Secure Boot Personalizado

Guia para criação de uma assinatura personalizada para **Secure Boot** tornando possível configurar a **BIOS** dos dispositivo para inicializar apenas com o sistema operacional específico

Pré-requisitos

1. Recomenda-se usar um ambiente Linux (via Live USB/WSL) para facilitar a execução das ferramentas.
2. Acesso administrativo ao Windows e à BIOS/UEFI.
3. Uma máquina com UEFI (não Legacy/BIOS) e Secure Boot habilitado.
4. Ferramentas instaladas:

OpenSSL	Para gerar chaves.
efitools	Para manipular chaves UEFI.
sbsigntools	Para assinar arquivos EFI.

Passo 1: Gerar as Chaves Secure Boot

1.1 Criar Diretório de Trabalho

```
mkdir -p secureboot-keys && cd secureboot-keys
```

1.2 Gerar Chaves com OpenSSL

```
 # Gerar PK (Platform Key)
openssl req -newkey rsa:4096 -nodes -keyout PK.key -new -x509 -sha256 -days
3650 -subj "/CN=My Platform Key/" -out PK.crt

# Gerar KEK (Key Exchange Key)
openssl req -newkey rsa:4096 -nodes -keyout KEK.key -new -x509 -sha256 -days
3650 -subj "/CN=My Key Exchange Key/" -out KEK.crt

# Gerar db (Database Key)
openssl req -newkey rsa:4096 -nodes -keyout db.key -new -x509 -sha256 -days
3650 -subj "/CN=My Signature Database Key/" -out db.crt

# Gerar dbx (Opcional)
openssl req -newkey rsa:4096 -nodes -keyout dbx.key -new -x509 -sha256 -days
3650 -subj "/CN=My Revoked Signatures Key/" -out dbx.crt
```

Passo 2: Converter Chaves para Formato UEFI

As chaves devem ser convertidas para o formato **EFI Signature List (ESL)**.

2.1 Instalar efitools

No Linux como **root**

```
apt-get install efitools
```

2.2 Converter Certificados

Substitua **<UUID>** por um **UUID** gerado (ex: $(uuidgen) no Linux).

```
# Converter PK
cert-to-efi-sig-list -g <UUID> PK.crt PK.esl
sign-efi-sig-list -k PK.key -c PK.crt PK PK.esl PK.auth

# Converter KEK
cert-to-efi-sig-list -g <UUID> KEK.crt KEK.esl
sign-efi-sig-list -k PK.key -c PK.crt KEK KEK.esl KEK.auth

# Converter db
cert-to-efi-sig-list -g <UUID> db.crt db.esl
sign-efi-sig-list -k KEK.key -c KEK.crt db db.esl db.auth
```

Passo 3: Assinar o Bootloader do Windows

O bootloader do Windows (bootmgfw.efi) deve ser assinado com sua chave db.

3.1 Localizar o Bootloader

O arquivo está em:

```
/EFI/Microsoft/Boot/bootmgfw.efi (partição EFI do Windows).
```

3.2 Assinar com sbsigntools

```
sudo sbsign --key db.key --cert db.crt --output bootmgfw-signed.efi
bootmgfw.efi
```

3.3 Substituir o Bootloader

Faça backup do original e substitua pelo arquivo assinado.

Passo 4: Configurar a BIOS/UEFI

Acesse a BIOS/UEFI (geralmente pressionando Del, F2, ou F12 durante a inicialização).

1. Navegue até as opções de Secure Boot.
2. Exclua todas as chaves existentes (PK, KEK, db, dbx).
3. Adicione as novas chaves:

PK:	Carregue PK.auth.
KEK:	Carregue KEK.auth.
db:	Carregue db.auth.

Salve e saia.

Passo 5: Ativar Secure Boot

Na BIOS:

- Item de lista não ordenadaDefina Secure Boot Mode para Custom ou User.
- Ative Secure Boot.
- Reinicie o sistema.

Verificação: Inicialize o Windows 11. Se tudo estiver correto, o sistema iniciará.

Use o comando no PowerShell para confirmar:

```
Confirm-SecureBootUEFI
```

Deve retornar **True**.

Notas Importantes

- Backup: Sempre faça backup das chaves originais e dos arquivos EFI.
- Atualizações do Windows: Após atualizações, o bootloader pode ser substituído. Reassine-o sempre.
- Problemas: Se o sistema não iniciar, restaure as chaves padrão da Microsoft na BIOS.
- Se precisar de ajuda adicional, informe-se na documentação do seu fabricante de UEFI!