Analyst session
secure elements and secure issuance

November 3, 2014
Disclaimer

This communication does not constitute an offer to purchase or exchange or the solicitation of an offer to sell or exchange any securities of Gemalto.

This communication contains certain statements that are neither reported financial results nor other historical information and other statements concerning Gemalto. These statements include financial projections and estimates and their underlying assumptions, statements regarding plans, objectives and expectations with respect to future operations, events, products and services and future performance. Forward-looking statements are generally identified by the words “will”, “expects”, “anticipates”, "believes", "intends", "estimates", “target”, and similar expressions. These and other information and statements contained in this communication constitute forward-looking statements for purposes of applicable securities laws. Although management of the Company believes that the expectations reflected in the forward-looking statements are reasonable, investors and security holders are cautioned that forward-looking information and statements are subject to various risks and uncertainties, many of which are difficult to predict and generally beyond the control of the Company, that could cause actual results and developments to differ materially from those expressed in, or implied or projected by the forward-looking information and statements, and the Company cannot guarantee future results, levels of activity, performance or achievements. Factors that could cause actual results to differ materially from those estimated by the forward-looking statements contained in this communication include, but are not limited to: trends in wireless communication and mobile commerce markets; the Company's ability to develop new technology and the effects of competing technologies developed; effects of the intense competition in the Company's main markets; challenges to or loss of intellectual property rights; ability to establish and maintain strategic relationships in its major businesses; ability to develop and take advantage of new software, platforms and services; profitability of the expansion strategy; effects of acquisitions and investments; ability of the Company's to integrate acquired businesses, activities and companies according to expectations; ability of the Company to achieve the expected synergies from acquisitions; and changes in global, political, economic, business, competitive, market and regulatory forces. Moreover, neither the Company nor any other person assumes responsibility for the accuracy and completeness of such forward-looking statements. The forward-looking statements contained in this communication speak only as of the date of this communication and the Company or its representatives are under no duty, and do not undertake, to update any of the forward-looking statements after this date to conform such statements to actual results, to reflect the occurrence of anticipated results or otherwise except as otherwise required by applicable law or regulations.
Securing devices to protect transactions
Richer and more open environments are harder to secure

- Rich operating environments have larger “attack surfaces”
  - Software: rich APIs, access to i/o, network connectivity, strict rights management impacts app convenience, counter-measures impact performance
  - Hardware: tamper resistance difficult to implement

- Development and certification time and costs grow with environment size and openness

- Length of supply chain impacts ability to formally check security
Finding the right recipe: security and flexibility

‘Component’ Security & Cost

Secure Elements

TEE “fills the gap” in device protection
Increases security at system level

Trusted Execution Environment

Rich Mobile OSes

Flexibility & Features
Secure network access requires secure devices

• Whatever the security objective, the keystone to digital exchanges is authentication of users

• Authentication typically relies on
  – something you know, something you are (secret, biometry)
  – something you have (a trusted local device to protect the identification process)

• The trusted device should be un-cloneable and impossible to forge

• To mitigate large scale attacks, use diversified keys and check credentials locally

• Whatever the client, the service provider back-end remains a concern and critical keys should be stored in tamper resistant appliances (HSM)
Typical mutual chip-based authentication

De-centralized dynamic data mutual chip-based authentication

Credential provisioning process into the secure computing environments needs to be handled with care
The economics of secure clients

• Ensuring reliable confidentiality and integrity of digital interactions has a cost (a couple of € per year at large scale)
  – Provisioning the trusted device and managing credentials
  – The secure computing chips
  – Certifications, audits, and additional design and operating constraints

• Once need is established, not equipping users with secure computing chips
  – saves the cost of the chips (only a fraction of the total cost)
  – significantly increases the rest of the cost due to
    • The need for alternative risk mitigation systems
    • Remaining fraud (direct cost as well as damage to brand equity)

This is why when usage of a network increases in volume and value, the relevance of securing clients increases
What’s inside a secure element (secure computing environment)?

Client software embedded in a secure element protects the identity of the user and the authentication process

- Identity certificates of the user
- Reference information: a PIN, biometric template, etc.
- Cryptographic keys for online data exchange
  - Data exchange ciphering
  - Verifies the authenticity of a credential
  - Performs user authentication
  - Checks server identity
- Application and cryptographic software that checks the ID and communicates externally
Secure elements and self-defense

Software defenses

- True random number generation
- Sophisticated cryptographic computation
- Code/logic obfuscation – \([a+b] \) or \( [(a^b)/a + (b/a)^a + ((a^b)/(a^b-1)) - b] \)
- Constant-time programming
- Redundancy and consistency checks
- Data integrity verification
- Detection of wrong execution flow
- Encryption of secret data – cryptographic keys…
- Random delays in processing

Hardware defenses

- Single-component chip design
- Active shielding
- Glue logic design – mixed functional blocks on silicon
- Encrypted buses and memories
- Layered production – buried buses, scrambled memories
- Reduced power signal and electromagnetic emissions
- Analogical Sensors – monitor environment variations (voltage, frequency, light, temperature)
- Logical sensors – detection of inconsistent processing
- Error correction code and memory integrity
Multi-tenancy in secure elements: sharing the computing chip

Service provider encrypts software with their key so they can trust the client and make sure data isn’t snooped by other “tenants”

Each service has a key to access the secure element, this key only grants access to a specific security domain.

Each security domain within the secure element has a unique key from the secure element issuer.

Operating system and supervisory layer assigns keys and creates security domains.

Service providers achieve the same level of risk and data control as issuing their own trusted device.
“Trust me, I’m secure” : Standardization and certification processes

Certification checks that certain security objectives defined by the applicant are achieved.

Target of Evaluation (ToE)

Function & security objectives regarding information assets (keys, algorithms, …)

Tests

Correctness
The behavior of a target relative to a certain specification

Robustness
The resilience of a target relative to a set of faults or attacks

Results

- 7: Formally Verified Design and Tested
- 6: Semiformally Verified Design and Tested
- 5: Semiformally Designed and Tested
- 4: Methodically Designed, Tested and Reviewed
- 3: Methodically Tested and Checked
- 2: Structurally tested
- 1: Functionally tested

Independent labs evaluate products against requirements, typically takes between 8 and 30 weeks. Certification is mandatory by all major banking schemes, GSM operators, and governments.
Identifying users with biometrics instead of secrets

Usage of biometrics does not change authentication schemes

**Pros**
- Convenient for the user
- For governments, bridges digital identity to physical identity

**Cons**
- Not secret, so higher risk of theft
- Cannot be changed if compromised
- Static data, can be replayed
- Risk of false positives and negatives limits accuracy
- Additional privacy implications

Something unique the person is
*Biometrics (fingerprint, facial recognition)*
Software and data stacks in secure elements

User profile

Customer profile and applications

Industry applications

Operating system

Secure hardware
Personalization & Trusted Service Management
Secure provisioning and personalization

How does the supply chain protect sensitive information?

Key ceremonies are performed between stakeholders. Silicon vendors, product companies, personalization providers, and issuers exchange keys locally, using HSMs, to extend the chain of trust.

1. Transport keys from Gemalto are embedded in chips at production

2. For finished products, Gemalto changes transport key, installs OS and sets personalization keys before sending finished product to personalization provider
Secure provisioning and personalization

Personalization provider adds issuer application and data, user data, network certificates in a “perso” bureau or over-the-air using preloaded post-issuance keys to create unique user credentials.
Trusted Service Management: installing and managing secure services over-the-air on a secure client

1. **Creation** of a Security Domain for service providers within the secure client
2. **Download & installation** of the applications in the Security Domain
3. **Personalization & activation** of applications
4. **Lifecycle management** of activated services
Separation of functions, interoperable standards and robust key management enable a many-to-many ecosystem

**Secure Element Issuer TSM**
- End-user eligibility check
  - Secure element, handset and subscription eligibility
- Create security domains on request
- Service delivery
  - Load, install, activate, remove services at request of SP TSM (simple mode)
  - Issue token to SP TSM to load, install, activate, remove services (delegated mode)

**Service Provider TSM**
- Service Installation
  - Eligibility check
  - Data preparation
  - Application download, installation and Personalization
- Over-the-Air Lifecycle (post-issuance)
  - Counter reset (payment)
  - Credential Management (ticketing, access rights, boarding passes, car keys)
  - Lock-UnLock-Delete service

**Types of secure clients**
- Multi-tenant SIM, Embedded Secure Element (eSE), Micro SD (µSD) and Trusted Execution Environment (TEE)

**Types of services**
- Payment, transport, ticketing, physical access, online identity, retail and loyalty
High level of security made possible by the TSM is a result of a carefully monitored chain of trust between parties.

- **Service Provider**
  - Issuance system
  - Customer Care
  - Other IT systems

- **Gemalto**
  - KMS
  - Over-the-Air gateway

- **Secure Element Issuer**
  - KMS
  - Over-the-Air gateway

**Key Actions**
- Master key given to Gemalto
- Keys deployed to encrypt data inside security domain
- Keys deployed to protect access to each security domain
- Master key given to Gemalto
The Trusted Service Hub interconnects existing or new TSMs

TSM for banks
TSM for transit
TSM for onlineID

TSM-SP

TSM-SEI

TSH
Trusted Service Hub

On site, from Gemalto or not
Services by Gemalto
To join, serviced by Gemalto or not

tens ➔

thousands ➔

to join

to join

to join

hundreds ➔
Gemalto offers market neutrality, expertise and wide reach

For Service Providers

- One single contract, with Gemalto

  Access to all devices, preserving direct relationship to users

  Preservation of business independence

For Secure Element Issuers

- Trusted Services Hub
  Available today, to all stakeholders, directly from Gemalto
  Access to a wide range of service providers
  Integration with all types of secure elements

The broadest expertise and field experience
In payment, expectations for trust and cost efficiency are rising.

**In-store**
- Magnetic stripe
- Card Not Present payment app and related cloud service
- Chip-based EMV

**Online**
- PAN manual entry, login/password, sms verification
- SE-Secured in-app and in-browser online payment

Previous generations of payment technologies are progressively replaced to reach new market expectations for security and cost efficiency.

Per issuer, **1** digital payment instrument

Per issuer, **Multiple** digital payment instruments
For banks, the Trusted Service Hub delivers secure payment data into a diverse range of devices.

Management of the payment enablement data in the device on behalf of the issuing bank.
More generally, an acceleration in the spread of secure elements expands our market.

**BEFORE**
- 1 application (SIM)
- 1 type of device (Phone)
- 1 data mgmt service (OTA)

**AFTER**
- Many applications
- Many types of devices
- Many data mgmt services

Proportion of SIM cards sold annually that are 4G or multitenant moving from 0 to 15%

2% CAGR

+50bp CAGR

The opportunity described in our development plan is materializing.
Embedded SIMs need both a SIM and subscription management

1. Integration of the SIM
   - SIM integrated by OEMs
   - Based on an advanced operating system, multitenant
   - Contains a bootstrap MNO profile and access keys to enable further provisioning

2. Subscription management service
   - Issuance of a new profile and access keys by the selected MNO
   - Loading of the secure data into the preinstalled SIMs
   - Based on the typical 2-sided TSM architecture (Supervisor=OEM, Service Provider=MNO)

Value for Gemalto

- Gemalto’s added value is unchanged (embedded OS, applications, secure processes, scale)
- Consumer device lifetime similar to postpaid SIM lifetime
- In place for the M2M market since 2011

Value for Gemalto

- An additional TSM service is necessary to manage MNO-issued subscriptions throughout the lifetime of a device
- Activation rate in line with current SIM renewal rate (higher for prepaid and lower for postpaid SIM markets)
- It is a many-to-many ecosystem served by Gemalto Trusted Service Hub
Gemalto
Enabling trust in the digital world

- World Leader in Digital Security
- Markets in Strong Development
- Unique Technology Portfolio
- Blue Chip Customers
- Large Free Float and Robust Financials
- A Business Model with Strong Leverage on Growth