# Secure Element – Protecting Your Digital Life

gemalto
security to be free

Dr. H. Karen Lu
July 27, 2016

# We enable our clients to bring **trusted and convenient digital services** to billions of people

**€3.1bn**
2015 REVENUE

**14,000+**
EMPLOYEES

**117**
NATIONALITIES OF OUR EMPLOYEES

**3,000**
R&D ENGINEERS

**4000+**
PATENTS

**+2bn**
END USERS BENEFIT FROM OUR SOLUTIONS

**180+**
COUNTRIES WHERE OUR CLIENTS ARE BASED

**30,000+**
Enterprise Customers

**3000+**
Financial institutions

**450**
MNOs

**80+**
Government programs

gemalto


BILLIONS OF PEOPLE AND THINGS WITH UNIQUE, PROTECTED IDs
BUSINESSES AND GOVERNMENTS WITH DIGITAL ASSETS
WE AUTHENTICATE IDENTITIES AT THE EDGE OF NETWORKS
WE PROTECT DATA AT THE CORE OF NETWORKS
WE EMBED SOFTWARE IN PRODUCTS
WE DEPLOY PLATFORMS & SERVICES
ID AUTHENTICATION
DATA PROTECTION
STRONG ID VERIFICATION
ID ISSUANCE
Software & products
Software licenses
Software licenses
Services

# Amazing digital future for man and machines

- Internet of Everything
  - We use our smart phones, tablets, laptops in every aspect of our lives
  - Our **smart homes** anticipate our needs
  - We live in **smart cities**
  - Our data and robot intelligence live in the **cloud**

# Great new convenience and productivity

- Our automobiles drive themselves
- Our drudgework “chores” disappear
- Automatic backup of *everything*
- We can be productive while riding in our cars
- $CO_2$ emissions dramatically reduced

# Terrifying vulnerabilities

- Many things are automated
  - Cities, homes, finances, appointments…
  - Our smart homes and online services know everything about us
- Automation may introduce vulnerabilities
  - Many of today's systems have little protection
    - e.g., power grid, HVAC, water supply
  - What about state-sponsored or terrorist group attacks?
- What about our privacy?
  - How do we keep our personal data away from wrongdoers?

# You are not as safe as you think

"In the space of one hour, my entire digital life was destroyed."
- Mat Honan 08.06.12 8:01 PM

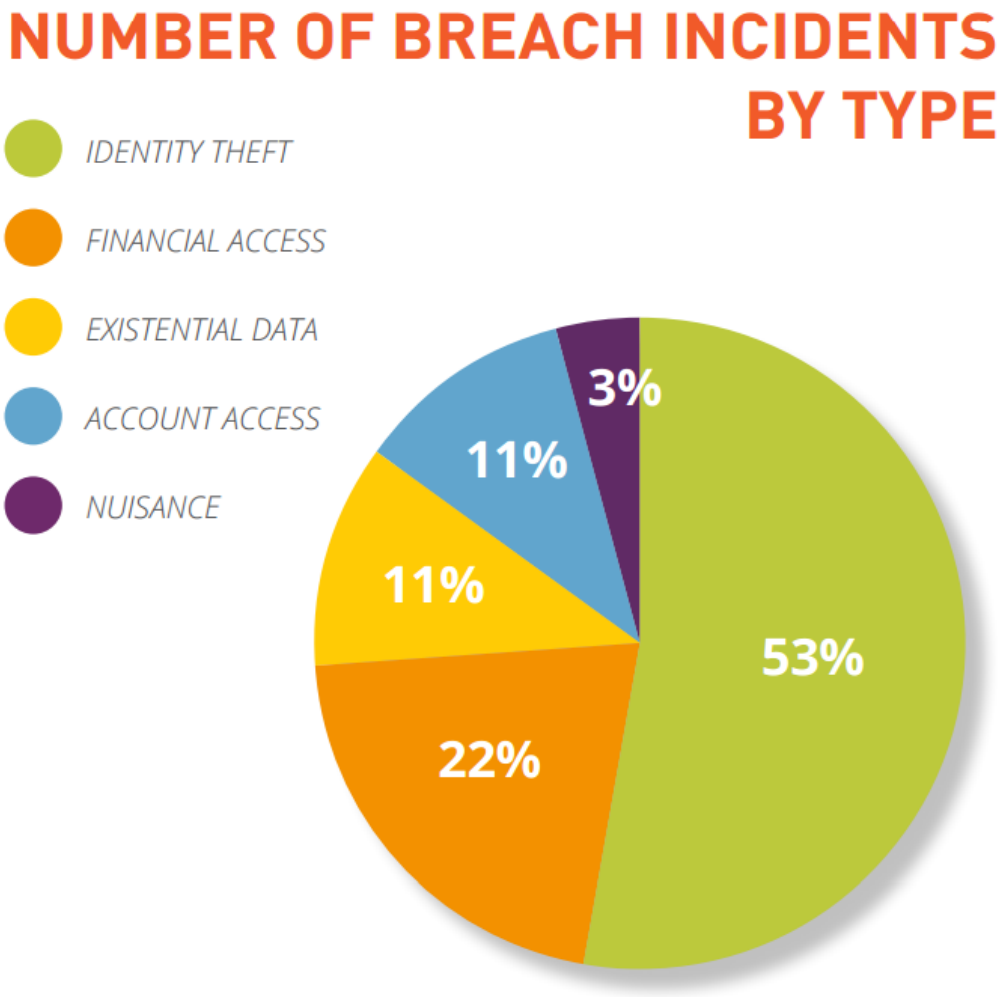




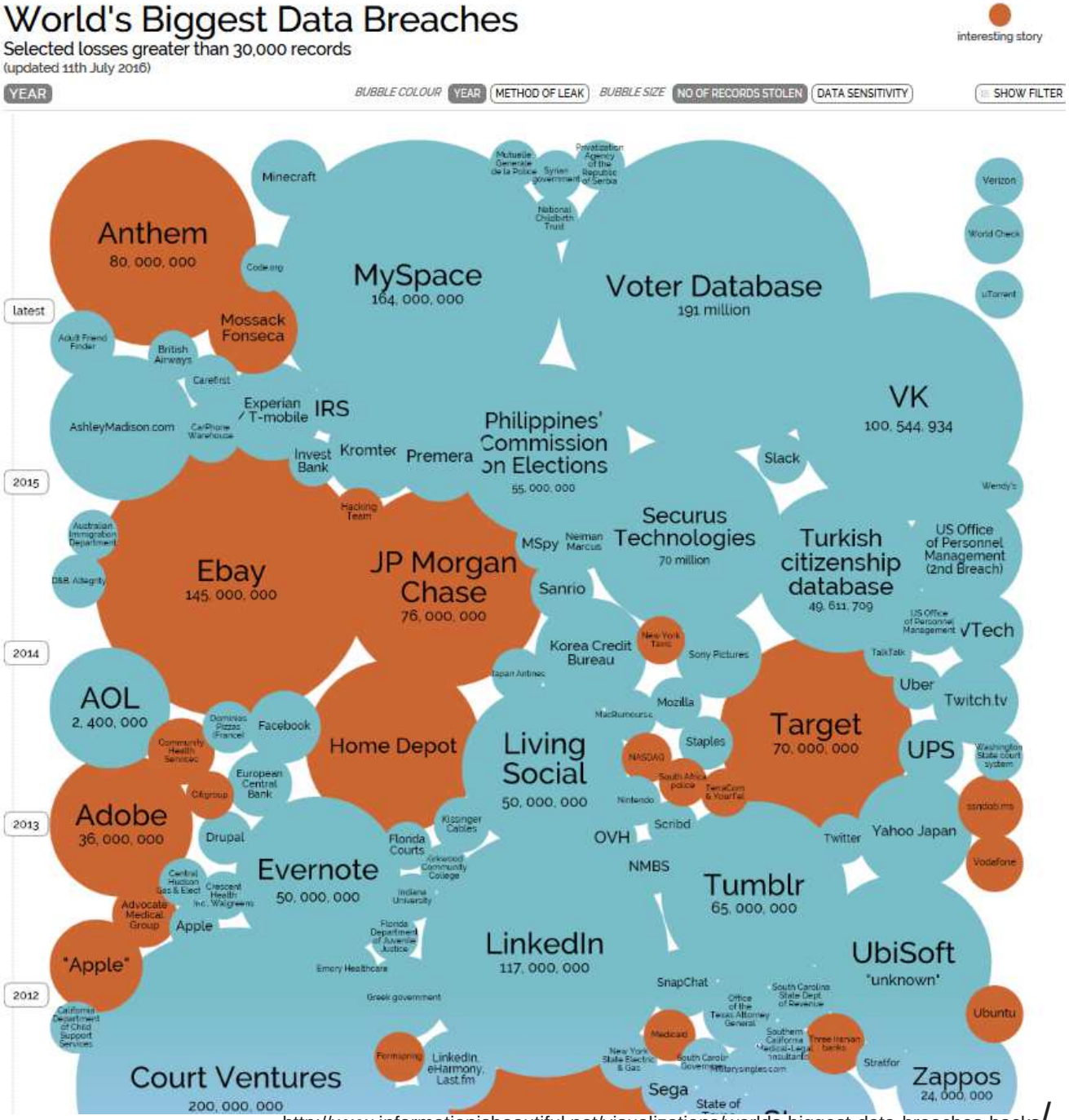
*Theft of identities and personal information retains top spot, accounting for 53% of data breaches; healthcare and government overtake retail as most-targeted sectors*

**AMSTERDAM – February 23, 2016** — Gemalto (Euronext NL0000400653 GTO), the world leader in digital security, today released the latest findings of the Breach Level Index, revealing that 1,673 data breaches led to 707 million data records being compromised worldwide during 2015.

http://www.gemalto.com/press/Pages/Gemalto-releases-findings-of-2015-Breach-Level-Index.aspx




http://www.gemalto.com/brochures-site/download-site/Documents/Gemalto_H1_2015_BLI_Report.pdf




http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

# What does it take to break a password?

| Numerals | 0123456789 | | | | | | |
|---|---|---|---|---|---|---|---|
| Password | | Class of Attack | | | | | |
| Length | Combinations | Class A | Class B | Class C | Class D | Class E | Class F |
| 2 | 100 | Instant | Instant | Instant | Instant | Instant | Instant |
| 3 | 1000 | Instant | Instant | Instant | Instant | Instant | Instant |
| 4 | 10,000 | Instant | Instant | Instant | Instant | Instant | Instant |
| 5 | 100,000 | 10 Secs | Instant | Instant | Instant | Instant | Instant |
| 6 | 1 Million | 1½ Mins | 10 Seconds | Instant | Instant | Instant | Instant |
| 7 | 10 Million | 17 Mins | 1½ Mins | 1½ Mins | Instant | Instant | Instant |
| 8 | 100 Million | 2¾ Hours | 17 Mins | 1½ Mins | 10 Seconds | Instant | Instant |
| 9 | 1000 Million | 28 Hours | 2¾ Hours | 17 Mins | 1½ Mins | 10 Seconds | Instant |

| Mixed Alpha and Numerals | 0123456789AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWwXxYyZz | | | | | | |
|---|---|---|---|---|---|---|---|
| Password | | Class of Attack | | | | | |
| Length | Combinations | Class A | Class B | Class C | Class D | Class E | Class F |
| 2 | 3,844 | Instant | Instant | Instant | Instant | Instant | Instant |
| 3 | 238,328 | 23 Secs | < 3 Secs | Instant | Instant | Instant | Instant |
| 4 | 15 Million | 24½ Mins | 2½ Mins | 15 Secs | < 2 Secs | Instant | Instant |
| 5 | 916 Million | 1 Day | 2½ Hours | 15¼ Mins | 1½ Mins | 9 Secs | Instant |
| 6 | 57 Billion | 66 Days | 6½ Days | 16 Hours | 1½ Hours | 9½ Mins | 56 Secs |
| 7 | 3.5 Trillion | 11 Years | 1 Year | 41 Days | 4 Days | 10 Hours | 58 Mins |
| 8 | 218 Trillion | 692 Years | 69¼ Years | 7 Years | 253 Days | 25¼ Days | 60½ Hours |

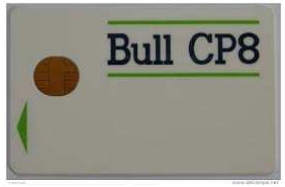
Friday 10th July 2009 03:01

We have to look for better solutions…

http://www.lockdown.co.uk/

# How do we protect our digital life?

# Secure Element (SE)

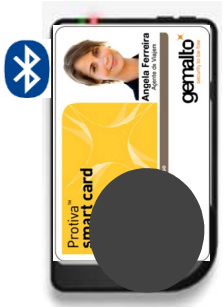




- Smart Card (IC Card) was invented in 70’s.
- Tamper-resistant platform
  - With an embedded microprocessor
  - Secure memories; ROM, Flash, RAM
  - Secure hardware and secure firmware/software
  - Hardware cryptographic engine
  - Host application, confidential data, and cryptographic keys
- Secure hardware
  - Sensors to detect power supply fluctuation, clock manipulation, physical tampering.
  - Circuit designed to prevent side channel attacks (EM, power draw, timing)
  - Automatic shut-down and data erased when attack detected
- Secure personalization and deployment
  - Remotely manage the life cycle of digital credentials
- Multiple form factors and means of communications

# Secure Elements


Via NFC



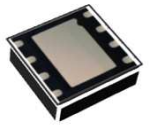

Via
Bluetooth



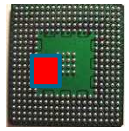
Via contact


MicroSD

UICC



eSE



TEE

**Detached SE**

**Semi-detached SE**

**Embedded SE**

# Applications

- Strong authentication
- Secure banking
- Trusted identity for mobile phones and remote machines
- Digital signature
- Data encryption and decryption
  - Crypto keys are strongly protected
- Internet of Things (cars, smart homes, …)
- Many more and coming…

# Classical Smart Card Applications

# Subscriber identification module (SIM)

- Used to identify and authenticate subscriber
- Inside SIM
  - ICCID: integrated circuit card identifier – internationally identified
    - Network specific information
  - IMSI: International mobile subscriber identity
    - Uniquely identify the SIM card in its operator network
  - Authentication key
    - *Authenticate the mobile device to the network*
  - Preferred networks – for roaming
  - SMS messages and contacts (before smart phones)

# Identification (ID) Cards

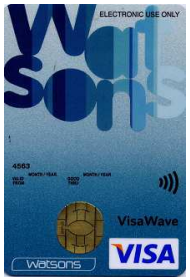
- Adoptions
  - Government
    - e.g. Personal Identification Verification (PIV)
  - Enterprise
  - Health care



- Usage
  - Physical access
  - Logical access
    - Login to computer networks
    - VPN
  - Encryption / decryption documents, emails
  - Digitally signing documents, emails

# Banking card


- Magnetic strip credit cards are easy to duplicate
- Smart card is secure and tamper resistant




- Practically impossible to duplicate a smart card
  - Banks trust it!
- Chip card is widely used around the world
- Finally arrived in America…

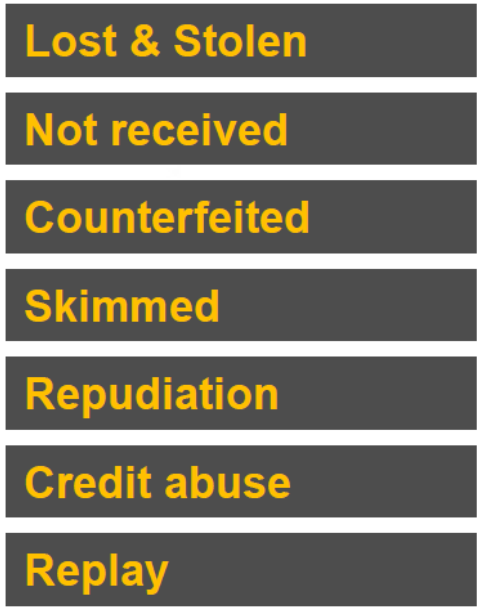
# What is EMV?

# EMV

- EMV is a technical standard for smart payment cards, payment terminals, and automated teller machines (ATMs).
- EMV stands for Europay, MasterCard, and Visa.
  - Introduced in 1994
- The standard is now managed by EMVCo
  - Consortium of Visa, Mastercard, JCB, American Express, China UnionPay, and Discover

# Why EMV?

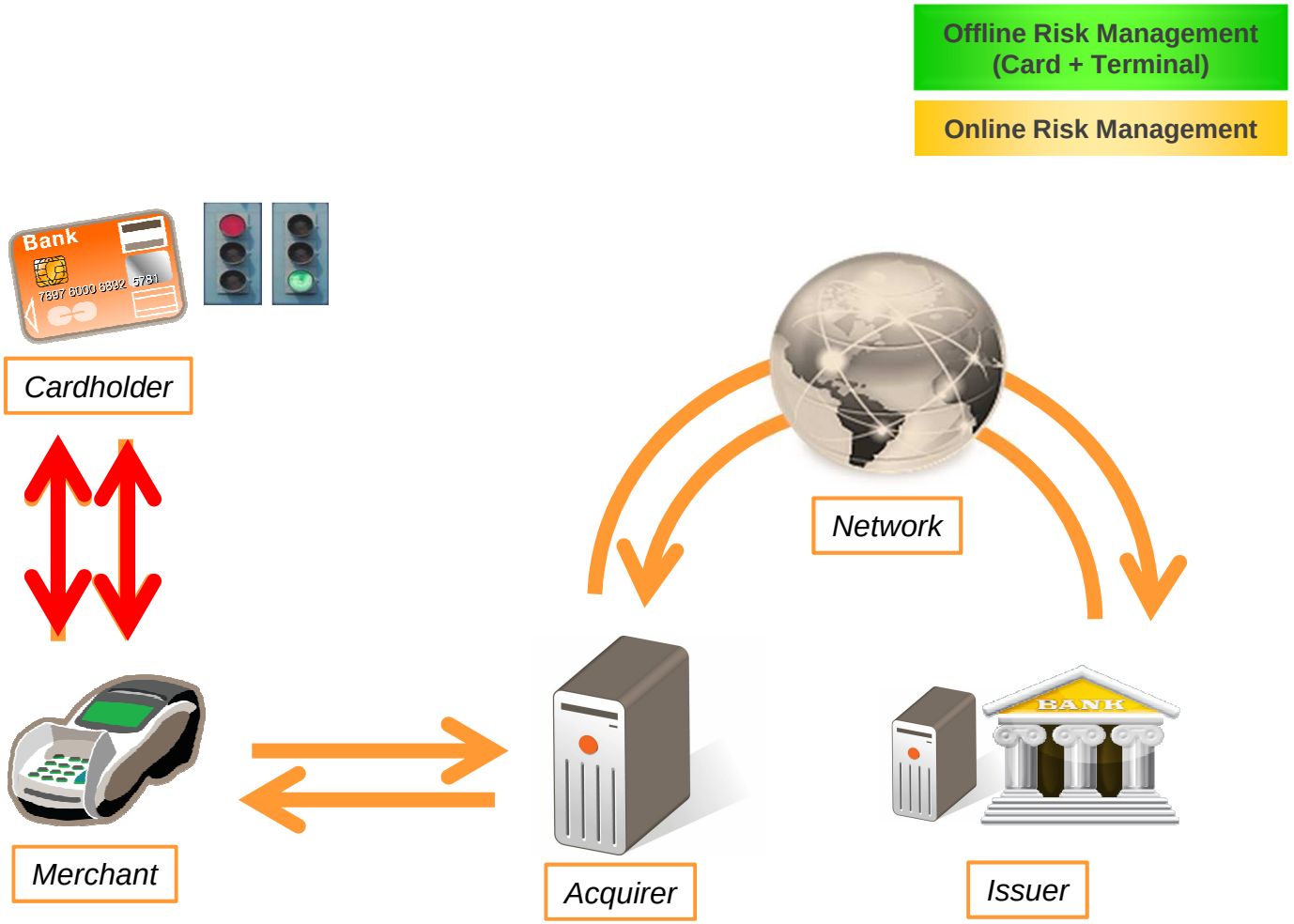
- Improve fraud protection
- Achieve global interoperability
- Reduce transaction cost
- Improve acceptance with offline transactions



# Important security measures in EMV

- Card Authentication (CAM)
  - Is the card genuine?
  - Using asymmetric key cryptography
  - Against counterfeit fraud
- Cardholder Verification Method (CVM)
  - CVM is method used to ensure that a credit card being used is in the possession of its owner
  - EMV supports several CVMs
- Risk management and authorization
  - Authorization Request Cryptogram (ARQC)
  - Control financial risks

# EMV Transaction (Online – no CVM)




Credits to Jack Jania of Gemalto for this and the following EMV slides

# EMV chip transaction – Online


- Transaction initiation: POS and card exchange data
  - Track 2 equivalent data
  - Card settings and capabilities
  - Transaction data (amount, currency, date, etc)
  - …

# EMV chip transaction – Online


- Card generates an Authorization ReQuest Cryptogram (ARQC).
- ARQC is the encryption of card and terminal data using a secret key specific to that card. This key can be retrieved by the issuer authorization system.
- ARQC is a DYNAMIC cryptogram: it is different for each transaction

# EMV contact transaction – Online


- Authorization request is sent to the issuer authorization system
  - Same data as for magstripe transaction
  - Additional EMV data

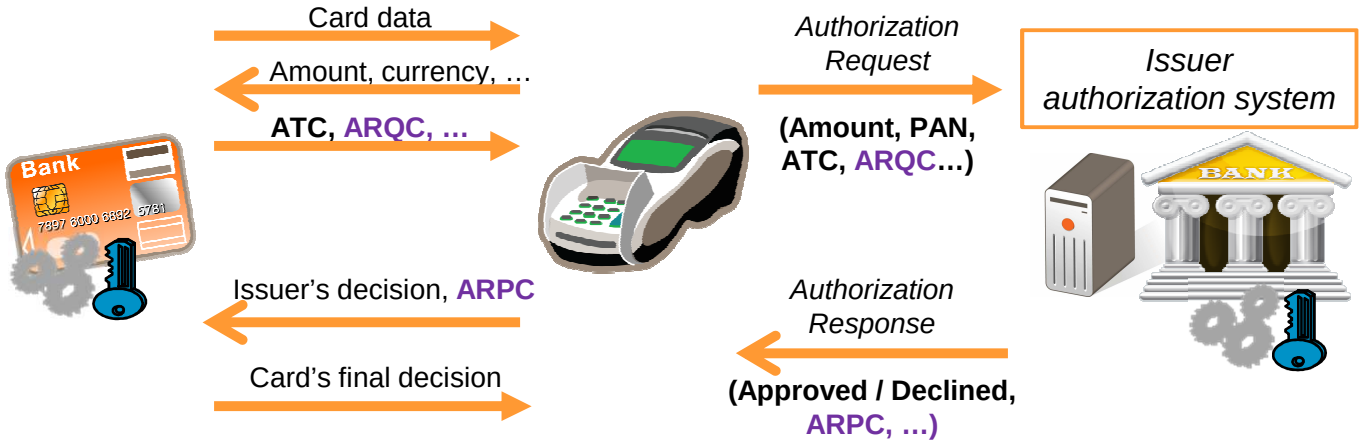
# EMV contact transaction – Online


- The authorization system performs risk management
- It also checks the validity of the ARQC by recalculating it using:
  - the data transmitted in the authorization request
  - the secret key associated to that card
- If the ARQC is validated, the card is considered genuine, and there is a guarantee that the transaction data have not been tempered with (amount, …)

# EMV contact transaction – Online

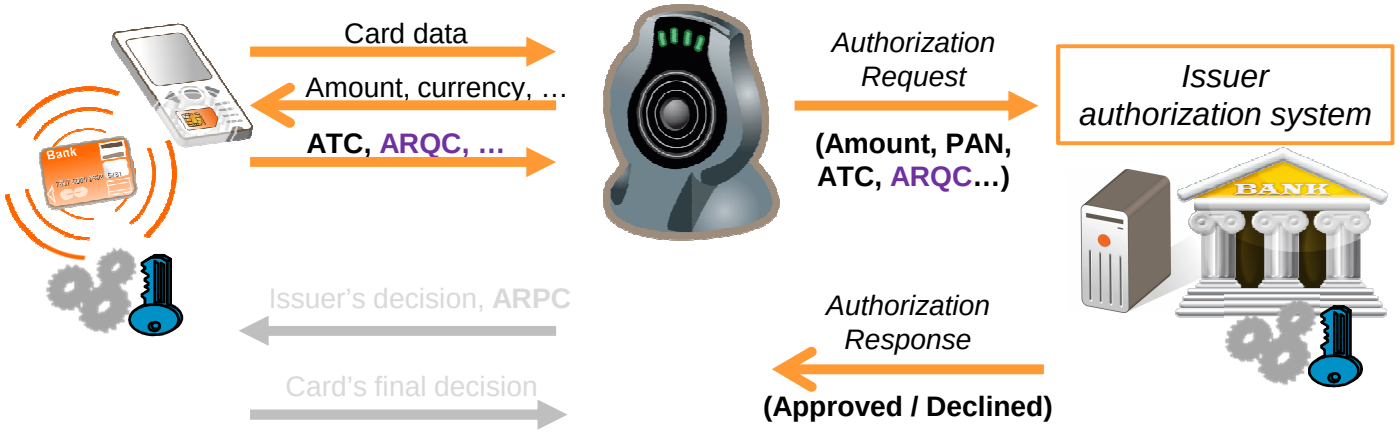
- Card authentication is based on DYNAMIC data (ARQC) generated by the card secret key
- Card secret key cannot be retrieved from a card and duplicated onto another card

# EMV contact transaction – Online




- Issuer host generates an authorization response
- Response may include an Authorization ResPonse Cryptogram that authenticates the issuer and the issuer decision. The card may validate the ARPC before giving its final decision.

# EMV contactless and NFC transactions – Online



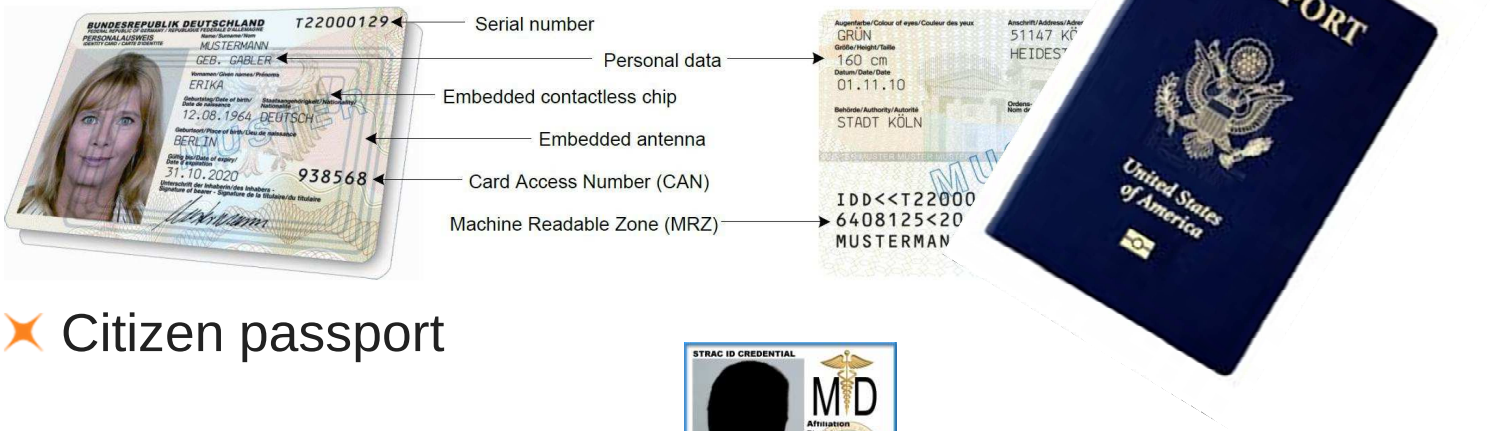

- Contactless and NFC transactions offer the same level of security as contact transactions.

- Contactless and NFC devices leave the field before the authorization response is received by the POS. Issuer actions can be performed:
  - Card: during the next contact transaction
  - Mobile phone: using the OTA (over-the-air) channel

# Modern Applications

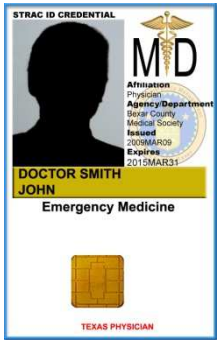
# Emerging Applications

- National eID




- Citizen passport

- Health care card




*Southwest Texas Regional Advisory Council (STRAC) ID Card*

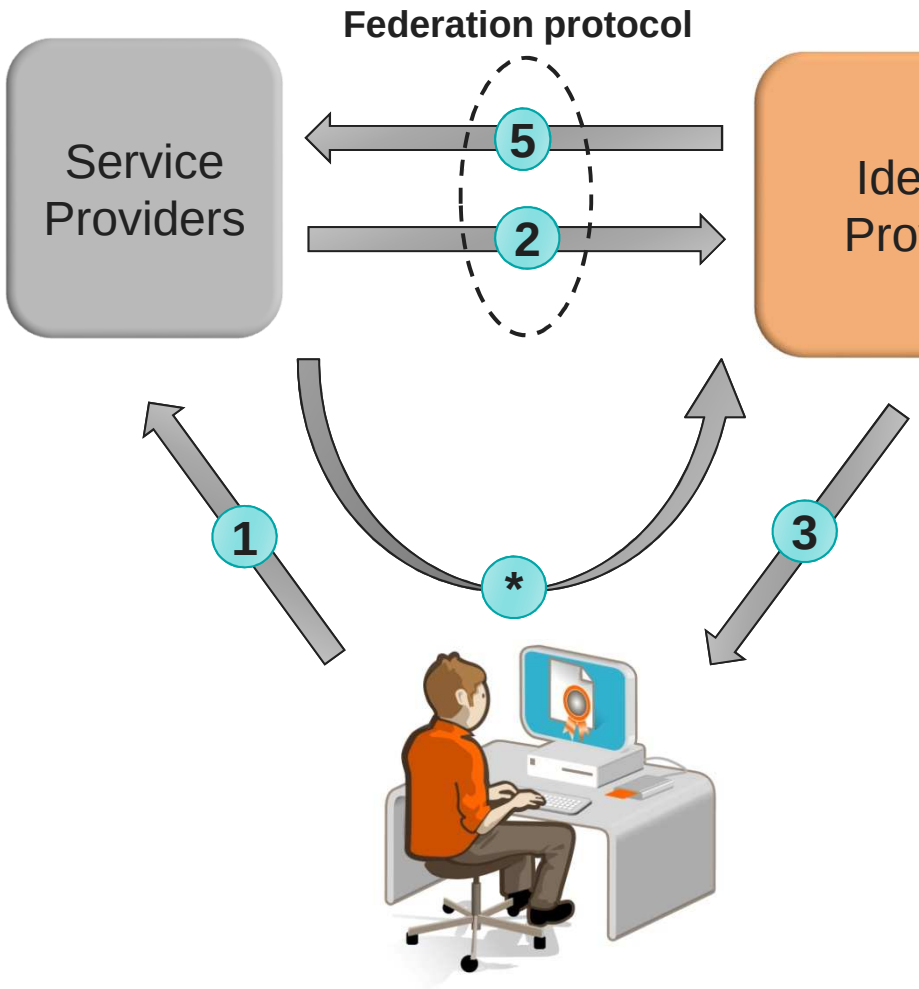
- Online applications

- Mobile Payment

# Multi-Factor Authentication

- What you know
  - password, passphrase, mother's maiden name
- What you have
  - Smart card, OTP token
- What you are or what you do - biometrics
  - Iris, finger print, face, voice, typing dynamics
- Authentications using more than one factors are called strong authentications

# Identity Federation: Single Sign-On




1. *User tries to access a service*
2. *Service providers delegates authentication to Identity Provider*
3. *Identity Provider authenticates user*
4. *Identity Provider retrieves user identity and attributes*
5. *Identity and attributes are returned to service provider*

# Secure Element and Privacy

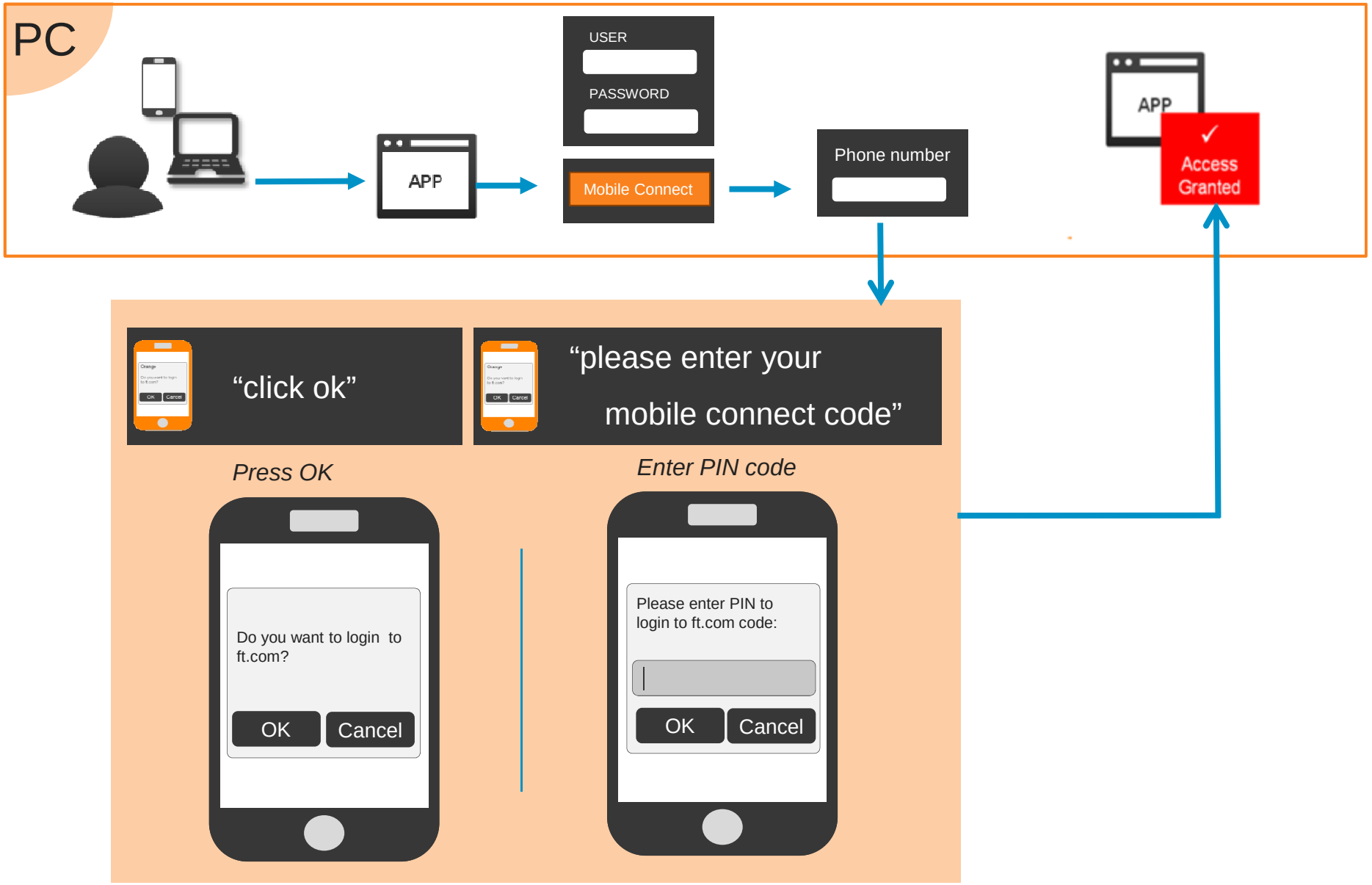
- Secure vault for sensitive data
  - protect against theft
- Privacy cryptography
  - enable anonymous transactions
  - prevent tracking
- Only disclose the needed information
- Trusted offline transactions

# Mobile Connect

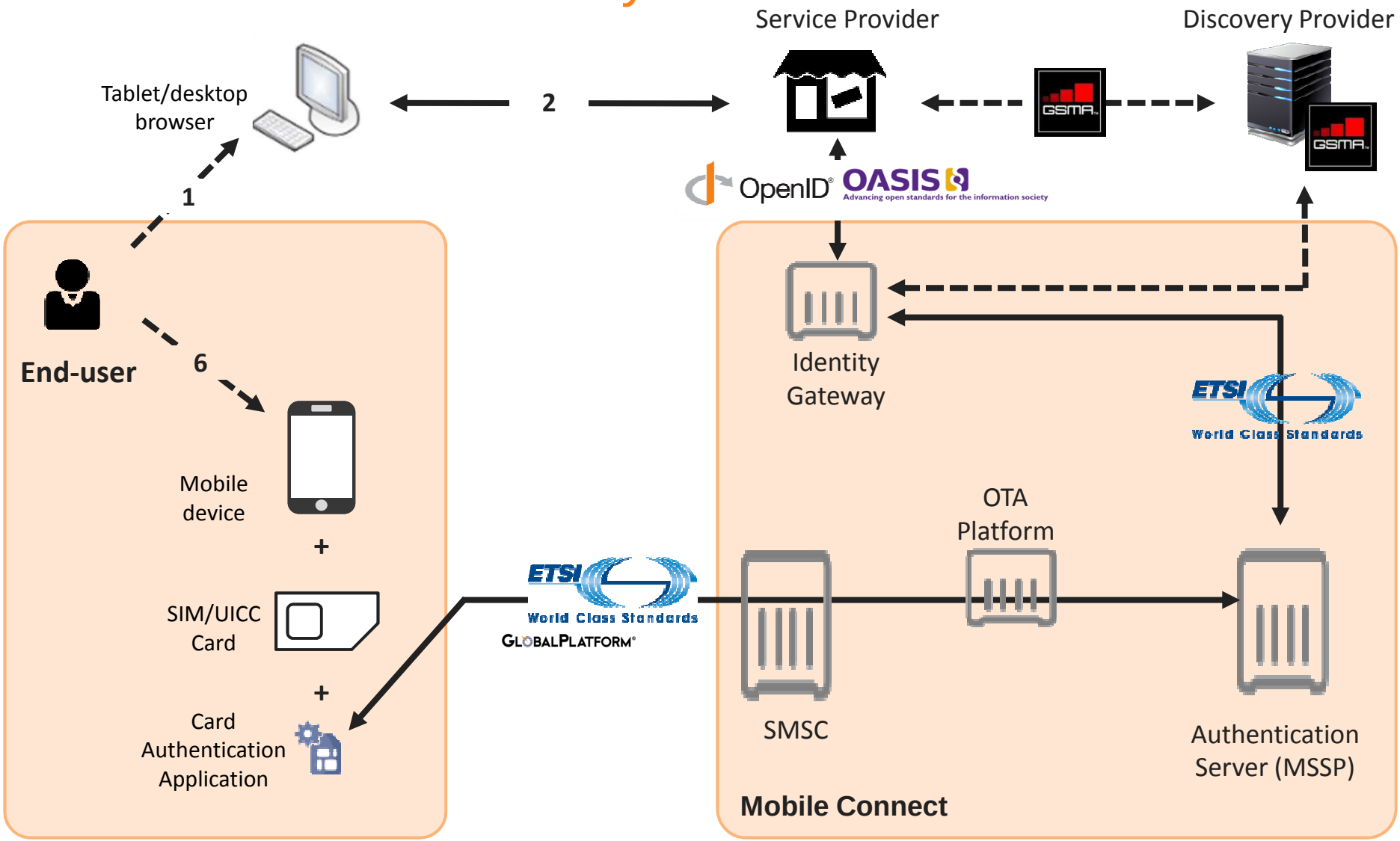
- Uses your mobile device as your identity
- Services
  - Authentication
  - Transaction signing
  - Attributes sharing

- Federated identity service
- Various authentication mechanism transparent to the user.
- GSMA standard

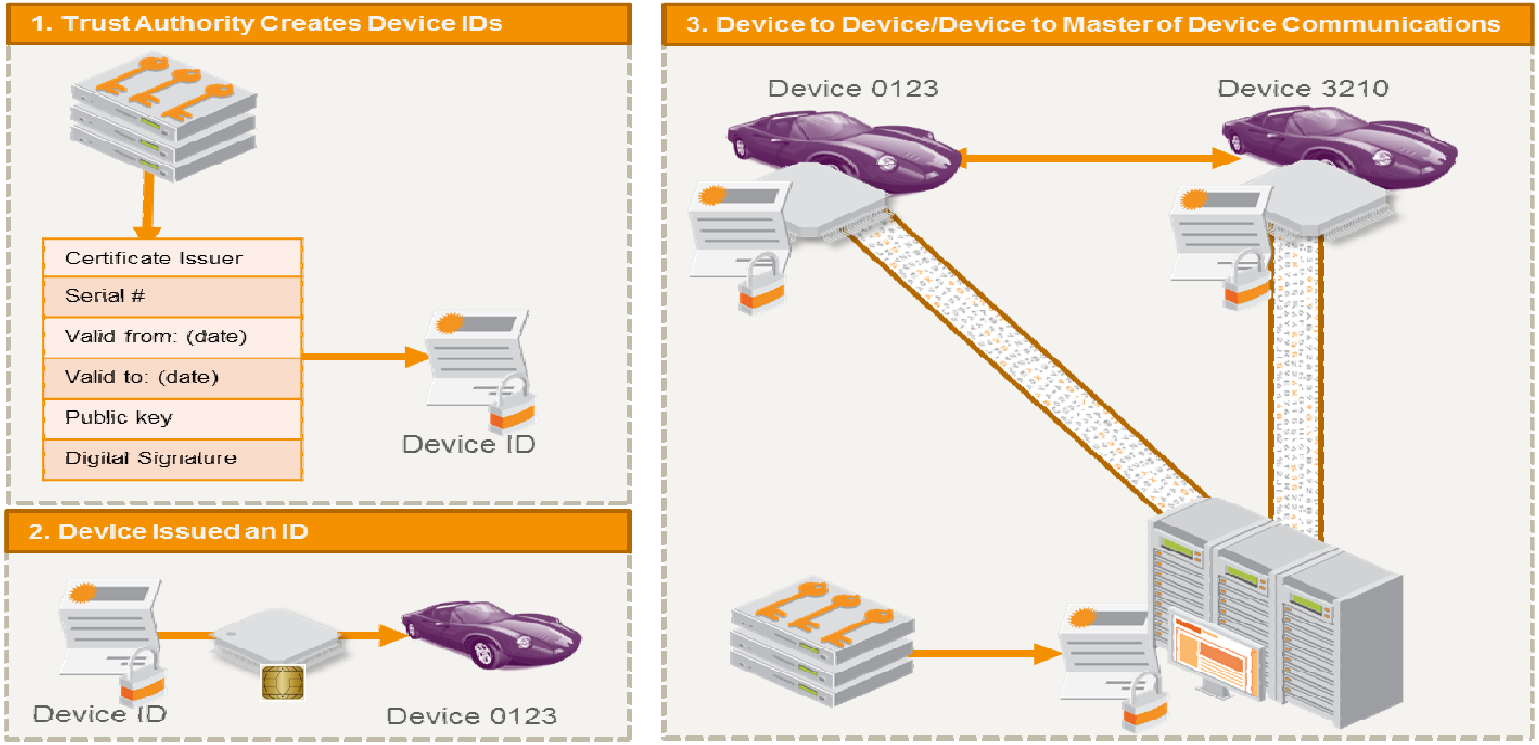
# Provide the **simplest user experience**



# Mobile Connect ecosystem



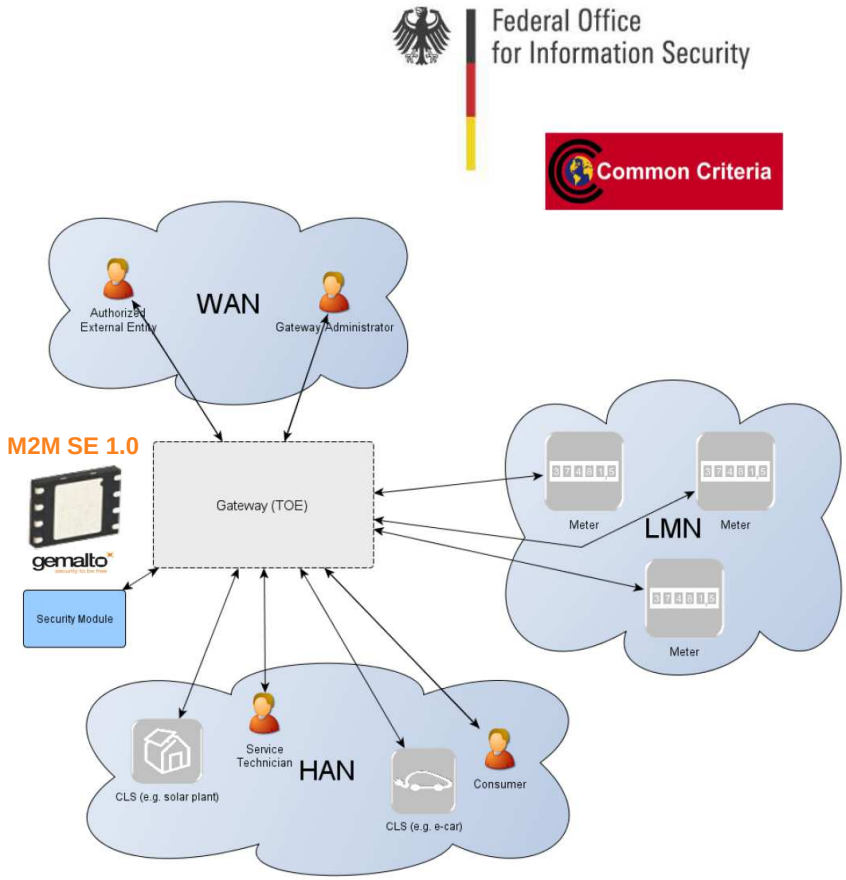
# Securing cars, infrastructure, and services




1. **Authentication into diagnostic tool** used by dealer and independent garages **to issue new /replacement car keys.**
2. **Signing of tokens done with PKI and root in HSM**
3. **Issuance of RSA public keys** and certificates to Electronic Control Units (ECU).
4. **SE protects private keys and crypto processes.**
5. **Enable remote updates of firmware/software to ECUs in the field**.
6. **User authentication to the car – SE-based authentication**
7. **Communication to cellular network**

# Smart Metering Gateway

- **Gateway**
  - Firewall
  - Collects, processes and stores the records from Meter(s)
  - Access control
  - Meter Data encrypted and signed before sending
- **Security Module**
  - Cryptographic service provider
  - Secure storage




Assets to be protected:

- **Meter Data**
- **System/Consumer log data**
- **Gateway time**
- **Personally Identifiable Information** (PII)
- **Configuration data** (meters, gateway)
- **Firmware**
- **Cryptographic keys**

# Takeaways

- Technology advances provide amazing benefits, productivity, and convenience
- Adversaries also use technologies to steal data and identities for financial gains and other malicious purposes
- Secure elements are effective tools for protecting our digital identities

# Thank you!