ITEA3

Project Results

ViSCa

Giving cloud services a silver security lining

EXECUTIVE SUMMARY

ViSCa (Virtual Machine for SmartCard/USIM) set out to provide a ubiquitous multi-device platform for the deployment of services that require a strong security protocol with full interoperability and access from any user device. The concept prevents possible attacks by third parties, guaranteeing the confidentiality of personal data, bank accounts or private information.

PROJECT ORIGINS

Only large companies can afford traditional end-to-end security solutions that provide the security functionality over e-payment environments. Most of these solutions cannot easily (or affordably) be customised. So the ITEA ViSCa project took to the task of providing an essential extra layer of security in the communication and execution protocols to guarantee secure service access anytime, anywhere and through any device that supports the required security mechanisms. By virtualising the traditional Smart Card, creating a Virtual Smart Card (VSC) running in the cloud, ViSCa makes this type of security solution available to companies of any size, and any single user that owns more than one personal device can access every secure application.

TECHNOLOGY APPLIED

The ViSCa concept focused on the execution of the user authentication protocol on the user device and the cloud architecture that executes the secure application. The ViSCa solution has a secure client-server protocol for a secure data link between the secure authentication module on a user device and VSC in the cloud. Being cloud-based, the Smart Cards as a Service (SCaaS), as proposed by ViSCa, not only gives the user the flexibility to access the Virtual Machine from different host devices, but also allows

multiple user sessions. However, smart card services in the cloud require more enhanced cloud security to boost improved trust and increased use of smart cards in the cloud.

ViSCa enables simple customisation of the service environment. The project's proof-of-concept focused on e-payments and tele-medicine environments. Since ViSCa exposes application programming interfaces on both the mobile device side and service domain side, customisation is simplified. The end-to-end, cloud-based secure mobile payment system allows users to run a secure authentication procedure prior to the secure execution of applications and services. This
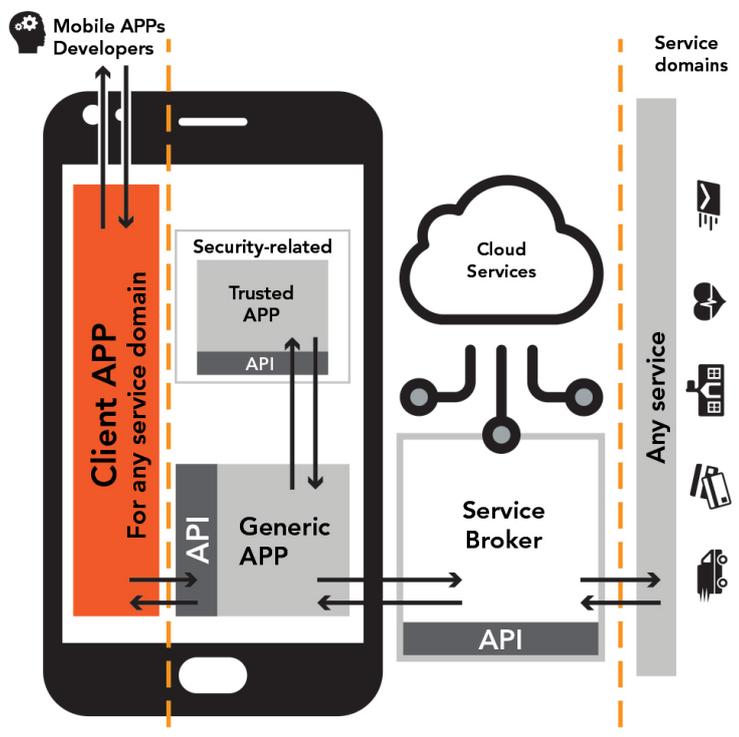
ViSCa conceptual architecture

is geared to secure information exchange between ViSCa users like mobile customers and merchants whereby customer payments are made via ViSCa in the store without the physical Smart Card reader.

In the telemedicine use case, a Holter Monitor uses a mobile phone application

ITEA3

and a physical device to measure blood pressure. The application can use ViSCa to sign the retrieved data using the user's private key on the ViSCa Secure VM to ensure that the data has been read on the right device and store the values (signed or not) on the user's ViSCa Secure Storage Area; storing the data on ViSCa enables the user to have a copy that can be read from other ViSCa applications while keeping the information encrypted (by default the data only can be deciphered by its owner). If the client application is also ViSCa enabled, a feedback can also be included to allow the doctor to write a report about the results and send it back encrypted with the patient's public key using a ViSCa Message.

MAKING THE DIFFERENCE

The ViSCa platform is a perfect fit within the smart cities environment; any user (or device) can authenticate, encrypt information, deliver data to authorised destinations, etc. by using any device since the power of smart card processes stays in the cloud rather than in a single physical element.

There are three key areas for ViSCa applications: e-Commerce services, telemedicine services and public and private services including e-Government and private

company environments where new tools are needed to guarantee security in the acquisition, management and sharing of private and confidential data. A further, important consideration of the ViSCa project was that the results should also benefit the smaller companies and users that will now have access to the same solutions as their larger and financially stronger counterparts.

In terms of exploitation, the ViSCa project results have attracted the attention of banking companies as well as m-Commerce and public services that allow NFC payments, including newly developed participation banks like Vakif Katilim, Ziraat Katilim and Halk Katilim that have the strong support of the Turkish government. Interest is also tangible from other banking institutions such as KFH (Kuwait Finance House) and its subsidiaries in Bahrain, Malaysia, and Dubai, banks in the Middle East and Africa that collaborate with KFH, and KT Bank AG in Frankfurt, Germany, and its branches in Cologne, Berlin and Mannheim. RGB Medical Devices is setting up several pilots for telemedicine services and is in discussion with Philips to provide the ViSCa solution in combination with the latter's e-Health platform.

MAJOR PROJECT OUTCOMES

Dissemination
- 4 publications (e.g. EUREKA/H2020 Ko-summit, Journal of intelligence and information systems, IEEE)
- Several presentations at exhibitions and fairs (e.g. MEDICA'13 Düsseldorf, ESA'14 Stockholm, ASA'14 New Orleans, MEDICA'14 Düsseldorf, ESA'15 Berlin, Congrès de la SFAR 2015 Paris, AAGBI Annual Congress Edinburgh 2015)

Exploitation (so far)
- RGB is in discussion with Philips to provide the ViSCa solution in combination with their e-health platform
- Promising opportunities to exploit ViSCa in banking, m-Commerce and public services that allow NFC payments through newly developed participation banks like Vakif Katilim, Ziraat Katilim and Halk Katilim. Interest is also tangible from other banking institutions such as KFH (Kuwait Finance House) and its subsidiaries in Bahrain, Malaysia, and Dubai, banks in the Middle East and Africa that collaborate with KFH, and KT Bank AG in Frankfurt, Germany, and its branches in Cologne, Berlin and Mannhein