# Protecting sensitive information

—


Team members

Ramírez Fuentes Edgar Alejandro

Rodríguez Melgoza Ivette

Salmerón Contreras María José

# Table of contents

## Problem to solve

The CEO of a certain company is promoting less use of paper. He wishes that sensitive documents be digital. Thus, these documents usually are signed by the board of directors (a group of people that take decisions in the company). Also only the board of directors can see the content of these sensitive documents. They do not want to share a unique key, i.e. every member of the board must have her/his own key or keys. Imagine that your team is hired to develop a solution for this company.

## Cryptographic services

- ### Privacy

  This service will be useful to hide the information that each sensitive document contains. As mentioned in the problem to solve, only the board of directors will be able to see the content, and privacy is the service that will help us to hide the information from any other user that does not belong to the board of directors.

- ### Integrity

  As mentioned before the documents contain sensitive data that must not be altered in any way. That is why our system must provide integrity and keep the data without any alteration by a third party.

- ### Non-repudiation

  The problem to solve mentions that the documents are usually signed by the board of directors, which means that the system should implement a way to help the users to sign a certain document and prevent them from denying previous commitments or actions.

- ### Authentication

  To guarantee that each entity in a communication is who it claims to be, we propose a login with a secret password which is going to be hashed with SHA3, implementing this the communication is authenticated.

## Cryptographic primitives

- ### RSA-PSS

  RSA Probabilistic Signature Scheme (PSS) will be used as cryptographic primitive to the cryptographic service of Non-repudiation and Integrity, specifically in the part of the sign used for the documents. PSS was specifically developed to allow modern methods of security analysis to prove that its security directly relates to that of the RSA problem. [1]

- ### SHA-3

  SHA-3 will be used in the login of our system to hash the password of our users, and in the process of signing a document. It will help us to provide privacy to our users.

- ### AES

  Privacy is covered using AES, which is the cryptographic algorithm responsible for encrypting and decrypting the sensitive documents.

## System architecture

The next figure shows the architecture of our system, it is easy to find the cryptographic primitives that we use and where in the program is used.

All starts with the sender and the pdf document, it is necessary to sign the document before is saved in the database, for that we use SHA-3 to hash the document and RSA- PSS (Probabilistic digital signature) to sign it, then the sign is saved in the database. In another thread, the pdf document is ciphered using a hybrid scheme (RSA/AES) and it is sent to the receiver.

The receiver deciphers the document using the same hybrid scheme and then using SHA-3 to compare this hashed message with the one saved in the database, if both are equal then the message is authentic if not, the message is not authentic.

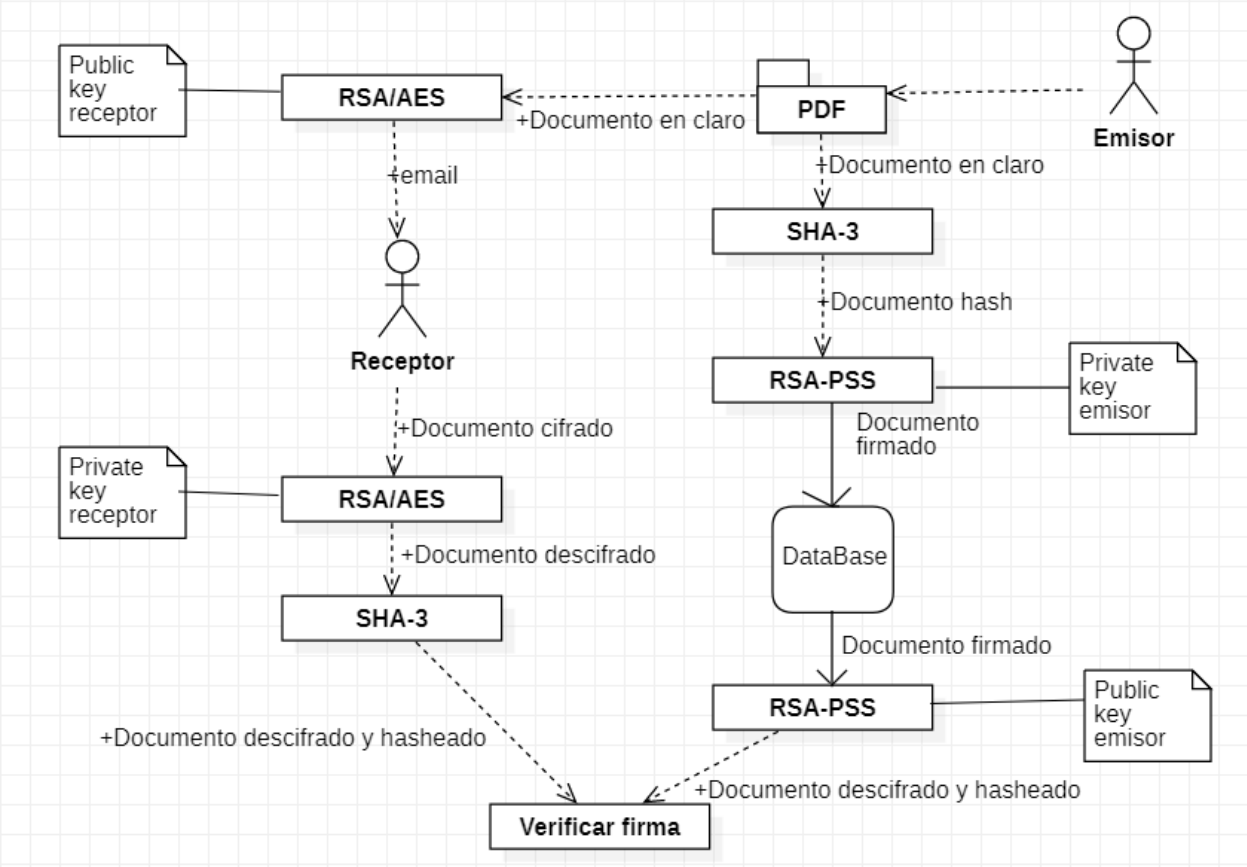


Figure 1. System Architecture

## Introduction to the system

## Requirements

## References

[1] Wikipedia, «Probabilistic signature scheme,» [En línea]. Available: https://en.wikipedia.org/wiki/Probabilistic_signature_scheme.

C. Paar and J. Pelzl, *Understanding Cryptography*, 1st edition, Springer, 2010