common/whats\\_new/COM\(2008\)807\\_en.pdf](http://ec.europa.eu/taxation_customs/resources/documents/common/whats_new/COM(2008)807_en.pdf)
26. <http://www.reuters.com/article/pressRelease/idUS209469+24-Apr-2008+BW20080424>
27. [http://actuarialwiki.org/~actuarial/index.php?title=Incurred\\_claims\\_\(or\\_claims\\_incurred\)](http://actuarialwiki.org/~actuarial/index.php?title=Incurred_claims_(or_claims_incurred))
28. HELLENIC General Secretariat for Information Systems - [www.gsis.gr](http://www.gsis.gr)
29. HELLENIC GENERAL ACCOUNTING OFFICE - [www.mof-glk.gr](http://www.mof-glk.gr)
30. HELLENIC Financial Control Committee - [www.edel.gr](http://www.edel.gr)
31. HELLENIC General Secretariat for Investments and Development - [www.ggea.gr](http://www.ggea.gr)

32. HELLENIC MINISTRY OF TRANSPORT & COMMUNICATIONS -

[www.yme.gov.gr](http://www.yme.gov.gr)

EVALUATION REPORT ON THE  
APPLICABILITY OF THE iWebCare  
PLATFORM FOR THE IDENTIFICATION  
OF CUSTOMS FRAUDS

European Technologies and Innovation Ltd – ETI Ltd

Contents
----------

COMPANY PROFILE.....	93
INTRODUCTION .....	94
KNOWN FRAUD CASES .....	96
IMPACT .....	99
EXISTING DATA & SYSTEMS .....	103
RULES & FRAUD DETECTION.....	105
TECHNICAL ADJUSTMENTS REQUIRED.....	107
CONCLUSIONS.....	111

## 1. COMPANY PROFILE



European Technologies and Innovation Ltd  
1 Kings Avenue  
N21 3NA  
London  
UK

ETI Ltd is a London based innovation consulting firm aiming to provide solutions on issues related with growth through innovation. Its clients are multiscale and cover both private and public owned institutions. The main aim of the company when it was formed back in 1999, was to provide integrated innovation management services via:

- Utilizing best practices in research and innovation with the aim of identifying new growth opportunities for its clients
- Smoothly establishing the much needed innovation culture within its clients having in mind their short and long term benefits
- Leveraging the experience gained from its past involvement in similar projects when consulting for new business deals or licensing agreements in order to bring solutions to market as fast as possible.

ETI Ltd offers these services covering diverse technological areas where the commercialisation and implementation of new technologies is the best path to follow. The areas at which it has a specific expertise include

- e-Health applications
- e-Government systems
- e-Commerce

Via its participation in several projects the firm has collaborated with research institutions, public bodies, SMEs as well as individuals with the aim of commercialising technologies and putting real and innovative business cases into different markets.

The company's expertise lies in assessing the utility and commercial advantages of emerging technologies and assisting its clients in the development of their specific requirements, so they can utilise these technologies for the enhancement of their business.

The strength of the company lies in the multidisciplinary combination of experts with both strong academic background and extensive experience in large industrial projects as well as in the close collaboration with leading European and international industrial organisations and research institutes. The firm operates very closely with its customers, which are located all over Europe and include both large leading technology based companies, as well as technology users with specific needs such as the various regional innovation policy making authorities. It offers the full spectrum of services required for the efficient introduction of edge technologies in complex business environments, including; feasibility studies and business plans, requirements analysis, business modelling, systems integration, re-engineering and project management.

To summarize ETI combines:

- IT Consulting Services
- Market and Technology Trends Watch
- Strategic Business Planning
- Regional Innovation Strategies
- Technology Licensing
- Consulting Services for the Creation of High-Tech Start-Ups and Spin-Offs
- Corporate Finance for High-Tech Start-Ups
- Access to Funds
- International Networking and Business Development

in order to ensure the optimum application of emergent technologies in real business environments as well as the fastest amortization of the perspective investments.

ETI's competitive advantages accrue from:

- The pan European multidisciplinary network of specialised consultants with long term experience in innovation management.
- The close cooperation with leading research centers and SMEs that develop innovative technologies as well as international business groups with major access in the global market.
- The continuous participation of the company in European R&D projects.
- The proactive monitoring of emergent technologies
- The firms position between sources of innovation, financial resources, and different business environments.

## 2. INTRODUCTION

Customs is an authority or agency in a country responsible for collecting and safeguarding customs duties and for controlling the flow of goods including animals, personal effects and hazardous items in and out of a country. Depending on local legislation and regulations, the import or export of some goods may be restricted or forbidden, and the customs agency enforces these rules. The customs agency may be different from the immigration authority, which monitors persons who leave or enter the country, checking for appropriate documentation, apprehending people wanted by international arrest warrants, and impeding the entry of others deemed dangerous to the country.

The customs protect citizens from the illegal imports of dangerous or piratical products, dangerous games and foods that can place our health and safety at risk. Still more impressive it is the fact that the custom block the way to the chemical substances that can be used for the production of dangerous narcotics, such as ecstasy. Moreover, the customs impede the illegal imports of internationally protected animals or animals that can transmit illnesses. At the same time, they protect also our cultural heritage through the monitoring of illegal distribution of artistic

treasures, while they check the legality of export of sensitive technologies that could be used in the manufacture nuclear or chemical arms.

The scope of the current report is to provide an evaluation of the iWebCare platform as regards its applicability in the Customs domain, as well as suggest the modifications and customizations required in order for it to be as efficient as possible and be able to interact with existing information systems utilized. In order to achieve this ultimate goal, the report also indicates the various customs fraud cases that have been brought to light until today, as well as makes a rough estimation of the impact that these fraud cases have upon the fiscal accountability reports of the various member states and of the European Union as a whole.

### 3. KNOWN FRAUD CASES

A customs duty is a tariff or tax on the import of or export of goods. Since the establishment of customs duties, people have tried to evade these taxes, either through simplified or more complex ways, many times with success as well as many times with failure. The methods that are used for the evasion or for the reduction of such taxes are:

- Misclassifying products to avoid or decrease import tariffs, since different products belong to different tax imposition categories. In most cases, this method of tax avoidance is rather primitive and relies upon the evasion of control at the customs.
- Falsely undervaluing imported products misrepresenting antidumping duty obligations.
- Misstating country of origin to avoid anti-dumping duties or to gain preferential duty status in programs such as the Caribbean Basin Initiative.
- Misdesignating country of origin to avoid apparel quotas and thereby causing an underpayment of tariffs.
- Smuggling goods. This includes substantial smuggling activities where importers avoid taxes by completely bypassing customs procedures, cases where importers engage in fraud with the co-operation of corrupt customs officials, and cases where importers physically bypass customs and enter the country through alternative routes. Smuggling mainly involves three types of goods, namely cigarettes, alcohol and narcotic substances.
- The carousel scheme, which is similar to smuggling cross-border VAT fraud. It involves the import and export of small in size, high-value goods. Carousel or input VAT fraud is committed when a chain of supplies of goods exists and one or several links of this chain do not pass on VAT proceeds to the tax authorities. This involves mostly supplies from one EU Member State to another. At the place of destination the goods are resold, with the buyer reclaiming input tax.
- Forgery of certificates, in which case the copies of the accompanying receipts are returned as certified, with the signatures of the corresponding employees of the frontier Customs forged. The case of certificate forging can also include the cases of virtual imports and exports, in which various goods are supposedly exported from one country and imported to another, with this transaction never actually taking place.
- Gifts. This recent trend, which started blooming the last few years, along with the blooming of e-commerce, regards marking items as gifts. Due to the fact that fees are charged for items over a specific value (~50 Euros) in most European countries, e-buyers regularly ask their vendors to wrap the purchased item as a gift, so as to evade customs. This has become a regular plan for buyers through Amazon and e-bay, two of the most famous e-marketplaces worldwide.

Perhaps one of the most renowned cases of mis-classification of products in the recent history is that of PepsiCo<sup>2</sup>. PepsiCo manufactures brand names like Pepsi(TM) and Diet Pepsi(TM) in its Ireland facility. It then imports the cola soda beverage concentrate, "duty free" (or tax free) into the United States. PepsiCo has argued that the product is classified as an "odoriferous substance," because it contains the secret cola flavor. Relator Winslow on the other hand has argued that the cola concentrate is predominantly sugar and water, which is subject to a 6.4% tax by weight. As alleged in the suit, each drum of soda concentrate can be worth a million dollars or more. In fact, during the 2004 to 2005 time period, PepsiCo imported more than a billion dollars worth of soda concentrate into the United States, tax free. Relator Winslow has alleged PepsiCo may well have avoided paying \$500,000,000 in customs duties. If Winslow is correct, the Government can collect three times that amount plus penalties, pursuant to the False Claims Act, or \$1.5 billion for the national treasury.

One of the most renowned cases of falsely undervaluing imported products that came to the light only recently was that of the international organized crime group that had been in the import business of meat and meat products from Denmark, Belgium, the Netherlands and France. Only for the year 2004, through one of these countries alone, 750 imports of meat and meat products were delivered to Bulgaria. Each of the deliveries weighed between 20 and 25 tons. During the check-ups into the activity of different companies related to 35 cases so far, it was established that the goods had been double invoiced at rates that were many times lower than their real value. Unauthentic invoices, certificates and changed delivery conditions were presented to the Bulgarian customs. The crime group had been using off-shore companies registered on islands in the English Channel, USA, Cyprus, etc. for the purpose of double invoicing. The group had been using similar fraud mechanisms for import of Turkish, Dubai and Chinese cargo as well<sup>3</sup>. According to Lieutenant-General Boyko Borissov, this customs and tax fraud network that was dismantled, had affected the state budget by millions of euro.

Similar is the case of Distilleries Corporation of Sri Lanka (DCSL), which was proved to have been swindling the state for the last 10 years for over Rs.1500 million with under invoicing through processing fraudulent documents<sup>4</sup>.

One of the most renowned cases of misstating country of origin to avoid anti-dumping duties is that of the elaborate international import/export scam involving 1.7 million litres of honey that was trialed at the end of 2007<sup>5</sup>. Between July 2001 and June 2002, 28 consignments of Chinese honey were imported into Australia by CHS Enterprises Pty Ltd and 'JHM Trading Company' in 125 shipping containers. The honey was imported into Australia as a Chinese product, and was then re-labeled as an Australian product by the importer and repacked for export from Australia to the United States of America. The complex fraud was part of a world-wide scam in an attempt to circumvent anti-dumping duties imposed on Chinese honey by the United States, since Australian honey was not subject to such duties. The court imposed fines and costs totaling \$451,200.

Smuggling of various goods, and in most cases of cigarettes and alcohol is one of the most common customs duties evasion methods. A renowned case is that of Ylber Rraci<sup>6</sup>, the head of

---

<sup>2</sup> <http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=104&STORY=/www/story/06-01-2007/0004600245&EDATE=>

<sup>3</sup> [http://press.mvr.bg/en/News/news050117\\_02.htm](http://press.mvr.bg/en/News/news050117_02.htm)

<sup>4</sup> <http://sundaytimes.lk/070909/FinancialTimes/ft315.html>

<sup>5</sup> <http://www.australia.to/story/0,25197,23040466-735,00,00.html>

<sup>6</sup> <http://www.setimes.com/cocoon/setimes/xhtml/mk/features/setimes/newsbriefs/2002/05/020519-IVAN-002>

the Kosovo Customs Administration, whom the UN police forces arrested in Kosovo on 17 May 2002, over suspicion of fraud and abuse of power. The accusations against Rraci increased after a sacked customs officer revealed cases of corruption and showed a map of smuggling routes in Kosovo. The Serbian authorities burnt more than 80 tones of smuggled cigarettes (\$60m worth of cigarettes) to emphasize the government's commitment to clamping down on crime. Especially cigarette smuggling has become a very serious problem across the entire EU. Each year, the European Union loses hundreds of millions of Euro in customs duties. In addition, in the numerous cases of narcotic substances smuggling, the cases of the 34 year old Albanian Georgi Sore, who was arrested during customs research, trying to smuggle 821 Kgrs of hashes from Albania into Greece hidden in his truck, and of the 34 year old Spanish J. Patino, trying to smuggle 26 Kgrs of pure heroin from Turkey to Greece hidden inside his jeep should also be included<sup>7</sup>. However, smuggling of arms, jewellery, precious stones, watches, textiles and alcoholics is also widespread internationally.

The carousel scheme is very similar to smuggling, but instead of involving cigarettes and alcohol, it involves small, high-value goods such as computer chips and mobile phones. The methods of carousel fraud are multiple. Enterprises are frequently set up with front. Organised VAT fraud is then carried out through highly complex groups of companies pretending to trade in cheap or small goods. The authorities are deceived by means of fictitious invoices and fictitious deliveries. Formal evidence is also manufactured: by using other businesses' VAT identification numbers or firms that are in bankruptcy. These smokescreen methods enable embezzler to reclaim input tax for trade in valueless or imaginary goods with impunity. In other words, these goods are imported free of VAT, then sold on to another trader with the VAT added - after which the fraudster disappears without sending the VAT to the customs authorities. The goods are then re-exported, the VAT reclaimed and the goods re-imported and sent round the carousel again. The same goods may often go from country to country earning fraudulent tax at every stage. Increasingly, the goods may not even physically move.

In general, criminals based in East Europe are exploiting lax policing of customs and tax systems because member-states have failed to compensate for abolition of border controls by updating crime-fighting systems and sharing information. Four years after the abolition of border controls, member-states continue to act as 15 separate entities, providing a free-for-all for the criminals. Cigarettes are the biggest business for customs fraudsters. The tax system set up for goods moving from outside the EU through member-states involves 18 million operations a year, all by paper and open to fraudsters. Goods such as cigarettes or alcohol are simply unloaded clandestinely en route and placed on the black market. Nobody knows the extent of the fraud. Estimates vary by billions from country to country<sup>8</sup>.

---

<sup>7</sup> <http://www.gsis.gr/customs/dioxi.htm>

<sup>8</sup> [http://www.europedia.moussis.eu/books/Book\\_2/3/5/1/4/index.tkl?lang=gr&all=1&pos=53&s=1&e=10](http://www.europedia.moussis.eu/books/Book_2/3/5/1/4/index.tkl?lang=gr&all=1&pos=53&s=1&e=10)

## 4. IMPACT

Tackling customs fraud is tough for agency officials to take on alone. Commercial entries have been increasing steadily since as early as the 1990s, while the number of Customs fraud investigations remains low, due to the limited personnel and the insufficient technological support. According to the OECD 2008 Factbook<sup>9</sup>, the import of goods has doubled since 2000, topping at 8381,7 billion US dollars in 2006, while it is estimated that it has exceeded the 1000 billion US dollars barrier in 2008, while EU15 is responsible for half of the total import of goods of this economic globalization.

	2000	2001	2002	2003	2004	2005	2006
Australia / Australie <sup>1</sup>	67,8	60,9	69,5	84,8	103,8	118,9	132,7
Austria / Autriche	67,4	69	71,4	91,5	111,2	120	134,2
Belgium / Belgique	171,7	178,7	198,1	234,8	285,5	320,2	353,7
Canada / Canada <sup>1</sup>	240	221,6	222,4	240,2	273,4	314,4	349,9
Czech Republic / République tchèque <sup>1</sup>	32,2	36,5	40,7	51,2	68,1	76,5	93,4
Denmark / Danemark	44,4	44,3	49,3	56,2	66,9	75	84,5
Finland / Finlande	34,1	32,2	33,6	41,6	50,1	58,5	69,5
France / France	304	304,2	303,8	362,4	434,4	476	529,9
Germany / Allemagne	495,4	486,3	490,1	601,8	718,2	777,4	919
Greece / Grèce	29,8	28,2	32,5	44,9	52,8	54,9	63,7
Hungary / Hongrie	32,1	33,7	37,6	47,7	60,2	65,9	77
Iceland / Islande	2,6	2,3	2,3	2,8	3,6	5	5,6
Ireland / Irlande	50,7	51,1	52,3	54,2	62,3	70,3	76,4
Italy / Italie	237,3	236,1	246,6	297,4	351,1	380,6	405,7
Japan / Japon	379,7	348,6	337,6	383,5	455,2	515,9	579,1
Korea / Corée	160,5	141,1	152,1	178,8	224,5	261,2	309,4
Luxembourg / Luxembourg	10,6	11,2	11,5	13,6	16,8	17,6	19,5
Mexico / Mexique <sup>1</sup>	171,1	165,1	165,7	170,5	196,8	221,8	256,1
Netherlands / Pays-Bas	174,7	169,9	163,4	209	257,7	283,2	331,5
New Zealand / Nouvelle-Zélande	13,9	13,3	15	18,6	23,2	26,2	26,4
Norway / Norvège	34,4	33	34,9	41,2	48,5	55,5	64,2
Poland / Pologne	48,9	50,2	55,1	68	88,2	101,5	125,6
Portugal / Portugal	39,9	39,5	40	47,1	54,9	61,2	65,9
Slovak Republic / République slovaque <sup>1</sup>	12,7	14,7	16,6	22,6	29,1	34,2	44,4
Spain / Espagne	152,9	155	165,9	209,7	259,3	289,6	330
Sweden / Suède	73,1	63,5	67,1	84,2	100,5	111,4	127,1
Switzerland / Suisse	82,5	84,2	83,7	96,4	110	126,6	141,4
Turkey / Turquie	54,5	41,4	51,3	69,3	97,5	116,8	137,4
United Kingdom / Royaume-Uni	339,4	338	359,4	393,5	461,3	515,8	606,4
United States / États-Unis	1258,1	1180,1	1202,3	1305,1	1525,3	1732,3	1919
EU15 total / Total UE15 <sup>2</sup>	2225,6	2207,1	2285	2741,8	3282,8	3611,5	4120,2
OECD total / Total OCDE <sup>3</sup>	4816,4	4633,7	4771,8	5522,7	6590,3	7384,3	8381,7

More or less, the same applies for the export of goods, with the numbers being a little lower, as illustrated in the following table:

<sup>9</sup> <http://www.oecd.org>

	2000	2001	2002	2003	2004	2005	2006
Australia / Australie	63,8	63,3	65	70,2	86,4	105,8	123,3
Austria / Autriche	62,3	64,7	71,3	89,2	110,8	117,7	134,1
Belgium / Belgique	185,2	190,3	215,8	255,5	306,5	334	369,2
Canada / Canada	277,6	261,1	252,6	272,1	316,9	360,1	388
Czech Republic / République tchèque	29,1	33,4	38,5	48,7	67,2	78,2	95,1
Denmark / Danemark	49,6	50,1	55,7	64,6	74,8	83,3	90,1
Finland / Finlande	45,8	42,8	44,7	52,5	60,8	65,2	77,3
France / France	295,6	299,8	304,9	357,9	413,9	434,4	479
Germany / Allemagne	550,2	572	615,6	748,5	911,8	977,8	1125,8
Greece / Grèce	11	10,3	10,8	13,7	15,2	17,5	20,9
Hungary / Hongrie	28,1	30,5	34,3	43	55,5	62,3	74,1
Iceland / Islande	1,9	2	2,2	2,4	2,8	3,1	3,5
Ireland / Irlande	76,3	77,4	88,3	92,9	104,3	110	108,9
Italy / Italie	239,1	244,2	254,3	299,4	349,1	367,9	400,6
Japan / Japon	479,2	402,6	416,7	472	565,7	594,9	646,7
Korea / Corée	172,3	150,4	162,5	193,8	253,8	284,4	325,5
Luxembourg / Luxembourg	7,9	8,3	8,6	10	12,2	12,7	13,6
Mexico / Mexique	165,3	157,5	160	164,9	188	214,2	250
Netherlands / Pays-Bas	180,1	175,5	175,3	227,3	290,5	320,1	370,3
New Zealand / Nouvelle-Zélande <sup>1</sup>	12,7	13,3	13,8	16,5	20,3	21,7	22,4
Norway / Norvège	59,9	59	59,6	70,3	82,2	103,8	122,2
Poland / Pologne	31,6	36,1	41	53,5	73,8	89,4	109,3
Portugal / Portugal	24,4	24,1	25,8	31,8	35,7	38,1	42,1
Slovak Republic / République slovaque	11,8	12,6	14,5	22	27,6	31,9	41,7
Spain / Espagne	113,3	116,1	125,9	156,3	182,7	192,8	214,1
Sweden / Suède	87,4	76,3	82,9	102,4	123,2	130,3	147,4
Switzerland / Suisse	80,5	82,1	87,9	100,7	116,8	130,9	147,9
Turkey / Turquie	27,8	31,3	35,8	47,3	63,1	73,5	85,3
United Kingdom / Royaume-Uni	282,9	272,6	280,6	307,7	348,2	384,4	444,4
United States / États-Unis <sup>2</sup>	780,3	731	693,2	723,7	817,9	904,3	1037
EU15 total / Total UE15 <sup>3</sup>	2210,9	2224,5	2360,5	2809,8	3339,8	3586,2	4033,9
OECD total / Total OCDE <sup>4</sup>	4432,7	4290,7	4438	5110,9	6078	6645	7505,9

Nevertheless, the key statistic that is missing from the annual "Accountability Report" of all Customs Services, is the amount of money that federal governments have lost due to customs fraud. This is because accurate estimates are hard to come by. However, hard estimations can be made, and they also account for billions of dollars per country. Europe is losing billions of € in customs and tax revenue as international criminals benefit from abolition of border controls and lax revenue policing.

According to the Guardian, based on HM Revenue & Customs reports, In the United Kingdom carousel fraudsters carried out a record 7.4 billion pounds (£) of imports and exports in the first quarter of 2006, up from its original estimate of 5.5 billion pounds (£)<sup>10</sup>. Alan Castle, an economist at Lehman Brothers investment bank, calculated that based on existing trade data, activity could rise to 10 billion pounds (£) or more, meaning fraudulent trade volumes could easily hit 35 billion pounds (£), more than triple the 2005 figure and 10 times the amount in 2004. According to the same report, EU officials claim that losses to member states could amount to € 50 billion a year.

<sup>10</sup> <http://www.guardian.co.uk/business/2006/jul/15/2>

In addition, as regards the United Kingdom, a report from the National Audit Office has highlighted weaknesses in the IT system used by Customs & Excise to fight fraud<sup>11</sup>. Customs & Excise officials estimate that VAT fraud costs the department up to 10,2 billion pounds (£) a year. The National Audit Office also reported that, overall, Customs' VAT IT systems are large, old and complex, and depend upon significant resources for support.

Furthermore, according to its Economy Minister, Russia is losing about \$5 billion in revenue a year from customs fraud, i.e. falsely labeled goods and undervalued merchandise, and smuggling by companies and government employees<sup>12</sup>.

In Austria, in the fight against fraud, the following impressive numbers were obtained between the beginning of 2005 and the middle of 2006: The seizing of 161.8 million cigarettes and 299.5 kg of narcotic drugs as well as 28,244 inspections of businesses resulted in 9,506 charges. Tax audits yielded €3.03 billion in additional tax revenues<sup>13</sup>. As regards retroactive field and in-company customs audits completed in 2006, they resulted in the collection of additional duties in the amount of €17.7 million.

In addition, in 2007 the quantities of chemical substances that can be used for the production of dangerous narcotics that were confiscated by the customs would be enough for the production of narcotic valued more than €1 billion<sup>14</sup>.

Moreover, the enterprise “Diabolo” that took place in April 2007 aimed at bringing into justice the smuggling of cigarettes. OLAF coordinated this enterprise in which 27 member states participated, along with Interpol, Europol and the International Customs Organisation. This enterprise revealed 135 millions counterfeited cigarettes and more than half million other counterfeited products, such as clothes and mobile telephones, as well as poultry. If these illegal attempts had been glorious, the smugglers would have gotten away with the payment of duties and special consumption taxes of € 220 millions, for the cigarettes only. The evasion of payment of duties and special consumption taxes for cigarettes, usually through smuggling, is one of the most important sectors of fraud that OLAF is dealing with. In one sole enterprise, in March 2008, that took place jointly with the Authorities of Germany and Poland, roughly seven millions cigarettes, approximately €3 million in cash and nine Kgrs of gold and jewels were confiscated<sup>15</sup>.

Overall, it is estimated that about 3% of the total net value of the legally imported goods per country is added because of the successes of the customs control. This sums up to an approximate total of € 300 billion internationally, or approximately € 150 billion for EU15. However, it is also estimated that the successes of the customs control, account for only a fraction of the evaded taxes, and more specifically account for approximately 20% of the customs frauds<sup>16</sup>. This indicates approximately € 600 billion that federal governments loose annually due to customs frauds. Collecting duties and taxes from the imports of agricultural products, the customs employees do not simply apply the commercial rules, but also

---

<sup>11</sup> <http://www.computerweekly.com/Articles/2002/12/19/191675/audit-office-report-highlights-flaws-in-customs-fraud.htm>

<sup>12</sup> <http://www.iht.com/articles/2005/12/08/business/ibrief.php>

<sup>13</sup> Combating fraud In the interest of the taxpayers, Federal Ministry of Finance, April 2007

<sup>14</sup> <http://www.tovima.gr/default.asp?pid=2&ct=32&artid=241354>

<sup>15</sup> [http://europa.eu/pol/fraud/overview\\_el.htm](http://europa.eu/pol/fraud/overview_el.htm)

<sup>16</sup> U.S. Customs and Border Protection, Performance and Accountability Report, Fiscal Year 2006

significantly contribute in the financing of the EU, since this income accounts for approximately 15% of the Community budget. Moreover, fighting the fraud with regard to the VAT, they contribute in the maintenance of an income source that accounts for approximately 16% of budget<sup>17</sup>.

---

<sup>17</sup> [http://europa.eu/pol/cust/overview\\_el.htm](http://europa.eu/pol/cust/overview_el.htm)

## 5. EXISTING DATA & SYSTEMS

Law-enforcement services cannot work without reliable information. Customs administrations need accurate, up-to-the-minute information. For this reason, the EU has built an information system which ensures that officers have immediate access to information on suspicious border crossings across the EU<sup>18</sup>.

The aim of the European Union's customs information system (CIS) is to enable national customs services to exchange and disseminate information on smuggling activities and requests for action. It assists in preventing, investigating and prosecuting serious contraventions of national laws by increasing the effectiveness of cooperation and control procedures of the customs administrations of the Member States. The information system offers immediate access to relevant customs information to all Member States, without communication barriers. Since information can be accessed quickly, legitimate trade is facilitated while officers can act effectively, on the basis of information, regarding possible illegal activities.

The CIS consists of two databases, one falling within the framework of European Community actions, and the other falling under inter-governmental action. The legal base for the inter-governmental database, the CIS Convention, sets out the procedures to be adopted in the use of information technology for customs purposes. It outlines the broad parameters of information that may be stored, the manner in which information can be amended, security systems and data-protection provisions. The main categories of information collected relate to:

- commodities;
- means of transport;
- businesses;
- persons;
- fraud trends;
- availability of expertise;

Direct access to data is reserved exclusively for the national authorities designated by each Member State (i.e customs administrations). Information is delivered through the Antifraud Information System (AFIS) terminals in the Member States. AFIS is an integrated information system which has been installed with the financial support of the EU in the member countries (so far in the EU15 but not integrated in EU25 until now).

As regards personal data, these are confined to:

- name, maiden name, forenames and aliases;
- date and place of birth;
- nationality;
- sex;
- any particular objective and permanent physical characteristics;

---

<sup>18</sup> [http://ec.europa.eu/justice\\_home/fsj/customs/informsystem/fsj\\_customs\\_informsystem\\_en.htm](http://ec.europa.eu/justice_home/fsj/customs/informsystem/fsj_customs_informsystem_en.htm)

- reason for inclusion of data;
- suggested action;
- warning code indicating any history of being armed, violent or escaping.

The CIS has been developed and is currently managed by the European Anti-Fraud Office (OLAF). The European Commission's Justice and Home Affairs DG and the Taxation and Customs Union DG are also involved in the development of policy.

This integrated anti-fraud system also includes:

- AFIS-mail, a secure e-mail service for the exchange of confidential information between the various member states, as well as between the member states and OLAF. The most significant information received through the AFIS mail are messages of reciprocal subscription that concern Customs researches for cases of frauds that have taken place in some State/Member and they are also likely to take place in other member states. Research guidelines are given to the Customs, the results of which are transmitted to the EU through the system
- The Early Warning System(E.W.S), which is a “pre-briefing” system of the destinating Customs, for the prevention of deviation from the transit of certain sensitive goods (cigarettes, alcohol, etc.) and their entry in the EU grounds without duties and taxes
- The MARINFO system, which concerns exchange of information on the distribution of products (mainly cigarettes, alcohol and narcotic substances) via marine containers.
- The MarSur subsystem, which concerns exchange of information relating to researches on ship transitions.
- The World Base Data Bank which includes the legally functioning companies in world level.
- The CELEX Database which includes the all Community legislation.

Furthermore, in the framework of the CIS enhancement, a new data base of ongoing and completed Member State investigations into customs fraud has been proposed, since the Convention only allowed information exchange regarding established breaches of customs legislation. The new data base, called Customs Files Identification Database (FIDE), only contains information on investigations into serious infringements of customs regulations. "Serious" is defined as a breach "punishable by at least one year in prison or a fine of at least Euro 150000"<sup>19</sup>. This measure enables customs authorities in one Member State to coordinate better with their counterparts in other Member States. Importantly, authorities are able to search a database with a pan-European scope and thus avoid unnecessary duplication of work. Accordingly, this enables authorities to channel their saved time and resources more effectively. The data covers only the following categories:

- a person or a business which is or has been the subject of an investigation file opened by a competent authority of a Member State
- the field covered by the investigation file

---

<sup>19</sup> Council Act of 8 May 2003, Official Journal of the European Union, 2003/C 139/01

- the name, nationality and contact information of the Member State's authority handling the case, together with the file number

In addition, apart from the CIS which is an integrated information system, other subsystems are also under development or have been developed, the electronic data of which can also enforce the data mining subsystem of iWebCare. As such, the following should be included:

- The National Council of Textile Organizations (NCTO) in the U.S. came up with the deployment of the False Claims Act, a powerful, civil anti-fraud statute to Report Fraud Using Online Forms<sup>20</sup>. This online customs fraud reporting system, that started running in the beginning of 2008 includes a one page form that can be filled out online and sent electronically to the NCTO on a confidential basis, while the information is then forwarded to the U.S. Customs.
- SAS has customized a data mining solution which has enabled the national tax authority in Peru to reduce customs fraud and tax evasion by 14 percent<sup>21</sup>.

## 6. RULES & FRAUD DETECTION

As we have already presented in the previous section, the introduction of information systems and formal trans-national procedures in the customs organizations is already mature, and, as a result, **a large amount of imports- and exports- related data has been gathered** and stored at several databases, repositories and systems. Therefore, **the use of advanced, intelligent information technology solutions in the frauds detection in customs is required.**

For example, SAS' data mining solutions have enabled the national tax authority in Peru to reduce customs fraud and tax evasion by 14 percent [SAS]. SUNAT (Superintendencia Nacional de Administración Tributaria) is the government tax collections authority, responsible for administering, collecting and levying duties (including customs tariffs). Ruth Salcedo, SUNAT's IT division manager, said, "The idea to improve results using data mining came at the same time as we merged the tax and customs divisions. By processing both domestic and international information, we could generate a complete profile of taxpayers and foreign businesses. The SUNAT's first project with SAS involved generating profiles of tax evaders and of undervalued imported goods." SUNAT is the first tax and customs organization in Latin America to successfully use data mining in the fight against customs fraud and contraband.

Apart from the usage of information technology in the customs frauds detection (where the iWebCare platform is more than willing and capable to contribute), a number of guidelines, rules and processes should be identified and formally documented in order to support the identification of customs fraud cases.

An indicative (non-exclusive) categorized list of customs fraud prevention rules should include:

<sup>20</sup> <http://www.ncto.org/newsroom/pr20080114.pdf>

<sup>21</sup> <http://www.sas.com/news/preleases/021805/news1.html>

- in the scope of the **assessment of import or export duties and taxes**, the customs frauds identification procedures should focus on the methods of calculation of the initial value of goods and the import tariffs that depend directly on the classification and the origin of goods. Thus, the respective rules should provide adequate support in the prevention and/or detection of fraud cases
  - in respect of the **value of goods**, based on the commercial invoices presented to the customs of the country of exportation and importation, the documentation showing current export or import prices, the declaration of value made on exportation or importation of the goods, the latest trade catalogues and price lists published in the country of exportation or in the country of importation;
  - in respect of the **tariff classification of goods**, based on the analyses carried out to determine the tariff classification of the goods and the tariff description declared on importation or exportation; and
  - in respect of **the origin of goods**, based on the declaration of origin made on exportation and the customs status of the goods in the country of exportation (Customs transit, customs warehouse, temporary admission, free zone, free circulation, exported under drawback, etc.)
  
- in the scope of the **customs control**, the customs services should focus on the authenticity of the products, as well as the lawfulness of the commercial transactions. Therefore, the respective rules should prove:
  - the **authenticity** of official documents produced in support of a declaration of goods made to the customs authorities;
  - the **lawfulness of the importation of goods** into the territory of an EU Member from the territory of another country (EU or non-EU member); and
  - the **lawfulness of the exportation of goods** from the territory of an EU Member into the territory of the another country (EU or non-EU member).
  
- in scope of **smuggling and carousel scheme information provision**, the customs frauds detection procedures should focus on information sharing and circulation regarding persons, their methods and vessels involved in such cases. Thus, the type of information that should be communicated includes:
  - persons finally convicted of smuggling;
  - persons suspected of smuggling or apprehended in the act of smuggling in the territory of the EU;
  - methods of smuggling and other fraud; and
  - vessels involved in smuggling.

At this point, we should identify and short-list the rules and guidelines (included in the above mentioned listing) that could be potentially combined with the iWebCare platform in order to provide an innovative information system that will enable the detection of customs suspicious cases and frauds. We should exclude the customs control rules category, because of the fact that all the listed guidelines involve significant physical presence and their respective business logic cannot be incorporated in an IT system. As a result, the utilization of information technology (and the usage of the iWebCare platform in particular) in customs frauds cases involving forgery of certificates, smuggling goods and the carousel scheme is considered to be inadequate.

On the other hand, a set of rules with regard to the assessment of the initial value of rules, as well as the proper calculation of the tax and tariffs of the importation of goods based on the correct declaration of the origin and the classification of goods could be in-detail specified (including measures and metrics) and integrated in the iWebCare platform (please, see next section of the technical adjustments details) so as to support the identification of suspicious cases and the detection of custom frauds, such as on-purpose misclassifying products, falsely undervaluing imported products, on-purpose misdesignating or misstating the country of origin, and the continuous marking of products as gifts.

Given these guidelines, it is estimated that another 5-10% of the undisclosed annual frauds may come to light. Based on the impact analysed in section 3, given that federal governments loose approximately € 600 billion annually due to customs frauds, it is thus estimated that approximately € 30 - 60 billion will be the annual profit, or the annual decrease of loss for federal governments.

## 7. TECHNICAL ADJUSTMENTS REQUIRED

The designed iWebCare conceptual architecture and ontology-based fraud detection approach (documented mainly in the formal deliverable D03 “iWebCare Overall Architecture and Technical Specifications”) combine a layer of pure software modules implementing the **domain-specific business logic** of the fraud detection services and a persistence layer responsible for preserving all those pieces of **domain-specific information** that are required to be permanent and meaningful in the system.

Although the iWebCare consortium has proposed a high-level, generic framework for the provision of integrated services for the detection of suspicious (either erroneous or fraudulent) data submissions, there is **a number of domain-specific artifacts that should be implemented and maintained**, integrating the respective experts’ domain knowledge in the general-purpose iWebCare fraud detection platform. Thus, the already developed and tested prototype of the iWebCare platform, which is composed by a set of structural software components and conceptual models, **should undergo a series of significant adjustments, extensions and/or customizations** in order to be successfully applied and deployed to the “Customs Fraud Detection” domain.

The technological choices that have been adopted in the development of the iWebCare platform, including (among others) the Service-Oriented Architecture, the Web Services technology, the J2EE software development platform, and the BPEL process orchestration

language, are considered to be adequate for the cross-domain deployment of the integrated fraud detection services. Moreover, the software modules realizing generic, utility like tasks, e.g. user authentication and data encryption, as well as the main iWebCare components, i.e. the Validation Engine and the Self-Learning Engine, which utilize domain-specific rules and datasets for inference purposes, frauds identification and rules evolution, are designed and implemented for cross-domain applicability and will be exploited in other e-government domains with no further customization. On the other hand, the validation-related business logic and services, the semantic models and rules, and the related applications datasets schemes **should meet the respective domain-driven requirements**.

In particular, the following adjustments should take place (in order the iWebCare platform to be efficiently and effectively applied to the “Customs Fraud Detection” domain):

- at the **Persistence Layer**, the existing domain-specific information ontology, which provides conceptually sound metadata for the entities of healthcare domain, as well as the interrelations among them, should be either extended or (even) replaced by another **ontological structure** that will provide **a formal representation and specification of the objects, concepts, and other entities that are assumed to exist in the “Customs” knowledge domain**. The customs-specific ontology should cover the conceptual modelling of the main facets of the domain, i.e. the customs’ structure, organization and procedures, the value-added tax (VAT) issues across the European Union, and the categorization of both goods and services that are shipped among different countries.

Therefore, this customs-specific ontology should enclose the resources listed below:

- the **VAT Topical Ontology**<sup>22</sup> that has been designed in the frame of the FFPOIROT IST project<sup>23</sup> through an analysis of the website of the Taxation and Customs Union<sup>24</sup> of the European Union. The VAT Topical Ontology, which is comprised of 173 terms, 66 roles and 276 lexons, provides the formal modelling of the VAT core-concepts (as derived by the European Union respective website), including classifications of the VAT-related key documents, of the traders and of the consumers, and conceptualization of the VAT routines and procedures, and of the respective control and anti-fraud regulations. Moreover, the VAT Topical Ontology incorporates the Sixth European Council Directive (77/388/EEC) of 17 May 1977 that pertains to the harmonization of the laws of the Member States relating to turnover taxes, proposing rules and definitions of VAT related concepts in order to achieve a common system of value added tax in the European Union.

---

<sup>22</sup> <http://www.ffpoirot.org/Publications/ffpoirot.d2.3.TopicalOntologyVAT-v1.1.pdf>

<sup>23</sup> <http://www.ffpoirot.org/>

<sup>24</sup> [http://ec.europa.eu/taxation\\_customs/common/about/welcome/index\\_en.htm](http://ec.europa.eu/taxation_customs/common/about/welcome/index_en.htm)

- the **DAML version<sup>25,26</sup> or the RDF-S version<sup>27</sup> of the “ontologized” UNSPSC<sup>28</sup>** (standing for the Universal Standard Products and Services Classification Code) that was created when the United Nations Development Program and Dun & Bradstreet Corporation merged (in 1998) their separate commodity classification codes into a single open system, constituting the first coding system to classify both products and services for use throughout the global marketplace. The management and development of the UNSPSC Code is coordinated by ECCMA<sup>29</sup>, the Electronic Commerce Code Management Association. The current version consists of more than 16.000 terms. The codeset is available in English, French, German, Spanish, Italian, Japanese, Korean, Dutch, Chinese, Portuguese, Danish, Norwegian, Swedish, and Hungarian.
  - the **European Union’s customs-specific resources<sup>30</sup>** including the EU Customs Strategy<sup>31</sup>, the organizational and procedural aspects of customs, the calculation of customs duties (both at European and International level) in accordance to the respective rules of origin, and the customs control processes.
- at the **Persistence Layer**, the existing rules information, which refers to metadata about suspicious values or combination of values for the entities of the ontology of the healthcare domain, should be replaced by the customs-specific rule-set. Therefore, **the RSL type declarations and query and validation functions**, which are specified and documented in the formal project’s document entitled “RSL - Rule Specific Language Reference Manual”, **will be further utilized and extended (if required) in the scope of the description of the Customs domain**. Furthermore, the developed “**Fraud Report**” domain should be extended with a “**Customs Report**” sub-domain to support the formal provision of evidences in an identified customs fraud case. Finally, the Customs domain should be populated with a critical mass of domain-specific rules composed by experts, **transforming the qualitative and empirical auditing and validation rules** (that are presented in previous sections of this report) **into machine readable- and - interpretable rules**.

---

<sup>25</sup> <http://www.ksl.stanford.edu/projects/DAML/UNSPSC.daml>

<sup>26</sup> <http://www.daml.org/ontologies/106>

<sup>27</sup> [www.cs.vu.nl/~mcaklein/unspsc/](http://www.cs.vu.nl/~mcaklein/unspsc/)

<sup>28</sup> [www.unspsc.org](http://www.unspsc.org)

<sup>29</sup> <http://www.eccma.org/>

<sup>30</sup> [http://ec.europa.eu/taxation\\_customs/index\\_en.htm](http://ec.europa.eu/taxation_customs/index_en.htm)

<sup>31</sup> Modernised Customs Code (Regulation (EC) No 450/2008) adopted in April 2008

- at the **e-Government Application Layer**, the existing XML Schemas used for the exchange of documents, e-forms and datasets among the iWebCare platform and the involved software applications **should be customized and/or extended to facilitate the customs-specific suspicious data submissions.**
- at the **Web Services Layer**, the **Web Services realizing domain-specific validation tasks**, e.g. submission of data for inspection, submission of rules, submission of entity definitions, submission of erroneous data for training, etc., **should be either customized or even replaced, so as to support the customs-specific fraud identification services.**

## 8. CONCLUSIONS

Summarizing, iWebCare can prove to be a useful tool for the detection of frauds in the Customs, contributing in an approximate € 30 - 60 billion annual profit for federal governments. However, the modifications proposed in Section VI need to be addressed in order for the system to be efficient in this domain. The overall evaluation of the system from the user perspective can be summarized in the following table:

Target	Evaluation (1: Lowest, 5: Highest)					Comments
	1	2	3	4	5	
<b>Functional suitability</b>			X			The technical adjustments explained in Chapter 6 are required
<b>Reliability</b>				X		Significant amount of data need to be fed to the data mining subsystem in order to produce accurate rules. Such data are available (Chapter 4)
<b>Usability</b>				X		The GUI was user-friendly and usable
<b>Efficiency</b>					X	The performance was very satisfactory. The task response time was low.
<b>Interoperability</b>			X			As is the case with the functional suitability, modifications and customizations need to be made for iWebCare to be interoperable with existing systems.