конференция
РусКрипто

Ежегодная международная научно-практическая конференция

«РусКрипто’2022»

Особенности извлечения данных из мобильных устройств с пофайловым шифрованием

Карондеев Андрей,
ООО «Оксиджен Софтвер»

File-Based Encryption (FBE)

- Поддерживается начиная с Android 7
- Повсеместное внедрение начиная с Android 10
  - Huawei начиная с Android 7
  - Samsung начиная с Android 9
- Реализация на основе ФС Ext4 и F2FS
  - Huawei, Xiaomi F2FS
  - Oppo, Realme Ext4
- Inline Crypto Engine
  - FBE ключи никогда не покидают TEE
- У каждого пользователя устройства есть два хранилища

File-Based Encryption (FBE)

Trusted Execution Environment (TEE)

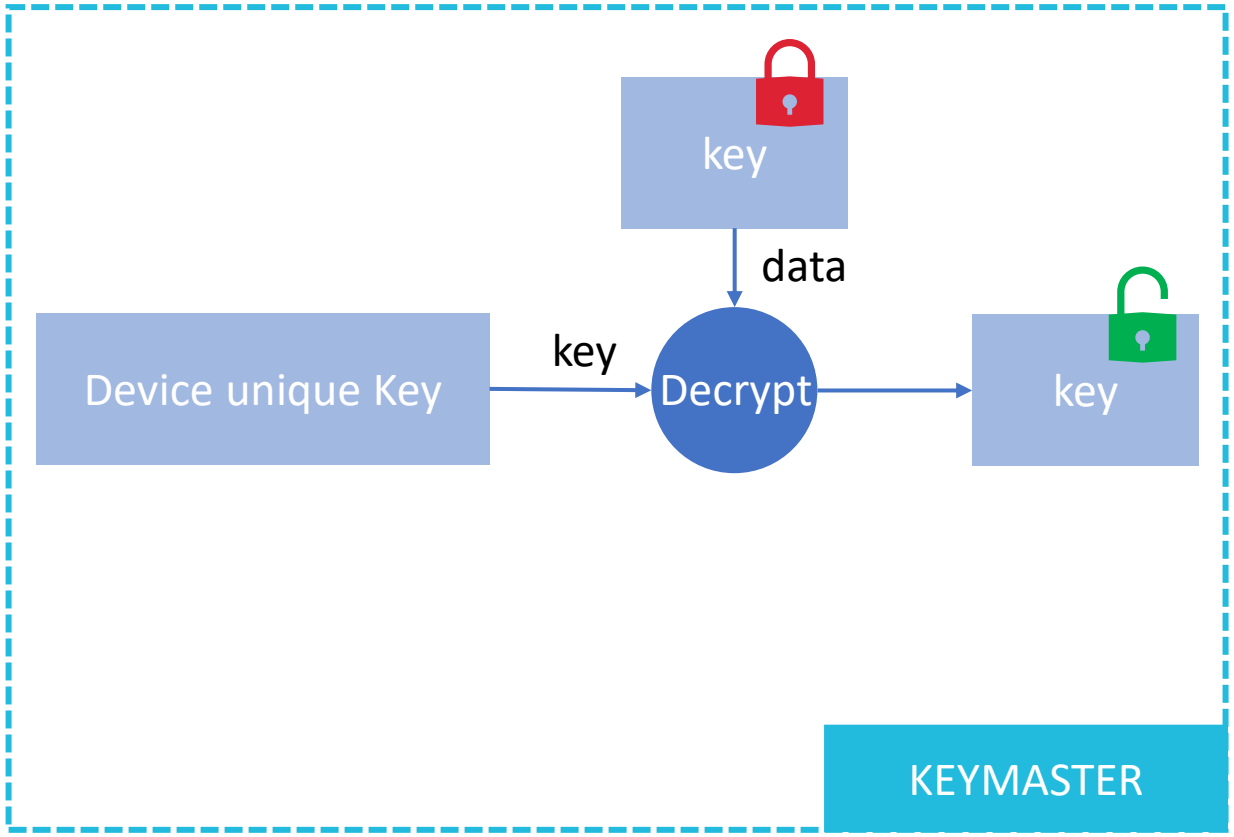
Наиболее интересные части:

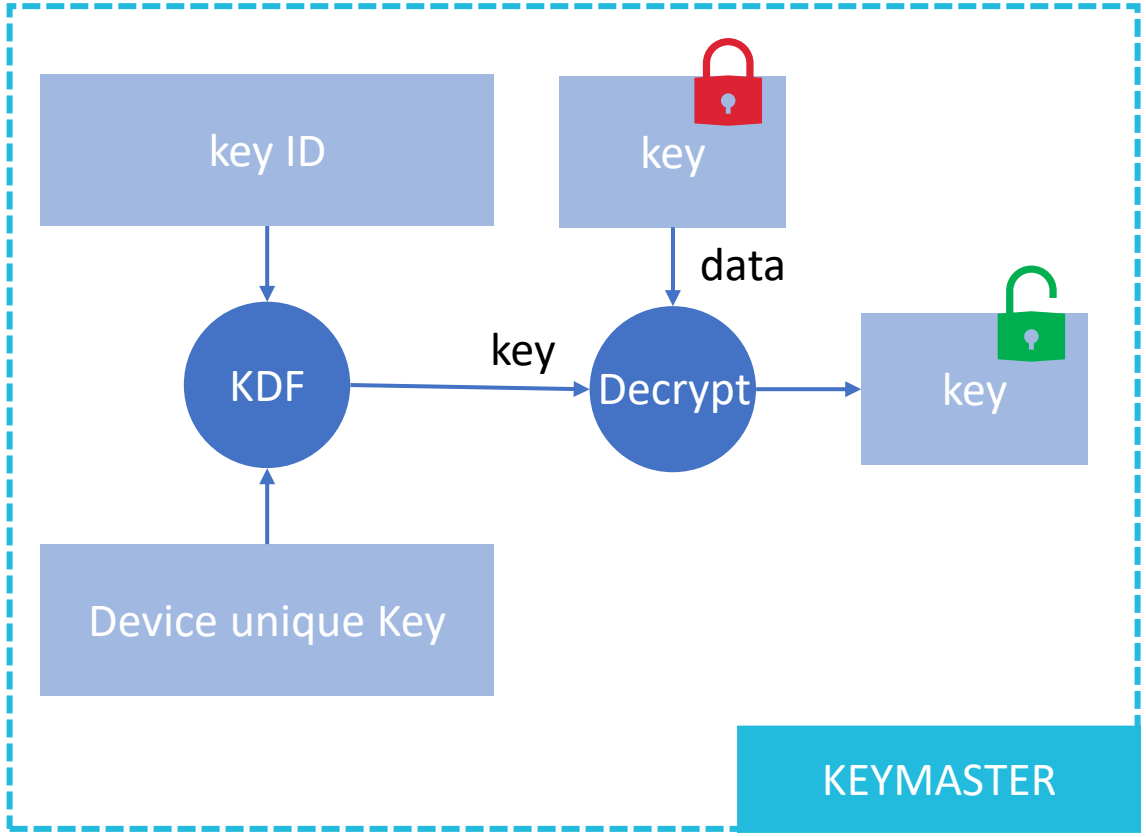
- KEYMASTER
- GATEKEEPER

- Со стороны Android стандартизированные API
- Реализация на усмотрение производителя

Шифрование DE ключей

- keymaster_key_blob

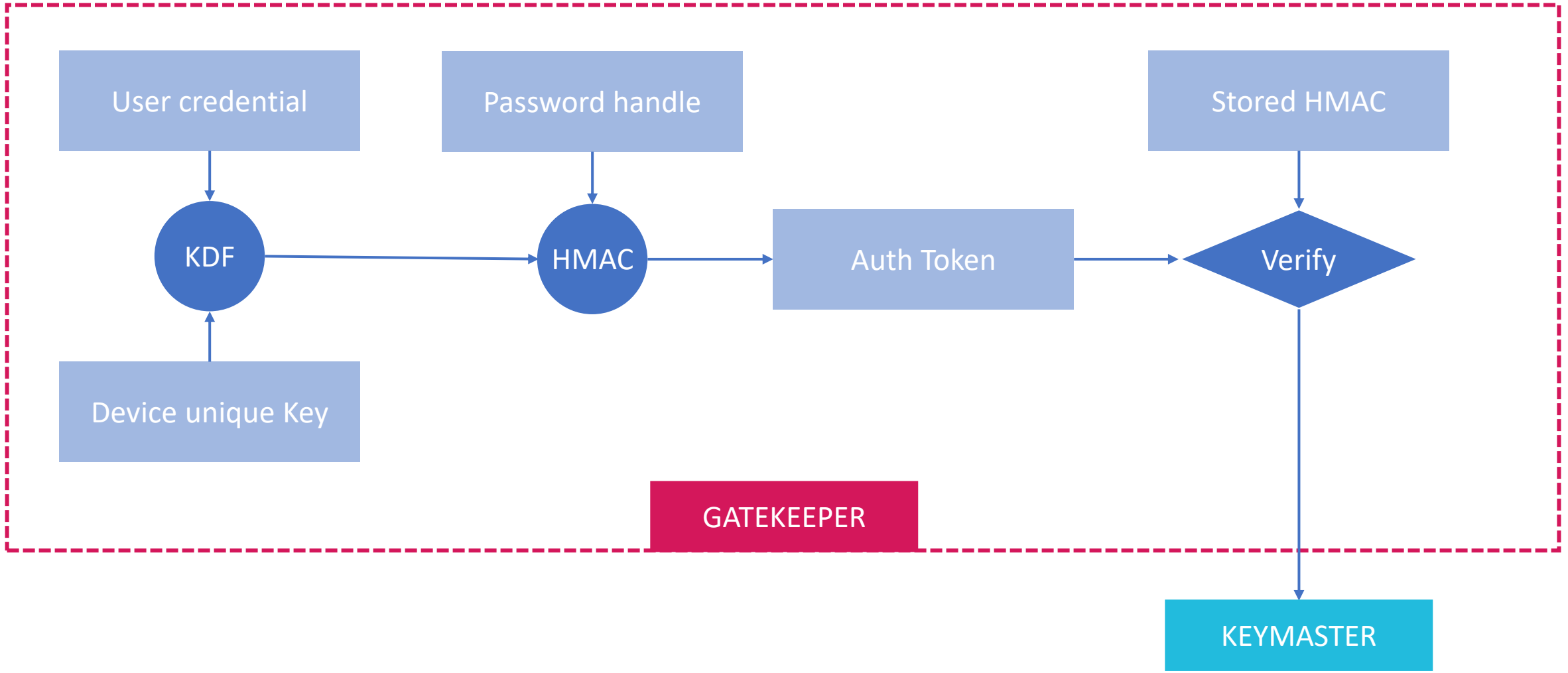


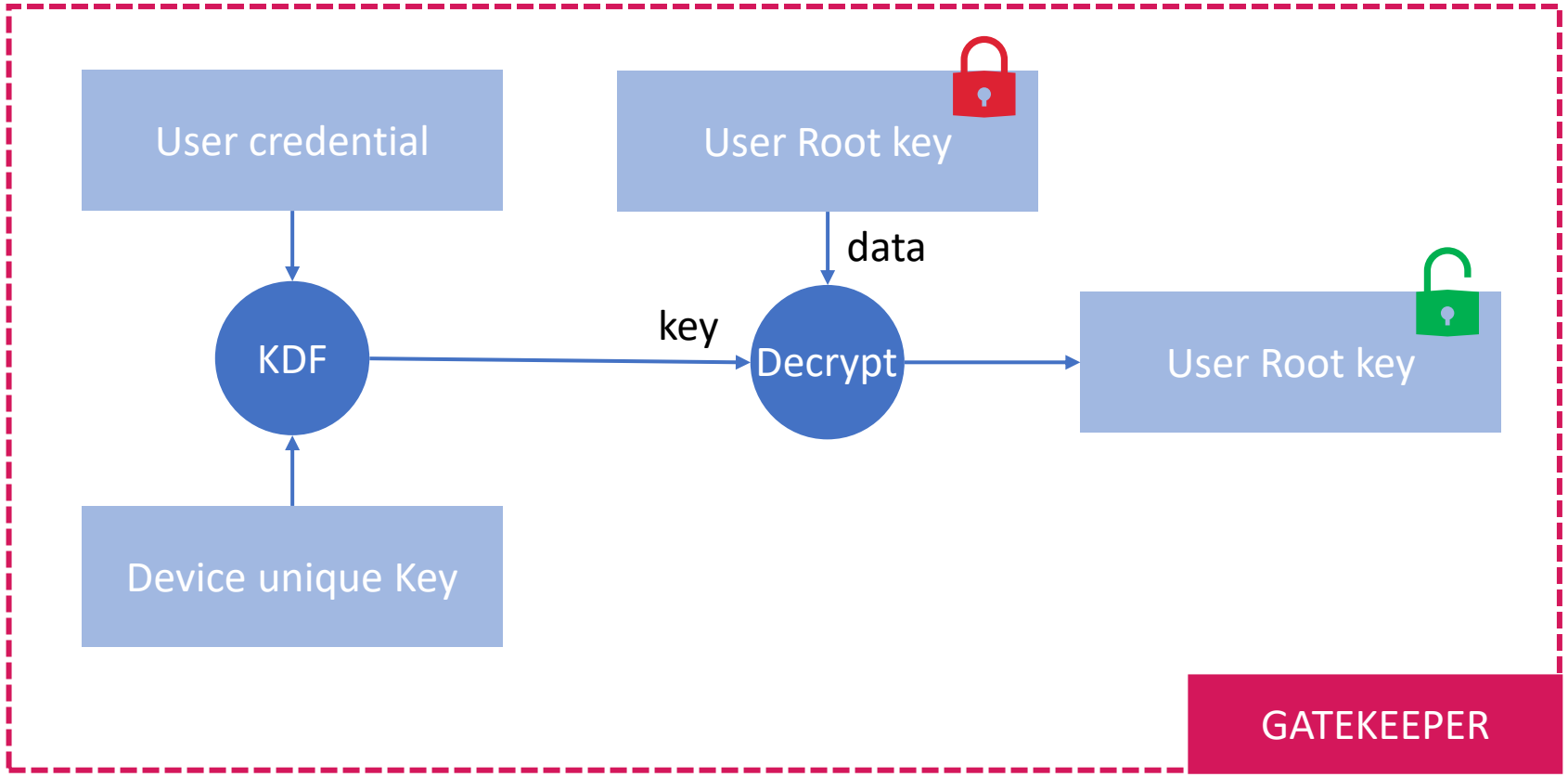


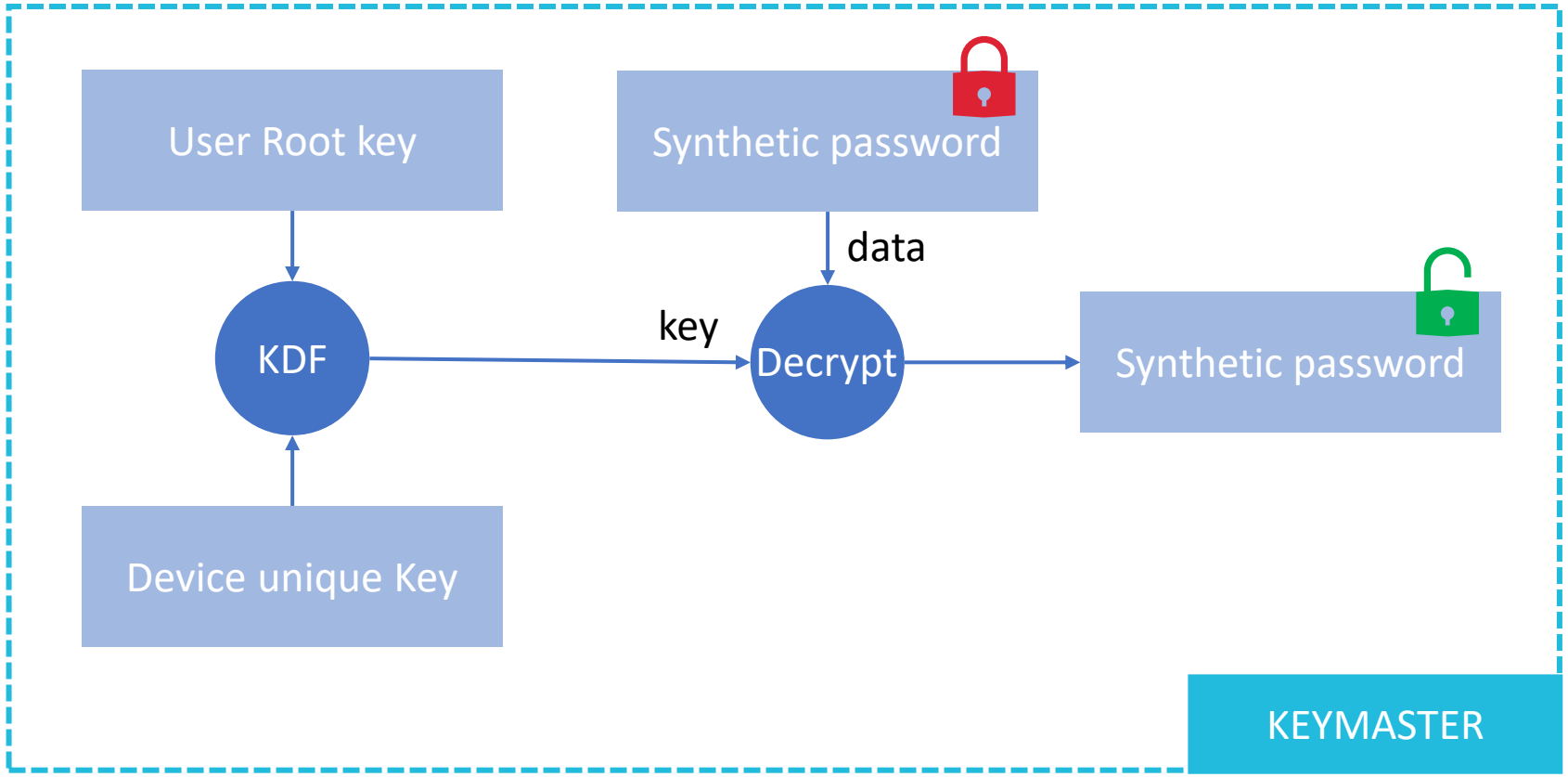
Шифрование CE ключей

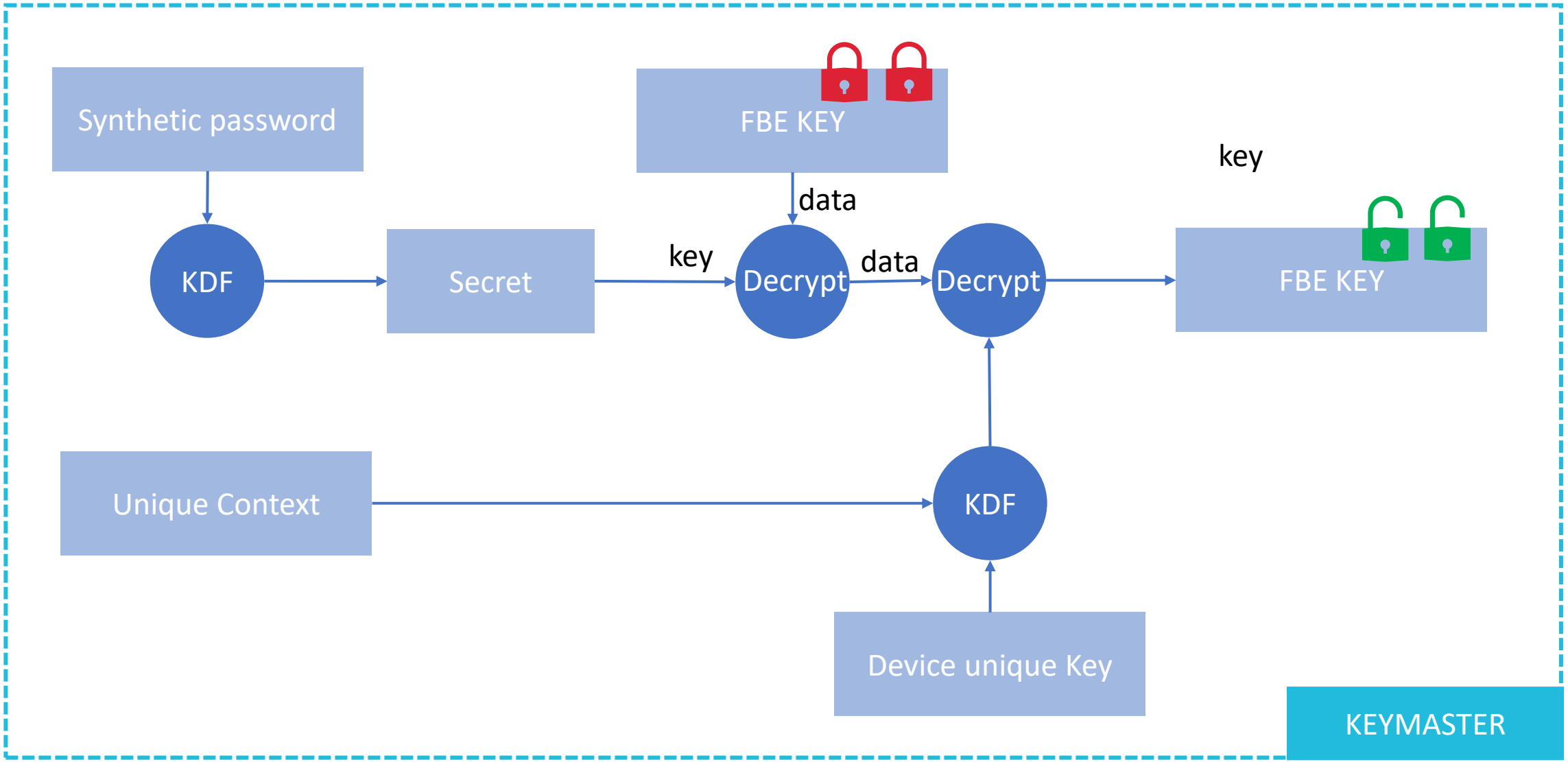
- Если пароль не задан, то процесс аналогичен DE
- Иначе со стороны Android https://cs.android.com/

```
passwordTokenToGkInput
unwrapPasswordBasedSyntheticPassword
- pwdToken = computePasswordToken(credential, pwd);
 - scrypt(pwd, salt)
- gkPwdToken = passwordTokenToGkInput(pwdToken);
 - personalisedHash(PERSONALIZATION_USER_GK_AUTH, token);
 - personalisedHash(byte[] personalisation, byte[]... message)
 - sha512(padding(personalisation, 128) + messages)
- gatekeeper.verifyChallenge(fakeUid(userId), 0L,
                             pwd.passwordHandle, gkPwdToken)
```


User credential
Password handle
Stored HMAC
KDF
HMAC
Auth Token
Verify
Device unique Key
GATEKEEPER
KEYMASTER


User credential
User Root key
data
KDF
key
Decrypt
User Root key
Device unique Key
GATEKEEPER

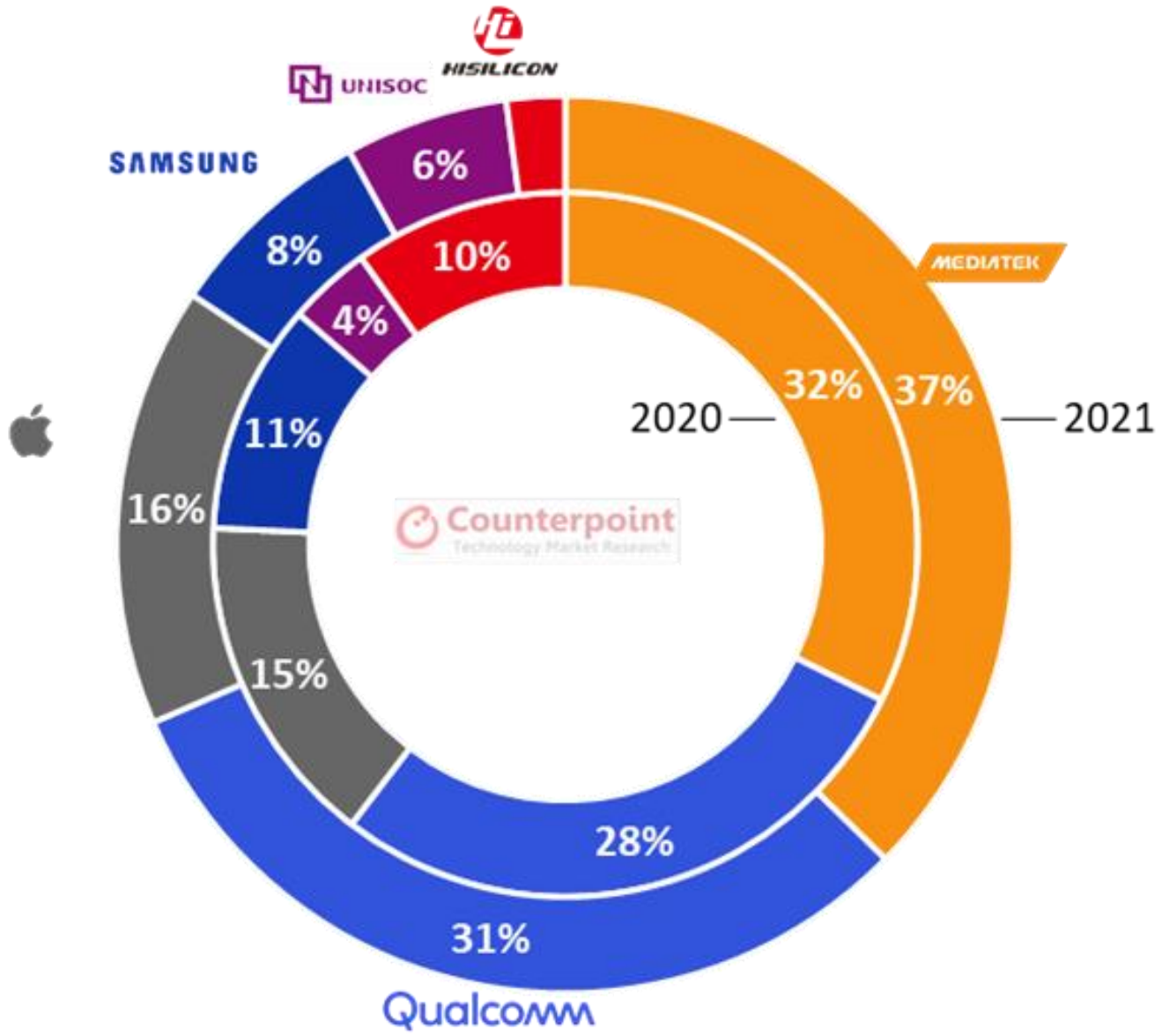

User Root key
Synthetic password
data
KDF
key
Decrypt
Synthetic password
Device unique Key
KEYMASTER


Synthetic password
FBE KEY
data
key
KDF
Secret
key
Decrypt
data
Decrypt
FBE KEY
Unique Context
KDF
Device unique Key
KEYMASTER

Подбор пароля

- Для подбора пароля вне устройства необходимо извлечь Device unique Key и восстановить алгоритм KDF
- Для подбора пароля на устройстве необходимо скомпрометировать gatekeeper

- Некоторые производители реализуют функционал gatekeeper в Secure Processing Unit (SPU)
- Использование SPU существенно препятствует получению возможности подбирать пароль

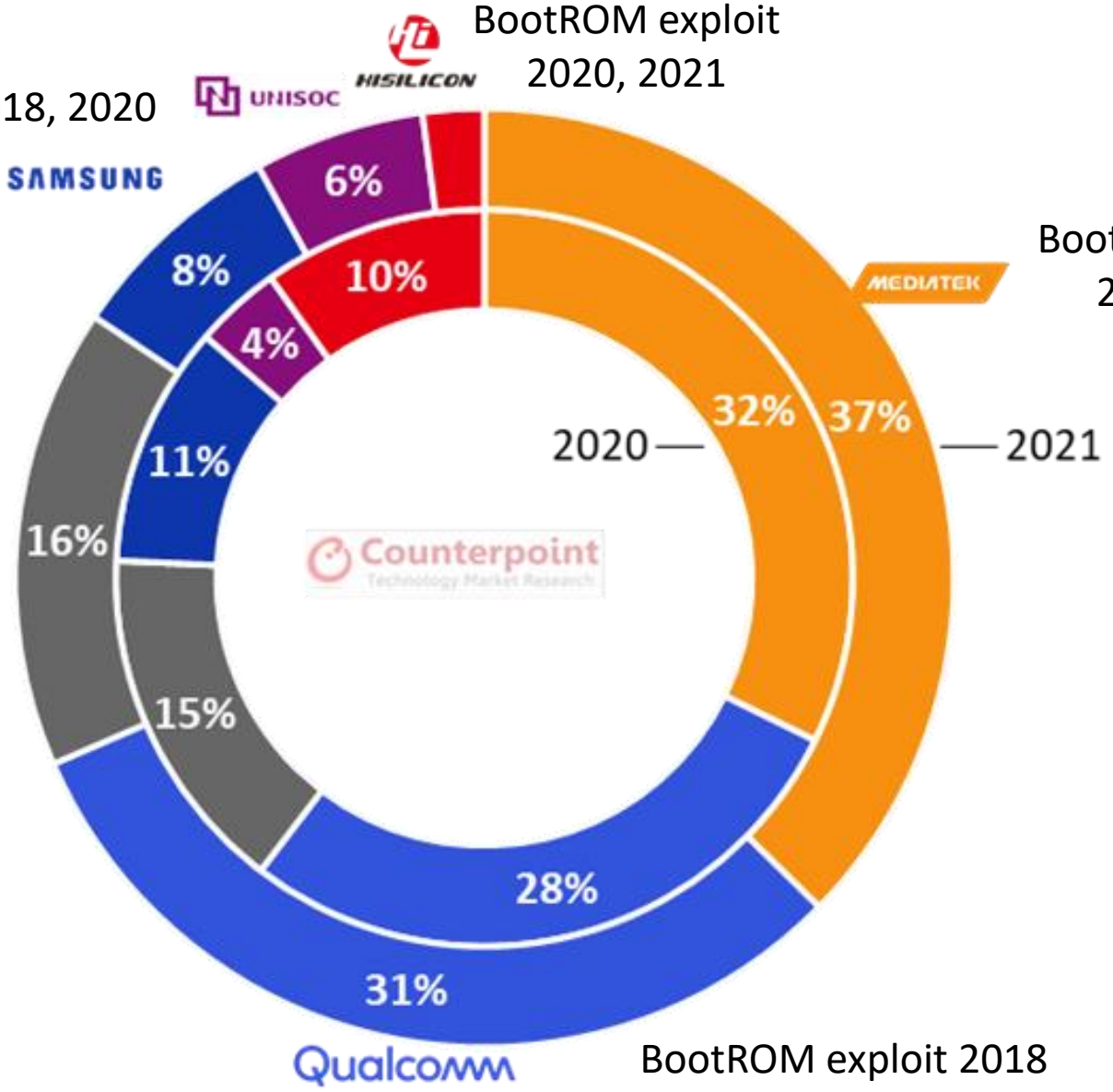

HISILICON
UNISOC
SAMSUNG
6%
8%
10%
4%
11%
16%
15%
32%
37%
2020
2021
28%
31%
MEDIATEK
Qualcomm
Counterpoint
Technology Market Research

BootROM exploit
2020, 2021

Boot exploit 2018, 2020

BootROM exploit
2019, 2021

BootROM exploit 2019



BootROM exploit 2018

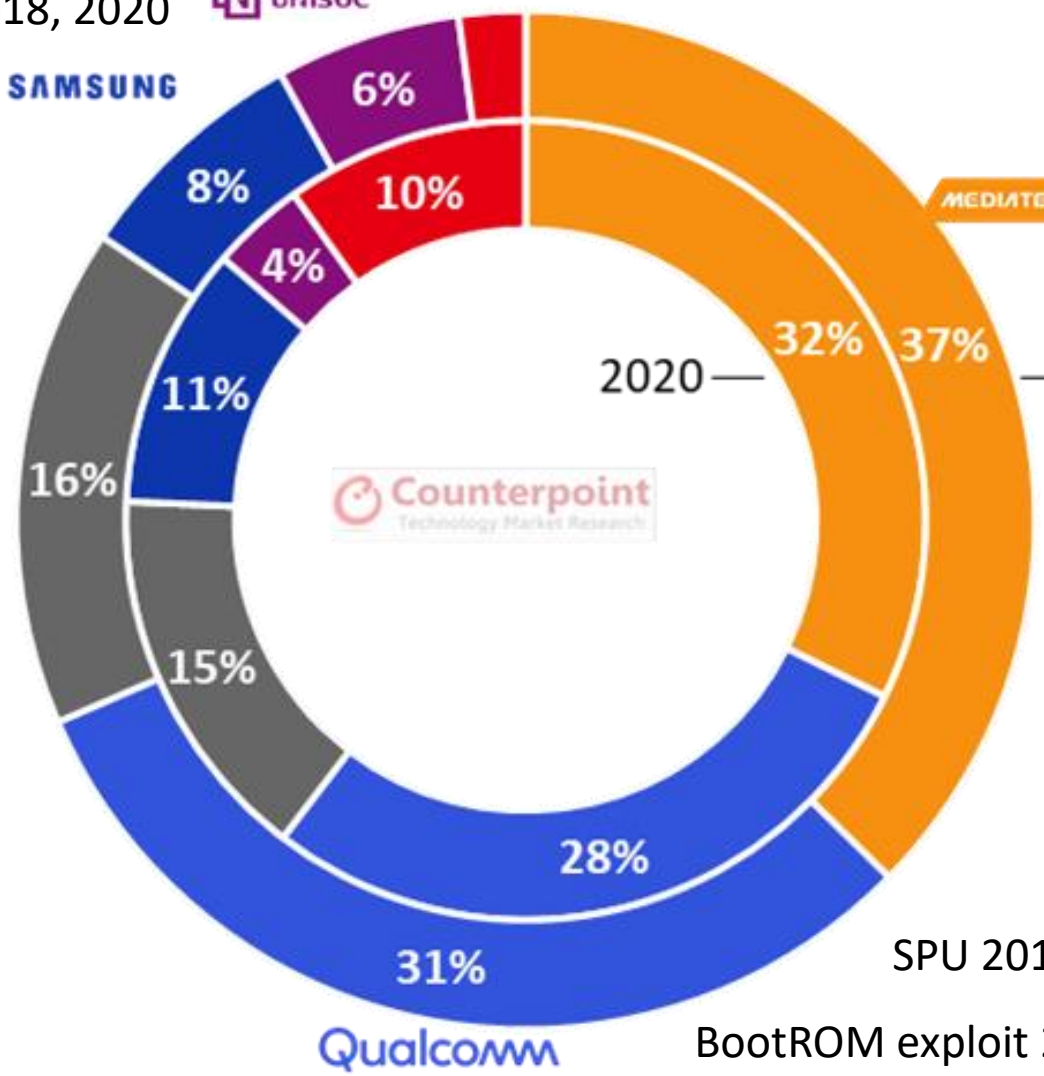
BootROM exploit
2020, 2021

SPU 2021 (2016*)

Boot exploit 2018, 2020
src leak 2022

BootROM exploit
2019, 2021

BootROM exploit 2019
SEP 2016
SEP exploit 2020



SPU 2019

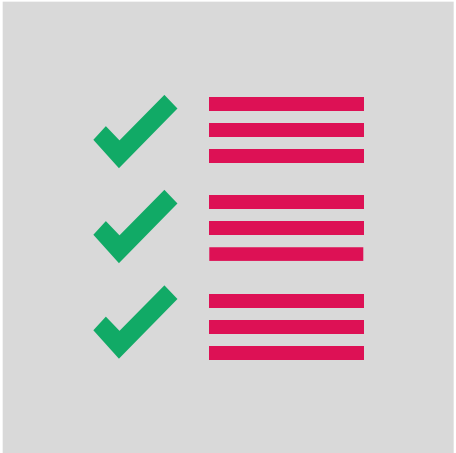
BootROM exploit 2018

Trusted Execution Environment (TEE)

- Qualcomm
  - QSEE
- Exynos
  - KINIBI, TEEGRIS
- HiSilicon
  - Huawei TEE
- MediaTek
  - MICROTRUST, KINIBI, TRUSTY, T6, RSEE …

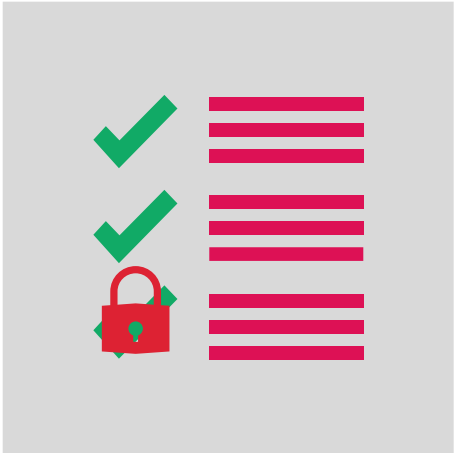
MediaTek

- BootROM exploit
- SPU нет / не используется
- Не сложено достать Device unique Key
  - ME_ID / CHIP_ID
- Реализуем подбор пароля вне устройства



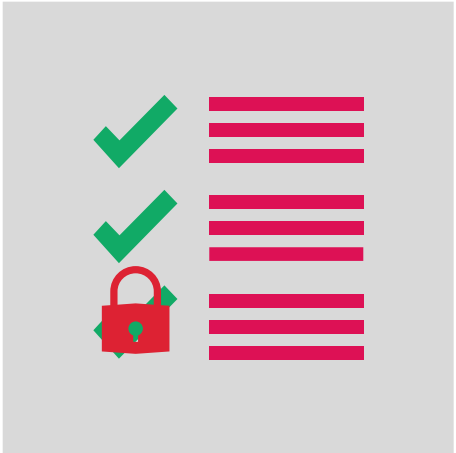
Huawei HiSilicon Kirin

- BootROM exploit
- SPU
  - Появился в 2016
  - Начал использоваться в 2021
- Не сложено достать Device unique Key
- Подбор пароля
  - до 2021 вне устройства
  - май-июнь 2021 на устройстве
  - после июля 2021 …

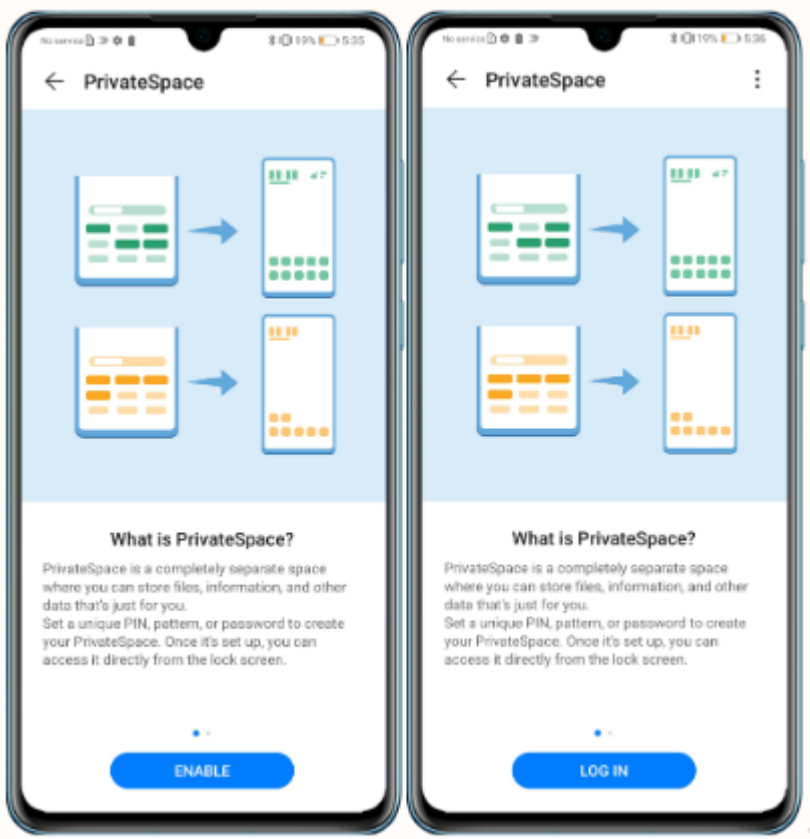


Samsung Exynos

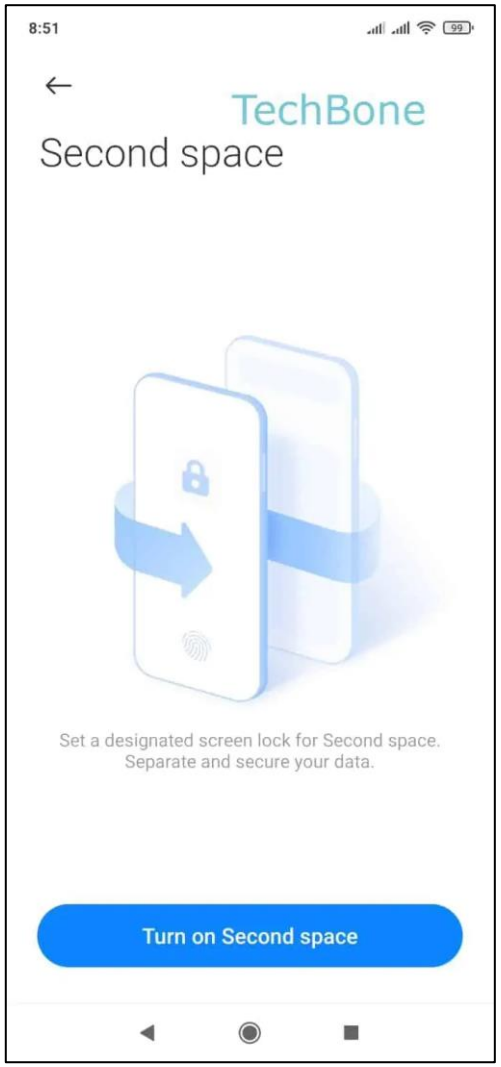
- Boot exploit
- GATEKEEPER exploit
  - до v3.3 включительно
  - до v3.5 включительно
- Реализуем подбор пароля на устройстве

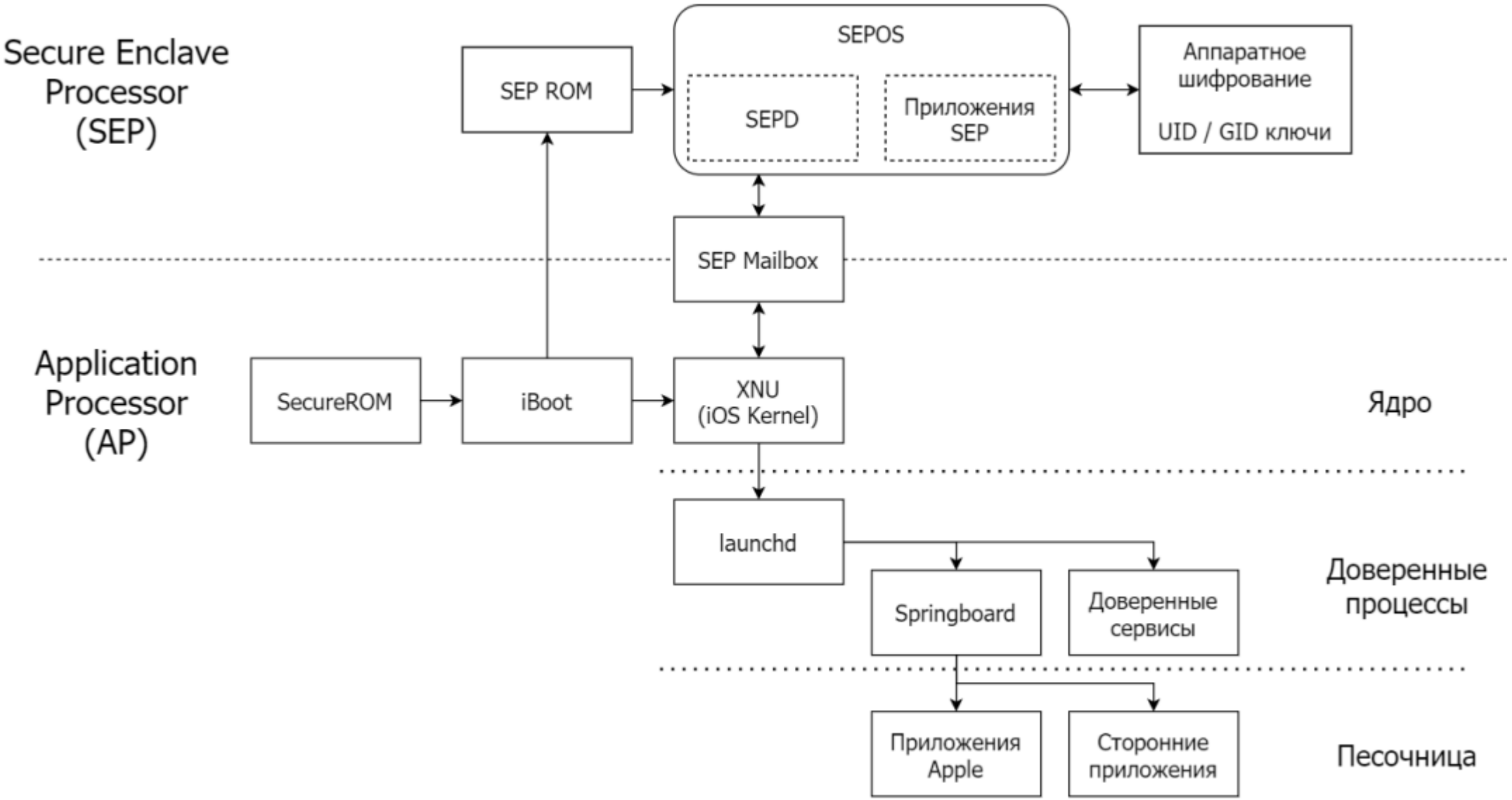


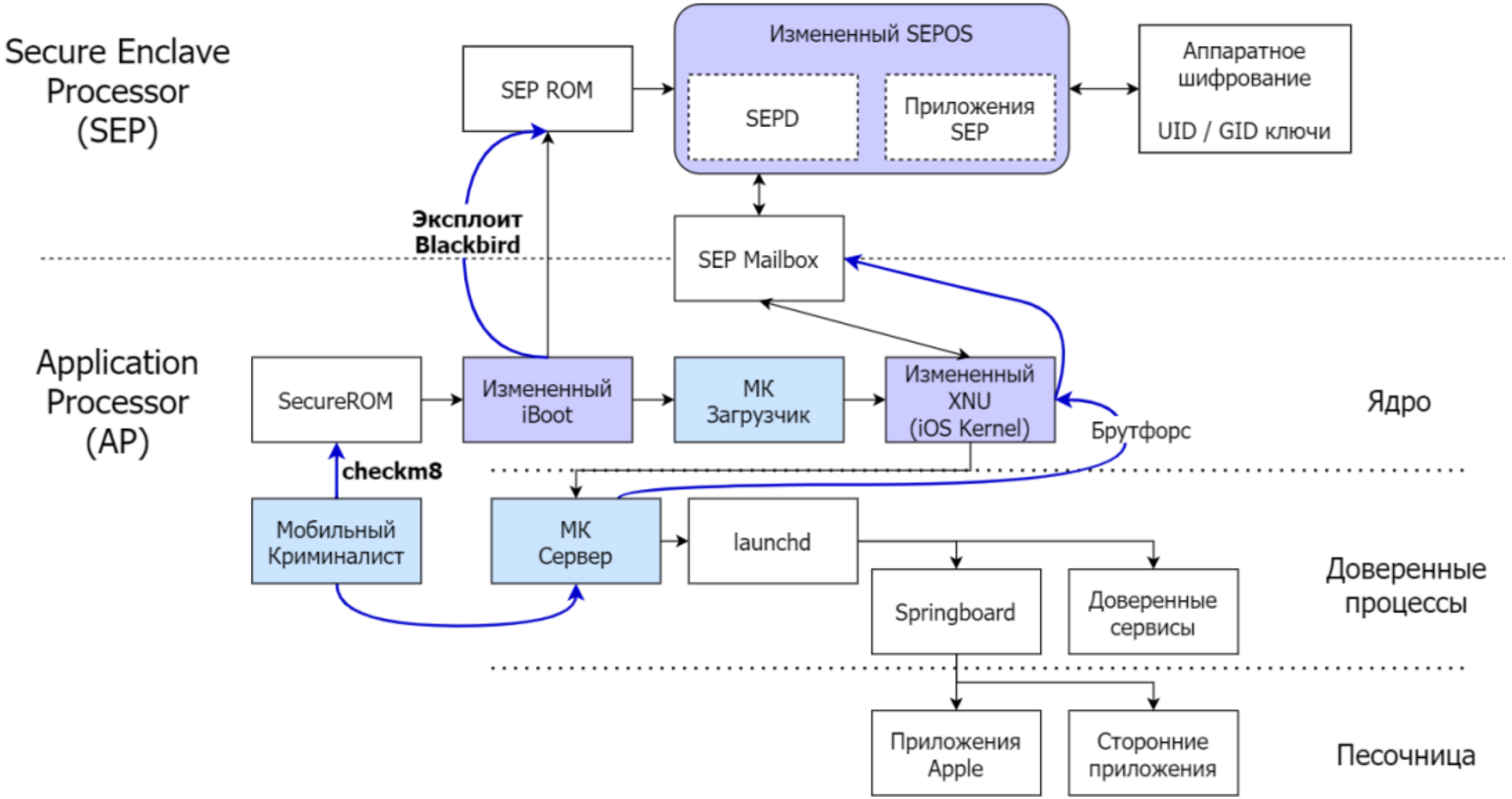
Второе дно


PrivateSpace
What is PrivateSpace?
PrivateSpace is a completely separate space where you can store files, information, and other data that's just for you.
Set a unique PIN, pattern, or password to create your PrivateSpace. Once it's set up, you can access it directly from the lock screen.
ENABLE
PrivateSpace
What is PrivateSpace?
PrivateSpace is a completely separate space where you can store files, information, and other data that's just for you.
Set a unique PIN, pattern, or password to create your PrivateSpace. Once it's set up, you can access it directly from the lock screen.
LOG IN


My Galaxy
Samsung Pay
Phone
Settings
Facebook
Gallery
Camera
Select multiple items
Remove shortcut
Add to Secure Folder
Sleep
Uninstall
App info
SECURE FOLDER
Lock
Add apps
Add files
Edit apps
Facebook
Pinterest
Gallery
WhatsApp
Camera

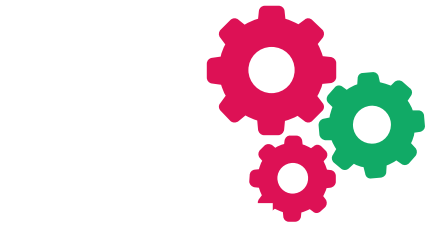

TechBone
Second space
Set a designated screen lock for Second space.
Separate and secure your data.
Turn on Second space

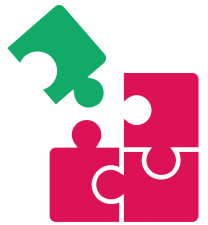

Secure Enclave Processor (SEP)
SEP ROM
SEPOS
SEPD
Приложения SEP
Аппаратное шифрование
UID / GID ключи
SEP Mailbox
Application Processor (AP)
SecureROM
iBoot
XNU (iOS Kernel)
Ядро
launchd
Springboard
Доверенные сервисы
Доверенные процессы
Приложения Apple
Сторонние приложения
Песочница


Secure Enclave Processor (SEP)
SEP ROM
Измененный SEPOS
SEPD
Приложения SEP
Аппаратное шифрование
UID / GID ключи
Эксплоит Blackbird
SEP Mailbox
Application Processor (AP)
SecureROM
Измененный iBoot
MK Загрузчик
Измененный XNU (iOS Kernel)
Ядро
Брутфорс
checkm8
Мобильный Криминалист
MK Сервер
launchd
Springboard
Доверенные сервисы
Доверенные процессы
Приложения Apple
Сторонние приложения
Песочница

Подведем итоги

- Существуют подходы к извлечению данных из устройств с FBE
- Многое зависит от вендора и SoC
- Наблюдается переход на использование SPU
- Использование SPU существенно препятствует получению возможности подбирать пароль
- Для многих устройств пока доступны только подходы для ситуаций, когда пароль известен или не задан
- При извлечении данных через root exploit или программу-агент стоит учитывать возможное наличие второго дна





Вопросы

???

Контактная информация

Электронная почта:

karondeev@oxygensoftware.com

Телефон:

+7 (963) 649-70-44

Telegram:

@karondeev

Сайт:

www.oxygensoftware.ru