



РусКрипто'2018

21-22 марта

Россия

Их нравы. Некоторые особенности применения криптографии в Intel ME 11

POSITIVE TECHNOLOGIES

ptsecurity.com

Максим Горячий

MGoryachy@ptsecurity.com

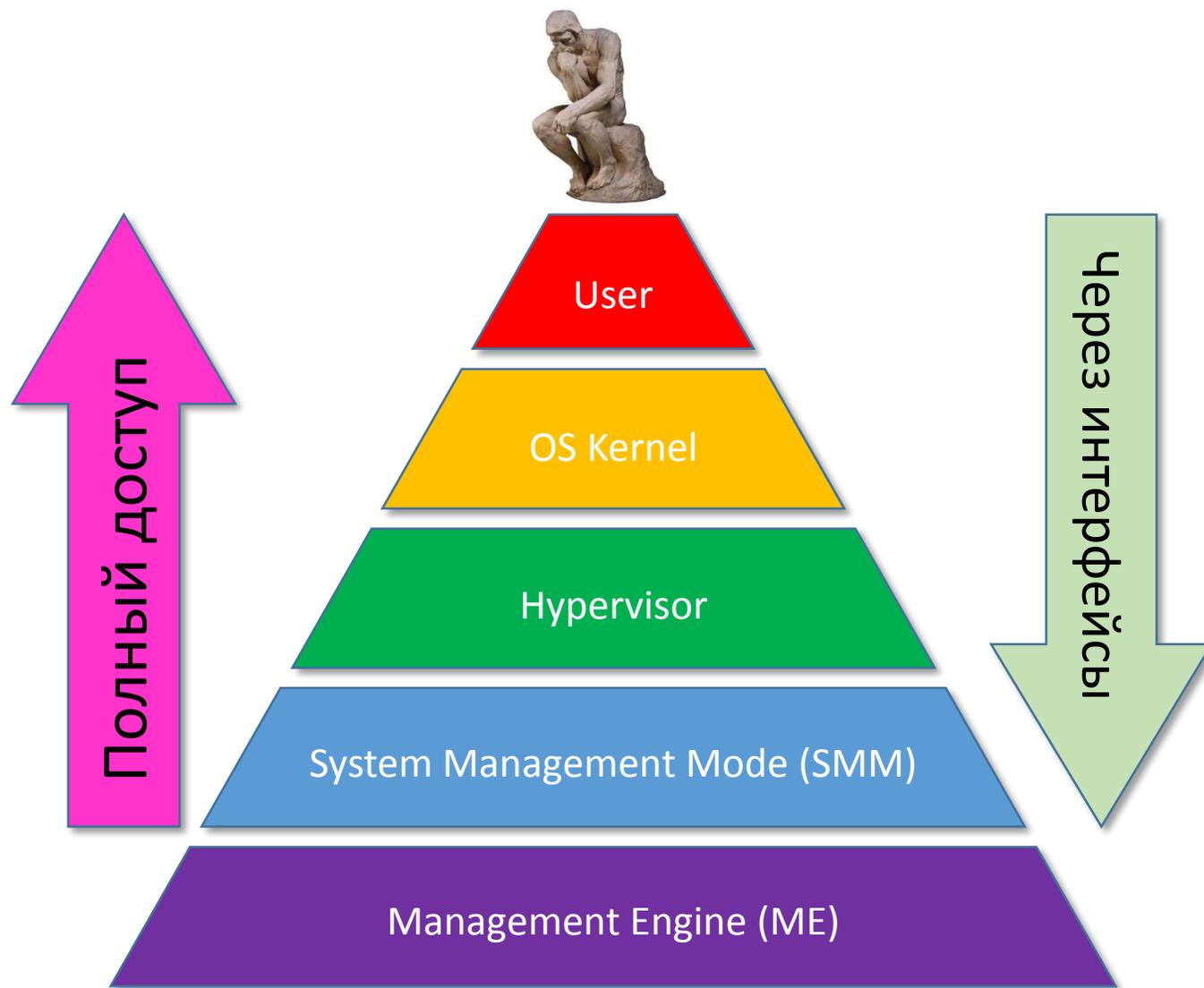
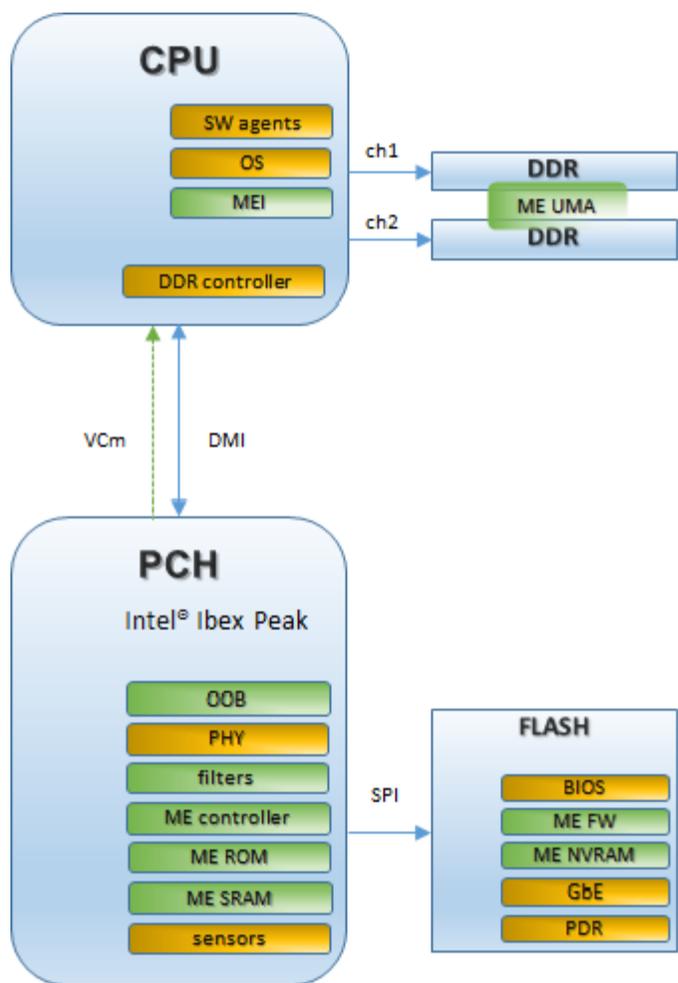
Марк Ермолов

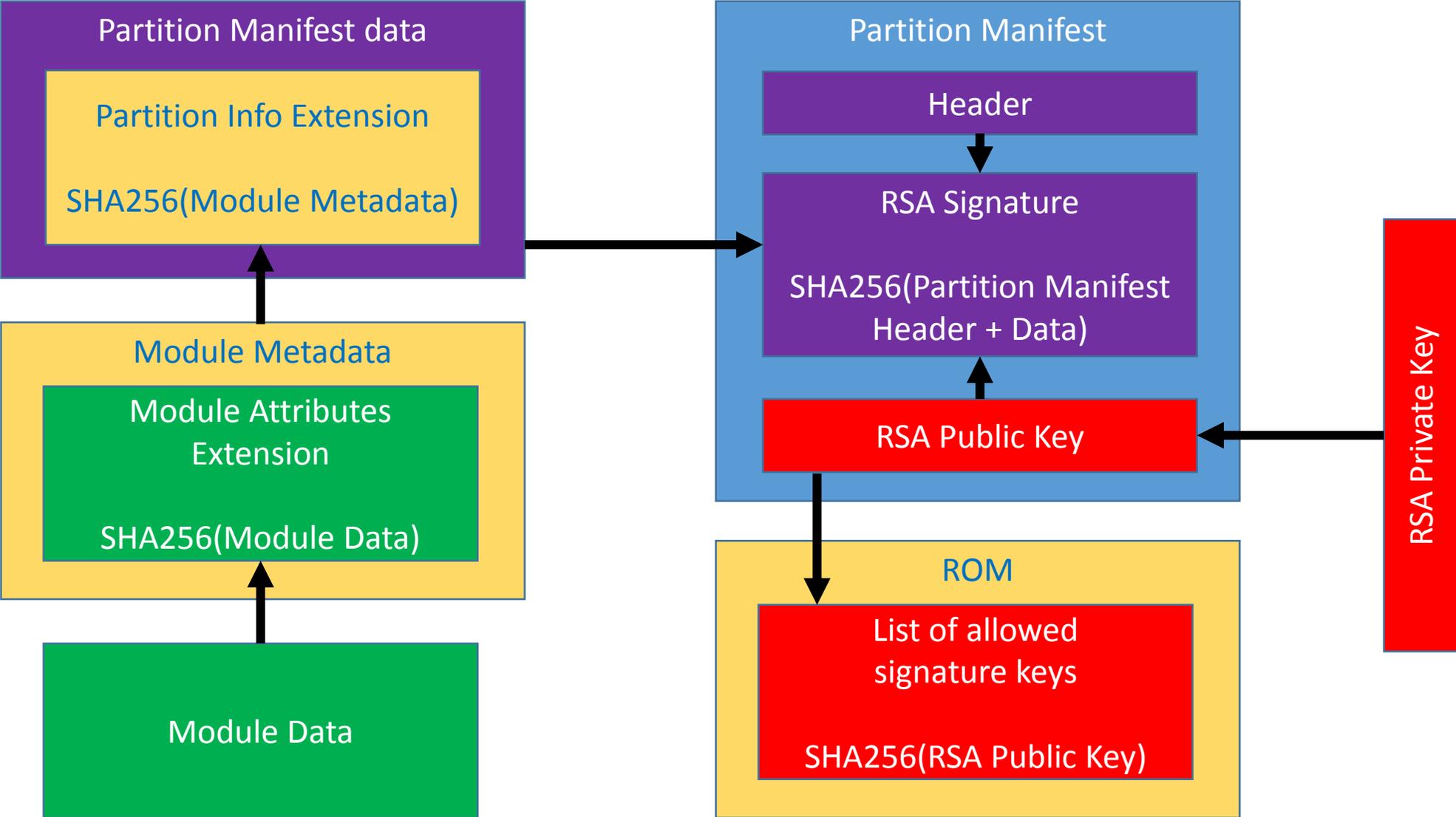
MErmolov@ptsecurity.com

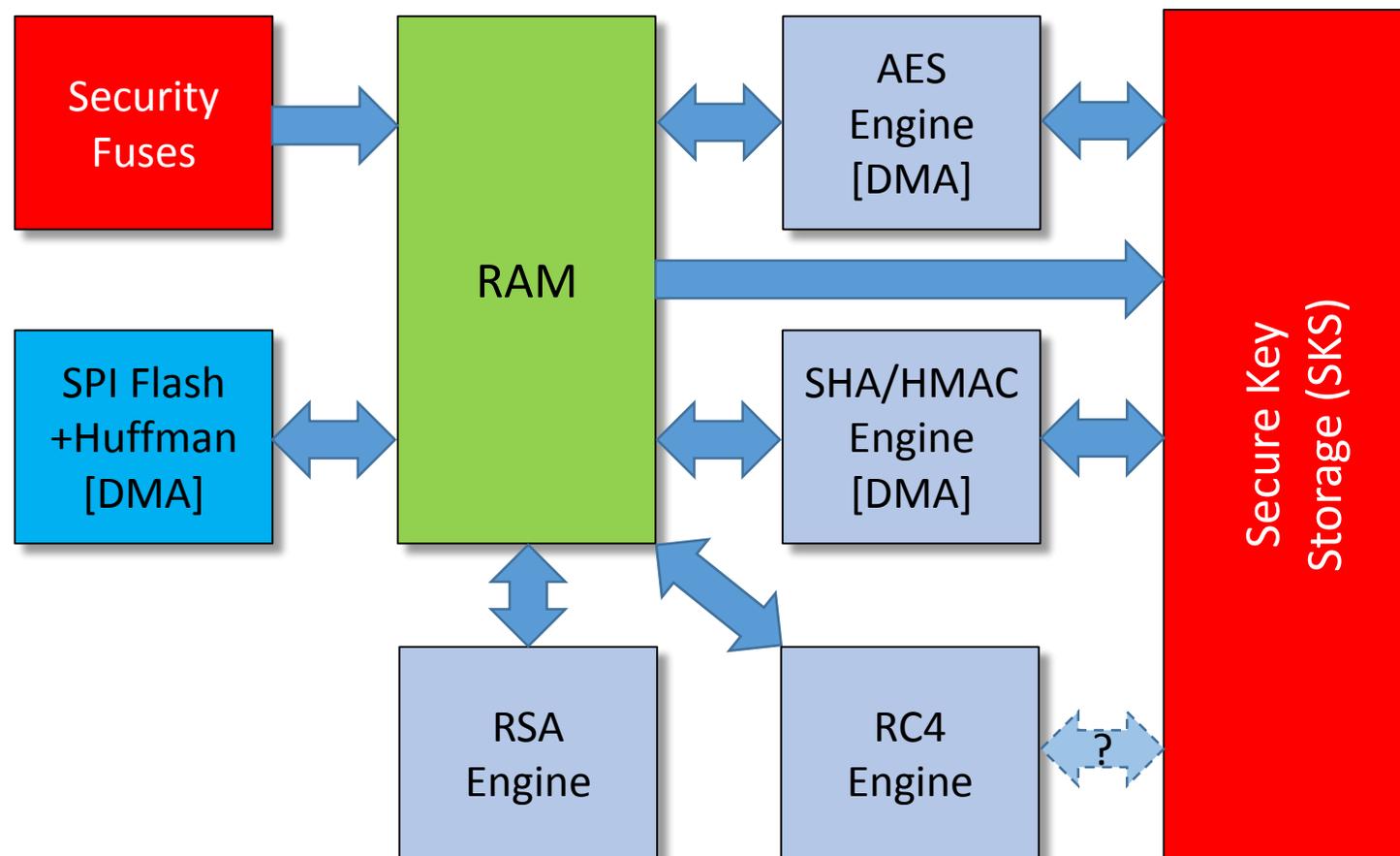
Дмитрий Скляр

DSklyarov@ptsecurity.com

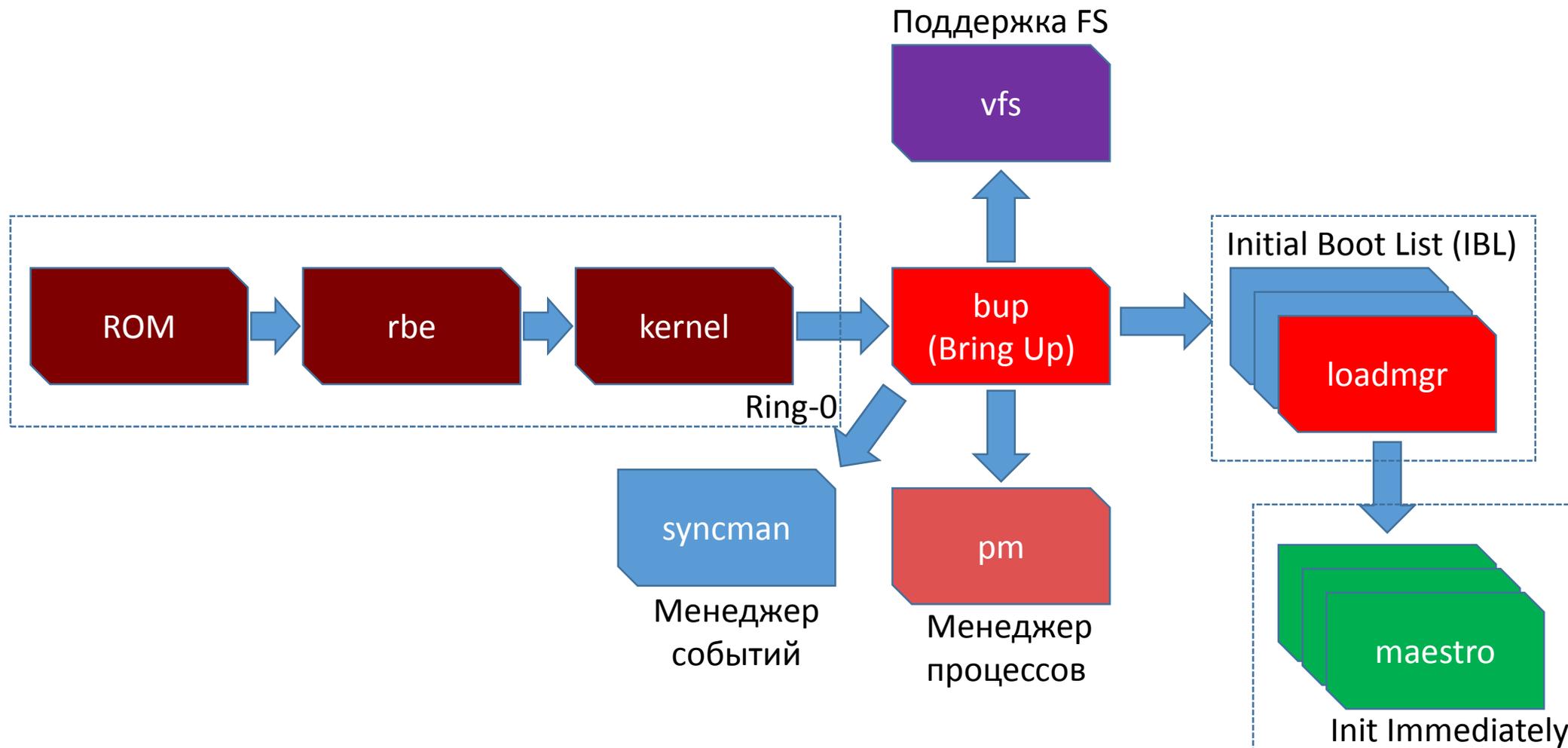
Архитектура Intel ME 6+







- Отображены в адресное пространство ME
- Доступны из режима ядра (ROM, rbe, kernel)
- Доступны приложениям ME, если в их манифесте прописаны соответствующие разрешения (доступ к RSA/AES/HMAC/SKS только у модулей `bu` и `crypto`)



- Содержит разделы BIOS/UEFI, GbE, ME, ...
- Хранит исполняемый код и настройки
- Может отображаться в память
- Имеет встроенный Huffman Decompressor (для кода модулей ME)

- Слоты 1..11 для 128-битовых, 12..21 для 256-битовых ключей
- Ключ может быть задан явно или взят из результата AES/HMAC
- Сохраненный ключ не может быть извлечен (только использован в связке с AES/HMAC)
- Существуют политики ключей (результат AES Encrypt можно положить в память, результат AES Decrypt – только в SKS)

- Поддерживаются ключи размером 128 и 256 бит
- Поддерживаются режимы ECB, CBC, CTR
- Ключ шифрования может быть задан явно или взят из SKS
- Данные могут передаваться явно или через DMA

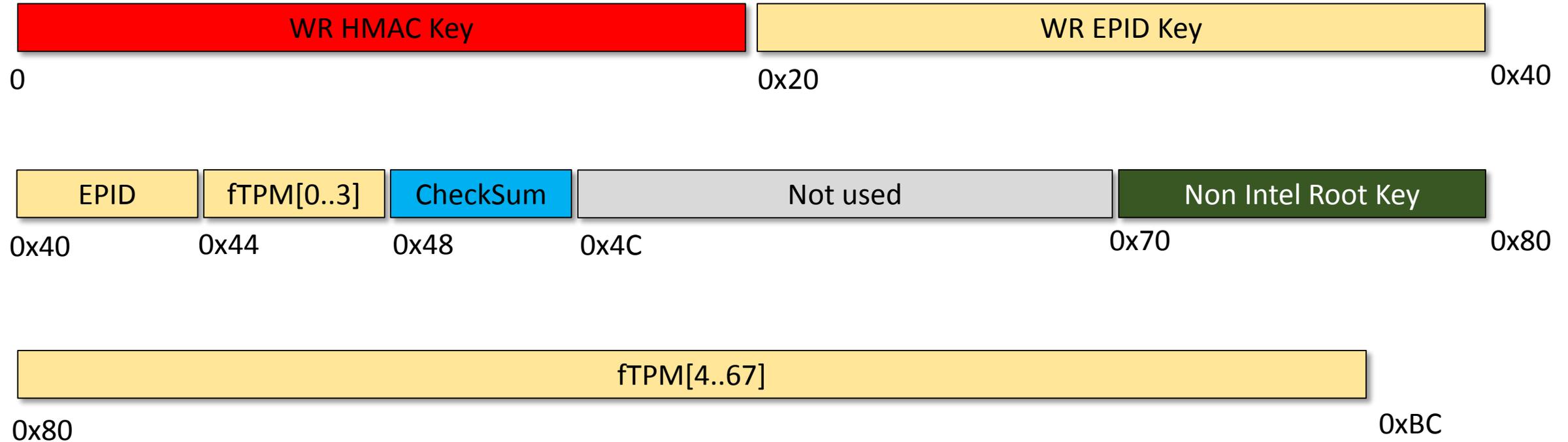
- Умеет вычислять SHA-1, SHA-256, SHA-384, SHA-512
- Поддерживаются ключи HMAC размером 128 и 256 бит
- Ключ HMAC может быть задан явно или взят из SKS
- Данные могут передаваться явно или через DMA
- Может работать в связке с AES

- Умеет выполнять модульное экспоненцирование
- Применяется в ROM (и не только) для проверки цифровой подписи
- Вероятно, используется приложениями ME

- Точно присутствует, но не исследовался нами
- Не используется для обеспечения безопасности собственно ME
- Вероятно, используется приложениями ME (для поддержки протоколов WiFi, SSL и т.п.)

- Инициализируются в процессе производства
- Не могут быть перезаписаны
- Доступны для чтения (после сброса платформы) только заданное число раз (обычно – 1)
- Частично блокируются в случае активации JTAG

Security Fuses (GEN)



Для обеспечения безопасности FS используется до 10 ключей

| | |
|---|---------------------------|
| Intel Integrity | Non-Intel Integrity |
| Текущие ключи (для текущего SVN [†]) | |
| Intel Confidentiality | Non-Intel Confidentiality |

| | |
|--|---------------------------|
| Intel Integrity | Non-Intel Integrity |
| Предыдущие* ключи (если существуют) | |
| Intel Confidentiality | Non-Intel Confidentiality |

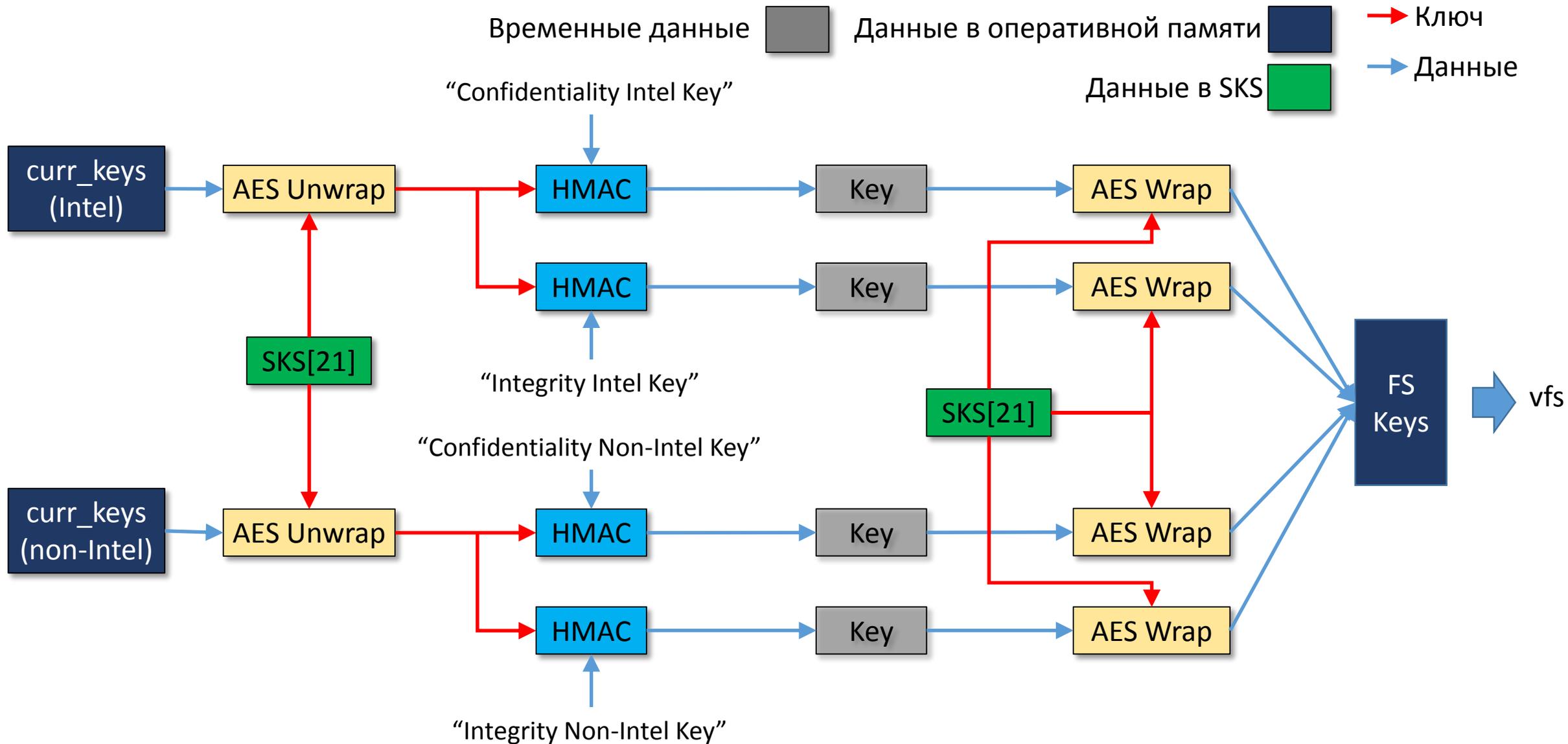
| | |
|-----------------|-----------------|
| RPMC HMAC #0 | RPMC HMAC #1 |
|-----------------|-----------------|

Replay-Protected Monotonic Counter (RPMC) может быть реализован в SPI Flash chip

*Предыдущие ключи вычисляются если $SVN > 1$ и раздел PSVN содержит валидные данные. Эти ключи используются для миграции файлов, созданных до обновления SVN.

[†]Secure Version Number (SVN) увеличивается в случае исправления серьезных уязвимостей для предотвращения отката к уязвимой версии

Генерация ключей файловой системы (bup)





Спасибо!

POSITIVE TECHNOLOGIES

ptsecurity.com