# Gemalto

Over-The-Air Platform Security Review

White Paper

August 17, 2010

# TABLE OF CONTENTS



Submitted By:
Vijay Akasapu
*Technical Director*

24 West 40th Street
9th Floor
New York, NY 10018

Phone 212.764.0435
Fax 212.764.0436
Email vijay.akasapu@mandiant.com

## EXECUTIVE SUMMARY

Gemalto's Over-the-air Long Term Evolution (OTA LTE) Platform, the industry's first OTAr LTE platform, enables operators to activate subscriptions, manage the subscribers' Universal Integrated Circuit Cards (UICCs) and provide high-speed, low latency, personalized services over an IP-based LTE mobile network. This new way of dialogue with UICCs requires a new interface called "OTA IP Gateway" on the OTA LTE Platform, which exposes it directly to a carrier's wireless network. Classic OTA platforms were previously connected to the SMSC in the core network of the mobile operator and had a reduced risk associated with them. Given this exposure, Gemalto hired Mandiant to assess the interface and enumerate any vulnerability that might leave a carrier's network or its users' data exposed to compromise.

Mandiant performed an in-depth security review of the OTA LTE platform between December 2009 and February 2010. This paper focuses on the critical interface exposed to a carrier's wireless network.

Mandiant concluded that the OTA IP Gateway interface was well secured. Mandiant did not find any vulnerability that exposed a carrier or its users to severe abuse of service or data. Exposure was limited to information disclosure and, furthermore, was mitigated since exploitation required an attacker to successfully authenticate with the interfaces using unique keys embedded in the UICC cards.

**About Mandiant**

Mandiant is an information security company providing consulting services, managed services, products and education to commercial and federal clients including: Fortune 500 companies, financial institutions, government agencies, domestic and foreign police departments and several of the U.S.'s leading law firms. Mandiant engineers and security consultants are acknowledged experts in the information security industry. In addition to authoring nine books and numerous articles about rootkits, computer forensics and incident response, members of Mandiant's team have been featured on news programs including CBS's *60 Minutes*, CNN's *Talkback Live*, NBC News and FOX News.

**About Gemalto**

Gemalto is the world leader in digital security with 2009 annual revenues of €1.65 billion, and over 10,000 employees operating out of 75 offices, research and service centers in 41 countries.

Gemalto is at the heart of our evolving digital society. The freedom to communicate, travel, shop, bank, entertain, and work—anytime, anywhere—has become an integral part of what people want and expect, in ways that are convenient, enjoyable and secure.

Gemalto delivers on the growing demands of billions of people worldwide for mobile connectivity, identity and data protection, credit card safety, health and transportation services, e-government and national security. We do this by supplying to governments, wireless operators, banks and enterprises a wide range of secure personal devices, such as subscriber identification modules (SIM), Universal Integrated Circuit Card (UICC) in mobile phones, smart banking cards, smart card access badges, electronic passports, and USB tokens for online identity protection. To complete the solution we also provide software, systems and services to help our customers achieve their goals.

As the use of Gemalto's software and secure devices increases with the number of people interacting in the digital and wireless world, the company is poised to thrive over the coming years.

For more information please visit www.gemalto.com.

## INTRODUCTION

The UICC is the smart card used in mobile terminals. The card authenticates the subscriber to the network while ensuring the integrity and security of their personal data. In addition, it also stores applications for both operator and end-user use for the correct deployment of mobile services.

The integration of UICC into IP networks and the ability for carriers to use the UICC for plug and play personalization of the handset, thereby offering a more tailored service for their subscribers, exposes not only the end-user UICC card but also the carrier's OTA LTE platform to attacks. For this reason, Gemalto designed specific security schemes to not only protect the OTA LTE platform but also the end-user UICC.

Mandiant performed an in-depth security review of the OTA LTE platform from the perspectives of not only external attacks but also a malicious user that has compromised UICC cards and is able to successfully authenticate to the OTA LTE platform.

### PLATFORM OVERVIEW

Gemalto's OTA LTE Platform introduces an important innovation in OTA management by using HTTPs protocol and by reversing the classical OTA server push model to a pull model, in which the UICC initiates the dialogue.

This approach relies on field-proven protocols and architecture to achieve performance, reliability, scalability and availability. Moreover, it makes integration and deployment schemas in carrier networks easier. The high-level architecture of the OTA LTE platform is shown in the picture below:

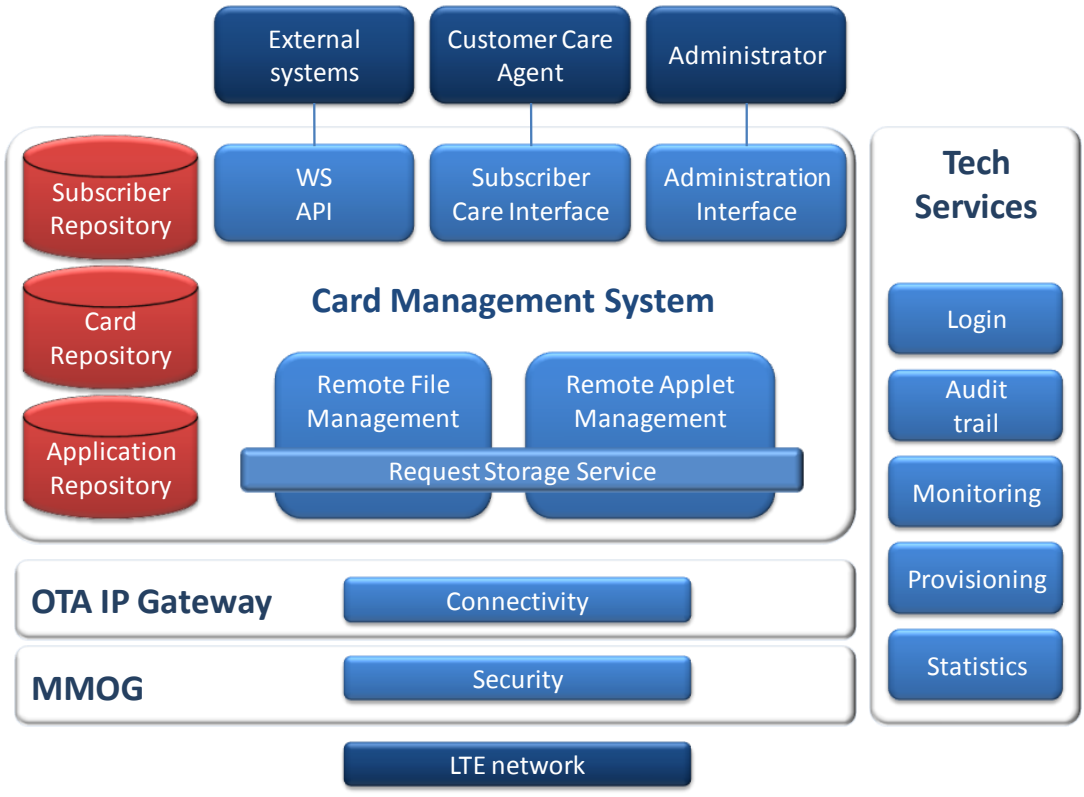



**Figure 1: OTA LTE platform high-level architecture**

The Card Management System is in charge of preparing and storing commands for each request submitted by external systems or customer care agents. When a card contacts the OTA platform, the pending commands are sent to the card on which they are executed.

The image of each card is updated after the OTA update and stored in the Card Management System.

Gemalto implemented two interfaces to protect the Card Management System from external attacks:

- An MMOG HTTPS interface implemented over PSK-TLS based on private keys known by both entities, to ensure mutual authentication, integrity and privacy.
- An OTA IP Gateway implemented using SOAP over HTTP that makes available specific services.

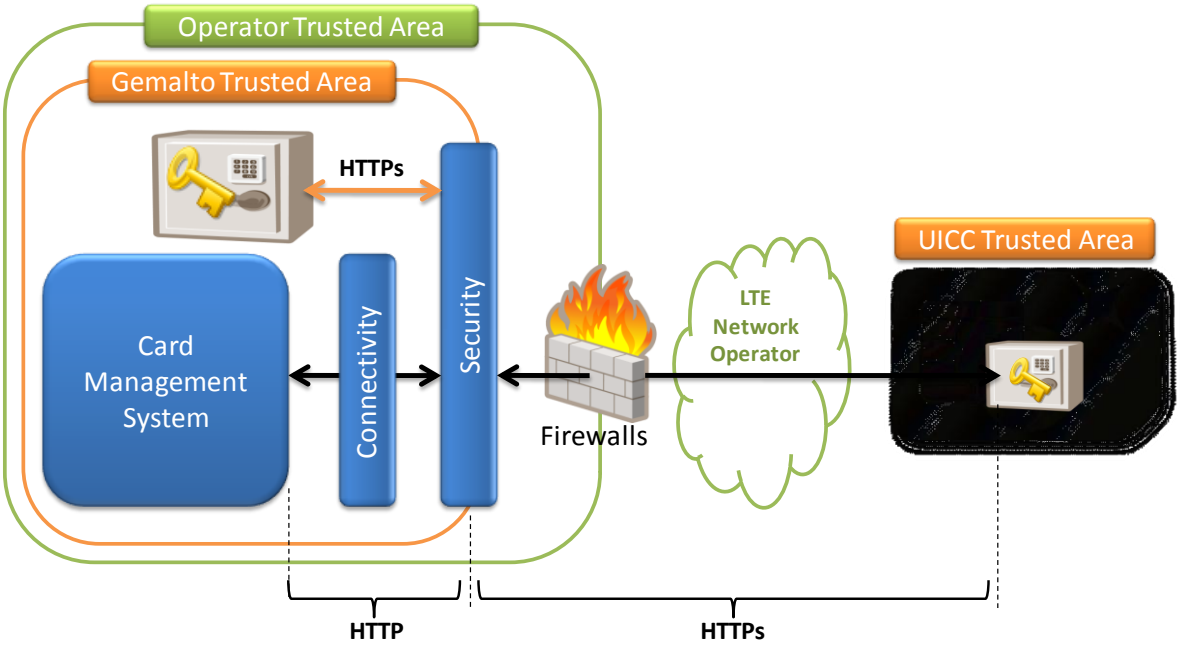



**Figure 2: Trust Boundaries**

## MANDIANT TESTING METHODOLOGY

Mandiant used the following methodology to test the OTA IP Gateway:

- OTA attack model
- Application assessment

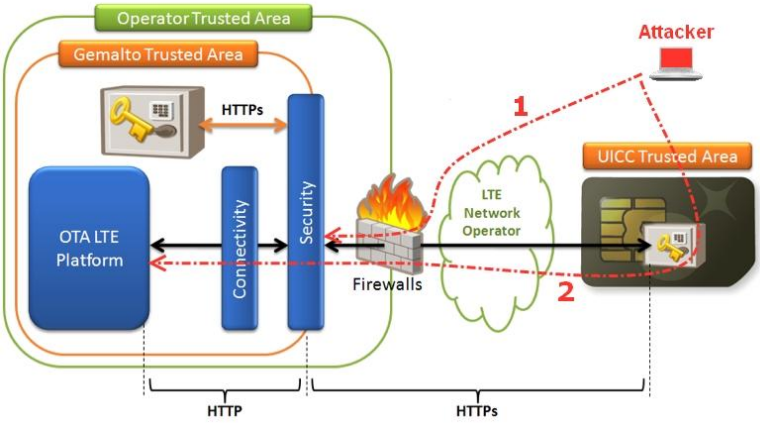
### OTA Attack Model

Mandiant followed the steps below in order to build an attack model for the OTA IP Gateway interface:

1. Documentation review: Mandiant reviewed the relevant product documentation in order to identify some of the use cases and possible abuse cases.

2. Data flow analysis: Mandiant performed a high-level data flow analysis for some of the major use cases for the product. This helped to identify some of the critical components of the product.

3. Attack identification and classification: Based on prior experience and an understanding of the product, Mandiant identified attacks that an attacker could use against the product.




### Attack Surface

Mandiant identified two attack vectors from an external perspective:

1). An attacker with knowledge of the external IP address of the OTA LTE platform attempts to compromise the PSK-TLS protocol implementation of the MMOG HTTPS interface

2). An attacker who has access to a valid SIM card authenticates to the OTA IP Gateway and attempts to compromise the HTTP-based OTAP IP Gateway interface

### Application Assessment

In order to test the two interfaces, Mandiant did the following:

- Generated and issued fuzzed traffic against the MMOG HTTPS and OTA IP Gateway interfaces.
- Performed a configuration review of the MMOG HTTPS interface to ensure weak ciphers were not supported.
- Reviewed the key management algorithm used by the MMOG HTTPS interface to negotiate security with the UICC.
- Reviewed the OTA IP Gateway interface from within the Gemalto Trusted Area in order to simulate an attack where the attacker had successfully authenticated to the MMOG HTTPS interface using valid keys.

## CONCLUSION

With the increase in the usage of all-IP mobile networks for communications between UICC cards and OTA LTE platform, the security of the OTA LTE platform interface related to IP connectivity becomes critical to ensuring the confidentiality and integrity of requests to and from UICC cards.

Gemalto's implementation of the OTA LTE platform and the related interfaces, MMOG HTTPS and OTA IP Gateway, ensures that these security requirements are met. Mandiant did not find any critical vulnerability on either the MMOG HTTPS or OTAP IP Gateway interfaces.

Mandiant's review of the OTA LTE platform was completed in February 2010. As with every product, feature additions or modifications as well as the discovery of new vulnerabilities introduce new risks that may require additional mitigating controls not currently implemented. At this time, however, based on its in-depth analysis, Mandiant is confident that the controls in place ensure that the MMOG and OTA IP Connectivity interfaces are properly secured from malicious external entities.