

The world's fastest NFC test tool

**cilab**

Test smart. Certify easy.

NFCW ▶ **NFC WORLD**FEATURED
PARTNERSABOUT OUR
PARTNERS**LATEST** NFC Forum adds certification for NFC wireless charging

SimplyTapp proposes secure elements in the cloud

By [Sarah Clark](#) • 19 September 2012

A US-based start-up has developed an alternative approach to storing the sensitive data required to make a transaction with an NFC phone. Rather than placing it in a secure element on the phone, SimplyTapp stores the data in the cloud on a “remote secure element” and passes encrypted transaction data through the phone to a point-of-sale terminal when the user makes a purchase.

A US start-up, co-founded by an NFC engineer who has been working in the field since 2005, has come up with a new approach to managing the sensitive data involved in making a payment with an NFC phone.

Instead of storing private data, such as payment card details, in a secure element (SE) on the phone, SimplyTapp stores data in a “remote secure element” in the cloud. When a consumer makes a purchase, the data is pulled down from the remote secure element and passes through the phone to the POS terminal, where the data is presented in the same format as that used in standard card emulation mode transactions.



SIMPLYTAPP: Stores secret data in a “remote secure element” in the cloud

The concept runs counter to accepted wisdom on how to keep sensitive transaction data secure within a mobile phone. NFC security standards for “card emulation mode” — the term used when an NFC phone presents itself to a POS terminal as if it were a contactless card — are based on the idea that a mobile phone is not a safe environment for sensitive data. All such data, therefore, is stored within a physical secure element on the phone, located within a SIM card, embedded into the handset or added to the device via an external microSD device.



Critical to this type of secure system is that, when a transaction is made, data is exchanged between the secure element and the POS terminal without the data ever passing through the phone’s main memory.

But that’s a 1990s concept of how to handle sensitive data, SimplyTapp’s Doug Yeager has told NFC World. “We absolutely believe that payments now have the ability to evolve beyond a 90s card-based technology. With today’s smartphone technology, secure cloud based payments are absolutely possible.”

SimplyTapp has been working with the team that runs the **CyanogenMod** operating system to make the technology available on “modded” Android phones in the first instance, via a Host Card Emulation (HCE) patch for the operating system.

Host Card Emulation, which was first supported by BlackBerryOS, allows a contactless point-of-sale terminal to interrogate an app that runs within a host operating system on a device instead of interrogating a secure element that is attached to the device, says Yeager. “From a user perspective, the main difference between a HCE and a SE interrogation is the speed,” he explains. “Because HCE uses the Arm processor on the phone, it is way way faster than an SE.”

“Host Card Emulation is created to add functionality to a device and does not address the security aspects of the data being transmitted,” says Yeager. “However, because secure element payments are based on dynamic data being passed with each transaction, it is possible for the transactional data

being generated by the secure element to be rather benign, and suitable for access by an app running on the host operating system.”

CyanogenMod is a version of Android that allows developers to expand the functionality of their phone beyond the limitations put in place by carriers, Yeager adds, and the company picked the operating system for its initial launch since it allows more freedom than a more mainstream OS. “In addition, with an audience of more than five million users, and a track record of features being adopted by a more mainstream OS, Cyanogen provides a great start and a path to mainstream adoption.”

SimplyTapp is [available today for developers to run on modded Android phones](#), allowing them to add the SimplyTapp app as well as a variety of stored value cards to their phones, including the [McDonald's Arch Card](#) and SimplyTapp's own prepaid card.

All Blackberry OS NFC devices currently support HCE, and SimplyTapp is currently working to support these as well.

How secure could such a solution ultimately prove to be? “I think it's absolutely possible for EMV transactions to be done using remotely hosted credentials,” says Yeager. “We're not suggesting vulnerable keys are kept in the operating system itself. We are locating them in the cloud and passing only the transactional data that is generated from them securely through the phone to the POS device.

“Because the cloud has knowledge of the authorisation of a credential and can now have knowledge of transactional data being requested, a more secure end-to-end solution is possible that still leverages the existing POS infrastructure.”

“We want to see NFC payments grow without constraint. Instead of tying credentials to the handset, our solution ties them to the individual in the cloud.”

So, could this approach be used in a mass market, commercial environment? “Absolutely, yes,” says Yeager. “SimplyTapp is a commercial start-up and we're very serious about this.”

Next: [Visit the NFCW Expo to find new suppliers and solutions](#)

Explore: [Android](#), [ARM](#), [McDonald's](#), [SimplyTapp](#)

Learn more: [Android](#), [BlackBerry 7 OS](#), [Card emulation](#), [Cloud](#), [Cloud-based NFC](#), [Contactless](#), [Credentials](#), [Cryptographic keys](#), [CyanogenMod](#), [Doug Yeager](#), [Embedded](#), [EMV](#), [Host Card Emulation \(HCE\)](#), [Infrastructure](#), [Main](#), [McDonald's Arch Card](#), [MicroSD](#), [NFC-SIM](#), [Operating system](#), [POS](#), [Remote secure element](#), [Secure element](#), [Security](#), [SIM](#), [Technology](#), [WNIP](#)

Comments Got something to add or correct? [Let us know!](#)

FEATURED PARTNER



Dejamobile ReadyToTap™ — Cloud-based payments for card issuers built on HCE and tokenization technology. [Find out more.](#)



[Visa releases Olympics NFC and contactless usage statistics](#)

[HTC unveils WP8 NFC phone](#)



3 comments on this article

Hans Schaeffer

20 SEPTEMBER 2012 AT 08:10 BST

Excellent idea! So much more secure than having the SE on the phone itself or on the SIM. The notion that a phone service provider should become a stakeholder in mobile payments is absolutely inappropriate for several reasons and must be avoided at all costs.

Paul

21 SEPTEMBER 2012 AT 07:34 BST

I can't see how the transactions peed required could be achieved. Also, imagine using it for a transit card, in an underground station.

Sam

21 SEPTEMBER 2012 AT 23:36 BST

This has already been done by a Canadian startup, AlfredNFC, with a patent pending idea. Check out <http://alfrednfc.com>.

Comments are closed.

Titles

[NFCW](#)
[Contactless World Congress](#)
[NFC World](#)
[What's New in Payments](#)
[Transit Ticketing Today](#)

Resources

[NFCW Knowledge Centre](#)
[Contactless World Congress](#)
[NFCW Expo](#)
[Email newsletters](#)

Company

[Advertise with us](#)
[Privacy policy](#)
[Legal](#)

[Back to top](#)

Copyright © 2008-2023 [SJB Research Ltd.](#) All rights reserved. ISSN 2976-5315. Made with ❤ in [Wales](#).

