Обновление Secure Boot UEFI с использованием сертификатов UEFI CA 2023

Введение

Безопасная загрузка (Secure Boot) — это функция безопасности, которая помогает гарантировать загрузку системы только с использованием программного обеспечения, которому доверяет производитель оборудования. Она является частью спецификации Unified Extensible Firmware Interface (UEFI) и предназначена для предотвращения загрузки несанкционированного программного обеспечения, драйверов и операционных систем во время процесса загрузки системы. Microsoft внедрила Secure Boot начиная с Windows 8, и теперь это является основным требованием безопасности для операционных систем Windows.

При запуске системы микропрограмма проверяет цифровые подписи программного обеспечения, предшествующего загрузке (включая диспетчер загрузки Windows), по набору доверенных центров сертификации (ЦС), хранящихся в микропрограмме системы. Если подписи действительны, система загружается, и микропрограмма передает управление загрузчику Windows, который, в свою очередь, проверяет необходимые компоненты, загружает их в память и запускает операционную систему. Этот процесс помогает гарантировать, что буткиты, руткиты или другое низкоуровневое вредоносное ПО не смогут быть загружены.

Функция Secure Boot обеспечивает первую линию защиты системы и безопасности Windows. Она основана на прошивке UEFI и использует иерархию ключей, чтобы гарантировать запуск системы в доверенном и проверенном состоянии каждый раз при включении.

Ниже приведены ключи, используемые для безопасной загрузки:

1. Ключ платформы (PK), устанавливающий права собственности на систему, обычно принадлежит производителю оборудования (OEM).
2. Ключ обмена ключами (KEK), который разрешает обновление доверенных баз данных и может включать в себя ключ обмена ключами от Microsoft и другие ключи обмена ключами от производителей оборудования (OEM).
3. База данных разрешенных подписей (DB), в которой хранятся подписи одобренных загрузчиков и драйверов.
4. База данных запрещенных подписей (DBX), содержащая список отозванных или вредоносных подписей.

В процессе загрузки микропрограмма проверяет цифровую подпись каждого компонента по этим базам данных, блокируя любой ненадежный или измененный код до загрузки операционной системы.

С момента первого внедрения поддержки Secure Boot в Windows Server 2012 и Windows 8 все устройства под управлением Windows используют один и тот же набор сертификатов Microsoft Secure Boot (CA 2011) в UEFI KEK и DB. Однако срок действия оригинальных сертификатов CA 2011 Secure Boot истекает в 2026 году, как указано в таблице сроков действия, приведенной ниже.

Сертификаты	Дата окончания	Новые сертификаты	Место хранения
Microsoft Corporation KEK CA 2011	Июнь 2026	Microsoft Corporation KEK CA 2023	KEK
Microsoft Windows Production PCA 2011	Октябрь 2026	Windows UEFI CA 2023	DB
Microsoft UEFI CA 2011	Июнь 2026	Microsoft UEFI CA 2023	DB
Microsoft UEFI CA 2011	Июнь 2026	Microsoft Option ROM CA 2023	DB

Для замены истекающих в 2026 году сертификатов Secure Boot, Microsoft начиная с 2025 года начала распространение обновлений для автоматической замены истекающих сертификатов Secure Boot UEFI. Возможно, вам потребуется принять меры и вручную инициировать обновление сертификатов Secure Boot и загрузчика Windows, пописанного сертификатами Windows CA 2023, чтобы обеспечить безопасность устройства с Windows по истечении срока действия сертификатов в 2026 году.

Ручное обновление сертификатов

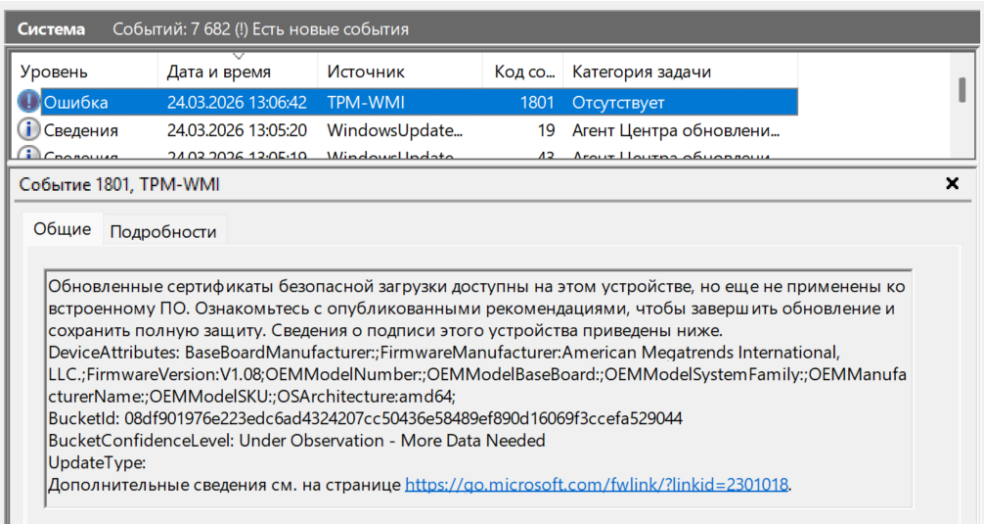
Microsoft автоматически доставляет обновления с новым сертификатами на все устройства с поддерживаемыми версиями Windows, и включенным режимом UEFI Secure Boot. Если вы регулярно ставите накопительные обновления, значит сертификаты уже скопированы на ваше устройство, но по умолчанию не активированы. Однако, вы можете вручную инициировать обновление сертификатов Secure Boot на своем Windows устройстве, не дожидаясь их автоматического развертывания. Это может понадобится разработчикам и системным администраторам, которые хотят протестировать работу какого-то специализированного ПО или оборудования, которое может затронуть обновление сертификатов UEFI CA 2023 и загрузчика.

> *Что будет, если не обновлять сертификаты Windows UEFI CA 2023?*
> *Если ваше устройство не получило обновления по какой-то причине, или используемые сертификаты не будут заменены до момента истечения срока действия предыдущих, это не вызовет проблем с загрузкой Windows или невозможностью использовать устройства со старыми сертификатами.* ***Перестанет работать только механизм доверенной загрузки Secure Boot****, делая компьютеры уязвимыми перед заражением буткитами.*

Первым шагом требуется установить все последние обновления безопасности через Центр обновления Windows. Ваша версия ОС Windows должна быть не ниже 23H2 (или Windows Server 2022 и выше), а также в BIOS включен параметр Secure Boot (Enabled).

1. Проверка статуса обновления

Если на компьютер доставлены обновления, которые содержат новые сертификаты Secure Boot, но еще не применены, в журнале System будет появляться ошибка от источника TPM-WMI с кодом 1801.



После установки обновлений безопасности, выпущенных после октября 2025 года, Microsoft добавила несколько ключей реестра, позволяющих контролировать статус обновления сертификатов Secure Boot.

Текущий статус обновления сертификатов можно узнать из ключа UEFICA2023Status:

```
Get-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Control\SecureBoot\Servicing\
-Name UEFICA2023Status | Select-Object UEFICA2023Status
```

Возможные значения:

- NotStarted – обновление не запущено
- InProgress – обновление запущено, или завершено либо добавление сертификата в UEFI или обновление загрузчика
- Updated – обновление полностью завершено. Обновлены как сертификаты, так и подпись загрузчика.

Перед обновлением сертификатов и загрузчика рекомендуется приостановить защиту BitLocker, либо убедиться, что у вас сохранен 48-значный ключ восстановления (в аккаунте Microsoft, можно хранить ключ восстановления BitLocker в AD, на внешнем носителе или распечатать).

2. Добавление новых сертификатов и обновление подписи загрузчика Windows

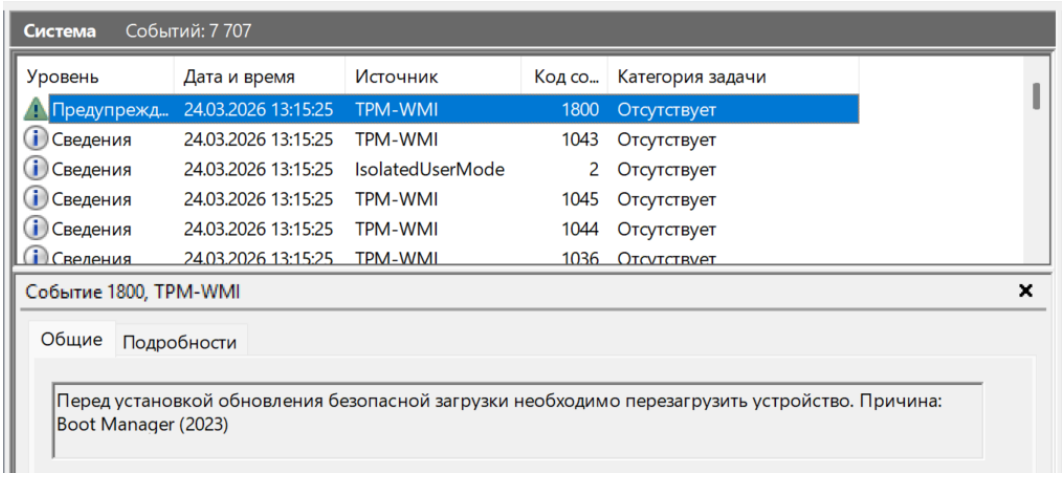
Чтобы разрешить установку новых сертификатов Secure Boot, измените значение параметра AvailableUpdates на 0x5944.

```
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecureBoot' -Name
'AvailableUpdates' -Value 0x5944
```

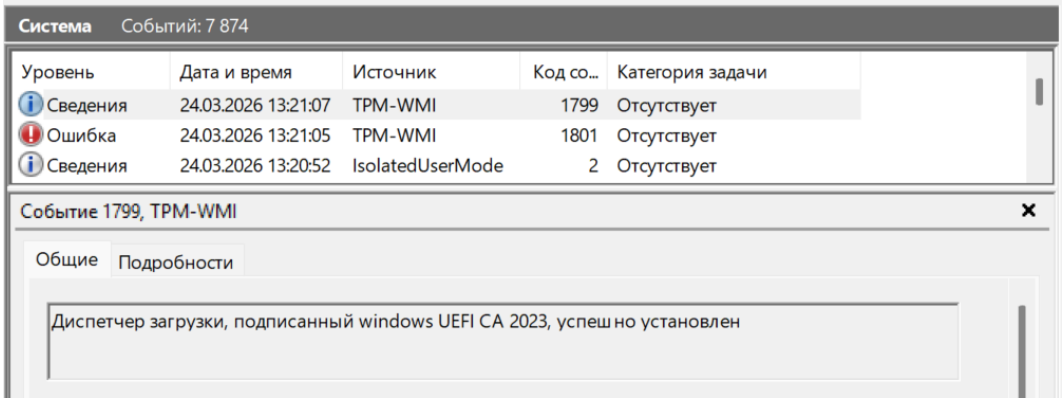
После этого запустите задание планировщика Secure-Boot-Update. Это запустит цепочку задач по замене сертификатов в UEFI и обновления загрузчика Windows.

```
Start-ScheduledTask -TaskName '\Microsoft\Windows\PI\Secure-Boot-Update'
```

Проверяйте в Event Viewer, когда обновление сертификатов будет завершено по событиям от TPM-WMI в журнале System. Компьютер потребует перезагрузки.

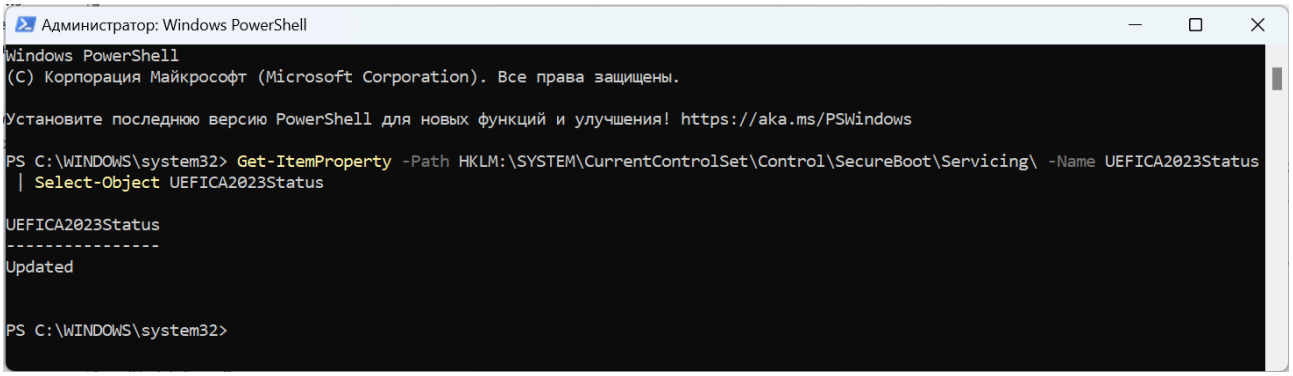


После перезагрузки еще раз запустите задание обновления Secure-Boot-Update. Контролируйте статус выполнения по событиям в Event Viewer.

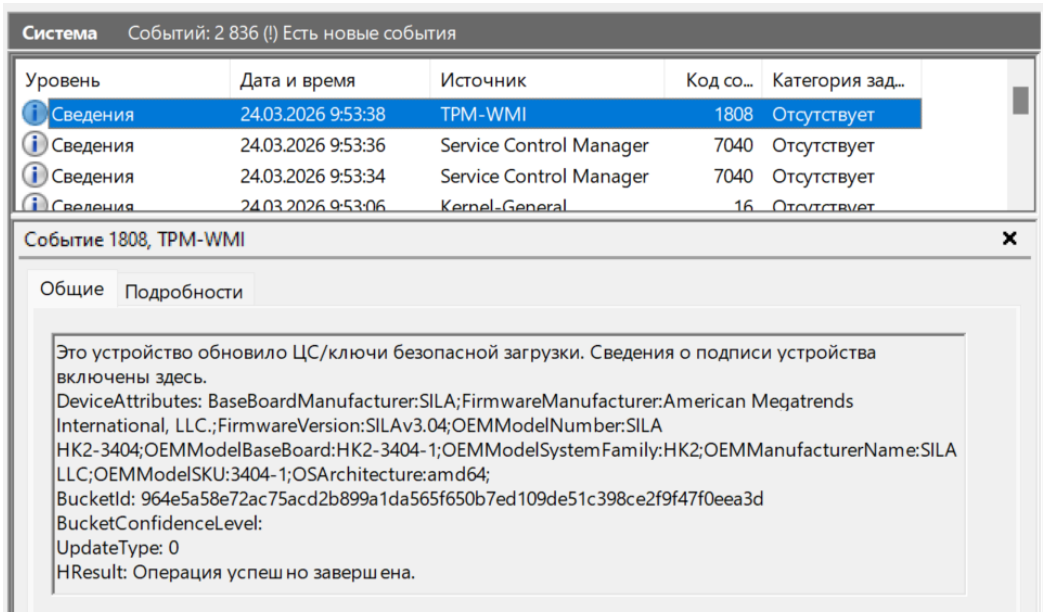


3. Проверка добавленных сертификатов и подписи загрузчика

После завершения обновления сертификатов проверьте, что значение UEFICA2023Status изменилось на Updated.



А также в Event Viewer вы получите запись события от TPM-WMI об успешном обновлении ЦС/ключей безопасной загрузки.



Убедиться, что установлены все сертификаты можно командами:

```
[System.Text.Encoding]::ASCII.GetString((Get-SecureBootUEFI DB).Bytes) -match 'Windows UEFI CA 2023'

[System.Text.Encoding]::ASCII.GetString((Get-SecureBootUEFI DB).Bytes) -match 'Microsoft UEFI CA 2023'

[System.Text.Encoding]::ASCII.GetString((Get-SecureBootUEFI KEK).Bytes) -match 'Microsoft Corporation KEK 2K CA 2023'
```

Если для каждой команды в выводе присутствует значение `True`, значит, сертификат включен.