

Distr.: General
13 April 2012

ENGLISH ONLY

Economic Commission for Europe

Inland Transport Committee

Working Party on Customs Questions affecting Transport

**Informal Ad hoc Expert Group on Conceptual and
Technical Aspects of Computerization of the TIR Procedure**

Twentieth session

Prague, 19-20 April 2012

Item 5 of the provisional agenda

Financial implications of the introduction of the eTIR international system

Draft cost-benefit analysis (part 1)

Note by the secretariat

I. Background

1. At its forty-eighth session, further to requests from the Inland Transport Committee (ITC), WP.30 and Informal Ad hoc Expert Group on Conceptual and Technical aspects of Computerization of the TIR Procedure (GE.1), the TIR Executive Board mandated the secretariat to conduct a cost-benefit analysis of the eTIR Project (TIRExB/REP/2011/48final para. 10). Consequently, taking into account the funds available in the TIRExB consultancy budget line and the task to be undertaken, the TIR secretariat requested the relevant services in the United Nations Office at Geneva (UNOG) to issue a tender. In line with the applicable United Nations procurement principles, rules and procedures, UNOG sent out a request for quotes to five companies. Two companies submitted a bid, which were evaluated. Subsequently, the contract was awarded to the qualified bidder whose bid substantially conformed to the requirements set forth in the solicitation documents and who had been evaluated as being most cost-efficient for the United Nations.

2. Considering that the cost-benefit analysis has not yet been finalised and consolidated into a single document, the various chapters are presented independently. The draft cost-benefit analysis is reproduced in the annexes of the following informal documents:

Informal document GE.1 No.6a (2012)	System Architecture alternatives
Informal document GE.1 No.6b (2012)	Costs Analysis
Informal document GE.1 No.6c (2012)	Benefits Analysis and Cost-Benefit Analysis
Informal document GE.1 No.6d (2012)	Executive summary and recommendations
Informal document GE.1 No.6e (2012)	Annex : References and applicable documents

II. Disclaimer

3. All parts of the cost-benefit analysis, including but not limited to the various assumptions on which they are based, are the sole responsibility of the authors and do not necessarily reflect the views of the UNECE secretariat. As yet, the UNECE secretariat's contribution to the analysis has been limited to ensuring that the methodologies required for a successful cost-benefit analysis have been properly applied. Considering that the cost-benefit analysis is still under review and may, possibly, be subject to further amendments, the results presented in the annex should be considered as provisional and as merely intended to brief GE.1 on the current state of play with regard to the issue at stake.

III. Further considerations

4. The GE.1 may wish to consider the part of the cost-benefit analysis as contained in the annex, provide comments or suggestions for its improvement as well as, possibly, formulate first and preliminary recommendations with regard to the most appropriate – or most realistic – option to be pursued.

Annex System Architecture alternatives

United Nations

Economic Commission for Europe

Inland Transport Committee

Project:

Cost Benefit analysis of the eTIR system

Publication reference:

SIVECO Romania SA

Contact address:

SIVECO Romania SA

Victoria Park

73-81. Bucuresti-Ploiesti Drive, Building C4,

District 1, 013685 Bucharest, Romania

Tel: +40 21 302 3300

fax: +40 21 318 1202

System Architecture alternatives

April 2012

Version: Draft-02-41

DRAFT

System Architecture alternatives*

Deliverable: Phase 1: Project Setup

Ref: UNECE-eTIR-CBA-ARCH

Version 02-41 / 12/04/2012 - draft

Delivered by SIVCO ROMANIA SA	Accepted UNECE
Name: Iacob Crucianu	Name: André Sceia
Position: Team Leader	Position: Project Manager
Signature:	Signature:
Date:	Date:

**Deliverable sent to UNECE for Acceptance.*

Revisions

Version	Rev.	Date	Description	Author	Action (*)	Chapter
01	11	07/02/2012	Creation	Iacob Crucianu	I	All
01	21	08/02/2012	Update Comparison between Cloud providers	Iacob Crucianu	I	3.6, 3.7
01	31	10/02/2012	Update comparison between different solutions (architectural alternatives)	Iacob Crucianu	I	3.10
01	41	13/02/2012	Change SaaS schema	Iacob Crucianu	U	3.7.3
01	41-AS	17/02/2012	Remarks on the whole Document	Andre Sceia	C	All
01	51	21/02/2012	Solve remarks received from AS	Iacob Crucianu	U	All
02	21	12/03/2012	Corrections, remove detailed explanations, new architecture schema	Iacob Crucianu	U	All
02	41	11/04/2012	Review	Iacob Crucianu	U	All

(*) Actions: I = Insert, U = Update, D = Delete, M = Merge, C=Comments

TABLE OF CONTENTS

TABLE OF CONTENTS	5
TABLE OF FIGURES	8
0. DOCUMENT CONTROL	9
0.1. Issue Control	9
0.2. Distribution Control	9
1. INTRODUCTION	10
1.1. Overall Objective	10
1.2. Purpose of the eTIR-CBA	10
The purpose of the eTIR-CBA Architecture Alternatives	12
2. SOLUTION	13
2.1. Introduction	13
2.2. eTIR Objectives and boundary	14
2.2.1. eTIR Objectives	14
2.2.2. Boundary of the eTIR Project	15
2.3. Technical Characteristics	17
2.3.1. Centralized approach	17
2.3.2. Web-based system, online data entry	17
2.3.3. Service Oriented Architecture (SOA)	18

2.3.4. Data exchange using XML and Web Services	18
2.3.5. Integration with third party applications, in particular reporting tools	18
2.3.6. Reusability of data	19
2.3.7. Scalability	19
2.3.8. System Performance	19
2.3.9. High availability	20
2.3.10. Reliability and stability	20
2.3.11. Expansibility, configurable at runtime	21
2.3.12. General technical requirements	21
2.4. The eTIR international context	21
2.5. Conceptual architecture	23
2.5.1. Solution Security Layer	24
2.5.2. Software infrastructure, IT Management, Monitor, Audit Layer	24
2.5.3. Access Layer	25
2.5.4. Kernel Layer	26
2.6. Logical architecture	30
2.7. Solutions Overview	32
2.8. Clouds for eTIR	32
2.8.1. Clouds definitions[1]	32
2.8.2. Clouds implementations	33
2.8.3. Clouds alternatives[1][3][6][7]	34
2.9. New hardware and software environment	38
2.10. Hosting the eTIR system at the premises of other IT systems	40
Solution Comparison.	41
2.10.1. Explanations regarding categories	41
Annexes	46

DRAFT

TABLE OF FIGURES

FIG 1.	STAKEHOLDERS AND ACTORS[R1]	16
FIG 2.	ETIR INTERNATIONAL CONTEXT.....	22
FIG 3.	ETIR CONCEPTUAL ARCHITECTURE.....	23
FIG 4.	ETIR LOGICAL ARCHITECTURE.....	31
FIG 5.	CLOUDS DEFINED BY NIST[1]	33
FIG 6.	ETIR IN IAAS	35
FIG 7.	ETIR IN PAAS	37
FIG 8.	HOSTING ETIR AT OWN PREMISES	39

DRAFT

0. DOCUMENT CONTROL

0.1. ISSUE CONTROL

This document has been issued by:

- SIVCO Romania SA,

This document refers to SIVCO Romania SA in the present document as **SIVCO** and to the current project, the Cost Benefit Analysis of eTIR, as **eTIR-CBA**.

This document is to be reviewed by UNECE and accepted.

0.2. DISTRIBUTION CONTROL

Copy No.	Name	Project Title	Company
X01	File Copy	Original Master	SIVCO Project Office
X02	Andre Sceia	Project Manager	UNECE
X03	Artur Bouten	Alternate Project Manager	UNECE
X04	Dan Tuhar	eCustoms Director	SIVCO
X05	Iacob Crucianu	Team Leader	SIVCO

1. INTRODUCTION

1.1. OVERALL OBJECTIVE

The overall objective of the eTIR-CBA project is to analyze, from a technical and financial perspective, the technical options for the implementation of the eTIR system.

The first step in accomplishing this objective is the definition of architectural alternatives, which is the subject of the present document.

1.2. PURPOSE OF THE ETIR-CBA

The purpose of the eTIR-CBA is to realize a cost benefit analysis of several possible alternatives for the implementation of the eTIR system.

The eTIR-CBA Project will achieve the following:

- **Present several alternatives for the hardware and software architectures that can be used in the eTIR system. The present document wants to reach this achievement.**
- **For each proposed architecture, analyze the strong points and the weak points. The perspectives used to analyze will be (see &3.10):**
 - **24/7 Reliability (Uptime is Imperative);**
 - **Performance;**
 - **Security;**
 - **Scalability;**
 - **Availability / Access From Anywhere;**

- **Flexibility & Customization;**
- **Mental Blocks / Culture;**
- **Maturity of technology**
- **Administration.**

The next steps of the present project will achieve:

- For each proposed architecture, evaluate costs:
 - TCO (Total Cost of Ownership) for the owner of the system;
 - Costs for Customs authorities;
 - Costs for the Trader community;
 - Other costs.

The costs will be analyzed for two scenarios:

- Step-by-step implementation over a longer period of time;
- One step implementation for all actors involved.
- For each proposed architecture, evaluate benefits:
 - Direct benefits;
 - Indirect benefits.

The benefits will be analyzed for two scenarios:

- Step-by-step implementation over a longer period of time;
- One step implementation for all actors involved.
- Make a hierarchy of proposed alternatives from a technical and a financial point of view.
- Summarize all the previous aspects in:
 - Recommendations document;
 - Non-technical Executive Summary document.

THE PURPOSE OF THE eTIR-CBA ARCHITECTURE ALTERNATIVES

The use of the Architecture Alternatives Chapter is to present:

- Technical requirements of the system;
- Conceptual architecture of the system;
- Logical architecture of the system;
- System architectural alternatives;
- Strong and weak points of each alternative;
- Comparison matrix of the envisaged solutions, based on 10 criteria.

DRAFT

2. SYSTEM ARCHITECTURE ALTERNATIVES

2.1. INTRODUCTION

This chapter presents different architectures that could be envisaged for the implementation of the eTIR international system. This document does not present use cases, processes and activity diagrams as they are described in detail in the eTIR Reference Model v3.0 [R1-R5]. It is assumed that the system will cover ALL the functionalities described in the eTIR Reference Model v3.0.

This Chapter is organized as follows:

First, we recall the eTIR objectives and boundaries, as contained in the eTIR Reference Model v3.0. Then, we present the technical requirements that have been taken into account for the eTIR-CBA.

This is followed by the conceptual architecture, which is based on four system tiers (Security, Management, Access, Kernel) and is independent of any hardware and software platform. In continuation, we introduce the logical architecture, in which all main logical components are presented.

Starting with the conceptual and logical architecture, we formulate proposals for two main categories of system solutions:

- Solutions based on clouds: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as Service (SaaS);
- Solutions based on the implementation at Premises (Premises) (either in a new environment or by means of using an existing environment).

For architectures based on clouds, a technical comparison is made between the three main cloud providers: Amazon, Google and Microsoft.

Finally, a technical comparison of the various architectural alternatives is made.

The document does not refer to the system workload, as this will be the subject of the next documents of the costs analysis.

2.2. eTIR OBJECTIVES AND BOUNDARY

2.2.1. eTIR Objectives

According to what has been established in the eTIR Reference Model [R1-R5], the objectives of eTIR are described below:

The final objectives of the eTIR Project are:

- Integrating the computerized TIR procedure in the overall process of technological development in international transport, trade and Customs procedures:
 - Simple and cost effective data capture and data transmission;
 - Facilitation of global intermodal application of the TIR Procedure;
 - Real time exchange of information among actors;
- Improving the efficiency and quality of the TIR procedure:
 - Reduction of processing times at border crossings and final destination;
 - Increased efficiency of internal administrative and control procedures;
 - Increased accuracy and reduction of errors;
 - Reduction of costs;
 - Progressive replacement of paper TIR Carnet;
 - Full use of international standard codes in order to eliminate language barriers;
 - Availability of advance cargo information;

- Reducing the risk of fraud and improving security:
 - Automatic generation of data for risk assessment;
 - Facility to implement early-warning system;
 - Easy access to information for control and risk management purposes.

2.2.2. Boundary of the eTIR Project

The final objective of the eTIR project encompasses the computerization of the whole TIR Carnet life cycle (from issuance and distribution via the TIR transport to return and repository) and is ultimately aimed at replacing the current paper TIR Carnet. However, the eTIR Project will inevitably have repercussions on other parts of the TIR Procedure. Therefore, it is important to identify the boundaries of the project in order to realize the full impact the project may have and to ensure that the views of all stakeholders are taken into due account. The boundaries are defined along two axes: stakeholders and information.

2.2.2.1 Stakeholders

A stakeholder is defined as someone (or something) who is materially affected by the outcome of the system but may or may not be an actor of the system. Actors are stakeholders who are involved in the specific project as users and are thus part of the Reference Model. Stakeholders inside the boundary of the system are involved in the project as active participants in the work and/or members of decision-making bodies; those outside the boundary may participate in meeting to ensure any future compatibility where necessary.

Figure 1 shows the stakeholders inside and outside the boundaries of the project and emphasizes those who are also actors.

Stakeholders and actors

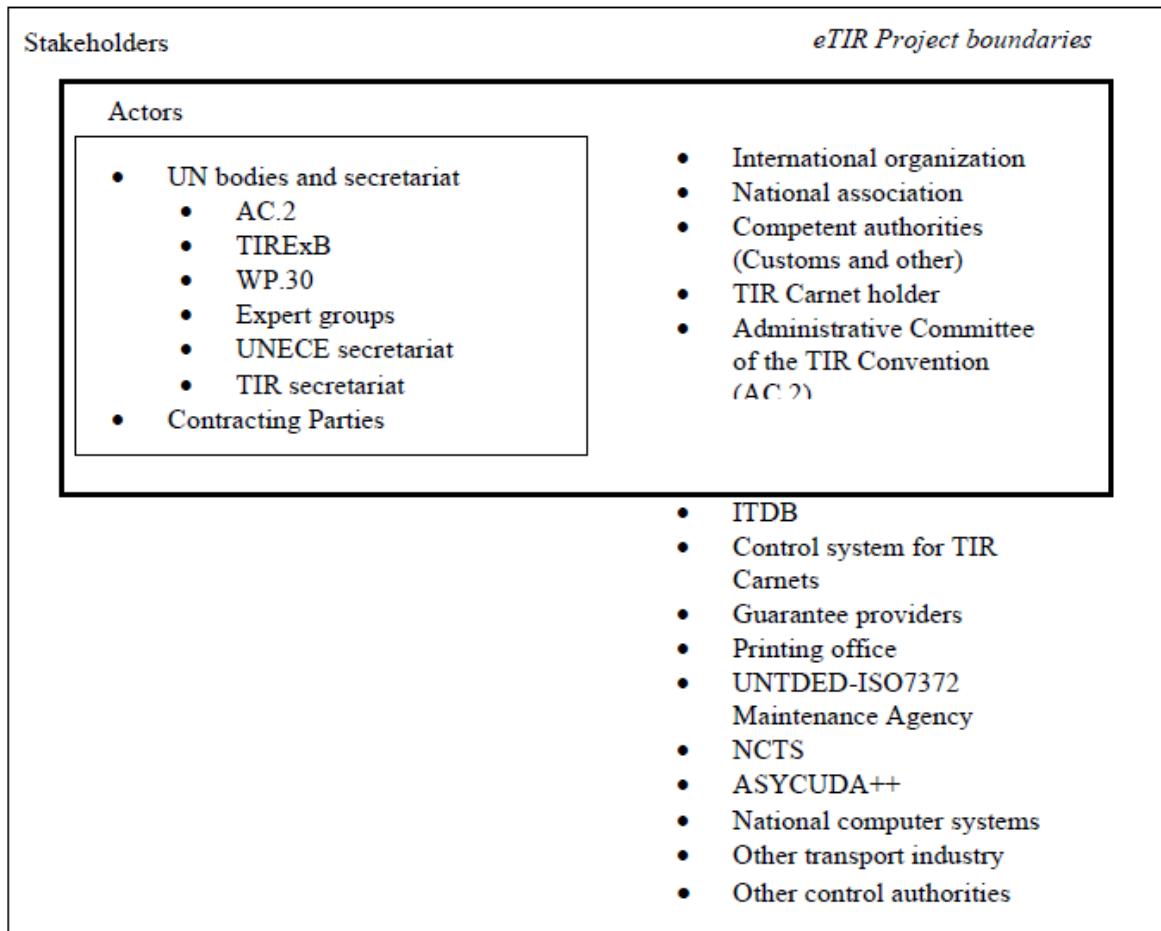


Fig 1. Stakeholders and actors[R1]

2.2.2.2 Information

The data elements inside the boundaries have been identified and are listed in Annex 3 of the eTIR Reference Model. These data elements reflect the information contained in the current, paper-based, TIR Carnet and provide the basis for the elaboration of a minimal set of data to be computerized.

2.3. TECHNICAL CHARACTERISTICS

2.3.1. Centralized approach

The eTIR international system will be fully centralized, both from a data and application point of view. Centralization of data will be accomplished by:

- Storage of all main information in only one central database;
- Access to external modules via a single communication interface, based on XML format.

Centralization of application will be accomplished by:

- Development of a dispatcher mechanism, used to orchestrate message exchange between actors involved (mainly Customs administrations). Exchange of messages will be done using web services. Both the synchronous and asynchronous mode will be used. In synchronous mode, notifications of data reception will be sent in response to a message. In asynchronous mode, more complicated notifications or messages will be sent as a result of status change of a document;
- Development of a web based system, with clients on web browsers used to view or update data. View of data will be accessible any time, under any circumstances. Process data in a web based centralized system will be possible as a fallback procedure, when the systems linked in the Service Oriented Architecture (SOA) environment do not work properly, or for situations when such systems do not provide a good data entry mechanism.

2.3.2. Web-based system, online data entry

The eTIR international system will be fully WEB based. It will follow J2ee or .NET organization. The servers will be J2ee servers, or Microsoft .NET.

Clients will be:

- Customs IT applications, connected to the eTIR central system using web services;

- Web browsers or smart clients accessing the main server, for data view or fallback procedures.

2.3.3. Service Oriented Architecture (SOA)

Service-Oriented Architecture (SOA) is defined as “the policies, practices and frameworks that enable application functionalities to be provided and consumed as sets of services published at a granularity relevant to the service consumer.

Services can be invoked, published and discovered and are abstracted away from the implementation by means of using a simple, standard-based forms of interface.”

The eTIR architecture will be compliant with the above definition of SOA. Web-services protocols will be “standard-based forms of interface” for eTIR. The eTIR functionality that is deemed to be of interest to other applications from Customs, from the External Domain or from other Government Agencies will be exposed at appropriate granularity levels via standard-based interfaces. New software applications (even in the next 10 or 20 years) will be able to consume these services and integrate with the eTIR international system because their interfaces are based on standards and are not proprietary.

2.3.4. Data exchange using XML and Web Services

Data exchange will be possible in the following ways:

- **Web Services: users (IT systems of national/regional Customs administrations) use web service to exchange data with the eTIR international system.**
- **Web application: users (Customs officers) access the eTIR international system by means of a secure web application that allows them to view and change data (according to roles). This option is mainly envisaged as a fallback solution**

2.3.5. Integration with third party applications, in particular reporting tools

The system will have also a layer of **web services** offering data to external modules.

2.3.6. Reusability of data

Data will be registered by each Customs administration which will be the owner and the responsible entity for it.

All exchanged messages will also be stored in the central eTIR international system with their full history.

2.3.7. Scalability

The system will have a completely scalable architecture, both horizontally and vertically. The system will be able to handle larger volumes of data and users in a cost-effective manner by adding more processors and/or memory to the existing machines or by employing multiple servers without changes in the application code or general architecture.

The system will be modular and be prepared to be implemented in a scalable environment.

To cope with larger numbers of users or increased calculation complexity, the system should also be able to scale with only configuration changes and/or additional hardware.

2.3.8. System Performance

The response time of the application will be closely monitored and optimized throughout all phases during the system life cycle.

The system will have the capability to handle an unlimited number of registered users.

This will be achieved using an extensible user management solution, either a Lightweight Directory Access Protocol (LDAP) or a customized security module, neither having any limitations in the number of users that can be stored.

To address the problem of concurrent sessions, the application will use software clustering on the existing hardware to improve availability and scalability. Similar application solutions have shown to support an almost linear dependency between the number of cluster nodes and the number of supported concurrent sessions.

The system should provide acceptable data exchange response times. For Customs-to-Customs (C2C) connections, in synchronous mode, the response time should be less than 1 second;

The system should provide acceptable screen response times in case the web user's interface is used (less than 3 seconds per page view during normal working hours, and less than 5 seconds per page view at peak time). Peak hours will be established depending on the maximum number of operations at a specific hour. Considering the actual statistics, peak time will be considered for time zones between GMT+1 (Central Europe) and GMT+3(Russia).

2.3.9. High availability

The application will be designed to allow all the tiers to run on clustered hardware and be deployed on a virtual cluster of one node. This will allow clustering without changing the application code.

The system is considered to be a mission critical application and, thus, should be 99.99% available. For calculation purposes, the maximum allowed downtime will be 1 hour per week.

2.3.10. Reliability and stability

The system should support advanced mechanisms to ensure reliable data delivery and processing, such as durable topics, local transactions, message expiration and acknowledgement.

- The system should support an initial capability of 80 concurrent system to system connections, exchanging data by means of using web services (68 possible Customs systems, plus possible other actors and a reasonable free number of connections);
- The system should support an initial capability of 1000 concurrent users accessing the web interface. The web user interface is developed as an alternative for a C2C system, for situations such as fallback procedures, or in case Customs systems do not yet provide sufficient services for the electronic treatment of TIR Carnets.

2.3.11. Expansibility, configurable at runtime

Modules can be easily added, with or without minimal changes in the current architecture. Also because of the common Application Programming Interfaces (API) used: Simple Object Access Protocol (SOAP), Remote Method Invocation (RMI), Java Naming and Directory Interface (JNDI), etc. Third party software will be able to integrate seamlessly.

2.3.12. General technical requirements

Below follows a list of general technical requirements that need to be met by the eTIR international system:

- Unicode compliance;
- For all documents: history of operations as well as owner of the document will be stored in the database.

2.4. THE eTIR INTERNATIONAL CONTEXT

The eTIR international system is a centralized system, which will be responsible for data exchange between the IT systems of different national Customs administrations

Data exchange will be possible via two channels:

- Via web services. There will be system-to-system connections between national Customs administrations and the eTIR international system;
- On a web interface (usually on https) where users enter and view data in a web user interface. This is mainly designed for fallback procedures.

The relation between the eTIR international system and other IT systems is presented in the figure below:

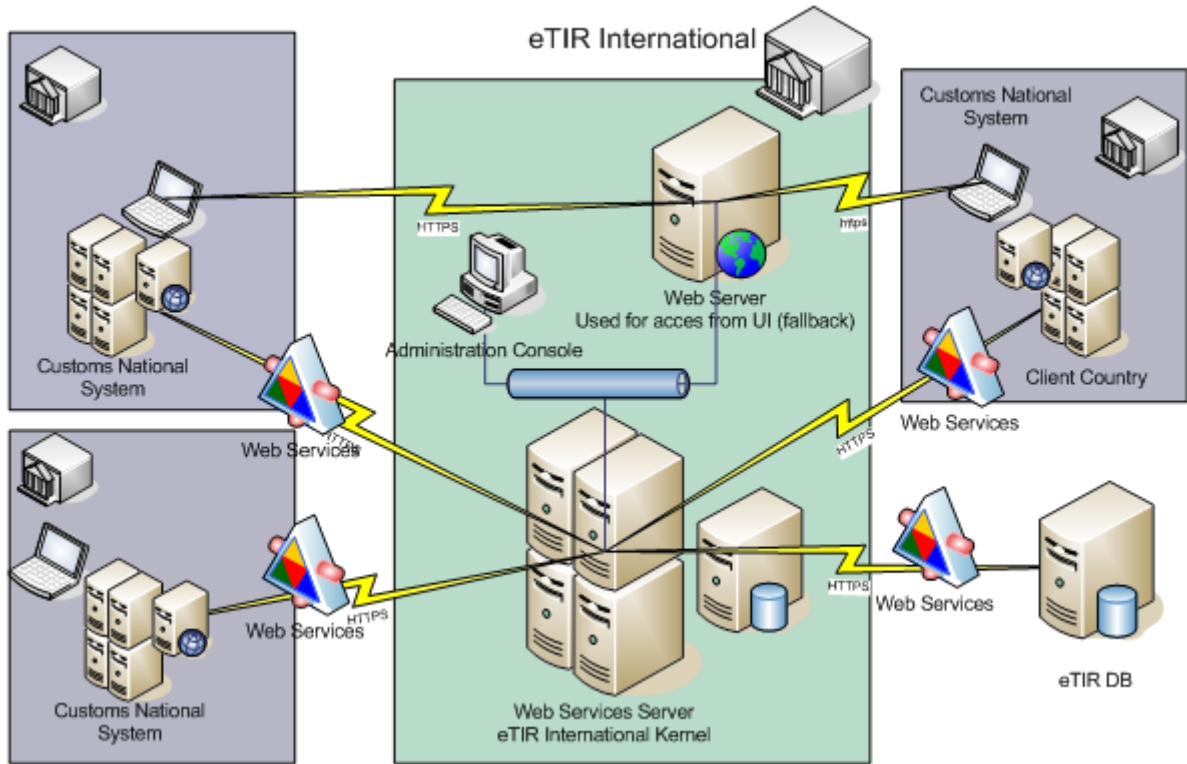


Fig 2. eTIR international context

2.5. CONCEPTUAL ARCHITECTURE

The eTIR system will integrate several multi-tier architecture systems in a global SOA concept. Each particular system will have a very well-defined functionality and will work both integrated, in the global SOA architecture, and separately, as a stand-alone application.

The conceptual architecture, presented in the figure below, is built up of several layers:

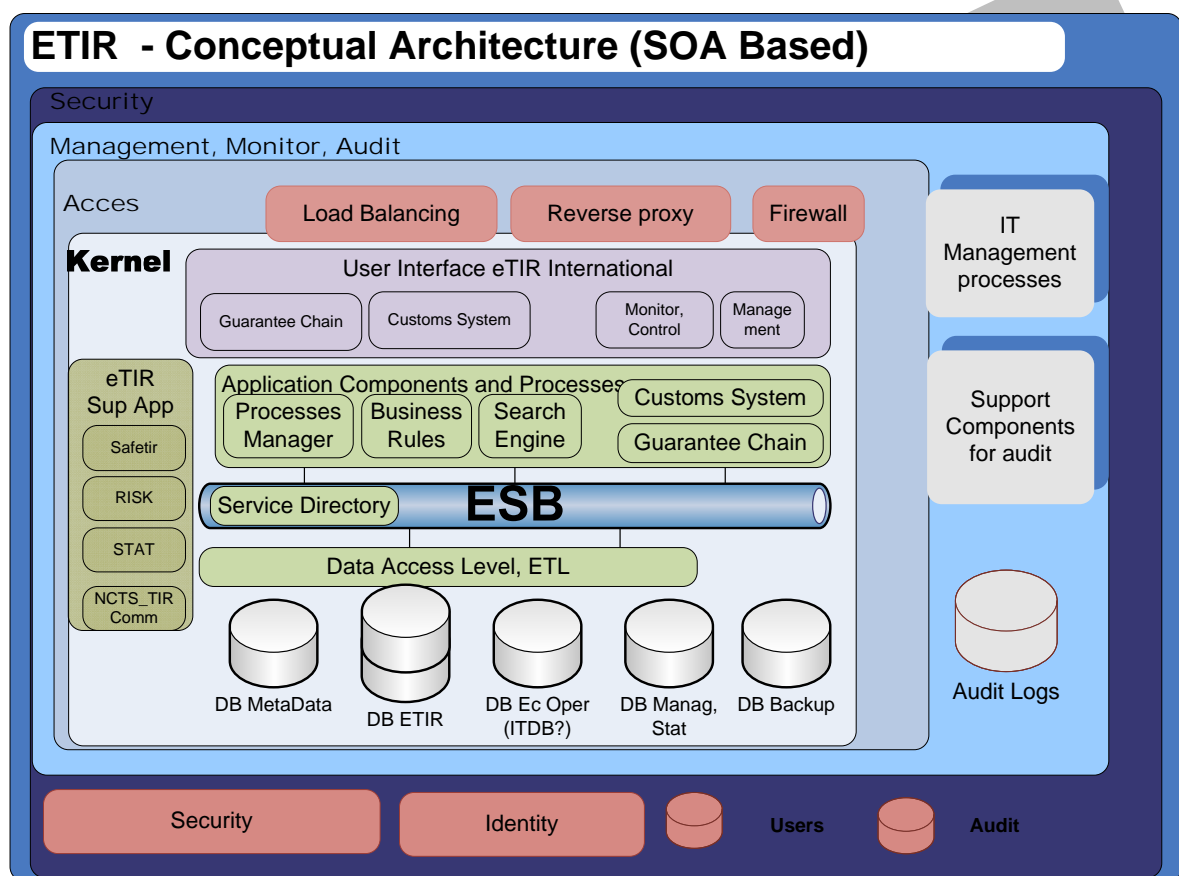


Fig 3. eTIR Conceptual Architecture

The following main layers are considered:

- Solution Security Layer;
- Software infrastructure, IT Management, Monitor, Audit Layer;

- Access Management and Load Balancing Layer;
- Kernel Layer.

2.5.1. Solution Security Layer

Due to the fact that, in any modern application, security is paramount, a complex security solution will be implemented, which will ensure data confidentiality in each application layer (Cross-layer security). All access information will be stored in a central repository, which will be implemented either as a Customs secure repository implementation or using LDAP.

The security system will implement both data security and functional security.

The application will be compliant with EU regulation EU 1663/95 and will follow the directives stated in ISO Standard No. 17799.

The application will use the principle of Single Sign-On and, once a user is authenticated, he will not be required to re-enter his credentials during the on-going session.

Data sent via Web Services will be signed and encrypted, using a private public pair key. Access to web services will be allowed only for well-known secured IPs. Firewalls and reverse proxy will protect systems from unauthorized access.

2.5.2. Software infrastructure, IT Management, Monitor, Audit Layer

IT Management, Monitoring and Auditing systems will be set up in order to avoid potential problems of the system in reporting incomprehensible or incoherent errors.

Two main aspects will be considered:

- The management and monitoring of Software systems;
- Error treatment.

2.5.2.1 Management and monitoring

A comprehensive, integrated management solution that helps businesses achieve high levels of performance and availability and reduce the costs of managing applications is required. This should, proactively, monitor the health of all application components, the hosts that they run on and the key business processes that they support.

Besides monitoring and diagnostics, management of the configuration of application environments through its integrated configuration management tool is also required. Management will include:

- Ensuring performance and availability;
- Resolving problems quickly if they occur in order to minimize their impact;
- Containing the on-going costs associated with managing the applications;
- Aligning IT and line-of-business priorities so that the resources are deployed towards those activities which generate the greatest benefits for business.

2.5.2.2 Error detection and recording

Errors, displayed to the system users, will have defined error types identified by appropriate numbers. Additionally, each error type reported by the application will be recorded with a unique number, enabling its identification by the system administrator.

The application will provide detailed error handling regarding two types of errors that may occur: business and application errors.

2.5.3. Access Layer

The Access Layer will be based on Application Server components and clusters. Also at the access layer, the following is necessary:

- Web server load balancing - to load-balance transactions to the least-highly-loaded HTTP server (HS);

- Cluster instance load balancing;
- Automated Storage Load balancing. Shared disk storage resources can alternatively be assigned to individual databases and easily be moved from one database to another as processing requirements change;
- Data Guard Load Balancing - load balancing between standby databases.

2.5.4. Kernel Layer

The **Kernel Layer is responsible for the business process in the eTIR international system.** It is also composed of several tiers:

UI (Presentation) Tier;

Application Tier;

Persistence Tier.

The **UI (Presentation) Tier** contains the user interface and is responsible for the interaction between the end user and the application. The client will use a standard Web Browser (Microsoft Internet Explorer, Mozilla Firefox, Apple Safari, Opera, etc.) to interact with the application. Every modern operating system has a Web Browser, so no additional software will be needed in order to use the application. On the server side, this tier will be composed of a Web Server, which will serve the static content and will act as a reverse proxy for the Application Server. It should be noted that the presentation tier will follow the Single Access Window concept. This allows users to use the same entry point for data in all system modules.

This User interface is for fallback procedure, as the main functionality of the system is based on data exchange via web services.

The **Application (Middle) Tier** will encapsulate the application logic and behavior and will be based on a standard JEE application server or .NET application Server.

The proposed application server is able to run in a clustered environment and to load balance requests to all the nodes, share state information between nodes and recover from server failure.

The **Persistence Tier** is responsible for data storage and retrieval and will be a Relational Database Management System (RDBMS) instance.

2.5.4.1 Presentation Tier

The presentation tier contains the user interface and exposes the services of the system to the user. The client will access the application using a standard Web Browser, which will require JavaScript.

The HTML pages displayed by this tier will be generated in the application tier. Simple validation will be carried out on the client side (through a browser using JavaScript), but the final data validation will be done in the application tier.

For security reasons, some, or all, communications will be done through HTTPS, a protocol which adds a layer of Secure Socket Layer (SSL) encryption over standard HTTP. The use of this protocol will ensure confidential communication between the server and the client.

The web application will use a single point of authentication. The user will be authenticated only once per session. The user interface is generated dynamically and the user will see and have access only to the functionalities for which he is authorized.

2.5.4.2 Application (Middle) Tier

The Application Tier is divided into two distinct but interconnected parts: the domain logic and the application logic. The domain logic models the processes of the business, while the application logic models the aspects of this software implementation.

The domain logic will be implemented using simple domain objects and business objects. The domain objects will be simple objects, which do not contain any business logic; they merely hold the state of the application. These domain objects will be shared between the three layers of the application. The business objects will

encapsulate the business rules and are responsible for the business logic. The core business logic will be encapsulated in packages and Java distinct classes, which will allow a consistent implementation across the different modules and promote code re-usability.

The application logic boundary will be defined using a Service Layer, a layer of services that establishes a set of available operations and coordinates the application response to each operation. The service layer will coordinate the persistence.

In this way, the modules could work in a SOA environment, as orchestrated services or as a choreography established by the process manager. They could also work separately, with very well-defined functionalities, to couple to the SOA architecture, when necessary.

The Application Tier will contain the business logic for the following modules:

- eTIR Main business:
 - eTIR transport (registration and exchange of declaration information)
 - eTIR operations;
 - Enquiry and recovery;
 - Reference data and authorizations.
- Guarantee management.
- Management and monitoring modules:
 - Management and administrations;
 - Monitoring system;
 - Knowledge base.
- eTIR Sub modules:
 - SafeTir communications;
 - NCTS_TIR data exchange module;
 - Reports, Statistics.

- Connectivity to the ITDB. This might be a submodule to be developed.

2.5.4.3 Persistence (Data Source) Tier

This tier will be responsible for storing and retrieving the data processed by the Business Tier. The data will be stored in an RDBMS database. The database should be compatible with the platform chosen, such as, for instance, Oracle Database. But in a cloud of type PaaS (Platform as a service), other options are available, like Microsoft Azure. The business layer will access the data source tier through the persistence layer located in the Business Tier.

The database should offer centralized administration and built-in validation, data protection and disaster recovery facilities, through the use of standard management tools.

Employing data constraints like foreign keys, unique keys and field constraints will ensure information integrity. The database should support internationalization and will use the UTF-8 Character set, which provides support for almost any alphabet and language.

The database should refer to the following logical components:

- DB Metadata – will contain the metadata used to define all configurations of the eTIR international system. Also reference tables will be stored there;
- DB eTIR – will contain the main data used by the eTIR international system. Messages received via web services or sent via web services, with all history and accompanying information, will be stored there;
- DB Ec Operator – will contain information about TIR Carnet holders. It is recommended to use the International TIR Database (ITDB), but if this tool is not available online, it is recommended to use a local database for this purpose;
- DB Management and Statistics – this will be a staging database used to store data for Data Warehouse purpose, reports, statistics;
- DB Backup – this will be a staging database used for backups.

In order to integrate different data sources, a Data ETL (Extract, Transform, Load) module will be available.

2.6. LOGICAL ARCHITECTURE

The components described in the conceptual model could logically be grouped, based on their main functionality, in:

- **eTIR international kernel. (called also eTIR kernel)**

This part is responsible for:

- business logic implementation,;
- communication management using web services or web access,;
- data persistence;
- public interfaces to other modules or systems;

- **eTIR user interface**

This part will be responsible for data viewing and processing, via a web user interface.

It will call processes defined in the eTIR kernel and will be used mainly as a fallback procedure, when system-to-system communications between the eTIR kernel and other participants in the eTIR life cycle will not work properly.

- **eTIR administration console**

This part has functions for system administration and monitoring. It will be used by the system administrator to manage users, roles, and reference data, to monitor system functionality and to audit the processes.

The distribution of logical components and the relation with external interfaces is presented in the figure below.

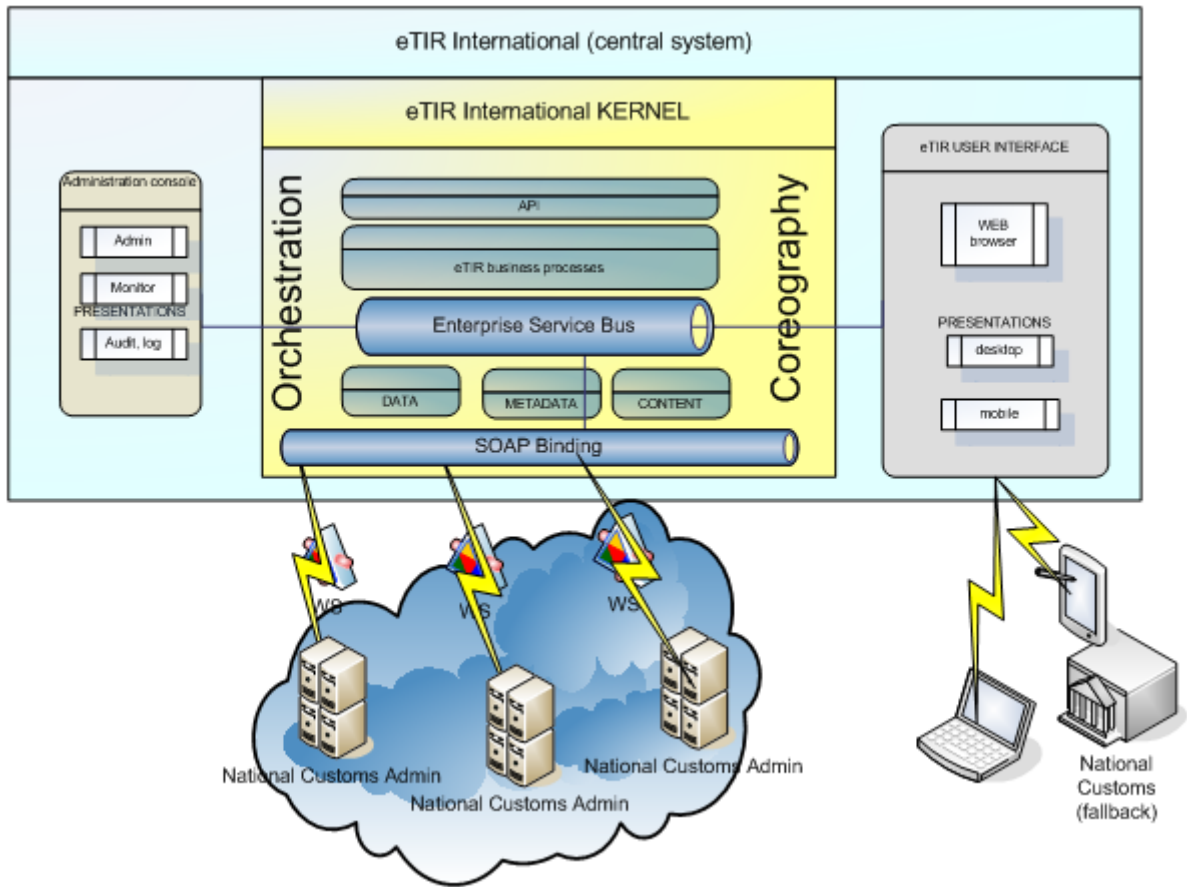


Fig 4. eTIR logical architecture

2.7. SOLUTIONS OVERVIEW

This section presents the envisaged solutions. Based on the efforts already made in the eTIR Reference Model V3.0, it was established, during the inception phase, that the analysis will include the main architectural alternatives.

Three major alternatives, each one with several options will be considered in the evaluation of the cost-benefit analysis:

- Implementation using cloud computing concepts (described below in Chapter 3.7):
 - a. Infrastructure as a Service (IaaS);
 - b. Platform as a Service (PaaS);
 - c. Software as a Service (SaaS);
- Hosting all hardware infrastructure, hardware systems and software systems at the premises of the owner of the eTIR system and using a completely separate environment ('Premises', described in Chapter 3.8).
- Implementation using cloud computing concepts by hosting the eTIR system at the premises of other IT systems ('UNICC/UNOG', described in Chapter 3.9). This alternative is similar to IaaS or PaaS, but the infrastructure or the platform will be provided by a third party, e.g. UNOG (United Nations Office at Geneva) or UNICC (United Nations International Computing Center);

The next Chapters will present a detailed description of all alternatives to be considered.

2.8. CLOUDS FOR ETIR

2.8.1. Clouds definitions[1]

As defined by American National Institute for Standards and Technology (NIST),

“Cloud computing is a pay-per-use model for enabling available, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. “

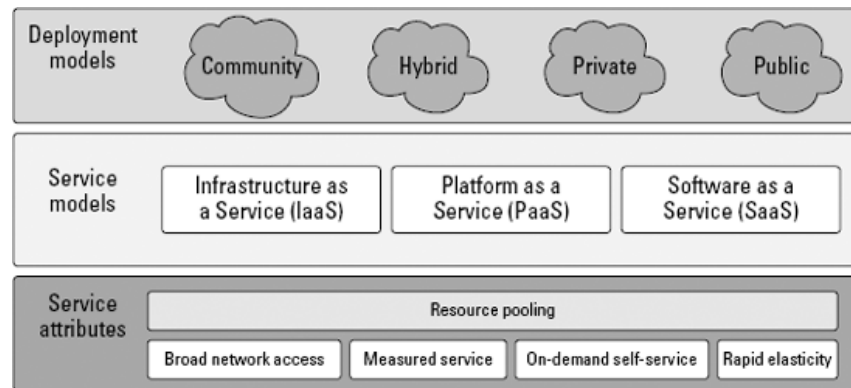


Fig 5. Clouds defined by NIST[1]

2.8.2. Clouds implementations

There are several implementations of the concept of cloud computing. Mainly they could be categorized in:

- *Private cloud.* The cloud infrastructure is owned or leased by a single organization and is operated solely for that organization;
- *Community cloud.* The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations);
- *Public cloud.* The cloud infrastructure is owned by an organization selling cloud services to the general public or to a large industry group;
- *Hybrid cloud.* The cloud infrastructure is a composition of two or more clouds (internal, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting).

Each deployment model instance has one of two types: internal or external.

Internal clouds reside within an organization’s network security perimeter and external clouds reside outside the same perimeter.

This will be the first architectural option described and analyzed.

2.8.3. Clouds alternatives [1][3][6][7]

When discussing alternatives for clouds, the following sub-alternatives will be presented:

- Infrastructure as a Service (IaaS);
- Platform as a Service (PaaS);
- Application as a Service (AaaS) or Software as a Service (SaaS).

The proposed implementation of the eTIR international system by means of clouds alternatives will have the following characteristics:

2.8.3.1 Infrastructure as a Service (IaaS)

For this alternative:

- The hardware and infrastructure are owned and maintained by a **cloud provider**. (for example: Amazon). For the purpose of this analysis, a private cloud is necessary (dedicated hardware owned by a cloud provider and used only by UNECE). The costs are per usage of data storage, processor operations and network traffic;
- Platforms are owned, installed, configured and maintained by **UNECE**;
- The eTIR international system is developed, owned, installed, configured and maintained by **UNECE**;

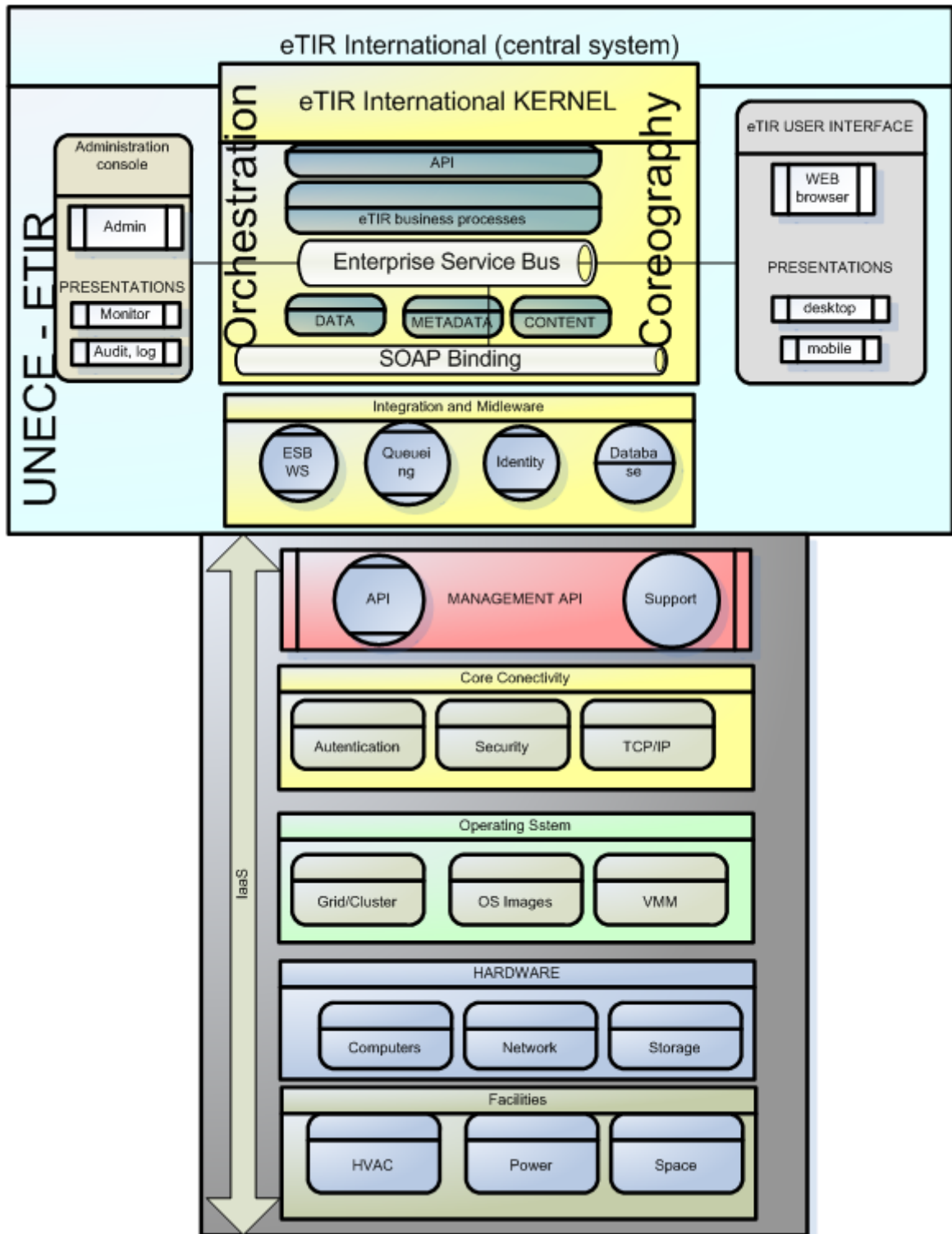


Fig 6. eTIR in IaaS

2.8.3.2 Platform as a Service (PaaS)

For this alternative:

- The hardware and infrastructure are owned and maintained by a **cloud provider** (for example: Google or Microsoft). The cloud should be a private cloud (dedicated hardware for UNECE usage only);
- Platforms are owned, installed, configured and maintained by a **cloud provider. Platforms are defined by UNECE.** The costs are per usage of data storage, processor operations and network traffic;
- The eTIR international system is developed, owned, installed, configured and maintained by **UNECE**;

DRAFT

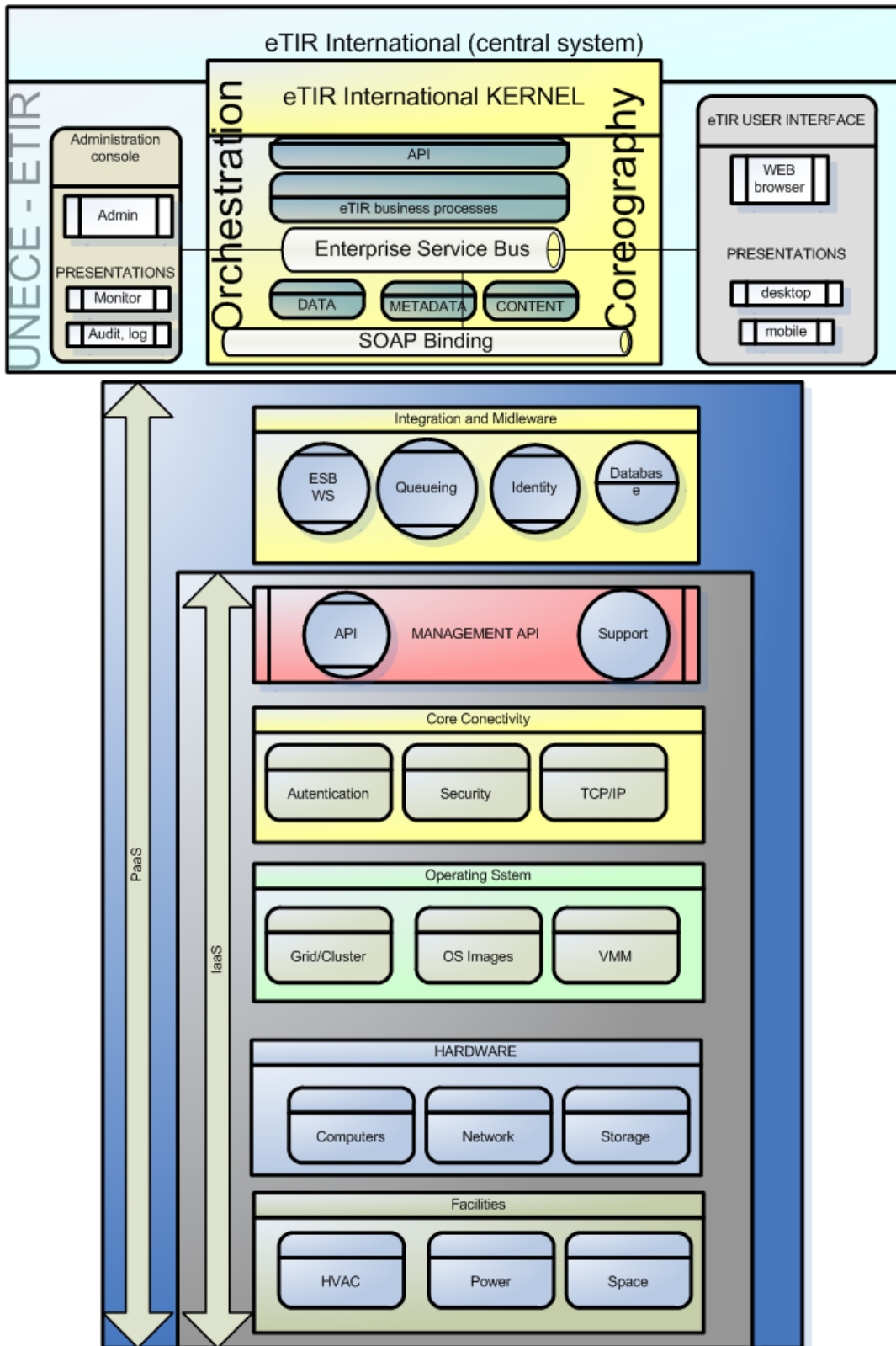


Fig 7. eTIR in PaaS

2.8.3.3 Software as a Service (SaaS)

For this alternative:

- The hardware and infrastructure are owned and maintained by a **cloud provider** (for example: a private company able to develop Customs software services). The cloud should be a private cloud (dedicated hardware for UNECE usage only). It might also be obtained from another provider, like for PaaS or IaaS;
- Platforms are owned, installed, configured and maintained by a **cloud provider**;
- The eTIR international system is developed, owned, installed, configured and maintained by a **cloud provider contracted by UNECE according to strict criteria and conditions**. The costs are per guarantee;

From an architectural point of view, the implementation is similar to the at premises alternative. The big difference resides in the fact that at premises everything (hardware, software) is owned, maintained and operated by UNECE, whereas in SaaS everything (hardware, software) is owned, maintained and operated by the SaaS provider.

2.9. NEW HARDWARE AND SOFTWARE ENVIRONMENT

This option considers building the whole system from scratch: from building space, facilities, up to the eTIR software system.

The architecture considers a fully web-based centralized system, accessible from any place. High availability, scalability and high performance are the most important requirements for such a system.

For this alternative:

- The hardware and infrastructure are owned and maintained by **UNECE**;
- Platforms are owned, installed, configured and maintained by **UNECE**;

- The eTIR system is developed, owned, installed, configured and maintained by **UNECE**;

For this alternative, the following items will be taken into account:

- Infrastructure (buildings, heating, power supply, facilities, backups, etc);
- Hardware environment (computers, networks);
- Software environment (operating systems, databases, frameworks, monitoring systems);

All expenses for buying, installing and maintaining the components will be considered.

The architecture is presented in the figure below

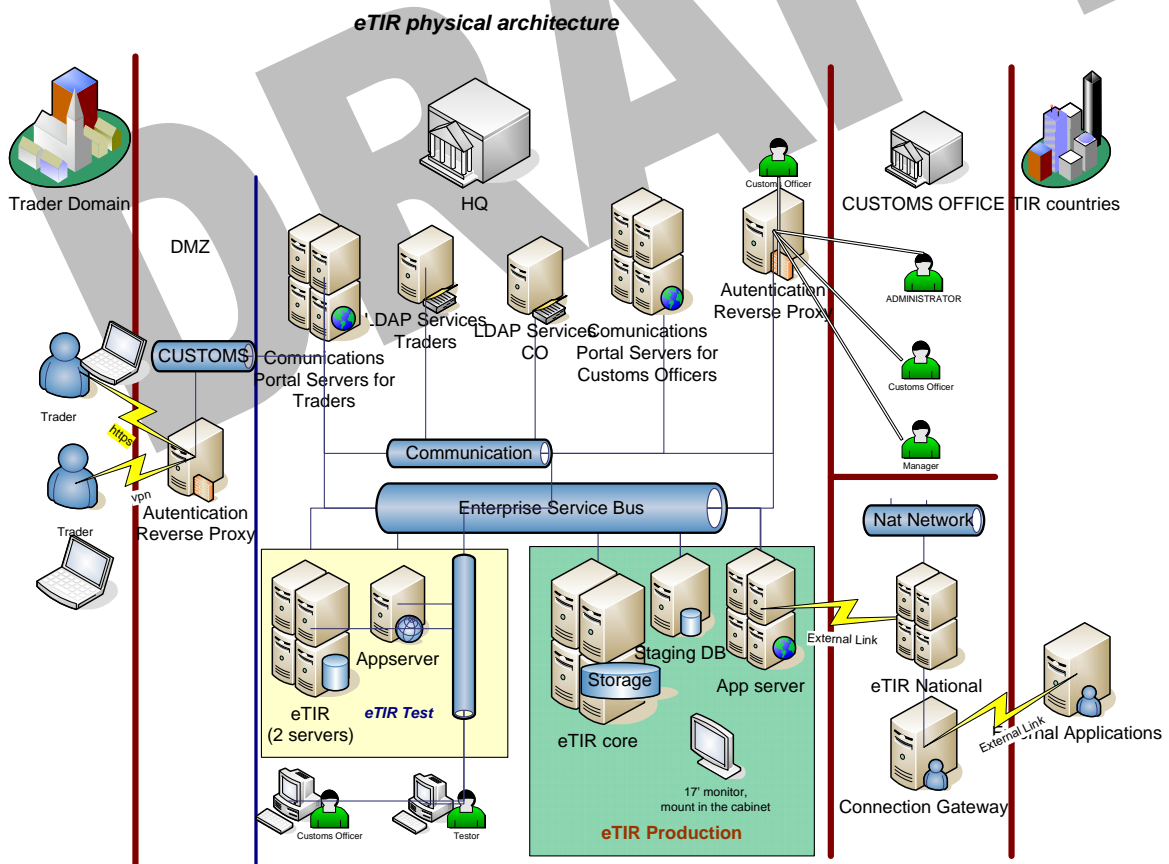


Fig 8. Hosting eTIR at own premises

The components which define the physical architecture are presented in the figure above.

2.10. HOSTING THE eTIR SYSTEM AT THE PREMISES OF OTHER IT SYSTEMS

This option might be similar to a private cloud. The eTIR (IaaS) will be hosted in the environment of an existing IT system, like UNOG or UNICC. The difference between cloud-PaaS and this approach refers to the owner of the infrastructure and the relation between the eTIR owner and the infrastructure owner.

This option assumes that the eTIR international system will be installed using the hardware and software infrastructure of an organization involved in the eTIR international system or a specialized company.

From a technical point of view, this solution is similar with cloud-PaaS. For this reason, all elements of PaaS will be considered as part of its assessment. It offers a platform where the system could be developed.

Differences might also be when we refer to the quality of service. But such differences exist between all PaaS providers.

It is particularly important to note that the mentioned providers (UNOG, UNICC) are strongly linked to the eTIR community

For this alternative:

- The hardware and infrastructure are owned and maintained by **UNICC/UNOG**;
- Platforms are owned, installed, configured and maintained by **UNICC/UNOG**;
- The eTIR system is developed, owned, installed, configured and maintained by **UNECE**;

The deployment schema is similar to the one for PaaS (fig 6), with the difference that the hosting is done at UNUG premises.

SOLUTION COMPARISON.

This paragraph contains a review of the solution comparison, with explanations of the criteria used.

Qualitative points are given from 1 to 5, where 1 point means that the solution is not considered appropriate for the eTIR system and 5 points mean that the solution is considered as very appropriate for the eTIR system.

The more points in a specific category, the stronger the recommendation of the alternative is recommended.

No	Category	IaaS	PaaS	SaaS	UNOG/ UNICC	Premises
1	24/7 Reliability (Uptime is Imperative)	4	5	5	4	3
2	Performance	4	5	3	3	2
3	Security	1	3	3	4	5
4	Scalability	4	5	2	3	3
5	Availability/Access From Anywhere	4	5	5	4	3
6	Flexibility & Customization	4	3	2	3	5
7	Mental Blocks / Culture	3	3	2	4	5
8	Administration	3	4	5	4	1
9	Maturity of technology	3	2	1	4	5
	Total	30	35	27	33	32

In conclusion, from a technical point of view, PaaS and UNOG/UNICC provide the best solutions.

It should, however, be noted that clouds are evolving very rapidly and that, in the near future, good solutions for current weak points could very well be found.

2.10.1. Explanations regarding categories

24/7 Reliability

Reliability: the ability of the system or components to perform the required functions under stated conditions for a specified period of time.

SaaS/Cloud computing is going to be housed in a datacentre usually staffed around the clock, with redundant power, air-conditioning, etc.

Premises servers can be accessed from anywhere with a stable, high-bandwidth Internet connection, but most privately owned datacentres do not have the redundancy that a cloud provider datacentre has, nor do they have 24/7 support staff. The latter can be mitigated by engaging a managed IT service provider.

The scale of cloud computing networks and their ability to provide load balancing and failover makes them highly reliable, often much more reliable than can be achieved in a single organization.

From a reliability point of view, considering the above, PaaS and SaaS are classified as most reliable (5 points)

IaaS is given 4 points, as it offers only the hardware solution. The software platform should be maintained by the user. The same is true for UNOG/UNICC.

Premises qualifies as the weakest in this category, because it is difficult to achieve the redundancy of a datacentre, nor does it have 24/7 support staff (3 points).

Performance:

System performance is measured in number of transactions per second, medium time to view a page and medium time to call a web service.

For cloud systems, performance could be obtained as defined in Service Level Agreements (SLA). For on premises performance, this is dependent on the hardware and platform installed.

It is easier to define a SLA for a better performance than to install a very good platform at premises.

In PaaS, a SLA can be defined according to the requirements. Hardware and software will be updated by the provider in line with the SLA. This is regarded as the best solution (5 points).

For IaaS, the SLA can be defined only at the hardware level. For this reason, it is considered less appropriate than PaaS (4 points).

As UNOG/UNICC are not specialized in cloud, it is not certain that a SLA with high requirements could be established. For this reason, these options have been given 3 points.

Regarding SaaS, considering that the whole system is outsourced to a cloud provider, the contract is usually based on the services, not on the performance. For this reason, it also gets 3 points.

Premises is the weakest in this category, because it has to be computed from scratch and is not adjustable to real system needs. Thus, it gets 2 points.

Security.

This aspect refers to computer security, network security, and, more broadly, information security.

There are a number of security issues/concerns associated with cloud computing, but these issues fall into two broad categories: Security issues, faced by cloud providers (organizations providing SaaS, PaaS or IaaS via a cloud) and security issues faced by their customers.

Compared with Premises, cloud implementations are considered less secure. The characteristics of private clouds offer good solutions to address security issues.

Premises is considered the most secure solution, because it provides full control (5 points), followed by the use of UNOG/UNICC (4 points) and PaaS (3 points), where both hardware and software are maintained by the cloud provider, which in turn could define a dedicated cloud. SaaS is considered just as secure as PaaS as it resides entirely with the cloud provider and a dedicated cloud could be attributed to it (3 points). IaaS is considered least secure; even if dedicated clouds are used, this is not a usual approach (1 point).

Scalability.

This is the ability of a system, network or process, to handle growing amounts of work in a capable manner or its ability to be enlarged to accommodate that growth. Cloud implementations are much more scalable, as more computing power could be added as needed.

Scalability is important in the eventuality of an increasing number of eTIR Carnets submitted for processing in the coming years (more than planned initially).

The risk of not being scalable is materialized in the necessity to redesign the system.

PaaS is considered as most scalable; resources (hardware and software) are allocated as they are needed (5 points), followed by IaaS, because only hardware resources can be added as needed. Software resources might be not scalable (4 points). SaaS is awarded 2 points, because the cloud provider is developing a solution which might or might not be scalable. The risk of SAAS not being scalable is materialized in the availability of the system or more costs per processing unit. Premises could be scalable if so designed, but the risk of not being well-scalable is greater than for the other solutions. At premises there is a limited amount of resources and usually systems are designed to fit the existing resources. Thus, compared to SaaS, it also gets 3 points. UNOG/UNICC are considered as scalable, as at premises (3 points).

Availability/Access From Anywhere

Availability is the degree to which a system, subsystem, or equipment is in a specified operable and committable state at the start of a mission, when the mission is called for at an unknown, i.e., a random, time. Simply put: availability is the proportion of time that a system is in a functioning condition.

Availability depends on the redundancy of the system, on the time required for balancing or restoration, on the way the system is monitored, on the way the system is configured to perform critical operations, etc.

Access From Anywhere refers to the availability of the system from any place where the system needs to function.

Bearing the above in mind PaaS and SaaS are considered as most accessible (5 points). IaaS and UNOG/UNICC come next, as they offer only the hardware solution, whereas the software platform needs to be maintained by the user (4 points). Premises is the weakest in this category (high costs are involved to increase this characteristic under this solution) (3 points).

Flexibility & Customization

While SaaS vendors generally come out with updates far more frequently than server-based applications, they cannot be customized easily, or not at all, in some cases. The business will generally align its processes around how the product functions versus making the SaaS behave as desired. This also means that there will be significantly less third-party add-ons, especially if the vendor has not made his APIs Application Programming Interfaces (API) available. In other words: a SAAS is made for initial specifications; subsequent changes in business processes are difficult to implement.

Premises is considered as the most flexible as this process of customization could be performed immediately (5 points). IaaS comes next, as only hardware infrastructure is from the cloud provider. All the other parts are under control of the eTIR owner and could be immediately customized (4 points). PaaS and UNOG/UNICC are less customizable, because the whole platform is owned by a cloud provider and customizations are limited (3 points). SaaS is considered least flexible, because everything is owned and maintained by a cloud provider and customizations depend entirely on the cloud SaaS provider (2 points).

Mental Blocks & Culture

Hosting any kind of data or business process off-premises is a big leap of faith for business owners, especially those who are not yet comfortable with information technology.

For these reasons, Premises is awarded 5 points, whereas UNOG/UNICC get 4 because they are well-known organizations. 3 points are given equally to IaaS and PaaS, because there is limited access to resources and 1 point to SaaS because there is no access to resources.

Administration

This aspect counts the effort necessary to administer the system. No administration is necessary for SaaS. (5 points). PaaS and UNOG/UNICC only require application administration (4 points). Application and platform administration are necessary in IaaS (3 points). Because Premises requires full administration, it only gets 1 point.

Maturity of technology

For a system where time is critical and subject to aligned to technological constraints, like the eTIR system, it is important to use a mature technology, with proven results in other systems.

When developing at premises, one has the full possibility to choose. In other situations, the technology should be chosen from a limited list of possibilities and usually the latest available technology has not necessarily been proven as being the most stable. From this point of view, Premises is regarded as the most mature solution, obtaining 5 points. The others are in a decreasing order of points: UNOG/UNICC (4 points), IaaS (3 points), PaaS (2 points), SaaS (1 point)

DRAFT

ANNEXES

Annex 0- Referenced documents - UNECE-eTIR_CBA-EST-ANNEX-0-REF-v02-21

Annex I – Cloud Computing definitions and short presentation - *UNECE-eTIR_CBA-ARCH-ANNEX-I-Cloud-v01-51*

Annex II - UNECE-eTIR_CBA-ARCH-ANNEX-I-Cloud-v01-51- *UNECE-eTIR_CBA-ARCH-ANNEX-II-CloudProviders-v01-51*

DRAFT

BIBLIOGRAPHY

Bibliography

- [1] Barrie Sosinsky – **Cloud Computing Bible** - John Wiley & Sons – 2011
- [2] Barry Boehm, Chris Abts, A. Winsor Brown, Sunita Chulani, Bradford K. Clark, Ellis Horowitz, Ray Madachy, Donald J. Reifer, and Bert Steece, '**Software cost estimation with COCOMO II**, Englewood Cliffs, NJ:Prentice-Hall, 2000.
- [3] David S. Linthicum - **Cloud Computing and SOA Convergence in Your Enterprise: A Step-by-Step Guide** - Addison-Wesley Professional – 2009
- [4] Frederick P. Brooks Jr.- **The Mythical Man-Month: Essays on Software Engineering, Anniversary Edition** - Addison-Wesley Professional – 1995
- [5] Jibitesh Mishra; Ashok Mohanty - **Software Engineering** - Pearson Education India - 2011
- [6] John Rhoton and Risto Haukioja – **Cloud Computing Architected** – Recursive Press – 2011
- [7] John Rhoton and Risto Haukioja – **Cloud Computing Explained** – Recursive Press – 2011
- [8] Steve McConnell - **Software Estimation: Demystifying the Black Art** (Best Practices (Microsoft)) - 2006
- [AC] Amazon.com - Amazon clouds documentation
- [GC] Google.com – Google clouds documentation
- [MC] Microsoft.com - Microsoft Azure documentation
- [OC] Oracle – Oracle clouds documentation
- [DGTAXUD] NCTS documentation