Николай Костригин

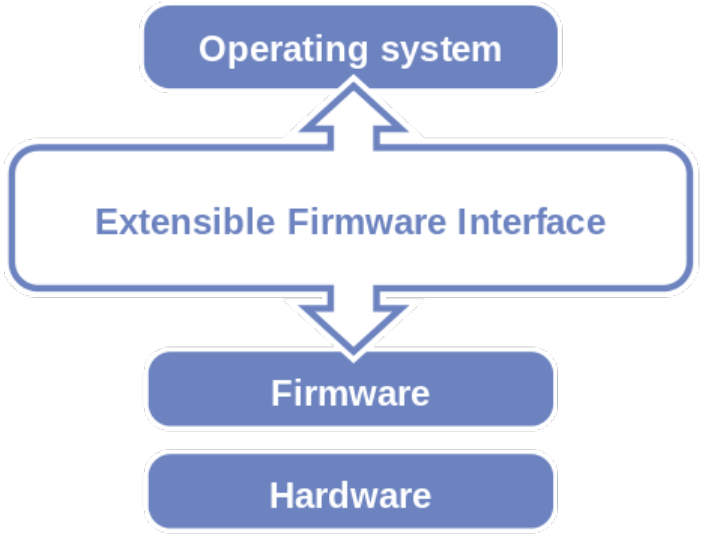
Доверенная загрузка GNU/Linux в режиме UEFI Secure Boot в 2021 году

base alt

Что такое UEFI?

Unified Extensible Firmware Interface

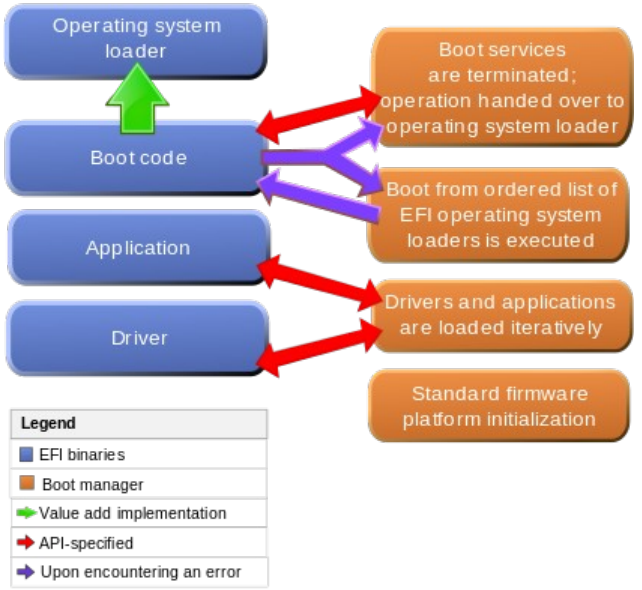
	BIOS	UEFI
Режим исполнения	16-бит реальный	32/64-бит защищенный (объем доступной памяти больше)
Размещение прошивки	ROM / EEPROM(десятки — сотни КБайт)	EEPROM (единицы-десятки МБайт)
Размещение драйверов загрузочных устройств	ROM / EEPROM	EEPROM / FAT32 партиция накопителя (объем почти не ограничен)



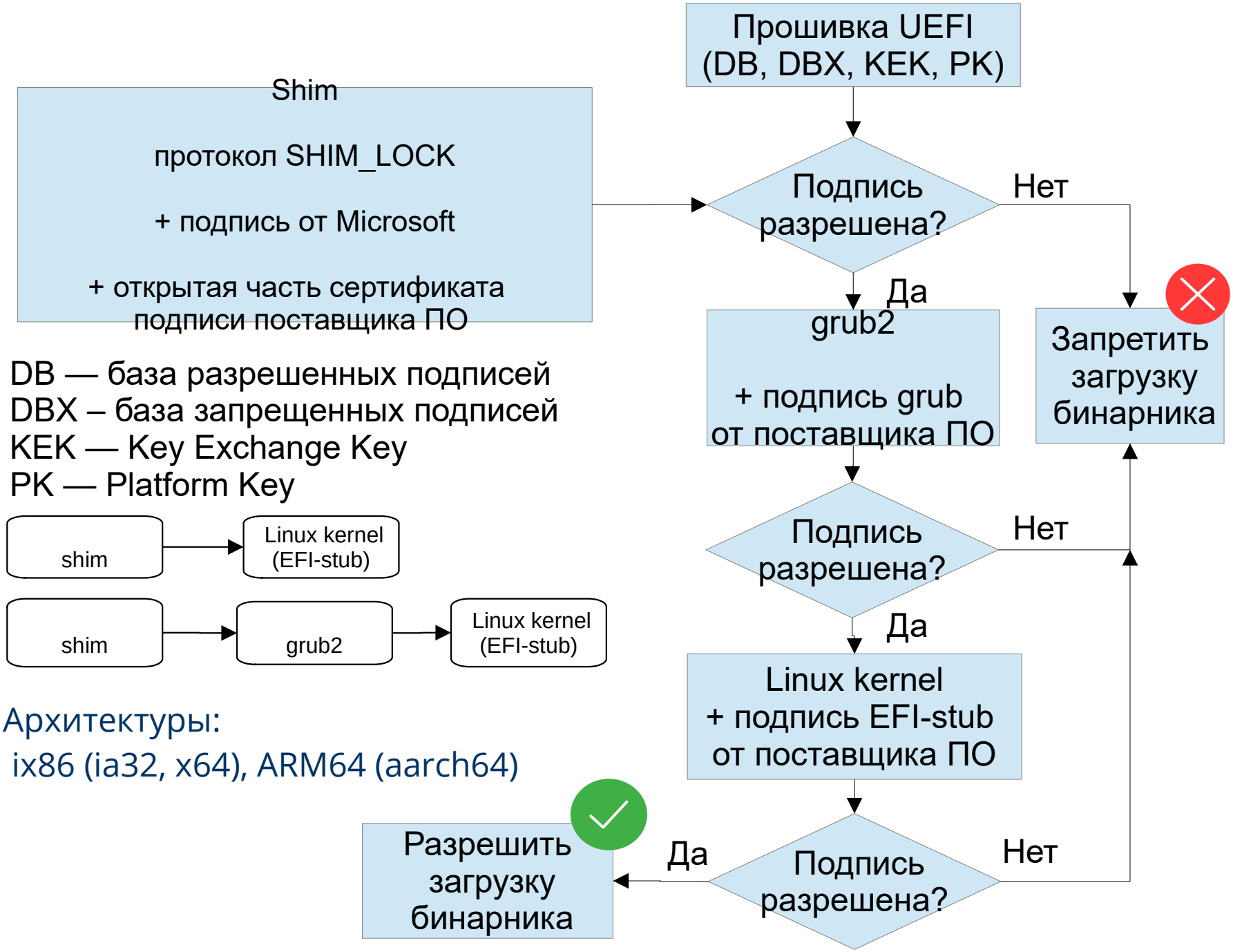
Архитектуры: ix86 (ia32, x64), ARM/ARM64 (aarch32, aarch64), RISCV32/RISCV64, существует реализация для MIPS, упоминается неофициальная реализация для PowerPC

Tianocore/edk2: открытая реализация спецификации от UEFI.org

https://github.com/tianocore/edk2



UEFI Secure Boot

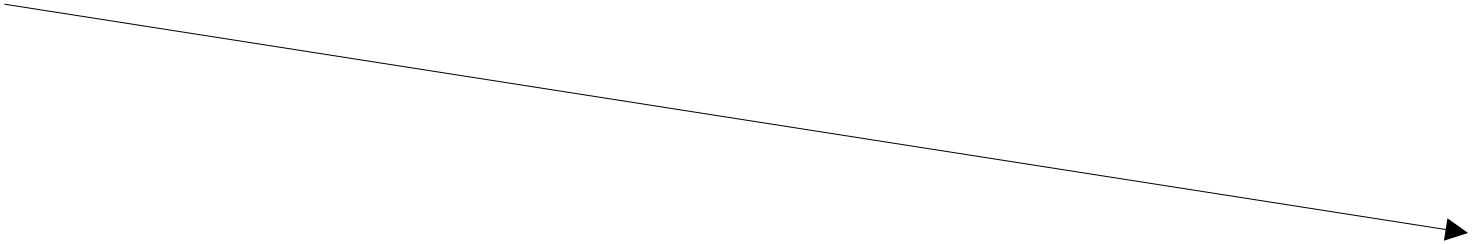


DB — база разрешенных подписей
DBX – база запрещенных подписей
KEK — Key Exchange Key
PK — Platform Key

Архитектуры:
ix86 (ia32, x64), ARM64 (aarch64)

Shim-review: начало

2013 год:
* упрощенное ревью кода
* льготные сертификаты Code Sign ($99)
* доступно одиночным разработчикам



2018 год :
* shim-review: ревью кода, воспроизводимая сборка
* только организации
* EV Code Sign сертификат (>$400)
* регистрация организации в международном бизнес справочнике (например DUNS)

Shim + grub2
BootHole и SB Bypass 2021 (BootHole2)

Инцидент	CVE	Кол-во патчей grub2
BootHole (2020)	CVE-2020-10713, CVE-2020-14308, CVE-2020-14309, CVE-2020-14310, CVE-2020-14311, CVE-2020-15705, CVE-2020-15706, CVE-2020-15707	28
BootHole2 (2021)	CVE-2020-14372, CVE-2020-25632, CVE-2020-25647, CVE-2020-27749, CVE-2020-27779, CVE-2021-20225, CVE-2021-20233, CVE-2021-3418	123

SBAT: Secure Boot Advanced Targeting.

Объем DBX в NVRAM (128кБ) ограничен 32кБ

Отзыв всех уязвимых, подписанных до сего дня бинарников занимает 16кБ

Внедрение SBAT +
замена сертификата подписи UEFI-бинарников или добавление уязвимых бинарников в dbx, vendor.db

Примеры «.sbat» секции в UEFI-бинарниках .

SBAT for shim:

sbat,1,SBAT Version,sbat,1,https://github.com/rhboot/shim/blob/main/SBAT.md
shim,1,UEFI shim,shim,1,https://github.com/rhboot/shim
shim.altlinux,1,ALT Linux,shim,15.4-alt2,http://git.altlinux.org/gears/s/shim.git

SBAT for grub:

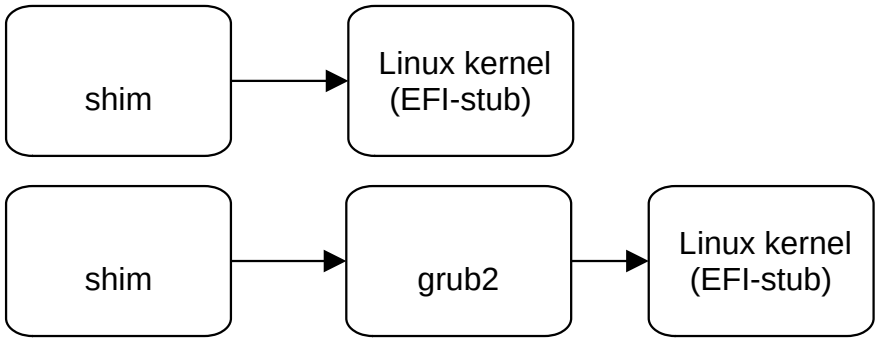
sbat,1,SBAT Version,sbat,1,https://github.com/rhboot/shim/blob/main/SBAT.md
grub,1,Free Software Foundation,grub,2.06-rc1,https://www.gnu.org/software/grub/
grub.altlinux,1,ALT Linux,grub,2.06-alt1.rc1,http://git.altlinux.org/gears/g/grub.git

SBAT for fwupd has the same style

sbat,1,UEFI shim,sbat,1,https://github.com/rhboot/shim/blob/main/SBAT.md
fwupd,1,Firmware update daemon,fwupd,1.5.9,https://github.com/fwupd/fwupd
fwupd.altlinux,1,ALT Linux,fwupd,1.5.9-alt1,http://git.altlinux.org/gears/f/fwupd.git

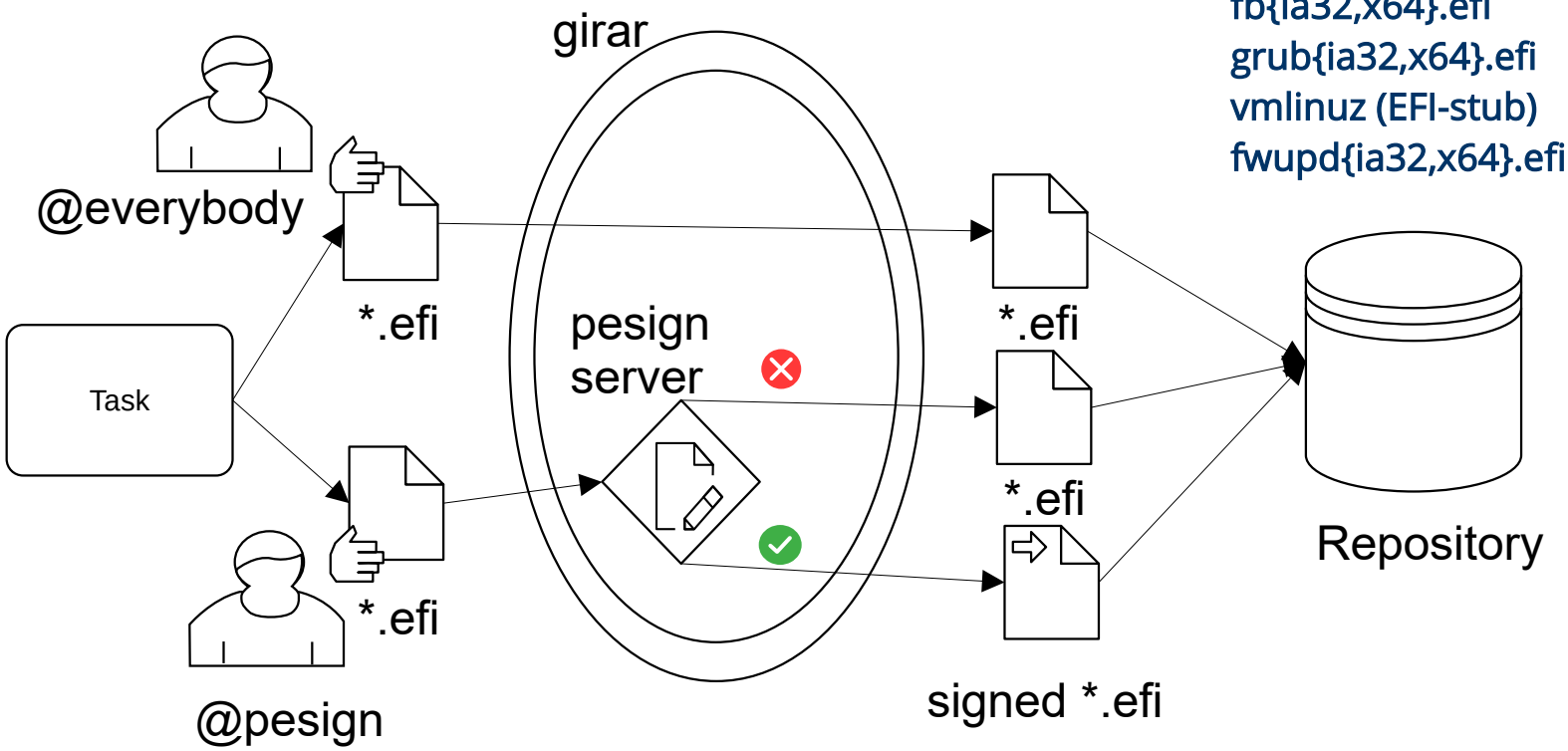
Спасение утопающих - дело рук самих утопающих: воспроизводимая сборка бинарников shim и участие заявителей в воспроизведении сборки бинарников других заявителей в процессе shim-review.

Требования к инфраструктуре репозитория и сборочной системы.



Сокращение количества доверенных UEFI загрузчиков и программ

- mm{ia32,x64}.efi
- fb{ia32,x64}.efi
- grub{ia32,x64}.efi
- vmlinuz (EFI-stub)
- fwupd{ia32,x64}.efi



Проблемы реализации прошивок на базе спецификации UEFI

- все дороги ведут в Microsoft

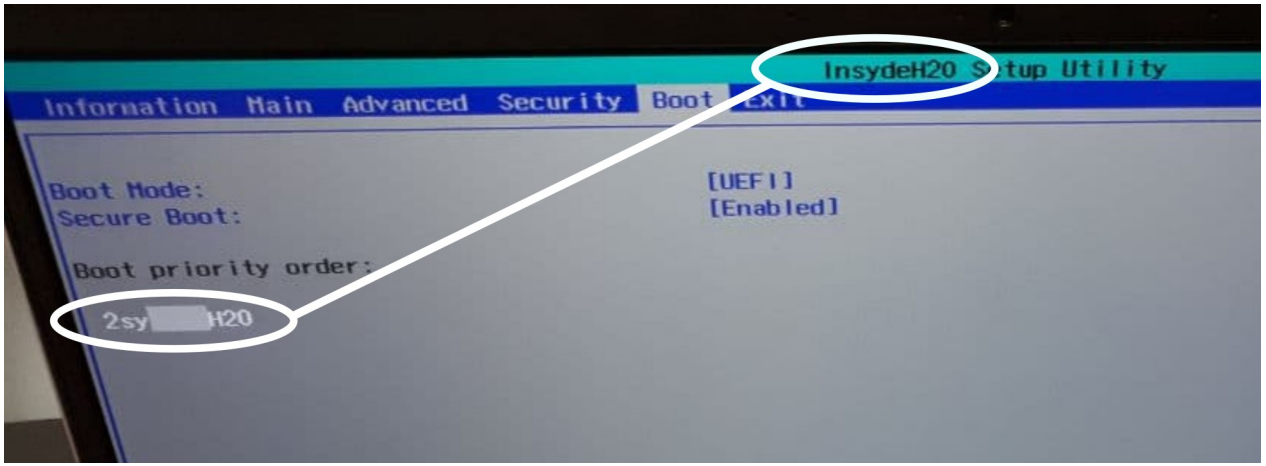
Доверенные сертификатов одной из серийных машин предустановленных при производстве.

- CSM реализован с приоритетом UEFI: в гибридных образах загрузчиков инсталлятора активация режима CSM (Legacy BIOS) все равно приводит к старту машины в режиме UEFI и запуску соответствующего инсталлятора, если обнаружена загрузочная партиция EFI.
- загрузочная переменная созданная efibootmgr исчезает, если на FAT32 EFI-партиции нет директории */EFI/*BOOT

```
/boot/efi/
`--EFI
   |--altlinux
   |   |--shimx64.efi
   |   |--grubx64.efi
   |   |--mmx64.efi
   |   |--fbx64.efi
   |   |--grub.cfg
   |   `--BOOTX64.CSV
   `--BOOT
      |--BOOTX64.EFI
      |--grubx64.efi
      |--fbx64.efi
      `--grub.cfg
```

Проблемы реализации прошивок на базе спецификации UEFI

- отсутствие тестирования UEFI-прошивок на совместимость с ОС отличными от MS Windows



Чтение произвольных областей памяти в UEFI прошивке Acer Swift 3

Тенденции:

- невозможность отключения Secure Boot
- невозможность замены доверенных сертификатов на пользовательские

UEFI SB по ГОСТу

Март 2021 года: спецификация UEFI 2.9 не содержит поддержки криптографии по ГОСТ (только DSA и RSA).

В число организаций, участвующих в UEFI Forum от России, входят ИСП РАН и Kraftway.
Возможно они могли бы стать пионерами применения криптографии по ГОСТ, сначала в локальных версиях прошивок, а затем и предложив эти изменения в апстримный код.

Также для отечественных систем с локализованной версией UEFI разумно было бы встраивать ключи российских производителей и центра сертификации наряду с иностранными.

Список ссылок

1. UEFI SecureBoot mini-HOWTO (2013):
https://en.altlinux.org/UEFI_SecureBoot_mini-HOWTO

2. Инструкция по подписи UEFI-программ от Microsoft :
https://techcommunity.microsoft.com/t5/hardware-dev-center/updated-uefi-signing-requirements/ba-p/1062916

3. Рабочая площадка комитета shim-review:
https://github.com/rhboot/shim-review

4. Инцидент Boot Hole (2020)
https://eclypsium.com/2020/07/29/theres-a-hole-in-the-boot/

5. Инцидент SB Bypass2021 (BootHole2)
https://msrc.microsoft.com/update-guide/vulnerability/ADV200011

6. UEFI SB
http://www.rodsbooks.com/efi-bootloaders/secureboot.html

Спасибо за внимание!