암호화/복호화

개요

암호화/복호화는 보안을 위하여 데이터를 암호화하거나 암호화된 데이터를 복호화하기 위해, GPKI(Government Public Key Infrastructure)를 통한 데이터의 암호화 및 복호화 기능을 제공한다. 부가적으로 GPKI를 통한 전자서명 및 전자서명 확인 기능도 제공한다.

전제조건

GPKI의 암복호화 기능을 사용하기 위해서는 별도로 사용하기 위해서는 행정전자서명 인증관리센터(Government Certification Management Authority)를 통해 GPKI 암복호화 모듈 및 서버인증서를 발급받아야 한다.

보다 자세한 사항은 공통컴포넌트의 GPKI 인증서 로그인 서비스를 참조하거나 행정전자서명 인증관리센터 (http://www.gpki.go.kr)를 참고한다.

설명

GPKI 암복호화는 서비스를 통해 데이터 암호화 및 복호화를 제공하는 기능으로 별도의 화면을 제공하지 않는다. 다만 테스트를 위한 JSP 화면만 제공된다.

패키지 참조 관계

암호화/복호화 패키지는 요소기술의 공통 패키지(cmm)에 대해서만 직접적인 함수적 참조 관계를 가진다.

- 패키지 간 참조 관계 : 보안 Package Dependency

관련소스

유형	대상소스	비고
Controller	egovframework.com.sec.pki.web.EgovGPKITestController.java	암호화/복호화 테스트를 위한 컨트롤러 클래스
Service	egovframework.com.sec.pki.service.EgovGPKIService.java	암호화/복호화를 위한 서비스 인터페이스
ServiceImpl	egovframework.com.sec.pki.service.impl.EgovGPKIServiceImpl.java	암호화/복호화를 위한 서비스 구현 클래스
JSP	/WEB-INF/jsp/egovframework/com/sec/pki/EgovGpkiTest.jsp	암호화/복호화 테스트를 위한 jsp페이지

환경설정

GPKI 암호화/복호화 기능을 활용하기 위하여 필요한 항목 및 그 환경 설정은 다음과 같다.

GPKI API 설치파일 확인

먼저 GPKI 인증서 로그인 기능을 위해서는 행정전자서명 인증관리센터(http://www.gpki.go.kr)에서 시스템에 맞는 GPKI API를 신청하여 발급받아야 한다. 서버에 구성해놓은 표준보안 API는 IBM AIX용으로 WINDOWS계열이나 다른 유닉스 시스템에서 사용할 수는 없다.

표준 API 구성요소

구분	형태	파일명/폴더	설명
표준API Native모듈	라이브러리	libgpkiapi64.a	IBM AIX용 (행정용)
표준API Native모듈	라이브러리	libgpkiapi64_jni.a	IBM AIX용 (행정용)
표준API Native모듈	라이브러리	libibmldap64n.a	IBM AIX용 (민간용)

환경파일 (conf)	환경 파일	gpkiapi.conf	인증서 검증에 필요한 정보 포함
테스트프로그램 (sample)	코드	/java	Cert.java, Cms.java, Crypto.java, Ivs.java, Main.java, Tsa.java, Util.java (소스코드)
테스트프로그램 (sample)	실행 파일	/class	/Sample (테스트 프로그램을 돌리기 위해서 필요한 데이터)Cert.class, Cms.class, Crypto.class, Ivs.class, Main.class, Tsa.class, Util.class (테스트 프로그램)
표준API	jar파일	libgpkiapi_jni.jar	표준보안 API

클래스, 라이브러리 경로 설정

```
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
```

JAVA용 표준보안API (libgpkiapi_jni.jar)를 사용하기 위해서는 jar 파일이 클래스 경로에 잡혀있어야 하며, JAVA용 표준보안API에서 호출하는 JNI 파일의 경로를 잡아주어야 한다.이 때, 이 JNI 파일은 C/C++용 표준보안API와 LDAP 라이브러리와 연결되어있어 이 두 라이브러리의 경로도 잡아주어야 한다.

인증서 위치 (예시)

```
/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
```

프로퍼티 파일 설정

globals.properties

인증서에 대한 정보를 지정하기 위해서는 globals.properties 속성 파일에 추가 속성을 설정하여야 한다.

globals.properties에 관련된 내용은 요소기술 프로퍼티 및 명령어 쉘스크립트 부분을 참조한다.

```
...
Globals.GPKIConfPath = /product/jeus/egovProps/conf/gpki.properties
...
```

gpki.properties (예시)

```
#---------------------------
# for GPKI LDAP access
#---------------------------
gpki.ldap.ip=ldap.gcc.go.kr
#gpki.ldap.ip=10.1.7.140
gpki.ldap.port=389
gpki.ldap.basedn=ou=Group of Server,o=Government of Korea,c=kr
gpki.ldap.attribute=usercertificate;binary

#---------------------------
# 인증서 정보
# 실제 인증서 관련 파일들은 각 속성들을 조합해서 얻음
#---------------------------
gpki.certificate.path = /product/jeus/egovProps/gpkisecureweb/certs/
gpki.certificate.server = 1310123456
gpki.privatekey.password = test
```

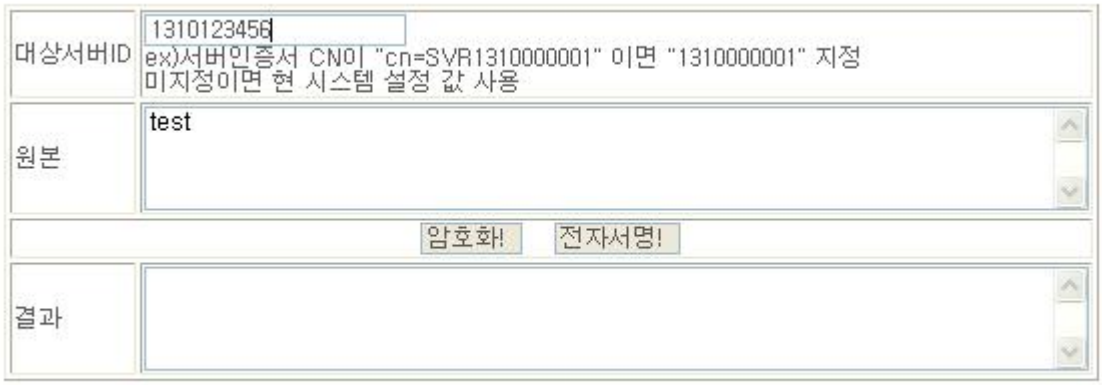
대상시스템에 대한 인증서를 GPKI의 ldap을 통해 취득하며 다음과 같은 코드로 해당 서버 정보 등을 처리한다.

```
        //------------------------------------
        // LDAP 관련 정보 얻기
        //------------------------------------
        String serverIp = EgovProperties.getProperty(config, "gpki.ldap.ip");
        String serverPort = EgovProperties.getProperty(config, "gpki.ldap.port");
        String basedn = EgovProperties.getProperty(config, "gpki.ldap.basedn");
        String readEntry = "cn=SVR" + code;
        String attribute = EgovProperties.getProperty(config, "gpki.ldap.attribute");
...
        //------------------------------------
        // 설정 정보 (암호화용 인증서 정보 필요)
        //------------------------------------
        String path = EgovProperties.getProperty(config, "gpki.certificate.path");

        String certForEnvFile = path + "/SVR" + EgovProperties.getProperty(config, "gpki.certificate.server")
+ "_env.cer";
        String keyForEnvFile = path + "/SVR" + EgovProperties.getProperty(config, "gpki.certificate.server")
+ "_env.key";
        String pinForEnv = EgovProperties.getProperty(config, "gpki.privatekey.password");
...
        //------------------------------------
            설정 정보  전자서명용 인증서 정보 필요
```

```
        //          (                          )
        //-------------------------------------
        String path = EgovProperties.getProperty(config, "gpki.certificate.path");

        String certForSignFile = path + "/SVR" + EgovProperties.getProperty(config,
"gpki.certificate.server") + "_sig.cer";
        String keyForSignFile = path + "/SVR" + EgovProperties.getProperty(config, "gpki.certificate.server")
+ "_sig.key";
        String pinForSign = EgovProperties.getProperty(config, "gpki.privatekey.password");
```

관련화면

암복호화 테스트 화면은 다음과 같다.



테스트는 원본에 대한 암호화 및 전자서명 처리, 결과에 대하여 복호화 및 전자서명확인 처리를 제공한다.