



SmartTrust Broker™

Unleashing the potential of SIM cards

SIM cards are rapidly gaining new capabilities that will fuel growth in today's and the future ecosystem for mobile applications. Near Field Communication (NFC) is an example of an area that holds the promise to revolutionize the future of payments, information distribution and ticketing. SmartTrust Broker securely and effectively launches upgrades and personalizes applications on Java SIM cards.

The Challenge

With the advent of new interesting use cases for Java UICCs (Universal Integrated Circuit Cards), such as NFC, the need for Remote Application Management (RAM) increases. New use cases often require the implementation of new business processes in the provisioning and enrollment workflows.

Many SIM-resident Java applications have a need for over-the-air (OTA) personalization. For example, an NFC payment application needs to be personalized with user credentials OTA. New Service Providers taking advantage of the new NFC ecosystem also need to perform SIM OTA operations to manage their own applications.

When downloading and personalizing revenue-critical Java applications as part of a provisioning flow, or as a result of a commitment to a third party, the need for a high-capacity data bearer increases. Using SMS as bearer for RAM will need to be complemented with high-capacity bearers.

When Security Domains are delegated to a third party, it is important to ensure organized control and management of the UICC. For example, it should be made certain that OTA traffic goes through the mobile network and OTA platform in a secure fashion and then only to the correct Security Domain. As well, it should be possible to enforce a list of policies: for example, it should be possible to disable third-party services that subscriber wishes to discontinue or cancel, or that violate a legal regulations.

The Solution

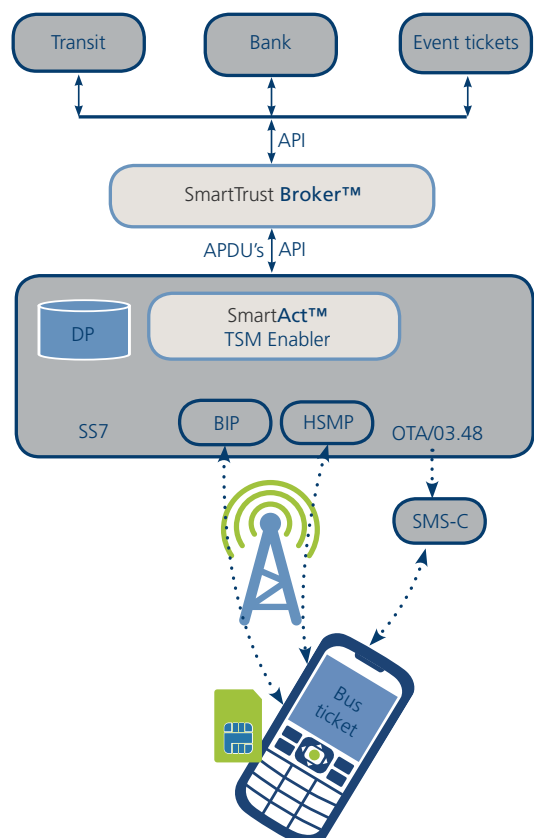
SmartTrust Broker is a product built on the SmartTrust Delivery Platform, enabling secure Remote Application Management of SIM cards using the GlobalPlatform 2.2 standard. It is Telco-grade, meeting the demanding needs of operators upon service availability, operability and maintainability.

The SmartTrust Broker server can be deployed at the mobile operator, for managing SIM-based Java applications in the operator's domain. It is also possible to install remote instances of the SmartTrust Broker server at third party locations such as banks, Mobile Virtual Network Operators (MVNOs) or Trusted Services Managers (TSMs).

Benefits

By using SmartTrust Broker, new revolutionary revenue-generating business cases involving the SIM card can be implemented, such as NFC-based payments and ticketing, selling or leasing areas of the SIM card to MVNOs for running SIM-based applications, and mobile TV. The delegated management authority in SmartTrust Broker allows third parties to securely and independently manage their applications transparently over the mobile network. SmartTrust Broker enables a truly open, yet secure NFC ecosystem.

SmartTrust Broker provides unequalled capacity and flexibility within Remote Application Management, by deploying high-capacity data channels such as GPRS and UMTS using a Bearer Independent Protocol (BIP) like BIP CAT_TP or BIP TCP.



Features

Remote Application Management for Java SIM Cards

Loading and life cycle management of applications to Java SIM/UICC cards.

Remote Java Cardlet personalization

Personalization of existing applets, for example supplying payment applets with user credentials and adding new tickets to a ticketing application.

OTA management of Security Domains

Ability to perform RAM operations on Security Domains according to GlobalPlatform. Ability to create new Security Domains, and allocate Security Domain keys.

Separate instance at 3rd party

The possibility to provide OTA functionality to third parties by deploying a separate instance at a Service Provider. For example a bank or public transportation operator. Service Providers are then able to download and personalize Java applications to their Security Domains on SIM cards.

Double encryption

All OTA traffic from third parties goes through a Mobile Operator's OTA platform. According to GlobalPlatform, ETSI and 3GPP specifications, OTA messaging can be built in two steps: the first one at the remote OTA instance, the second one at the mobile operator's own instance. This ensures the organized and controlled overall management of the SIM card and the secure specific management by the third party of their own applications.

High-capacity bearers

Remote Application Management is performed via SMS and for high traffic scenarios using the BIP protocol in GPRS and UMTS networks. The system is able to detect whether a certain handset / SIM combination supports BIP and selects the bearer accordingly.

The Future

Java SIM cards with Security Domain technology bring a multitude of new possibilities to build new revenue-generating solutions, built upon the Mobile Operator's SIM OTA platform. These solutions involve payment, ticketing, MVNO application management and Mobile TV. When these solutions are implemented, the SIM OTA platform will be a key element in the business processes required.

The economically most important application on the Security Domain platform is NFC. Much has been written about the future of NFC. Given the customer reactions to the numerous trials that have been executed, and the obvious end-user value that can be generated, it seems clear that NFC will happen. Key questions that are currently most discussed are: when it will actually happen, and what applications will be deployed first. Different business models and solution architectures will exist in parallel. The SIM card as a Secure Element seems to have a bright future in NFC, given its property as a portable, inherently secure device, and the platform of different standards that makes the SIM truly interoperable. In this playground, there is a large revenue opportunity for the service providers, too large to be disregarded.

SmartTrust Broker

SmartTrust Broker brings the Remote Application Management functionality, delegation capabilities, security functions, capacity, and throughput, that the mobile operator needs to implement business processes for new use cases around Security Domain technology and NFC.

The key components of SmartTrust Broker are:

SmartTrust DP8

The SmartTrust OTA platform enabling the over-the-air communication.

SmartTrust TSM Enabler

A module that allows integration of delegated OTA instances, either the SmartTrust Broker server or from other vendors.

SmartTrust Broker server

A Remote Application Management server that can either be deployed locally at the mobile operator, or remotely at third parties.

Related SmartTrust Products and Services

SmartAct™

The SmartTrust SIM management platform - a total solution for reliable Over-the-Air management of the SIM life cycle over-the-air. It uses the Remote File Management standard, supports vendor specific OTA protocols from all major SIM suppliers and supports Remote Applet Management according to the ETSI specifications for Java™ Card based SIMs.

SmartTrust endeavors to ensure that the information in this document is correct and fairly stated, but does not accept liability for any error or omission. The development of SmartTrust products and services is continuous and published information may not be up to date. It is important to check the current position with SmartTrust. This document is not part of a contract or license save insofar as may be expressly agreed. SmartTrust is a trademark of SmartTrust AB. All other trademarks are the property of their respective owners. SmartTrust is a part of the Giesecke & Devrient Group.

© SmartTrust January 2010. All rights reserved.

For more information about SmartTrust, please visit us at www.smarttrust.com