AISS Secure Mail

Gonçalo Carito
Instituto Superior Técnico

Dário Nascimento
Instituto Superior Técnico

Applications and Implementations of Security Systems
May 14, 2013

TÉCNICO
LISBOA

TÉCNICO LISBOA

Outline

1. **Overview**
   - Motivation
   - Requirements
   - Goals
   - Related Solutions
   - Challanges
2. **System architecture**
3. **Results**
4. **Future Work**
5. **Conclusions**

Outline

1. Overview
   - Motivation
   - Requirements
   - Goals
   - Related Solutions
   - Challanges
2. System architecture
3. Results
4. Future Work
5. Conclusions

Motivation

Overview
Motivation
Requirements
Goals
Related Solutions
Challanges
System architecture
Results
Future Work
Conclusions

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

TÉCNICO LISBOA

Requirements

Overview
Motivation
Requirements
Goals
Related Solutions
Challanges
System architecture
Results
Future Work
Conclusions

AISS Secure Mail provides:

- Hidden Text & Attachments;
- Sender Authentication via Citizen Card
- Email Sending Time Assurance
- Secure Email Exchange

TÉCNICO LISBOA

Goals

Overview
Motivation
Requirements
Goals
Related Solutions
Challanges
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
Challanges
System architecture
Results
Future Work
Conclusions

Comparation with other solutions:

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

Challanges

Overview
Motivation
Requirements
Goals
Related Solutions
Challanges
System architecture
Results
Future Work
Conclusions

- Memory Constraints
- Efficiency
- Unstable Citizen Card library

Outline

1. Overview
   - Motivation
   - Requirements
   - Goals
   - Related Solutions
   - Challanges
2. System architecture
3. Results
4. Future Work
5. Conclusions

System architecture

Overview
Motivation
Requirements
Goals
Related Solutions
Challanges
System architecture
Results
Future Work
Conclusions

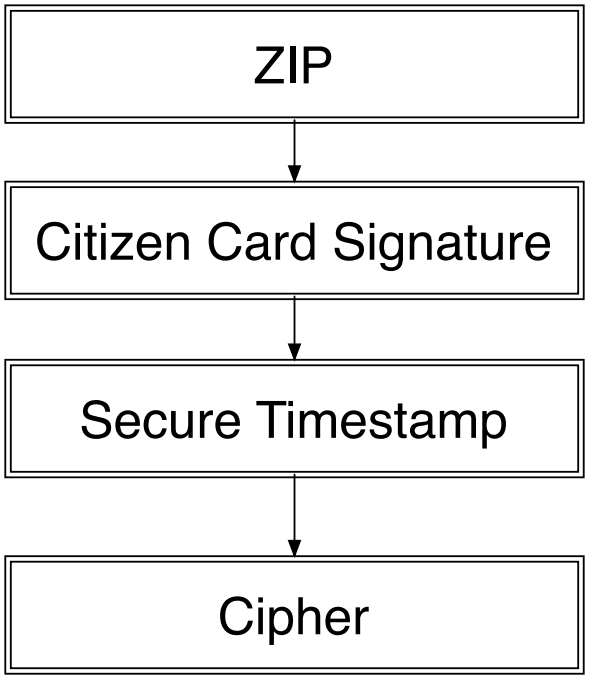

Figure 1: System Architecture architecture.

AISS Secure Mail

Zipping

Overview
Motivation
Requirements
Goals
Related Solutions
Challanges
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

Citzen Card Signature

- PKCS11 Portuguese Citizen Card
- SHA-1, RSA

Overview
Motivation
Requirements
Goals
Related Solutions
Challanges
System architecture
Results
Future Work
Conclusions

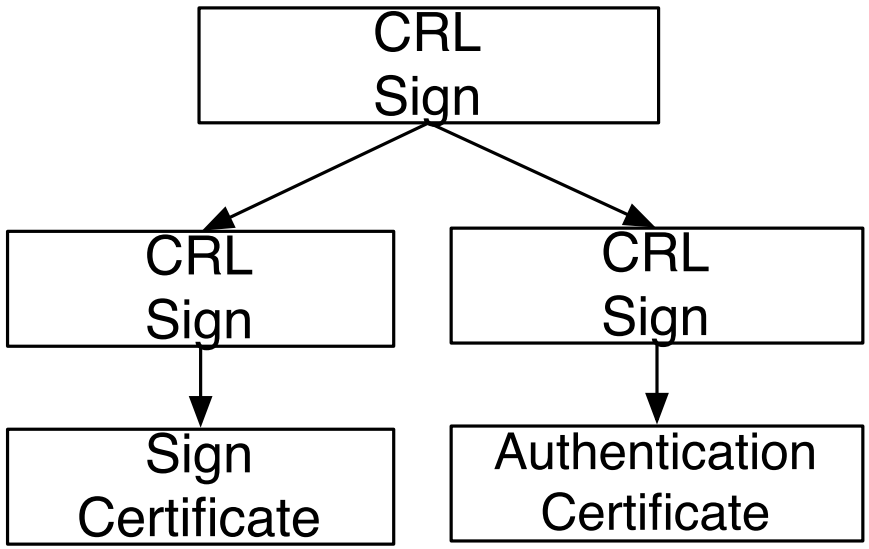

Figure 2: Certificate Tree

AISS Secure Mail

Secure Timestamp

Overview
Motivation
Requirements
Goals
Related Solutions
Challanges
System architecture
Results
Future Work
Conclusions

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

AISS Secure Mail

Cipher

Overview
Motivation
Requirements
Goals
Related Solutions
Challanges
System architecture
Results
Future Work
Conclusions

Cipher using ethernet box:

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

TÉCNICO LISBOA

Outline

1 Overview
- Motivation
- Requirements
- Goals
- Related Solutions
- Challanges

2 System architecture

3 Results

4 Future Work

5 Conclusions

Results

Overview
Motivation
Requirements
Goals
Related Solutions
Challanges
System architecture
Results
Future Work
Conclusions

Fazer um teste para ver quanto tempo a zippar Quanto tempo a assinar Quanto tempo a cifrar Isto para um ficheiro grande
Tempo de utilização para uma pessoa comum

TÉCNICO LISBOA

Results

Trace-driven simulation experiments

Overview
Motivation
Requirements
Goals
Related Solutions
Challanges
System architecture
Results
Future Work
Conclusions

Simulation

- IBM Thinkpad T22
- HP's Chai JVM (limited to 7/8 Mbytes of Heap Size)

Performance metrics

- *Total offloading delay*
- *Average interaction stretch*
- *Total bandwidth requirement*

TÉCNICO LISBOA

Results

Trace-driven simulation experiments

Overview
Motivation
Requirements
Goals
Related Solutions
Challanges
System architecture
Results
Future Work
Conclusions

Results

Prototype experiments

Overview
Motivation
Requirements
Goals
Related Solutions
Challanges
System architecture
Results
Future Work
Conclusions

Mobile Device (emulated)

- 266 MHz HP laptop;
- 11 Mbps 802.11b

Surrogate

- 733 MHz HP Kayak PC workstation
- 128 Mbytes of RAM

Network

- 10Mbps

TÉCNICO LISBOA

Results

Prototype experiments

Overview
Motivation
Requirements
Goals
Related Solutions
Challanges
System architecture
Results
Future Work
Conclusions

TÉCNICO LISBOA

Results

Prototype experiments

Overview
Motivation
Requirements
Goals
Related Solutions
Challanges
System architecture
Results
Future Work
Conclusions

Offloading, constrained memory

- 1.5% - 5.7% more slow;
- Cost of monitoring, remote accesses and partitioning increases the execution time.

Outline

1. Overview
   - Motivation
   - Requirements
   - Goals
   - Related Solutions
   - Challanges
2. System architecture
3. Results
4. Future Work
5. Conclusions

Future Work

Overview
Motivation
Requirements
Goals
Related Solutions
Challanges
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;
- Integration with Thunderbird and Gmail
- Drag Drop interface

Outline

1. Overview
   - Motivation
   - Requirements
   - Goals
   - Related Solutions
   - Challanges
2. System architecture
3. Results
4. Future Work
5. Conclusions

Overview
Motivation
Requirements
Goals
Related Solutions
Challanges
System architecture
Results
Future Work
Conclusions

Conclusions

Overview
Motivation
Requirements
Goals
Related Solutions
Challanges
System architecture
Results
Future Work
Conclusions

- Pervasive application delivery with fidelity;
- Avoid expensive application rewriting;
- **What**: Efficient partition selecting
- **When**: Fuzzy Control Model to achieve adaptability, stability and configurability;
- **Where**: Modified Java Virtual Machine
- **How**: Remote Process Call - RPC
- Relieve memory constraints for mobile devices.

TÉCNICO LISBOA

Overview
Motivation
Requirements
Goals
Related Solutions
Challanges
System architecture
Results
Future Work
Conclusions

Thank you!

Q&A