consult hyperion

project report

The use of Near Field Communication (NFC) technology in mobile phones for public transport ticketing

Department for Transport

Chyp doc ref:	Prj 1057/D15
Version:	1.2a
Date:	11 November 2009
Authors:	John Elliott, Andrew Whitcombe
Approved:	John Elliott

Consult Hyperion
Tweed House
12 The Mount
Guildford
GU2 4HN
t: 01483 301 793 f: 01483 561 657
www.chyp.com

REVISION HISTORY

Version	Date	Author	Detail
0.1	28 May 2009	AW	Chyp internal review
0.2	29 May 2009	AW/JE	First full draft delivered to DfT for review.
1.0	30 June 2009	AW/JE	Version of document for DfT to add the copyright disclaimer to. Updated to reflect DfT comments on version 0.2: • Figure 2 removed at the request of DfT • Section 2 significantly reduced in volume, with relevant content regarding deliverables being moved to section 3 • Section 1.1.4 removed • Section 1.3 Project Partners added to provide more information about the roles performed by different organisations • Section 3 re-structured to explicitly address the objectives, scope and findings of each work package • Section 3.2 detail regarding risks and countermeasures significantly increased • Section 3.4 extra detail added into the objectives section to clarify the underlying requirements for the ITSO specification enhancements • Section 3.5 sample bench test technical message flow diagram added • Section 4.1.5.1 two sample bench test transaction analysis graphs added • Additional explanatory text added throughout
1.1	5 August 2009	AW	• Re-written executive summary to more clearly link conclusion with objectives • Minor rewordings throughout based on DfT comments • Section 3.4.4 new section added • Section 3.4.5 new section added
1.2a	11 Nov 2009	JE	• Actioning final comments from DfT • Added Appendix B Extracts from Trial User Manual in order to show the phone usage and screen shots.

This report has been produced by Consult Hyperion under a contract with the Department for Transport. Any views expressed in this report are not necessarily those of the Department for Transport.

© Queen's Printer and Controller of HMSO - 2009.

All enquiries relating to the copyright in the work should be addressed to HMSO, The Licensing Division, St Clements House, 2-16 Colegate, Norwich, NR3 1BQ.

EXECUTIVE SUMMARY

This is the report for the 18-month research project into "The use of Near Field Communication technology in mobile phones for public transport ticketing", performed as part of the Department's Transport Technology and Standards research programme.

The Transport Technology and Standards Research programme has identified NFC as a technology with potential as both an ITSO ticket carrying device and an ITSO ticket reading device (for retail sales and / or ticket validation).

The project objectives were to:

1. Demonstrate the use of an NFC device as a certified ITSO customer medium;
2. Demonstrate additional functionality to enable an NFC device to perform as an ITSO compliant Terminal capable of reading, validating and updating ITSO customer media;
3. Develop the ITSO Specification changes necessary to enable the certification of an NFC device acting as an ITSO *terminal* as per objective 2.

A further objective to demonstrate NFC devices acting as ITSO *terminals* in the *live* environment was dependent on the enhancement of the ITSO specification being accepted in time. The scope of this enhancement has wider application than NFC and discussions are still continuing in ITSO Technical and Security Committees. If approved, the enhanced specification would enable trials or implementation of NFC for remote retail/validation.

The project was broken down into the following tasks:

- ***Scoping Study***: To document the requirements for the project and use those requirements to identify the technical and logistical scope of the project.
- ***Risk Analysis***: To ensure that the use of NFC devices in an ITSO environment did not introduce new security vulnerabilities, i.e. the overall level of security within the ITSO environment should not reduce. All identified risks were catalogued and suitable countermeasures defined.
- ***Trial***: To assess the suitability, both technically and socially, of NFC devices as ITSO customer media.
- ***ITSO Specification Analysis***: to identify and document the minimum changes necessary to the ITSO specifications to enable NFC devices to be used as ITSO POSTs, communicating with an ISAM in a back-office server. Also, to actually draft an ITSO Part 11 for consideration by the ITSO technical committee.
- ***Bench test***: to implement and validate the proposed enhancements identified by the ITSO specification analysis.

The following key lessons relating to ITSO on NFC were learned during the project:

- Read range is a key factor in the reliability of a contactless ticket. Particularly in a high throughput, "touch and go" environment such as transit.
- Despite being considerably slower based on lab analysis, the speed disadvantage of CMD2 was not noticed in the trial. The speed of interaction between the card and terminal is not necessarily the bottleneck, depending on how the customer experience has been implemented. In the trial, the additional second required to process CMD2 made no discernable difference to the trialist experience.
- NFC devices are capable of being made sufficiently secure to act as an ITSO POST for all transaction types to all customer media types.
- It was of great benefit to the trial that the phones were used across three different operators. This enabled us to clearly identify faults that were related to ETM configuration issues rather than the NFC phone.
- The ITSO certification processes need to allow for non-card form factors, for example by including more read range testing to ensure different antenna designs function adequately.
- Certified equipment needs to be extensively field tested by the scheme operator before deployment to ensure correct operation in the field. Employing certified terminals may not be enough to ensure correct operation in the field or provide adequate protection against transaction failures.

The following conclusions were drawn from the experiences during the project:

- The six-month trial clearly demonstrated the potential for NFC devices as an alternative housing for ITSO customer media. The technology worked, thus fulfilling the first project objective. The majority of users were extremely positive. However, there are some issues beyond the technology that may limit any commercial service in the short term. In particular:
    - ***NFC market penetration***. There are a limited number of handsets commercially available; this limitation was acceptable for a trial but may cause issues for a real service. It is expected that NFC-enabled mobile handsets will gain significant traction during 2010.
    - ***NFC application delivery***. The trialists were delivered handsets preloaded with necessary software. The standards to enable delivery of applications to people's existing mobile phones are still developing.
    - ***ITSO scheme maturity***. Live ITSO schemes are still in the early stages of learning how best to deploy the technology for their staff and customers.
- Whilst the trial proved NFC devices can be successfully used as Customer Media, the second project objective was to investigate whether off-the-shelf NFC devices could be used as ITSO POSTs. The bench test proved

that this was definitely possible, implementing a number of successful prototypes and fulfilling the second objective. However there are certain limitations that require consideration, should this concept be taken forward:

- ***CMD2 speed issues.*** The majority of NFC phones going forward are expected to use the mobile phone SIM as the secure element. This would mean that under current ITSO specifications they would have to operate as CMD2. It is likely that in the short to medium term it would be difficult to develop ITSO applications for SIMs that meet the new CMD2 performance requirements without the mobile operators having to purchase new SIMs.
- ***Online issues.*** The presence of the ISAM in a back-office server means all such transactions have to be on-line in real time. There are some speed-critical operational environments where such a requirement will be a distinct disadvantage. Where speed of transaction is essential, such as a high throughput gating system, a standard POST is likely to continue to be more appropriate to maintain the speed of transactions.

- As occasional ticket inspection devices, personal terminals, or lower volume terminals (e.g. bus depot ticket offices) however, NFC provides the potential for considerably cheaper hardware alternatives for ITSO POST applications.
- As per the third project objective, potential ITSO specification enhancements were identified and proposed to ITSO for consideration, to enable NFC devices to be used as ITSO POSTs in a live environment.
- Once suitable ITSO specification enhancements have been made, there would be considerable value in carrying out live trials of NFC POSTs.
- Such terminals could then be used to test the reliability and performance of an NFC POST architecture in various scenarios, enabling:
  - Visualisation of tangible commercial applications;
  - More accurate figures on reliability and performance.
- A suite of fully functional demonstration devices capable of demonstrating commercial applications to which the technology is applicable would be a powerful tool in communicating both the potential and limitation of NFC devices as ITSO POSTs.

ABSTRACT

This is the report for the 18-month research project into “The use of Near Field Communication technology in mobile phones for public transport ticketing”, performed as part of the Department’s Transport Technology and Standards research programme. It contains a summary of all the work undertaken, a discussion of the matters arising, conclusions and recommendations.

CONTENTS

1 INTRODUCTION 1

1.1 Background 1
1.2 Project Objectives 2
1.3 Project Partners 3
1.4 Document Scope 3
1.5 Reference Documents 3
1.6 Terms and Abbreviations 3

2 METHODOLOGY 5

2.1 Overview 5
2.2 Project Management 5
2.3 Scoping Study 6
2.4 Risk Analysis 6
2.5 Trial 6
2.6 ITSO Specification Analysis 6
2.7 Bench test 6

3 RESULTS 7

3.1 Scoping Study 7
3.2 Risk Analysis 8
3.3 Trial 11
3.4 ITSO Specification Analysis 15
3.5 Bench Test 17

4 DISCUSSION 22

4.1 NFC 22
4.2 ITSO 27

5 CONCLUSIONS 29

5.1 Objective 1 29
5.2 Objective 2 29
5.3 Objective 3 30

6 RECOMMENDATIONS 31

6.1 NFC-related recommendations 31
6.2 ITSO-related recommendations 31

APPENDIX A PROJECT DELIVERABLES 33

APPENDIX B TRIAL USER MANUAL EXTRACTS 34

B.1 Using the phone for travel 34
B.1.1 Using Stored Travel Rights 34
B.1.2 Using the period pass 34
B.1.3 Presenting the phone to a reader 35
B.2 The NoWcard phone application 36
B.2.1 Starting the application 36
B.2.2 Card details 37
B.2.3 Available products 38
B.2.3.1 Concession product details 38
B.2.3.2 Stored Travel (NoWcard) 39

B.2.3.3 Period Pass product details....40
B.2.4 Feedback....41
B.2.4.1 If you select zero....42
B.2.4.2 If you select one to five, or more than five....43
B.2.4.3 Feedback reminders....44
B.2.5 Support....44

1 INTRODUCTION

This is the Report for the 18-month research project into "The use of Near Field Communication technology in mobile phones for public transport ticketing", performed as part of the Department's Transport Technology and Standards research programme. It contains a summary of all the work undertaken, a discussion of the matters arising, conclusions and recommendations.

1.1 Background

This section provides the reader with some brief background material on the technologies and organisations behind this project.

1.1.1 What is NFC?

Near Field Communication (NFC) is a short wave radio communication technology that is capable of both securely reading from and writing to other radio communications media, such as contactless smartcards, RFID tags or other NFC enabled devices.

NFC devices can operate in two modes:

- ***Passive***: An NFC device can operate passively, acting much like a contactless card.
- ***Active***: An NFC device can operate actively, searching out other devices with which to talk to, acting much like a contactless terminal.

NFC can be used in a variety of devices; however, it is in the mobile phone market where the technology has achieved most traction thus far.

NFC devices contain a special piece of security hardware known as a secure element. The secure element enables the NFC device to store encryption keys and secret data in much the same way as a standard contactless smartcard, such as those used for Contactless banking payments, or contactless travel schemes such as Oyster or ITSO.

1.1.2 Contactless ticketing in Transit

Contactless smart card technology has become an increasingly significant in initiatives to improve ticketing security and efficiency in the transport sector. Schemes such as the Octopus card in Hong Kong and the Oyster card in London have shown the value of such a scheme in increasing speed and convenience with more robust protection against counterfeit ticketing.

A number of standards and specifications are available in the transit sector, one of which is ITSO. More detail is given below.

1.1.2.1 CEN 1545

This is an international standard that defines the structure of data elements for use in smart card based transport systems. The most recent version was published in 2006 and has two parts:

- Identification card systems - Surface transport applications - Part 1: Elementary data types, general code lists and general data elements
- Identification card systems - Surface transport applications - Part 2: Transport and travel payment related data elements and code lists

These two documents define the building blocks necessary to create a standard set of data elements and code lists for use in the creation of surface transport related data sets which may reside on a transport card.

CEN 1545 explicitly states that compliance with these specifications does not ensure for interoperability. It is left to the application builders to provide for interoperability.

1.1.2.2 CEN 15320 (IOPTA)

CEN 1532, more commonly referred to as IOPTA (Interoperable Public Transport Applications) was most recently updated in 2008.

IOPTA describes the minimum requirements for an interoperable transport application that may exist on a machine readable card. IOPTA is technology neutral, describing data sets, security requirements and card / terminal interactions at the logical level.

1.1.2.3 ISO 24014-1

Last updated in 2007, ISO 24014-1 (Public transport – Interoperable fare management system – Part 1: Architecture) defines a common architecture for the implementation of Interoperable Fare Management Systems (IFMS). The IFMS architecture includes definitions of functions such as:

- Management of Application;
- Management of Products;
- Security management.

1.1.2.4 ITSO

ITSO was formed in 1998 to build and maintain a specification for secure 'end-to-end' interoperable ticketing transactions, utilizing relevant ISO and emerging CEN standards. The ITSO Specification supports CEN 1545, 15320 and ISO 24014-1. It is a common specification at both the card and application level, to enable the use of interoperable smart cards in transport primarily in the UK.

As well as maintaining the specifications, the ITSO organisation is also responsible for certifying cards (known as Customer Media) and terminals (known as POSTs) and supplying the terminal security SAMs (known as ISAMs) necessary to implement the scheme.

1.2 Project Objectives

The Transport Technology and Standards Research programme identified NFC as a technology with potential as both an ITSO ticket carrying device and an ITSO ticket reading device (for retail sales and / or ticket validation).

The project objectives were to:

1. Demonstrate the use of an NFC device as a certified ITSO customer medium in a live ITSO environment.
2. Demonstrate additional functionality to enable an NFC device to perform as an ITSO compliant Terminal capable or reading, validating and updating ITSO customer media.
3. Develop the ITSO Specification changes necessary to enable the certification of an NFC device acting as an ITSO terminal as per objective 2.

A further objective to demonstrate NFC devices acting as ITSO *terminals* in the *live* environment was dependent on the enhancement of the ITSO specification being accepted in time. The scope of this enhancement has wider application than NFC and discussions are still

continuing in ITSO Technical and Security Committees. If approved, the enhanced specification would enable trials or implementation of NFC for remote retail/validation.

1.3 Project Partners

Consult Hyperion was the lead organisation for the project and managed the whole project, providing the majority of the effort in project management, trial management, analysis, specification, design, build and report writing.

Consult Hyperion was assisted by the following project partners:

- ***ESP Systex*** (experts in ITSO implementation with certified products). ESP provided some ITSO software components for use on the phone SIM and personalization services to configure the phones for the trial, as well as detailed technical advice throughout the project

- ***MVA*** (incumbent technical consultants to NoWcard) who acted as primary liaison with the organisations involved in the live trial and bridged any gaps between the trial and the transport operators).

We also wish to acknowledge the contribution of the following organisations:

- ***O_2*** provided expert advice on running successful NFC trials, and supplied and unlocked the trial phones;

- ***Nokia*** provided advice on successfully utilising the NFC features;

- ***NoWcard*** and those organisations participating in that scheme, including the bus companies and the local council, provided volunteers to trial the technology.

1.4 Document Scope

This document is intended to provide a clear overview of the research project, its objectives, work packages, results and conclusions.

The scope of the research project is defined in more detail as the individual work packages are discussed in Section 2.

1.5 Reference Documents

This report summarises the findings from a number of project deliverables. For a list of all the project documentation cited in this report, see Appendix A.

1.6 Terms and Abbreviations

The following table lists the common terms and abbreviations used in this report.

Term	Meaning
CM	Customer Medium. An ITSO term referring to the media used to hold a customer product (e.g. a contactless smartcard)
CMD	Customer Media Definition. Refers to the specific hardware specification of the Customer Media.

Term	Meaning
CMD2	One of the eight different CMDs currently defined for ITSO. CMD2 is known as generic microprocessor.
CMD3	One of the eight different CMDs currently defined for ITSO. CMD3 is the definition for ITSO on a MIFARE 4k platform.
CMI	Customer Media Interface. Refers to the device that interacts with customer media (i.e. the device containing the card reader).
ETM	Electronic Ticket Machine
GPRS	General Packet Radio Service, a means of providing a data connection to mobile phones
HOPS	An ITSO term. Host Operator or Processing System
IFMS	Integrated Fare Management System
IOPTA	Interoperable Public Transport Application
IPE	ITSO Product Entity. An ITSO term referring to the data element stored in Customer Media containing an ITSO product.
ISAM	ITSO Secure Application Module (ISAM). An ITSO term for the smart card used to (amongst other things) implement the secure processing required within an ITSO terminal for the creation and validation of ITSO products.
ITSO	Originally stood for Integrated Transport Smartcard Organisation.
MIFARE	A proprietary technology owned by NXP used to deliver contactless applications.
NFC	Near Field Communication
POST	An ITSO term meaning Point Of Sale Terminal.
PDA	Personal Digital Assistant
RFID	Radio Frequency Identification
SAM	Secure Application Module.
SIM	Subscriber Identity Module. The smart card used within a GSM phone to identify it to the network
SRA	Structured Risk Analysis. A Consult Hyperion methodology for the structured analysis of IT systems for the purpose of identifying where those systems might expose the organisation operating them to risk.
STR	Stored Travel Rights, an ITSO product to which value can be credited and debited.
SWP	Single Wire Protocol. An emerging standard defining the communication between the NFC chip set and a secure element held within the GSM SIM.

2 METHODOLOGY

This section describes the different work packages undertaken as part of this project, the objectives of each work package, and the approach taken to meet those objectives.

2.1 Overview

In order to meet the project objectives as outlined in Section 1.2, a number of inter-related work packages were performed, as shown in Figure 1 below:

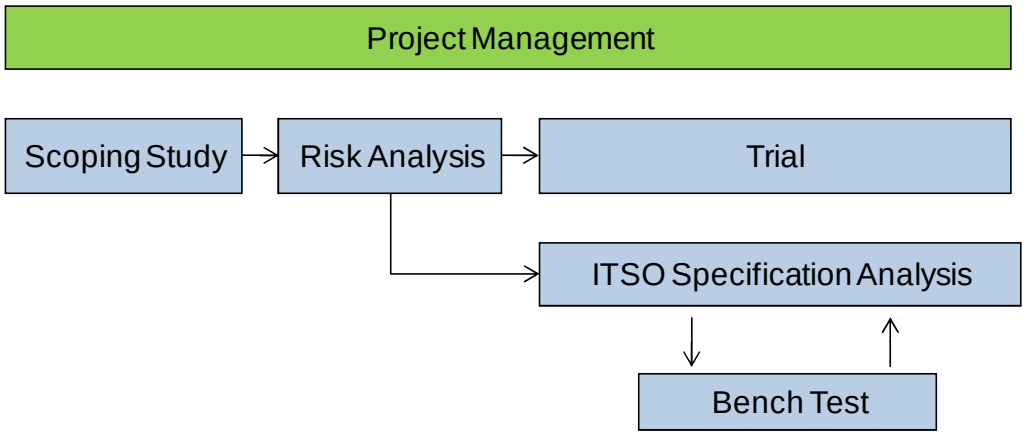

Figure 1: Project work package overview

Each of the work packages shown in Figure 1 is briefly described in the following subsections. A brief description of each of these work packages and how the inter-relate is given in the following subsections. For more detail on the specific approach and findings of each work package can be found in Section 3.

2.2 Project Management

The following table summarises and shows the four layers that were established to ensure suitable project governance, and the organisations that were involved in the various layers.

Project Governance Layer	Summary of responsibilities	Participants
Steering Committee	Presented with project progress at key decision points in the project. Provided advice on these key decisions.	DfT, NoWcard, Consult Hyperion
Project Board	Presented with project progress on a monthly basis. Responsible for project oversight, and review and acceptance of project deliverables	DfT, ITSO, O2, Consult Hyperion

Project Governance Layer	Summary of responsibilities	Participants
Project Management	Responsible for the day to day running of the project, including: • Arranging, preparing and minuting all Steering Committee and Project Board meetings • Maintaining the project risk, issue and action logs • Providing DfT with timely information on project progress	Consult Hyperion
Project Team	Responsible for the execution of the project work packages	Consult Hyperion, ESP Systex, MVA Consultancy

Table 1: Project governance summary

2.3 Scoping Study

The first stage of the project was to perform a scoping study to define in more detail the way in which the tasks outlined in the work specification would be achieved.

2.4 Risk Analysis

After the scope had been fully agreed, a risk analysis was performed on the environment defined in the scoping study to ensure that the use of NFC devices in an ITSO environment did not introduce new security vulnerabilities, i.e. the overall level of security within the ITSO environment should not reduce.

2.5 Trial

Once the project had been fully scoped, and the primary technical and project risks identified and countered, a live trial using NFC devices as Customer Media was performed. See Appendix B for a description of the phone capability developed for the trial.

2.6 ITSO Specification Analysis

In parallel to the live trial, analysis was performed in order to identify and document the minimum changes necessary to the ITSO specifications to enable NFC devices to be used as ITSO POSTs, communicating with an ISAM in a back-office server, based on basic architectural principals outlined in the scoping study.

2.7 Bench test

The main objective of the bench test was to implement and validate the proposed enhancements identified by the ITSO specification analysis.

3 RESULTS

This section summarises the results of the various phases of the project. The issues that arise from these results and the lessons that can be learned are then discussed in Section 4.

3.1 Scoping Study

3.1.1 Objectives

The objectives of the scoping study were as follows:

- To document the requirements for the project, as agreed with key stakeholders
- To use those requirements to identify the technical and logistical scope of the project:
  - ***Technical*:** how should the trials and bench test be defined technically?
  - ***Logistical*:** How should the trials and bench test be carried out from a logistical perspective? Who should be the users, what training do they require, etc?

3.1.2 Approach

In order to meet the above objectives, the following tasks were undertaken:

- A requirements gathering workshop was held with key stakeholders;
- A number of technical options were identified regarding how the work could proceed;
- The requirements and technical options were reviewed by Consult Hyperion, MVA, ESP and ITSO;
- Preferred options were identified, and the reasoning behind those choices were documented, reviewed by the Project Board and approved by the Steering Committee;
- A project plan was produced to define the path to delivery.

3.1.3 Findings

The analysis performed in the scoping study led to the following key decisions being made.

- The trial would use a Nokia 6131 phone as ITSO customer media in the live operating environment. The primary reason for this was that it was the only commercially available NFC handset freely available at the time the purchasing decision had to be made.
- The ITSO Shell set-up and ticket types supported were defined in order to be compatible with the live scheme chosen. It was decided that the set-up should be identical to a card type already trialled within NoWcard so as to minimise issues arising that are unrelated to NFC.
- The three organisations to provide trialists were identified. By splitting the trialists across 3 organisations it was hoped to increase the resilience of the trial.

The scoping study also resulted in the logistical and commercial scope of the project, including:

- Resource plan for ITSO specification analysis and bench test development;
- Other project planning:
  - Definition of the project communication strategy;
  - Definition of the project data protection strategy.

3.2 Risk Analysis

3.2.1 Objectives

The primary objectives of the risk analysis work package were to:

- Identify technical risks from the introduction of NFC into an ITSO environment and ensure suitable countermeasures are available to maintain ITSO security.
- Identify risks to the project, as outlined in the scoping study and identify mitigating actions that can be taken to minimize those risks.

3.2.2 Approach

A two-pronged approach was taken to analysing risk:

- ***Analysing technical risk*:** Technical risks were identified using Consult Hyperion's established Structured Risk Analysis (SRA) methodology
- ***Analysing project risk*:** A systematic analysis of the risks to the tasks outlined in the project plan was undertaken to identify risks to the successful completion of the pilot project

The approach taken to assessing these two types of risk for the project is shown in the figure below:

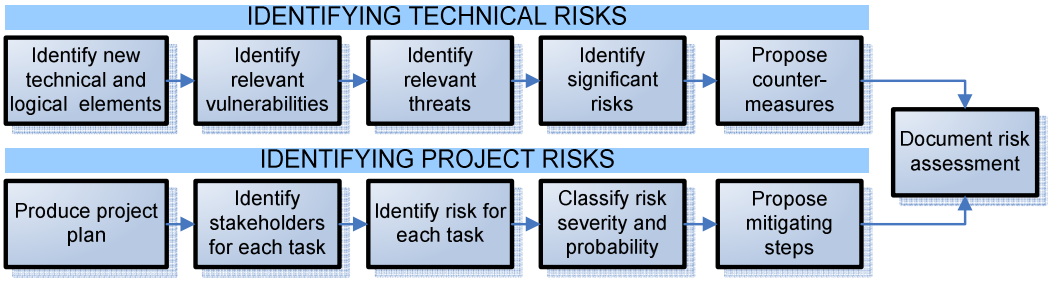

Figure 2: Risk Assessment process

All identified risks were catalogued and suitable countermeasures defined.

3.2.3 Findings

The performance of the Risk Analysis as outlined above led to the identification of a small number of significant technical and project risks.

3.2.3.1 Technical Risks

One significant new area of risk was identified by the analysis for the use of an NFC phone as ITSO customer media, as shown in Figure 3.

.

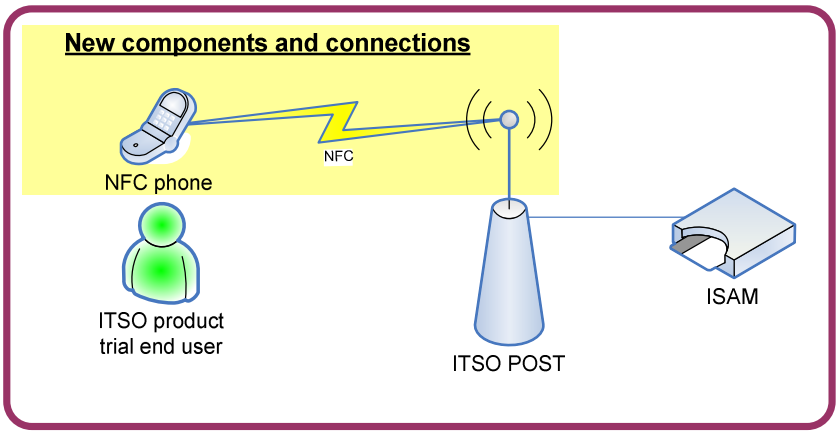

Figure 3: NFC as customer media architecture assessed in Risk Analysis

- **RISK 1:** The NFC phone might be used as a point of attack to attempt to compromise the integrity of ITSO IPEs in order to defraud an ITSO scheme.

  This risk is analogous to potential attacks in other approved ITSO customer media. However, an NFC handset is inherently more complex and flexible than existing ITSO customer media, and therefore merits specific consideration with regard to the risks introduced.

Three further significant new risks were identified by the analysis of the use of an NFC phone as an ITSO POST talking to an ISAM held in a back office server, as shown in Figure 4.

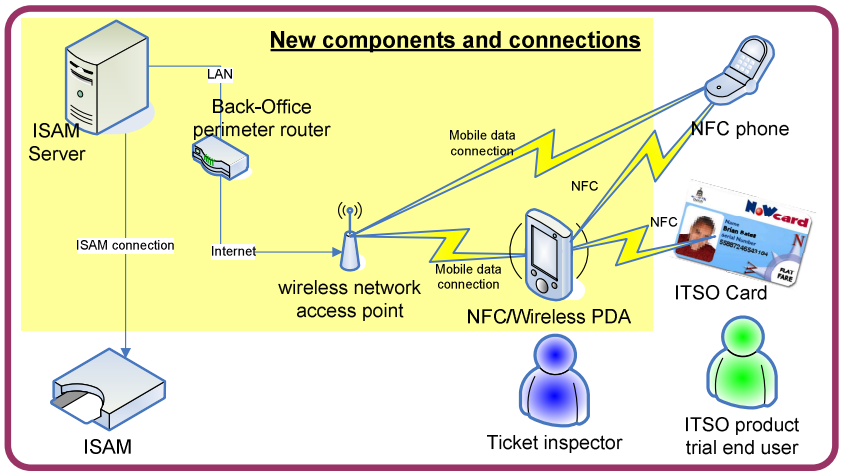

Figure 4: Distributed POST physical model assessed in Risk Analysis

- **RISK 2:** The mobile data connection between the PDA or phone and the wireless network access point may be used as a point of attack to attempt to compromise the integrity of ITSO IPEs (enabling them to obtain fraudulent travel rights) and ISAM communications (enabling them to fraudulently validate a ticket) in order to defraud an ITSO scheme.

  This is a new risk, introduced by the separation of the point of interaction with the ITSO customer media (for validation and sales purposes) from the ISAM, requiring communications with the ISAM to travel over the mobile data connection.

- **RISK 3:** The Internet connection between the wireless network access point and the Back Office perimeter router may be used as a point of attack to attempt to compromise the integrity of ITSO IPEs and ISAM communications in order to defraud an ITSO scheme.

  This is a new risk, introduced by the separation of the point of interaction with the ITSO customer media (for validation and sales purposes) from the ISAM, requiring communications with the ISAM to travel over the Internet.

- **RISK 4:** The Internet connection between the wireless network access point and the Back Office perimeter router may be used as a point of attack to attempt to compromise the confidentiality of ITSO IPEs and ISAM communications in order to discredit the security and privacy protections of the ITSO NFC scheme.

  This is a new risk, introduced by the separation of the point of interaction with the ITSO customer media (for validation and sales purposes) from the ISAM, requiring communications with the ISAM to travel over the Internet.

3.2.3.2 Technical Countermeasures

Two technical countermeasures were proposed to ensure that the risks identified were sufficiently mitigated to maintain the integrity of ITSO security:

- **COUNTERMEASURE 1:** The ITSO NFC phone should undergo full ITSO CM certification, with careful consideration given by ITSO as to whether this new type of customer media is suitably secure to be introduced into live ITSO environments.

  Certification of the phone as customer media has always been the intention for this pilot, before deploying in a live ITSO environment. This countermeasure mitigates against Risk 1.

- **COUNTERMEASURE 2:** A suitable security protocol should be devised (over and above the protection provided by ITSO seals) to protect communication between the ITSO NFC PDA and the ISAM, as this communication travels over insecure networks (i.e. the mobile data network and the Internet).

  This could be using a standard security protocol, such as https, or something proprietary to the distributed ISAM architecture. The most appropriate way forward needs to be decided during bench test design, but some additional security on this communication is required to take into account the fact that it is distributed over insecure networks.

  The techniques required to secure such a system are well understood and in commercial use in the finance and mobile industries.

  This countermeasure mitigates risks 2, 3 and 4.

  The ITSO specification changes put forward must include security requirements that ensure that all subsequent developments in the commercial sector also implement this countermeasure.

3.2.3.3 Project Risks

A number of project risks were identified and managed throughout the lifetime of the project. The five most severe risks and how they were managed are shown in Table 2.

Description	Probability	Severity	Mitigating action
ITSO products might not have worked in the MIFARE emulation required for the NFC phones. This had not been proven prior to the start of the project.	Low	High	This was tested as early as possible in the project. The testing completed successfully
The trial might not have received the necessary co-operation from the participating operators and users.	Low	High	Trial participants were well trained and kept up to date throughout the trial. Relationships already existed between the organizations participating in the trial. Users were incentivised by being allowed to keep their phone post trial.
NFC phones being used as media might have caused damage to ITSO scheme customer media readers.	Low	High	The NFC phones were certified as Customer Media by ITSO. The ITSO certification process makes sure that the phone acts correctly as media in a way that is compatible with compliant readers.
NFC phones being used as media readers might have caused damage to ITSO scheme customer media when being read.	Low	High	The ITSO certification process ensured that any phone used as a reader will interact safely with card media.
It might have been difficult to source the NFC-capable handsets, or handsets of the correct type.	Low	High	A handset manufacturer and mobile operator were invited to be involved in the project. They were able to ensure access to quantities of suitable handsets at a time when they were not commercially available.

Table 2: Summary table of high severity project risks

3.3 Trial

3.3.1 Objectives

The objective of the trial was to assess the suitability, both technically and operationally, of NFC devices as ITSO customer media.

3.3.2 Approach

The requirements gathering process during the scoping study was used to discuss, define and approve the scope of the trial.

The approach to running the trial was as follows:

- A maximum of 50 trialists would be supported (the final number used was 40);
- The trial would run for six months;
- Trialists were split across three organisation to minimize the possibility of organisational issues biasing the trial results;
- Three different bus fleets were used to minimise the possibility of bus specific issues biasing the trial results;
- A summary of the trial was provided to key stakeholders within the organisations providing trialists;
- A training session was provided to these key stakeholders showing them how to use the phone, and enabling them to pass on the training to others;
- A comprehensive User Manual was provided to all trialists;
- A support website was made available to all trialists;
- A detailed set of operational procedures were established and carried out periodically throughout the trial to ensure things ran as smoothly as possible;
- Trialists were requested to provide weekly feedback on phone usage
- Multiple channels were set up to gather both empirical and subjective trial results:
    - Weekly feedback reports via support website or phone;
    - An exception reporting process via trial co-ordinators;
    - Back office data gathered from NoWcard;
    - An end of trial questionnaire;
- The trial results were analysed and a final report produced for DfT.

Before the trial could take place there were also a number of technical tasks that had to be completed:

- The loading of ITSO shells to the NFC phone by ESP Systex
- The Certification of the phone as customer media by Integri
- The development and testing of the software on the phone to enable the customer to interact with their ITSO shell to read last 3 transactions, balances etc.
- The development and testing of web and phone feedback and support applications
- The personalisation and delivery of the trial phones to the trial co-ordinators

See Appendix B for a description of the phone capability developed for the trial.

3.3.3 Findings

A four pronged approach was taken to gathering trial data:

- ***Weekly feedback reports*:** trialists were encouraged to fill in a simple feedback report on a weekly basis, indicating the amount they had used the phone, and the extent to which that usage had been successful.
- ***Exception reports*:** trial co-ordinators were provided with a means to contact the project team to report any significant errors on behalf of their trialists.

- ***HOPS transaction logs*:** the transaction logs from the NoWcard HOPS were processed to extract details of all successful transactions performed with trial phones.
- ***End of trial questionnaires*:** upon completion of the trial, each trialist was requested to fill in a brief questionnaire detailing their experiences during the trial.

The results gleaned from each of these four approaches are summarised in the following subsections.

3.3.4 Weekly feedback reports

The trialists were provided with a mechanism via their phone or via the trial support website to provide weekly feedback reports regarding their usage and experience with the phone over the previous week. An analysis of these reports alongside the data taken from the HOPS transaction logs (Section 3.3.6) identified that:

- The peak usage of the trial was in the first two months;
- The reliability of the trial technology improved considerably during the last two months of the trial.

These trends are consistent with known issues identified in the Exception reports (see Section 3.3.5).

3.3.5 Exception reports

The trialists were able to report specific issues to their trial co-ordinator. Over the course of the trial, 40 such exceptions were raised. Analysis of these reports led to the following findings:

- The vast majority of the errors reported were due to a specific hardware problem on one fleet of buses, unrelated to the NFC trial. When this hardware fault was resolved with two months of the trial still to run, reliability improved considerably.
- A specific problem with the NFC phones was identified. The NFC phones used in the trial, Nokia 6131 have an embedded antenna that is significantly smaller than that embedded in a standard contactless card. As a consequence, the distance from which the phone can successfully communicate with a bus ticket machine is shorter. This led to the phone being more susceptible to torn[1] transactions.
- The increased susceptibility to torn transactions identified a possible issue with the bus ticket machines with regards to how they recovered from torn transactions. The full diagnosis and resolution of existing ticket machine issues were beyond the scope of this trial. However, a detailed technical report of our findings was provided to NoWcard technical consultants to enable further investigation.

3.3.6 HOPS transaction logs

Detailed transaction logs were provided to the trial team from the ITSO scheme HOPS. In total, 1,476 transactions were performed over the trial period. Analysing these logs alongside the weekly feedback reports led to some interesting results.

- Trialists coming from one bus operator experienced no failed transactions at all during the trial period (out of 198).

[1] A torn transaction is one where the phone is removed from the reader before transaction processing has successfully completed.

- Transaction failures dropped considerably (by circa 50%) after the identified terminal hardware issues on the other bus fleet were fixed.
- The transaction logs showed some STR balance discrepancies. This finding was consistent with the potential terminal problem identified with regards to the handling of torn transactions that had already been reported to NoWcard technical consultants.

3.3.7 End-of-trial questionnaires

All trialists were presented with an end of trial questionnaire and requested to fill it in by their trial co-ordinator, but, as anonymous volunteers, were under no obligation to do so. Twenty-five trialists returned the end-of-trial questionnaire. These were evenly spread across the three trial organisations.

Ten representatives attended a detailed debrief session to discuss the trial results, including the trends identified in the analysis of the questionnaire. None of the trialists attending this debrief were aware whether any of the 15 non-respondents did not respond for negative reasons (e.g. disappointment with the technology or neutral reasons e.g. simply too busy). Therefore, the results summarised below are assumed to be indicative of the trial population as a whole.

The following list summarises the responses received:

- "Do you prefer using a phone or a card?"
  - 14 had also had experience of using a NoWcard. Of these 14, three expressed a preference for the card.
- "Did you find the phone application helpful?"
  - All respondents were positive about the value of the phone application enabling ongoing access to card balance and the last three transactions.
- "Was there anything about the trial that wasn't made clear to you in the training material you were provided with?"
  - All were happy with the training material for users.
  - Concern was expressed that more driver training should have been given.
  - One user pointed out that if they had been aware of the intermittent nature of some faults that would have helped.
- "If the technology was offered as a full service, would you prefer to use a card or a phone?"
  - Three trialists expressed a preference for a card:
    - Two because they don't always carry their phone.
    - One because they had concerns over the reliability of the phone technology.
- "When you provided feedback, did you mostly use the phone application or the website?"
  - All the respondents preferred the phone in general, though one did express that the website was more useful for in depth feedback.
  - The phone is always with you at point of use.
  - The website log-in process was a barrier to entry.
- Fifteen respondents took the opportunity to provide additional feedback

- Four users expressed particular enthusiasm in seeing the technology rolled out.
- Ten users highlighted the importance of driver training and support.
- Five trialists stated that initial problems with ETMs had tarnished their experience.
- Three users pointed out the importance of fall-back procedures when technology fails.

3.4 ITSO Specification Analysis

3.4.1 Objectives

The objective of this work package was to define the necessary ITSO specification enhancements to enable NFC devices to be used as ITSO POSTs.

The business requirements for the ITSO specification enhancement analysis performed were driven by recognition that they should be consistent with the requirements underpinning the ITSO specification. These can be summarised as follows:

1. **The NFC POST shall be capable of performing all the functions of a standard POST**

   The Work Specification for the research made clear that it should investigate the possibility of NFC devices being used for all ITSO POST functions (Retailer, Service Operator, Application Issuer). Therefore the NFC POST should be capable of being certified as meeting all existing POST requirements.

2. **The NFC POST shall be at least as secure as a standard POST**

   The research must provide evidence that the proposed enhancements to the ITSO specification do not increase the risk of fraud within an ITSO environment. This may result in new security requirements for NFC POSTs in addition to existing POST security requirements.

3. **All CMDs shall be supported unless it is not possible to do so without compromising security**

   The research project was tasked with maintaining the principal of enabling all cards to interact with all terminals or provide compelling evidence as to why this was not possible.

4. **The recommended ITSO enhancements should not favour any particular implementation, where options exist**

   The resulting recommendations should be generic technical requirements, constraining implementation as little as possible.

5. **The recommended ITSO enhancements should not unnecessarily hinder relevant commercial activity of which DfT or the research team are aware**

   The only relevant work identified was an *ISAM-Array proposal* that had been submitted to, and discussed by, the ITSO Technical Committee. All aspects of this proposition that weren't deemed to be in conflict with the other requirements were included in the first Part 11 draft written by Consult Hyperion.

The significant departure from the existing specification was:

6. **The ISAM shall not be co-located with the card reader**

The possibility of including an ISAM in an NFC device was discussed during the project scoping study, but this would be another implementation of a standard POST. Only the distributed approach was therefore pursued

3.4.2 Approach

The approach to this work package was as follows:

- An initial proposal of the required specification changes was drafted based on the technical conclusions of the Scoping Study and the findings of the Risk Analysis.
- The initial proposal was reviewed by DfT and ITSO and updated based on comments provided.
- The bench test was implemented in accordance with the recommended enhancements in order to assess their viability.
- A final enhancements recommendation was produced once the bench test was complete.
- The final set of enhancement recommendations were then used as the basis for producing a draft ITSO Part 11 for submission to the ITSO Technical Committee.

3.4.3 Findings

A number of basic principles were used to shape the recommended ITSO specification enhancements. These principles are taken from a number of different sources.

From the ITSO specifications, any specification changes:

- Must maintain interoperability, loss-less data transmission and security.
- Must not favour particular implementations.

From the project Risk Strategy:

- The new risks introduced by decoupling of the ISAM from the Customer Media Interface (CMI) must be directly addressed.

From existing relevant proposals to the ITSO Technical Committee:

- An ISAM Array, with distributed Card Media Interface(s) is a core enabler to allowing innovative service delivery (such as NFC POST devices).

With these principles in mind, the following enhancements were deemed to be necessary to allow NFC devices to be used as ITSO POSTs:

1. Strong Mutual Authentication is required between the back-office systems and the Customer Media Interface. This will require secure hardware (e.g. a mobile phone SIM) within the device reading the ITSO Customer Media.
2. Data between the back-office systems and the Customer Media Interface shall be encrypted.
3. If the above requirements are met, then special provision does **not** need to be made in the specification to allow for the restriction of acceptable CMDs at the ISAM Array, and no restrictions need to be placed on the functionality of an NFC POST, beyond the existing requirements on a standard POST.

3.4.4 Alternative Approach

The recommendations of this project were presented to the ITSO technical committee and, whilst it was acknowledged that the recommendations were necessary to meet all the

objectives defined in Section 3.4.1, there is interest amongst the ITSO community in an alternative approach that is technically simpler, but with some operational limitations.

The alternative approach would be to have a Customer Media Interface without the additional security defined in this section, but reducing exposure to risk by restricting its usage to certain operational scenarios, and limited Customer Media types. Whilst this would not satisfy research objectives 1 and 3 in Section 3.4.1, it does have potential commercial application provided the necessary ground work is done to ensure it is implemented securely, and suitable agreement is reached that allow such a device to be restricted to communicate with a subset of ITSO Customer Media.

3.4.5 Conclusion

The proposal put forward by this project enabled an NFC device to be used in a distributed architecture as if it were any other POST device, with no restriction on usage or architecture. The downside, however, is a more complex client implementation, which may not be attractive to implement in non-NFC contexts.

The alternative approach would be able to be implemented using far simpler clients, but particular POST implementations would need to be assessed in order to understand and mitigate potential fraud (for example, this approach might be suitable for downloading tickets to a phone after purchasing over the internet, but not for implementing a hand held ticking device for a train guard). Also, the alternative approach would not be suitable for use with some of the cheaper CM types that have less security capability built into the card.

It may be that both approaches have a future role depending on the operational requirement. The simpler alternative approach described above is currently being pursued for ITSO Part 11 in the Technical Committee.

3.5 Bench Test

3.5.1 Objectives

The objective of the bench test was to implement the proposed ITSO specification enhancements in order to identify any changes necessary to the recommendations before delivery.

3.5.2 Approach

The following approach was taken to produce the bench test:

- A functional specification of the bench test was produced;
- The functional specification was reviewed by DfT and ITSO and updated based on feedback proved;
- A technical design was produced based on the functional specification;
- The bench test was implemented and tested based on the design specification;
- The bench test was demonstrated to the steering committee;
- A bench test final report was produced detailing the outcome of the bench test.

The bench test functional specification defined a high level architecture as shown in Figure 5.

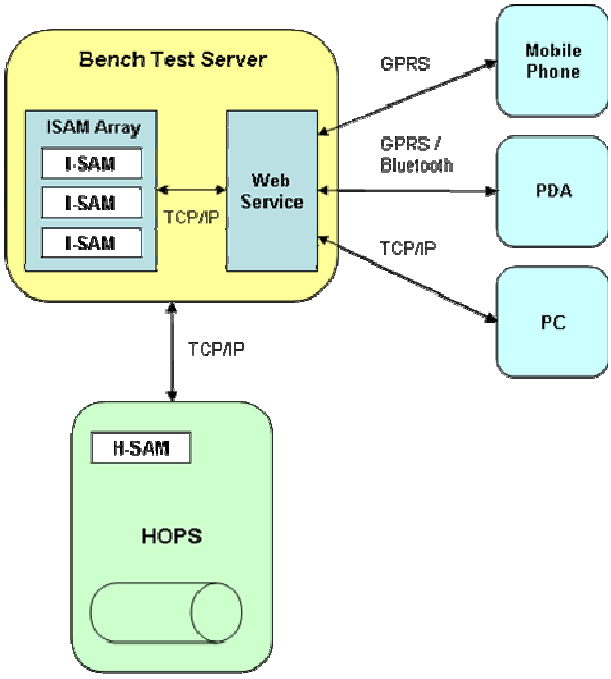

Figure 5: Bench test architecture

The function specification defined a number of use cases for which this architecture was used:

- Top-up of value for the purchase of travel on mobile phone via mobile phone application;
- Validate ticket products on mobile phone or card using a PDA;
- Top up of stored-value on mobile phone or card using PC based terminal;
- Addition of Product (Concession) to mobile phone or card via PC based terminal.

All the use cases were implemented with the mobile phone operating as both CMD2 & CMD3 in order to provide a more complete picture of the impact of the proposed ITSO Specification enhancements.

The bench test technical specification defined the technical implementation of the use cases in the functional specification, including detailed design of the message flows for both CMD2 & CMD3 for the implemented use cases. Figure 6 shows an example of one of the message flows from the bench test technical specification.

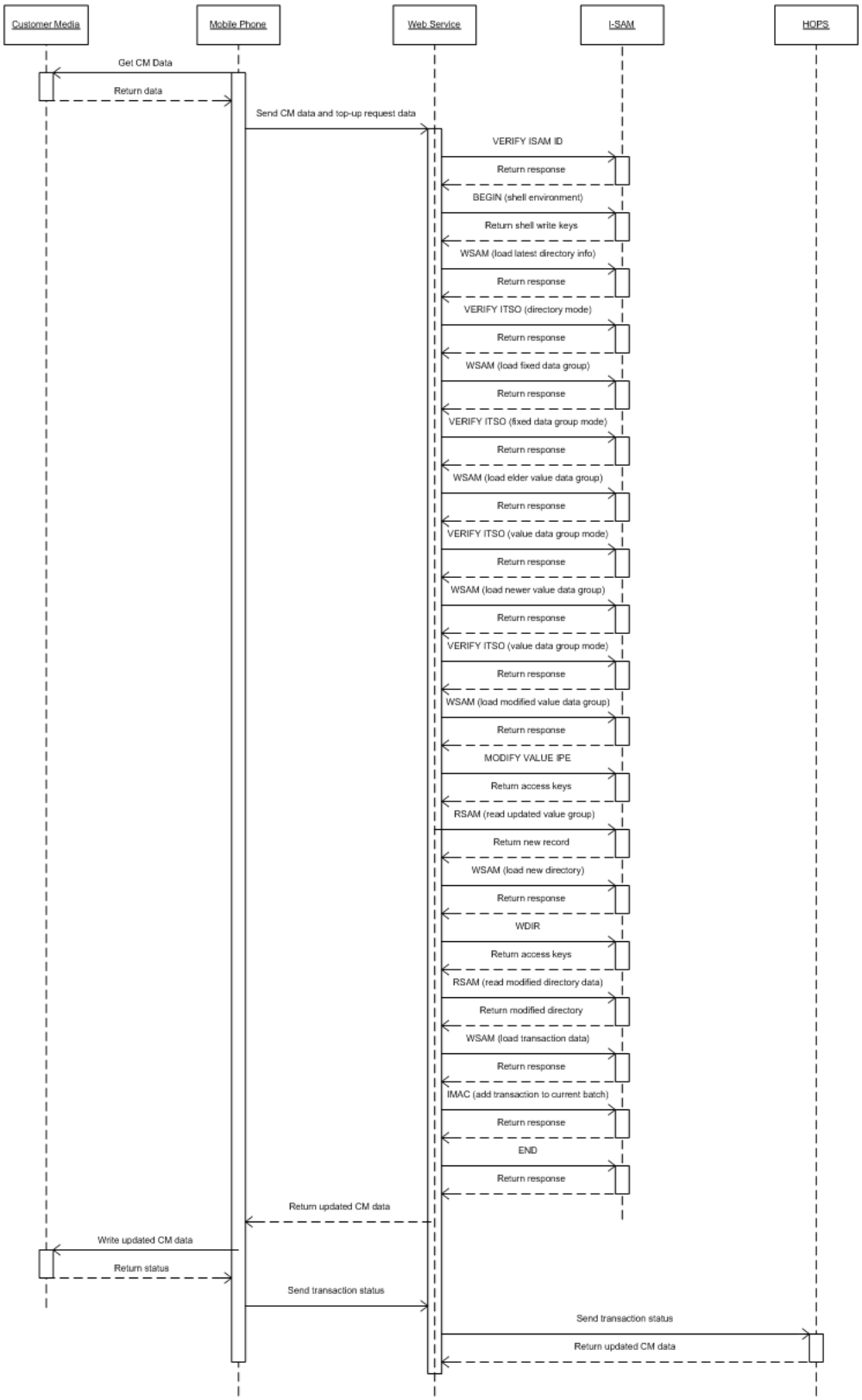

Figure 6: Mifare top-up message flow

In order to test out the recommended ITSO specification enhancements, a new security layer was implemented between the web service and the Customer Media Interface (CMI), as shown in Figure 7

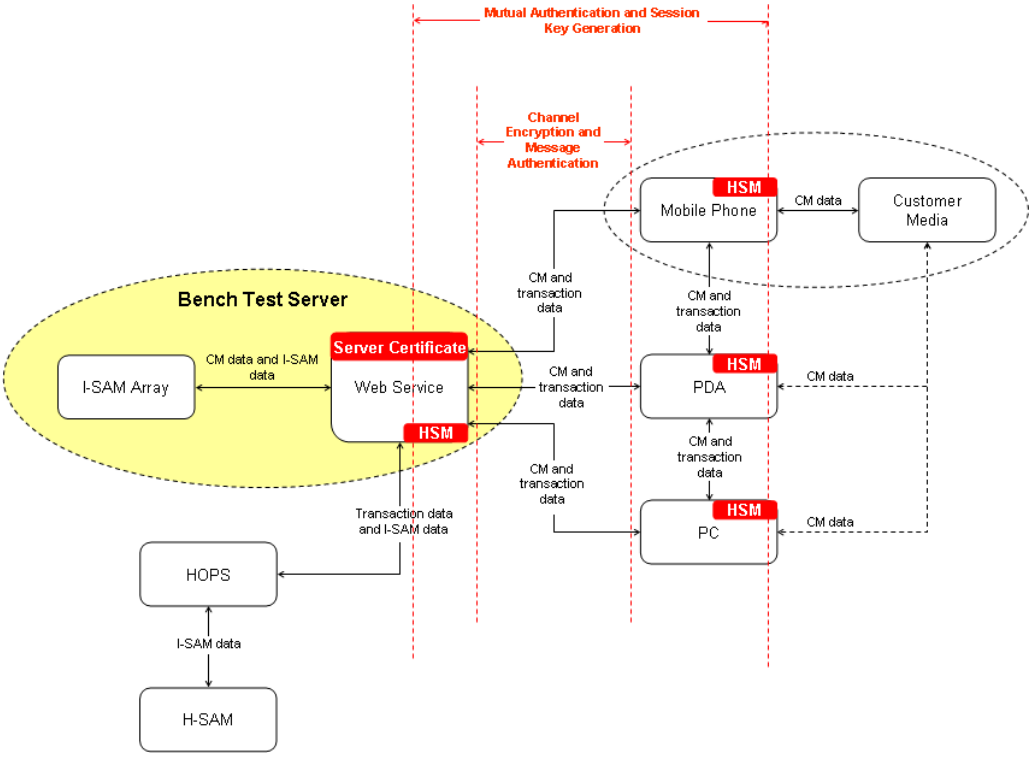

Figure 7: Bench test security layer

3.5.3 Findings

Transaction bench marking was then performed across all the use cases in order to identify the impact of this additional security on transaction performance. The bench test was not optimized for speed or reliability; therefore the results were purely comparative and not indicative of potential real world performance.

The results were as follows:

- Provided that the master key for a given CMI (e.g. phone, PDA or PC) is suitably stored and processed in secure hardware, it makes sense for derived session keys to be used in software environment to improve transaction performance (provided the lifetime of each session key is limited to a single transaction or one minute, whichever is sooner). This improved the efficiency of the bench test security layer by a factor of three.
- The increase in transaction times from the addition of the security layer shown in Figure 7 is considerably less than the difference between using CMD2 (Generic Microprocessor) and CMD3 (MIFARE 4K) without any additional security. This is due to the overhead of implementing secure messaging for CMD2. E.g. MIFARE using a distributed POST architecture and the additional security required to protect it is still significantly faster than a generic microprocessor card without the additional security. In our bench test environment, an unsecured CMD2 transaction was just

over one second slower than an unsecured CMD3 transaction. Adding the security layer to both CMD types lengthened the transaction by approximately 300 ms.

- The biggest single factor influencing transactions times across the three different client platforms tested on the bench test was the different communication networks used between the CMI and the Web Service. Communications where network latency and transmission times are highly variable give the most widely distributed results and the worst performance, as evidenced by the data gathered using Bluetooth and GPRS compared to a fixed line.
- The bench test analysis also looked at the impact the different CMI platforms and the different transactions types performed had on transaction performance, however, these were insignificant in comparison to the impact of the three factors mentioned above.

4 DISCUSSION

This section presents the points of interest to come out of the research described in the previous two sections. A number of issues arose, and a number of lessons were learned from the work. These issues and lessons fell into two basic categories:

- ***NFC*:** The majority of the points of interest that arose were directly related to NFC phones or supporting technologies;
- ***ITSO*:** Some of the issues were not directly NFC related, rather, were specific to the problem of implementing ITSO on an NFC device.

4.1 NFC

The following subsections detail the issues identified and lessons learned that come directly from the use of NFC technology.

4.1.1 Phone read range

As outlined in Section 3.3.5, the NFC phone used, the Nokia 6131, has an antenna that is considerably smaller than that in a standard contactless smartcard. Thus, whilst from a processing and security perspective the NFC phone operates as a standard Java Card, where it does differ is in the physical dimensions of the radio antenna embedded in the device.

This smaller antenna meant that terminals could not read the NFC phones from as far away as a standard card. In our laboratory testing the phone read range read (2.5 cm) was only around 40% the read range of a standard card (6 cm). This lead to the phone being more vulnerable to transaction "tearing". A torn transaction is one where the processing on the card is unable to successfully complete due to it being forcibly removed from the terminal's RF field too early. If the distance away from the Terminal at which that RF field is strong enough to communicate with the card is short, then the probability of tearing is increased.

This problem is not a problem with NFC in general, rather it is a feature of the Nokia 6131 handset in particular. For example, Nokia's next generation NFC phone (6212) has a considerably larger antenna, and therefore is not anticipated to experience this problem. The Nokia 6131 was used for this trial because it was the only commercially available NFC handset when the project began. More and more NFC handsets are appearing. The ITSO certification process will need to be streamlined to deal with the extremely high turnover of such handsets (replaced on average every 18 months with a new model).

It is likely that a majority of the errors reported when the phone did not work at the first attempt, and then worked on subsequent re-presentment, were torn transactions, due to this fact that the trial phones were more prone to tearing than cards. It would also explain why there seems to be considerable variance in the error rates from one individual to another. For example, when looking at the five heaviest users amongst the trialists, two did not report a single transaction failure, whereas one experienced a trial error rate of at least 30%. The extent to which an individual experiences torn transactions with a device that is prone to such an error will be dependant on the presentation technique of the individual. For example, do they put the phone on the reader or hold it just above? Do they wave it or keep it still? How long do they leave it there? Also, the physical orientation of the terminals varied between bus fleets. On one bus fleet, the card reader was horizontal, allowing the phone to be placed onto the reader and let go. However, on another fleet, the reader was at an angle, meaning that trialists using these buses had to keep hold of the phone throughout the transaction.

All these factors would significantly increase the likelihood of a torn transaction.

4.1.1.1 Lessons learned

- Read range is a key factor in the reliability of a contactless ticket. Particularly in a high throughput, "touch and go" environment such as transit.
- User technique in presenting the phone to the reader can have a significant impact on reliability.
- The physical location and orientation of card readers can affect user practice, and therefore transaction reliability.

4.1.2 CMD Issues

The ITSO specification currently supports eight different card types (CMDs). The ITSO cards currently in circulation are dominated by two of these types:

- CMD2 – Generic Micro-processor;
- CMD3 – MIFARE 4K.

The NFC chip in the Nokia phone used for the trial is a Java Card, which is a type of generic microprocessor card, and therefore capable of acting as CMD2. It was also capable of emulating CMD3.

At the start of the trial, the NoWcard ETMs were only able to support MIFARE, and the scheme had a derogation from ITSO to allow that situation.

However, the derogation was due to expire during the trial. Therefore it was highly likely that the ETMs would be upgraded to support all other CMDs (including CMD2) during the trial period.

Whilst the derogated terminal worked with a MIFARE emulation, the ITSO specifications contain clauses that disallows a fully compliant POST from accepting a generic microprocessor card (CMD2) emulating a MIFARE card.

For these reasons the phone was issued with the capability to act as both MIFARE and generic microprocessor.

The phone was used as MIFARE for the first four months of the trial and generic microprocessor for the last two months.

4.1.2.1 Issues with MIFARE

During the course of the trial ITSO decided to discontinue MIFARE as an ITSO CMD. MIFARE Cards will no longer be able to be issued after the end of 2009, and all MIFARE cards will be removed from circulation by the end of 2016. This is due to a security flaw with the platform highlighted by recently published academic research.

Thus, a future NFC implementation of ITSO Customer media would not be able to do so by emulating MIFARE after the end of 2009. A number of NFC secure elements are based on Java Cards with built in MIFARE emulation capability. However, similar products are also able to emulate DESFIRE, which is the CMD type most likely to replace MIFARE as the most issued type in the medium term.

4.1.2.2 Issues with generic microprocessor

The generic microprocessor CMD type supports a secure messaging protocol that requires far greater interaction between the terminal and the card than MIFARE. Therefore, even though the computing power of the card is greater, the ITSO transactions are typically considerably

slower. This was certainly a fact confirmed by the results of our bench test, where typically generic microprocessor transactions took three times longer than MIFARE transactions.

The transaction times for CMD2 platforms currently deployed have led ITSO, during the course of the trial, to put a timetable in place for discontinuing CMD2 implementations that do not meet a newly defined minimum benchmark transaction time. The implementation of CMD2 used in the bench test would not be able to meet this new benchmark. One possible way round this would be through allowing CMD2 card platforms unable to meet the requirements to emulate other, faster media such as DESFIRE, however, under current ITSO rules, a fully compliant ITSO POST is not allowed to interact with a generic microprocessor card emulating a less secure alternative CMD (forcing the generic microprocessor to be used).

4.1.2.3 Lessons learned

- Despite being considerably slower based on lab analysis, the speed disadvantage of CMD2 was not noticed in the trial. The speed of interaction between the card and terminal is not necessarily the bottleneck, depending on how the customer experience has been implemented. In the trial, the additional second required to process CMD2 made no discernable difference to the trialist experience, as the overall time it took the bus driver to interact with the ETM was considerably longer than the actual transaction time.

4.1.3 Accessibility Issues

A number of issues relating to accessibility were raised during the trial by users that provided useful lessons to anyone wishing to roll out NFC services to a wide demographic:

- Size of display, brightness of display and font size can be a real barrier to some customers.
- Familiarity with mobile phones varied dramatically and made a significant difference in user confidence when interacting with the trial phones.

4.1.3.1 Lessons learned

- Phone applications that allow users to interact with their ITSO data should be configurable to maximise accessibility (e.g. font sizing, audible interaction, etc.).
- User training is vital to helping achieve a minimum level of competence with the technology to avoid the customer having early bad experiences with a tool that should be a benefit.
- Driver training is equally important. A suspicious or uncertain driver will only compound the issues experienced by unconfident customers.

4.1.4 NFC provisioning Issues

There are wider issues to do with NFC that, whilst beyond the scope of this particular project, are important to consider for any future live services and therefore worth outlining in this report.

The model for issuing and personalising mobile phone ITSO applications has the potential to be far more complex than that for a card. The application issuer is not necessarily the hardware issuer, creating security, commercial and logistical issues.

4.1.4.1 Security Issues

In our trial, the phones were personalised in a bureau in the same way as a card, before delivery to the customer. Thus we were able to use existing card processes. In the future, it is

expected that NFC phones will have applications and content loaded over the air using secure protocols. However, these protocols were not in place at the time of this project.

4.1.4.2 Commercial Issues

For a real service, the relationship between the hardware owner (the mobile phone operator) and the application issuer need to be carefully defined, particularly with regards to exception handling and customer service handover.

4.1.4.3 Logistical Issues

Once an NFC phone with an ITSO application has been successfully provided to a customer, there are a number of on-going issues for a phone that do not apply to a card:

- What if the customer changes mobile operators?
- What if the customer upgrades their phone?
- What if the customer's phone application is deleted?

A mobile phone service can be delivered using existing card personalisation processes, however it is unlikely to be the most desirable approach when delivering services on a large scale.

Mobile phone standards bodies are currently working on business models and standards to enable such services to be securely delivered directly to the mobile phone, whilst in the hand of the customer. However, it may be a while until such standards are mature.

4.1.5 NFC devices as terminals

The bench test focussed on the potential for using NFC devices as ITSO POSTs. The results of the bench test, make it clear that such a device is viable, but there are performance and reliability issues (depending on the implementation) that limit its applicability to carefully selected operational use cases.

4.1.5.1 Lessons learned

- NFC devices are capable of being made sufficiently secure to act as an ITSO POST for all transaction types to all customer media types.
- Whilst technically capable of performing as an ITSO POST, functional, performance and reliability issues will mean that in practice, NFC devices will be most suitable for use in particular operational use cases (e.g. devices with good, high speed online connections, and lower transaction throughput requirements). For example, Figure 8 and Figure 9 show the performance over 20 transactions of a stored value top-up transaction using the bench test. The first figure shows top-up via a mobile phone, using GPRS. The second shows top-up via a PC based terminal using a broadband internet connection. The three lines correspond to the implementation of a distributed terminal with an ISAM in a back end server with the following security options implemented:
    - No additional security (this provided a performance benchmark to assess the relative impact of the security on transaction speed but does not comply with the recommended enhancements).
    - Software security. This is when transient session keys only are used in software. Persistent card keys will still only be stored and used in secure hardware.
    - Hardware security. This is when all keys, persistent or transient are only stored and used in secure hardware.

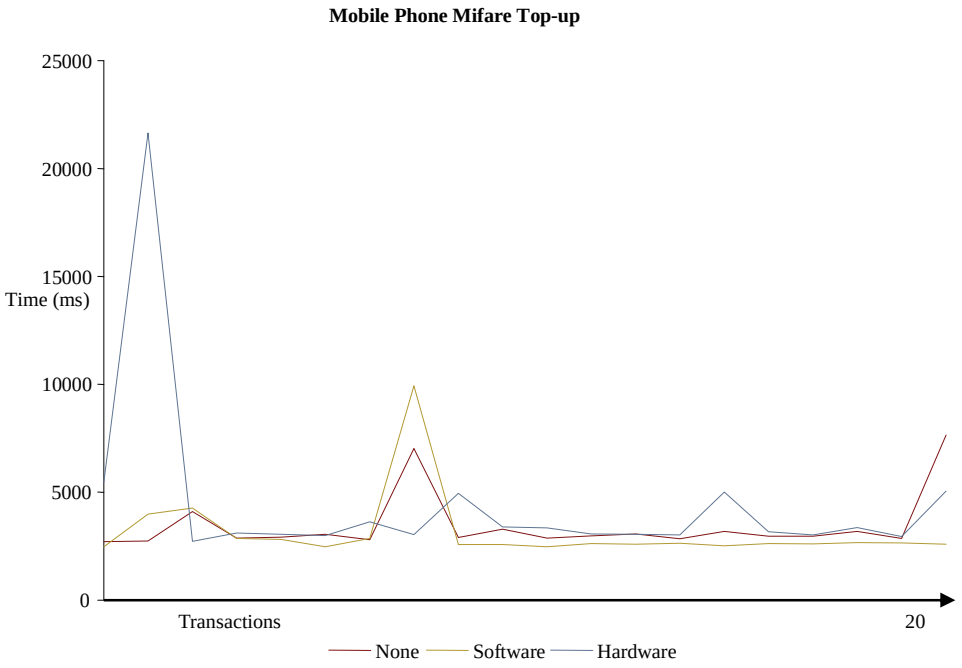

Figure 8: Transaction performance for STR top-up using GPRS

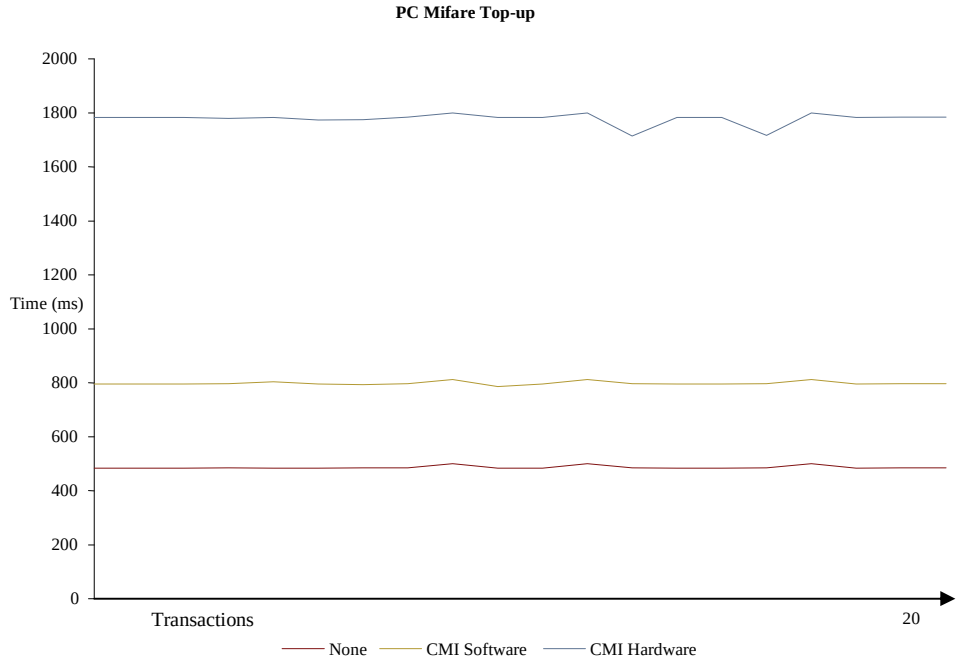

Figure 9: Transaction performance for STR top-up using fixed line internet

It is clear from these figures that different implementations of an NFC terminal will vary considerably in terms of performance and reliability, and not all implementations will be applicable to all terminal use cases. E.g. it may be acceptable for home top-up of your personal balance via your mobile phone to take over 20 seconds one time in 20, but it will certainly not be acceptable at a high-throughput transit gate.

4.2 ITSO

The following subsections detail issues and lessons that have arisen from the project that are ITSO related.

4.2.1 Implementation Issues

There is a considerable amount of complexity in implementing the ITSO specification, the majority of which is to ensure future interoperability. For example, a certified ITSO terminal must be fully capable of interacting with all eight ITSO cards types, even though the scheme within which it is operating may only be issuing one of those card types to its customers. This adds considerable complexity to any ITSO terminal implementation.

Because the ITSO POST development in the research was done in a bench test environment, we were able to focus on the two CMD types capable of being supported by the trial phones (CMD2 and CMD3). However, if an NFC ITSO POST were to be deployed commercially in a live environment it would have to be capable of supporting all eight card types.

According to the scheme operator, one of the side benefits of the trial was that the reduced read range of the mobile phones helped flush out ETM issues that would otherwise have taken longer to identify.

4.2.1.1 Lessons learned

- It was of great benefit to the trial that the phones were used across three different operators. This enabled us to clearly identify faults that were related to ETM configuration issues rather than the NFC phone.
- The complexity of ITSO that is necessary to achieve interoperability places a considerable ETM management overhead on ITSO scheme operators. The pioneer operators are currently working hard to establish processes to ensure that this management can be successfully performed. The lessons they are learning will be of considerable value to future ITSO operators. ETM issues were proven to be the source of the majority of errors experienced by the trialists, and the management overhead and terminal complexity made it very difficult to identify and resolve these issues quickly.

4.2.2 Certification Issues

The ITSO certification process is designed to support the interoperability requirements and necessarily has to test a number of operational and interoperability scenarios that will only occur very occasionally in the current market. This interoperability should provide considerable long term benefit.

With regards to the mobile phone trials, ITSO certification was far less straightforward than initially expected. This was predominantly due to the need for the testing process to be adjusted to deal with non-card form factors, as the existing tests implicitly assume credit-card-sized tokens.

4.2.2.1 Lessons learned

- The ITSO Certification processes are currently card-centric and need to allow for non-card form factors. For example:
    - More read-range testing to ensure different antenna designs function adequately.
    - The ITSO certification service has a very specific remit to perform a set of tests on submitted cards and POSTs and report back on the result and does not currently provide much in the way of diagnostics or assistance in

identifying reasons for failure. For a specification as complex as ITSO, such diagnostic capability would be of tremendous value.

- The issues experienced with ETMs in the phone trial highlight the fact that testing in the lab is not enough to ensure correct operation in the field. It is important that certified equipment is extensively field tested by the scheme operator before deployment, as deploying certified terminals does not, in itself provide adequate protection against transaction failures due to ETM technical issues.

5 CONCLUSIONS

This section concludes what has been achieved against the project objectives. As stated in Section 1.2, the project objectives were to:

1. Demonstrate the use of an NFC device as a certified ITSO customer medium;
2. Demonstrate additional functionality to enable an NFC device to perform as an ITSO compliant Terminal capable of reading, validating and updating ITSO customer media;
3. Develop the ITSO Specification changes necessary to enable the certification of an NFC device acting as an ITSO terminal as per Objective 2.

5.1 Objective 1

Demonstrate the use of an NFC device as a certified ITSO customer medium

The six month trial, described in Sections 2.5 and 3.3 has clearly demonstrated the potential for NFC as an ITSO customer media. The technology worked. The majority of users were extremely positive. Therefore, the conclusion of this project is that NFC technology is suitable for use as NFC customer media today.

However, the following should be considered:

- **CMD2 speed issues.** The majority of NFC phones going forward are expected to use the mobile phone SIM as the secure element. This would mean that under current ITSO specifications they would have to operate as CMD2. It is likely that in the short to medium term it would be difficult to develop ITSO applications for such SIMs that meet the recent clarification by ITSO of CMD2 minimum performance requirements. Further development of SIMs, potentially in co-operation with an interested mobile operator, would be required to overcome this issue. Work is already underway to produce a CMD2 platform implementation that can meet the ITSO speed requirements.

In the short term, NFC market penetration may be a limiting factor for introduction of any widespread commercial services. However, NFC capability is expected to be widespread in most new mobile handsets by the end of 2010.

The question of NFC application delivery will also need to be considered. The technology may currently be best suited to a large closed user group services (e.g. or a mobile operator's customer base or a university campus) such that any phones could be delivered pre-personalised to customer with a pre-established interest in the technology.

5.2 Objective 2

"Demonstrate additional functionality to enable an NFC device to perform as an ITSO compliant Terminal capable of reading, validating and updating ITSO customer media."

In order to achieve this objective with off-the-shelf NFC phones, it is necessary to separate the ISAM from the device and place it in a back-office server. Our risk analysis identified some key new risks that such an architecture exposes. Our recommended specification enhancements and subsequent bench test showed how those risks could be mitigated to ensure overall ITSO security is maintained.

The conclusion of this project is that off-the-shelf NFC devices could be used as ITSO POSTs.

However, the following limitation would need to be considered:

- **Online issues.** The presence of the ISAM in a back-office server means all such transactions have to be on-line in real time. There are some speed-critical operational environments where such a requirement will be a distinct disadvantage. Where speed of transaction is essential, such as a high throughput gating system, a standard POST is likely to continue to be more appropriate to maintain the speed of transactions. As occasional ticket inspection devices, personal terminals, or lower volume terminals (e.g. bus depot ticket offices) however, NFC provides the potential for considerably cheaper hardware alternatives for ITSO POST applications.

5.3 Objective 3

"Develop the ITSO Specification changes necessary to enable the certification of an NFC device acting as an ITSO terminal as per objective 2."

This project developed a set of recommended changes to the ITSO specifications. Discussions with the ITSO Technical Committee highlighted that there were different views on the scope and requirements for the addition to the Specification. An alternative proposal is progressing through the ITSO Technical and Security Committees.

These recommendations (as summarized in Section 3.4) have been provided to ITSO for consideration. There is as yet no indication as to whether they will be accepted in a form that will enable the deployment of the bench test technology in a live ITSO environment.

If suitable specification enhancements were made, the conclusion of this project is that there would be considerable value in implementing those recommendations in terminals suitable for trialing in a live environment.

Such terminals could then be used to test the reliability and performance of an NFC post architecture in various scenarios, enabling:

- Visualisation of tangible commercial applications;
- More accurate figures on reliability and performance.

6 RECOMMENDATIONS

As with Section 4, our recommendations are separated into two sections, those relating to NFC and those relating to ITSO.

6.1 NFC-related recommendations

NFC devices have potential to act as both customer media and POSTs. We recommend that any party looking to pursue either of these ideas commercially consider the following:

1. For customer media
    a. ***Define service delivery model***: The technology for performing transactions is ready, but the standards around service delivery are still maturing. It is important to have a clear and workable service delivery model before commencing deployment. The simplest service delivery model would be one which involves the delivery of phones to customers pre-configured with an ITSO application. Configuration of phone post delivery provides far more flexibility but is far more complex.
    b. ***Consider performance requirements***: A potential stumbling block to commercial services of this kind might be the performance of existing CMD2 implementations. To meet these requirements may require some bespoke SIM card development before a commercial service is viable.
    c. ***Familiarity with technology***: A customer and driver training programme is required if any commercial service is to be successful. This would set their expectations of the technology and ensure that they know what to do in the event of any failures.
2. For POSTs:
    a. Give careful consideration to the operational environment in which you wish to deploy NFC. The bench test results clearly show that distributed terminals will not be suitable for all operational scenarios, as for some (particularly high throughput) environments it will always be preferable for the ISAM to be co-located with the card media interface to ensure optimal transaction speed.
    b. There is a need for extensive user acceptance testing before going live with any ITSO terminals, as it became clear from the trial results that ITSO certification alone may not guarantee successful field operation.

6.2 ITSO-related recommendations

Some things could be done to make engagement with ITSO for the development of this type of technology easier in the future:

1. The presentation of a new form factor for ITSO certification as an existing CMD should trigger some pre-defined processes to consider the wider impacts for security and commercial impact. For example, does the new platform introduce new security risks? How should the new form factor be branded[2]?

[2] As part of this project, Consult Hyperion advised ITSO on the development of branding guidelines for ITSO compliant mobile phones.

2. It would be beneficial to have a more outward facing ITSO resource – “an account manager” who would be able to help members better understand and engage with ITSO processes.

APPENDIX A PROJECT DELIVERABLES

The information provided in this report is a summary of the findings of a number of work packages performed for the DfT. The following is a list of the deliverables produced as part of this project, from which the information provided in this report is taken:

Reference
Bench test Functional Specification, v1.0, 12th August 2008
Bench test Final Report, v1.2, 22nd April 2009
Bench test Technical Specification, v1.0, 9th April 2009
Requirements and Scoping Study, v1.0, 3rd April 2008
Risk Strategy, v1.0, 3rd April 2008
ITSO Specification Enhancement Recommendations, v1.0, 31st October 2008
Scoping and requirements note, v1.0, 1st May 2009
Trial 1 Report, v1.0, 30th April 2009
User Manual, Trial 1, v1.0, 21st May 2008

APPENDIX B TRIAL USER MANUAL EXTRACTS

This Appendix contains extracts from the Trial User Manual that Consult Hyperion wrote to explain to the trialists how to use their phone in place of an ITSO card and also to give trial feedback.

B.1 Using the phone for travel

The phones are configured for use as Stored Travel Rights (STR) products, alongside a Youth Concession. The phones are also configured such that they can support period passes as well. However, the bus ticket machines are set up to give a higher priority to the Youth Concession alongside STR, therefore the period pass will only ever be used if this preference is specifically over-ridden by the bus driver.

B.1.1 Using Stored Travel Rights

Stored travel rights works in a similar way to the change in your pocket. You load up the stored travel product on your phone with value (up to a maximum balance of £50) and then that value is decremented each time you present your phone for travel.

Real money will not be used to top-up the value held on the phone for the purposes of this trial. You will be provided with vouchers to enable you to top-up your application. These vouchers should be handed to the driver when you perform top-up.

If you run out of vouchers, more can be obtained from your trial co-ordinator.

Your phone can be presented to the ITSO card reader on the bus in order to either:

- Top up the stored value
- Debit the stored value (at youth concessionary rates)

All phones will be configured such that the holder will be eligible for youth concessionary rates, irrespective of the actual age of the trialists. This will enable more journeys to be made between top-ups and make the trial more convenient for you.

B.1.2 Using the period pass

The purchase of period passes is beyond the scope of this trial. However, if your phone is configured with a valid period pass, then this will enable you to carry out your trial journeys without having to top-up or debit the STR product.

In this case, you will be required to present your phone to the ITSO card reader on the bus, and the driver will see that you are eligible for travel without any further payment.

If your phone is set up with a valid period pass you will be informed by your trial co-ordinator when it is provided to you.

B.1.3 Presenting the phone to a reader

The Nokia 6131 is a “clam shell” style phone that can be used as a ticket both when closed and when open. We recommend that the phone be presented to the reader in the closed position, face down, with the phone hinge pointing towards you, as shown in Figure 10.



Figure 10: Presenting a closed phone to the bus card reader

The phone should also be read successfully by the reader on the bus if open, provided the screen, rather than the keypad, is presented, as shown in Figure 11 (face down) or Figure 12 (face up).



Figure 11: Presenting the phone to the bus card reader open, face down



Figure 12: Presenting the phone to the bus card reader open, face up

B.2 The NoWcard phone application

Your trial phone contains an application that enables you to see what ITSO data is on your phone, provide feedback and request support.

B.2.1 Starting the application

To start your phone's NoWcard application, do the following:

- Select "Menu"
- Select "Apps."
- Select "NoWcard ITSO Trial"

The application will now start, and you will be presented with the main menu:



Figure 13: NoWcard ITSO Trial application main menu

B.2.2 Card details

If you select card details from the main menu, you are presented with the following screen, informing you of the ITSO serial number allocated to your phone, and the expiry date associated with that serial number. During normal usage, you will not need to access this information; however you may be requested to provide it, if at any time during the trial you require technical support.



Figure 14: Card details

B.2.3 Available products

If you chose to view available products from the main menu, you will be presented with the following choices:



Figure 15: Available products menu

B.2.3.1 Concession product details

When you select to view the Concession product details from the available products menu you are presented with a description of the type of concession, and the expiry date.



Figure 16: Concession product details

B.2.3.2 Stored Travel (NoWcard)

When you select Stored Travel (NoWcard) from the available products menu, you are presented with expiry and balance details, as shown in Figure 17.



Figure 17: Stored Travel product details

If you select “History”, at the bottom of the screen, you will be presented with a record of the last three transactions, as shown in Figure 18.



Figure 18: Stored Travel transaction history

B.2.3.3 Period Pass product details

When you select to view Period Pass product details from the available products menu, you are presented with the Period Pass expiry details, as follows:



Figure 19: Period Pass product details

If you select “History” at the bottom of the screen, you are then presented with details of the last three times the pass was used.



Figure 20: Period Pass transaction history

B.2.4 Feedback

When you select feedback from the main menu, you are presented with a short series of simple questions, the first of which is shown in Figure 21.



Figure 21: First phone feedback question

Depending on whether or not you have used your phone for travel in the last week, you will then be presented with one or two further questions, as described in the following two subsections.

B.2.4.1 If you select zero

If you have not used your phone for travel in the last week, select zero and you will then be given the opportunity to tell us why. You will then be asked to confirm your feedback.

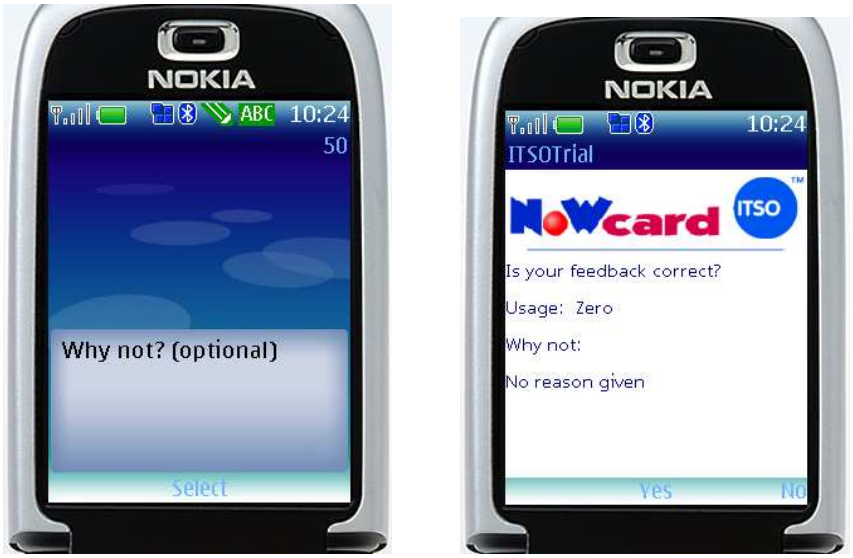

Figure 22: Feedback after no usage in the past week

When asked to confirm your feedback, if you select 'yes', the phone will ask your permission to send a text message containing the feedback report (your phone will be provided to you with plenty of credit to ensure that feedback text messages will not cause you to incur costs). Once this message is sent, the application will return to the main menu. If you select 'no', the feedback will not be sent, and the application will return you to the first feedback question (see Figure 21).

B.2.4.2 If you select one to five, or more than five

If your answer to the first feedback question indicates that you have used the phone for travel recently, then we just want to ask you a couple of questions with regards to how successful that usage has been. If your attempts to use the phone for travel have worked first time, every time, over the last week then the feedback process will work as shown in Figure 23.

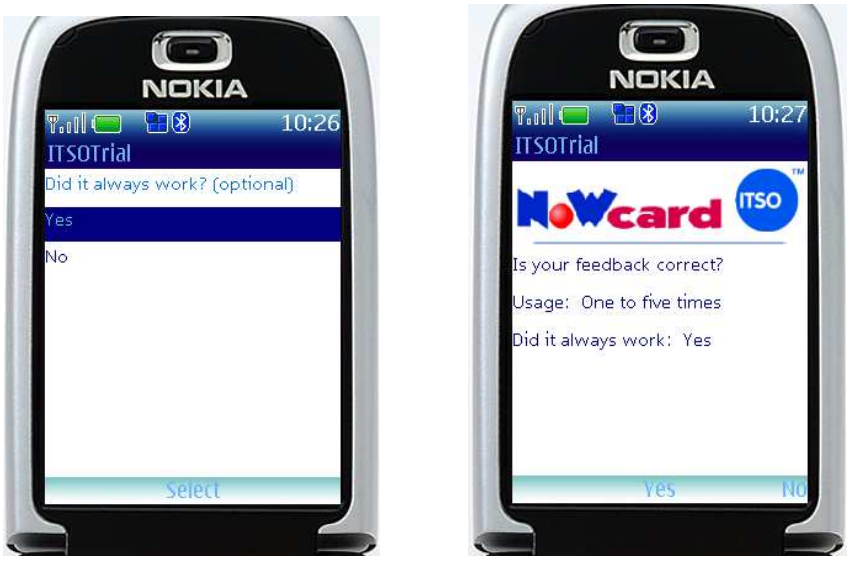

Figure 23: Feedback when phone usage has always been successful

Once again, when asked to confirm your feedback, if you select 'yes', the phone will ask your permission to send a text message containing the feedback report (your phone will be provided to you with plenty of credit to ensure that feedback text messages will not cause you to incur costs). Once this message is sent, the application will return to the main menu. If you select 'no', the feedback will not be sent, and the application will return you to the first feedback question (see Figure 21).

If you have experienced some problems, however, we will also give you the optional opportunity to provide us with more detail about the problems you have encountered. Therefore, after you have selected 'no' to the question did it always work? You will be presented with the following screens:

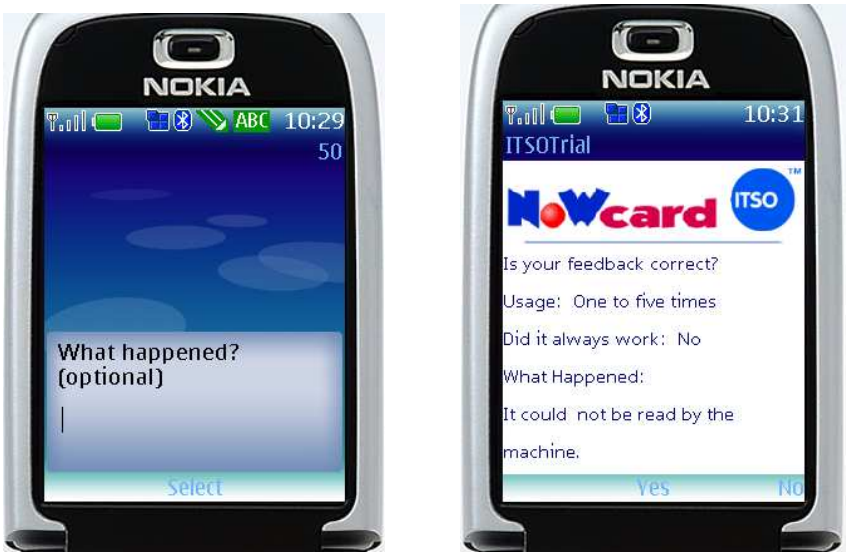

Figure 24: Feedback when phone usage has not always been successful

Once more, when asked to confirm your feedback, if you select 'yes', the phone will ask your permission to send a text message containing the feedback report (your phone will be provided to you with plenty of credit to ensure that feedback text messages will not cause you to incur costs). Once this message is sent, the application will return to the main menu. If you select 'no', the feedback will not be sent, and the application will return you to the first feedback question (see Figure 21).

B.2.4.3 Feedback reminders

If we have not received feedback from you for a while, we may send you a text message, which will cause the phone application to ask your permission to start up. If you click "OK" to this request, the application with start up and immediately present you with the feedback form.

B.2.5 Support

If you have any problems during the trial, there are a number of support options open to you. If you select support from the phone application, you will be presented with the following screen:

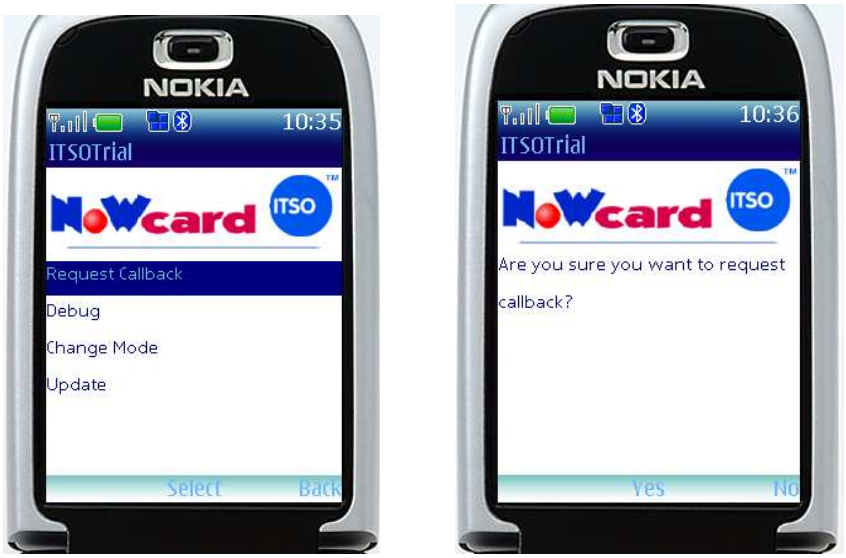

Figure 25: Phone Support menu

END OF DOCUMENT