ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ УНИТАРНОЕ ПРЕДПРИЯТИЕ
«НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ «ВОСХОД»

Особенности криптографических протоколов и инфраструктуры расширенного контроля доступа к данным и функциям удостоверения личности гражданина Российской Федерации

Докладчик: Мелузов Антон Сергеевич

Дата: 19 марта 2015 г.

Удостоверение личности гражданина России

- Электронный паспорт для гражданина, а не для государства
- УЛГ – скорость оказания госуслуг
- Единый автоматизированный интерфейс для всех ФОИВ

Удостоверение личности гражданина России


РОССИЙСКАЯ ФЕДЕРАЦИЯ

УДОСТОВЕРЕНИЕ ЛИЧНОСТИ ГРАЖДАНИНА

фамилия
КУЗНЕЦОВ
имя
ВЛАДИМИР
отчество
ВАЛЕРЬЕВИЧ
дата рождения
12.12.1986
пол
М
место рождения гражданина
ГОР. МОСКВА
личная подпись гражданина
дата оформления
29.01.2015
срок действия
29.01.2025
номер удостоверения личности
BAKA0AKA1


BAKA0AKA1

код подразделения ФМС 78039

СНИЛС 119-306-080 37 ИНН 771886651849

ОБРАЗЕЦ

Гознак, МТ, Москва, 2014.

IDRUSBAKA0AKA10<<<<<<<<<<<<<<<

8612124M2501291RUS<<<<<<<<<<<0

KUZNETSOV<<VLADIMIR<<<<<<<<<<

Стандарты и технологии

- ГОСТ Р ИСО/МЭК 7816
- ГОСТ Р ИСО/МЭК 14443
- ISO/IEC 10 536
- ISO/IEC 15 693
- ISO/IEC 10373
- ISO/IEC 7810
- ГОСТ 18725-83

- ГОСТ Р 34.10, ГОСТ Р 34.11, ГОСТ 28147-89

- TECHNICAL REPORT. RF PROTOCOL AND APPLICATION TEST STANDARD FOR E-PASSPORT - PART 2. TESTS FOR AIR INTERFACE, INITIALISATION, ANTICOLLISION AND TRANSPORT PROTOCOL. Version: 1.02. Date – Feb 20, 2007

Структура данных и функций

Биометрическое приложение

- данные загранпаспорта
- фото владельца
- отпечатки пальцев.

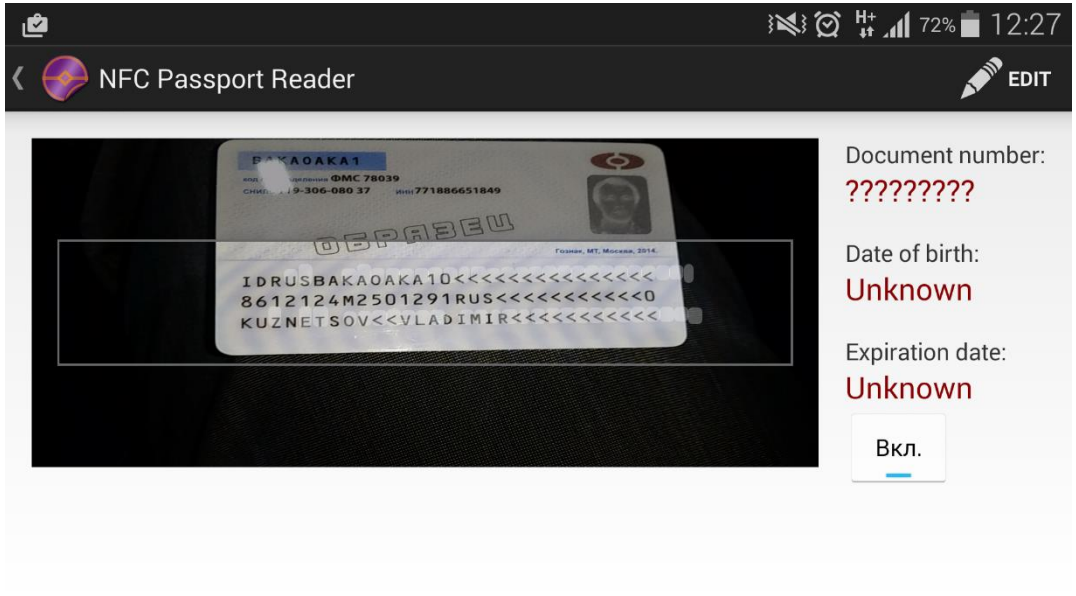
Приложение электронного удостоверения личности

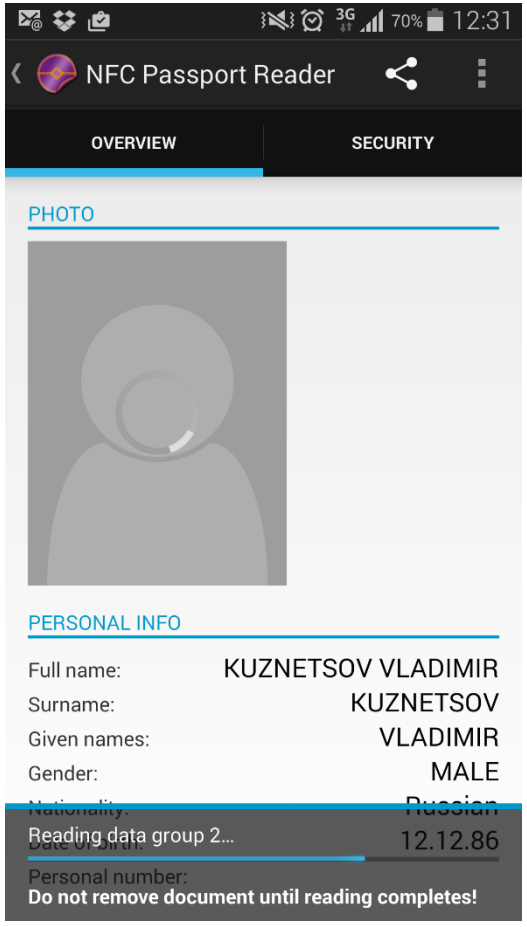
- данные общегражданского паспорта
- ИНН
- СНИЛС

Приложение электронной подписи

- СКПЭП
- функция вычисления КЭП
- фукнция смены ключей

Чтение приложения ePassport





Чтение приложения ePassport

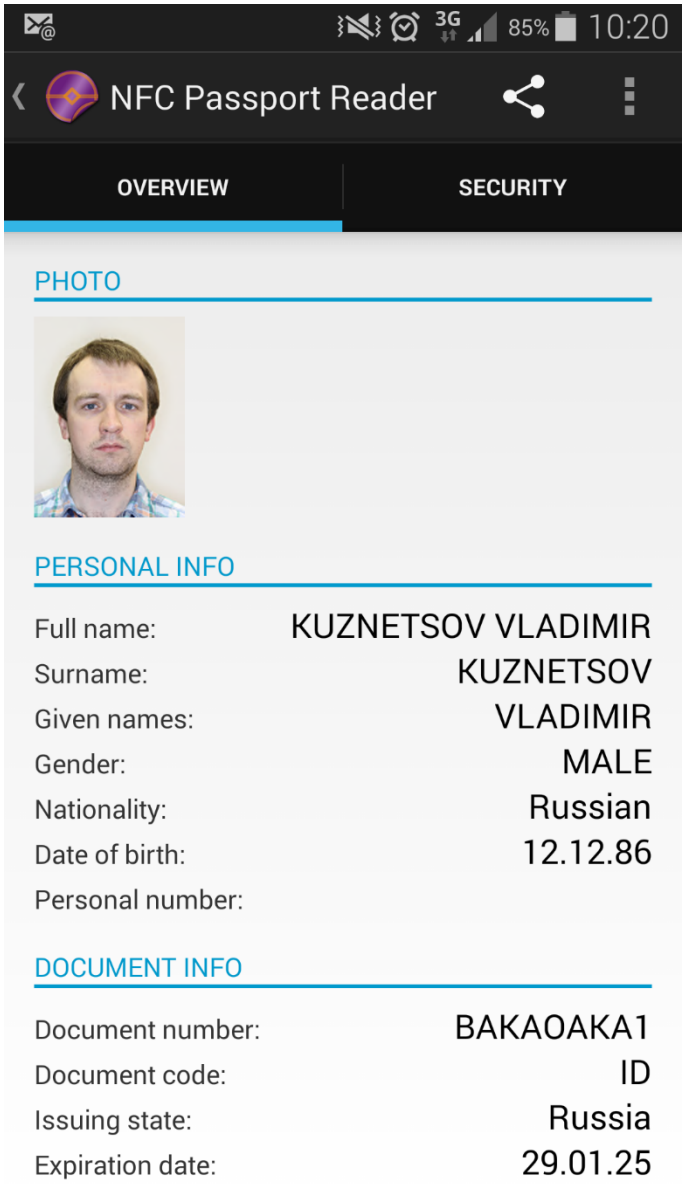


Схема доступа

Общая процедура аутентификации (ОПА):

1. Установление соединения на основе аутентифицированного пароля – MRZ, CAN, PIN или PUK (PACE);
2. Аутентификация терминала на основе CV-сертификатов (Terminal authentication);
3. Пассивная аутентификация (Passive authentication);
4. Аутентификация микросхемы (Chip Authentication).

Password Authenticated Connection Establishment

MRTD Chip (PICC)		Terminal (PCD)
static domain parameters D_{PICC}		
choose random nonce $s \in_R Dom(E)$		
$z = \mathbf{E}(K_\pi, s)$	$\langle \frac{D_{PICC}}{z} \rangle$	$s = \mathbf{D}(K_\pi, z)$
additional data required for **Map**( )	$\langle - \rangle$	additional data required for **Map**( )
$\tilde{D} = \mathbf{Map}(D_{PICC}, s)$		$\tilde{D} = \mathbf{Map}(D_{PICC}, s)$
choose random ephemeral key pair $(\widetilde{SK}_{PICC}, \widetilde{PK}_{PICC}, \tilde{D})$		choose random ephemeral key pair $(\widetilde{SK}_{PCD}, \widetilde{PK}_{PCD}, \tilde{D})$
check that $\widetilde{PK}_{PCD} \neq \widetilde{PK}_{PICC}$	$\langle \frac{\widetilde{PK}_{PCD}}{\widetilde{PK}_{PICC}} \rangle$	check that $\widetilde{PK}_{PICC} \neq \widetilde{PK}_{PCD}$
$K = \mathbf{KA}(\widetilde{SK}_{PICC}, \widetilde{PK}_{PCD}, \tilde{D})$		$K = \mathbf{KA}(\widetilde{SK}_{PCD}, \widetilde{PK}_{PICC}, \tilde{D})$
	$\langle \frac{T_{PCD}}{} \rangle$	$T_{PCD} = \mathbf{MAC}(K_{MAC}, \widetilde{PK}_{PICC})$
$T_{PICC} = \mathbf{MAC}(K_{MAC}, \widetilde{PK}_{PCD})$	$\frac{T_{PICC}}{} \rangle$	

Terminal Authentication

Chip :
$pk_{CA}, \mathrm{ID}_C, sk_C, pk_C, cert_C$

TERMINAL AUTHENTICATION

Terminal :
$pk_{CA}, cert_T, \mathrm{ID}_C, sk_T$

$cert_T$ ←

If $\mathsf{CVf}(pk_{CA}, cert_T) = 0$, abort

extract pk_T (from $cert_T$)

generate $(esk_T, epk_T, \mathrm{D}_C)$

$\mathsf{Compr}(epk_T)$ ←

$r_1 \xleftarrow{\$} \{0,1\}^\lambda$

r_1 →

$s = \mathsf{Sig}(sk_T, (\mathrm{ID}_C, r_1, \mathsf{Compr}(epk_T)))$

s ←

If $\mathsf{SVf}(pk_T, s, (\mathrm{ID}_C, r_1, \mathsf{Compr}(epk_T))) = 0$, abort

Chip Authentication

Chip :	CHIP AUTHENTICATION	**Terminal :**
	$cert_C, pk_C, \mathrm{D}C \longrightarrow$	If $\mathsf{CVf}(pk_{CA}, cert_C) = 0$, abort
	$\longleftarrow epk_T$	
verify that epk_T matches $\mathsf{Compr}(epk_T)$		
$\mathcal{K} = \mathrm{DH}(epk_T, sk_C)$		$\mathcal{K} = \mathrm{DH}(pk_C, esk_T)$
$r_2 \xleftarrow{\$} \{0,1\}^\lambda$		
$\mathcal{K}_{\mathrm{ENC}} = \mathcal{H}_1(\mathcal{K}, r_2)$		
$\mathcal{K}_{\mathrm{MAC}} = \mathcal{H}_2(\mathcal{K}, r_2)$		
$\mathcal{K}'_{\mathrm{MAC}} = \mathcal{H}_3(\mathcal{K}, r_2)$		
$\mathrm{T} = \mathsf{MAC}(\mathcal{K}'_{\mathrm{MAC}}, (epk_T, \mathrm{D}C))$		
	$\mathrm{T}, r_2 \longrightarrow$	
		$\mathcal{K}_{\mathrm{ENC}} = \mathcal{H}_1(\mathcal{K}, r_2)$
		$\mathcal{K}_{\mathrm{MAC}} = \mathcal{H}_2(\mathcal{K}, r_2)$
		$\mathcal{K}'_{\mathrm{MAC}} = \mathcal{H}_3(\mathcal{K}, r_2)$
		If $\mathsf{MVf}(\mathcal{K}'_{\mathrm{MAC}}, \mathrm{T}, (epk_T, \mathrm{D}C)) = 0$, abort
key$=(\mathcal{K}_{\mathrm{ENC}}, \mathcal{K}_{\mathrm{MAC}})$		key$=(\mathcal{K}_{\mathrm{ENC}}, \mathcal{K}_{\mathrm{MAC}})$
$sid = (epk_T, pk_C, \mathrm{D}C, r_2)$		$sid = (epk_T, pk_C, \mathrm{D}C, r_2)$
$pid = \emptyset$		$pid = pk_C$

Инфраструктура разграничения доступа на базе специальной PKI (CV-сертификаты)

CV-сертификаты

- Бинарный формат
- Маленький размер (около 100 байт)

- Права доступа определяются конъюнкцией прав всей цепочки сертификатов

- Маленькие сроки действия
- Отсутствие списков отозванных сертификатов
- Отсутствие доверенного источника времени у микросхемы

Обоснование стойкости

Модель Bellare-Rogaway:

- Стойкость к пассивному нарушителю;
- Стойкость к активному нарушителю в ходе выполнения протоколов;
- Стойкость в случае наличия большого количества одновременных сессий;

- Строится игра, в которой нарушитель должен отличить выработанный чипом и терминалом ключ от случайной последовательности;
- Если вероятность победы мало отличается от 50%, то стойкость достигнута
- Построение цепочки игр с учетом изменения вероятности победы