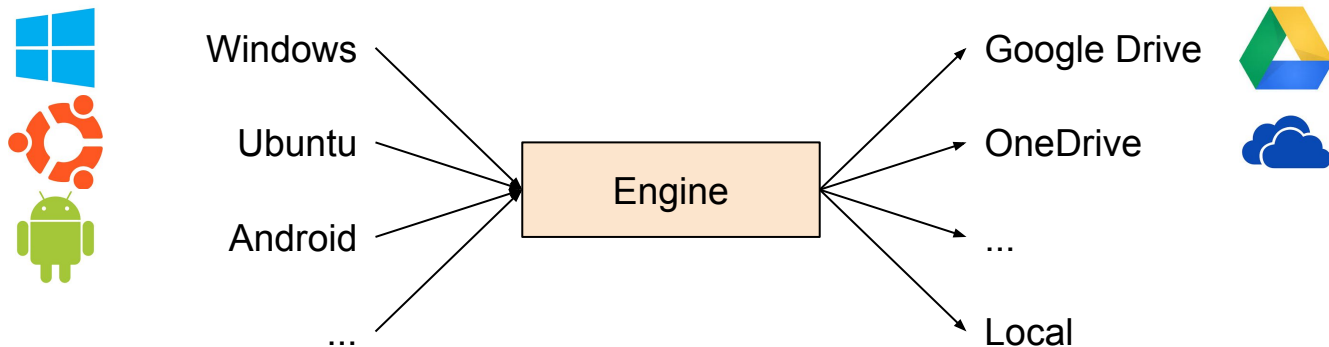


Safe Vault

Sistema para proteção de pastas e arquivos

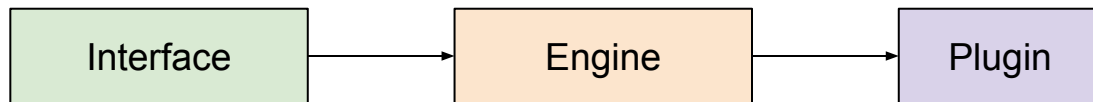
Projeto

Framework que garante a segurança de pastas e arquivos em armazenamentos.

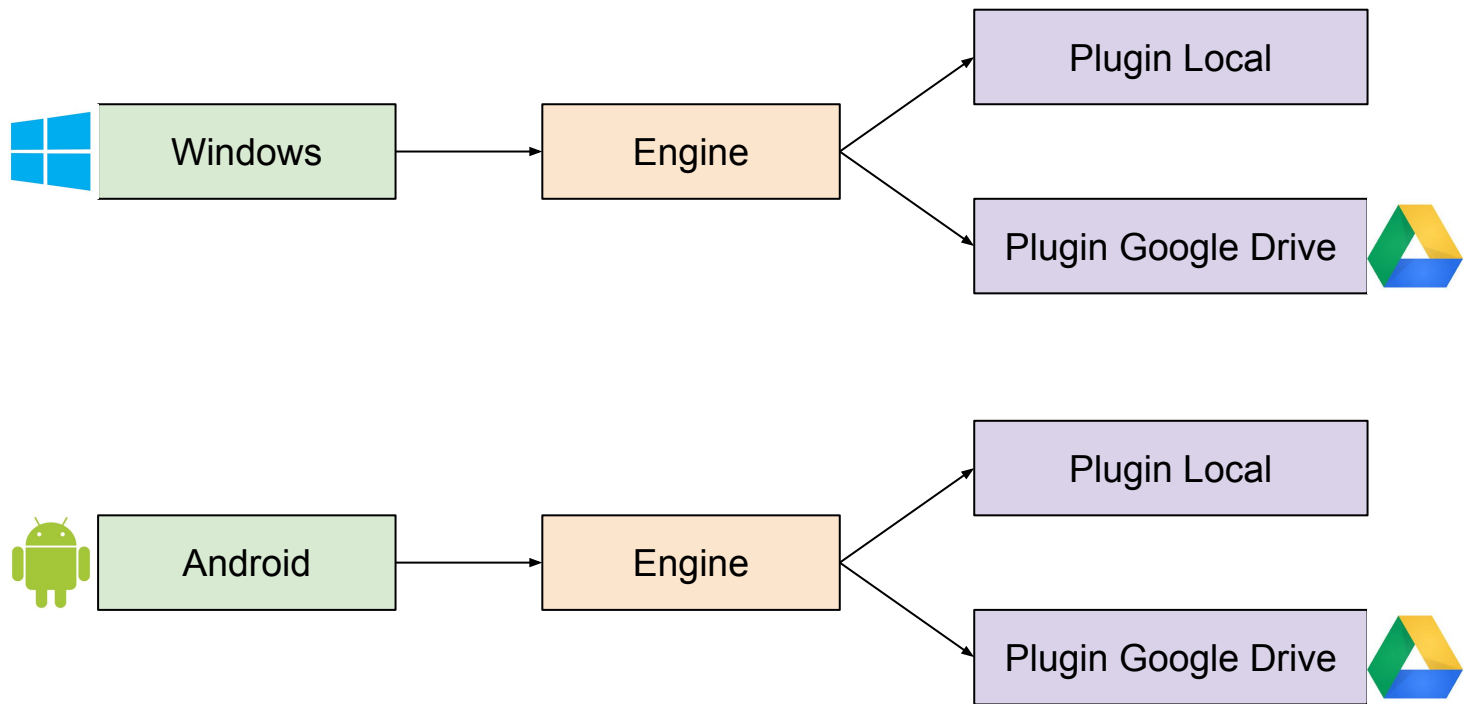


Projeto

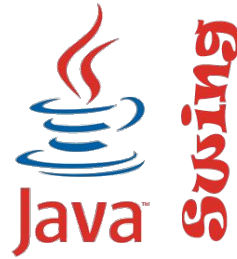
3 Camdas



Projeto



Conhecimento prévio



Segurança da informação

Integridade

Autenticidade

Confidencialidade

Controle de Acesso

Disponibilidade

Irretratabilidade

Man-in-the-middle attack

Janela de Tempo

Sequenciamento

Função Hash Criptográfica

Resumo de Mensagem

Criptografia Simétrica

Criptografia Assimétrica

Envelope Digital

Assinatura Digital

Google Drive API



Armazenamento dos arquivos

- Metainformação dos arquivos
- Criação de pasta ou arquivo
- Atualização de conteúdo de arquivo
- Download de conteúdo de arquivo
- Remoção de pasta ou arquivo
- Busca de pasta ou arquivo

Google Drive API



Busca de pasta ou arquivo pela metainformação

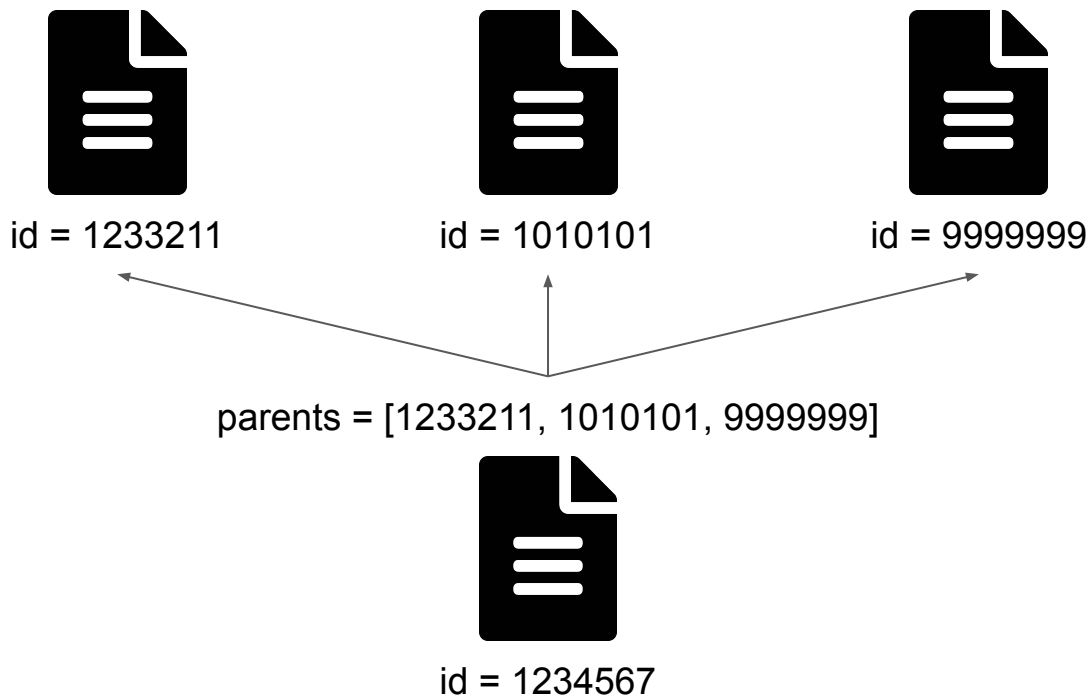


Metainformações

- id
- name
- mimeType
- trashed
- parents

```
mimeType = 'application/vnd.google-apps.folder'  
trashed = false  
name = 'exemplo'
```


Google Drive API

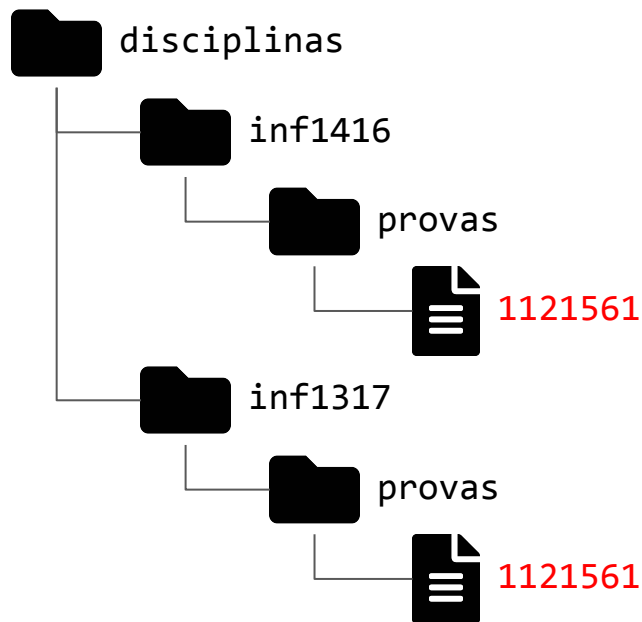


Google Drive API



`"/disciplinas/inf1416/provas/1121561"`

`q("name = '1121561'");`



Google Drive API



"/disciplinas/inf1416/provas/1121561"

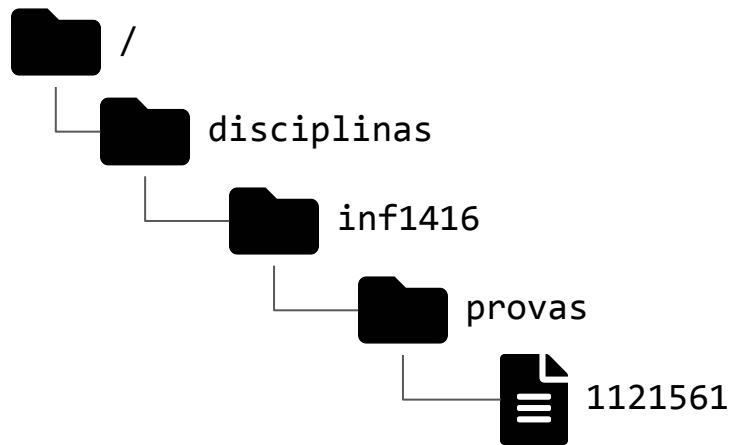
```
root = get("root");
```

```
disciplinas = q("parents = 'root'  
               and name = 'disciplinas'");
```

```
inf1416 = q("parents = 'disciplinas'  
           and name = 'inf1416'");
```

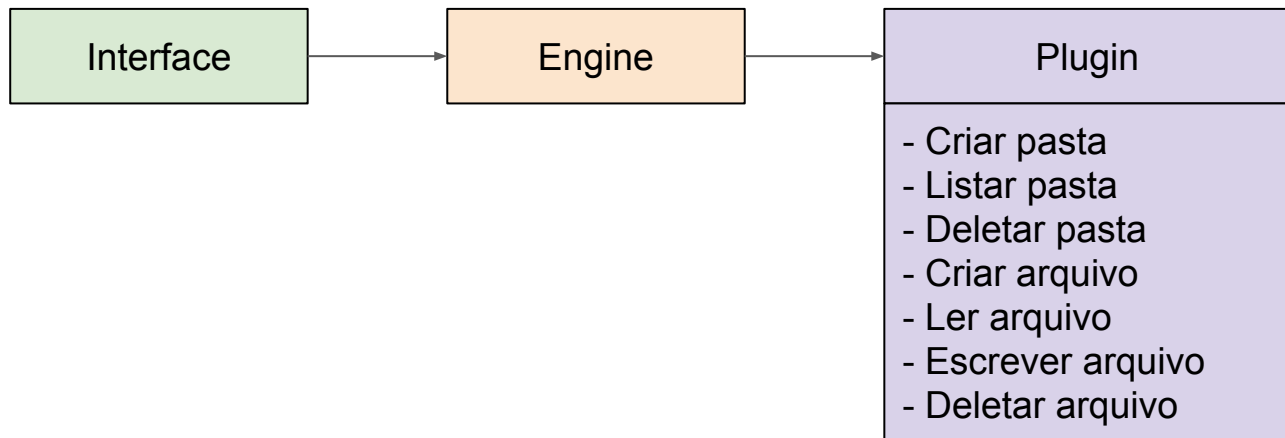
```
provas = q("parents = 'inf1416'  
          and name = 'provas'");
```

```
file = q("parents = 'provas'  
        and name = '1121561'");
```



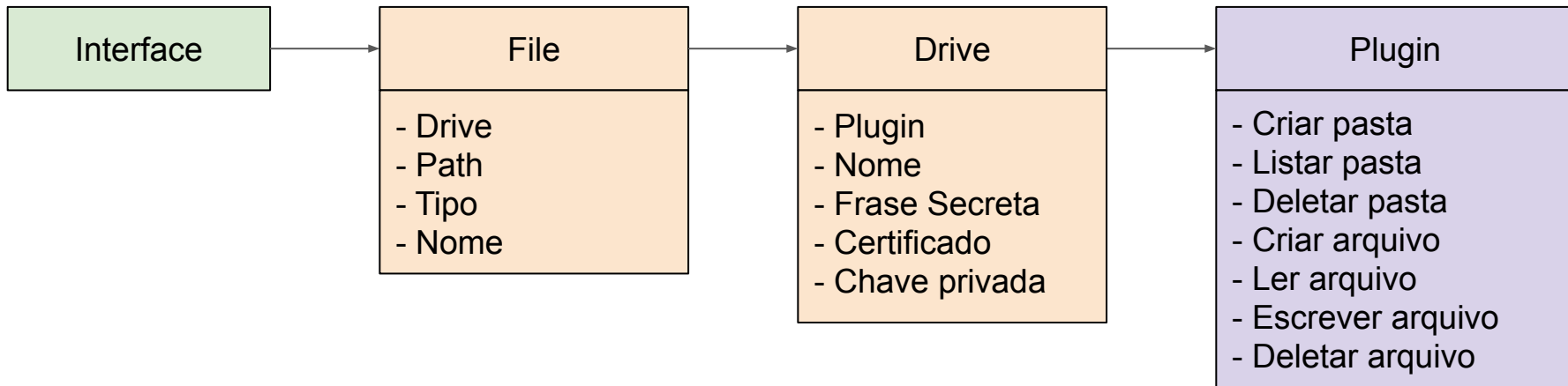
Plugin

Arquitetura minimalista

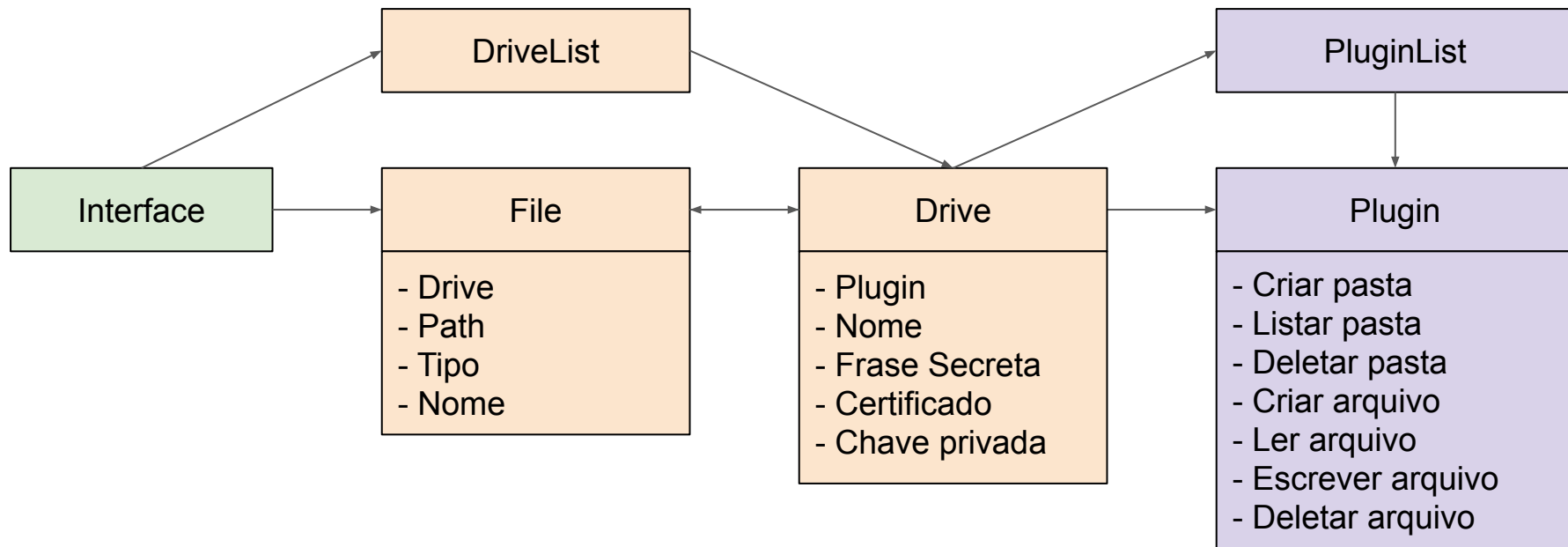


Engine

Representação de arquivos, pastas e drives

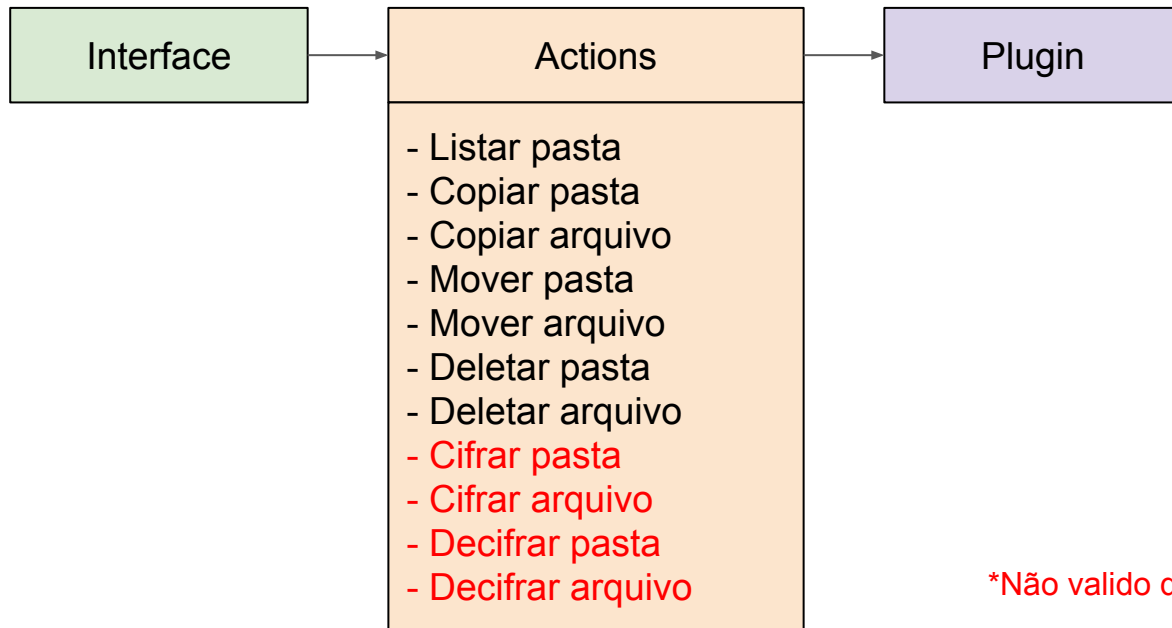


Engine



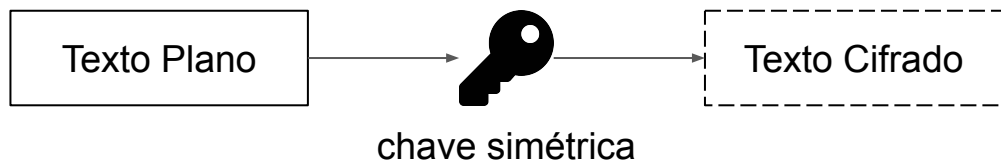
Engine

Ações sobre arquivos e pastas

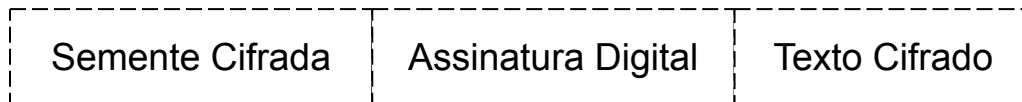


*Não valido dentro do vault

Engine



Novo conteúdo do arquivo

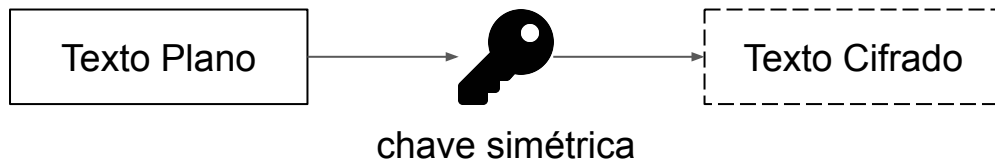


Engine

`SecureRandom()` → seed

`SecureRandom(SHA1PRNG)` → `setSeed(seed)` → `key(AES)`

`Cipher(AES)` → content + key → ciphered content



Engine

Cipher(RSA) → seed + public key → ciphered seed

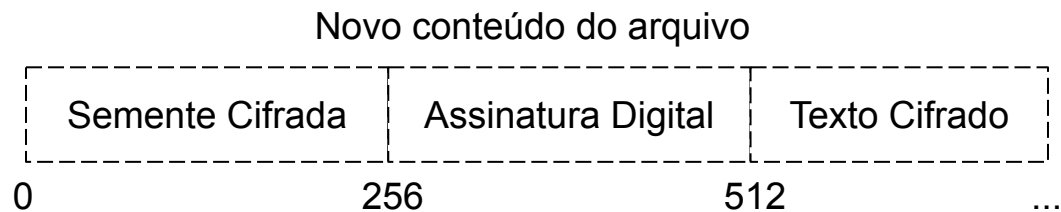


Signature(SHA256withRSA) → content + private key → digital signature



Engine

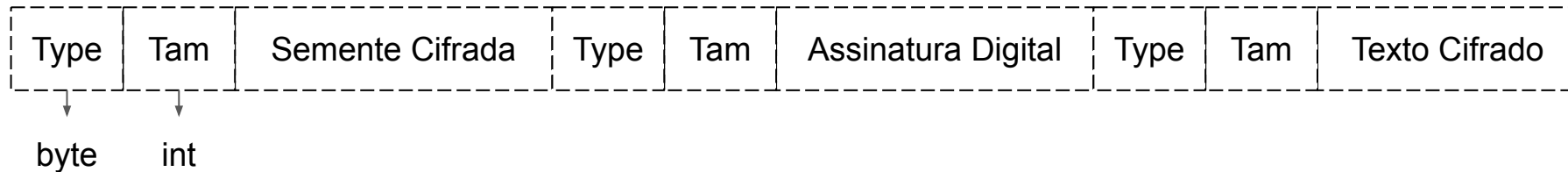
Problema



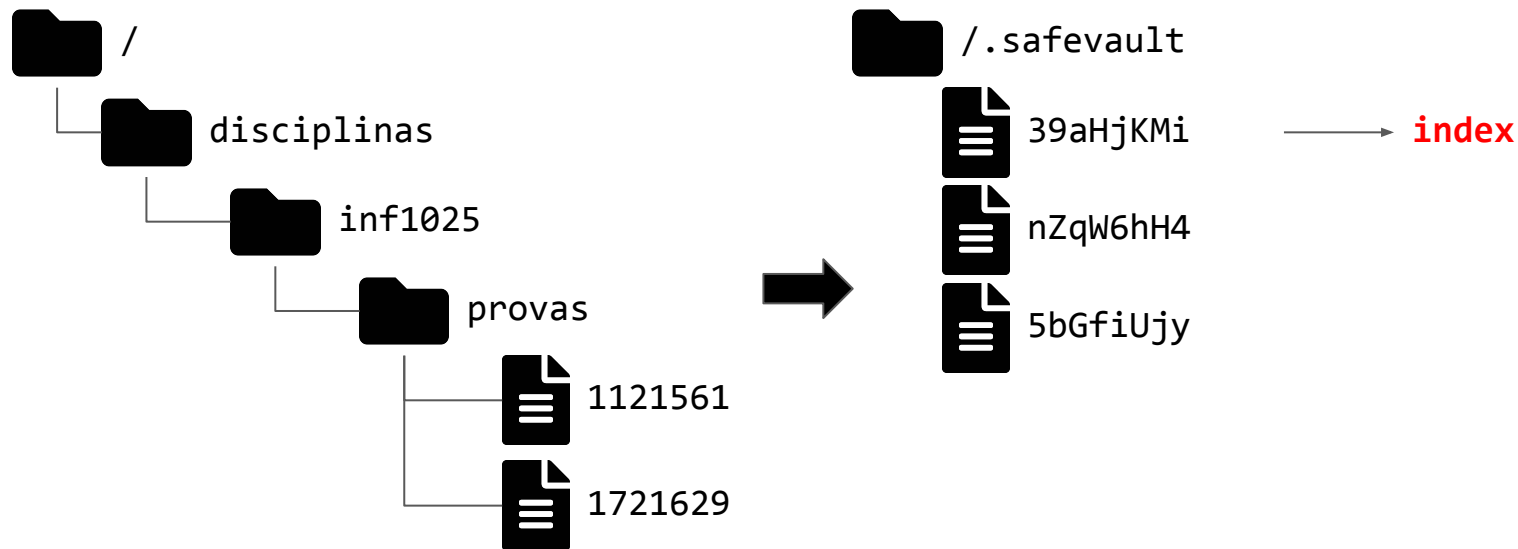
Engine

Solução

Novo conteúdo do arquivo



Engine



SecureRandom(SHA1PRNG) → secret phrase → index name

Engine

Index

/arquivo.txt

/documentos/trabalho.xls

/fotos/amigos.jpeg

/fotos/festa/super_amigos.jpeg

...

sor028g6

1dTkBFEH

VKmLvaup

2WHOhahM

file

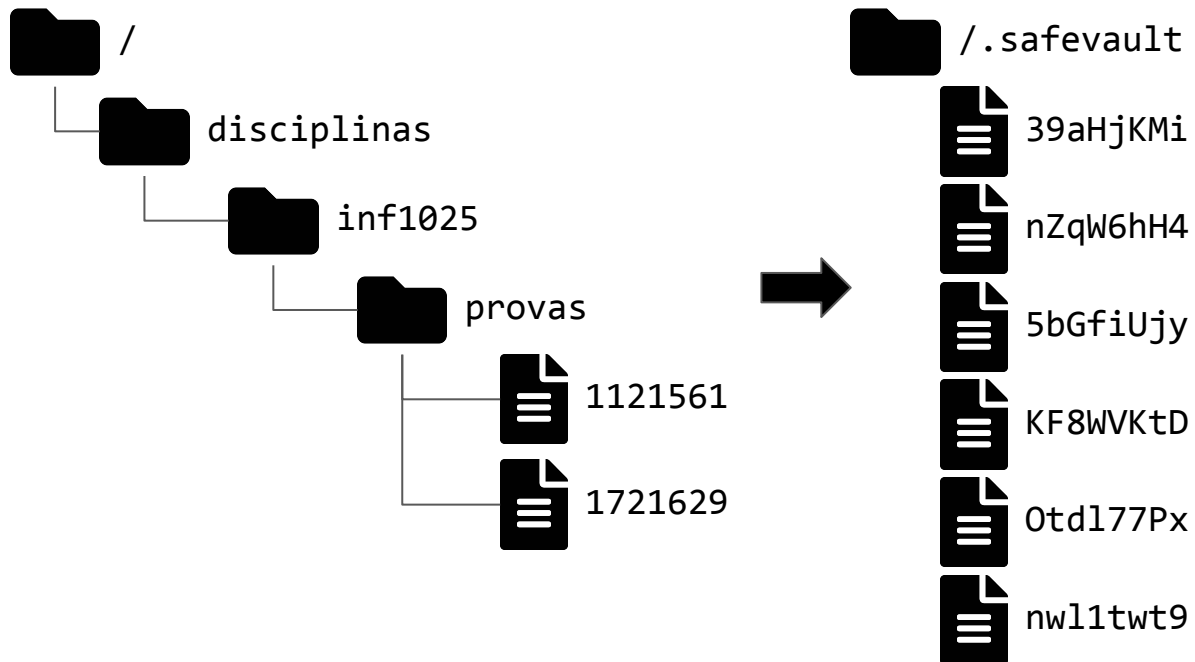
file

file

file

Engine

Melhoria



Engine

Index

/senha.txt

/pictures

/git

/notas.xls

...

scrNk7ED

xV6mvJtw

YM9P1E9f

JYYpR99V

file

folder

folder

file

Engine

git

/puc-inf1950

/puc-inf1416

/puc-inf1317

/puc-inf1025

...

QFkCVk2q

aAa7Kb6A

ICf3ESgk

0wqsklas

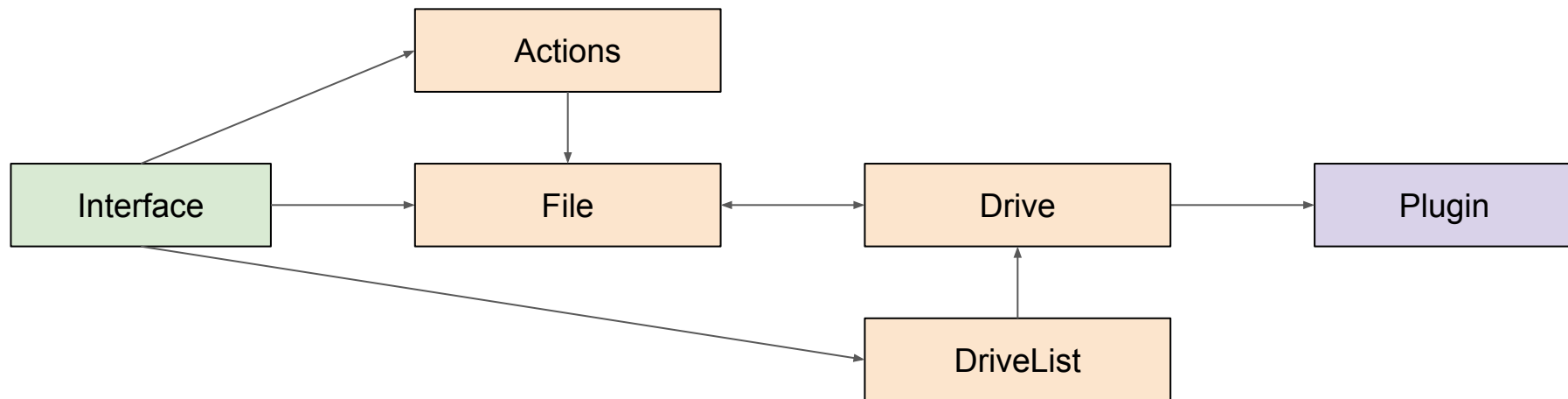
folder

folder

folder

folder

Engine



Metas Futuras

Melhorar a arquitetura de segurança.

Implementação de uma interface para mobile.

Limitação do tamanho dos arquivos por uso de array de bytes.

Criação de um cache local para evitar requisições ao armazenamento.

Conclusão

Framework providência um ambiente seguro para arquivos e pasta.

Cobra chave privada e frase secreta para recuperação dos arquivos.

Não se limita a ações relacionadas a segurança.

Capacidade de alcançar diversos dispositivos e armazenamentos.

Pequena e simples framework para ser usada como base para grandes projetos.