Report on the Common Requirements for a Secure Domain to support the Trust Management Model

Deliverable 1.4

March 2010

Grant Agreement number: IST-2007-214787
Project acronym: IFM PROJECT
Project title: INTEROPERABLE FARE MANAGEMENT PROJECT

Funding Scheme: Support Action
Project Coordinator: John Graham Verity
Head of Compliance
ITSO Limited, United Kingdom

Tel: +44 121 634 3700
Fax: +44 121 634 3737
E-mail: compliance@itso.org.uk
Project website address: http://www.ifm-project.eu

This report is an Output from the IFM Project -
a project funded through the 7th EU Framework Program

For further information please contact

Work package 1 leader

ITSO Ltd

John Verity
Phone +**+**44 121 634 3700
Fax : **+**44 121 634 3737
E-mail: compliance@itso.org.uk

Main authors

Newcastle University

Peter Stoddart
Phil Blythe
Phone **+**44 191 222 6420
Fax : **+**44 191 222 6502
E-mail: p.t.blythe@newcastle.ac.uk

For further information on the IFM Project, please contact:

Coordination

ITSO Ltd.

Phone +**+**44 121 634 3700
Fax : **+**44 121 634 3737
E-mail: compliance@itso.org.uk

Secretariat

TÜV Rheinland Consulting GmbH

Phone +49 221 806 4165
Fax +49 221 806 3496
E-mail: oliver.althoff@de.tuv.com

Visit the Webpage **www.ifm-project.eu**

This report is an Output from the IFM Project -
a project funded through the 7th EU Framework Program

Table of contents

This report is an Output from the IFM Project -
a project funded through the 7th EU Framework Program

Executive Summary

The aim of Work Package 1 is to explore and understand the complex issue of trust within an EU IFM environment. The first two deliverables were exploratory documents detailing, respectively, the existing Trust Models within the consortium and the wider Best Practice in other business sectors. Deliverable, D1.3, was originally intended to summarise the output from a workshop held on 6th April 2009. The purpose of that workshop was to explain the methodology for preparing a Trust Management Model but was also an opportunity to explore at an early stage the environment that this particular Trust Model would operate in. However the deliverable was extended to include high level a state of the art summary of the project with respect to trust and provided a number of discussion topics for the other Work Packages in their September workshops.

Subsequently Deliverable 1.4 has had an approved change of title due to the progress of the IFM project. Originally titled "Common Requirements for a *Security Access Module* to support the Trust Management Model", this has been changed to "Report on the Common Requirements for a *Secure Domain* to support the Trust Management Model". This change has come about due to two primary reasons:

- The technology discussion in other Work Packages has defined much of the technical security – particularly with reference to the smart media and it was felt that repetition here was unnecessary.
- There was a need to discuss the wider implications of IFM and as such the "domain" has been taken as the operational environment for IFM including and majoring on the customer offering and interfaces.

In addition Deliverable 1.4 is due before many of the other Work Package deliverables are due and so in a similar manner to previous deliverables from Work Group 1, has been used as a catalyst for discussions rather than a definitive statement. Deliverable 1.4 therefore presents a number of discussion points which later stages of IFM (e.g. IFM2) must address in their business model and business case. Many of the areas for discussion must examine the long term objective first in order to define the implementation approach. This is particularly true for the customer offering and we have chosen to discuss this in length as it illustrates the need for this approach.

The reader may like to keep in mind the VISA organisation as we discuss the points below. Visa represents many of the aspirations of IFM – albeit in a different business sector. Visa has grown in much the same way IFM is likely to do – separate schemes slowly getting together to provide a pan-European facility. Visa is also much simpler than IFM – it only has one product, IFM has many.

This report is an Output from the IFM Project -
a project funded through the 7th EU Framework Program

1. The trust management model

Deliverable 3 from WP1 proposed a methodology to develop both the trust and risk models for IFM. This methodology was as follows:

- Inventory
- Protection Requirements analysis
- Threat and Risk analysis
- Mitigation measures and residual risk analysis
- Repeat this process to accommodate the changes being proposed
- Review at regular intervals in a formal manner

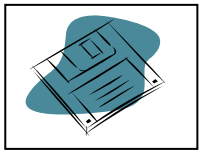
The timescales and scope of the IFM project do not allow for the execution of his methodology. Indeed Deliverable 7.3 only proposes the next possible steps for IFM and it is these subsequent phases which must deliver the actual trust and risk models based on whatever is to be developed.

2. The Secure Domain

We would suggest that there can be a number of definitions of 'secure' domain depending on which element of the environment the discussion pertains to. For example:

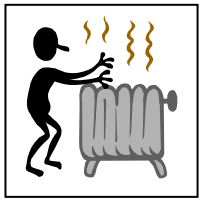
Physical security of machines, buildings, devices etc.

The technical security provided within the devices such as Global Platform provides.



The comfort factor provided to IFM participants by the rules of IFM and supporting activities such as Certification.

The warm feeling of security provided to the end customer by IFM.



It is these latter two areas around which the following discussions major – the remainder are assumed to be included in the output from the other Work Groups.

This report is an Output from the IFM Project -
a project funded through the 7th EU Framework Program

3. Customer offering

Who is the customer?
We should first define who the IFM customer is.

Is IFM:

- A facility which allows players in the Transport Sector to get together and share a domain with its respective facilities. In other words a “B to B“ organisation?

- Or a “B to C” facility for the traveller? Whereby they are provided with a common approach for:
  - Simple Registration if necessary;
  - Simple ways to get a “correct ticket”;
  - Standard procedures at each interface;
  - Easy System Access;
  - Understandable User Interface;
  - Standard appreciation of how to approach/use a Point of Service Operation (gates etc);
  - Ease of Ticket Purchase;
  - Consistent Customer Service through their own Customer Contract Partner;
  - Customer Service everywhere, where it is needed especially in "foreign systems" / in other regions;

Given the aspirations of IFM the answer to who the customer is, is surely then both of the above definitions. IFM is a brand or franchise for the traveller with a supporting organisation which governs the actions of its members. This supporting organisation must define the levels of service for the end user and the terms and conditions for the participants. These details would manifest themselves in such processes as Certification and Licensing or Franchising agreements.

This in turn begs the question of what am I, as an IFM player, signing up to?. Whilst the scenarios provide a very useful technology route, in these commercial areas all participants must know the end destination before they go too far along the road – it may not lead where they want to be!

Note to the reader – for simplicity sake in the remainder of this document we have called this governing body- EU.IFM

What does IFM mean to the customer?

In deliverable 1.2 we suggested that:

- IFM trusts that the customers will adopt IFM.
- Customer trusts that IFM delivers what it claims.

And that there were two time periods to consider:
- The present time, when interoperability is not widely experienced between public transport networks, especially between networks from different countries.
- The future, when multi-application cards are the norm (possibly owned by the customer or by their Mobile Network Operator), and global markets and operations are also the norm.

This report is an Output from the IFM Project -
a project funded through the 7th EU Framework Program

For the sake of this discussion we would like to examine a number of basic customer questions against these two timescales:

- How does this IFM work?
- How do I know it has worked?
- Is it worth the effort involved?

Scenario 1 – Immediately ("now" scenario)

Assuming the customer even knows about IFM (EU.IFM needs to market brand), he has say an ITSO card issued in the UK and wishes to go to Paris. The customer must:

- Go onto the IFM portal (another marketing task) through a PC and purchase the ticket. In return they will receive nothing other than a print out without even the assurance of the text containing a bar code as it would for an airline ticket.
- Present his card somewhere (ticket office or gate) to have the Navigo application added (application? – they bought a ticket not an application)
- Present his card to the gate at CDG station for the ticket to be downloaded.

If there is not enough room on the card the customer must do some card content management without any facilities.

If it does not work who will they call? The number on the back of the card is their local provider who is unlikely to know anything about the Navigo application and the purchase of the ticket.

Scenario 2 – The future

The customer has an iPhone or similar, is happy with the idea of applications which he downloads when he needs them and manages the content of his phone. He also browses the Web from his phone. The customer now:

- Uses his phone to buy the ticket which is downloaded to the phone. If necessary a new applications is added;
- Is able to see his tickets on the phone and as such can manage the content;
- Has a warm feeling about the success of the transaction before he sets out;
- Presents his phone to the gate for entry to the system;
- Is probably able to see the contact phone number on his phone as part of the application if required.

It would seem to WP1 that the "now" scenario will make for a very difficult implementation and therefore any further work on IFM should move as close to the future situation as possible. This is not as difficult as may sound with the new generation of phones now available.

A common experience for the customer – returning to the VISA analogy, the process that the customer experiences with VISA are very much the same wherever in the world the customer uses the Visa facilities. The messages may be slightly different, the card slot in a different place but on the whole the customer knows what to expect and has some comfort from this. This is enhanced by the ability of the hole in the wall machine being able in many situations to use the customers own language or alternatively one that they are likely to comprehend. Relating this to IFM:

Research by NUFC during a recent smartcard project in the UK has suggested that in the bus environment customers do not like talking to the driver and vice versa. How much truer is this given a foreign environment? The solution is of course tickets in advance together with a common experience or approach for the customer on arrival. A common standard for the procedures at ticket machines places an onus on EU.IFM to define and monitor these standards including a certification process.

This report is an Output from the IFM Project -
a project funded through the 7th EU Framework Program

The EU portal must relate to the customer in their language. Depending on the perceived role of the portal this may mean:

- That every Transport Operator who is in IFM must have his Web based ticket system in every EU language if the portal is simply a router;
- That the Web portal has the facility to sell products on behalf of operators and deals with the language issues. This would be easier to implement at the EU products stage but brings the EU.IFM into the commercial world with corresponding commercial agreements and risks, and a significant development effort;
- Or a combination of both.

Interoperability – the term means little to the customer but let us examine what the technical translation of the term means in the practical sense for each of the 3 levels of interoperability normally associated with smart media:

- Interoperability of media is the very essence of IFM but should be irrelevant to the customer. Provided the device they wish to use has the IFM approved stamp then it should do what it says on the can. This however puts again the onus on EU.IFM to control (certify?) these devices and to police the use of the brand.
- Interoperability of application should be transparent to the customers as they have no need of application knowledge. If a transaction needs a new application adding then the system should arrange this and perhaps the only thing the customer needs is an apology for the slightly longer transaction time.
- Interoperability of products is having a product (ticket or E purse) that can be used in more than one country on a single media according to the vision of IFM. The commercial relationships which define this interoperability are a matter for negotiations between the players.

However should there be an interoperable E purse then a completely different commercial arrangement must exist – possibly under the rules of a sponsoring banking organisation or the EU.IFM itself should it decide to be an E purse issuer. The VISA analogy applies again.

The (Technical) implementation steps proposed by WP3 are a challenge to customer management. They will surely expect the same facilities in each IFM country yet there must inevitably be staged implementations. So how will the customer know and appreciate what facilities are available. Is there a Minimum facility? Are the other facilities add ons until the minimum bar is raised?

4. Data transfer

Interoperability by definition means that data has to be delivered on an international scale often to IFM players who have no direct participation in the commercial ticket process, e.g.:

- A device (smartcard) issuer who is responsible for the device management will need to know of all the applications and products added to his device.
- One operator or a regional transport executive may provide back office services for other (smaller) operators and so process “not on us” transactions by simply passing on the data.

The EU.IFM scheme must therefore provide three basic security principles. The transactions must:

- Be “loss less”. An accountability trail from source to recipient must exist and data must remain recoverable until such time as the final recipient successfully informs the creator that he has received it. This trail could be broken down into a series of steps provided that the owner of the interim stopping off place abides by the loss

This report is an Output from the IFM Project -
a project funded through the 7th EU Framework Program

less transaction principles and accepts the associated risks (the bank clearing system demonstrates these principles).

- Be “secure”. Because the data may pass through a number of systems between creator and recipient the technical security system must ensure that transaction cannot be opened (possibly giving operators a view of the competitors business) or worse still the opportunity to alter that data.
- Be “private” . Once received by the owner the responsibilities do not end and the data must be kept private (see WP 2).

There is a role for EU.IFM here in that they must guarantee the security and police the operation.

5. Customer profile

The steps of the proposed implementation process introduce a customer profile. Whilst this product still has to be specified it will no doubt involve Disabilities (special requirements), Language and Eligibility.

The first two of these seem to require not only a definition of their use but perhaps also an onus on IFM members to use them and consequently an effect on IFM club rules and certification.

Eligibility: WP1 believes that IFM has the opportunity of taking ‘eligibility’ a step further than at present and the implementation of IFM should ask members if the acceptance is mandatory or optional and if so whether this is at a commercial level or political level. Similarly the criteria for eligibility must be common and the method of proof of eligibility to a reciprocal standard.

Whatever the outcome the customer must be clear as to what this product will bring him.

6. Relationships

At the October21st 2009 IFM meeting the analogy of exchanging IOUs (I owe you) was used (see fig. 1) to illustrate how interoperability can create relationships between strangers without their knowledge and the applicability of this to IFM. It is particularly so in the case of media management where it is likely that the media owner will learn of applications and products loaded from others with whom the only thing in common is IFM membership. This requires clear rules as to the players responsibilities and requirements, e.g. does the card manager have to maintain a device profile? Does an operator have to inform when the product has been used and can be deleted from the profile? These rules and monitoring of these rules imply a governance role for EU.IFM.

7. Help desks

The example used in the relationships section of the media manager extends further when we examine the customer help proposition. When something goes wrong – “who you going to call?” – probably the number on the back of your card or the phone issuer. So Vodaphone or Manchester city council will be expected to explain why the gate at Charles de Gaulle station won’t open despite there being a ticket on the device. Obviously this is impractical but they must be able to direct the customer to where they will be able to get help. This implies a

This report is an Output from the IFM Project -
a project funded through the 7th EU Framework Program

central log of IFM members, IFM media owners, IFM product owners etc., which is available to help desks. Another role for EU.IFM.

The Web portal also brings with it a requirement for a help desk – probably both on-line and phone. Only EU.IFM can provide this facility.

8. Brand

Returning again to the VISA analogy – IFM has to be a brand. A brand that not only tells the customer what to expect and trust but also one that Operators, Local Authorities and Politicians will aspire to. Whether "IFM" is the brand is a question for IFM2.

However a brand brings with it Marketing and Brand Management responsibilities. Another role for EU.IFM.

9. Black Listing

Blacklisting, white listing or hot listing on an EU wide basis will inevitably be impractical due to the volume of data involved. Whilst this volume could possibly be accommodated in the back offices, within the capabilities of even the latest points of service both the volume of data and perhaps more importantly the speed of transaction would make the holding and processing of complete lists impractical.

However blacklisting must take place – and therefore a balance must be determined - a balance of what is operationally possible and the risk involved -. IFM members must develop, agree and follow a code of practice which:

- Recognises the difference between the media, application and products. For example, if the media is stolen then all applications and products may well need to be stopped. Alternatively if a product requires stopping for say a revoked payment then the remaining contents of the media should not be affected by any action taken.
- Recognises a practical level of risk. For example:
    - If the media only contains a purse with a value of 3 Euros then it may be practical to simply replace that purse for the customer;
    - If the media is lost rather than stolen then it is perhaps sufficient to monitor for any future use and even then to enquire if the customer has found the media before blacklisting.
- Considers whether the media contains any 'international' products before blacklisting on an international basis, although this assumes that there is an entity who knows the entire contents of the media.
- Places an onus on all IFM players to handle and action 'imported' blacklists without favouring their own lists. This in turn implies a monitoring and arbitration role for EU.IFM.
- Provides the operational instructions for managing these lists such as deleting from an exported list if resolved at home or allowing the receiver to delete after a stated time whilst the exporter continues to monitor.

Examples of these codes of practice do already exist on an interoperable basis and could be used as a basis for this work.

This report is an Output from the IFM Project -
a project funded through the 7th EU Framework Program

10. EU.IFM

Within this discussion and within the deliverables of many of the other Work Packages various central activities have been identified. Whilst this project (IFM) and whatever may immediately follow (depending on the scale) can be managed on a Steering group/working party basis, any significant move into a practical IFM scheme must require the final vision of the central activities and how they will be managed and funded. One cannot ask partners to join in IFM without knowing what the commitment is in the longer term!

To date in the various Work Packages the following management activities for EU.IFM have been recognised:

- Technical
- Service
- Privacy
- Brand
- Marketing
- Contractual and Legal
- Administrative
- International Standards
- Risk and Trust
- Compliance

How these are to be provided must be an integral part of IFM deliverable 7 or at least a methodology for determining the outcome.

11. International Standards

Any EU.IFM organisation and scheme must be an integral player in the development and implementation of International standards and codes of practice. This is essential to not only protect the existing investment in the scheme but also to influence emerging work in order to represent the transport ticketing industry. A simple example of the latter would be the universal development of E purse standards where a standard suitable for banking and retailing solutions may well be unacceptable for transport due to slow speed of transactions. Little is done at present in this representation area due to the absence of a central transport representative body. However EU.IFM would be neglectful if it did not adopt this role.

Example of the present standards and codes of practice being developed where EU.IFM should be represented are:

- ISO TC204 WG8 / CEN TC278 WG3 SG5 dealing with IFM Systems (ISO24014) and PWI on EMV bankcards in transport;
- CEN TC224 dealing with IOPTA and EN1545;
- NFC Forum dealing with the use of mobile phones as contactless media in transport;
- Global Platform.

The standards which EU.IFM must consider are not necessarily only related to transport or smart media. Within Deliverable 2 from WP1 we identified ISO 27001 which in many respects impinges on the emerging EU.IFM and must be taken into account by that emerging organisation.

This report is an Output from the IFM Project -
a project funded through the 7th EU Framework Program

Summary

We reiterate an early statement that the risk and trust models will be created in IFM2 based on the outputs from the other WPs – outputs which have already been or still remain to be delivered.

Whilst the detailed technical requirements have been described by the other working parties there are some trust principles that are worth repeating here:

Security agreements:

- A common security agreement will be required amongst the EU IFM members and is the first part of the trust model.
- The security requirements for the Secure Element proposed in D3.2 has shown that security agreements must be set up between media owner and IFM schemes for enabling remote management of local or EU IFM ticketing application, i.e. loading, installing and personalising an application in an EU IFM compliant media. The security will be based on Global Platform technology, which also provides a standardized and confidential way for exchanging media key between stakeholders and is not requiring any change in the front office equipments.
- The security requirements for the ticketing application will require in the front office equipment the usage of the legacy native SAM when local ticketing applications are used or of an EU-IFM SAM or certificate when the new EU IFM application will be used.
- The recent publication of the European Payments Directive for contactless payment cards and the move towards a new Protection Profile, tested to level EAL4+, for such devices under Common Criteria is highly relevant to EU-IFM. It is important that EU-IFM maintains full compatibility with payment cards and any security requirements should be aligned. With EPC setting European-wide standards for security it is important that DGTREN does not mandate a separate requirement but uses the same framework to ensure European contactless payment cards can be used universally in transport applications.
- Additionally, the original brief for WP1 included the specification for an EU-SAM to secure data transfers between stakeholders. The development of security algorithms in the time since the proposals for IFM Project were published and agreed by DGINFSO, particularly through developments in relation to contactless payment cards has meant that PKI is now a valid security option to be considered, and one that may not require a SAM.

Customer's trust:

- The customer offering is paramount to the success of IFM and must be defined early in IFM2. This doesn't mean common products at this stage but it means a number of local IFM willing to join the new multi-application environment sufficient to attract customers and raise their trust in the future development of commercial offers.

Stakeholders' trust:

- A certification regime must exist which in essence creates the EU IFM Brand. This may be achieved however in part by an acceptance of other certification regimes.
- The EU portal and the possible use of other portals to download the EU application creates not only a new 'role' but with that role a new set of trust requirements which must be defined and agreed (see D4.3 & 5.2).
- The technical requirements and also the commercial aspects of the schemes e.g. the back office will create liabilities which must be clear in any accepted trust model (see D4.3).

This report is an Output from the IFM Project -
a project funded through the 7th EU Framework Program

- The EU IFM need to define and reach common agreement on the data model and specification of the EU application at an early date
- The contactless media not only must have the technical level of trust as defined by the protection profile of the media. It must also not effect the performance of the transport application for a good customer acceptance. E.g. a bank card must still perform at an acceptable level in terms of transaction speed for a transport application loaded on it.

This report is an Output from the IFM Project -
a project funded through the 7th EU Framework Program