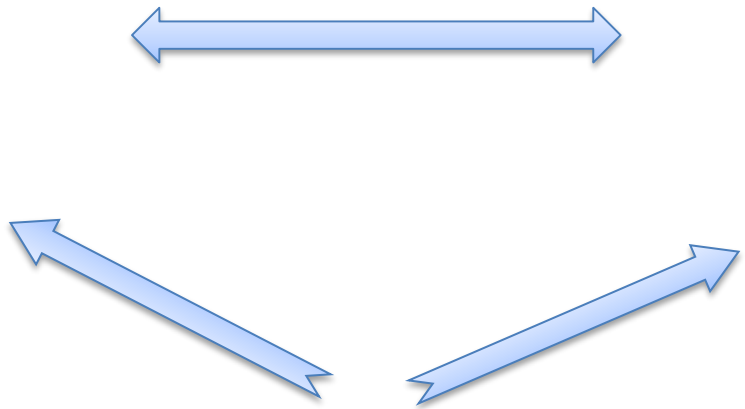
ИНТЕГРИРОВАННАЯ БЕЗОПАСНОСТЬ, КАК ОСНОВА SECURE BY DESIGN

Корольков Сергей
Доверенная платформа

ИНТЕГРИРОВАННАЯ БЕЗОПАСНОСТЬ

Угрозы

- Уязвимости прошивок и АО
- Утечки через встроенное ПО и СФ блоки
- НДВ в АО и встроенном ПО
- Манипулирование параметрами работы



Возможности

- Доверенная загрузка и корень доверия
- Изолированная среда для критических функций
- Безопасная среда для СКЗИ
- Защищенное хранение данных
- Контроль работы на аппаратном уровне
- Мониторинг и управление

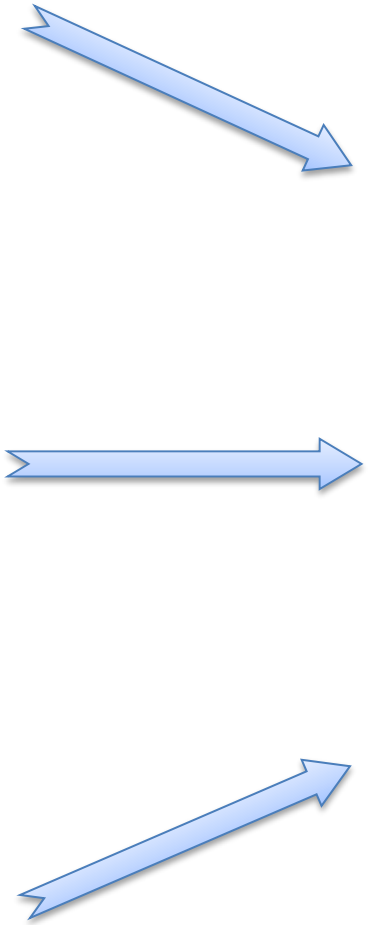
Развитие технологий

- Информационные системы «теряют» границы
- Все взаимодействует со всеми
- Рост и развитие интегрированных возможностей
- Автономные системы и «умные» устройства
- Смещение в сторону аппаратных возможностей

Интегрированная безопасность как предметная область

ОБЛАСТЬ ИНТЕГРИРОВАННОЙ БЕЗОПАСНОСТИ

- Реализация функций безопасности
  - Корень доверия
  - Доверенная загрузка
  - Среда для критических функций
  - Криптомодули
  - Доверенное хранилище
  - Контроль состояния
  - Отключение недоверенных блоков
- Служебные функции
  - Управление критическим АО
  - Удаленное управление
  - Мониторинг
- ЖЦ в процессе эксплуатации
  - Обновления
  - Вывод из эксплуатации



ПО пользователя

- Пользовательские приложения
- API и сервисы
- Драйверы
- Пользовательская ОС
- Загрузчик пользовательской ОС

Встроенное ПО

- UEFI/BIOS
- Опциональные приложения безопасности
- **Приложения безопасности**
- API и сервисы (опционально)
- Драйверы (опционально)
- ОС (опционально)
- Начальный загрузчик устройства

Служебное АО

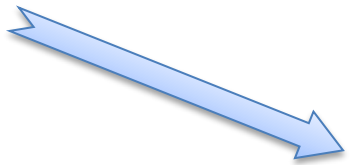
- AMT/IMM и др.
- Служебные ядра СнК
- **ARM TZ**
- **TPM**
- **Криптомодули, RNG**
- **OTP, eFuse, таймеры и др.**

Область интегрированной безопасности

SECURE BY DESIGN

Ожидание:

- Безопасность как равнозначная часть функционала
- Доступно пользователю без применения наложенных средств
- «Сквозная» реализаций функций безопасности
- Доступно производителю следующего уровня
- Опирается на ЭКБ



Требование:

- Безопасность как часть функционала во всем стеке АО и ПО
- Доступно производителю следующего уровня
- Опирается на ЭКБ

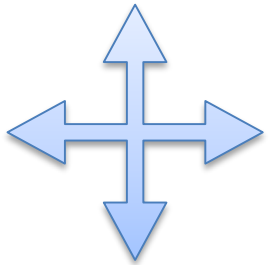
ДОВЕРИЕ vs БЕЗОПАСНОСТЬ vs РОССИЙСКОЕ

Secure By Design

- Затрагивает аспекты безопасности и доверия
- Позволяет комбинировать доверенное/недоверенное и российское/нероссийское
- Позволяет достичь требуемого уровня доверия и безопасности

Доверенное

- Безопасность процедур разработки
- Глубина верификации (сертификации)
- Достаточность функции безопасности
- Отсутствия ограничений на использование



Российское

- Набирает требуемое количество баллов по ПП
- Возможности глубокой верификации
- Отсутствие ограничений на использование

Безопасное

- Обладает требуемым функционалом
- Устойчивое к атакам
- Доверено загруженное
- Целостные критические компоненты
- Верифицированное состояние

Вопросы