UbuCon Korea 2023

OpenPGP Keysigning Party

한영빈 (Youngbin Han)
<youngbin@ubuntu-kr.org | ybhan@ubuntu.com>

PGP, GPG, PGP/GPG 키사이닝 파티란 ?

- 키사이닝 파티 참여 문서를 참고 해 주세요
- 이번 세션에서는 간략히 구두로 설명하고 넘어 가겠습니다 .
- https://github.com/ubuntu-kr/ksp-toolkits/blob/master/ksp/ksp-20230909/readme.md

준비물을 잘 지참 해 오셨나요 ?

- 참가자 명단 파일을 인쇄한 종이
  - 내려받은 참가자 명단 파일에 대해 본인이 직접 계산한 SHA256 체크섬을 수기로 기입해서 지참 하셔야 합니다 .
- 제출 하셨던 GPG 공개키에 대해 신원을 확인할 신분증
  - 주민등록증 , 청소년증 , 운전면허증 , 여권 , 외국인증 , 국가기술자격증 등 .

사전에 공개키를 제출하지 못했다면 ?

- 괜찮습니다 . 여전히 참여 가능합니다 .
- 동일한 준비물과 추가로 본인의 키 핑거프린트가 적인 쪽지를 지참하여 참여하세요 .
- 명단 파일 인쇄물을 지참 하셔서 , 함께 체크섬을 맞춘 경우 , 본인의 핑거프린트를 상대방이 직접 확인 하면 됩니다 .
- 본인의 핑거프린트가 적힌 쪽지만 있는 경우 , 서로 핑거프린트를 직접 대조해야 합니다 .

키사이닝 파티 프로토콜

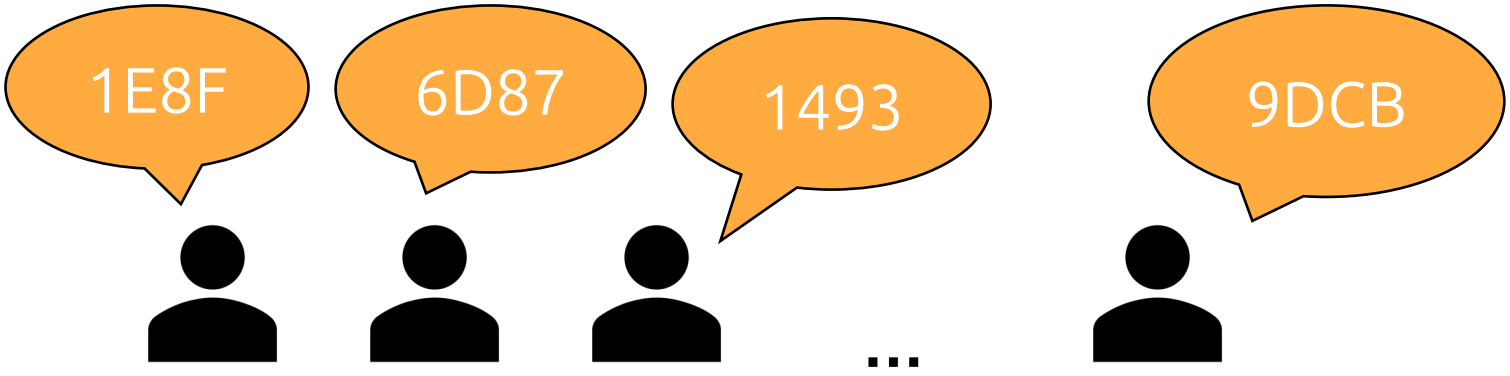
1. 먼저 다같이 각자가 계산해 온 체크섬 일치여부를 검증합니다 .
2. 자유롭게 돌아 다니면서 키사이닝을 할 상대를 만납니다 .
3. 참가자 목록 상에서의 번호를 물어봅니다 .
4. 체크섬을 다같이 확인할 때 체크 했는지 여부를 물어봅니다 .
5. 만약 체크 했다면 , 핑거프린트 일치 확인을 건너 뜁니다 .
6. 체크하지 않은 사람이라면 , 직접 핑거프린트를 대조합니다 .
7. 참가자 목록의 신원과 상대가 제시한 신분증 그리고 상대의 얼굴을 대조하여 신원을 확인합니다 .
8. 신원을 충분히 확인 했다면 , 인쇄물의 해당 항목에 체크 표시를 하고 확인 작업을 마칩니다 .
9. **만나서 인사 한 김에 수다도 떨고 이야기도 좀 나눕니다 .**

이제 다같이 체크섬을 맞추어 봅시다 !

- 수기로 체크섬을 기록한 참가자 목록 인쇄물과 필기구를 꺼내 주세요 .
- 돌아가면서 손을 들고 , 체크섬 앞자리부터 4 자리씩 외칩니다 .
- 다른 사람이 외친 체크섬 일부가 틀리다면 즉시 이의를 제기합니다 . 다음 사람이 동일한 부분을 다시 외칩니다 .
- 이렇게 마지막 자리까지 돌아가면서 외쳐서 체크섬이 일치함을 다같이 확인합니다 .
- 숫자는 로마자와의 혼동을 방지하기 위해 고유어로 부르겠습니다 .
  - (예 : **9E3D** [**아홉 , 이 , 셋 , 디**])

체크섬 확인 예시

체크섬이 1E8F 6D87 1493 ... 9DCB 라면...



SHA256 Checksum

EDC4 6371 **BE1A** 8697

9EC4 **A019** F663 **CEE3**

D828 FDAD **1CF2** 91D1

9940 **A082** FD78 **E5F8**

숙제 ! - 키사이닝 !

- 인쇄물에서 체크한 사람의 공개키에 키사이닝을 합니다 .
- 키사이닝한 공개키를 원래의 주인에게 전송합니다 .
- 다른 사람으로부터 키사이닝 된 본인의 공개키를 받아 본인의 PC 에 불러옵니다 .

Debian / Ubuntu 계열 - Caff 를 활용한 일괄 키사이닝

Signing-party 패키지 설치

```
> sudo apt install signing-party
```

caff 명령을 한번 실행하여 필요한 설정파일 초기화

```
> caff
```

~/.caffrc 설정

```
$CONFIG{'owner'} = '본인 이름';
$CONFIG{'email'} = '이메일 주소';
$CONFIG{'reply-to'} = 회신 받을 이메일 주소';
…
# Caff에서 사용할 GPG키 KeyID(핑거프린트 끝 16자리)입력.
$CONFIG{'keyid'} = [ qw{FEDCBA9876543210} ];
# 여러개 입력 시 공백으로 구분:
# $CONFIG{'keyid'} = [ qw{0123456789ABCDEF 89ABCDEF76543210} ];

# 위에서 입력한 GPG키가 여러개일 경우, 그 중 키사이닝에 쓸 키 지정
$CONFIG{'local-user'} = [ qw{0123456789abcdef 89abcdef76543210} ];
```

~/.caffrc 설정

```
…
# GPG 키 불러올 키서버 설정
$CONFIG{'keyserver'} = ‘keyserver.ubuntu.com’;
…
# 키사이닝된 공개키 전송에 쓸 메일의 메일서버 설정
# 아래는 Gmail 예시
$CONFIG{'mailer-send'} = ['smtps', Server => 'smtp.gmail.com', Port
=> 465, Auth => ['<Gmail 주소>’, ‘<Google 앱 패스워드 입력>']];
```

~/.caffrc 설정

…

 # 아래 메일 템플릿 주석 해제 처리

```
#$CONFIG{'mail-template'} = << 'EOM';
#Hi,
#
#please find attached the user id{(scalar @uids >= 2 ? 's' : '')}
…
#If you have any questions, don't hesitate to ask.
#
#Regards,
#{$owner}
#EOM
```

Caff - 키사이닝 및 메일 발송

다음 명령어 실행하여 수행

```
caff <key 1> <key 2> ... <key n>
```

Pius 를 이용한 키사이닝

https://www.phildev.net/pius/

Ubuntu Universe 저장소 활성화 후 , pius 패키지 설치

```
sudo apt install pius
```

다음 명령으로 키사이닝 일괄 진행 (Gmail 예제)

```
pius -H smtp.gmail.com -p 587 -u <Gmail 주소 > -A -r < 키링 경로 > -s
< 키사이닝에 쓸 키 ID>
```

키사이닝 된 내 공개키를 메일로 받았다면 ?

받은 암호화된 메일 화면에서 , 원문 보기 메뉴 선택 .

아래와 같은 부분 복사하여 파일로 저장 .

-----BEGIN PGP MESSAGE-----

< 암호화된 내용 >

-----END PGP MESSAGE-----

복호화 후 불러오기 gpg -decrypt < 파일명 > | gpg -import

필요한 경우 키서버에 업로드

gpg -keyserver < 키서버 주소 > --send-keys < 키 ID>

일일이 메일 주고 받기 귀찮다면...

상호 협의 하에 지정된 키서버에 업로드 하여 교환 .

```
gpg -keyserver <키서버 주소> --send-keys <키 ID>
```

감사합니다 .