
Felipe Andrés Corredor Chavarro
Professor, Faculty of Basic Sciences and Engineering, University of the Llanos, Villavicencio, Colombia.

Andrés Felipe Ardila
Systems Engineer, GITECX Research Group, University of the Llanos, Villavicencio, Colombia.

Diana Cristina Franco Mora
Professor, Faculty of Basic Sciences and Engineering, University of the Llanos, Villavicencio, Colombia.

Abstract
This paper presents the development of a telematic security system as an alternative for document management processes in higher education institutions.

The problem was addressed from the perspective of the inherent complexity of providing stricter security measures to document management systems (DMS), as users must use external tools and have specific knowledge in security. A software solution named GISMOD is proposed, which makes extensive use of open source software and was developed in a modular way. This user-friendly tool allows for the adoption of security mechanisms in document management, such as digital signatures, multifactor authentication, fingerprint biometrics, data encryption and channel security layers. Topics such as corporate security policies and the legal basis for document management were taken into account during GISMOD’s design and implementation phases. Finally, an application example of the complete process, verified at the University of the Llanos is presented.

Keywords: Digital signature, symmetrical cipher, multifactor authentication, fingerprint biometrics, document management.

INTRODUCTION
Information is one of the most relevant assets for any organization and must be protected with integrity, confidentiality and other security services, while guaranteeing access to it by authorized personnel. Failing to do so can generate economic losses, legal issues and information leakage [1]. That is why organizations are widely investing in information security, with a special focus on data and network protection, as the digital management of it has higher risks of potential attacks [2].

Although most corporate information is stored in information systems, a high percentage of information assets consist of documents stored in physical and digital media. As this information corresponds to large volumes of isolated files with their own privacy requirements and with a permanent need to share them among many users of different levels, it is necessary to use informatic systems for its management.

There are multiple functionally robust DMS in the market such as Orfeo, Alfresco, Nuxeo, OpenKm and Athento®, but they currently do not show a strict security scheme.

In this order of ideas, there is a clear need of modeling security systems for document management that have a high degree of information availability and confidentiality and provide security services like non-repudiation, preferably based on open source software. These systems will be viable solution alternatives for reducing document security issues in organizations.

During the last few years, organizations in Colombia have begun to implement document management systems, most of them private, and some with free licensing. Orfeo, one of the most relevant, is a “document management system initially developed by the Superintendence of domiciliary public services, licensed as free software under GNU/GPL. Orfeo allows the management of the documents of a corporation, keeping records in an automated way, with significant savings in time, money and resources such as printer toners, paper and photocopies, among others” [3]. Orfeo is a very complete solution from the functionality perspective but lacks several security aspects that must be incorporated when dealing with classified information, as stated by the Colombian Public Information Transparency Law [4] and the “zero paper” decree law [5].

The legal framework in Colombia has been strengthened to take on the technological processes for digital information management on which society is supported; some examples that take relevance for this project are presented in Table 1.

<table>
<thead>
<tr>
<th>NORM</th>
<th>TOPIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Law 1581 of 2012</td>
<td>“Whereby general provisions for the protection of personal data are issued”</td>
</tr>
<tr>
<td>Decree 1377 of 2013</td>
<td>“By which Law 1581 of 2012 is partially regulated”</td>
</tr>
</tbody>
</table>
Law 1712 of 2014  “Law on Transparency and the Right of Access to National Public Information”
Law 1273 of 2009 “By means of which the Penal Code is modified, a new protected legal good is created - denominated ‘on the protection of information’”
ISO 27001 of 2013 “Information security management system”
Decree 2609 of 2012 “Presidential Law-Decree for Document Management”
ISO 15489 of 2001 “Comprehensive management of documents and archival systems”
Law 527 of 1999 “Defines and regulates access and use of data messages, e-commerce and digital signatures…”

**PROBLEM**

The large amount of information generated by society has been growing exponentially and humanity’s memory must be recorded, which is why by 2007, 94% of it was already stored in digital media, by 2011 the amount of information reached 295 Exabytes [6] and by 2025 the global amount data will grow to 163 zettabytes [7]. Although the world has already solved the information storage problem by the means of devices such as IBM’s System Storage TS3100® which has storage capacity of 36 TB and 6Gbps transference speed, and other solutions such as RAS, NAS, and RAID; there are still two issues that need attention: management and security.

For the first issue, there are state policies, standards and good practices that have been implemented using proprietary software tools (or free ones without complete documentation), that do not impact society with all its capacity. On the other hand, they do not conceive the problem of security from its real and total dimension, limiting it to an authentication service without other equally important features such as non-repudiation, integrity, access control and confidentiality. This is especially important as not everyone in an organization should be able to access, with the same privileges, to all the information; currently a lot of organizations manage classified information without the adequate restrictions. According to Seagate by 2020, 67% of the global data will require some security measure and by 2025 it will be 87% [7].

Despite the fact that Law 1273 of 2009 states penalties between 48 and 120 months in jail due to abusive access or publication of restricted data, this measure is not enough: Norton reports that by 2012 more than 9.7 million people were victims of computer crimes in Colombia and that they had direct financial losses in the amount of $79,180 million COP [8].

At the same time, our society walks towards a state of total dependence on digital information and government policies such as the digital notary, the “zero paper” law, the total availability of public information to citizens, the access to government databases through the internet, MINTIC’s open data initiative, and others, offer a democratization of this digital age.

According to the still in force UIT-T X.805-2003 recommendation: “The action of transmitting and storing information requires security measures of great importance, including confidentiality which prevents data from being disclosed without authorization and guarantees that unauthorized entities cannot understand the data content, as well as integrity in the information transmitted so as to ensure the availability of this to authorized users at the time they need it” [9]. Combination of these security services, with an adequate adoption of the legal framework, standards and security policies, reduces the risk of incidents in organizations.

It is of concern that despite the rapid evolution of technological systems, most companies, academic institutions and government entities in Colombia are still unable to provide optimal information security services. According to a survey conducted by ACIS (Colombian System Engineers Association), integrity loss (12,5%), information leakage (10,53%), and data theft (7,24%), sum up to 30,27% of security failures in the various productive sectors of the country, moreover there has been an accelerated growth compared to previous years [10].

**MODEL**

GISMOD was the name chosen for this project. In addition, the following premises were assumed for its design and development: the use of free software, the OWASP test guide [11], a strong security component and modular architecture, as well as the consideration of the normative framework and the context of higher education institutions.

In Colombia, the presidential decree 2609 of 2012 states that all document management systems in the country must include the following features: compliance, interoperability, security, meta-description, availability and access, content addition, design and functionality, distributed management, and technological neutrality [5]; which are indeed relevant features for the design of this kind of systems [12].

The conceptual design process led to the definition of GISMOD’s modules, which are presented in Table 2.

<table>
<thead>
<tr>
<th>MODULE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>There are two login options: web and biometry.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Communication
Defines communication parameters between Java and PHP modules (which are web services called from the client machine).

Alerts
Indicates the number of document transactions not known by the user.

Reports
Generation and configuration of reports by document type, dependency, confidentiality levels, access quantities. These reports can be exported to PDF.

Management
Allows CRUD (Create, Read, Update and Delete) operations for users, confidentiality levels, series and subseries, document types, etc.

Confidentiality validator
PHP module that validates the application of confidentiality and non-repudiation policies in the transactions requested by the users, according to defined access control tables (confidentiality levels).

It was required for the authentication module to be able to perform the multifactor process [15] [16] [17], which can be done via web (with a random keyboard on screen and a captcha), as well as using biometric authentication. This last option limits functionality according to security policies and confidentiality levels. Following, there is a use case for GISMOD’s multifactor authentication service.

<table>
<thead>
<tr>
<th>Table III. Confidentiality Levels Structure</th>
</tr>
</thead>
<tbody>
<tr>
<td>LEVEL</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
</tbody>
</table>

The following figure illustrates the graphical interface for the management module that allows CRUD operations for confidentiality levels defined in GISMOD.

For a focused application of document protection measures, a structure for confidentiality levels was determined, which are guaranteed by a confidentiality validation module. This structure is shown in Table III.

Figure 1. Use case for GISMOD’s multifactor authentication service.

For a focused application of document protection measures, a structure for confidentiality levels was determined, which are guaranteed by a confidentiality validation module. This structure is shown in Table III.

For a focused application of document protection measures, a structure for confidentiality levels was determined, which are guaranteed by a confidentiality validation module. This structure is shown in Table III.

Figure 2. Web interface for CRUD operations in confidentiality levels.

A management module, with support for document management, and transactions associated with documents,
users and security, was designed. This module can co-operate with all the other security modules as needed, as shown in the following use case.

**Figure 3.** General GISMOD use case.

**IMPLEMENTATION**

GISMOD was implemented as a distributed system which modules have been developed in different programming languages, such as Java, for the biometric login module web service, and PHP for the rest of the system. GISMOD uses PostgreSQL as a database system.

Java code was written using NetBeans IDE with original modules and libraries; for PHP, the Laravel 5 framework was used, along with some encryption and digital signatures libraries.

Following, the login options provided by the authentication module are presented.

First one is the biometric login (implemented in Java), second one is web login (written in PHP). Both options implement multifactor authentication.

**Figure 4.** Process diagram, multifactor login.

The operative system security was based on GNU/Linux kernel modules, for volume encryption (cryptsetup) and OpenSSL[18]. Apache was used as web server and application container, its SSL module was used for the encrypted channel. All the technologies used in the development are presented in Table V.

The system was developed in a workstation especially equipped with all the hardware and software requirements, as well as a test server, that was later deployed in production. The workstation was a Windows XP machine (in order to guarantee backward compatibility) with a Java development environment (a.).

Hardware components consist of a high-speed portable scanner (b.), a thermal adhesive label printer (c.), a biometric fingerprint reader (d.), a barcode reader (e.), and a laser printer (f.).

**Table IV.** Devices in GISMOD’s Client.

<table>
<thead>
<tr>
<th>Item</th>
<th>Component / Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>Computer (HP, 4GB RAM, 500 GB H.D. Intel Core i3 processor), with Windows OS.</td>
</tr>
<tr>
<td>b</td>
<td>Fujitsu Scansnap S1300 Scanner.</td>
</tr>
<tr>
<td>c</td>
<td>Dymo 450 Turbo Label Printer.</td>
</tr>
<tr>
<td>d</td>
<td>U Are U 4500 Digital Persona Fingerprint Reader.</td>
</tr>
<tr>
<td>e</td>
<td>Honeywell Ms 7120 Barcode Reader.</td>
</tr>
<tr>
<td>f</td>
<td>Samsung SCX-4300 Laser Printer.</td>
</tr>
</tbody>
</table>
The symmetric encryption and digital signature processes were implemented in PHP, using the mcrypt and gnupg libraries respectively. The following figure shows the encryption and decryption processes implemented in GISMOD in order to provide the confidentiality and non-repudiation services.

**Table V. Parameters for encryption in Gismod.**

<table>
<thead>
<tr>
<th>Item/Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cifrar</td>
<td>Encryption operation using AES rijndael algorithm.</td>
</tr>
<tr>
<td>descifrar</td>
<td>Decryption operation using AES rijndael algorithm.</td>
</tr>
<tr>
<td>Key</td>
<td>128 – 256 bits symmetric key.</td>
</tr>
<tr>
<td>Iv</td>
<td>Initialization vector for applying the CBC operation mode.</td>
</tr>
<tr>
<td>source</td>
<td>File with the document to be encrypted.</td>
</tr>
<tr>
<td>result</td>
<td>Encrypted/Decrypted resulting file.</td>
</tr>
</tbody>
</table>

GISMOD’s encryption is defined and applied as follows:

\[
cifrar_{\text{Key,iv}}(\text{source}) = \text{result} \quad (1)
\]

Decryption is defined and applied in the following way:

\[
descifrar_{\text{Key,iv}}(\text{result}) = \text{source} \quad (2)
\]

The user has access to a management interface in which parameters for each level can be adjusted; these levels can also be created or deleted.
The digital signature process and its verification were based in the DSA asymmetric encryption with a 2048 bits key, incorporating GnuPG (gpg) as a PHP module in the application.

Signature:

\[ gnupg\_sign_{KS_u}\{\text{Hash}(\text{contenidoArchivo})\} = \text{archFirmado} \] (3)

Table VI. Parameters for Digital Signature on GISMOD

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>gnupg_sign</td>
<td>Signature function in GnuPG</td>
</tr>
<tr>
<td>KS_u</td>
<td>GISMOD user private key.</td>
</tr>
<tr>
<td>Hash</td>
<td>SHA-1 hash.</td>
</tr>
<tr>
<td>ContenidoArchivo</td>
<td>File which contains the document to be digitally signed.</td>
</tr>
<tr>
<td>ArchivoFirmado</td>
<td>Digitally signed document.</td>
</tr>
</tbody>
</table>

Finally, the ‘reports’ module was implemented based on the system’s transaction logs, which can be accessed in real time, and exported by document type, dependency, confidentiality level, and access quantities.

Reports can also be exported in PDF format (doompdf library).

Next, the software technologies used in GISMOD’s development are presented, each one with the module where it was used, its license type, kind of technology and a description of its usage.

Table VII. GISMOD’S Modules Description.

<table>
<thead>
<tr>
<th>MODULE/COMPONENT</th>
<th>TOOL</th>
<th>LICENCE</th>
<th>TYPE</th>
<th>USAGE DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Biometric authentication and verification</td>
<td>Java – JDK 1.7</td>
<td>JRL</td>
<td>Programming language</td>
<td>Environment where the GISMOD’s biometric system was developed.</td>
</tr>
<tr>
<td>Web authentication</td>
<td>Simple – captcha</td>
<td>MIT</td>
<td>Library</td>
<td>Captcha generation for protection against robots that try to decipher passwords by brute force.</td>
</tr>
</tbody>
</table>
MÓDULE/COMPONENT | TOOL | LICENSE | TYPE | USAGE DESCRIPTION
--- | --- | --- | --- | ---
Biometric authentication and verification | U.are.U SDK for Windows | EULA | Software development kit. | SDK for the usage of the persona U.are.u 4500 reader, provision of fingerprint recognition keys.
Persistence | PostgreSQL | PostgreSQL | Database system | Database system used in admin, server and client.
Document Management | LARAVEL 5 | MIT | Framework | PHP Framework in which the GISMOD’s management system was developed.
Server/Communication | Debian GNU/Linux Squeeze | GNU/GPL | Operative system | Server’s operative system.
Server/Administrator | Apache | Apache 2.0 | Web server | Web server where GISMOD is deployed.
Document management/Authentication | php5 | GNU/GPL | PHP Interpreter module | GISMOD’s development environment, authentication web service, and Mcrypt extension for hashing, encryption and digital signatures.
Authentication | NetBeans 8.0.1 | GPL2 | IDE, Development software | Integrated development environment used for the development of GISMOD’s biometric system.
Modeling | Er-master | BSD | Plugin – Eclipse | Graphical ER diagram editor used for GISMOD.
Modeling | StarUML | GNU/GPL | Software application | Generation of use case diagrams and sequences, based on UML.
Reports/Statistics | HighCharts | Creative Com Att- NonCo3. | PHP Library | Used for the generation of graphics for anomaly reports.
Reports/Statistics | DOMPDF | LGPL | Library | For reports in PDF format.

### DISCUSSION

In this section, a use case applied in the Faculty of Basic Sciences and Engineering at the University of the Llanos, which has more than 800 students and 60 full-time professors, is presented. This amount of students and professors causes large flows of information related to academic processes, correspondence, administrative documents, etc.

The physical resources for the use case are the same already defined in Table VIII, in addition to one server (a.) and two work stations (b.).

GISMOD was loaded with data from 30 dependencies of the Faculty of Basic Sciences and Engineering, as shown in the next figure.

![Figure 14. CRUD management module for dependencies, loaded.](image)

Public and private user keys were generated, taking the users ‘elvis /Decano’ (4) and ‘Felcorredor (Felcor)/directorGITECX’ (5) as references, through GPG, which were exported in flat files.

\[
GPG(\text{gen.key, decano}) = elvis.gpg \{K_{\text{elvis}} | K_{\text{elvis}} \} \tag{4}
\]
GPG(gen.key, docente) = 
\[ f_{\text{felcorredor}.gpg} \{ K_{P_{\text{felcor}}} | K_{S_{\text{felcor}}} \} \] (5)

Figura 15. List of GPG public keys for users ‘Decano’ and ‘Director GITECX’.

Plain text in the key files (llave.elvis.gpg and llave.felcorredor.gpg) simplifies its manipulation for reading and transmission to upload them to the Postgres database server, during the process of user creation, using GISMOD’s web interface.

Figure 16. Verification of key upload, through Postgres database.

Officials invited to the functionality and performance tests, interacted with the PHP web interface and the Java front-end, using both login ways. GISMOD was installed in six computers of the Faculty and in the Open Technologies Laboratory – GITECX.

Figure 17. Faculty officials interacting with GISMOD.

A detailed verification of a complete document management process was done, performing the trace to a confidential document, which consisted of an act without approval and was assigned the maximum confidentiality level (Level 5, AES 256 bits encryption in CBC mode, digital signature on the document, fingerprint verification, encrypted SSL channel transmission, and document permission verification). The document was sent by user ‘felcorredor/DirectorGITECX’ to user ‘elvis/Decano’.

Figure 18. GITECX’s director uploading the document to the system.

Once ‘felcorredor/DirectorGITECX’ (document sender) has logged in, the received documents area is displayed and the alerts module notices the presence of eight new documents (top-right corner).

The sending process starts when the document is created in GISMOD, dragging the document “ACTA No.02.docx” to the upload area, and its features such as type (Act), confidentiality level (5 – maximum), document receiver (‘elvis/Decano’) are parameterized.

Figure 19. Document upload module, uploading “ACTA No. 02.docx”.

The web interface allows the parameterization of type, permissions, conservation unit, confidentiality level, and the assigned receiver user.
Users are associated with one or more dependencies, in this case it was already done and the user ‘elvis/Decano’ could be assigned immediately.

Verification is done both in the sender user’s document output area and in the recipient user’s input area. The policies application process is executed on the server (AES encryption and DSA digital signature) and on the client (reading, modification and deletion permissions, as well as biometric identity confirmation).

Finally, all the access possibilities to the “ACTA No.2.docx” document were verified both from the web interface and from the Debian GNU/Linux server file system, evidencing full compliance with the security policy, AES encryption application, DSA digital signature and biometric identity verification.

These security mechanisms implemented from GISMOD help to mitigate the risks of crimes and fraud on corporate information, as well as to improve the accuracy of the transactions carried out, integrity, confidentiality, data encryption, and support to security and non-repudiation policies in DMS [20].

**CONCLUSIONS**

This project presented a technological alternative that shows the possibility of designing and building a tool applicable to document transactional processes, in any organization that requires strict implementation of confidentiality, availability and non-repudiation services.

Modularity and integration of a security component on each module are GISMOD features that will allow for its reutilization and the adoption of more complex mechanisms in future versions, based widely on open source software.

Technologies and security mechanisms such as digital signatures, multifactor authentication, fingerprint biometry, data encryption and channel security layers are insufficient measures if not oriented from the legal framework and adequate security policies.
ACKNOWLEDGEMENTS

The authors express their gratitude to God and their families for always supporting this project. In the same way, it is important to note that this work would not have been possible without the financial support of the University of the Llanos.

REFERENCES


