

Host card emulation - why it matters

What is HCE?

Android's recently release of Android 4.4 or KitKat has been greeted as highly significant because it enables NFC-based transactions through HCE. But what is HCE?

Host Card Emulation allows any app on any NFC_enabled Android 4.4 device - phone, tablet or any other device running Android 4.4 - to emulate a contactless smart card, letting users tap to initiate transactions with an app of their choice without needing a provisioned secure element (SE) in the device. Apps can also use a new Reader Mode to act as readers for HCE cards and other NFC-based transactions.

The device effectively becomes a contactless card that you can use to make purchases, display tickets and vouchers and present ID.

Why is this important to you?

Traditionally, you would have to store security information, for example the security keys from a debit card (which are stored in the tamper resistant card chip) in a similarly tamper resistant chip on your device – the Secure Element. The Secure Element emulates the card and can be found either on the UICC (SIM card) or in a chip embedded in the phone handset. In general the SIM is controlled by the mobile operator and the embedded chip by the handset manufacturer. If you are a bank or payments institution issuer, this causes commercial issues that have been instrumental in delaying widespread use of NFC.

Choosing to accept the security risk and avoid use of the SE was not previously possible because contactless reader data is automatically sent to the SE and not to a handset application.

In the past, the only way to get round this was to access lower level protocols by, for example, patching Android. While adequate for prototypes and demonstrations, this was not considered suitable for mass-market deployed solutions. Blackberry did however expose this capability in its BB7 and BB10 handsets.

HCE means that the contactless data is sent to the device and not to the SE. To allow it to be sufficiently protected in the phone environment what must be done is to load 'limited' versions of the security information into the mobile phone - information that can only be used for a day, or for a single transaction, or in a specific merchant. That information is called a 'token' and it can be updated or deleted as the issuer requires.

We refer to this sort of solution as No Secure Element or NOSE. Android's announcement about HCE makes NOSE mainstream. That means that the commercial discussions about the ownership of the SE and hence the ownership of the channel, whether through the SIM or the handset, can go away.

What do you have to consider?

This change away from either MNO or handset manufacturer ownership of the channel means a brand new ecosystem for NFC. That will have considerable implications for your service.

For example, what sort of security solution will you choose? Should you use a Trusted Execution Environment (TEE) for secure authentication (perhaps inside a FIDO framework) by HCE apps in the handset? Then, much like



Apple's use of the fingerprint sensor for purchasing on iTunes, the TEE would provide added security and convenience, but apps could still work without it.

What are the Schemes likely to do about HCE? We believe it fits in well with their drive towards tokenisation.

What are the commercial outcomes for your proposed service and for that of your competitors?

How we can help

For answers to these and other questions arising from this highly significant announcement, it makes sense to work with an organisation with an extensive background in No Secure Element NFC and Host Card Emulation. Consult Hyperion has been active in this area since 2007. That was the year when we first produced a HCE based EMV transaction for one of our clients and we've done more testing, prototyping and demonstrations of secure transactions using HCE since, both using Android patches and on Blackberries. This experience leaves us uniquely well suited to advise you on how to maximise the benefits to your service from this announcement.

Who are we?

Founded in 1985, Consult Hyperion offers consultants and associates expert in the design and implementation of contact and contactless based payment, NFC, mobile payments and POS, ticketing products and services, identity and internet services.

We are supported by Hyperlab - software and design engineers practised in the development and implementation of pilot and commercial grade products and services with expertise in standard programming and software development and management tools as well as technologies including: Microsoft .NET, Windows Phone, Android and iOS development (cross platform development with Xamarin tools), BlackBerry, embedded C, Java, JavaCard, MULTOS, HTML5 and Python, and by an extensive test laboratory used to optimise or certify the operation of these systems.

Why work with Consult Hyperion?

We are independent - we have no off-the-shelf products. Nor do we sell or promote third-party solutions, partner or form strategic relationships with third-party vendors. We are expert, understanding in great detail secure payments, identity management and fixed and mobile communication technology. We have detailed knowledge of the associated technical standards, regulations and business models and how they can be used to secure future revenue streams. We are globally recognised as thought leaders and experts within the areas of mobile, identity, contactless and NFC payment, EMV and ticketing. Our clients consistently praise us for being flexible, responsive, trusted, technically expert and innovative.

Our involvement in your project team will ensure that you deliver a marketing leading solution, underpinned by global best practice, readying you for the expected evolution of future technology.

More information

For more information about how Consult Hyperion can help your organisation transform its payments capabilities, strategies and operations and make informed and positive business decisions, please contact:

Nick Norman

Head of Sales
nick.norman@chyp.com
sales@chyp.com

Consult Hyperion

Tweed House
12 The Mount
Guildford
Surrey GU2 4HN
UK
Tel: +44 (0) 1483 301 793
Fax: +44 (0) 1483 561 657

Copyright © Consult Hyperion
All rights reserved
Please distribute.

