

AISS Secure Mail

Gonalo Carito
Instituto Superior Tcnico
Drio Nascimento
Instituto Superior Tcnico

Applications and Implementations of Security Systems
May 27, 2013



TCNICO
LISBOA

Outline

1 Overview

Motivation
Requirements
Goals
Related Solutions
Challenges

2 System architecture

3 Results

4 Future Work

5 Conclusions

Overview

Motivation
Requirements
Goals
Related Solutions
Challenges

System
architecture

Results

Future Work

Conclusions

1 Overview

Motivation
Requirements
Goals
Related Solutions
Challenges

Overview

Motivation
Requirements
Goals
Related Solutions
Challenges

System architecture

Results

Future Work

Conclusions

2 System architecture

3 Results

4 Future Work

5 Conclusions

Motivation

Overview

Motivation

Requirements

Goals

Related Solutions

Challenges

System

architecture

Results

Future Work

Conclusions

- **Wikileaks: 400.000 Top-Secret American Army Documents published**
- Internet - Main Enterprise Communication Mean



Overview

Motivation

Requirements

Goals

Related Solutions

Challenges

System architecture

Results

Future Work

Conclusions

AISS Secure Mail provides:

- Hidden Text & Attachments (*Confidentiality*)
- *Non-repudiation & Authenticity & Integrity*: Sender Authentication via Citizen Card
- Email Sending Time Assurance

Overview

Motivation

Requirements

Goals

Related Solutions

Challenges

System architecture

Results

Future Work

Conclusions

- User-friendly program
- Compatible with file based applications
- Mac OS X Compatible
- Good performance

Related Solutions

Overview

Motivation
Requirements
Goals
Related Solutions
Challenges

System architecture

Results

Future Work

Conclusions

Comparison with other solutions:

Related Solutions	Our Solution
Thunderbird interface	Generic Application Support
Manual Decipher Options	Automatic Process

Overview

Motivation

Requirements

Goals

Related Solutions

Challenges

- Memory Constraints
- Efficiency
- Unstable Citizen Card library

System architecture

Results

Future Work

Conclusions

Outline

1 Overview

Motivation
Requirements
Goals
Related Solutions
Challenges

Overview

Motivation
Requirements
Goals
Related Solutions
Challenges

System architecture

Results

Future Work

Conclusions

2 System architecture

3 Results

4 Future Work

5 Conclusions

System architecture

Overview

Motivation
 Requirements
 Goals
 Related Solutions
 Challenges

System architecture

Results

Future Work

Conclusions

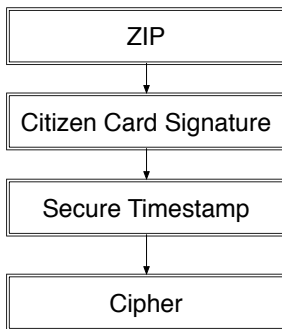


Figure 1: System Architecture architecture.

AISS Secure Mail

Zippping

Overview

Motivation
Requirements
Goals
Related Solutions
Challenges

System architecture

Results

Future Work

Conclusions

- All files and folder inside a directory are zipped;
- Support any file size
- Single file output

AISS Secure Mail

Citizen Card Signature

- PKCS11 Portuguese Citizen Card
- SHA-1, RSA

Overview

Motivation
Requirements
Goals
Related Solutions
Challenges

System architecture

Results

Future Work

Conclusions

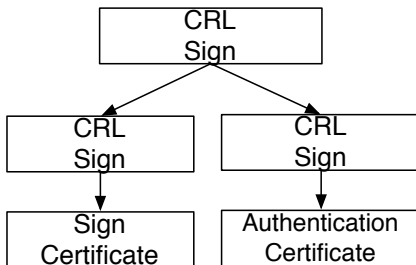


Figure 2: Certificate Tree

AISS Secure Mail

Secure Timestamp

Overview

Motivation
Requirements
Goals
Related Solutions
Challenges

System architecture

Results

Future Work

Conclusions

- Remote Raspberry Pi Server;
- Self signed RSA Keys;
- SHA-256;
- Retrieve hash from User and sign it
- Output: $K_p(H(m), T), T$

Overview

Motivation
Requirements
Goals
Related Solutions
Challenges

System architecture

Results

Future Work

Conclusions

Cipher using ethernet box:

- JNI + C Connection;
- Block update;
- All data in memory;

Outline

1 Overview

Motivation
Requirements
Goals
Related Solutions
Challenges

Overview

Motivation
Requirements
Goals
Related Solutions
Challenges

System architecture

Results

Future Work

Conclusions

2 System architecture

3 Results

4 Future Work

5 Conclusions

Overview

Motivation
Requirements
Goals
Related Solutions
Challenges

System architecture

Results

Future Work

Conclusions

Environment

- MacBook Pro 2.9 GHz Intel Core i7
- 8 GB memory 1600 MHz DDR3, SSD disk
- Mac OS X 10.8.3

Performance metrics

- *286 documents (PDF and Word)*
- *Total Size: 100 MBytes*

Results

Trace-driven simulation experiments

Overview

Motivation
Requirements
Goals
Related Solutions
Challenges

System architecture

Results

Future Work

Conclusions

Compression: 100MB to 95.5MB.

Cipher/Decipher: 100MB in 60 seconds

Sending: 6 seconds ¹

Reception: 3 seconds

¹excluding cipher

Results

Trace-driven simulation experiments

Overview

[Motivation](#)
[Requirements](#)
[Goals](#)
[Related Solutions](#)
[Challenges](#)

System architecture

Results

Future Work

Conclusions

Phase	Time (ms)	St. Deviation (ms)
Compression	4484	30
Hashing	700	10
Signature	936	24
Timestamp	70	5
To Base64 Write	1335	35
From Base64	1380	32
Timestamp Check	32	6
Signature Check	6	3

Outline

1 Overview

Motivation
Requirements
Goals
Related Solutions
Challenges

2 System architecture

3 Results

4 Future Work

5 Conclusions

Overview

Motivation
Requirements
Goals
Related Solutions
Challenges

System architecture

Results

Future Work

Conclusions

Overview

Motivation
Requirements
Goals
Related Solutions
Challenges

System architecture

Results

Future Work

Conclusions

This work contributes to future research directions:

- Change to file on disk update;
- Buy CA certificate for secure timestamp;
- Full Integration with Thunderbird and Gmail
- Drag & Drop interface

Outline

1 Overview

Motivation
Requirements
Goals
Related Solutions
Challenges

2 System architecture

3 Results

4 Future Work

5 Conclusions

Overview

Motivation
Requirements
Goals
Related Solutions
Challenges

System architecture

Results

Future Work

Conclusions

Conclusions

Overview

Motivation
Requirements
Goals
Related Solutions
Challenges

System architecture

Results

Future Work

Conclusions

- Confidentiality
- Integrity
- Non-repudiation & Authenticity
- Secure Timestamp (Premium)
- User-friendly

Overview

Motivation
Requirements
Goals
Related Solutions
Challenges

System architecture

Results

Future Work

Conclusions

Thank you!

Q&A