



Feedback Questionnaire for EPC-GSMA Trusted Service Manager and Service Management Requirements and Specifications V1

Background

The concept of using Mobile Phones to make Mobile Contactless Payments (MCP) in a secure and convenient manner is considered to be the next logical step in the development of mobile applications and payment services.

Realising this opportunity requires a close collaboration between the key players in Mobile Communications, Payments and NFC business ecosystems, in particular between the Mobile Network Operators (MNOs) and the Payment Services Providers acting as Issuers.

This document has been jointly developed by EPC and GSMA for the European (SEPA) market and focuses on the different roles and processes involved in provisioning and lifecycle management of the MCP Application on the UICC.

This document describes the main processes between Issuers and MNOs necessary to load and manage the MCP Application(s) on the UICC (note that the payment transaction itself is out of scope of this document). These processes are defined in terms of Service Management Roles (SMRs).

Responsibility and ownership of the SMRs falls entirely within the MNO and Issuer domains. Where the MNO or Issuer decides to delegate some SMRs to a third party, this third party is known as a Trusted Service Manager (TSM). One or more TSMs can be selected by MNOs and Issuers to implement SMRs. The document includes a description of a number of business models that support the implementation of these SMRs.

In order to accommodate the freedom of choice for the customer while supporting a level-playing field in the MCP, UICC-based ecosystem, Issuers and MNOs should have freedom of choice in selecting TSM(s) for implementing SMRs.

In order to develop a successful NFC ecosystem, that provides value for all, it is very important for the GSMA and EPC to gather industry opinion and feedback regarding our recent contributions.

As you are a key player in this new mobile NFC ecosystem or could potentially enter the ecosystem, the EPC and GSMA values your opinion and welcomes any feedback and comments that you can provide regarding the "EPC GSMA Trusted Service Manager and Service Management Requirements and Specifications Version 1" that was issued in January 2010.

We would be very grateful if you would complete this feedback form and return it by email by **Thursday 1st April 2010** to:

GSMA
e-mail: TSMconsultation@gsm.org

or EPC Secretariat
e-mail: TSM.consultation@europeanpaymentscouncil.eu

Thank you in advance for your kind co-operation.

Regards,

Nav Bains
Senior Director Mobile Money
GSMA

Dag-Inge Flatraaker
EPC M-Channel Working Group Chair
European Payments Council

Copyright Notice

Copyright © 2010 GSM Association, © 2010 Copyright European Payments Council (EPC) AISBL

Antitrust Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

Section 1: Your Details

Name:	Richard Martin
Title/Position:	Business Security Consultant
Organisation:	Payments Council
Role in the ecosystem	<input type="checkbox"/> Bank <input type="checkbox"/> MNO <input type="checkbox"/> Payment Scheme <input type="checkbox"/> Service Provider <input type="checkbox"/> Standards Organisation <input type="checkbox"/> UICC Manufacturer <input type="checkbox"/> TSM <input checked="" type="checkbox"/> Other (please specify): Strategic Payment Organisation_
Geographic coverage of your services/ organisation	<input checked="" type="checkbox"/> Europe (and if relevant please specify region(s) in Europe):_____ <input type="checkbox"/> Asia <input type="checkbox"/> North America <input type="checkbox"/> South America <input type="checkbox"/> Africa <input type="checkbox"/> Australasia <input type="checkbox"/> Worldwide <input type="checkbox"/> Other (please specify):_ _
Email Address:	Richard.martin@ukpayments.org.uk
Mobile Phone #:	

Data Privacy/Confidentiality

- Please check¹ this box if you wish your name and that of your organisation to remain anonymous as part of the consultation feedback review process.

¹ The box can be checked or unchecked by double-clicking the check box and setting the check box state to "checked" or "unchecked".

Section 2: Overall Opinion of the document

This section seeks your overall opinion of the “EPC-GSMA Trusted Service Manager and Service Management Requirements and Specifications V1” document; in terms of its aims, structure and flow. Please use a continuation sheet if necessary.

Question 1: What is your overall opinion of the document?

The Payments Council is the organisation that sets strategy for UK payments. Its core objectives include having a strategic vision for payments and leading the future development of cooperative payment services in the UK. We have a role in promoting innovations in payments, particularly where they can provide alternatives to less efficient means of payment such as cheques. The UK is a significant market for contactless technology, with several financial institutions currently undertaking a major contactless card payments trial involving around 8 million cardholders and over 23,000 merchants. The trial also includes a mobile phone-based solution that is not based on the approach described in the document.

Our view is that the document is helpful in describing the delineation of responsibilities between MNOs and issuers and many of their respective requirements. What it significantly lacks is a clear explanation of the role of TSMs and any specific requirements that are unique to them. It is highly likely that TSMs would face requirements that would not fit easily within the MNO or issuer spaces, and it would be difficult for a TSM to use this document to understand what is expected of them. The document touches on many matters with technical implications, but does not go into the level of detail that would be required in order to take the requirements forward to implementation.

The document paints a highly restricted picture of MCPs. Although the payment process is not described, it is strongly implied that all payments are made in a scenario where the phone is essentially a “large card” and all payment data flows across a standard card payment network. This ignores all other potential MCP scenarios, e.g. unattended point of sale, payment data flowing over an MNOs network etc. Our view is that contactless technologies may offer wider opportunities for payments than those explored in the consultation paper. For example the Mobey Forum has recently released a document entitled “*Alternatives for Banks to Offer Secure Mobile Payments*” that discusses some of these options in greater depth and demonstrates that the EPC and the GSMA should not attempt to use this document to restrict future options for financial institutions to one particular model.

Whilst the interests of MNOs are described in some detail, the interests of issuers are far less well defined. More work needs to be undertaken in order to ensure that any resulting MCP environment provides issuers with the potential for a profitable return on investment.

The title of the document makes no mention of mobile contactless payments, which would be helpful.

Question 2: What is your overall opinion of each section? (Please keep in mind that this document is not intended to be an implementation specification).

Executive Summary	None
Section 1: Introduction	<p>1.3. – makers and operators of contactless Point of Sale equipment should also be listed as stakeholders, as should the international card schemes.</p> <p>1.8 Definition of the term “<i>acquire</i>”. Depending on the context this definition is used in, it may be too simplistic, e.g. the merchant accepts MCPs and then banks their takings with their Acquirer some time later; who then negotiates value for them with the Issuer. The Acquirer, strictly speaking, doesn’t accept the MCPs. We recommend aligning the definition with that used in Section 2.2 of the document.</p> <p>1.8 Definition of the term “<i>customer-an MNO subscriber</i>”. The definition is restrictive. We would prefer to include other models of delivering MCPs including payment applications on the handset as opposed to the UICC.</p> <p>1.10 Term “<i>ISO</i>” – ISO is not an acronym, but rather a word in its own right derived from the Greek “<i>isos</i>”. The name of the organisation is the “International Organization for Standardization”..</p> <p>1.10 Definition of “<i>OTA</i>” –ETSI TS 102.225 defines MNO-handset over the mobile network, and NOT ISO14443 Proximity ICC to PCD. Care must be taken to precisely identify the standards being used, as there is a common tendency by many readers to confuse and conflate NFC with ISO14443, RFID and other terms.</p>
Section 2: Mobile Contactless Payment Overview	<p>2.1. – as discussed in Question 1 above, the vision of MCPs expressed in this document is too narrow and ignores or potentially blocks other interesting payment scenarios.</p> <p>2.1. – Provisioning. Can provisioning be implemented via NFC or Bluetooth, or via USB connection to a customer’s PC?</p>

Section 3: Guiding Principles for Service Management

3.1 Portability. Final bullet. Whilst not actually a re-issue of the 'virtual' card if it is stored on the UICC (which would be the case if the SE were in the handset), there is however the associated task of someone issuing a new Application UI which the card issuer will inevitably have to pay to have loaded.

3.2 Cross border usage with SEPA. *"The customer shall be able to use the MCP Application to make a transaction in another country than the one where he/she has an agreement with an MNO"* –the MCP payment as defined in the document does not make use of an MNO's network, so the customer should not require any connection to an MNO network in order to make a payment.

"If OTA is used for the MCP Application management abroad, then ...". – in which case, roaming must be supported.

3.4 Security. Security requirements also need to encompass the security of the mobile equipment and attendant NFC subsystems.

3.4 Security – what role if any does the TSM have with respect to security? This is critical as a TSM will be acting as intermediary between MNOs and issuers, thus inserting itself in many areas while also insulating/concealing MNOs and issuers from many aspects of security.

3.4 Security. All processes must meet PCI/DSS requirements where relevant.

3.5 Branding – proper presentation of issuer and scheme branding must be supported within the UI, which is defined in section 3.7 as an MNO responsibility.

3.7 Multiple issuers. Issuers may not be comfortable with an MNO controlling the card selection process. What is to prevent an MNO from presenting a "biased" selection interface? Why is provision of this interface an MNO responsibility? That sounds like a recipe for proprietary approaches leading to customer and issuer confusion.

3.7 *"A standardized data structure will be provided by the Issuer to represent the MCP Application in the MNO user interface"*. In use, the MNO user interface has to operate exactly as a physical contactless card at a POS if the POS terminal is to continue operating as now, i.e. unchanged for mobile 'virtual' cards. For example, it is not clear how counter reset would be undertaken in this environment. In the UK contactless card environment, the card has to be forced online after ten uses and we do not immediately see how this will be achieved in a MCP environment.

3.8 Requirements for the UI – In some markets where multiple applications existing on the same card, card selection may be done on the merchant terminal. Care must be taken to avoid possible conflicts.

3.8 *"This mechanism shall always be available"* – Is this true even when the battery is dead?

Section 4: Service Management

4.2 Service Management Roles, point 1 - "*The MNO is the owner of the UICC. His responsibility is to provide the "secure management framework".*" This section needs to be expanded in order that MNOs fully understand and appreciate issuer security requirements.

4.2.2. 3rd bullet. Within the context of "*An Indirect relationship*", "*MNOs want to grant their customers access to banking services without having to manage deals directly with Issuers*". This statement is highly misleading. It is issuers who wish to offer banking services to THEIR customers. MNOs wish to rent space on their UICCs.

4.2.2. "*Direct and Indirect commercial relationships can co-exist...*" What does this mean? Is this a reference to TSMs? If so then please say so!

4.2.2.2. B2B marketing. There is a real risk with this approach that issuer products will become commoditised where in fact they are highly competitive. Typos. "prospect" should be "prospective"

4.3.3. Combination model. It is unclear whether the customer will know who to contact in case of problems, and whether the TSM will be able to properly manage such an environment where a customer has multiple cards from multiple issuers.

Section 5: MCP Application Lifecycle Management

5.1 UICC management modes. Why is a TSM able to perform management, but an issuer apparently cannot? It would be important for an issuer to have this ability in cases as discussed in section 4.3.3. where an MNO and an issuer have a bilateral relationship not involving any TSM.

Clarity is required on personalisation profiles within the UICC. If each MNO is free to choose its own profile that potentially creates a minefield of essentially proprietary approaches. Further, it would make the task of properly assessing these profiles onerous. A common profile would greatly aid interoperability and simplify approval.

5.2.2. – “Load the MSP app via OTA” – that is not the only loading model – NFC and Bluetooth. What about download to a customer’s PC and then USB transfer? What about pre-loaded onto a micro-SD card by an issuer or TSM?

5.2.4. There is a need to ensure that a “two-tap” process is robust. What happens if the customer declines to tap a second time or the procedure is interrupted? Moreover, introducing a “two-tap” concept appears to be solutionising and therefore not needed in this document.

5.2.7. If contactless payments are offline, it may not be possible to block an MCP application locally at the merchant terminal. In the event of OTA blocking, what is to prevent a criminal from putting the handset in “Flight Mode” and therefore not receiving a Block command. Typo; “temporary” should read “temporarily”

5.2.9 – What happens then? How will the steps in section 5.2.5 – 5.2.7 occur?

Figure 7 – Steps 14 and 15. In the UK MNOs and issuers have agreed a set of mobile payment guidelines with the Government that create requirements for establishing a common reporting channel that ensures that a customer need only report once.

5.2.11. If value is to be stored on an MCP application, does this have legal implications for the MNO in terms of e-money issuance? Is it clear that any such funds are the sole responsibility of an issuer? Are such functions achievable via NFC, especially if contactless payments are offline?

5.3.2 – Scenario 2: typo. “form” should be “from”

5.3.2 – Process 5: What does “check the eligibility” mean in this context?

Section 6: Requirements for SM
in the MNO domain

MR.1 – Issuers have a material interest in the security of the UICC as it pertains to the security of their secret information, the security of the handset and the security of the MNO's network (including both OTA and from base station over the backbone landline network). Not only is this interest in the security of each individual component but, more importantly, it extends to the security of the system end-to-end when these components are inter-connected to form a channel over which MCP applications are managed.

MR.1 – “*triggered by New Threats*” – there is also a need to meet an initial set of requirements, and to meet any updated requirements whether any specific new threat has been identified or not.

MR.2. “...processes to certify UICCs and NFC services are being developed.” Who is developing them? Are the global card schemes directly involved in this development process?

MR.2 – “*this should include the NFC interface*” – prefer that this reads SHALL include...

MR.3. This requirement reads as if MNOs are responsible for issuing and re-issuing MCP applications. If that is the case then it is completely unacceptable as these are functions entirely within the issuer realm. Care should be taken that no payment sensitive data is stored on an MNO server. Typo? “*the purpose is to handle on...*” what is meant by “handle?”

MR.4. Why is the issuer not able to directly control deletion, blocking & unblocking of its own MCP applications? If a UICC runs out of space, is it clear who the customer needs to deal with?

MR.6 What is the definition of AID in this context? Are these the same AIDs as issuers have on their chip cards ? In which case, what AIDs do contactless POS terminals currently recognize and might this have to change with MCPs?

MR.8 – What is meant by “NFC Service” in this section? The terms does not appear to be used anywhere else.

MR.9 – This section refers to “simple SD” – what about other modes?

<p>Section 7: Requirements for SM in the Issuer domain</p>	<p>IR.1 – typo. “<i>Development MCP application...</i>” – insert “Development OF MCP application...”</p> <p>IR.1 – triggered by. Should also include new mobile equipment platforms, new point of sale equipment platforms, etc.</p> <p>IR.2 –The point starting “<i>The costumer [sic] uses this application...</i>” is out of scope.</p> <p>IR.3 – What third party approver is suggested? Is “approval” meant here or “certification”?</p> <p>IR.6 – Care must be taken that any sensitive card or payment data is properly protected at all times and at all stages. This requirement is strongly linked to MR.9</p> <p>IR.11 – Functions such as counter reset and script processing may not be currently supported by issuers.</p> <p>IR.13 – Danger of confusion. MR.11 states that “management of customer lifecycle events” is an MNO’s responsibility.</p>
<p>Section 8: Service Level Agreements for SM</p>	<p>“ <i>In order to foster a market place with a rich set of commercial actors performing several SMRs ...</i>” – is there a clear case or need for such a “rich” market?</p>
<p>Section 10: Referenced documents</p>	<p>None of the financial industry documents listed (10, 11, 12, 13, 14 and 16) are referenced anywhere in the document. This gives a lopsided impression. Additionally, some of the documents referenced are out of date and should be updated to point to the latest versions.</p>

Section 11. Annex I	<p>The processes illustrated in the diagrams are not very clear and it is difficult to get a sense of how they flow.</p> <p>11.2 - Change by Customer of the MNO - Whilst the new MNO registers their subscriber for the MCP application, there is no mention of the old MNO de-allocating any previous MCP application.</p> <p>11.3 - Change of Mobile Equipment by the Customer. As above, whilst the MCP application is downloaded to the customer's new equipment, there is no mention whether there is a new UICC and if so, that the MCP application on the old UICC is de-allocated</p> <p>11.5 - Stolen Mobile Phone. The path from box 16 up to boxes 5 and 3 should be totally separate from the path from box 13 down to box 18, and that there should not therefore be a path from box 16 to box 18</p>
---------------------	---

Section 3: Your support for the requirements

This section lists the requirements contained in the "EPC GSMA Trusted Service Manager and Service Management Requirements and Specifications V1" document. The aim of this section is to capture, in a quantitative and qualitative way, your opinion of each requirement. This will permit EPC and GSMA to perform an analysis of all the feedback received and hence gauge industry opinion regarding the current set of requirements.

You are requested to rate each requirement by entering "☒" in the appropriate check box. This can be done by double-clicking the check box and setting the check box state to "checked". The multiple choice categories are as follows:

"Very Good"	This recommendation is fully acceptable and your company will meet/support that requirement.
"Satisfactory"	This recommendation is acceptable and your company can meet/support that requirement.
"Consider Revising"	<p>This recommendation is not acceptable and your company cannot meet/support that requirement.</p> <p>Please provide further explanation.</p>

Please rate each requirement as either:

- Very Good (VG), or
- Satisfactory (S), or
- Consider Revising (CR).

(i.e. please check only **one** of the following check boxes). Also please use the space provided to give any additional feedback. Please feel free to use a continuation sheet if necessary.

3.1 Requirements for Service Management in the MNO domain

Requirement #	VG	S	CR	Additional Comments
M.1.1.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
M.1.1.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
M.1.1.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
M.1.2.1	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	How will certification be carried out, and against what? Is it clear that any chosen certification scheme meets issuer requirements?
M.1.2.2	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	How will certification be carried out, and against what? Is it clear that any chosen certification scheme meets issuer requirements?
M.1.2.3	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	How will certification be carried out, and against what? Is it clear that any chosen certification scheme meets issuer requirements?
M.1.2.4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
M.1.2.4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
M.1.3.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
M.1.3.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
M.1.3.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
M.1.3.4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
M.1.3.5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
M.1.4.1	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	How will the MNO be able to properly manage the UICC if the purpose of the SSD is to enable an issuer to protect a private space using their own keys?
M.1.4.2	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	How will the MNO be able to properly manage the UICC if the purpose of the SSD is to enable an issuer to protect a private space using their own keys?
M.1.4.3.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	How will the MNO be able to properly manage the UICC if the purpose of the SSD is to enable an issuer to protect a private space using their own keys?
M.1.4.4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
M.1.4.5	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Whoever receives a report of a lost/stolen handset must tell the other party. There seems to be no obligation to do so in these flowcharts
M.1.4.6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
M.1.4.7	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Care must be taken to avoid confusion as to the status of an MCP application as the card remains the property of the issuer. The issuer will at a minimum require notification that a customer has deactivated an application.

M.1.4.8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
M.1.4.9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
M.2.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
M.2.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
M.2.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
M.2.4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
M.2.5	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	[what strength of assurance do issuers need?]
M.3.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

3.2 Requirements for Service Management in the Issuer domain

Requirement #	VG	S	CR	Additional Comments
I.1.1.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
I.1.1.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
I.1.1.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
I.1.2.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
I.1.2.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
I.1.2.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
I.1.2.4	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	"The Issuer SHALL go through an MNO application validation process ...". Is this a separate application validation process with each MNO, or, if certified by one MNO will this be acceptable to all other MNOs ?
I.1.3.1.	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	What precise form does the "customer ID as provided by the MNO" take? Given the prevailing high rate of customer churn for MNOs, great care must be taken regarding the MNO ID in order to minimise ongoing management costs.
I.1.4.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
I.1.4.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
I.1.4.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
I.1.4.4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
I.1.4.5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
I.2.1	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	This is true only in a narrow sense. Security of the data is shared with the MNO, and wider security of the UICC platform is the MNO's responsibility.
I.2.2	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	It is essential to ensure that any sensitive card or payment data is properly protected at all times and at all stages. This also applies to boundaries between different domains (e.g. wired vs. wireless stages of a data

				link)
I.3.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

3.3 Service Level Agreements for Service Management

Requirement #	VG	S	CR	Additional Comments
SLA.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
SLA.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
SLA.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
SLA.4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
SLA.5	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Requiring “live and synchronous answers” is likely to be a heavy requirement. Is the case for it properly established, or are other options acceptable?
SLA.6	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	All these SLA requirements are worded as being between Issuers and MNOs – where do TSMs fit into the picture?

Section 4: Areas for improvement

Question 3: What are the key areas (gaps or weaknesses) that you feel should be addressed in Version 2 of the document?

The focus of this document is on the SEPA Card Framework. UK card issuers will want to ensure that any system for contactless mobile payments is compatible with existing global card schemes. To do otherwise risks consumers not being able to make payments in certain markets.

The interests of card issuers are not very evident in the document. The document majors on the commercial interests of MNOs and Trust Service Managers.

Further detail is required on technical matters. Although there is a case to avoid solutionising at this stage, there are several possible implementation paths that use existing technologies, and each one will have significant implications for how MNOs, issuers and TSMs approach the problem.

Clarity is required on the matter of contactless standards under discussion. Readers should not be able to confuse NFC with ISO14443, RFID or other contactless approaches.

Question 4: Did you identify any missing requirements that you feel should be addressed in the document? If so, please state them below.

Requirements specific to TSMs are not addressed in the document. This makes it very difficult for an issuer or an MNO to understand what to look for in a TSM, or for a TSM to understand what role it plays in the environment.

Question 5: Do you believe that the TSM models described in the document could support your business? Why? What are in your opinion the limits of this model? (Please keep in mind that this document is not intended to be an implementation specification)

No. See above.

Question 6: What are the most important requirements listed under section 3 for your business?

Compatibility with global card schemes.

Compatibility with a wide range of payment scenarios

Security requirements

Thank you for completing this survey!

Your feedback and comments are very important to us. Please return this form (by email) by **Thursday 1st April 2010** to:

GSMA Secretariat
email: TSMconsultation@gsm.org

or

EPC Secretariat
email: TSM.consultation@europeanpaymentscouncil.eu

Thank you in advance for your kind co-operation.

Regards,

Nav Bains
Senior Director Mobile Money
GSMA

Dag-Inge Flatraaker
EPC M-Channel Working Group Chair
European Payments Council