

Report on the follow-up workshop to explain and disseminate the agreed Common Methodology for preparing a Trust Management Model

Deliverable 1.3

August 2009

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

Hannah Bryan

Peter Stoddart

Phil Blythe

Phone +44 191 222 6420

Fax : +44 191 222 6502

E-mail: hannah.bryan@ncl.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

| | |
|---|----|
| Executive Summary | 4 |
| Introduction | 4 |
| Highlights from Previous Deliverables | 5 |
| Definition of Trust | 7 |
| The Methodology..... | 9 |
| Discussion Points | 10 |
| Scenarios | 10 |
| Scenario Implementation Steps | 11 |
| Step 0 | 12 |
| Step 1a): Download local Application | 12 |
| Step 1b): Initial Common Portal | 12 |
| Step 2: EU Profile Application | 13 |
| Step 3 onwards (common EU ticketing product) | 14 |
| Step Implementation | 15 |
| Customer Offering | 15 |
| Operator Challenges..... | 18 |
| Relationships..... | 19 |
| Certification and Qualification Process | 20 |
| Hotlistings and the Associated Rules | 20 |
| Conclusion | 21 |
| Appendix 1 – Minutes of meetings | 23 |
| Appendix 2 – ISO 27001 – Security Management Standard | 33 |
| Appendix 3 – Relationships | 35 |

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. This 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.

The outcome of the workshop was a simple methodology and a number of discussion areas which the various working parties could develop further.

Timescales for this deliverable have however allowed further work to be done on the discussion points and this deliverable therefore summarises the position as at the end of June 2009 and will provide input for further workshops in early September 2009 organised by working parties 3,4 and 5.

Introduction

The IFM project is researching the ways in which a transport smart ticket scheme between different countries and participating companies can be delivered. There are many challenges which need to be addressed and WP1 aims to understand and develop a Common Methodology for dealing with trust in such a complex environment, where relationships, interactions and risks are yet to be defined.

This deliverable documents the position at the end of June 2009 of the process which has followed the first two deliverables from WP1. The methodology for this has been to engage with members of the consortium at the various meetings and workshops which are occurring regularly, to engage with the IFM Forum using a presentation and breakout groups and to hold a workshop in Newcastle. Rather than document each individually in the report, the minutes from both the IFM Forum and the Newcastle Workshop can be found in Appendix 1, and the main themes that resulted from the discussion will be reported throughout this deliverable.

This deliverable describes the simple methodology for the development of the Trust Model and the state of play of a number of areas still under development;

- The development scenarios for an EU IFM
- The implementation steps of those scenarios
- The customer offering
- The operator challenge
- Certification /qualification
- The player relationships

In essence the IFM project is taking both a top down and bottom up approach. WP1 is the top down by identifying the initial Trust issues and the other Working Parties are the bottom

up as they look at each requirement, identifying the risks and to ensure that their WP is addressing the issues.

Highlights from Previous Deliverables

This section presents the highlights from the previous two deliverables, in order to provide both context and background to the findings of this deliverable.

In D1.1, *Inventory report on existing Trust Management Models based on the Questionnaire to each participating country to gather information*, WP1 had the following objectives, to:

- *Identify current Trust Models and Best Practice within the existing schemes*
- *Identify the common mitigation solutions and processes necessary to reduce common risks that make up a Trust Management Model.*
- *Begin identifying the Common Methodology for a Trust Management Model in support of EN 24014 (part 1)*

In order to achieve the objectives, the methodology employed was to, firstly, develop a Questionnaire to identify levels of risk and mitigation in relation to EN 24014-1 case studies. The theory was to establish the levels of risk for each case study, to determine if the participants were mitigating against this risk and finally whether the risk was captured within their existing model. The theory being, if participants mitigate against a risk it should then not feature within the Trust Model.

The questionnaire was circulated to the consortium and allowed WP1 to begin to understand the levels of trust per transaction and elements of residual trust required. Each case study was ranked in terms of high, medium or low risk which helps WP 1 to prioritise the cases. The use cases identified as a high risk to each of the respondents were:

- *Each component to be brought into the IFM shall meet the IFM requirements. Proof of this is given by checking this Component against a Set of Rules*
- *The generation, distribution, storage and termination of IFM security keys.*

In addition, one element was identified as a low risk to each of the respondents, and although still important within the Trust Model, higher priority should be placed on the other case studies:

- *Termination of Product by request of the CUSTOMER*

However, as the results suggested both a lack of consensus and overall understanding of trust, a Workshop was then used to build a common view of Trust for an EU IFM and EU SAM. The workshop addressed the questions arising from the questionnaire and was able to define exactly what a Trust Model means for an IFM, as below:

‘A statement of residual risks that need to be accepted between system Operators’

Discussions began to highlight the many different areas which must be considered during the WP1 activities. This led to the development definitions of player relationships and potential risks (see Figure1), and developed the idea of ‘Residual Trust’ as no risk can be

truly mitigated and therefore the residual trust that is still required must be documented in the Trust Model.

It also became apparent during the workshop process that none of the participating consortium members have an existing Trust Model that meet the requirements of an EU IFM; however, elements of the members' licences, contracts, membership rules, risk models, among other things, were found to be relevant and, therefore, could be considered for inclusion within a Trust Model. It was established that WP1 must define the methodology and outline of a Trust Model that will meet the needs of an EU IFM, facilitating unity and data sharing. The seeds of this process are documented in this report.

Scheme Model

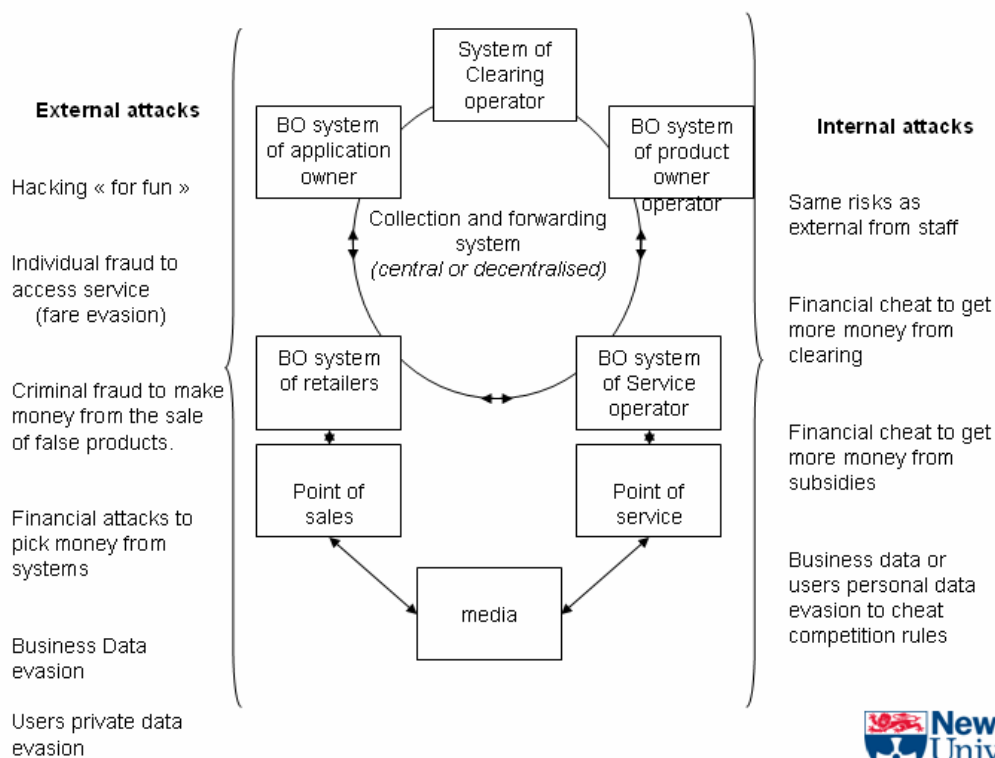


Figure 1: definition of player relationships and potential risks with an IFM

The second deliverable, D1.2, *Report on the commonality between approaches and compare to published Best Practice in other relevant business sectors*, looked much wider at the Best Practice in other relevant business sectors and to compare this with the results from Deliverable D1.1. The case studies documented were chosen as they demonstrate existing Trust Models that allow data sharing on a B to B and B to C level and, therefore, provided some valuable insight into the aspects for inclusion in an IFM Trust Model methodology. D1.2 had the following objectives:

- *Study of case studies and standards and compare to existing approaches found in D1.1*

- *Identify the internal and external common relationships present in the IFM that support and threaten Trust;*
- *Begin identifying a common methodology for a European Trust Management Model.*

The methodology employed was predominantly a desk study, however, some primary research was used through discussion with the consortium members and other external experts. Three case studies were used and the findings are summarised below.

Integrated Ticketing for Air and Rail:

- A Trust Model is a set of Procedures
- Responsibility to customers is vital

Local Government – taken from New York City:

- Demonstrates Trust Model procedure for authentication and data sharing
- Highlights need for a matrix of risk versus the impact to the players

Digital Economy

- Importance of Customer Trust
- Importance of Branding and Reputation
- Importance of fostering Shared Interest on issues such as privacy and security

Ultimately, no Best Practice completely fits the needs of an EU IFM, therefore WP1 must create the Methodology to ensure all elements are covered. This process began the procedure for identifying the common methodology for discussion at the workshop in April for D1.3.

Definition of Trust

Thus far, Trust has been defined as: ***‘A statement of residual risks that need to be accepted between System Operators’*** and the concept of Residual Trust has been introduced. During the process of discussions through the forum and the workshop, the concept has been extended to further distinguish risk from trust and is demonstrated in Figure 2. That is that a risk is identified, mitigated, closed, and accepted. With trust, the risk is identified but it cannot be mitigated, therefore is left open. It must still be accepted and this forms the Trust Model. Additionally, it should be noted that even if a risk has been mitigated, there may be underlying risk and therefore residual trust is still an option and should not be overlooked for inclusion in the Trust Model.

Trust = Risk Acknowledgement

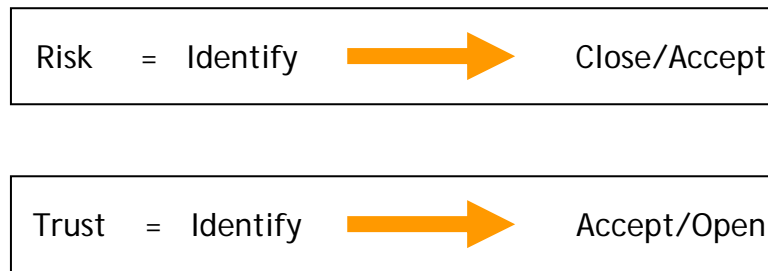


Figure 2: Concept of Trust

Additionally the discussions have suggested that trust may be described as having 4 elements, particularly where players are considered:

- Control – the extent to which the truster can manage the situation
- Assurance – the extent to which the system can control the risk
- Damage – the extent of the effect of the risk (referred to as ‘No worse off’ in this document)
- Benefits – the extent to which the player gains

This report uses the following 'Boston box' (see Figure 3) at various points throughout the deliverable to describe the relevance of these elements;

| | |
|----------------|------------------|
| Control | Assurance |
| Damage | Benefit |

Figure 3: Boston Box for fostering trust

Ownership of risk/trust

By definition every risk must have an owner in the sense of who takes responsibility should the risk occur. Similarly trust must have an owner although invariably it will be joint ownership – i.e. I trust him to do this. The eventual Trust Model must therefore define the ownership and the accountable body. This in itself raises the issue of the role of the EU IFM Body. For example, does it take on some of the risk or is it a shared ownership model?

The Methodology

The methodology for the development of the Trust Model is quite simple;

- Define all the risks
- Decide which of these risks can be mitigated
- Define the ownership of the residual trust

It is difficult at this stage to state exactly what each of these stages will include, particularly as the final approach and the nature of the EU IFM body are still to be defined but it is likely that the basis will be;

- Deliverable 1.1
- The existing scheme risk models
- Deliverable 1.4 subject areas
- Workshops based on the final outcomes from the other WPs

However, this in itself predetermines that there will be a need for the management by a central 'IFM body' of these trusted relationships between the players. The Trust Model will be defined by the IFM body as the minimum requirements for each existing scheme and any subsequent applicants, i.e. the model will contain a list of risks which must be either mitigated or trusted by each scheme in order to participate. The mitigation of these mitigated risks will be compulsory i.e. a minimum standard must be met. Trusted risks may, however, be mitigated by each participant over and above the minimum defined.

There is an underlying assumption present that not only is there a controlling body in terms of the initial definition but also a requirement that the minimum standard is monitored by that body (or alternatively an umbrella trust that the players are trusted to meet the requirement).

Additionally WP1 has looked at ISO 27001. This standard provides a series of headlines for different objectives and controls in a general IT system which can be used as a basis for the risk assessment. Examples of these are included in Appendix 2 and will be explored in more detail in D1.4. These examples have also been used to develop the top-down approach, to highlight areas where other WPs may need to focus attention to ensure that trust is dealt with throughout the project and to enable the gap analysis.

This deliverable does not provide any of the detail of the actual content of an IFM Trust Model as this is out of the scope of this project and will potentially be developed in the proposed IFM2 project. The purpose is to develop the methodology, not execute it. Should the methodology be followed, the end product aims to be the development of the Trust Model, which will be dependent on the environment, for example, structure, operation, activities, etc.

Discussion Points

As described earlier, this deliverable develops the simple methodology for the development of the Trust Model and the state of play of a number of areas still under development. These areas will be discussed in this section and are as follows;

- The development scenarios for an EU IFM
- The implementation steps of those scenarios
- The customer offering
- The operator challenge
- The player relationships
- Certification /qualification
- Hot listing and the associated rules

Scenarios

Key scenarios are being developed by WP3, dealing with media, to demonstrate the possible step process for introducing IFM interoperability across participating countries. They felt the objective was not to produce something compulsory for all participating countries but to take a collaborative approach. By providing options for progressive integration, existing systems and infrastructure can be retrofitted to deal with the EU IFM environment. As part of the process of engaging with and developing the essential content for the Trust Model from the other work packages, WP1 has looked specifically at each scenario developed by WP3 in order to:

1. Recognise the trust requirement areas;
2. Identify the impact upon the other WPs (see Appendix 2);

The risks and trust implications increase as the scenarios move on in time and implementations, and are further complicated by the varying speed of implementations between the IFM schemes. Within this deliverable the focus is upon steps 1a, Download local application, 1b, providing a common web portal, and 2, EU common application with EU status and product (as they are within the scope for this project). The subsequent steps are born in mind in order to ‘future-proof’ the model.

The current design philosophy is as follows and demonstrated in Figure 4:

Step 0: Existing System

Step 0 is the current situation where media are (mainly) native (i.e. non downloadable) media. Interoperability can be achieved by cross-acceptance in the form of mutual agreements to accept one another’s media.

Step 1a: Download local Application

This step allows the customer to download foreign applications through the internet directly from the foreign website. For example, a French customer can download an ITSO product (NB see below) from an ITSO compliant website. The product is downloaded directly onto the card at this point or via an action list (i.e. when the customer arrives in the country at a pre-determined machine).

NB: As the customer does not understand the difference between an application and a product, the customer will think they are just downloading a product, however the downloading of the application is part of that product process.

Step 1b: Common web Portal

This is the introduction of the EU portal, which simply connects or points the customer to the foreign website where the product (and therefore application) can be purchased and downloaded

Step 2: EU Application

Customers can benefit from their particular status eg age concession, all over Europe.

A common EU-Application is defined. The customer can have this application downloaded into his media. His home network will export the appropriate data into this EU-Application according to the common data model.

Other Applications will be able to import the status for use in their data model for the benefit of the customer.

Step 3: EU Products

Customers do not need to download a local application for their occasional trips any more: a standardised template has been implemented in the EU-application that can be used for local products.

Step 4: Only EU Application

Common products are proposed and hosted in the EU-application.

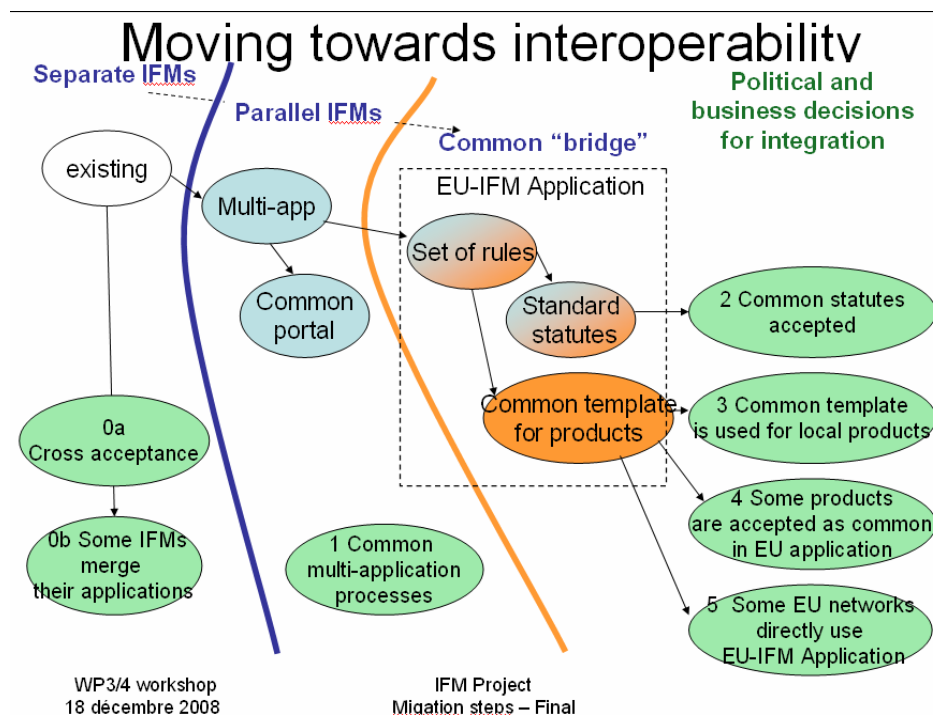


Figure 4: Scenarios developed by WP3

Scenario Implementation Steps

Each of these steps produces a growing hierarchy of Risk/Trust issues, as follows:

Step 0

is the current situation where media are (mainly) native (i.e. non downloadable) Media interoperability can be achieved by mutual agreements to accept each other's media. There is one prime example of this in the UK. Over 300 schemes accept interoperable cards and exchange the ensuing transaction data using the ITSO specification. The trust and risk philosophy is recognised by a combination of;

- certification of cards, hardware and software
- an operating licence for each IFM which defines the rules and standards which each player must adopt
- commercial agreements between product owners and operators

Later in this deliverable certification will be discussed. The structure of the EU IFM and any possible licence or club rules is under the remit of WP4. The final bullet is without IFM as this is a commercial agreement

Step 1a): Download local Application

Schemes must accept media that has been created by another IFM. On an international basis this is much more difficult and requires the definition of a certification process. This is in effect no different to step 0 except on a wider scale. The same issues apply, in that there must be agreed conditions for accepting media and the model must stipulate the rules and the mechanism for trust, for example, a 'logo' within the media that both the customer and the point of sale will recognise and trust. At this point data is also exchanged between IFMs with respect to card contents according to the rules of the EU IFM club but no commercial agreements need to be in place.

The Media technical requirements and certification process to ensure that these requirements will be met have been already addressed in WP3. [The business/commercial agreement, should be addressed in the next WP4 deliverable.](#)

[With respect to the main](#) exchanged data in this step is the media access keys.

Risk and trust consideration can be developed for this step regarding what may eventually happen once media key are in Application Owner hands. No risk is foreseen here as the keys are only "unlocking" access to a subpart of the SE dedicated for the application of the key recipient ... and this area is isolated from the rest of the SE.

However transaction data will also be exchanged and will require a security environment and some "club rules"

The customer offering takes on a different concept and this is discussed in a later section.

Step 1b): Initial Common Portal

The IFM customer offering takes a major step forward here requiring many of the trust principles referred to in deliverable 1.2 to be implemented on the IFM portal. See also the later section on customer offering.

D1.2 looks to other business sectors for best practice in trust. The third case study concentrates on internet transactions and looks firstly at e-commerce and secondly at

internet banking, both of which highlight the way to obtain customer trust online. The way that IFM customers relate to the scheme is likely to be predominantly through the internet and in this step, step 1b, the common portal will be the face for IFM, therefore the design and the effectiveness of this will greatly impact upon the trust the customer feels towards both the transactions they carry out and the actual brand. The following list is the areas highlighted by the case study as important for fostering customer and supplier trust online:

- Branding
- Endorsements from trusted third parties
- Demonstrating shared values
- Transparency
- Clear instructions for customers, particularly difficult when schemes are in different steps
- Security of data and transactions

In essence though this is a non merchant web site and common good practice should prevail in its design and function. The features of the initial EU portal will evolve as the implementation of the steps evolves, with the added complication that members will be at different stages of implementation.

Step 2: EU Profile Application

This step will be a significant discussion point in the September workshops but it is perhaps worth rehearsing some of the arguments here;

The currently suggested approach is;

- *The card holder will visit a home location and;*
 - *Either provides evidence of their eligibility*
 - *Or already has the home profile on his card*
- *The home location will then add the EU profile.*

The card holder then goes abroad and;

- *Either every POS recognises the EU profile (which is likely to be the case for new IFMs in the future) or where the POS's have had a software upgrade*
- *Or the card holder goes to specific POS's which can convert the EU profile to the local profile*

Note - This approach means the customer has to ;

- *Either visit two locations each of which has developed software or been upgraded*
- *Or one (home) location and the entire hardware base in the visited country will have been upgraded.*

Alternative approaches might be as follows;

- *Card holder has eligibility on their card and logs onto the EU portal. The portal recognises the home eligibility and asks where the customer is going to. The portal then loads either the local eligibility applicable for this location –ie*

*either the local one or the EU one (or perhaps both to future proof the card).
This process means only one central development of the EU portal*

- *Or perform Home to EU profile conversion on the Home network web site and EU profile to visited network conversion on the Visited network web site. This process can be eased thanks to customer redirection from the EU portal to the Home and Visited Network appropriate pages for EU profile handling.*

Acceptability of the customer profile/status

As different EU countries have their own way to profile customers, which often vary even within a country then the level of authenticity will be different. The ramifications of these variations need to be understood and the level of risk appreciated. This will be expanded upon in deliverable 1.4.

There is no doubt that the local profile may vary over time and that there are widely different local developments. Even if the EU profile support becomes a mandatory requirement from EU authorities, it's very likely that each PTO will keep the EU profile conversion under their responsibility simply because they will have to have to pay for its development. Then, it's up to each PTO to decide to handle the development internally or to subcontract it, Alternatively the EU IFM organisation may wish all PTO to subsidise a central entity for performing this development...

Data transfer

This step also introduces data issues in terms of how much information needs to be shared between schemes. Given that requirement the rules (and monitoring of those rules) must be part of the EU IFM organisation. These elements are being developed further by other WPs

Step 3 onwards (common EU ticketing product)

The introduction of common EU applications brings not only standardisation and political issues but commercial agreements which we would suggest will be the driving force behind any further expansion of the EU IFM principle. We would suggest that this requires a significant amount of speculative work.

Part of the data being exchanged equates to financial clearing when using EU common product purchased in one network and used for travelling in another one.

A risk and trust analysis should be done there, may be by analogy with the GSM ecosystem where clearing is done between MNOs for roaming customers.

It is very likely that Public Transport Operators will only accept financial clearing if relying on process supported and agreed by well established EU financial institutions.

Step Implementation

There will be an overlap between schemes in different steps, for example, some schemes will be in step 1, and others may be in step 4. This is a political decision as when to move between steps and it is important that the schemes are compatible, regardless of the step they have adopted, and kept clear and transparent for the customer.

Within the implementation steps a further variation needs to be discussed; Where say a French card holder wishes to travel in Holland then there is a situation where a single card issuer's card is used in a multiscard owner/ multi product environment. The transaction data can be collected by any of the participating schemes and collected by a number of acquirers who will wish to clear to IFMs outside their normal remit.

Customer Offering

The IFM project is about the technology of interoperability and it is for others to establish the business case and marketing. However, it is perhaps still worth discussing the customer offering at this stage to ensure the hooks are provided.

There appears to be two levels of trust involving the customer;

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

And 2 time periods to consider;

- Currently, when interoperability is not necessarily a high priority for customers (this is the position Visa was in when it started)
- And the future when multi-application cards are the norm (possibly owned by the customer), and global markets and operations are also the norm

It is perhaps first worth repeating here what the vision for the customer offering is as given in a paper to UITP re the IFM project:

The following scenario, presented in the project file, clearly illustrates the form of cooperation being sought as well as the goal of flexibility and adaptation to local fare policies and different customer segments.

“Mr Move is a cross-border worker. He lives in country A and works in country B. For his daily commute, he needs to carry two different fare cards. Of course, both are interoperable in their respective countries. However, country A and country B have two different IFMs. The only existing agreement concerns the rail link between city A and city B, on which either of the two cards can be used. For buses, trams and park & ride facilities, however, only the local card is accepted. Transport authorities in country A and country B have been discussing a fare agreement for buses, but their fare systems are so different that they have not been able to reach a settlement.

“IFM managers from country A and country B finally agree to issue and accept EU-IFM compatible cards. Mr Move is very pleased with this new situation. He has applied for the new A-Card which is now recognised in both countries. His colleague, who lives in country B, has done the same and applied for a new B-Card. The new card allows him to have all the products that he needs on one card but as yet none of the products are interoperable.

Next summer, Mr Move plans to travel to Rome and Paris. The transport authorities in both of these cities accept EU-IFM compatible cards from all over Europe. When Mr Move arrives in Rome and Paris, he will be able to use his new A-Card to buy – either with cash or by credit card – a transit pass in these cities for the duration of his stay. Alternatively if he has internet facilities he can pre-purchase the pass before he leaves and have it downloaded to his card either over the internet or on arrival at a specified terminal.

Because his new A-Card provides proof that he is a senior citizen, he will be able to benefit from any discount fares where available

“Mr Move’s son uses a contactless EU-IFM compatible mobile phone. He no longer needs any fare cards: long-distance railway tickets with seat reservation can be downloaded directly onto his mobile phone. He can avoid queuing to buy his bus ticket by prepaying for it online before leaving home or by using the electronic purse on the phone at the barrier. His tickets are stored in his mobile phone, which he uses to check in and to show to inspectors on request.

The September workshops should perhaps try to answer 2 questions;

- 1. Why would the customer want to do it now?**
- 2. Why would the customer want to do it in the future?**
- 3. Who can provide the service to the customer ?**
 - If we want to tackle the question of after sales services, we should also address the point of who will deliver the service to the customer. We’ve seen that in the NFC ecosystem, according to the case, services can be provided by the media owner, by the application owner, by both, ...

And these in turn raise a number of sub topics as demonstrated in Figure 5.

| | |
|--|--|
| <p>Control</p> <p>How does the card holder know about IFM and it's facilities?</p> <p>In the card holders own time.</p> | <p>Assurance</p> <p>Not using IFM may be a safer option in the customers eyes</p> <p>That the card works when they arrive</p> <p>If it doesn't work who do they call?</p> |
| <p>That the card works when they return</p> <p>Will I get the same level of service?</p> <p>No Worse Off</p> | <p>What is the incentive to use IFM?</p> <p>Convenience?</p> <p>Savings on card deposits</p> <p>Benefit</p> |

Figure 5: Customer issues /risks

Customer privacy:

Customer Privacy is explored in full in WP2; however, as this directly impacts upon customer trust it is important to discuss it here in D1.3. Essentially, the privacy decisions made within the project must be clear, open and transparent for the customer. The open forums felt that any decisions must be followed through and it is essential to get customer feedback about the decisions made. As highlighted in D1.2, this is the only way to foster shared values and earn customer trust. It is likely that privacy remains a local decision, however, if there is to be an international variation, then there needs to be a definition as to how this will work and be communicated to the customer. The EU IFM organisation must define the responsibilities and operational requirements of this (in essence) trusted service, which keeps the identity, and other data anonymous.

To avoid confusion there must be a single privacy policy which should be clear and made available on the EU Portal.

However we are not sure that a single privacy policy can be defined for EU in the light of the latest comments received from NL. If the need for staying with a local approach is confirmed, WP2 will have to take into account the diversity of the local rules regarding customer privacy.

Other customer issues:

During the workshops and the Forum meeting a number of comments have been recorded which emphasise the importance of this customer area. They are repeated here to again feed into the September workshops:

- *Trust is a feeling, you cannot tell people what to think or want. This requires guidance*
- *When in unfamiliar situations, fare/payment must be easy*
- *Commitment to the customer gives them confidence in use. The example given was of credit card use, in particular reimbursement when any money is stolen, etc. The solutions must be open.*
- *Explain solutions to customers so that they have an understanding of what they are getting and what they can expect – this is more than just information.*
- *Make parties known and be transparent*
- *The customer see what they are getting and get what they expect.*
- *Must have:*
 - *Comfort in transactions*
 - *Combine to tell who they are, name, brand and be clear about what is on offer but also what customers will not get*
 - *When one party is lacking this causes distrust – when one link is missing it will all fail.*
- *This is a different type of Trust, how is this achievable?*

Operator Challenges

In a similar way there exist a number of issues which address the operator's view of EU IFM;

- 1. Why would an operator want to do it now?**
- 2. Why would an operator want to do it in the future?**

And similarly there are a number of sub issues for discussion and presented in Figure 6.

| | |
|--|---|
| <p>Control</p> <p>Will the strange cards work? Ability to implement at their pace.</p> | <p>Assurance</p> <p>A set of rules about removing expired products in order to free space on the card.</p> <p>That their customers will get their level of service in another IFM</p> <p>That the EU IFM will control and impose sanctions</p> |
| <p>Why would the card issuer want to do IFM. Many see the card issuing as an income stream and/or a marketing tool</p> <p>Staff training costs</p> <p>Will there be damage to my brand?</p> <p>No Worse Off</p> | <p>Is there a business case for moving to IFM</p> <p>Benefit</p> |

Figure 6: Operator issues/risks

Relationships

Within the EU IFM environment there are a number of players;

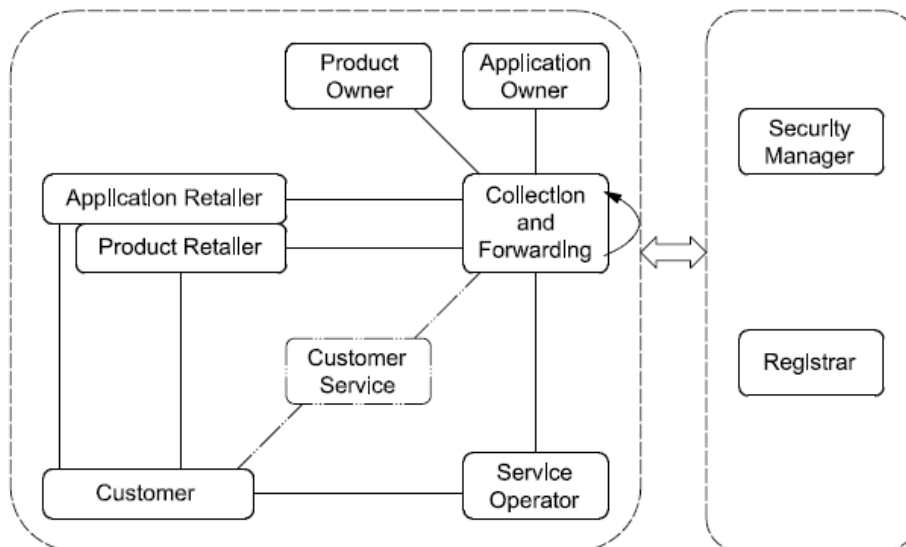


Figure 7: The two IFM domains (operational - Links between operational Entities within the IFMS- and management Entities) (taken from ISO/FDIS 24014-1 Architecture)

Any Trust management model needs to consider the relationships between these players and the functionality of those relationships. Given those definitions then the nature of the relationship can be established which in turn reflects the structure of the EU IFM organisation. For example – are these reflected in membership agreements, licenses or contracts?

In Appendix 3, the first analysis of the relationships has been included, although these are based on the current state of the scenarios and are, therefore, for example purposes only.

Certification and Qualification Process

In many respects any discussion here repeats earlier issues raised, for example:

- Is this media acceptable?
- Will the existing products on the media harm my scheme?
- Will the media still work when it returns home?
- Is the customer profile valid?

The Certification process from the EU IFM organisation must therefore formalise the answers to these issues *and* then monitor that process to ensure conformance.

In defining the process there needs to be some rationalisation as;

- existing schemes have their own certification processes
- Global Platform (which is the preferred approach) defines a composition model for certification of media and applications (this is not only a GP proposal, this is a scheme discussed beyond GP with MNOs, banks, ...)
- And an EU IFM scheme will introduce an international interoperability layer once the EU ticketing application will be rolled out

The composition evaluation scheme that splits the platform (media) from the application is a cross industry process that will take some time to be rationalized and endorsed by the different players. The EU IFM is ready to be part of such a scheme where media (SE) owner are responsible for SE certification and Transport operators (local ones and then EU application owner) will be responsible for transport application validation/certification.

One of the major risk identified so far is the lack of representation in these discussion of a public transport organisation (UITP ?).

Hotlistings and the Associated Rules

Within any single scheme Hotlisting provides an essential part of the scheme security but one that is manageable as the media and product owner are invariably the same people. Adding interoperability brings issues such as;

- When are items blacklisted
- Blacking my product on his card
- Blacking my card whilst his product is still on it
- Why should I handle other peoples black lists when I have large ones of my own.

There has to be a set of rules, a code of practice or contract which lays down procedures, monitoring and the sanctions

Adding an international interoperability only makes this a bigger issue as the implementation progresses which must be discussed by the back office Working Party. For example;

- Local application download and EU profile download : no need to exchange hot list
- EU application with local products : need for black list – what if a PTO black list a EU application which has products for others networks - is it legal ? Should a process be defined for EU application to block only usage for a given network ?
- EU application with EU product: same as above , who can decide to blacklist a EU application ? is it legal to prevent the service across EU if fraud is only detected by one network ?

Conclusion

This deliverable has suggested a simple methodology for the derivation of a Trust Model for IFM. However, the detail of this model will depend on what IFM is achieving, how it achieves it and the responsibilities accepted by each of the players; especially any new EU IFM organising body.

In order to understand this new environment better it is suggested that the workshops in early September consider at least the following areas:

- The scenarios and their implementations
- The customer offering
- The operator challenges
- Relationships including the EU IFM organisation
- Certification and qualification
- Hotlisting and other back office processes

Appendix 1 – Minutes of meetings

Feedback from IFM forum – Breakout Groups 31st March 09

Customer Offering

Trust is a feeling, you cannot tell people what to think or want.

When in unfamiliar situations, fare/payment must be easy

Commitment to the customer gives them confidence in use. The example given was of credit card use, in particular reimbursement when any money is stolen, etc. The solutions must be open.

Explain solutions to customers so that they have an understanding of what they are getting and what they can expect – this is more than just information.

Make parties known and be transparent – again the customer see what they are getting and get what they expect.

Must have:

- Comfort in transactions
- Combine to tell who they are, name, brand and be clear about what is on offer but also what customers will not get
- When one party is lacking this causes distrust – when one link is missing it will all fail.

IFM Application

There are 2 parts to this:

1. Separate IFMs using shared media. This was simplified to the profile issue. Gills is 61 regardless of the country he visits but it is a local, political decision to provide some sort of concession.

Different EU countries have their own way to profile customers, even within a country the process can be different, therefore, we need to know the formal procedures used to profile, such as, where you live, study or just your age.

Within IFM the different schemes will either need to trust that everyone is using the criteria they expect or another process will need to be introduced. Potentially some sort of security profile so that someone can check credentials in another country – this will form part of the security and EU SAM discussions.

There are data issues to be discussed here in terms of how much information needs to be shared between schemes or if in cases of uncertainty the scheme should call the issuer to confirm the status of the traveller.

2. The second relates to the TSM – This is not necessarily on a functional level but there is something to do with attribution and security. More straightforward than between different schemes (?)

Relationships

Considering 2 IFMs –

Cardholders have applications and if they are living and travelling locally, they will have the local application. When going further, they are trusting that the level of [service] (I have behaviour in my notes?) is the same as where they came from.

Application issuers receive new cards and encounter a number of risks – for example, was there damage to my scheme? Were the downloaded applications too big meaning the card can't be used when it returns? What happens if the card is damaged in some way? Who is liable? Will the issuer repair trusting that other schemes will return the favour?

What is the impact of 3rd parties on trust? This requires Interrelations but does this mean bilateral or multilateral agreements? What level of trust is needed here?

The issues of Standards were raised. When a media enters your scheme does everyone trust that it meets 14443? Security measures were raised about schemes trusting each other to operate in the expected way – ie not sending security information part way through a process – I'm not sure this is right.

Contracts – train and airlines have an implied contract, which could be used for recreations of damage and loss.

EU Directives, as with standards, there is trust that these are being implemented.

What are the commercial motivations for participation – this is likely to drive who gets involved.

Branding is an issue – schemes won't get involved if they believe their may be damage to their own brand. This also impact upon the customer as they will not want to put their card into any machine unless they recognise the brand – I'm not sure about this, I stuck my card in loads of different machines in Japan in the hope of getting cash! It is becoming obvious that branding is a key issue to the project.

Competition – there is competition within IFM because it is an open market and therefore there can be trust ...?

Data

Must use ISO Role Model – data depends on roles and who is having data.

They defined the data need and stated that data has a life cycle:

- trip usage
- pricing
- special events
- personal
- management
- application data/downloads
- security for example, keys

They considered what the host and visiting schemes might need but decided that this was part of the business rules!

If the security rules are agreed this must be applied to trust. If this relates to role model then there is no change – I don't get this

IFM WP1 – Trust Model Workshop 2 – 6th April 2009

Attendees:

Gilles de Chanterac (GdC)
Joseph Lutgen (JL)
Johan Vanieperen (JVa)
John Verity (JVe)
Peter Stoddart (PS)
Hannah Bryan (HB)
Eric Sampson (ES)

AGENDA

The purpose of the meeting is to:

- Begin to develop a Common Methodology for Trust
- Discuss the findings so far, feedback from IFM Forum and questions raised
- Develop credible scenarios and a vision for Trust
- Establish the contents of the EU SAM

LOCATION: Newcastle University, Cassie Building, Room 1.01

10:00-10:30 Welcome and Coffee

10:30 – 11:00 **Introduction:**

- The story so far
- Work left to deliver (D1.3 and 1.4)
- Format for the day
- Feedback from the Review (with discussion)

11:00-13:00 **Discussion 1: Forum**

- Feedback from the Forum breakout group work
- Key questions arising from the Forum
- Discussion regarding key questions, relation to each WP and impact upon Trust

13:00-13:30 Lunch with guests from Nexus (NE PTO)

13:30-15:00 **Discussion 2:** development of Common Methodology for Trust (feeds into D1.3)

- Broad Vision
- Scenarios

15:00-15:30 **Final discussions**

- D1.4
- Round up and next steps

Introductions

ES started the workshop by welcoming our guests

Page 25 of 38

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

HB introduced:

- The story so far
- Work left to deliver (D1.3 and 1.4)
- Feedback from the Review (with discussion)

Discussions followed and will be described below:

Description of Deliverables

D1.3 - report on the follow-up workshop to explain and disseminate the agreed Common Methodology for preparing a Trust Management Model (expected month 18)

This deliverable should be a set of requirements for the trust model but not any of the detail. The deliverable is a methodology subsequently to be adopted for this IFM Scenario. The conclusion of the methodology developed, should it be followed, will be to arrive at the Trust Model itself which will be expanded in IFM2.

D1.4 – report on the common requirements for an EU-SAM to support the Trust Management Model (expected month 20)

This will be a functional document about the ‘EU IFM Security System’ This will develop the security procedures that are described in D1.3 and will work very closely with the developments in WP3.

Common requirements in both D1.3 & D1.4 will include the security discussion, for example, hardware and security measures needed. What objects and services need protecting, etc. A risk assessment is required in order to identify the residual Trust. The qualification process, i.e. how schemes join, should also be discussed – can you join by just having the specified equipment or do you need to follow the Trust Model methodology?

The EU Reviewers wanted D1.3 and D1.4 to consider schemes wider than the consortium – this will be incorporated but no more than a paragraph per scheme.

Discussions about Trust Concept

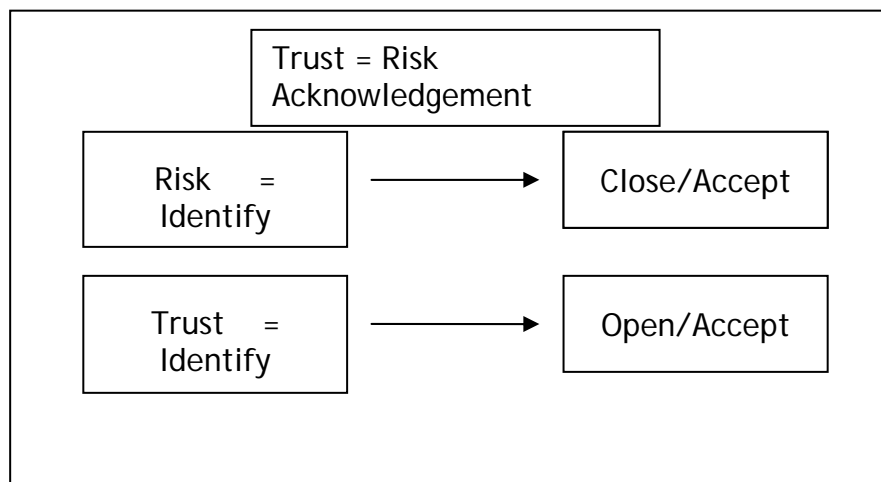


Figure 1: Concept of Trust

There is potential that following the method in D1.3 there may not be much Trust left but for whatever level of Trust, the process for reaching this level must be shown.

Validation of Trust Concept for IFM

This can be achieved using both a top down and bottom up approach. WP1 would be top down by identifying the initial Trust requirements in D1.3 and the other WPs would be bottom up as they look at each requirement, ensure that their WP is addressing the issues and therefore any gaps in the middle can be found.

In addition to this we will use the relevant standards. During the meeting ISO 27001 was looked at in detail – there are a series of headlines for different objectives and controls in a general IT system, these were used to identify any gaps that may need addressing by the other WPs. This is described later.

Scenarios from WP3

The discussion in WP3 has highlighted a set of scenarios for the steps within an IFM. It was agreed that WP1 should look at each scenario within D1.3 in order to understand the trust requirements, the impact upon the other WPs, and develop the methodology. The focus will be upon steps 1&2 (as they are within the scope for this project). The subsequent steps will also be addressed in order to ‘future-proof’ the model, with issues raised for each additional step.

Step 1: Download local Application

Schemes must trust media that has not been created by them. We should look to ITSO as cross-acceptance of media exists in their model.

Focus needs to be on making life easier for the customer.

In Oyster the process is a pyramid where lower levels receive their instructions from the top level. This is not the case in an IFM, it is more like the banking system where there is no top level but only trust in the system. Something similar should be attained for Step 1.

Step 2: EU Application

For Step 2, more is needed in addition to step 1 as when common access to the application is available, schemes will be able to see the secure keys to the media.

Step 3: Common Portal

For step 3, there must be agreed conditions for accepting media and the model must stipulate the rules and the mechanism for trust, for example, a logo within the media that the point of sale will recognise and trust. At this point no data will be exchanged or shared.

Step 4: EU Products

Step 5: Only EU Application

There will be an overlap of schemes in different steps, for example, some schemes will be in step 1, others may be in step 4. This is a political decision as when move between steps and

the schemes can still work together but will be able to do different things. This needs to be kept clear for the customer. For example, for step 2 ticket machines will need to be modified, say for languages, at this stage the change within the local infrastructure required between the steps is not formulated, it is likely to change from one scheme to another.

Use of the profile

PS raised an alternative implementation strategy for discussion by the other WPs along the following lines.

“ As I understand it the concept is that a customer will have the EU profile added to his card before he arrives (by using the portal). This does mean that every country that wishes to participate in IFM must change every ticket machine to read the EU Profile. I do see this as not only a costly exercise but an exercise that really is a showstopper – why would operators want to pay for this when the alternative is to give or sell their card.

What if the portal were not to add the profile but to create the specific product for the relevant country that would serve the same purpose?

It means that the planned stages 2&3 need to be changed over and it does not stop an EU profile being defined in the later stages but it does mean the user countries do not have an upgrade issue”

ISO 27001 – Security Management Standard

Security policy

Trust that there is a policy that is regularly updated and everyone is implementing it.
Is **WP5** is making recommendations for this?

Organisation of Information Security

Commitment, coordination, internal and external relationships

Asset Management

Responsibility of the manager to keep an inventory of assets and rules of acceptance
Information Classification – definition of confidential and non-confidential information –
WP4?

Human Resources

Roles and responsibilities, manager responsibilities – feeds into **WP5 and Back office**

Physical/Environment

Step 1: Card is secure – **WP3**

There is a lot of trust in the Point of service and ensuring it deals with the media, etc. in a secure way – **WP3?**

Communications and Operations Managements

- Procedures
- 3rd Party

- Trust in Back office – **WP5**
- System planning and acceptance to ensure building something that is properly accepted before use
- Media protection – Trust the level of security in original media, therefore it cannot corrupt/interfere with your scheme – **WP3**
- Media Handling - Although the media is secure, the chip must be readable, for example, the chip number, etc. **WP3** must deal with this criteria, for example, how the customer gets the media and the process to Trust for getting certificates onto the media. Core of global platform. Apparently this already exists – where? Also Trusting people will not download public keys?
- Backup – BtoC recreate card
- Network security – passing public keys and data – **WP5**
- Monitoring – Trust each transaction step is monitored
- e-commerce – Steps 3 and 4 – if there is a fee for downloading?

Aside – schemes extending – for example, in France all schemes have the same applications and data model but they have different keys. They could merge but there is a question of trust and image.

Access Control

- Business, users access and responsibility, network access control (will come out in D1.4), mobile computing access – each needs addressing in **WP3**
- What trusted entities of TSM? What are the common rules and requirements to ensure Trust? Is there a shift in balance towards a more regimented/prescribed process?

Aside –

We should look at EU Directives on E-signatures (JV to send), which describes how Trust from one member translates to another – there is a list of around 20 trusted partners – this can feed into D1.4

Set of Rules – who owns the application, governs, maintains and updates it?

Use Gilles' Chaining steps diagram – the objective of the project is not EU IFM application (in the diag.) but interoperability.

- Info systems development and maintenance
- Security regulations for introducing new systems. Trust always covers security and maintenance and development must not reduce security
- Trust that the correct process is in place to ensure measures and outputs are lostless
- Cryptographic – if anything goes wrong it must be recognised. Data on the card must be secure, including the mechanism for filing – source data?

Technical vulnerabilities – Trust is in sharing information about security weaknesses and passed around the network in a timely manner. Evidence must be collected about security breaches

Could introduce some sort of security forum for adoption BP in security

Incident Management

Trust in the process for reporting and managing incidents – highlighted earlier the need for common procedure to ensure the ‘show goes on’.

There needs to also be some sort of incident response rules and regulations (for example, if you do not use the stated equipment, etc. you are liable) – **WP5?**

Business Continuity

Trust EU IFM organisation has business continuity in place – **WP 4/5** dealing with this
Plans must be tested

Compliance

Legal requirement on schemes to follow standards, directives, privacy and technical rules, public specifications to comply with IOPTA, etc.

Trust is that this has been done as they are members or does there need to be some sort of audit considerations?

Therefore must consider: 1. legal requirements 2. Audit

Checking procedures – Step 2 with exchanging data

Trust will not be settled by verifying everything but this is a procedure, which if followed results in trust. Should each IFM do their own checking?

Discussion about the feedback from the Forum

IFM Application

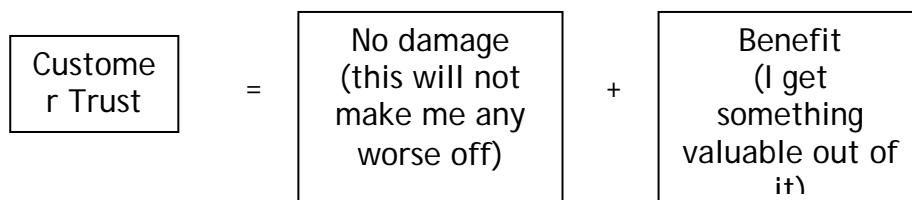
This will maintain a profile – the profile is undefined as yet

The trust is in this profile and therefore there is the potential to be defrauded. What are the criteria which must be forwarded to everyone for fare criteria?

TSM – Application loader – manages the loading – what is the relationships between IFMs and TSMs? This is a manager under special conditions, a 3rd party who deals with the handing out of public keys and assigns the trusted symbol within the media. This is covered in D3.3. This will be investigated in D1.4 – the security system should define the criteria for accepting a TSM and who should trust the TSM.

Customer Offering

This is a different type of Trust, how is this achievable?



No damage

Relates to managing expectations

Working out responsibilities for example, application owner will change applications from old media when a customer updates with media, and blacklist the old media. The customer must initiate this.

This introduces new use cases – for example, when the media owner knows nothing of the applications stored on the media

Benefit

1. I can use my own media (therefore saving 3Euros deposit for each new media)
2. I can potentially obtain concessions, etc, due to my stored profile

At the beginning there is no product only the application owner of the profile

- who is the application owner and what are the rules? How do you build an EU Application owner with embedded Trust?
- Create a Trusted entity/organisation for this?
- There is a governance Question – refer to E-signature directive

Data

There could be problems with capacity – need a process to manage this.

The cardholder deals with this and has choice to delete applications? If so, the customer must know what the applications are and have the choice as to how to deal with them.

Need to identify the basic requirements and what are just nice to know.

Format for D1.3

| TRUST | Step 1 | Step 2 |
|-------------------------------|---|---|
| B to C and C to B | Transparency (warm) Cold | Value Cold |
| B to B | Media Governance Technical and legal (Cold) | Application Governance Technical And legal |
| Plus (detail will be in D1.4) | Technical Security | Technical Security |

Some further questions for other WPs

- Applications cannot interact with other applications or with ticket machines eg worms from the card?
- What is the methodology of circulating the media keys?
- Is the profile accessed by the non host application just once or every time?

Appendix 2 – ISO 27001 – Security Management Standard

ISO 27001 provides a series of headlines for different objectives and controls in a general IT system, these can be used to identify EU IFM risks and the following have been included purely as examples, highlighting which WP it relates too;

Security policy

Trust that there is a policy that is regularly updated and everyone is implementing it. **WP5**

Organisation of Information Security

Commitment, coordination, internal and external relationships - **WP1/2/5?**

Asset Management

Responsibility of the manager to keep an inventory of assets and rules of acceptance
Information Classification – definition of confidential and non-confidential information –
WP4?

Human Resources

Roles and responsibilities, manager responsibilities – feeds into **WP5**

Physical/Environment

Step 1: Card is secure – **WP3**

There is a lot of trust in the Point of service and ensuring it deals with the media, etc. in a secure way – **WP3?**

Communications and Operations Managements

- Procedures –**WP4**
- 3rd Party – **WP4**
- Trust in Back office – **WP1/5**
- System planning and acceptance to ensure building something that is properly accepted before use – **WP4**
- Media protection – Trust the level of security in original media, therefore it cannot corrupt/interfere with your scheme – **WP3**
- Media Handling - Although the media is secure, the chip must be readable, for example, the chip number, etc. **WP3** must deal with this criteria, for example, how the customer gets the media and the process to Trust for getting certificates onto the media. Core of global platform. Apparently this already exists – where? Also Trusting people will not download public keys?
- Backup – BtoC recreate card – **WP3**
- Network security – passing public keys and data – **WP5**
- Monitoring – Trust each transaction step is monitored – **WP4**
- e-commerce – Steps 3 and 4 – if there is a fee for downloading – **WP4?**

Access Control

- Business, users access and responsibility, network access control (will come out in D1.4), mobile computing access – each needs addressing in **WP3**
- What trusted entities of TSM? What are the common rules and requirements to ensure Trust? Is there a shift in balance towards a more regimented/prescribed process? **WP3**
- Info systems development and maintenance – **WP5**
- Security regulations for introducing new systems. Trust always covers security and maintenance and development must not reduce security – **WP3/5**
- Trust that the correct process is in place to ensure measures and outputs are lossless – **WP3/5**
- Cryptographic – if anything goes wrong it must be recognised. Data on the card must be secure, including the mechanism for filing – source data? – **WP5**

Incident Management

Trust in the process for reporting and managing incidents – highlighted earlier the need for common procedure to ensure the ‘show goes on’.

There needs to also be some sort of incident response rules and regulations (for example, if you do not use the stated equipment, etc. you are liable) – **WP4/5?**

Business Continuity

Trust EU IFM organisation has business continuity in place – **WP 4/5?**

Compliance

Legal requirement on schemes to follow standards, directives, privacy and technical rules, public specifications to comply with IOPTA, etc.

Trust is that this has been done as they are members or does there need to be some sort of audit considerations?

Therefore must consider: 1. legal requirements 2. Audit – **WP4**

Appendix 3 – Relationships

IFM Scenarios – Developed by WP3

The following document sets out the scenario steps which have been developed by WP3 and the subsequent impact of each step on the players defined in ISO-24014 (part 1). Extra players have been added to take into account the wider relationship between schemes in the form of the IFM registrar and the Media Owner.

The relationships defined below each step are cumulative and therefore not repeated as the scenarios develop.

Step 0 – within an existing IFM

| | | | | | | | | | |
|------------------|-------------|-------------------|----------------------|---------------|------------------|------------------|------------------|-----------|--|
| Customer | Media Owner | Application owner | Application Retailer | Product owner | Product retailer | Service operator | Security manager | Registrar | |
| <i>All local</i> | | | | | | | | | |

Step 1a – Download Local Application

Scenario: A French Customer wishes to travel in the UK and upload an ITSO application onto their French card

| Customer | Media Owner | Application Owner | Application Retailer | Product owner | Product Retailer | Service Operator | French Registrar | UK Security Manager | UK registrar |
|--|-------------|---|--|---|------------------|------------------|------------------|---------------------|--------------|
| French | RATP | ITSO | National Express (as an ITSO licensee) | National Express | National Express | National Express | RATP | ITSO | ITSO |
| Customer gets the media from the domestic IFM | | | | | | | | | |
| | | Customer downloads the UK application from local retailer (in field or remotely)* | | | | | | | |
| | | | | Customer buys UK product from UK product retailer (in field or remotely) and uses it on a train | | | | | |
| | | French Media Owner requires to know which applications are loaded on the media | | | | | | | |
| <p>UK Security Manager requires media to be guaranteed as safe and that Card security works and application is independent, etc * requires ticket machines in the UK to be upgraded to act as perso devices or a new process has to be devised.</p> | | | | | | | | | |

Step 1b– Download Local Application

Scenario: A French Customer wishes to travel in the UK and upload an ITSO application onto their French card

| Customer | Media Owner | EU PORTAL Owner | UK Application Owner | Application Retailer | Product owner | Product Retailer | Service Operator | French Registrar | UK Security Manager | UK registrar |
|--|-------------|--|----------------------|---|------------------|------------------|------------------|------------------|---------------------|--------------|
| French | RATP | EU Co. | ITSO | National Express (as an ITSO licensee) | National Express | National Express | National Express | RATP | ITSO | ITSO |
| Customer gets the media from the domestic IFM | | | | | | | | | | |
| | | Customer downloads the UK application from application owner via the EU portal | | | | | | | | |
| | | | | Customer buys UK product from UK product retailer (in field or remotely) and uses it on a train | | | | | | |
| French Media Owner requires to know which applications are loaded on the media | | | | | | | | | | |
| UK Security Manager requires media to be guaranteed as safe and that Card security works and application is independent, etc | | | | | | | | | | |

Step 2 – EU Application

Scenario: A French Customer wishes to travel in the UK and upload their EU profile before travelling - Add profile in France, use in UK

| Customer | Media owner | Domestic application retailer | EU- Application Owner | EU- Application Retailer | UK Application owner | UK Application retailer | Product owner | Product Retailer | Service Operator | UK Security Manager | UK registrar |
|--|-------------|-------------------------------|--|-------------------------------|--|-------------------------------------|------------------|---|------------------|---------------------|--------------|
| French | SNCF | RATP | To be defined : e.g; ETAP | RATP & ITSO as ETAP licensees | ITSO | National Express (as ITSO licensee) | National Express | National Express | National Express | ITSO | ITSO |
| C gets the media from his domestic IFM | | | | | | | | | | | |
| | | | C downloads the EU-application from portal) | | | | | | | | |
| | | | C export the profiles he wishes to share into the EU-App | | | | | | | | |
| | | | | | C downloads the UK appl from UK retailer (in field or remotely) | | | | | | |
| | | | | | UK App retailer imports the profiles from the EU-application into the UK application * | | | | | | |
| | | | French Media Owner requires to know which applications are loaded on the media | | | | | | | | |
| | | | | | | | | C buys product from UK product retailer (on field or remotely) and uses it on a train | | | |
| <p>UK Security Manager requires media to be guaranteed as safe, and trust with EU-App security manager UK Product owners need to trust the imported data.</p> <p>Note: * Additional Trust issue – French UK will develop facilities to READ the product on all equipment. Trust element that the enormous expense of developing these facilities will be forthcoming.</p> | | | | | | | | | | | |