Certificate login

Summary

Certificate login provides the function which is identical with existing **GPKI certificate login**. However, in the case of GPKI certificate login, the standard security API which is distributed by the administrative electronic signature certificate management center. For specific items related with corresponding API, refer to the summary or precondition of GPKI certificate login service.

Description

The certificate login function is provided through the GPKISecureWeb module furnished by the administrative electronic signature certificate management center (www.gpki.go.kr).

Package Dependency

Login Package has direct functional dependency only for the common package (cmm) of element technology. However, in order to be executed without error during the component distribution, the distribution file is constituted with format/date/calculation, mail connection interface, and system package in accordance with the dependency between packages.

- Dependency between packages: User directory/integrated certification Package Dependency

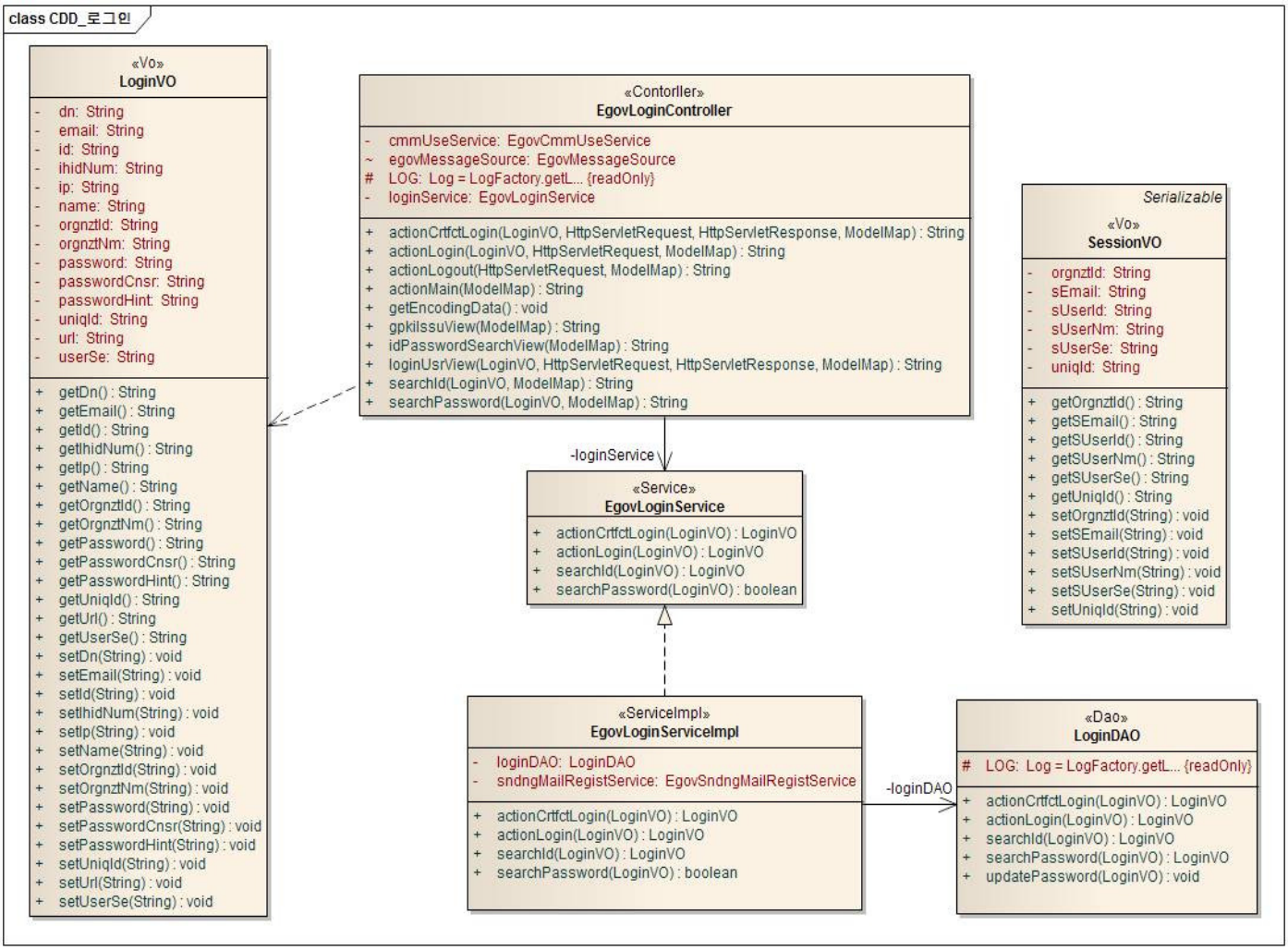
Related Sources

Type	Name of Corresponded Source	Remarks
Controller	egovframework.com.uat.uia.web.EgovLoginController.java	Controller class processing general login, certificate login
Service	egovframework.com.uat.uia.service.EgovLoginService.java	Business interface class processing general login, certificate login
ServiceImpl	egovframework.com.uat.uia.service.impl.EgovLoginServiceImpl.java	Business implementation class processing general login, certificate login
VO	egovframework.com.cmm.SessionVO.java	VO class for session
VO	egovframework.com.cmm.LoginVO.java	VO class for login
DAO	egovframework.com.uat.uia.service.impl.LoginDAO.java	DAO class processing general login, certificate login
JSP	WEB_INF/jsp/egovframework/com/uat/uia/EgovGpkiIssu.jsp	JSP page for certificate guide
JSP	WEB_INF/jsp/egovframework/com/uat/uia/EgovGpkiRegist.jsp	Login

		certification JSP page
Query XML	resources/egovframework/sqlmap/com/uat/uia/EgovLoginUsr_SQL_Mysql.xml	QUERY XML for MySQ for general login, certificate login
Query XML	resources/egovframework/sqlmap/com/uat/uia/EgovLoginUsr_SQL_Oracle.xml	QUERY XML for Oracle for general login, certificate login
Query XML	resources/egovframework/sqlmap/com/uat/uia/EgovLoginUsr_SQL_Tibero.xml	QUERY XML for Tibero for general login, certificate login
Query XML	resources/egovframework/sqlmap/com/uat/uia/EgovLoginUsr_SQL_Altibase.xml	QUERY XML for Altibase for general login, certificate login
Message properties	resources/egovframework/message/com/message-common_ko_KR.properties	Message properties for general login, certificate login

The controller among the above classes is the controller class for performing test at eGovFrame, and during actual application, corresponding functions are supposed to be converted with the basis of applied Web MVC framework. Even if MVC framework is not applied, it can easily be converted with servlet basis or corresponded JSP.

Class Diagram



Configuration of web.xml

In the case of CertProcessFilter and CertProcessRequestWrapper, if HTMLTagFilter(egovframework.rte.ptl.mvc.filter.HTMLTagFilter) of eGovFrame is used, addition shall identically be performed to the web.xml as follows. HTMLTagFilter automatically converts the tag for the request parameters because this portion shall be excluded from the certificate login processing section.

```
<filter>
    <filter-name>HTMLTagFilter</filter-name>
    <filter-class>
        egovframework.rte.ptl.mvc.filter.HTMLTagFilter
    </filter-class>
</filter>
<filter-mapping>
    <filter-name>HTMLTagFilter</filter-name>
    <url-pattern>*.do</url-pattern>
</filter-mapping>

<!-- Restoration from HTMLTagFilter's action (certification login) -->
<filter>
    <filter-name>CertProcessFilter</filter-name>
    <filter-class>
        egovframework.com.utl.sec.filter.CertProcessFilter
    </filter-class>
</filter>
<filter-mapping>
    <filter-name>CertProcessFilter</filter-name>
    <url-pattern>/utl/sec/certLogin.do</url-pattern>
```

```
    </filter-mapping>
    <filter-mapping>
        <filter-name>CertProcessFilter</filter-name>
        <url-pattern>/utl/sec/certInfoPopup.do</url-pattern>
    </filter-mapping>
```

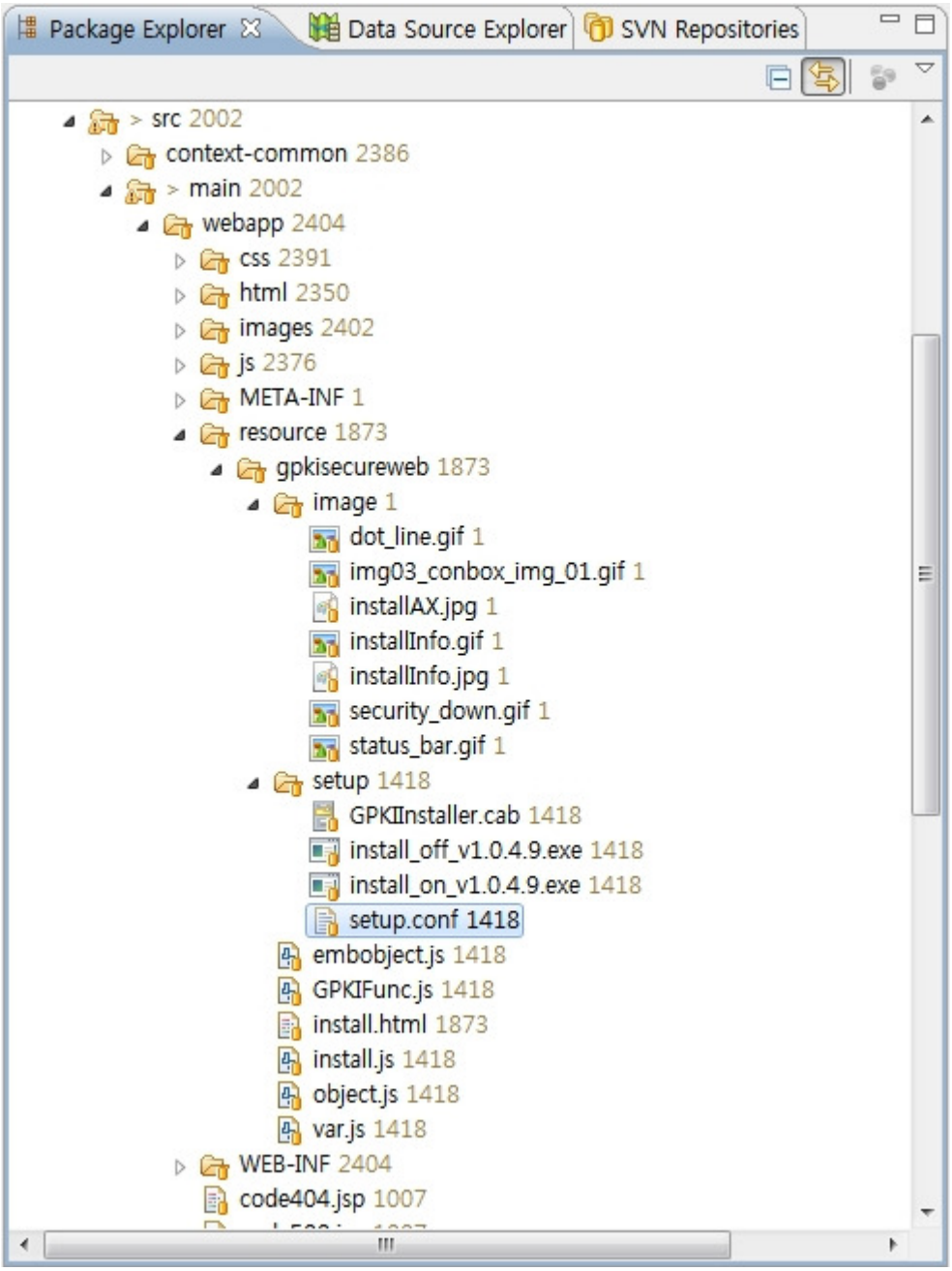
If HTMLTagFilter filter is not applied in the above description, the CertProcessFilter filter mentioned above needs not be applied either.

Configuration

First of all, locate the GPKISecureWeb module provided by MOPAS at the following route.

/src/main/webapp/resource/gpkisecureweb

Applied example is as follows.



According to the guide provided with corresponding module, part of the file shall be changed, however, in the case of applying current certificate login module, only following setup.conf needs to be revised.

- /resources/gpkisecureweb/setup/setup.conf

```
[Install_Info]
InstallDir          = GPKISecureWeb
ServerAddr        = 192.168.100.101:80
SetupFilePath    = /resource/gpkisecureweb/setup/install_on_v1.0.4.9.exe
Version   = 1049
```

Only for the ServerAddr section of above, IP and Port of current site needs to be designated. Cautionary point is that the certificate login ActiveX will normally be installed only when the corresponding file is distributed as EUC-KR.

Confirmation of GPKI API installation file

For the GPKI certificate login function in the first place, the GPKI API which suits to the system shall be applied to and issued by the administrative electronic signature certificate management center (http://www.gpki.go.kr). The standard security API configured in the server is for IBM AIX and it cannot be used in the WINDOWS series or other UNIX system.

Configuration element of standard API

Classification	Type	File name/folder	Description
Standard API Native module	Library	libgpkiapi64.a	For IBM AIX (for administration)
Standard API Native module	Library	libgpkiapi64_jni.a	For IBM AIX (for administration)
Standard API Native module	Library	libibmldap64n.a	For IBM AIX (for civilian)
Environmental file (conf)	Environmental file	gpkiapi.conf	Including the information required for certificate verification
Test program (sample)	Code	/java	Cert.java, Cms.java, Crypto.java, Ivs.java, Main.java, Tsa.java, Util.java (source code)
Test program (sample)	Execution file	/class	/Sample (Data required for operating the test program) Cert.class, Cms.class, Crypto.class, Ivs.class, Main.class, Tsa.class, Util.class (test program)
Standard API	jar file	libgpkiapi_jni.jar	Standard security API

Setup of class, library route

```
export GPKI_HOME=/product/jeus/egovProps/libgpkiapi
export CLASSPATH=$GPKI_HOME/libgpkiapi_jni.jar:$CLASSPATH
export LIBPATH=/product/jeus/egovProps/libgpkiapi/gpkiapi
export PATH=$PATH:/product/jeus/egovProps/libgpkiapi/gpkiapi
```

In order to use the standard security API (libgpkiapi_jni.jar) for JAVA, the jar file shall be located at the class route and the route of JNI file to be called shall be taken by the standard security API for JAVA. At this moment, this JNI file is connected with the standard security API for C/C++ and LDAP library, therefore, these 2 routes shall also be taken.

Location of certificate (example)

```
/product/jeus/egovProps/gpkisecureweb/certs/SVR..._env.cer
/product/jeus/egovProps/gpkisecureweb/certs/SVR..._env.key
/product/jeus/egovProps/gpkisecureweb/certs/NPKIRootCA1.der
/product/jeus/egovProps/gpkisecureweb/certs/GPKIRootCA1.der
```

Setup of property file

Following dsjdf.properties file shall be located at the user home directory. For windows, the "C:\Documents and Settings\[user account]" becomes the home directory in general, and for the Unix account, the directory (generally "/home/[user account]") which is to be entered when logging in becomes the home directory.

Otherwise, the dsjdf.properties file of specific location can be designated on the WAS starting script as follows.

java ... -Dcom.dsjdf.config.file="/product/jeus/egovProps/gpkisecureweb/conf/dsjdf.properties"

dsjdf.properties

#[Log relation]
logger.driver=com.dsjdf.jdf.DefaultLoggerWriter

#[Directory which leaves log]
#Log directory 의 Absolute Path
logger.dir=/product/jeus/egovProps/gpkisecureweb/log

#[Log level]
logger.sys.trace=false
logger.err.trace=true
logger.warn.trace=false
logger.info.trace=true
logger.debug.trace=false
logger.autoflush=true

#[Project setup file or server setup file]
pbf.propertiesFile=/product/jeus/egovProps/gpkisecureweb/conf/gpkisecureweb.properties

This is the file which performs the DSJDF environment setup, and it is used when the calling is conducted at Config of DSJDF. When driving the Application with DSJDF, this file will normally be operated only when the absolute route of this file is described to the com.dsjdf.jdf.config.file value by giving the java –D option. Otherwise, it needs to be existed in the root folder of the Web Application Server. Through the setup of logger.dir=/product/jeus/egovProps/gpkisecureweb/log, GPKI certification related log file can be stacked.

gpkisecureweb.properties

#===
====================
In the case of Servlet and JSP, this is the file to conduct the GPKISecureWeb environment setup, and it shall be located at /conf/gpkisecureweb.properties by designating JavaBean directory in the WAS as the root, and otherwise, the GPKISecureWEBConfigException will be generated. The installation location of this file is as follows.
=> [GPKISecureWeb installation directory]/conf/gpkisecureweb.properties in the web server/WAS
#==
==
# When the location of GPKI server certificate //is changed, WAS shall be driven again.
# Absolute Path of GPKI server certificate
GPKISecureWeb.CertFilePathName = /product/jeus/egovProps/gpkisecureweb/certs/SVR131..._env.cer
GPKISecureWeb.PrivateKeyFilePathName =
/product/jeus/egovProps/gpkisecureweb/certs/SVR131..._env.key
GPKISecureWeb.PrivateKeyPasswd = test

# Setup of GPKI API route
GPKISecureWeb.gpkiapi.ConfFilePath=/product/jeus/egovProps/gpkisecureweb/conf
GPKISecureWeb.CheckChallenge = yes

Number of ROOTCA certificate

GPKISecureWeb.TrustedROOTCACert.count=2

Location of ROOTCA certificate
ROOTCA certificate shall be updated before expiring the effective period.
In the case of ROOTCA certificate, if the certificate of corresponding location is double clicked (on the window), its effective period on the screen can be confirmed.
ROOTCA certificate can be obtained with LDAP browser,
and in the case of GPKI, the CN=Root CA,OU=GPKI,O=Government of Korea,C=KR is downloaded from the ldap://152.99.56.86:389, and in the case of NPKI, it will be downloaded from the cACertificate;binary entry of LDAP for the CN=KISA RootCA 1,OU=Korea Certification Authority Central,O=KISA,C=KR at the ldap://dir.signkorea.com:389.
Location of ROOTCA certificate shall be generated as much as the number of the ROOTCA certificate.
GPKISecureWeb.TrustedROOTCACert.FilePathName.1 =
/product/jeus/egovProps/gpkisecureweb/certs/NPKIRootCA1.der
GPKISecureWeb.TrustedROOTCACert.FilePathName.2 =
/product/jeus/egovProps/gpkisecureweb/certs/GPKIRootCA1.der

From the above, it is the location of #GPKI server certificate and the #GPKI API route setup section that shall be set up. 1 certificate is possessed by each server and 2 files (cer file and key file) are existed as being set up in the above. The one shown in the following is the password of certificate. The gpki.conf and gpkiapi.conf files shall always be existed at the Gpkiapi.confFilePath. The gpkiapi.conf is the file provided by the standard API, and the gpki.conf is the file existed in the route where the GPKIClientActiveX is installed.

Related Functions

Certificate login

Business Rule

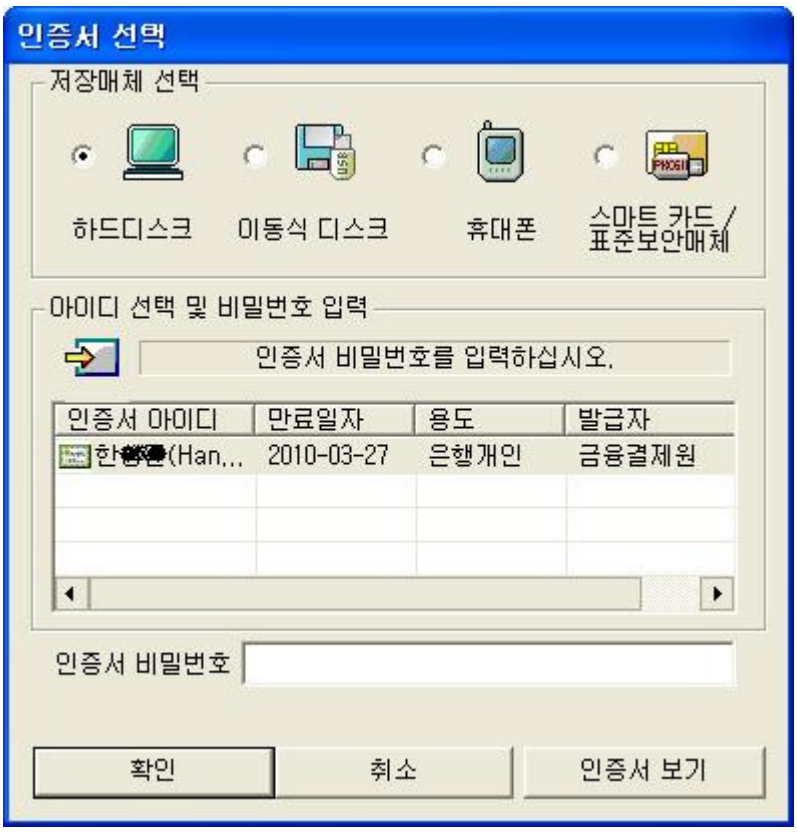
The certificate selection screen is appeared at the certificate login or certificate registration page, etc.

Related Code

N/A

Screen and execution manual

Action	URL	Controller method	JSP
Login screen	/uat/uia/egovLoginUsr.do	loginUsrView	“egovframework/com/uat/uia/EgovLoginUsr.jsp”
Certificate login	/uat/uia/actionCrtfctLogin.do	actionCrtfctLogin	“egovframework/com/uat/uia/EgovLoginUsr.jsp”
Certificate guide screen	/uat/uia/egovGpkiIssu.do	gpkiIssuView	“egovframework/com/uat/uia/EgovGpkiIssu.jsp”


인증서 선택
저장매체 선택
하드디스크
이동식 디스크
휴대폰
스마트 카드 / 표준보안매체
아이디 선택 및 비밀번호 입력
인증서 비밀번호를 입력하십시오.
인증서 아이디
만료일자
용도
발급자
한[redacted](Han...
2010-03-27
은행개인
금융결제원
인증서 비밀번호
확인
취소
인증서 보기