



GTS 32 | SP 12/2018

GCrypt:

Criptografia para humanos

Claudio Netto

claudio.netto@corp.globo.com

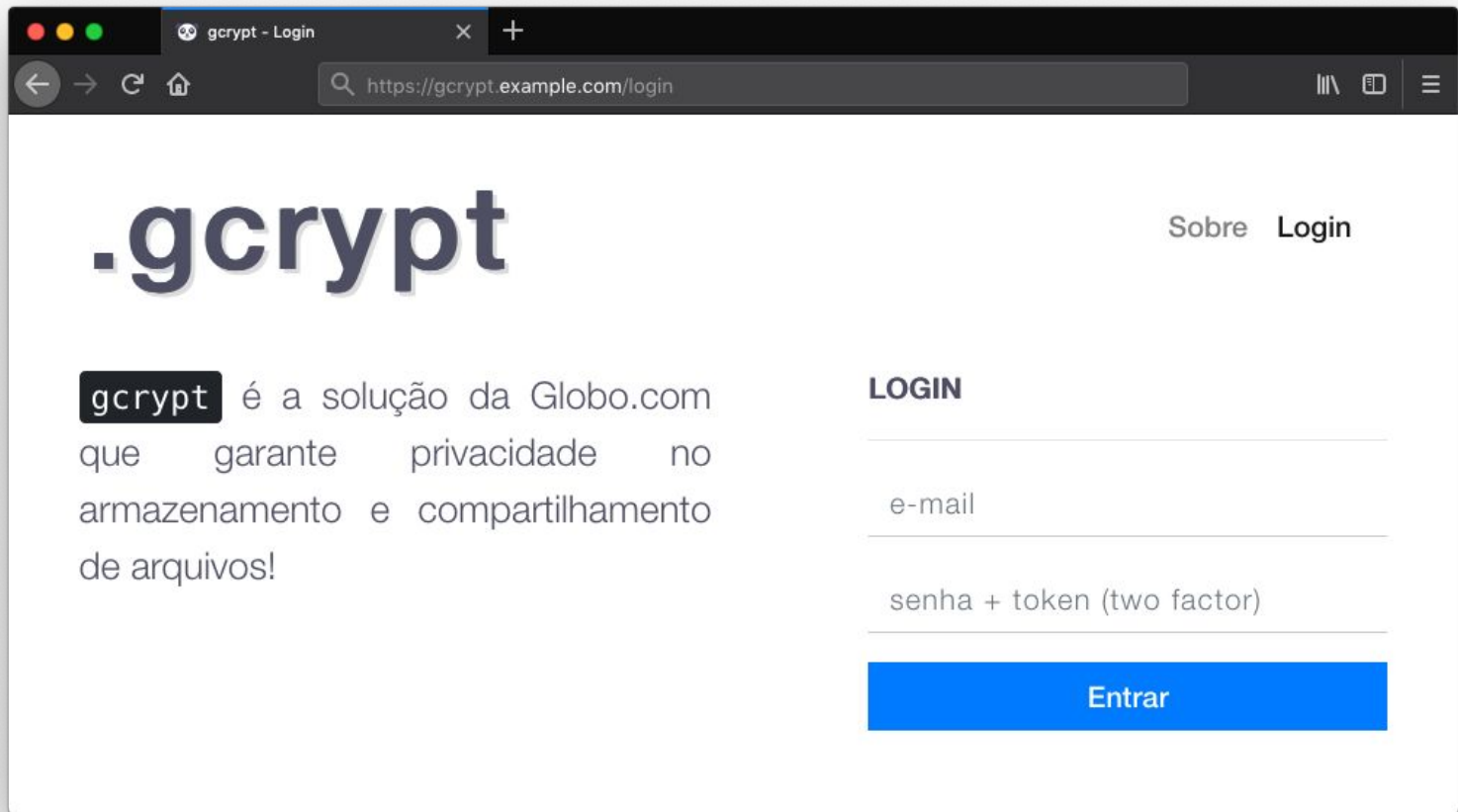
1. Motivação
2. O que NÃO é o GCrypt?
3. O que é o GCrypt?
4. Arquitetura
5. Fluxos de uso
6. Desafios no desenvolvimento
7. Métricas de uso
8. Próximos passos

.gcript

- **Prevenção** de vazamento de informações sensíveis corporativas e pessoais.
- **Pluralidade** tecnológica e cultural nas empresas.
- **Disseminação** de boas práticas de Segurança da Informação para colaboradores.

- Não é criptografia própria.
- Apesar da similaridade de nomes, não tem relação com GNU Crypt (libgcrypt).

O que é o GCrypt?



gcrypt - Login

https://gcrypt.example.com/login

.gcrypt

Sobre Login

gcrypt é a solução da Globo.com que garante privacidade no armazenamento e compartilhamento de arquivos!

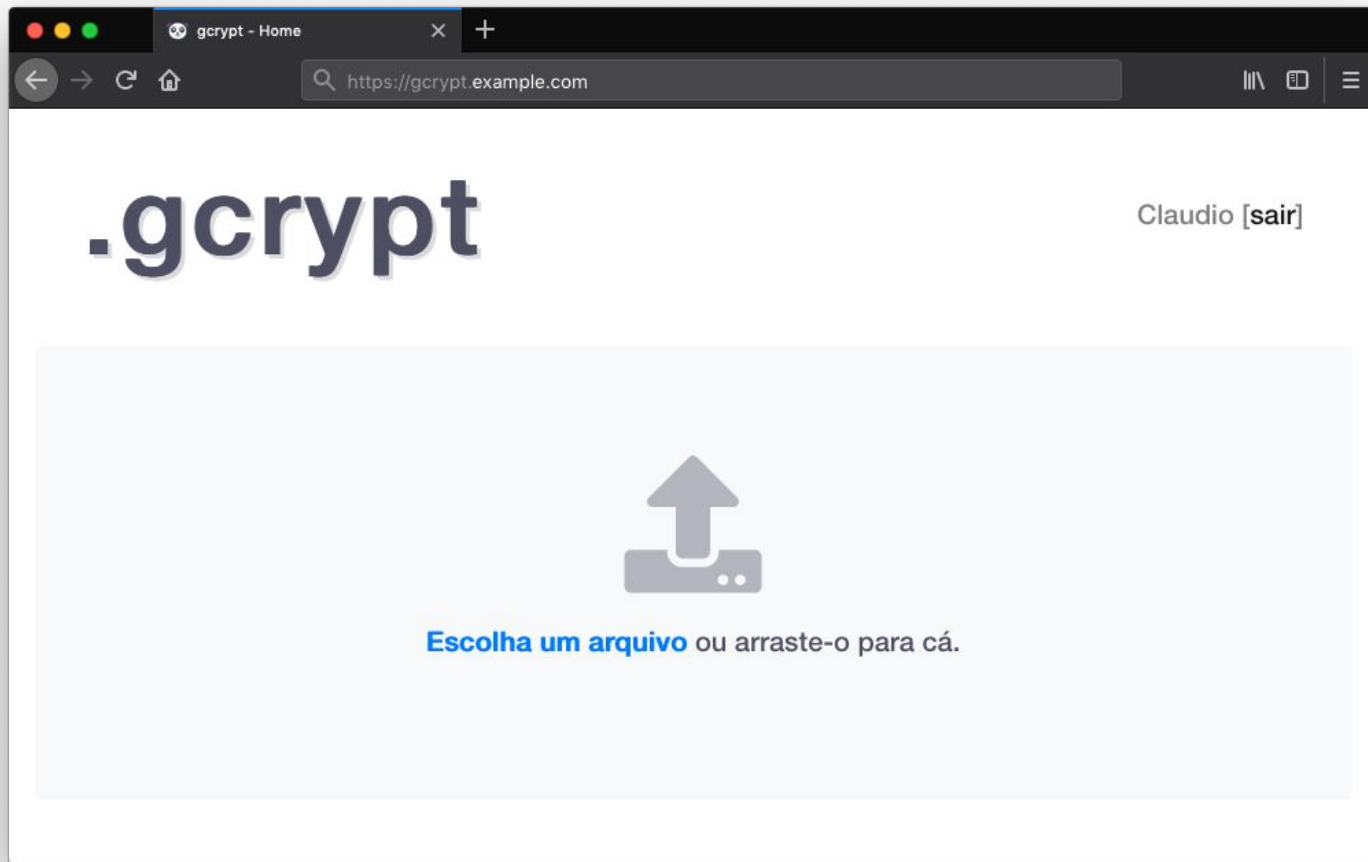
LOGIN

e-mail

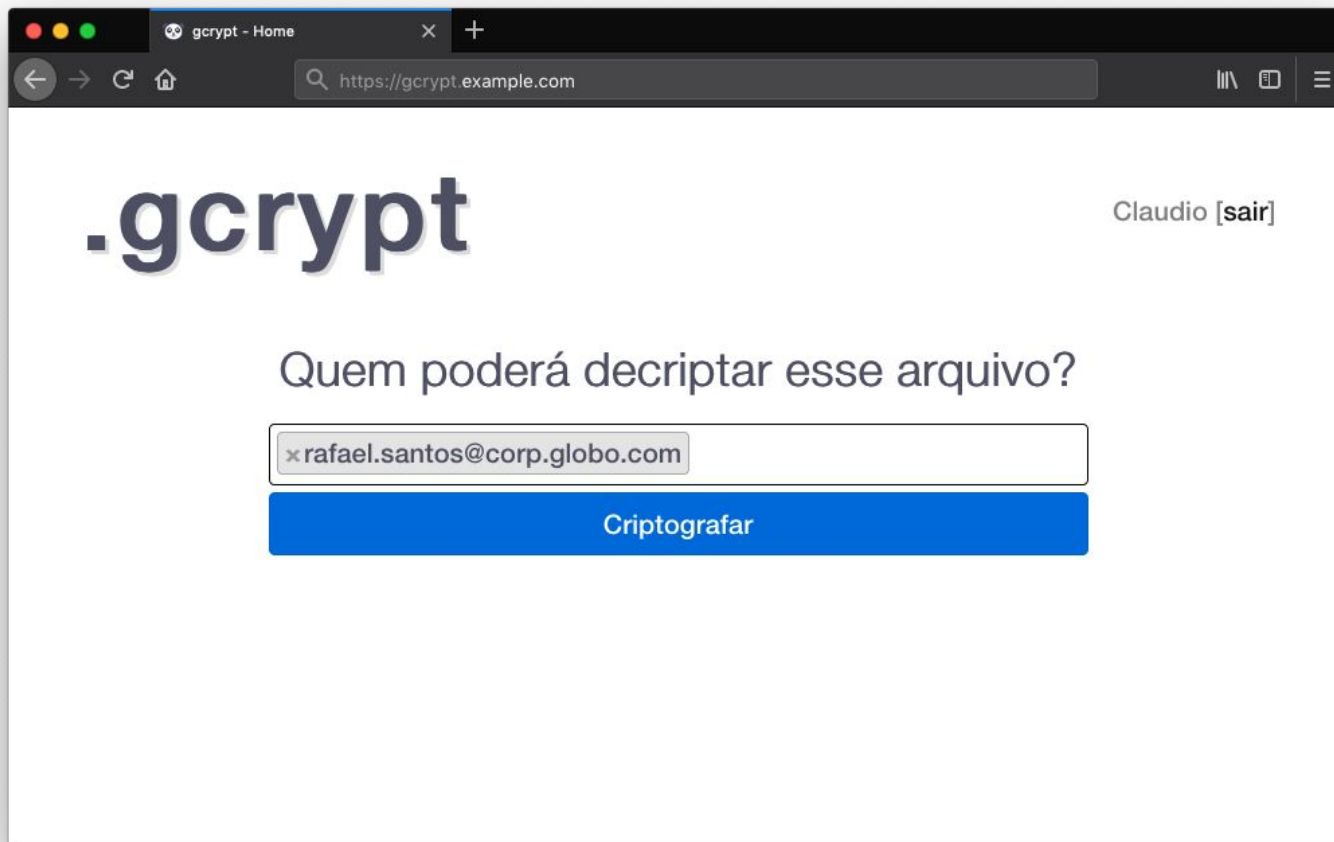
senha + token (two factor)

Entrar

O que é o GCrypt?



O que é o GCrypt?



The screenshot shows a web browser window with the following elements:

- Browser Tab:** "gcript - Home" with a close button and a plus sign for additional tabs.
- Address Bar:** "https://gcript.example.com" with navigation icons (back, forward, refresh, home) and a search icon.
- Page Content:**
 - Header:** ".gcript" in large, bold, dark blue font on the left, and "Claudio [sair]" in smaller black font on the right.
 - Main Text:** "Quem poderá decifrar esse arquivo?" (Who will be able to decrypt this file?) centered on the page.
 - Input Field:** A text box containing "xrafael.santos@corp.globo.com" with a small 'x' icon on the left to clear the text.
 - Action Button:** A large blue button labeled "Criptografar" (Encrypt) centered below the input field.

O que é o GCrypt?



Magic (para os usuários finais).

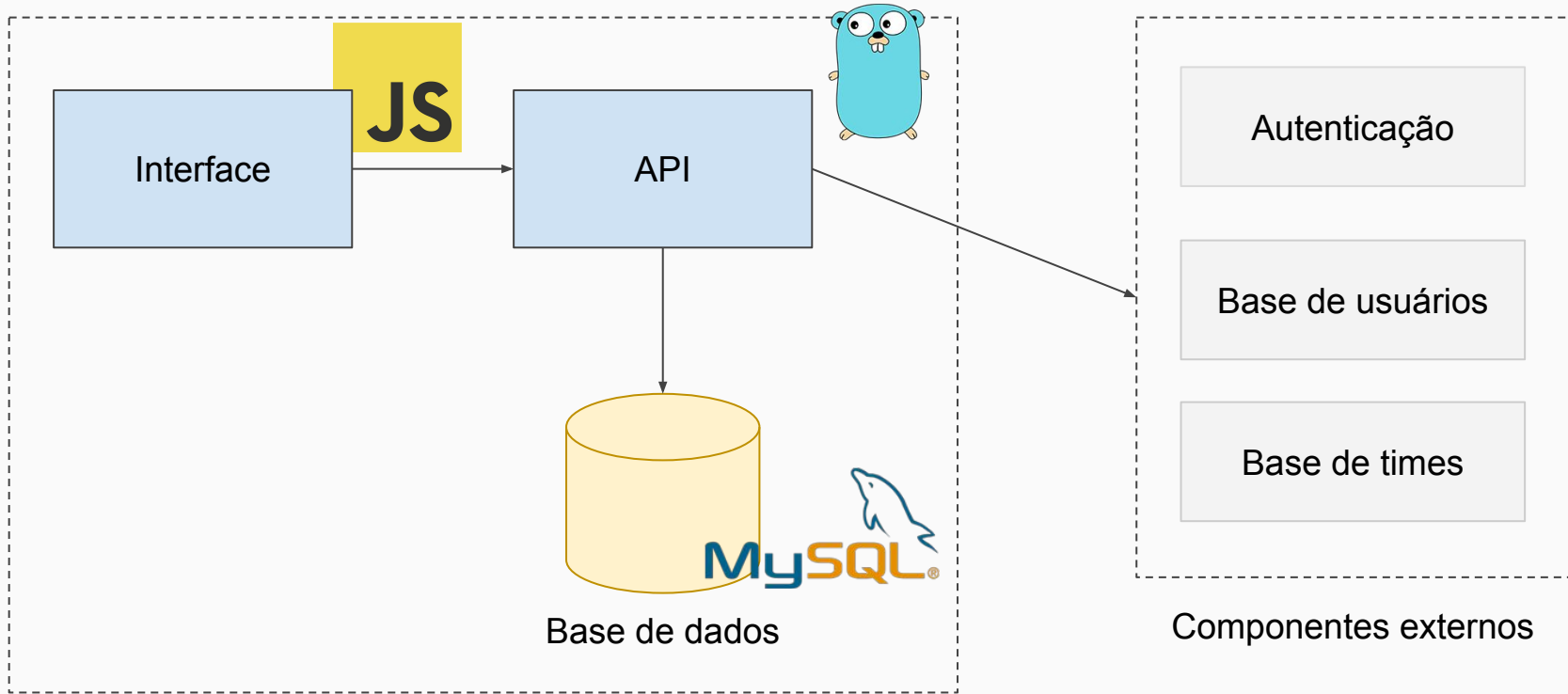
O que é o GCrypt?

```
$ file senhas.txt.gcrypt
senhas.txt.gcrypt: Zip archive data, at least v2.0 to extract
```

```
$ unzip senhas.txt.gcrypt
Archive:  senhas.txt.gcrypt
replace senhas.txt.gcrypt? [y]es, [n]o, [A]ll, [N]one, [r]ename: A
  inflating: senhas.txt.gcrypt
```

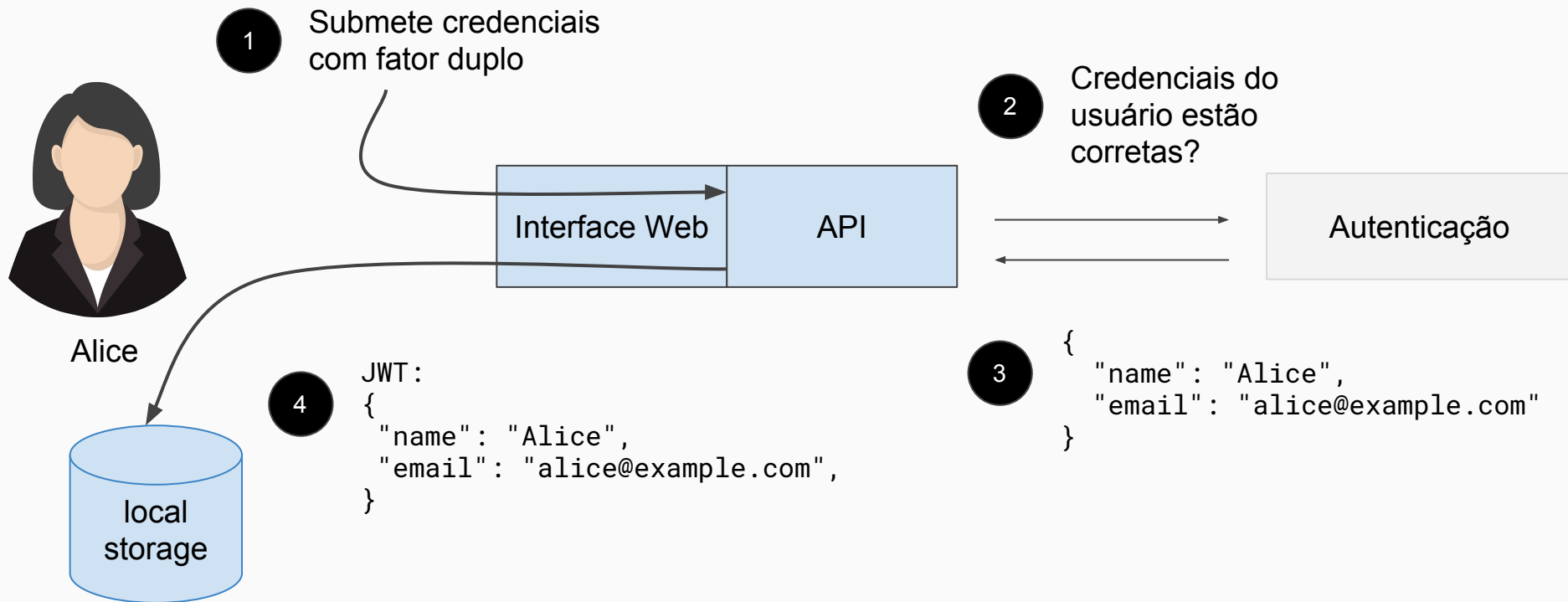
O que é o GCrypt?

```
$ hexdump -C senhas.txt.gcrypt
00000000 37 62 32 32 36 34 36 31 37 34 36 35 32 32 33 61 |7b2264617465223a|
00000010 32 32 33 32 33 30 33 31 33 38 32 64 33 31 33 32 |22323031382d3132|
00000020 32 64 33 31 33 32 32 30 33 32 33 32 33 61 33 31 |2d31322032323a31|
00000030 33 31 33 61 33 32 33 33 32 32 32 63 32 32 36 38 |313a3233222c2268|
00000040 36 31 37 33 36 38 35 66 36 39 36 34 32 32 33 61 |6173685f6964223a|
00000050 32 32 34 31 36 31 35 31 33 35 37 39 34 66 37 32 |2241615135794f72|
00000060 34 66 34 63 36 62 36 38 35 30 36 63 36 33 34 66 |4f4c6b68506c634f|
00000070 36 66 35 39 34 65 33 38 34 31 33 39 33 32 36 61 |6f594e384139326a|
00000080 33 32 36 32 36 38 36 64 35 34 35 32 36 62 37 61 |3262686d54526b7a|
00000090 33 32 36 65 35 34 34 38 36 39 34 65 34 34 33 31 |326e5448694e4431|
000000a0 35 30 37 38 35 39 36 66 33 64 32 32 32 63 32 32 |5078596f3d222c22|
000000b0 36 38 36 31 37 33 36 38 35 66 36 36 36 39 36 63 |686173685f66696c|
000000c0 36 35 32 32 33 61 32 32 32 32 32 63 32 32 37 36 |65223a22222c2276|
000000d0 36 35 37 32 37 33 36 39 36 66 36 65 32 32 33 61 |657273696f6e223a|
000000e0 32 32 33 32 32 65 33 30 32 32 37 64 32 34 33 30 |22322e30227d2430|
000000f0 37 37 36 33 35 32 33 31 35 35 36 39 36 38 36 66 |776352315569686f|
00000100 37 39 36 35 33 32 36 62 35 30 32 66 35 37 33 38 |7965326b502f5738|
00000110 34 63 36 34 34 31 34 62 35 33 33 35 32 62 33 32 |4c64414b53352b32|
00000120 34 34 35 38 35 33 35 31 36 32 36 39 34 32 36 33 |4458535162694263|
00000130 37 32 36 37 37 39 36 61 35 36 36 35 37 33 34 34 |7267796a56657344|
00000140 33 38 34 64 33 64 2a 34 35 63 39 32 39 38 37 37 |384d3d45c929877|
```

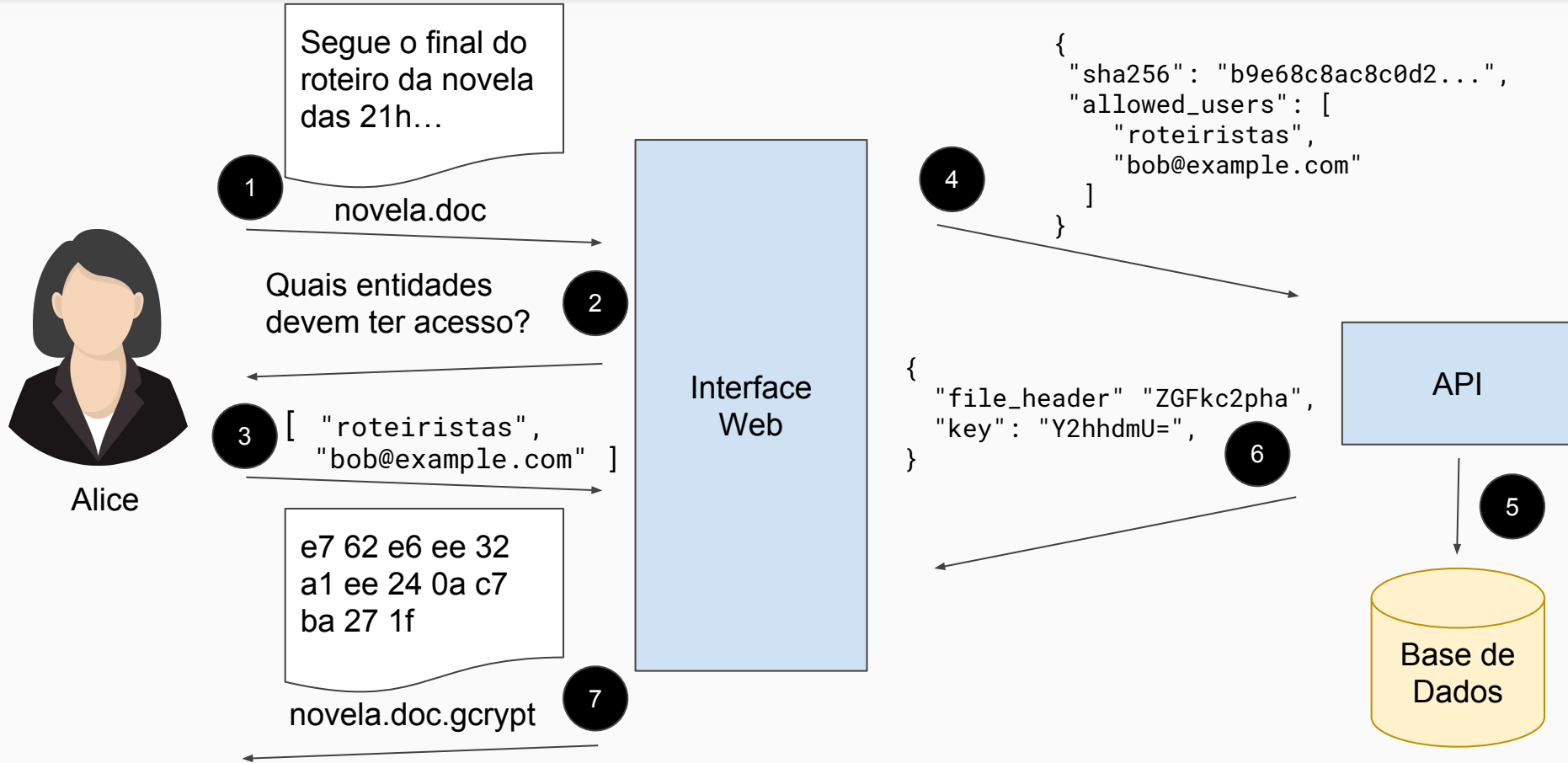


Componentes GCrypt

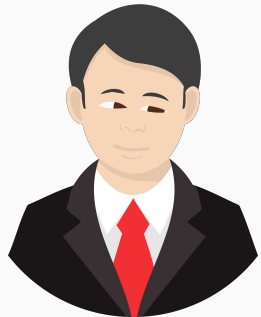
Fluxo de uso: autenticação



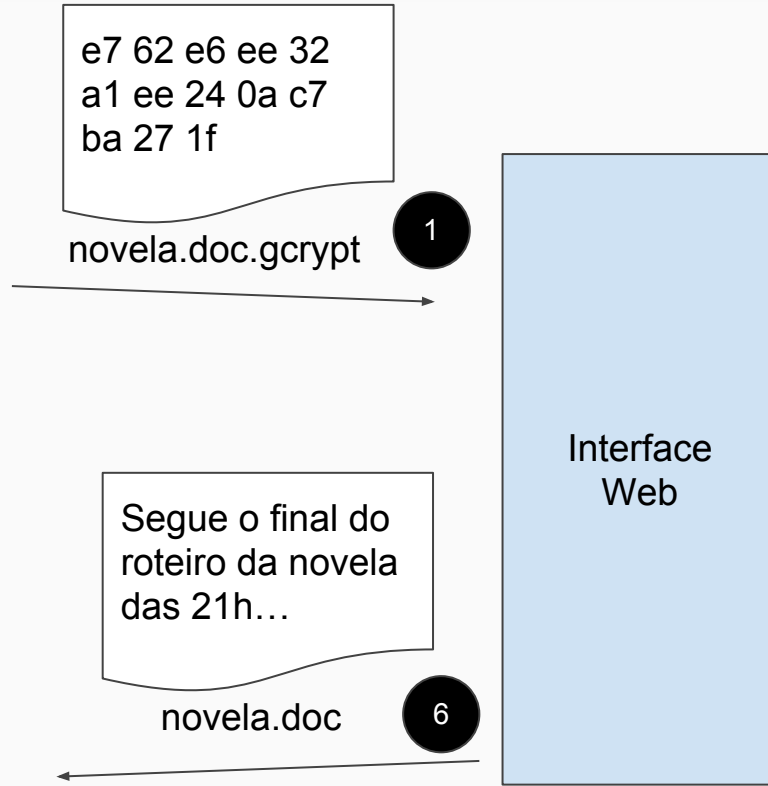
Fluxo de uso: encriptação



Fluxo de uso: descriptação



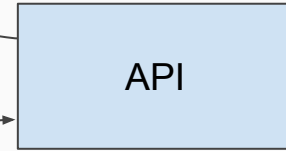
Bob



2 Qual a chave privada do arquivo com este cabeçalho?

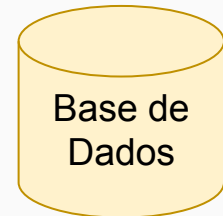
```
{  
  "file_header" "ZGFkc2pha",  
}
```

3 Este usuário pode descriptar esse arquivo?



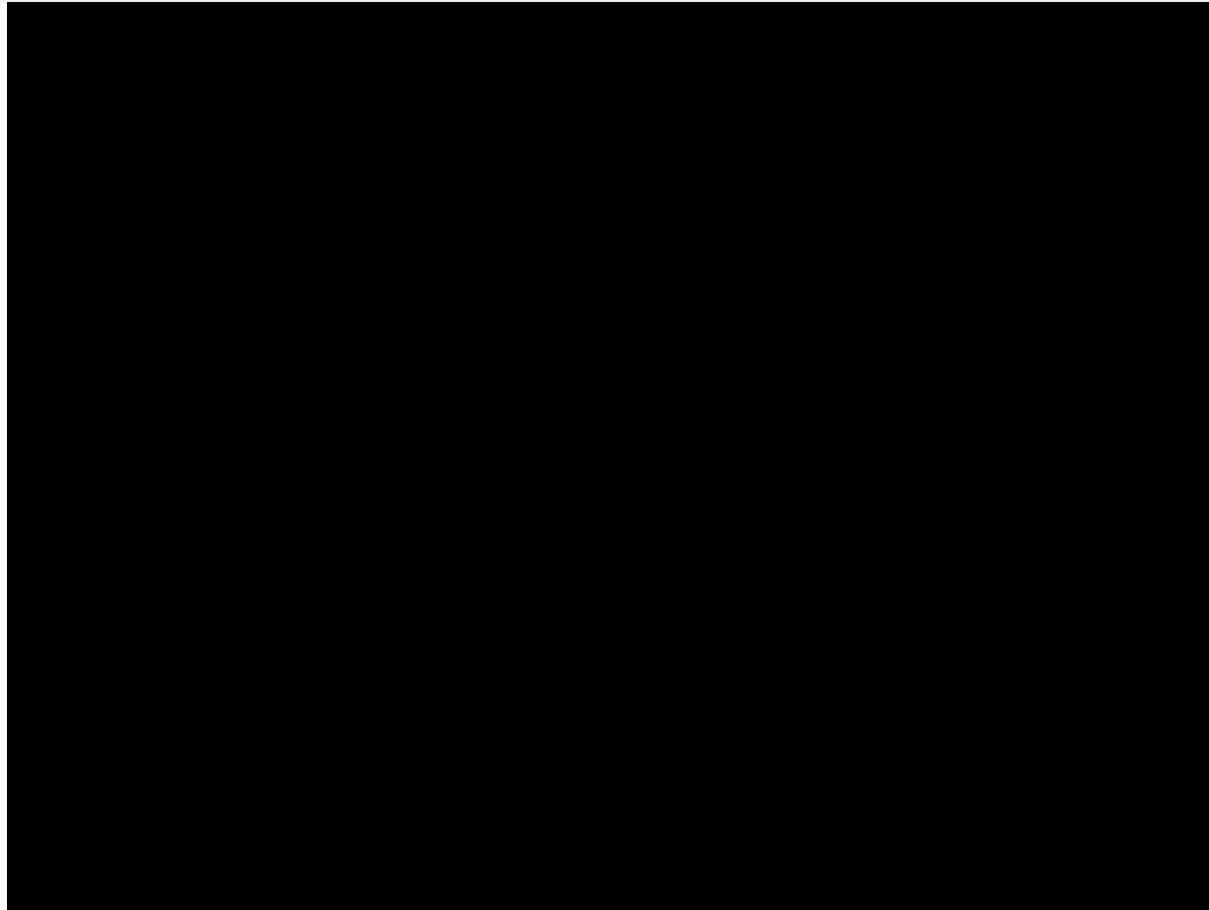
4

```
{  
  "key": "Y2hhdmU=",  
}
```



Base de Dados

Fluxo de uso: exemplo



- Ser simples para o usuário final.
- Criptografia realizada no navegador:
 - + infraestrutura
 - ponto de falha para casos de vazamento
 - privacidade
 - suporte dos navegadores
 - *troubleshooting*

Chave de acesso AWS ▸ Caixa de entrada ✕

Douglas 

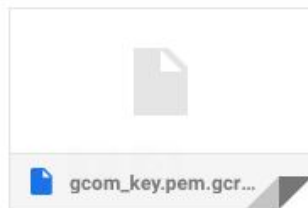
para Suporte, 

Boa noite,

Criei em produção uma chave para acesso como usuário local que será utilizada na criação de todas as

texto omitido intencionalmente

Att,



Lista de usuários

Caixa de entrada x

Pedro [redacted]

Pessoal, preciso da lista de usuários com os domínios

3

Rodrigo [redacted]

para Pedro, [redacted]

Segue a lista dos usuários.



usuarios.txt.gcrypt

682

arquivos .gcript pelo mundo...

- Integração com Vault para armazenamento de chaves privadas.

- Integração com Vault para armazenamento de chaves privadas.
- Remoção de entidades autorizadas depois da criptografia.

- Integração com Vault para armazenamento de chaves privadas.
- Remoção de entidades autorizadas depois da criptografia.
- Suporte a chaves assimétricas (para usuários avançados).

Para a comunidade...

globo
.com



GTS 32 | SP 12/2018

Fork me on GitHub

.gcrypt

github.com/globocom/gcrypt

globo .com



GTS 32 | SP 12/2018

Perguntas?

Claudio Netto

claudio.netto@corp.globo.com



GTS 32 | SP 12/2018

GCrypt:

Criptografia para humanos

Claudio Netto

claudio.netto@corp.globo.com