TSM: Friend or Foe To The NFC Market Place?

Are trusted service managers a barrier to the wide-scale adoption of near field communication services?
EXECUTIVE SUMMARY

As near field communications (NFC) services continue to transform the way that end-users go about their daily lives at a national level – from contactless payment, to transit and loyalty – the NFC ecosystem stakeholders are looking to capitalise on this lucrative technology by expanding services across borders and eventually going global.

However, they face a major hurdle; the challenge of global interoperability. With a lack of cooperation and standardisation, it is impossible to deliver seamless services worldwide. This is further exacerbated by the fact that a number of projects need to be seen to be making a return on investment, and focusing on regional markets can often be easier.

There are a number of very successful high profile use cases on a regional scale which are regarded as the benchmark for NFC rollouts. This includes ISIS in the USA, Cityzi in France, as well as the initiative in Singapore where the government and the country’s three mobile operators SingTel, M1 and Starhub have built a shared infrastructure.

In the middle of this interoperability challenge are the trusted service managers (TSMs). The TSMs are the broker between other actors in the ecosystem, and they securely manage the business relationships and connections between mobile network operators (MNOs) and other organisations that have a claim on the secure element (SE) of mobile phones.

There are a number of organisations that are developing guidelines and standards to promote interoperability; most notably GlobalPlatform, a standards body for managing applications on secure chip technology. But, adoption is slow, and there are a number of reasons why this is the case which will be discussed in the following chapters.

The key focus of this whitepaper will be to explore whether the TSM is a friend or foe to the globalisation of NFC services. It will also explore how TSMs can be tested prior to implementations to mitigate the risks and ensure, as far as they can, a return on investment.

Additionally, the environment is evolving quickly and alternative solutions, such as host card emulation (HCE) and other cloud-based offerings are coming to market. They are, however, less secure and leave the MNOs, service providers, end-users and other stakeholders vulnerable to security risks that could jeopardise the reputation of those involved and the viability of services moving forward.

It is without doubt that NFC services are gaining traction and trust with the end-users; so the key is to find a way to interoperate to ensure secure robust processes that will see NFC services reach their full potential to the benefit of the whole NFC ecosystem.
CONTENTS

Chapter 1
THE CHALLENGES OF INTERCONNECTIVITY

Chapter 2
THE NEED FOR INTEROPERABILITY

Chapter 3
GOING GLOBAL – IS IT EVEN POSSIBLE?

Chapter 4
CREATING CONFIDENCE

Chapter 5
TSM: A VITAL ROLE

ABOUT FIME

MEET THE AUTHOR
THE CHALLENGES OF INTERCONNECTIVITY

There are more than 70 countries across the globe that are at different stages of testing, trialling and deploying NFC-based services.

In parallel, there has been a significant increase in the sale of NFC-enabled handsets provided by mobile network operators (MNOs).

In fact, IHS Technology recently reported 275 million global shipments of NFC-enabled mobile phones in 2013, with a further 416 million units – indicating growth of 50% - forecast to be shipped in 2014, while Berg Insight has estimated that 53% of the world’s POS terminals will be NFC ready by 2017.

It is therefore no surprise that the device makers are showing widespread support for this technology. Berg Insight also reports that the top ten handset vendors released almost 100 NFC-enabled models in the same year, and that it predicts one billion NFC handsets will be shipped by 2017.

In support of this technology, the analyst firm also highlights the number of NFC-ready point of sale (POS) terminals is set to rise dramatically from 6.7 million in 2012 to 44.6 million in 2017. This is important as contactless payment is an enabler for other NFC services such as ticketing, vouchers and sharing data.

GLOBAL NFC TRACTION

To illustrate the traction of NFC, there are a number of well-regarded use case examples that have been implemented in countries across the world:

ISIS in the USA is a joint venture between AT&T Mobility, T-Mobile USA and Verizon Wireless. It has developed a mobile commerce platform which facilitates the collaboration of some of the USA’s leading banks, payment networks, merchants and wireless service providers. ISIS’ primary objective is to create a widely accepted, consumer-friendly mobile wallet.

This mobile wallet application can store payment cards as well as coupons and loyalty cards on the end-user’s smartphone and transmit this information to the payment terminal at NFC-enabled merchants. The technology has been widely adopted and continues to gain momentum.

Launched in 2010, Cityzi in France is probably regarded as the gold standard for NFC rollouts. The initiative brings together the leading telecom operators, banks, transport operators, traders and industry players. According to trade association, Association Française pour le ‘Sans Contact’ Mobile (AFSCM) which facilitates the technical development of NFC and promotes contactless mobile services, there are now 2.5 million NFC-enabled phones that work with the French MNOs’ Cityzi NFC platform; up from one million in 2012. In addition, 55,000 French merchants are equipped with Cityzi-compatible contactless payments terminals and, NFC transit ticketing

---


services have also started to be rolled out. For instance, Orange and Visa Europe recently announced a commercial launch of Orange Cash in Caen and Strasbourg, two cities with the highest use of contactless payments in the country. This makes Orange the first MNO in France to offer mobile contactless payments to its customers.

Singapore’s three mobile operators – SingTel, M1 and Starhub – have built a shared NFC infrastructure which also has government backing. The sheer scale of this rollout is what makes it stand out on the worldwide stage, as it has gained significant traction with businesses and consumers. Payments can be made at tens of thousands of POS terminals that accept EZ-Link payments including supermarkets, taxis and fast food outlets.

THE ROLE OF THE TRUSTED SERVICE MANAGER

Within each of these models is a trusted service manager (TSM). It works ‘behind-the-scenes’ to securely manage the business relationships and connections between MNOs and other organisations that lay claim to the secure element (SE) on mobile phones. The SE is essential for NFC services to guarantee the protection of security-critical applications and to achieve the same security standards as those we expect when using debit or credit cards.

When implementing NFC deployments, the TSM faces a number of challenges, but the main issue is that of interconnectivity. It is in the interests of MNOs to connect with as many service providers as possible in order to deliver NFC services to end-users and generate additional revenue. At the same time, it is in the interest of the service provider to get its services into the mobile phones of consumers.

The technical and business variations of each player, and how it wants to implement and deliver its services, creates a complex ecosystem in which to operate. This inevitably leads to increased time and delays in bringing services to market and increases the investment required. This is also leading to delays in deployments.
Despite the success of many NFC implementations, large-scale commercial launches of NFC-based services are still rare and restricted to regional or national geographic areas. There are, however, some that are looking to change this. In early 2014, Asian telecom operators Chunghwa Telecom (Taiwan), HKT (Hong Kong), KDDI (Japan), and SK Planet (South Korea) announced the formation of the Asia NFC Alliance. This group aims to extend existing NFC services beyond national borders to accelerate the adoption of compatible NFC services worldwide.

It is this cross-border opportunity, also called NFC-roaming, that is getting the industry excited as it presents as many opportunities in the future as it currently does challenges for MNOs and service providers.

That being said, scalability is the biggest hurdle to meet demand. While scalability within regions is starting to gather pace, the issue with going across-borders is interoperability, as there are no open standards, as yet, and there are different applications in different regions. There are industry bodies and associations that are working on this; for example, GlobalPlatform, which has developed specifications that support TSMs and the mobile payments ecosystem. It has developed a common language, and defined roles and responsibilities of each actor to promote market clarity. These documents are fully endorsed by the GSMA, an association which supports the interests of mobile operators worldwide. This will be discussed in the following chapter.

Transit, loyalty and mobile wallets are just a few examples of the services that will benefit from going global.
IS HCE NOT THE ANSWER?

HCE (host card emulation) has been seen by some as the answer to cross-border activity as it doesn’t need an SE and therefore removes much of the complexity associated with delivering NFC services. HCE enables a secured application to be used in the cloud, bypassing the need for an SE and TSM to enable NFC applications such as contactless payment.

Residing in the mobile operating system (OS), it allows an application to talk directly to a merchant terminal to validate a transaction without having to go through an SE and TSM. HCE also removes the need to conform to card provisioning restrictions that are put in place by the MNOs.

Although simpler, as it goes through a mobile application loaded in the open OS of the handset and simply loaded on whatever application store, it leaves service providers, MNOs and consumers more vulnerable to security risks because of the inherent nature of the technology. More information can be found in the FIME whitepaper titled ‘The NFC Security Quiz’.

It is predicted that there will be variations in how HCE will be implemented and its role in the ecosystem depending on regional infrastructures. For example, countries that have adopted EMV are more likely to capitalise on the secure chip framework already established. As NFC SE-based deployments have been trialled and are ready for mass rollout, it is expected that these implementations will move forward without delay.

Long-Term Vision

Payment tokenisation, combined with HCE, or other technologies such as QR code or Bluetooth, will coexist with payment cards and SE NFC payment in the future and have a wider impact on the market. This, however, will not happen in the near-term as the technology is new and the market will have to overcome challenges starting with standardization to ensure interoperability and implement pilots before large scale, global deployments can begin.

While the trusted execution environment (TEE) - a secure area that resides in the main processor of a smart phone (or any mobile device) and ensures that sensitive data is stored, processed and protected in a trusted environment - is not yet widely utilised, this technology could become increasingly important as a way to enhance security for HCE. Some payment schemes are already developing proof of concept.

Tokenisation or TEE, both technologies require provisioning (for token and trusted applications). Isn’t this the role of the TSM?
Delivering NFC services is complex despite the strides made to standardise implementation. Current standards support many different business models and actors, and with so many options available, and with numerous ways to interpret them in terms of language and messaging used, it is hard to know what exact technical requirements apply to each deployment region by region.

The vision for the future of NFC is without doubt for the global citizen to be able to access services internationally. The solution to the TSMs’ challenge to reach this goal is interoperability; to create a sustainable and global framework that all TSMs can use as the basis to manage the lifecycle of applications.

If these standards are not realised, the TSM could become a barrier to NFC reaching its potential rather than the enabler. Now is the time for TSMs to demonstrate that they are a friend and not foe to this dynamic ecosystem.

**WHO ARE THE PLAYERS?**

The TSMs that are involved in this challenge fall broadly into three categories — they are the MNOs, the smartcard card vendors and newcomers that are looking to take advantage of the NFC explosion. These newcomers tend to be linked in some way to the vertical markets that will benefit from NFC services, such as telecoms or payments for example.

These TSMs can be further categorised as follows:

- **SE Issuer (SEI) or Root-TSMs** are responsible for managing access and allocation of space and privileges on SEs, such as for MNOs and handset makers of embedded SEs. The SEI-TSM will also interact with SP-TSMs.

- **SP-TSMs** provision, manage and personalise application content onto the SE. SP-TSMs interact with the SEI-TSMs to communicate changes to applications and manage their own secure environment.

- **TSMs** can be in-house, which is often favoured by those service providers or MNOs that want to stay in control of their transactions and interactions; or outsourced to a specialist TSM, as it isn’t the service provider’s core business and allows it to benefit from both the TSMs’ expertise and scalability.

Most TSM providers can also deliver the services of a SP-TSM or a SEI-TSM. In addition to this, TSM providers coming from the smartcard industry have existing relationships with MNOs and service providers — notably banks — which means that they can easily integrate applications and deliver NFC services. As a result, smartcard manufacturers currently dominate the market.

In most regions, there are multiple TSMs active; all of which are involved in multiple relationships with other TSMs, creating very complex ecosystems.
Figure 2: Who are the players.
Diagram showcases the complexity of the TSM landscape and different actors involved.
STANDARDISATION WILL FACILITATE GLOBALISATION

TSMs are working together to develop a set of international standards, but are being very slow to adopt them and put them into practice.

This is inevitably making globalisation of NFC services prohibitive as to connect with each new application, a TSM must ensure its system is compatible, the service being delivered is secure, and a business model is agreed. This takes time. If a TSM needs to connect with another TSM internationally, it faces the same challenges: how do I connect; how do I communicate and is the infrastructure secure?

As previously discussed, there are a number of organisations that are creating standards that TSMs can adopt in an effort to accelerate the deployment of these services, most notably:

- **Technical body EMVCo** was founded to develop specifications for secure payment transactions. Collectively owned by American Express, Discover, JCB, MasterCard, UnionPay and Visa, this collaborative work has paid dividends as it has created a number of specifications around payments technologies including EMV Contactless, EMV Common Payment Application (CPA) and EMV Card Personalisation. More recently, the body has also focused on mobile payments and defined the proximity payment secure environment (PPSE) which allows a contactless NFC payment terminal to effectively identify which payment application is to be used for each transaction quickly and securely. EMVCo recently published an EMV Payment Tokenisation Specification that can be leveraged for cloud payments. As payment is an important enabler of NFC services, the advancement of EMVCo continues to play a central role in the ecosystem.

- **The GSMA** has established a mobile commerce programme which is designed to stimulate global commercial deployments of UICC-based NFC services. The GSMA is an organisation that works with the best interests of the MNOs at its core, and as such is working with them to help create a global, inter-industry ecosystem which will facilitate NFC rollouts and projects across borders.

  The GSMA has published guidelines for handset, SIM and TSM requirements, titled ‘NFC Mobile Network Operator - Service Provider Interface Business Process Implementation’ to try to facilitate interoperability between NFC devices. The GSMA believes that ‘standardised requirements will drive economies of scale in SIM, handsets and infrastructure by creating a common framework for implementation and product interoperability’. It fully endorses the work of GlobalPlatform.

- **GlobalPlatform** is a not for profit organisation that works across all industries in order to create specifications which enable secure and interoperable deployments and the management of multiple applications on secure chip technology.

  Its tried and tested specifications focus on the SE, TEE and system messaging. These specifications are regarded as the international gold standard for building a trusted end-to-end solution which serves multiple actors and supports several business models. GlobalPlatform is industry agnostic and is building a set of specifications that are looking to resolve the global interoperability issues of TSMs.
Despite standardisation advances in the globalisation challenge, many TSMs are unable to continually align with the new guidelines that are being produced. This is due to business constraints or technical advancements, for example, waiting for system updates to be required to incorporate the latest industry direction. Projects are also still focusing more on the immediate market, with many innovative deployments facing unexpected challenges, which in turn has meant deadlines have not been met, and as a result many are yet to become compliant.

This being said, there are strong plans in place to reach global compliance. The question for most TSMs is how?

GlobalPlatform key achievements in the TSM landscape

GlobalPlatform’s cross sector approach to standardisation has resulted in:

- The development and ongoing advancement of the Card Specification v2.2, which supports the implementation and management of tamper-resistant chips such as smartcards and SEs, is well adopted in UICC.
- The standardisation of the TEE and supporting functionality.
- The definition of messages that clarify how market participants from the finance, mobile NFC, government and transit sectors can interconnect their backend systems within a secure application’s ecosystem. This is achieved by defining ‘who’ is responsible for ‘what’ and agreeing the ‘language’ (messages) that will be used. This messaging is extremely important to the TSMs as it will play a key role in how services can be utilised globally as it promotes interoperability.
- The release of an end-to-end framework which showcases how the whole solution can work together in a format that addresses the specific technical requirements of different market sectors.

This important development will be discussed in more detail in the next chapter.

Tried and tested in real-world environments

Regardless of the challenges faced, there are strong plans in place to reach global compliance. The question for most TSMs is how?
The payment infrastructure is globally interoperable. It is therefore inevitable that NFC services will aim to be delivered across borders. In a push for interoperability, GlobalPlatform has developed two powerful market leading documents that represent major strides in standardising the role of the TSM.

1. GlobalPlatform System Messaging Specification for Management of Mobile NFC Services outlines how NFC applications should be provisioned and managed. GlobalPlatform is collaborating with key industry bodies including EMVCo, the European Payments Council (EPC), GSMA and France's AFSCM in order to standardise how service providers connect and communicate with other actors in the complex NFC ecosystem.

This specification provides clarity around common language and messaging in that the same answer and behaviour is expected regardless of region or actor. It defines what messages should be sent, and what answers should be received, when and by which actors. This defined messaging should be used by all to ensure cross-border consistency when managing secure applications over mobile networks. For this to succeed, all players must agree, hence the collaboration with other key industry bodies.

As a working document, the latest version addresses how service providers can connect and communicate with other actors operating in the NFC ecosystem such as payment systems or transit operators, and includes how to engage with trusted third parties such as MNOs and TSMs.

The content of this document has become the industry standard as other bodies adopt its messaging. For example, the GSMA launched its ‘Business Process Implementation Guidelines’ which uses the protocols set out by GlobalPlatform to create a framework that MNOs can adopt in order to reach full global interoperability.
2. **GlobalPlatform End-to-End Simplified Service Deployment Framework** is the final part of the GlobalPlatform puzzle to have been developed to reduce ambiguity and support new players, such as service provider, entering the SE chip landscape. The document is a guide to the whole infrastructure as defined by the standards body. It is very prescriptive and explains in detail the different implementation configurations, for example for UICC or embedded SE deployments. In response to industry needs, the first framework focuses on mobile payments.

As service providers are starting with a basic configuration template, it allows services to be deployed faster and across borders. Specifically, it details:

a. How to achieve a seamless user experience by defining the workflows between actors.

b. The architecture to provide clarity in data flow and implementation.

c. The configurations to use to ensure interoperability across all interfaces and devices.

![GlobalPlatform end-to-end simplified framework.](image-url)
Another key aspect of the framework offering is ‘processes’. Messaging has a specific sequence as it defines what should be asked, when and what the answer should be, and which actor in the ecosystem should be asking and sending them.

This clarity of language or messaging, roles and responsibilities, as well as the development of an end-to-end framework, will facilitate alignment and standardisation within the NFC ecosystem which includes MNOs, TSMs and service providers. This will ultimately result in the delivery of collaborative services making globalisation and interconnectivity a reality.

This framework is the first real direction that the industry has had which will prove to be very important for the TSMs. It will help to lower implementation costs; a major headache for those involved as return on investment from existing projects is key. It should also accelerate the launch of trusted and compliant mobile services.

MORE THAN JUST COMMUNICATION

While the TSM must know who to speak to and when, it must also guarantee the security of the SE. A key challenge today is managing the certification of both the SEs and the applications that are issued by various industry bodies. Each has a different issuance and expiry date and needs to align with the current security requirements of the issuers and service providers. As a trusted party which has full access, TSMs need to manage this risk.

There is still an element of standardisation to be done here, and GlobalPlatform is developing the missing pieces to overcome the cross-border challenge; and the TSMs will play an important role in ensuring overall security.
Chapter 4

CREATING CONFIDENCE

While certification of some secure applications such as payment is important, TSMs need to ‘validate’ their offering to ensure it is flexible to long-term demands and end-user requirements. Using this approach will improve connectivity between all actors in the NFC ecosystem. For these reasons, testing the technology to see if it works in real-world environments is a key part of accelerating NFC deployments across borders.

TSM COMPLIANCE

GlobalPlatform is developing a compliance program to fill the gap. Initially, it will be limited to the most commonly deployed configurations, namely Simple Mode, Delegated Mode and Dual Mode and will focus on two major players, SP-TSM and SEI-TSM. The testing will leverage the end-to-end simplified framework document’s use cases. Once up and running, TSM providers could get the qualification status for their TSM products. It will deliver the following benefits to the market:

- **Help MNOs and service providers** to select their providers making sure the TSM proposed supports the configuration they will use;

- **Strengthen the interoperability** by having a common and agreed testing method among the different stakeholders;

- And, because key functionalities have already been tested, **speed up the rollout**.

Connections between SP-TSM and SEI-TSM will be much easier, particularly when two TSM competitors are involved. As the compliance programme will have already vigorously tested the functionalities supported by the TSM, with nominal behaviour and abnormal behaviour, the connection integration between the two TSMs would be limited to performance of the TSM itself which is out of the scope of the qualification. Without this qualification status, however, each individual TSM function would have to be tested and it could be very difficult to achieve the same in-depth testing because abnormal behaviour cannot always be predicted and tested accordingly.

GlobalPlatform is also working with a number of different organisations, and specifically with the GSMA, in an effort to streamline this testing process.

While the process is clearly defined in GlobalPlatform’s End-to-End Simplified Service Deployment Framework, how can it be proven to work with so many variables at play? There are two approaches that are complementary and will contribute towards interoperability. First is TSM compliance to GlobalPlatform Messaging Specification, and second is the interoperability testing, also known as end-to-end testing.
When analysing the challenges that stakeholders face during project deployment—despite the fact that each piece of the NFC ecosystem has been tested—there are still issues when bringing it all together.

To overcome this, there needs to be a way to test all the elements together to achieve interoperability. This could be done via an ‘end-to-end’ platform on which all elements can be tested. The platform would include, for example, a set of reference handsets, reference SEs and reference readers, each with different use cases such as payment or transit.

With a combination of all these elements the risks can be mitigated. For example, the handset will be tested with the UICC from different vendors, it will ensure that the payment application is loaded properly with external events that can occur simultaneously, such as receiving an SMS for instance. Once the test has evaluated that the payment application has been loaded and personalised, it will confirm that a transaction is undertaken correctly with a terminal. The test would then perform the same functions with a transit application.

This interoperability test platform would allow in-depth analysis in case of failure which may be difficult to test in a live environment. It will benefit different stakeholders as it is the first time that different components are brought together; and the first time real interoperability can be tested with different handsets, different SEs, and different terminals.

To avoid the number of handset/SE combinations becoming prohibitive in a testing environment, it is possible to select the reference platform with specific criteria. For example, samples from different manufacturers, with different OSs and contactless chips (CLFs); thereby selecting a representative panel of common/widely deployed devices which will optimise the platform and testing process.

Using this testing framework will enable MNOs to operate separately from the service providers to release new devices or UICCs while still being committed to a high quality service. As it is a controlled environment, it provides a means to test and analyse any failures before they come to market. Importantly, expanding the end-to-end platform to test TSM interoperability allows providers to demonstrate that they support any SE vendor.

More widely, it should be noted that combining TSM compliance with interoperability testing will mitigate risk when implementing on a large scale. This is because compliance tests only focus on one component within the chain, which means errors can occur when the whole system comes together. As more and more actors from different markets converge technologies to deliver solutions, this level of interoperability testing combined with component compliance testing, will be vital to ensure the efficient and success operation of mobile services once live in the marketplace.

In the future, GlobalPlatform will extend its compliance programme to other configurations that are relevant to the market and other actors such as service providers and Controlling Authorities (CAs).
Today, the TSM is the trusted middle-man that enables NFC services to be delivered at a local and national level; this role is even more important in the quest for global delivery of NFC services. Why? Because, security in a mobile device is crucial and the TSM is the security coordinator creating a chain of trust.

There is a role for TSMs beyond NFC. For example, within the TEE ecosystem, one entity needs to manage the lifecycle of the trusted applications residing in the TEE. Within HCE, TSMs can play a role in combing the SE NFC offering and back-office systems of the cloud for token provisioning to offer an agnostic solution to service providers.

Creating a standardised framework today will allow TSMs to formalise and validate their role and contribution in the marketplace. It will deliver transparency to other ecosystem participants and offer the industry a platform on which to advance the mobile services network. It will allow TSMs to be a true friend and enabler of NFC service delivery.

The consequences of TSMs not complying in a standardised environment will result in the fragmentation of the market and the true potential of NFC services will not be realised.

It could also lead to less secure technologies coming to market as service providers look for alternative ways to deliver their services.

It is expected that GlobalPlatform will release its certification programme towards the end of 2015, and between now and then, there is still a lot of progress to be made in terms of needing to expand the scope to include other elements in the ecosystem to ensure comprehensive interoperability. The need for end-to-end as well as adhoc testing of components is vital to ensure the robustness of the system. This will inevitably limit the risk when deploying and launching services and therefore maximise the return on investment.

Consistency, transparency and interoperability among the stakeholders in the ecosystem will safeguard the true potential of NFC services to the benefit of everyone involved.
FIME is a trusted consultant and advanced end-to-end testing services provider within the payment, mobile telecom, e-ID and transit sectors. Its work ensures the successful and efficient market integration of products and solutions which use secure chips. Its wealth of testing knowledge and skills accelerates product time to market and promotes security, interoperability and confidence that products will deliver optimum performance once launched.

FIME has extensive EMV testing expertise working with banks, technology providers and authorities to develop the testing frameworks for international and domestic EMV-compliant payment schemes. In more recent years FIME has lead testing activity that supports the validation of secure applications to facilitate the deployment of near-field-communication (NFC) services, and advances within the trusted execution environment (TEE) and trusted service manager (TSM) ecosystems.

To ensure global testing expertise is delivered within a regional framework, FIME is expanding its network of ISO 17025 accredited laboratories and operations. It currently offers a local presence across America (Canada and the United States), Asia (India, Japan, South Korea and Taiwan), Europe (France), and the Middle East (Dubai).

FIME partners with leading payment schemes and industry bodies to provide certifications and enhance the secure-chip ecosystem: American Express, Calypso Networks Association, China UnionPay, Discover, eftpos, EMVCo, EMV Migration Forum, First Data, Global Certification Forum (GCF), GlobalPlatform, GSMA, Interac, Isis, JCB, MasterCard, Network for Electronic Transfers (NETS), NFC Forum, National Payments Corporation of India (NPCI), National Standard for Chip Card Specification (NSICC), OSCar Consortium and Visa.
Stéphanie EL RHOMRI
NFC & Payment Vendors Business Line Manager at FIME
and Chair of the GlobalPlatform Device Compliance Programme.

Stéphanie El Rhomri is in charge of developing FIME’s offers for NFC and payment vendors. She joined FIME in 2007 and created FIME’s international pre-sales force after spending 10 years working as head of technical support for a portable and embedded terminal manufacturer. Stéphanie works closely with all of FIME’s international offices in order to provide new services for the banking, transportation and telecom sectors. She is the lead of the Device Compliance Working Group within GlobalPlatform as well as the chair of its sub-Transportation Task Force. In addition to her involvement with GlobalPlatform, Stéphanie actively contributes to the NFC Forum and is engaged in EMVCo and GSMA activities.
TSM: FRIEND OR FOE TO THE NFC MARKET PLACE?
TSM: Friend or Foe to the NFC Market Place?

www.fime.com

twitter: @FIMEnews

join FIME on Linkedin