INE5429 - Segurança em Computação
Trabalho Individual III

16100725 - Fabíola Maria Kretzer

30 de abril de 2019

Certificado PGP ou GPG

Questão 1:

O certificado PGP criado seguido o tutorial presente em:
https://help.ubuntu.com/community/GnuPrivacyGuardHowto

RNP > Segurança em redes > Servidor de chaves PGP do CAIS

Public Key Server -- Get "0xdd971f2e575d256c "

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: SKS 1.1.6
Comment: Hostname: raxus.rnp.br

mQENBFy/bT8BCACl7tuoENRQwi//6Fil0aLlzomF4yfn2+r4kONzXyc7QCosPi1Gfcbed82/
9l6tlXDjuFUUw0kRShVkS5qZngUM3m3hgl3PKaXaB17pcUvNncrpq6nB2WlSq7RbCy6qW9sN
4ovYecxtklnQWL2sPFSiWI/Gp8FMkuO8YeKrbRNXPOan0rNLLW5WjA1F+kpOViCvrdTfcYuD
tOOFKzNDXz9uUDvNqRBZibkkXWHyI19o6k55T/4RQYTt2fSpRziFKQrfmrezy9bF50RC97VI
1HuqalvVIT3b0xfzXe8pdQI4Z1TbEqouBsgsfZ7BrmUWGanw56/8/iWcDou4EWFvxOTJABEB
AAG0eUZhYmlvbGEgTWFyaWEgS3JldHplciAoUXVlcj8gRmHDp2EgYWNvbnRlY2VyIHF1ZSBh
IMO6bmljYSBjb2lzYSBxdWUgY2FpIGRvIGPDqXUgw6kgYSBjaHV2YSEpIDxmYWJpb2xha3Jl
dHplckBob3RtYWlsLmNvbT6JATMEEAEIAB0WIQSukAwrgnGJuEDTXJ2Gu3Q8py5vrAUCXMDc
AQAKCRCGu3Q8py5vrNPLB/0Xla5rwo2SsWNCuYZ4XMTPAa9frWyup4J5JCVyEUzT86mpdONg
JAwdSnQYEqhQS6J6EFD+2zgi7R37QWYMFpba38fWo0fcdKtu0R6FriEZftxPemZvi3ITax/O
dxDf315jt0ShUgBdM+x32PTLi9B6Hb5Zjvg8aUXUR+//kasJMhDKeLCrU3Ndue0fVhe0YjVS
AoQSwFa8RI4Xdq5f+y3/iBLBQPsriG7gyuyRn8LiB8v032bfmDgIh7onEAUc0nW6493Fcc3U
Si5fH4SRtGGY7juetanshIsrGudmQw0c/S01dBthOssKvV3IfORKo3VM6gzY0+LND+ozWeTr
6AlPiQE4BBMBAgAiBQJcv20/AhsDBgsJCAcDAgYVCAIJCgsEFgIDAQIeAQIXgAAKCRDdlx8u
V10lbOyQB/4y/s0MxEglB+fepRnKcFcGueLDSthB0Y85R6rSvwXDgd20QTVt0wdwnYzvgART
Va1HYzbMV3LOZFAn9yj9RDDaHEkVXnBKhK/POcF0SrochT2ovZf+dgMt24QoAdCgSupPRUmE
BWgy1OEmBXlq7w9eOc0bRFxo8hlaCWfOoPK+KHajiTJtbiCgnYH22L26O6DSJbDTC7unO7RQ
pSUUB/sKH1Iw1KoGw1rfSlonoA5DBjcLlZNKvB4WMz8MnIK2PuU8sfs+4Go4RwuUA+P2exzh
bLEziFnVMj/DtLDDy8X3Cqww18ka1ljLOcD7aUdtMpp06fki+5yNFdJoFPgDdgPDuQENBFy/
bT8BCACwGInsBQblOwP/m+lyl1PxAQUE6iZvdjK6bQE88/MbqTqnE6LNk/kpp7GHE+v1PsQ4
idzsbPRwiSf+68cthmbmR6yAmZNG6DmHJyoe0Nm5AYegblhov+2SbCW20SsWGfda1pWuwiVF
IBiBm5CbzrfH7VA3JsHVxnpz7PzOXC+chjPgBDHCklPcav5jHaBhFCW4JJlv3KfyogRpcuvf
GKOZ8cR7HyAM9K+CqsAp4zHVVF6IVg0Nfub5inr/ytTKe7U+by11iGe+dcO2xeORIgLGy48e
93/+LZWZKD661+5rD+r7obSjQcLLJN2SB20YLf5omh0kLc9xTZD+jeSE/QzbABEBAAGJAR8E
GAECAAkFAly/bT8CGwwACgkQ3ZcfLlddJWzDfwf/UB1NUofxIG7vWW9+rpG15yN76/l7XSpz
BpO4dIt9QevXgkXaIeKkfDHRpPPLFM3ztIUCVliT7vlf9n9DKSgB8tnj+7j8kCw9LO6S/mvz
mzNPvXUvNvd2wHxO2ijrw720NPS36kygb/1T5J5RHyvRLbIc+NQYiBT6Gn+tDm27A0atdp+4
/p1sXvNDkXLa6rshqpHbQWfmDz+cFVjpuzmY3VQmrZnQca6mZV0g04lXXazfGFYNyJqSUc8W
/xVgzmDClCnkMS7E44kk+RiHlTJ5DzyvgAVKf49wIGo7sZqCnI/S2qS8tvypAlK64Ow0qx94
R3FmK9ufGrkFwojWZoNzsA==
=ZxbL
-----END PGP PUBLIC KEY BLOCK-----
```

Figura 1: Certificado criado com o *keyID* 0x575d256c

Questão 2:

Primeiramente criei o certificado PGP com *keyID* E9E27696 usando o comando:

```
$ gpg –gen-key
```

Depois coloquei a chave pública no servidor do ubuntu:

```
$ gpg –send-keys –keyserver keyserver.ubuntu.com E9E27696
```

```
Type bits/keyID     cr. time   exp time   key expir
------------------------------------------------------------------------

pub  3072R/E9E27696 2019-04-25

uid Fabiola Kretzer <fabiolakretzer@hotmail.com>
sig  sig3  E9E27696 2019-04-25 __________ 2021-04-24 [selfsig]

sub  3072R/259812BB 2019-04-25
sig sbind  E9E27696 2019-04-25 __________ 2021-04-24 []
```

Figura 2: Imagem mostrando o certificado 0xE9E27696 no servidor do ubuntu

Em seguida, coloquei a chave pública no servidor da RNP utilizando a interface do link https://memoria.rnp.br/keyserver, mas poderia ter sido feito por linha de comando, substituindo keyserver.ubuntu.com no o comando anterior por keyserver.cais.rnp.br.

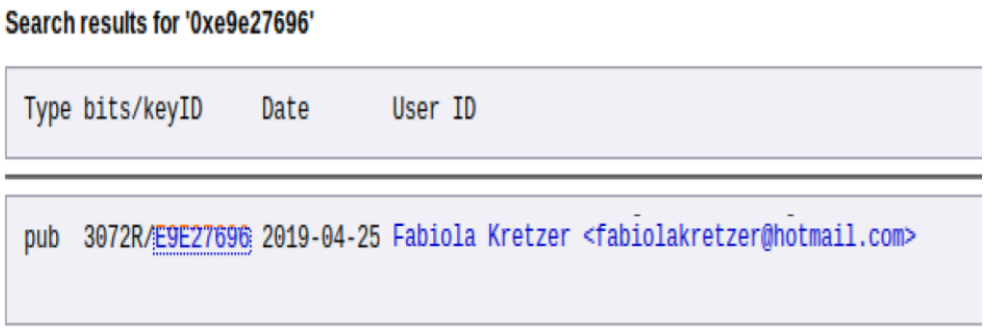

Figura 3: Imagem mostrando o certificado 0xE9E27696 no servidor RNP

Também criei um arquivo chamado revprivate.key com a chave privada com os dois comando abaixo, pois a única forma de revogar uma chave pública do servidor é enviando um certificado de revogação, que irá requerer acesso à chave privada.

```
$ gpg –list-secret-keys
```

```
$ gpg -ao revprivate.key –export-secret-keys E9E27696
```

Então, necessário gerar um certificado de revogação a partir da sua chave privada usando o comando abaixo:

```
$ gpg -o certificado_revoga.asc –gen-revoke -armor E9E27696
```

Importar o certificado no GnuPG:

```
$ gpg –import certificado_revoga.asc
```

Enviar o certificado para o servidor de chaves RNP e ubuntu:

```
$ gpg –keyserver keyserver.ubuntu.com –send-key E9E27696
```

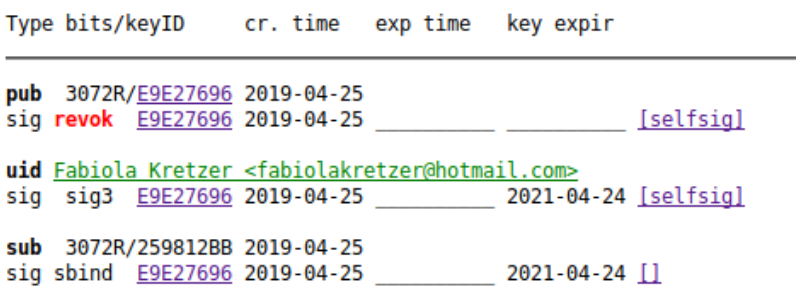

Figura 4: Imagem mostrando o certificado 0xE9E27696 revogado no servidor do ubuntu

```
$ gpg –keyserver keyserver.cais.rnp.br –send-keys E9E27696
```

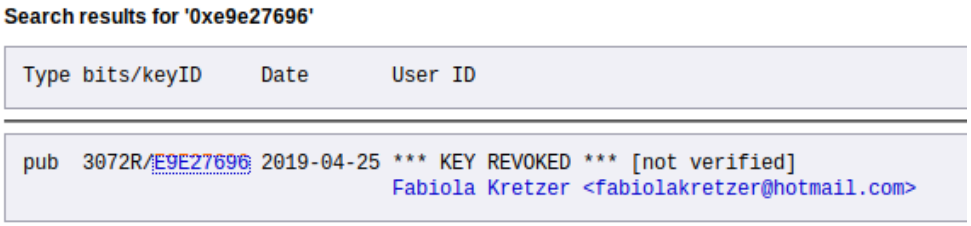

Figura 5: Imagem mostrando o certificado 0xE9E27696 revogado no servidor RNP

Questão 3:

A assinatura de um certificado inicia pela identificação do *keyID* de outra pessoa. Neste caso, será assinado a chave com *keyID* igual à 0x4706F0CB. Primeiro recupere as chaves:

```
$ gpg –recv-keys 4706F0CB
```

Depois assine o certificado:

```
$ gpg –sign-key 4706F0CB
```

E, por fim envie a assinatura para o servidor RNP:

```
$ gpg –send-keys –keyserver keyserver.cais.rnp.br 4706F0CB
```

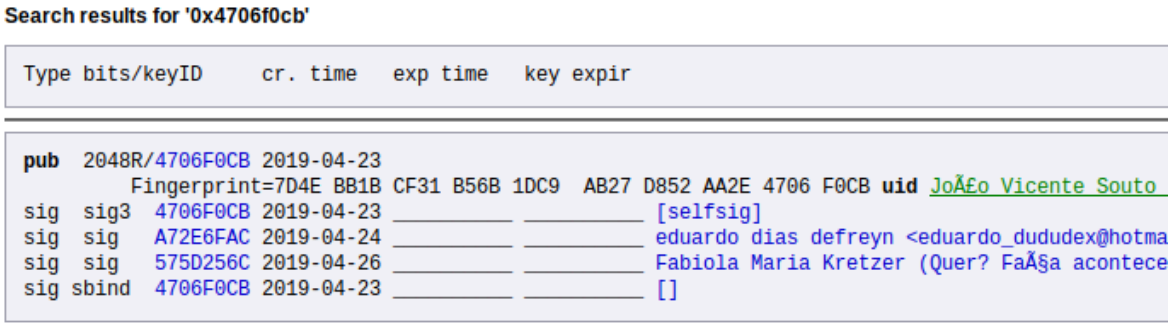

Figura 6: Imagem mostrando o certificado 0x4706F0CB assinado no servidor RNP

Com o intuito de revogar a assinatura realizada foi utilizado os comandos a seguir, passando como parâmetro o *keyID* do certificado assinado anteriormente.

$ gpg –edit-key 4706F0CB

gpg> revsig

gpg> save

Este comando enviar a assinatura do certificado para o servidor de chaves RNP:

$ gpg –send-keys –keyserver keyserver.cais.rnp.br 4706F0CB

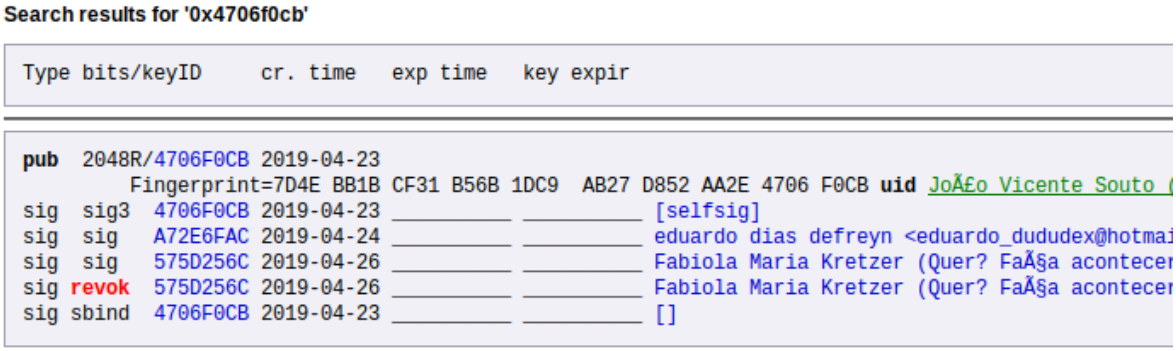

Figura 7: Imagem mostrando a assinatura do certificado 0x4706F0CB revogado o servidor RNP

Questão 4:

Um anel de chave consiste em uma chave pública e sua chave privada correspondente, ambas necessárias para ler (descriptografar) os dados [4]. Cada usuário mantém duas estruturas de dados de porta-chaves: um chaveiro privado para seus próprios pares de chaves pública/privada e um chaveiro público para as chaves públicas de correspondentes. As chaves públicas e privadas são armazenadas em arquivos de chaveiro presentes no diretório /.gnupg.

Os proprietários das chaves retêm e transmitem os chaveiros em seus certificados [5]. Como o nome indica, geralmente há mais de uma chave no chaveiro [5]. A primeira chave é chamada de chave mestra e seu uso principal é agir como a identidade do proprietário [5]. Outras chaves incluídas no anel de chaves são chamadas de sub-chaves [5]. Estas são as chaves que o anel de chaves PGP realmente usa para criptografar e assinar dados no mundo real [5]. A chave mestra assina as sub-chaves como uma prova de que elas realmente pertencem ao certificado e são tão confiáveis quanto a chave mestra [5].

O anel de chave privada é uma tabela de linhas contendo [3]:

- Registro de data e hora: quando o par de chaves foi gerado;
- ID da chave: 64 dígitos menos significativos da chave pública;
- Chave pública: a parte pública da chave;
- Chave privada: a parte privada, criptografada usando uma frase secreta.
- ID do usuário: geralmente o endereço de e-mail do usuário (ou keyID). Pode ser diferente para pares de chaves diferentes.

O porta chaves ajuda o usuário a gerenciar chaves GPG de uma maneira conveniente e segura. A segurança é garantida pois o acesso ao porta-chaves é garantido apenas a quem possui a senha das chaves mestras, ou seja, o dono das chaves públicas e privadas.

Questão 5:

Quando o usuário cria as chaves, ele poderá assiná-la localmente com sua própria chave privada para confiar nela [7]. Não é necessário fazer isso, mas significa que não precisa verificar todas as impressões digitais mais tarde toda vez que for verificar uma compilação [7]. Ao assinar localmente as chaves, a confiança na chave permanecerá puramente local em seu sistema e não se tornará parte da rede de confiança [7]. Se o usuário confia plenamente nessa chave e deseja declarar esse fato (por exemplo, se você está convencido da autenticidade, confiando plenamente que o que está lendo agora é legítimo e verificou que essa chave foi assinada por pessoas em quem você confia) então poderá pode assinar normalmente [7]. Ou seja, ao assinar uma chave e enviar a assinatura para o servidor o usuário confia que a chave assinada é é verdadeira [7].

Questão 6:

O usuário distribui sua chave (pública) dando-a pessoalmente aos seus correspondentes [6]. Entretanto, na prática as chaves são frequentemente distribuídas por e-mail ou algum outro meio de comunicação eletrônico, sendo inaceitável, se as pessoas que precisam de sua chave pública não souberem onde encontrá-lo [6]. Para resolver esse problema, os servidores de chave pública são usados para coletar e distribuir chaves públicas [6]. Uma chave pública recebida pelo servidor é adicionada ao banco de dados do servidor ou mesclada com a chave existente, se já estiver presente [6]. Quando uma solicitação de chave chega ao servidor, o servidor consulta seu banco de dados e retorna a chave pública solicitada, se encontrada [6].

Usando um servidor de chaves torna o processo um pouco mais fácil [6]. Quando Beto assina a chave de Alice, ele envia a chave assinada para o servidor de chaves [6]. O servidor

principal adiciona a assinatura de Beto à sua cópia da chave de Alice [6]. Indivíduos interessados em atualizar sua cópia da chave de Alice, consultam o servidor de chaves por iniciativa própria para recuperar a chave atualizada [6]. Alice nunca precisa se envolver com distribuição e pode recuperar assinaturas em sua chave simplesmente consultando um servidor de chaves [6].

Quando mais assinaturas um certificado tiver mais confiável ele será.

Questão 7:

As sub-chaves são chaves adicionais e são como as chaves públicas e privadas, exceto pelo fato de estarem ligadas ao par de chaves mestra (chave pública e privada) [2]. Uma sub-chave pode ser usada para assinatura ou criptografia [2]. A parte realmente útil das sub-chaves é que elas podem ser revogadas independentemente das chaves mestras e também armazenadas separadamente delas [2].

O GnuPG usa somente uma chave somente para assinatura e cria uma sub-chave de criptografia automaticamente [2]. Sem uma subchave para criptografia, você não pode ter e-mails criptografados com o GnuPG [2]. Isso ocorre pois as sub-chaves facilitam o gerenciamento de chaves [2]. O par de chaves mestre é a melhor prova de sua identidade *online* e se você a perder, você precisará começar a construir sua reputação do zero [2]. Se qualquer outra pessoa tiver acesso à sua chave mestra privada ou à sua sub-chave privada, ela fará com que todos acreditem que a outra pessoa é você. [2]

Você tem uma sub-chave de criptografia criada automaticamente e cria outra sub-chave para assinatura e as mantém no computador principal [2]. Você publica as sub-chaves nos servidores de chaves normais e todos os outros os usarão em vez das chaves mestras para criptografar mensagens ou verificar suas assinaturas de mensagens [2]. Da mesma forma, você usará as sub-chaves para descriptografar e assinar mensagens [2].

A criação ou revogação de sub-chaves não afeta a reputação da chave mestra [2]. Portanto, caso sua sub-chave seja roubada enquanto sua chave mestra permanecer segura, você poderá revogar a sub-chave comprometida e substituí-la por uma nova sub-chave sem precisar reconstruir sua reputação e sem reduzir a reputação das chaves de outras pessoas assinadas com sua chave mestra [2].

Desta forma, a chave mestra princiapl somente será usada quando assinar a chave de outra pessoa ou revogar uma assinatura existente, quando você altera a data de vencimento da sua chave entre outros casos [2].

Questão 8:

Com a finalidade de adicionar sua imagem à sua chave PGP usando o GnuPG no Linux use:

```
$ gpg –edit-key 0x575d256c
```

```
gpg> addphoto
```

Em seguida, deve ser colocado o caminho até a imagem ou foto que será colocada no certificado. E, então você salva as alterações.

```
gpg> save
```

Este comando enviar o cerificado com a foto para o servidor de chaves RNP:

```
$ gpg –send-keys –keyserver keyserver.cais.rnp.br 0x575d256c
```

Questão 9:

Um servidor de chaves (uso pessoal ou rede), necessita da excecução do protocolo *Synchronizing OpenPGP Key Server (SKS)* em seu servidor [1]. O SKS é um servidor-chave *OpenPGP* que lida corretamente com todos os recursos do *OpenPGP*, incluindo pacotes photoID e várias sub-chaves [1]. A implementação desse servidor de chaves usa um algoritmo de reconciliação eficiente e confiável para manter o banco de dados em sincronia com outros servidores SKS [1]. Possui necessidade de um espaço de armazenamento de 11GB para o *download* de um banco de dados completo com um total de 23GB após a importação do banco de dados [1].

Questão 10:

Criar e verificar assinaturas usa o par de chaves pública/privada em uma operação diferente da criptografia e da descriptografia [8]. Uma assinatura é criada usando a chave privada do usuário que deseja enviar o documento [8]. A assinatura é verificada usando a chave pública correspondente [8]. Por exemplo, Alice usaria sua própria chave privada para assinar digitalmente sua última submissão ao jornal [8]. O editor Beto associado que lida com o envio dela usaria a chave pública de Alice para verificar a assinatura e verificar se a apresentação realmente veio de Alice e que ela não havia sido modificada desde que Alice a enviou [8]. Uma consequência do uso de assinaturas digitais é que é difícil negar que você fez uma assinatura digital, pois isso implicaria que sua chave privada foi comprometida [8].

A opção de linha de comando –sign é usada para fazer uma assinatura digital [8]. O documento a assinar é inserido (document.pdf, mas também pode possuir outras extensões) e o documento assinado é retornado (document.sig) [8].

```
Alice: $ gpg –output document.sig –sign document.pdf
```

O documento é compactado antes de assinado e a saída está em formato binário [8]. Para verificar a assinatura, use a opção –verify e para verificar a assinatura e extrair o documento, use a opção –decrypt [8].

```
Beto: $ gpg –output document.pdf –decrypt document.sig
```

Questão 11:

Uma chave pública e privada tem uma função específica ao criptografar e descriptografar documentos [9]. Com a chave pública um usuário qualquer criptografa um documento, esse documento é colocado no "cofre seguro"[9]. A chave privada correspondente é a combinação que pode reabrir o cofre e recuperar o documento [9]. Em outras palavras, somente a pessoa que detém a chave privada pode recuperar um documento criptografado usando a chave pública associada [9]. Se quiser criptografar uma mensagem para Alice, criptografe-a usando a chave pública de Alice e ela a descriptografa com sua chave privada [9]. Se Alice quiser enviar uma mensagem, ela a criptografa usando sua chave pública e você a descriptografa com sua chave privada [9].

Para criptografar um documento, a opção –encrypt é usada [9]. Deve-se ter as chaves públicas dos destinatários pretendidos [9]. O resultado criptografado é colocado na saída padrão ou conforme especificado usando a opção –output [9]. A opção –recipient é usada

uma vez para cada destinatário e recebe um argumento extra, especificando a chave pública para a qual o documento deve ser criptografado [9]. O documento criptografado só pode ser descriptografado por alguém com uma chave privada que complementa uma das chaves públicas dos destinatários [9].

Alice: $ gpg –output document.gpg –encrypt –recipient 0x575d256c document.pdf

Para descriptografar uma mensagem, a opção –decrypt é usada [9]. É necessário aa chave privada para a qual a mensagem foi criptografada [9]. Semelhante ao processo de criptografia, o documento a ser descriptografado é inserido e o resultado descriptografado é gerado [9].

Beto: $ gpg –output document2.pdf –decrypt document.gpg

Referências

[1] Roll. PGP Key Server. Disponível em: <https://roll.urown.net/server/pgp-keyserver.html>. Acessado em 26 de Abril de 2019.

[2] Debian. Subkeys. Disponível em: <https://wiki.debian.org/Subkeys>. Acessado em 26 de Abril de 2019.

[3] Dr. Bill Young. Foundations of Computer Security - Department of Computer Science of University of Texas at Austin. Disponível em: <http://www.cs.utexas.edu/ byoung/ cs361/lecture70.pdf>. Acessado em 26 de Abril de 2019.

[4] Key ring. Business dictionary. Disponível em: <http://www.businessdictionary.com/ definition/key-ring.html>. Acessado em 26 de Abril de 2019.

[5] Understanding Key Rings. Imaeses. Disponível em: <http://www.imaeses.nl/ KeyRing/What_is_PGP.html>. Acessado em 26 de Abril de 2019.

[6] Distributing keys. GnuPG. Disponível em: <https://www.gnupg.org/gph/en/ manual/x457.html>. Acessado em 26 de Abril de 2019.

[7] PGP Signatures. Review Board. Disponível em: <https://www.reviewboard.org/ downloads/pgp-signatures/>. Acessado em 26 de Abril de 2019.

[8] Making and verifying signatures. GnuPG. Disponível em: <https://www.gnupg.org/ gph/en/manual/x135.html>. Acessado em 26 de Abril de 2019.

[9] Encrypting and decrypting documents. GnuPG. Disponível em: <https://www.gnupg.org/gph/en/manual/x110.html>. Acessado em 26 de Abril de 2019.