INSTITUTO DE PESQUISAS TECNOLÓGICAS

COMUNICAÇÃO TÉCNICA

Nº 180157

Boot seguro em distribuição baseados em Debian: cadeias de confiança, implementação e seus desafios.

Rodrigo Neves Ribeiro
Alexandre de Faustino Miranda

Palestra apresentada no MINIDEBCONF, 7., 2026, Campinas. 19 slides

Instituto de Pesquisas Tecnológicas do Estado de São Paulo S/A - IPT
Av. Prof. Almeida Prado, 532 | Cidade Universitária ou
Caixa Postal 0141 | CEP 01064-970
São Paulo | SP | Brasil | CEP 05508-901
Tel 11 3767 4374/4000 | Fax 11 3767-4099

www.ipt.br

Boot seguro em distribuições baseadas em Debian: Cadeias de confiança, implementação e seus desafios.

Rodrigo Neves Ribeiro
Alexandre de Faustino Miranda

ipt INSTITUTO DE PESQUISAS TECNOLÓGICAS

2026 MINI DEB CONF
CAMPINAS - BRASIL

Tópicos

- Boot seguro UEFI
- Cadeias de confiança
- Implementação no Debian
- Processo de submissão do SHIM para distros derivadas
- Como o usuário pode assumir o papel de CA

2026
MINI
DEB
CONF
CAMPINAS - BRASIL

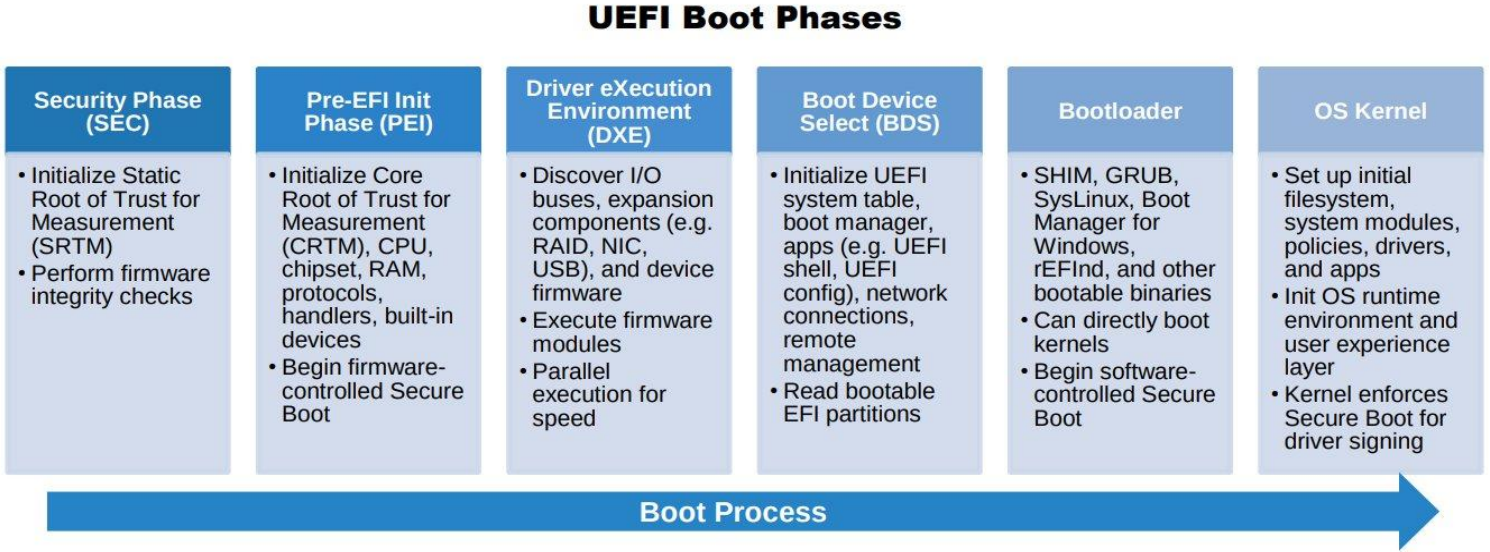
O que é o Boot Seguro?

- Funcionalidade desenvolvida pela Interface Unificada de Firmware Extensível (UEFI)
- Validação dos binários no processo de boot
- Verificação de assinaturas utilizando certificados embarcados na máquina
- Mitigar vulnerabilidades em tempo de boot
- Garantia da integridade dos binários

Aplicações

- Anti-Malware
- Ameaça interna (coordenado com restrição acesso a configuração da UEFI)

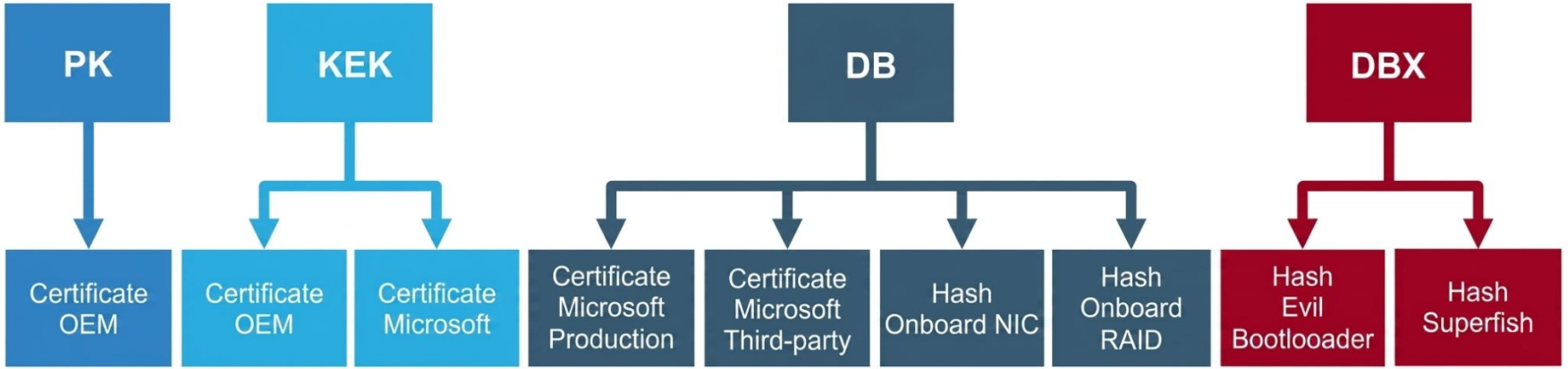
Processo de Boot



2026 MINI DEB CONF
CAMPINAS - BRASIL

fonte: [NSA - Secure Boot Customization]

Cadeia de Confiança - Certificados presentes na UEFI



fonte: Adaptado de [NSA - Secure Boot Customization]

Abordagem do mundo GNU/Linux

- Liberdade?
- Possível gargalo
- Mundo gnu/linux se adapta
- Debian 10 Buster
- SHIM
- MOK

2026 MINI DEB CONF
CAMPINAS - BRASIL

shim

- Mini bootloader
- MOK (Machine Owner Key)
- SBAT (Secure Boot Advanced Targeting)
    - Revogação baseada em número de geração

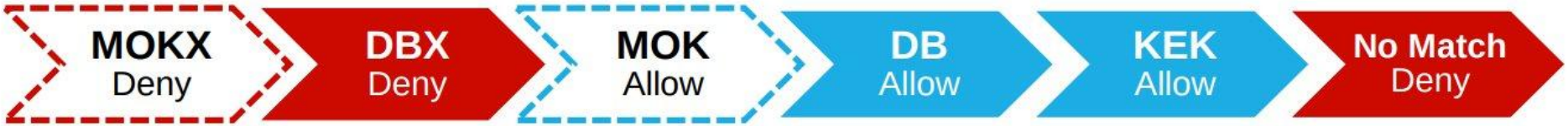
shim - sbat

```
shimx64.efi: formato do arquivo pei-x86-64

Conteúdo da seção .sbatlevel:
 86000 00000000 08000000 37000000 73626174  ........7...sbat
 86010 2c312c32 30323330 31323930 300a7368  ,1,2023012900.sh
 86020 696d2c32 0a677275 622c330a 67727562  im,2.grub,3.grub
 86030 2e646562 69616e2c 340a0073 6261742c  .debian,4..sbat,
 86040 312c3230 32343031 30393030 0a736869  1,2024010900.shi
 86050 6d2c340a 67727562 2c330a67 7275622e  m,4.grub,3.grub.
 86060 64656269 616e2c34 0a00               debian,4..
```

```
sbat,1,UEFI shim,sbat,1,https://github.com/rhboot/shim/blob/main/SBAT.md
fwupd-efi,1,Firmware update daemon,fwupd-efi,1.4,https://github.com/fwupd/fwupd-efi
fwupd-efi.debian,1,Debian,fwupd,1:1.4-1,https://tracker.debian.org/pkg/fwupd
```

Ordem de prioridade na verificação do Boot seguro



fonte: [NSA - Secure Boot Customization]

Processo de submissão do shim para distros derivadas

- Permite cadeia de confiança própria
- Necessário passar por board de aprovação da comunidade do shim
- A submissão requer os binários do shim, acompanhado de um dockerfile para o build reprodutível
- Necessário preencher um formulário com diversos tópicos
- Após a aprovação é necessário a submissão para a CA

Formulário de submissão

Principais características:

- Garantir a autenticidade da submissão
- Comprovar necessidade da distribuição ter a sua própria cadeia de boot
- Compliance em relação as diretrizes do boot seguro, como por exemplo Kernel com parâmetros de lockdown e sig_enforce
- Validade do certificado e método de armazenamento

Formulário de submissão

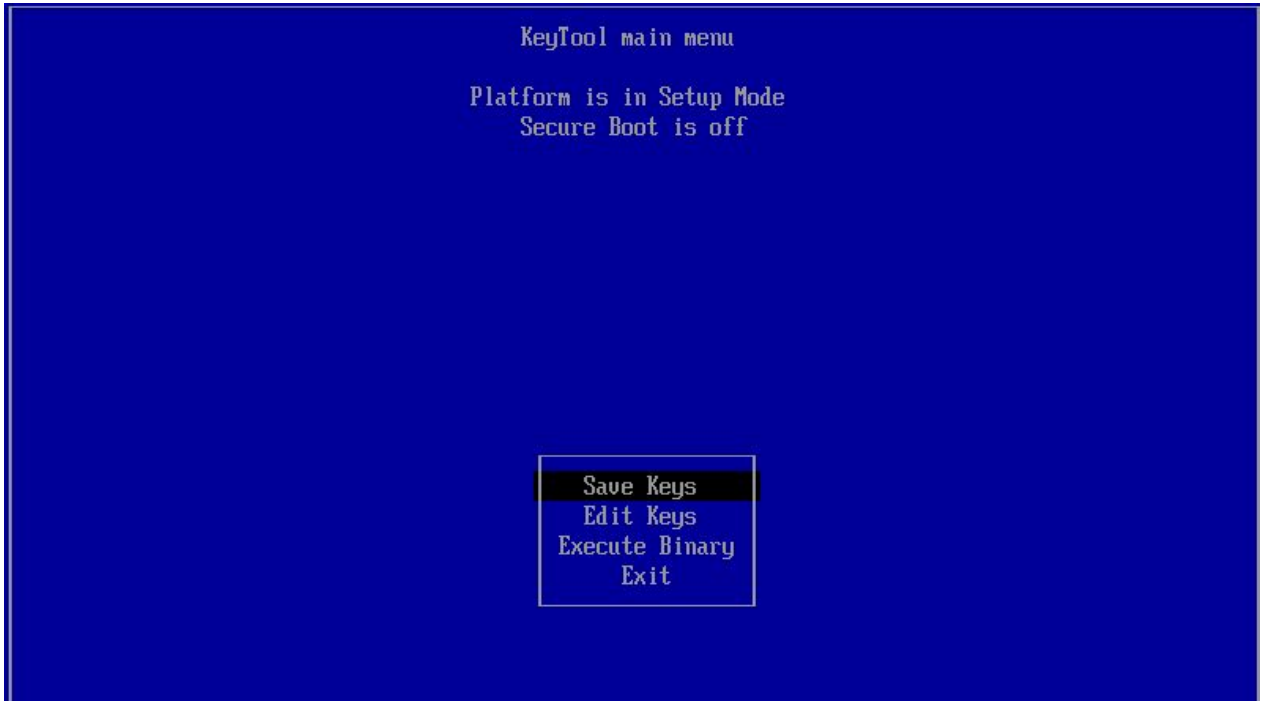
- https://github.com/rhboot/shim-review

Como o usuário pode assumir o papel de CA

É possível alterar os certificados presentes na UEFI:

- Opção presente na própria configuração da UEFI
- Ferramenta KeyTool presente no pacote efitools

Como o usuário pode assumir o papel de CA



Ferramentas importantes

- Assinatura de binários .EFI
  - sbsign presente no pacote sbsigntool
- Assinatura de módulos de kernel
  - sign-file presente no source do kernel linux
- Verificar status do boot seguro
  - mokutil --sb-state
- Verificar assinaturas de binários
  - sbverify --list
- Inspecionar seções dos binários
  - objdump

Ferramentas importantes

```
grubx64.efi.signed: formato do arquivo pei-x86-64

Conteúdo da seção .sbat:
 28d000 73626174 2c312c53 42415420 56657273  sbat,1,SBAT Vers
 28d010 696f6e2c 73626174 2c312c68 74747073  ion,sbat,1,https
 28d020 3a2f2f67 69746875 622e636f 6d2f7268  ://github.com/rh
 28d030 626f6f74 2f736869 6d2f626c 6f622f6d  boot/shim/blob/m
 28d040 61696e2f 53424154 2e6d640a 67727562  ain/SBAT.md.grub
 28d050 2c352c46 72656520 536f6674 77617265  ,5,Free Software
 28d060 20466f75 6e646174 696f6e2c 67727562   Foundation,grub
 28d070 2c322e31 322c6874 7470733a 2f2f7777  ,2.12,https://ww
 28d080 772e676e 752e6f72 672f736f 66747761  w.gnu.org/softwa
 28d090 72652f67 7275622f 0a677275 622e6465  re/grub/.grub.de
 28d0a0 6269616e 2c352c44 65626961 6e2c6772  bian,5,Debian,gr
 28d0b0 7562322c 322e3132 2d392b64 65623133  ub2,2.12-9+deb13
 28d0c0 75312c68 74747073 3a2f2f74 7261636b  u1,https://track
 28d0d0 65722e64 65626961 6e2e6f72 672f706b  er.debian.org/pk
 28d0e0 672f6772 7562320a 67727562 2e646562  g/grub2.grub.deb
 28d0f0 69616e31 332c312c 44656269 616e2c67  ian13,1,Debian,g
 28d100 72756232 2c322e31 322d392b 64656231  rub2,2.12-9+deb1
 28d110 3375312c 68747470 733a2f2f 74726163  3u1,https://trac
 28d120 6b65722e 64656269 616e2e6f 72672f70  ker.debian.org/p
 28d130 6b672f67 72756232 0a677275 622e7065  kg/grub2.grub.pe
 28d140 696d6167 652c322c 43616e6f 6e696361  image,2,Canonica
 28d150 6c2c6772 7562322c 322e3132 2d392b64  l,grub2,2.12-9+d
 28d160 65623133 75312c68 74747073 3a2f2f73  eb13u1,https://s
 28d170 616c7361 2e646562 69616e2e 6f72672f  alsa.debian.org/
 28d180 67727562 2d746561 6d2f6772 75622f2d  grub-team/grub/-
 28d190 2f626c6f 622f6d61 73746572 2f646562  /blob/master/deb
 28d1a0 69616e2f 70617463 6865732f 73656375  ian/patches/secu
 28d1b0 72652d62 6f6f742f 6566692d 7573652d  re-boot/efi-use-
 28d1c0 7065696d 6167652d 7368696d 2e706174  peimage-shim.pat
 28d1d0 63680a00 00000000 00000000 00000000  ch..............
```

```
image signature issuers:
 - /CN=Debian Secure Boot CA
image signature certificates:
 - subject: /CN=Debian Secure Boot Signer 2022 - grub2
```

2026 MINI DEB CONF
CAMPINAS - BRASIL

Referências

NSA - Secure boot customization

Shim-review

Rodsbooks

SecureBoot - Debian Wiki

Obrigado

INSTITUTO DE PESQUISAS TECNOLÓGICAS

2026 MINI DEB CONF
CAMPINAS - BRASIL