

# Common Electronic Purse Specifications

## Technical Specification

Version 2.3

March 2001

Copyright CEPSCO 1999, 2000, 2001

All rights reserved

# TABLE OF CONTENTS

<b>1.</b>	<b>REVISION LOG .....</b>	<b>1</b>
<b>2.</b>	<b>DOCUMENT OVERVIEW.....</b>	<b>8</b>
2.1	PURPOSE .....	8
2.2	INTENDED AUDIENCE .....	9
2.3	INCLUDED IN THIS DOCUMENT .....	10
2.4	NOT INCLUDED IN THIS DOCUMENT .....	10
2.5	REFERENCE INFORMATION .....	10
2.5.1	<i>Requirement Numbering</i> .....	10
2.5.2	<i>References</i> .....	11
2.5.3	<i>Notational Conventions</i> .....	12
2.6	DOCUMENT ORGANIZATION .....	14
<b>3.</b>	<b>ENTITY OVERVIEW .....</b>	<b>16</b>
3.1	MERCHANT ACQUIRER.....	16
3.1.1	<i>PSAM Creators</i> .....	17
3.2	LOAD ACQUIRER .....	17
3.3	CARD ISSUER .....	20
3.4	FUNDS ISSUER.....	21
3.5	PROCESSOR .....	21
3.6	SCHEME PROVIDER .....	22
3.6.1	<i>Processor for the Scheme Provider</i> .....	22
3.6.2	<i>Certification Authority</i> .....	23
<b>4.</b>	<b>POS DEVICE TRANSACTION OVERVIEW .....</b>	<b>24</b>
4.1	PURCHASE.....	24
4.2	CANCEL LAST PURCHASE.....	25
<b>5.</b>	<b>LOAD DEVICE TRANSACTION OVERVIEW .....</b>	<b>26</b>
5.1	LOAD.....	26
5.2	CURRENCY EXCHANGE .....	27
<b>6.</b>	<b>CERTIFICATES AND SIGNATURES.....</b>	<b>28</b>
6.1	RETRIEVAL OF CERTIFICATES FROM THE CEP CARD.....	28
6.2	PROCESSING CERTIFICATES FROM THE POS DEVICE.....	31
6.3	VERIFYING CERTIFICATES .....	32
6.3.2	<i>The CEP Card Certificate Hierarchy</i> .....	33
6.3.3	<i>The PSAM Certificate Hierarchy</i> .....	37
6.4	DYNAMIC SIGNATURE VERIFICATION .....	41
6.5	CRYPTOGRAPHIC MECHANISMS .....	41
6.6	UNLINKED LOAD SECURITY FLOW .....	43
6.7	SECURITY FLOW FOR POS DEVICE VALIDATION OF CEP CARDS .....	44
<b>7.</b>	<b>SCHEME PROVIDER PROCEDURES.....</b>	<b>48</b>
7.1	OPERATING RULES AND REGULATIONS .....	48
7.2	CERTIFICATION.....	49
7.3	CERTIFICATION AUTHORITY MANAGEMENT.....	50
7.4	RISK MANAGEMENT .....	51
7.5	OPERATING RULES .....	53

7.6	AGGREGATION PARAMETERS .....	54
7.7	DISPUTE MANAGEMENT .....	55
7.8	TRANSACTION FLOWS .....	55
<b>8.</b>	<b>CEP CARD REQUIREMENTS.....</b>	<b>56</b>
8.1	COMPATIBILITY .....	56
8.2	MULTIPLE CURRENCIES.....	56
8.3	INTERFACE TO TERMINALS.....	57
8.3.2	<i>Load Devices</i> .....	57
8.3.3	<i>POS Devices</i> .....	57
8.3.4	<i>Monitoring Devices</i> .....	57
8.3.5	<i>Personalization Devices</i> .....	57
8.4	GENERAL STATUS CONDITIONS .....	58
8.5	TRANSACTION PREPARATION.....	59
8.5.1	<i>Message Flow</i> .....	60
8.5.2	<i>Reset</i> .....	60
8.5.3	<i>Application Selection</i> .....	60
8.6	ISO/IEC COMMANDS.....	60
8.6.1	<i>Select</i> .....	61
8.6.2	<i>Read Record</i> .....	62
8.7	NON-TRANSACTION COMMANDS.....	64
8.7.1	<i>CEP Inquiry - Slot Information</i> .....	64
8.7.2	<i>CEP Inquiry - Reference Currency</i> .....	67
8.7.3	<i>CEP Inquiry - Transaction Logs</i> .....	69
8.7.4	<i>Implementation Specific Inquiries</i> .....	74
8.7.5	<i>Get Previous Signature</i> .....	74
<b>9.</b>	<b>POS DEVICE CHARACTERISTICS .....</b>	<b>77</b>
9.1	OVERVIEW OF A POS DEVICE .....	77
9.2	REQUIREMENTS.....	78
9.2.1	<i>Scheme Specific Data</i> .....	78
9.2.2	<i>Compliance with Standards</i> .....	78
9.2.3	<i>Card Acceptance</i> .....	79
9.2.4	<i>Card Reader</i> .....	79
9.2.5	<i>Display and Cardholder Interface Design</i> .....	79
9.2.6	<i>Split Transaction Processing</i> .....	80
9.2.7	<i>Power Failure</i> .....	81
9.2.8	<i>Data Store Requirements</i> .....	81
9.2.9	<i>Batch Management</i> .....	85
9.2.10	<i>PSAM Hardware and Software Requirements</i> .....	86
<b>10.</b>	<b>POS DEVICE TRANSACTION PROCESSING.....</b>	<b>89</b>
10.1	PURCHASE TRANSACTION .....	89
10.1.1	<i>Initiate Transaction</i> .....	92
10.1.2	<i>Recovery of the CEP Card Public Key</i> .....	95
10.1.3	<i>Recovery of the PSAM Public Key</i> .....	97
10.1.4	<i>Debit CEP Card</i> .....	100
10.1.5	<i>Incremental Purchase Processing</i> .....	110
10.1.6	<i>Purchase Reversal Processing</i> .....	115
10.1.7	<i>Complete Transaction</i> .....	117
10.1.8	<i>Exception Processing</i> .....	124
10.2	CANCEL LAST PURCHASE TRANSACTION .....	128
10.2.1	<i>Initiate Transaction</i> .....	129
10.2.2	<i>Credit CEP Card</i> .....	132
10.2.3	<i>Exception Processing</i> .....	137

<b>11.</b>	<b>MERCHANT ACQUIRER PROCESSING .....</b>	<b>138</b>
11.1	TRANSACTION PROCESSING .....	138
11.1.1	Validating Collected Batches.....	139
11.1.2	Creating Issuer Batches.....	142
11.2	TRUNCATION.....	145
11.3	POS DEVICE MANAGEMENT .....	145
<b>12.</b>	<b>LOAD DEVICE CHARACTERISTICS.....</b>	<b>148</b>
12.1	OVERVIEW OF A LOAD DEVICE.....	148
12.2	REQUIREMENTS.....	149
12.2.1	Support for Multiple Schemes and Currencies .....	149
12.2.2	Compliance with Standards.....	149
12.2.3	Card Acceptance.....	150
12.2.4	Card Reader.....	150
12.2.5	Display and Cardholder Interface Design.....	151
12.2.6	Financial PIN Security .....	152
12.2.7	Date and Time Processing .....	155
12.2.8	Power Failure.....	155
<b>13.</b>	<b>LOAD ACQUIRER PROCESSING - LOAD TRANSACTIONS.....</b>	<b>156</b>
13.1	NORMAL PROCESSING.....	158
13.1.1	Initiate Transaction.....	158
13.1.2	Communicate with Card Issuer.....	166
13.1.3	Communicate with Funds Issuer.....	168
13.1.4	Credit CEP Card.....	169
13.1.5	Notification to Cardholder.....	173
13.2	EXCEPTION PROCESSING .....	174
13.2.1	Linked Load .....	174
13.2.2	Unlinked Load .....	178
13.2.3	Transaction Completion Messages .....	187
13.3	ADDITIONAL REQUIREMENTS FOR UNLINKED LOADS .....	188
13.3.1	Processing Requirements.....	188
13.3.2	LSAM Hardware and Software Requirements .....	189
<b>14.</b>	<b>LOAD ACQUIRER PROCESSING - CURRENCY EXCHANGE TRANSACTION .....</b>	<b>191</b>
14.1	NORMAL PROCESSING.....	192
14.1.1	Initiate Transaction.....	192
14.1.2	Communicate with Card Issuer.....	196
14.1.3	Exchange Currencies on CEP card .....	198
14.1.4	Notification to Cardholder.....	200
14.2	EXCEPTION PROCESSING .....	201
14.2.1	Exception Conditions.....	201
14.2.2	Transaction Completion Messages .....	205
<b>15.</b>	<b>FUNDS ISSUER PROCESSING.....</b>	<b>207</b>
15.1	UNLINKED LOAD TRANSACTIONS.....	207
15.1.1	Normal Processing.....	207
15.1.2	Exception Processing.....	207
<b>16.</b>	<b>CARD ISSUER PROCESSING .....</b>	<b>208</b>
16.1	ADMINISTRATIVE PROCESSING.....	208
16.1.1	Card Management .....	208
16.1.2	Key Management .....	209
16.2	LOAD TRANSACTIONS .....	210

16.2.1	Normal Processing.....	210
16.2.2	Exception Processing.....	214
16.3	CURRENCY EXCHANGE TRANSACTIONS.....	215
16.3.1	Normal Processing.....	216
16.3.2	Exception Processing.....	219
16.4	POS TRANSACTIONS.....	219
<b>17.</b>	<b>PROCESSING NODE TRANSFERS .....</b>	<b>224</b>
17.1	TRANSACTIONS ORIGINATING AT POS DEVICES .....	224
17.2	TRANSACTIONS ORIGINATING AT LOAD DEVICES.....	224
<b>18.</b>	<b>DATA ELEMENTS.....</b>	<b>226</b>
18.1	LIST OF DATA ELEMENTS .....	226
18.1.1	ACCTYPE (Source Funds Account Type).....	227
18.1.2	ADL (Application Data Locator).....	227
18.1.3	AID (Application Identifier for a CEP).....	228
18.1.4	ALG <sub>LSAM</sub> (LSAM Algorithm for Unlinked Loads).....	229
18.1.5	ALGH (Hash Algorithm code).....	229
18.1.6	ALGP (Cryptographic Algorithm Used with Public Keys).....	229
18.1.7	AM <sub>CEP</sub> (Authentication Method).....	230
18.1.8	AP <sub>CEP</sub> (Application Profile of a CEP Card).....	231
18.1.9	AT (Authentication Token).....	232
18.1.10	AVN <sub>CEP</sub> (Application version number).....	232
18.1.11	BAL (Balance of a CEP card slot).....	233
18.1.12	BAL <sub>max</sub> (Maximum Balance of a CEP slot).....	233
18.1.13	BAL <sub>maxISS</sub> (Advisory Maximum Balance).....	233
18.1.14	CALPHA (Alpha Code of a Currency).....	233
18.1.15	CC <sub>ACQ</sub> (Completion Code from Merchant Acquirer).....	234
18.1.16	CC <sub>CEP</sub> (Completion Code of a CEP Command).....	234
18.1.17	CC <sub>ISS</sub> (Completion Code from a Card Issuer).....	234
18.1.18	CC <sub>LACQ</sub> (Completion Code from a Load Acquirer).....	235
18.1.19	CC <sub>PDA</sub> (Completion Code from a POS Device).....	235
18.1.20	CC <sub>TRX</sub> (Completion Code of a transaction).....	235
18.1.21	CED (Certificate Expiration Date).....	236
18.1.22	CNTRY (Country).....	236
18.1.23	CPO <sub>CEP</sub> (Card Purchase Options).....	236
18.1.24	CSN (Certificate Serial Number).....	236
18.1.25	CURR (Currency).....	237
18.1.26	CURRC (Currency Code).....	237
18.1.27	CURRE (Currency Exponent).....	237
18.1.28	DD (Discretionary Data).....	237
18.1.29	DEXP (Expiration Date for Transaction).....	237
18.1.30	DOM (Domain).....	237
18.1.31	DS (Digital Signature).....	238
18.1.32	DTHR (Transaction Date and Time).....	238
18.1.33	DTRM (Transmission Date).....	238
18.1.34	E <sub>6</sub> (Encrypted S <sub>6</sub> ).....	238
18.1.35	E <sub>6</sub> ' (Encrypted S <sub>6</sub> ').....	238
18.1.36	H <sub>CEP</sub> (Hash Generated by CEP Card).....	238
18.1.37	H <sub>LSAM</sub> (Hash Generated by LSAM).....	239
18.1.38	H <sub>2LSAM</sub> (Hash Generated by LSAM).....	239
18.1.39	ID <sub>ACQ</sub> (Identifier for a Merchant Acquirer).....	239
18.1.40	ID <sub>BATCH</sub> (Identifier for a POS Transaction Batch).....	239
18.1.41	ID <sub>CEP</sub> (Serial Number of a CEP Card).....	239
18.1.42	ID <sub>ISS</sub> (Card Issuer BIN).....	240

# Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

## Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

## Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

## Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

## API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

## LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

## FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

## E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.