OS Day 2023

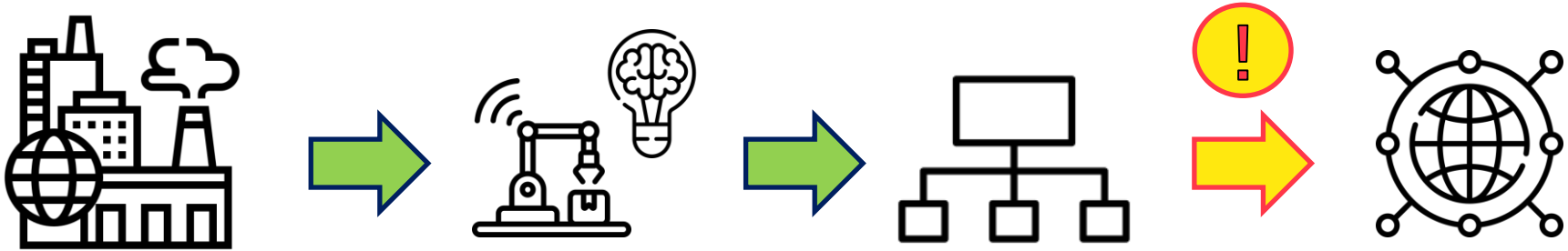
Один из подходов для создания безопасной системы реального времени на базе KasperskyOS

Сергей Барсуков
Разработчик

Игорь Сорокин
Руководитель группы системных исследований

kaspersky

Угрозы в системах реального времени



Индустрия 4.0

Больше умных устройств

Больше сетевых соединений

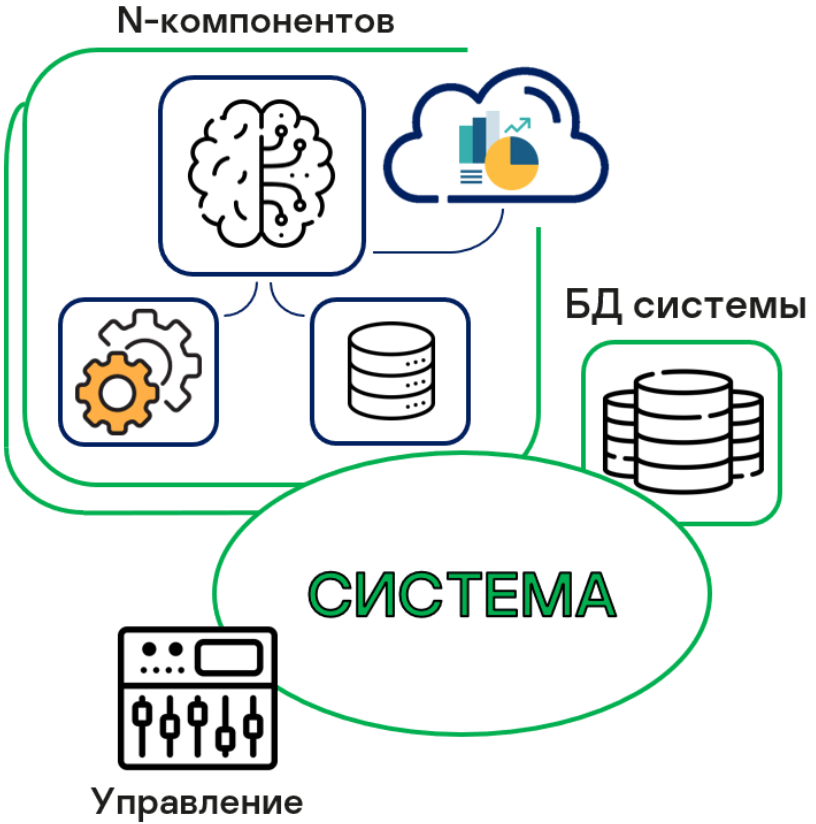
Сети общего доступа

Взаимодействие по сетям общего назначения

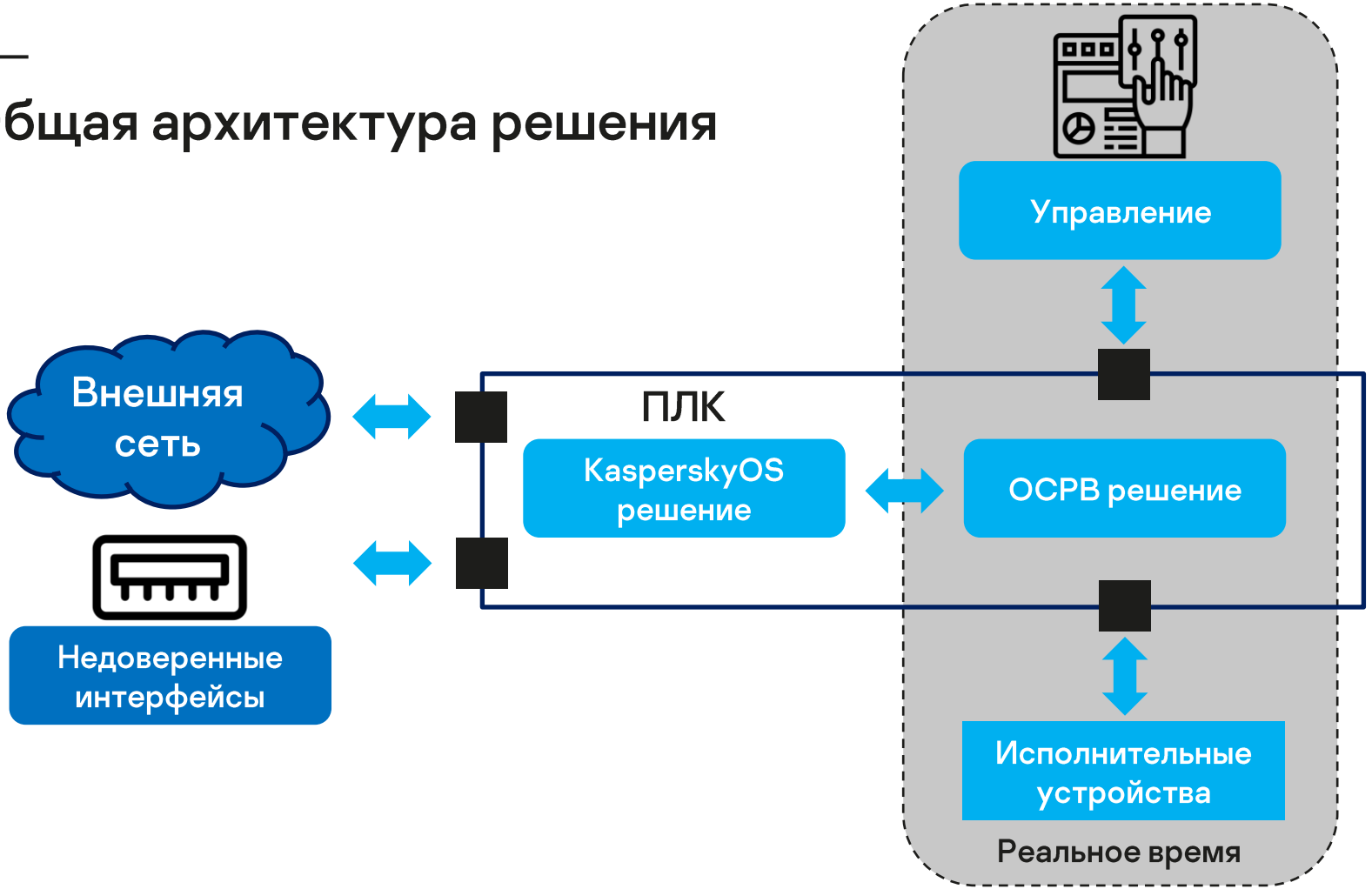
Системы реального времени могут иметь N-компонентов с доступом к внешним сетям.

Возможные направления:

- Интернет вещей
- Сети электроснабжения
- Телемедицина
- Умная одежда
- Системы мониторинга
- прочее



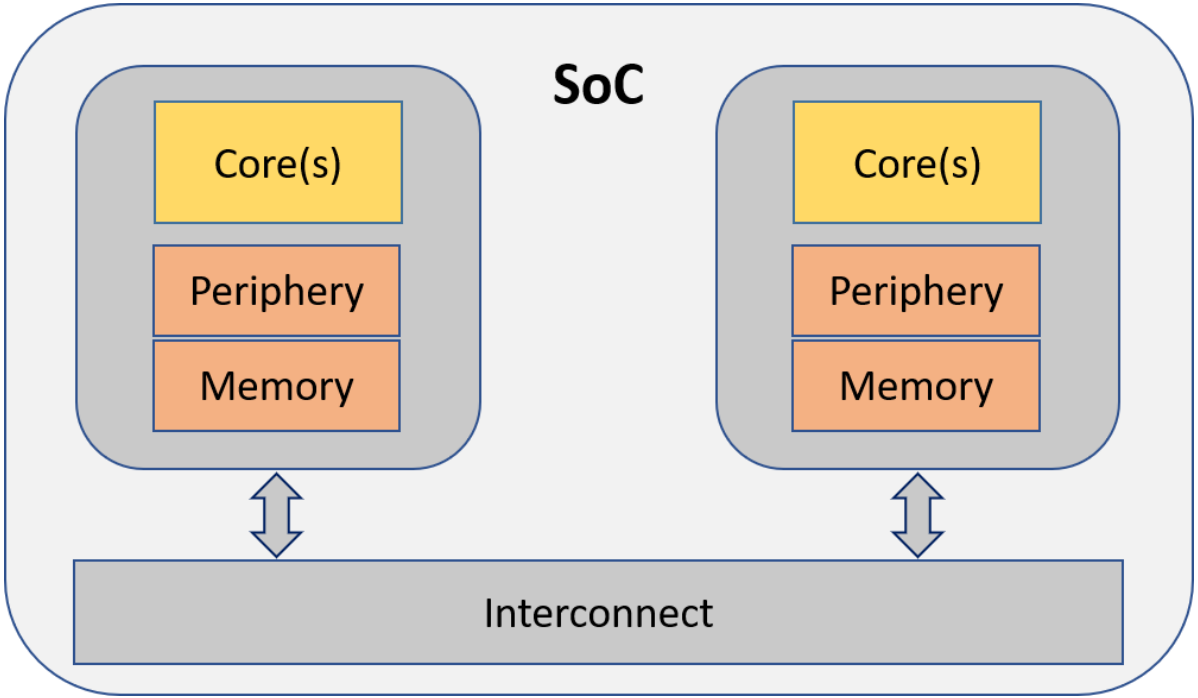
Общая архитектура решения



Реализация на одном SoC

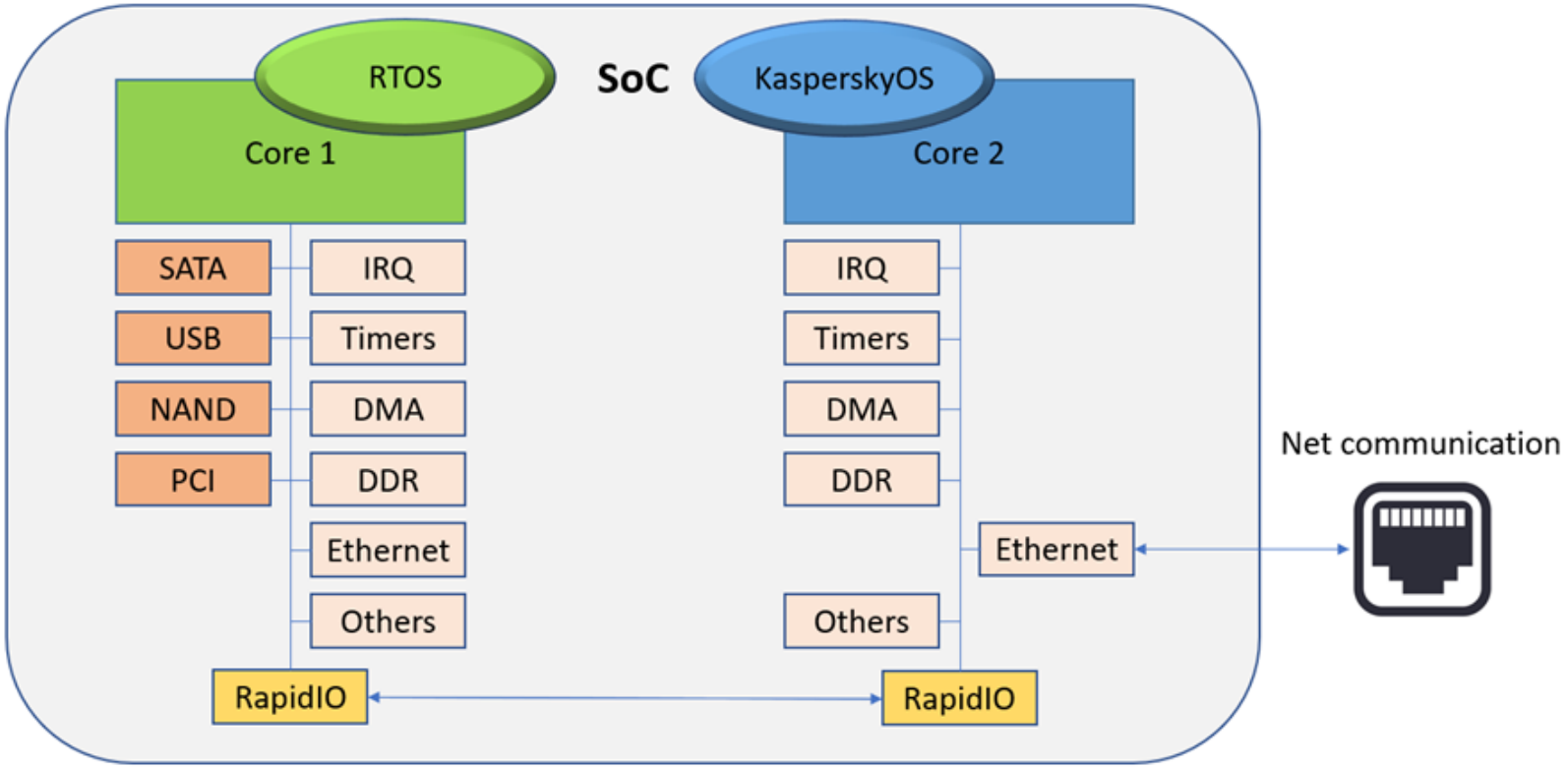
Примеры устройств:

- NXP i.MX Series
- Renesas R-Car Series
- TI Sitara AM6 Series
- Xilinx Zynq UltraScale
- Intel Stratix 10



Структурная схема SoC в рассматриваемом подходе

Отечественная система на кристалле

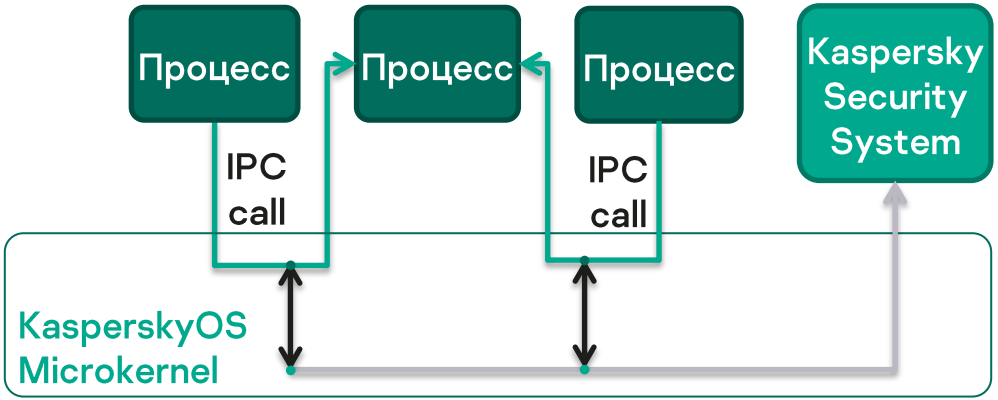


Портирование KasperskyOS

Цели портирования:

Расширяем поддержку MIPS в KasperskyOS

Базовые принципы KasperskyOS



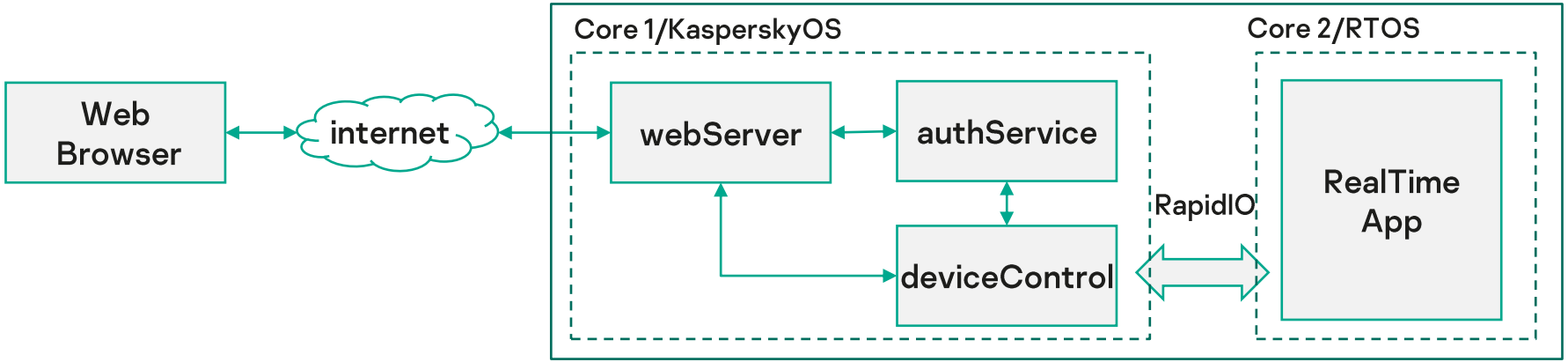
Микроядерная операционная система

Взаимодействие между доменами только по IPC-каналам

Изоляция приложений и их частей в отдельных доменах безопасности (MILS)

Контроль IPC-взаимодействий с помощью политик безопасности (Kaspersky Security System)

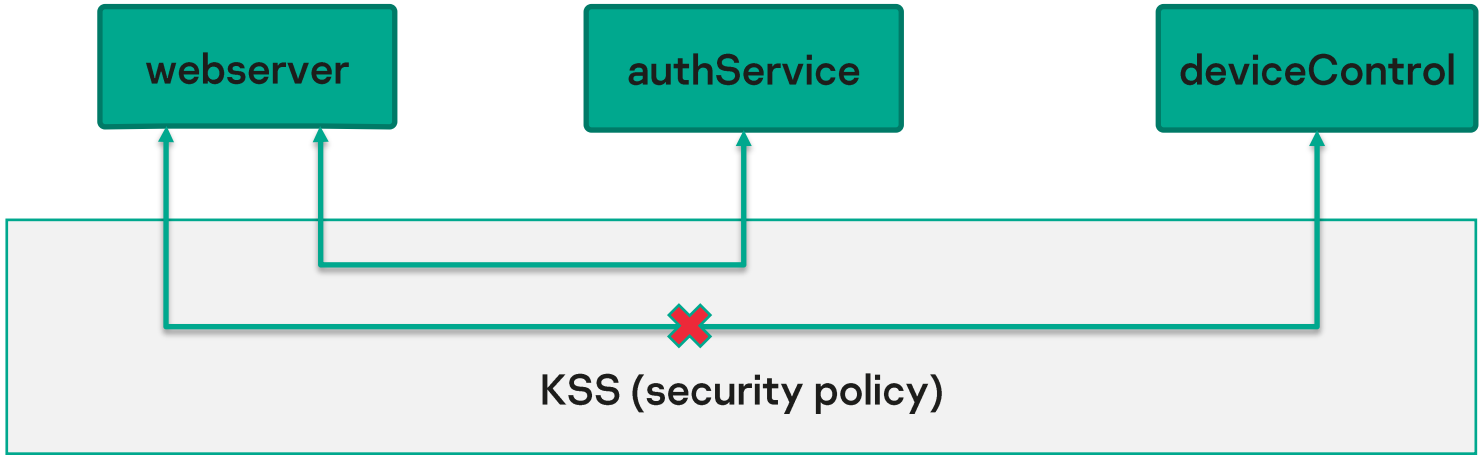
Архитектура решения на базе KasperskyOS и ОСРВ «Багет»[9]



Задачи:

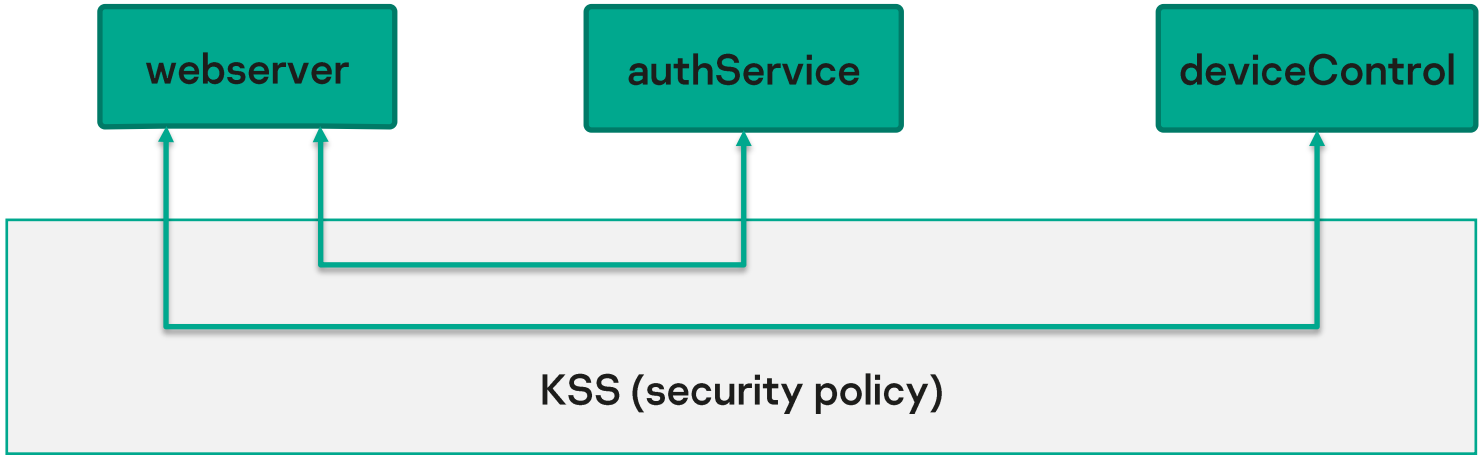
- Передача команд в RTOS возможна только аутентифицированным пользователям
- Безопасная передача критической информации
- Безопасный доступ к служебной информации решения

Авторизация к интерфейсу взаимодействия с ОСРВ



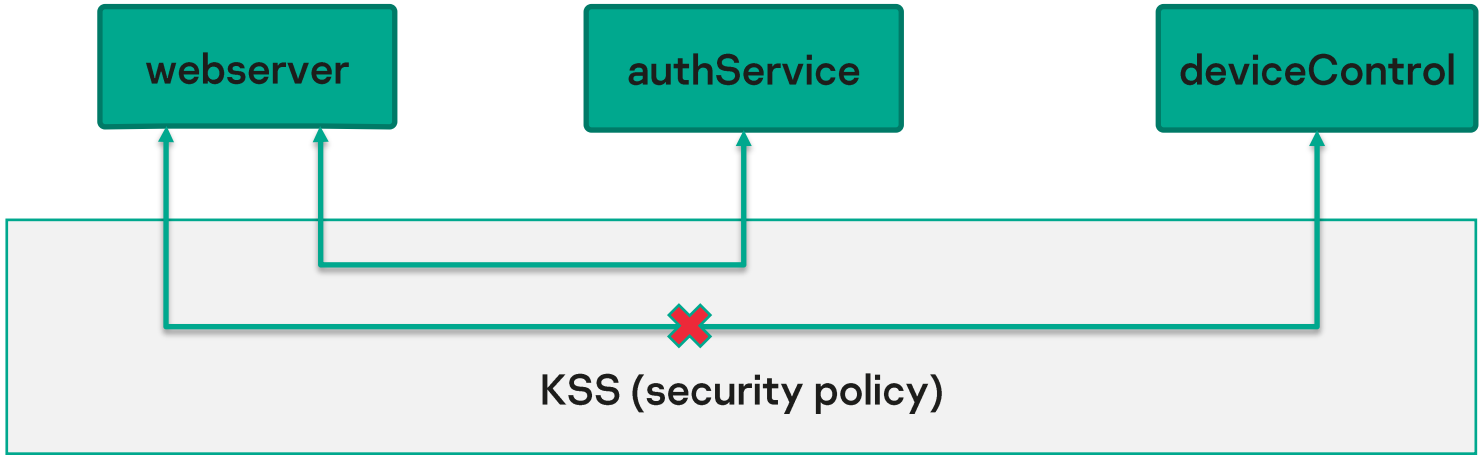
- Инициализация IPC-соединений

Авторизация к интерфейсу взаимодействия с OCPB



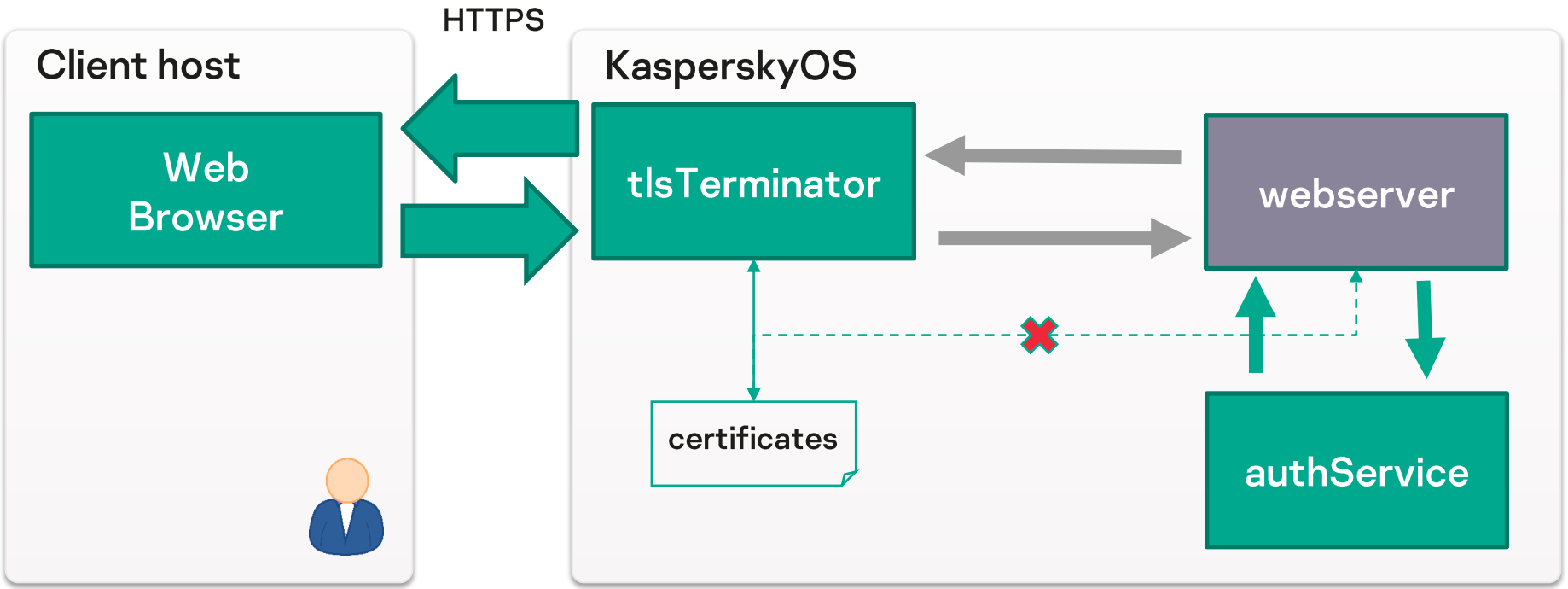
- Инициализация IPC-соединений
- Авторизация, инициализация сессии
- Работа

Авторизация к интерфейсу взаимодействия с OCPB

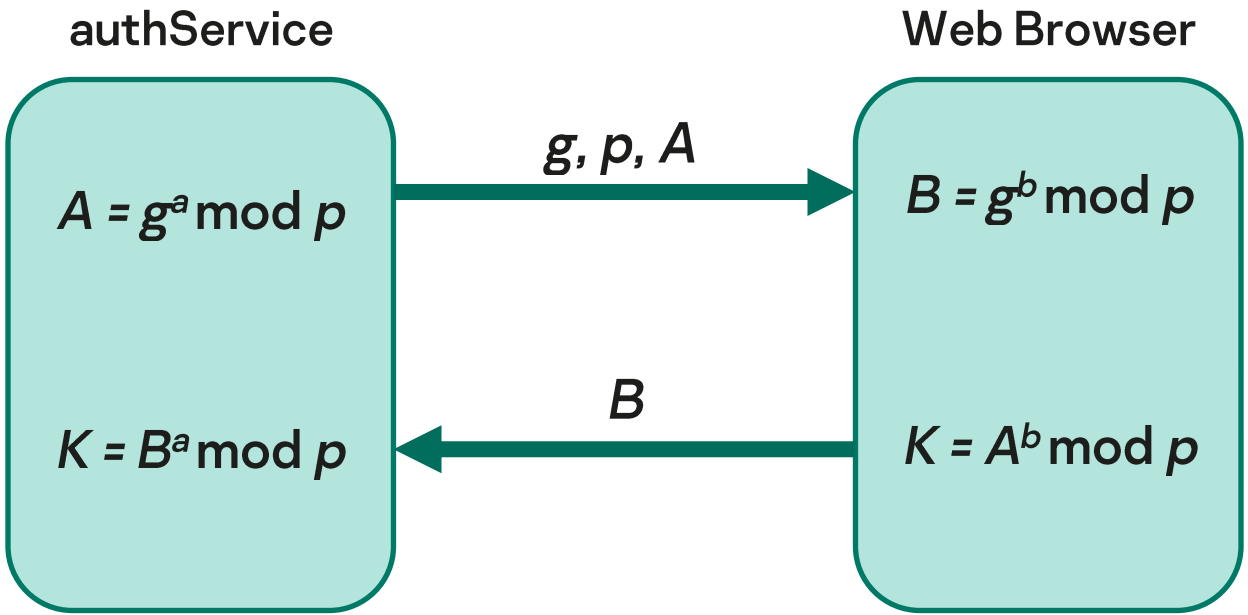


- Инициализация IPC-соединений
- Авторизация, инициализация сессии
- Работа
- **Завершение сессии**

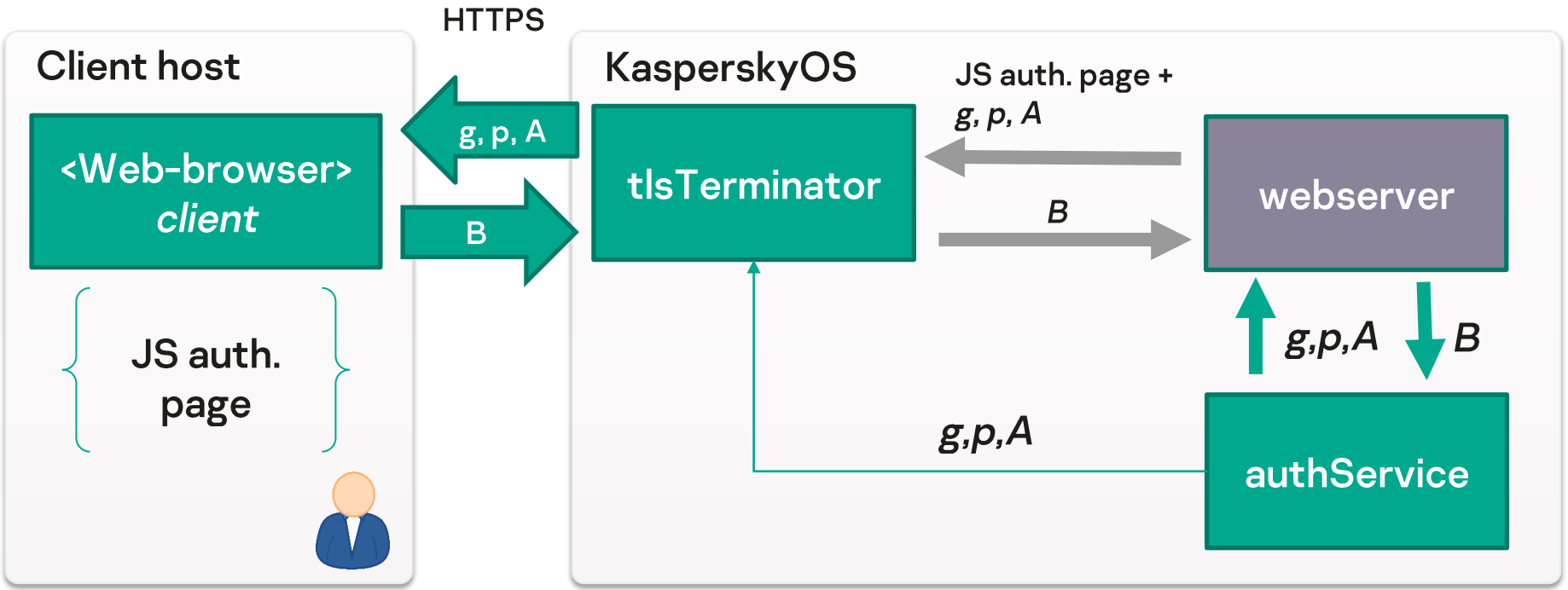
Передача критической информации



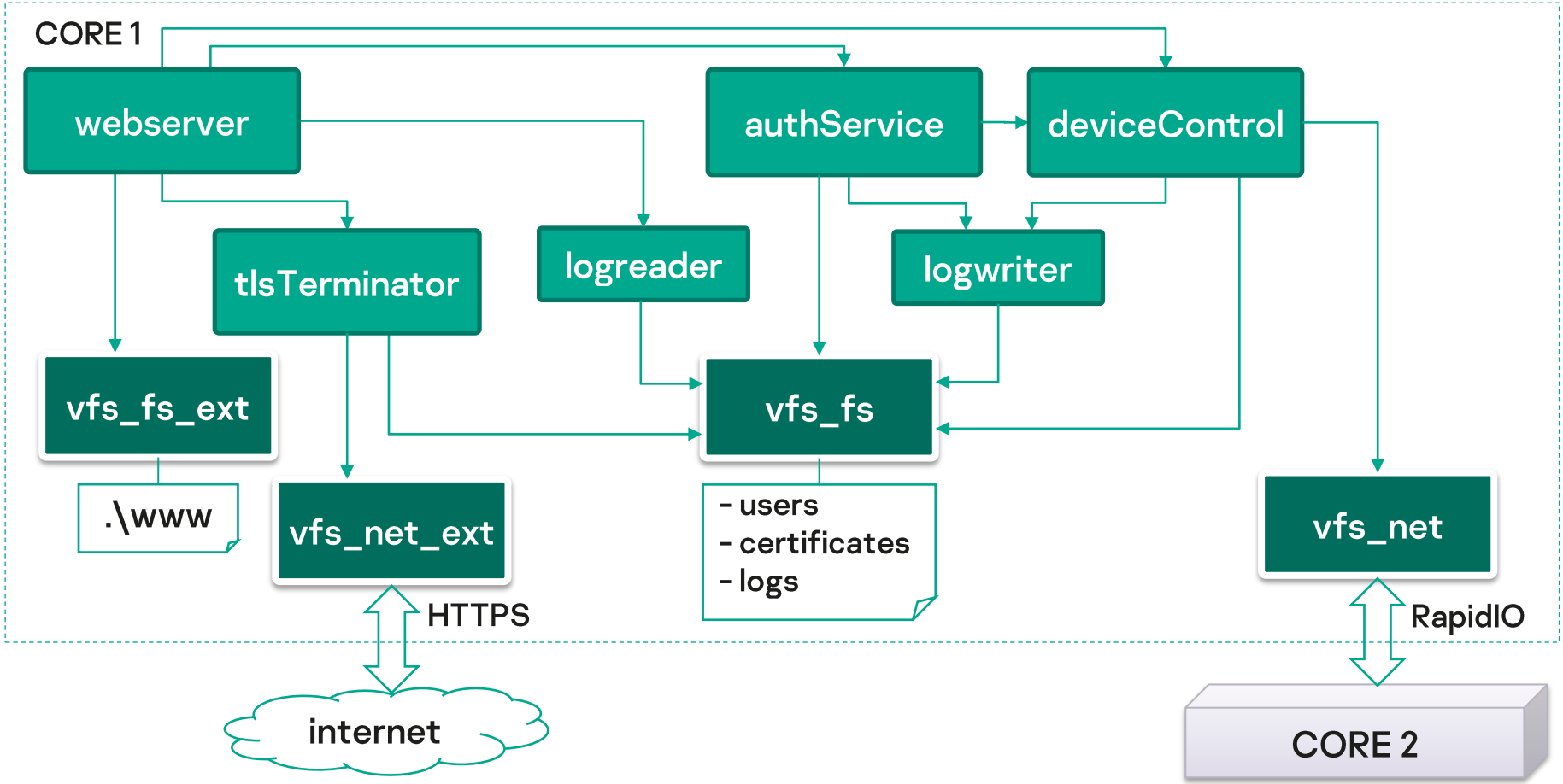
Использование схемы Диффи — Хеллмана



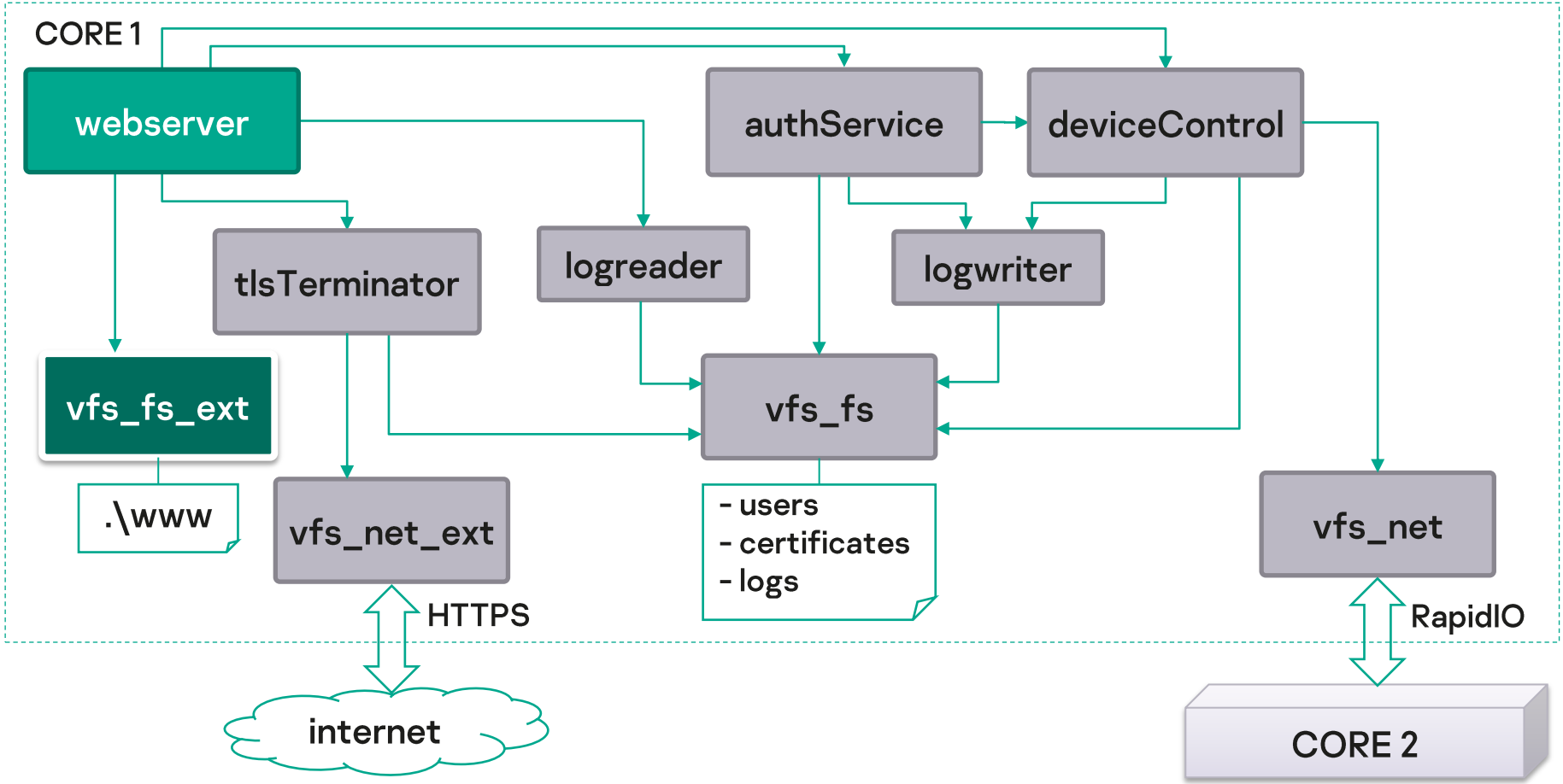
Передача критической информации с помощью DH-алгоритма



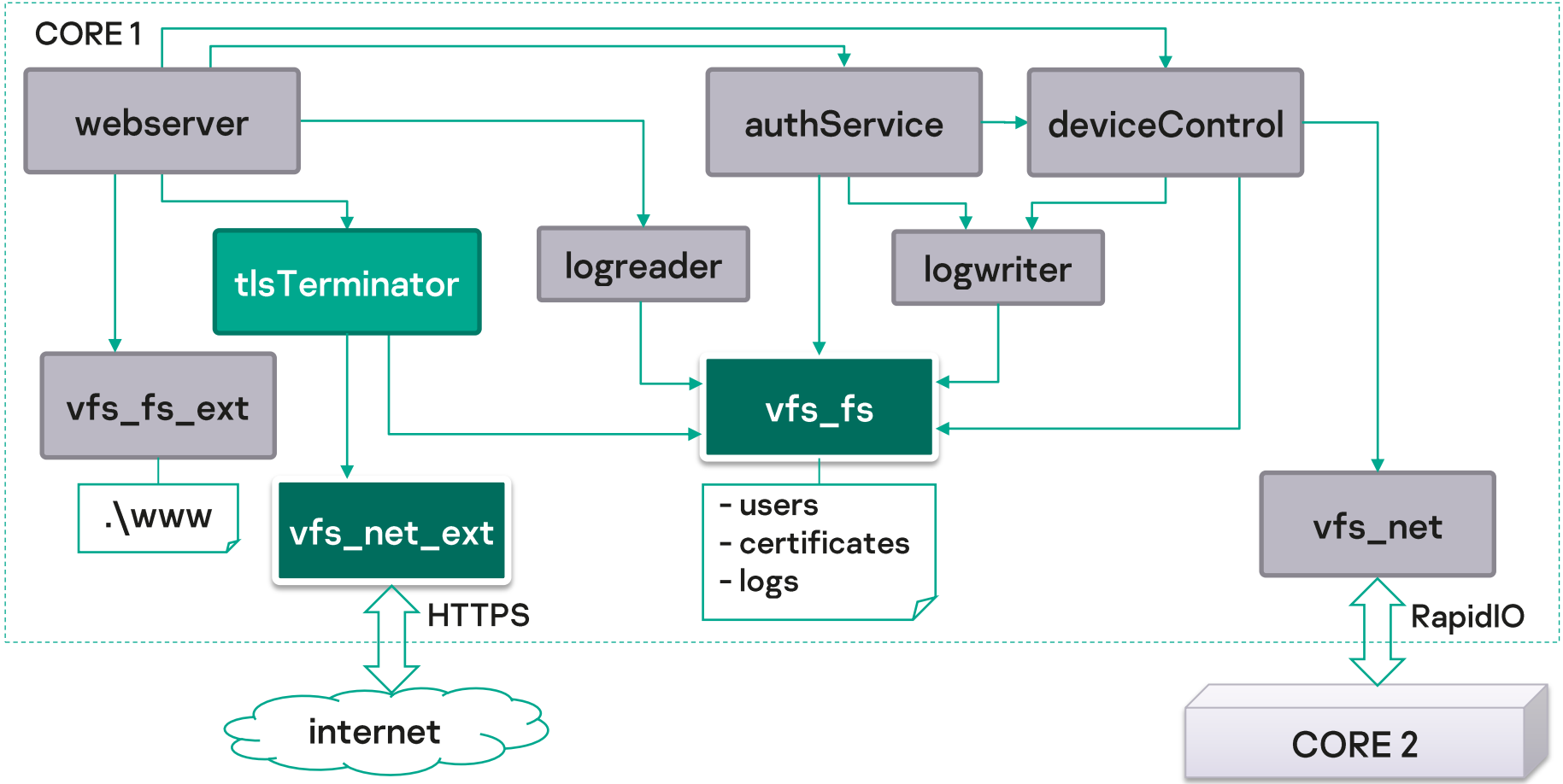
Общая архитектура решения



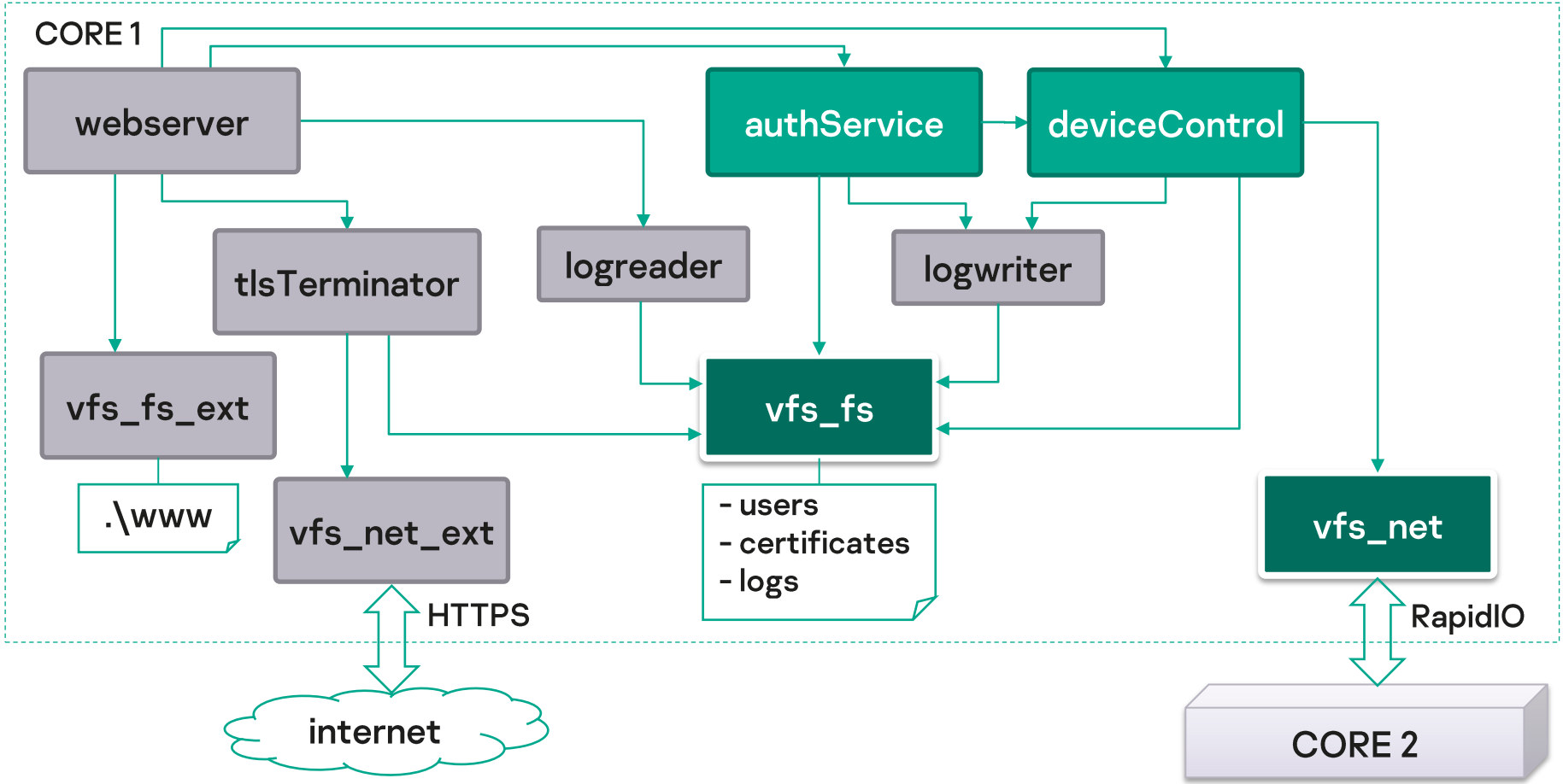
Безопасный доступ к служебной информации



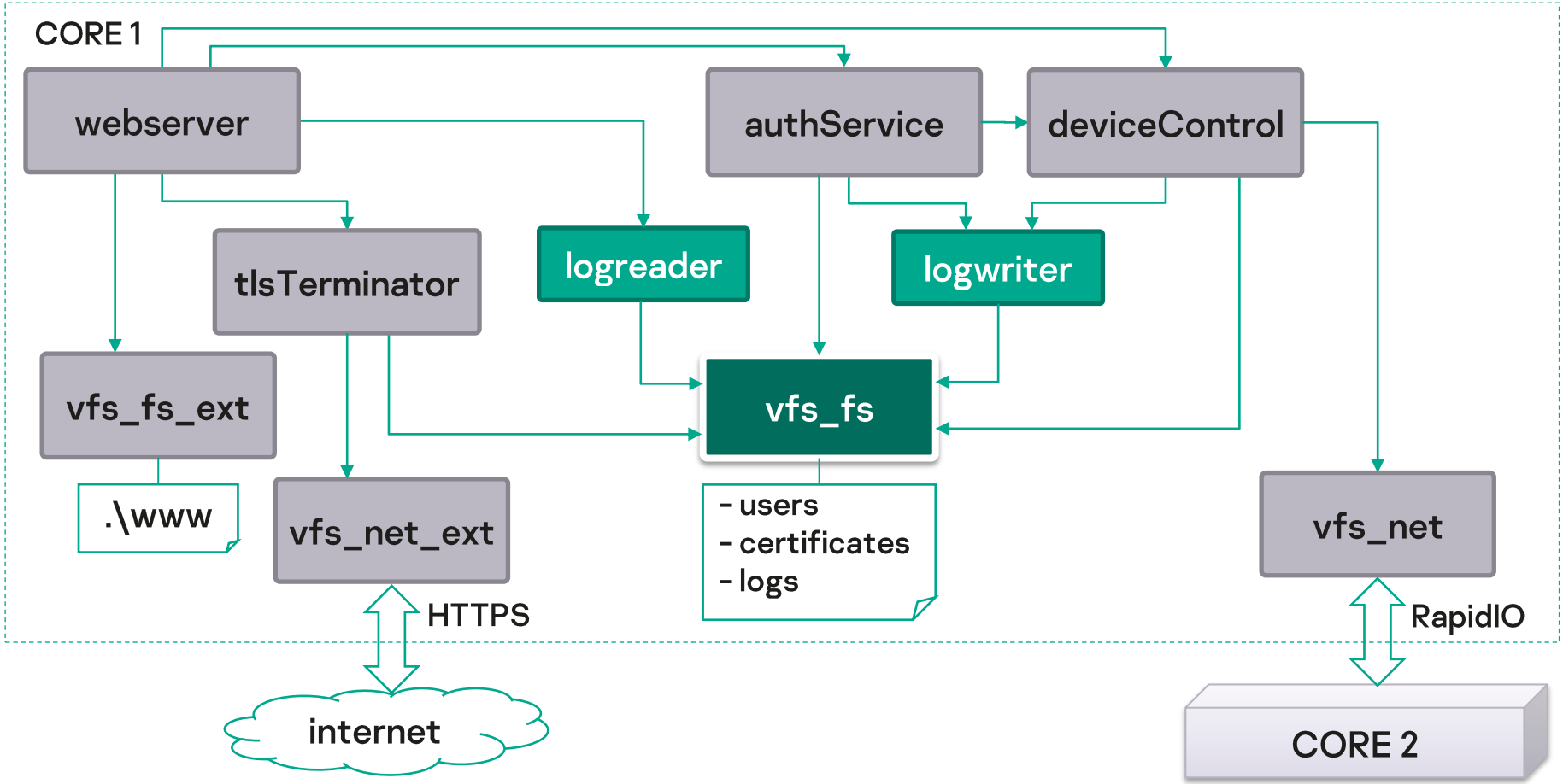
Безопасный доступ к служебной информации



Безопасный доступ к служебной информации



Безопасный доступ к служебной информации



Синергия совместной работы

ОСРВ Багет

Спасибо за внимание!

Сергей Барсуков — **Разработчик** — **Sergey.Barsukov@kaspersky.com**

Игорь Сорокин — **Руководитель группы системных исследований** — **Igor.Sorokin@kaspersky.com**

kaspersky