

POSE2E Gateway Manual

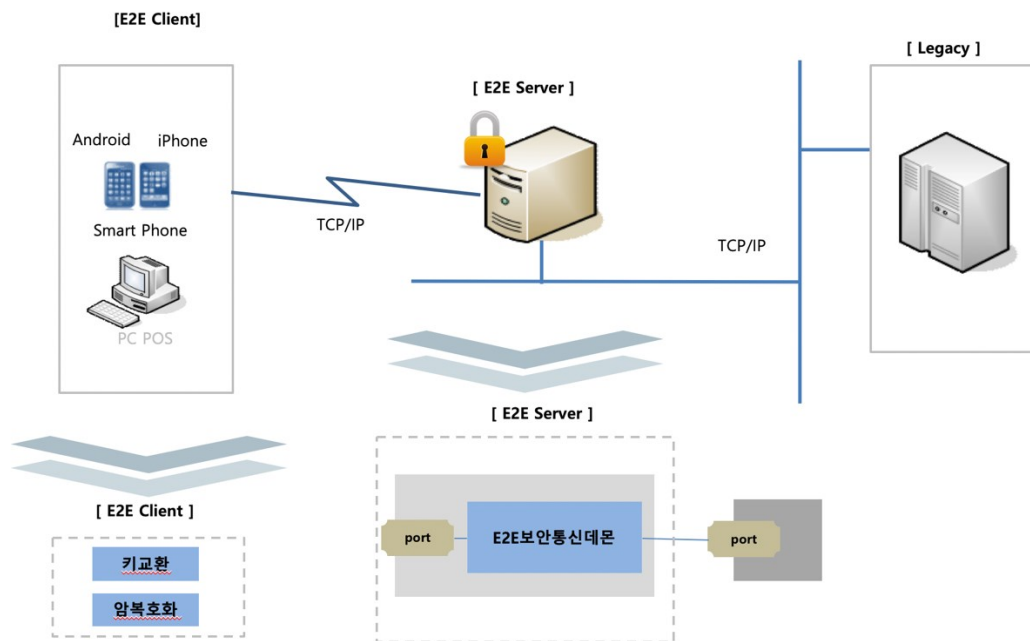
1. 개요	- 4 -
1.1 시스템 구성	- 4 -
2. 용어의 정의	- 5 -
3. 설치	- 6 -
3.1 사용환경	- 6 -
3.2 설치 및 운영	- 9 -
4. POS E2EGateway Message Format	- 10 -
4.1 입력요청정보	- 10 -
4.2 메시지 포맷	- 10 -
5. POS E2EGateway Server API	- 12 -
5.1 E2EGWS_Init	- 12 -
5.2 E2EGWS_GenerateKeyPair	- 12 -
5.3 E2EGWS_GetPublicKey	- 12 -
5.4 E2EGWS_EncBlockData	- 13 -
5.5 E2EGWS_DecBlockData	- 13 -
5.6 E2EGWS_RSAAEncData	- 13 -
5.7 E2EGWS_RSADecData	- 14 -
6. POS E2EGateway Client API	- 15 -
6.1 E2EGateway Clinet 전역변수	- 15 -
6.2 E2EGWC_Init	- 15 -
6.3 E2EGWC_GetServerCert	- 15 -
6.4 E2EGWC_MakeSessionKey	- 15 -
6.5 E2EGWC_GetEncSessionKey	- 16 -
6.6 E2EGWC_GetEncSessionKeyAndroid	- 16 -

6.7	E2EGWC_ExchangeKey	- 16 -
6.8	E2EGWC_ExchangeKeyAndroid	- 17 -
6.9	E2EGWC_MakeMessage	- 17 -
6.10	E2EGWC_EncBlockData	- 18 -
6.11	E2EGWC_DecBlockData	- 18 -
6.12	E2EGWC_RSAAEncData	- 18 -
6.13	E2EGWC_RSADecData	- 19 -
7.	기타	- 20 -
7.1	오류코드	- 20 -

1. 개요

POS용 인터넷중계프로그램.

1.1 시스템 구성



POS Client에서 TCP/IP로 E2E Gateway와 통신한다.

2. 용어의 정의

XXX : 용어정의.

3. 설치

3.1 사용환경

가. 사용환경

업무시스템에 설치되어 Legacy와 연계하여 서비스가 제공되기 위해서는 아래와 같은 환경에서 사용 가능합니다.

- . Java 환경 : 구동환경

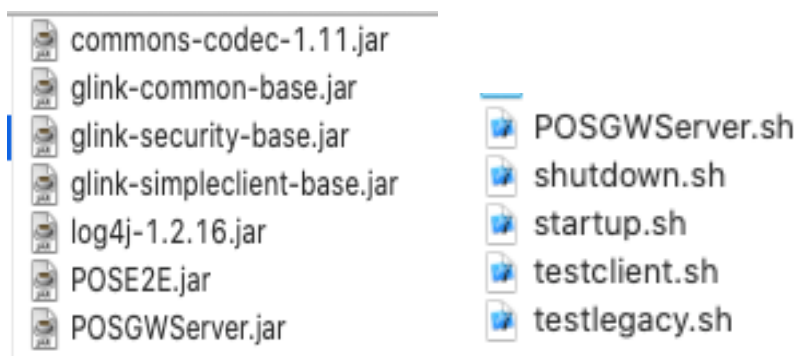
- . Network : Legacy와 연계하여 메시지를 송수신 처리할 수 있도록 Legacy와 접근이 가능해야 함 (Client IP주소와 Port로 접속 가능해야 하며, Legacy 역시 POS Gateway의 IP주소와 Port로 접속이 가능해야 함).

나. 디렉토리 구조

Direcotry 구조			설명
\$HomePath	/E2EGateway	/lib	라이브러리 디렉토리
		/bin	실행 및 중지 명령어
		/conf	서버실행 관련 properties파일 저장디렉토리(※사용자정의)
		/logs	로그 디렉토리(※사용자정의)
		/cert	키 대한 정보 저장디렉토리(※사용자정의)

※ 라이브러리 파일

※ 실행관련 파일



bcprov-ext-jdk15on-150.jar (HSM ←)

다. startup / shutdown / POSGWServer

-. POSGWServer.sh

```

export JAVA_HOME=/Library/Java/JavaVirtualMachines/jdk1.8.0_144.jdk/Contents/Home/jre
export JAVA=$JAVA_HOME/bin/java
export POS_HOME=/Users/gglimsoftmac03/Documents/WorkSpace/03.Projects/prj2020.posgw
export POS_CONF=$POS_HOME/conf/POSGWServer.properties
export POS_LIB=$POS_HOME/lib
export POS_LOGS=$POS_HOME/logs
export POS_CLASSES=$POS_HOME/classes

echo $POS_LIB
echo $POS_CONF
export POS_CLASSPATH=.:$POS_LIB/glink-common-base.jar:$POS_LIB/glink-security-base.jar:$POS_LIB/
log4j-1.2.16.jar:$POS_LIB/glink-simpleclient-base.jar:$POS_LIB/commons-codec-1.11.jar:$POS_LIB/
POSE2E.jar:$POS_LIB/POSGWServer.jar

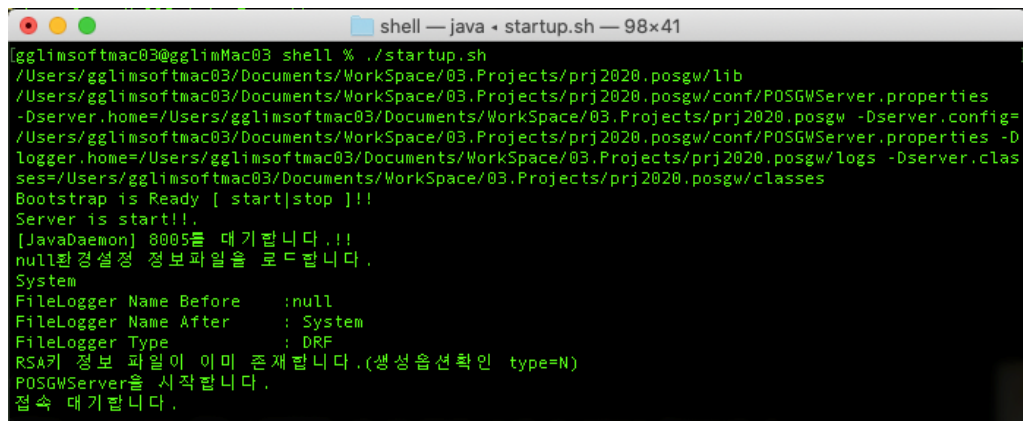
JAVA_PROPERTY="-Dserver.home=$POS_HOME"
JAVA_PROPERTY="${JAVA_PROPERTY} -Dserver.config=${POS_CONF}"
JAVA_PROPERTY="${JAVA_PROPERTY} -Dlogger.home=${POS_LOGS}"
JAVA_PROPERTY="${JAVA_PROPERTY} -Dserver.classes=${POS_CLASSES}"

echo $JAVA_PROPERTY

${JAVA} ${JAVA_PROPERTY} -classpath $POS_CLASSPATH com.gglimsoft.glink.gw.startup.Bootstrap $1
POSGWServer 8005

```

-. 기동 : startup.sh (UNIX)

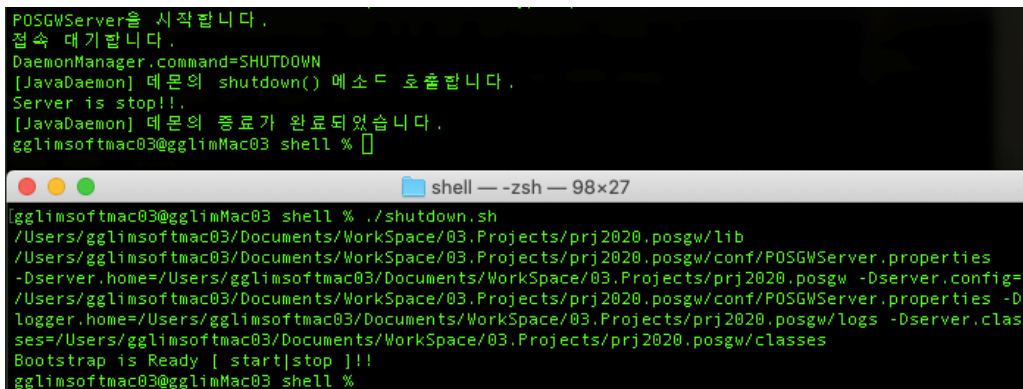


```

[gglimsoftmac03@gglimMac03 shell % ./startup.sh
/Users/gglimsoftmac03/Documents/WorkSpace/03.Projects/prj2020.posgw/lib
/Users/gglimsoftmac03/Documents/WorkSpace/03.Projects/prj2020.posgw/conf/POSGWServer.properties
-Dserver.home=/Users/gglimsoftmac03/Documents/WorkSpace/03.Projects/prj2020.posgw -Dserver.config=
/Users/gglimsoftmac03/Documents/WorkSpace/03.Projects/prj2020.posgw/conf/POSGWServer.properties -D
logger.home=/Users/gglimsoftmac03/Documents/WorkSpace/03.Projects/prj2020.posgw/logs -Dserver.clas
ses=/Users/gglimsoftmac03/Documents/WorkSpace/03.Projects/prj2020.posgw/classes
Bootstrap is Ready [ start|stop ]!!
Server is start!!
[JavaDaemon] 8005를 대기합니다.!!
null환경설정 정보파일을 로드합니다.
System
FileLogger Name Before      :null
FileLogger Name After       : System
FileLogger Type              : DRF
RSA키 정보 파일이 이미 존재합니다.(생성 옵션확인 type=N)
POSGWServer을 시작합니다.
접속 대기합니다.

```

-. 중지 : shutdown.sh(UNIX)



```

POSGWServer을 시작합니다.
접속 대기합니다.
DaemonManager.command=SHUTDOWN
[JavaDaemon] 데몬의 shutdown() 호출합니다.
Server is stop!!
[JavaDaemon] 데몬의 종료가 완료되었습니다.
gglimsoftmac03@gglimMac03 shell %

```

```

[gglimsoftmac03@gglimMac03 shell % ./shutdown.sh
/Users/gglimsoftmac03/Documents/WorkSpace/03.Projects/prj2020.posgw/lib
/Users/gglimsoftmac03/Documents/WorkSpace/03.Projects/prj2020.posgw/conf/POSGWServer.properties
-Dserver.home=/Users/gglimsoftmac03/Documents/WorkSpace/03.Projects/prj2020.posgw -Dserver.config=
/Users/gglimsoftmac03/Documents/WorkSpace/03.Projects/prj2020.posgw/conf/POSGWServer.properties -D
logger.home=/Users/gglimsoftmac03/Documents/WorkSpace/03.Projects/prj2020.posgw/logs -Dserver.clas
ses=/Users/gglimsoftmac03/Documents/WorkSpace/03.Projects/prj2020.posgw/classes
Bootstrap is Ready [ start|stop ]!!
gglimsoftmac03@gglimMac03 shell %

```

라. 환경설정파일 (POSGWServer.properties)

- E2E Gateway 서비스정보

```

POSGWServer.E2E.Port=55500.  ← 서버포트

POSGWServer.Config.HSM=N  ← HSM을 사용하는 경우 "Y"

POSGWServer.Config.CertPath=/Users/gglimsoftmac03/Documents/WorkSpace/cert/

    → 서버인증서 경로

POSGWServer.Config.CertificationKeyGen=N → 인증서생성여부 ( Y이면 서버 재기동할때마다 인증서를 생성함.)

POSGWServer.client.sessionTime=10 → 세션키관리 세션타임아웃설정 (일정시간지나면 삭제처리함)

## Legacy 서버 아이피 및 포트

CardServer.Ip=192.168.1.4  ← Legacy 서버아이피

CardServer.Port=65500.    ← Legacy 서버 포트

HSM.Ip=192.168.1.1

HSM.Port=1555

```

- Logger정보

```

logger.name=System

logger.type=DRF

logger.class=com.cosmos.logger.FileLogger

logger.prefix=POSE2EGateway  ← 로거파일명

logger.suffix=.log

logger.timestamp=true

logger.debug=1

logger.level=ALL

```


3.2 설치 및 운영

가. 사전 준비 사항

(1) AES256 사용을 위한 사전준비로 Java 버전에 맞추어 Unlimited Strength정책 파일을 다운받아 설치합니다.

- Java6 / Java7 / Java8 버전의 경우 local_policy.jar, US_export_policy.jar 파일을

<JAVA_HOME>/jre/lib/security/폴더로 기존정책을 덮어 복사함

- Java 8u151 Release Notes에서는 별도 다운로드 없이 Unlimited Strength정책을 추가 번들이 같이 제공됨.

#<JAVA_HOME>/jre/lib/security/policy 경로에 limited와 unlimited 폴더구분

java.security 파일의 설정을 해제된 처리 (`crypto.policy=unlimited`)

- Java8u161 Release Notes 부터는 기본정책이 Unlimited 이며, 길이를 제한하고 싶은 경우 crypto.policy를 주석처리함

나. 작업순서

(1) 서버 설치 파일 압축을 풀어 실행디렉토리에 저장

(2) Properties 파일 경로 설정

(3) ./startup.sh 로 프로세서 기동

4. POS E2EGateway Message Format

4.1 입력요청정보

- POSE2EGateway Server 연결정보 : POSE2EGateway 의 IP주소(Local IP : 127.0.0.1) 및 Port정보
- KeyType : 1: PublicKey, 2: PrivateKey 3:SessionKey
- SessionKeyType : KeyType이 "3" 인 경우 SessionKeyType으로 1:RSA

4.2 메시지 포맷

가. 요청 메시지 포맷 (길이,Type)

길이정보(5,9)	거래구분(2,X)	버전(2,X)	오류코드(4)	데이터(variable)
-----------	-----------	---------	---------	---------------

- 길이정보 : 길이정보 5자리를 포함한 전체 전문 길이

Ex) 거래구분 (2)+ 버전(2) + 오류코드(4) + 데이터(30)

인 경우 길이정보는 43이되며 "00043"로 셋팅

- 거래구분 : '80' : Handshake, '20' : Data Transmission
- 버전 : 예비영역 (사용하지 않음) Default Value '01' ('00'이면 평문)
- 데이터 : '80' 인 경우 Handshake 포맷, 응답 '81'
- '20' 인 경우 암호화된 데이터, 응답 '21'
- '90' 인 경우 Echo 전문

('20' 전문 수신 완료 Ack 전문 / Echo없을경우 망상취소 진행)

나. 응답 메시지 포맷 (길이,Type)

길이정보(5,9)	거래구분(2,X)	버전(2,X)	오류코드(4)	데이터(variable)
-----------	-----------	---------	---------	---------------

- 거래구분(2) : '81' : Handshake, '20' : Data Transmission, '90' : Echo
- 오류코드 : "0000" 정상이며, 나머지는. 7.1 오류코드 참고

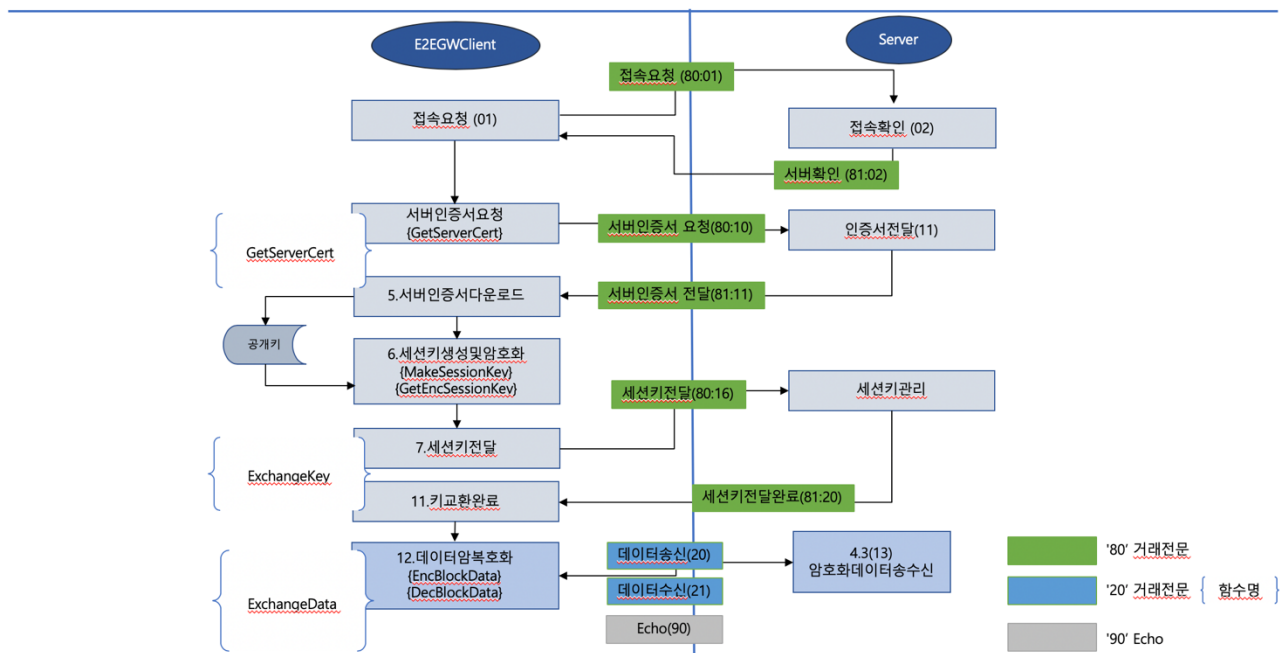
다. Handshake 포맷 (길이,Type)

거래구분(2,X)	길이정보(5,9)	데이터(variable)
-----------	-----------	---------------

- 거래구분(2) : '01' : Client 요청 '02' : Server확인 <= 기본
- '10' : 인증서요청 '11' : 서버인증서 전달

'16' : 클라이언트 세션키 전달 '20' : 키교환 종료

- '01'/'02' 데이터 : 버전정보(2,X)
- '10' 데이터 : 없음.
- '11' 데이터 : 인증서정보 *.pem 형태로 전달
- '16' 데이터 : Public Key로 암호화된 세션키정보
- '20' 데이터 : 없음.



5. POS E2EGateway Server API

5.1 E2EGWS_Init

static void E2EGWS_Init(Properties config)

가. Parameters :

- config : 환경설정정보

나. Remarks : E2EGWServer 서버를 초기화 설정

(인증서경로정보, 인증서생성여부, 세션키 세션매니저설정)

다. Return Value : 없음

5.2 E2EGWS_GenerateKeyPair

void E2EGWS_GenerateKeyPair(String type)

가. Parameters :

- type : 'Y' 이면 서버 재기동 할때마다 RSA 인증서정보(공개키,개인키)를 생성한다

'N'이면 서버 재기동할때 인증서 저장위치에 인증서가 없을 경우에만 생성한다

나. Remarks : RSA 공개키 및 개인키를 생성하여 특정위치에 저장한다

다. Return Value : 없음

5.3 E2EGWS_GetPublicKey

String E2EGWS_GetPublickKey()

가. Parameters : 없음

나. Remarks : 서버공개키를 읽어온다.

다. Return Value : 인코딩된 서버공개키

5.4 E2EGWS_EncBlockData

String E2EGWS_EncBlockData(String SessionKey, byte[] PlainData)

가. Parameters :

- SessionKey : 암호화키(세션키)

- PlainData : 평문 데이터

나. Remarks : 세션키로 데이터를 AES256으로 암호화한다

다. Return Value : 세션키로 암호화된 인코딩 데이터

5.5 E2EGWS_DecBlockData

byte[] E2EGWS_DecBlockData(String SessionKey, String EncData)

가. Parameters :

- SessionKey : 복호화키(세션키)

- EncData : 암호화된 인코딩데이터

나. Remarks : 세션키로 암호화된 데이터를 AES256으로 복호화한다

다. Return Value : 복호화된 데이터

5.6 E2EGWS_RSAAEncData

public String E2EGWS_RSAAEncData(byte[] PlainData);

가. Parameters

- PlainData : 평문데이터

나. Remarks : 서버에 저장된 개인키를 이용하여 암호화한다.(RSA)

다. Return Value : 암호화된 인코딩 데이터 (Base64 Encoding)

5.7 E2EGWS_RSADecData

```
public byte[] E2EGWS_RSADecData(byte[] EncData);
```

가. Parameters

- EncData : 암호화된 데이터

나. Remarks : 서버에 저장된 개인키로 복호화한다.

다. Return Value : 복호화된 평문데이터

6. POS E2EGateway Client API

6.1 E2EGateway Clinet 전역변수

가. Socket

6.2 E2EGWC_Init

```
public static void E2EGWC_Init(Socket socket)
```

가. Parameters :

- Socket : POSE2EGateway 연결 소켓 디스크립터

나. Remarks : 모듈 초기화.

다. Return Value : 없음

6.3 E2EGWC_GetServerCert

```
public String E2EGWC_GetServerCert();
```

가. Parameters : 없음

나. Remarks : E2E Gateway서버로 서버인증서를 요청하여 서버인증서를 다운로드한다

다. Return Value : 서버인증서 (*.pem 형태로 base64인코딩된 정보)

6.4 E2EGWC_MakeSessionKey

```
public String E2EGWC_MakeSessionKey();
```

가. Parameters : 없음

나. Remarks : 서버와 보안 통신에 필요한 세션키를 생성한다.

다. Return Value : 클라이언트에서 생성한 세션 키

6.5 E2EGWC_GetEncSessionKey

```
public String E2EGWC_GetEncSessionKey(String ServerCert, String SessionKey);
```

가. Parameters :

- ServerCert : 서버인증서(공개키)

- Session : 클라이언트세션키

나. Remarks : 세션키를 서버인증서로 암호화한다(RSA)

다. Return Value : 서버인증서로 암호화된 인코딩된 세션 키 (Base64 Encoding)

6.6 E2EGWC_GetEncSessionKeyAndroid

```
public String E2EGWC_GetEncSessionKeyAndroid(String ServerCert, String SessionKey);
```

가. Parameters :

- ServerCert : 서버인증서(공개키)

- Session : 클라이언트세션키

나. Remarks : 안드로이드에서 세션키를 서버인증서로 암호화할때 사용(RSA)

다. Return Value : 서버인증서로 암호화된 인코딩된 세션 키 (Base64 Encoding)

6.7 E2EGWC_ExchangeKey

```
public String E2EGWC_ExchangeKey(String ServerCert);
```

가. Parameters :

- ServerCert : 서버인증서(공개키)

나. Remarks : E2EGWC_MakeSession() 함수를 통해 세션키를 생성하고,

생성된 세션키를 E2EGWC_GetEncSessionKey()를 호출하여 공개키로 암호화 후 암호화된

세션키를 서버로 전송한다.

다. Return Value : 클라이언트에서 생성한 세션키

6.8 E2EGWC_ExchangeKeyAndroid

```
public String E2EGWC_ExchangeKeyAndroid(String ServerCert);
```

가. Parameters :

- ServerCert : 서버인증서(공개키)

나. Remarks : E2EGWC_MakeSession() 함수를 통해 세션키를 생성하고,

생성된 세션키를 E2EGWC_GetEncSessionKeyAndroid()를 호출하여 공개키로 암호화 후

암호화된 세션키를 서버로 전송한다.

(세션키 인증서 암호화할때 E2EGWC_GetEncSessionKeyAndroid 사용으로 함수 분리)

다. Return Value : 클라이언트에서 생성한 세션키

6.9 E2EGWC_MakeMessage

```
public byte[] E2EGWC_MakeMessage(String Tx, String Hscode, byte[] Data);
```

가. Parameters :

- Tx : 거래코드 (80/20)

- Hscode : 키교환 상세코드 (01/10/16)

- Data : 서버로 전송할 데이터

나. Remarks : 서버로 전송할 포맷으로 데이터생성.

다. Return Value : 서버로 전송할 전문

6.10 E2EGWC_EncBlockData

```
public String E2EGWC_EncBlockData(String SessionKey, byte[] PlainData);
```

가. Parameters

- SessionKey : 암호화키(세션키)

- PlainData : 평문데이터

나. Remarks : 세션키로 AES256 암호화한다.

다. Return Value : 암호화된 인코딩 데이터 (Base64 Encoding)

6.11 E2EGWC_DecBlockData

```
public byte[] E2EGWC_DecBlockData(String SessionKey, String EncData);
```

가. Parameters

- SessionKey : 복호화키(세션키)

- EncData : 암호화된 인코딩 데이터

나. Remarks : 세션키로 AES256 복호화한다.

다. Return Value : 복호화된 데이터

6.12 E2EGWC_RSAAncData

```
public String E2EGWC_RSAAncData(String ServerCert, byte[] PlainData);
```

가. Parameters

- ServerCert : 서버인증서(공개키)

- PlainData : 평문데이터

나. Remarks : 공개키로 RSA 암호화한다.

다. Return Value : 암호화된 데이터 (Base64 Encoding)

6.13 E2EGWC_RSADecData

```
public byte[] E2EGWC_RSADecData(String ServerCert, String EncData);
```

가. Parameters

- ServerCert : 서버인증서(공개키)
- EncData : RSA 개인키로 암호화된 인코딩 데이터

나. Remarks : 서버인증서로 복호화 한다

다. Return Value : 복호화된 데이터

7. 기타

7.1 오류코드

구분	오류 코드	오류메시지	오류상황
0	000	정상	
9	901	posgw.properties 파일이 존재하지 않습니다.	서비스 기동중 환경파일이 존재하지 않을 경우
9	002	인증서가 존재하지 않습니다.	서비스 기동중 인증서가 존재하지 않을 경우
9	003	세션키가 존재하지 않습니다.	서비스 처리중 세션키가 존재하지 않을 경우
9	999	Timeout 발생했거나 연결이 종료되었습니다.	Socket 연결이 종료되었거나, Timeout 발생
9	998	데이터 수신중 오류가 발생하였습니다.	기타 데이터 수신중 오류 발생
9	997	Legacy 서버 접속 실패.	Legacy 서버 접속 실패.

Changes

유형	일자	버전	내용
신규	2020.04.01	1.0.0	최초작성
추가	2020.04.16	1.0.1	HSM기능 추가 glink-security-base.jar POSE2E.jar 업데이트