

# MOBILE PAYMENT SECURITY: REVIEW, TESTING AND CERTIFICATION

Mobile payment is gaining momentum, but as soon as discussions start on mobile payment solutions, concerns are raised on the security of these concepts. For example, the mobile handset as an open platform with Internet connectivity raises security questions. We help our customers to understand the risks of their mobile payment products and test their implementations before they are put on the market.

### Typical questions that we receive from our customers include:

- 1 What are the security requirements from the payment industry regarding mobile payment? And, is there a difference with those from the telecom industry?
- 2 Is security testing of the handset required for my mobile payment solution?
- 3 What is the security impact of choosing a separate secure element over the UICC chip?
- 4 Does the MIDlet of my payment solution need a security review?
- 5 Do I need to use a secure element for my NFC payment product?
- 6 Can I trust the firewall of my Java Card UICC to protect the assets of my application?
- 7 What is the impact of new Global Platform developments on mobile payment applications?
- 8 Which security assessments need to be performed on my TSM platform?
- 9 How security sound is my mobile payment architecture?
- 10 After integrating all mobile payment components, does my solution still provide sufficient security?

### SECURITY CHALLENGES

In the traditional card payment industry, the security certification of smart cards and terminals has become mature and consolidated processes run by schemes like EMVco, MasterCard and Visa. For the mobile industry it is more complex to address security issues in a common approach.



There are a large number of players including lots of Mobile Network Operators, Trusted Service Managers, financial institutions and manufacturers of different components of the mobile payment solution. These different parties do not always have the same business strategy which makes alignment of security requirements a challenge. Furthermore, there are numerous applications based on varying architectures, technologies and standards.

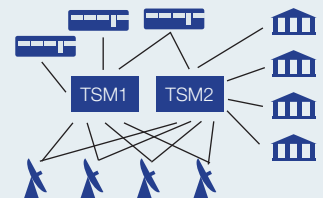
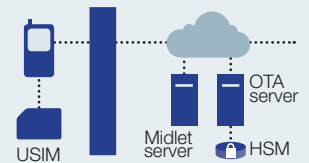
### REVIEW, TESTING AND CERTIFICATION

Having an excellent understanding of the playing field and deep knowledge on the technology, Riscure offers security review and testing services to manufacturers, vendors, mobile network operators and financial institutions that are involved in mobile payment business. At any stage in the development cycle or at issuance of a final product, we can review your architecture design and test the strength of your implementation. Further, if you are a payment scheme, we can assist you in establishing an effective security certification process.

Our expertise includes review, testing and certification of mobile devices, mobile payment applications, secure elements, USIMs, provisioning, NFC, SWP, Java Card, SCWS, Global Platform, OTA and post-issuance downloading.

For a decade Riscure has been testing and researching the security aspects of applications, architectures, implementations, standards and technologies in the mobile and the payment industry. Some highlights are:

<p><b>2001 SMS of Death</b></p>	<p>Riscure discovered the possibility of terminating phones of a specific brand and type by simply sending an SMS with corrupted content. The handset manufacturer used our findings to resolve the issue in newer products.</p>
<p><b>2002 Security Test tool</b></p>	<p>We developed JCworkBench for our Java Card security testing services. JCworkBench challenges the security features of Java Card, Global Platform and SIM Tool Kit implementations.</p>
<p><b>2003 First MasterCard evaluation</b></p>	<p>Riscure performed its first MasterCard CAST evaluation of a Java Card using JCworkBench.</p>
<p><b>2004 Malicious MIDlet</b></p>	<p>We developed a rogue J2ME gaming MIDlet to demonstrate to our customers the threat of installing a stealth key-logger to eavesdrop secret information and attack payment applications on a mobile phone.</p>
<p><b>2005 Security evaluation of mobile payment specification</b></p>	<p>For an international card issuer we evaluated the specifications of the first stand-alone payment application that was intended to run on a mobile handset.</p>
<p><b>2006 Security evaluation of mobile payment solution in Asia with Java MIDlet</b></p>	<p>For one of our customers we evaluated the J2ME MIDlet, the backoffice server application and the provisioning process for a nation-wide handset independent mobile payment solution.</p>
<p><b>2007 Security audit of TSM performing mobile provisioning</b></p>	<p>For a customer we evaluated the provisioning infrastructure and systems used by a Trusted Service Manager.</p>
<p><b>2008 Security evaluation of mobile payment solution using NFC</b></p>	<p>We evaluated security aspects of several mobile payment solutions using NFC for transaction exchange.</p>
<p><b>2009 Review of UICC configuration of Global Platform specification</b></p>	<p>For one of our customers, we reviewed the draft Global Platform specification for the configuration of smart cards in a mobile context.</p>
<p><b>2010 Riscure becomes a participating member of Global Platform</b></p>	<p>In 2010 Riscure has joined Global Platform and contributes to defining the security standard for payment applications in the Security Working Group.</p>
<p><b>2010 Security review of Blackberry and iPhone security</b></p>	<p>For different customers Riscure has analyzed the security of Blackberries and iPhones used in mobile payment solutions</p>



Riscure is committed to support its customers in creating a secure mobile payment solution. Please feel free to contact us for more information about our services at [inforequest@riscure.com](mailto:inforequest@riscure.com) or visit our website at [www.riscure.com](http://www.riscure.com).

**Riscure B.V.**  
 Phone: +31 (0)15 251 4090  
 Fax: +31 (0)15 251 4099  
 E-mail: [inforequest@riscure.com](mailto:inforequest@riscure.com)  
 Website: [www.riscure.com](http://www.riscure.com)

MPS1.X.XXXX

