eIDs and Mobile IDs

ePassport and eID

Current Passport

ePassport

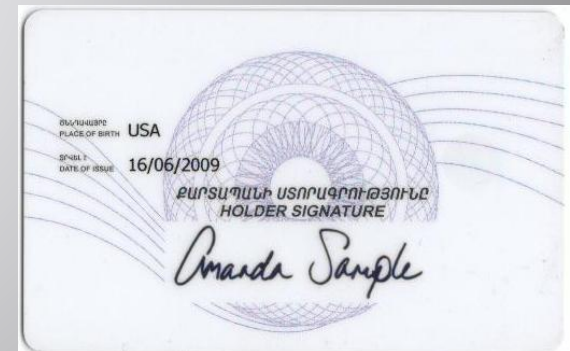**eID**

eID Card content

- On the Card
  - Citizen basic information and photo

- In the Card (built in Chip)
  - Citizen basic information + biometrics
  - Certificate for Authentication
  - Certificate for Digital Signature

eID Chip and Operating System

The SmartMX (P5CC080) microprocessor is positioned to service high volume eGovernment applications.

JCOP (Java Card Open Platform) Operating System which will be delivered is a full-featured operating system for electronic ID. Main features of the operating system JCOP2.4.1 R3:

- 80 of EEPROM (product version: J2A080)
- Java Card™ v2.2.2
- Global Platform v2.1.1
- support of Data Encryption Standard (DES), dual/triple key DES3 - 56/112/168 bits and AES - 256 bits via co-processor
- support of PKI via co-processor for RSA to 2048 bits and ECC to 320 bits.
- support of SHA-1, SHA-2
- Protection of reading data transmission through secure messaging,
- CC EAL certification 5+.

eID Application & Supported Services

Cv act ePasslet/EuCCB (IAS-ECC) is part of cryptovision's cv act ePasslet Suite, a set of Java Card applets for e-ID document applications.

Supported Services
- Identification
- Knowledge based user authentication
- Biometric based user authentication
- Symmetric device authentication
- Secure Messaging
- Digital signature with last round of hashing performed by the card
- Client/server authentication
- Encryption key decipherment

eID Additional Applications

There are the following additional applets available in CV applets suite:
• Basic Access Control
• Extended Access Control v1.11
• Extended Access Control v2 / ICAO SAC
• German eID- EACv2/PACE, Restricted ID
• European Citizen Card - profile as defined by Gixel IAS-ECC specification
• International Driving License
• ID, Authentication, Sig + Match on Card
• Qualified Signature
• European Health Insurance
• Electronic Vehicle Registration

eID Middleware

The smart card middleware implements the most popular PKI functionalities like documents signing, secure e-mail communication and user authentication into IT environment.

The following lists the basic functions of the middleware:

The middleware is supporting the following interfaces:
- Microsoft CSP (CryptoAPI),
- PKCS #11,
- TokenD.

One card – multiple usage possibility

Identification Card

Driving License

Medical Card

Bank Card

??? Services

Benefits of the eID

- Secure identification of a person both in offline and online environment
- Common identification system
- One card – multiple usage possibility
- Built-in digital signature
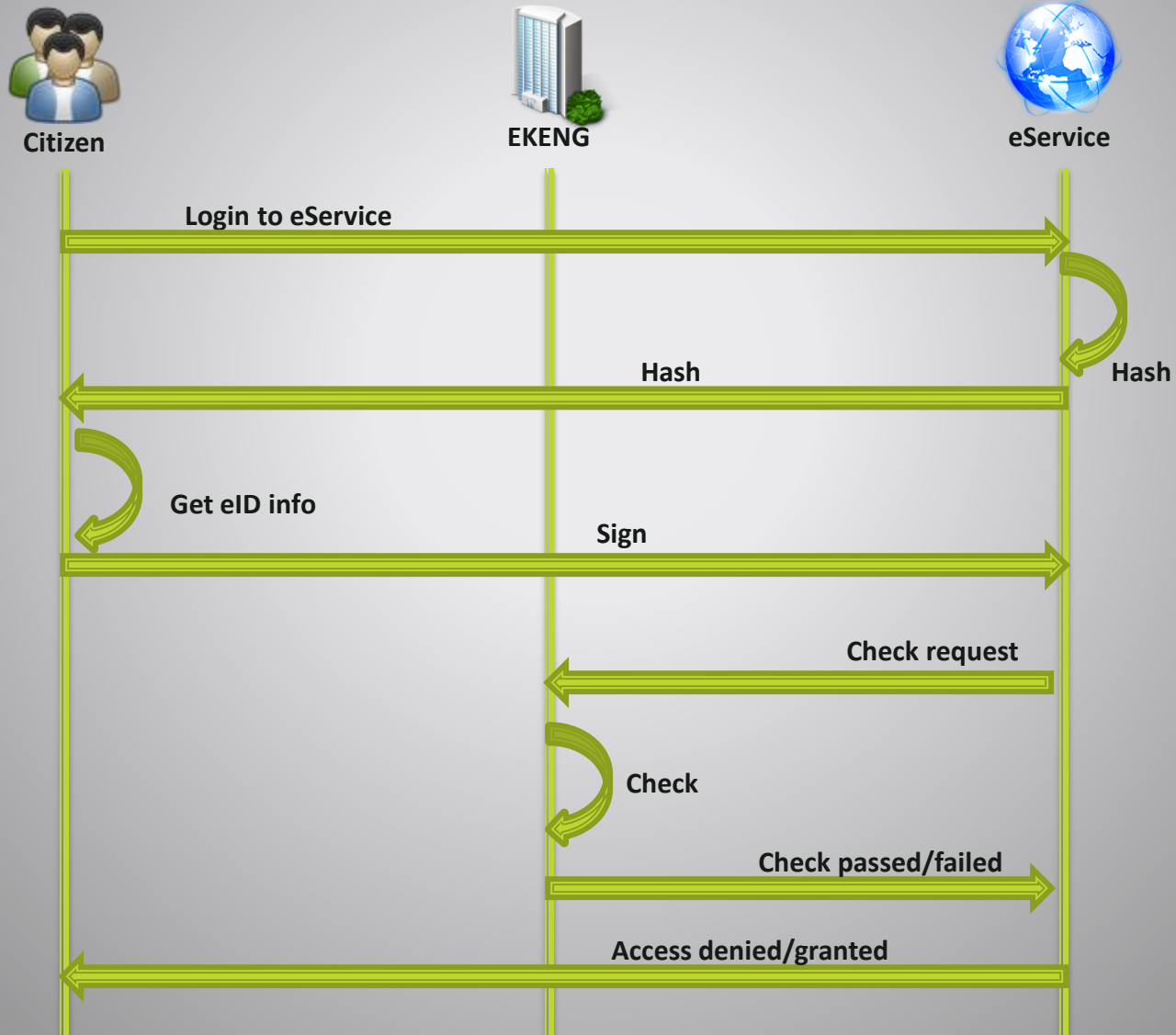- More effective G2C and G2B cooperation

Certification Authority

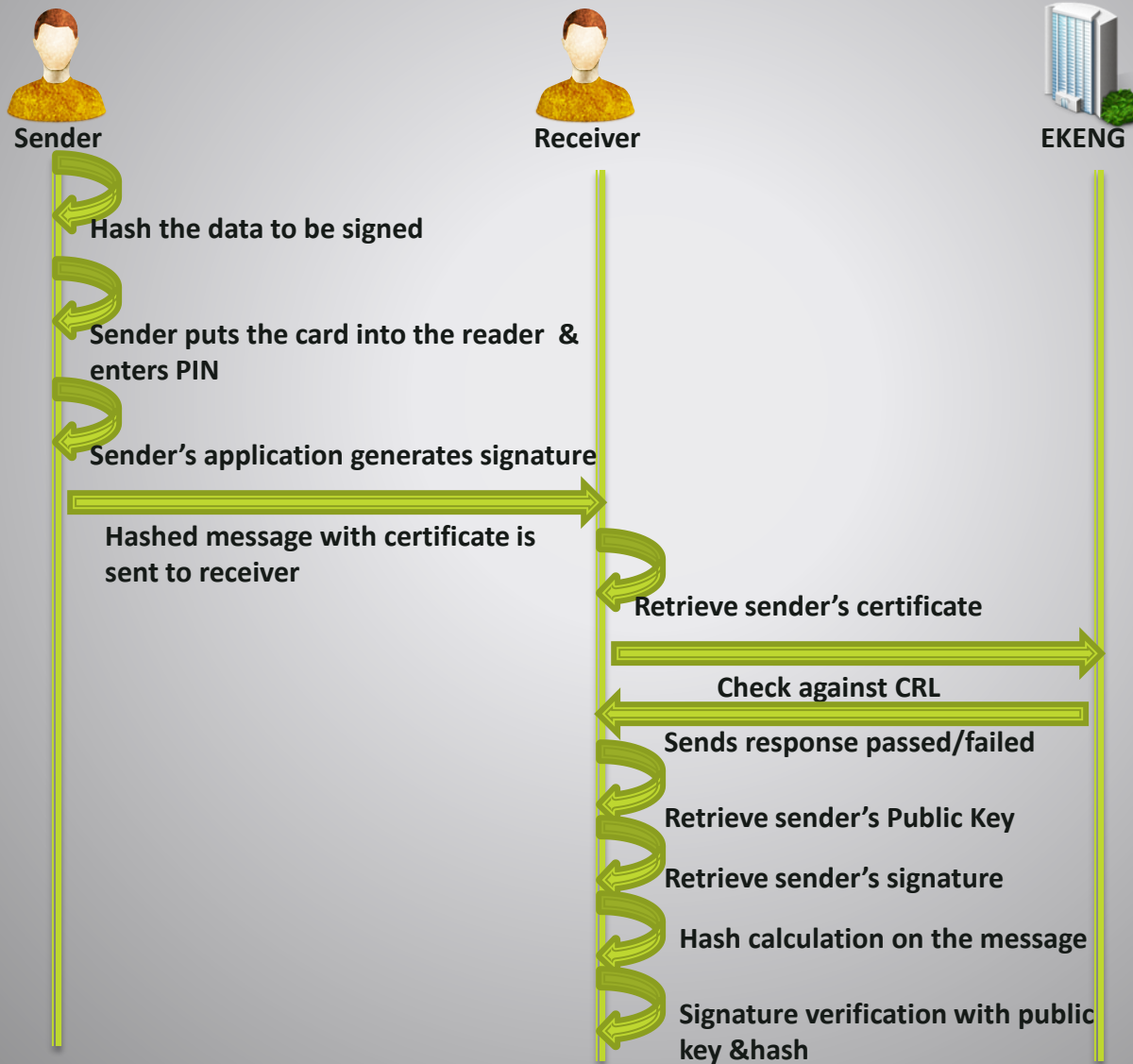**Authentication**

Electronic Signing
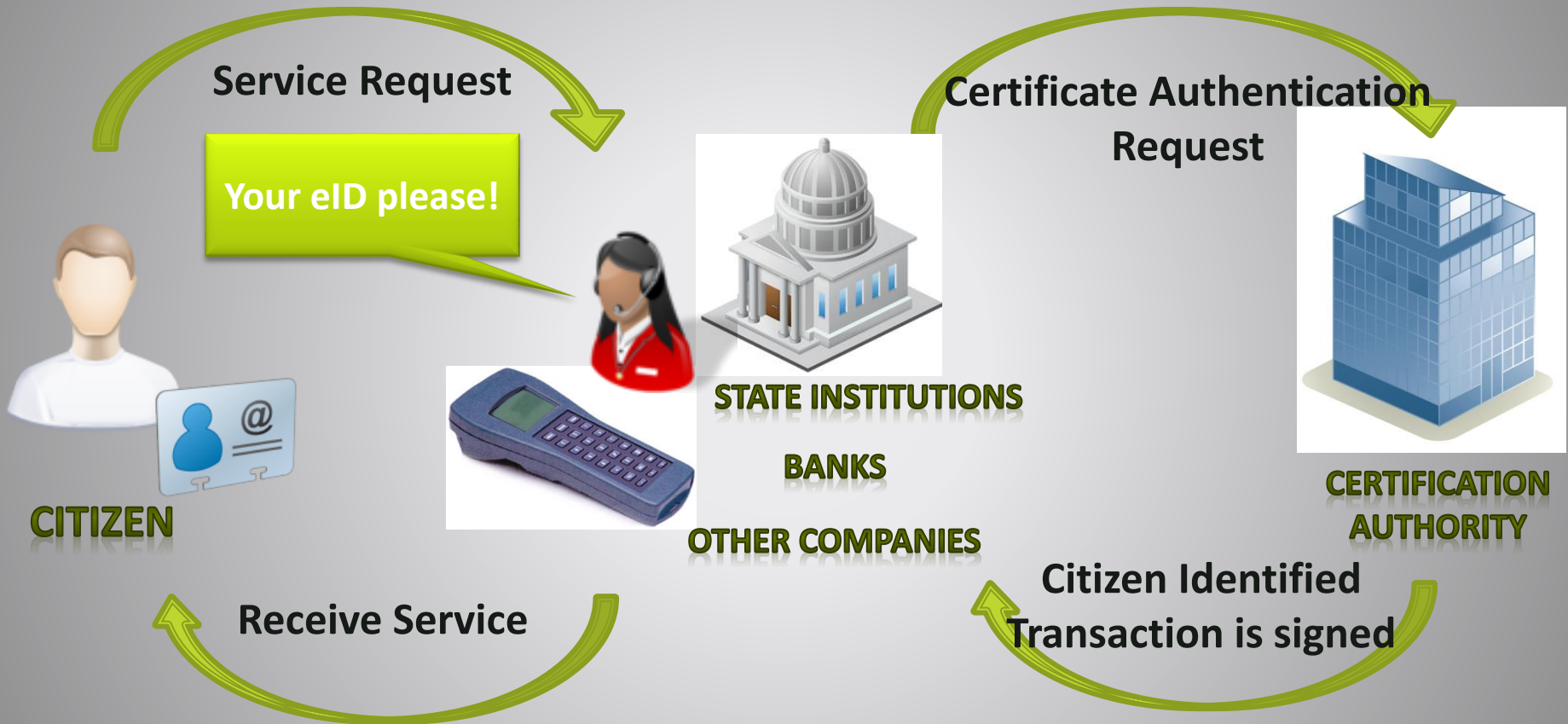
Certified e-Document Authority

Authentication

Citizen   EKENG   eService

Login to eService

Hash   Hash

Get eID info

Sign

Check request

Check

Check passed/failed

Access denied/granted

Electronic Signing & Verification

Sender

Receiver

EKENG

Hash the data to be signed

Sender puts the card into the reader & enters PIN

Sender's application generates signature

Hashed message with certificate is sent to receiver

Retrieve sender's certificate

Check against CRL

Sends response passed/failed

Retrieve sender's Public Key

Retrieve sender's signature

Hash calculation on the message

Signature verification with public key &hash

eID Card Usage

e-Service Request

Your eID please!

CITIZEN

Certificate Authentication Request

E-....
E-GOV
E-TAX
E-REGISTER
E-CADASTRE
E-BANKING

CERTIFICATION AUTHORITY

Use Service

Access granted

eID Card Usage

E-Commerce

Apply L/C

Buyer

Bank

Transaction document

Confirm

Quote

Transaction doc.

Hub of digital document exchange

✓Exchanging trade documents via TTPR
✓Delivering trusted digital documents to the receiver;
✓Preventing from repudiation during transactions between parties;
✓Creating a single point of contact for all parties.

Secure storage of trade documents

✓Officially registering all documents;
✓Time stamping at the registration;
✓Creating a certificate for status change;
✓Access control;
✓Security management.

Inquiry

Order

Invoice

L/C

Transaction document
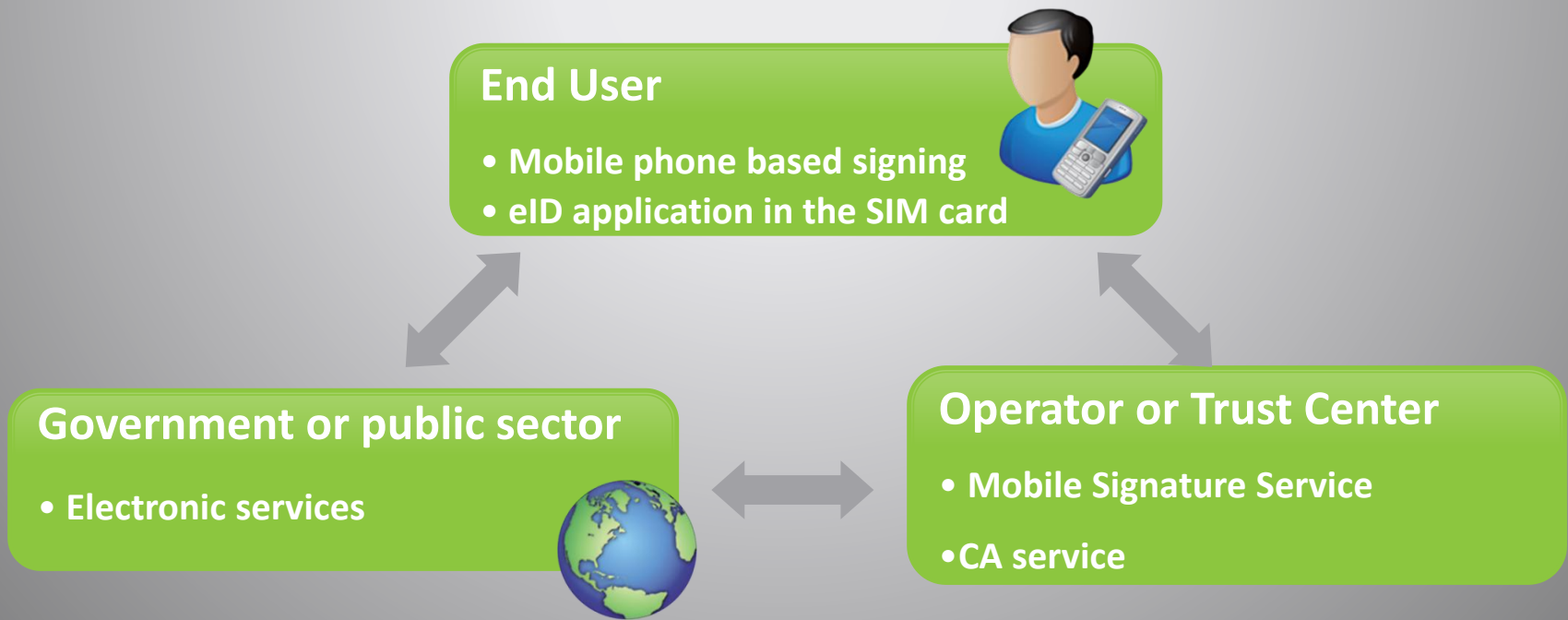
Bank

Confirmed LC

Seller

Mobile ID

Mobile Life

Mobile IDs provide strong PKI based authentication, encryption, and digital signature services as for eID.

Mobile ID makes things easier

- Allows you to forget all passwords, bank codes and IDs
- Enables strong authentication and **legally binding signatures** for all web, mobile, voice call services and in face-to-face transactions
- Based on digital signatures created in the SIM card

End User
- **Mobile phone based signing**
- **eID application in the SIM card**

Government or public sector
- **Electronic services**

Operator or Trust Center
- **Mobile Signature Service**
- **CA service**

What is Mobile ID?

Leverages on the existing eID infrastructure

- Starting point is the PKI based digital identity: eID smart card + reader
- Identity is provisioned on a SIM card with PKI capabilities
- Card reader is replaced with mobile phone, which reduces investments on card readers and their service and maintenance costs
- Phone display and keypad are used as the user interface
- Mobile eID is used as complementary electronic identity
- Authentication using digital signatures through the mobile channel
- Current and new eGovernment services are deployed and accessed as before
- Existing and new services can be introduced through new channels, e.g. mobile, voice, POS
- Brings electronic services closer to the whole population

Solution Architecture

Citizen

Government

Registrar e.g. police

eGovernment Services

Citizen Database

Mobile eID Integration Layer
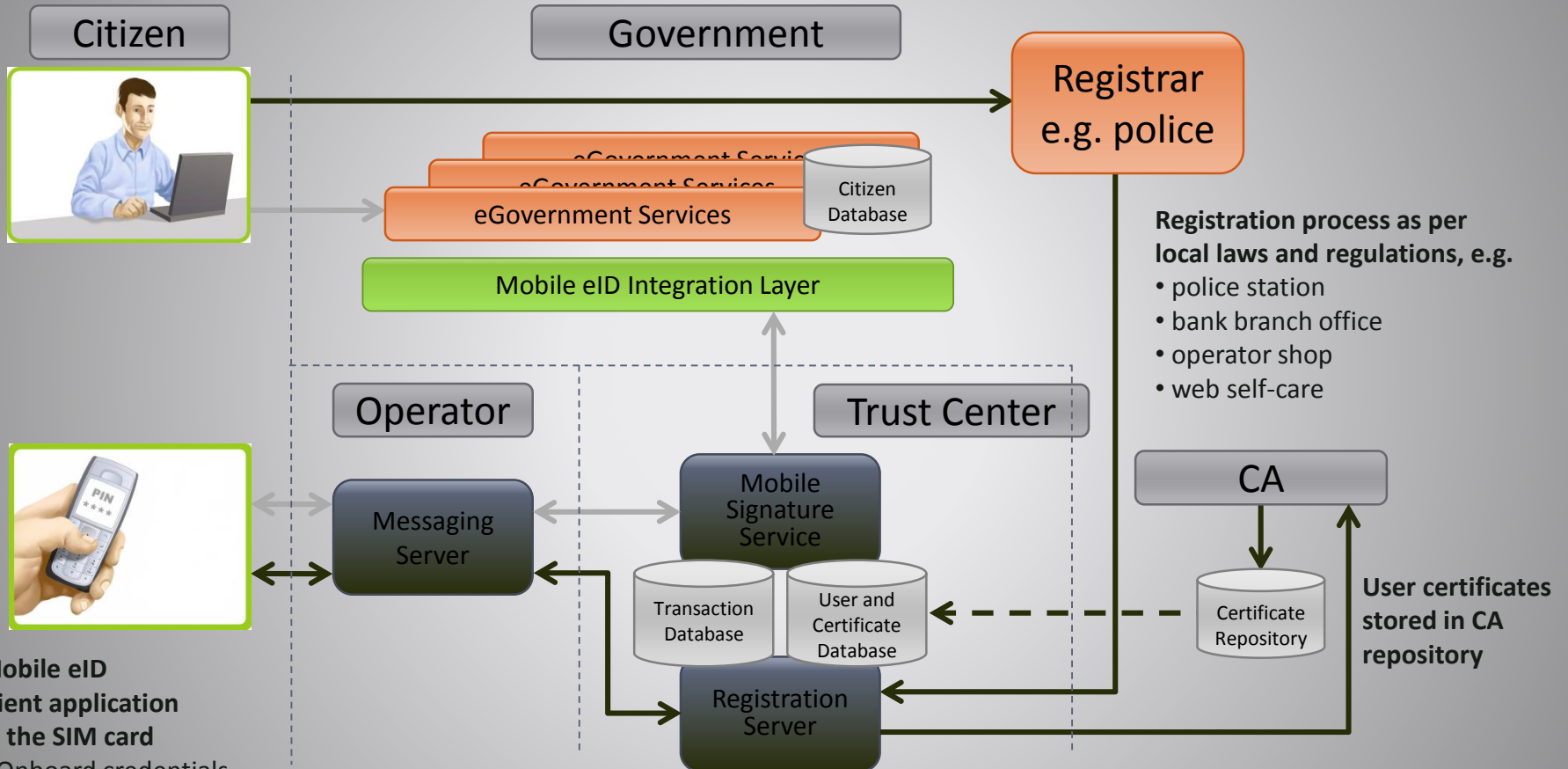
Registration process as per local laws and regulations, e.g.
• police station
• bank branch office
• operator shop
• web self-care

Operator

Trust Center

CA

Messaging Server

Mobile Signature Service

Transaction Database

User and Certificate Database

Certificate Repository

Registration Server

User certificates stored in CA repository

Mobile eID client application in the SIM card
• Onboard credentials generation
• RSA cryptography for digital signatures
• User controlled PIN management

Any governmental service requiring strong authentication can be integrated with the Mobile Signature Service

Mobile Signature Service Evolution
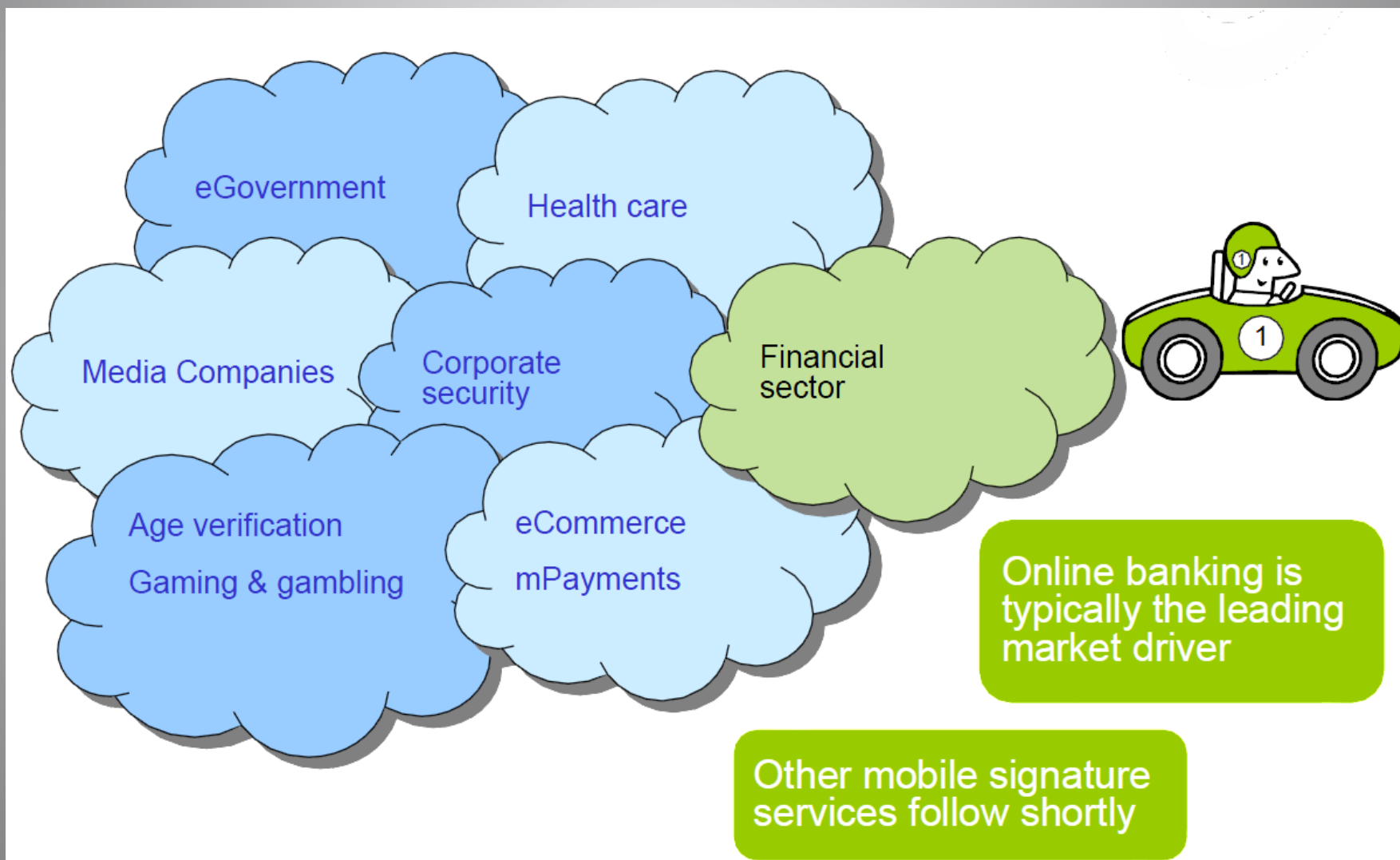
Example: eBanking, Entities & Action Flow

End User

Banks & Financial institutions

Certification Authority

Bank

Mobile Operator
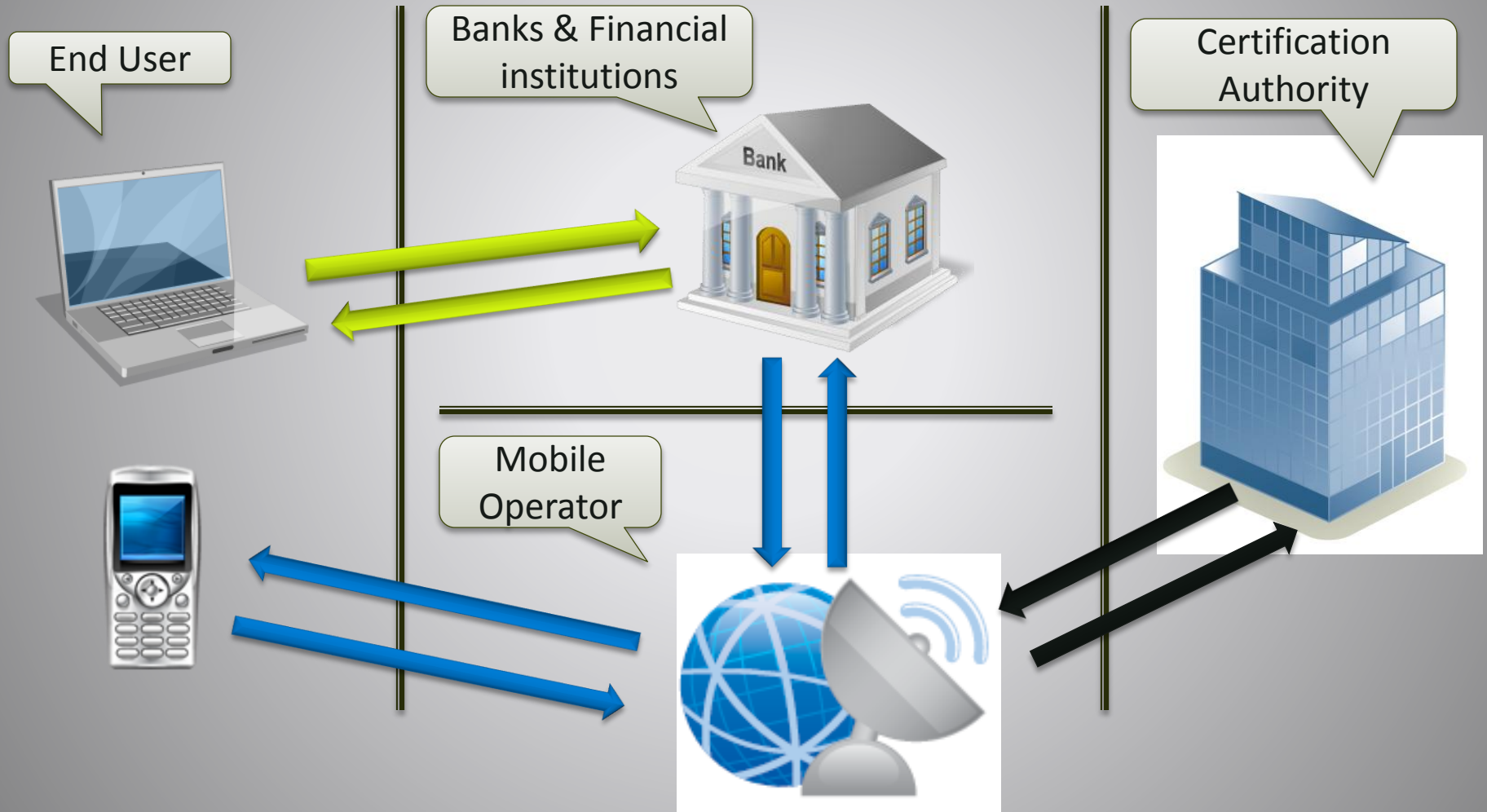
Mobile ID Use Cases

Government declarations/reporting:
- Automated and online processes for regulatory reporting
- Allows the responsible persons to submit the necessary information fast and securely
- Benefits for the government and corporates:
  - Simplified procedures for compliance to government regulations
  - Documented workflow processes for third-party auditing
- Benefits for the end-users:
  - No separate security tokens needed
  - Reporting service enabled anywhere, 24/7, not tied to any specific computer

Access to one's private healthcare records:
- Private mobile phone subscribers can sign up for a webservice storing:
  - A) Their own medical records, or
  - B) A log history of the medical professionals who have accessed the above
- Users may also authorize doctors or nurses to have access to their records in the webservice
- Benefits for the service provider:
  - Transparent record keeping meeting regulatory requirements
- Benefits for the end-users, citizens /patients:
  - Secure access to their own health information and other related issues, 24/7
  - Decreased need for travelling
    - Decrease in costs, indirect savings for the environment

Mobile ID Use Cases

Mobile ID in Healthcare Services:
- Doctors sign e-prescriptions, enabling patients to collect their medication without paperwork
- Doctors can review and renew periodic prescriptions through the application
- Benefits for the Healthcare Service provider:
  - Faster prescription issuing and processing
- Benefits for the end-user: citizen / patient:
  - Less paperwork, fewer needs to visit the pharmacy or doctor for prescriptions

Power of Attorney in healthcare services:
- Relatives can be entitled to collect a patient's medication with a signed mobile PoA
- The collection of medication can be documented and time-stamped
- Benefits for the healthcare service provider
  - Easier processes when dealing with prescriptions and patient proxies
- Benefits for the end-user: patient / citizen:
  - Ability to collect medication on behalf of a relative
  - Provides an easier way to collect the needed medication for patients with difficulties to move
  - Decreased need for travelling
    - Decrease in costs, indirect savings for the environment

Mobile ID Use Cases

Mobile ID in e-Voting

- Citizens could get the possibility to vote remotely on municipal/government polls or elections
- Benefits for the Municipal or Government:
  - Active, (local) democracy with an increased level of voting activity
  - Instant data availability and reports of the poll results and voting activity percentages
    - Possibility to real-time audits
  - Decreased printing costs with decreased need for manual voter history scanning
  - Facilitated exception handling
- Benefits for the end users, citizens:
  - Use convenience, mobile signature makes it easier to make a difference and have one's say
  - Decreased need for travelling
    - Decreased travelling costs and indirect savings for the environment

Mobile ID Use Cases

CUSTOMS

- Electronic customs declarations
    - The declarations can be handled on-the-go thanks to Mobile eID
    - Authentication and signing using mobile phone and Mobile eID
- Replaces time-consuming and sometimes critically slow paperwork
    - Improved customs clearing times
- Customs officers can concentrate on examinations of vehicles and containers
    - Reduced operating costs for the customs
- Customs processes available 24/7 independent of the physical location
    - Less time spent on the border queues
    - Everything easily available in electronic form

Mobile ID Use Cases

TAXATION

- Online tax declarations and forms
    - All forms can be legally signed using Mobile eID
    - Possibility to use mobile authentication to gain access to tax authority services
- Electronic processes bring reduced operating costs for the government
    - More efficient processes as all information is in digital form from the beginning
    - Improved government service availability for the citizens
        - Tax services available 24/7, anywhere
- Less need for the citizens to physically visit the tax office
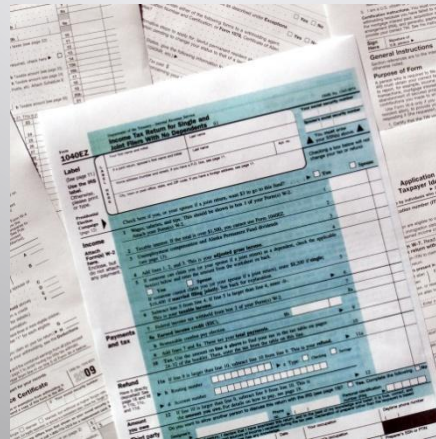
# Mobile eID - eID Cards Become Mobile

Mobile eID allows users to:

- **Have a digital counterpart of paper and plastic ID cards**
  - eID on your mobile phone, always carried with you, always under your control
- **Have one identity in different services**
  - eGovernment, e/mBanking and e/mCommerce
  - easy to use services, easy to use identity
- **Use Mobile Phone in the identification process**
  - based on a private-public key pair stored on a secure SIM card
  - works in all mobile phones as an identity tool
- **Have service channel independence, e.g. use**
  - both PC and Mobile
  - Point of Sales
  - Call Center

Mobile eID is a natural development for eID cards when used for electronic authentication and digital signing

Financial Streams between Actors
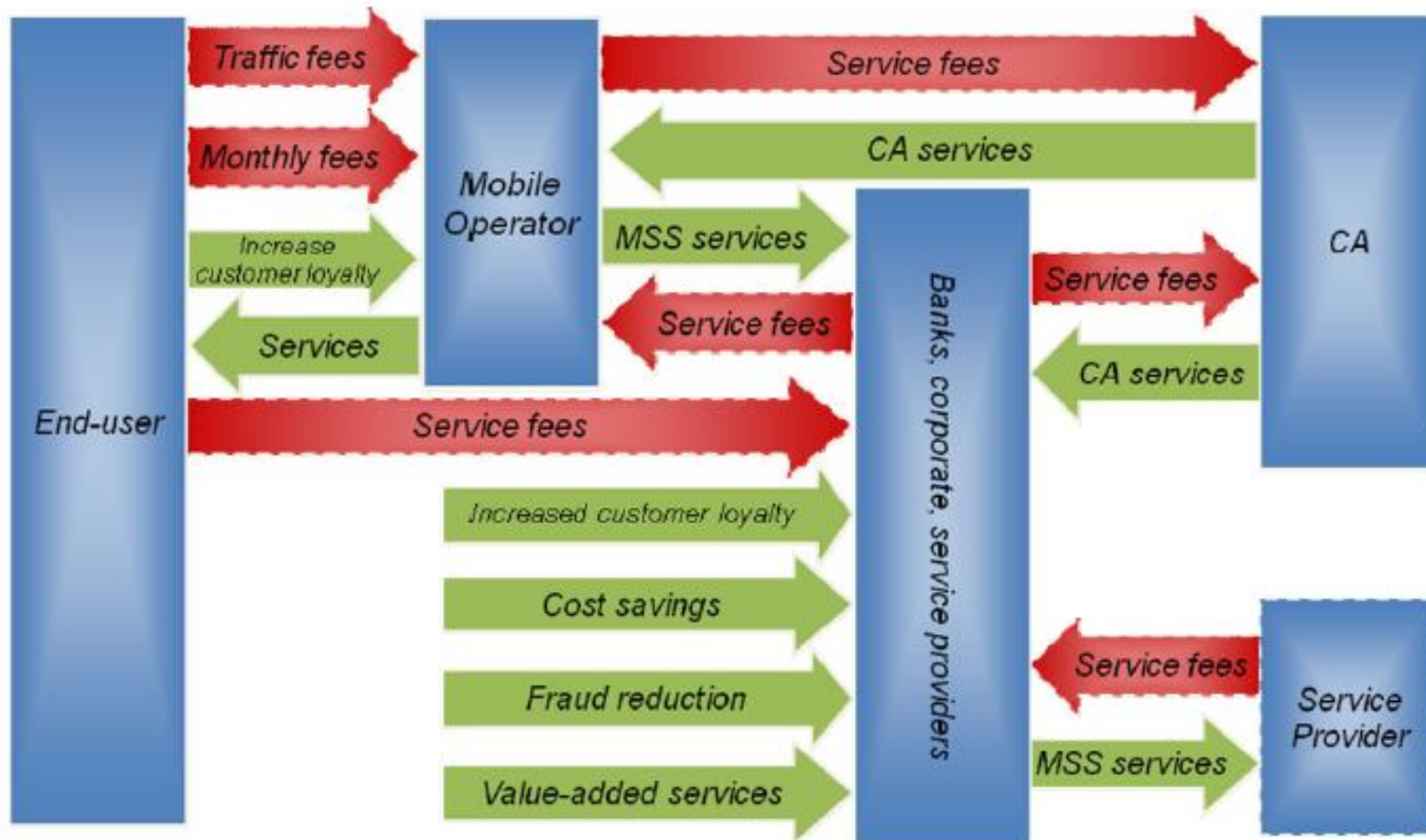
Direct revenue opportunities for Operators

- Increased SMS traffic

- Premium SMS traffic

- Financial transaction sharing

- Transaction charging per signature access

- Customer subscription

- UICC space rental

- Registration Process charging

QUESTIONS?
THANK YOU!