Digital Security concept to market

2014 Gemalto Expert Day

Gemalto Investor Relations
<table>
<thead>
<tr>
<th>Time</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>12:00 – 12:45</td>
<td>General Q&amp;A</td>
</tr>
<tr>
<td>12:45 – 13:45</td>
<td>Digital security principles and concepts</td>
</tr>
<tr>
<td>13:45 – 14:45</td>
<td>Client security and personalization services</td>
</tr>
<tr>
<td></td>
<td>Break</td>
</tr>
<tr>
<td>15:00 – 15:30</td>
<td>Real implementation: Trustonic</td>
</tr>
<tr>
<td>15:30 – 16:00</td>
<td>Platform security</td>
</tr>
<tr>
<td>16:00 – 16:30</td>
<td>Solution deployment</td>
</tr>
<tr>
<td>16:30 – 17:00</td>
<td>Real implementation: Trusted Service Management</td>
</tr>
</tbody>
</table>
Digital security principles and concepts
Increasing value of dematerialized exchanges calls for trust

The roots of trust lie in the integrity and the confidentiality of exchanges.

Trust can be enabled through a reliable identification process and cryptography.

This is our business.
The pillars of digital security

Data integrity
Verifying the origin of confidential information and ensuring it has not been modified

Confidentiality
Keeping sensitive information secret and managing access rights

System availability
Protecting infrastructure from threats to maintain service accessibility & continuity
Trust in the digital world starts with a reliable identification.

When this step is done properly, the “cloud” is sure who is accessing it and exchanges can begin.
Authentication lessons: the very basic one

Something unique the person knows or is
- Secret (PIN, password, knowledge-based questions)
- Biometrics (fingerprint, facial recognition)

Main Threats & Risks
- Theft and sharing of credentials
- Password database hack
- Shoulder surfing, key logging software, phishing scams

NOT GOOD ENOUGH ➔ How can you better protect user credentials…?
Authentication lessons: encrypted transmission

Something unique the person knows or is

Cryptographic algorithm

Encryption key

Computing environment

Secure network

Database of credentials

Cryptographic algorithm

Database of encryption keys

sent to the network for verification in an encrypted format

Compromised client leads to compromised keys and by consequence compromised credentials

NOT GOOD ENOUGH → How can you protect the client…?
Authentication lessons: static data chip-based authentication

Something unique the person knows or is

Secure network
- Database of credentials
- Cryptographic algorithm
- Database of encryption keys

Secure computing environment
- Cryptographic algorithm
- Encryption key

Main Threats & Risks

Without compromising anything, encrypted data exchange can be copied and replayed

NOT GOOD ENOUGH → How do you make the exchange inimitable…?
Authentication lessons: dynamic data chip-based authentication

Main Threats & Risks

User could be fooled into performing an exchange and access a fake server

NOT GOOD ENOUGH → How do you establish mutual trust…?
Authentication lessons: dynamic data mutual chip-based authentication

The user credentials for the system are stored in a centralized database at the service provider creating massive damage in case of intrusion.

How can it be better ➔ How do you decentralize user credentials…?
Authentication lessons: de-centralized dynamic data mutual chip-based authentication

Main Threats & Risks

It starts to be reasonably reliable authentication…
But the credential provisioning process for the secure computing environments needs to be handled with care

In the “personalization” section, we’ll see how you securely distribute credentials

Secure network
- Database of credentials
- Cryptographic algorithm
- Database of authentication keys

Reference ID & Local comparison
- Cryptographic algorithm
- Authentication key
- Secure computing environment

Mutual challenge-based authentication
In summary…

• 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)
Additional notes: Biometrics

As you can see, 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)**
Additional notes: algorithm symmetry and dissemination of secrets

Shared secrets for authentication
• Appropriate if the one who performs authentication manages the keys (mobile network operators)

• “Closed loop”

Only public keys are shared (PKI)
• Authenticating entity does not manage the keys, PKI must be used (TLS and server authentication)

• Produces publicly verifiable signatures as required

• “Open loop”

Symmetric algorithm
Same key to encrypt and decrypt (DES, 3DES, AES)

Asymmetric algorithm
Two different keys to encrypt and decrypt (RSA, ECC)
Exercise: Applying the principles

- Cloud security / “secure element in the cloud”
- Online transactions
- One time password (locally generated, remotely generated)
- User and device profiling (fingerprinting)

EMV, Host Card Emulation and Tokenization...
Exercise: Classic EMV (online / offline)

Offline Data Authentication
Identification of card, OS, establishment of secure channel (SDA, DDA, or CDA)

Cardholder verification via method agreed by the card
Identification of the cardholder (online/offline PIN, signature, no CVM)

Card risk/action analysis
resulting in offline decline, offline approval or online check

Online processing
(optional)

Validation by the card of online processing
Based on PKI integrity and non-repudiation

POS risk/action analysis

Payment approved or rejected
Exercise: Token-based EMV (online only)

How does the user authenticate to the network?
• Device and user should be securely authenticated when asking for token.
• Token must go to intended recipient and be protected in transit.

Where does the sensitive data live?
• Token itself, if stored locally, must be secured.
• If stored remotely, authentication credentials must be secured.

Effective security of the system still relies on trustworthy user identification and secured endpoints.
Personalization services & Client security
Authentication principles: secure provisioning and personalization

Transport keys from Gemalto are embedded in chips at production.

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

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

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.
Authentication principles: secure provisioning and personalization

Personalization provider adds issuer data, user data, network certificates in a “perso” bureau or over-the-air using preloaded post-issuance keys to create unique user credentials.
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

Secure operating system and supervisor layer

- 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

<table>
<thead>
<tr>
<th>Target of Evaluation (ToE)</th>
<th>Tests</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Function &amp; security objectives regarding information assets (keys, algorithms,…)</td>
<td>Correctness</td>
<td>Formally Verified Design and Tested</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Semiformally Verified Design and Tested</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Semiformally Designed and Tested</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Methodically Designed, Tested and Reviewed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Methodically Tested and Checked</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Structurally tested</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Functionally tested</td>
</tr>
<tr>
<td></td>
<td>Robustness</td>
<td>Common Criteria Evaluation Assurance Level (EAL)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

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.
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
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
Gemalto Security Labs
At Gemalto, we employ an end-to-end security strategy

Secure client software development

Secure platform software development

Secure implementation and processes
Security labs overview

- Gemalto internal core security laboratories
- Largest pool of experts in the industry dedicated to cryptography and security
- Practical expertise in telecommunications, payment, electronic identity and enterprise IT
- Hundreds of patents in cryptography and security software
- Scope goes from back-end security to tamper resistant device including mobile security
Mission 1: Implement secure software

- Design specific protocols and influence standards
- Implement robust cryptographic engines
- Inject secure patterns and key SW components
- Adapt software to hardware characteristics
- Prove security; certify the software and product

- Design specific protocols and influence standards
- Security best practices on infrastructure running the application or web service
- Prove overall security by certifying the datacenter environment
Mission 2: Design security attacks for in-house evaluation

• Run physical Attacks against secure tokens
  – Invasive probing
  – Reverse engineering
  – Fault injection
  – Side-Channel analysis
  – Relay attack

• Run software attacks against server and mobile applications
  – Penetration testing
  – Cross Site Scripting
  – Spoofing
  – Denial of Service
  – Challenge protocols and stack implementations

• Run mathematical attacks against cryptographic protocols
  – Cryptanalysis
  – Brute force
Mission 3: Monitor, Test, Support

**Prevent**
- Site audits: more than 200 audits in 2013
- Penetration testing: 650 hosts inspected, 100 products scrutinized a year
- Vulnerability scanning: almost 10,000 IT components each month

**Detect**
- Intrusion detection, integrity control, system log optimization.
- Log aggregation and correlation for automatic alerting.
- Security and technology watch

**React**
- Decentralized incident handling process
- Central **Computer Security Incident Response Team** support
Unlocking Value Through Device Trust

Christophe Colas
VP Product Marketing
Christophe.Colas@trustonic.com
April 2014
Trustonic

OUR FOCUS
We develop a secure environment, embedded at the heart of smart connected devices, that provides service providers with an open, accessible means to utilize the hardware security capabilities of these devices.

We call this technology a **Trusted Execution Environment (TEE)**

FORMATION AND OWNERSHIP STRUCTURE

<table>
<thead>
<tr>
<th>Launched in Dec 2012</th>
<th>ARM</th>
<th>Gemalto</th>
<th>G+D</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>40%</td>
<td>30%</td>
<td>30%</td>
</tr>
</tbody>
</table>

Merged leading TEE businesses from Gemalto and G&D and ARM, the leading provider of processors to the mobile industry.

Over 90 Employees (80% Engineering) in Europe, Asia and USA.
How Trustonic Operates

TRUSTONIC *enables* devices with a Trusted Execution Environment (TEE) and root-of-trust at manufacture and sells ACCESS to TEE containers to service providers in need of TRUST.
TEE Brought to Life

Enriching, simplifying, and expanding people’s digital lives by securing valued services on smart devices.
Service providers can:

- **deploy on-demand** hardware protected services into devices secured with ARM TrustZone® with secure access to large device memory and high performance.
- protect sensitive assets (cryptographic keys, certificates, data, secure movie playback, …) in a hardware-protected environment.
- protect user interactions with hardware-based **Trusted User Interface** (login/password/code entry, explicit trusted user validation, biometry,…)

### Use Cases

- VPN
- BYOD
- User & device authentication
- Secure dual persona
- Secure MDM
- Storage encryption
- Logical and physical access control
- Secure wallet and NFC HCE transactions
- Secure messaging (voice and data)
- Data loss prevention
- 2-Factor Authentication
- Install on demand secure video services
Finding the right recipe: security and flexibility

‘Component’ Security & Cost

Secure Elements

Trusted Execution Environment

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

Flexibility & Features

Rich Mobile OSes
## Trustonic Partners

### Chipset and Device Vendors
- Samsung
- LG Electronics
- Qualcomm
- NVIDIA
- MediaTek
- AMD
- Texas Instruments

### Verticals
<table>
<thead>
<tr>
<th>Vertical</th>
<th>&lt;t-dev Partners</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile Financial Services</td>
<td>MasterCard Worldwide, Proxama, INTERPAY, KooLabs</td>
</tr>
<tr>
<td>Enterprise</td>
<td>Good, Symantec, ExacTik, KoolSpan, CertiVoX</td>
</tr>
<tr>
<td>Identity</td>
<td>Nok Labs, intercede, SECURE KEY, Plextek, INTERDigital</td>
</tr>
<tr>
<td>Network Operators</td>
<td>Orange, SK telecom</td>
</tr>
<tr>
<td>Premium Content Protection</td>
<td>VO, Elliptic, InsideSecure, verimatrix, irideta</td>
</tr>
<tr>
<td>Various Segments App Development</td>
<td>Gemalto, Giesecke &amp; Devrient, SRI International, Vellva, ARXAN</td>
</tr>
<tr>
<td>HW/IP Providers</td>
<td>ARM, Synaptics</td>
</tr>
</tbody>
</table>

### Additional Partners
- Trustonic
- Vertical
- <t-dev Partners
Platform security
What types of attacks are directed at servers?

**Design level**
- Passive man in the middle (sniffing)
- Active man in the middle
- Session replay
- Session hijacking
- Relay attack

**Development level**
- Buffer overflow
- Backdoor exploits
- Parsing error, SQL injection

**Operations**
- Distributed Denial of Service (DDoS)
- Default and process account vulnerabilities
- Password cracking (brute force, rainbow tables)
Protecting a platform starts in R&D and follows the software development lifecycle

**Design**
- Architects design transaction flows to identify key security touchpoints
- Select appropriate authentication mechanism establish secure channel for all access points
- Implement proper time stamping for tracing and detection of malicious interference

**Development**
- Follow state of the art secure coding standards and practices
- Systematic code review and static code analysis
- Stringent input validation (white list vs. black list)
- Explicit security testing phase including third party audits

**Operations**
- Strong security policies
  - Infrastructure administration
  - Password management
  - Separation of duties
- Multi-factor authentication to operating environment
- Implement system hardening (fewer functions, remove unnecessary services)
- Comply with standards where applicable (i.e. EMV, PCI DSS)
- Preventive monitoring
Practical example: Gemalto Secure Authentication Server

Authentication Server services:
- Customer Account & Credentials management
- Application Enrollment Service
- Smartphone Application Management
- Cryptographic services

Business platform server (from Gemalto or third party)

1. Secure element
   - OoB authentication (Out of Band)
   - Code obfuscation (whitebox crypto)
   - Device fingerprinting

2. Authentication handler
   - HTTPS
   - OAUTH 1.0
   - Challenge / response

3. KMS
   - Hardware Security Module

145912
Customers with high expectations…

- **Highly secured solutions**
  - Compliance with industry specific security standards
  - ISO 27001
  - PCI DSS, PA DSS, payment scheme specific

- **High performance environment**
  - Service Level Agreements (SLA) between 99.5% to 99.999%
  - Active/Active configuration
    (Primary and DR both handle production traffic)
  - Geographic redundancy
  - Full disaster recovery and business continuity plans in place and regularly tested

- **High levels of usability for end users**
  - Easy to enroll in service
  - Easy to use the service

These can be conflicting requirements so compromise against context and time to market is standard.

Security solutions can scale with the magnitude of the deployment.
Solution deployment
Gemalto Global Services

• GGS is responsible for deploying turnkey Platform & Services solutions from Integration (project-based) to Operations (SaaS) and has more than 1000 dedicated engineers.

• Portfolio of offerings includes amongst others, OTA platforms, TSM, mobile payment platforms, government border integration solutions, and authentication servers.

• Over 800 solutions for 348 customers worldwide:
  – ~60% deployed on premise,
  – ~40% deployed as a Service.

• The keys to successful service delivery are: expertise, know how, flexibility and reliability.
Expertise: adding value with solutions beyond technical services

Industry-specific solution architects

MOBILE  BANKING  TRANSPORTATION  ENTERPRISE  GOVERNMENT  MACHINE-TO-MACHINE

combined with technical expertise

SERVER SECURITY  NETWORK ENGINEERING  DATABASE ADMINISTRATION  SYSTEMS ENGINEERING  PERFORMANCE MONITORING & MANAGEMENT

In order to deliver on these megatrends

Need for Trust  Convergence to mobile
Know how: implementing industry best practices

Gemalto solutions have been designed, from the beginning, for a service-oriented business model

Gemalto processes

ITIL services

PMI standards & guidelines
Flexibility: direct operations interface to R&D

- Product roadmap complemented by additions based on feedback from field
- Software add-ons result from scope changes by customers or observations by Gemalto

![Diagram of product roadmap with add-ons in Design, Development, Deployment, and Operations stages.]
Reliability: delivering mission critical systems worldwide

International footprint
• Service centers in 18 countries
• Datacenters on 3 continents

High availability
• Active/active configurations
• Geo-redundancy
• Up to 99.999% uptime SLA

Highly secured
• PCI DSS
• EMV certified
• ISO 27001
• Scheme certifications
Gemalto Secure Datacenters

- Separate physical access control for every level
- No remote administration allowed
- Sensitive cryptographic tasks occur in level 3 only
- Only a level 2 host can access level 3
- Certified by Visa, MasterCard and compliant with PCI DSS
Trusted Service Management
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.
High level of security made possible by the TSM is a result of a carefully monitored chain of trust between parties.
TSM hubs enable much more than payment
Gemalto covers a large part of possible market configurations

Payment service provider
- Classic card data
- Token data

Other service provider
- Other identification and security credentials and applications

OS / emulated card

From many
OS provider

From many
handset manufacturers

From many
network operators

From many
service providers