THE NILSON REPORT

FOR 46 YEARS, THE LEADING PUBLICATION COVERING PAYMENT SYSTEMS WORLDWIDE JANUARY 2017 / ISSUE 1102

Software-based TEE for Mobile Cards

Mobile payment wallet providers including handset manufacturers, financial institutions, and mobile network operators use outside technology companies to provision tokenized card credentials to smartphones and wearable devices. Those companies, which include Sequent Software, Bell ID, Oberthur, Gemalto, and G&D, must work with multiple types of hardware and software technologies in mobile devices that protect credentials linked to applications for payment (including transit), government, healthcare, identification, loyalty, and access control.

Hardware that stores data and sensitive logic and executes cryptography can come in the form of secure elements, SIM cards, and trusted platform modules. NXP and ARM are top hardware manufacturers for secure elements in mobile devices. Other manufacturers include Qualcomm, which makes chips that include the secure element for Apple Pay. Software includes "white box" encryption, available from companies including Arxan, Inside Secure, and WhiteCryption. Other companies including V-Key combine encryption with threat analytics to create what they call a virtual secure element.

MagicCube is a start-up that has created what it claims to be an industry first — a full, entirely software-based trusted execution environment (sTEE) platform. Its patented, device agnostic software is offered to mobile wallet and IoT (Internet of Things) providers to be linked to their payment application in the cardholder's device. The MagicCube SDK creates an intelligent software secure element the company refers to as "the Cube" that protects data storage and sensitive logic and conducts cryptographic operations.

Device agnostic software is offered to mobile wallet and IoT providers.

MagicCube clients also receive a secure appliance called a miniCloud, which includes a hardware security module and trust authority. The appliance works with the Cube through a proprietary security connection, which includes multiple technology layers, protocols, encryption, and obfuscations to handle listeners, loggers, man-in-the-middle attacks, network threats, and impersonation.

Unlike other software that stores tokenized card credentials, MagicCube can facilitate offline payments when a mobile phone can't get a network signal, such as when underground for a transit application. MagicCube is compliant with EMVCo token service provider specifications.

The company earns revenue from yearly license fees for the miniCloud. Each license comes with a select number of Cubes. MagicCube has received funding from Visa, Epic Ventures, and BVP.

Sequent Software, which digitizes payment, transit, loyalty, and identification cards for wallet providers, is the first card credential provisioning company to form a partnership with MagicCube. Sequent works with every type of hardware and software on the market that safely contains tokenized card credentials for smartphones and wearables.

Sam Shawki is CEO at MagicCube in Sunnyvale, California, (650) 863-9723, sam@magiccube.co, www.magiccube.co.

Hans Reisgies is CTO at Sequent in Santa Clara, California, (408) 888-9080, hans@sequent.com, www.sequent.com.