



С.М. Муругов,
генеральный
директор
ООО "Тон Кросс"

На мой взгляд, ситуацию в России на конец 2006 г. можно охарактеризовать как начало перехода из количества в качество. На ноябрьском PKI-форуме-2006 в Санкт-Петербурге были представлены количественные показатели соотношения числа заявленных УЦ и потенциальных пользователей, что ставит нас в один ряд со странами, в которых PKI-проекты стартовали много ранее, чем у нас.

Следующим логическим шагом, скорее всего, будет укрупнение, технически более грамотное объединение доменов доверия и интеграция различных PKI-систем с появлением новых сервисов. На этом пути потребуются решение некоторых задач, которые уже сейчас вполне обозначены. Перечислю некоторые из них.

Во-первых, для интеграции PKI-систем потребуется обеспечить их фактическое соответствие требованиям международных рекомендаций, другими словами, потребуется создание тестового материала и комплекта самих тестов, аналогичного принятому в мировой практике комплекту тестов Национального института стандартов и технологий (NIST) США.

Во-вторых, на рынке должны появиться конкурентные аппаратные решения, поддерживающие отечественные криптографические алгоритмы, рассчитанные на выполнение "на борту" криптографических операций и работу с ключевым материалом для размещения как на стороне пользователя,

так и на стороне серверов. Для этого потребуется как минимум разработка отечественного профиля PKCS#11 и создание условий для его международного признания, и только после этого следует ожидать появления отечественных HSM, USB-токенов и смарт-карт.

В-третьих, задачи международной интеграции PKI-систем и трансграничного электронного документооборота потребуют создание системы служб "Третьей доверенной стороны" в терминах X.842, или, как их еще называют, служб "Электронного нотариата".

В-четвертых, внедрение или переход к использованию так называемой "расширенной подписи", включающей в себя и "штампы времени" и другую служебную информацию, позволяющую более полно и достоверно принимать решение о действительности ЭЦП в соответствии и с ФЗ "Об электронной-цифровой подписи" (ФЗ "Об ЭЦП").

В-пятых, в связи с наметившимся укрупнением доменов доверия и принятым ФЗ "О персональных данных" потребуется предложить на рынке решения, обеспечивающие PKI-системе работу с персональной информацией пользователей в связке с внешне изданными сертификатами, не содержащими персональные данные. Наиболее очевидным видится использование в PKI-системах атрибутивных сертификатов и средств обеспечения их жизненного цикла.

И наконец, в-шестых, расширение предложений на рынке прикладных систем с компонентами отечественной PKI как отечественного, так и зарубежного производства. К последним в качестве примера можно отнести системы Oracle E-Business Suite, SSO, SAP и системы ЭДО различных производи-