Turkish e-ID Card Based Derived Mobile Credentials

Edona FASLLIJA, Elif USTUNDAG SOYKAN
Outline

- The need for Mobile ID
- Existing Solutions
- The idea of derived mobile credentials
- Turkish e-ID card, Dissemination, Features
- Proposed Solution
  - Lifecycle, Issuance
- Trust Propagation
- Additional requirements
- Benefits
The need for Mobile-ID

e-ID card roll outs are increased, yet usage is restricted due to not so much killer app - Mobile era could leverage usage of e-ID card

Growing need to access e-Gov services securely through mobile environments

Bad news - Card reader requirement poses a challenge for mobile environments

So, usable, secure and trusted mobile identity authentication is still a challenge
Existing solutions for mobile ID

Mobile ID/Mobile Signature Solutions
Austria, Estonia, Turkey

Mobile device for out of band authentication via OTP

SIM modules for ID/signature token

Needs dedicated lifecycle management
The idea - Derived mobile credentials

Derived ID Credential: A credential that is issued based on proof of possession and control of a previously issued credential without duplication of the identity proofing process.

Aim is to provide ID-card enabled authentication services from the mobile device to remote IT systems in a secure, reliable and interoperable way.

Derived Credential is Not using the Primary Card with the device, but an alternative token to the Primary ID Card.
History of ID Documents

1904
Devlet-i Aliye-i Osmaniye Tezkiresi
Collection of Biographies of Ottoman Empire

1926
ID Paper
(as notebook format)

1976
ID Paper
(as card format)

2016
e-ID Card
E-ID Card Dissemination Road Map

First card was issued in Kırıkkale on March 2016

9 cities followed Kırıkkale on November 2016

E-ID cards are being issued everywhere in Turkey since the Jan 2017

All citizens will be given e-ID card within three years
Features of e-ID Card

- Small, portable, durable environmentalist
- Secure
- Multi biometrics (Fingerprint, finger vein, palmvein)
- Role based access mechanism
- Compliant with international standards (ISO-7816, ISO-14443, ICAO 9303)
- Electronic signature can be loaded
- Travel Document (ICAO 9303 Passport application)
Usage areas of e-ID Card

Health Establishment
- Analysis delivery
- Report delivery
- Examination Report delivery

School
- Selecting lesson
- Renewing the record
- Student certificate
- Application for identity/free pass
- Thesis/homework delivery
- Graduation document/transcript

Law court
- Application for registration record
- Court article demand

Electric, water, natural gas etc. delivery companies
- Subscription opening/close/transfer
- Official Petition

Bank
- Opening/Closing account
- Official petition

Municipality
- Official petition

Any establishment
- Official petition
- Service contract
- Document demand

Armlet unit
- Official Notification
- License
- Passaport

Land Registry
- Examination of the register of deeds

Public Notary
- The document following
Authentication Factors

- Digital Certificate
- Digital Photo
- PIN
- Biometry
Identity Verification Scenario

Identity Verification Request

Verification of e-ID Card

Biometric Verification

PIN Verification

******
(PIN) ✓
Primary Lifecycle Activities of the Derived Credential

Initial Issuance
Maintenance
Activation
Usage
Initial Issuance (remote)

1. Issuance triggered
2. Request for derived credential issuance
3. RA redirects to IVS for authentication
4. Authentication Req
5. Authentication Resp
6. OTP via SMS
7. MPA initialized, Key pair is generated
   Credential holder requested to enter protection PIN,
   Certificate request along with OTP is sent to RA
8. Certificate Request
9. Signs and Forwards Certificate Request
10. Generates the Derived Certificate

Provides Substantial Level of Assurance
Initial Issuance (in-person) -

1- Issuance triggered

2- Request for derived credential

3- RA redirects to IVS for authentication

4- Authentication Request

5- Authentication Response

6- OTP via SMS

7- MPA initialized, Key pair is generated, Credential holder requested to enter protection PIN, Certificate request along with OTP is sent to RA

8- Certificate Request

9- Signs and Forwards Certificate Request

10- Generates the Derived Certificate

Provides High Level of Assurance

CA

OCSP Server

Identity Verification Server

RA (e-gov)
Termination/Revocation

If mobile phone containing the derived credential is stolen, lost, damaged
If mobile phone transferred to another individual
If e-Idd card containing the primary credential terminated for any reason (expired, changed, lost)

Re-key

If certificate is expired or compromised then initial issuance shall be followed
If certificate of a higher level of assurance is requested then initial issuance shall be followed.
Trust Propogation

RA (e-gov)

CA

OCSP Server

Identity Verification Server

Trust Domain-A

Trust Domain-B

Trust Domain-C

Trust Domain-D
Additional Security Requirements

The cryptographic algorithm and key size requirements for the derived credential certificate and private key are the same as the requirements for the primary e-ID card.

For high level of assurance, key pair must be generated on hardware cryptographic module compliant with FIPS Level 2 or 3 e.g. not exporting private key, for substational level of assurance FIPS Level 1 requirements must be satisfied.

Use of derived credential shall be protected by PIN and shall be blocked after a number of consecutive failed attempts.
Benefits

Main advantage: Leverage Identity Proofing and vetting results of a current valid Credential. Eventually cost savings

Simplified Lifecycle Management processes

Minimized security breach damage due to limited validity period and permissions

Possible multiple derived credentials from a single primary credential
Challenges/Future Directions?
Thank You

Any Questions?