Доверенная загрузка

Антон Чуварин

Антон Чуварин

Старший инженер по разработке СнК
Команда логического дизайна, YADRO

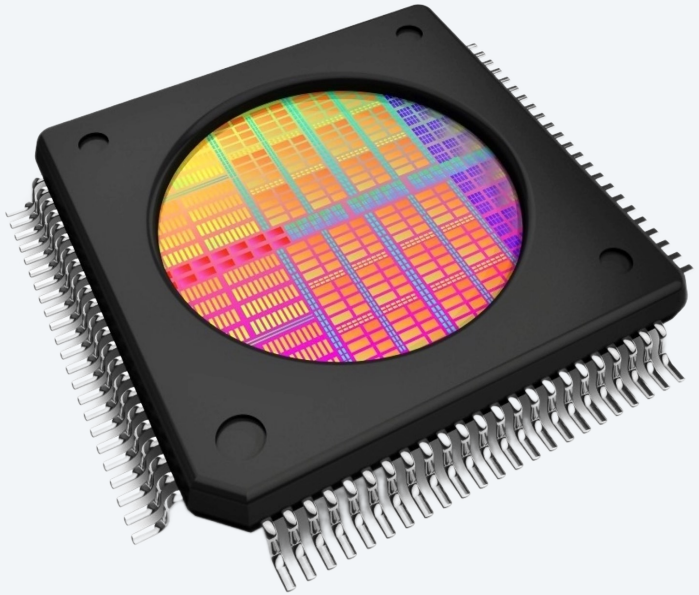
Система на кристалле

Синонимы СнК

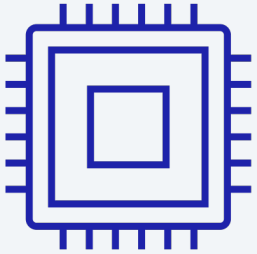
01 Чип

02 Процессор

03 SoC

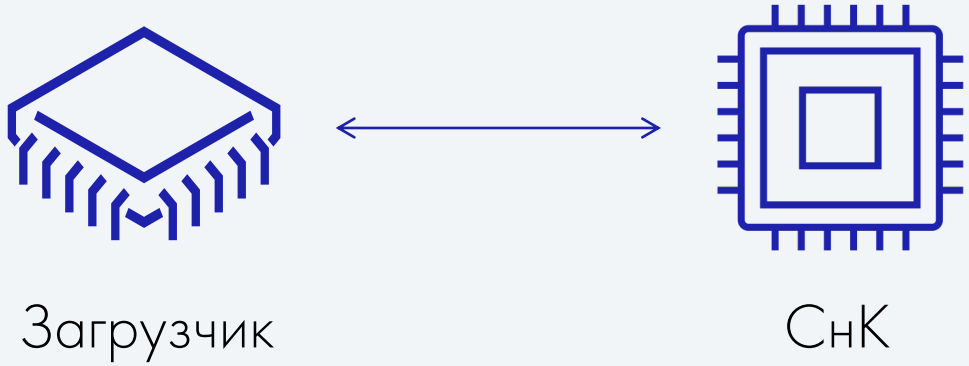


Процесс загрузки СнК



СнК

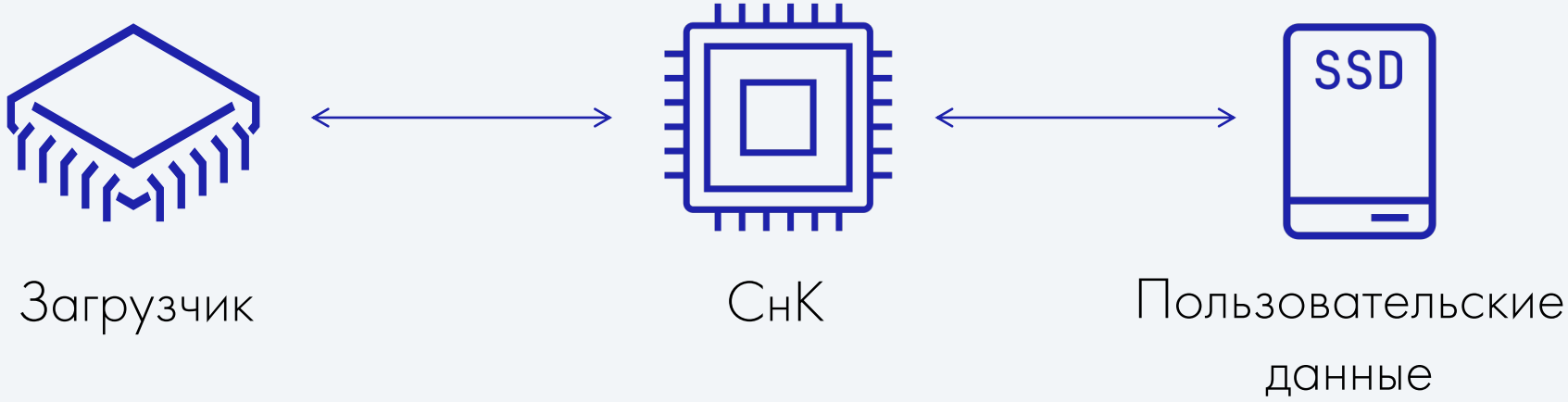
Процесс загрузки СнК



Загрузчик

- Инициализация СнК
- Поиск и передача управления загрузчику операционной системы

Процесс загрузки СнК



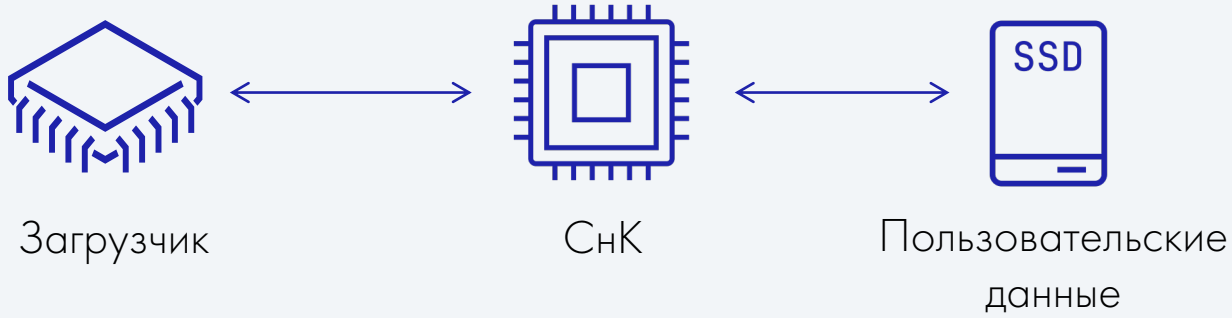
Загрузчик

- Инициализация СнК
- Поиск и передача управления загрузчику операционной системы

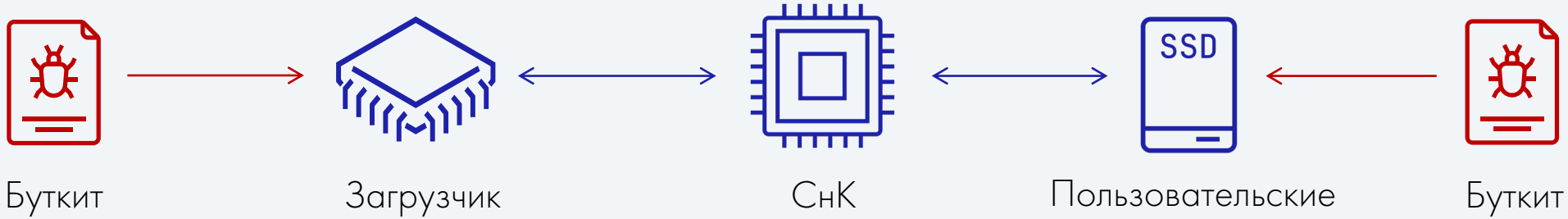
Пользовательские данные

- Загрузчик операционной системы
- Операционная система

От чего защищаемся?



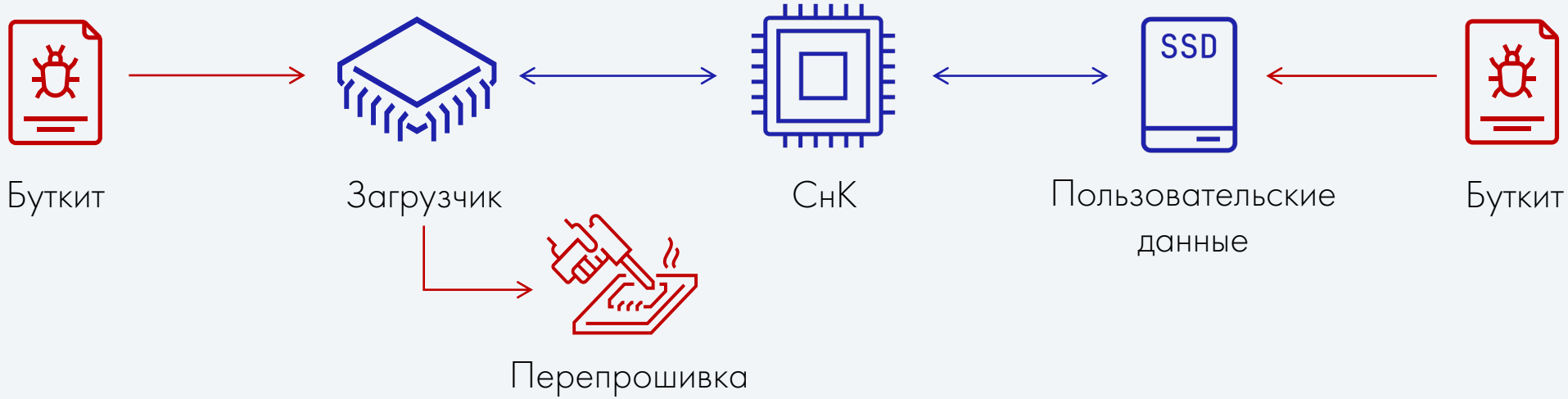
От чего защищаемся?



Необходима защита от атак

- Программные атаки

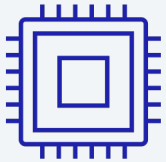
От чего защищаемся?



Необходима защита от атак

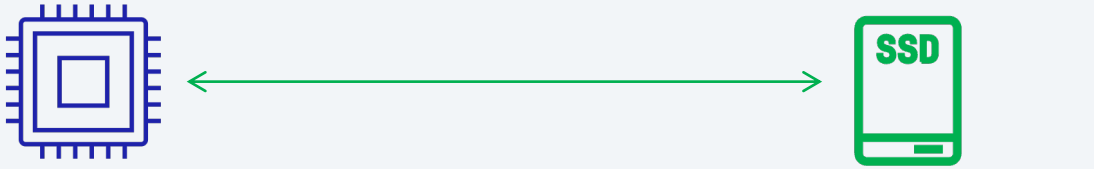
- Программные атаки
- Усложнение атак при наличии физического доступа

Что защищаем?



СнК

Что защищаем?



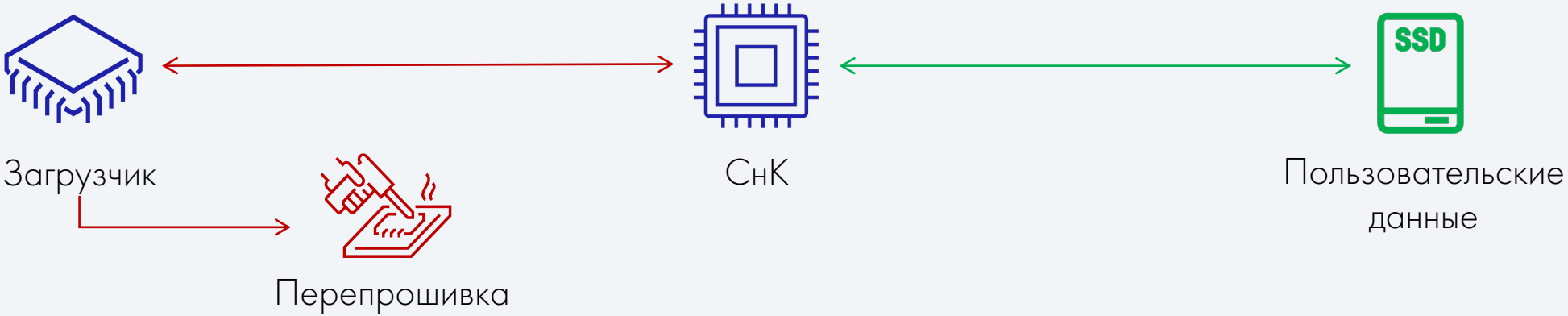
СнК

Пользовательские данные

Операционная система

- Загрузка ОС может быть защищена с помощью механизма «secure boot». Принцип отражен в стандарте **«Unified Extensible Firmware Interface (UEFI) Specification»**
- ОС защищена встроенными средствами или специализированным ПО

Что защищаем?



Загрузчик

- Необходима защита для случаев обновления программного обеспечения
- Необходима защита для случаев взлома ОС
- Защита от подмены ключа извне

Операционная система

- Загрузка ОС может быть защищена с помощью механизма «secure boot». Принцип отражен в стандарте **«Unified Extensible Firmware Interface (UEFI) Specification»**
- ОС защищена встроенными средствами или специализированным ПО

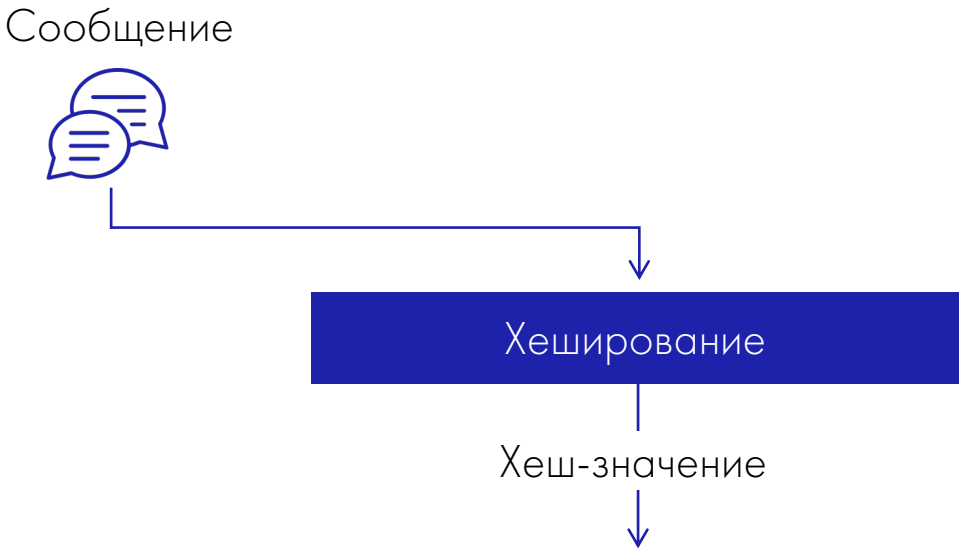
Основа безопасности

Сообщение

Цифровая подпись

- Хеш-функция
- RSA алгоритм

Основа безопасности



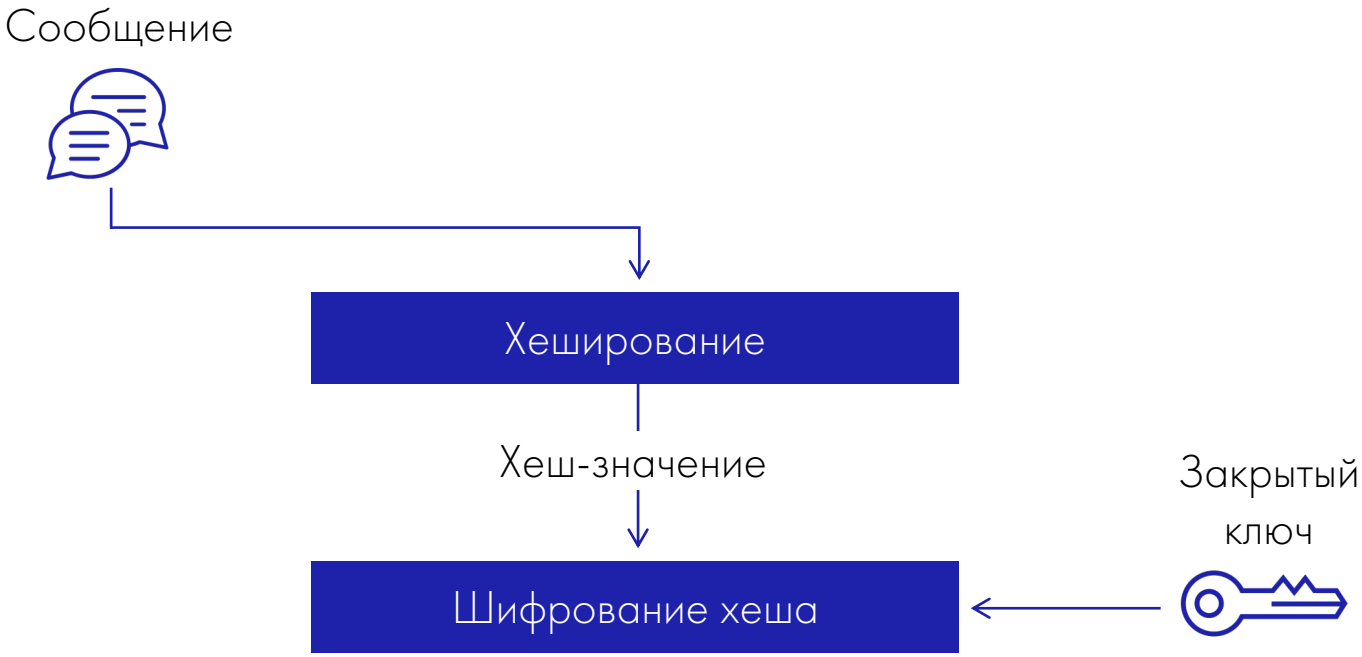
Цифровая подпись

- Хеш-функция
- RSA алгоритм

Свойства хеш-функции

- Изменение исходного сообщения значительно изменяет значение функции
- Низкая вероятность нахождения коллизии

Основа безопасности



Цифровая подпись

- Хеш-функция
- RSA алгоритм

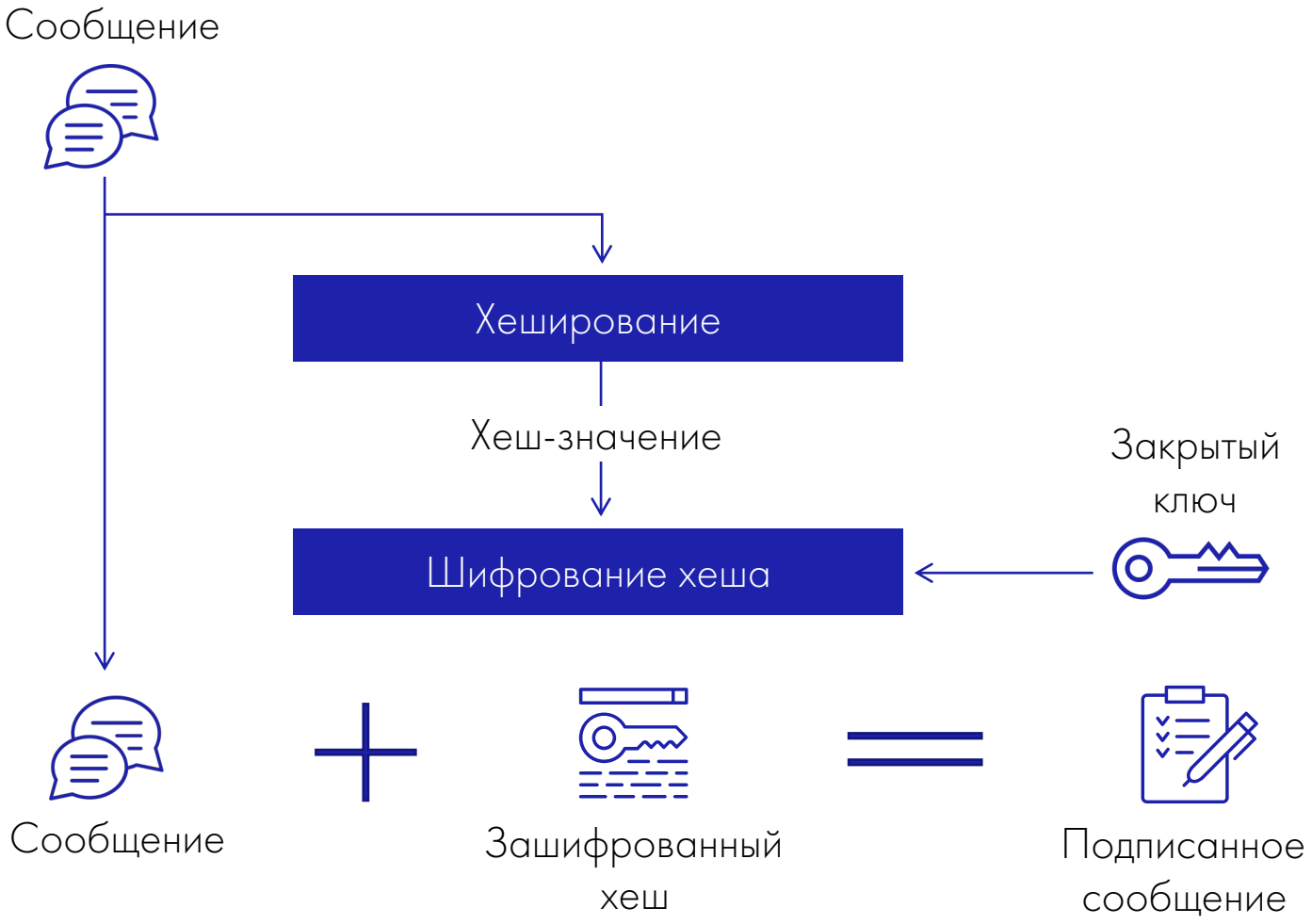
Свойства хеш-функции

- Изменение исходного сообщения значительно изменяет значение функции
- Низкая вероятность нахождения коллизии

Свойства RSA (Ривест, Шамир, Адлеман)

- Односторонняя функция
- Открытый и закрытый ключи

Основа безопасности



Цифровая подпись

- Хеш-функция
- RSA алгоритм

Свойства хеш-функции

- Изменение исходного сообщения значительно изменяет значение функции
- Низкая вероятность нахождения коллизии

Свойства RSA (Ривест, Шамир, Адлеман)

- Односторонняя функция
- Открытый и закрытый ключи

Основа безопасности

Подписанное сообщение

Цифровая подпись

- Хеш-функция
- RSA алгоритм

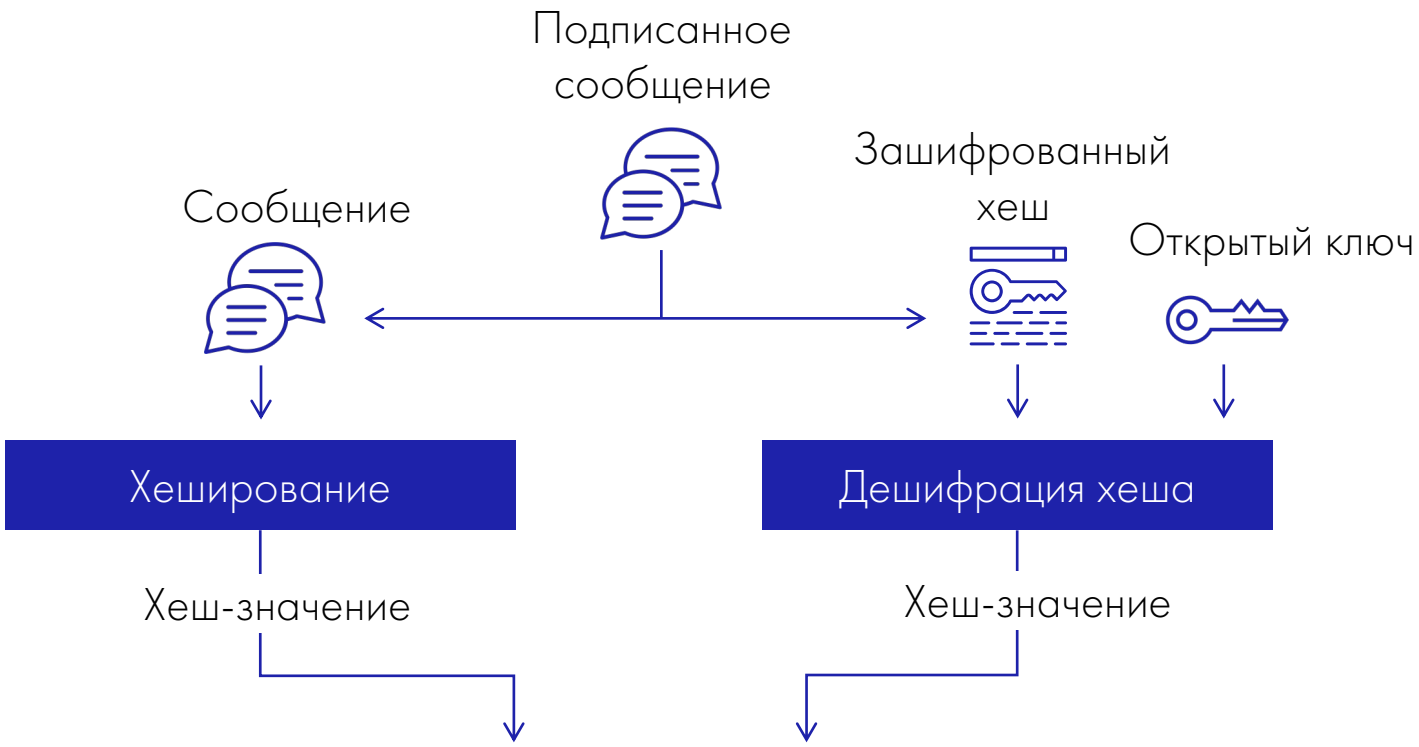
Свойства хеш-функции

- Изменение исходного сообщения значительно изменяет значение функции
- Низкая вероятность нахождения коллизии

Свойства RSA (Ривест, Шамир, Адлеман)

- Односторонняя функция
- Открытый и закрытый ключи

Основа безопасности



Цифровая подпись

- Хеш-функция
- RSA алгоритм

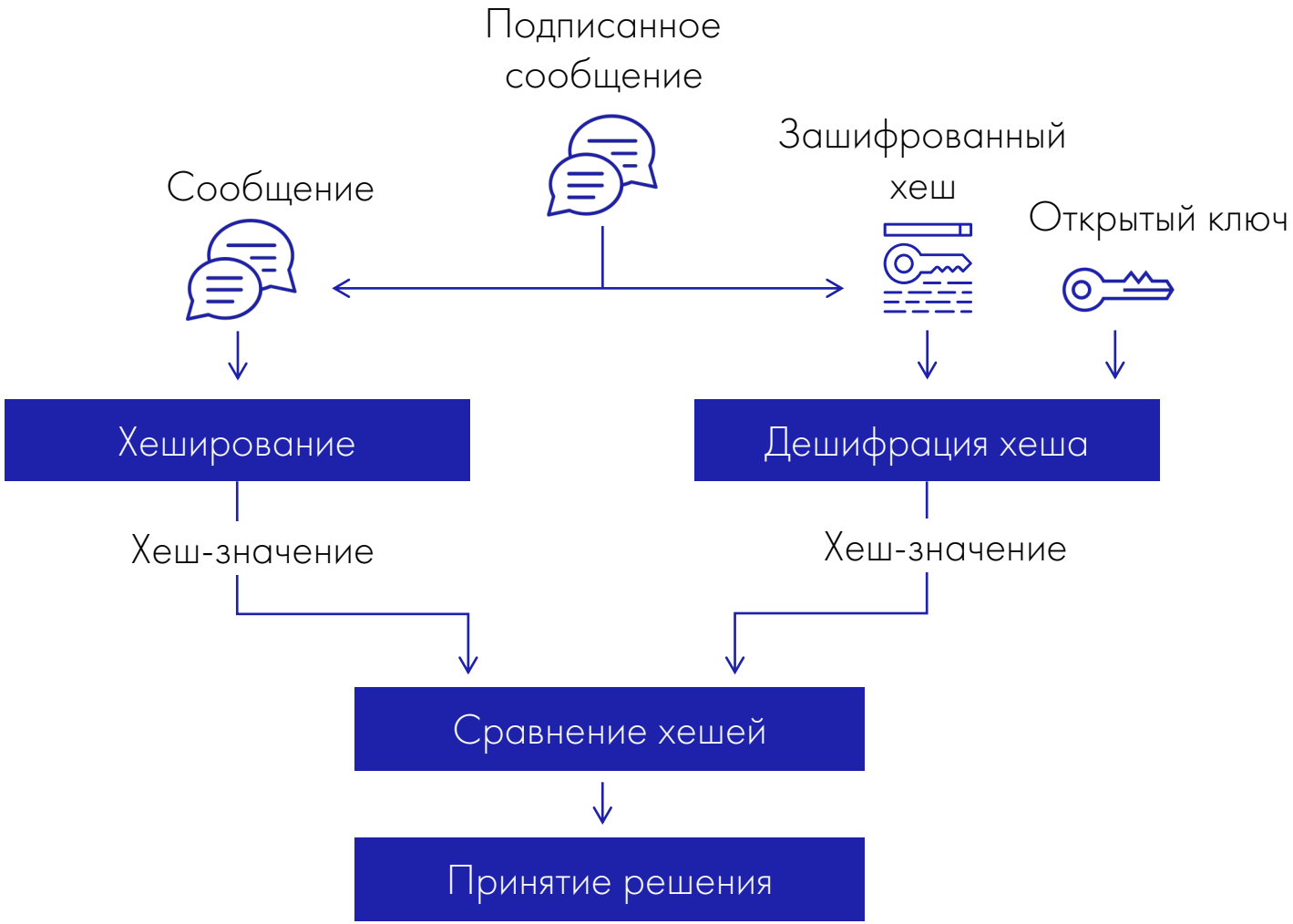
Свойства хеш-функции

- Изменение исходного сообщения значительно изменяет значение функции
- Низкая вероятность нахождения коллизии

Свойства RSA (Ривест, Шамир, Адлеман)

- Односторонняя функция
- Открытый и закрытый ключи

Основа безопасности



Цифровая подпись

- Хеш-функция
- RSA алгоритм

Свойства хеш-функции

- Изменение исходного сообщения значительно изменяет значение функции
- Низкая вероятность нахождения коллизии

Свойства RSA (Ривест, Шамир, Адлеман)

- Односторонняя функция
- Открытый и закрытый ключи

Надежность RSA и SHA. Рекомендации NIST

Уровень безопасности	RSA
<80	K=1024
112	K=2048
128	K=3072
148	K=4096
192	K=7680
256	K=15360

Уровень безопасности		К 2030	2031 и далее
<112	Применение для шифрования	Не допускается	
	Обработка зашифрованных данных	В режиме поддержки	
112	Применение для шифрования	Допускается	Не допускается
	Обработка зашифрованных данных	Допускается	В режиме поддержки
128	Применение для шифрования и обработка зашифрованных данных	Допускается	Допускается
192		Допускается	Допускается
256		Допускается	Допускается

Надежность RSA и SHA. Рекомендации NIST

Уровень безопасности	RSA
<80	K=1024
112	K=2048
128	K=3072
148	K=4096
192	K=7680
256	K=15360

Уровень безопасности		К 2030	2031 и далее
<112	Применение для шифрования	Не допускается	
	Обработка зашифрованных данных	В режиме поддержки	
112	Применение для шифрования	Допускается	Не допускается
	Обработка зашифрованных данных	Допускается	В режиме поддержки
128	Применение для шифрования и обработка зашифрованных данных	Допускается	Допускается
192		Допускается	Допускается
256		Допускается	Допускается

Время для взлома алгоритма

$T=2^{(\text{Уровень безопасности}-1)}*(\text{Время шифрования и сопоставления})=$

$2^{(147)}*10^{-9}$ с $=1.8*10^{(35)}$ с $=5.6*10^{(27)}$ лет

Надежность RSA и SHA. Рекомендации NIST

Уровень безопасности	Хеш-функция цифровой подписи
<80	SHA-1
112	SHA-224
128	SHA-256
192	SHA-384
256	SHA-512

Уровень безопасности		К 2030	2031 и далее
<112	Применение для шифрования	Не допускается	
	Обработка зашифрованных данных	В режиме поддержки	
112	Применение для шифрования	Допускается	Не допускается
	Обработка зашифрованных данных	Допускается	В режиме поддержки
128	Применение для шифрования и обработка зашифрованных данных	Допускается	Допускается
192		Допускается	Допускается
256		Допускается	Допускается

Надежность RSA и SHA. Рекомендации NIST

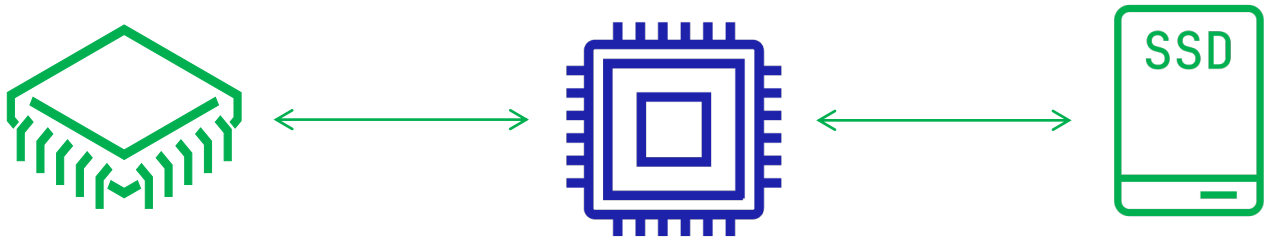
Уровень безопасности	Хеш-функция цифровой подписи
<80	SHA-1
112	SHA-224
128	SHA-256
192	SHA-384
256	SHA-512

Уровень безопасности		К 2030	2031 и далее
<112	Применение для шифрования	Не допускается	
	Обработка зашифрованных данных	В режиме поддержки	
112	Применение для шифрования	Допускается	Не допускается
	Обработка зашифрованных данных	Допускается	В режиме поддержки
128	Применение для шифрования и обработка зашифрованных данных	Допускается	Допускается
192		Допускается	Допускается
256		Допускается	Допускается

Время для взлома алгоритма

$T=2^{(\text{Уровень безопасности}-1)}*(\text{Время хеширования и сопоставления})=$
$2^{(191)}*10^{(-9)}\ с=3.1*10^{(48)}\ с=9.9*10^{(40)}$ лет

Загрузчик и ключи

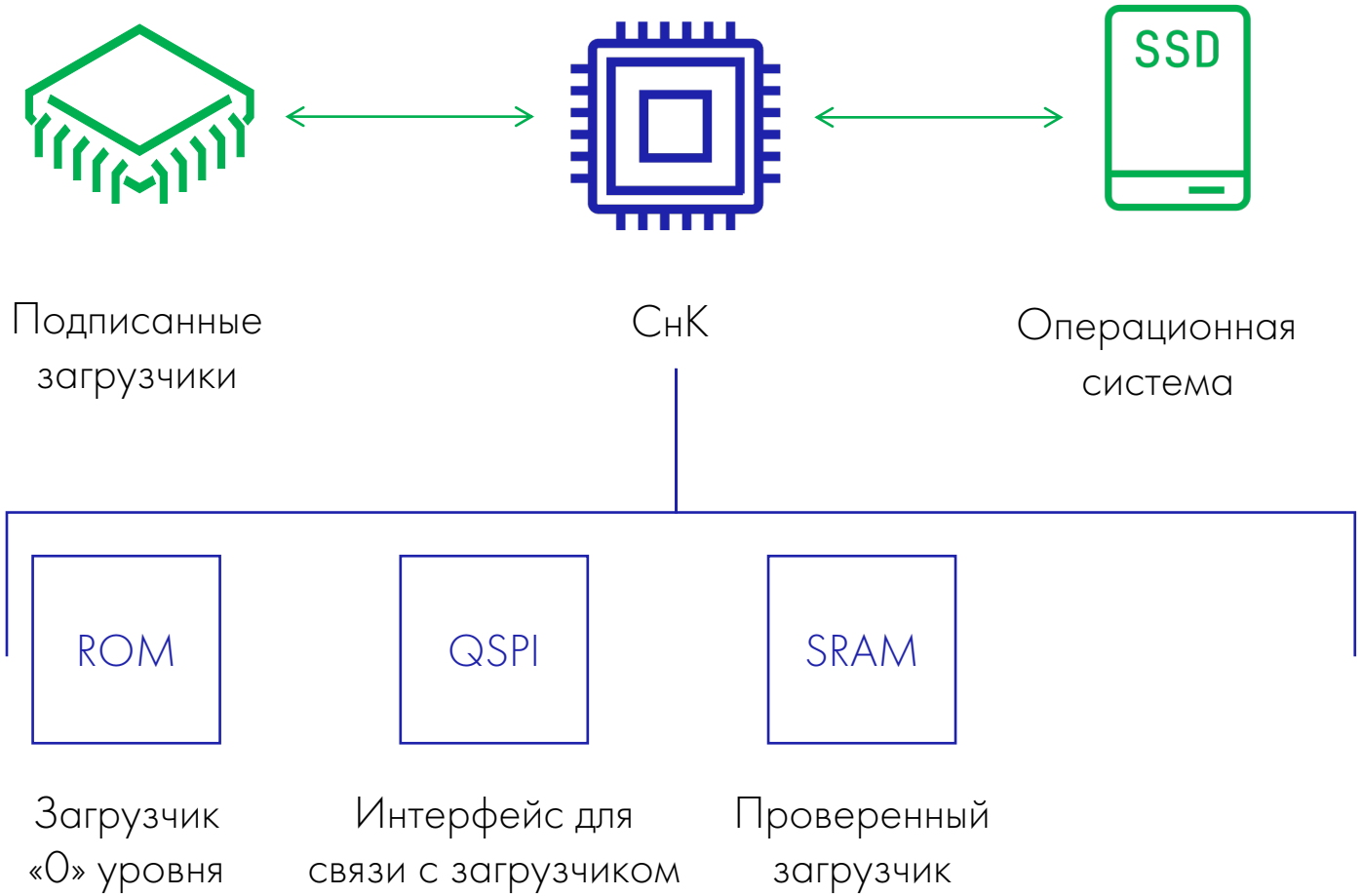


Подписанные загрузчики

СнК

Операционная система

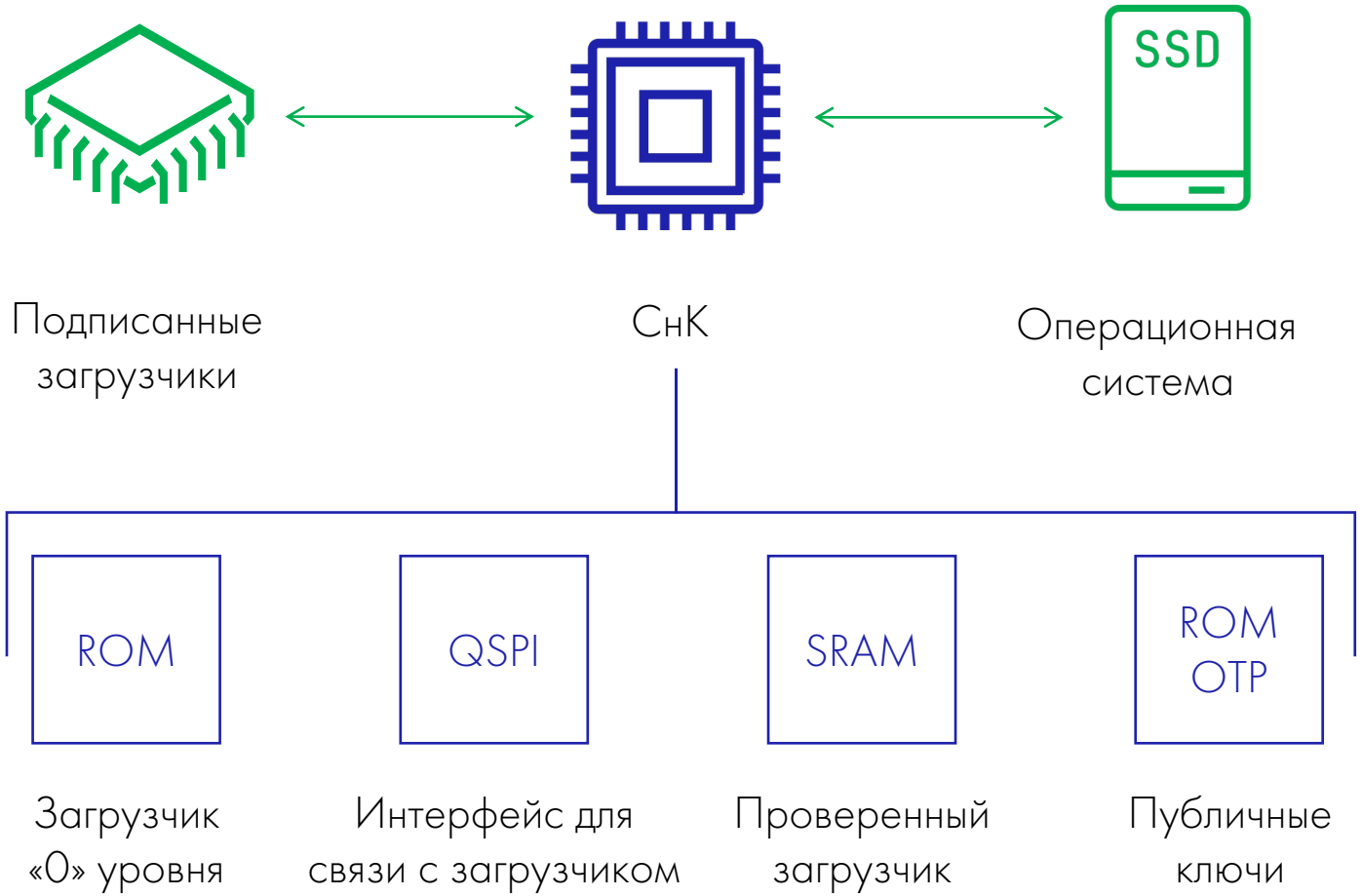
Загрузчик и ключи



Загрузчик

- Разделяется на несколько уровней
- Загрузчик нулевого уровня не должен изменяться
- Загрузчик нулевого уровня содержит минимальный размер кода
- Необходим интерфейс для связи с остальными частями загрузчика
- Необходима память для хранения проверенных частей загрузчика

Загрузчик и ключи



Загрузчик

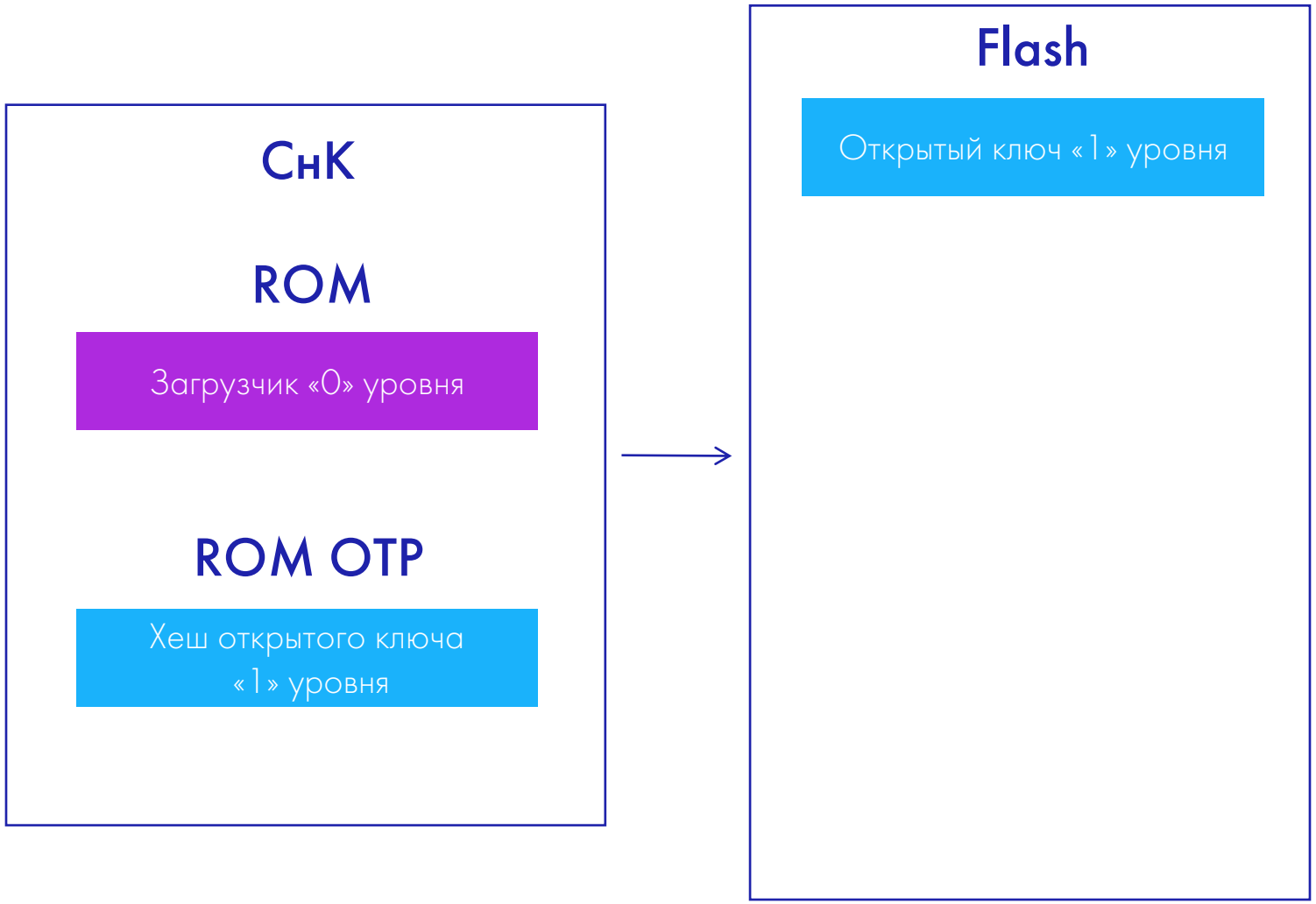
- Разделяется на несколько уровней
- Загрузчик нулевого уровня не должен изменяться
- Загрузчик нулевого уровня содержит минимальный размер кода
- Необходим интерфейс для связи с остальными частями загрузчика
- Необходима память для хранения проверенных частей загрузчика

Публичный ключ и ROM OTP

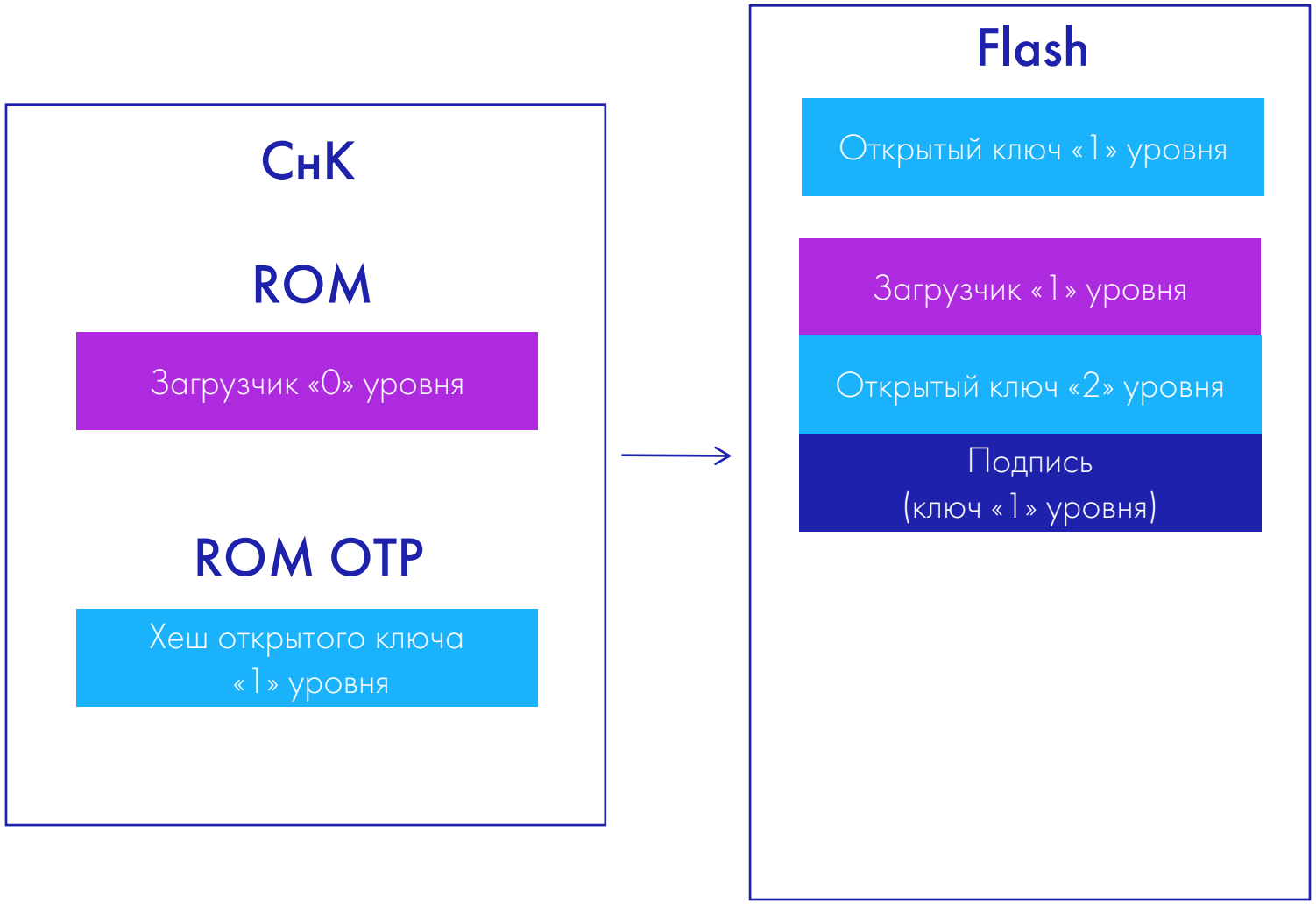
- Защищен от доступа со стороны
- Возможность замены ключа
- Хранение отозванных ключей

Цепь доверия

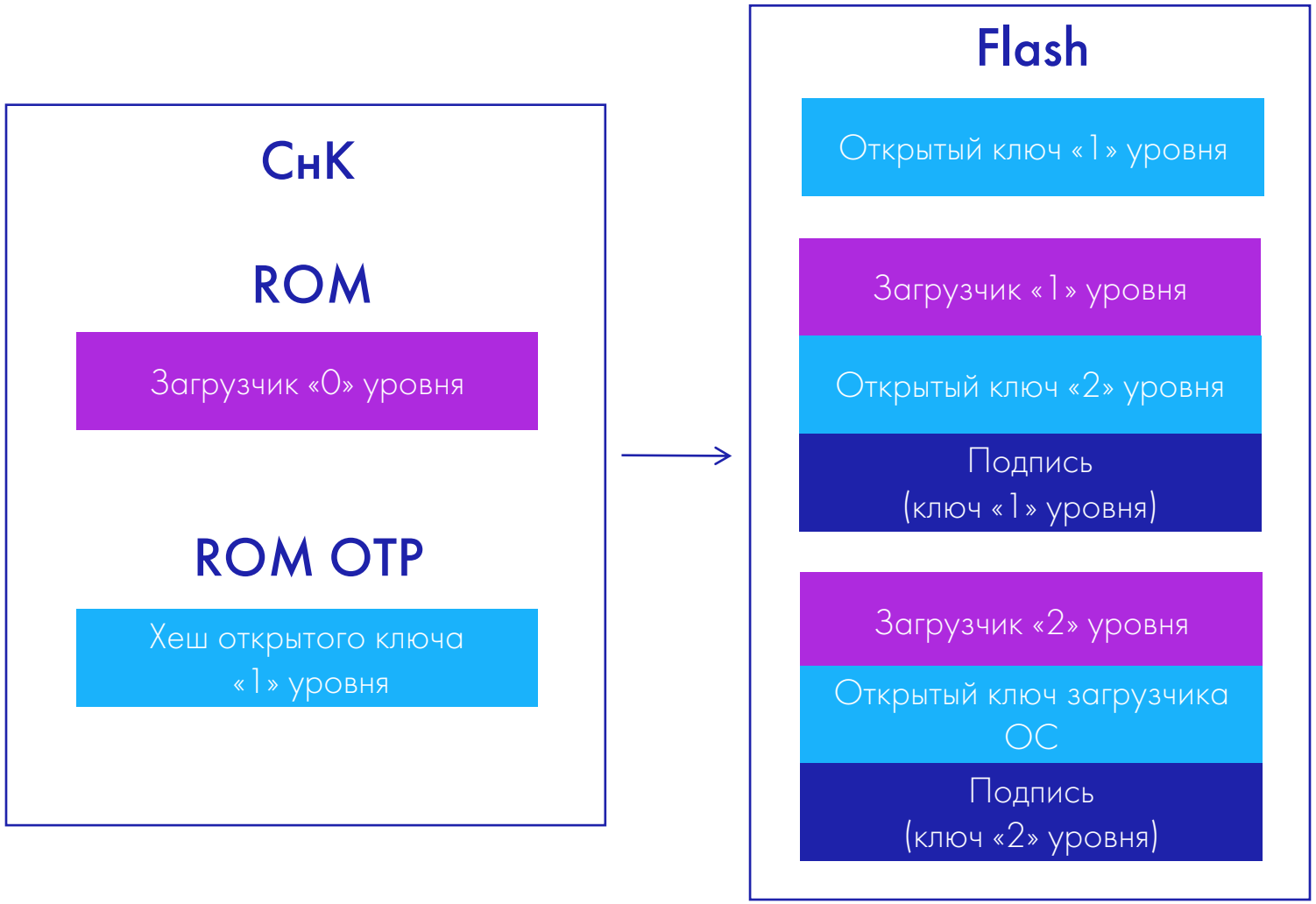
Цепь доверия



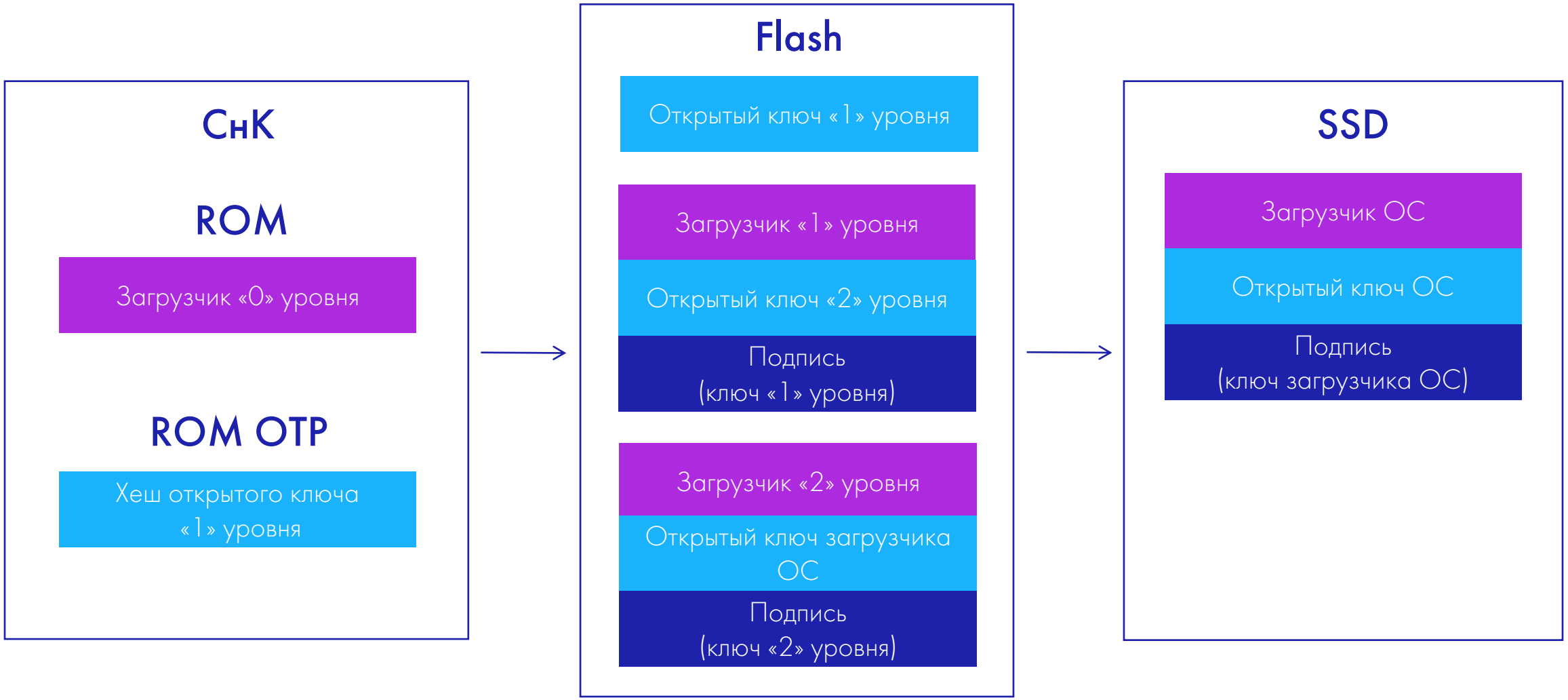
Цепь доверия



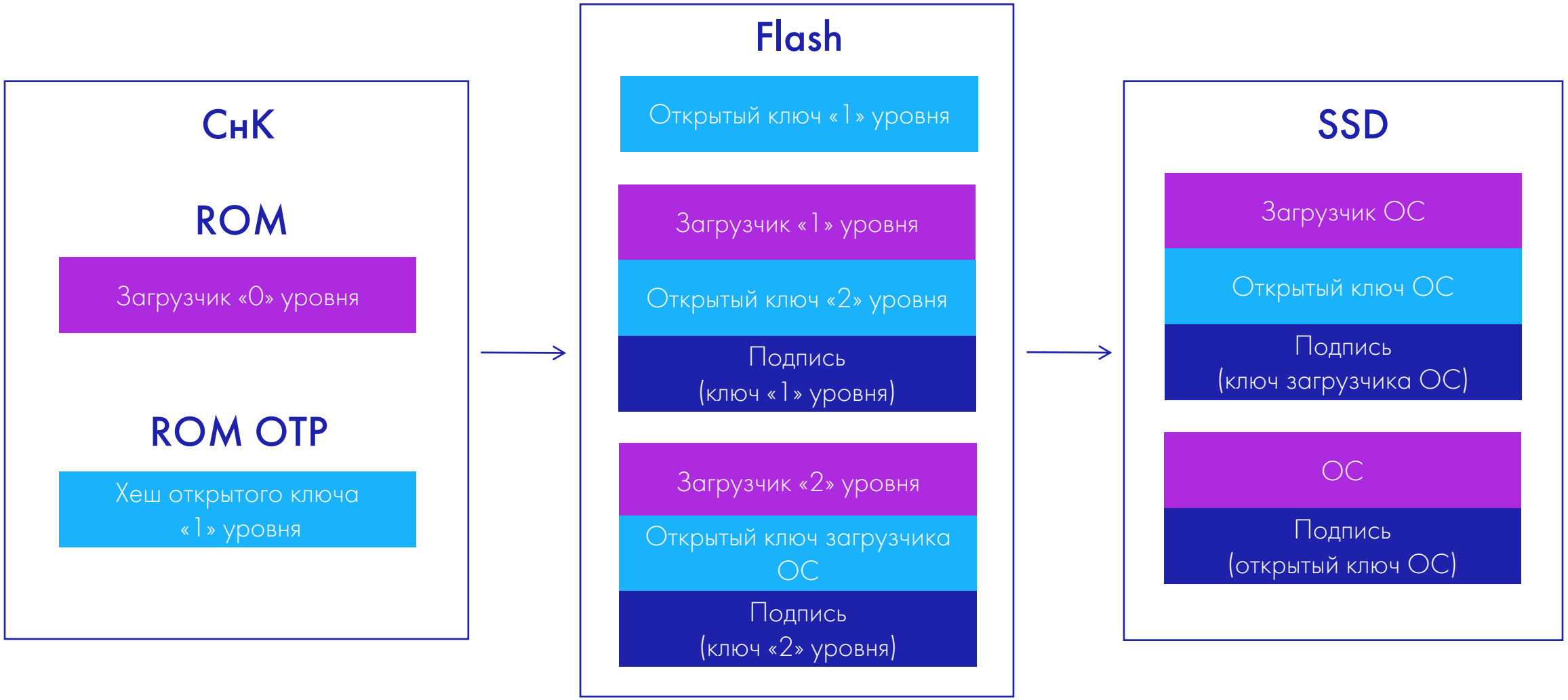
Цепь доверия



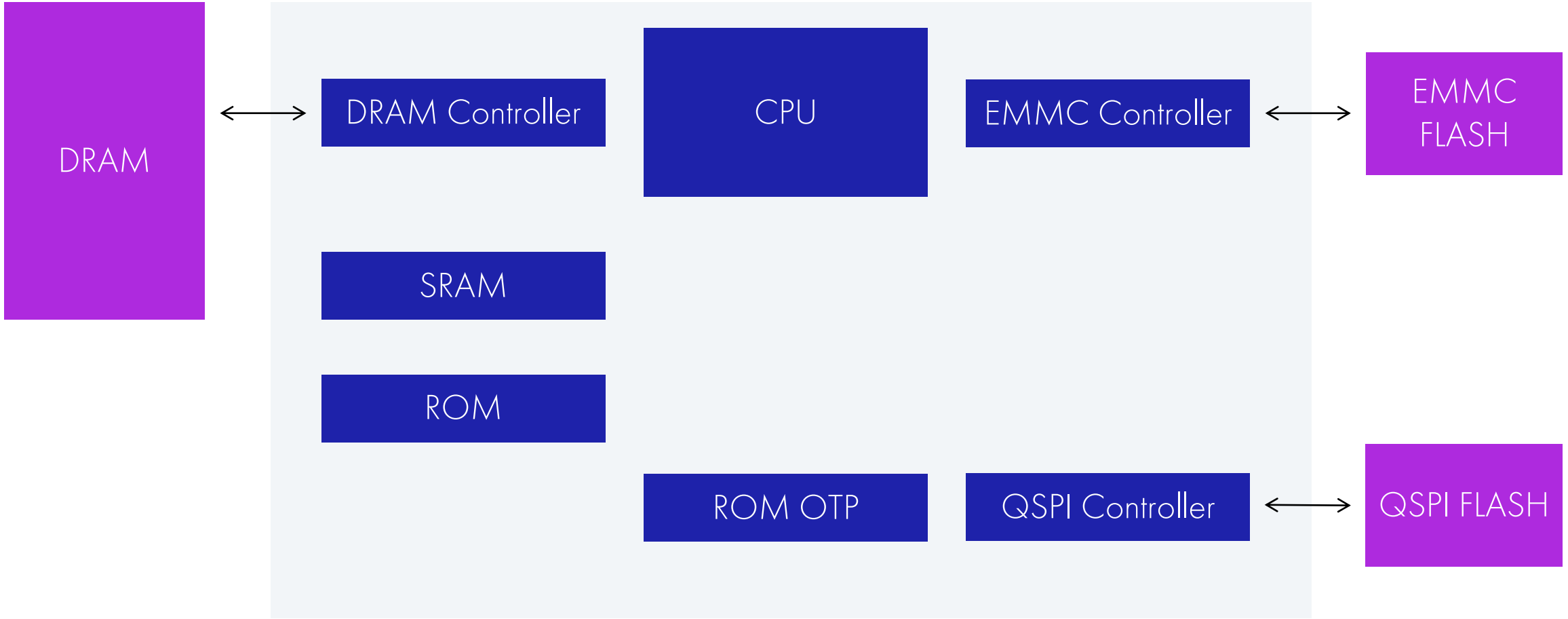
Цепь доверия



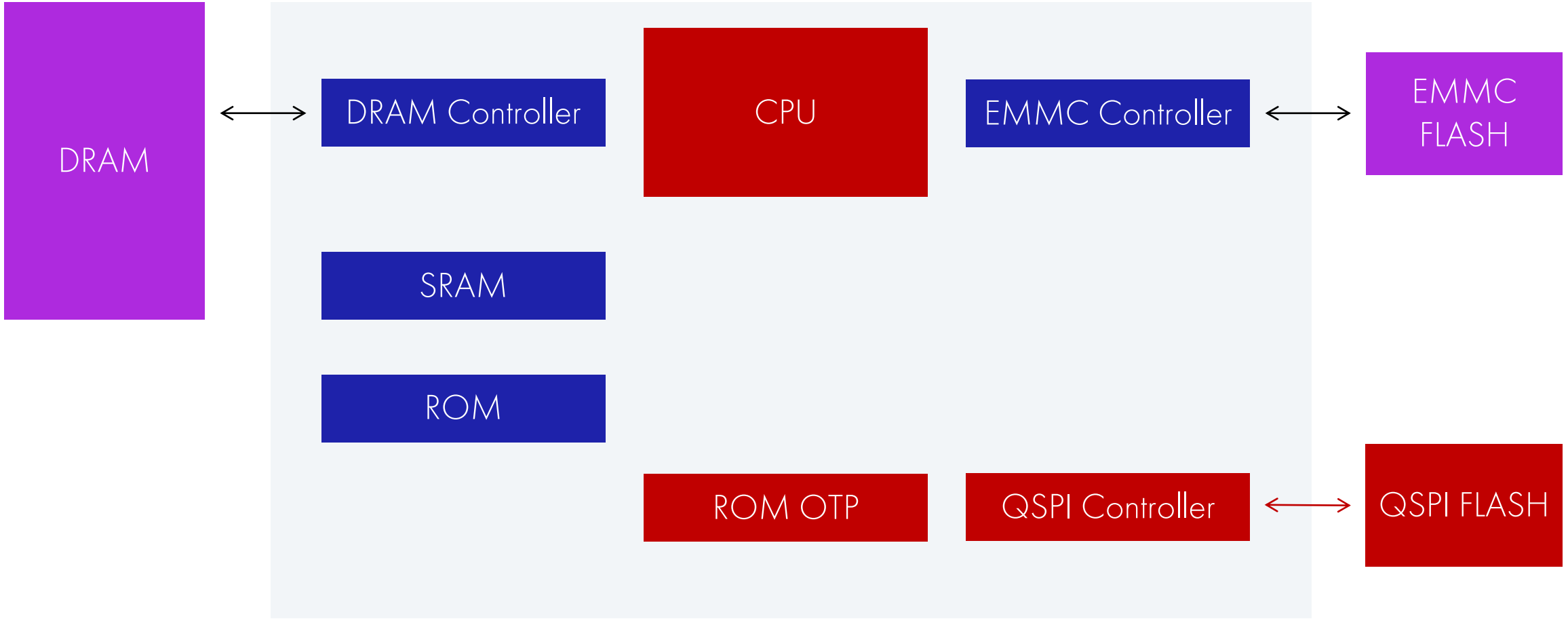
Цепь доверия



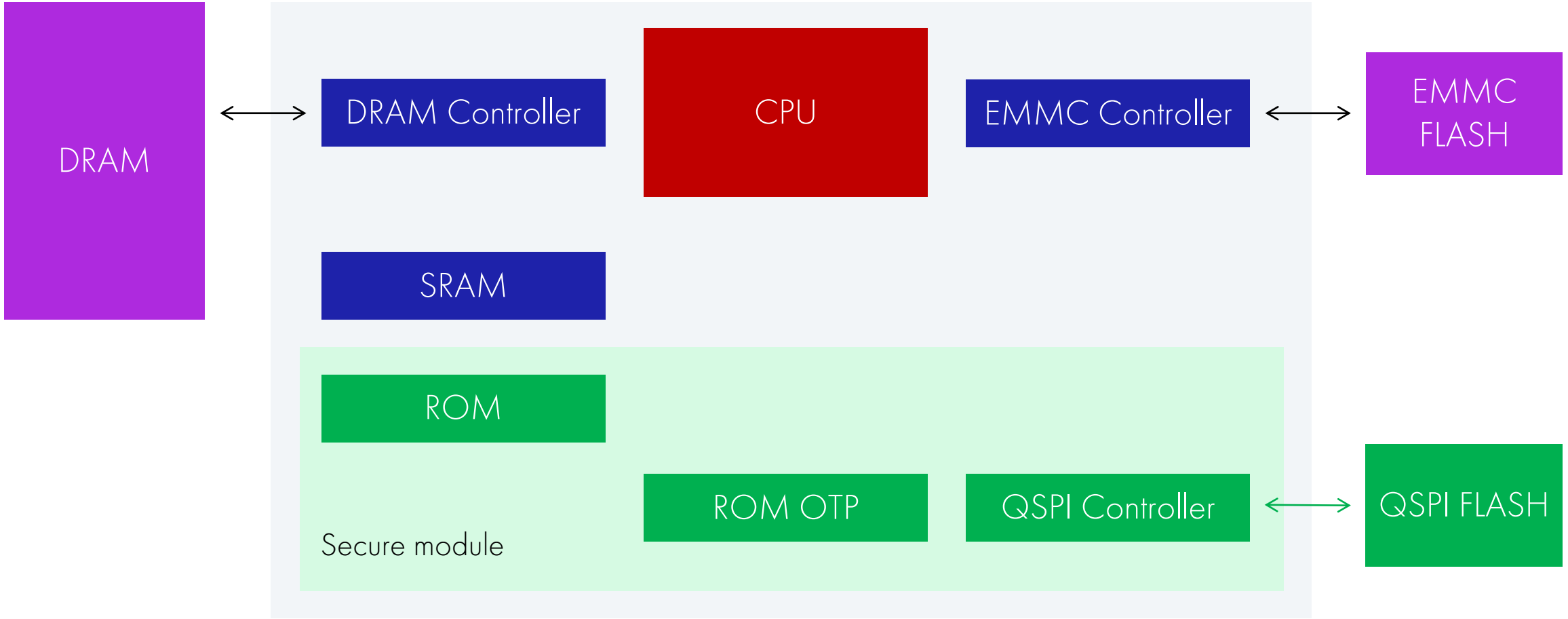
Архитектура СнК с поддержкой безопасной загрузки



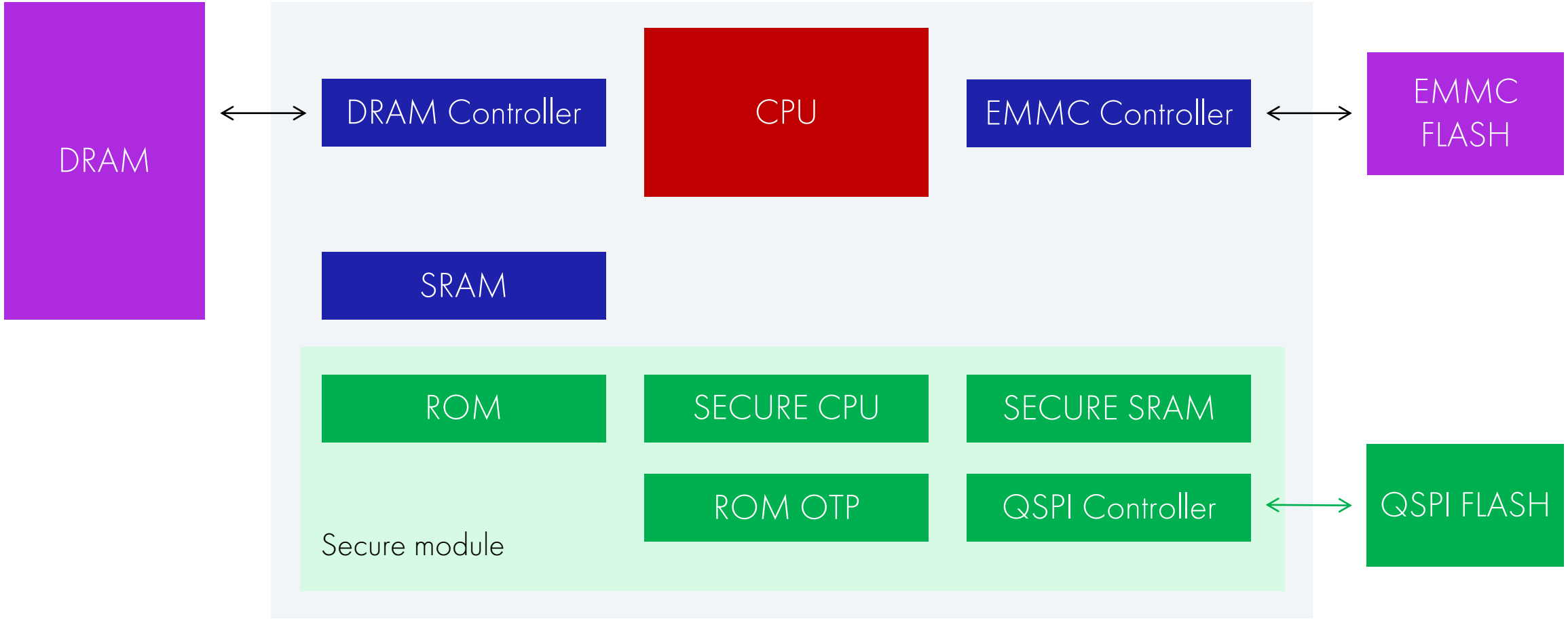
Архитектура СнК с поддержкой безопасной загрузки



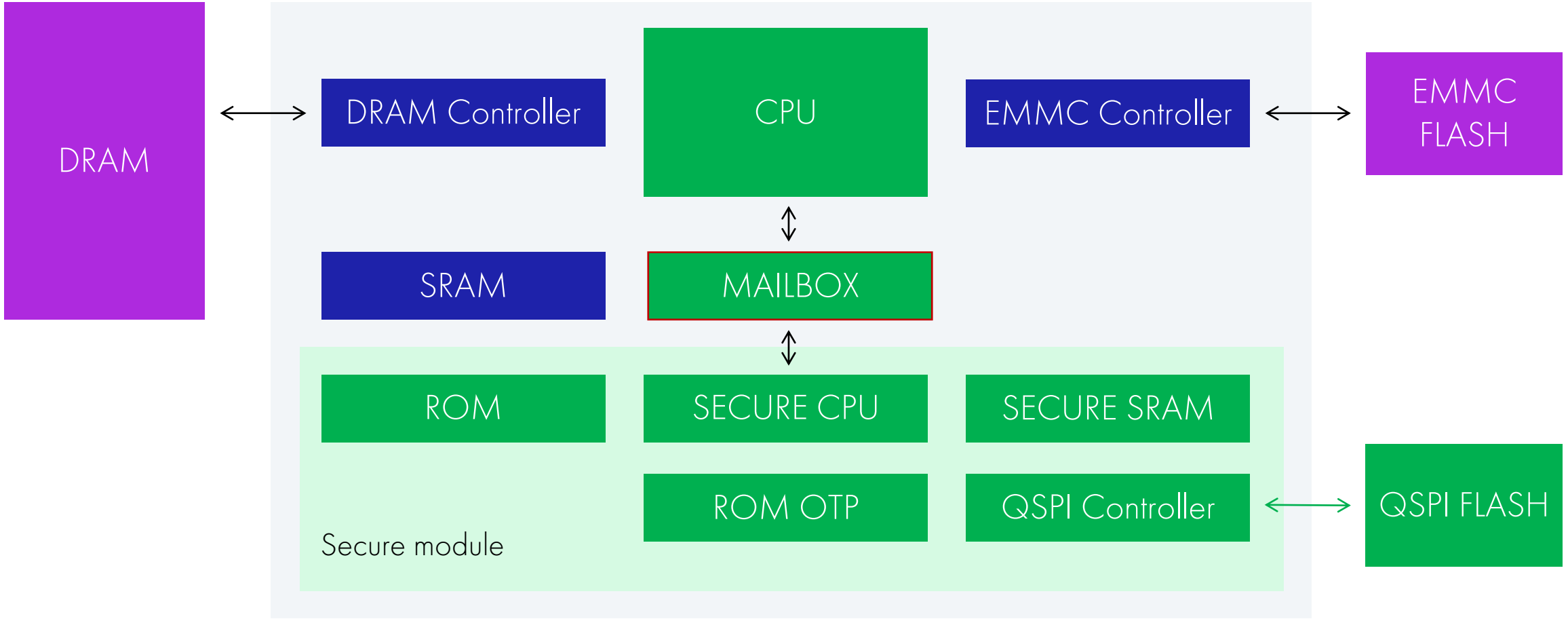
Архитектура СнК с поддержкой безопасной загрузки



Архитектура СнК с поддержкой безопасной загрузки



Архитектура СнК с поддержкой безопасной загрузки




БУДУЩЕЕ
В НАШИХ
РУКАХ

Партнеры конференции

Наши ресурсы

Как найти сообщество

FPGA-Systems.ru

FPGA-Systems Magazine (FSM)

@fpgasystems

admin@fpga-systems.ru

Youtube

@fpgasystems