Yini Seed 메뉴얼

문의 : mcj41@daum.net (http://blog.daum.net/mcj41)

1. 제품설명

본 제품은 Web Service를 위한 DB암호화(개인정보)를 위하여 개발된 제품 입니다.

해당 제품을 이용하여 여러 응용서비스에 적용 할수 있으며, 제품의 적용은 아래와 같습니다.

가. 운영환경

1) O/S : Microsoft Windows XP (SP3) 이후 Version 모두 지원
(단 64Bit O/S 및 제온 CPU 제외)

2) Web : Microsoft IIS and VC++ (COM), VB, ASP 등

나. 제품규격

1) 암호화 알고리즘 : KISA 기반 128Bit SEED 암호화 (정부표준)

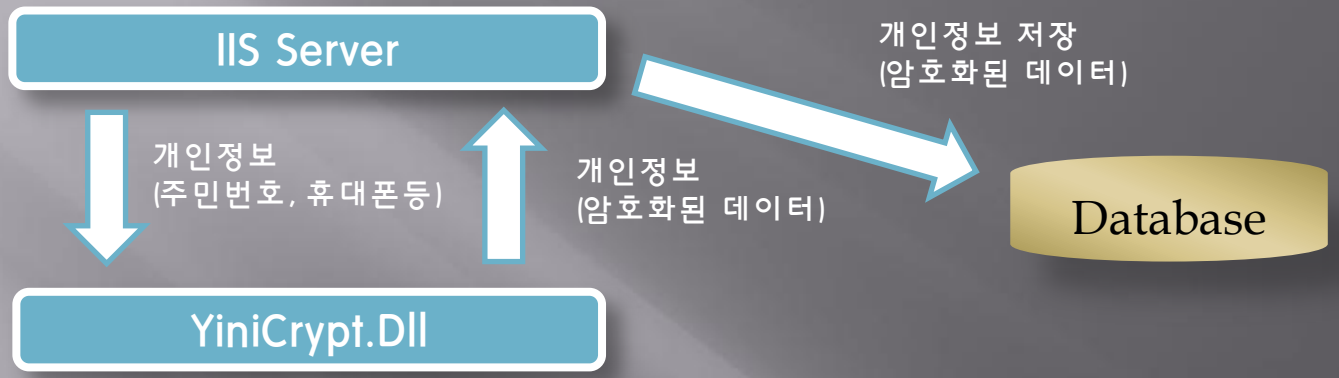
2) 운영모드 : CBC 알고리즘

3) PADDING : PKCS5

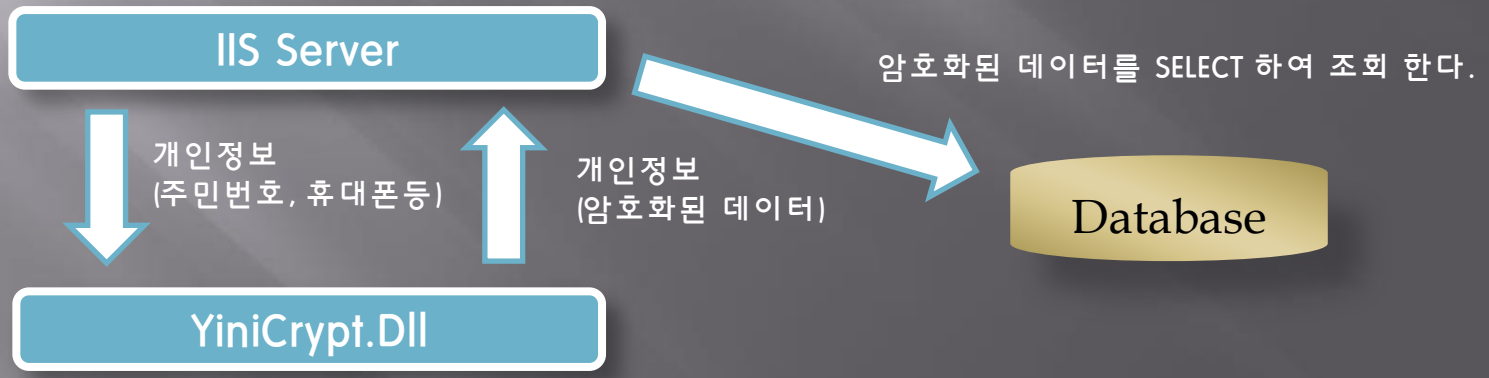
4) 출력 DATA : BASE64

다. DB 암호화 운영 방법

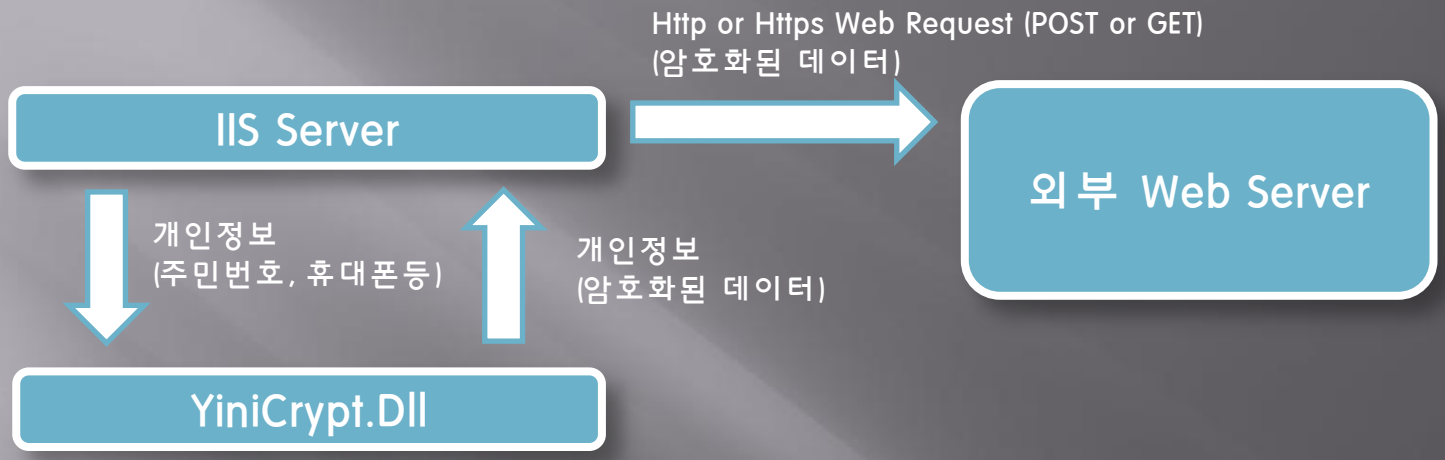
- 데이터 암호화 후 저장 방법 [복호화 절차 동일]



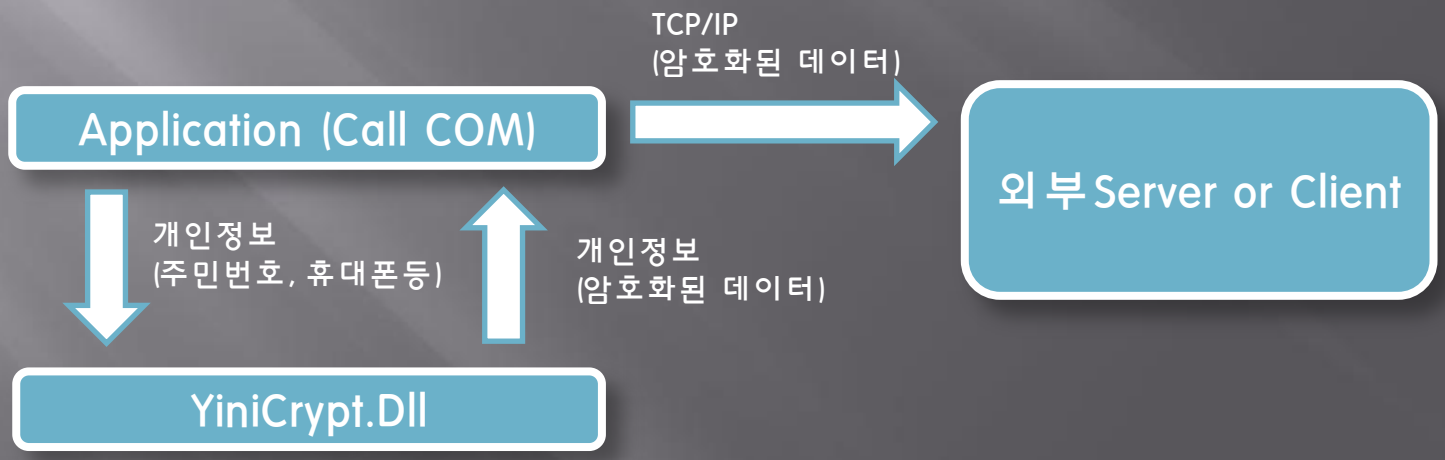
- 암호화된 데이터 조회 방법



< 부록 1. : Web Page Data 암호화 용으로 확장 >



< 부록 2. TCP/IP 암호화 통신 용으로 확장 >



2. 제품구성

가. 사용자 매뉴얼

나. 암호화 모듈

다. C# SAMPLE

3. 제품설치 전 우선 설치내용

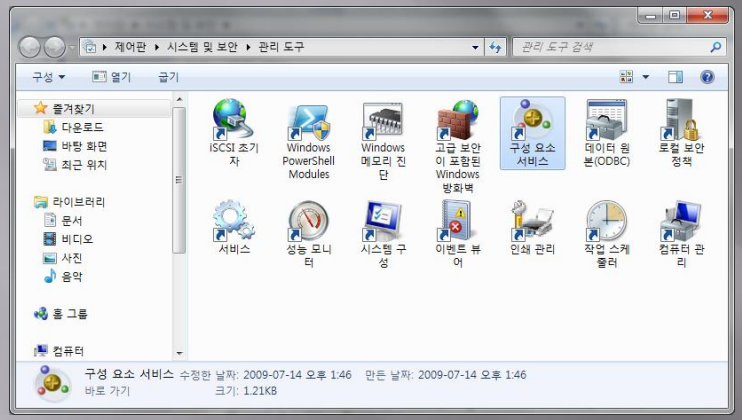
본 제품 Microsoft COM 기반으로 Visual Studio 2010으로 개발되었습니다.
이에 따라 설치 하고자 하는 Server 또는 PC에 Microsoft 재배포 팩키지가
우선적으로 설치 되어 있어야 정상적으로 모듈 설치가 가능 합니다.

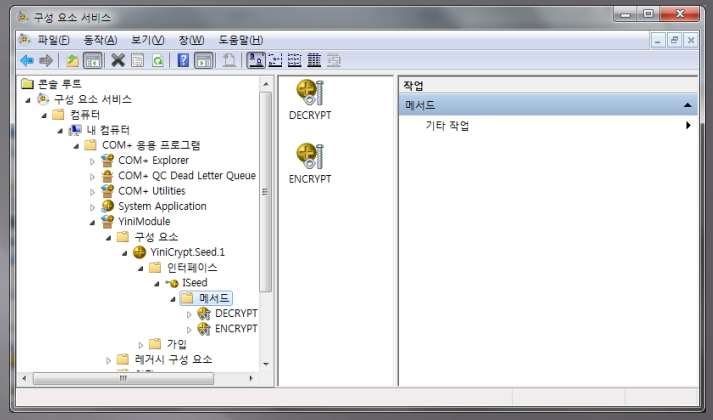
가. Down Load URL (2011년 12월 6일 기준)

http://www.microsoft.com/downloads/ko-kr/details.aspx?FamilyID=c32f406a-f8fc-4164-b6eb-5328b8578f03

4. 제품설치

본 제품의 설치를 위해서는 다음 아래와 같이 수행 합니다.

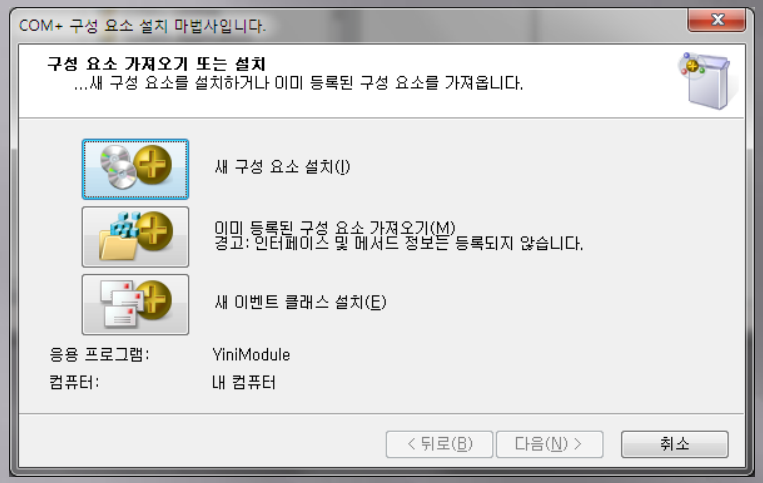


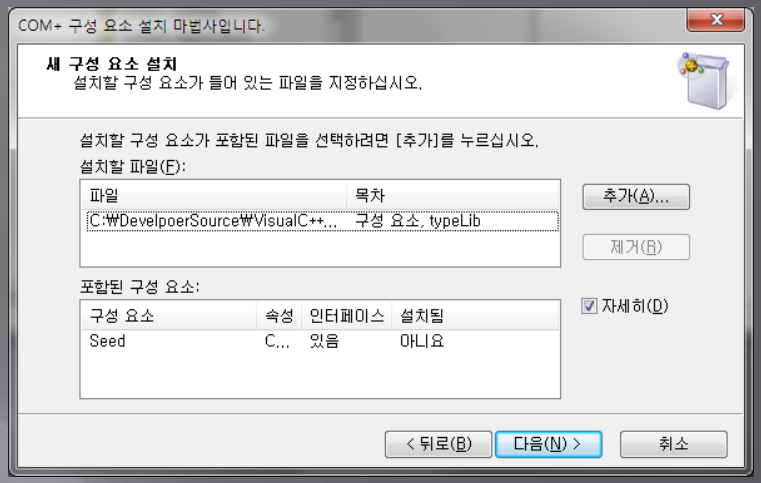


Window 제어판에서 [구성요서 서비스] 를 선택 합니다.

구성요소 서비스에서 [COM+ 응용프로그램] 을 선택 하여 마우스 오른쪽 버튼을 사용하여 새로운 이름으로 [응용프로그램] 을 생성 합니다.

새로이 생성된 응용프로그램 Tree에서 마우스 오른쪽 버튼을 사용하여 [새로만들기]를 선택하여 [COM+ 구성요소 시작 마법사] 를 통하여 등록 작업을 시작 합니다.

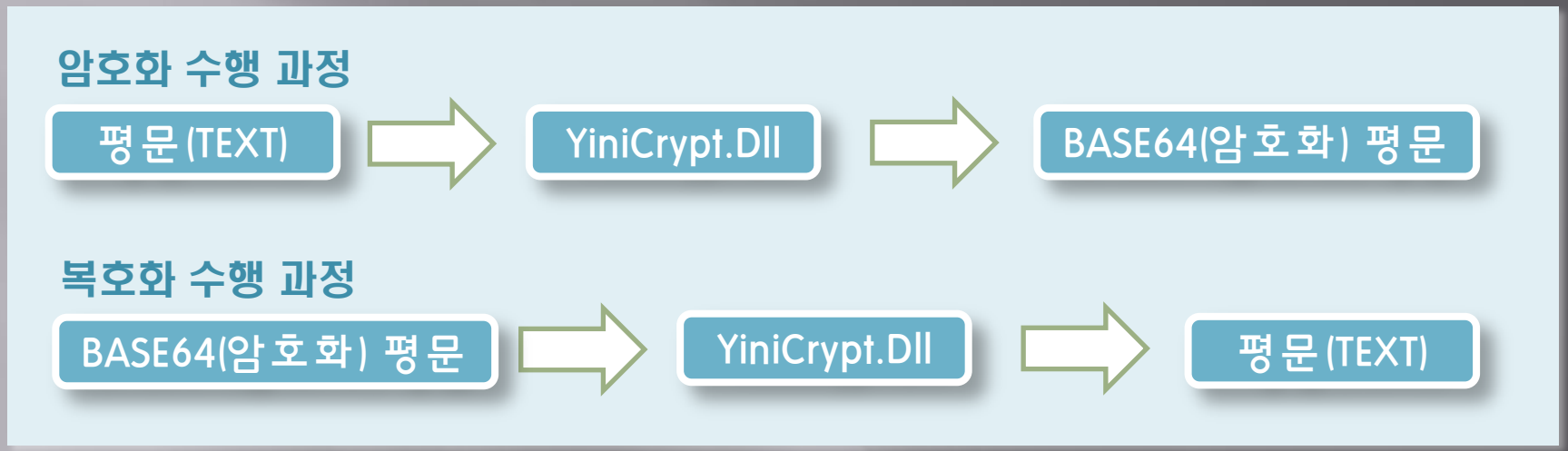




구성 요소 (모듈) 을 정상적으로 설치 한다면 [새 구성 요소 설치] 화면에서 [포함된 구성 요소] 항목이 정상적으로 출력 됩니다.

만약 [포함된 구성 요소] 항목이 정상적으로 보이지 않는다면 재배포 팩키지가 정상적으로 설치 되지 않은 것입니다. (본 문서 3Page 참조)

4. Function List



Function Name	Desciption
ENCRYPT	입력된 TEXT에 대하여 SEED암호화 후 BASE64 Encoding하여 TEXT 출력
DECRYPT	입력된 BASE64 TEXT에 대하여 BASE64 Decoding하여 SEED복호화 후 TEXT로 출력

가. IIS ASP에서 호출 방법

```
<?
    Dim KEY
    Dim IV
    Dim InputData
    Dim OutputData
    Dim Ret

    KEY = "1234567890123456"
    IV     = "1234567890123456"
    InputData = "본 문자열은 SEED/PKCS5/CBC 암호화 후 BASE64 출력 테스트 입니다."

    Set objs = Server.CreateObject("YiniCryptLib.Seed.1")
    Ret = objs.ENCRYPT(KEY, IV, InputData, OutputData)
    Response.write OutputData
?>
```

나. C#에서 호출 방법 (C#에서 참조개체 선택 후)

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Windows.Forms;

using YiniCryptLib;
….,
        YiniCryptLib.Seed      seed;
        seed = new YiniCryptLib.Seed();
         InPut = textBox1.Text;
        nRet = seed.ENCRYPT(KEY, IV, InPut, out OutPut);
```

5. Function REF

[API 함수 원형]

ENCRYPT (VARIANT inKEYVALUE, VARIANT inINITVALUE, VARIANT inINPUT , VARIANT *outOUTPUT)

F/N	Parameter	Length	Type	Description
필수	inKEYVALUE	16	C	SEED KEY (16 Byte 길이필수, 공백 사용불가)
필수	inINITVALUE	16	C	SEED IV (16 Byte 길이필수, 공백 사용불가)
필수	inINPUT	1024	C	암호화 대상 데이터 (TEXT)

F/N	Parameter	Length	Type	Description
	outOUTPUT	1024	C	SEED후 Base64로 변환된 데이터

– SAMPLE

```
int nRet = 0;
object InPut;
object OutPut;
object KEY = "1234567890123456";
object IV  = "1234567890123456";

YiniCryptLib.Seed      seed;

seed = new YiniCryptLib.Seed();

InPut = textBox1.Text;
nRet = seed.ENCRYPT(KEY, IV, InPut, out OutPut);

textBox2.Text = (String)OutPut;
```

[API 함수 원형]

DECRYPT (VARIANT inKEYVALUE, VARIANT inINITVALUE, VARIANT inINPUT , VARIANT *outOUTPUT)

F/N	Parameter	Length	Type	Description
필수	inKEYVALUE	16	C	SEED KEY (16 Byte 길이필수, 공백 사용불가)
필수	inINITVALUE	16	C	SEED IV (16 Byte 길이필수, 공백 사용불가)
필수	inINPUT	1024	C	복호화 대상 데이터 (BASE64 SEED)

F/N	Parameter	Length	Type	Description
	outOUTPUT	1024	C	복호화된 데이터 (TEXT)

– SAMPLE

```
int nRet = 0;
object InPut;
object OutPut;
object KEY = "1234567890123456";
object IV = "1234567890123456";

YiniCryptLib.Seed seed;

seed = new YiniCryptLib.Seed();

InPut = textBox3.Text;
nRet = seed.DECRYPT(KEY, IV, InPut, out OutPut);

textBox4.Text = (String)OutPut;
```

6. Q/A

Q. 1 라이선스 범위는 어떻게 되나요 ?
A. 1 무료 입니다. 물론 재배포 (저작권자 표기 필수) 및 기업의 서비스 용도로 사용 가능 합니다. 다만 판매 목적 또는 상업적 목적을 위한 배포는 저작권료를 지불해야 합니다.

Q. 2 ASP 나 ASP.NET(C#)에서만 사용 가능 한가요 ?
A. 2 아닙니다. COM 기반 제품이므로 COM호출이 가능 한 개발TOOL에서는 모두 사용 가능 합니다.

Q. 3 왜? SEED암호화 후 BASE64를 사용하나요?
A. 3 암호화된 데이터는 BINARY형태 입니다. 이 경우 ASP나 VB에서는 사용하기 어려우며 암호화된 데이터를 Database에 INSERT 또는 SELECT , UPDATE 할때 많은 불편함을 초래 하기 때문 입니다. (기술적 어려움이 많음)

Q. 4 다른 O/S환경이나, COM이 아닌 정규 DLL or MFC용은 없나요?
A. 4 아닙니다. 다만 별도 문의를 해야 합니다.
UNIX GCC, LINUX GCC, MFC DLL, STD DLL, JAVA, PHP등 모두 구비 되어 있습니다.

Q. 5 다른 시스템 또는 환경과 호환이 되나요?
A. 6 네, 표준을 준수 했으므로, 이기종의 시스템 및 JAVA와 같은 환경에서 생성된 암호화된 데이터와 정상적으로 호환 됩니다.