Trabalho Individual sobre o GPG

INE 5429
Prof. Ricardo Custódio

Importante: Coloque todos os relatórios parciais em um **único arquivo PDF** e entregue este arquivo.

Pré-requisito: Utilizando OpenPGP, gere o seu certificado:

- Criar certificado pgp. Obs.: SALVAR A CHAVE PRIVADA E NÃO ESQUECER SENHA
- Publicar a chave pública em um repositório PGP. Exemplos:
    - Keyserver da RNP (use o Google para encontrar o site)
    - MIT PGP Public Key Server
    - Keyserver PGP.com

Referências: gpg --help e https://help.ubuntu.com/community/GnuPrivacyGuardHowto

1) Certificado de Revogação

Explique do que se trata
Crie um novo certificado PGP para este trabalho individual (Não use o teu certificado para alguns dos testes abaixo, como por exemplo, para verificar como revogar um certificado). Coloque esse certificado de testes no servidor PGP. Depois verifique seu status. Então, crie um certificado de revogação e revogue o certificado de testes.

É importante lembrar que a base de dados local (anéis de chaves privadas e públicas) precisam ser atualizadas com o conteúdo dos servidores PGP. Utilizer a pção "reflesh" periodicamente para fazer isso.

Resultado Esperado:

Faça um relatório do que você fez.

2) Revogação de assinaturas

Assine um certificado qualquer PGP (de outra pessoa). E envie esse certificado para o servidor PGP. Depois verifique o status do certificado. E então, revogue a assinatura que você fez. Confira o resultado no servidor PGP.

Resultado Esperado:

Faça um relatório do que você fez.

3) Comandos do GPG

Explique e mostre exemplos (crie seus próprios exemplos - experimente os comandos) de cada um dos seguintes comandos do GPG. Escolha pelo menos 10 comandos.

Comandos:

-s	--sign	make a signature
	--clearsign	make a clear text signature
-b	--detach-sign	fazer uma assinatura separada
-e	--encrypt	cifrar dados
-c	--symmetric	cifrar apenas com criptografia simétrica
-d	--decrypt	decifrar dados
	--verify	verificar uma assinatura
-k	--list-keys	listar as chaves
	--list-sigs	listar as chaves e as assinaturas
	--check-sigs	list and check key signatures
	--fingerprint	listar as chaves e as impressões digitais
-K	--list-secret-keys	listar as chaves secretas
	--gen-key	gerar um certificado PGP
	--gen-revoke	gerar um certificado de revogação
	--delete-keys	remover chaves do porta-chaves público
	--delete-secret-keys	remover chaves do porta-chaves secreto
	--sign-key	assinar uma chave
	--lsign-key	assinar uma chave localmente
	--edit-key	assinar ou editar uma chave
	--passwd	Trocar uma sennha
	--export	exportar chaves
	--send-keys	exportar chaves para um servidor
	--recv-keys	importar chaves de um servidor
	--search-keys	procurar chaves num servidor de chaves
	--refresh-keys	atualizar todas as chaves a partir de um servidor de chaves

	--import	importar/fundir chaves
	--card-status	print the card status
	--card-edit	change data on a card
	--change-pin	change a card's PIN
	--update-trustdb	atualizar o banco de dados de confiabilidade
	--print-md	Imprime o resumo da mensagem
	--server	Executar em modo servidor

Resultado Esperado:
Faça um relatório do que você fez.

4) Opções aos comandos do GPG

Explique e mostre exemplos de pelo menos 10 das seguintes opções GPG. Crie seus próprios exemplos. Experimente cada opção.

-a	--armor	criar saída com armadura ascii
-r	--recipient USER-ID	encrypt for USER-ID
-u	--local-user USER-ID	use USER-ID to assinar ou decifrar
-z N		set compressão para o nível N (0 desabilita)
	--textmode	usar modo de texto canônico
-o	--output FILE	write output to FILE
-v	--verbose	detalhado
-n	--dry-run	não fazer alterações
-i	--interactive	perguntar antes de sobrepôr
	--openpgp	use strict OpenPGP behavior

Faça um pequeno relatório do que você fez.

5) Usando Certicados PGP no Webmail do INE (ou outro)

Instale o seu certificado GPG no servidor Webmail do INE (Ou outro cliente de email com suporte ao GPG). Use-o para enviar e receber mensagens (e-mails) assinados para e de seus colegas. Experimente também enviar e receber e-mails sigilosos.

Resultado Esperado:

Enviar um e-mail assinado digitalmente para a lista da disciplina.

6) Comando --edit-key

O comando --edit-key é um comando especial com uma série de funcionalidades. Explique e mostre seus próprios exemplos de pelo menos 10 dessas funcionalidades - listadas abaixo

quit	sair deste menu
save	gravar e sair
help	mostra esta ajuda
fpr	show key fingerprint
list	lista chave e identificadores de usuários
uid	seleciona ID de usuário N
key	select subkey N
check	check signatures
sign	sign selected user IDs [* see below for related commands]
lsign	sign selected user IDs locally
tsign	sign selected user IDs with a trust signature
nrsign	sign selected user IDs with a non-revocable signature
adduid	adiciona um novo ID de usuário
addphoto	adiciona um identificador fotográfico
deluid	delete selected user IDs
addkey	add a subkey
addcardkey	add a key to a smartcard
keytocard	move a key to a smartcard
bkuptocard	move a backup key to a smartcard

delkey	delete selected subkeys
addrevoker	adiciona uma chave de revocação
delsig	delete signatures from the selected user IDs
expire	change the expiration date for the key or selected subkeys
primary	flag the selected user ID as primary
toggle	toggle between the secret and public key listings
pref	lista preferências (perito)
showpref	lista preferências (detalhadamente)
setpref	set preference list for the selected user IDs
keyserver	set the preferred keyserver URL for the selected user IDs
notation	set a notation for the selected user IDs
passwd	muda a frase secreta
trust	muda os valores de confiança
revsig	revoke signatures on the selected user IDs
revuid	revoke selected user IDs
revkey	revoke key or selected subkeys
enable	enable key
disable	disable key
showphoto	show selected photo IDs
clean	compact unusable user IDs and remove unusable signatures from key
minimize	compact unusable user IDs and remove all signatures from key

* The `sign' command may be prefixed with an `l' for local signatures (lsign), a `t' for trust signatures (tsign), an `nr' for non-revocable signatures (nrsign), or any combination thereof (ltsign, tnrsign, etc.).

Resultado Esperado:

Faça um relatório do que você fez.

7) Responda as seguintes perguntas

7,1 O que é o anel de chaves privadas? Como este está estruturado? Na sua aplicação GPG onde este anel de chaves é armazenado? Quem pode ser acesso a esse porta chaves?

7,2 Qual a diferença entre assinar uma chave local e assinar no servidor?

7,3 O que é e como é organizado o banco de dados de confiabilidade?

7,4 O que são e para que servem as sub-chaves?

7,5 Coloque sua foto (ou uma figura qualquer) que represente você em seu certificado GPG.

7,6 O que é preciso para criar e manter um servidor de chaves GPG, sincronizado com os demais servidores existentes?

7,7 De um exemplo de como tornar sigiloso um arquivo usando o GPG. Envie esse arquivo para um colega e que enviar para você outro arquivo cifrado. Você deve decifrar e recuperar o conteúdo original.

7,8 De um exemplo de como assinar um arquivo (assinatura anexada e outro com assinatura separada), usando o GPG. Envie uma mensagem assinada para um colega. Esse colega deve enviar para você outra mensagem assinada. Verifique se a assinatura está correta.

Resultado Esperado:

Respostas das perguntas do relatório PDF e certificado com foto publicado no servidor PGP.