УДК 681.3.06:519.248.681

ЦЕЛИ И ТРЕБОВАНИЯ ICAO К ИНФРАСТРУКТУРЕ ОТКРЫТЫХ КЛЮЧЕЙ ЭЛЕКТРОННЫХ ПАСПОРТОВ

Казимиров А.В.
Научный руководитель д.т.н. Горбенко И.Д.
Харьковский национальный университет радиоэлектроники

Целью создания инфраструктуры открытых ключей (ИОК) Украины для международной системы электронных паспортов (ЭП) является оказание внутренним пользователям – физическим лицам Украины – услуг по изготовлению международных ЭП с цифровой подписью их электронных данных, согласно стандартам ICAO, обеспечение услуг аутентификации, базового и расширенного доступа, аутентификации чипа и терминала [1] на всех этапах жизненного цикла паспортов, изготовленных в Украине. ИОК системы ЭП Украины должна соответствовать требованиям ICAO в области международной инфраструктуры открытых ключей.

В соответствии с требованиями ICAO, использование сертификатов открытых ключей ИОК MRTD (машиночитаемых проездных документов) обеспечивает надежную связь открытых ключей с личными ключами владельцев паспортов, которые записаны в их паспорта, и позволяет системе проверки производить аутентификацию ЭП, базовый и расширенный доступ, аутентификацию чипа ЭП и терминала.

ИОК ЭП позволяет интегрировать сертификаты открытых ключей, криптографические преобразования с открытыми ключами и уполномоченные сертифицировать органы.

Проведенный анализ показал, что при интеграции ИОК Украины в глобальную информационно-телекоммуникационную систему ЭП должен быть выполнен ряд условий и требований, которые соответствовали бы международным стандартам.

Обоснованы требования по разработке архитектуры инфраструктуры открытых ключей для применения в перспективной электронной паспортной системе Украины. Рассматриваются основные проблемные вопросы ЕЦП электронных паспортов.

1. BSI, Technical Guideline: Advanced Security mechanism for Machine Readable Travel Documents - Extended Access Control (EAC). TR-03110, 2006.