AISS Secure Mail

Gonçalo Carito
Instituto Superior Técnico

Dário Nascimento
Instituto Superior Técnico

Applications and Implementations of Security Systems
May 28, 2013

TÉCNICO
LISBOA

TÉCNICO LISBOA

Outline

Outline

Motivation

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

Requirements

AISS Secure Mail provides:

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

TÉCNICO LISBOA

Goals

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

Related Solutions

Comparation with other solutions:

- Bounded to Email Applications

Challanges

- Memory Constraints
- Efficiency
- Unstable Citizen Card library

Outline

System architecture

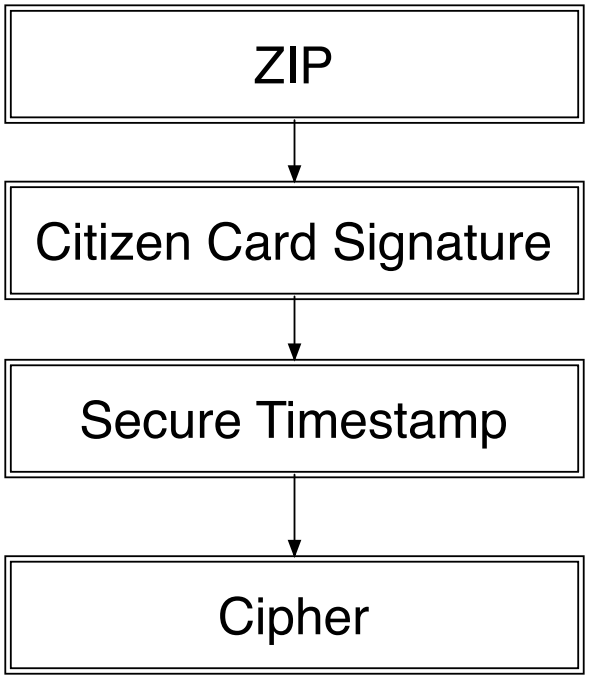

Figure 1: System Architecture architecture.

AISS Secure Mail

Zipping

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

AISS Secure Mail

Citzen Card Signature

- PKCS11 Portuguese Citizen Card
- SHA-1, RSA
- Sender Identification
- Signature Validation

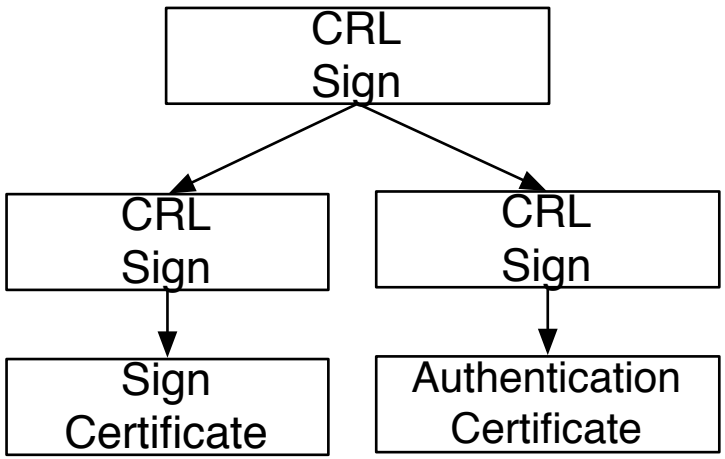

Figure 2: Certificate Tree

AISS Secure Mail

Secure Timestamp

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

AISS Secure Mail

Cipher

Cipher using ethernet box:

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

TÉCNICO LISBOA

Outline

Results

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

Compression: 100MB to 95.5MB.
Cipher/Decipher: 100MB in 60 seconds

Sending: 6 seconds [1]
Reception: 3 seconds

[1] excluding cipher

TÉCNICO LISBOA

Results

Trace-driven simulation experiments

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

Future Work

This work contributes to future research directions:

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

Outline

Conclusions

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

TÉCNICO LISBOA

Thank you!

Q&A