Cyphertext Policy Attribute Based Encryption

User Manual

Document Owner:	Fincons SpA
Publication Date:	01/10/2016
Version:	v1.0

VERSION HISTORY

NBR	DATE	NOTES AND COMMENTS
v1.0	01/10/2016	First Version

DOCUMENT ACRONYMS AND DEFINITIONS

	Full Name/Explanation
PROVIDER	Fincons SpA
SOFTWARE PRODUCT	Cyphertext Policy Attribute Based Encryption

Contents

List of Figures

1 Software Disclaimer

This SOFTWARE PRODUCT is provided by the PROVIDER "as is" and "with all faults." The PROVIDER makes no representations or warranties of any kind concerning the safety, suitability, lack of viruses, inaccuracies, typographical errors, or other harmful components of this SOFTWARE PRODUCT. There are inherent dangers in the use of any software, and you are solely responsible for determining whether this SOFTWARE PRODUCT is compatible with your equipment and other software installed on your equipment. You are also solely responsible for the protection of your equipment and backup of your data, and the PROVIDER will not be liable for any damages you may suffer in connection with using, modifying, or distributing this SOFTWARE PRODUCT.

2 Introduction

The purpose of this software system is to provide a CP-ABE (Ciphertext Policy Attribute Based Encryption) based service to protect information using more sophisticated encryption techniques that avoid having to share keys among users and that can encrypt the information according to a specific access policy the encrypting user has to specify.

Access policies specify which characteristics the user's profiles must have in order to be able to decrypt the file. When generating a user's decryption key, the ABE Service takes into account the user's profile, stored in an LDAP service, to generate the user's key. When decrypting the protected information, the user has to provide his/her decryption key and the decryption process will succeed only if the user's characteristics (i.e., user's profile attributes) used to generate the decryption key meet the access policy embedded in the protected information (encrypted file). The ABE Service uses an LDAP server to store user's profiles.

The ABE platform provides (bulleted list with the gear icon layout):

- **Registration and Login feautures**

This features permit to register new users and the access to encryption/decryption functionalities

- **Policy Generation and Encryption**

this function requires the provision of an input the file to be encrypted and of the access policy to be used to encrypt the file through a graphical editor. These information are uploaded to the service that returns the encrypted file with cpabe file extension.

- **Key Generation**

Generates the personal decryption key for the logged in user. The generated key is based on the user's attributes as stored in the LDAP server.

- **Decryption**

The user uploads the encrypted file and provides his/her Personal Decryption Key. If the key satisfies the access policy the file decryption will succeed and the user will be prompted to download and save the decrypted file.

3 User Manual

3.1 Registration

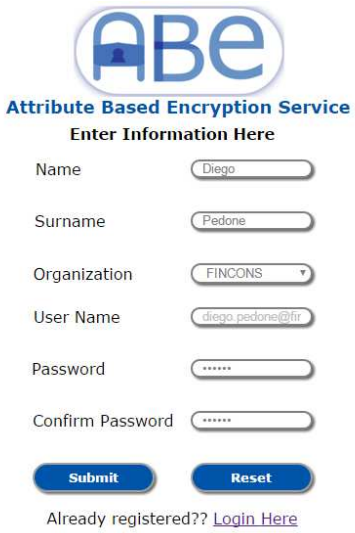

Figure 1 - ABE Registration Form

In this page the user can register. The user must insert all the fields and that fields are the main attributes of the user. As User Name the user must specify an e-mail address so to assure having a unique attribute for LDAP searches. In case of error the service redirects the user to the error page. All the form sections have a form validation mechanism to guide the user during the data imputation.

3.2 Login

Figure 2 - ABE Login Form

In this page the user can login, providing the Username (i.e., his/her e-mail address). The service first verifies the user is actually present in the LDAP and, if so, enables the Password field. After clicking the Login button the service authenticates the user and redirect the user to the service's functionalities page in case of success.

3.3 Encryption

If the login operation has success, the user will be redirect to the Home Page that provides three different sections (tabs). The first tab is the Encrypt tab:

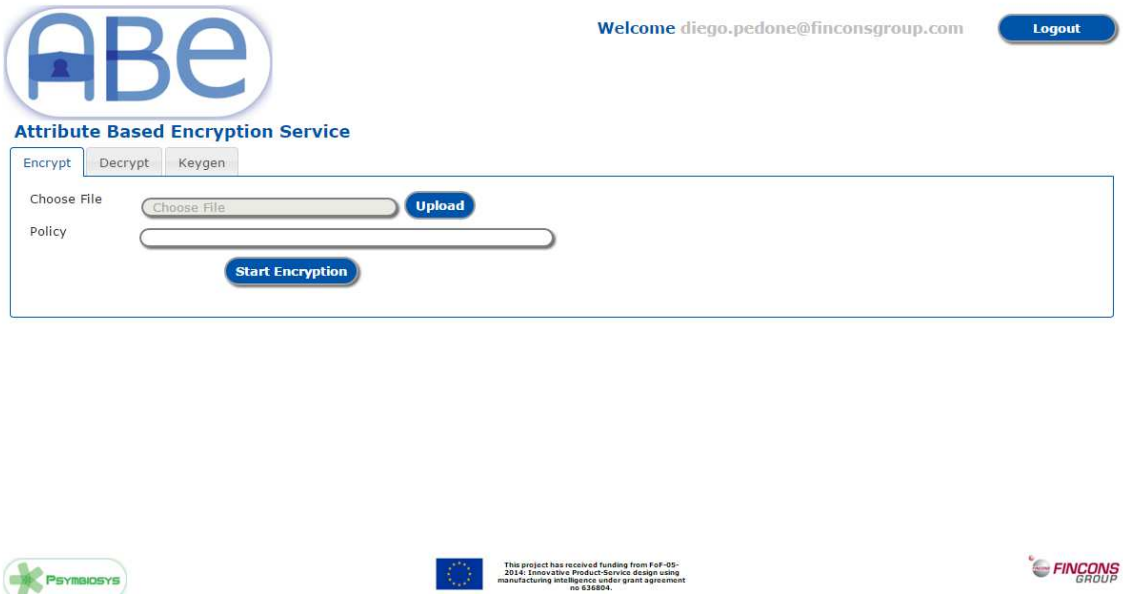

Figure 3 - ABE Encryption Tab

In this tab the user can select and upload the file to encrypt using the Upload button, and then specify the access policy in the Policy text area. When the user has completed the form, he/she has to click the Start Encryption button to actually upload and encrypt the file. If the encryption does not have unexpected errors the service starts downloading the encrypted file and the user is prompted to save it locally.

3.4 Decryption

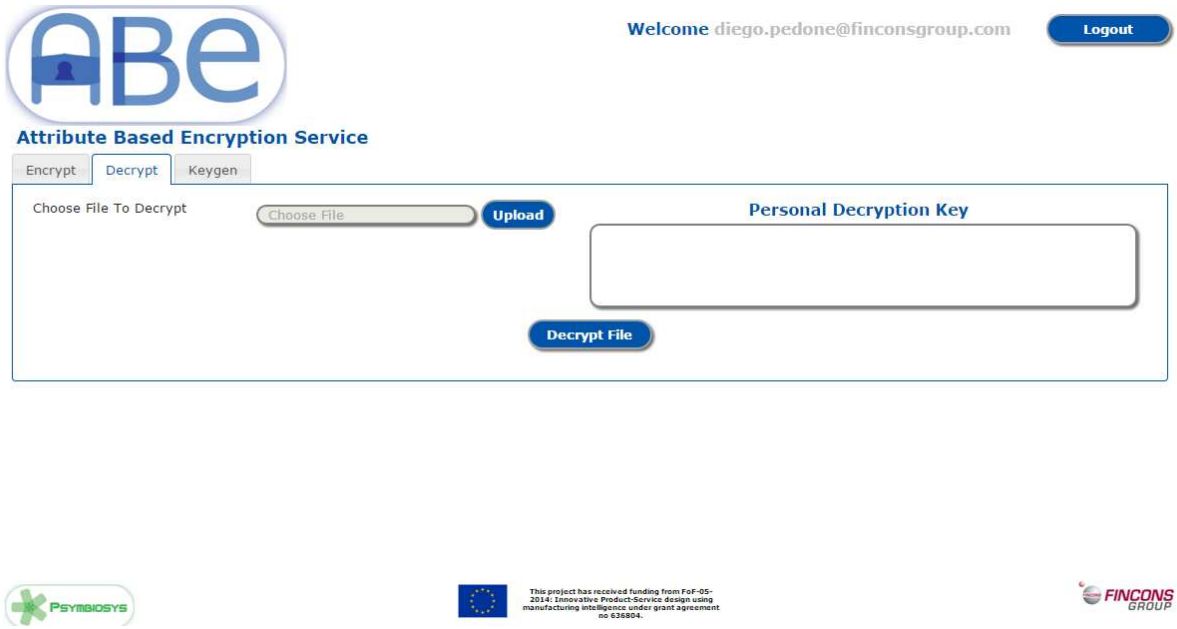

Figure 4 - ABE Decryption Tab

In the second tab the user can upload the encrypted file selecting it using the Upload button (an encrypted file must have a .cpabe extension). In the text area the user must insert his/her personal decryption key (see the Keygen tab). After completing the form the user must click the Decrypt File button to actually upload the file and the key. If the provided key meets the file's access policy the decryption will succeed and the service will download the decrypted file prompting the user to save it locally. In case the provided key does not meet the file's access policy the service will show an error message stating that the user's attributes are not in line with the file's access policy.

3.5 Keygen

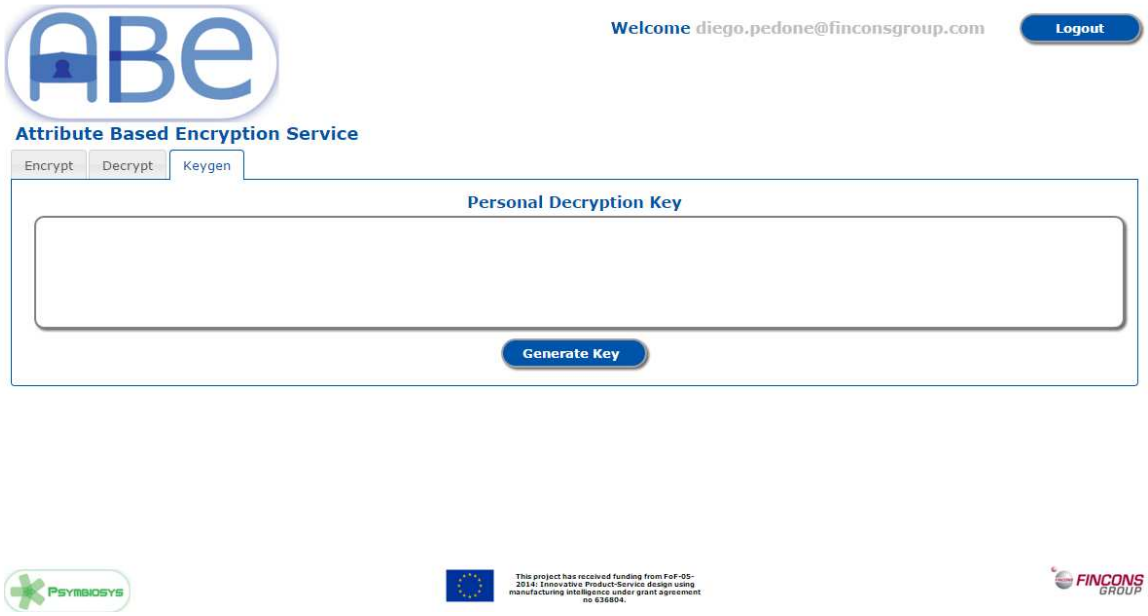

Figure 5 - ABE Key Generation Tab

In the Keygen tab the user can only press Generate Key to request the generation of his/her personal key which is generated using the users' attributes as stored in the LDAP service. The generated key is returned in the Personal Decryption Key text a. In case of errors the service shows an error message to user.