



033591
STOLPAN
STORE LOGISTICS AND PAYMENT WITH NFC

6th Framework IST project
Specific Targeted Research Project
IST-2005-2.5-8 – ICT for Networked Businesses

D6 – 1

**Overall description of the NFC purse
operation including its back-office
functions and operation**

Due date of deliverable: Sept. 2007
Actual submission date: Feb. 2008

Start date of project: 01.07.2006

Duration: 36 months

Organisation name of lead contractor for this deliverable:

SafePay (CR2)

Final

Date:	15/02/08
Author:	András Vilmos
Version:	Final

Project co-funded by the European Commission within the Sixth Framework Programme (2002-2006)		
Dissemination Level		
PU	Public	
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission	
CO	Confidential, only for members of the consortium (including the Commission Services)	CO

The Consortium consist of

Participant No.	Participant Name	Short Name	Country
1	Motorola Ltd.	Motorola	HU
2	SafePay Systems Ltd.	SafePay	HU
3	Deloitte Ltd.	Deloitte	HU
4	Budapest Tech, John von Neumann Faculty of Informatics	BMF	HU
5	Auto-ID-Labs St. Gallen	Auto-ID-Lab	CH
6	BULL Ltd.	BULL	HU
7	Consult Hyperion	Chyp	UK
8	Fornax Plc.	Fornax	HU
9	Philips Austria Gmbh.	Philips A	AT
10	University of Technology and Economics	BME	HU
11	Banca Popolare di Vicenza	BPVI	IT
12	Libri Bookstores Ltd.	Libri	HU
13	Baker &McKenzie	BMcK	HU
14	Consorzio Triveneto S.P.A.	Constriv	IT
15	SUN Microsystems Ltd.	SUN	HU
16	T-Systems Hungary Ltd.	T-Systems	HU
17	Philips Italia Spa.	Philips IT	IT
18	Motorola Gmbh.	Moto DE	DE
19	University of Rome	Cattid	IT

Content list

1	INTRODUCTION	7
2	THE PAYMENT PROCESS	9
2.1	OFFERING MONEY	9
2.2	REQUESTING MONEY	10
3	ON-LINE TRANSACTIONS	11
3.1	ISSUANCE.....	11
3.2	PERSONALIZATION.....	11
3.3	TOP-UP	11
3.4	STATUS QUERY	13
3.5	PAYBACK.....	13
4	FEATURES.....	14
4.1	OFF-LINE PAYMENT.....	14
4.2	P2P PAYMENT	14
4.3	VALUE ADDED FUNCTIONS.....	15
4.3.1	<i>Balance information.....</i>	<i>15</i>
4.3.2	<i>Transaction history.....</i>	<i>15</i>
4.3.3	<i>On-line balance query.....</i>	<i>15</i>
5	THE BANKING PROCEDURES	16
5.1	ISSUANCE OF DIGITAL MONEY	16
5.2	CLEARING AND SETTLEMENT.....	17
6	TECHNOLOGY	18
6.1	FRONT-END	18
6.1.1	<i>Contactless interface</i>	<i>18</i>
6.1.2	<i>Secure element</i>	<i>18</i>
6.1.3	<i>J2ME.....</i>	<i>18</i>
6.2	BACK-END.....	19
6.2.1	<i>Bank back office.....</i>	<i>19</i>
6.2.2	<i>Purse module.....</i>	<i>19</i>
6.3	ARCHITECTURE.....	19
7	USABILITY ISSUES.....	21
7.1	GENERAL CONCEPT	21
7.2	USABILITY FACTORS TO CONSIDER	21
8	SECURITY SOLUTIONS.....	23
8.1	FRONT-END	23
8.1.1	<i>Secure element.....</i>	<i>23</i>
8.1.2	<i>JAVA midlet.....</i>	<i>24</i>
8.2	BACK-END.....	25
8.2.1	<i>Location.....</i>	<i>25</i>
8.2.2	<i>User authentication</i>	<i>25</i>
8.2.3	<i>Employee privileges.....</i>	<i>25</i>
8.2.4	<i>Transaction logging</i>	<i>25</i>
8.3	LIMITS	26
8.3.1	<i>Issuance limit.....</i>	<i>26</i>
8.3.2	<i>Storage limit</i>	<i>26</i>
8.3.3	<i>Single transaction limit.....</i>	<i>26</i>

8.4	SHADOW ACCOUNT	26
8.5	COMMUNICATION	27
8.5.1	<i>Digital signature and end-to-end data encryption of OTA communication</i>	27
8.5.2	<i>Encryption of proximity communication</i>	27
8.6	TRANSACTIONS.....	29
8.6.1	<i>No value creation</i>	29
8.6.2	<i>All value is accounted for</i>	29
8.6.3	<i>Authentication</i>	29
8.6.4	<i>Roll back</i>	29
8.6.5	<i>No repetition</i>	30
9	TECHNICAL DESCRIPTION OF THE TRANSACTION FLOW	31
9.1	COMMUNICATION	32
9.2	SECURE CHANNEL	32
9.3	TRANSACTIONS.....	32
9.4	SECURITY QUESTIONS.....	32
9.4.1	<i>Authentication</i>	32
9.4.2	<i>Authorization</i>	33
9.5	TOP UP.....	33
9.6	PAYBACK PROCESS	33
10	REQUIREMENT SPECIFICATION	34
10.1	GENERAL REQUIREMENTS	34
10.2	FUNCTIONAL REQUIREMENTS	35
10.3	MODULE REQUIREMENTS.....	37
10.3.1	<i>Front end- Handset</i>	37
10.3.2	<i>Front end- SE</i>	38
10.3.3	<i>Back office module</i>	39
10.3.4	<i>Purse back office module</i>	40
11	MESSAGES	41
11.1	TRANSACTION MESSAGE	41
11.1.1	<i>Payment</i>	41
11.2	VALUE ADDED MESSAGES	41
11.2.1	<i>Load purse</i>	41
11.2.2	<i>Load midlet</i>	42
11.2.3	<i>Personalize purse</i>	42
11.2.4	<i>Load value request</i>	43
11.2.5	<i>Loading value</i>	43
11.2.6	<i>Payment initiation</i>	43
11.2.7	<i>Payment request</i>	44
11.2.8	<i>PayBack request</i>	44
11.2.9	<i>PayBack acknowledgement</i>	44
11.2.10	<i>Status request</i>	45
11.2.11	<i>Status response</i>	45
11.2.12	<i>On-line balance query</i>	46
11.2.13	<i>On-line balance response</i>	46
11.2.14	<i>Local balance query</i>	46
11.2.15	<i>Local balance response</i>	47
11.2.16	<i>Transaction history query</i>	47
11.2.17	<i>History response</i>	47

List of figures

Figure 1. The purse operation.....	8
Figure 2. Process of offering money	9
Figure 3. Process of requesting money	10
Figure 4. Process of purse top up.....	12
Figure 5. P2P chain payment	14
Figure 6. Settlement in the multi issuer model	17
Figure 7. Purse architecture.....	20
Figure 8. Transaction flow	31