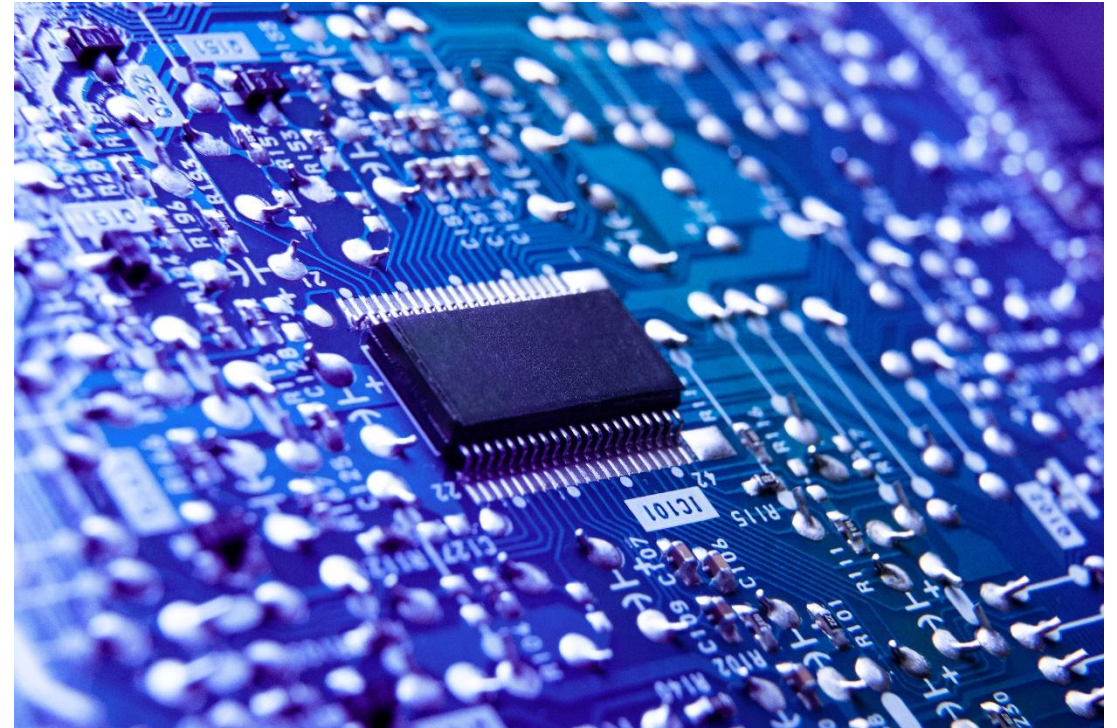


ТРМ. Как обрести почву под ногами и начать ей доверять?

Василий Николаев
Cryptography Services

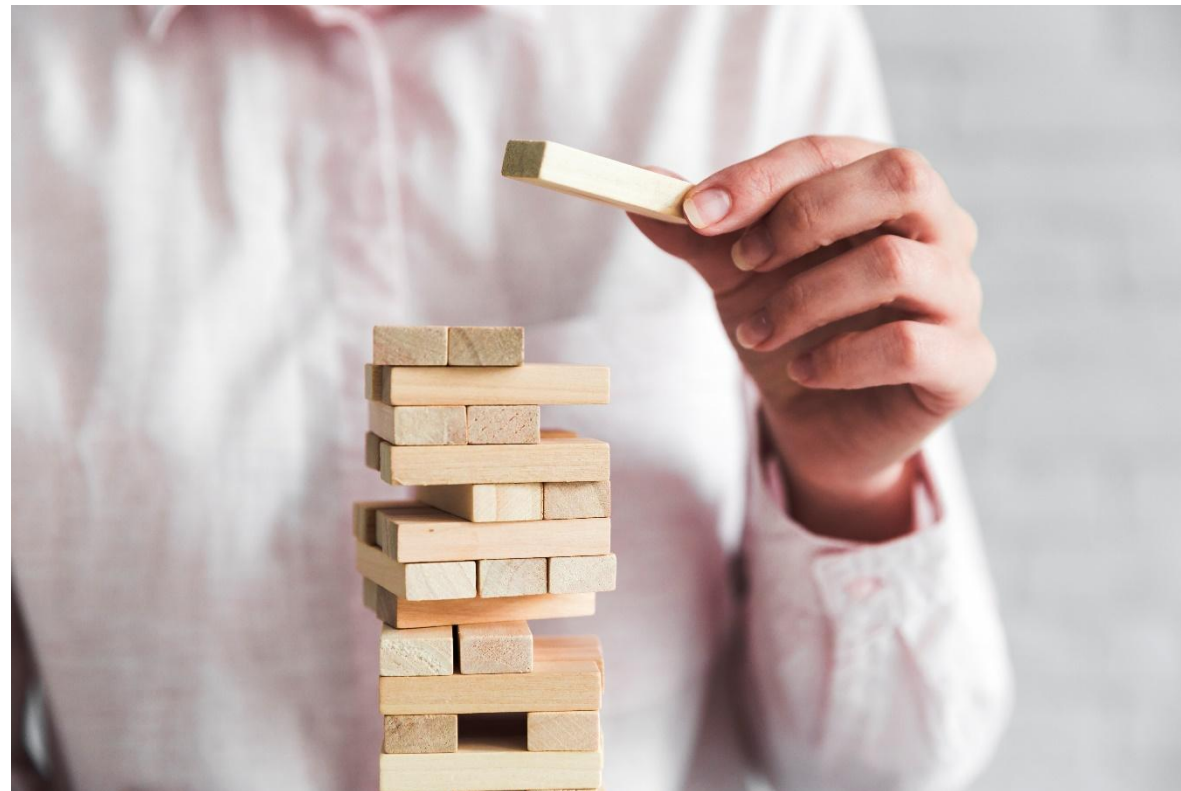
Trusted Platform Module

- Аппаратный (почти всегда) модуль.
- Ключевое хранилище.
 - Корень доверия – ЕК.
- Криптографический API.
- Platform Configuration Registers
- Единый интерфейс (TCG).



Обычные сценарии использования

- ФДСЧ
- Шифрование дисков
- Доверенная криптография
- Хранение ключей
- DAA
- Secure Boot
- Аттестация платформ



Потенциальные проблемы

- Отлучение от PKI вендоров.
- Слабое исследование протоколов DAA и аттестации.
- ГОСТ-алгоритмов нет как класс.
- Пора думать про постквантовую криптографию.
- А что с требованиями регуляторов?



Вопросы?



Василий Николаев
Software Developer
Cryptography Services
vasnikolaev@yandex-team.ru