

**IFM**
PROJECT
INTEROPERABLE FARE MANAGEMENT

Collection of Information on Existing Trust Management Models

Deliverable 1.1

February 2009

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

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

Hannah Bryan

Peter Stoddart

Newcastle University

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

Table of Contents

0	Executive Summary	4
1	Introduction	5
2	Description of Process	6
2.1	IFM - Best Practice Trust Management	6
2.2	Response to the Questionnaire	7
2.3	Existing Trust Models	9
2.4	Workshop 1	9
3	Additional issues	11
3.1	Precursors	11
3.2	Definition of a Trust Model	11
3.3	Level of Trust Model	12
3.4	Risk and Trust	12
3.5	Pre-requisites for a Trust Model	14
4	Work Package 1 Future Implementation Plan	15
5	Additional work	15
6	Conclusions	16
	Appendix 1	17
	Appendix 2	30
	Appendix 3	36
	Appendix 4	40

0 Executive Summary

The first Work Package (WP1) for IFM has the objectives to identify the Trust Models already in place within the consortium, and to understand and recommend the process to be adopted in the production of an EU IFM Trust Model for existing members. This first deliverable is concerned with collating data about all the schemes within the project and their existing Trust Models. The initial task for WP1 was to identify the different ways in which the consortium members approach trust and to determine their level of agreement. The subsequent tasks for this WP will investigate by comparing existing Best Practice from other business sectors with the findings from this report and to establish recommendations for a Trust Model. Alongside this, meetings will be held with members of the consortium to consider the Best Practice for an IFM.

In order to obtain the results documented in this deliverable, a questionnaire was developed to analyse existing risk, mitigation and contents of the Trust Models, and sent to all consortium members. The results from this questionnaire provided some understanding of main risks and mitigations to the schemes; however, it did not provide a clear understanding of the existing models which may have been the result of a difference of opinion for the definition of a Trust Model. This suggested that an alternative methodology should be employed to enable a more rigorous and in depth understanding. The follow-on methodology was to carry out a workshop with the relevant members of the consortium in order to clarify Trust related questions, provide a greater understanding of the existing Trust Management Models and to agree an overall definition of Trust.

In addition to this alternative approach, it has become apparent that in order to recommend and produce the methodology for an EU IFM Trust Model, the outputs of the other Work Packages will be essential. This is because the shape and delivery of the Trust Model is ultimately dependent upon the shaping of the whole project, such as the system, architecture, and nature of transactions, and the technical outcomes.

The result of this process has been described in this report, with the issues and challenges for the future phases highlighted.

1 Introduction

The Interoperable Fare Management (IFM) Project is an EU FP7 funded project which aims to reduce the barriers to interoperable ticketing between cities, regions and, ultimately, countries making public transport more user-friendly. The objective is to avoid the establishment of enduring isolated national solutions and to define roadmaps leading the way toward European and wider interoperability. The project aims to do this by facilitating seamless accessibility to different public transport networks through a shared style of contact-less media which can be used for multiple transport products.

The IFM Project aims to be a European wide initiative dedicated to the establishment of attractive public transportation with modern fare management which is safe, reliable and comfortable for both users and operators. Once achieved, this may serve as a model for many further countries outside of Europe faced with the need to strengthen the use of public transport. However, this type of initiative creates a number of challenges as different participating countries seek to exchange data and/or money, and to share services or infrastructure. There are potentially many risks to each participant, which may not have been anticipated, therefore, it is essential to have a Trust Model. This Model serves as a framework for each prospective participant and provides guidelines for the level of trust and authentication required for each player. As part of this Work Package (WP) there are a number of tasks associated with achieving the following aims:

- Identifying current Trust Management Models, and Best Practice
- Identifying the Trust Management Model in support of EN24014
- Defining the outline of an EU-IFM Management Model
- Defining the Trust Requirements for an EU-SAM

This initial deliverable by WP1 is aimed at investigating what exists in terms of Trust Models amongst existing regional or local IFM schemes who are participating within the project. It also records and discusses some of the elements which may be useful to the subsequent deliverables for WP1 and the other WPs

2 Description of Process

2.1 IFM - Best Practice Trust Management

The process as defined in the original project brief for the development of the Trust Model was as follows:

1. Circulation of the questionnaire to partners for them to comment on and verify;
2. Subsequent questionnaire circulated to partners for distribution and completion by the parties they feel relevant;
3. Compilation of results from the returned questionnaires;
4. Initial results delivered back to respondents to enable them to update any accidental omissions;
5. Compilation of Inventory report of existing Trust Management Models;
6. Study of published Best Practice approaches in other relevant business sectors;
7. Workshop to disseminate the results of the questionnaire and study to discuss the development of the EU-IFM and EU-SAM.

2.1.1 The Questionnaire

In order to achieve the objectives, stated in the project brief, of understanding the existing Trust Models within the consortium, task 1.1 required WP1 to prepare and circulate a questionnaire. The purpose of the questionnaire was to understand, from those with practical experience, the risks and mitigations related to establishing an IFM System, and to create an inventory report on existing Trust Management Models within the consortium. Consequently, it was intended that the responses would be used to draft a Trust Model which covers the risk areas that are not and cannot be mitigated by the parties involved.

In compiling the questionnaire, the project wished to consider both the elements of a scheme and the interrelationship of scheme players as defined in EN ISO 24014-1:2007. As a basis for the questionnaire, the use cases from this standard were used. Respondents were asked to consider each use case, the perceived risks and, where relevant, the mitigation. As part of this process, respondents were also asked to provide copies of their existing Trust Models. A copy of this questionnaire, with the results, can be found in Appendix 1.

The results from the questionnaire would then be analysed and sorted into 3 categories:

- Risks which are actively mitigated by all participants
- Risks which are mitigated by some but not all participants
- Risks which no participants are mitigating

It had been anticipated that this latter category, and perhaps some of the previous category, would define the Trust Model and lead to the development of the EU-IFM

Management Model, and defining the Trust Requirements for an EU-SAM as outlined in WP1.

It was anticipated that the process above (steps 1-7) would generate a comprehensive list of risks and possible mitigations. However, once steps 1 to 4 were complete it became apparent that sufficient information, required for steps 5 and 6, was not available. As a result it was decided that a more interactive approach, in the form of a workshop with predefined discussion topics, would stimulate a more in depth debate with the other working parties.

2.1.2 The Workshop

The process adopted to stimulate debate was to propose a definition of the Risk/Trust spectrum and to identify a number of overarching project criteria which could be confirmed or negated. These would include a number of questions relating to the scope of the project, which would pull together the views and approaches of each of the other WPs. The results from this workshop could then be used to inform this deliverable and shape the output of future deliverables.

A copy of the presentation used at the workshop is included as Appendix 2 of this report.

2.2 Response to the Questionnaire

Three of the consortium answered the questionnaire. The responses to the list of use cases were given as a variation on risk level (High, Medium, Low), if the risk was mitigated and if it was included in their Trust Model. Nearly all risks in the questionnaire were mitigated, suggesting that schemes are aware of the risk status, however, it was also stated that nearly all risks were in their existing Trust Model, yet no scheme provided a definitive Trust Model. This suggests that each of members may not have a specifically defined Trust Model or may have a definition which differs from the one stated within this WP. This methodology, therefore, provided little input for a Trust Model. However, it did highlight which factors were of the highest risk and, therefore, should be of the highest priority.

There were two risks which all of the respondents stated were of the highest threat to an IFM. These were:

Q1.2	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
Q6.2	The generation, distribution, storage and termination of IFM security keys.

Table 1: Highest Risk for all respondents

There were also a number of risks where two out of three of the respondents described the threat as high. These were:

Q1.1	Each Organisation which wants to participate in the IFM shall agree to abide by the Set of Rules.
Q1.3	Each Application Specification and Template to be brought into the IFMS shall meet the IFM requirements. Proof of this is given by checking this Application Specification and Template against a Set of Rules.
Q2.1	A unique identification is given to each Organisation.
Q3.4	Termination of Application Template by request of the IFM Manager.
Q4.3	Termination of Product Template on decision of the IFM Manager. (Forced termination)
Q6.1	The monitoring of the processes and data life cycle (generation of data, movement of data, storage of data, use of data, changes of data and deletion of data) shall guarantee the secure operation of the IFMS, providing the required trust by the customers and operators concerning handling and protection of assets and sensitive information.
Q6.3	Provision of a security list by the Security Manager.

Table 2: Highest risks for 2 out of 3 of the respondents

There was only one risk which all of the respondents stated was of a low threat to an IFM. This was:

Q4.7	Termination of Product by request of the CUSTOMER.
------	--

Table 3: Lowest risk for all respondents

Of the use cases presented to the respondents, nearly all the risks were mitigated by each participant. However, the following were not mitigated by all the participants and should be discussed during later phases of this WP:

Q 2-3	A unique identification is given to each Application Template.
Q 2-5	A unique identification is given to each Product Template.
Q 5-2	SERVICE OPERATOR checks and collects the data of a Customer Medium using the public transport service.
Q 5-5	The PRODUCT OWNER performs the clearing procedure and distributes the results to relevant Entities

Table 4: Risks which have not been mitigated by all respondents

2.3 Existing Trust Models

As part of the task the respondents were asked to supply their existing Trust Models if they have one. Only one scheme had specifically generated a written Trust Model. This was ITSO and the model is included as Appendix 3. The other respondents in acknowledging the risks may well have elements of a Trust Model but these may be found in their existing Contracts, Risk Models, Licences or Scheme Rules.

However, it can be argued that this ITSO document in itself is not a pure Trust Model as it contains mitigated risks. It does, however, demonstrate that even where a risk is mitigated there may still be some elements of risk and, therefore, residual trust required. For example;

Issue	Risk Assessment	Trust Model	ITSO Mitigation	Residual Trust
Certification of Equipment and Software used	Products can be written to or modified.	Operators will only use ITSO Certified equipment and software and will audit to verify that it is used unaltered	ITSO Spec part 3 ITSO certify equipment for use.	That ITSO certification is adequate
Security of ISAM	ISAM is compromised	CLEF accreditation has addressed all current security threats	ITSO Spec Part 7,8 CLEF is a snapshot and requires repeating after ISAM changes	That CLEF is adequate
Message Handling	Messages are not passed to their intended recipients	HOPS will pass on all 'not-on-us' transactions	ITSO Spec part 4,6,9 ISAM generates secure message for each transaction and will not delete them until secure acknowledgement received.	That players do their part

Table 5: Examples where Residual Trust is required

2.4 Workshop 1

As the questionnaire did not reveal all the information desired, WP1 then sought a workshop with the other WPs to discuss a number of key questions which would move the process forward and begin the process of understanding what a Best Practice IFM Trust Model should include. In order to do this, questions regarding the shape of the overall project were very important as this will affect the level of trust required. The discussion section which follows distils the conclusions of this workshop in relation to the key questions asked, and then suggests a variance in the deliverables and tasks for WP1. The questions were as follows:

1. Are there no Trust Models?
2. Is the Project considering only media interactions (and not product)?
3. What cards is the project considering?
 - Scheme cards
 - EMV
 - IFM card
4. Is there a need for an EU IFM standard or specification, for example, for:
 - Media types?
 - How to identify a product?
5. Is there a need for a set of club rules, for example, for:
 - Permissions to delete (and inform)?
6. Is there a need for a key management service?
7. Is there a need for Brand Management?
8. Is there a need for certification, for example, for:
 - Media?
 - Terminals?
 - Methodology, for example, Process?
 - Acceptability of other certification, for example, EMV, ITSO, VDV?

The discussion resulting from these questions have been categorised and were as follows:

a. Definition of a Trust Model (Q1)

As it was clear that each of the schemes have a different approach to trust, it was resolve that a definitive definition for an IFM should be agreed. There were a number of definitions discussed, again reflecting this spectrum of risk/trust. WP1 has adopted the original project definition for future work on their deliverables. This is **'A statement of residual risks that need to be accepted between system Operators'**. As discussed earlier, this should be expanded to include the concept of **'residual trust'**.

b. Scope of project- interoperability (Q2)

There are two equally valid definitions of interoperability:

- Media from one scheme used in another
 - Interoperable media
- Products being used or retailed between schemes
 - Interoperable products

Other WPs have suggested that the scope of the project at this stage does not include the latter. However this would appear to contradict the objectives quoted within the WP1 work definition; **'IFMS offer an open system allowing trusted transactions to be made between systems'**.

WP1 now understand that interoperable products are out of the scope of this project. WP1 believe that there will still be operational data which must be exchanged (as against transactional data). The infrastructure and environment for this exchange must be defined and the subsequent risk/trust issues

identified.

c. System Architecture (Q3, 4 & 6)

These questions cannot be divorced from the infrastructure and operational methodology being proposed by the other WPs. This would include a common download and security policy, which needs to be agreed by the other WPs from which a Trust Model can be defined.

d. EU IFM Scheme rules (Q5, 7 & 8)

WP 4 will define the scheme rules and the commercial structure and again the risk/trust spectrum will follow. In addition there is a piece of work to be done to define the EU IFM brand and the associated rules.

3 Additional issues

Whilst researching this deliverable a number of items were discussed which WP1 would like to record for future use in the following sections:

3.1 Precursors

Trust is an essential part of an IFM open system as partners must agree to trust each other on an equal level to enable transactions to take place and the system to succeed. Thus, a full understanding of the IFM system, architecture, nature of transactions and the research being addressed in each of the WPs must be taken into consideration and used to inform the research, conclusions and recommendations made as a result of the WP1 tasks. Each of the WP outputs will be considered in terms of impact upon trust in addition to findings from tasks 1.1, collection of information on existing Trust Management Models, and 1.2, processing of questionnaire responses.

At this stage it has been agreed that transactions will be limited to the development of a common EU-Application, allowing the status (such as age if a concession is required or language preference) of the individual to be shared between IFM members and products from member IFMs to be uploaded to the card prior to travelling to the country of choice.

3.2 Definition of a Trust Model

The Trust Model definition within the IFM project WP1 description is;

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

This reflects the view that Risk and Trust are the opposite ends of a spectrum. However to define the risks, the spectrum (project) must first be defined including the method of operation. Having done so then the risks may be mitigated either through the technology used or by legal agreements such as membership

agreements, operating licenses or contracts.

WP1 therefore suggest that their work and later deliverables can only be finalised in conjunction with and slightly behind the outputs from the other WPs. This is supported by the definition of the place of the Trust Model by ITSO, who suggest the following;

“The Trust Model works alongside the ITSO Business Model, the ITSO Physical Model and the ITSO Data Model.”

Within the IFM project each of these models is the subject of other WPs.

3.3 Level of Trust Model

The Trust Model within IFM must work on a number of levels and reflect not only the numerous B to B relationships but also the B to C offering - although perhaps in the case of IFM it would be more correct to describe this as the C to B trust model. The following are examples of these levels (and not meant to be an exhaustive list);

- End user expectations (customer proposition)
- Scheme to scheme
- Operators (and other players)
 - o Operational
 - o HMI
 - o Transactions/data
- IFM organisation itself
- Status providers

3.4 Risk and Trust

Continuing this discussion on the spectrum of risk/trust we can perhaps better illustrate this with two diagrams. In the first we have illustrated some typical risks based on external and internal attacks, and also shown a basic schematic of the operation.

Scheme Model

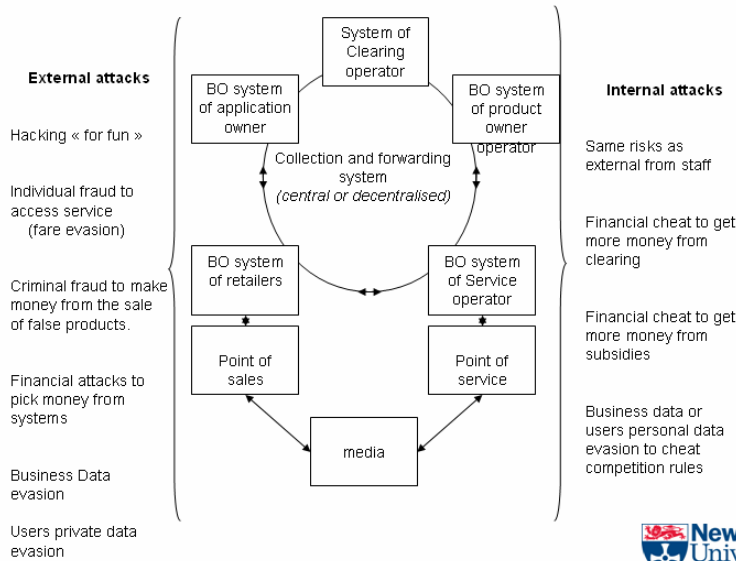


Figure 1: Risks related to players within a scheme

We have picked 3 risk examples to illustrate the spectrum;

- Hacking into the system
- The media itself
- Financial cheating to gain more subsidies eg Driver records more passengers than actually travelled

Each of these has a method of mitigation which may be applied, with a varying degree of mitigation;

Risk	Mitigation	Mitigation level
- Hacking into the system	Firewall	99.99%
- The media itself	Card security level	80%
- Financial cheating to gain more subsidies	Random audits	25%

So in essence there remains a (varying) degree of trust;

- trusting the firewall
- trusting the cards security
- trusting the driver

This type of element is defined as 'residual trust' within this project.

Risk or Trust

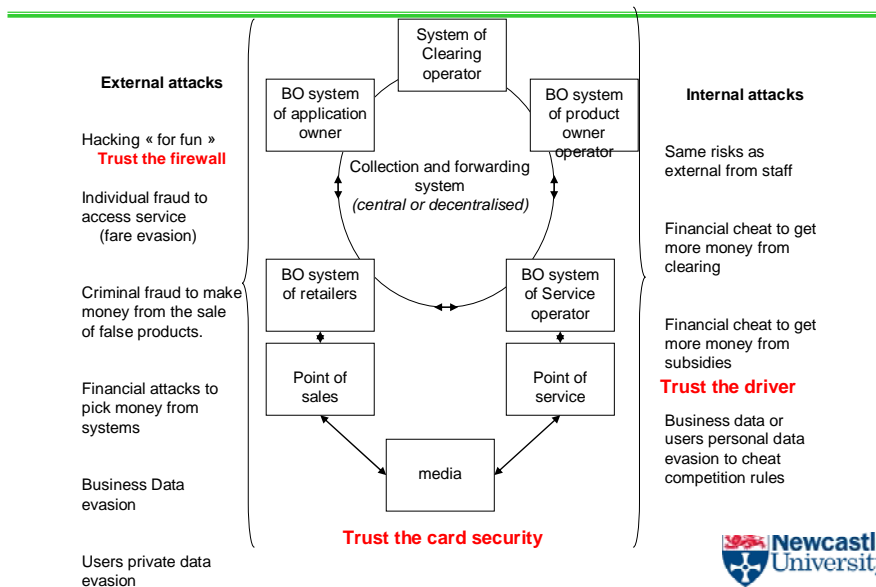


Figure 2: Residual Trust

The level of trust within a scheme is a commercial decision for that scheme. Between two schemes it becomes a contractual arrangement. Within an IFM, one to one contracts become untenable due to the volume and so some alternative must be found in the form of 'club rules', whether these be, for example, a central IFM contracting body, with licenses, or a membership agreement. Before the Trust element can be defined, the business model to be adopted must be partially designed.

3.5 Pre-requisites for a Trust Model

Whilst the Trust Model itself should include a list of unmitigated risks there has to be an understanding of the role of the Trust Model - WP1 has termed these the pre-requisites. These pre-requisites may well include some generic overarching trust issues that sit at a higher level than the project itself. Some examples of these pre-requisites are;

- That the security regime (eg 3DES) remains industry Best Practice;
- That Global Platform continues to be the acceptable industry standard;
- That each and every player within the scheme can be identified and each adopts the roles within the EU standards;
- That the Trust Model itself is openly published and adopted by the players;
- That a set of rules pertaining to the operation of the IFM scheme is agreed and kept in place by a contractual arrangement such as a licence, contract or membership agreement. Such rules would cover procedures such as hot listing, deleting card entries to create space, informing the card owner of changes to the card.

4 Work Package 1 Future Implementation Plan

The deliverables, as defined in the original IFM Project brief, which follow this report (deliverable 1.1) are:

- 1.2 Report on the commonality between approaches and compare to published Best Practice in other relevant business sectors
- 1.3 Report on the follow-up workshop to explain and disseminate the agreed Common Methodology for preparing a Trust Management Model
- 1.4 Report on the common requirements for an EU-SAM to support the Trust Management Model

There are elements of these deliverables which have changed as a result of this report and the output of the other WPs as the overall objectives have been more clearly defined.

Deliverable 1.2 has not changed as this can be achieved given the results to date.

Deliverable 1.3 will require WP1 to shadow each of the other WPs to understand their output and its effect on the Trust Model. Following this a Workshop will be organised to disseminate, test and agree the Common Methodology.

Deliverable 1.4 will depend upon the system architecture as defined by WPs 3 and 4. A recent workshop, held by WPs 3 and 4, suggested that an EU-SAM will only be required if there is to be a common EU-application. WP1 will await the outcome of these discussions and redefine the deliverable, if necessary. The common definition for EU-SAM which will be used throughout this project is: 'Trust services to be set up in order to ensure the shared use of Transport Applications across different IFM schemes'.

The vision for this project and beyond as created by WPs 3 and 4, during their workshop on 18th December 2008, is presented in Appendix 4.

5 Additional work

There are further deliverables/tools which have become apparent as a result of the tasks carried out for this deliverable. Although perhaps not within the scope of this IFM project, it is worth noting at this stage recommendations for additional work. These are:

- The creation of a comprehensive risk register for emerging IFMs;
- An entry level requirement for a scheme's risk/trust acknowledgement when joining the EU IFM;
- Definition of the trust requirements for interoperable products; and
- Definition of the trust requirements for common payment criteria.
- Definition of a clear customer proposition
- Methods of payment within the IFM

6 Conclusions

This deliverable presents the first findings for Work Package 1 of the IFM project. The objectives were to identify the existing Trust Models already in place within the consortium and to being the process of understanding and recommending the procedure to be adopted for an EU IFM Trust Model for existing members. The first deliverable has collated data about all the schemes within the project and their existing Trust Models. This was achieved firstly by designing and distributing a questionnaire, and secondly, by holding a workshop to gather a more in depth understanding. It was found from the questionnaire, which was developed to analyse existing risk and mitigation, that there is some ambiguity between Trust and Risk, and that the definition of a Trust Model in this project may not have been shared by all the partners. The questionnaire enabled the identification of some key risks which must be addressed in later WP1 tasks. It also highlighted some risks which may not be mitigated by all partners at present, and so these should also be a focus in future stages of this work package.

The follow-on workshop was held with the relevant members of the consortium in order to clarify the Trust-related questions resulting from the questionnaire, provide a greater understanding of the existing Trust Management Models and to agree an overall definition of Trust. The result of this was that the definition of a Trust Model first presented by the project would be accepted with the addition of the concept of 'residual trust' required to deal with the remaining risks, and differing levels of trust required for different transactions, and to reflect the many relationships both B to B and B to C.

In addition to this, it has become apparent that in order to recommend and produce the methodology for an EU IFM Trust Model, the outputs of the other Work Packages will be crucial. For example, during the workshop it became apparent that any decisions made regarding the media by WP3 would directly feed into the development of the Trust Model as the underlying risks are identified. In order to shape the delivery of the Trust Model, this is ultimately dependent upon the shape of the whole project, such as the system, architecture, and nature of transactions, and the technical outcomes. Therefore, it is recommended that communications and shadowing of the activities and outcomes of other WPs must be carried out for the remainder of the project.

Appendix 1

The responses from the questionnaire

Risks, Mitigation and Trust						
Certification						
Q 1-1	Is there a Risk?		Do you mitigate against this risk?		Does this risk feature in your Trust Model?	
	Yes					
Each Organisation which wants to participate in the IFM shall agree to abide by the Set of Rules.	High	<input type="checkbox"/>	Yes	<input type="checkbox"/>	Yes	<input type="checkbox"/>
	Medium	<input type="checkbox"/>	No	<input type="checkbox"/>	No	<input type="checkbox"/>
	Low	<input type="checkbox"/>				

ITSO	H	Y	Y
RATP	H	Y	Y
VDV KA	M	Y	Y

Q 1-2	Is there a Risk?		Do you mitigate against this risk?		Does this risk feature in your Trust Model?	
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.	High	<input type="checkbox"/>	Yes	<input type="checkbox"/>	Yes	<input type="checkbox"/>
	Medium	<input type="checkbox"/>	No	<input type="checkbox"/>	No	<input type="checkbox"/>
	Low	<input type="checkbox"/>				

ITSO	H	Y	Y
RATP	H	Y	Y
VDV KA	H	Y	Y

Q 1-3	Is there a Risk?		Do you mitigate against this risk?		Does this risk feature in your Trust Model?	
Each Application Specification and Template to be brought into the IFMS shall meet the IFM requirements. Proof of this is given by checking this Application Specification and Template against a Set of Rules.	High	<input type="checkbox"/>	Yes	<input type="checkbox"/>	Yes	<input type="checkbox"/>
	Medium	<input type="checkbox"/>	No	<input type="checkbox"/>	No	<input type="checkbox"/>
	Low	<input type="checkbox"/>				

ITSO	H	Y	Y
RATP	H	Y	Y
VDV KA	M	Y	Y

Q 1-4	Is there a Risk?		Do you mitigate against this risk?		Does this risk feature in your Trust Model?	
Each Product Specification and Template to be brought into the IFM shall meet the IFM requirements. Proof of this is given by checking this Product Specification and Template against a Set of Rules.	High	<input type="checkbox"/>	Yes	<input type="checkbox"/>	Yes	<input type="checkbox"/>
	Medium	<input type="checkbox"/>	No	<input type="checkbox"/>	No	<input type="checkbox"/>
	Low	<input type="checkbox"/>				

ITSO	M	Y	Y
RATP	H	Y	Y
VDV KA	L	Y	Y

Registration						
Q 2-1	Is there a Risk?		Do you mitigate against this risk?		Does this risk feature in your Trust Model?	
A unique identification is given to each Organisation.	Yes					
	High	<input type="checkbox"/>	Yes	<input type="checkbox"/>	Yes	<input type="checkbox"/>
	Medium	<input type="checkbox"/>	No	<input type="checkbox"/>	No	<input type="checkbox"/>
	Low	<input type="checkbox"/>				

ITSO	H	Y	Y
RATP	H	Y	Y
VDV KA	M	Y	Y

Q 2-2	Is there a Risk?		Do you mitigate against this risk?		Does this risk feature in your Trust Model?	
A unique identification is given to each Component.	High	<input type="checkbox"/>	Yes	<input type="checkbox"/>	Yes	<input type="checkbox"/>
	Medium	<input type="checkbox"/>	No	<input type="checkbox"/>	No	<input type="checkbox"/>
	Low	<input type="checkbox"/>				

ITSO	L	Y	Y
RATP	H	Y	Y
VDV KA	M	Y	Y

Q 2-3	Is there a Risk?		Do you mitigate against this risk?		Does this risk feature in your Trust Model?	
A unique identification is given to each Application Template.	High	<input type="checkbox"/>	Yes	<input type="checkbox"/>	Yes	<input type="checkbox"/>
	Medium	<input type="checkbox"/>	No	<input type="checkbox"/>	No	<input type="checkbox"/>
	Low	<input type="checkbox"/>				

ITSO	L	Y	Y
RATP	L	N	N
VDV KA	M	Y	Y

Q 2-4	Is there a Risk?		Do you mitigate against this risk?		Does this risk feature in your Trust Model?	
A unique identification is given to each Application.	High	<input type="checkbox"/>	Yes	<input type="checkbox"/>	Yes	<input type="checkbox"/>
	Medium	<input type="checkbox"/>	No	<input type="checkbox"/>	No	<input type="checkbox"/>
	Low	<input type="checkbox"/>				

ITSO	L	Y	Y
RATP	H	Y	Y
VDV KA	M	Y	Y

Q 2-5	Is there a Risk?		Do you mitigate against this risk?		Does this risk feature in your Trust Model?	
A unique identification is given to each Product Template.	High	<input type="checkbox"/>	Yes	<input type="checkbox"/>	Yes	<input type="checkbox"/>
	Medium	<input type="checkbox"/>	No	<input type="checkbox"/>	No	<input type="checkbox"/>
	Low	<input type="checkbox"/>				

ITSO	L	Y	Y
RATP	L	N	N
VDV KA	M	Y	Y

Q 2-6	Is there a Risk?		Do you mitigate against this risk?		Does this risk feature in your Trust Model?	
A unique identification is given to each Product.	High	<input type="checkbox"/>	Yes	<input type="checkbox"/>	Yes	<input type="checkbox"/>
	Medium	<input type="checkbox"/>	No	<input type="checkbox"/>	No	<input type="checkbox"/>
	Low	<input type="checkbox"/>				

ITSO	L	Y	Y
RATP	H	Y	Y
VDV KA	M	Y	Y

Management of Application

Q 3-1	Is there a Risk?		Do you mitigate against this risk?		Does this risk feature in your Trust Model?	
	Yes					
Dissemination of an Application Template enables the authorised Retailer to sell an Application and an authorised Service Operator to access this Application.	High	<input type="checkbox"/>	Yes	<input type="checkbox"/>	Yes	<input type="checkbox"/>
	Medium	<input type="checkbox"/>	No	<input type="checkbox"/>	No	<input type="checkbox"/>
	Low	<input type="checkbox"/>				

ITSO	M	Y	Y
RATP	H	Y	Y
VDV KA	M	Y	Y

Q 3-2	Is there a Risk?		Do you mitigate against this risk?		Does this risk feature in your Trust Model?	
An Application is loaded on the Customer Medium.	High	<input type="checkbox"/>	Yes	<input type="checkbox"/>	Yes	<input type="checkbox"/>
	Medium	<input type="checkbox"/>	No	<input type="checkbox"/>	No	<input type="checkbox"/>
	Low	<input type="checkbox"/>				

ITSO	L	Y	Y
RATP	H	Y	Y
VDV KA	M	Y	Y

Q 3-3	Is there a Risk?		Do you mitigate against this risk?		Does this risk feature in your Trust Model?	
	An Application Template is terminated in the IFM by request of the Application Owner.	High	<input type="checkbox"/>	Yes	<input type="checkbox"/>	Yes
Medium		<input type="checkbox"/>	No	<input type="checkbox"/>	No	<input type="checkbox"/>
Low		<input type="checkbox"/>				

ITSO	M	Y	Y
RATP	H	Y	Y
VDV KA	M	Y	Y

Q 3-4	Is there a Risk?		Do you mitigate against this risk?		Does this risk feature in your Trust Model?	
	Termination of Application Template by request of the IFM Manager.	High	<input type="checkbox"/>	Yes	<input type="checkbox"/>	Yes
Medium		<input type="checkbox"/>	No	<input type="checkbox"/>	No	<input type="checkbox"/>
Low		<input type="checkbox"/>				

ITSO	H	Y	Y
RATP	H	Y	Y
VDV KA	M	Y	Y

Q 3-5	Is there a Risk?		Do you mitigate against this risk?		Does this risk feature in your Trust Model?	
	An Application is terminated on the Customer Medium.	High	<input type="checkbox"/>	Yes	<input type="checkbox"/>	Yes
Medium		<input type="checkbox"/>	No	<input type="checkbox"/>	No	<input type="checkbox"/>
Low		<input type="checkbox"/>				

ITSO	L	Y	Y
RATP	H	Y	Y
VDV KA	M	Y	Y

Q 3-6	Is there a Risk?		Do you mitigate against this risk?		Does this risk feature in your Trust Model?	
Application is put on a security list by request of the APPLICATION OWNER	High	<input type="checkbox"/>	Yes	<input type="checkbox"/>	Yes	<input type="checkbox"/>
	Medium	<input type="checkbox"/>	No	<input type="checkbox"/>	No	<input type="checkbox"/>
	Low	<input type="checkbox"/>				

ITSO	M	Y	Y
RATP	H	Y	Y
VDV KA	M	Y	Y

Management of Product

Q 4-1	Is there a Risk?		Do you mitigate against this risk?		Does this risk feature in your Trust Model?	
	Yes					
Dissemination of registered Product Template enabling authorised Actors to handle the Product.	High	<input type="checkbox"/>	Yes	<input type="checkbox"/>	Yes	<input type="checkbox"/>
	Medium	<input type="checkbox"/>	No	<input type="checkbox"/>	No	<input type="checkbox"/>
	Low	<input type="checkbox"/>				

ITSO	M	Y	Y
RATP	L	Y	Y
VDV KA	M	Y	Y

Q 4-2	Is there a Risk?		Do you mitigate against this risk?		Does this risk feature in your Trust Model?	
Termination of Product Template on decision of the PRODUCT OWNER.	High	<input type="checkbox"/>	Yes	<input type="checkbox"/>	Yes	<input type="checkbox"/>
	Medium	<input type="checkbox"/>	No	<input type="checkbox"/>	No	<input type="checkbox"/>
	Low	<input type="checkbox"/>				

ITSO	M	Y	Y
RATP	L	Y	Y
VDV KA	M	Y	Y

Q 4-3	Is there a Risk?		Do you mitigate against this risk?		Does this risk feature in your Trust Model?	
Termination of Product Template on decision of the IFM Manager. (Forced termination)	High	<input type="checkbox"/>	Yes	<input type="checkbox"/>	Yes	<input type="checkbox"/>
	Medium	<input type="checkbox"/>	No	<input type="checkbox"/>	No	<input type="checkbox"/>
	Low	<input type="checkbox"/>				

ITSO	H	Y	Y
RATP	H	Y	Y
VDV KA	M	Y	Y

Q 4-4	Is there a Risk?		Do you mitigate against this risk?		Does this risk feature in your Trust Model?	
Management of an Action List enables actions related to Products or Applications.	High	<input type="checkbox"/>	Yes	<input type="checkbox"/>	Yes	<input type="checkbox"/>
	Medium	<input type="checkbox"/>	No	<input type="checkbox"/>	No	<input type="checkbox"/>
	Low	<input type="checkbox"/>				

ITSO	M	Y	Y
RATP	H	Y	Y
VDV KA	M	Y	Y

Q 4-5	Is there a Risk?		Do you mitigate against this risk?		Does this risk feature in your Trust Model?	
Acquisition of PRODUCT enabling CUSTOMER to benefit from a transport service.	High	<input type="checkbox"/>	Yes	<input type="checkbox"/>	Yes	<input type="checkbox"/>
	Medium	<input type="checkbox"/>	No	<input type="checkbox"/>	No	<input type="checkbox"/>
	Low	<input type="checkbox"/>				

ITSO	L	Y	N
RATP	H	Y	Y
VDV KA	M	Y	Y

Q 4-6	Is there a Risk?		Do you mitigate against this risk?		Does this risk feature in your Trust Model?	
Modifying changeable Product parameters for an existing Product.	High	<input type="checkbox"/>	Yes	<input type="checkbox"/>	Yes	<input type="checkbox"/>
	Medium	<input type="checkbox"/>	No	<input type="checkbox"/>	No	<input type="checkbox"/>
	Low	<input type="checkbox"/>				

ITSO	L	Y	Y
RATP	H	Y	Y
VDV KA	M	Y	Y

Q 4-7	Is there a Risk?		Do you mitigate against this risk?		Does this risk feature in your Trust Model?	
Termination of Product by request of the CUSTOMER.	High	<input type="checkbox"/>	Yes	<input type="checkbox"/>	Yes	<input type="checkbox"/>
	Medium	<input type="checkbox"/>	No	<input type="checkbox"/>	No	<input type="checkbox"/>
	Low	<input type="checkbox"/>				

ITSO	L	Y	N
RATP	L	Y	Y
VDV KA	L	Y	Y

Management of Product

Q 5-1	Is there a Risk?		Do you mitigate against this risk?		Does this risk feature in your Trust Model?	
Product is put on a security list by request of the PRODUCT OWNER.	High	<input type="checkbox"/>	Yes	<input type="checkbox"/>	Yes	<input type="checkbox"/>
	Medium	<input type="checkbox"/>	No	<input type="checkbox"/>	No	<input type="checkbox"/>
	Low	<input type="checkbox"/>				

ITSO	M	Y	Y
RATP	H	Y	Y
VDV KA	M	Y	Y

Q 5-2	Is there a Risk?		Do you mitigate against this risk?		Does this risk feature in your Trust Model?	
	High	<input type="checkbox"/>	Yes	<input type="checkbox"/>	Yes	<input type="checkbox"/>
SERVICE OPERATOR checks and collects the data of a Customer Medium using the public transport service.	Medium	<input type="checkbox"/>	No	<input type="checkbox"/>	No	<input type="checkbox"/>
	Low	<input type="checkbox"/>				

ITSO	L	N	N
RATP	H	Y	Y
VDV KA	M	Y	Y

Q 5-3	Is there a Risk?		Do you mitigate against this risk?		Does this risk feature in your Trust Model?	
	High	<input type="checkbox"/>	Yes	<input type="checkbox"/>	Yes	<input type="checkbox"/>
The COLLECTION AND FORWARDING receives data and checks the completeness and integrity of the data.	Medium	<input type="checkbox"/>	No	<input type="checkbox"/>	No	<input type="checkbox"/>
	Low	<input type="checkbox"/>				

ITSO	M	Y	Y
RATP	M	Y	Y
VDV KA	M	Y	Y

Q 5-4	Is there a Risk?		Do you mitigate against this risk?		Does this risk feature in your Trust Model?	
	High	<input type="checkbox"/>	Yes	<input type="checkbox"/>	Yes	<input type="checkbox"/>
The COLLECTION AND FORWARDING forwards data.	Medium	<input type="checkbox"/>	No	<input type="checkbox"/>	No	<input type="checkbox"/>
	Low	<input type="checkbox"/>				

ITSO	H	Y	Y
RATP	M	Y	Y
VDV KA	L	Y	Y

Q 5-5	Is there a Risk?		Do you mitigate against this risk?		Does this risk feature in your Trust Model?	
	The PRODUCT OWNER performs the clearing procedure and distributes the results to relevant Entities	High	<input type="checkbox"/>	Yes	<input type="checkbox"/>	Yes
Medium		<input type="checkbox"/>	No	<input type="checkbox"/>	No	<input type="checkbox"/>
Low		<input type="checkbox"/>				

ITSO	L	N	N
RATP	H	Y	Y
VDV KA	L	Y	Y

Security Management

Q 6-1	Is there a Risk?		Do you mitigate against this risk?		Does this risk feature in your Trust Model?	
		Yes				
The monitoring of the processes and data life cycle (generation of data, movement of data, storage of data, use of data, changes of data and deletion of data) shall guarantee the secure operation of the IFMS, providing the required trust by the customers and operators concerning handling and protection of assets and sensitive information.	High	<input type="checkbox"/>	Yes	<input type="checkbox"/>	Yes	<input type="checkbox"/>
	Medium	<input type="checkbox"/>	No	<input type="checkbox"/>	No	<input type="checkbox"/>
	Low	<input type="checkbox"/>				

ITSO	H	Y	Y
RATP	H	Y	Y
VDV KA	M	Y	Y

Q 6-2	Is there a Risk?		Do you mitigate against this risk?		Does this risk feature in your Trust Model?	
	The generation, distribution, storage and termination of IFM security keys.	High	<input type="checkbox"/>	Yes	<input type="checkbox"/>	Yes
Medium		<input type="checkbox"/>	No	<input type="checkbox"/>	No	<input type="checkbox"/>
Low		<input type="checkbox"/>				

ITSO	H	Y	Y
RATP	H	Y	Y
VDV KA	H	Y	Y

Q 6-3	Is there a Risk?		Do you mitigate against this risk?		Does this risk feature in your Trust Model?	
	Provision of a security list by the Security Manager.	High	<input type="checkbox"/>	Yes	<input type="checkbox"/>	Yes
Medium		<input type="checkbox"/>	No	<input type="checkbox"/>	No	<input type="checkbox"/>
Low		<input type="checkbox"/>				

ITSO	H	Y	Y
RATP	H	Y	Y
VDV KA	M	Y	Y

Q 6-4	Is there a Risk?		Do you mitigate against this risk?		Does this risk feature in your Trust Model?	
	Aggregation of security list data concerning Components, Customer Medium, installed Products and installed Applications.	High	<input type="checkbox"/>	Yes	<input type="checkbox"/>	Yes
Medium		<input type="checkbox"/>	No	<input type="checkbox"/>	No	<input type="checkbox"/>
Low		<input type="checkbox"/>				

ITSO	M	Y	Y
RATP	H	Y	Y
VDV KA	M	Y	Y

Q 6-5	Is there a Risk?		Do you mitigate against this risk?		Does this risk feature in your Trust Model?	
	The adding of a Component to, or removing of a Component from, a security list.	High	<input type="checkbox"/>	Yes	<input type="checkbox"/>	Yes
Medium		<input type="checkbox"/>	No	<input type="checkbox"/>	No	<input type="checkbox"/>
Low		<input type="checkbox"/>				

ITSO	M	Y	Y
RATP	H	Y	Y
VDV KA	M	Y	Y

Q 6-6	Is there a Risk?		Do you mitigate against this risk?		Does this risk feature in your Trust Model?	
	The adding of an Application Template to, or removing of an Application Template from, a security list.	High	<input type="checkbox"/>	Yes	<input type="checkbox"/>	Yes
Medium		<input type="checkbox"/>	No	<input type="checkbox"/>	No	<input type="checkbox"/>
Low		<input type="checkbox"/>				

ITSO	M	Y	Y
RATP	H	Y	Y
VDV KA	M	Y	Y

Q 6-7	Is there a Risk?		Do you mitigate against this risk?		Does this risk feature in your Trust Model?	
	The adding of an Application to, or removing of an Application from, a security list.	High	<input type="checkbox"/>	Yes	<input type="checkbox"/>	Yes
Medium		<input type="checkbox"/>	No	<input type="checkbox"/>	No	<input type="checkbox"/>
Low		<input type="checkbox"/>				

ITSO	M	Y	Y
RATP	H	Y	Y
VDV KA	M	Y	Y

Security Management

Q 7-1	Is there a Risk?		Do you mitigate against this risk?		Does this risk feature in your Trust Model?	
The adding of a Product Template to, or removing of a Product Template from, a security list.	High	<input type="checkbox"/>	Yes	<input type="checkbox"/>	Yes	<input type="checkbox"/>
	Medium	<input type="checkbox"/>	No	<input type="checkbox"/>	No	<input type="checkbox"/>
	Low	<input type="checkbox"/>				

ITSO	-	-	-
RATP	H	Y	Y
VDV KA	M	Y	Y

Q 7-2	Is there a Risk?		Do you mitigate against this risk?		Does this risk feature in your Trust Model?	
The adding of a Product to, or removing of a Product from, a security list.	High	<input type="checkbox"/>	Yes	<input type="checkbox"/>	Yes	<input type="checkbox"/>
	Medium	<input type="checkbox"/>	No	<input type="checkbox"/>	No	<input type="checkbox"/>
	Low	<input type="checkbox"/>				

ITSO	M	Y	Y
RATP	H	Y	Y
VDV KA	M	Y	Y

Customer Service Management

Q 8-1	Is there a Risk?		Do you mitigate against this risk?		Does this risk feature in your Trust Model?	
	Yes					
CUSTOMER SERVICE provides "helpline" and any similar facilities.	High	<input type="checkbox"/>	Yes	<input type="checkbox"/>	Yes	<input type="checkbox"/>
	Medium	<input type="checkbox"/>	No	<input type="checkbox"/>	No	<input type="checkbox"/>
	Low	<input type="checkbox"/>				

ITSO	M	Y	Y
RATP	H	Y	Y
VDV KA	L	Y	N

Appendix 2

The ITSO Trust Model

Introduction

For Retailers, Carriers and System Operators to confidently allow ITSO to securely handle their "Products", or record their usage, and for customers to accept ITSO Products onto their smartcards, they must all TRUST the ITSO environment.

ITSO offers an OPEN system, allowing trusted transactions to be made even when the system is off-line.

The ITSO model that underpins this environment is called the **ITSO Trust Model**.

Prerequisites for the ITSO Trust Model

The Trust Model must:

- Continue to verify that 3DES & RSA (1024bits) remains Best Practice for symmetric and asymmetric cryptography and messaging in the contactless transport smartcard environment and for ITSO to use it at all appropriate stages
- Continue to verify that CLEF is an adequate test of the ISAMs intrinsic security and that the ISAM certificate is applicable and up-to-date
- Identify each and every player, define their roles and boundaries transparently, and gain their commitment to supporting and complying with the Trust Model.
- Include, where appropriate, specific technological elements beyond the contractual commitments, to protect against abuse by players outside the Trust Model.
- Publish openly the Trust Model amongst members so that they can all recognise their equal footing, and their responsibilities for their own scheme and those who belong to it. The ITSO Trust Model is geared towards interoperable public transport (potentially up to international travel), but can be extended to other complementary transactions.
- Allow any card with an ITSO Shell to be loaded with Product subject to space being available on the card and not Hot Listed.
- Allow Card Users to read the data on their card without hindrance, and at the same time protect the Product Owner by only allowing data to be written, modified or deleted with the Product Owner's explicit permission.
- Allows deletion of expired products under commonly agreed terms to prevent clogging up of the system
- Require Operators to circulate and selectively use Hot Lists of withdrawn media and products

Background to the ITSO Trust Model

The Trust Model is owned by the ITSO Members and is not proprietary. It needs to be kept constantly under review, both by its members to ensure the adoption of Best Practice, and independently for signs of strain, unusual activity, errors, or abuse. It includes bodies given specific trusted roles, and the hardware and protocols used. The keys used must therefore be securely protected and archived by a trusted body of the highest repute.

The Trust Model works alongside the ITSO Business Model, the ITSO Physical Model and the ITSO Data Model. The latter two are described through the ITSO Specification (Crown Copyright); the former through the ITSO Operators License. ITSO itself supplies the necessary technological elements and support (the ISAM and the Security Management Service).

The Trust Model is not by itself 100% secure. ITSO have a formalised Risk Management Process by which risk and threat are collated, analysed and actioned, always accepting that there are some risks that have to be accepted. There is a continual review process in place.

The Trust Model can be used to define a specific monitoring programme to provide detection as well as protection.

External References

The ITSO Trust Model is based on and benchmarked to:

IOPTA: The EC Interoperable Passenger Transport Application model
BS7799: The Code of Practice for Information Security Systems
Common Criteria Level 4 / CLEF

Owners

ITSO	ITSO members
LO	ITSO Licensed Operators
RS	ITSO Registered Suppliers
ISMS	ITSO Security Management Service (currently Royal Bank of Scotland)
Ecebs	

The ITSO Trust Model

Issue	Risk Assessment	Trust Owner	Trust Model	ITSO Mitigation
Player Identification	Players can anonymously create shells and products	LO	License terms are complete and un-ambiguous.	ITSO Spec Part 5 ITSO License
		ITSO	KYC checks are comprehensive and up-to-date	KYC carried out by RBS to Banking Standards
		ITSO	Failure to comply with License is directly actioned and keys withdrawn	All players must have unique OID and keys are only issued after License issued and Know Your Customer (KYC) checks completed
Card Authentication	Cards can be replicated	LO	Operators will circulate and selectively use Hot Lists to determine most likely attack	ITSO Spec Parts 2,7,8,10 Hot Lists circulated to all Operators
		ITSO	MID is robust and Manufacturers have processes to record MID of all cards produced	Shell sealed with seal using ITSO shell key and Manufacturers ID (MID).
		LS	Encryption is secure	Data cannot be copied onto another card as seal specific to MID
		LO	Shell owner can block card if lost or stolen and recreate shells.	Shell owner required to retain record of Products on card
		RS	Equipment is certified as completing transactions in under 200mS	Transactions are as close to "Real Time" as practicable to minimise the time to intercept and modify transactions
Product Authentication	Products can be replicated	ITSO	Data can be read by anyone.	ITSO Spec Part s 5,7,8 Product Instance sealed with seal using ITSO shell key and Manufacturers ID (MID).
		LO	Operators will circulate and selectively use Hot Lists to determine most likely attack	Product owner receives a message confirming creation of Product Instance
		RS	Equipment is certified as completing transactions in under 200mS	Transactions are as close to "Real Time" as practicable to minimise the time to intercept and modify transactions

Issue	Risk Assessment	Trust Owner	Trust Model	ITSO Mitigation
Certification of Equipment and Software used	Products can be written to or modified.	LO	Operators will only use ITSO Certified equipment and software and will audit to verify that it is used unaltered	ITSO Spec part 3 ITSO certify equipment for use.
		ITSO	ISAM cannot be woken up by unauthorised user	Licensed Operators specify who is to receive their keys. Keys held in secure module (ISAM) which is used to write and authenticate seals
		RS	POSTs have been tested off-line and the correct shut down occurs after time interval	ISAM will safely shut down if not in contact with host beyond given time frame.
Card handling and loading / use of Products	Unauthorised writing or modification of Products	LO	Critical equipment such as Card Personalisation and Retailing is carried out in secure environments	ITSO Spec part 3
		ITSO	ISAM is secure from attack	Key is specific to each Operator and each Product Embodiment.
		ITSO	Synchronous encryption keys are securely locked in ISAM	Seal to specific embodiment on a card made up from Card ID, Product, and Owner
		LO	Encryption is secure and Operators will change keys if threat seen	Encryption of the transaction between card and POST aerial
Security of ISAM	ISAM is compromised	ITSO	CLEF accreditation has addressed all current security threats	ITSO Spec Part 7,8 CLEF is a snapshot and requires repeating after ISAM changes
		Ecebs	Design of the ISAM is kept secure and private	Design is held in secure Ecrow

Issue	Risk Assessment	Trust Owner	Trust Model	ITSO Mitigation
Message Handling	Messages are not passed to their intended recipients	LO	HOPS will pass on all 'not-on-us transactions	ITSO Spec part 4,6,9 ISAM generates secure message for each transaction and will not delete them until secure acknowledgement received.
	Messages are altered	LO	HOPS will not alter records once unsealed	
		ITSO	Records cannot be read over VPN by unauthorised users	VPN is securely encrypted
		ITSO	ISAM design prevents deletion of records without secure acknowledgement that record has been satisfactorily delivered to its intended recipient	ISAM will safely verify a message before acting on it
	Action on receipt of a message is not carried out	LO	Card owner does not interfere with card messages	Operator does not receive secure acknowledgement allowing it to Hot List card
Security keys	Keys are passed to unauthorised parties	ITSO	Encryption is not broken	ITSO Spec part 8
	Key encryption is broken	ISMS	The HSM is held in a secure environment, and Master Keys are diversified and held securely off site in separate components.	
	Keys are lost preventing Products from being used	ITSO	Keys are always unique and cannot be de-crypted within a meaningful time horizon	Keys are only passed to trusted parties having completed KYC checks successfully
		ITSO	Seals are sufficiently diversified to allow each variable to be included	
	ITSO	Keys are securely archived		

Issue	Risk Assessment	Trust Owner	Trust Model	ITSO Mitigation
Products can be safely deleted remotely	Product Owner authorises deletion, but product remains live	LO	Key equipment such as Card Personalisation and Retailing is carried out in secure environments	ITSO Spec part 7,8
		ITSO	ISAM is secure from attack	Key is specific to each Operator and each Product Embodiment.
		ITSO	Encryption is secure and Operators will change keys if threat seen	Seal to specific embodiment on a card made up from Card ID, Product, and Owner
Failure of Security System	Players will not respect the requirements of the Trust Model	ITSO	ITSO will monitor activity and withdraw License (and keys) for inappropriate activity outside the License	Operating License
ITSO inappropriately operates the ITSO Security System	Licensed Operators loose trust in system	ITSO	Board and IPC and the Governance Structure are appropriate and regularly verified as working satisfactorily	Memorandum and Articles of Association Members Guide ITSO Procedures Independent ITSO Security Committee Compliance Manager
Reliance on ITSO Transactions for Clearing & Settlement	ITSO transactions are incomplete or inaccurate	LO	POSTs connect their ISAMs to a HOPS and transactions are downloaded	ITSO Spec Part 4,7,8,9
		LO	HOPS pass on all transactions	All transactions are lossless
POSTs pass on all transactions	ITSO transactions are incomplete or inaccurate and lack Batch Control	RS	POSTs operated correctly	ITSO Spec Part 3,4,9
		ITSO	C&T certification covered these aspects	Sequence numbers generated for all transactions
Security of POSTs	Stolen POSTs can continue to operate	ITSO	ISAM memory will hold transactions until downloaded securely and acknowledgement received	ITSO Spec Part 3
	Internal POST logic is used to create false transaction	ITSO	ISAM goes to sleep as predicted	ISAM goes out of use after fixed time

Appendix 3

Copy of the presentation given at the workshop held as part of task 1.2 for WP1.

IFM
Integratable Fair Management Project

WP1

An initial workshop

IFM Why?

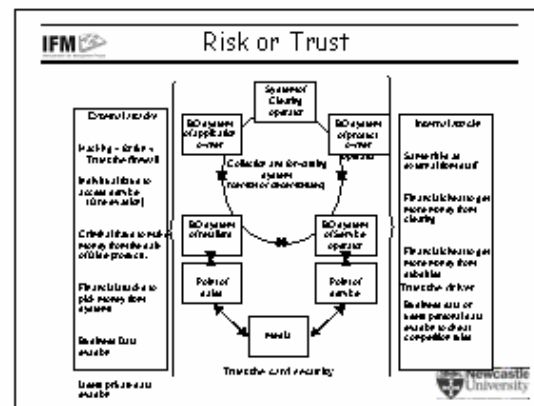
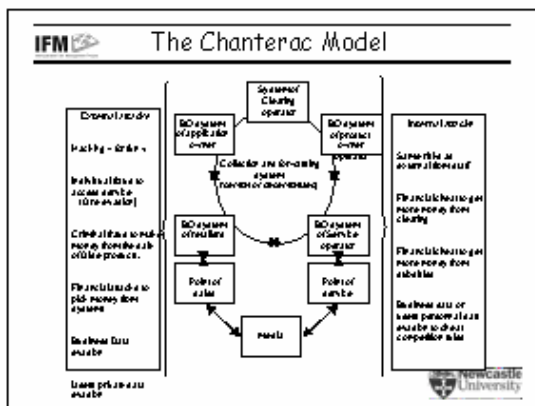
- There are NO transport trust models
- But
- There are
 - Contracts
 - Licenses
 - Membership rules
 - Risk Models

IFM Purpose of workshop

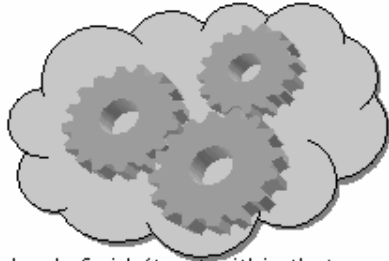
- Put down some pegs
- Mark some boundaries
- Run some things up the flagpole and see who salutes them
- Scope of project
- Overlap with other WPs
- Test some of our issues

IFM TRUST MODEL


- Trust is an unmitigated risk
- Trust model describes the extent and limitations of that mitigation for the particular scheme (in this case an EU IFM)



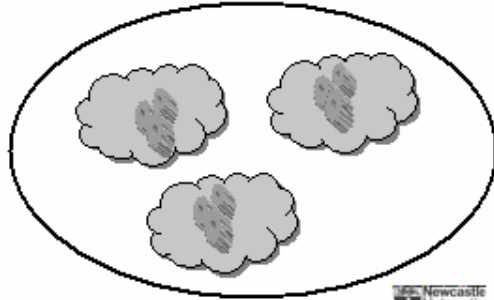

IFM An IFM (a scheme)



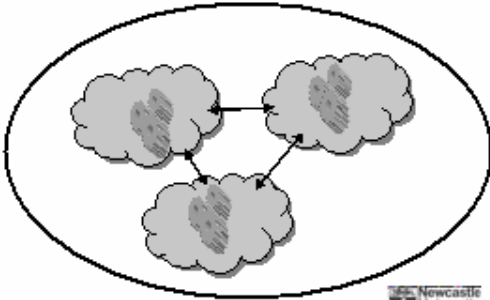

The level of risk/trust within that scheme is a commercial decision



IFM An EU IFM





IFM An EU IFM


IFM The relationships

- Media from one scheme used in another
 - Interoperable media
- Products being used or retailed between schemes
 - Interoperable products




IFM Interoperable Media
Some trust issues – no 1

- Is the media fit for my purpose?
 - Is it acceptable to me and my product?
 - Will it work in my scheme?
 - Is the security strong enough?
- I need some assurance
 - Standards or specification
 - Minimum configuration
 - Certification




IFM Interoperable Media
Some trust issues – no 2

- Can I actually use it?
 - Where do the keys come from?
 - Is there enough space?
 - Can I make space?
- I need some input
 - Keys from a KMS
 - Specification for the common contents
 - Permission rules




IFM Interoperable Media
Some trust issues - no 3

- Does the customer know where and how to use his media?
- Brand issues/rules




IFM Interoperable Media
Some trust issues - no 4

- Will the cards still work when it returns home?
 - Will it still physically work?
 - Can I delete the products?
 - Where do the keys come from?
- I need some input
 - Keys from a KMS
 - Specification for the common contents
 - Permission rules




IFM The relationships

- Media from one scheme used in another
 - Interoperable media
- Products being used or retailed between schemes
 - Interoperable products




IFM Products being used or retailed between schemes

- Interoperable products
- Exchange of data and/or money

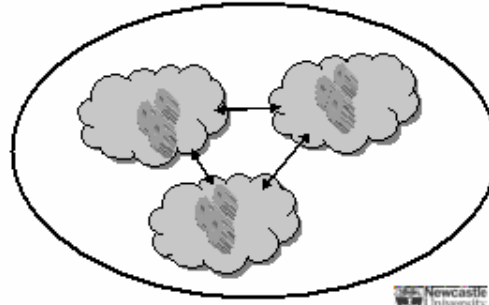



IFM Products being used or retailed between schemes

- Interoperable products
- Exchange of data and/or money
 - Will I get my money /data?
 - Will my customers get the level of service?
- Due diligence.....IFM approved scheme with underwriting



IFM An EU IFM

IFM To debate or confirm

1. There are no trust models
2. That we are considering only the first of the interactions - the media
3. What cards are we considering?
 1. Scheme cards
 2. EMV
 3. IFM card



IFM To debate or confirm

4. The need for an EU IFM standard or specification e.g.
 - Card types
 - How to identify a product
5. The need for a set of club rules e.g.
 - Permissions to delete (and inform)
6. The need for a key management service



IFM To debate or confirm

7. The need for Brand Management
8. The need for certification e.g.
 - Card
 - terminals
 - methodology eg Process, self
 - acceptability of other certification e.g. EMV, ITSO, VDV



Appendix 4

Vision for IFM project and beyond - created by WP 3 and 4 during workshop on 18th December 2008.

Vision	as the following steps	WP7 + WP6
to be defined by IFM1		
Step 1. Common media		WP3
	Common acceptance criteria for media	WP3
	Security	WP3
	Downloading ability	WP3
	Link with product owner	WP3
organisation model is defined by IFM1 , technical aspects and implementation by IFM2		
Step 2. Common application for common data (no product)		
	1st content definition	WP7 + WP6
	Data model	CEN 224 (EN1545/IOPTA)
	Corresponding MMI	IFM2
	Business organisation (IFM 24014)	WP4
	Owner, retailer, set of rules	WP4
	Trust and Privacy model	WP1 + WP2 + WP4
	Security of application (level, public/private)	WP4 + WP5
Step 3. (Common portal)		WP7 + WP6
	Owner, technical interface	WP4 + WP5
	Set of rules	WP1 + WP4
	Customer interface	IFM2
organisation model and technical implementation by IFM2		
Step 4.	Consensus about 2nd content, common structure	WP7 + WP6 + IFM2
	Common structure for products	CEN (1545/IOPTA 2)
IFM1 defines the vision ; schemes implement according to their policies		
Step 5.	Commercial content	WP7
	3rd content, common product	EACH SCHEME
Step 6	Local applications merge	EACH SCHEME
Step 7	Local applications disappear	EACH SCHEME