Loader Service:
The Tipping Point for Secure NFC Payments

by Charles Dachs, NXP Semiconductors

A new Loader Service, used to configure the security functions that protect NFC transactions, could be what NFC needs to truly take off in payments.

MasterCard's recently announced initiative to turn any consumer gadget into a payment device promises to expand the use of mobile payments. It introduces a better way to add secure payment capabilities, based on Near Field Communication (NFC), to just about any object, whether it's things you carry with you, like car keys, or things you wear, like wristbands, jewelry, and other fashion accessories.

More specifically, the initiative makes it much easier to add the security functions needed to protect an NFC payment. NFC payments use a microcontroller-based circuit, called a secure element, to safeguard payment information and conduct the NFC transaction in a secure way. The secure payment functions are then added to the companion app that's used by, for example, a wristband, so the wristband can start making payments.

By making it easier to configure the secure element, the MasterCard initiative could be what NFC payments need to reach what the Canadian journalist and best-selling author, Malcolm Gladwell, calls the "tipping point" – that moment when a technology "crosses the threshold and spreads like wildfire."

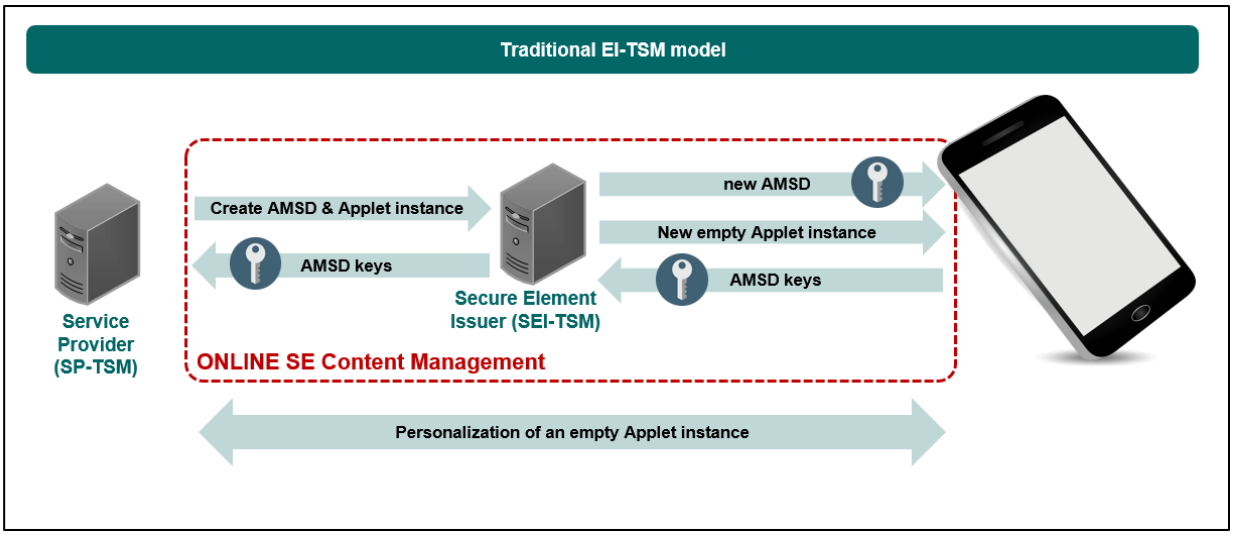
The challenge for NFC payments

NFC is a remarkably intuitive technology to use and many thought NFC would indeed spread like wildfire as it became available for payment transactions. The reality, though, is that adoption rates, while steadily increasing, haven't gone up as quickly as some predicted Why? Because even though NFC itself is easy to use, the process for deploying a secure NFC payment application hasn't been so easy. In fact, the process has been complex enough that some developers have avoided taking it on entirely.

Complexity is a barrier to entry

The complexity of deploying a secure NFC application comes, in large part, from the way the secure element is "onboarded," or equipped with the service credentials needed for processing a payment.

Onboarding involves the use of a Trusted Service Manager (TSM), which is a service with a back-end infrastructure. Two TSMs, a Secure Element Issuer (SEI) TSM and a Service Provider (SP) TSM are used to deploy an application that uses NFC with a secure element. The SEI TSM lets the issuer of the secure element manage cryptographic keys and maintain the lifecycle of the secure element. This includes creating, deleting, or blocking any security domains or secure applications (applets) residing in those domains. The SP TSM is then used by a service provider to load the service credentials onto the secure element.



The traditional SEI-TSM model adds complexity to onboarding

Integration of the SEI TSM and SP TSM can be challenging. The methods and techniques can vary from vendor to vendor, and make it harder to manage content across multiple secure elements. That adds time and complexity to the development cycle, increases operating costs, and raises overall risk.

In general, the TSM model has created boundaries between service providers and the manufacturers of secure elements, and has, overall, made it harder to bring a secure NFC payment application to market.

The technical complexity of the TSM model has made it especially hard for smaller companies to deploy NFC. Startups and other small companies are often the key drivers of innovation – especially in emerging areas, such as the Internet of Things (IoT) – but smaller businesses may not have the technical staff or resources needed to support a more challenging process like the TSM model, and that can discourage them from choosing NFC as a platform.

A better approach to security

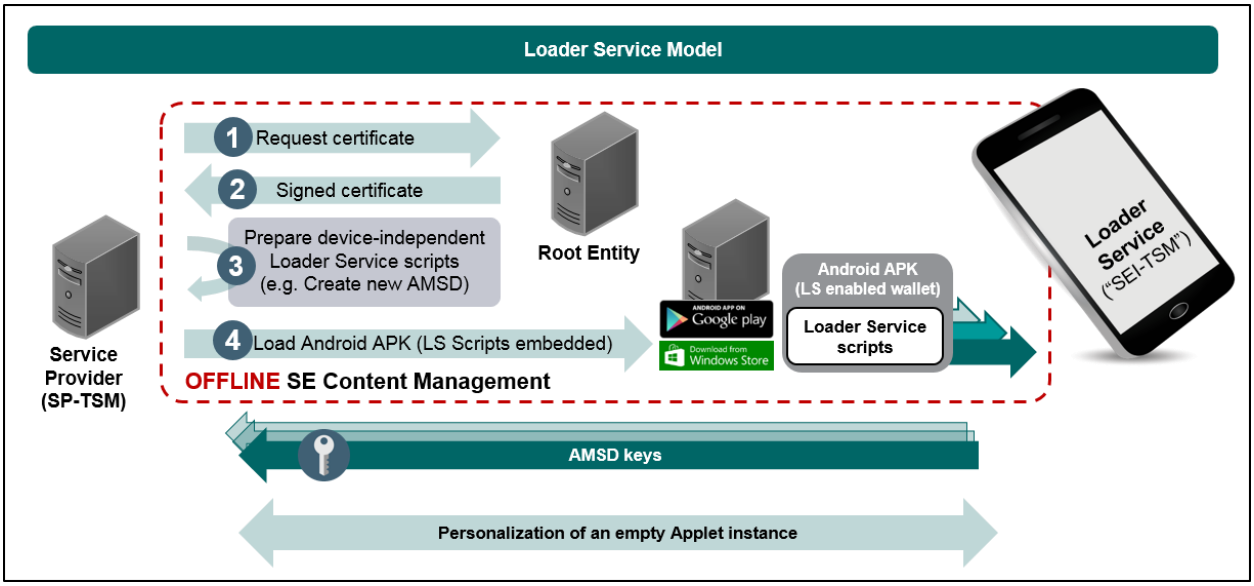
What's needed is an easier way to deploy secure applications, so service providers can create a single, simple user experience across different secure services. The MasterCard initiative meets this need. It replaces the TSM model with what's called a Loader Service, an approach that makes it much easier – and more cost-effective – to deploy a secure NFC payment application.

The Loader Service, which was developed by NXP Semiconductors, the co-inventor of NFC, is available with NXP's PN6x line of NFC modules. Each module contains an NXP secure element, the only Common

Criteria certified EAL6+ product for mobile applications. The Loader Service is preconfigured on the secure element itself, as an applet and client, so developers have immediate access to the Loader Service.

How the Loader Service works

The Loader Service's Root Entity delegates content-management rights, using certificates. Applets can be loaded on a large scale, without using an SEI TSM. The necessary scripts are already embedded into an Android application package (APK), and can trigger card content-management services. For example, the scripts can create security domains and inject keys, load and update applets, instantiate and customize the applet, and delete security domains. All the scripts and content-management operations can be used on multiple devices, and can be scaled across entire product lines.



The NXP Loader Service model simplifies onboarding

The Loader Service coexists with the TSM-based model, yet represents a plug-in replacement for conventional SEI TSM formats. Since the Loader Service uses just one real-time connection, it reduces system testing and minimizes the risk of failure. The Loader Service also offers the highest level of data protection and encryption, and produces a fully EMV-certified system that can be used anywhere in the world. Any applications developed with the Loader Service are fully compatible, backward and forward, with the payment infrastructure.

Any device can be a payment device

With the Loader Service, NFC and the secure element become easy-to-use design resources, and make secure NFC payments as straightforward to deploy as any other mobile app using a standard technology, such as GPS, Bluetooth, or Wi-Fi. Issuing a commercial agreement is as easy as using a "secure application store" concept, and end users can install and manage secure payment applications the same way they do other mobile apps. Any service provider, small or large, local or global, can now deploy a secure NFC payment application.

Also, because the infrastructure and maintenance tasks are already taken care of by the Loader Service, developers have more time to focus on creating an exceptional user experience that will distinguish their products.

A better ecosystem = faster adoption

NXP's secure elements are already trusted for their ability to deliver the highest level of data protection and encryption to payment issuers, manufacturers, and end users. The Loader Service makes it easier for developers to take advantage of these features.

NXP has recently initiated standardization of Loader Service under the name "Secure Element Management Service" with GlobalPlatform, an international industry standard for trusted end-to-end secure deployment and management solutions. Its standardized infrastructure empowers service providers to develop digital services once and deploy them across different devices and channels. The GlobalPlatform standardization will therefore greatly increase the scalability and interoperability of the Loader Service.

By making the NXP Loader Service a part of the payment ecosystem, MasterCard is offering developers a simpler, better way to ensure security. The MasterCard model uses the Loader Service to lower setup and maintenance costs, enables scalability and flexibility, and removes the need for complex TSM infrastructures. The initiative shows that MasterCard recognizes the importance of making a technology that's not only easy to use, but also easy to deploy. And that could be what pushes secure NFC payments past the tipping point, helping the concept spread like wildfire.

For more about NFC and what it means for payments visit NXP's dedicated site for NFC at www.nxp.com/nfc.

www.nxp.com

Date of release: Feb 2016