EP26996 : SIROCCO PROJECT

Autor:
Data de publicació: 05-03-2015

SIROCCO aims at developing an integrated electronic ticketing, payment and information access application based on state of the art information technology, which will enhance the physical mobility of the users and supports a new business model for the cooperation of banking institutions and transport operators.

EP26996 : SIROCCO PROJECT
Smart-cards in banking and transport ticketing

Keywords: Enterprise Systems Integration, Electronic ticketing, electronic purse, Contact & contactless smart cards, Combicard, Point of sale terminal devices, Public transport operators, banking institutions, merchants, Transport and banking

Project Summary
SIROCCO aims at developing an integrated electronic ticketing, payment and information access application based on state of the art information technology, which will enhance the physical mobility of the users and supports a new business model for the cooperation of banking institutions and transport operators.

SIROCCO builds on a market opportunity created by the emergence of four factors :

Public transport operators must improve their business performance to cost-efficiently handle the ever increasing number of passenger transit transactions. Ticket issuing and payment processes are a key factor. State-of-the-art information technology provides an answer to these needs.

Banks want to promote Electronic Purse schemes for payment of small cash amounts, which cannot be cost-efficiently handled by credit/debit cards. To develop a large scale market acceptance, the Electronic Purse must be directly linked to other applications which generate large number cash payments, such as payment for transport tickets.

Smart cards support to the user's by facilitating access to services and to inform when he or she is on the move. The current scheme of one card per application is not convenient for the user who ends up with carrying too many cards.

The evolution of smart card technology now enables the integration of various applications in a single card. The Secure Combicard supports contact operation and security standards required for electronic payment and contactless operation needed for "touch and pass", 10 cm distance operation suitable for transport ticketing applications.

There is an opportunity for Europe to improve performance of its passenger transport service industry and to improve the quality of service provided to the mass transit users with a new business model based on the collaboration of banks and transport operators and a new technology of integrated transport ticketing and payment applications.

SIROCCO aims at providing a validation of this business model and the associated technology which will be based on the Secure Combicard, as developed in the Esprit project COCLICO EP23246, by achieving in particular the following main objectives:

To develop, implement and evaluate a new business model for a collaboration of financial institutions and public transport operators, who will be co-branding an innovative smart card combining transport ticketing, electronic payment and information services access.

To carry out the developments required for adaptation of the system components to SIROCCO, i.e. system and application software for the Combicard, the terminals, the transport management and the banking system and to integrate the required hardware and software into a consistent application system

To provide a benchmark of this application in real world conditions in a medium scale pilot, to evaluate user acceptance, demonstrate benefits for user and operators, demonstrate and promote the extendibility and transferability of the concept to other sites in Europe.

The project will be carried out by a consortium of companies, who combine the required expertise and have a strategic interest in result exploitation: DGPT (regional transport authority of Catalunya), Banco Sabadell (a leading Spanish group of banks), Sistema 4B (service provider for 38 banks), Gemplus (leading smart card manufacturer who develops the COCLICO Combicard), Almex/Metric (specialist of transport ticketing applications) and Dassault AT (manufacturer of banking and point of sales terminals).

Participants
Sistema 4B (E), Ferrocarrils de la Generalitat / Direccion General de Transports (E), Gemplus (F), Almex Metric (UK), Banco Sabadell (E), Dassault AT (F)

Contact Point
Mr Carlos Triay (Tony Emery-Almex-Cirencester)
Arttic
5, Aavenue de Verdun
F-94204 Ivry-sur-Seine
France
Tel.: +33 1 45 15 2472
Fax: +33 1 45 15 2460
E-mail: (email removed)
WWW: http://www.arttic.com/projects
Karlsuhe Technic: https://publikationen.bibliothek.kit.edu/16222002/1201

return into index table -OR- return to top

SIROCCO
As an example of Electronic Ticket policy, the SIROCCO project ([PeHe02],[PeHe99],[Pava99]) is explained in this section. It has been devel¬oped in Barcelona (Spain) by the transport company FGC (Ferrocarrils de la Generalitat de Catalunya) using a CombiCard, which allows the user to use contact as well as contact-less interfaces.

In this policy the smart card provides ticketing and e-purse applications, therefore, it contains virtual money and transport tickets. These transport tickets are denoted as “Titles”, and the card is called Transport Purse Card (TPC), Gemplus [CaHu02] supplies the cards for this project with the GemCom- biWGlO CombiCard operative system following the norm ISO-7856 [Int], Their storage capacity varies from 2K up to 8K bytes and contains logs and secret keys that comply with WG10 European banking security standards for both e-purse and ticketing applications.

The users can choose between personalized and anonymous cards. The project is developed in conjunction with the bank “Banc Sabadell” [Banc] and therefore if the user chooses to personalize his card, it will be linked to his account at this bank. In figure 4, there is a scheme with the connections between the bank and the operations permitted by the card. The user can charge the card by means of the bank Automatic Teller Machine (ATM) with the financial environment “4B” and in other POS like ticketing machines or shops. When paying for public transportation, parking areas or when using other e-purse applications the information on the transactions is stored in a central database of the bank.

Anonymous cards have to be charged by cash or by electronic payment systems in the POSs provided by the transport agent FGC, To perform pay¬ment the card uses its serial number to sign the transactions and be authenti¬cated by the system. This way the system is able to reconstruct the contents of the TPC in case of its destruction or unreadabilitv, so even when the card is anonymous it is still traceable.

The restricted files are protected by the operating system installed in the card and designed for this project. The security attributes fix the security conditions that shall be satisfied to allow operations on the files. These access conditions are defined for a group of commands, which are different depending on the file one is referring to (EF or DF), The file access conditions can be:

- Free, which means the file can be treated without any restriction,
- Secure Code, only modifiable if the knowledge of a password has been proven,
- Locked, which means the file is never accessible and
- Secret Key, only accessible if the terminal proves the knowledge of the secret key; in this case, any operation must be performed in a secure way, sometimes with cipher text.

The system works with a session key for authentication (SKauth) and a key for secure messaging (SKsecure) both of them are 8-bvtes random numbers received from the terminal.

All the transactions include the following steps:

1, Session key generation, 16 bytes
2, Card authentication signature
3, Terminal authentication signature
4, Transaction authentication signature

The authentication is based on cryptographic signatures and DES, Triple- DES symmetric algorithms are used for the transactions. Each Title file owns

2 cryptographic keys to perform this symmetric encryption: a 16-bvtes key used for reloading existing Titles and an 8-bvte key used to validate them in the ticketing terminal.

After their implementation in the Issuer’s company, in this case Gemplus, the cards are sent to the Banc Sabadell which is responsible for its delivery to the transport company. The user will have to contact the public transport central office to apply for either a personalized or an anonymous card. When applying for a personalized card, the application is sent together with the users data to the 4B financial environment system, which is also responsible for selling the Titles, Once the user has his own card, he is able to acquire transport Titles from the point of sale terminals, ticketing machines (MAE) of the station or the automatic teller machines (ATM) of the financial environment system 4B (from Banc Sabadell), Occasional travelers have the possibility to pay with an e-purse to acquire single fare tickets.

The uploaded Titles could be single Titles, multi-trip Titles, monthly Titles or annual Titles allowing different zones of travel. The fare depends on the costumer who buys them (normal, student, children, retired people, etc.). Besides the Titles implemented now, the system allows for future changes.

ATM Ticketing Shops Parking Bus Train
Machines
Figure 4: Project SIROCCO

The ticketing machines (MAE) are designed to enable various payment modes, but as they only have one reader slot, the card which stores the titles should also be the card which is used to pay for them (only one card can be inserted), A problem arises during the identification process of special fares (students, children or retired people). In that case, digital accreditation must be introduced first, keeping the data in a latent state inside the MAE for its use at the appropriate moment. When inserting the TPC, the MAE will show the Titles included as well as the free Title space (the storage of Titles is limited to three) giving the user the options to upload a new Title, re-charge the existing Titles or change any of them.

The automatic teller machines of system 4B work in a similar way as the MAEs to acquire the Titles, They cannot sale Titles that need accreditation (for special fares), but they offer the possibility to re-charge this kind of Titles if they have been previously granted in FCG MAEs, According to its location, the ATM will display three default Titles (for the zone in which the user is located). If the user needs a ticket that is not displayed, the MAE will contact the central host for further information.
Once the tickets are stored in the card, their cancellation is performed by the contact-less interface of the smart card. When the user approaches the smart card to the reading device during a brief lapse of time, the display of the ticketing terminal shows the information about the process. In the subway, the ticketing terminals are connected to the gateway that will open when the Title is valid.

The Titles stored in the card have different priorities that define which Title is going to be used at the next transaction. These priorities can be changed by means of a new device introduced in the project called “Prese¬lector”, The Title stored as “default Title” has the highest priority and it is the one used for the cancellations while the other two ones are designated by first and second Subtitle and are only checked if the default Title is not valid. In case the card does not store any valid ticket, the user is not allowed to get on board.
The use of the Preselector device is a disadvantage in comparison to other projects since the execution of another operation is necessary if the user wants to change the default Title, Furthermore, the speed of boarding gained by the contact-less interface is reduced by this device as it can lead to cause queues of people who want to use it.

The user cancels his tickets at the ticketing terminal. This terminal owns a screen on which the following data are displayed:

- “Terminal out of order” or
- “Terminal is idle” and

— date,
— time,
— error messages (together with an acoustic signal),
— information about the successful cancellation (=validitv) of a Ti¬tle,
— after cancellation, in case of a multi-trip Title: number of remain¬ing trips,

A multi-trip Title can be used for several travelers if there are not more than two seconds between two cancellations. Since it is needed to check the validity of the tickets in order to avoid fraud, the controllers of the travel sector have a portable device which allows them to check the TCPs of the travelers. This device permits to check the active Title in the card as well as the history file that contains the last 10 trips. With this device, the controller may also change the Title selected as default.

The information about cancellations is stored in a central database, which is used to provide statistical data as well as a commercial profile through individualized tracking or by any other means.

After having explained the EPT policy and especially this project, it can be concluded that an EPT policy does not have the advantage provided by an AFC system regarding the pricing policy for tickets. It also lacks the con¬venience of not selecting the fare previous to the travel, but the advantage is that the user only has to draw the card once per travel. The main difference that can be found between SIROCCO and other EPT projects is the use of Titles uploaded to the card instead of selecting the fare before boarding. As a matter of fact this has also to be done if the default ticket has to be

changed and therefore, the speed of boarding is only increased when the user always uses his default ticket. The transition from the current system to an electronic system with EPT policy is not very drastic. This is important because adapting the behavior of the user to a new system needs time. Re¬garding this project, the behavior must not be changed as much as in other projects. The Preselector device is a new idea integrated in this system that may represent a big change in the user's way of thinking about charging and paying for public transportation.

_____

SIROCCO: A BREAKTHROUGH IN MULTI-MODAL TICKETING
Tony Emery

e-Europe, Madrid

13/14 June 2002

WHAT IS SIROCCO?PROJECT HEADLINE
"Mobility Enhancement

with

Interoperable Smart Card Applications

Using Combicards"

WHAT IS SIROCCO?PROJECT DRIVERS

Banks need more transactions flowing through their electronic purses

TWO KEY DRIVERS:

Transport operators need efficient and convenient ticket technology, but do not want slow bank e-purses

WHAT IS SIROCCO?PROJECT OBJECTIVES

Develop integrated multi-modal electronic ticketing and information services for public transport

WITH EU (ESPRIT) FUNDING SIROCCO HAS THREE OBJECTIVES:

Evaluate the benefits of ‘state-of-the-art’ dual-interface smart card technology

Develop a new operating model for co-operation between banks and transport operators

WHAT IS SIROCCO?WHERE IS THE BREAKTHROUGH?

PROJECT SCOPE:

First ‘real world’ multi-modal dual-interface commuter ticketing

COMMERCIAL BREAKTHROUGH:

Co-operation between banks and transport operators

TECHNOLOGY BREAKTHROUGH:

Dual interface cards to support multi-applications & fast transit

WHAT IS SIROCCO?PROJECT SCOPE

WHAT IS SIROCCO?PROJECT SCOPE
CITY

BARCELONA

Station gates

60 (Contactless)

Bank Terminals (ATM)

100

Point of Sales

100 (Station area)

Buses

5

5 (Contactless)

Car Parking

30 (In Stations)

Ticket Sales Machines

SmartCards

10.000

SIROCCO PROJECT PARTNERS

CARD MANAGEMENT

PUBLIC TRANSPORT

WHAT IS SIROCCO?PROJECT PLAN

WORK PACKAGE DELIVERABLE/STATUS

WP1 SPECIFICATIONS D1 / FINISHED

WP2 BANKING SYSTEM D7 / FINISHED

WP3 TRANSPORT SYSTEM D6 / FINISHED

WP4 VALIDATOR DEVELOPMENT D2,D4,D5 / FINISHED

WP5 SMART CARDS D8 / FINISHED

WP6 POINT OF SALES (POS) D3 / FINISHED

WP7 INTEGRATION & VALIDATION D9 / FINISHED

WP8 PILOT D10 / FINISHED

WP9 DISSEMINATION & EXPLOITATION PLAN D11 / FINISHED

WP10 PROJECT MANAGEMENT D12 / FINISHED

TECHNOLOGY BREAKTHROUGHWhat is a dual interface card?
SINGLE DUAL INTERFACE CHIP

(contact & contactless)

ISO 7816

CONTACT

INTERFACE

ISO14443-B

CONTACTLESS

INTERFACE

2 TECHNOLOGIES, 1 CHIP, 1 CARD

Contact

interface

E²PROM

memory

Microprocessor

Contactless

interface

TECHNOLOGY BREAKTHROUGH Which dual-interface card?Mirage (Moto/Atmel), ST16RF4x (SGS-Thomson), Mifare Pro (Philips)
Compatible

ISO7816-4

ISO 14443 - A

(Mifare Pro)

or 14443 - B

(Moto / ST)

TECHNOLOGY BREAKTHROUGHWhich dual-interface card?

Under Esprit Project Coclico Almex & S4B Worked With Motorola & Gemplus To Develop The Mirage Card

MIRAGE was the obvious choice for SIROCCO providing a test-bed for the new technology

Fabricated by GEMPLUS

TECHNOLOGY BREAKTHROUGHWhich dual-interface card?

MIRAGE CARD PICC
Industry standard M68HC05 instruction set

ISO14443-B Modulation and anti-collision schemes

10cm contactless operating range

Contact interface to ISO 7816

13.56MHz RF interface with up to 141kbits/s data transfer

Single memory/dual contact & contactless micro controlled interfaces

4 Kbytes EEPROM, 1mS erase, 3mS write times

TECHNOLOGY BREAKTHROUGHGemCombi Card Operating System (OS)
SINGLE OS for both contact and contactless operation, gives:-

Operational flexibility

Easy to share data

Excellent security for e-purse

ISO7816-4 files and commands + secure messaging with 4 different 16byte secret keys
Each transaction includes Mutual Authentication, unique transaction counter, 3DES session key and triple 3DES signatures

TECHNOLOGY BREAKTHROUGHGemCombi Card Operating System (OS)

For the Transport application, the single OS for both contact and contactless operation, gives:

Ticket loading through contacts with full security.

Each transport ‘contract’ can have two ‘sub-contracts’ to allow concurrent contract renewal.

Contactless debit transaction and refund secured with 3DES session key, & mutual authentication, with transaction duration < 200mS

TECHNOLOGY BREAKTHROUGHALMEX SmartFare Validator

The Almex SmartFare validator integrates the Coclico contactless card reader to provide :

Generic unit for bus, rail and parking

13.56Mhz interface to ISO14443 type B

6 cm contactless operating range

Fast parallel interface to the main processor which handles the travel rules for card validations

Compact housing providing 2x16 LCD display, traffic light LEDs and keypad

SIROCCO PILOT16 OCTOBER 2000 – DECEMBER 2001
VALIDATORS

CARDS

7383 Cards:
5093 Anonymous
2290 Personalised

79 Station gates & ticket
pre-selectors

5 Bus validators

TICKET SALES

3 Parking validators

29 SIROCCO sales machines

INSPECTION TERMINALS

20 Handheld Terminals

100 POS terminals

DATA MANAGEMENT

101 ATM’s near Stations

41 Station ‘Concentrators’

SIROCCO PILOT

SABADELL-RAMBLA

SANT CUGAT

UNIVERSIDAD

PL. CATALUNYA

SIROCCO PILOTSOME STATISTICS
INITIAL CARD TICKET SALES

78% DIRECT SALES AT STATION MACHINES

20% EXCHANGED MAGNETIC TICKETS

2% AT ATM

MAINLY FREQUENT TRAVELLERS
WEEKLY TRAVEL PASS
MONTHLY TRAVEL PASS
NOT DAILY

AT LEAST 50% COMMUTER JOURNEYS

15% START AT SABADELL-RAMBLA

12% START AT SANT CUGAT

23% RETURN FROM PL. CATALUNYA

SIROCCO PILOTRESULTS

BENEFITS FOR THE COMMUTER:

CONVENIENCE!!!

TICKET LOADING via the contact interface available 24/7, using the existing ATM infra-structure

SPEED – faster ticket validation

SIROCCO PILOTRESULTS

BENEFITS FOR THE OPERATOR:

Improved passenger service

Single ticket medium for multiple services

Reduced ticket issuing costs and management

Reduced coin handling costs

And Potentially Reduced fraud

SIROCCO PILOTRESULTS

BENEFITS FOR THE BANK:

Increased use of ATMs

Marketing opportunities through increased client base

And Potentially

Transaction revenue

Float ownership
Increased e-purse use

BEYOND SIROCCOPotential for transport operators

SIROCCO PROJECT HAS SHOWN:

Enhanced mobility for passenger

Increased ticketing flexibility at reduced operating cost using ATMs

Potential expansion to public transport throughout the Barcelona region – new tender expected in 2003

SIROCCO and finally . . . . DID WE MEET OUR OBJECTIVES?

Develop integrated multi-modal electronic ticketing and information services for public transport – YES!

Evaluate the benefits of ‘state-of-the-art’ dual-interface smart card technology – IT WORKS!

Develop a new operating model for co-operation between banks and transport operators – MAYBE?

SIROCCO: A BREAKTHROUGH IN MULTI-MODAL TICKETING
THANK YOU

ANY QUESTIONS?

www.metricgroup.co.uk

SOME CLUES ABOUT THE SIROCCO WIND

Sirocco (Scirocco)

Location: Mediterranean Sea and coasts

The term Sirocco (sometimes also spelled Scirocco) is an all-inclusive name given to hot and subsequently humid southeast to southwest winds originating as hot, dry desert-air over Northern Africa, flowing northward into the southern Mediterranean basin.

Siroccos occur in advance of surface and upper level depressions moving eastward across the southern Mediterranean Sea or northern Africa. These cyclones originate either over North Africa or sometimes south of the Alps, primarily in the Gulf of Genoa in the latter case.

Depending on where you are, the Sirocco is inhibiting substantially different characteristics and has many different local names, too. Along the northern African coast the hot air originates directly from the Sahara desert, producing hot, dry and dusty conditions. Visibility becomes very poor and the fine blowing dust might result in danmage to instruments and equipment. On rare occasions the Sirocco is picking up enough dust and sand to produce even sandstorms.

However, the term Sirocco is not used in North Africa, where it is called chom (hot) or arifi (thirsty); Simoom in Palestine, Jordan, Syria, and the desert of Arabia; Ghibli (or Chibli, Gibla, Gibleh) in Libya; Chili (or Chichili) in Tunisia and S Algeria; Khamsin (or Chamsin, Khamasseen) in Egypt and around the Red Sea and Sharavin Israel.

As the air travels northward across the Mediterranean Sea, the Sirocco picks up much moisture because of its high temperature, and reaches the eastern coast of Spain (known there as Xaloc in Catalonia and Valencia; Leveche, Solano, Jaloque or Xaloque in Murcia), Portugal as Xaroco, France as Marin, Malta, Sicily, southern Italy as Scirocco, Croatia as Jugo and even Greece as a very enervating, hot, humid wind. In some parts of the Mediterranean region the word may be used for any warm oppressing southerly wind, often of foehn type. For example, in the extreme southwest of Greece a warm foehn crossing the coastal mountains is named Sirocco di Levante and a sirocco wind on Madeira and the Canaries is known as Leste.

As it travels northward, it causes clouds, fog and rain over northern Mediterranean areas. The sweltering, sultry and close waether during an Sirocco event causes headaches and insomnia for many. The hot humid wind causes overnight temperatures of 30°C and above, while thermometer may well reac 40°C during daytime. Extreme temperature differences (up to 20°C) may occur with the following cold front and its dust may reach even Britain and northern Europe.

Sirocco events tend to occur year-round without a favored month or season. However, strong gale-force siroccos are most common during the spring. The average duration of continuous gale force winds during a Scirocco is 10 to 12 hours and occasionally as long as 36 hours. The onset of a gale-force Sirocco often occurs as a surface low moves into the Gulf of Gabes from Tunisia, combined with the passage of a deep 500 mb trough extending well into north Africa and positioned west of the Gulf of Gabes. The gale-force Sirocco is most common during the spring and may reach wind forces between 5 and 8 Bft.