Expresso V3 y firmas electrónicas

En el siguiente enlace se encuentra información respecto al uso de certificados electrónicos en Expresso V3:

■http://comunidadeexpresso.serpro.gov.br/mediawiki/index.php/Admins/Certificados

Otro enlace más:

■https://www.serpro.gov.br/linhas-negocio/certificacao-digital

Tutorial de certificados digitales en Expresso:

■https://demonstra.serpro.gov.br/tutoriais/autenticacao_token_linux/html/index.html?mod=3

Es posible utilizar certificados en soporte de software (archivos .p12) y hardware a través de tarjeta inteligente o token USB configurado en el navegador web.

La funcionalidad de "criptografía de correo" utiliza un APPLET de Java, ver el siguiente enlace:

■http://comunidadeexpresso.serpro.gov.br/mediawiki/index.php/Admins/Certificados#Habilitando_a_criptografia_de_Email

Descargué el código fuente Expresso V3 del siguiente enlace:

■http://comunidadeexpresso.serpro.gov.br/portal/downloads/kristina.20150223.06.tar.bz2

Al descomprimir el archivo se obtiene la siguiente estructura:

```
aaraujo@moe:~/desarrollo/2015/correo/kristina.20150223.06$ ls -l
total 25204
drwxr-xr-x 11 aaraujo aaraujo     4096 abr  8 16:21 ActiveSync
drwxr-xr-x 15 aaraujo aaraujo     4096 abr  8 16:21 Addressbook
drwxr-xr-x 13 aaraujo aaraujo     4096 abr  8 16:21 Admin
drwxr-xr-x 10 aaraujo aaraujo     4096 abr  8 16:21 AppLauncher
-rw-r--r--  1 aaraujo aaraujo     1382 abr  8 16:21 bootstrap.php
drwxr-xr-x 16 aaraujo aaraujo     4096 abr  8 16:21 Calendar
-rw-r--r--  1 aaraujo aaraujo      690 abr  8 16:21 config.inc.php.dist
-rw-r--r--  1 aaraujo aaraujo      938 abr  8 16:21 CREDITS
drwxr-xr-x  2 aaraujo aaraujo     4096 abr  8 16:21 docs
drwxr-xr-x  3 aaraujo aaraujo     4096 abr  8 16:21 domains
drwxr-xr-x 18 aaraujo aaraujo     4096 abr 27 09:15 Expressomail
drwxr-xr-x  2 aaraujo aaraujo     4096 abr  8 16:21 fonts
drwxr-xr-x  6 aaraujo aaraujo     4096 abr  8 16:21 images
-rwxr-xr-x  1 aaraujo aaraujo      981 abr  8 16:21 index.php
-rw-r--r--  1 aaraujo aaraujo     1516 abr  8 16:21 init_plugins.php
-rw-r--r--  1 aaraujo aaraujo 25509982 abr 27 07:47 kristina.20150223.06.tar.bz2
-rwxr-xr-x  1 aaraujo aaraujo    24405 abr  8 16:21 langHelper.php
drwxr-xr-x 22 aaraujo aaraujo     4096 abr  8 16:21 library
-rw-r--r--  1 aaraujo aaraujo   132767 abr  8 16:21 LICENSE
drwxr-xr-x 12 aaraujo aaraujo     4096 abr  8 16:21 Messenger
-rw-r--r--  1 aaraujo aaraujo     3583 abr  8 16:21 plugin.php
-rw-r--r--  1 aaraujo aaraujo     9254 abr  8 16:21 PRIVACY
-rw-r--r--  1 aaraujo aaraujo     1282 abr  8 16:21 README
-rw-r--r--  1 aaraujo aaraujo     1164 abr  8 16:21 RELEASENOTES
drwxr-xr-x 12 aaraujo aaraujo     4096 abr  8 16:21 Setup
-rwxr-xr-x  1 aaraujo aaraujo      373 abr  8 16:21 setup.php
drwxr-xr-x 13 aaraujo aaraujo     4096 abr  8 16:21 Tasks
drwxr-xr-x  5 aaraujo aaraujo     4096 abr  8 16:21 themes
-rw-r--r--  1 aaraujo aaraujo     2426 abr  8 16:21 tine20.php
drwxr-xr-x 49 aaraujo aaraujo     4096 abr  8 16:21 Tinebase
drwxr-xr-x  8 aaraujo aaraujo     4096 abr  8 16:21 vendor
drwxr-xr-x 13 aaraujo aaraujo     4096 abr  8 16:21 Webconference
-rw-r--r--  1 aaraujo aaraujo      485 abr  8 16:21 worker.php
drwxr-xr-x 19 aaraujo aaraujo     4096 abr  8 16:21 Zend
```

Luego en el directorio Expressomail se encuentra el archivo:

```
-rw-r--r-- 1 aaraujo aaraujo 10895 abr  8 16:21 Smime.php
```

En el archivo Smime.php se implementa todo el proceso de verificación de un correo electrónico firmado.

Se está utilizando el estándar SMIME (■https://es.wikipedia.org/wiki/S/MIME) a través de llamadas a funciones de PHP. La verificación de un correo electrónico firmado se realiza a través de:

openssl_pkcs7_verify — Verifica la firma de un mensaje S/MIME firmado (■https://php.net/manual/es/function.openssl-pkcs7-verify.php)

En algunos casos se hacen llamadas a sistemas en PHP para ejecutar el comando openssl como en el siguiente caso:

```
...
$w = exec('cat ' . $msgTempFile . ' | openssl smime -pk7out | openssl pkcs7 -print_certs',$output);
...
```

Para la firma electrónica se utiliza un applet de Java. Encontré un repositorio de github con los códigos:

■https://github.com/ComunidadeExpresso/expressolivre/tree/master/security/ExpressoCertMail

No estoy seguro si son los que se utilizan con Expresso V3.

En el archivo Expressomail/js/Expressomail-FAT.js descargado se hace una llamada

a la función signMessage:

```
...
try{
	document.getElementById("SignatureApplet").signMessage(Tine.Expressomail.fixIEUserAgent(),this.id,c)
}
...
```

Se carga el applet de java para ejecutar la firma.

En un mensaje del foro de Expresso se describe la manera en que se realiza la firma electrónica en Expresso V3:

■http://comunidadeexpresso.serpro.gov.br/portal/index.php?option=com_kunena&view=topic&catid=5&id=249&mesid=1282&Itemid=482&lang=pt-BR

En general:

A aplicação web se comunica através da applet através dos métodos 1- signMessage 2- encryptMessage 3- decryptMessage 4- verifyMessage

En la presentación [Expresso V3 Segurança com Certificaçao Digital] hay una descripción general y oficial sobre Expresso V3.