
# Report on access rights management & security requirements

# D5.1

Project Number: FP6 - 045389

Deliverable id: D5.1

Deliverable name: Access Rights Management and Security Requirements

Date: 25 October 2007

| COVER AND CONTROL PAGE OF DOCUMENT | |
|---|---|
| Project Acronym: | VITALAS |
| Project Full Name: | Video & image Indexing and Retrieval in the Large Scale |
| Document id: | D 5.1 |
| Document name: | Report on Access Rights Management and Security Requirements |
| Document type (PU, INT, RE) | PU |
| Version: | 1.5 |
| Date: | 2007-10-25 |
| Authors:<br>Organisation:<br>Email Address: | Cristina Martinez<br>Robotiker<br>cristina@robotiker.es<br>Alex Rodríguez<br>Robotiker<br>arodriguez@robotiker.es<br>Iñaki Etxaniz<br>Robotiker<br>etxaniz@robotiker.es<br>Angel Rego<br>Robotiker<br>angelr@robotiker.es |

Document type PU = public, INT = internal, RE = restricted

**ABSTRACT:** This document defines the security requirements and the access rights requirements of the security management component of the VITALAS system (SECAPI). SECAPI will provide access rights management according to the existing users' roles, will allow creating new roles and will guarantee the secure transfer of contents, the user's privacy and the secure management of personal data.

**KEYWORD LIST:** content protection, access rights management, user authentication and authorization, user privacy and anonymity.

| MODIFICATION CONTROL | | | |
|---|---|---|---|
| Version | Date | Status | Author |
| 0.1 | 2007-05-10 | Draft (TOC) | Cristina Martínez |
| 0.3 | 2007-08-23 | Draft | Angel Rego |
| 1.0 | 2007-09-13 | First diffused version | Alex Rodriguez, Iñaki Etxaniz, Angel Rego |
| 1.1 | 2007-09-28 | V1.1 | Added Access Rights chapter |
| 1.2 | 2007-10-08 | V1.2 | INRIA review |
| 1.3 | 2007-10-15 | V1.3 | Belga and IRT review |
| 1.4 | 2007-10-17 | V1.4 | Integration |
| 1.5 | 2007-10-25 | V1.5 | Final Version |

List of Contributors

- Robotiker
- Belga
- IRT
- INA

# Contents

# 1. INTRODUCTION

## 1.1. Purpose of this document

This document is the D5.1 deliverable of the VITALAS Project. It analyzes the requirements of the Security Management component (SECAPI), which addresses security management in the VITALAS system.

SECAPI will manage the access rights of VITALAS users according to the existing users' profiles, it will allow creating new profiles and will guarantee the secure transfer of contents, the user's privacy and appropriate personal data management.

The SECAPI requirements derived in this document will be complemented by D5.2 deliverable *Report on Personalization requirements of the system*, produced in Task 5.2 – Personalization (T6-T18). In this task the criteria for personalization will be defined according to end users' preferences and the content of users profiles will be established and implemented.

The definition of the requirements is closely related with the outputs of WP1, in particular with deliverable *D1.1 Use cases & Users requirements*.

The document is structured as follows:

Section 2 explains basic principles of security notion. In section 3, the security systems of future end users are analysed and security use cases are defined in section 4 in order to specify the security requirements for the VITALAS system in section 5. Section 6 concludes this document.

## 1.2. Preliminary considerations

In this chapter a brief description of the VITALAS system and the different types of users involved in the system is given.

VITALAS is a project intended for storing multimedia information using annotations and retrieving them from external users who have been previously registered. In this context, we can set three different kind of main users (these users will be subcategorized in further releases of this document):

- √ **External users.** Users who want to consume the different services that VITALAS can provide (e.g.: search for a sports related picture in the multimedia database)
- √ **Internal users.** Users who analyze and annotate the new multimedia information.
- √ **Administrators.** Users with special roles for managing the system, solve problems, etc.

Although this document is devoted only to requirements and no architecture issues, we assume that the VITALAS system is composed of several existing multimedia solutions integrated by an upper layer with common functionality for accessing and managing the data.

All the security issues in VITALAS are managed in a module named **SECAPI**. This module is responsible for managing the **access rights** for users and data and also managing all the

**security issues** among other modules in the system (mainly transmission of data in a secure environment).

## 1.3. Related Documents

| REFERENCE | DESCRIPTION |
|---|---|
| D1 | VITALAS – Description of Work – Version 1 - EC approved |
| D2 | D1.1 Use cases & Users requirements |
| D3 | D5.2 Report on Personalization requirements of the system |

The document 1-Description of Work resumes the VITALAS project, its objectives, tasks, effort and schedules. This document is the deliverable D5.1 as a result of the task 5.1. The document 2-Use Cases & User Requirements as served as a basis for defining the different users of the system and the operations they perform. The document 3-Report on Personalization Requirements will be elaborated afterwards, and is closely related with this document because explores further the relation of the system with its users, covering the characteristics it has to offer to the different user profiles and to individual users' preferences.

## 1.4. Glossary

| TERM | DESCRIPTION |
|---|---|
| ANONYMITY | A condition in which an individual's true identity is unknown. |
| AUTHENTICATION | The process for verifying that someone or something is who he or what it claims to be. |
| AUTHORIZATION | The process of determining, by evaluating applicable access control information, whether a subject is allowed to have the specified types of access to a particular resource. Usually, authorization is in the context of authentication. Once a subject is authenticated, it may be authorized to perform different types of access. |
| AVAILABILITY | Ensuring that authorized users have access to information and associated assets when required. |
| CONFIDENTIALITY | Ensuring that information is accessible only to those authorized to have access. |

| | |
|---|---|
| **IDENTIFICATION** | A process through which one ascertains the identity of another person or entity. |
| **INFORMATION SECURITY** | Information security is characterized by the preservation of confidentiality, integrity and availability. |
| **INTEGRITY** | Safeguarding the accuracy and completeness of information and processing methods. |
| **SECAPI** | Security Management component in the VITALAS system. |
| **SSL** | Secure Sockets Layer |
| **PRIVACY** | The right for an individual to be free from identification, classification, or observation by another party without their consent. Also involves the right of individuals to control third party access to information about them that may be considered personal in nature. |
| **VITALAS** | Video & image Indexing and Retrieval in the Large Scale. |

# 2. SECURITY FOUNDATIONS

## 2.1. Introduction

Security notion covers a very extensive problem domain. System security concerns the physical and logical protection of operational systems, whereas Software security addresses part of this spectrum by focussing on the security properties of software.

Security of software systems is realized by protection and assurance. The goal of **protection** is to design and implement adequate security mechanisms in order to protect sensitive information, while **assurance** makes sure that the realization of these mechanisms is achieved appropriately.

In the rest of this section we analyze some security mechanisms that are commonly used to ensure an adequate level of confidentiality, integrity, and availability of the information in software systems.

Information security manifests in many ways according to the specific situation and requirements. But regardless of who is involved in a transaction all parties must have confidence that certain objectives associated with information security have been met.

ISO standard 17799 defines five categories of security services:

- √ Authentication: protection against masquerading.
- √ Access control: protection against non-authorized access to resources.
- √ Confidentiality: protection against non-authorized exposure of information.
- √ Data integrity: protection against non-authorized creation, altering or removal of data.
- √ Non-repudiation and accountability: protection against falsely denial of participation in communication or certain actions.

## 2.2. Authentication

Identity Management comprises two processes: User identification and User Authentication. Identification is the process of assertion of an identity. Authentication is the process of reliably verifying the identity of someone (or something).

Classically, there are three different ways how you can authenticate yourself or a computer to another computer system:

- You can tell the computer **something that you know**; for example, a password. This is the traditional password system.

- You can "show" the computer **something you have**; for example, a digital certificate, a card key, a smart card, one-time pads, a challenge-response list, and so on.

- You can let the computer measure **something about you**; for example, your fingerprint, a retina scan, voiceprint analysis, and so on.

Some systems combine these approaches. For example, a smart card that requires the user to enter a personal identification number (PIN) to unlock it is a combination of something you have (the card) and something you know (the PIN).

It is considered a good idea to combine at least two mechanisms, because people can steal either one: the thing you have is susceptible to ordinary theft, and the thing you know is compromised by sniffing if it passes over the Internet; but it is rare for somebody to be able to get both at once. For example, in an e-business application server environment, a common approach to user and server authentication is to **implement secure sockets layer (SSL)** and **digital certificates** to "show the computer something you have" while also using **passwords** to tell the computer "something you know."

## 2.3. Access Control

Access Rights Management comprises two processes: User Authorization and Access control.

User Authorization is finding out if a person, once identified, is permitted to have a certain resource. This is usually determined by finding out if that person is part of a particular group, if that person has paid admission or has a particular level of security clearance.

Access control is a much more general way of talking about controlling access to a resource. Access can be granted or denied based on a wide variety of criteria, such as the network address of the client, the time of day, or the browser which the visitor is using.

Access control is used in situations where it is possible to construct a controlled software layer between an attacker and the information that is to be protected. For instance, most operating systems include access control techniques to protect the information that is stored on disk, since this information is normally only accessed through the operating system.

An access control model defines a generic framework for describing the access control policy, and their relationships. Most access control models are defined in terms of subjects and objects. A subject is a computer system entity that can initiate requests to perform an operation on objects. An object represents a sensitive resource that is to be protected, which can be either a user resource or a system resource.

Different access control models exist, each featuring different characteristics such as confidentiality, integrity and maintainability. We can distinguish among others Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Role-Based Access Control (RBAC). All of these models are used in practice in operating systems, databases, web servers, and so forth.

With **role-based access control**, access decisions are based on the roles that individual users have as part of an organization. Users take on assigned roles. The process of defining roles should be based on a thorough analysis of how an organization operates and should include input from a wide spectrum of users in an organization.

Access rights are grouped by role names, and the use of resources is restricted to individuals authorized to assume the associated role.

The use of roles to control access can be an effective means for developing and enforcing enterprise-specific security policies, and for streamlining the security management process.

## 2.4. Confidentiality

Confidentiality is the need to ensure that information is disclosed only to those who are authorized to view it.

Confidentiality is an important principle because it functions to impose a boundary on the amount of personal information and data that can be disclosed without consent. Confidentiality arises where a person disclosing personal information reasonably expects his or her privacy to be protected, such as in a relationship of trust.

## 2.5. Data Integrity

Data Integrity describes the assurance that the data is unchanged from its source and has not been accidentally or maliciously modified, altered or destroyed.

Often such integrity is ensured by the use of a number referred to as a Message Integrity Code (MIC) or Message Authentication Code (MAC).

In cryptography and information security in general, integrity refers to the validity of data. Integrity can be compromised through:

- √ Malicious altering, such as an attacker altering an account number in a bank transaction, or forgery of an identity document
- √ Accidental altering, such as a transmission error, or a hard disk crash

A cryptographic message authentication code (MAC) is a short piece of information used to authenticate a message. A message integrity code (MIC) is another name for a MAC that is usually used when the acronym "MAC" is defined to mean something else, like when it means Media Access Control in networking contexts.

## 2.6. Non-repudiation and accountability

Accountability is the act of collecting information on resource usage for the purpose of capacity and trend analysis, cost allocation, auditing and billing. Accounting management requires that resource consumption is measured, rated, assigned, and communicated between appropriate parties. Typical information that is gathered in accounting is the identity of the user, the nature of the service delivered, when the service began, and when it ended.

Non-repudiation means that it can be verified that the sender and the recipient were, in fact, the parties who claimed to send or receive the message, respectively. In other words, non-repudiation of *origin* proves that data has been sent, and non-repudiation of *delivery* proves it has been received.

Traditional methods such as seals or signatures are vulnerable to forgery. Digital transactions are also potentially subject to fraud, such as when computer systems are broken into or infected with trojan horses or viruses, or the network connecting the systems allows for a man-in-the-middle attack. Participants can potentially claim such fraud to attempt to repudiate a transaction.

When engineers use the term ‘non-repudiation’ in an engineering sense, they mean that there is a high (and specifiable) degree of probability that the protocol can demonstrate a document or message was sent or received by a particular computer.

# 3. Analysis of security systems in use by VITALAS final users

In this section we intend to define the different users and the several operations managed in the systems employed by the final users –INA, BELGA and broadcasters associated with IRT- nowadays. The aim being to see in what extent it is possible to unify them in the future VITALAS system.

Most of the information has been extracted from the scenarios and use cases descriptions contained in Deliverable 1.1-Use Cases. The rest of it reflects typical user roles and functionality of a *standard* application.

In order to gather the needs of final users about security issues in the VITALAS system, a questionnaire was issued. The questionnaire comprised 39 questions grouped in these five areas: Authentication, Access Control, Confidentiality, Data Integrity and Non-Repudiation,

The questionnaire and respective answers are collected in the Annex1. The main conclusions extracted from the process are the following ones:

- √ For web users, the login-password authentication is sufficient (no need to create certificates, manage tokens, etc).
- √ The system must be designed to add new roles (profiles) for users, once the system is on "production mode" (not only in the system design phase).
- √ The user privileges may vary depending on the media type.
- √ An extensive log system must be implemented (to store transactions data and retrieve information easily).

## 3.1. Users

| USERS | DESCRIPTION |
|---|---|
| **EXTERNAL PROFESSIONAL USER** | Editors, producers, broadcasters, directors, archivists coming from external companies with subscriptions |
| **GENERAL PUBLIC** | Users who access to use the application without a subscription. |

| | |
|---|---|
| **ARCHIVIST** | Archivists are in charge of the following tasks:<br>√ Identification processes (segmenting and cataloguing channels),<br>√ Synthetic analysis and annotation of resources<br>√ Production of metadata adapted for selling purposes,<br>√ Juridical analysis of clients selections,<br>√ Search process for external clients<br>√ Exploitation of the data resources for broadcast analysis purposes<br>√ Control of quality of metadata |
| **TECHNICIAN** | Users with advanced knowledge on different areas like image, sound, video etc. |
| **ADMINISTRATOR** | The role responsible for the enterprise's data resources and for the administration, control, and coordination of all data related analysis activities. |

## 3.2. Operations

| OPERATION | DESCRIPTION |
|---|---|
| **MODIFY ANNOTATIONS** | Read, modify and erase the annotations associated to the different media elements (Video, Audio and Photo). |
| **READ ANNOTATIONS** | Read the annotations associated to the different media elements (Video, Audio and Photo). |
| **LOG CONSULTATION** | The analysis of records stored in the log file. |
| **SET AV CONTENT** | Store new AV content in the database. |
| **GET AV CONTENT** | To see AV content of the database. |
| **MANAGE AV CONTENT** | To delete or modify AV content of the database. |

| | |
|---|---|
| **ACCESS_IMAGE_FORUM** | Link giving an authorized access (for some logged in clients) to another picture provider (in this case AFP Image Forum) without having to re-authenticate |
| **ADMIN_GALLERIES** | To create a new Coverage or Gallery<br>Galleries: Set as Top*, Special, Hide, delete<br>Coverages: Set as Special*, Hide, Delete, Select*<br>In the Coverage or Gallery details page: you can Mail, Modify, Add pix, Hide, Delete, Set as top, Set as Special<br>Coverage or Gallery picture: you can move, set as top*, delete<br>----------<br>Selection of pictures presented on the website:<br>* Top: Galleries that appear in a 'Top galleries' box<br>* Special: Coverages or galleries that appear in a 'Special' pictures box<br>*Select: Coverages appear in a 'Coverage selection' box<br>*Top: to select the picture that should appear first in the coverage or gallery |
| **DOWNLOAD_PREVIEW** | To download a preview version only of the picture. |
| **DOWNLOAD_PREVIEW_OR_HIGHRES** | Choice between downloading the preview or high resolution version of the picture |
| **EXPORT_PICTURE** | Send (export) pictures to selected clients by FTP |
| **FETCH_PICTURE** | For internal staff: to be able to download pictures without passing through the billing system. |
| **FORBID_DOWNLOAD** | To forbid the download of a media file. |

| | |
|---|---|
| **DELETE_DOWNLOADED** | For picture Sales department: to remove from the billing (after agreement with the client) a download -> picture not charged |
| **TRANSFER_PICTURE** | For picture editors: quick way to transfer pictures directly to a local drive (e.g to edit them) |

## 3.3. Access Rights

Taking into account the previous definitions, we can depict a table representing the user's rights to access any operation.

| | **EXTERNAL USERS** | | **INTERNAL USERS** | | |
|---|---|---|---|---|---|
| | 1.Professional User<br>2.General public | | 3.Archivist<br>4.Technician<br>5.Administrator | | |
| **OPERATION** | 1 | 2 | 3 | 4 | 5 |
| **MODIFY ANNOTATIONS** | | | X | | X |
| **READ ANNOTATIONS** | X | X | X | X | X |
| **LOG CONSULTATION** | | | | X | X |
| **SET AV CONTENT** | | | X | | |
| **GET AV CONTENT** | X | X | X | | |
| **MANAGE AV CONTENT** | | | X | X | X |
| **ACCESS_IMAGE_FORUM** | X | X | X | | |
| **ADMIN_GALLERIES** | | | X | X | X |
| **DELETE_DOWNLOADED** | | | | | X |
| **DOWNLOAD_PREVIEW** | X | X | X | X | X |
| **DOWNLOAD_PREVIEW_OR_HIGHRES** | X | | X | X | X |
| **EXPORT_PICTURE** | | | X | X | X |
| **FETCH_PICTURE** | X | X | X | X | X |
| **FORBID_DOWNLOAD** | | | X | X | X |
| **TRANSFER_PICTURE** | | | X | X | X |

# 4. SECAPI USE CASES

Based on the two main users described in the previous chapters, we can define some common security use cases. The analysis of these cases will produce security requirements, related with user functionality.

The use cases presented here are low-level use cases, needed to reflect those actions of the user related with security issues. No direct relation among the high-level functional use cases covered in the deliverable D1.1 and these use cases exists. The former ones reflected the main functionalities of the system, the business rules while the later ones are dedicated exclusively to security aspects that are common to many different applications.

Below are described the use cases which involve SECAPI module functionalities.

## 4.1. User Registration

**Internal user:**

The new user should request a new profile to the administrator, and this one will check the required permissions and rights for that new user (e.g.: he can annotate only pictures). The administrator will provide (via email, phone call or whatever) the required data (user and password, certificate) for accessing the system according a profile.

**External user**:

Since external users will often access by the Internet, the registration process starts when the user fills a registration form in the VITALAS system. This form is processed by an administrator who fits the user request with the appropriate profile requirements (e.g.: check if the user works for a trusted company, if the bill has been paid, etc). Then, the administrator will generate the profile data for that user and will send the information (profile, authentication data, instructions, etc) by e-mail. The user must validate the registration by clicking on a link provided in the previous e-mail. Then the user can access the VITALAS system by using the authentication data provided previously.

| Use Case S1.1 | | | |
|---|---|---|---|
| task name: | User registration | Use case reference : | UC S1.1 |
| Created by: | ROB | Last updated by: | ROB |
| Date created: | 2-08-07 | Date last updated: | 22-08-07 |
| Role: | New user, administrator | | |
| Goals/Description: | Registration of new user. | | |

| | |
|---|---|
| Scenario example: | A new user wants to join the VITALAS system |
| Pre conditions: | |
| Success & failure conditions: | Administrator will accept or reject the request |
| Priority: | High |
| Frequency of use: | Often |
| Activity step Description: | SECAPI receives a user request.<br>The SECAPI module can accept/reject the new user admission.<br>The administrator will provide the required data for accessing the system. |
| Exceptions : | |
| Special Requirements: | |
| Assumptions : | |
| Notes and issues: | |
| Non functional requirements: | Secure transport channel |

## 4.2. Unregister

**Internal user**:

A VITALAS worker is assigned to a different task, the administrator is ordered to cancel the user access to the system. He cancels the current profile for that user and notifies him. In order to keep the log of transactions made by that user, this one is not removed, but changed the status in the database to “old user”.

**External user**:

The request for disassociating a user can be done by filling a form in the web site and wait for the response. The administrator will analyze all the aspects involved in the process (all the bills have been paid off, etc), and then the system will send a confirmation e-mail to the user. If the user answer is ok, the user profile will be cancelled.

| Use Case S1.2 | | | |
|---|---|---|---|
| task name: | Unregister a user | Use case reference : | UC S1.2 |
| Created by: | ROB | Last updated by: | ROB |
| Date created: | 2-08-07 | Date last updated: | 22-08-07 |
| Role: | any user profile, administrator | | |
| Goals/Description: | Unregister a user. | | |
| Scenario example: | A VITALAS worker is assigned to a different task, the administrator is ordered to cancel the user access to the system | | |
| Pre conditions: | User has been previously registered | | |
| Success & failure conditions: | | | |
| Priority: | High | | |
| Frequency of use: | sometimes | | |
| Activity step Description: | SECAPI receives user request.<br>The administrator will deactivate the access to the system for that user. | | |
| Exceptions: | | | |
| Special Requirements: | | | |
| Assumptions: | | | |
| Notes and issues: | | | |
| Non functional requirements: | Secure transport channel | | |

## 4.3. Login

The user knows the data required to be authenticated in the system (login-password), or the information is stored in a safe container in his computer (e.g. a digital certificate in the browser keystore). Once the user fills the data in the VITALAS login page, the system will validate the user, his profile will be loaded and he can access services according to their access rights from the profile.

| Use Case S1.3 | | | |
|---|---|---|---|
| task name: | User login | Use case reference: | UC S1.3 |
| Created by: | ROB | Last updated by: | ROB |
| Date created: | 2-08-07 | Date last updated: | 22-08-07 |
| Role: | Any registered user | | |
| Goals/Description: | Login in the system. | | |
| Scenario example: | A user wants to search some multimedia data in the VITALAS system, and he must be authenticated in the system | | |
| Pre conditions: | Any client who wants to connect to the system must be registered in VITALAS previously. | | |
| Success & failure conditions: | Check user's login data in SECAPI | | |
| Priority: | High | | |
| Frequency of use: | Always | | |
| Activity step Description: | User fills the login form.<br>SECAPI validates the user.<br>The user will be able to access to the system according to their access rights from his profile. | | |
| Exceptions: | | | |
| Special Requirements: | | | |

| | |
|---|---|
| Assumptions: | |
| Notes and issues: | |
| Non functional requirements: | Secure transport channel |

## 4.4. Logout (or timeout)

When the user finishes consuming services in VITALAS, he will click on the ”logout” link in the web page. The system will finish the session for that user.

Timeout implies that, for security reasons, if the user is not interacting with the application for a specified time, the system will logout the user automatically.

| Use Case S1.4 | | | |
|---|---|---|---|
| task name: | User logout | Use case reference: | UC S1.4 |
| Created by: | ROB | Last updated by: | ROB |
| Date created: | 2-08-07 | Date last updated: | 22-08-07 |
| Role: | Registered & Logged user | | |
| Goals/Description: | Logout from the system. | | |
| Scenario example: | The user closes the browser. | | |
| Pre conditions: | User logged in the system. | | |
| Success & failure conditions: | | | |
| Priority: | Medium | | |
| Frequency of use: | Always | | |

| | |
|---|---|
| Activity step Description: | User clicks the logout button or the user is not interacting with the application (The user has closed the browser.)<br>The system will finish the session for that user. |
| Exceptions: | |
| Special Requirements: | |
| Assumptions: | |
| Notes and issues: | Session timeout can be configured in the web server |
| Non functional requirements: | |

## 4.5. Consuming services

External users, internal users or administrators can perform several operations depending on Their profile data: for each user, this profile contains the rights he owns to access content, modify annotations, search in the index, etc. Thus, in every operation to be executed, the system will check the required right to perform that operation with the user's rights in his profile data. The user interface should hide operations not allowed for each profile, but this "validation before execution" ensures the system to provide only allowable services for that user.

| Use Case S1.5 | | | |
|---|---|---|---|
| task name: | Consuming services. | Use case reference: | UC S1.5 |
| Created by: | ROB | Last updated by: | ROB |
| Date created: | 2-08-07 | Date last updated: | 22-08-07 |
| Role: | External users, internal users or administrators | | |
| Goals/Description: | Access & use the VITALAS services | | |
| Scenario example: | A internal user (Archivist) wants to add & annotate a new multimedia document (i.e.: a new picture). | | |

| | |
|---|---|
| Pre conditions: | User logged in the system. |
| Success & failure conditions: | The system provide only allowable services for user. |
| Priority: | High |
| Frequency of use: | Very Often |
| Activity step Description: | Access the system<br>Perform operations |
| Exceptions: | |
| Special Requirements: | |
| Assumptions | |
| Notes and issues: | |
| Non functional requirements: | Secure transport channel |

# 5. SECAPI REQUIREMENTS

SECAPI requirements will be classified by ISO security services. This method is also useful in the next steps of the development, when the requirements will me matched with the functionalities.

Thus, the requirements are organized according to the categories previously presented in this document. Some of the requirements can be contained in various categories, but for simplicity we will put each requirement in only one category.

Notation

Requirement's code is composed of the following characters: YYY-nn

- √ YYY express the type of requirement (i.e: AUThentication)
- √ nn is the number of requirement (starting from 01)

For example, ACC-01 means "Requirement of security, *type* **ACC**ess control, *Number* **01"**

## 5.1. Authentication requirements

| CODE | DESCRIPTION |
|---|---|
| **AUT-01** | Data transmission between a user and the VITALAS system must be done in a secure environment. In order to achieve that, the user must be previously authenticated in the system. |
| **AUT-02** | Authentication will last for the session lifetime. The session will be ended either because the user has requested to log out or because of the session expiration, that is, the user hasn't performed any actions for a time-out period. |

## 5.2. Access control requirements

| CODE | DESCRIPTION |
|---|---|
| **ACC-01** | Only authorized users can access to the system. Each user has a profile data stored in the system. By reading the data, the system will control what kind of information the user can create, access, modify etc. |
| **ACC-02** | The VITALAS system must be able to manage profiles dynamically. For instance, we can have only one profile for internal users (can create data, modify, delete), but if we want to create a new profile "internal- read-only", the system must be flexible enough to add it. |

| | |
|---|---|
| **ACC-03** | Only a user with an administrator profile can accept/reject the user's admission request of new users, remove already admitted users or manage profiles. |

## 5.3. Confidentiality requirements

| CODE | DESCRIPTION |
|---|---|
| **CON-01** | The different components involved in VITALAS (databases, web servers) will exchange information in a safe way. Only the component which requests information and the one which sends it are able to access and process that data. No other modules can access it. |
| **CON-02** | The user information useful for personalization issues (e.g. previous search strings) must be kept as private as possible. These data will be used, in an anonymous way, for the analysis of general behaviour, or kept available only to himself. |
| **CON-03** | The process of registering a new user must ensure that the user's private data (personal data, user keys, etc…) will be kept confidential when submitting and also when is stored. That is, nobody can see the data during the process. |

## 5.4. Data integrity requirements

| CODE | DESCRIPTION |
|---|---|
| **DAT-01** | The communication among the several components of VITALAS system must ensure that the data have not been tampered during the transit from the source to the consumer. That is, if the data is modified in some way, the change can be detected. |

## 5.5. Non-repudiation & accountability requirements

| CODE | DESCRIPTION |
|---|---|
| **NON-01** | The system must provide a log system, storing all the relevant information for operations such as registering a new user, deleting information, buying content, modifying a user's profile. That information must be enough to identify the user performed that operation (user's IP address, username, date of transaction, certificate, etc…) |
| **NON-02** | The log files of the system must provide irrefutable evidence of the origin of a transaction. |
| **NON-03** | The log files of the system must provide irrefutable evidence of the target of a transaction. |

# 6. CONCLUSION

The security concerns of the VITALAS system have been gathered and analyzed in this document. Although the main objectives of the system focuses on archiving and retrieval in large databases of multimedia documents, the security module should be designed to permit the safe execution of all functionalities and user tasks defined for VITALAS.

Based on the final users' feedback, security-specific use cases have been established in order to define a set of requirements, which have been classified by the categories defined by ISO standard 17799:

- √ Authentication
- √ Access Control
- √ Confidentiality
- √ Data integrity
- √ Non-Repudiation and Accountability

As a first conclusion to extract, we see that no especially strong security measures are necessary for VITALAS, apart from the standard ones employed in applications that involves internal and external users, internet based access and payment of services.

The ultimate goal of this report is to serve as the base to design the security solution of the system. Future upgrades of the report or extensions of it will be needed to achieve that goal in the most effective way. For example, we will need to minimize ambiguity of requirements specification by adding details to use cases; or to fine-tune the scope of the VITALAS system regarding aspects like customer management, identity management, etc. Meanwhile, we think that the specified requirements are a strong driver to define the security architecture.

# 7. Annex A

| | |
|---|---|
| Filled by: | Marie-Luce Viaud, Agnès Saulnier |
| Organization: | INA |
| Date: | 22 June 2007 |
| Contact email: | mlviaud@ina.fr, asaulnier@ina.fr |

User Authentication Requirements

Protection against masquerading

| Code | Question | Priority (0-5) | Detailed answer/Comments |
|---|---|---|---|
| AU01 | Would it be enough to use a login/password authentication to control access to the system? | 4 | YES, for Inamedia consultation, OGP purchase or archives consultation/annotation. |
| AU02 | Would it be convenient the use of digital certificates to authenticate users? | 1 | Possibly, for extract delivery on Inamedia. |
| AU03 | Do you envision any other type of authentication method? | 1 | Possibly, temporary password for extract delivery on Inamedia. |
| AU04 | Should the system support different types of authentication? | 1 | Always login/password authentication in consultation process |
| AU05 | If yes, depending on what (p.e. user's profile, access point) ? | 1 | other type for purchase or delivering processes. |
| AU06 | Describe briefly what actions are available before user authenticates into the system | | nothing on Inamedia and navigation/consultation on OGP |
| AU07 | Other considerations about user authentication | | Other distinction between users who can modify annotation or just read. |

Authorization and Access Control Requirements

Protection against non-authorized access to resources

| Code | Question | Priority (0-5) | Detailed answer |
|---|---|---|---|
| AC01 | What type of users roles are implemented in your system? (p.e. Regular users, non regular users) | | About 10 profiles in archives annotation/consultation. |
| AC02 | Should VITALAS system support any new roles to control access to resources? | | |
| AC03 | What user roles do you identify in VITALAS? | | external professional user (different profils on Inamedia), general public (ogp), internal users (archivists, technicians, administrators, hotline, guest, informaticians ) |
| AC04 | What privileges attributes do you identify in the system? (these attributes are part of the credentials a user gets when he or she is authenticated) | | media access (search on part of the data); modification of metadata; exportation of data. |
| AC05 | Please, assign the privileges to the defined roles | | … depends on roles and processes engaged. |
| AC06 | Can a user have different privileges depending on the media type? | | yes |
| AC07 | Apart from Default Rights (set, get, manage, use) what new custom rights do you identify in VITALAS? | | statistical analysis and overview of the database. |
| AC08 | Describe briefly what legal rights are involved in your multimedia resources (rights of users and producers) | | copyright (financial implication) and content owners right (people on picture - no financial implication) |
| AC09 | How are these legal rights negociated and established? | | agreement with SACEM |
| AC10 | Considerations about how the VITALAS system could manage with legal rights | | no concern by VITALAS |
| | | | |

Confidentiality Requirements

Protection against non-authorized exposure of information

| Code | Question | Priority (0-5) | Detailed answer |
|---|---|---|---|
| CF01 | Is, in the system, some data to be keep private? | | Yes |
| CF02 | If yes, what type of data? (users personal data, resources, metadata...) | | logs consultation |
| CF03 | Do users require some kind of anonimity? | | confidentiality between users on the same level (inamedia, archivists) |
| CF04 | If yes, explain it | | folio can only be access by his homeowner or superior |
| CF05 | Would it be necessary to encrypt some data? | | yes (at present nothing done) |
| CF06 | If yes, explain what type of data and when (to store, to send) | | for paiement (at present done by external organism) |
| CF07 | Should VITALAS system guarantee privacy of the searchs processes performed by a user? | | yes |
| CF08 | If yes, explain it | | for concurrence, …. |
| CF09 | Should VITALAS system protect the confidentiality of some messages in transit? | | |
| CF10 | If yes, explain it | | |
| CF11 | Other considerations about user confidentiality | | hotline must preserve user confidentiality |

Data Integrity Requirements

Protection against non-authorized creation, alteration or removal of data

| Code | Question | Priority (0-5) | Detailed answer |
|---|---|---|---|
| DI01 | Do users need some mechanism to assure that the downloaded digital audio-visual content is authentic and not altered (data origin authentication)? | | yes |
| DI02 | If yes, explain it | | for extract dowload size test or check sum. |
| DI03 | Should the VITALAS system provide protection against non-authorized creation, altering or removal of data? | | yes |
| DI04 | If yes, explain it | | essential for audiovisual production |
| DI05 | Other considerations about Data Integrity | | |

Non-Repudiation Requirements

Protection against falsely denial of participation in certain actions

| Code | Question | Priority (0-5) | Detailed answer |
|---|---|---|---|
| NR01 | Should the system maintain a log of users actions? (data modification, removal, download…) | | yes |
| NR02 | If yes, explain it | | to ensure the database quality |
| NR03 | Should VITALAS system implement some mechanisms to refute a user that denies some previous actions? | | exceptionally on ogp, very exceptionally on inamedia |
| NR04 | If yes, explain it | | risk to stop an important client |
| NR05 | Should VITALAS system provide irrefutable evidence of proof of origin of data to the recipient? | | yes |
| NR06 | If yes, explain it | | |
| NR07 | Should VITALAS system provide irrefutable evidence of proof of origin of receipt of data to the sender | | yes |
| NR08 | If yes, explain it | | |
| NR09 | Other considerations about Non repudiation | | |

| | |
|---|---|
| Filled by: | Fairouz Nasr and Tom Wuytack |
| Organization: | Belga |
| Date: | 26 06 07 |
| Contact email: | naf@belga.be / wut@belga.be |

User Authentication Requirements

Protection against masquerading

| Code | Question | Priority (0-5) | Detailed answer/Comments |
|---|---|---|---|
| AU01 | Would it be enough to use a login/password authentication to control access to the system? | 5 | we think this is sufficient, no token or similar needed |
| AU02 | Would it be convenient the use of digital certificates to authenticate users? | 0 | |
| AU03 | Do you envision any other type of authentication method? | | No |
| AU04 | Should the system support different types of authentication? | 0 | |
| AU05 | If yes, depending on what (p.e. user's profile, access point) ? | | No |
| AU06 | Describe briefly what actions are available before user authenticates into the system | | in our picture website the user can see the coverages, galleries, pictures but can't download them to his desktop.... We are not sure if for Vitalas specific this should be the case as well. |
| AU07 | Other considerations about user authentication | | maybe not the specific answer to your question, but the system should allow that e.g. A contineous feed of e.g. Pictures is interpreted without a user having to access it manually first |

Authorization and Access Control Requirements

Protection against non-authorized access to resources

| Code | Question | Priority (0-5) | Detailed answer |
|---|---|---|---|
| AC01 | What type of users roles are implemented in your system? (p.e. Regular users, non regular users) | | within belga picture we make a difference between internal (admin)users and external clients. within each type of user there are differences in permissions/credits/privileges<br>a) **Permissions:** users allowed to performed different actions (see AC05)<br>b) **Credits:** some can make a search in pictures from other sources<br>c) **Privileges:** gateways: e.g. link and access to other partner agencies pictures website |
| AC02 | Should VITALAS system support any new roles to control access to resources? | 5 | |
| AC03 | What user roles do you identify in VITALAS? | | * By user's profile. Personalization of search tool: preferred type of pictures received: Editorial: politics, economics/business, public figures, sports, art and entertainment, leisure (e.g. travel), media, health and science, social issues, environment, … Creative<br>* + 3 roles defined above |
| AC04 | What privileges attributes do you identify in the system? (these attributes are part of the credentials a user gets when he or she is authenticated) | | see AC05 |
| AC05 | Please, assign the privileges to the defined roles | | a) Permissions: ACCESS_DPA, ACCESS_IMAGE_FORUM, ADMIN_GALLERIES, BELGA_ONLINE, DELETE_DOWNLOAD, DELETE_PICTURE, DOWNLOAD_PREVIEW, DOWNLOAD_PREVIEW_OR_HIGHRES, EXPORT_PICTURE, FETCH_PICTURE, FORBID_DOWNLOAD, HIDE_CUSTOMER_NAME, HIDE_GALLERIES, MODIFY_FIELDS, SEARCH_INTERMEDIA, TRANSFER_PICTURE)<br>b) Other sources: ANP, EPA, BELPRESS, ...<br>c) Link to AFP images |

| | | | |
|---|---|---|---|
| AC06 | Can a user have different privileges depending on the media type? | 5 | |
| AC07 | Apart from Default Rights (set, get, manage, use) what new custom rights do you identify in VITALAS? | | digital rights |
| AC08 | Describe briefly what legal rights are involved in your multimedia resources (rights of users and producers) | | up to today a picture is identified by a credit. For some picture sources belga owns 100%, for other 50% (meaning that if we sell e.g. A picture for 20 euro, Belga gets 10€ and the other party the remaining amount). Another aspect is the usage of a picture. the pricing is different if e.g. used for an illustrative picture in a magazine vs a full sized advertisement on a billboard. (for this purpose in belgium an organisation SABAM exists which has predefined prices depending on usage/n°copies...). For the moment this is not integrated in the Belga picture site (but yes in ANP Photo)<br>another aspect, difficult to manage, is the usage in time. Normally a sold picture may only be used once. if used a second time, one has to repay... which is very hard to trace (e.g. next to our sales portal, Belga pushes pictures to our shareholders...). Legally they are only allowed to store these for just one week, but we notice that some don't care and reuse them later on...<br>in most of the cases Belga buys the rights from the photographer. if this is not the case, other arrangements are in place (but we have no experience with this)<br>for creative pictures the rights are different (e.g. royalty-free... ) |
| AC09 | How are these legal rights negociated and established? | | mostly by negiotating |
| AC10 | Considerations about how the VITALAS system could manage with legal rights | | my suggestion would be to create an 'open system' which can make use of a legal rights module (if this should exist) |

Confidentiality Requirements

Protection against non-authorized exposure of information

| Code | Question | Priority (0-5) | Detailed answer |
|---|---|---|---|
| CF01 | Is, in the system, some data to be kept private? | 3 | |
| CF02 | If yes, what type of data? (users personal data, resources, metadata...) | | it's obvious that user A may not see any personal info of user B etc... |
| CF03 | Do users require some kind of anonimity? | 2 | |
| CF04 | If yes, explain it | | |
| CF05 | Would it be necessary to encrypt some data? | 0 | |
| CF06 | If yes, explain what type of data and when (to store, to send) | | no need |
| CF07 | Should VITALAS system guarantee privacy of the searchs processes performed by a user? | 2 | |
| CF08 | If yes, explain it | | it should be possible for Belga to analyze the user's browsing/searching behaviour (but with respect to privacy law of course) |
| CF09 | Should VITALAS system protect the confidentiality of some messages in transit? | 0 | |
| CF10 | If yes, explain it | | |
| CF11 | Other considerations about user confidentiality | | |

Data Integrity Requirements

Protection against non-authorized creation, alteration or removal of data

| Code | Question | Priority (0-5) | Detailed answer |
|---|---|---|---|
| DI01 | Do users need some mechanism to assure that the downloaded digital audio-visual content is authentic and not altered (data origin authentication)? | 1 | |
| DI02 | If yes, explain it | | no high priority for pictures, maybe otherwise for video |
| DI03 | Should the VITALAS system provide protection against non-authorized creation, altering or removal of data? | 2 | |
| DI04 | If yes, explain it | | we should make sure that only administrative/internal users have these rights |
| DI05 | Other considerations about Data Integrity | | |

Non-Repudiation Requirements

Protection against falsely denial of participation in certain actions

| Code | Question | Priority (0-5) | Detailed answer |
|---|---|---|---|
| NR01 | Should the system maintain a log of users actions? (data modification, removal, download…) | 3 | |
| NR02 | If yes, explain it | | yes, even if it's just for troubleshooting |
| NR03 | Should VITALAS system implement some mechanisms to refute a user that denies some previous actions? | 1 | |
| NR04 | If yes, explain it | | |
| NR05 | Should VITALAS system provide irrefutable evidence of proof of origin of data to the recipient? | 1 | |
| NR06 | If yes, explain it | | |
| NR07 | Should VITALAS system provide irrefutable evidence of proof of origin of receipt of data to the sender | 1 | |
| NR08 | If yes, explain it | | |
| NR09 | Other considerations about Non repudiation | | |