



Импортюлучшение

корпоративного центра сертификации
Microsoft CA в Т-Банке

SAFETECH 

 **Т БАНК**



Сертификаты
применяются повсеместно
в инфраструктуре любого
масштаба:

- VPN сервисы
- E-mail
- Аутентификация и шифрование данных
- Взаимодействие оборудования
- Доменные сервисы (Active Directory)
- Вход пользователей

И многое другое ●●●



Внешнее давление



Гетерогенный IT-ландшафт



- Microsoft приостановил деятельность на территории России
- SSL.COM, LET'S ENCRYPT, ZERO SLL поступили аналогично
- Блокирующие санкции и риски невыполнения требований по импортозамещению

- Машины на Windows / MacOS / Linux
- iOS / Android – устройства
- Софт собственной разработки
- Железо и софт от разных производителей

- Российская и западная криптография, HSM
- Классическая виртуализация и контейнеризация (*Docker, OpenShift*)
- Поддержка отечественных ОС и СУБД
- Микросервисная легко масштабируемая архитектура
- Возможность изоляции PKI-сервисов
- Поддержка различных протоколов:

MS-WSTEP

полноценная замена
Microsoft CA

SCEP

работа с MacOS, iOS,
Android, Linux, Cisco

REST API

интеграция сторонних
систем самостоятельной
и сторонней разработки

CMP

базовый стандарт для API
OpenSSL, Bouncy Castle,
Nexus и других

EST

системы MDM

ACME

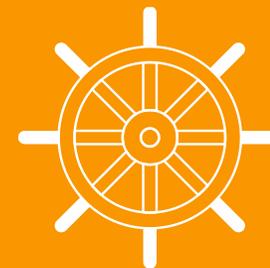
TLS для веб-порталов,
Kubernetes, Openshift

О ЗАДАЧАХ

ЗАДАЧИ, РЕШАЕМЫЕ Т-БАНКОМ



Учесть
ландшафт



Повысить
управляемость

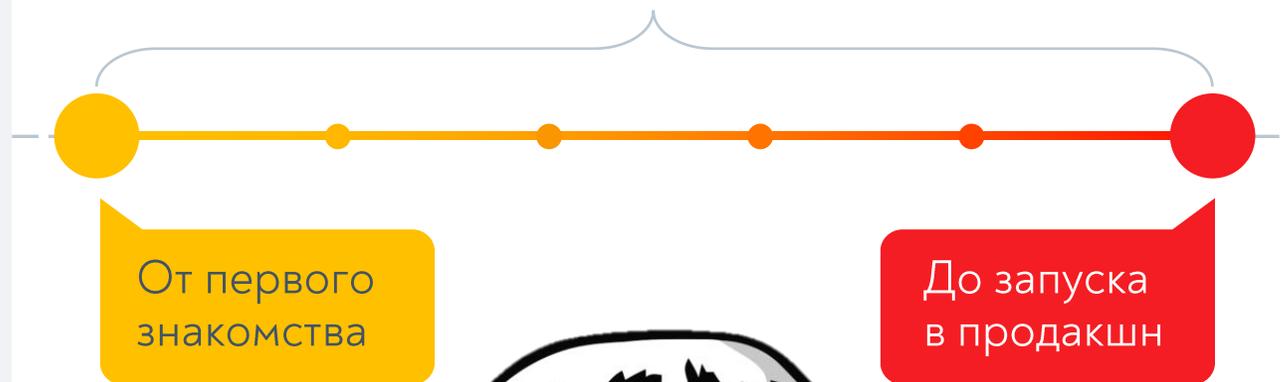


Повысить
безопасность



Выполнить
требования
регуляторов

6 МЕСЯЦЕВ

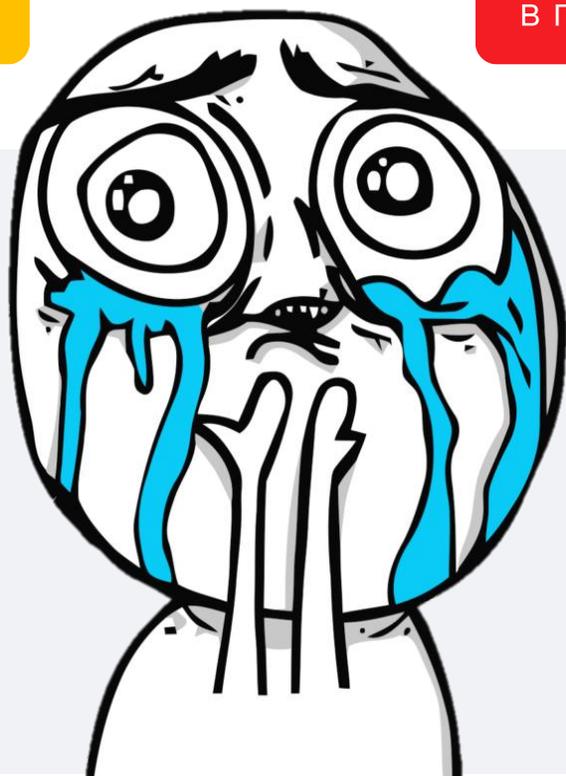


4 месяца
срок пилота

2 месяца
срок проекта

2 больших
контуров сервисов СА

>10 000
сертификатов



-  Команда специалистов Т-Банка показала экспертизу экстра класса
-  За время пилотирования было обнаружено и исправлено несколько багов в продукте
-  Roadmap продукта значительно наполнился «на вырост»



ЦЕЛЬ ПРОЕКТА

Создание 2 контуров:

- **Внутренний**
Вся инфраструктура Группы «Т-Технологии»:
АРМ, серверы, сетевые устройства, WI-FI
- **Внешний**
Авторизация контрагентов по
mTLS-сертификатам



Дополнительная задача

бесшовный перевод на
новый СА инфраструктуры
Росбанка



РЕЗУЛЬТАТЫ ПРОЕКТА



Внутренний контур
(включая Росбанк)
полноценно работает
в продакшн



Внешний контур
работает в продакшн
и находится в стадии
совершенствования
процессов



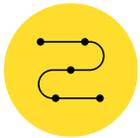
MS CA отключен
от выпуска новых
сертификатов
(оставлен только CRL)



Все новые
сертификаты
выпускаются
на **SafeTech CA**



Т-Банк особо отмечает:



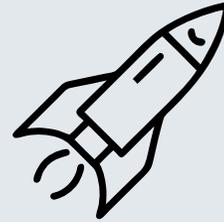
Четкий прогнозируемый roadmap



Быстрые доработки по сценариям SCEP, MS Enroll, NDES



Адекватная лицензионная политика



Планы на будущее:

- Публикация сертификатов в LDAP
- Хранение сертификатов в HSM
- ACME
- Развитие: статистика, отчеты, настройки

Спасибо
за внимание!



safe-tech.ru

+7 (495) 120-99-09

info@safe-tech.ru