Project Number IST 2000-26081

Schlumberger

MasterCard Europe

Infineon Technologies AG

EADS-CCR

T-Systems ISS GmbH

IT Innovation

Transport & Travel Research LTD

D1.7 FINAL PROJECT REPORT

Version 2.1– 27/02/2004

	Signature	Date signed
Prepared by: **Schlumberger** **Name:** Alain Couchard		
Reviewed & Approved by: MasterCard Name: André-Jacques Sélezneff		
Infineon Technologies AG Name: Serge Petit		
EADS-CCR Name: Rémy Lopez		
T-Systems ISS GmbH Name: Cézary Glowacz		
IT Innovation Name: Ilesh Dattani		
Transport & Travel Research LTD Name: Tom Parker		

Intended Audience

This report is intended for the readership and evaluation of the European Commission, and other group(s) only upon the written consent of the OmniPurse consortium (confidentiality level**: PU**)

Executive Summary

OmniPurse is a technical proof-of-concept project, designed to demonstrate and consequently enable high-speed and highly secure (CEPS compliant) transactions via a dual interface (contact / contact-less) smart card system.
This deliverable provides an overview of the main results and achievements obtained during the project.

Contents

Document overview

1.1 Purpose of this document

The purpose of this document is to present, in a first part a reminder of the objectives and in a second part the main results of the project, with highlights on exploitation and lessons learned from its execution.

This report is the last deliverable related to the DOW document.

1.2 References and applicable documents

	Issuer of document	Title and Date of issue
1	ISO 7810	Integrated circuits cards with contacts - Physical characteristics - 1987
2	ISO 7813	Integrated circuits cards with contacts - Dimensions and location of the contacts -1988
3	ISO 7816	Integrated circuits cards with contacts - Electronics signals and transmission protocols - 1989 (+ amendment 1 – 1992 / amendment 2 - 1994
4	ISO 7816	Integrated circuits cards with contacts - Inter-industry commands for interchange - 1994
5	EMV	Integrated Circuit Card Specification for Payment Systems – Europay, MasterCard & Visa - EMV, Version 3.1.1, May 31 1998
6	CEPSCo	Common Electronic Purse Specifications – Business Requirements. CEPS, Version 7.0, March 2000
7	CEPSCo	Common Electronic Purse Specifications – Functional Requirements. CEPS, Version 6.3, Sept 1999
8	CEPSCo	Common Electronic Purse Specifications – Technical Requirements. CEPS, Version 2.1, Sept 1999
9	CEPSCo	Joint Card Specification for CEPS – Version 2.1.2 March 2000
10	CEPSCo	Errata for Joint Card Specification 2.1.2 – Last updated 05/01/2000
11	CEPSCo	Joint Card Interface Specification Vol1 – Version 1.0 April 2000
12	CEPSCo	Joint Card Interface Specification Vol2 – Version 1.0 April 2000
13	MasterCard Europe	CLIP - Europay's Interoperable Purse – Product Guide – Final draft – February 2000
14	MasterCard Europe	CLIP – Security Aspects – Version 0.5.1 September 15, 2000
15	ISO 14443	Parts 1/2/3/4
16	ITSO	/1000 Parts –1/2/3/4/5/6
17	CEPSCo	Common Electronic Purse Specifications: Functional Requirements v 6.3 CEPSCO, September 1999
18	CEPSCo	Common Electronic Purse Specifications: Business Requirements v 7.0 CEPSCO
19	CEPSCo	CEPS spec v2.2

20	CEPSCo	Errata for CEPS spec
21	OmniPurse	Annex I for OmniPurse
22		Data controllers brief guide. UK Government web page. 2000.
23	ITSO	ITSO 6.2 = HMI DETR. 2000.
24	KW Ogden	Privacy Issues in electronic toll collection. Transportation Research Part C 9 (2001) 123 – 134.
25	Hans Rat	Transmart, ITS International, Jan/Feb 2001
26	Transport & Travel Research Ltd	Ergonomic and Operational aspects of a smart card trial in Liverpool, 1995
27	CEN ISSS	EU Policy and User Requirements - 2002
28	Smart Card Alliance	Contactless Payment and the Retail POS – March 2003
29	EU/CE	Directive 2000/46/CE du 18 Septembre 2000
30	MasterCard Europe	Mchip4 Card Application Specifications for Debit and Credit V1.0 – October 2002
31	MasterCard Europe	MCE Proximity Chip Payment – EMV Profile – V0.1(d) – January 2003
32	MasterCard Europe	MasterCard Open Data Storage – Technical Specifications – version 2.0 Draft
33	Java Card	Java Card 2.1.1 Application Programming Interface rev 1.0 – May 2000
34	Open Platform	Card Specification – version 2.0.1 – June 2001

1.3 Abbreviations

CA	Certification Authority
ITS	Intelligent Transport System
KAC	Key Administration Centre
LSAM	Load Secure Application Module
MAC	Message Authentication Code
OS	Operating System
PIN	Personal Identification Number
PSAM	Purchase Secure Application Module
SAM	Secure Application Module
URI	User Requirements Interface

1.4 Contributors

Alain Couchard, Schlumberger
André-Jacques Selezneff, MasterCard Europe
Cézary Glowacz, T-Systems ISS GmbH
Ilesh Dattani, IT Innovation
Tom Parker, Transport & Travel Research LTD

1.5 Document History

Version 1.0	09/12/2003	Initial draft
Version 1.1	10/12/2003	Inputs AJ.Sélezneff
Version 2.0	11/12/2003	draft
Version 2.1	27/02/2004	Final version (effort table)

2. Project objectives

2.1 Introduction

Transport systems are becoming more interconnected and operators need ticketing solutions, which deliver fast transactions and increased security for multiple services, at a time when their current magnetic stripe technology has exhausted its potential.

OmniPurse is an Innovative European Commission R&D project to demonstrate the capability to perform on a smart card secure and fast CEPS-compliant contactless payment transactions and to handle public transport applications with the same card, via a microprocessor dual interface (contact / contact-less). The demonstration is performed by developing the required technical system infrastructure (proof of concept) to optimise ticketing applications and open the door to multiple contract handling - for underground rail, buses, ferries to automated car parking.

To address multiple markets requiring high security, e-purse and high throughput applications, such as ticketing and identification, a smart card solution with dual interfaces is needed.

The OmniPurse concept relies on a multi-application smart card , and therefore greatly contributes to facilitate the access of citizens to multiple services like transport while allowing them to pay easily with the same contact / contact less card in various environments.

2.2 Key objectives

The objective of the OmniPurse project is to enable secure and high speed contact-less e-purse payments and ticketing transactions via a micro processor dual interface smart card, and to develop the necessary technical infrastructure, at the card, protocol, reader and SAM levels, to allow for high speed and highly secure transactions.

OmniPurse demonstrates the feasibility of high performance levels in terms of transaction speed to ensure a satisfied flow to urban travellers and the high security level necessary to fight against fraudulent payment transactions in a unique system.

The system is evaluated by security experts and users in order to validate its final acceptability in terms of performance, it demonstrates a proof of concept, and suggests to adapt this concept to become a basis for standardization.

It is essential, in such a high level technological project, to adopt a strong system approach, in order not to put aside any component involved in an off-line transaction (e-purse transaction type). The detailed technical objectives are as follows:

- Gather and exploit requirements from transport and financial sectors to define the appropriate speed and security, using CEP specification as an interoperable basis for the payment solution and define business requirements
- Define the security target and protection profiles
- Develop a Crypto processor Contact/contact-less chip platform with high level security mechanisms, to be used for cards and contact chip for SAM, based on public key cryptography
- Develop a numerical modelling tool to allow the optimisation of the contact-less card/reader interface, and better predict the performance of the system

- Develop a card operating system architecture ready to support CEPS payment functions in a multi application environment
- Develop a contact-less reader with high communication speed
- Implement and optimise ticketing and payment applications in card, reader and Secure Access Module, in order to track and build on CEPS standards
- Make a functional and security evaluation of the hardware and software of the complete designed system, to give a high confidence level to related operators
- Develop the solution in close relationship with transport operators, through the participation in transport workshops, and propose or adapt this concept to become a basis for standardisation in Europe
- Build a demonstrator to show the benefits of the contact-less e-purse in the context of a business application scenario, with the participation of banks and transport operators.

2.3 Technical challenge

The Mass-transit business segment offers different types of contracts described in the Business Requirement (Cf. [BUSIN]) such as subscription, pre-paid / real-time or post-paid multiple-ticket, single ticket or one day card etc.

Only unmanned e-purse / real-time / single ticket transaction are taken into account in the demonstration.
The technical challenge is to deliver the main objectives of the project, that means providing a CEPS compliant contact/contact-less card with appropriate levels of (a) performance to match operators' requirements and (b) security as specified by the CEPS security standards.

In other words, the technical challenge is to perform a contact-less (which imposes time versus power restrictions) CEPS (which requires computational power for 1024-bit RSA) transaction within 300 ms (which is required by the transport operators).

The target of 300 ms relates to a single ticket, real-time unmanned e-purse payment transaction excluding human or mechanical movements of the gate to ensure smooth flows through tollgates in the transport sector.

The contact-less technology simplifies access to transport via a swift and easy gesture. The action for the customer is simple, fast and undemanding. It's important to stress that the project does not produce a market-ready system, but does lay the groundwork for producing such a system, by addressing and solving the technical issues described above.

The main progress brought by the OmniPurse project over existing systems such as Calypso is to perform a contact-less ticketing transaction **including payment** by means of a loadable CEPS e-purse, linked to the banking system (customers bank account); and ensuring interoperability regarding the use of public keys.

2.4 Measuring Success

The overall success of the project is measured by the following achievements.

- Achievement of a performance level never reached and a payment transaction time suitable for transport operators, down to 150 ms if possible, or at least less than 300 ms
- Design both an innovative high performance and security contact-less system with cards, reader and SAM
- Proof of the technical feasibility and concept by implementing the designed solution on one demonstrator.
- Contribution to the definition and harmonisation of transport standards
- Input and proposals on CEPS specifications to improve them with contact-less technology
- Marketing and commercial sustainability by implementing the contact-less payment function on a unique card, thus providing multiple benefits for end users
- Fine knowledge of the contact-less technological environment, using a numerical modelling approach re-usable for new product development
- Implementation of an interactive demonstrator as proof of concept, shown during conferences throughout Europe.
- Ready to start pilot projects with implementation of multiple applications through this performing system and dissemination of the proposed card solution through different European Cities.

3. Main results

We can follow item by item what we indicate as success factors, and what is achieved.

- Performance:

That is the most interesting part of the project result, even if the 300ms has not been demonstrated, we demonstrate (cf D10.1 Performance and functional report), that with the final chip, it will be fully achievable, as we calculated during the feasibility analysis,.

This result confirms OmniPurse' decision taken during the GO/NOGO meeting to pursue the project development, even if the final contact/contact-less chip has not been available during the project duration. This decision allowed us to develop all components of the system in the perspective of exploitation in future products.

- System design:

All components of the system were developed:

  - Card (in contact mode) with integration in an hybrid solution for contact-less interface support (Electronic Units),
  - PSAM,
  - Reader supporting high performance RF communication baud rates (up to 848kbds) and packaged antenna for integration in automated devices,

- Proof of technical feasibility:

We integrated all components in one demonstrator, to support dissemination activities.

- Participation / Inputs to standards:

We proposed some modifications to the CEP specification, in order to try to easily obtain the required transaction time, but CEPSCo did not react to these propositions.

We also investigated with Transport Operators' standardisation bodies how to integrate our product in their schemes, that lead to our card architecture allowing access to a transport application to the ticket proof generated by a CEPS transaction. On this issue we faced an absence of standard in the Transport Standards about a "ticket proof", even though the need has been identified.

- Knowledge of the CL technological environment:

Using the modelling simulation tool, we have elaborated a process for designing antenna, packaging and integration that allow us, as validated by experimental results, to skip the mock-up phase in defining the final terminal product. That will give a real advantage in terms of development cost and time to market.

- Interactive demonstrator:

All functionalities of the system are demonstrated, and we use the upper part of an existing Transport Operator gate.

- Ready to start pilot projects:

We couldn't answer positively to this criteria. The main reasons that we faced during the project are:

  - The final contact-less chip is not available,
  - The CEPS application is not in the focus of Financial Institutions, who are currently deploying their EMV infrastructure for debit and credit

Pilot projects must rely on an other type of Financial application, EMV pre-authorized for example, but all components we developed are directly usable in this perspective.

4. Overview of Exploitation plans

It's very important to notice in preamble, that all initial exploitation plans, for technology partners mainly, were based on the success of the CEPS application in the market. As we saw during the project, this was not the case and will not be in a near future. As a consequence, Exploitations plans rely on direct results obtained in the project, as follows (cf Technological Implementation Plan):

1. Secure 32bits core chip platform capable of high level performance qualified
2. Shift from CEPS focus to EMV Pre-authorized focus
3. Review opportunities and impact of Multi-Issuer card operation
4. Availability of additional arguments for a Business Model for the relationship between Banks and Transport Operators

5. Increased organisation's scientific quality, potential for growth and competitiveness with new services
6. Multi-Application Operating System for contact/contact-less Smart Card in an open architecture (Java, OP) and on a 32bits chip
7. Penetration Techniques and Testing Tools for Security evaluations
8. Improvement of numerical simulation for coupling optimisation of smart cards and terminals
9. Determination of modelling strategy for ferrites absorbing materials
10. Chip Contact-less interface for high speed support protocol qualified
11. SLE88 chip certification finalized (CCEAL5+)
12. SLE88 Development tools qualified
13. OmniPurse demo
14. Design and packaging of antenna and numerical RF demodulator supporting high baud rates (ISO14443) for integration in automated devices.

As a summary of the exploitation plan for the project, we can highlight the following points:

- Time to application / market (in months from the end of the research project) : from 0 to 12
- Tools, testing techniques directly available from the project (numerical simulation, security domains)
- Available arguments for Business Model for relationship between Banks & transport Operators.

All these elements are very positive results from the OmniPurse project.

5. Lessons learned

We want to highlight some points that we gather from the project and could be of interest for future projects. We selected:

- Description of Work:

We think, and particularly the coordinator that the project split in twelve work-packages is to much. Also, directly linked to this, the number of deliverables: **37** (without revised versions, phase2 proposal) are not useful. We recommend concentrating this type of project in less WP and deliverables.

- Budget:

Also, the WP split brings difficulties to easily follow all workload reports, and again to help for the good evolvement of the project.

- DOW evolutions:

It's very important for the entire consortium to be able to manage some evolutions in tasks and objectives, during the life of the project, and we appreciate the good cooperation with the commission in this domain.

- R&D project type:

This type of project is R&D oriented, but required also some Marketing/Product line involvement. This is not very easy task, as they couldn't see direct benefits for their to-day business. So this mix is a difficulty to manage.

- The GO/NOGO decision meeting/milestone is very important to keep in this type of project, as it helps to manage evolutions in scope or objectives in the project.

6. Conclusion

The main conclusion that can be drawn from the OmniPurse project is that in spite of the rapid change of the environment that had allowed to define the project initially, the R&D results obtained from OmniPurse do pave the way, from the technology standpoint, for developments in the cooperation between the Financial and Transport communities, which were not possible at the start of the OmniPurse project.

Most of the results obtained by OmniPurse can be re-used in either current or future products, and the scene setting made possible by the project allows from a marketing point of view for further discussions to be held with the assurance that technology is ready.

One can regret that the opportunity for CEPS deployment that was identified as a key success factor at the time when the project was launched, has not materialized, but this was out of reach of the parties to the project.

A direct consequence of this change of environment, which impacts the project, is that the target contactless chip is not available at this time. It is fair to recognise that these changes have significantly shifted in time the business opportunity for the chip supplier.

ANNEX

1. TABLE OF RESOURCE CONSUMPTION:

	WP1	WP2	WP3	WP4	WP5	WP6	WP7	WP8	WP9	WP10	WP11	WP12	TOTAL
CO1 – Schlumberger	24,00												**24,00**
CR1 – Schlumberger		1,57	5,37	10,48	16,40	29,02	2,30	70,86	4,70	6,29	4,77	2,50	**154,25**
CR2 – MasterCard	2,36	7,94	0,85	0,52						0,14	6,53	1,21	**19,55**
CR3 – Infineon				1,60			56,77						**58,37**
CR4 – MS&I				3,76									**3,76**
AC5 – T-Systems		3,00	3,00				12,50			28,63			**47,13**
CR6 – IT Innovation		3,00		2,16							17,03	3,87	**26,06**
CR7 – TTR	1,10	4,00									6,20	2,28	**13,68**
CR8 – EADS-CCR				2,00	21,47								**23,47**
Total	**27,46**	**19,51**	**9,22**	**20,52**	**37,87**	**29,02**	**71,57**	**70,86**	**4,70**	**35,06**	**34,52**	**9,96**	**370,27**

2. LIST OF DELIVERABLES:

Deliverable Code & Name	*Actual delivery date*
D 1.1: Progress Report period 1	**Aug. 2001**
D 1.2: Progress Report period 2	**March 2002**
D 1.3: Progress Report period 3	**Oct. 2002**
D 1.4: Progress Report period 4	**Feb. 2003**
D 1.5: Progress Report period 5	**Sept. 2003**
D 1.6: Progress Report period 6	**Dec.2003**
D1.7: Final Project Report	**Dec. 2003**
D 2.1: Business Requirements V1.0.1 **V1.2** **V2.0**	**Sept. 2001** **March 2002** **June 2003**
D 3.1: Security guidelines	**Feb. 2002**
D 3.2A: Preliminary list	**July 2002**
D 3.2B: Documentation for card eval.	**April 2003**
D 4.1: RF Simulation framework	**March 2002**
D 4.2: System and funct. Requir. V1.2 **V2.0**	**July 2002** **July 2003**
D 4.3: Feasibility Analysis V1.0 **V2.0**	**Dec. 2001** **July 2002**
D 4.4: Go/No Go status	**July 2002**
D 5.1A: RF coupling opt. Num. Modeling	**Oct. 2002**
D 5.1B: new version	**March 2003**
D 5.2: Numerical framework	**Oct. 2002**
D 6.1: First qualification report	**June 2003**
D 6.2: Reader prototype	**June 2003**
D 7.1: Chip platform emulator and tools	**Nov. 2001**
D 7.2: First contact silicon version	**Dec. 2002**
D 7.3: Security evaluation report	**Nov. 2003**
D 7.4: Contact/contact-less modules	**June 2003**
D 8.1A: e-purse source code V1	**Oct. 2002**
D 8.1B: e-purse source code V2	**July 2003**
D 8.2: First card prototype	**Jan. 2003**
D 8.3A: e-purse eng. Samples PCB	**Feb. 2003**
D 8.3B: e-purse eng. Samples	**Oct. 2003**
D 8.4: PSAM source code	**Nov. 2002**
D 8.5: First PSAM proto. for term valid.	**Nov. 2002**
D 8.6: PSAM eng. samples	**March 2003**
D 9.1: Report on integration	**Nov. 2003**
D 9.2: Full system demonstrator	**Sept. 2003**
D 10.1: Perf. and functional report	**Nov. 2003**
D 10.2: Security report (card)	**Nov. 2003**

D 10.3: Reader HW certification report	**June 2003**
D 11.1: Report on Comm. & Standardization actions	**Nov. 2003**
D 11.2: Report on implem. demonstrator	**Nov. 2003**
D 11.3: Dissemination & use plan	**Oct. 2001**
D 11.4: Dissemination report	**Nov. 2003**
D 12.1: Pilot preparation report	**Dec. 2003**