Экосистема TLS в России

Алексей Рогдев

Генеральный директор ООО «ТЦИ»

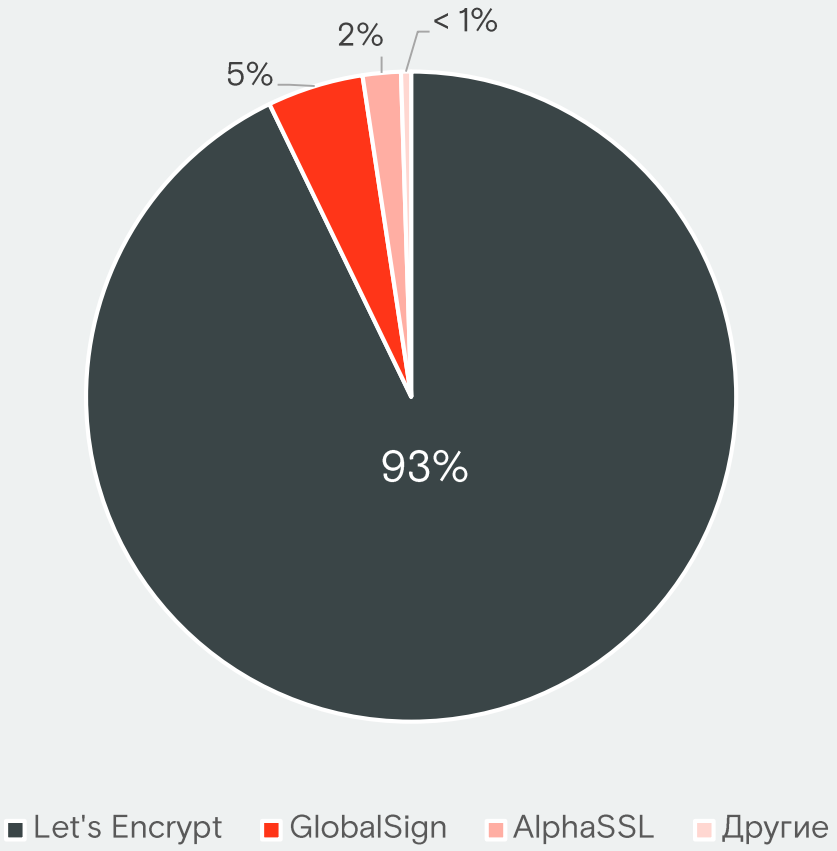
Текущая ситуация

Проблемы с общедоступным PKI:

- сертификаты для веб-ресурсов (**TLS**);
- сертификаты для электронной почты (**S/MIME**);
- сертификаты для **подписи кода** (для разработчиков ПО);
- сертификаты для **eSIM/eUICC**.

TLS-сертификаты:

Распределение по ЦС*



*Статистика за март 2023 года по данным ресурса «Домены России» (statdom.ru)

Создание в России распределенной системы PKI на основе отечественных решений

Отечественные решения в области TLS

Национальный удостоверяющий центр (Минцифры):

- Получение TLS-сертификатов путем подачи заявки **на портале Госуслуг**
- **Корневой сертификат НУЦ** является **доверенным** в «Яндекс.Браузер» и «Atom»

Центр сертификации ТЦИ (tlscc.ru):

- Самостоятельно **разработанное с нуля** ПО →
- **Отсутствие зависимости** от стороннего ПО (в т.ч. зарубежного) →
- **Отказоустойчивость** и **безопасность** использования

Центр сертификации ТЦИ

tlscc.ru

- Выпуск сертификатов как ECDSA, так и ГОСТ для одного домена и Wildcard
- Выпуск сертификатов ECDSA для электронной почты (S/MIME)
- Сертификаты сроком на 90 и 365 дней
- Поддержка Certificate Transparency Log Яндекса и Вконтакте
- Автоматизация ряда функций (генерация CSR и проверка домена)

Планируется добавление функционала **по выпуску сертификатов для подписи кода**, а также создание **корпоративного центра сертификации**.

Система регистрации:

последние изменения и планирующиеся обновления

Последние изменения в Системе регистрации

ЕСИА (6 марта 2023 года):

- Добавлен атрибут **oidEsia** в объект **Contact** (хранение идентификатора объекта в Единой системе идентификации и аутентификации)
- На текущий момент поле **не обязательно** к заполнению
- Подготовка к **изменениям в законодательство** (связанным с внедрением регистрации доменных имен с использованием ЕСИА)

Планирующиеся обновления

RDAP (29 мая 2023 года)**:**

- **Запуск** модуля поддержки RDAP **для реестра .SU**
- **Изменения ответа** модуля поддержки RDAP **для реестров .RU и .РФ** (при запросе информации о **доменном имени**, которое содержится в **стоп-листе**)

Планирующиеся обновления

Новая Система регистрации:

- Переход на **новое ПО** без изменения функционала

Нормализация данных контактов администраторов .RU/.РФ:

- Упорядочение данных в **объектах Contact**
- Создание **новой модели данных** объекта Contact, максимально соответствующей **модели данных ЕСИА**

Спасибо за внимание!

Алексей Рогдев

Генеральный директор ООО «ТЦИ»