

Rebel Alliance to Restore
the Republic



High Commission for
Development Affairs



Jedi High Council

Jedi Academy

PACS

Fonaments criptografia
asimètrica
(Sprint#2)

SdS Software Factory

Rebel Alliance to Restore the Republic

TOP SECRET

Only for your eyes

Índex

Anàlisi de requeriments	¡Error! Marcador no definido.
Anàlisi del sistema	¡Error! Marcador no definido.
Identificació d'actors i casos d'ús.....	¡Error! Marcador no definido.
Diagrama de context	¡Error! Marcador no definido.
Detall del cas d'ús.....	¡Error! Marcador no definido.
Especificació del cas d'ús.....	¡Error! Marcador no definido.
Diagrama d'activitats.....	¡Error! Marcador no definido.
Prototipat de PACS.....	¡Error! Marcador no definido.
Diagrama de classe Secure Core	¡Error! Marcador no definido.
Especificacions per a l'analista Jedi.....	¡Error! Marcador no definido.

Context

El sistema d'activació d'escuts d'energia per la salvaguarda dels planetes que es troben sota la protecció de l'aliança rebel per la restauració de la república, (Planetary Protection Shield Program - PPSP) es manté des que es va instaurar ara fa 230 unitats galàctiques anuals, però la seva tecnologia ha quedat obsoleta i presenta múltiples forats de seguretat.

Aprofitant un d'ells, La Primera Ordre ha atac amb èxit el planeta Takodana.

El HCDA ha demanat a SdS Software Factory reformular tot el sistema de validació de credencials d'accés als planetes, i crear un nou software que anomenarem PACS (Planetary Access Control System)

Un pilar d'aquest sistema de seguretat resideix en la seguretat de les comunicacions i la verificació adequada que les naus que penetren en el camp de força del planeta estan degudament autoritzades.

Per a poder dur a terme aquesta verificació, els aprenents de Jedi han de dominar les diferents tècniques criptogràfiques

Criptografia de clau pública

Com a part dels requeriments expressats en l'anàlisi funcional **PACS Inner Ring Validation**, cal poder realitzar una sèrie de verificacions i cal poder encriptar i desencriptar algunes dades sensibles utilitzant criptografia asimètrica o de clau pública.:

Exercici pràctic

Cal fer un programa amb C# de tipus Windows Forms amb 2 formularis per tal d'explorar les possibilitats de la criptografia de clau pública.

El primer permetrà la generació de un parell de claus Públic-Privat d'encriptació RSA que posteriorment s'utilitzaran per encriptar i desencriptar petits missatges.

De fet la desencriptació dels missatges es realitzarà en aquest mateix formulari que tindrà el següent aspecte:

The screenshot shows a Windows application window titled "Desencriptar". The window contains a form with the following elements:

- A section titled "Gestió de claus" (Key Management) containing:
 - A text box labeled "Nom KeyContainer".
 - A text box labeled "Fixer XML Public key" with a browse button (three dots) to its right.
 - A button labeled "Generar claus" (Generate keys).
- Below the "Gestió de claus" section, a text box labeled "Missatge encriptat" (Encrypted message) with a button labeled "Desencriptar" (Decrypt) to its right.
- At the bottom, a text box labeled "Missatge original" (Original message).

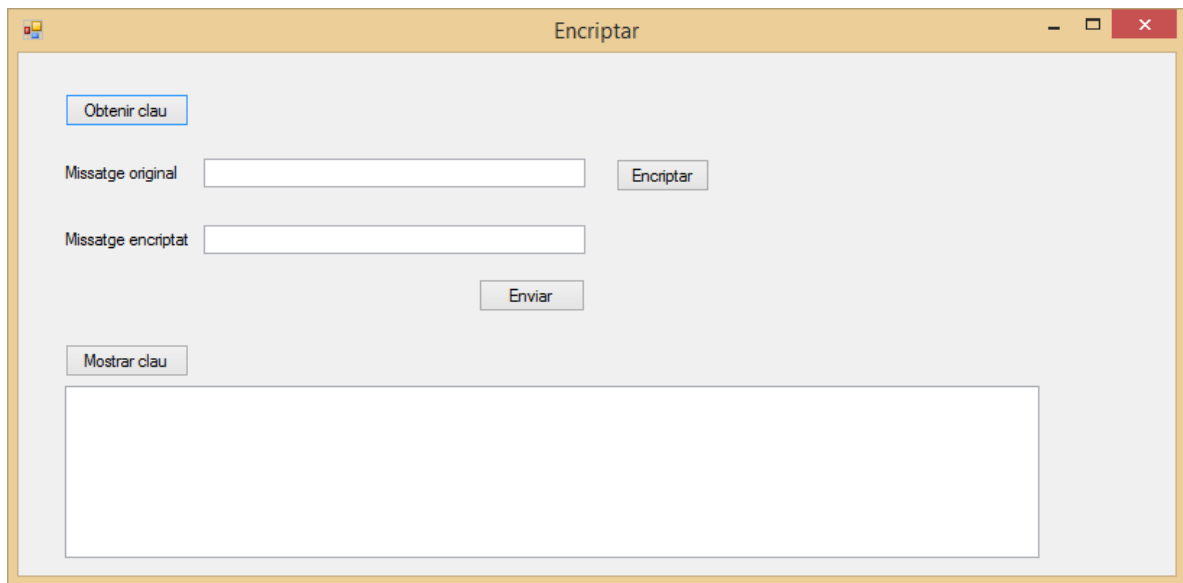
En l'apartat de **Gestió de claus** caldrà fer constar el nom del **KeyContainer** on volem emmagatzemar la nostra clau privada i el nom i la ubicació on volem persistir la nostra clau pública en format XML. Per fer-ho utilitzarem el botó del costat del textbox (marcat amb 3 punts) que obrirà el quadre de diàleg apropiat per indicar aquesta dada.

Un cop això estigui ben configurat el botó **Generar Claus** generarà un parell de claus Pública-Privada i les guardarà cadascuna on toca i de la forma que toca.

Un cop fet això restarà a l'espera de rebre un missatge a desencriptar. Aquest missatge el rebrà a partir d'una propietat de tipus array de bytes que s'omplirà des de l'altre formulari amb el resultat de l'encryptació d'un missatge i que es mostrarà en el textbox del missatge encriptat (un cop convertit a string).

Un cop hagi passat això, es podrà desencriptar el missatge (en format array de bytes) i mostrar-lo en la casella missatge original amb el botó **Desencriptar**

El segon formulari serveix per a encriptar un missatge i té el següent disseny:



El botó **Obtenir clau** obrirà el quadre de diàleg apropiat per seleccionar el fitxer xml que conté la clau pública i un cop seleccionat l'utilitzarà per a crear un objecte RSA que utilitzi aquesta clau.

El botó **Encriptar** utilitzarà aquest objecte RSA per encriptar el contingut del **textbox missatge original**, i convertir el resultat en una cadena que es mostrarà a la casella missatge encriptat.

El botó **Enviar** utilitza les propietats de l'altre formulari per enviar el text i l'array de bytes encriptats

El botó **Mostrar clau** mostra la clau pública en format XML en el control assignat.