Министерство транспорта, связи и высоких технологий
Информационно-Вычислительный Центр

“Развитие инфраструктуры открытых ключей и статус нового УЦ в проекте электронного удостоверения личности в Республике Азербайджан”

Маилов Ариф

PKI-FORUM РОССИЯ 2017

Национальный Центр Сертификационных Услуг

www.e-imza.az

История технологии

- Директива Европейского Парламента о правовых основах регулирования электронной подписи - Декабрь 1999
- Решение Комиссии о принятии трех рабочих соглашений CEN в качестве технических стандартов - Июль 2003
- “Электронная подпись и электронный документ” Закон Республики Азербайджан – 9 Марта 2004
- “Постановление Кабинета Министров Республики Азербайджан об утверждении нормативно-правовых актов, касающихся электронной подписи и электронного документа” – 28 Января 2006
- Изучение опыта по PKI и криптографии различных стран (Германия, Австрия, Россия, Эстония и другие страны) - 2007 – 2008

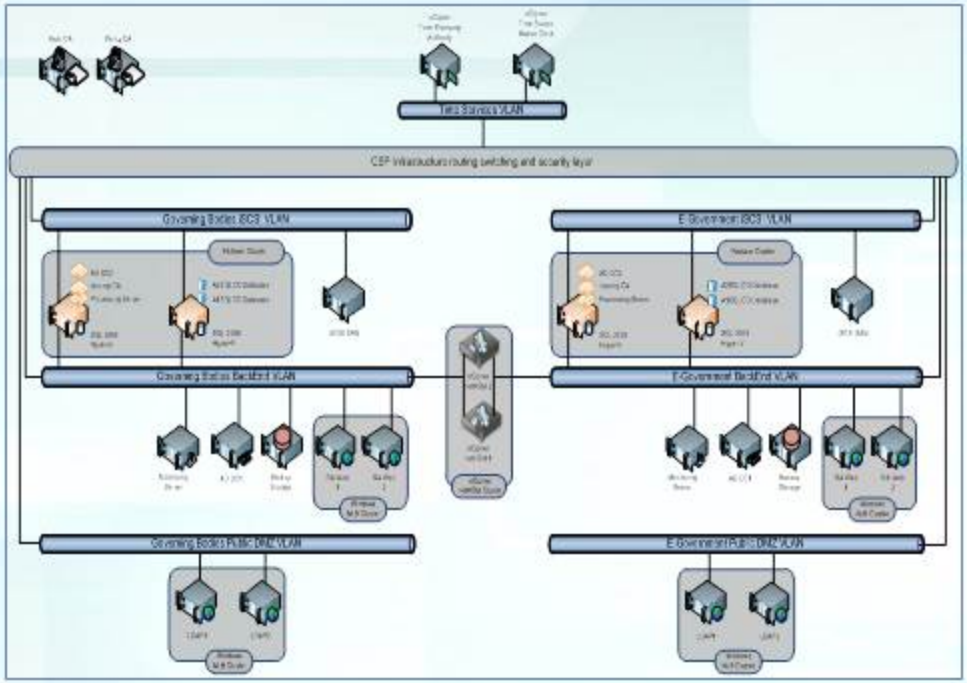
История технологии

- Установка и ввод в эксплуатацию PKI в ИВЦ Министерства Транспорта, Связи и Высоких технологий (Microsoft) – Сентябрь 2011 (Приказ 57 МТСВТ)
- Широкое использование электронной подписи в государственном управлении (портал электронного правительства) – с 2012 года

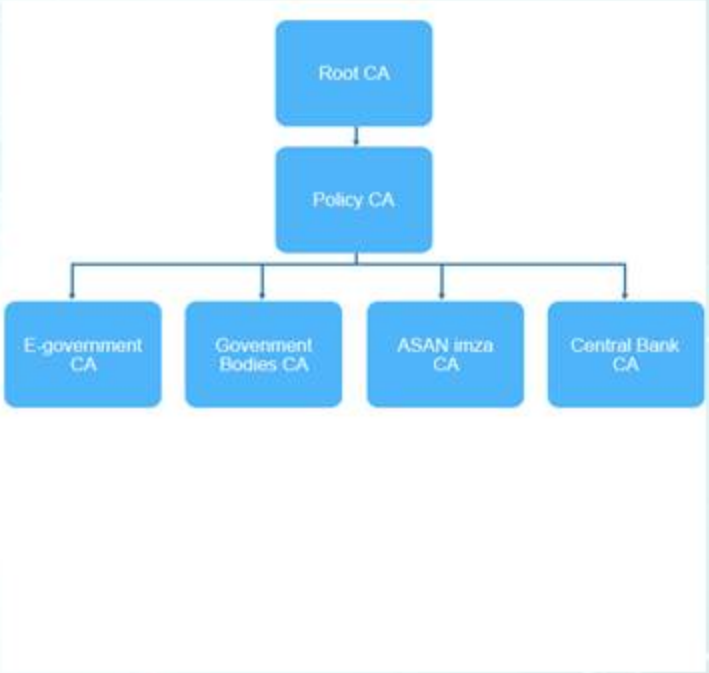
Основные требования к PKI в концепции электронной подписи

✓Инфраструктура должна соответствовать национальному законодательству и международным стандартам. Должна быть обеспечена высокая безопасность.
✓Модель CA доверия должна быть легко управляемой

Microsoft PKI



Модель доверия - иерархическая



- ✓Исходный код программ доступен
- ✓ Подготовка тех. перонала
- ✓ В соответствии со стандартами (ETSI TS 102 042; ETSI TS 101 456 1.4.3) и национальными законами

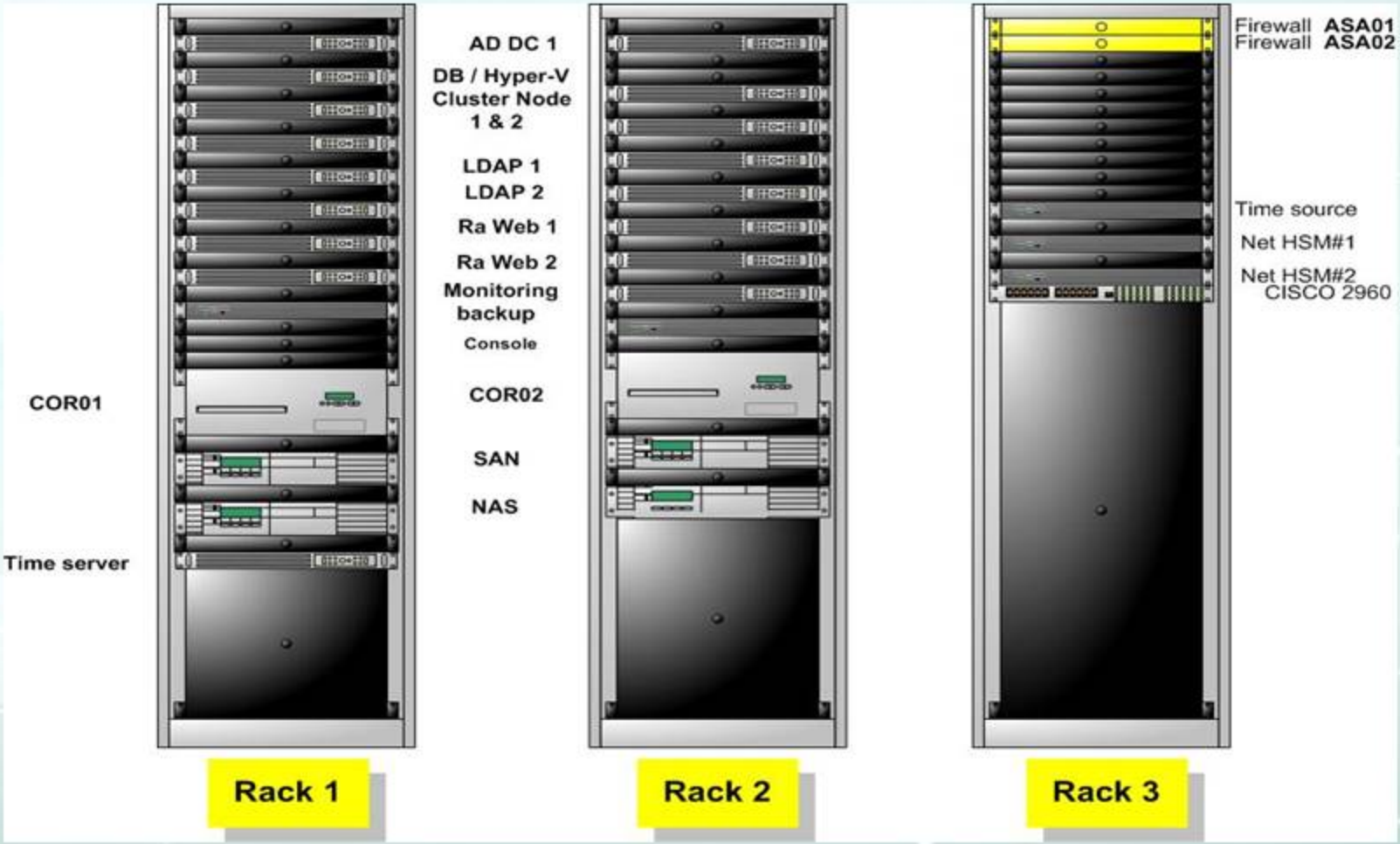
3-х уровневая PKI
Легко управляемая модель

Оборудование инфраструктуры

Адмнинтративных органов
Центр Сертификации

Электронного правительства
Центр Сертификации

Сетевое оборудование



Аппаратные модули безопасности

nCipher HSM2000

1. Асимметричный алгоритм : RSA до 4096 bit, DSA, Diffie-Hellman, El-Gamal,...
2. Симметричный : AES, DES, Triple DES, ...
3. Хэш : SHA1, SHA2
4. Криптография на эллиптической кривой (ECC)

nCipher Time Source Master clock

Временная точность:
NTP: 1-10 мсек ,
GPS 1PPS: +/- 100 нсек,
IRIG: +/- 10 мсек,
Годичная точность: +/- 300 мсек,
Сертифицирован FIPS 140-2 Level 3, CC EAL4+

Сервер временных отметок

nCipher Time Stamp Server

Алгоритм подписи: NTP - protocol RSA 4096 bits,
Производительноть (Временных отметок / сек) :
RSA 2048 bits - 145
RSA 1024 bits - 400
Сертификация: FIPS 140-2 Level 3, CC EAL4+

Серверный зал:

- ✓ **Клетка Фарадея**
- ✓ **Видеонаблюдение;**
- ✓ **Доступ устройствами считывания отпечатков пальцев;**
- ✓ **Система автоматического огнетушения**

Критические зоны рабочего процесса (регистрация и персонализация):

- **Видеонаблюдение;**
- **Вход в помещения устройствами считывания карт доступа**

Носители ключей и сертификатов Центра Сертификационных Услуг

Смарт карты

USB токены

Siemens и Gemalto смарт карты

Крипто-алгоритмы:
RSA 2048 Bit (PKCS#1), SHA1, SHA2
DES, Triple-DES,
Операционная система:
Siemens CardOS 4.4
Common Critera EAL4 +
EEPROM 64 kb

FEITIAN USB токены

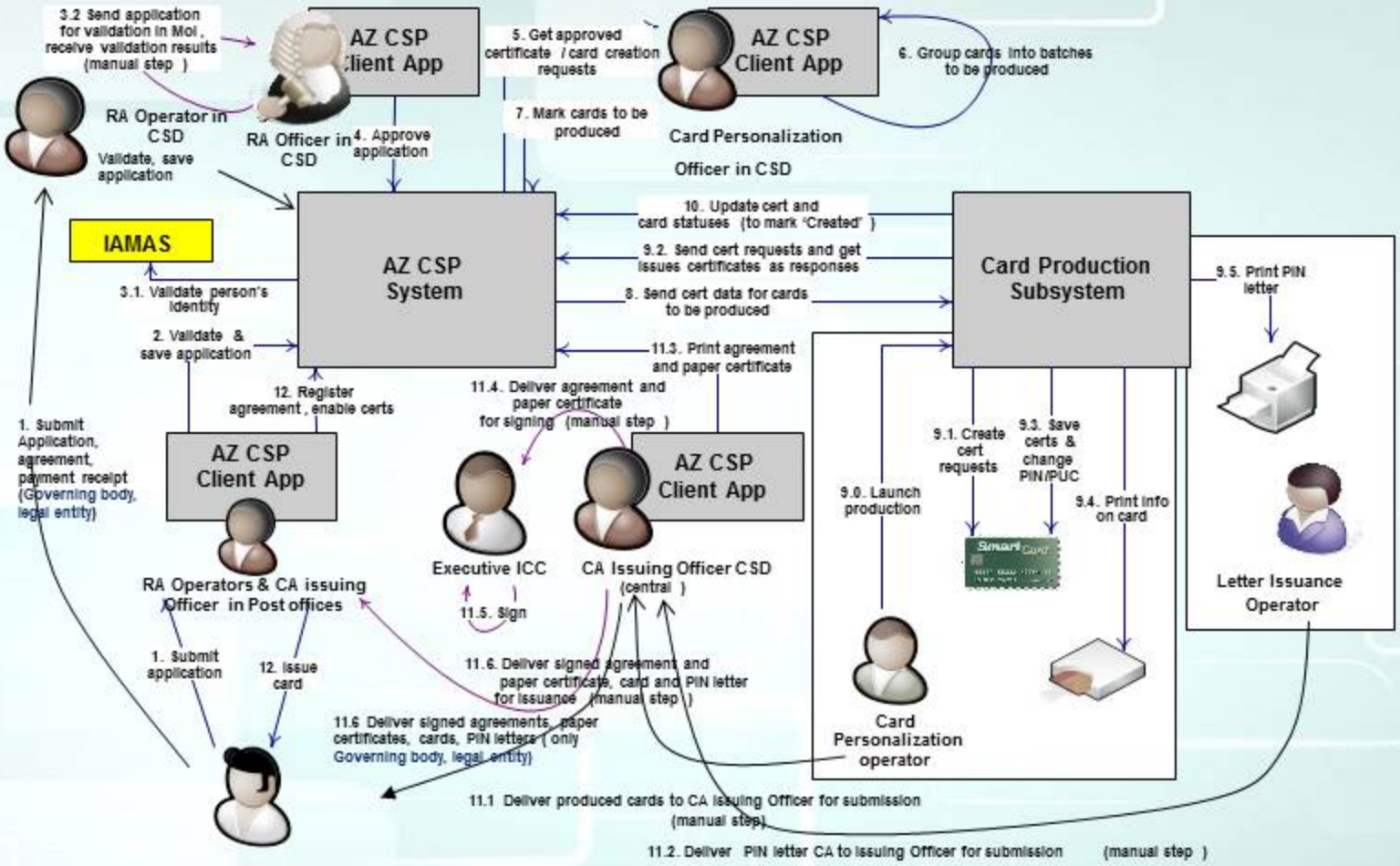
Крипто-алгоритмы:
RSA 2048 Bit (PKCS#1), SHA1,
SHA2, DES, Triple-DES,
Операционная система:
Java Card 2.2.2
Common Critera EAL5 +
SOLID FLASH, 400 kb

Генерация 2-х пар ключей в чипе

Срок действия сертификатов выдаваемых НЦСУ - 3 года

Сроки действия корневого сертификата (самоподписан) – 18 лет
сертификата политики - 12 лет
сертификата CA - 6 лет

Процесс изготовления карт электронной подписи



“Матрица ролей” содержит 15 различных ролей операторов, тех. администраторов и внутреннего аудитора.

Документы требуемые для получения сертификатов электронной подписи

Граждане

1. копия документа, подтверждающего личность владельца подписи;
2. доверенность выданная лицу уполномоченному действовать от имени владельца подписи (нотар);

Юридические лица

1. Нотариально заверенные копии документов (свидетельство о регистрации юридического лица, выписка из государственного реестра),;
2. Доверенность уполномоченного представителя, действующего от имени юридического лица (утвержденный печатью и подписью руководителя юридического лица) и копия и оригинал документа, удостоверяющего личность представителя;
3. Официальное свидетельство или официальное письмо о банковских реквизитах юридического лица;
4. Утвержденный список сотрудников юридического лица обратившихся для получения сертификата электронной подписи и копии документов, удостоверяющих личности этих сотрудников;
5. Выписка из приказа о занимаемой должности руководителя получающего сертификат ;
6. Документ, утверждающий печать руководителя.

Госслужащие

1. Копии документов, подтверждающих регистрацию организации (министерства, ведомства, учреждения);
2. Доверенность, выданная руководящим лицом уполномоченному представителю (утвержденного подписью и печатью руководителя) и копия и оригинал документа, удостоверяющего личность представителя;
3. Официальное свидетельство или официальное письмо о банковских реквизитах организации;
4. Утвержденный руководителем список сотрудников обратившихся для получения сертификата электронной подписи и копии документов, удостоверяющих личности этих сотрудников;
5. Выписка из приказа о занимаемой должности руководителя получающего сертификат;
6. Документ, утверждающий печать руководителя.

Безопасность информационной системы

Система управления информационной безопасности (ISMS) при ИВЦ работает с 2014

Аудиторская компания SGS (Societe Generale de Surveillance)

- 20 August 2014 ISO27001:2005 certificate
- 10 July 2015 ISO27001:2013 certificate

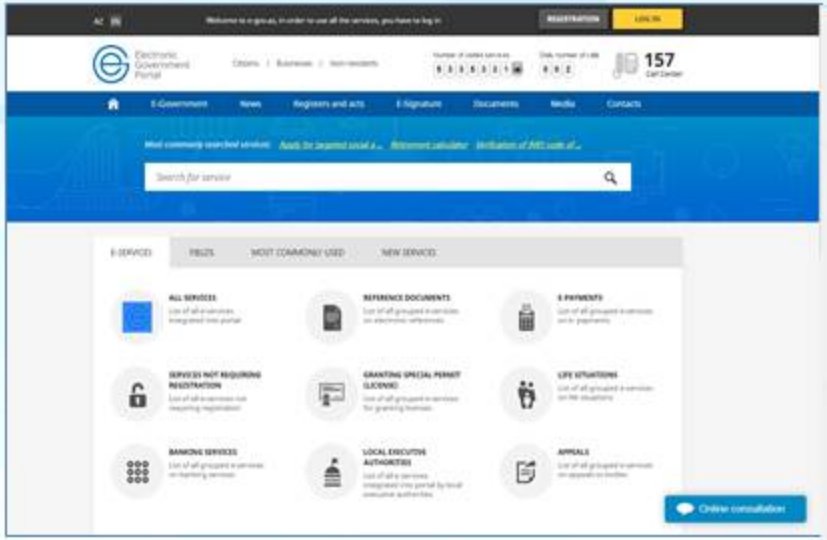
Проделанная работа

- ✓ Риск анализ;
- ✓ Подготовка политики информационной безопасности;
- ✓ Правила безопасности;
- ✓ Правила защиты физической среды и оборудования;
- ✓ Процедуры для back up данных;
- ✓ Безопасность сети and процедуры контроля доступа среды;
- ✓ Процедуры для мобильных устройств;
- ✓ Процедуры для внутреннего ISMS аудита;
- ✓ Отчеты подтверждающие работу ISMS.

Microsoft Partner
Silver Application Integration

20 Августа 2015 “Microsoft Silver” партнер впервые среди государственных организаций

Сферы применения электронной подписи



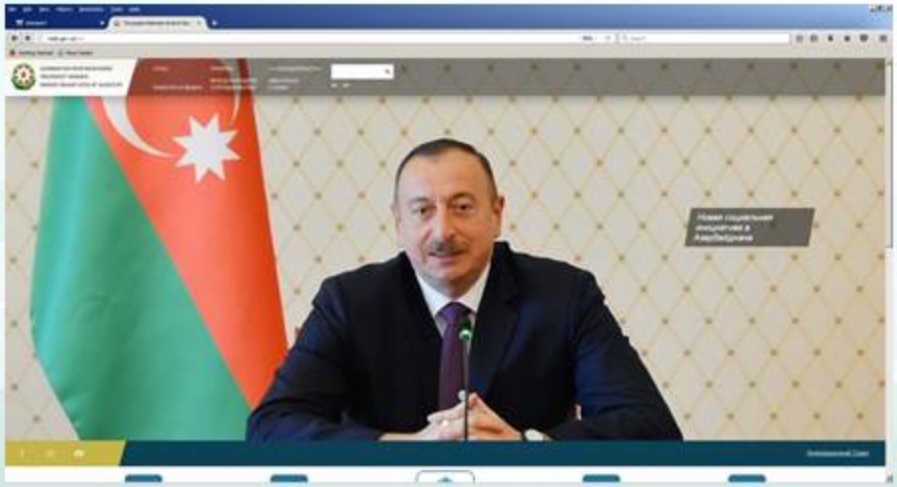
- **Информационно-Вычислительный Центр - Оператор портала с 2012 года**
- **454 электронных услуг**
- **42 государственных органа (министерства, комитеты, презид. аппарат, парламент, суды)**
- **Опрос ООН э-правительства 2016 (индекс развития) - 56 позиция, (индекс участия) - 47 позиция среди 192 стран**
- **С 2012 года э-услуги использовались ~ 53 500 000 раз**

Таможенные и налоговые декларации, электронное обращения к коллегии по апелляционной жалобе, заявления об обязательном страховании, выдача сертификатов гражданам и т.д.

Сферы применения электронной подписи

Цифровой торговый узел www.azexport.az

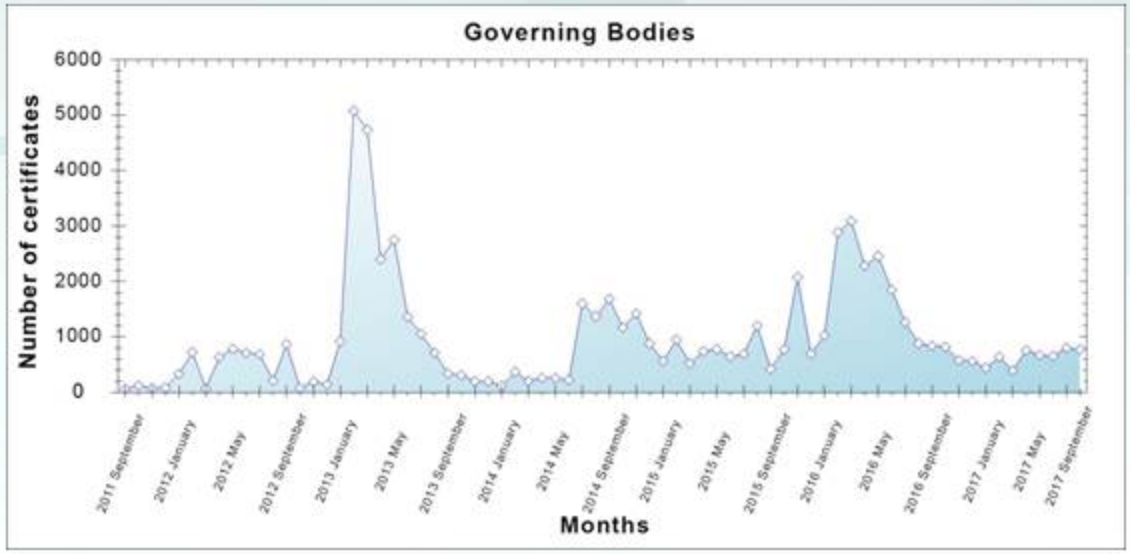
Страховые компании www.azsigorta.az



Государственное агентство жилищного строительства www.mida.gov.az

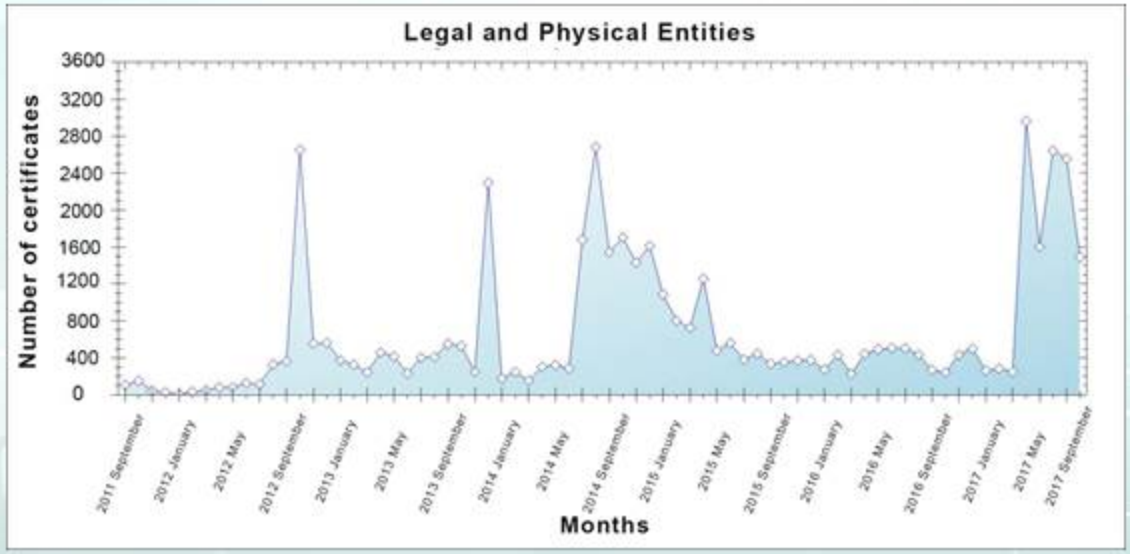
Государственный Таможенный Комитет www. customs.gov.az

Статистические отчеты



Госструктуры:

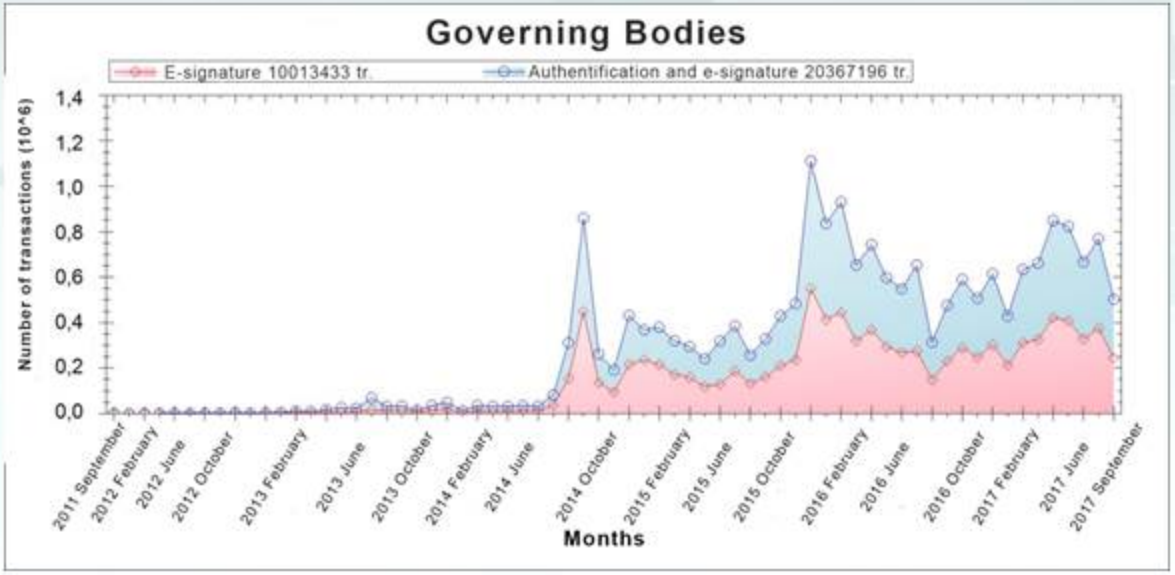
Сертификатов выдано
71 256



Юридические и физические лица:

Сертификатов выдано
45 552

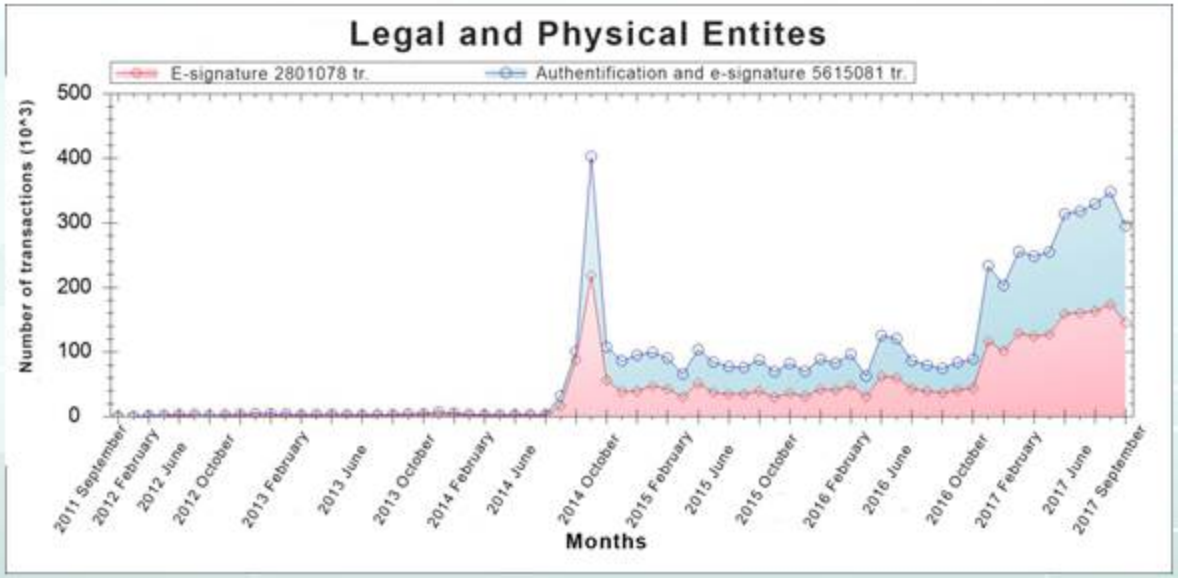
Статистические отчеты



Госструктуры:

Транзакции аутентификаций и э-подписи

~ 20 300 000



Юридические и физические лица:

Транзакции аутентификаций и э-подписи

~ 5 600 000

Новое поколение удостоверений личности (e- ID карты)

Указ Президента Азербайджанской Республики от 28 ноября 2014 года о новом удостоверении личности (статья 2)

2. Министерству Связи и Высоких Технологий поручается

“создание нового центра сертификационных услуг для включения сертификатов усиленной подписи с чипы удостоверений личности нового поколения…”

Азербайджан - 01.01.2015
(Гос. Комитет Статистики)
Административные регионы - **66**
Население ~ **9 590 000**
свыше 15 лет – **7 410 300**
Ниже 15 лет – **2 152 700**

свыше 15 лет – **запись в чип 2 сертификатов (Auth + Sign)**
От 10 до 14 лет - **запись в чип 1 сертификата (Auth)**
Ниже 10 лет – **нет записи сертификатов**

Электронное удостоверение личности (e-ID карта)

Чип NXP - P60D144,
Операционная система - Gemalto Sealys MultiApp ID v3.1; двойной интерфейс - RFID, контактный); ICAO стандарт

Емкость памяти EEPROM - 114 кбайт, ROM - 384 кбайт
RAM - 8.125 кбайт

Крипто-алгоритмы, сертификация:

Шифрование - 256-bit эллиптические кривые
Хэш функция - SHA2
Чип, ОС сертификация - FIPS 140 v2, CC EAL6+

Производитель карт – Trüb Trading (International) AG
ОС хостует 3 JavaCard аплета:

1. **ICAO – eTravel 2.1 реализует BAC, EAC**
2. **PKI – IAS Classic 4.2 обеспечивает функциями для интеграции карты в PKI**
3. **CDA – для запоминания и изменения внутренних персо-данных гражданина**

✓криптография на эллиптических кривых более пригодна для e-ID ;

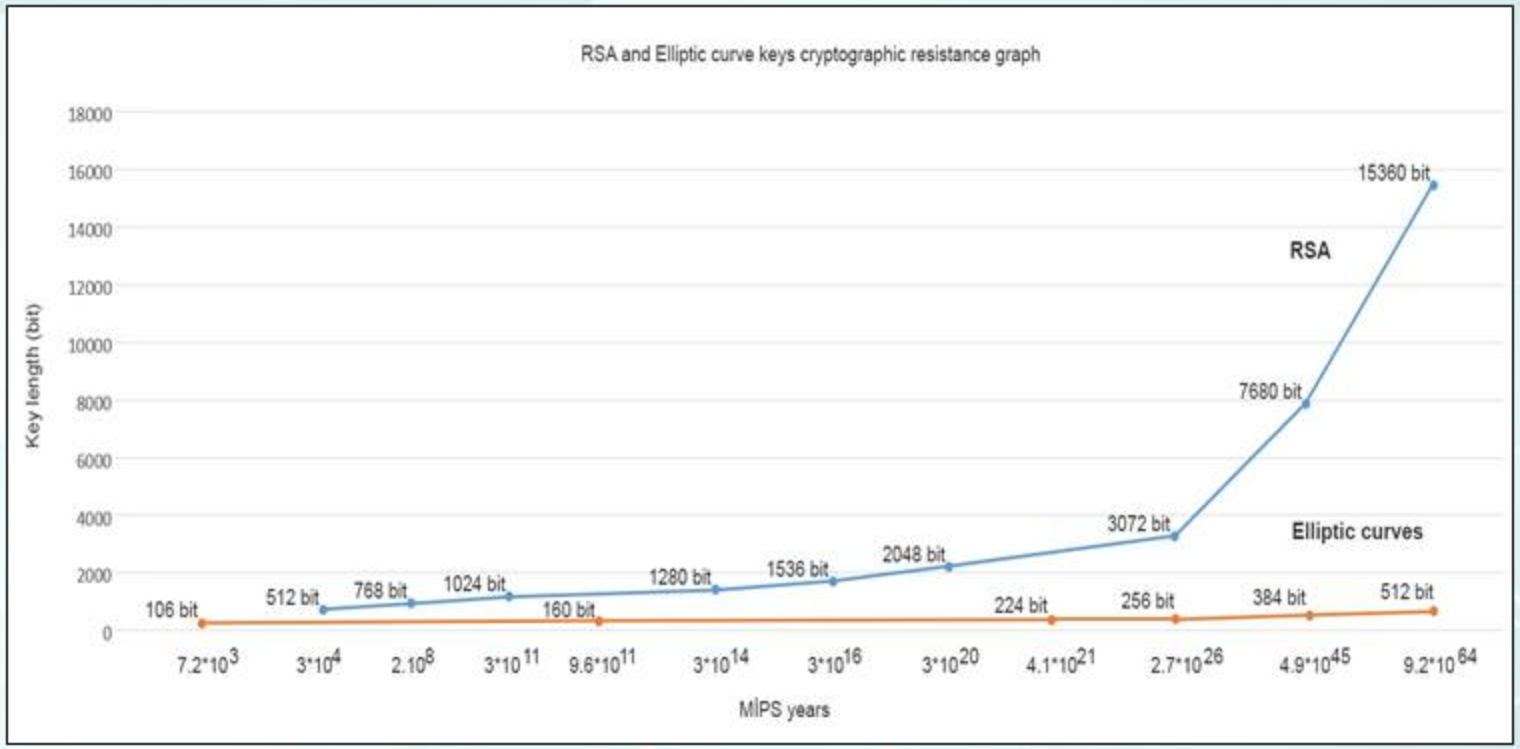
✓ NIST secp256r1

("International Journal of Innovative Research in Computer and Communication Engineering", vol.3, Issue 5, 2015)

Type of elliptical curve	Key length (bit)	Key generation time (msec)	Encryption time (100Kb plaintext) (msec)	Decryption time (100Kb plaintext) (msec)
BrainpoolP224r1	224	9	38	49
BrainpoolP256r1	256	12	47	62
BrainpoolP320r1	320	19	72	94
BrainpoolP384r1	384	31	103	140
BrainpoolP512r1	512	66	201	299
NIST curves				
Secp224r1	224	8	32	53
Secp256r1	256	12	41	68
Secp320r1	320	17	53	83
Secp384r1	384	28	102	125
Secp512r1	512	68	227	279
RSA				
RSA512	512	46	52	53
RSA1024	1024	307	312	293
RSA2048	2048	2777	2896	3011
RSA3072	3072	12898	23668	14157
RSA4096	4096	42619	49196	38892

Сравнение времен требуемых для решения Elliptic Curve Discrete Logarithm Problem (ECDLP) и Integer Factorization Problem

$$C_{ECDLP(n)} \approx 2^{n/2}$$ длина ключа n-бит



- **Эллиптическая криптография в 256-бит обеспечивает такой же уровень безопасности как и RSA шифрование в 3072 бит**

Время требуемое для взлома 256-бит ключа алгоритма на эллип. кривой

$\approx 2.7 \cdot 10^{26}$ MIPS years !!

Процесс обработки e-ID карты

Сырая карта & чип инитиал.

Пронумерованные карты

Персонализацио нная машина

Персонализущий центр

Персонализова нная карта

PIN, PUK код

МВД

Запрос сертификата, Открытый ключ

НЦСУ

Сертификаты аутентификации & Цифровая подписи

TRÜB

Швейцария

Азербайджан

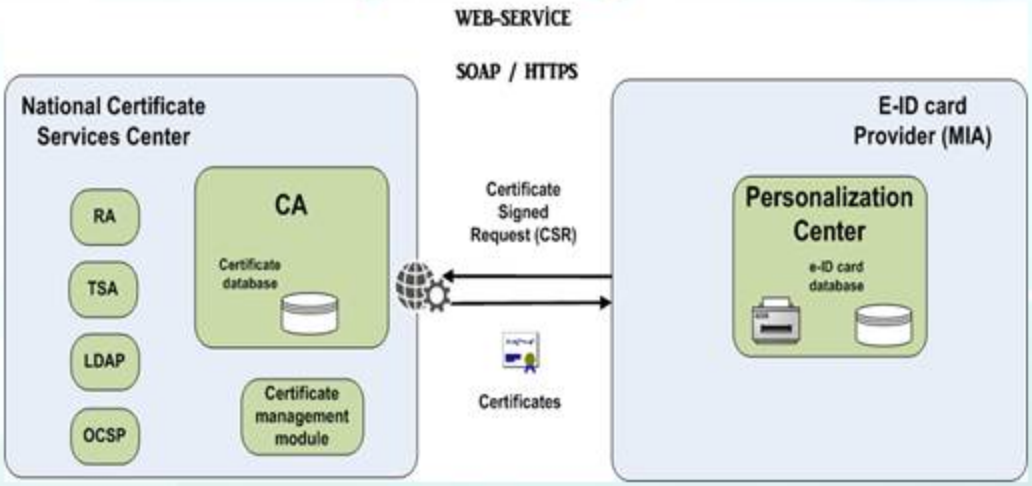
Регистрация на получение e-ID карты – **80 районных отделов полиции**
11 ASAN центров

Персонализация e-ID карточек - **9 персонализационных центров МВД**
общая производительность ~ 10 000 квал. сертификатов / день

Безопасная Гбит-ная оптическая сеть между МВД и НЦСУ

Удостоверения личности будут действительными на срок 10 лет.
Срок действия квалифицированных сертификатов 5 лет.

Сервис интеграции



2-х сторонняя SSL аутентификация; формат запроса (CSR) PKCS#10

Статус проекта по включению квалифицированнх сертификатов подписи в e-ID карты в Азербайджане

1. Этап интеграции нового центра сертификации с персонализирующими центрами МВД - сентябрь 2017
2. Церемония ключей – конец сентября 2017
3. Продолжение тестов – октябрь – ноябрь
4. Подготовка к аудиту – ноябрь 2017
5. Выдача первого удостоверения личности с сертификатами подписи – 1 января 2018

Большое спасибо за внимание !