
ГОСТ в OpenSSL:
12 лет
международного
взаимодействия
Технический
Центр
Интернет

Технический
Центр
Интернет

ГОСТ в OpenSSL: 12 лет международного взаимодействия

Дмитрий Белявский, ТЦИ

Калуга
24 сентября 2017 года

Дмитрий Белявский

- С 2010 – Технический Центр Интернет, https://tcinet.ru/
  Backend-провайдер для .RU/.РФ
- 2004-2006 – ООО «Криптоком», http://www.cryptocom.ru/
- OpenSource проекты:
  XMLSec
  OpenSSL
  Net::DRI
  …

ГОСТ в OpenSSL: история

Технический
Центр
Интернет

0.9.8: нет ГОСТа, отдельный патч

1.0.0: ГОСТ engine, патчи по мелочи

2014: Heartbleed

1.1.0: ГОСТ поддержан через engine
engine отдельный проект

Версия 0.9.8

Технический
Центр
Интернет

Исходное состояние: RSA, DSA, (EC)

Рынок: проприетарные решения

Криптоком: патч для добавления алгоритмов

- Нарушение бинарной совместимости

+Основа для переговоров

Разработка версии 1.0

Технический
Центр
Интернет

Криптоком:
деньги + патч

+

OpenSSL Team:
архитектура

=

Версия 1.0

Libcrypto:
Engine API

LibSSL:
Список и много case

Патчи:
Много мелочёвки по спискам

2014: HeartBleed

Технический Центр Интернет

«Уязвимость масштаба интернета»

↓

Индустрия увидела проблему

↓

Расширение Core Team

↓

Выработка процедур и RoadMap

Разработка версии 1.1

Технический Центр Интернет

Новые стандарты по ГОСТ + OpenSSL Team: личное знакомство = Версия 1.1

Engine:
Отдельный проект

Core:
Переработка архитектуры

LibSSL:
Выделение управляющих структур

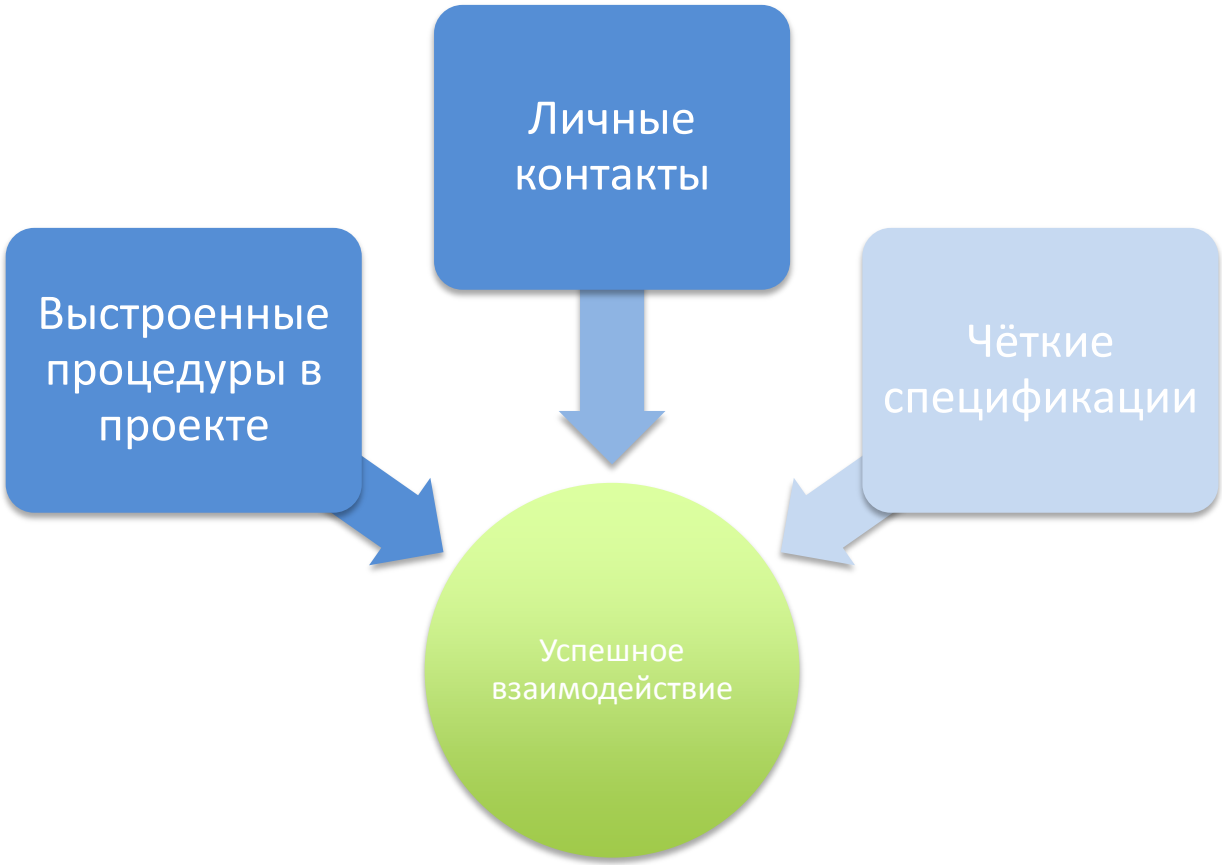
Не только криптография

Технический
Центр
Интернет

- Русские буквы
- Утечки памяти
- X.509 extensions

Секреты эффективности

Технический Центр Интернет



Добавить gost engine в дистрибутивы

- AltLinux
- Debian
- RedHat
- …

Ссылки

- ООО «Криптоком»
  http://www.cryptocom.ru/
- OpenSSL
  https://www.openssl.org/
- ТК26
  http://tc26.ru/
- GOST engine
  https://github.com/gost-engine/engine
- Certificate limitation profile
  https://github.com/beldmit/clp

Вопросы?

beldmit@tcinet.ru