Повышение качества и безопасности разработки встраиваемых систем на основе типовых шаблонов проектирования

Игорь Сорокин
старший программный архитектор

kaspersky

Шаблоны проектирования

№ 1: Передача критической информации

Передача критической (с точки зрения безопасности) информации через недоверенные компоненты системы

№ 2: Контроль доступа к информации

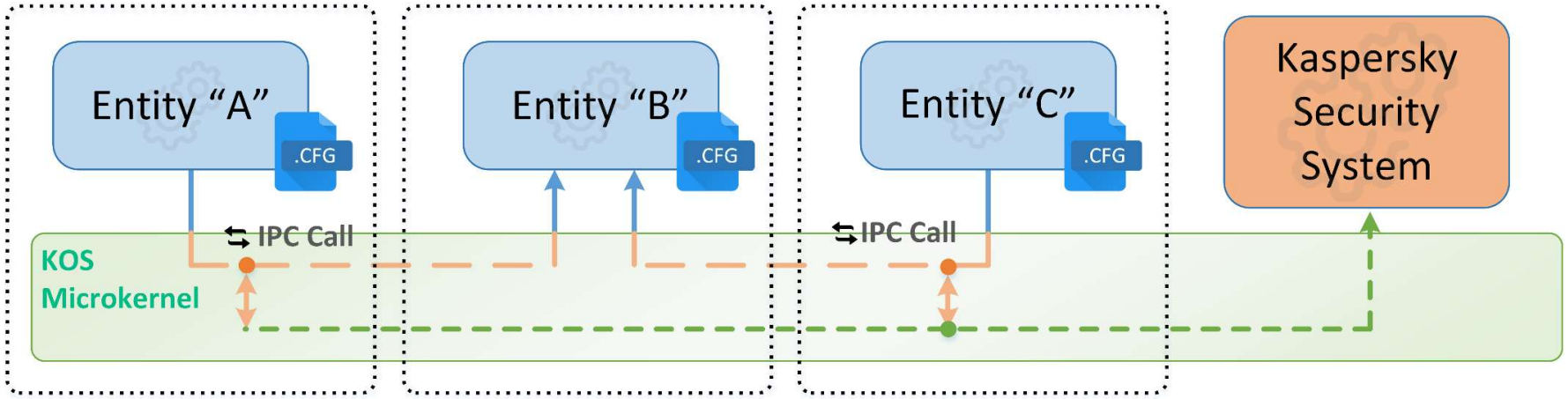
Обеспечение целостности и контроля доступа к различной по контексту критической информации

№ 3: Безопасное логирование

Организация безопасной работы с информацией (логирования) с возможностью обнаружения ее искажений

kaspersky

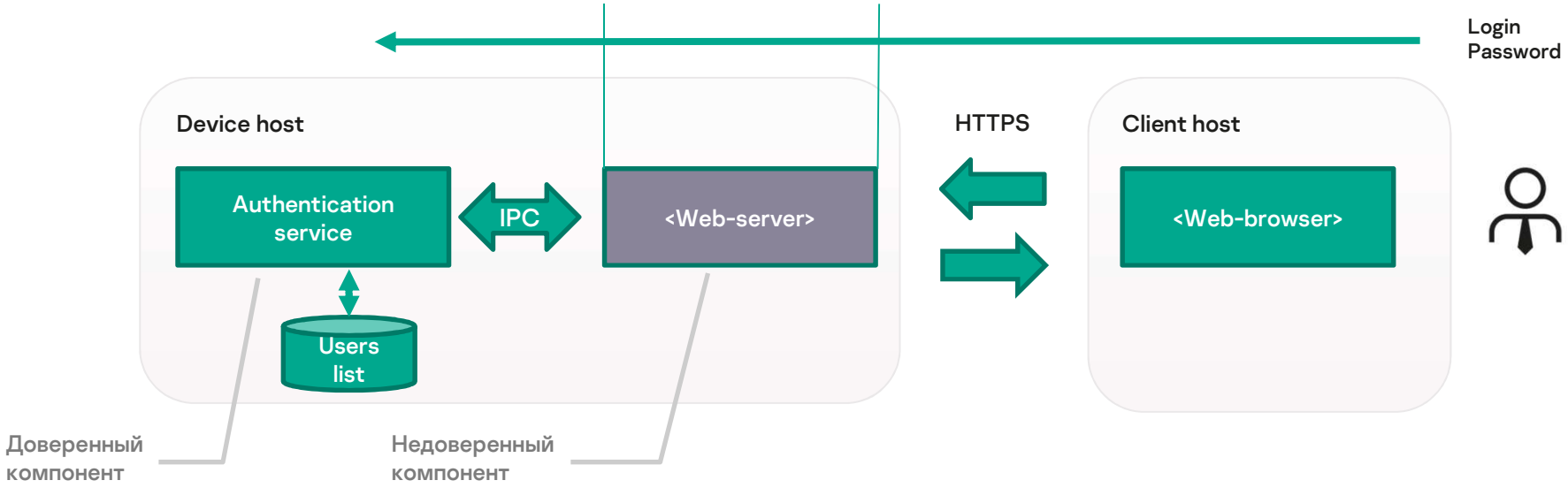
Базовые принципы KasperskyOS



1. Микроядерная операционная система
2. Изоляция приложений и их частей в отдельных доменах безопасности
3. Взаимодействие между доменами только через IPC-каналы
4. Контроль IPC-взаимодействий с помощью политик безопасности (Kaspersky Security System)

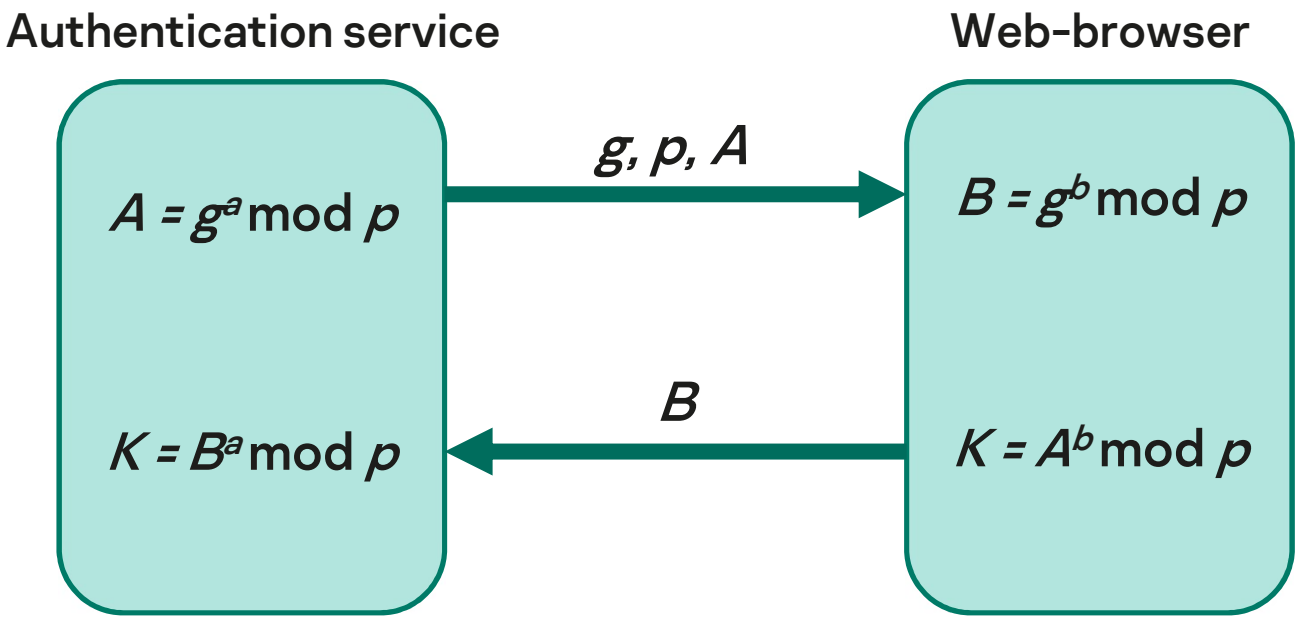
kaspersky

Передача критической информации через недоверенные компоненты системы



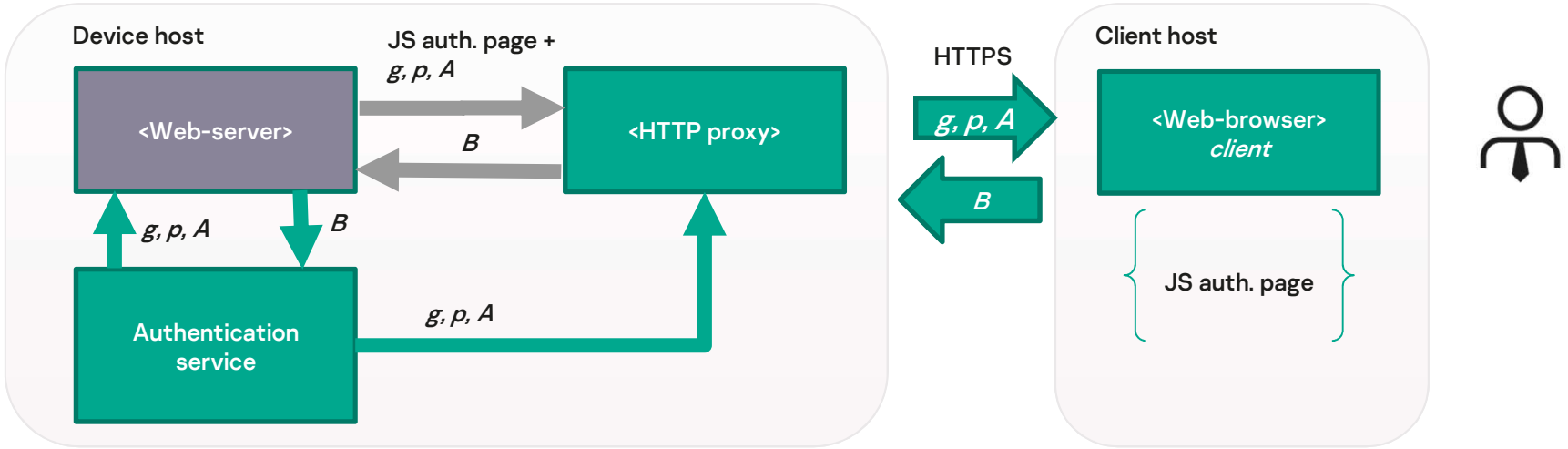
kaspersky

Передача критической информации через недоверенные компоненты системы



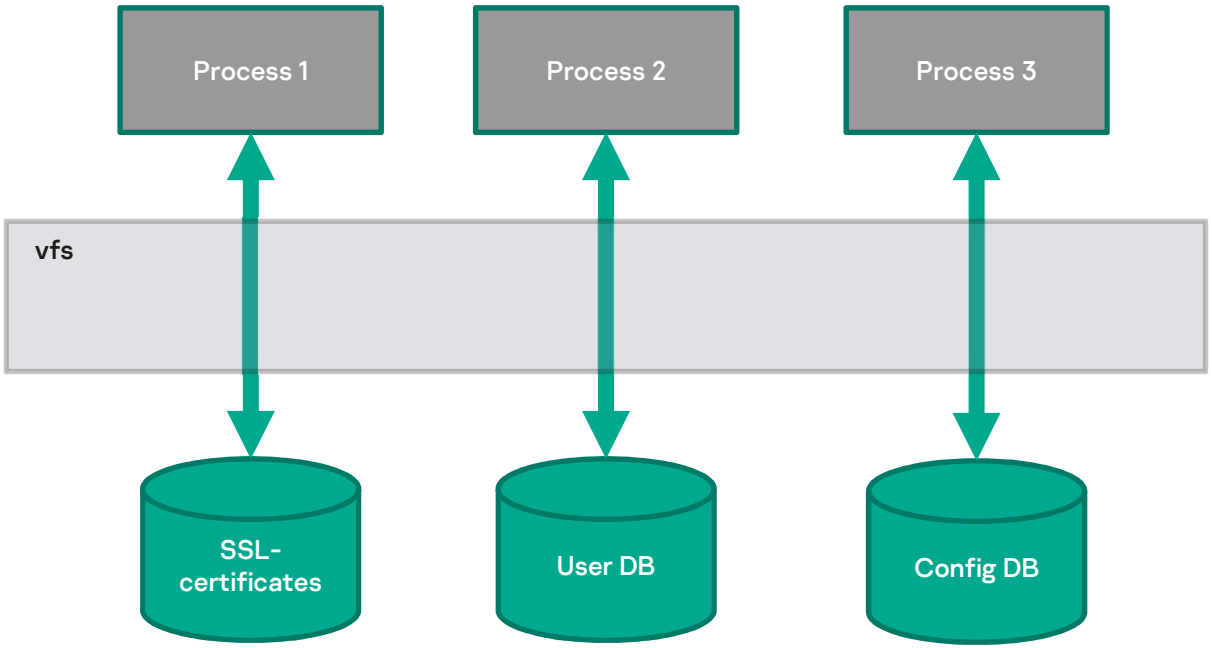
kaspersky

Передача критической информации через недоверенные компоненты системы



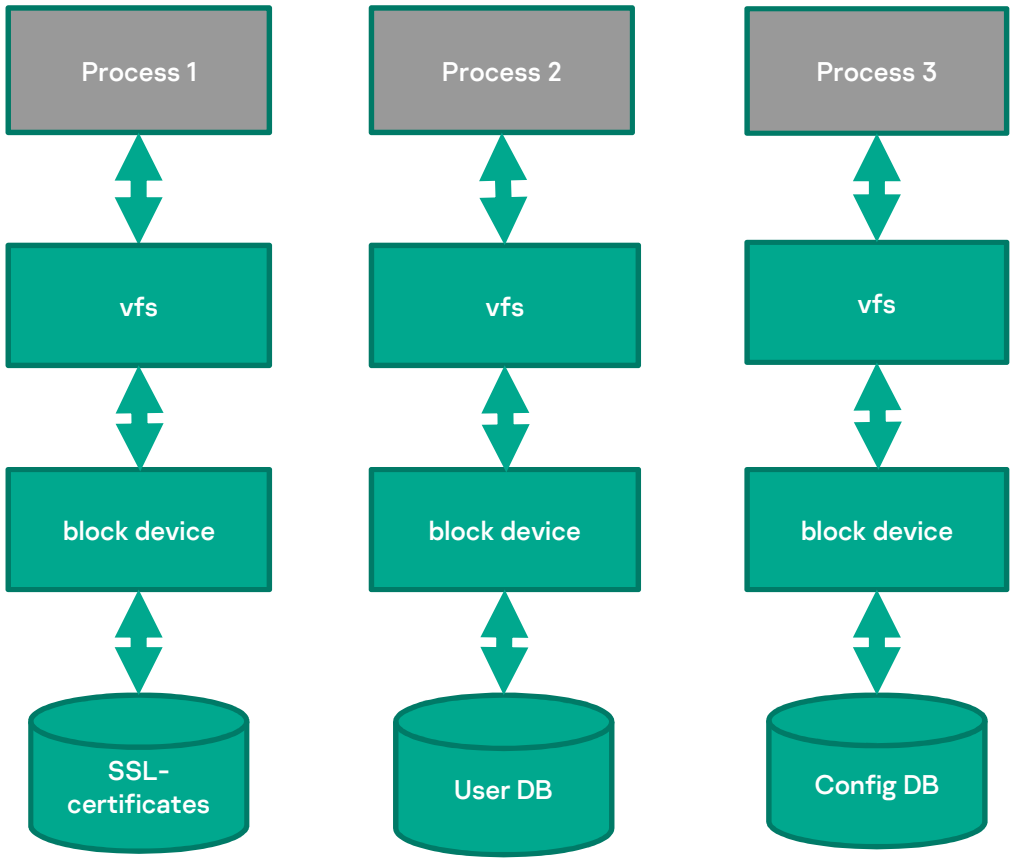
kaspersky

Обеспечение контроля доступа к информации



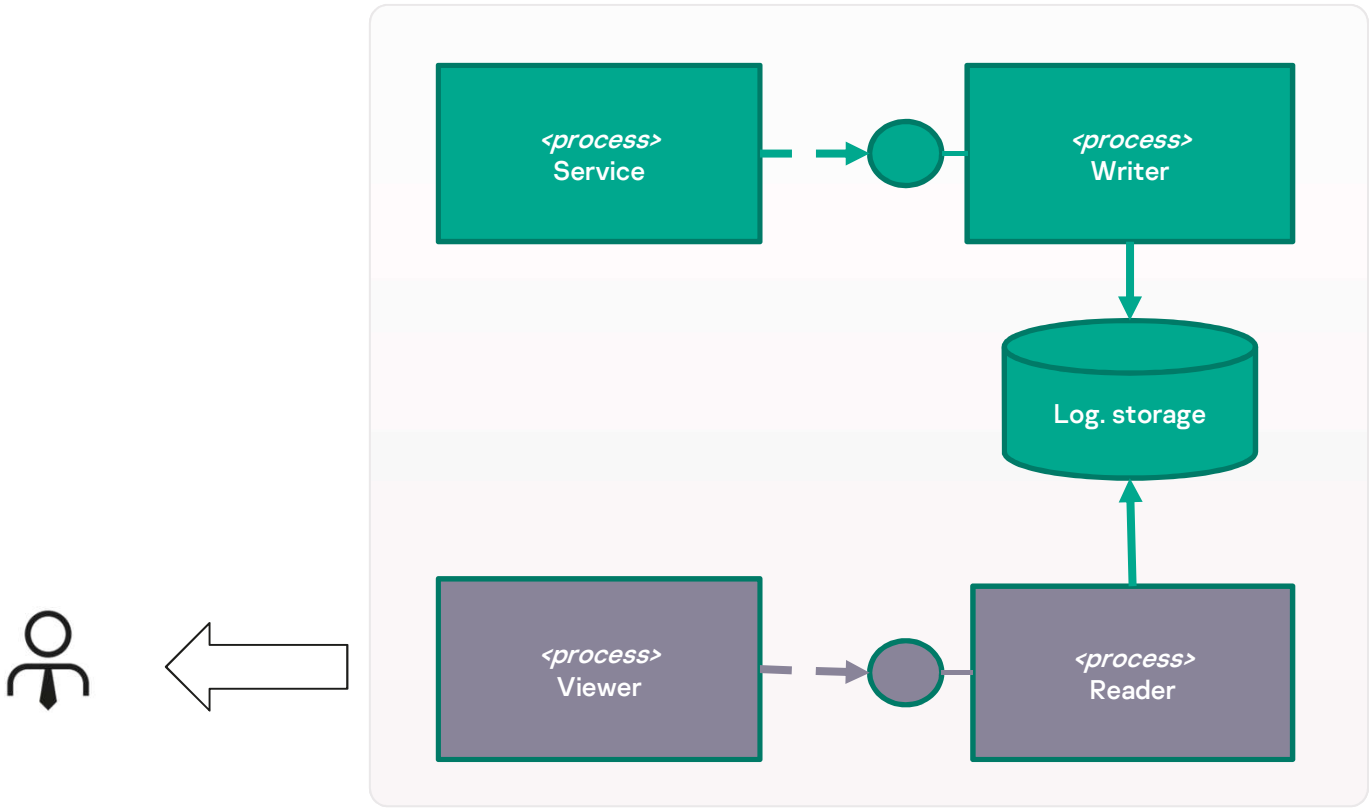
kaspersky

Обеспечение контроля доступа к информации



kaspersky

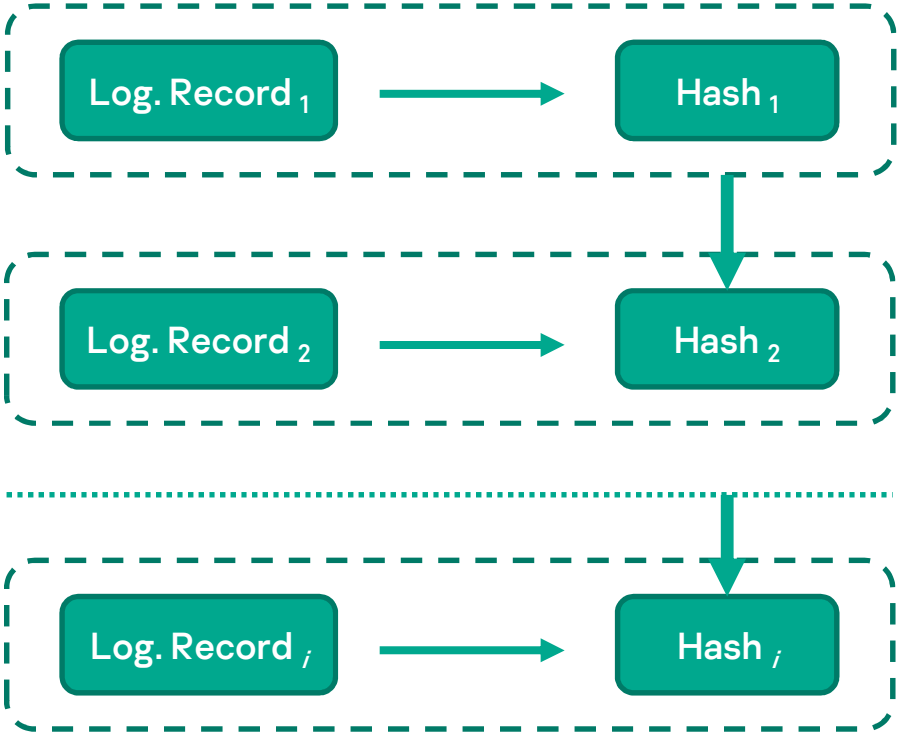
Безопасное логирование: разделение каналов записи и чтения



kaspersky

Безопасное логирование: обеспечение целостности

$$h_i = hash(record_i, h_{i-1})$$



kaspersky

Спасибо за внимание!

kaspersky