

비정형데이터 암호솔루션

CryptoSwell 매뉴얼

목 차

제 1 장. CryptoSwell 개요

제 2 장. CryptoSwell 실행

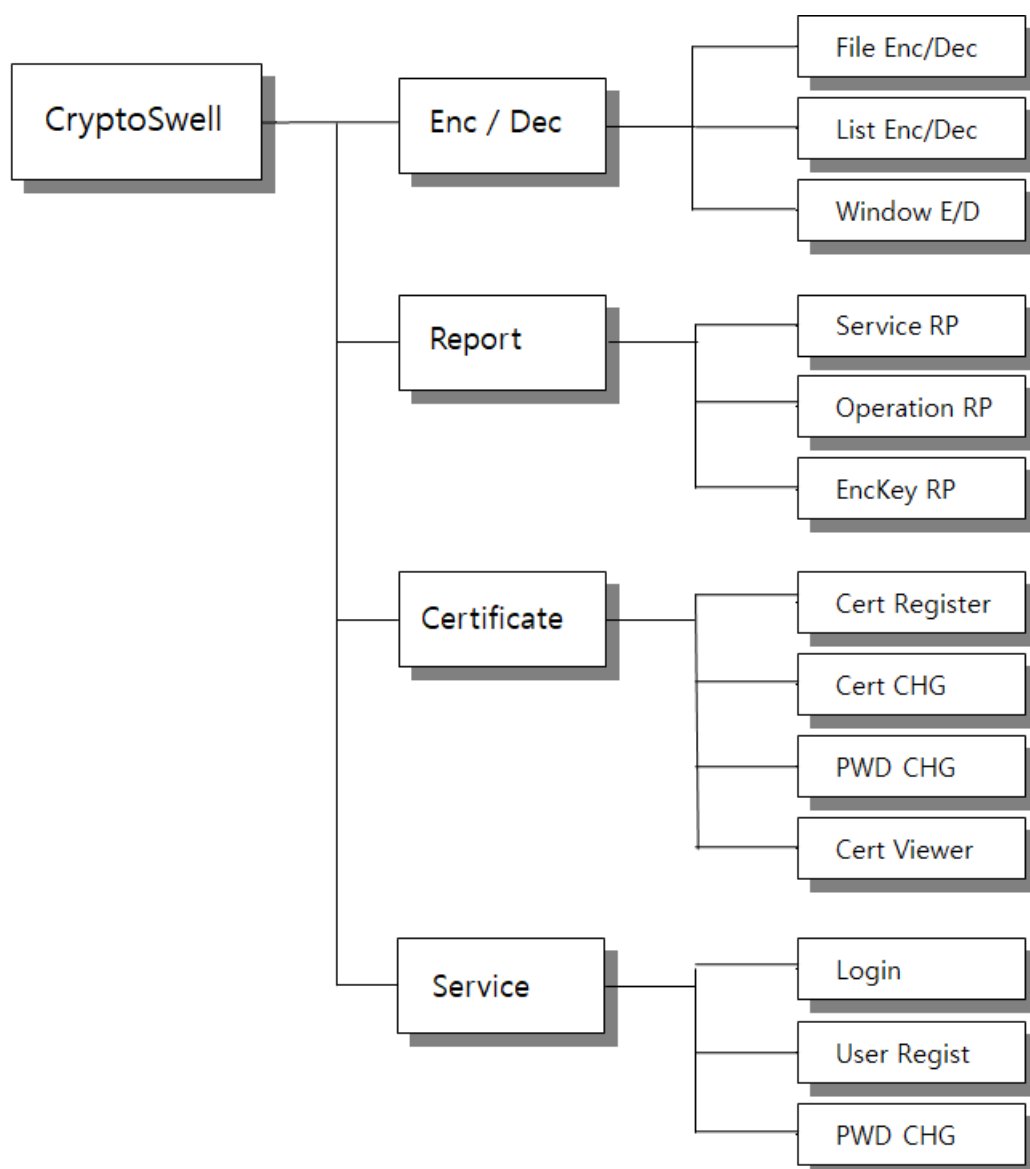
제 3 장. Log File

제 4 장. 메뉴 상세 설명

제 1 장 CryptoSwell 개요

CryptoSwell은 client와 Server로 구성되어 있으며, 비정형데이터(문서파일, 이미지, 동영상 등)를 암호하는 솔루션입니다. 암호에 사용되는 암호키를 관리하고, 서비스 이력과 관리자의 운영을 모두 로그로 저장한다.

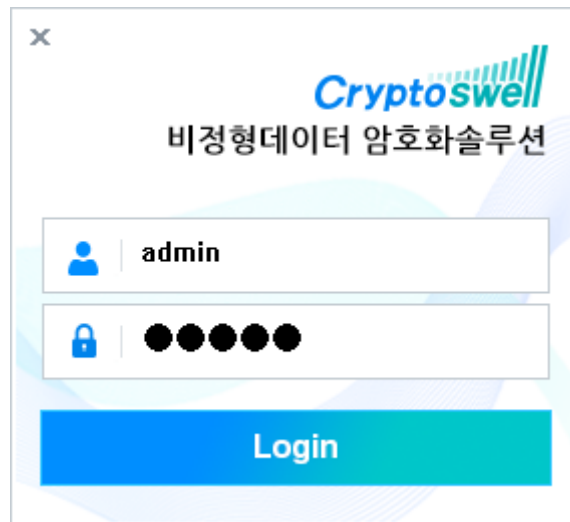
· 메뉴구성



제 2 장 CryptoSwell 실행

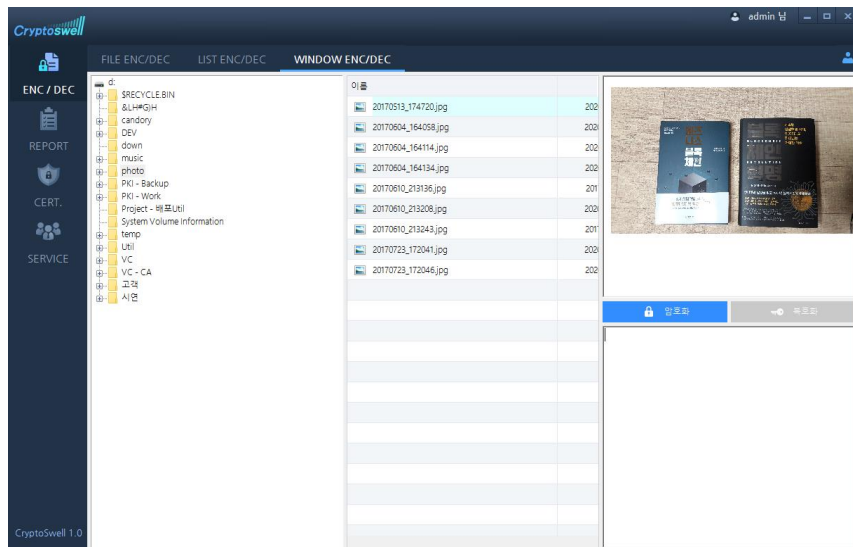
1. CryptoSwell 실행

가. 윈도우의 시작->프로그램-> CryptoSwell ->CryptoSwell Client를 클릭합니다.



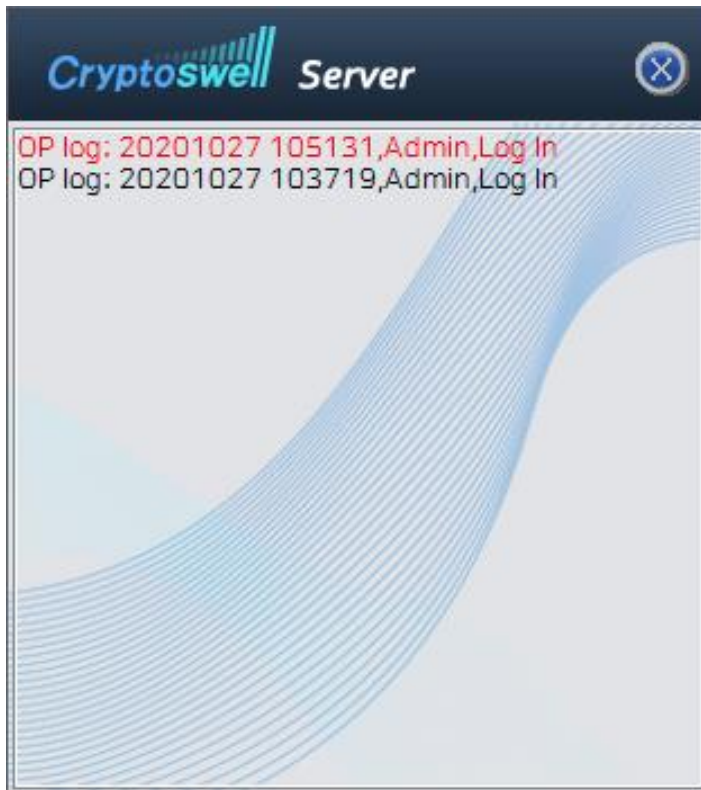
나. ID와 Password를 입력합니다.


다. Login 버튼을 클릭합니다.



2. CryptoSwell Server 실행

가. 프로그램을 설치하면 CryptoSwell Server는 자동실행 됨



나.  버튼을 누르면 “TrayIcon”으로 동작



제 3 장 LOG File

1. Service Log

- 이름 : “년월일.csv” 예) “20201022.csv”
- 위치 : Server 설치된 폴더 밑에 “log”라는 디렉토리에 있음
- 용도 : 암호, 복호한 내역을 저장
- 생성 : Client에서 비정형데이터를 암호, 복호할 때마다 생성
- 내용 : Time, file name, Client, Type(Enc, Dec), Tool(API, exe), PC Name

이름	수정한 날짜	유형	크기
20200701.csv	2020-10-23 오전 1:48	Microsoft Excel ...	24KB
20200702.csv	2020-10-23 오전 1:48	Microsoft Excel ...	35KB
20200703.csv	2020-10-23 오전 1:48	Microsoft Excel ...	29KB
20200704.csv	2020-10-23 오전 1:48	Microsoft Excel ...	9KB
20200705.csv	2020-10-23 오전 1:48	Microsoft Excel ...	8KB
20200706.csv	2020-10-23 오전 1:48	Microsoft Excel ...	10KB
20200707.csv	2020-10-23 오전 1:48	Microsoft Excel ...	11KB
20200708.csv	2020-10-23 오전 1:48	Microsoft Excel ...	10KB
20200709.csv	2020-10-23 오전 1:48	Microsoft Excel ...	59KB
20200710.csv	2020-10-23 오전 1:48	Microsoft Excel ...	29KB
20200711.csv	2020-10-23 오전 1:48	Microsoft Excel ...	9KB
20200712.csv	2020-10-23 오전 1:48	Microsoft Excel ...	8KB

	A	B	C	D	E	F	G
1	20201022	admin	d:\photo\20170608\20170127_152450.jpg	LEEYPMINIPC	EXE	ENC	
2	20201022	admin	d:\photo\20170608\20170127_152450.jpg.crp	LEEYPMINIPC	EXE	DEC	
3	20201022	admin	d:\photo\20170608\20170127_152450.jpg	LEEYPMINIPC	EXE	ENC	
4	20201022	admin	d:\photo\20170608\20170120_180722.jpg.crp	LEEYPMINIPC	EXE	DEC	
5	20201022	admin	d:\photo\20170608\20170127_152450.jpg.crp	LEEYPMINIPC	EXE	DEC	
6	20201022	admin	d:\photo\20170608\20170127_152457.jpg	LEEYPMINIPC	EXE	ENC	
7	20201022	admin	d:\photo\20170608\20170127_152457.jpg.crp	LEEYPMINIPC	EXE	DEC	
8	20201022	admin	d:\photo\20170608\20170603_202040.jpg	LEEYPMINIPC	EXE	ENC	
9	20201022	admin	d:\photo\20170608\20170603_202040.jpg.crp	LEEYPMINIPC	EXE	DEC	
10							
11							
12							

2. Crypt Key Log

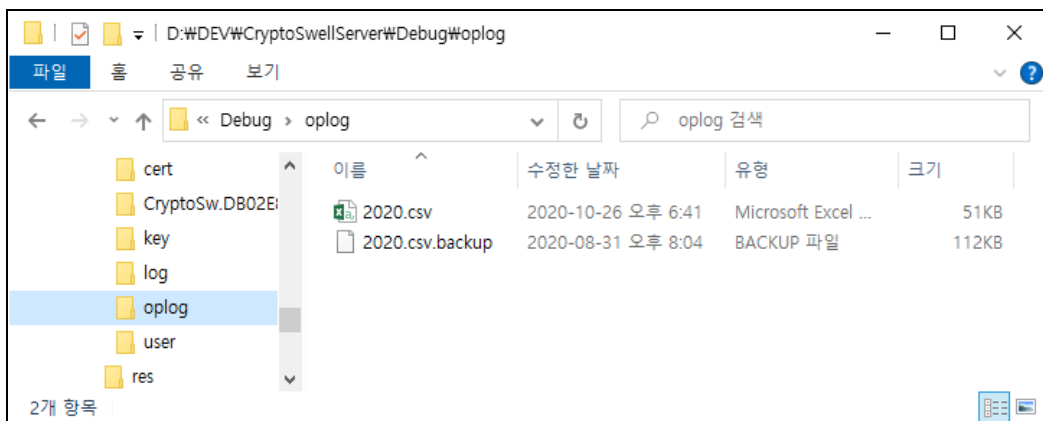
- 이름 : “년월일.csv” 예) “20201022.csv”
- 위치 : Server 설치된 폴더 밑에 “key”라는 디렉토리에 있음
- 용도 : Server가 Client에 내려 보낸 암호키를 저장
- 생성 : Client에서 암호키를 요청할 때 키를 보내고, 로그 저장
- 내용 : Time, Client, Encrypted CryptKey and Vector

이름	수정한 날짜	유형	크기
20200701.csv	2020-10-23 오전 1:48	Microsoft Excel ...	29KB
20200702.csv	2020-10-23 오전 1:48	Microsoft Excel ...	38KB
20200703.csv	2020-10-23 오전 1:48	Microsoft Excel ...	29KB
20200704.csv	2020-10-23 오전 1:48	Microsoft Excel ...	10KB
20200705.csv	2020-10-23 오전 1:48	Microsoft Excel ...	10KB
20200706.csv	2020-10-23 오전 1:48	Microsoft Excel ...	10KB
20200707.csv	2020-10-23 오전 1:48	Microsoft Excel ...	10KB
20200708.csv	2020-10-23 오전 1:48	Microsoft Excel ...	10KB
20200709.csv	2020-10-23 오전 1:48	Microsoft Excel ...	67KB
20200710.csv	2020-10-23 오전 1:48	Microsoft Excel ...	29KB
20200711.csv	2020-10-23 오전 1:48	Microsoft Excel ...	10KB

	A	B	C	D	E	F
1	20201022 213330	admin	PFUITQE5P0Bk9RZ/	i48xcHahG8bF9yoR		
2	20201022 215144	admin	PFUITQE5P0Bk9RZ/	i48xcHahG8bF9yoR		
3	20201022 223538	admin	Lk5Q3jhN42dPkeNL	2qnjH/hG+zT4z0D9		
4	20201022 223833	admin	zSxCccOzcrtmA3/V	1+rmWMQV+GalCjVo		
5	20201022 223901	admin	FWcyibf4yXdy3V3T	1c9BB70M+U1IAo34		
6						
7						
8						
9						
10						
11						

3. Operation Log

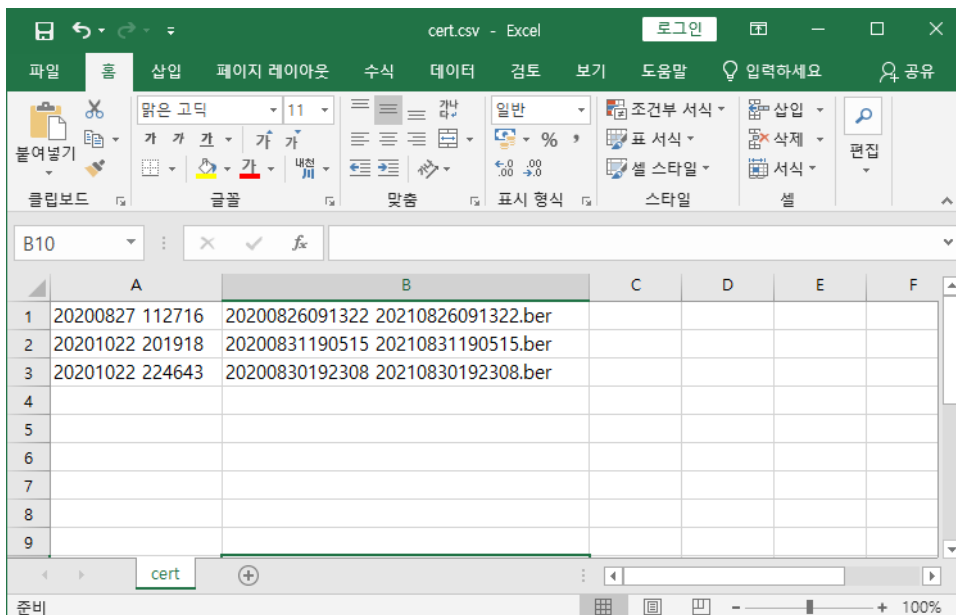
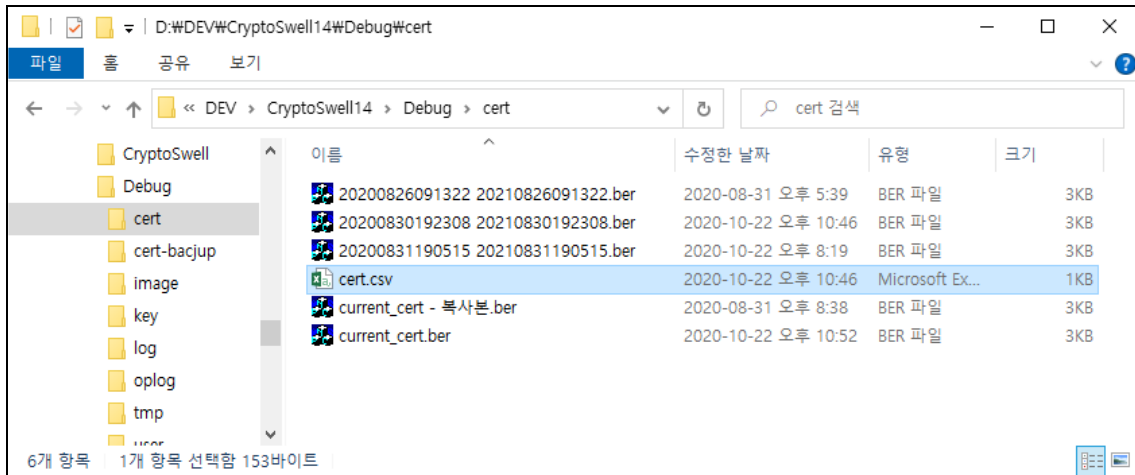
- 이름 : “년.csv” 예) “2020.csv”
- 위치 : Server 설치된 폴더 밑에 “oplog”라는 디렉토리에 있음
- 용도 : 운영자가 운영한 내역을 저장
- 생성 : CryptoSwell을 운영할 때 생성 예) 로그인, 인증서 변경 등
- 저장되는 내용
 - 1) 운영 : 로그인, 로그오프, 비밀번호변경
 - 2) 인증서 : 인증서 등록, 변경, 조회, 비밀번호변경
 - 3) 암호키 : 암호키 생성, 변경, 조회
 - 4) 사용자 : 등록, 삭제, 변경
 - 5) 서비스 : 파일 암호/복호, 리스트 암호/복호, 윈도우 암호/복호



	A	B	C	D	E	F	G
1	20200831 203838	admin	인증서변경				
2	20200831 211437	admin	인증서 비밀번호 변경				
3	20200901 142117	TEST1	Send User Authority !				
4	20200901 142117	TEST4	Send User Authority !				
5	20200901 142117	TEST5	Send User Authority !				
6	20200901 142117	TEST6	Send User Authority !				
7	20200901 142117	TEST7	Send User Authority !				
8	20200901 142118	TEST8	Send User Authority !				
9	20200901 142118	TEST9	Send User Authority !				
10	20200901 142118	TEST10	Send User Authority !				
11	20200901 142118	TEST11	Send User Authority !				

4. Certification Log

- 이름
 - 1) 인증서 변경 이력 : “Cert.csv”
 - 2) 현재 인증서 : “current_cert.ber
 - 3) 지난 인증서 : “유효기간시작일_유효기간종료일.ber”
예) 20200831190515 20210831190515.ber
- 위치 : Server 설치된 폴더 밑에 “cert”라는 디렉토리에 있음
- 용도 : 운영자가 인증서를 변경한 내역을 저장
- 생성 : 인증서를 변경할 때마다 로그와 새로운 인증서 파일이 생성




인증서

Col1	Col2
20200827 112716	20200826091
20201022 201918	20200831190
20201022 224643	20200830192

일반

자세히



인증서정보

인증서의 용도:

† 1.2.410.200020.1.1.3
 † 모든 용도 정적

발급대상 :

TestUser02

발급자 :

BlueSwellCA1

유효기간 :

유효기간(시작) 2020-8-30 부터
2021-8-30 까지













확인

인증서

Col1	Col2
20200827 112716	20200826091
20201022 201918	20200831190
20201022 224643	20200830192

일반

자세히

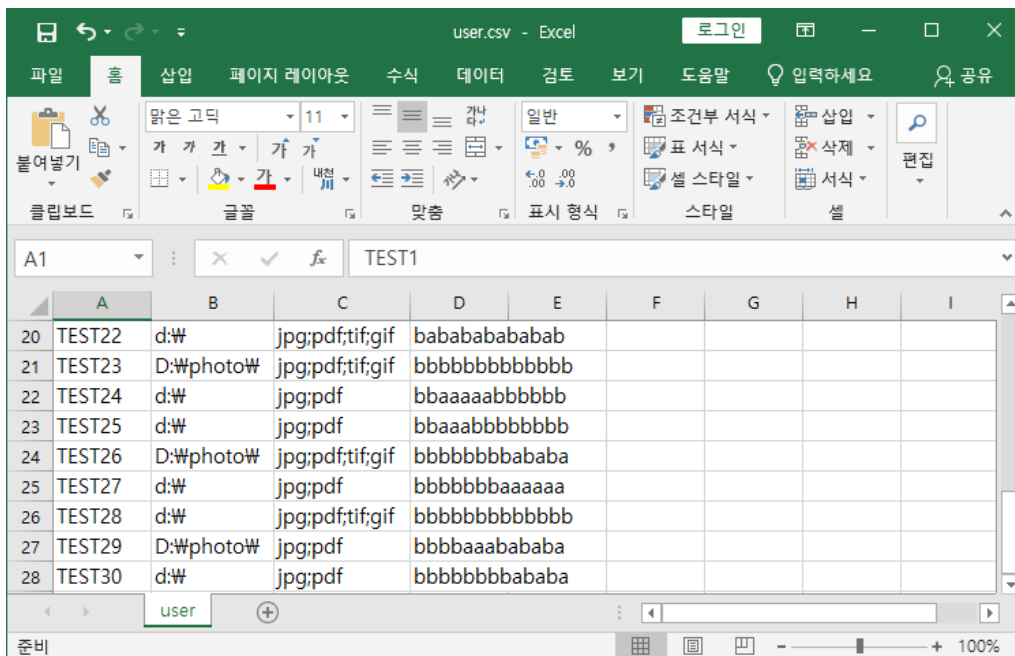
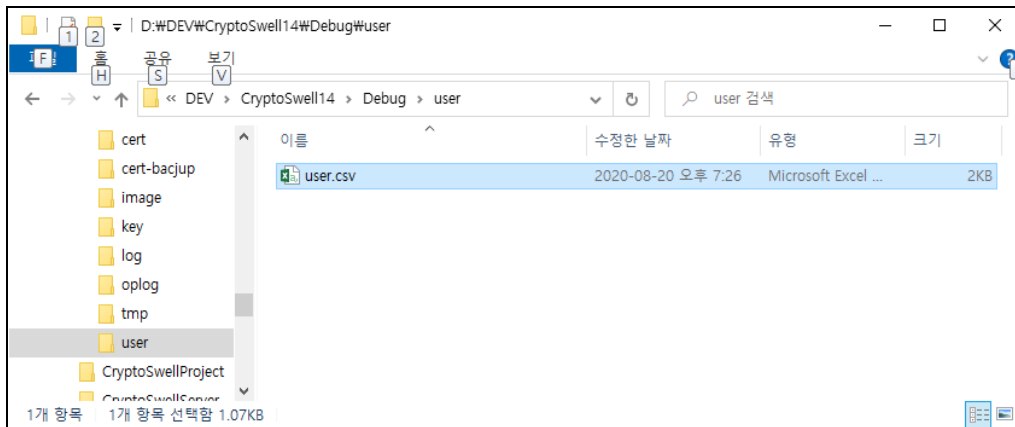
필드	값
 버전	3
 일련 번호	1234
 서명 알고리즘	sha256RSA
 서명 해시 알고리즘	sha256
 발급자	BlueSwellCA1, BlueSwell, ...
 유효 기간(시작)	2020년08월30일 19:23:08
 유효기간(끝)	2021년08월30일 19:23:08
 주제	TestUser02, BlueSwell, M...
 공개 키	RSA(2048bits)
 공개 키 매개 변수	05 00
 기관 키 식별자	KeyId=30228020d7c2f1...
 주제 키 식별자	0420d7c2f1843e109d92...

CN = TestUser02
 OU = BlueSwell
 O = Medical
 C = KR

확인

5. User File

- 이름 : “년.csv” 예) “2020.csv”
- 위치 : Server 설치된 폴더 밑에 “oplog”라는 디렉토리에 있음
- 용도 : 운영자가 운영한 내역을 저장
- 생성 : CryptoSwell을 운영할 때 생성 예) 로그인, 인증서 변경 등
- 저장되는 내용



제 4 장 메뉴 상세 설명

1. REPORT

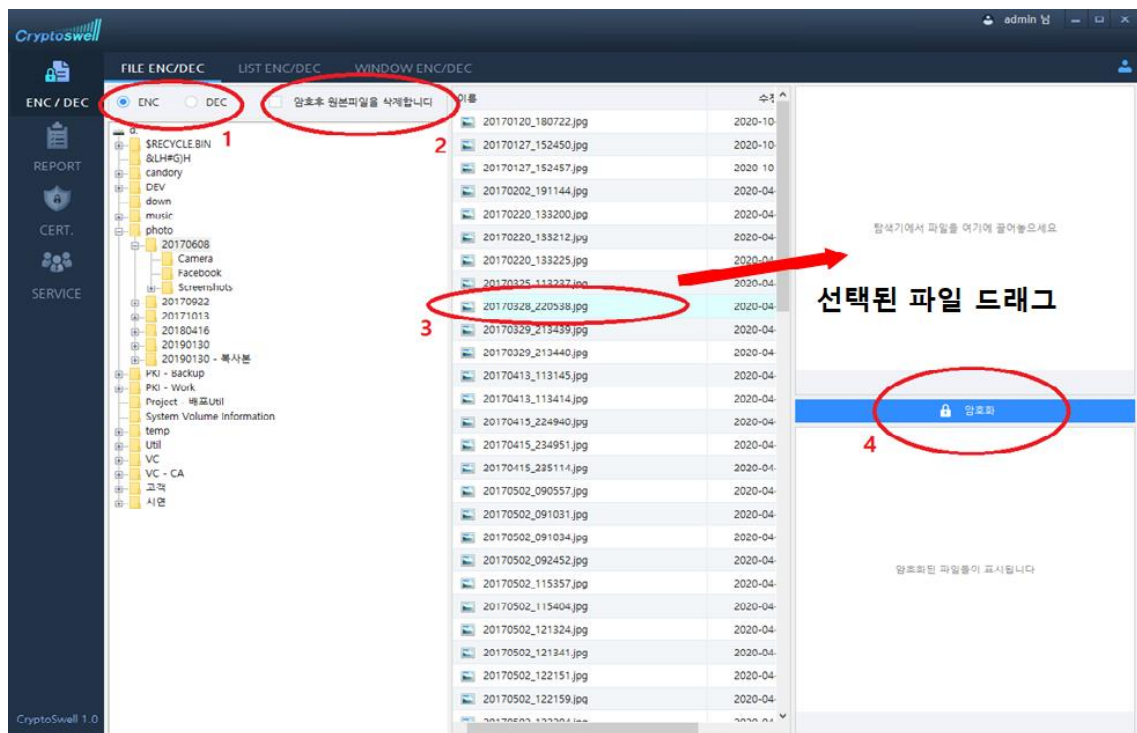
1) FILE ENC/DEC

선택한 파일을 암호, 복호합니다.

화면에 CryptoSwell 탐색기에서 파일을 선택하여 암호 또는 복호하면 됩니다.

서비스로그, 암호키로그를 남깁니다.

- ① 암호, 복호 선택
- ② 암호/복호 후 원본 삭제 선택
- ③ 선택된 파일 드래그
- ④ 암호/복호 버튼 클릭 (버튼의 글자는 1번의 선택에 따라 바뀜)



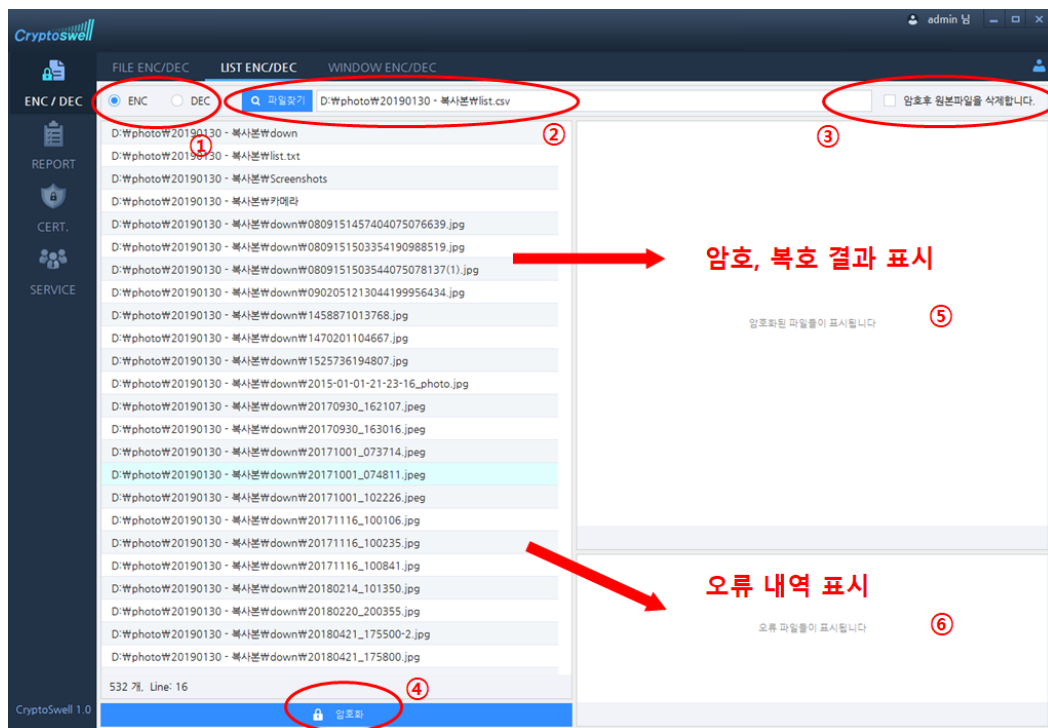
2) LIST ENC / DEC

파일리스트를 만들어 파일을 암호, 복호 합니다.

파일은 “.csv” 타입으로 만들어 드래그 하면 됩니다.

서비스로그와 암호키로그를 남깁니다.

- ① 암호, 복호 선택
- ② 리스트파일(예 list.csv) 선택
- ③ 원본 삭제 선택
- ④ 암호, 복호 버튼 클릭



* 리스트 파일 샘플 “list.csv”

	A	B
1	1	D:\photo\20190130 - 복사본\down
2	2	D:\photo\20190130 - 복사본\list.txt
3	3	D:\photo\20190130 - 복사본\Screenshots
4	4	D:\photo\20190130 - 복사본\카메라
5	5	D:\photo\20190130 - 복사본\down\0809151457404075076639.jpg
6	6	D:\photo\20190130 - 복사본\down\0809151503354190988519.jpg
7	7	D:\photo\20190130 - 복사본\down\0809151503544075078137(1).jpg
8	8	D:\photo\20190130 - 복사본\down\0902051213044199956434.jpg
9	9	D:\photo\20190130 - 복사본\down\1458871013768.jpg
10	10	D:\photo\20190130 - 복사본\down\1470201104667.jpg
11	11	D:\photo\20190130 - 복사본\down\1525736194807.jpg
12	12	D:\photo\20190130 - 복사본\down\2015-01-01-21-23-16_photo.jpg

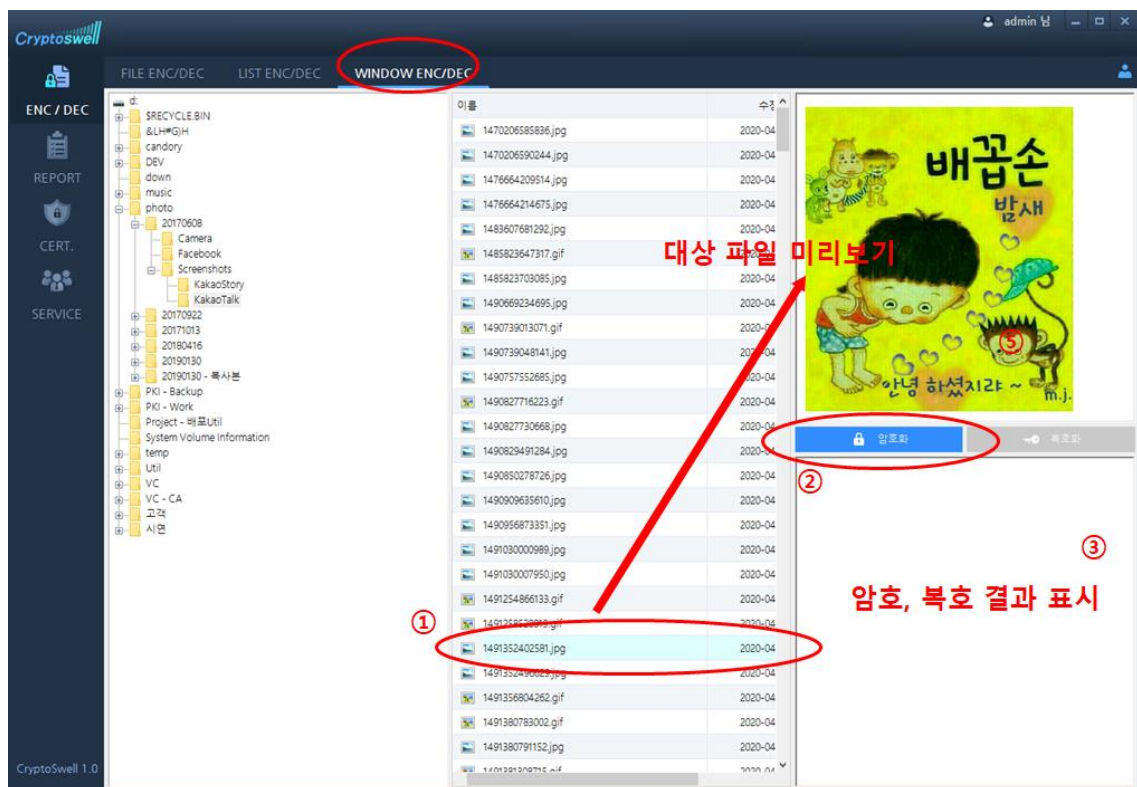
3) WINDOW ENC / DEC

파일리스트를 만들어 파일을 암호, 복호 합니다.

파일은 “.csv” 타입으로 만들어 드래그 하면 됩니다.

서비스로그와 암호키로그를 남깁니다.

- ① 파일을 선택. 파일에 따라 암호, 복호가 결정
예) 확장자 “.crp” -> 복호, 나머지 확장자는 암호
- ② 미리보기에서 확인
- ③ 암호/복호 버튼 클릭



2. REPORT

: 운영 내역을 조회하는 서비스

1) SERVICE REPORT

암호, 복호 내역을 조회합니다.

검색 조건은 OR 또는 AND 방식으로 추가됩니다.

로그는 “log”디렉토리 밑에 저장되어 있습니다.

- ① ID로 암호, 복호 내역 검색
- ② 날짜로 암호, 복호 내역 검색
- ③ 검색 조건 선택 : 암호, 복호, EXE, API
- ④ 파일 이름으로 암호, 복호 내역 검색

No	DATE/TIME	ID	EXE	File	ENC/DEC	ComputerName
0	20200704 121212	TEST11	EXE	abc.txt	DEC	YangPC
1	20200704 121212	TEST11	EXE	abc.txt	DEC	YangPC
2	20200704 121212	TEST11	EXE	abc.txt	DEC	YangPC
3	20200705 112121	TEST12	EXE	bbb.txt	ENC	Yang PC
4	20200705 112121	TEST12	EXE	bbb.txt	ENC	Yang PC
5	20200705 112121	TEST12	EXE	bbb.txt	ENC	Yang PC
6	20200706 112121	TEST12	EXE	sadfsdabc.txt	ENC	YangPC
7	20200706 112121	TEST12	EXE	sadfsdabc.txt		YangPC
8	20200706 112121	TEST12	EXE	sadfsdabc.txt		YangPC
9	20200707 112121	TEST12	api	ssssssssssssabc.txt	enc	YangPC
10	20200707 112121	TEST12	api	ssssssssssssabc.txt	enc	YangPC
11	20200707 112121	TEST12	api	ssssssssssssabc.txt	enc	YangPC
12	20200708 112121	TEST12	api	kkkkkkkkkkabc.txt	abc	YangPC
13	20200708 112121	TEST12	api	kkkkkkkkkkabc.txt	abc	YangPC
14	20200708 112121	TEST12	api	kkkkkkkkkkabc.txt	abc	YangPC
15	20200709 123456	TEST1	EXE	abc.txt	ENC	minipc
16	20200709 133456	TEST2	EXE	abc.txt	ENC	YangPC
17	20200709 143456	TEST3	EXE	next.png	DEC	YangPC
18	20200709 151234	TEST4	api	abc.txt	ENC	YangPC
19	20200709 164559	TEST5	EXE	demo.png	DEC	LeeSungCheolPC
20	20200709 174559	TEST6	EXE	1234.txt	DEC	nonamepc
21	20200709 184559	TEST7	EXE	박성윤.png	DEC	LeeSungCheolPC
22	20200709 123456	TEST1	EXE	abc.txt	ENC	minipc
23	20200709 133456	TEST2	EXE	abc.txt	ENC	YangPC

2) OP. REPORT

Admin 또는 User가 운영한 내역을 조회합니다.

검색 조건은 OR 또는 AND 방식으로 추가됩니다.

로그는 “oplog” 디렉토리 밑에 저장되어 있습니다.

- ① ID로 운영 내역 조회
- ② 날짜로 운영 내역 조회

The screenshot displays the 'OP. REPORT' section of the CryptoSwell application. The interface includes a sidebar with navigation options like 'ENC / DEC', 'REPORT', 'CERT.', and 'SERVICE'. The main area shows a table of operations. The table has columns for 'No', '날짜/시간', '아이디', and '내용'. The table is filtered by 'ID' (20200715 222219) and 'DATE' (2020-07-01 to 2020-10-27). A search button is located in the top right corner. Red circles and numbers 1-4 highlight key features: 1. ID input field, 2. DATE input field, 3. Search button, 4. Search results table.

No	날짜/시간	아이디	내용
0	20200715 222219	TEST1	Send User's Information !
1	20200715 222219	TEST2	Send User's Information !
2	20200715 222219	TEST3	Send User's Information !
3	20200715 222219	TEST4	Send User's Information !
4	20200715 222219	TEST5	Send User's Information !
5	20200715 222219	TEST6	Send User's Information !
6	20200715 222219	TEST7	Send User's Information !
7	20200715 222219	TEST8	Send User's Information !
8	20200715 222219	TEST9	Send User's Information !
9	20200715 222219	TEST10	Send User's Information !
10	20200715 222219	TEST11	Send User's Information !
11	20200715 222219	TEST12	Send User's Information !
12	20200715 222219	TEST13	Send User's Information !
13	20200715 222219	TEST14	Send User's Information !
14	20200715 222219	TEST15	Send User's Information !
15	20200715 222219	TEST16	Send User's Information !
16	20200715 222219	TEST17	Send User's Information !
17	20200715 222219	TEST18	Send User's Information !
18	20200715 222219	TEST19	Send User's Information !
19	20200715 222219	TEST20	Send User's Information !
20	20200715 222219	TEST21	Send User's Information !
21	20200715 222219	TEST22	Send User's Information !
22	20200715 222219	TEST23	Send User's Information !
23	20200715 222219	TEST24	Send User's Information !
24	20200715 222219	TEST25	Send User's Information !
25	20200715 222219	TEST26	Send User's Information !

④
조회 결과 표시

3) ENCKEY REPORT

암호키를 조회합니다.

암호키는 client가 암호를 할 때마다 생성 됩니다.

로그는 “key”디렉토리 밑에 저장되어 있습니다.

- ① ID로 암호키 조회
- ② 날짜로 운영 내역 조회

ENCKEY REPORT

ENC / DEC

REPORT

CERT.

SERVICE

CryptoSwell 1.0

admin 님

2020-07-01 2020-10-27

조회

No	DATE/TIME	ID	KEY	VECTOR
0	20200701 112345	test1	JSFn8NEH+eHtc1gn	KB5B7g2WkmLLdm
1	20200701 234511	TEST2	hUZV2T3SkqteKaCK	p4750GT38z0gM+I
2	20200701 334566	TEST3	wChyJaRD/OL4jNGI	OSRloXUuN2zg051
3	20200702 001234	TEST4	ADVwdN+5ADASo5a0	753zpEYVbUIU0thG
4	20200702 123454	TEST5	w5V7/PBI1AlmHR7	x03y3M0d0wJ11IKB
5	20200702 124455	TEST6	J+Y/orYRliYijjNSJ	4QZBSA09VMwDsfI
6	20200702 124553	TEST7	7aBTF6pISENX7+qm	dcSYYd7adpJGV5aJ
7	20200703 123520	TEST8	xPhMwV94g932c	yVjcGK+VbDPCuFXh
8	20200703 123521	TEST9	uoqYneq07EHdBRK	TBz9nI2JOIHEZwS/
9	20200703 131212	TEST10	9bLJVWUr20bela00	pmTxk8P5qVqYAZ1S
10	20200704 121212	TEST11	IBbVY5SWEMpSP3	G9h7H0Eku4300t
11	20200705 112121	TEST12	Y+YpIIVmaVMUMsC	htm2ouHBOPW+an3
12	20200706 112121	TEST12	vqa/UryvWwKMb+6N	MnhY1XVL7hukjPz
13	20200707 112121	TEST12	WpgITArclOIMDuZ	TaYpINI+aFhsIc+X
14	20200708 112121	TEST12	+57uG7PIZ3SOMPVO	GIDnlnSePISFwg
15	20200709 123456	TEST1	+UKsZpDpn5a0wY3Z	IG/TM6cS8QJMBuG
16	20200709 1334567890	TEST2	5o8HRSN83x0TXL1	IG/TM6cS8QJMBuG
17	20200709 143456	TEST3	G1e5rLuMc0n0IZMW	IG/TM6cS8QJMBuG
18	20200709 151234	TEST4	ZoamT6qIPpncJWBE	IG/TM6cS8QJMBuG
19	20200709 164559	TEST5	pHsb+JpCSgs2cghd	IG/TM6cS8QJMBuG
20	20200709 174559	TEST6	FFbjmVijM9Fd8/A	IG/TM6cS8QJMBuG
21	20200709 184559	TEST7	heKaG090E9dmlL8	IG/TM6cS8QJMBuG
22	20200710 123520	TEST8	G0gOLUJO7auJDQhJ	Ga+ESTBsszciBc
23	20200710 133520	TEST9	uS5jkncS1mwOrat	Ga+ESTBsszciBc
24	20200710 152547	TEST10	SuvKp4skVd8VlyIJC	Ga+ESTBsszciBc
25	20200711 121212	TEST11	Q+MT3E1H+G+akM	h+Vd8I1e4MwucG07

조회 결과 표시

3. CERTIFICATE

1) REGISTER CERT.

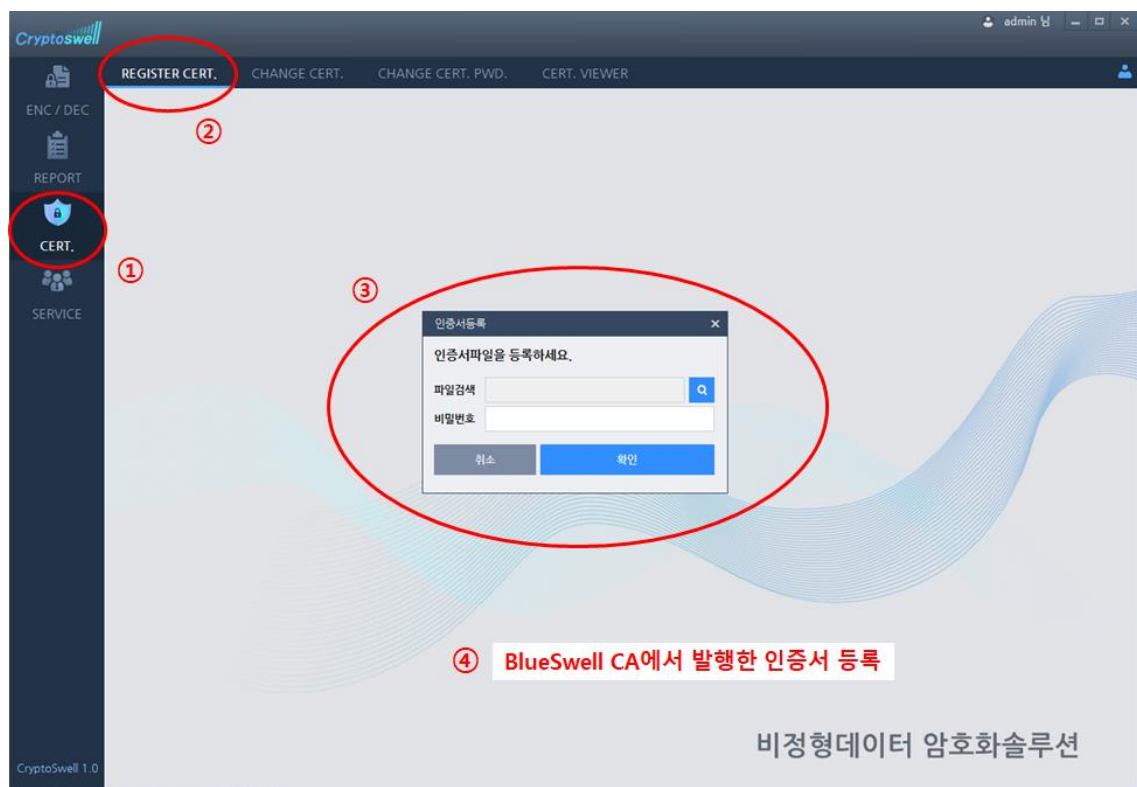
인증서를 등록합니다.

인증서가 등록되지 않으면 “SERVICE” 메뉴를 이용할 수 없습니다.

인증서는 “cert” 디렉토리에 저장됩니다.

사용가능한 인증정책은 “1.2.410.200020.1.1.3” 입니다.

- ① “CERT” -> “REGISTER” 를 선택
- ② BlueSwell에서 발급한 인증서를 입력
- ③ 인증서 비밀번호를 입력



2) CHANGE CERT.

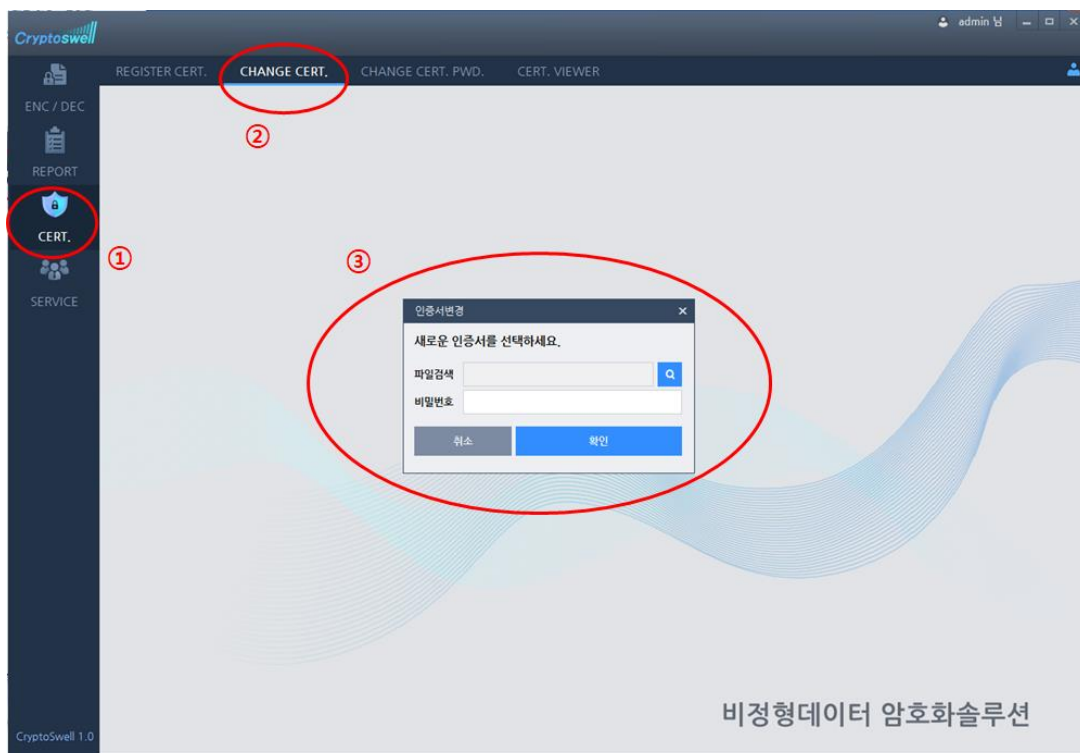
인증서의 유효기간이 지나면 갱신해야 합니다.

인증서를 갱신하지 않으면 서비스를 이용할 수 없습니다.

갱신한 인증서는 “cert” 디렉토리에 저장되고, 이력도 “cert.csv”에 기록 됩니다.

사용가능한 인증정책은 “1.2.410.200020.1.1.3” 입니다.

- ① “CERT” -> “CHANGE CERT.” 를 선택
- ② BlueSwell에서 발급한 인증서를 입력
- ③ 인증서 비밀번호를 입력

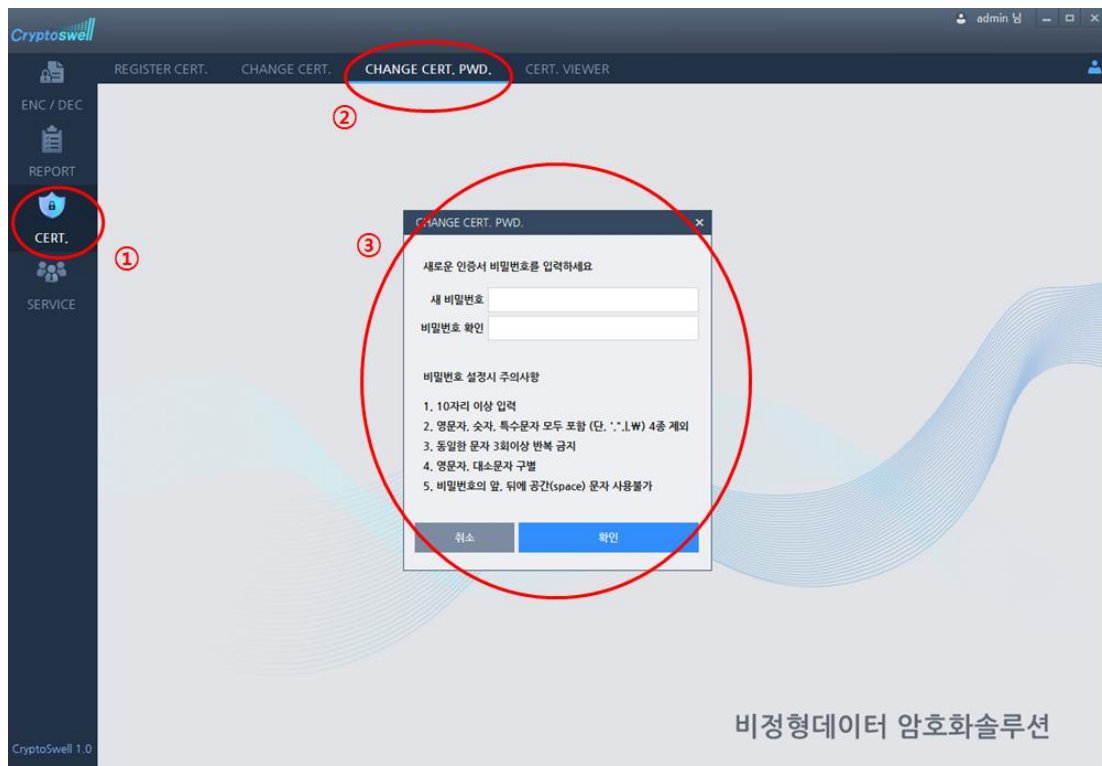


3) CHANGE CERT. PWD.

인증서의 비밀번호는 변경할 수 있습니다.

비밀번호를 변경하면 “current_cert.ber”에 변경된 비밀번호가 반영 됩니다.

- ① “CERT” -> “CHANGE CERT. PWD” 를 선택
- ② 새로운 인증서 비밀번호를 입력

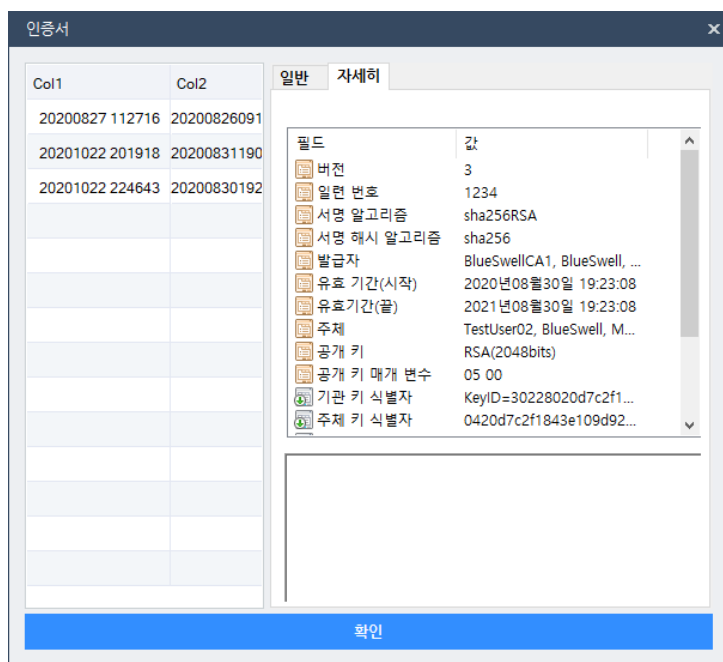
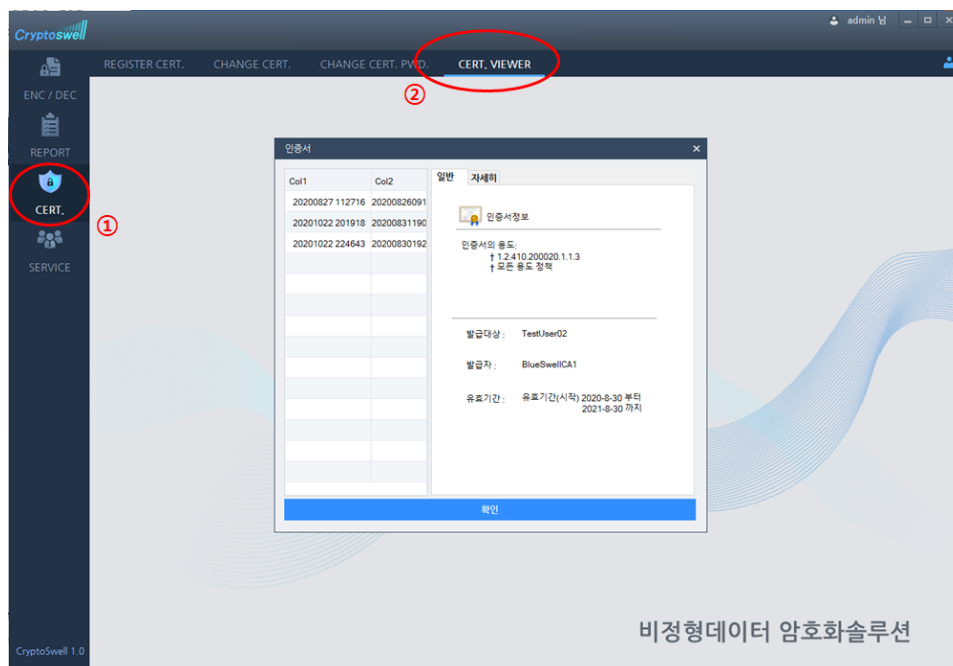


4) CERT. VIEWER

현재 사용하고 있는 인증서 정보를 볼 수 있습니다.

인증서의 유효기간은 인증서보기 메뉴를 통해 확인합니다.

- ① “CERT” -> “CERT. VIEWER” 를 선택
- ② 인증서의 유효기간 등을 확인



4. SERVICE

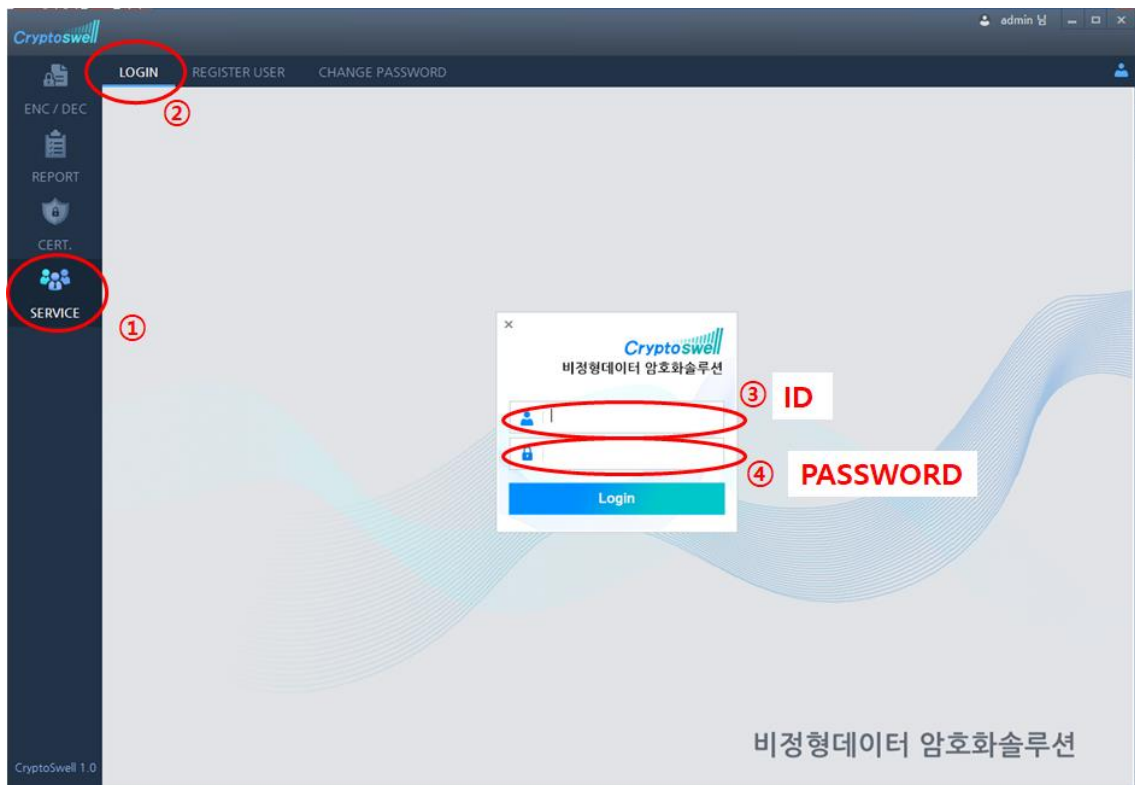
: 운영자가 CryptoSwell 을 관리하는 메뉴 입니다.

1) LOGIN

CryptoSwell을 사용하기 위해서는 login을 해야 합니다.

로그인 정보는 user_login.ini 에 저장 됩니다.

- ① “SERVICE” -> “LOGIN” 선택
- ② ID 와 Password를 입력



: user_login.ini 샘플

[USER]

id = admin

EncID = hQLMI dv/Se+iBPr1DlzIFLjy2dyVzfCi/dJAZvDx+1/3J7nvZe jlg bFQOStuB

EncPWD = hQLMI dv/Se+iBPr1DlzIFLjy2eHdyVzfCi/Dx+1/3J7nvZe jlg bFQOStuB

2) REGISTER USER

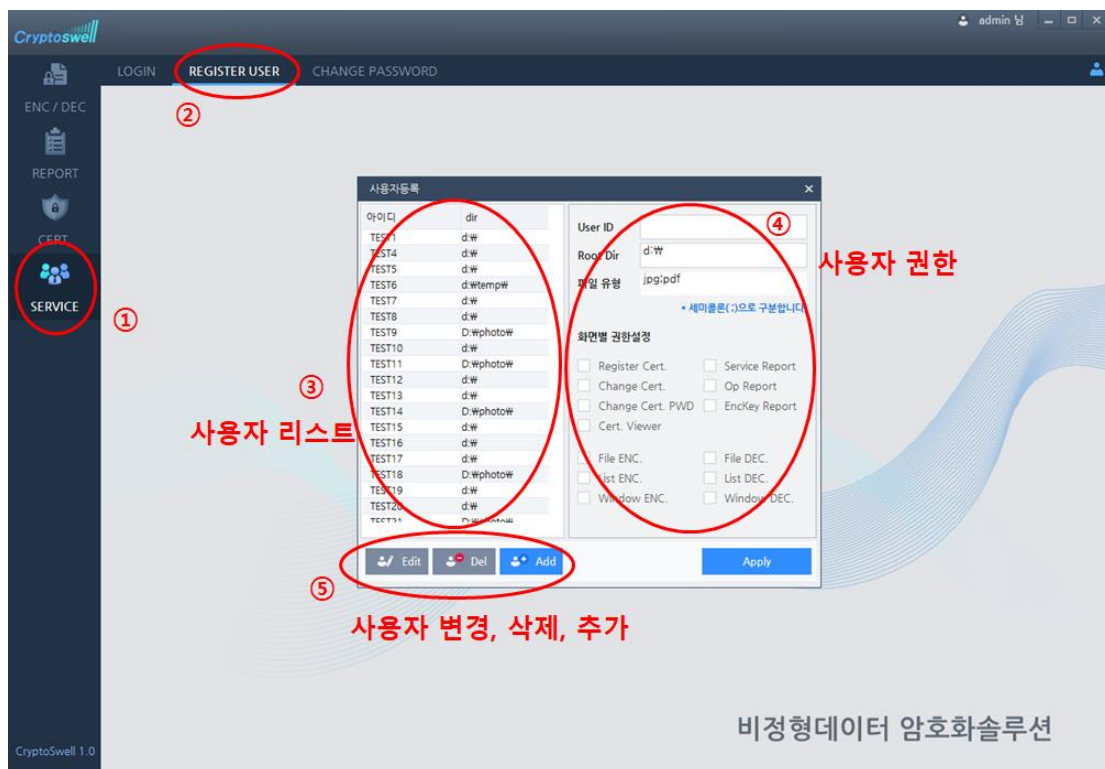
Admin 기능 입니다.

Admin는 Client를 등록할 수 있습니다.

등록된 Client만 CryptoSwell을 사용할 수 있습니다.

User정보는 “user” 디렉토리에 저장 됩니다.

- ① “SERIVCE” -> “REGISTER” 선택
- ② 사용자 리스트에서 사용자를 선택
- ③ 사용자를 추가할 경우는 “user id”에 새로운 id를 입력하면 됨
- ④ 사용자 권한 부분에 필요한 권한을 부여
- ⑤ “edit”, “Del”, “Add” 버튼을 상황에 맞게 사용



3) CHANGE PASSWORD

CryptoSwell을 Client의 비밀번호를 변경할 수 있습니다.
변경된 비밀번호는 user_login.ini 에 저장 됩니다.

- ① “SERVICE” -> “CHANGE PASSWORD” 선택
- ② 새로운 Password를 입력

