Единый стандарт ключевого носителя.

Миф или реальность?

Стандартизация PKI в России:

- RFC 4357. Additional Cryptographic Algorithms for Use with GOST 28147-89,GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms.
- RFC 4490. Using the GOST 28147-89, GOST R 34.11-94,GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS).
- RFC 4491. Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile
- Драфты TLS.
- …

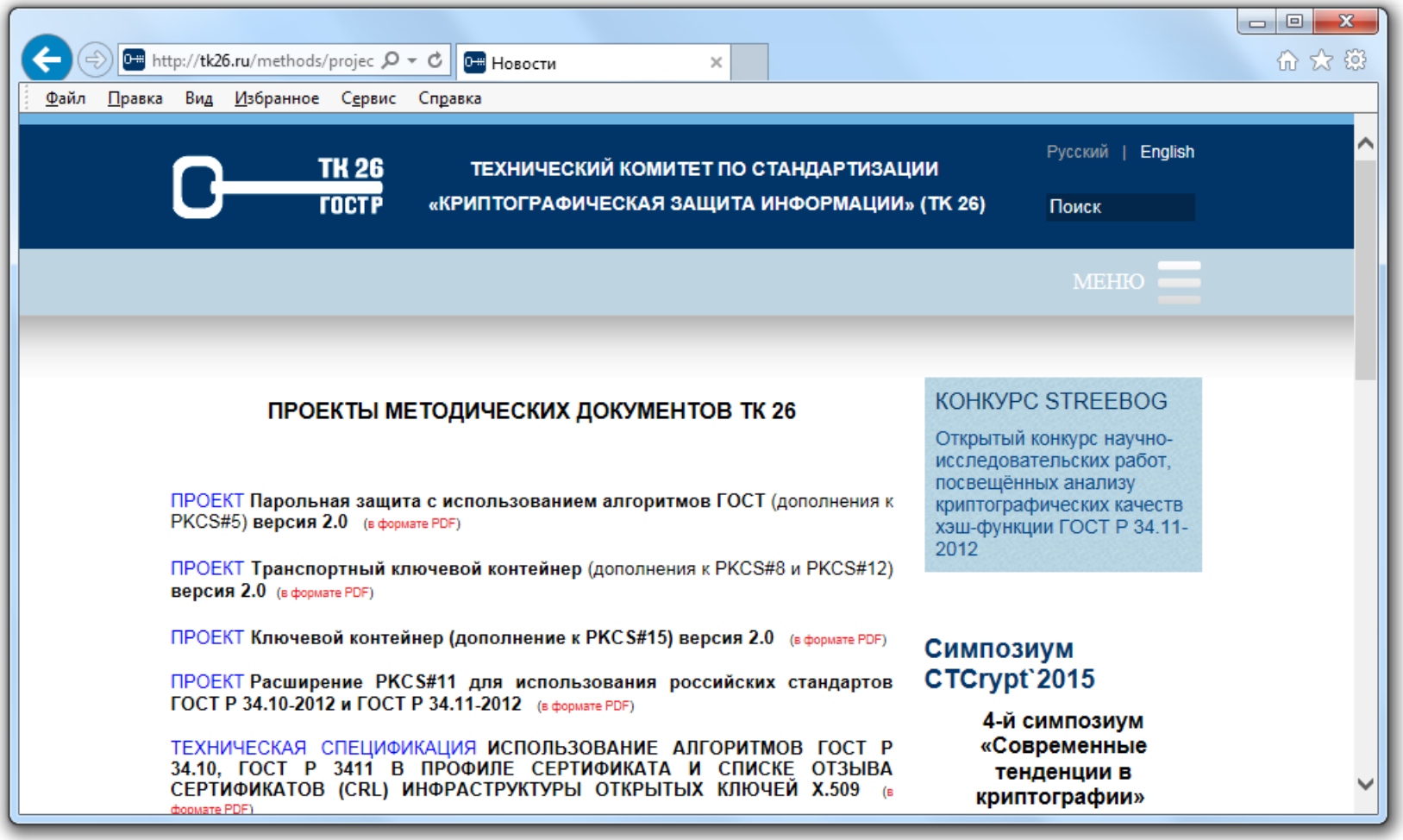
Рекомендации ТК26

- “Методические рекомендации технического комитета по стандартизации. Парольная защита с использованием алгоритмов ГОСТ. Дополнения к PKCS#5 Версия 1.0”
- “Методические рекомендации технического комитета по стандартизации. Транспортный ключевой контейнер. Дополнения к PKCS#8 и PKCS#12. Версия 1.0
- “Методические рекомендации технического комитета по стандартизации. Ключевой контейнер. Дополнение к PKCS#15. Версия 1.0

Рекомендации ТК26 2014 г.

- “Методические рекомендации технического комитета по стандартизации. Парольная защита с использованием алгоритмов ГОСТ. Дополнения к PKCS#5 Версия 2.0”
- “Методические рекомендации технического комитета по стандартизации. Транспортный ключевой контейнер. Дополнения к PKCS#8 и PKCS#12. Версия 2.0
- “Методические рекомендации технического комитета по стандартизации. Ключевой контейнер. Дополнение к PKCS#15. Версия 2.0

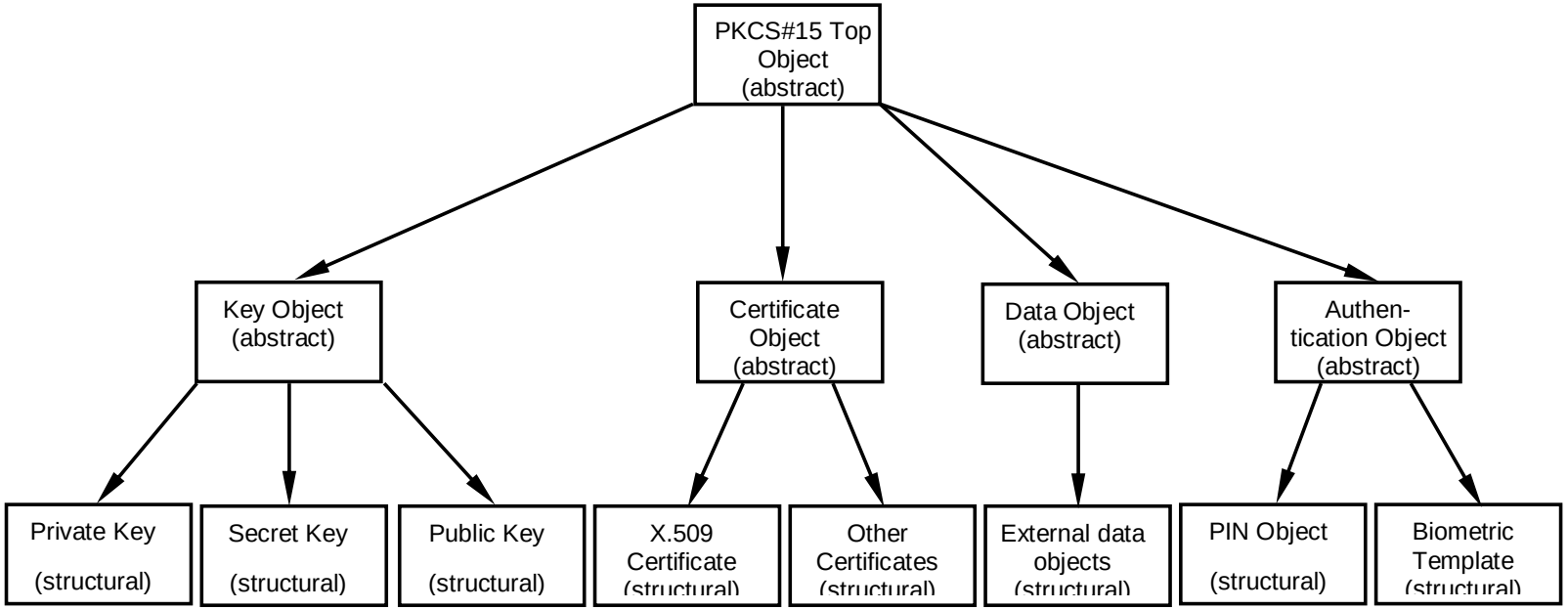
http://tk26.ru/methods/project/



Открытая реализация PKCS#15

http://www.factor-ts.ru/support/pkcs15.zip

Используемые типы из PKCS#15



Дополнительные OID.

- Начальное заполнение ПДСЧ (1. 3.6.1.4.1.13312.503.1.1)
- Список отзыва сертификатов (1. 3.6.1.4.1.13312.503.1.2).

Резюме.

- Открытый стандарт.
- Есть свободно распространяемая кросс-платформенная реализация.
- Гибкий стандарт. Допускает свободное расширение.
- Стандарт прошёл экспертную оценку в профильных организациях.

Контакты:

Федотов Андрей Владимирович
Заместитель начальника отдела
разработки и внедрения СЗИ
департамента телекоммуникационных систем ООО «Фактор-ТС».
Тел. +7 (495) 644-31-30
fedotov@factor-ts.ru