



RNEP-GW

MÓDULO PGP, RFC & TLP



PGP – PRETTY GOOD PRIVACY

Chaves Públicas / Chaves Privadas

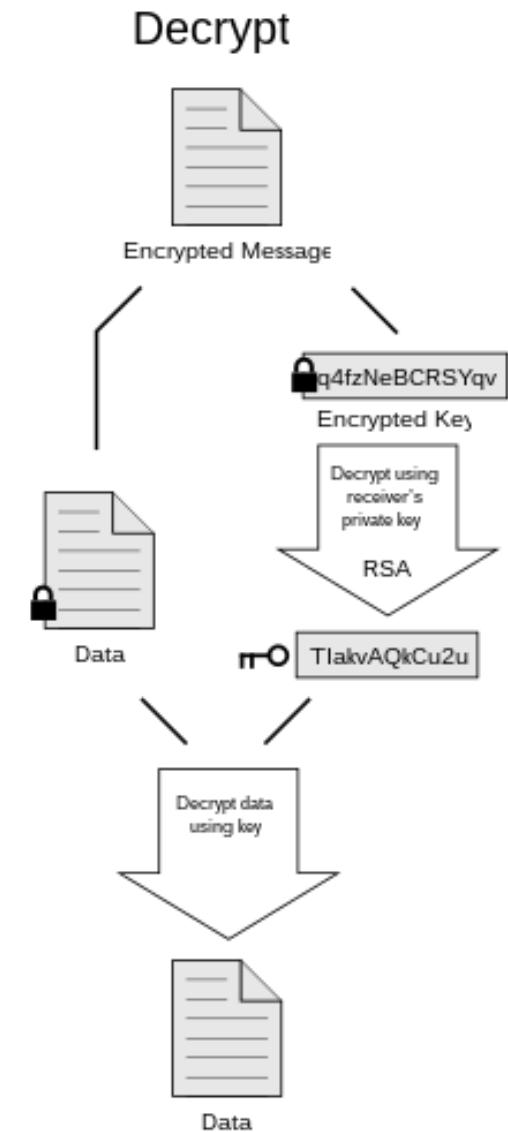
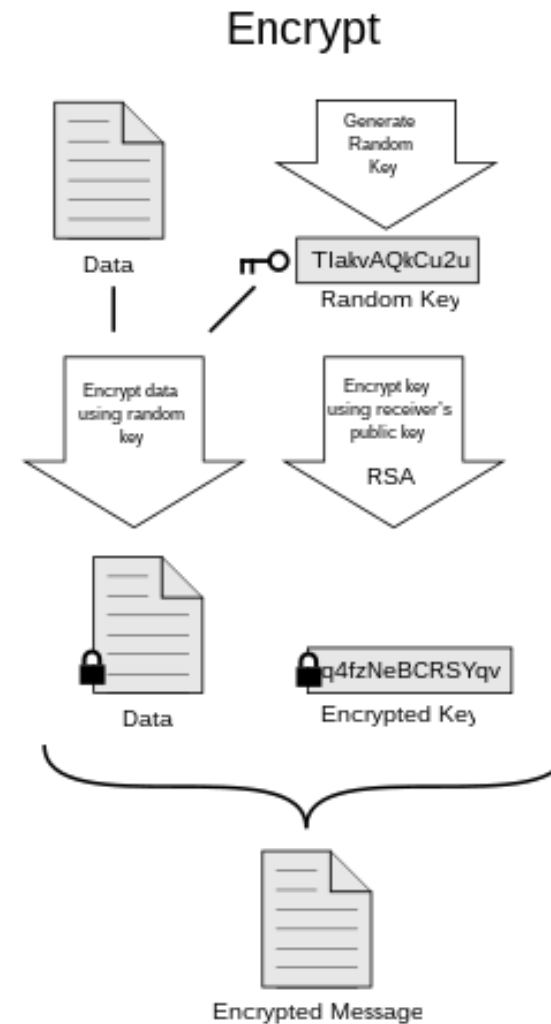
Depósitos de Chaves Públicas

Funciona para receber informação cifrada ou assinar

ASSINAR / DECIFRAR

Assinamos com a nossa chave privada

Deciframos as mensagens de terceiros com a chave pública desses terceiros



PGP – REPOSITÓRIOS

openpgp.circl.lu

keys.openpgp.org

keyserver.ubuntu.com

keyserver.pgp.com

pgp.mit.edu



PGP – REPOSITÓRIOS

OpenPGP keyserver - openpgp.circl.lu

Search for an OpenPGP Public Key, ie 0x..

 Search Key

 Submit Key

[Advanced Options](#)

[about](#) | [statistics](#)



circl.lu
Computer Incident
Response Center
LUXEMBOURG

Provided as a public service by [CIRCL.LU](#).

PGP – CHAVE PÚBLICA

Search results for 'report@csirt.fct.pt'

Type	bits/keyID	cr. time	exp time	key expir
pub	rsa4096/31dfd2e5be47ab8dbd88a46d2a0dc930fbfb7c66	2025-06-04T10:14:41Z		
	Hash=9803fb693be26a46821ba383a6cca3e1			
uid	CSIRT FCT <report@csirt.fct.pt>			
sig	sig 2a0dc930fbfb7c66	2025-06-04T10:14:41Z	2027-06-04T10:14:41Z	_____ [selfsig]
sub	rsa4096/666d47f3fc7460b4bfe3b7c3f56dd9146cda90af	2025-06-04T10:14:41Z		
sig	sbind 2a0dc930fbfb7c66	2025-06-04T10:14:41Z	_____	2027-06-04T10:14:41Z []

PGP – CHAVE PÚBLICA

-----BEGIN PGP PUBLIC KEY BLOCK-----

Comment: Hostname: openpgp.circl.lu

Version: Hockeypuck ~unreleased

xsFNBGAHJEAEAC3w8AP5zNt68pob/3Mvp1l8fUHeK25GfC6rLbpPrOb2ve2UTZP
nBtsbjY6E174xXtd2LQSQWGXrtHYn79pNYtHLYUOWWSB9MYWovwNsffk09YCUk
aQMY2Dc0vRZNqzW1jDNenPNDpEpbwO+gUGvIvR3iTUSNyJOsoh4d0sthfuBd7yeN
teAu8YD+KsV0Vqlw3Mvb3Sy104K2k4zSnS59J/wiHtnvQhh+XeLfMYkXjxjz8Y9p
vmIj07kpmQnGqJofbUT16ULctUEYzEQ1cvW40AoezC1kgqSw9sdp1YNoDngHX68r
Hka1K8mEeTtrXjhorUZFQErSDDCk9TPDcGuLiCramlFHQavNvXUTLkocRwbwIMkD
2mnbfUD1b08ryMcc2jxbbuT98KntqoP00AcW6a/FA7FuSccBdMy7jpYiOYhV2jeT
fuzRR/UATF0LBgdZHWZMGqOsdAGl/wU4/Ewhkpp8MEMtdQ0MJkipAaw5L3GyyvC5
Nkr57IbzcAETtyl0PZhc1qjJkfjAwP+01GqmVufuNH1QQakODQgaw/uiT10BmWON
1MYC2quhJiSdDwxk1D3eYm4yzm4tvfUzNrx81smXDt8QXra0t7bH3IdxDtcdKaM
QtN3RVUP4wXjyTR8pH2rjKJYQ8vJVFCH5hGgvj9xSEBUYC8d40tkpvSHwwARAQAB
zR9DU01SVCBGQ1QgPHJlcG9ydEBjc2lydC5mY3QucHQ+wsGXBBMBcGBBFiEEMd/S
5b5Hq429iKrtKg3JMPv7fGYFAmhAHJECGwMFCQPCZwAFcwIBwICiGIGFQoJCA5C
BBYCAwECHgcCF4AACgkQK3JMPv7fGYOExAArhBFBPjF3eh8jGttki/zYDbpkeK/
eNZebOqoYjAtn++vEY09CSHziS69raRBbuaccDJQ1J3x0zp2s9KPz2gzDRyv9JUO
fuf60GGxdL2qD8R/5hUKXhomKj6pP+wx2p7BsZU6YZbTYISZ3T2Mkha8ZQyumIiC
yHX0mhVK/PQy8im8jRN+29A1I1BMytvNyxTm/t3jrCy1VruRCV2XYn2Lm8daWe
fXbM91CoChr/gd7jaLawqBcW4bHV9DoNZto+m/bU6MvQyE7dGDGCCJ+7/onEJLJv
raL9o+Dvq0tR5YVXkfA3RHhyFdurfvvzjcUekAaoOKG7yZTRSj0xuZJxU6iLhVVB
rz0pwZ8B2NYVDqPa41nz7MFCVz74LQDwvUQwgETtQdTh+6TTNjgH0vOe06d70iG8
DWAq9C+1OI7C7P1JHxwAcTIY9mafhhqfdmLT1b1vGzljg657WE8DZ0AjlqxxU9upT
mTKEgZeqWU0FKeQcv81ZLwfhlzEq9iOdzbRBift57R4M4cXj9grnh8Ds19L/NRGz
Oz60BX8c+iJWqjRuKGs5IS26tSoSNjIS9ZTvsjDAfrI4sMaxZy4Le9AHBrvuaAcJ
bGGk8+hpU44EKjFkHstnB5CnxH9GfarwPGbGSiWGH/0m4Nz3Ca9C4Q12FCbGdK1+
Ejgb8yf5FZ1QtMnOwU0EaEackQEANvpZtRjg4msIyuxMXro2M3km4LieKYRe8f2
6C872ZV019dkQ0R0/bU57TXEut+yI7jjp60MrQSLwRMfCFFi5th3gym2hJiayo+I
pTw3RMdpkgOc1X+p1+1P71r4YVJ9P7Fw+x8jqWoZ+Ot/DwSsYSDG21FnhIAY4wCz
70R0rfA9s7B89LIGECM4xbAm8/ojHL+BVneVHVJtzQ21kxkFr0mZ1z38qKfoAWtM
a8+v/1trOLzRwp0dmMpTV4ENxTRU8Mctkzh2Gj+BMhPUXBHSmPch6K4M11uMY8Gb
2FdpXb7c8zWzXg0nC8ix91/+h8w4V12BjoOko+3gT93+wchXhEVWuPVDZg0+O5y1
w2GjE0/7vFgl7Cbrz9bJc3f58S400wrJXMgbwd8Xxji35/nuFk3pf/LHladEWfQR
5IQwxpRvgtNbHGAXLecorU1zrJ3QwxwQ3PM3gr4Zi1Izh+8R8PMVKD9yap/cM9za
cKNc8p1r0TLVRcVO/I6yydz5DsX6Efg3OX21/KLySRgHivvHLVRB4yNXjar1YpL4
nLeeXp5ZWVHHzTstd97Y1ZL25dbrGNXTwXdxJnm1DBYg0uTH/roucPVCq+eeJNJf
jRNEUveOx+hLTmn0R+hvxS0z61w1CP520S0bykG/gek3tPeu5AbZb5C9rXYO4j5M
wZrEbozZABEBAACwXwEGAECACYWlQX39Llvkerjb2IpG0qDckw+/t8ZgUCAEac
kQIbDAUJA8JnAAAKCRAQDckw+/t8ZpmaD/4zkYD5x91w7/FKyzDHDm/xqPInIQQw
SZoe6XJywpIK2p3zqQeSDqRAMuwadzePY9Xz3WqdxfqV0i+gz2jqSK2YzmvZbIE
nvvhV9sCdCUH0ZSP+BhjULMzfESK5uJKnKtfduwYTKjHEmvODX1++edp1wKGzGQ/
HgekEJFHBQMo0kZZjoPppHJixkua5Bi63FzaXQusOzqbF/nFx9bshoiqgG3Hicj50
wPFF1PobQB22AyyPQ/ECUzHLsk2oivLTYvtF6xVZHyK7PgAT864dp4E6LfiLKXQI
dyhRqrod2H/wefl8Ekskf5PTeyv7m09s/zYrmJYrBLgdhQyPV2JgA0cMdmMYOSfo
WGjCIzzeR2MbKrR2y7L9xn1Cf3PhhRh1adHGz/W9bwIYjFAdz500fuIoOc+o/uoU
roPmSCGVYxY1pBeEKoCF5RH1e6P7o1Z+MoUNr54QgX1b2sJI8IfbC0fbs9/wHUL
Tsfd1BzJiIKKurYgHNeu/Ya0KrP7DAUqAj1caoMfveZk7KNpB8q3chpVssQ612E8
hkxNMk7pkzRYFQZ1BqcWw9DwBjZHsubwiwEeZgtc3JhHVSDw9HrgOXQFFXCZNF92
C4fs/pEF7bt4Wmo0OK0mLUkNjCCnyrzMKZaRkx8nJBKIDXE5gjdUip1XveTd5Kxs
7aKnjX+p1EoZrA==

=6jZo

-----END PGP PUBLIC KEY BLOCK-----

PGP – COMO CRIAR?

Num sistema Linux, com o software instalado:

```
gpg --full-gen-key
```

Selecione o tipo de chave desejado:

(1) RSA e RSA

(2) DSA e Elgamal

(3) DSA (apenas de assinar)

(4) RSA (apenas de assinar)

(9) ECC (de assinar e cifrar) *pré-definição*

(10) ECC (apenas de assinar)

(14) Chave do cartão existente

PGP – COMO CRIAR?

Qual tamanho de chave você quer? (3072) 4096

Especifique quando a chave expira.

0 = chave não expira

<n> = chave expira em n dias

<n>w = chave expira em n semanas

<n>m = chave expira em n meses

<n>y = chave expira em n anos

Introduzir Nome verdadeiro e Endereço de email

PGP – PUBLICAR!

OpenPGP keyserver - openpgp.circl.lu

Search for an OpenPGP Public Key, ie 0x...

Search Key

Submit Key

Advanced Options

[about](#) | [statistics](#)



circl.lu
Computer Incident
Response Center
LUXEMBOURG

Provided as a public service by [CIRCL.LU](https://www.circl.lu).

Submit Your OpenPGP Public Key

Enter your ASCII-armored OpenPGP public key here

Close

Submit Public Key

IDEIAS CHAVE



É uma forma de assinar conteúdo próprio e também de decifrar conteúdo de terceiros



Conservar as chaves privadas em local seguro, publicar as chaves públicas



As chaves têm que ser renovadas

RFC2350

DEFINIR FORMALMENTE A EQUIPA

<https://www.csirt.fct.pt/pt/sobre/rfc2350/>

RFC2350

Secções:

- 1) Informações sobre o documento
- 2) Informações de contacto
- 3) Guião
- 4) Políticas
- 5) Serviços

RFC2350 – INFORMAÇÕES SOBRE O DOCUMENTO

- 1) Data da última atualização
- 2) Listas de distribuição para notificações
- 3) Acesso ao documento
- 4) Autenticidade
 - normalmente o documento é assinado com PGP

RFC2350 – INFORMAÇÕES DE CONTACTO

- 1) Nome da equipa
- 2) Endereço Postal
- 3) Zona horária
- 4) Telefone
- 5) Fax
- 6) Endereço de Correio Eletrónico
- 7) Outras telecomunicações
- 8) Chaves públicas e informação de cifra
- 9) Membros da equipa
- 10) Outra informação
- 11) Meios de contacto para utilizadores

RFC2350 – GUIÃO

- 1) Missão
- 2) Comunidade servida
- 3) Filiação
- 4) Autoridade

RFC2350 – POLÍTICAS

- 1) Tipos de incidente e nível de suporte
- 2) Política de privacidade
- 3) Comunicação e autenticação

RFC2350 – SERVIÇOS

- 1) Tratamento de incidentes de segurança
- 2) Disseminação de alertas [opcional]
- 3) Auditorias de segurança [opcional]
- 4) Awareness de segurança [opcional]
- 5) ...

IDEIAS CHAVE



Permite a uma equipa ser reconhecida e contactável por outras equipas

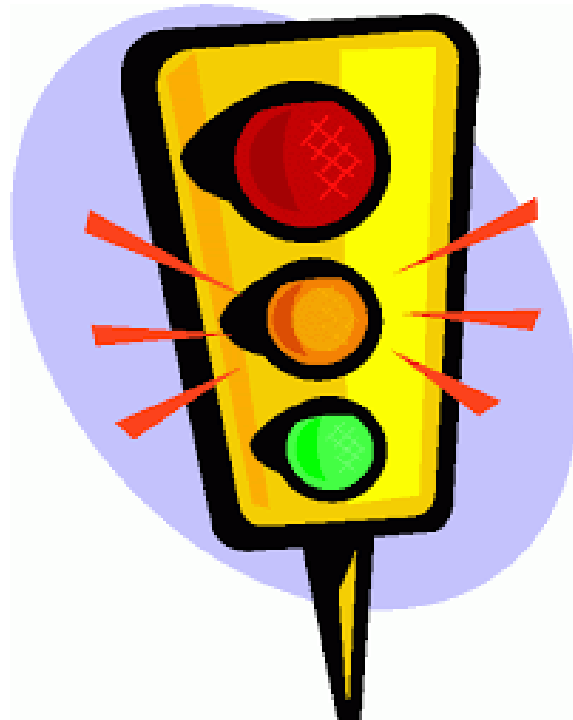


É crítico estabelecer as expectativas sobre o que a equipa faz para a comunidade servida



É importante actualizar o documento e ter bem definidos os recursos pelos quais a equipa responde

TRAFFIC LIGHT PROTOCOL (TLP)



DEFINIÇÕES DO TLP

Comunidade: Grupo que partilha de práticas e objetivos em comum e mantém relações de confiança informais. Ex.: a comunidade de profissionais de cibersegurança de um país.

Organização: Grupo que partilha de uma afiliação comum através de uma filiação formal e que está conectado pelas políticas estabelecidas pela organização da qual fazem parte.

Clientes: Pessoas ou entidades que recebem serviços de cibersegurança de uma organização.

DEFINIÇÕES DO TLP

TLP:RED	Para conhecimento estrito dos recipientes individuais, informação não deve ser partilhada.
TLP:AMBER TLP:AMBER+STRICT	Os recipientes da informação podem partilhar a informação apenas com membros da própria organização e clientes. Se a informação for restrita apenas a membros da própria organização, o TLP:AMBER+STRICT deve ser usado.
TLP:GREEN	Partilha limitada, recipientes podem partilhar a informação dentro da sua comunidade. Informação pode ser partilhada com colegas e organizações parceiras dentro da sua comunidade, mas não por canais publicamente acessíveis.
TLP:CLEAR	Não existem restrições para a divulgação da informação.

IDEIAS CHAVE



O *Traffic Light Protocol* é o standard de-facto de classificação de informação usado na comunidade CSIRT



A classificação AMBER+STRICT é tipicamente uma classificação por omissão segura



Questões?

Obrigado.



csirt.fct.pt/podcast



csirt.fct.pt/mooc



csirt.fct.pt/etc