



TruGPG (Gnu Privacy Guard) File Level Encryption

Windows User Manual

목 차

1. TRUGPG 소개	3
1-1. TRUGPG 개요.....	3
1-2. GNUPG 특징.....	4
2. TRUGPG 기능	6
2-1. TRUGPG 메뉴	6
1) 환경설정	7
2) TruGPG 프로세스 상태	8
3) 자동 암호화 프로세스 설정	9
4) 자동 암호화 파일타입 지정	11
5) 일괄처리 암/복호화 실행	12
6) 암호화 키 관리	18
7) 자동 암호화 프로세스 시작 (Enable).....	20
8) 자동 암호화 프로세스 종료 (Disable).....	22

1. TruGPG 소개

1-1. TruGPG 개요

TruGPG(Gnu Private Guard)는 GnuPG OpenSource 를 사용한 제품으로 통신상의 또는 디지털 데이터 저장 시 보안을 확보하는 도구이고, 또한 TruGPG는 데이터를 암호화하고 전자 서명을 만들 수 있으며, 암호화 제품인 PGP를 완벽하게 대체할 수 있으며, 특히 특히 알고리즘(IDEA)을 전혀 이용하지 않은 제품이므로 아무런 제한 없이 사용할 수 있다.

TruGPG 는 공개키 방식의 암호화 기법을 사용하므로 더욱 안전하게 통신할 수 있다. 공개키 방식에서는 사용자마다 개인키 (private key) 와 공개키(public key)를 쌍으로 가지고 있어 사용자의 개인키는 노출되지 않고 안전하게 보관되어야 하며, 공개키는 사용자와 통신하려는 다른 이들에게 나눠줘 안전한 통신 또는 암호화를 할 수 있도록 구현한다.

TruGPG 자체는 그래픽 도구를 사용하지 않는 명령 줄(Command Line) 도구로 명령 프롬프트, 셸 스크립트 또는 다른 다양한 프로그램에서 직접적으로 사용할 수 있는 실제 암호화 엔진이므로 다른 애플리케이션의 백 엔드 프로그램으로 도 간주하여 사용 할 수 있는 장점을 가진다.

- 공개/개인 키 암호화를 사용하여 디지털 데이터를 암호화
- 디지털 데이터의 암호를 복호화
- 디지털 서명을 생성
- 디지털 서명을 확인
- 암호화 키를 생성
- 암호화 키를 인증
- 자동 파일 암호화 프로세스
- 일괄처리 파일 암호화/복호화 프로세스
- 파일 사용자 자동 감지 기능

1-2. GnuPG 특징

➤ Command Line Interface (명령 줄 인터페이스)

GnuPG 의 명령 줄 인터페이스(Command Line Interface)는 자동화 된 프로세스 및 웹 기반 응용 프로그램과도 신속하게 통합 할 수 있으며, 이 명령 줄 인터페이스를 사용하여 대칭 암호화, 키 관리, 사용자 정의 키 쌍 생성, 키 폐기 그리고 키 저장소에서의 키 게시 와 키 복구 기능 등을 수행한다.

➤ GnuPG Technical Specifications

Public-key Encryption

- RSA (keys up to 4096 bits)
- DSA (Keys up to 1024 bits)
- Elgamal (Keys up to 40967 bits)

Private-key Encryption

- AES (128, 192 or 256 bits)
- Blowfish
- CAST-5
- Triple-DES
- Twofish (256 bits)

Message Digest Algorithm

- MD5
- RIPE MD-160
- SHA-1
- SHA-256

Supported Systems

- Linux on Intel (RedHat/SuSE)
- HP Tru64 UNIX

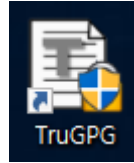
- HP OpenVMS
- HP-UX
- Oracle Solaris
- IBM AIX
- Windows

➤ **GnuPG Features**

- PGP를 완전하게 대체
- 배타적인(특히) 알고리즘은 전혀 사용하지 않습니다.
- GPL(General Public License) 를 준수합니다..
- 필터 프로그램처럼 사용할 수 있습니다.
- PGP나 보안성이 강화된 PGP 2보다 나은 기능을 가지고 있습니다.
- PGP 5, 6, 7 메시지를 풀고 검증합니다.
- 새로운 알고리즘을 모듈 형태로 쉽게 추가할 수 있습니다.
- 사용자 ID는 표준 형식을 따르도록 만듭니다.
- 키와 서명의 만료 기간을 정할 수 있습니다.
- 온라인 도움말 시스템.
- 익명 메시지 수신자들을 선택할 수도 있습니다.
- HKP 키 서버를 완벽하게 지원합니다.([wwwkeys.pgp.net](http://www.keys.pgp.net)).

2. TruGPG 기능

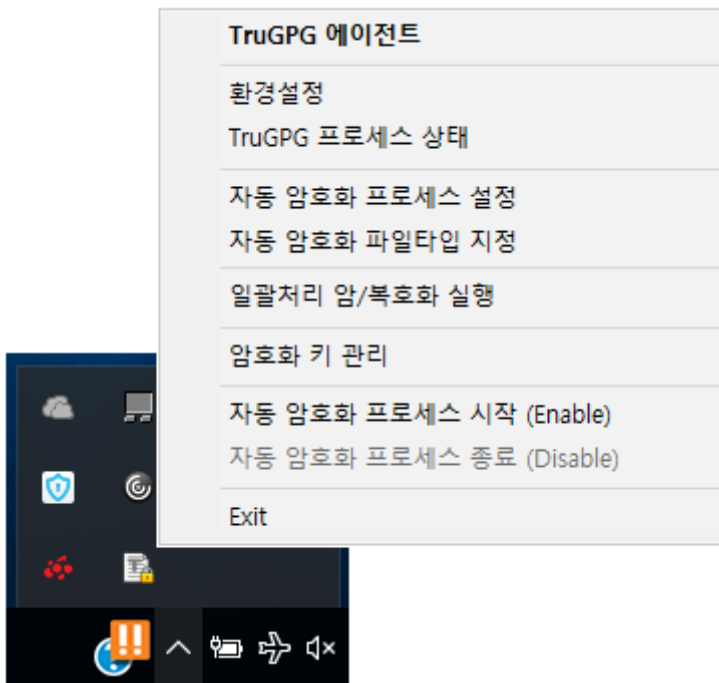
2-1. TruGPG 메뉴



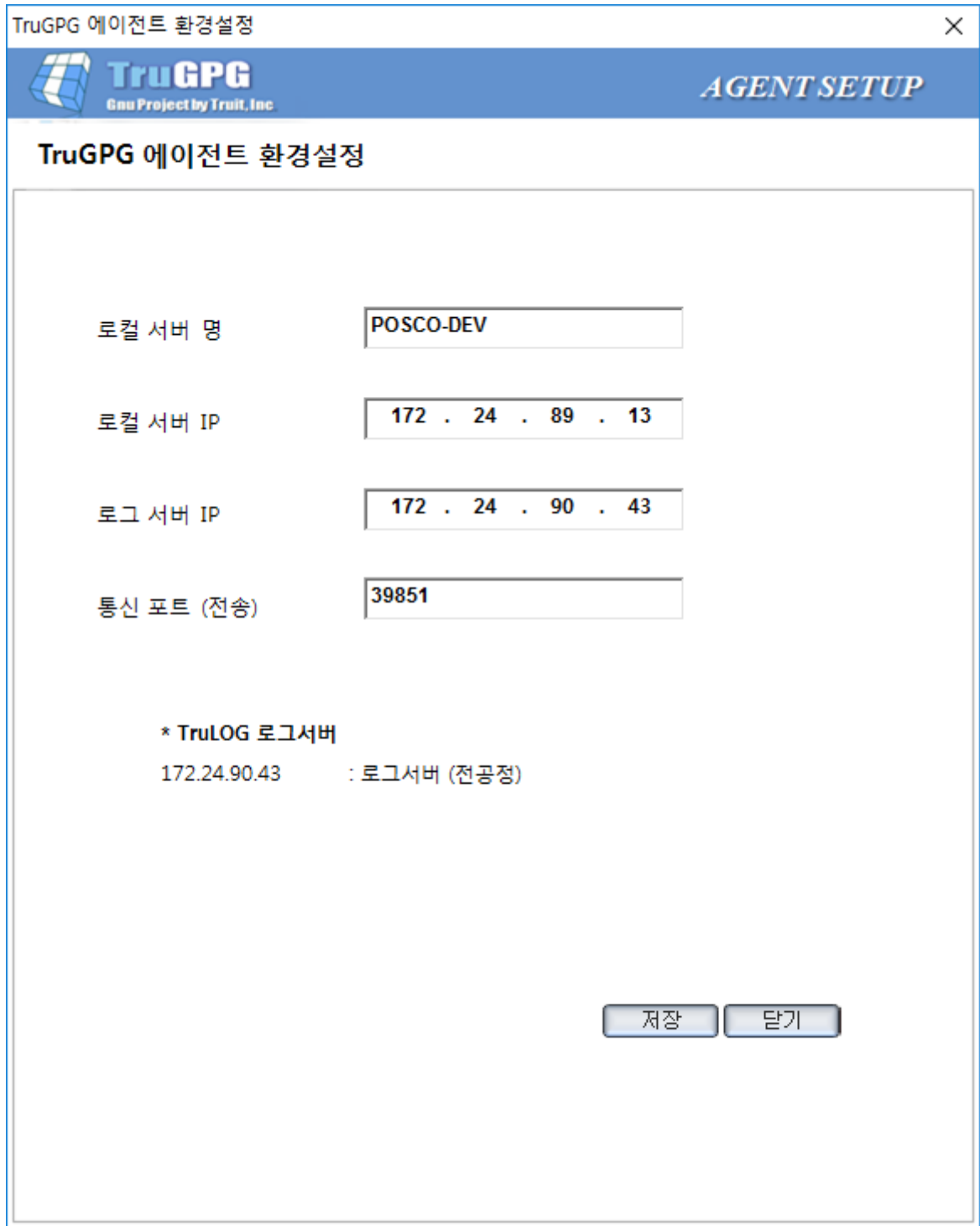
TruGPG 설치가 완료되면 바탕화면에 **<TruGPG 아이콘>**이 생성되는데, 이는 **"C:\Program Files (x86)\Wtrugpg\Agent\Wtrugpg_setup.exe"** 프로그램이 실행되면서 왼쪽 아래 트레이 박스 안에 **<TruGPG 트레이 아이콘>**이 생성된다.

"TruGPG 에이전트" 메뉴를 선택하기 위해선 **<TruGPG 트레이 아이콘>**을 선택한 상태에서 우측버튼을 누르면 나타나는데, 이 메뉴를 통해서 **TruGPG 서버 환경설정, 자동 암호화 프로세스 설정, 일괄처리 암호/복호화 실행, 암호화 키 관리 및 자동 암호화 프로세스 시작/종료** 등을 처리할 수 있다.

[TruGPG 에이전트 메뉴]



1) 환경설정



The screenshot shows a window titled "TruGPG 에이전트 환경설정" (TruGPG Agent Environment Settings). The window has a blue header with the TruGPG logo and the text "AGENT SETUP". The main content area is titled "TruGPG 에이전트 환경설정" and contains the following configuration fields:

로컬 서버 명	POSCO-DEV
로컬 서버 IP	172 . 24 . 89 . 13
로그 서버 IP	172 . 24 . 90 . 43
통신 포트 (전송)	39851

Below the fields, there is a note: "* TruLOG 로그서버" (TruLOG Log Server) with the IP address "172.24.90.43" and the label ": 로그서버 (전공정)" (Log Server (Production)).

At the bottom right, there are two buttons: "저장" (Save) and "닫기" (Close).

로컬 서버 명 : TruGPG 에이전트가 설치된 서버 이름 (논리 서버 이름으로 입력 가능)

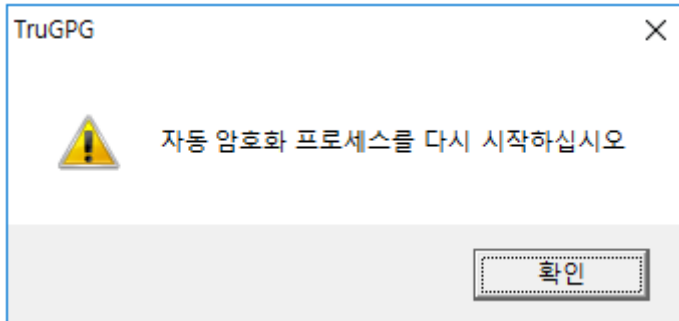
로컬 서버 IP : 서버 IP

로그 서버 IP : 전 공정 TruLOG 로그서버 IP 를 입력한다. (172.24.90.43)

통신 포트 (전송) : 39851 (TruSHM : SRM with HFM 과 공용)

입력 후 “저장” “닫기” 버튼을 차례로 누르면, 아래와 같이 TruGPG Agent 를 다시 시작하라는 창이 나타난다. 이때 “확인” 을 누르고, **TruGPG 에이전트 메뉴** (이하 “메뉴” 라 칭한다) 에서 **“자동 암호화 프로세스 시작 (Enable)”** 을 누른다.

만약 자동 암호화 프로세스가 Enable 상태이면 종료(Disable) 후 다시 시작(Enable) 한다.



2) TruGPG 프로세스 상태




현재 자동 암호화 프로세스 가 실행 중... 즉, Enable 상태이다.



현재 자동 암호화 프로세스 가 중지 상태... 즉, Disable 상태이다.

3) 자동 암호화 프로세스 설정


AGENT SETUP

자동 암호화 프로세스 설정

번호	Key ID	암호화 폴더	파일타입	관리
1	truit1	D:\WTEST4		

암호화 대상 폴더

암호화 파일 타입 (예, .c, .cpp, .h)

Key_ID

Enable
 Disable
 자동 일괄처리
 시간

(자동 암호화 Disable 상태에서 일괄 암호화 실행하는 시간지정)

확인
삭제
저장
닫기

1. 암호화 대상 폴더 : 자동으로 암호화 할 대상 소스 폴더
2. 암호화 파일 타입(PREFIX_TYPE) : 파일 타입(확장자)을 지정한다. 여러 종류의 확장자가 있을 경우에는 “,” 를 구분자로 하여 입력한다. (예, “.c, .cpp, .h”) 확장자에는 “.”을 필히 포함하여 입력한다. 만약 없을 경우에는 무시한다.
3. KEY_ID : 암호화 키에 대한 ID (지정 소스 폴더 내 파일 들을 암호화 할 Key_ID)

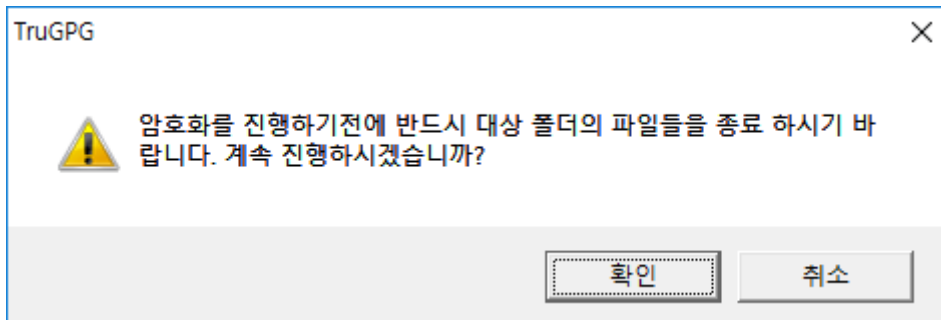
4. 폴더 별 자동 암호화 : “Enable”인 경우, 등록된 리스트 중에서 암호화를 자동으로 실행하는 대상이며, “Disable”인 경우는 리스트에 있어도 자동 암호화를 실행하지 않는다. 위 목록에는 “관리” 칼럼에 (E/D) 로 표시된다.

5. 자동 일괄처리 : 이 설정은 변경관리 진행 과정 또는 자동 암호화 Disable 상태에서 작업이 진행되지 않고 있을 때, 설정된 시간에 자동으로 해당 폴더를 일괄처리 암호화를 하는 기능이다. 이 기능은 자동 암호화가 Enable 되어 있는 경우에는 동작되지 않으며, 체크박스가 체크되어 있지 않으면 ‘자동 일괄 암호화’ 처리를 하지 않는다. (Default)

Enable 시키기 위해서 체크박스를 체크하고 시간선택 콤보박스에서 시간을 선택한다. 만약 체크박스가 체크되어 있더라도 시간 선택이 공백(Null) 일 때에는 자동 일괄처리 암호화가 진행되지 않는다.


즉, 이 기능은 자동 암호화가 Disable 되어있을 때만 입력된 시간에 일괄처리 암호화가 실행되며, 작업이 끝난 후 자동으로 자동 암호화가 Enable 되지 않고 현 Disable 상태를 유지한다.

자동 암호화에서는 지정 폴더 내에 사용자가 존재하거나 Open 된 파일이 존재하면 해당 폴더 정보와 Open 상태 정보를 로그로 남기며, 해당 폴더에 한해서는 자동 암호화 처리를 실행하지 않는다.



5) 일괄처리 암호/복호화 실행


- 암호화 실행

**TruGPG**
Gnu Project by Truit, Inc. *AGENT SETUP*

일괄처리 암호/복호화 실행

암호화 복호화

실행	번호	Key ID	암호화 폴더	파일타입	관리
<input type="checkbox"/>	1	truit	D:\POSCO\SRC1	.c	A
<input type="checkbox"/>	2	truit	D:\POSCO\SRC2	.c	A

암호화 대상 폴더 

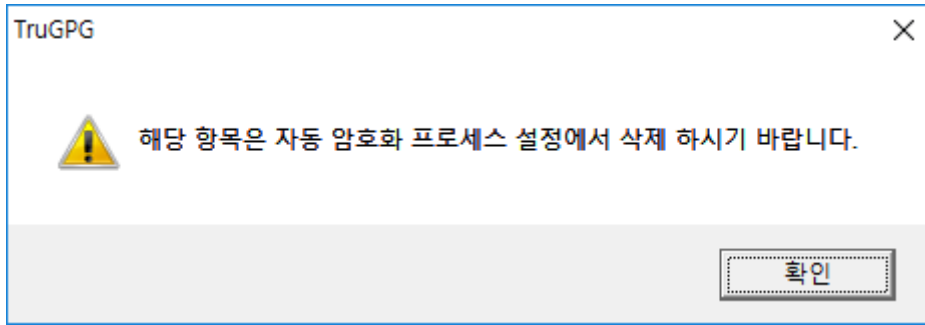
암호화 파일 타입 (예, .c, .cpp, .h)

Key_ID

확인 삭제 저장 닫기 실행

일괄처리 암호화를 실행한다.

“자동 암호화 프로세스 설정”에 등록된 폴더는 관리에 “A”(Auto) 로 표시되며, 이 설정에서는 변경 또는 삭제가 불가하고, “자동 암호화 프로세스 설정”에서만 가능하다. 만약 삭제를 시도할 때는 아래와 같은 경고 메시지가 나타난다.



이곳에서 등록된 폴더에 대해서는 관리에 "M"(Manual) 로 표시된다.

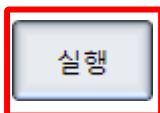
입력할 내용은 "자동 암호화 프로세스 설정" 과 동일하다.

일괄처리 암호화를 실행하기 위해서는 상단의 대상 리스트 중 실행을 원하는 해당 폴더의 "실행" 체크박스에 체크하고, 아래 "실행" 버튼을 클릭하면 된다. 마찬가지로 여러 폴더를 같이 실행하려면, 해당 폴더들의 체크 박스를 체크하고 "실행" 버튼을 클릭하면 된다.

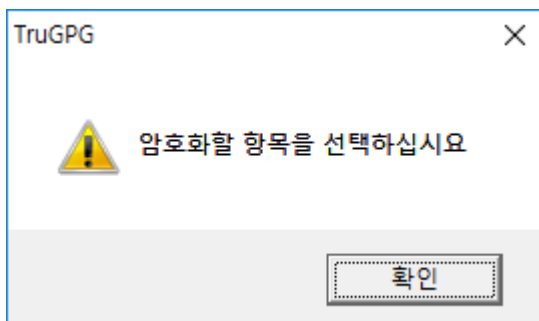
일괄처리 암/복호화 실행

암호화 복호화

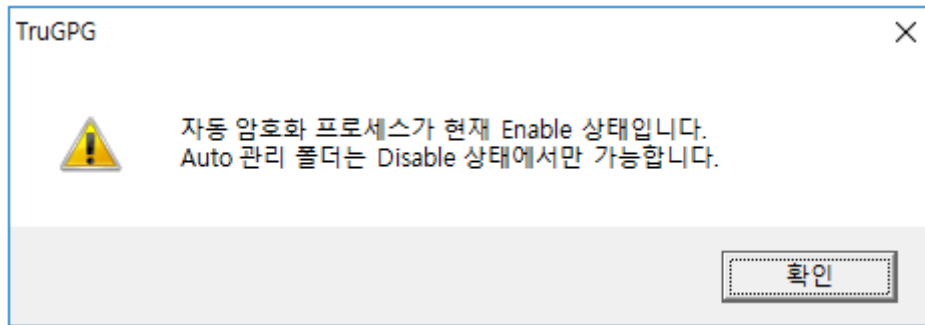
실행	번호	Key ID	암호화 폴더	파일타입	관리
<input type="checkbox"/>	1	truit	D:\POSCO\SRC1	.c	A
<input checked="" type="checkbox"/>	2	truit	D:\POSCO\SRC2	.c	A
<input type="checkbox"/>	3	truit	D:\POSCO\m_SRC	.c	M



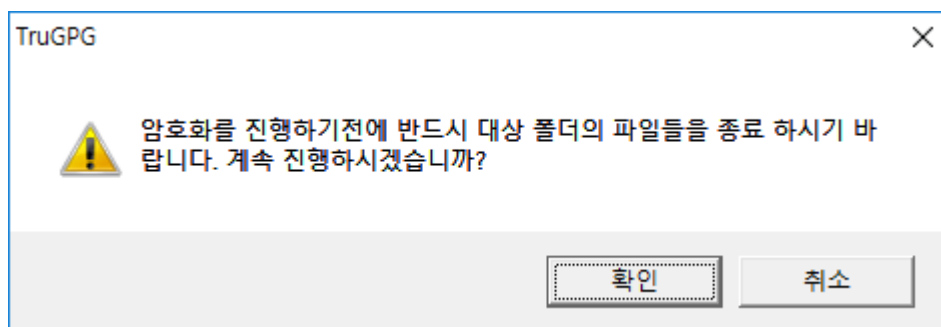
하지만 상단 리스트의 "실행" 체크박스에 선택된 폴더가 없으면 다음 확인 창이 나타난다.



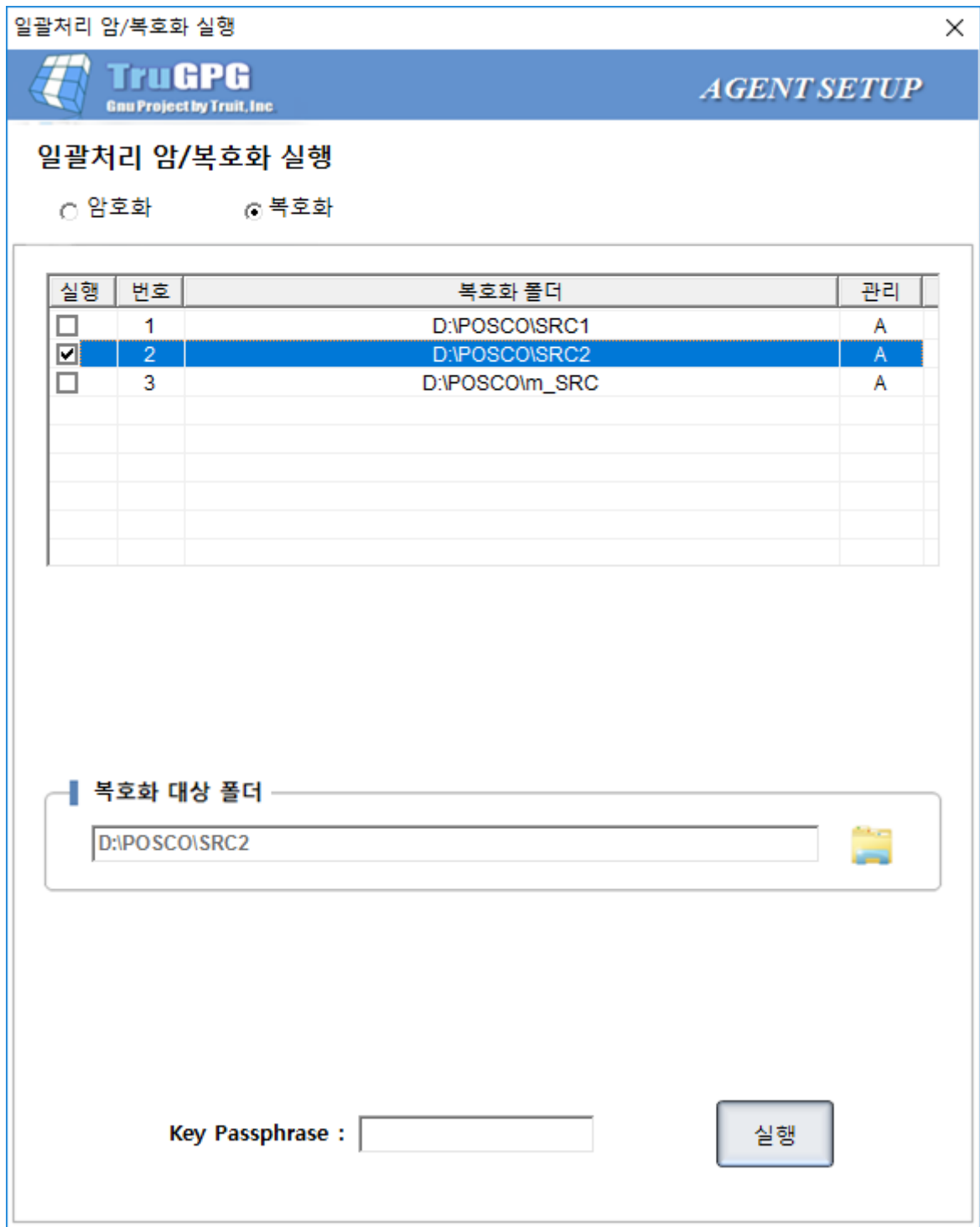
(조건 1) 관리에 "A" 로 표시되어 있는 폴더는 자동 암호화 프로세스가 Disable 상태여야 한다.



(조건 2) 이곳에서 등록된 관리 “M” 폴더는 자동 암호화 프로세스 상태와 관계없이 해당 폴더를 암호화를 실행할 수 있다. 다만, 자동 암호화와 마찬가지로 지정 폴더 내에 사용자가 존재하거나 Open 된 파일이 존재하는지를 재차 확인하기 위한 창을 띄운다.

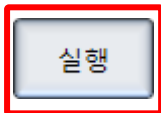


- 복호화 실행

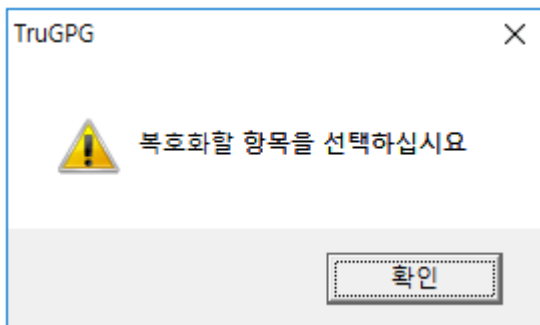


등록된 목록은 “일괄처리 암호화 설정”에서 설명한 바와 같이 “자동 암호화 프로세스 설정”에서 등록된 폴더는 관리에 “A”(Auto) 로 표시되며, “일괄 처리 암호화 실행”에서 등록된 폴더는 “M”(Manual) 로 표시된다. 그리고 일괄처리 복호화를 실행하기 위해서는 상단의 대상 리스트 중 실행을 원하는 해당 폴더의 “실행” 체크박스에 체크하고, 아래 “실행” 버튼을 클릭하면 된다.

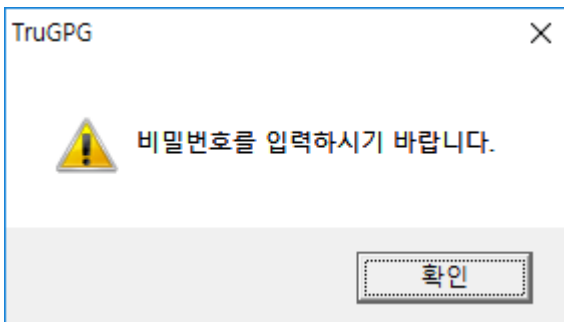
마찬가지로 여러 폴더를 같이 실행하려면, 해당 폴더들의 체크 박스를 체크하고 “실행” 버튼을 클릭하면 된다.



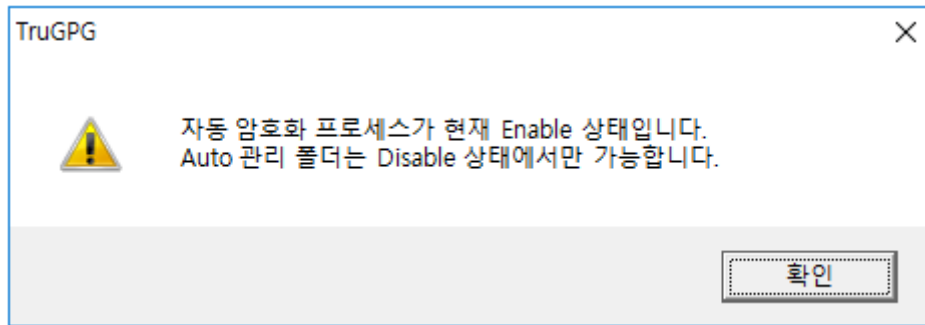
하지만 상단 리스트의 “실행” 체크박스에 선택된 폴더가 없으면 다음 확인 창이 나타난다.



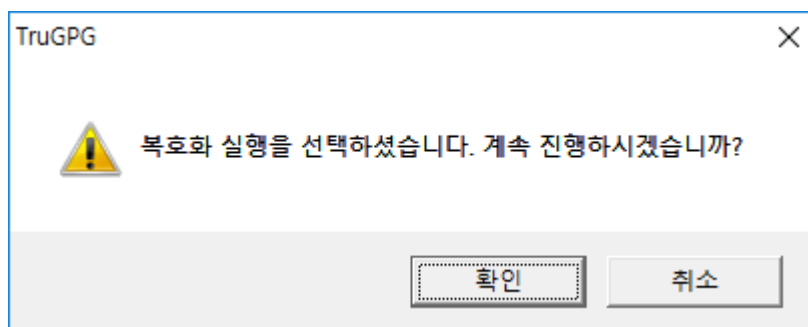
그리고 일괄 처리 복호화에서는 필수적으로 Key Passphrase(암호) 가 필요하며, 실행 버튼 누르기 전에 Key Passphrase가 입력되어 있어야 한다. 만약 Passphrase 입력 없이 실행 버튼을 누르면, 아래와 같은 경고 창이 나타난다.



(조건 1) 관리에 “A” 로 표시되어 있는 폴더는 자동 암호화 프로세스가 Disable 상태여야 한다.



(조건 2) 이곳에서 등록된 관리 "M" 폴더는 자동 암호화 프로세스 상태와 관계없이 해당 폴더를 복호화를 실행할 수 있다. 다만, 자동 암호화와 마찬가지로 지정 폴더 내에 사용자가 존재하거나 Open 된 파일이 존재하는지를 재차 확인하기 위한 창을 띄운다.



6) 암호화 키 관리

암호화 키 관리

TruGPG
Gnu Project by TruIT, Inc

AGENT SETUP


암호화 키 관리

중앙 키 관리 설정

- 중앙 키 관리 서버

키 관리 서버 1	172 . 24 . 80 . 9
키 관리 서버 2	172 . 24 . 146 . 50
계정	trugpg
암호	trugpg
Key_Rings 저장소	/home/trugpg/TruGPG_Key_Rings

- 로컬 서버

로컬 서버 명	POSCO-DEV
로컬 키 저장소	C:\truit\TruGPG\gnupp 

저장 닫기

암호화 키 저장 암호화 키 복구

각 서버에는 KEY_RING (비밀 키 + 공용 키) 폴더가 존재한다. 이 키 들은 암호화/복호화 하는 없어서는 안 되는 중요한 내용이므로 두 TruITM 서버에 동시 보관을 원칙으로 하며, 서버 정보는 다음과 같다.

- 키 관리 서버 1 : 172.24.80.9

- 키 관리 서버 2 : 172.24.146.50

- FTP 계정 : u : trugpg p : trugpg

- Key_Rings 저장소 : /home/trugpg/TruGPG_Key_Rings

- Local Directory of Key Ring : C:\Wtruit\WTruGPG\Wgnupg

(GnuPG 의 Home Directory 는 키 생성 계정의 Home Directory 아래에 생성되지만, 모든 계정에서 공통으로 Key_Ring 폴더를 사용하기 위하여 C:\Wtruit\WTruGPG\Wgnupg 로 정의 한다. 즉, 시스템 환경변수 GNUPGHOME 에 정의된 폴더를 의미한다.

참조 : 키 보관 절차 (Key_Ring 폴더 전체를 저장 한다.)

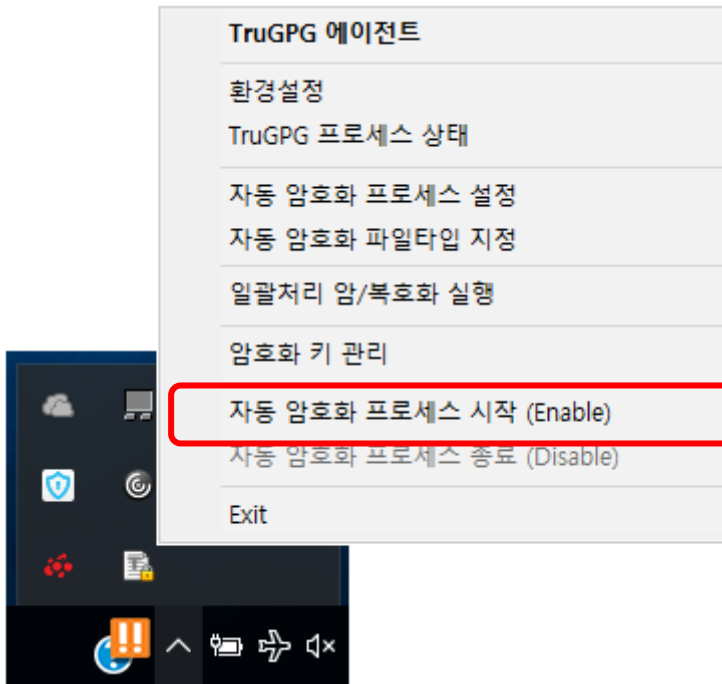
- 1) tar cf gpg_key.tar <C:\Wtruit\WTruGPG\Wgnupg>
- 2) ftp 172.24.80.9
- 3) ftp 172.24.146.50

암호화 키 저장 : tar 한 gnupg 폴더를 tar 한 gpg_key.tar 파일을 2개의 FTP 서버에 저장한다.

암호화 키 복구 : FTP 서버에 저장된 gpg_key.tar 을 사용하여 암호화 Key 를 복구한다.

암호화 키 저장/복구 시 실패 할 경우, 소스 암호화 담당자에 보고하고, 조치 이후 다시 키 저장/복구를 실행한다.

7) 자동 암호화 프로세스 시작 (Enable)



자동 암호화 프로세스는 백 그라운드 프로세스로서 지정된 폴더 내에 암호화되어 있지 않은 파일이 존재할 때, 실시간 검출하여 자동으로 암호화를 강제시키는 프로세스 이다.

자동 암호화 프로세스 상태를 나타낼 때 프로세스가 동작 중 인 상태를 '자동 암호화 Enable' 상태라 하며, 프로세스가 중단된 상태를 '자동 암호화 Disable' 상태라 한다.

만약 Enable 상태에서 해당 폴더에 암호화되어 있지 않은 파일이 존재하면 암호화를 하지만, 누군가가 그 파일을 Open 하고 있을 경우에는 해당 파일에 대한 정보와 Open하고 있는 Open 상태의 내용을 로그로 남긴다.

변경 관리 시스템과의 연동 관계는 변경관리 Check-Out 시 자동으로 Disable 상태로 되며, Check-In 시에 자동으로 Enable 되도록 작동된다.

즉, 변경관리에 의한 작동은 자동으로 Enable/Disable 상태가 변경되므로 현 메뉴를 사용 할 필요가 없지만, 수동으로 서버내의 소스 프로그램에 관한 작업이 필요 할 때 사용되는 기능이다.

- Enable 시켜야 하는 경우 :

1. 소스 프로그램 작업이 없는 평상시
2. 변경관리 Check-In 후 (자동실행)
3. 일괄처리 암호화 작업 완료 후 (수동실행)

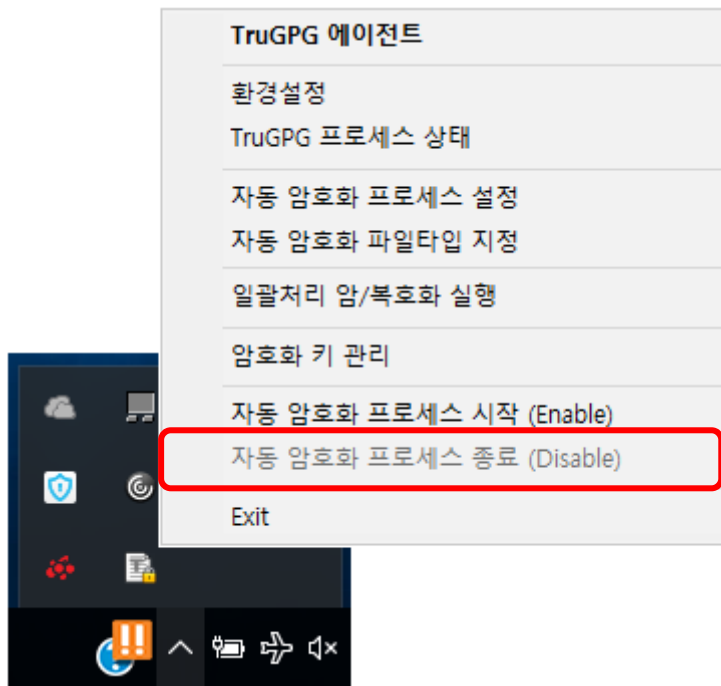
- 프로세스 확인 (작업 관리자) :

- TruGPG_Auto_Prc : 자동 암호화 프로세스

- TruGPG_Mon_Prc : 일괄처리 암호화 실행 프로세스

이름	6% CPU	38% 메모리	0% 디스크	0% 네트워크
Windows Shell Experience Host	0%	34.4MB	0MB/s	0Mbps
Windows Defender notification icon	0%	3.7MB	0MB/s	0Mbps
> VPWalletService(32비트)	0%	1.3MB	0MB/s	0Mbps
VestCert(32비트)	0%	12.1MB	0MB/s	0Mbps
Veraport Handler(32비트)	0%	1.8MB	0MB/s	0Mbps
TruSRM_WIN_Agent(32비트)	0.5%	4.1MB	0MB/s	0.1Mbps
TruSRM_Agent_Mon(32비트)	0%	0.8MB	0MB/s	0Mbps
TruGPG_Mon_Prc(32비트)	0%	1.0MB	0MB/s	0Mbps
TruGPG_Auto_Prc(32비트)	0%	1.0MB	0MB/s	0Mbps
TODO: <파일 설명>(32비트)	0%	72.3MB	0MB/s	0Mbps
> TeamViewer 11(32비트)	0%	3.1MB	0MB/s	0Mbps
> SynapticsWBF Policy Service (COGENT)	0%	5.2MB	0MB/s	0Mbps
Synaptics TouchPad 64-bit Enhancements	0%	4.8MB	0MB/s	0Mbps
Synaptics Pointing Device Helper	0%	0.7MB	0MB/s	0Mbps
> srwany(32비트)	0%	0.5MB	0MB/s	0Mbps

8) 자동 암호화 프로세스 종료 (Disable)



[기본 내용은 Enable 상태를 참조...

- Disable 시켜야 되는 경우 :

1. 변경관리 Check-Out 후 (자동실행)
2. 변경관리와 관계없는 소스검색/테스트 작업 시 (수동실행)
3. 일괄처리 복호화 작업 전 (수동실행)