PMPC ATM Functional description

Edition 11.04.2001

Author O. Pannke - 3FE5

Status DRAFT/CONFIDENTIAL

Version 0.9

Giesecke & Devrient GmbH
Prinzregentenstr. 159
Postfach 80 07 29
81607 München

Giesecke & Devrient GmbH
Prinzregentenstr. 159
P.O.B. 80 07 29
81607 Munich
Germany

Content

1 General principles

This document describes the functional requirements for ATMs to be used within the scope of the Malaysia Payment Multi Purpose Card. The electronic purse "Proton" application (e-cash) is provided by Banksys s.a. All issues regarding this functionality is considered to be entirely external intellectual property and not described here, instead a reference to the appropriate version of the Proton specifications is done. The naming follows the requirements of the CRFP, wherever possible.

An ATM is the most obvious terminal to load an electronic purse. Indeed it is currently already used to withdraw cash. Within the electronic money environment, this cash withdrawal can be substituted by purse loading. Furthermore due to the on-line nature of the ATM, it can also be very easily used to update the card (change of parameters, etc...).

1.1 Document history

Version 0.5	**09.11.1998**	Draft versions
Version 0.6	**20.11.1998**	Draft versions
Version 0.7	**30.11.1998**	Draft versions
Version 0.9	**01.03.1999**	Final Draft

All amendments to earlier versions are marked grey.

2 Functional Description

2.1 Types of ATMs

Two types of ATMs can be distinguished:

- ATMs direct connected to MEPS
- ATMs connected to participating bank

2.2 Physical Requirements

The extra physical requirements to support the load operation or the off-line cash-withdrawal (if applicable) are minimal. The ATM must only support a hybrid reader, able to read both magnetic stripe and chip cad based cards. The characteristics of the chipcard reader can be found in the document [TERMSPEC].

The reader shall at least support the protocols T=1 and T=0.

2.3 Functionality

Following extra functionalities regarding the chip card are introduced in the ATM:

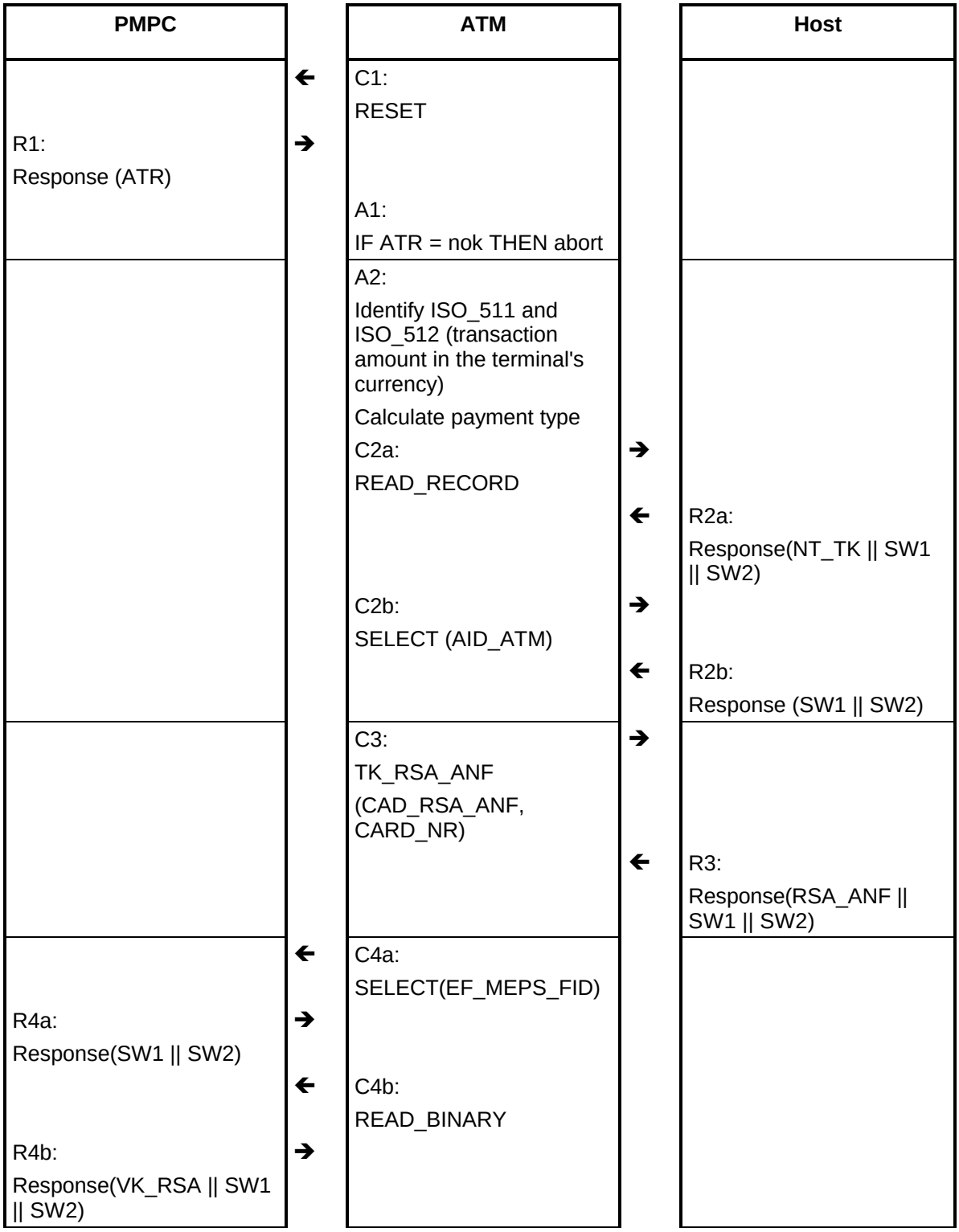
- chip card based ATM transactions, both off-line and on-line
- Proton IEP Load and Unload Transaction
- card update transaction to change card parameters (such as the maximum balance, authorization parameters and the current key version on the card).

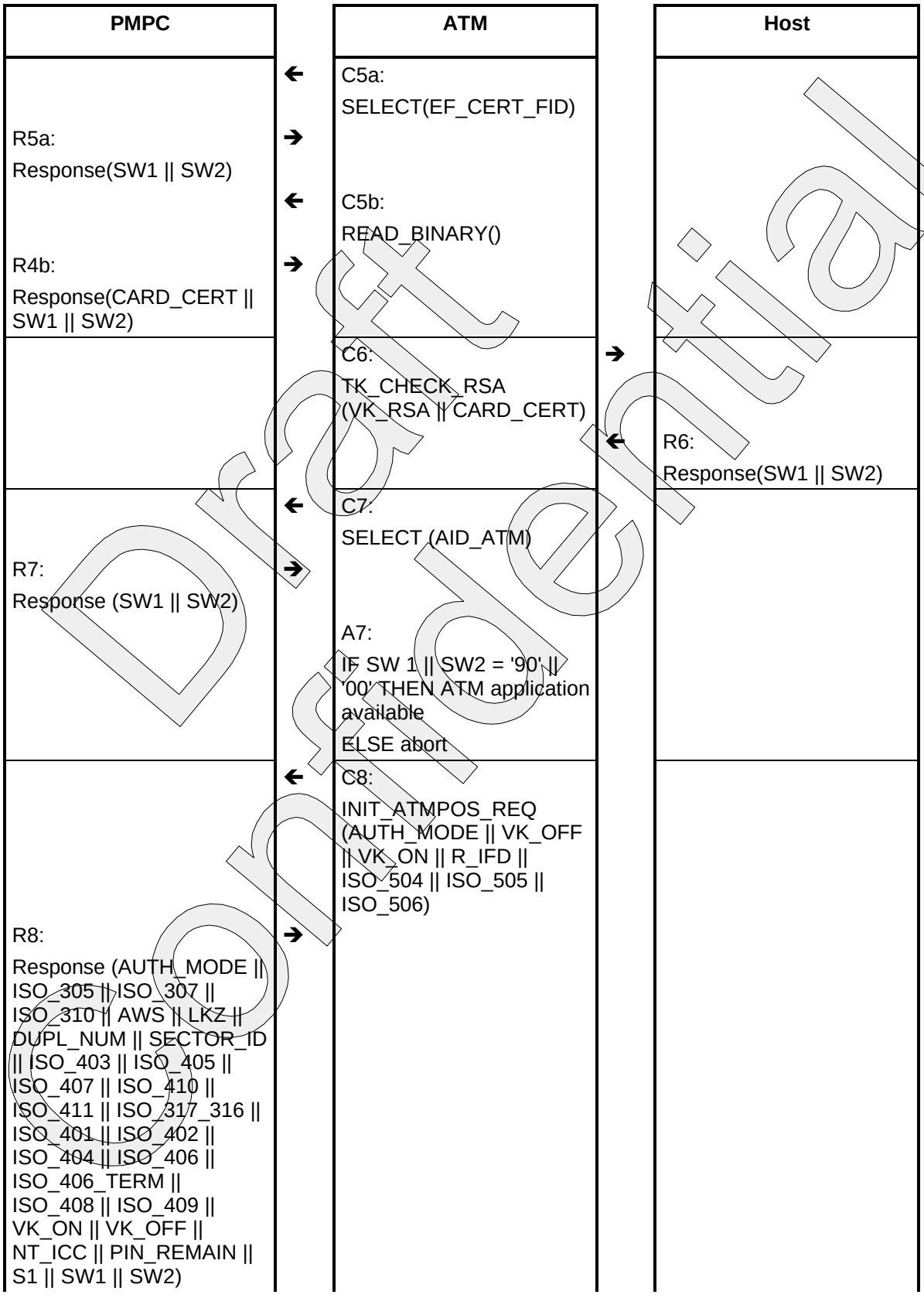
2.4 Application Selection

The ATM shall select first the Debit/ATM Application with implicit Application selection and after performing a correct on-line debit transaction the E-Purse transaction as described in the specifications provided by Banksys for performing an ECash load transaction.

2.4.1 Transaction Flows

2.4.1.1 ATM on-line Transaction





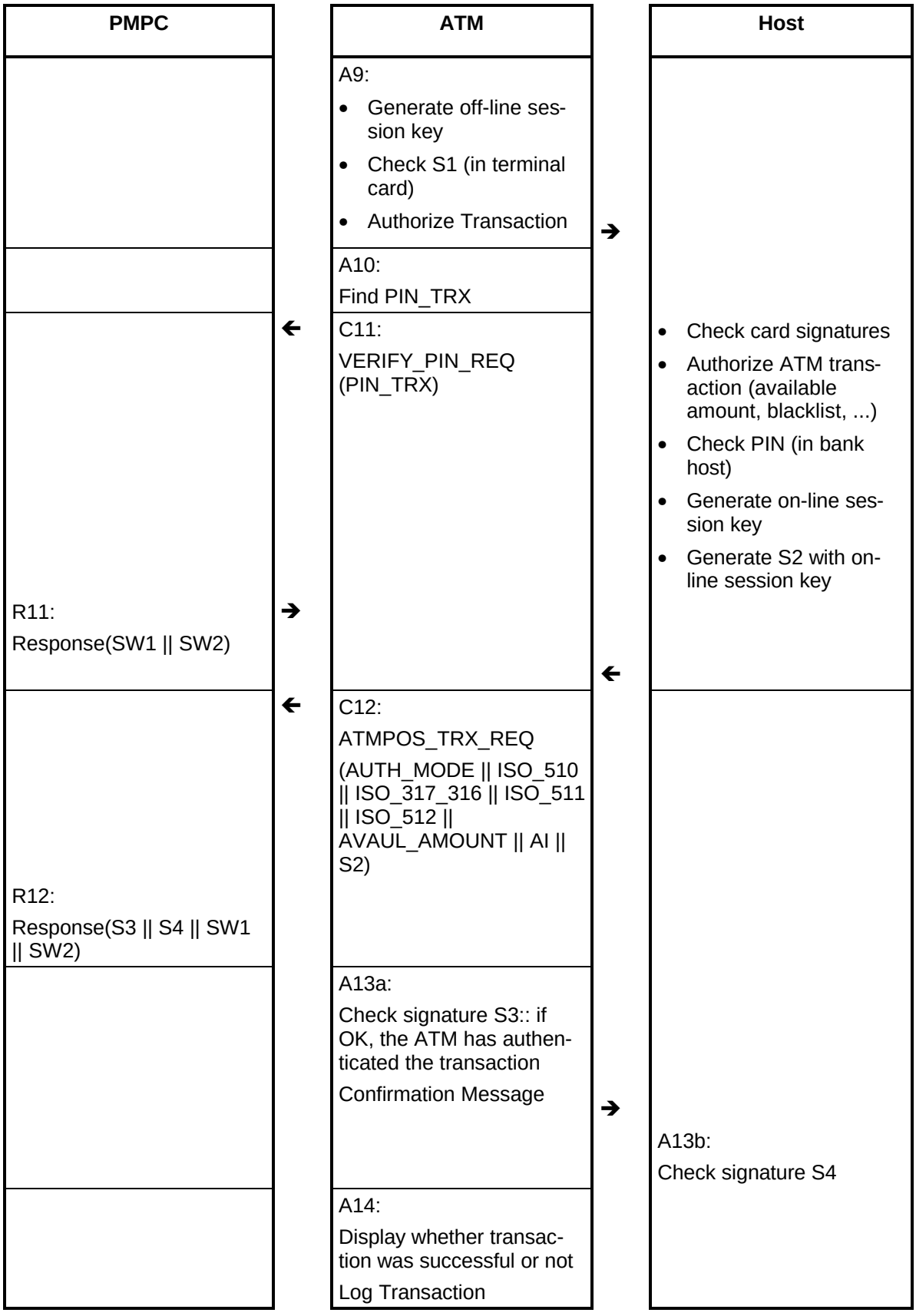
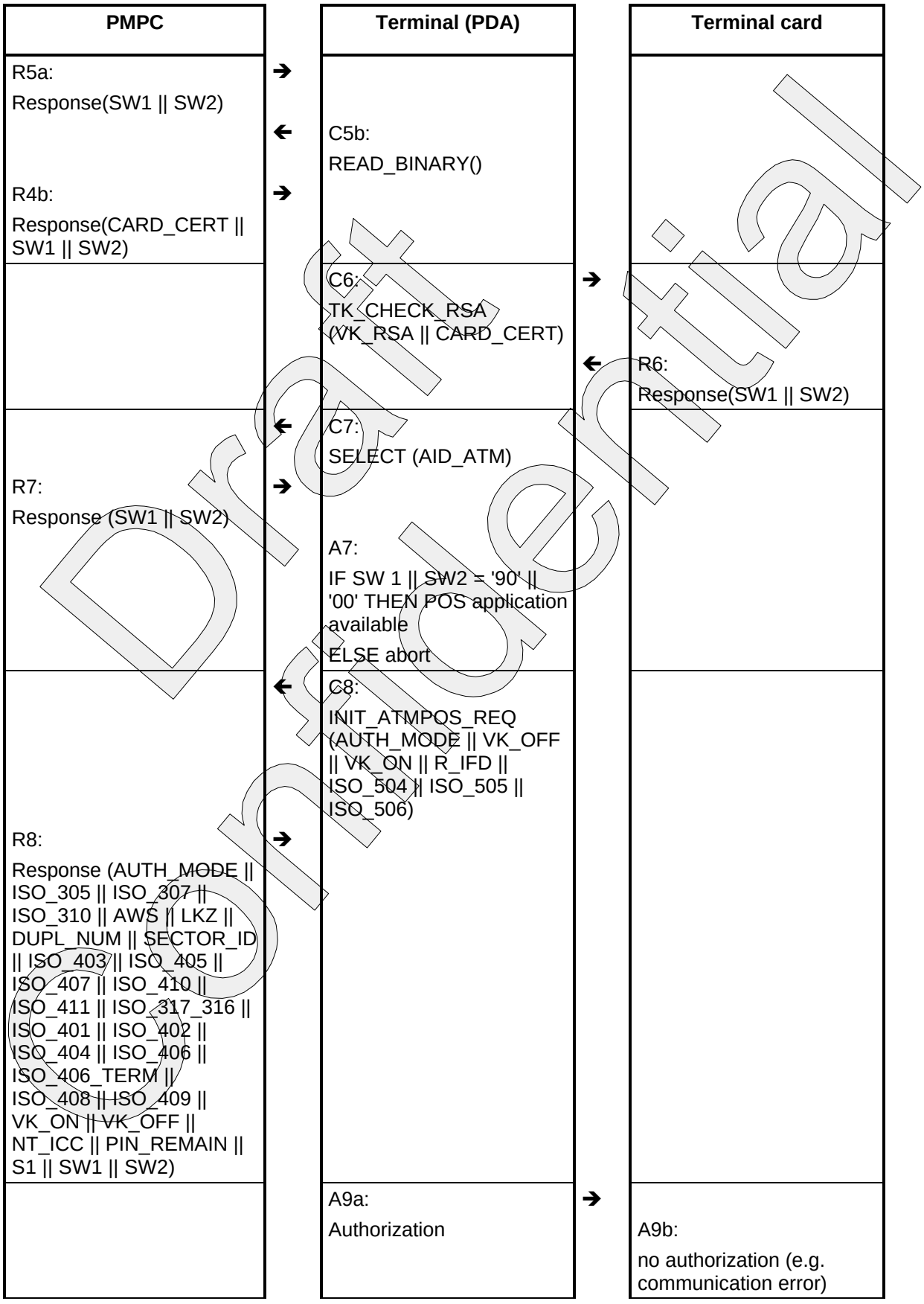


Figure 1: ATM on-line cash withdrawal


Draft
Confidential

2.4.1.2 ATM off-line Transaction

PMPC		Terminal (PDA)		Terminal card
	←	C1: RESET		
R1: Response (ATR)	→			
		A1: IF ATR = nok THEN abort		
		A2: Identify ISO_511 and ISO_512 (transaction amount in the terminal's currency) Calculate payment type		
		C2a: READ_RECORD	→	
			←	R2a: Response(NT_TK || SW1 || SW2)
		C2b: SELECT (AID_ATM)	→	
			←	R2b: Response (SW1 || SW2)
		C3: TK_RSA_ANF (CAD_RSA_ANF, CARD_NR)	→	
			←	R3: Response(RSA_ANF || SW1 || SW2)
	←	C4a: SELECT(EF_MEPS_FID)		
R4a: Response(SW1 || SW2)	→			
	←	C4b: READ_BINARY		
R4b: Response(VK_RSA || SW1 || SW2)	→			
	←	C5a: SELECT(EF_CERT_FID)		



PMPC		Terminal (PDA)		Terminal card
		A10: Find PIN_TRX		
	←	C11: VERIFY_PIN_REQ (PIN_TRX)		
R11: Response(SW1 || SW2)	→			
		C12: TK_INIT_ATMPOS_REQ (ISO_305 || ISO_307 || ISO_310 || AWS || LKZ || || DUPL_NUM || ISO_403 || ISO_405 || ISO_407 || ISO_410 || ISO_411 || ISO_317_316 || ISO_401 || ISO_402 || ISO_404 || ISO_406 || ISO_406_TERM || ISO_408 || ISO_409 || VK_ON || VK_OFF || NT_ICC || S1 || ISO_504 || ISO_505 ||ISO_511 || ISO_512 || AUTH_MODE || AI)	→	
			←	R12: Response (ISO_510 || AVAIL_AMOUNT || NT_TK || S2 || SW1 || SW2)
	←	C13: ATMPOS_TRX_REQ (AUTH_MODE || ISO_510 || ISO_317_316 || ISO_511 || ISO_512 || AVAIL_AMOUNT || AI || S2)		
R13: Response (S3 || S4 || SW1 || SW2)	→			
		C14: TK_POS_REQ (PIN_COUNTS || CC_ICC || S3 || S4)	→	
			←	R14: Response (S6 || SW1 || SW2)

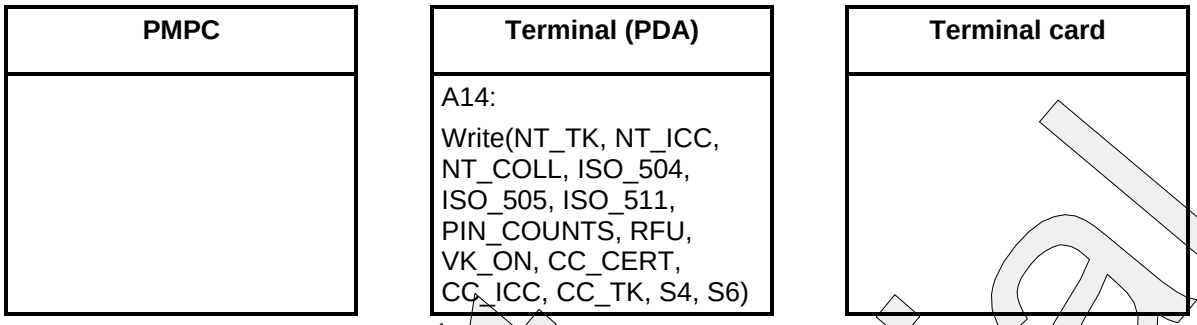


Figure 2: ATM off-line cash withdrawal

2.4.1.3 Differences between on-line and off-line ATM transaction

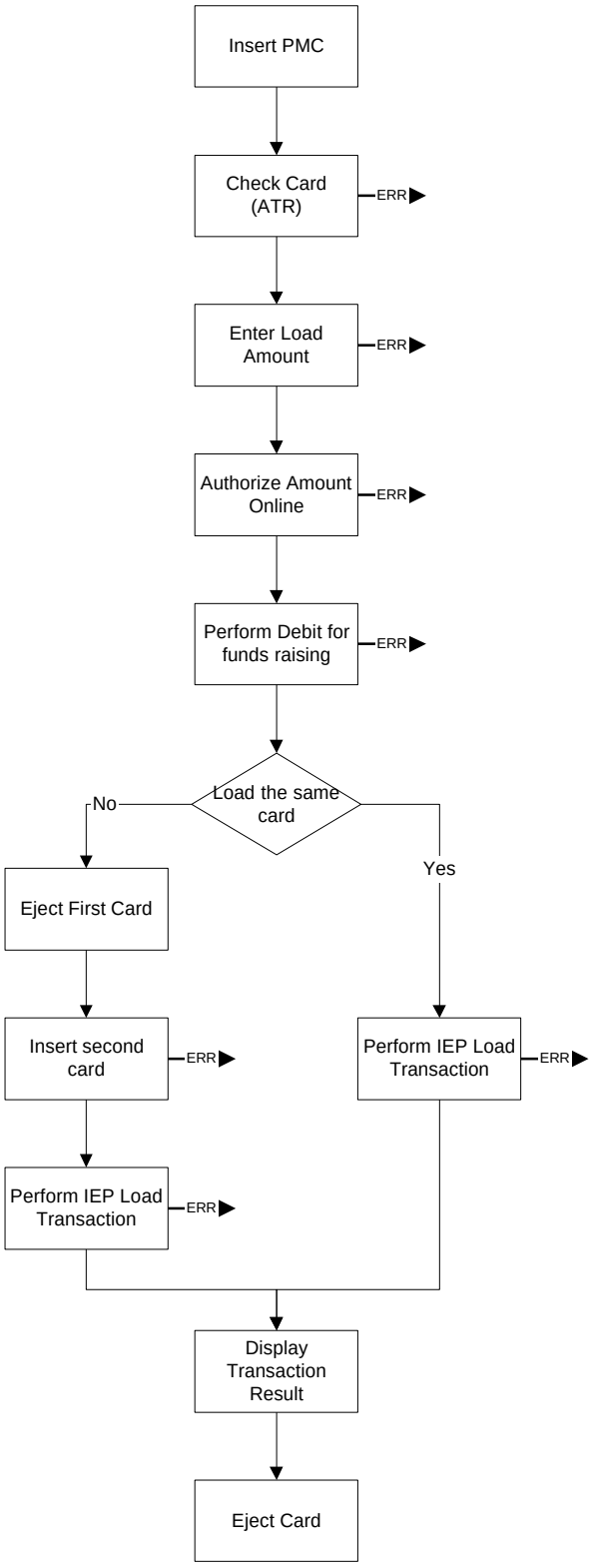
The main difference between off-line and on-line transaction are:

- the transaction authorization is not done by the host but by the ICC itself. Contrary to on-line authorization, an off-line authorization cannot overrule the card limit ISO_411.
- the signature S2 is generated with off-line session key instead of on-line session key
- signature S4 is only checked during clearing
- signature S6 is generated for approve the transaction from the terminal side.
- PIN checking is done only off-line

Note: The off-line ATM transaction serves only as a fallback strategy in case of a communication fault.

2.4.2 IEP Load Transaction

2.4.3 General Description



2.4.3.1 Description of the Load Diagram

- **Insert PMPC/Check Card:** The cardholder inserts the PMPC in the ATM. The ATM has to check, whether the inserted PMPC is a valid card. If the ATR of the card is not valid a appropriate message should be displayed on the ATM and the PMPC should be returned to the cardholder.

- **Enter Load Amount:** As for a regular cash withdrawal transaction, the cardholder has to enter the amount to be debited from the account related to the card.

- **Authorise Amount Online:** The transaction amount has to be authorized online. Within the on-line authorization also the signature S1 obtained from the card is checked in the backend system and the signature S2 is calculating for authenticating the back end system against the card. If the authorisation is denied, no debit and therefore no load transaction can be performed.

- **Perform Debit for funds raising:** The Debit transaction is performed with the PMPC card and a confirmation is sent to the back end system along with the signature S4 obtained from the PMPC.

- **Load the same card:** After the Debit transaction has been completed successfully, the cardholder has the possibility to change the card for loading the debited amount to an electronic purse residing on a other PMPC.

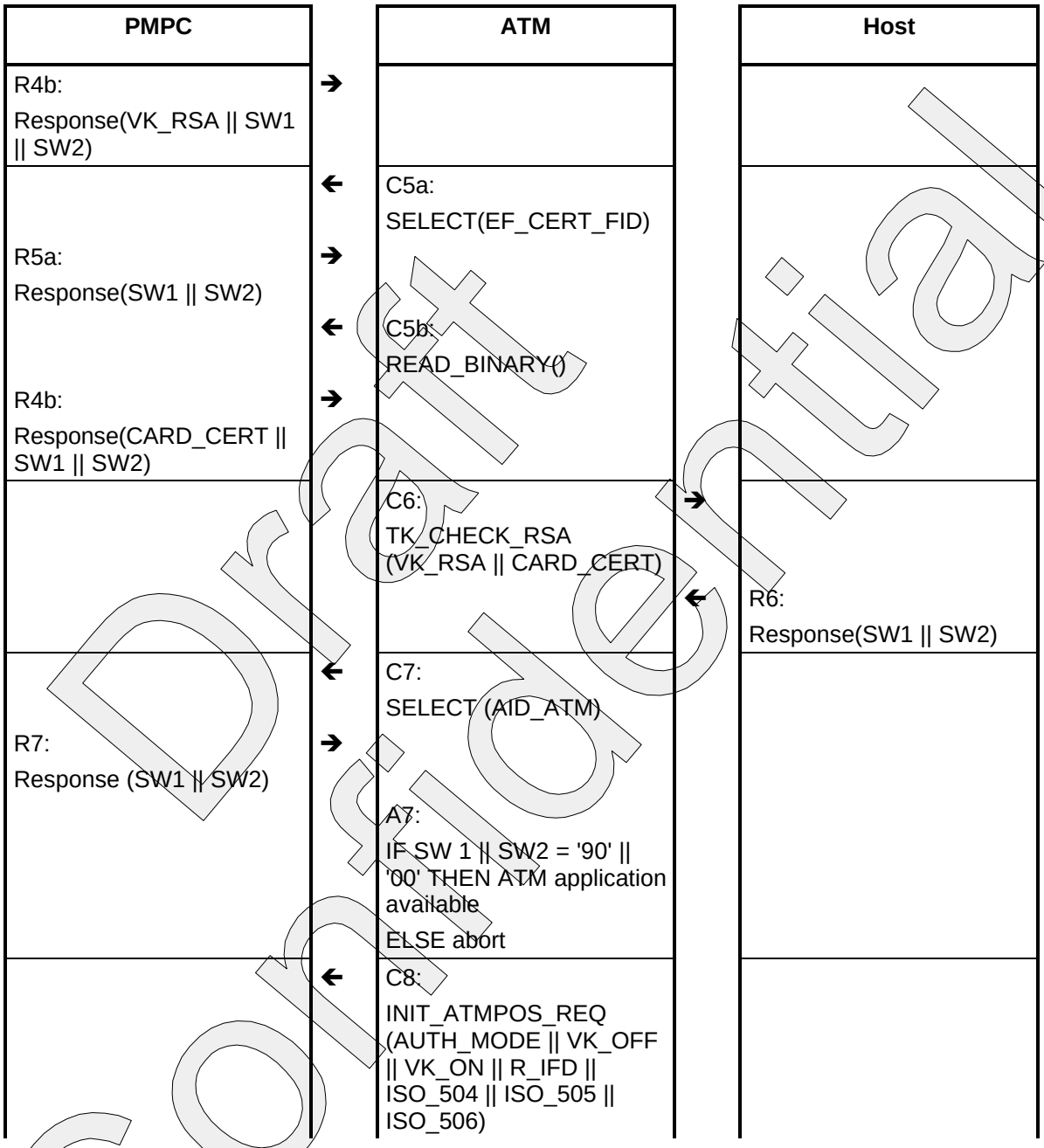
- **Perform IEP Load transaction:** The Proton IEP is loaded with the debited amount. The transaction has to be performed according to the Banksys specifications for IEP load.

- **Display transaction result:** The result of the transaction is displayed on the ATM and the card is returned to the cardholder.

2.4.3.2 Debit and Load transaction with the same PMPC

If the Debit transaction and the Purse Load transaction are performed with the same card, this allows a very easy and straightforward card loading, respectively unloading operation, whereby the cardholder only needs to insert the card and enter amount and PIN. The purse credit amount is automatically booked from the card linked account.

PMPC		ATM		Host
	←	C1: RESET		
R1: Response (ATR)	→			
		A1: IF ATR = nok THEN abort		
		A2: Identify ISO_511 and ISO_512 (transaction amount in the terminal's currency) Calculate payment type C2a: READ_RECORD	→	
			←	R2a: Response(NT_TK || SW1 || SW2)
		C2b: SELECT (AID_ATM)	→	
			←	R2b: Response (SW1 || SW2)
		C3: TK_RSA_ANF (CAD_RSA_ANF, CARD_NR)	→	
			←	R3: Response(RSA_ANF || SW1 || SW2)
	←	C4a: SELECT(EF_MEPS_FID)		
R4a: Response(SW1 || SW2)	→			
	←	C4b: READ_BINARY		



PMPC		ATM		Host
R8: Response (AUTH_MODE || ISO_305 || ISO_307 || ISO_310 || AWS || LKZ || DUPL_NUM || SECTOR_ID || ISO_403 || ISO_405 || ISO_407 || ISO_410 || ISO_411 || ISO_317_316 || ISO_401 || ISO_402 || ISO_404 || ISO_406 || ISO_406_TERM || ISO_408 || ISO_409 || VK_ON || VK_OFF || NT_ICC || PIN_REMAIN || S1 || SW1 || SW2)	→			
		A9: • Generate off-line session key • Check S1 (in terminal card) • Authorize Transaction	→	
		A10: Find PIN_TRX		
	←	C11: VERIFY_PIN_REQ (PIN_TRX)		• Check card signatures • Authorize ATM transaction (available amount, blacklist, ...) • Check PIN (in the bank Host) • Generate on-line session key • Generate S2 with on-line session key
R11: Response(SW1 || SW2)	→		←	
	←	C12: ATMPOS_TRX_REQ (AUTH_MODE || ISO_510 || ISO_317_316 || ISO_511 || ISO_512 || AVAUL_AMOUNT || AI || S2)		
R12: Response(S3 || S4 || SW1 || SW2)				

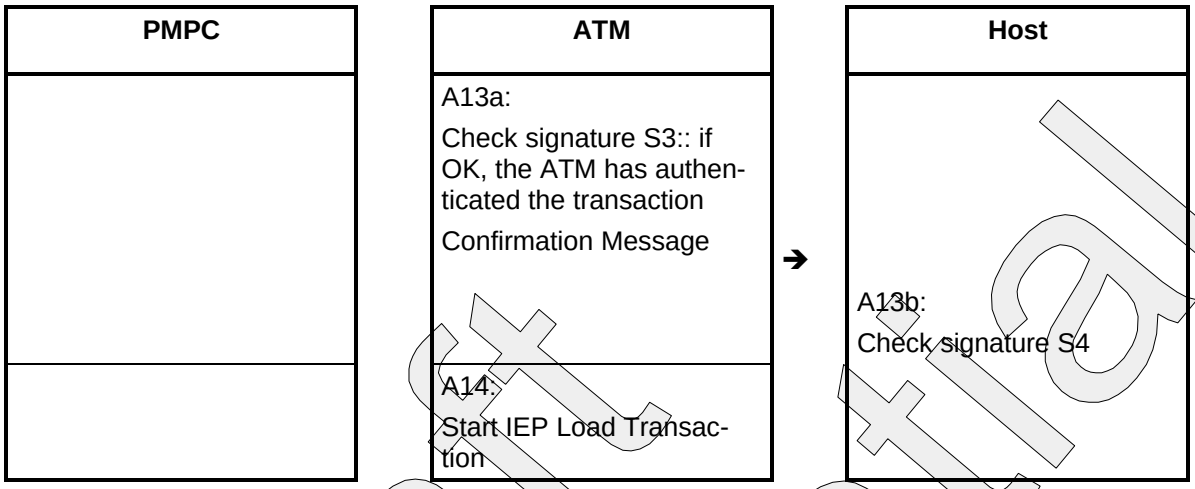
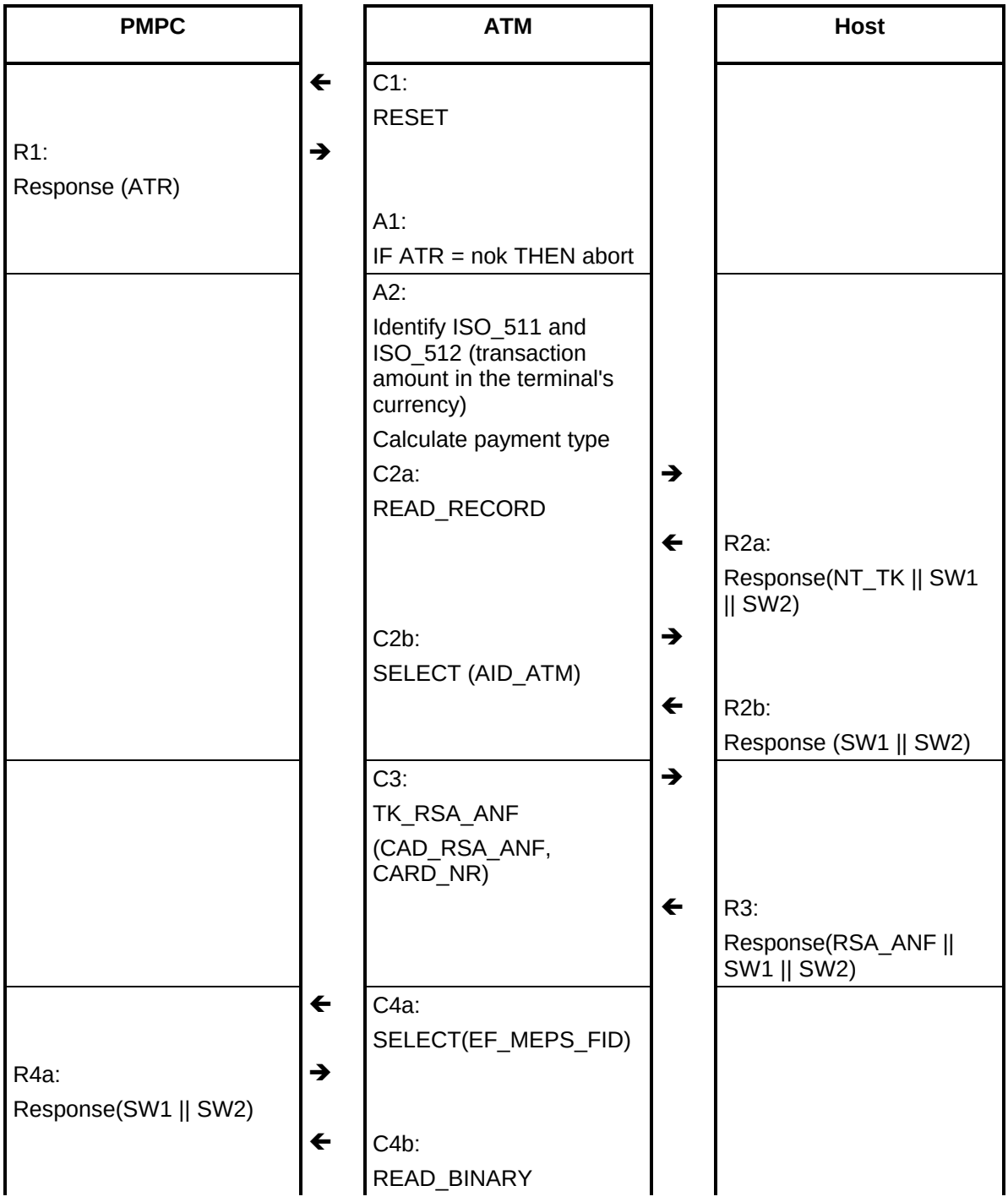


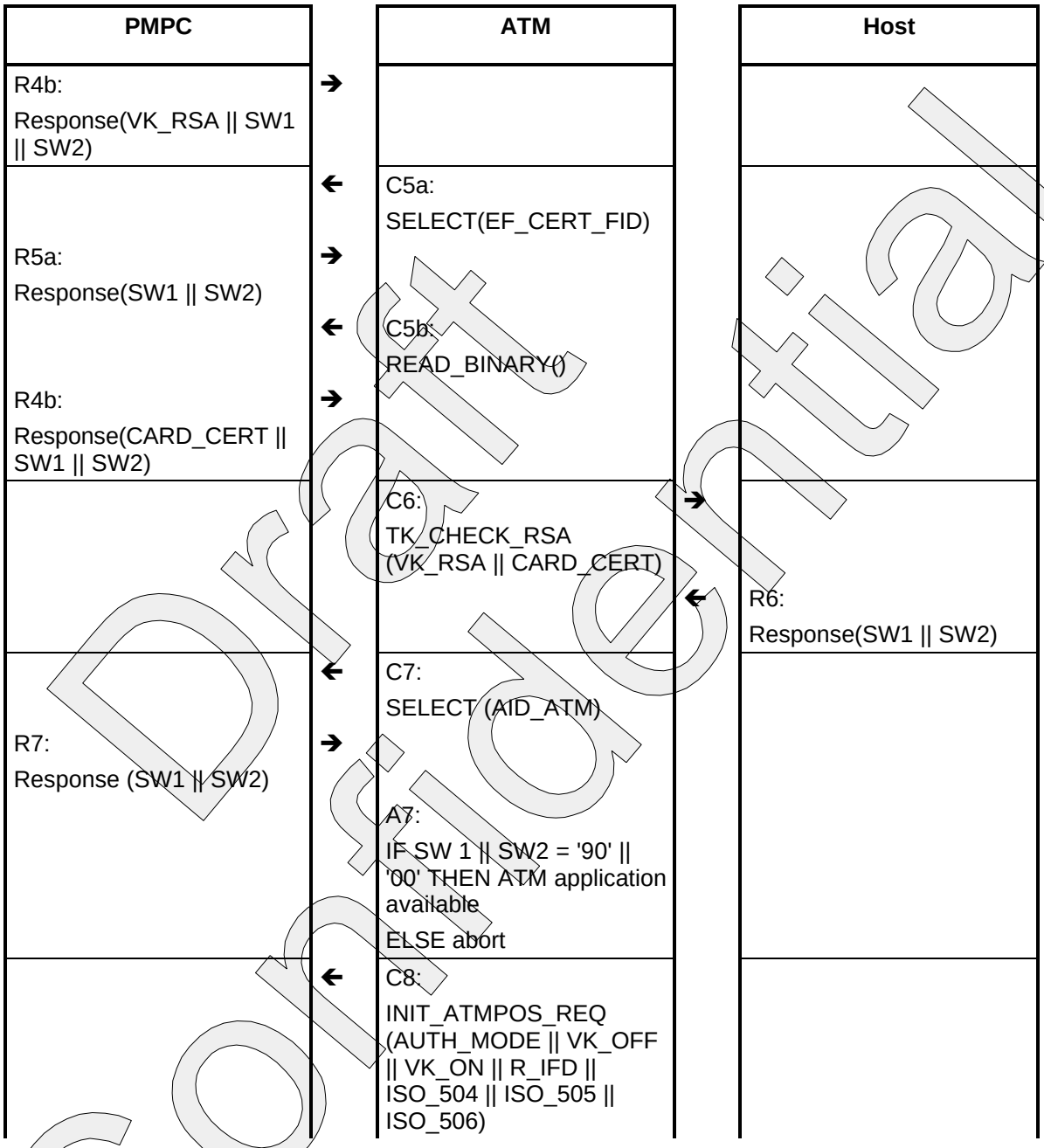
Figure 3: PMPC Load transaction

Note: After the ATM receives a correct response of the authorisation request, a reverse transaction has to be performed in case of an occurring fault while loading the electronic purse.

2.4.3.3 Debit and Load transaction with different PMPCs

As it is currently not common, to equip the ATM with two card readers, the cardholder must first insert the ATM card and enter load amount and PIN. After authorization, the cardholder retrieves the first card and inserts the card onto which he wants to load the previous debited amount.





PMPC		ATM		Host
R8: Response (AUTH_MODE || ISO_305 || ISO_307 || ISO_310 || AWS || LKZ || DUPL_NUM || SECTOR_ID || ISO_403 || ISO_405 || ISO_407 || ISO_410 || ISO_411 || ISO_317_316 || ISO_401 || ISO_402 || ISO_404 || ISO_406 || ISO_406_TERM || ISO_408 || ISO_409 || VK_ON || VK_OFF || NT_ICC || PIN_REMAIN || S1 || SW1 || SW2)	→			
		A9: • Generate off-line session key • Check S1 (in terminal card) • Authorize Transaction	→	
		A10: Find PIN_TRX		
	←	C11: VERIFY_PIN_REQ (PIN_TRX)		• Check card signatures • Authorize ATM transaction (available amount, blacklist, ...) • Check PIN (in the bank host) • Generate on-line session key • Generate S2 with on-line session key
R11: Response(SW1 || SW2)	→		←	
	←	C12: ATMPOS_TRX_REQ (AUTH_MODE || ISO_510 || ISO_317_316 || ISO_511 || ISO_512 || AVAUL_AMOUNT || AI || S2)		
R12: Response(S3 || S4 || SW1 || SW2)				

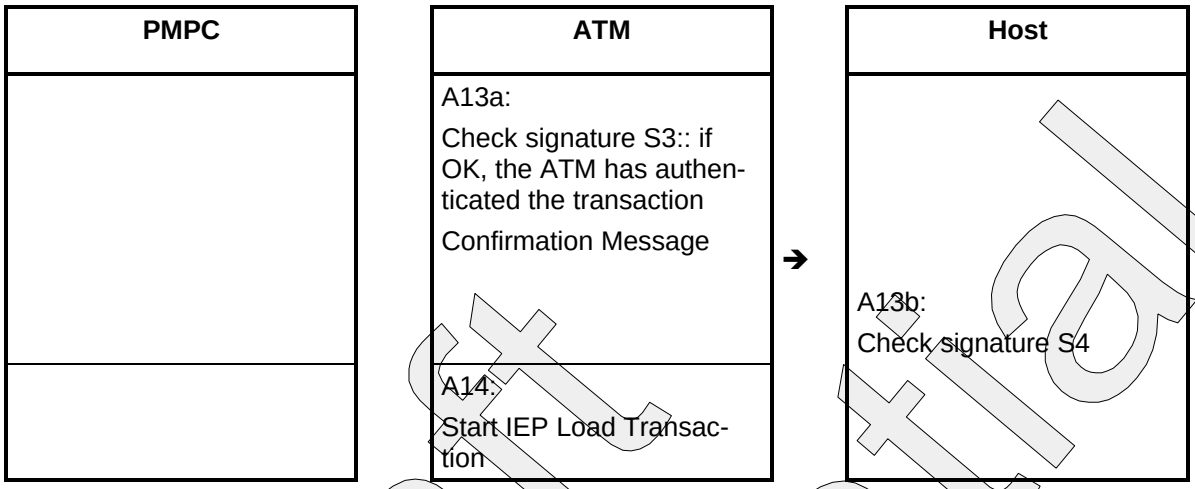


Figure 4: PMPC Load transaction

2.4.3.4 Error Recovery

The following error recovery is put in place:

- **PIN error:** If the cardholder enters a wrong PIN, the normal PIN retry logic applies. After three consecutive wrong PIN entries, the card is blocked and the transaction is aborted. No crediting on the card is performed. The ATM transaction with the host is reversed (comparable to an unsuccessful withdrawal).
- **Host authorization unsuccessful:** In such case the action indicator (AI) in the response message from the host indicates what to do: either return card (with no load), collect the card or invalidate the card.
- **Host communication error:** If the on-line authorisation fails, the transaction is aborted without loading. Off-line fallback is not supported for load transactions. Indeed due to their extreme sensibility, the master load keys are only stored centrally in the back end system and not held distributed in the ATMs.
- **ATM or load transaction fails on the cardholder fault (e.g. cardholder does not enter his purse card):** The transaction is aborted, no loading takes place. The ATM transaction with the host is reversed.

2.4.4 IEP Unload Transaction

An IEP unload transaction can only be performed with the same card. This means that the unloaded amount from the electronic purse, can only be loaded to the account related to the same card. Cash withdrawal within a electronic purse unload transaction is not possible. From the transaction point of view an IEP unload is an IEP purchase transaction followed by a transaction for crediting the customer account with the amount previously unloaded from the electronic purse.

Note: If an error occurs during the credit transaction, it is not possible to load the unloaded amount back to the electronic purse, because an off-line load transaction can not be performed for security reasons.

2.5 Hardware requirements

The following additional hardware requirements have to be fulfilled:

2.5.1 ICC reader

The ATM must have a hybrid reader, capable of reading both chip card and magnetic stripe. The chip card reader must completely be compatible to ISO-7816.

2.5.2 Terminal Card Interface

In order to implement more easily the necessary new cryptographic requirements, also the ATM shall be equipped with a terminal card. The ATM must be able to communicate with a terminal card using the T=1 protocol defined in ISO 7816-3.

2.6 Terminal Card

The ATM terminal card is used for calculating the transaction keys and for securing the communication between the ATM and the back end system. Therefore, the ATM terminal card has to store at least the following keys:

- **master off-line ATM key:** Used to authenticate the ATM and to secure an off-line ATM transaction. Only one instance of this master key is present in a Terminal Card. If this master key is broken, the next key version needs to be put in service.
- **master invalidation keys:** Allows the ATM to invalidate any file on customer cards. Different instances of this key must be stored (expiry year dependent).