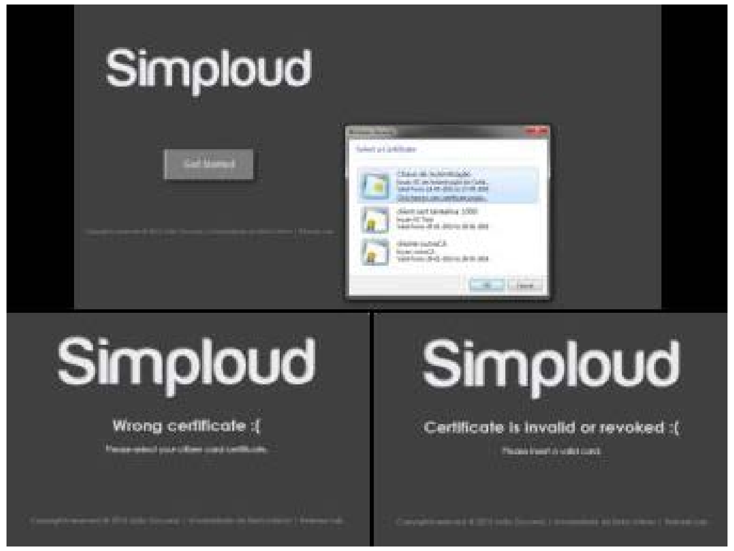
PRICE

Privacy, Reliability and Integrity in Cloud Environments

This project focused on the privacy, reliability and integrity of data in cloud environments. Diverse security and privacy problems associated with the use of cloud storage by private and commercial entities were investigated. Applications using novel cryptographic techniques in order to enforce security policies over data shared by multiple users on cloud storage applications were developed.


Simploud

Simploud

Wrong certificate :(

Simploud

Certificate is invalid or revoked :(

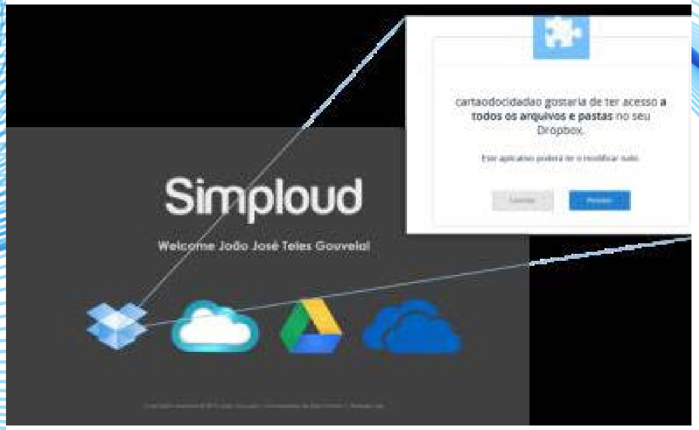
Main Project Team	
Paul Crocker	**NAP-Cv**
Simão Melo de Sousa	UBI
João Silveira	IT Covilhã
João Gouveia	IT Covilhã
VITOR PEREIRA	IT Covilhã
Adolfo Peixinho	IT Covilhã
Ricardo Azevedo	PT Inovação SA
Funding Agencies	
Portugal Telecom Inovação SA	**20,000€**
Start Date	01/09/2012
Ending Date	01/09/2013
Indicators	
Conference Papers	4
Concluded MSc	3

Two Main Publications

J. Gouveia, P. Crocker, S. Melo de Sousa, **E-Id Authentication and Uniform Access to Cloud Storage Service Provider**s, IEEE International Conference on Cloud Computing Technology and Science - CloudCom, Bristol, United Kingdom, Vol. 5, pp. 1 - 10, December, 2013

V.P. Pereira, S. Melo de Sousa, P. Crocker, **Criptografia Homomórfica como um Serviço: da Implementação à sua Aplicação,Inforum** - Simpósio de Informática, Evora, Portugal, Vol. 5, pp. 383 - 394, September, 2013

PROJECT WEBPAGE URL
https://spocs.it.ubi.pt/price/


Simploud

Welcome João José Teles Gouveia!

cartaodocidadao gostaria de ter acesso a **todos os arquivos e pastas** no seu Dropbox.

Este aplicativo poderá ler e modificar tudo.

Fig. 1 The simpcloud application.

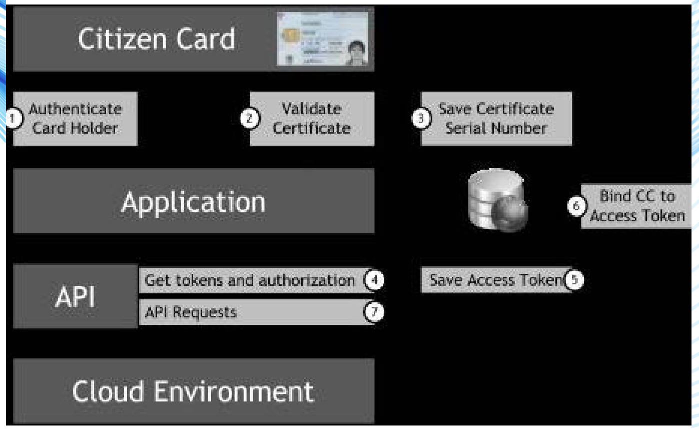

Citizen Card
1 Authenticate Card Holder
2 Validate Certificate
3 Save Certificate Serial Number
Application
6 Bind CC to Access Token
API
Get tokens and authorization 4
API Requests 7
Save Access Token 5
Cloud Environment

Fig. 2 Smart card authentication.

GENERAL MOTIVATION AND OBJECTIVES

Due to its large storage and processing capabilities, which are accessed transparently by end users with little or no concerns about the underlying technology, the cloud offers a natural solution to store and manage ever growing amounts of data. Nonetheless, it is obvious that the decision to send privacy sensitive data such as medical data (patient data, images etc.) leads to several security concerns that need to be carefully considered in order to protect the privacy of the patients. Other associated issues concerning data files shared by several cloud users has to do with the privacy and confidentiality properties of these files, when and how can then be accessed for instance. This project is precisely focused on those issues allowing enterprises to define data access policies and increase confidence in Cloud storage services.

The project addresses fundamental aspects of cloud computing and elaborates on the specific security and privacy requirements of cloud data and on how to assure that such data remains private and unaltered after being sent to the cloud and how it may be accessed by multiple users. The main motivation for this project came from the industrial partner PT Inovação SA which wished to research how novel cryptographic mechanisms could be applied to enhance privacy, reliability and integrity in cloud environments. PT is a Portuguese Telecoms company with several different cloud based solutions including for instance the MeoCloud storage application, virtual cloud based disks and cloud computing services.

CHALLENGE

The challenge of this project was to develop novel applications libraries and middleware's that leveraged existing mechanisms such as the national e-id frameworks for strong authentication as well as making use of novel cryptographic mechanisms. One of the main challenges was how to integrate these strong authentication mechanisms into easy to use software libraries and then use these libraries to develop, in collaboration with the projects partners, various proof of concept and useful applications. Another challenge was to suggest solutions for the problems associated with using multiple identities over multiple cloud services using two factor cryptographic tokens.

WORK DESCRIPTION AND ACHIEVEMENTS

Several end user demonstrator applications were developed. In particular SimpCloud a cloud Service that aggregates various cloud storage service provider was developed to make use of the strong identity services provided by national e-id smart cards to provide cryptographic resources for network communications and encrypted file services. This application permits the use of standard smart card based authentication mechanisms, standard cloud based authorization protocols and is compatible with a wide range of cloud service providers as well as attaching so called sticky security polices to shared cloud files. Applications were also developed to exploit less well known cryptographic mechanisms such as secret sharing and homomorphic encryption techniques. In particular a case study was developed that consists of a cloud-based inquiry/questionnaire application with homomorphic statistical inquires (Azure/Sql) and a Secret Sharing Web Based Framework was also developed for managing shared authentication and access rights or for accessing encrypted and signing documents needing only a subset of users.