

Merchant Guide for SSL Based Card Acquiring (PSIP).

Version 3.0

PBS A/S
Lautrupbjerg 10
DK-2750 Ballerup
T. +45 44 6844 68

1 Contents

1	CONTENTS.....	2
2	SYNOPSIS.....	4
3	PURPOSE7	
4	INTRODUCTION.....	8
4.1	OVERVIEW OF PSIP SHOPPING AND PAYMENT	9
4.2	CARDHOLDER SHOPS FROM HIS PC	10
4.3	TRANSACTION TYPES.....	10
4.3.1	<i>Authorization.....</i>	<i>10</i>
4.3.2	<i>Authorization Reversal.....</i>	<i>10</i>
4.3.3	<i>Capture.....</i>	<i>10</i>
4.3.4	<i>Return/Credit.....</i>	<i>10</i>
4.4	DETAILED DESCRIPTION OF SHOPPING AND PAYMENT.....	11
4.4.1	<i>Basic features of PSIP for ecommerce:.....</i>	<i>11</i>
4.4.2	<i>Transaction balancing.....</i>	<i>12</i>
4.4.3	<i>The basic message flow extended for IA in ecommerce environments.....</i>	<i>12</i>
4.4.4	<i>Implementing eDankort and 3-D Secure using the IA extension.....</i>	<i>16</i>
4.4.5	<i>Recurring transactions (subscription).....</i>	<i>22</i>
4.4.6	<i>Return/Credit.....</i>	<i>23</i>
4.4.7	<i>Clearing methods.....</i>	<i>23</i>
4.5	ERROR SITUATIONS, ROLES AND RESPONSIBILITIES.....	24
5	PROTOCOL SPECIFICATIONS.....	26
5.1	NETWORK LAYER.....	26
5.2	SSL LAYER	26
5.3	MESSAGE FORMAT AND TYPES.	26
5.3.1	<i>Introduction.....</i>	<i>26</i>
5.3.2	<i>Message Format.....</i>	<i>27</i>
5.3.3	<i>PGTM Routing header.....</i>	<i>27</i>
5.3.4	<i>PSIP header</i>	<i>28</i>
5.3.5	<i>PSIP messages.....</i>	<i>28</i>
5.3.6	<i>ISO 8583 v.1.....</i>	<i>28</i>
5.3.7	<i>PSIP Authorization Request.....</i>	<i>31</i>
5.3.8	<i>PSIP Authorization Response.....</i>	<i>37</i>
5.3.9	<i>PSIP Reversal Advice.....</i>	<i>40</i>
5.3.10	<i>PSIP Reversal Advice Response.....</i>	<i>42</i>
5.3.11	<i>PSIP Capture Request.....</i>	<i>43</i>
5.3.12	<i>PSIP Capture Response.....</i>	<i>47</i>

5.3.13	Definition TAG/LENGTH/VALUE data element:.....	49
5.3.14	Tag definition.....	49
5.3.15	Examples: Reconciliation Counter Id, Reconciliation Counter Name, and Card Name 53	
5.4	ISSUER AUTHENTICATION (IA) MESSAGES EXTENSION	54
5.4.1	Data transport /connection.....	54
5.4.2	Data dictionary	54
5.5	AUTHENTICATION INITIALIZATION.....	61
5.6	AUTHENTICATION DECLINE	62
5.7	AUTHENTICATION APPROVAL.....	63
6	SECURITY REQUIREMENTS	65
6.1	CARD SECURITY PROGRAMME (THE PCI STANDARD).....	65
7	REQUIREMENTS TO CARDHOLDER INTERFACE IN ECOMMERCE/IA ENVIRONMENTS	66
7.1	ORDER NUMBER	66
7.2	EXPIRATION DATES.....	66
7.3	CARD VERIFICATION DATA (CVD)	66
7.4	CARDHOLDER RECEIPT.....	67
7.5	TRUNCATION OF THE CARD NUMBER (PAN)	67
7.6	DISPLAYING SECURE SESSIONS	69
	APPENDIX A ACTION CODE	70
	APPENDIX B PGW RESPONSE CODE.....	74
	APPENDIX C MESSAGE SAMPLES: E-COMMERCE.....	75
C.1	AUTHORIZATION REQUEST	75
C.2	AUTHORIZATION RESPONSE	75
C.3	CAPTURE REQUEST	76
C.4	CAPTURE RESPONSE	76
	APPENDIX D RULES REGARDING CVD	77
D.1	CARDS WITH CVD	77
	APPENDIX E AUTHENTICATION PROCESSING IN 3-D SECURE.....	78
	APPENDIX F IMPLEMENTING OWN MPI	79

2 Synopsis

Document name	Merchant Guide for SSL Based Card Acquiring (PSIP).
Document Id	P:\Processor\Nytdkpr\ARKIV\KORTSELS\Merchant Guide\SSL merchant handbook\Merchant Guide SSL 3.0.doc
Document abbreviation	Merchant Guide SSL 3.0.doc
Purpose of the document	Guide/handbook for Merchants, Software-vendors or Web-hotels who wish to build Internet Merchant Servers interfacing with PBS SSL Payment Gateway.
Document history	<p>Version 0.1 03. December 1998, Henning Ploug, PBS International A/S</p> <p>Version 0.2 25. January 1999, Henning Ploug, PBS International A/S</p> <p>Version 0.3 22. February 1999, Henning Ploug, PBS International A/S</p> <p>Version 0.4 2. August 2000, Henning Ploug, PBS international A/S</p> <p>Version 1.0 9. January 2001, Henning Ploug, PBS international</p> <p>Version 2.0 1. May 2003, Henning Ploug, PBS Danmark A/S</p> <p>Version 2.1 10. June 2003, Thomas Juncker, PBS Danmark A/S</p> <p>Version 2.2 23. June 2004, Thomas Juncker, PBS Danmark A/S</p> <p>Version 2.3 22. September 2004, Thomas Juncker, PBS A/S</p> <p>Version 2.4 13. January 2005, Thomas Juncker, PBS A/S</p> <p>Version 2.5 3 March 2005, Thomas Juncker, PBS A/S</p> <p>Version 2.9 9 February , Thomas Juncker, PBS A/S</p> <p>Version 3.0 9 February , Thomas Juncker, PBS A/S</p> <p>New inserts in the newest version will be underlined and marked in the margin.</p>
Version date	10/03/2006 12:22 PM
Print date	13. March, 2006 - kl. 12:29
Writer	PBS A/S
Receiver	Merchants, Software vendors, Web-hotels, and IPSPs.
Copy to	
Document user	For internal use at Merchants, Software vendors, Web-hotels and IPSPs.

Quality assurance	Version 0.1	Draft, for use for pilot merchants/ web-hotels, quality assured internally by PBS International A/S.
	Version 0.2	Draft, for use for pilot merchants/ web-hotels, quality assured internally by PBS International A/S.
	Version 0.3	For use for pilot merchants/ web-hotels, quality assured by PBS International A/S, and the first pilot web-hotel.
	Version 0.4	For use by Merchants, Software vendors or Webhotels, quality assured by PBS international and selected software vendors.
	Version 1.0	For general use by Merchants, Software vendors and Web-hotels.
	Version 2.0	The "Netbank Authentication", "mPay" extension, and "card recognition on host" implemented and verified by pilot customers. Clarification adjustments implemented based on customer support.
	Version 2.1	128 bit DES and 1024 RSA demanded. Bitmap for some errors differ - only mandatory fields are present.
	Version 2.2	3-D Secure and new message types – internal review + external– not published
	Version 2.3	New message types discarded(postponed) Payment method choosing mandate for 3-D Secure. (Internal review. Pilot customer ensure quality.)
	Version 2.4	New appendix for setting up authentication result data, as an IPSP. Changes to Authentication Initialization message: re-presenting two fields mandatory in v. 2.0 for eDankort MerchantGmtoffset og PurchaseDate. Reversal of full authorized amount. New appendix for IPSP's having their own MPI.
	Version 2.5	CVD for Dankort mandatory - field 47 now only TAG's allowed - 6.3.14 TAG definition formats revised –Appendix E modulus 11 control removed - Appendix F revised.
	Version 2.9	Requirements to magnetic-stripe based terminals have been incorporated into this version of the ' <i>Merchant Guide for SSL Based Card Acquiring (PSIP)</i> '. Chapter 7 Security requirements now refer to the PCI standard published by MasterCard, Visa, Amex, Diners, and Discover etc. The mPay solution has been closed down. The former chapter 9 on 'Recommendations for Ecommerce' has been deleted – refer to PCI requirements – see Security Requirements. Appendices E and F have been modified. Text has been added to better readability, and explanation of terms and conditions has been improved.

	Version 3.0 Since new POS solutions must support ICC (Chip card), new magnetic-stripe based terminals will no longer be approved. Consequently, the references to magnetic-stripe based terminals have been removed from this version. Please refer to version 2.9, which also documents EFT-POS solutions already in operation.
Document maintenance	The Document will be maintained by PBS A/S.
Format	The Document is written in Microsoft Word 2002 for XP, and translated to PDF.
Changes	Any changes to the merchant or web-hotel systems, necessitated by changes to this specification, must be implemented in accordance with the agreement with PBS.
Copyright	ALL RIGHTS IN THE DOCUMENT, AND THE PSIP FORMAT, BELONG TO PBS A/S. THE MATERIAL, OR PARTS OF THE MATERIAL, MUST NOT BE DISTRIBUTED, OR BE AVAILABLE BY ANY WAY TO THIRD PARTIES.
Document info	<p>This document may contain technical inaccuracies. In case you find any, or if you have comments, please send these to:</p> <p>PBS A/S att: Thomas Juncker Lautrupbjerg 10 DK-2750 Ballerup</p> <p>e-mail: tfj@pbs.dk</p>

3 Purpose

The PSIP protocol - PBS SSL Internet Point Of Sale - described in this document has been designed for the exchange of payment card transactions via the internet using SSL as data encryption – a Cardholder shopping in an internet shop using a browser, keying in the payment card data in a secure (https) payment session

The document specifies the protocols used (PSIP, and IA extension), requirements for communication with the Cardholder, and the general security requirements which must be observed by an IPSP connected to PBS SSL Payment Gateway.

When used in this document, the following terms also have the following meaning:

Term	Meaning
Cardholder	Also covers: netbank user
Card brands/products	Also cover: eDankort
Payment card transactions	Also cover: eDankort transactions
IPSP (Internet Payment Service Provider)	A party that develops and/or operates a payment module designed on basis of this Merchant Guide.
Merchant	A party that has a merchant agreement with a card acquirer.

1. eCommerce

The document contains the information required by an IPSP in order to implement the necessary functions for the processing of payment transactions with payment cards (e.g. Dankort, MasterCard-products, Visa-products, JCB, Diners Club, American Express) or other payment methods using PBS's payment card infrastructure (e.g. eDankort).

An authentication protocol may be added to ecommerce transactions; the so-called IA extension (Issuer Authentication, cf. chapter 6.4). The IA extension is an HTML based protocol redirecting the cardholder's browser to the authentication system of the issuer.

The IA extension covers two concepts: eDankort and 3-D Secure (MasterCard Secure Code, Verified by Visa and J/Secure).

The PSIP protocol carries the Authentication Approval data.

4 Introduction

The PBS Authentication Router and/or SSL Payment Gateway can be accessed by any merchant that:

- implements the IA (Issuer Authentication) extension and/or PSIP protocol specified in this document
- successfully passes testing- and/or certification procedures as defined by PBS
- signs a merchant agreement with PBS or an acquirer who has an agreement with PBS on processing of payment transactions.

Instead of developing the IA extension and/or PSIP interface, merchants can use an IPSP (Internet Payment Service Provider) already certified by PBS.

This document specifies the network/transport, security and application message protocols, the character set, the error handling, the requirements to cardholder interface etc. in order for the merchant (or the IPSP - Internet Payment Service Provider) to be able to develop the interface to the PBS SSL Payment Gateway.

4.1 Overview of PSIP Shopping and Payment

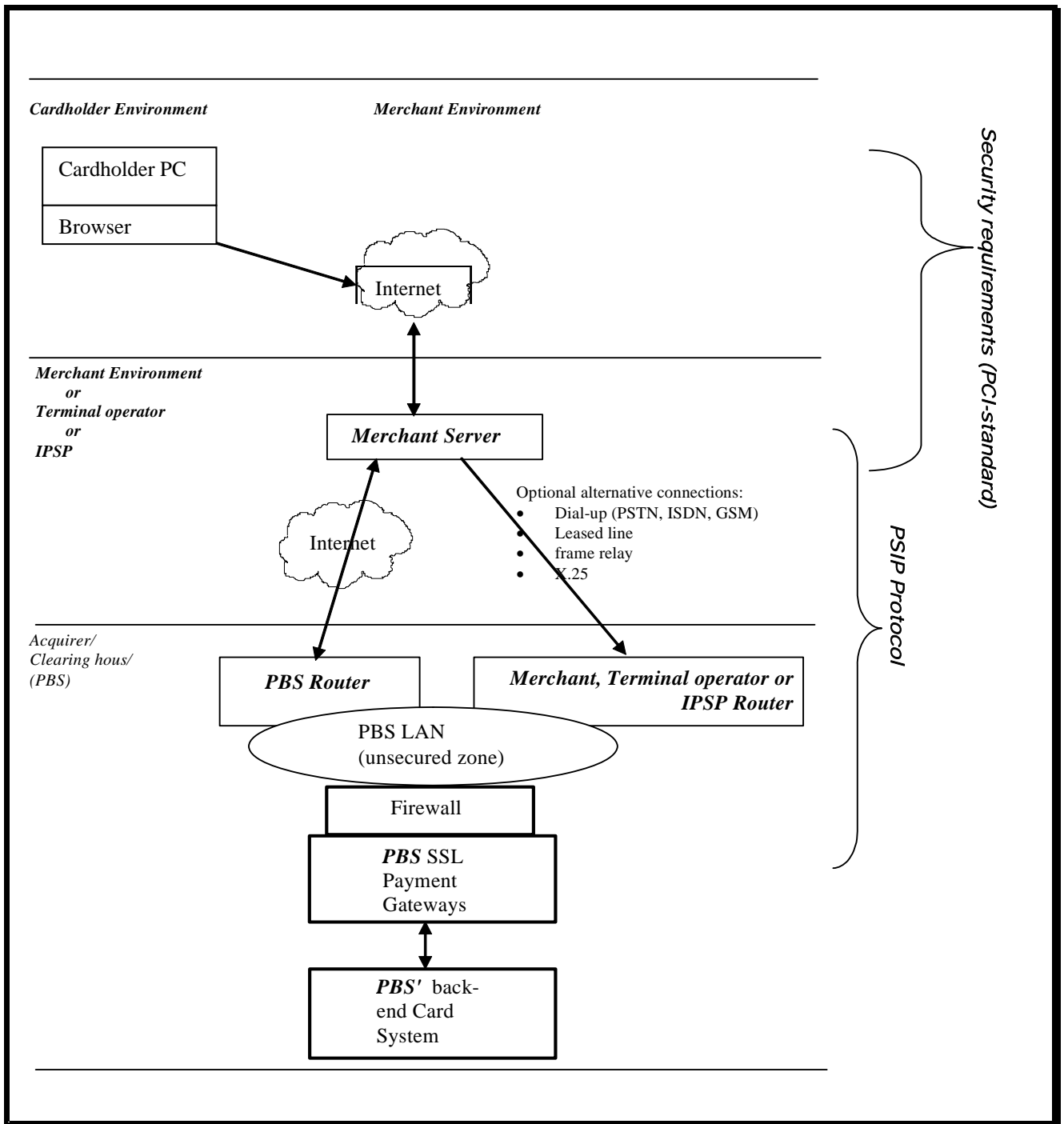


Figure 1: An overview of the PSIP-Protocol

4.2 Cardholder shops from his PC

The cardholder fills in his card data (card number (PAN), expiry date, and CVD) in the order confirmation page presented by the merchant.

SSL encryption must be used in order to protect the card data from being disclosed on the Internet.

When the merchant receives the card data, he forwards

1. an Authentication Initialization if he has registered for eDankort and/or 3-D Secure, and receives an Authentication Approval/Decline from the Issuer

and then/or just

2. forwards an Authorization Request to PBS using a PSIP message.
PBS will forward an Authorization Response – typically within seconds - with an action code which tells if the authorization was approved or declined (see Appendix A). The merchant then communicates the result of the Authorization Request to the cardholder.

When the merchant receives a PSIP Authorization Approval and has fulfilled the order (e.g. dispatched the goods or services), the merchant performs the financial data capture to claim his money from the acquirer.

4.3 Transaction types

4.3.1 Authorization

Authorizations can be requested for the 'accurate amount' or an 'estimated amount'.

4.3.2 Authorization Reversal

If after having performed a successful authorization, a merchant cannot fulfil the order in due time, an Authorization Reversal **should** be sent. The amount reversed must be the same as the amount authorized.

Especially when debit cards are involved, it can be critical for the cardholder's disposal of his account that the authorization is reversed. If the authorization is not reversed this could also affect the cardholder's possibility of placing a replacement order with the merchant.

4.3.3 Capture

Normally, the amount captured cannot exceed the amount authorized, except for specific merchant categories e.g. where gratuity is common. Besides, the merchant and the acquirer may have made special arrangements which the payment module must be able to support.

4.3.4 Return/Credit

The PSIP protocol supports credit transactions in settlement of formerly captured amounts. The merchant must be registered with its acquirer for this option.

Message Flow

4.4 Detailed description of Shopping and Payment

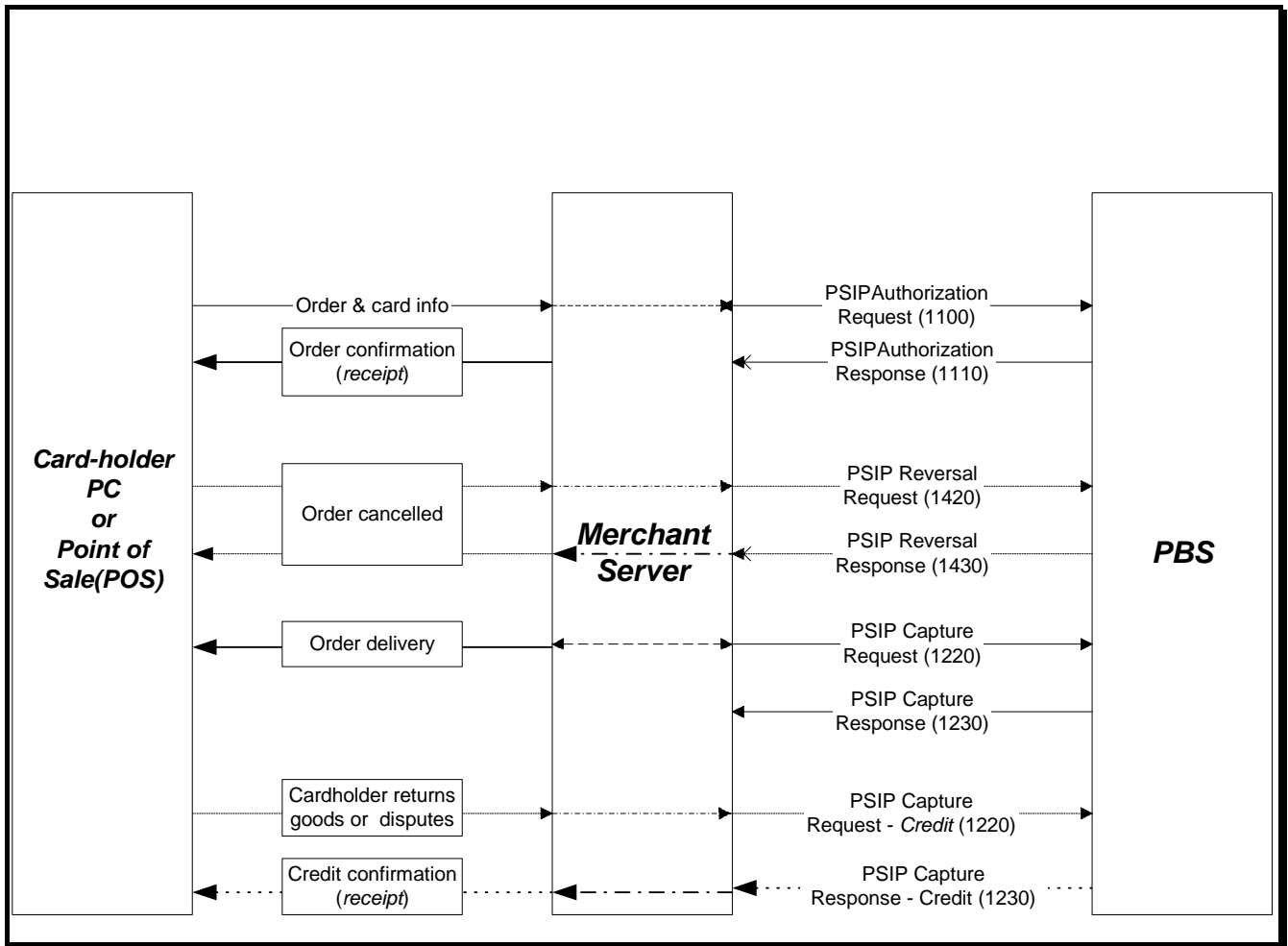


Figure 2: The basic message flow.

The protocol differs from many traditional POS-protocols, because it is optimized to take advantage of the Internet-communication channel and standard techniques used for program-to-program communication.

The PSIP-protocol consists of 3 sets of messages:

- PSIP-Authorization Request/Response (in short: Auth. Req., respectively Auth. Resp.)
- PSIP-Reversal Advice/Response (in short: Rev. Adv., respectively Rev. Resp.)
- PSIP-Capture Request/Response (in short: Cap. Req. respectively Cap Resp.)

The PSIP Capture Request/Response normally debits the cardholder's account, but in case of a cardholder dispute, a Capture Request/Response crediting the cardholder's account may be generated. This is known as the message set PSIP Capture Credit Request/Response.

4.4.1 Basic features of PSIP for ecommerce:

The basic features of this protocol are:

- At the time of ordering the merchant software generates a PSIP *Authorization Request*, receives a PSIP Authorization Response and stores (encrypted - see chapter 7) these messages in a database.
The status of the transaction is now "ready for fulfilment/delivery".

- The merchant's workflow must in the "order delivery process" provide a notification, when the order is shipped to the customer.
This notification changes the status of the transaction from "ready for fulfilment" to "ready for billing". The merchant software sends each cardholder billing as a single transaction and receives an individual receipt transaction for each billing. This is done by generating a PSIP Capture Request and PBS will reply with a PSIP Capture Response.

When generating the Capture Request, field 56 from the Authorization Response must be included. This field contains a unique token.

Capture Requests may at the merchant's request and against the merchant's payment of the costs in this relation be transmitted to PBS in batches.

4.4.2 Transaction balancing

PBS keeps track of a business transaction 'account' to allow only transactions if the account balances.

The rules are:

- First transaction must be an original authorization
- Reversal must not exceed authorized amount
- Capture Debit must not exceed authorized amount
- Capture Credit must not exceed the captured amount

4.4.3 The basic message flow extended for IA in ecommerce environments

In PSIP environments, the identity of the cardholder is not authenticated. Acquirers, issuers, and card organisations are demanding cardholder authentication to prevent rising fraud. One way of authenticating the cardholder is by using the financial institutions' netbank systems, which are in general use.

IA is beneficial to both merchant, acquirer and issuer, since the number of counterfeit payment transactions are reduced. Especially "card details misused by a third party" and "cardholder claims that he/she did not engage in or authorize the transaction" situations can be avoided.

The extension to support "IA" consists of 2 extra messages¹, which the merchant server must submit and accept before effecting the normal PSIP Authorization Request (see also Figure 3)

- "Authentication Initialization"
- "Authentication Approval/Decline"

These messages are HTML forms – see 5.5 **Authentication Initialization**, 5.6 **Authentication Decline**, and 5.7 **Authentication Approval**.

The PSIP Authorization Request message carries data, which proves the cardholder authentication.

¹ A merchant or IPSP that wants to implement its own authentication server (MPI), can drop the HTML messages, and set up the PSIP messages from the 3-D Secure messages processed, and the additional set-up defined in **Appendix F**.

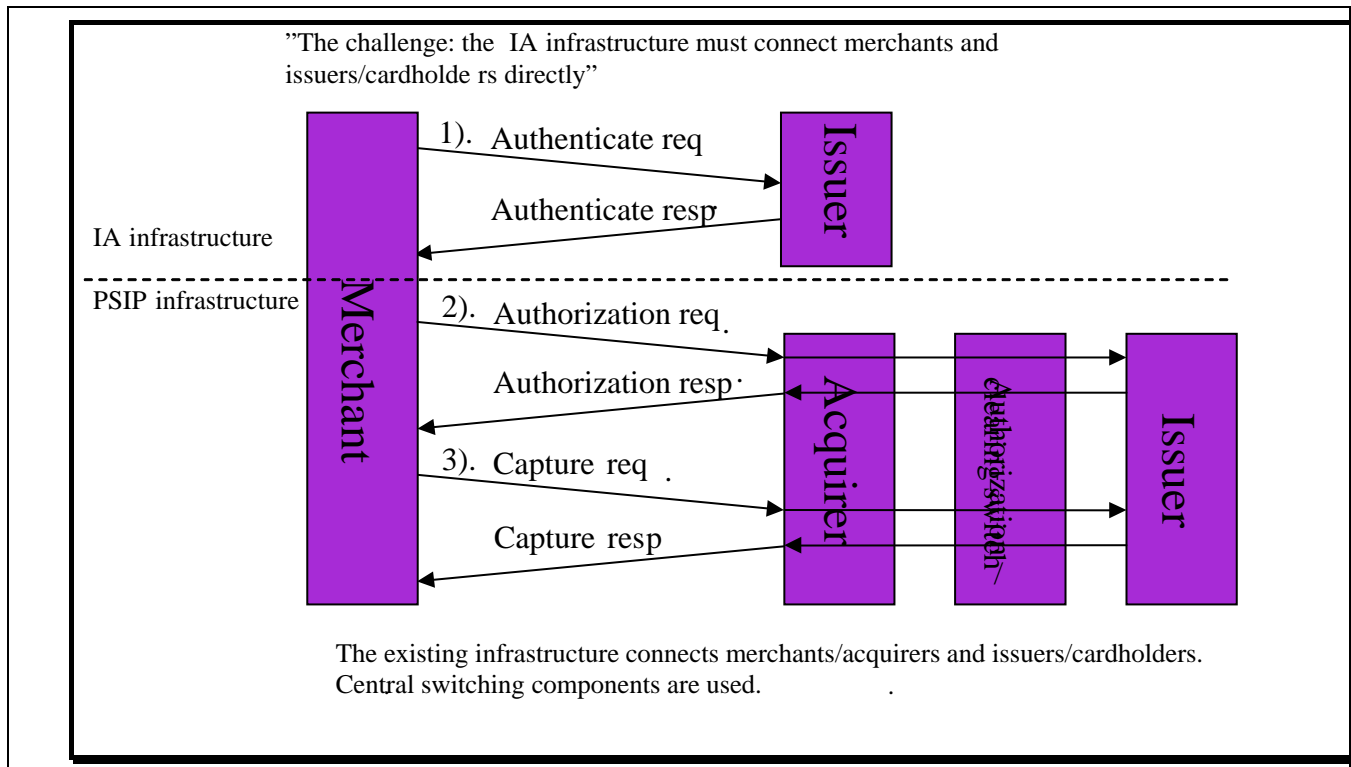


Figure 3: : Authentication as an extension of the existing infrastructure

On the next pages the "IA" extension is described. The description covers the flow from the point where the cardholder selects to pay with a card product using "IA" until the PSIP Authorization Request is sent from the merchant server to PBS. From this point the flow will be as described in figure 1 (PSIP).

IA can be used for "eDankort" transactions, 3-D Secure (known under logos like "Verified by VISA", "Secure Code" from MasterCard, and "J/Secure" from JCB).

Due to the fact that 3-D Secure is an enhancement of the payment cards, the payment page must show both the 3-D Secure logos and the payment card logos.

When it comes to the choice of payment, each set of card logos must be shown separately; see the example below. This is necessary to determine the field 'CardLogo' which is a data element in the Authentication transaction.

The following examples show

- 1) the payment cards, which the merchant accepts,
- 2) that the merchant is both 3-D Secure and eDankort enabled, and
- 3) that the merchant accepts Dankort without IA - PSIP (SSL solely) :

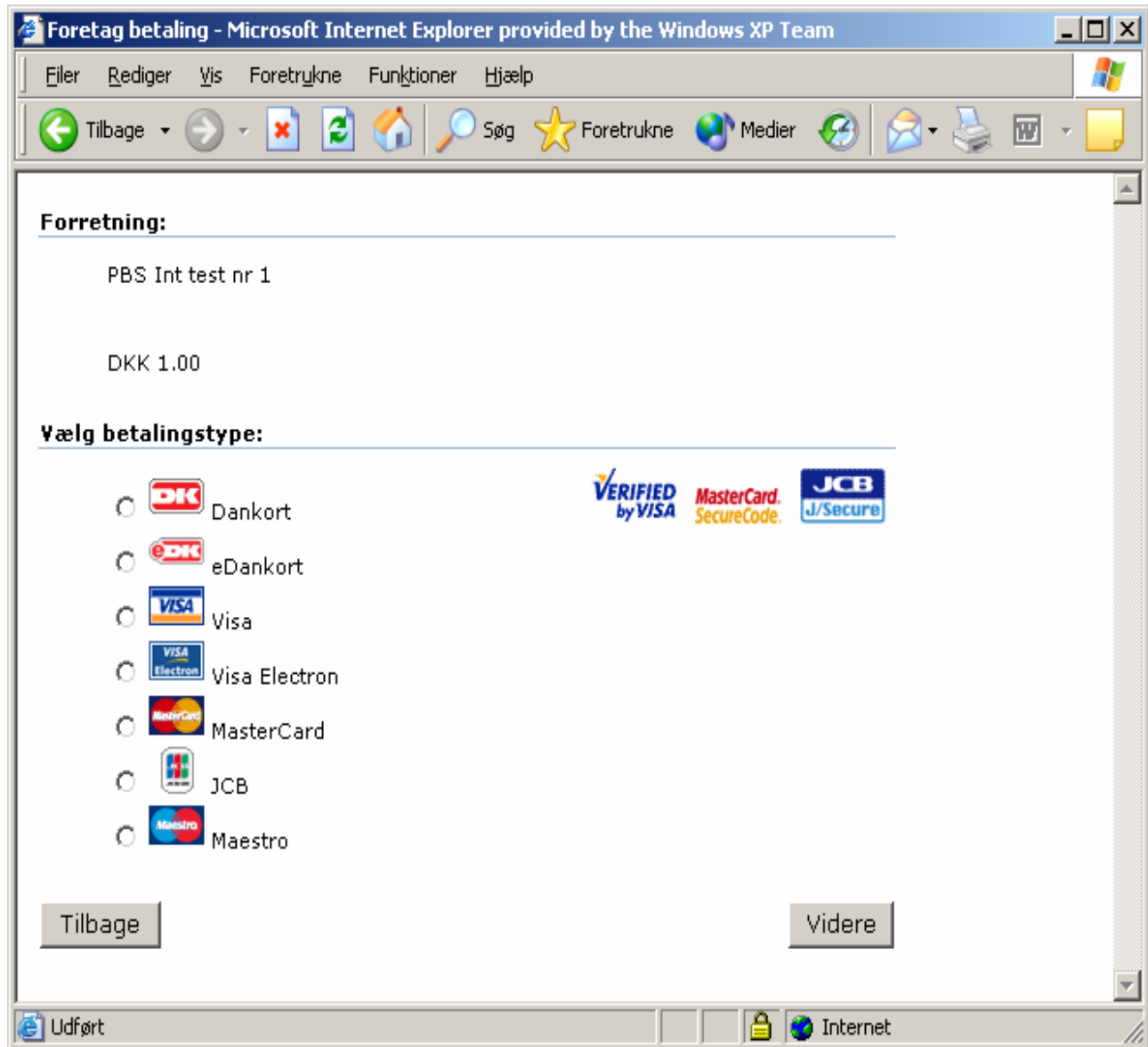


Figure 4: Payment select page

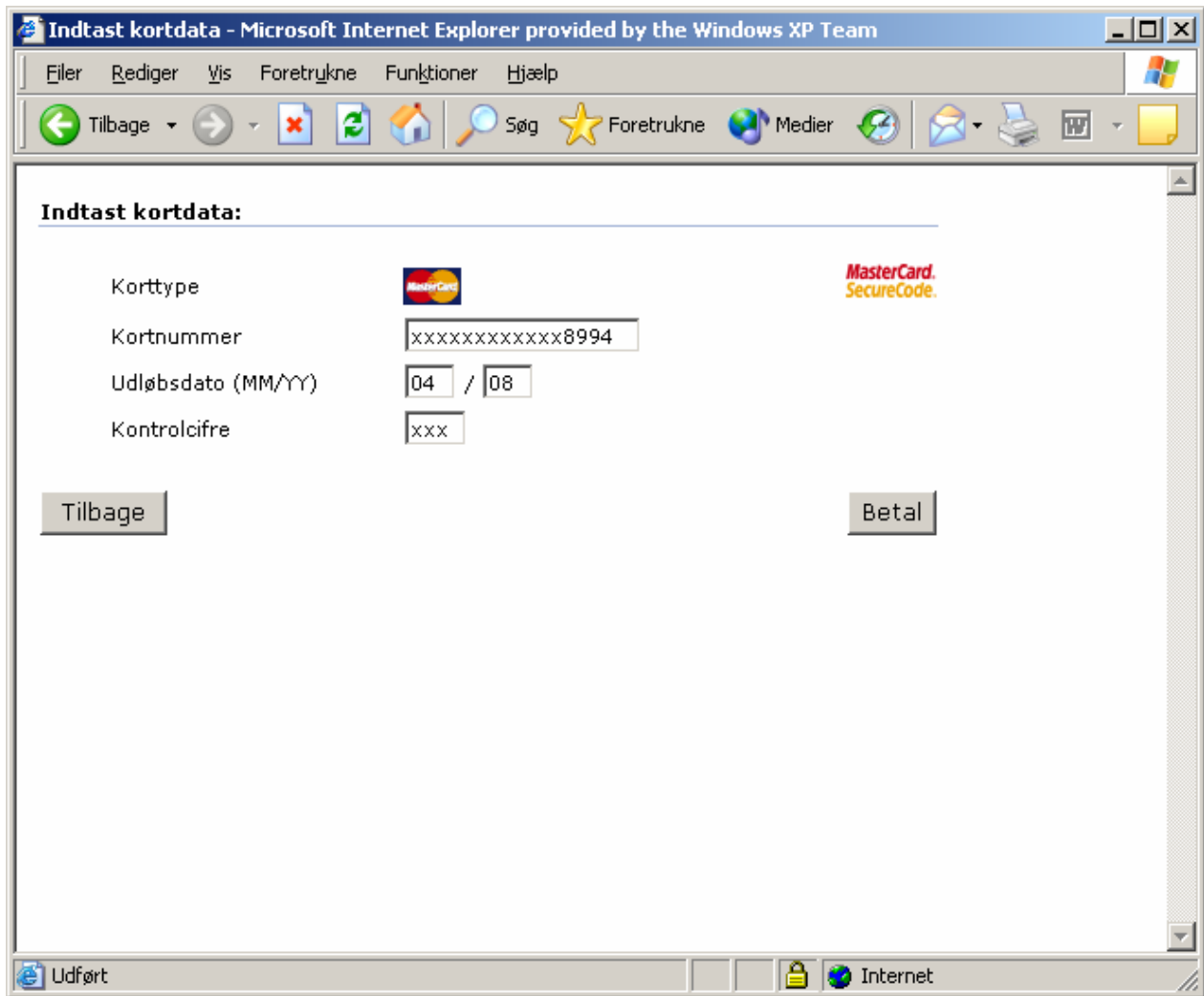


Figure 5: Payment data key-in page

For a 3-D Secure enabled merchant, each Visa(including Visa Electron), MasterCard(including Maestro), and JCB transaction will be handled as a "Verified by VISA", "Secure Code", or "J/Secure" transaction, which means that an authentication will be attempted.

If the cardholder is not fully authenticated (TransactionStatus not 'Y' - e.g. if cardholder is not 3-D Secure enrolled), the transaction may be completed(except for Maestro, which always requires cardholder authentication), see Appendix E.

In order to protect himself against fraud in these situations, the merchant should always request the CVD and include the CVD in the Authorization Request.

4.4.4 Implementing eDankort and 3-D Secure using the IA extension

The following describes how eDankort and 3_D Secure is implemented using the IA extension.

4.4.4.1 Implementing eDankort

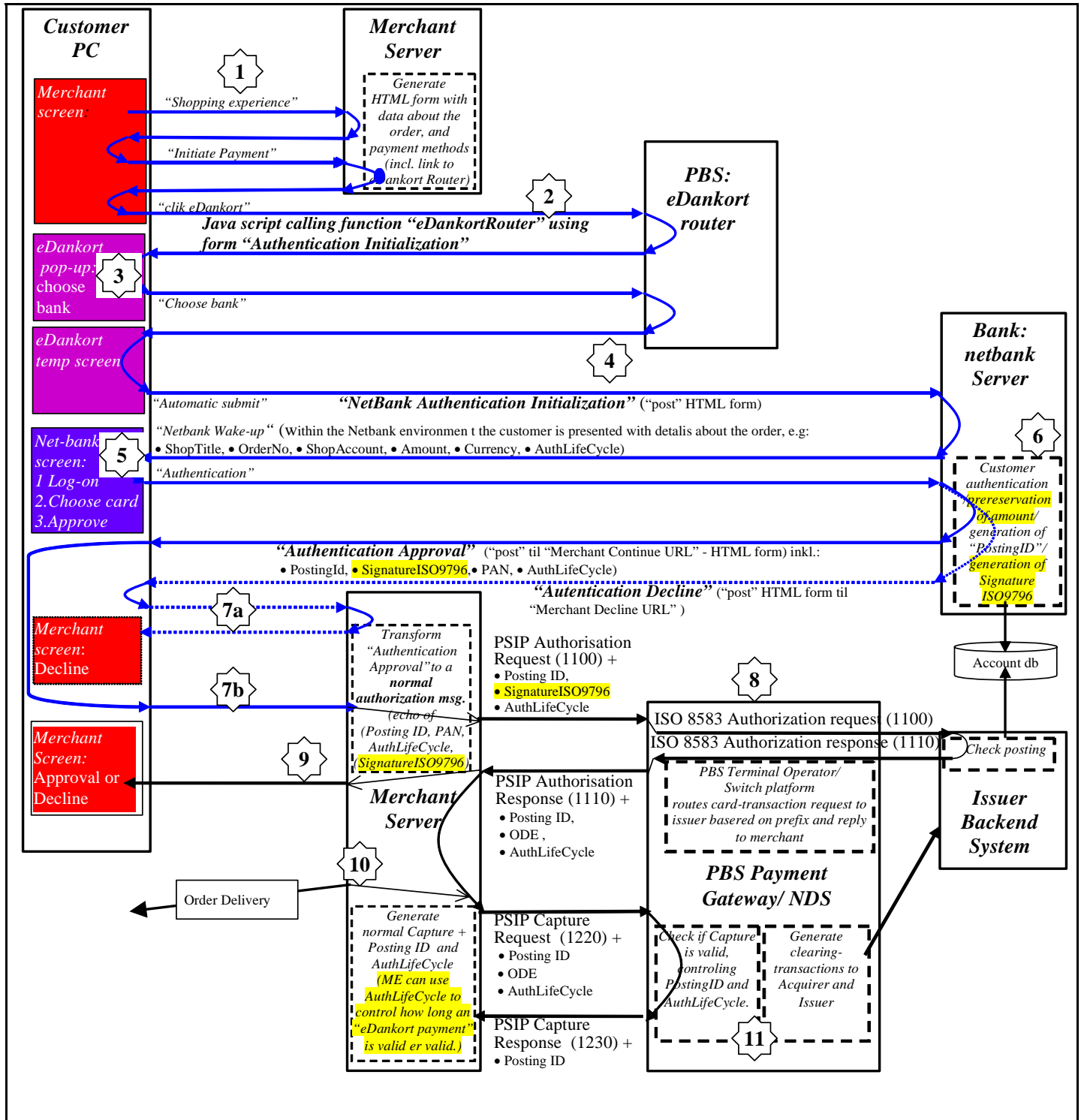


Figure 6: The basic message flow extended for eDankort.

Explanation to the figure:

- If a headline is underlined, the headline reflects a message definition, which the merchant must implement. Messages are defined in later chapters.
- Text shaded with yellow in the description and in the figure may optionally be used by the merchant and/or bank.



Initiate Payment:

The cardholder is shopping at the merchant. The merchant server generates a web-page containing the eDankort logo and a script (in the following referred to as the "eDK script" - see 4.4.4.2.3) activating the function "eDankortRouter" using the HTML form "Authentication Initialization" with data regarding the order.



Authentication Initialization :

When the cardholder chooses to pay using "eDankort" as payment method (by clicking the eDankort button/icon) the "eDK script" generates a pop-up window on the cardholder PC. The "eDK script" also submits the AuthenticationInitialization form to the eDankort router - which is responsible for the content of the pop-up window.

The Merchant Server is obligated to allow a time period of minimum 5 min. to receive the response messages, giving the customer the necessary time to complete the authentication process at the Netbank.



Select Netbank:

The customer is now able to choose the bank that has issued his/her eDankort in the drop-down list of participating netbanks. A "cookie" containing data regarding the bank, which the customer uses, may be stored on the customer's PC.



Netbank Authentication Initialization

When the cardholder has chosen his/her Netbank, the cardholder's browser is forwarded to the bank (via a temporary page²) with data originally obtained from the merchant regarding the payment (amount, merchant name, merchant ID, order number) in order for the cardholder to be able to uniquely identify the shop and to approve the eDankort payment in the Netbank.



Wake-up Netbank:

The netbank is started in the cardholder's browser, the cardholder logs on using his/her usual netbank password.

The cardholder is presented with information regarding the purchase.

The cardholder is now able to choose which card number/account to use for the eDankort payment from a list of his/her available cards/accounts.



Authentication:

The cardholder must then accept the purchase. The netbank authenticates the cardholder and generates authentication data.

² a page that automatically will submit itself



Authentication Decline:

This message is used when:

- the netbank is participating in the eDankort programme and a cardholder tried logging on, but the netbank could not authenticate cardholder.

If the netbank cannot authenticate the cardholder, the netbank application will direct the cardholder's browser to a web-page defined by the merchant (DeclineURL), forwarding the HTML form "Authentication Decline".



Authentication Approval

This message is used when:

- the netbank authenticates the cardholder

The NetBank server redirects the cardholder's browser to the merchant server (using the merchant defined approved URL), forwarding the HTML form "Authentication Approval" which include authentication data.

Also a field called "AuthLifeCycle" is generated. This field contains information on the period of time for which the authorization approval is valid. It is important that the merchant presents the financial claim (sends the PSIP "Capture Request") before the deadline mentioned in AuthLifeCycle expires, since PBS will automatically decline any later arriving captures.

Subsequently, the merchant must follow the normal PSIP flow.

If the transaction is approved by the netbank, the Merchant Server must now generate a "PSIP Authorization Request" by moving fields from the "Authentication Approval" message to the "PSIP Authorization Message".

The PSIP message contains more data elements than an SSL Ecommerce transaction e.g. PostingID.

The "Authentication Approval" is valid in the netbank for 1 minute – and the "PSIP Authorization Request" must be sent to the PBS SSL PGW as quickly as possible in order for the merchant to be able to complete the transaction within this timeframe.



PSIP Authorisation Transaction

PBS processes the "PSIP Authorization Request" and sends a "PSIP Authorization Response" message in return, which approves or declines the request including authentication data.



Order confirmation Transaction



Delivery of goods



PSIP Capture

The processing of these steps follows the normal PSIP flow.

4.4.4.2 **Mandatory content of merchant "checkout" page - eDankort**

The following must be contained in the web-page where the cardholder chooses to pay using eDankort.

4.4.4.2.1 **Image**

The following must be implemented by the merchant in a web document containing 'eDankort'.

```
<A HREF="javascript: void 0" onClick="eDankortRouter (document.
AuthenticationInitialization);" >
<IMG src="images/eDankort_20x45.gif" width="45" height="20" border="0"> </A>
```

4.4.4.2.2 **Form "Authentication Initialization"**

The merchant must fill in the form Authentication Initialization³

4.4.4.2.3 **"Authentication script"**

The following script must have a reference to the icon/logo and should be included in the HTML-header: <SCRIPT Language="JavaScript">

```
<!-- hide script for old browsers
function eDankortRouter(form) {

    var oHeight = 0;
    var oWidth = 0;
    var iHeight = 300;
    var iWidth = 350;
    var iLeft = 0
    var iTop = 0;

    oHeight = top.window.screen.availHeight;
    oWidth = top.window.screen.availWidth;

    if(oHeight > 3*iHeight)
        iHeight = oHeight/3;
    if(oWidth > 3*iWidth)
        iWidth = oWidth/3;

    if(oWidth > iWidth)
        iLeft = (oWidth - iWidth)/2;
    if(oHeight > iHeight)
        iTop = (oHeight - iHeight)/2;

    window.open("", 'router', 'scrollbars=yes, toolbar=no,
        directories=no, menubar=no, resizable=no, status=yes,
        width=' + iWidth + ', height=' + iHeight + ', left='
        + iLeft + ', top=' + iTop + 'dependent=yes');
    form.target = 'router';
    form.submit();
};
// -- end hiding --> </SCRIPT>
```

³ Please refer to chapter 6.5 for a description of the form.

4.4.4.3 Implementing 3-D Secure

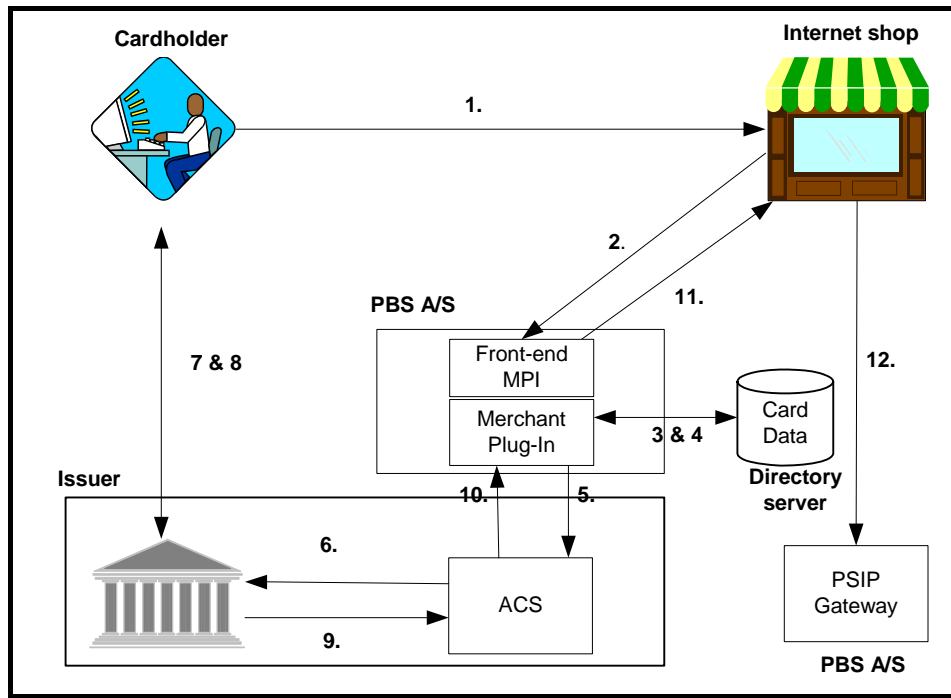


Figure 7: 3-D Secure payment flow

1. The cardholder shops at an internet merchant.
2. The payment application check-out to the 3-D Secure Merchant Plug In, using Authentication Initialization form.
3. The Merchant Plug In checks if the card is enrolled in 3-D Secure, at the directory server.
4. The directory server responds with enrolled/not enrolled.
5. The Merchant Plug In sends a Payer Authentication Request to the issuer Access Control Server.
6. The ACS asks the issuer system for authentication.
7. The issuer displays payment details and asks for the cardholder's secret code.
8. The cardholder verifies by keying his secret code.
9. The issuer responds with cardholder authenticated/not authenticated.
10. The ACS controls data and forwards the answer to the MPI .
11. The MPI controls data and forwards the answer to the merchant, using Authentication Approval form.
12. The merchant initiates a normal PSIP payment flow via the PSIP Gateway.

All links are TCP/IP connections. Point 2 and 5-11 are redirections via the cardholder browser, whilst 1, 3, 4 and 12 are direct navigations.

4.4.4.3.1 Example of of merchant "checkout" page content – 3-D Secure

The HTML source below refers to figure 5, and is an example which covers current requirements.

The authentication page following 'Payment data key-in page' must be an Inline page using the full screen.

While the inline authentication page is loading, the merchant should also display a short message such as the following:

"Processing, please wait.

Do not click the refresh or back button or this transaction may be interrupted or terminated."

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html>
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1" />
  <meta http-equiv="Content-Style-Type" content="text/css" />
  <title>Processing authentication request</title>
</head>
<body
onload="javascript:document.getElementById('AuthenticationInitialization').submit();">
<form id="AuthenticationInitialization" action="https://www.authentication-
router.pbs.dk/RouterWebApp/" method="post" onclick="target='_top';">
<p>
<input name="MerchantContinueURL" type="hidden"
value="https://IPSP.dk/3dsecurecallback" />
<input name="MerchantDeclineURL" type="hidden" value="https://IPSP.dk/reject" />
<input name="MerchantTitle" type="hidden" value="Shop name" />
<input name="OrderNo" type="hidden" value="Ordernumber 123" />
<input name="MerchantAccount" type="hidden" value="1234567" />
<input name="AmountTrn" type="hidden" value="000000000100" />
<input name="CurrencyTrn" type="hidden" value="DKK" />
<input name="TestFlg" type="hidden" value="P" />
<input name="DeviceCategory" type="hidden" value="0" />
<input name="MerchantCountry" type="hidden" value="208" />
<input name="MerchantUrl" type="hidden" value="http://www.theshop.dk" />
<input name="PAN" type="hidden" value="1234123412341234" />
<input name="PurchaseDateGMT" type="hidden" value="060131 10:23:09" />
<input name="ExpirationDate" type="hidden" value="0704" />
<input name="MerchantAcquirerBIN" type="hidden" value="957100" />
<input name="PurchaseExponent" type="hidden" value="2" />
<input name="PurchaseDescription" type="hidden" value="Order no.: 310106test1." />
<input name="CardLogo" type="hidden" value="2" />
</p>
</form>
<p>Processing, please wait.</p>
<p>Do not click the refresh or back button or this transaction may be interrupted or
terminated.</p>
<p>Should nothing happen;
press<a href="javascript:document.getElementById('AuthenticationInitialization').submit(
);">HERE</a></p>
</body>
</html>
```

4.4.5 Recurring transactions (subscription)

When a cardholder subscribes to a service or delivery of goods, the following procedure applies⁴⁵.

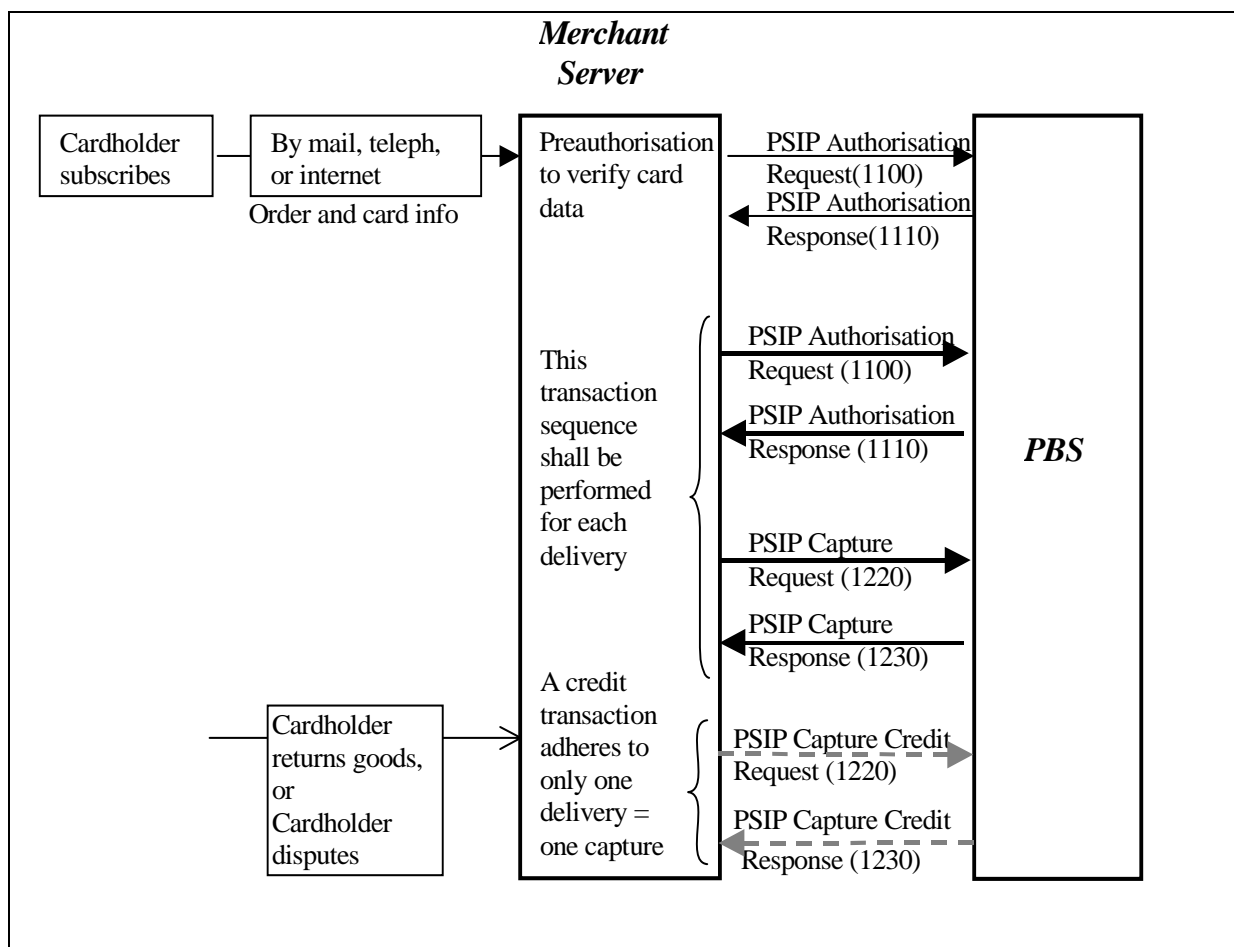


Figure 8: Recurring message flow

4.4.5.1 Recurring message flow

After having received a subscription order, the merchant initiates a preauthorization (Field 24 = 160) transaction to ensure validity of card data.

The amount of the transaction must be zero (e.g. field 4 = '0').

No capture should be sent for this preauthorization transaction.

This first transaction must contain "point of service data code" - field 22 - that corresponds to the appropriate Point Of Service environment (e.g. cardholder mails in card data: set field 22 to mail-order: '100020100110', or keys in data on a web-page: e.g. 'K00500K00130' for SSL or '880500887130' for a 3-D Secure transaction where the cardholder is successfully authenticated.)

For each delivery of goods or services, an authorization and a capture transaction must be initiated. The "point of service data code" - field 22 - for these transactions must always be 'K00540K00130'.

⁴ Instalment payment is not covered by the description in this chapter.

⁵ Not all payment methods allow recurring transactions, and special conditions may occur. Please refer to merchant agreement for conditions.

4.4.6 Return/Credit

As mentioned in the introduction (chapter 4), credit transactions from merchants to cardholders are available in PSIP.

A credit transaction (also known as a capture credit) may be used when a cardholder cancels his order or returns the merchandise to the merchant, and wants to have his account credited. The amount may be the full original capture amount, or part of the amount.

4.4.7 Clearing methods

Clearing of transactions can take place in two ways:

1. Single capture using PSIP – as described in this manual
2. Batch⁶ capture where PBS offers different formats – as described in dedicated manuals – see below:

- ISO 8583 format

This format supports

- * Clearing of card products of the PBS acquirer product range.
- * Clearing in agreed currencies

Format and conditions are described in the PBS document:

"Technical Reference Guide - ISO8583 Batch Communication for Merchant".

⁶ Definition of batches:

A batch is a file containing individual financial transactions (captures) for a period defined by the merchant. Batches may be transmitted to PBS 24 hours a day, but are only processed by PBS once a day. The merchant will receive a transfer receipt, including the number of errors in the batch, if any.

4.5 Error situations, roles and responsibilities

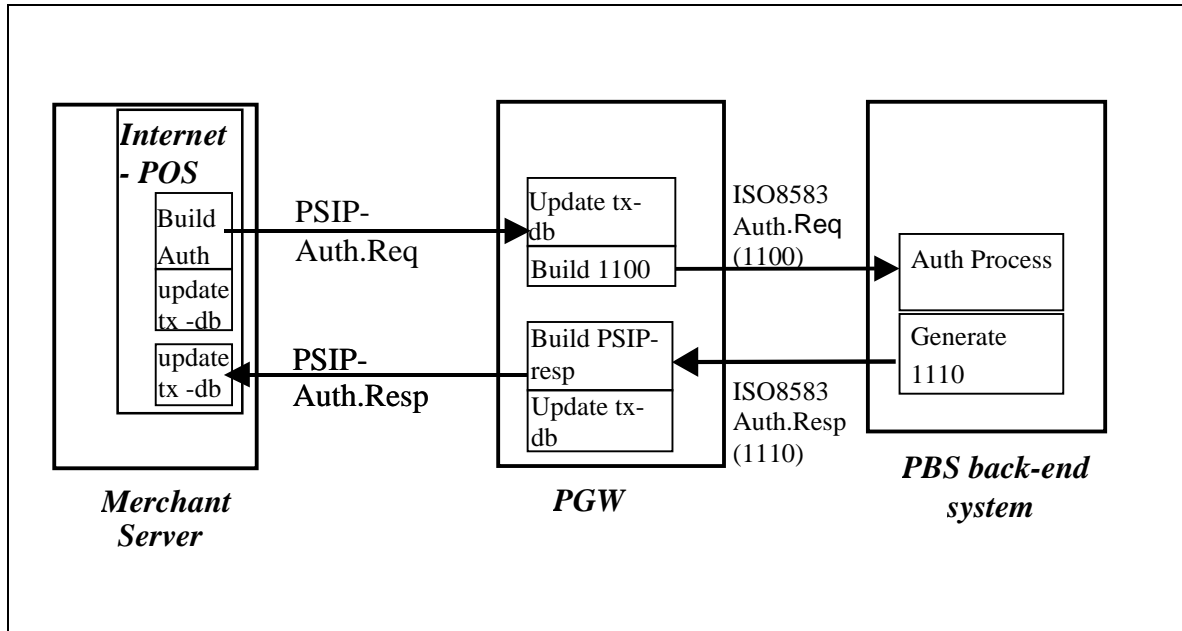


Figure 9: Which components do what.

This chapter lists different error situations, and the roles and responsibilities of the involved parties:

- **"Internet POS"** in the merchant server is responsible for:
 1. building the PSIP-message. The message contains data entered by the cardholder, configuration data as well as data, which must be generated by the Internet-POS device including the merchant reference/order number (is the key for merchant when receiving the response).
 2. The Internet-POS must validate the PSIP Authorization Response - and react to the action code (see Appendix A Action Code), which specifies the possible responses to the Authorization Request.
 3. The Internet-POS is also responsible for storing the necessary information from the Authorization Request/Response to build the Capture Request including the AUTH-ODE (field 56).
 4. An Authorization-/Capture Response is normally sent to the Internet POS in less than 30 seconds (and less for domestic cards). If the Internet POS does not receive an Authorization Response/Capture Response⁷, it is recommended that the merchant continue **repeating** the Authorization/Capture Request message a reasonable number of times (e.g. 5 times).

⁷ The recommended timeout value for the merchant server is 60 seconds.

5. When the merchant server identifies a case when a message must be **repeated**, the message must be an exact copy of the original message (**e.g. time stamp in field 12 is not updated.**) If the Internet POS receives an Authorization-/Capture Response, and the "action code" (field 39) indicates "system error" or "no reply" (see Appendix A), the transaction must be **re-submitted** by generating a completely new message (**i.e. a new time stamp in field 12 and a new order number in field 31 must be generated**).
 6. If a response is not received from PBS after the merchant server has repeated the message the desired number of times, the PBS-system (or a component between the merchant server and the PBS system) should be considered as being out of operation.
 7. If the Internet POS receives more responses to the same transaction, the system must be able to discard all responses, but the first.
- **PBS SSL Payment Gateway (PGW)** will:
 1. Receive the data and build an entry in the transaction database (tx-db) containing key data elements.
 2. The PGW will add additional fields to the message and forward the message to PBS' back-end card system.
 3. When the PGW receives an Authorization Response from the back-end system, it builds the AUTH-ODE (field 56). Then the PSIP Authorization Response is generated.
 4. The gateway will store the data from the response message which is necessary to make a duplicate check. This check ensures that an earlier received message, will not be sent to the legacy system for processing. Instead it will send the previous answer.
 5. In case an action code 946 is received in a response message, it indicates to the merchant that a system error occurred (e.g. format error in the input message),
In such response messages **only mandatory fields** will be present, as conditions cannot be stated at that stage.
 - The primary functions of the **PBS back-end system** are to:
 1. Switch the messages (Authorization/Capture) through to the card acquirer or issuer processing system, whether that is at PBS, another Danish card acquirer or issuer (such as the Danish banks), or a card acquirer or issuer located outside Denmark.
 2. Receive the response messages from the acquirer or issuer and send these to the PGW

5 Protocol specifications

This chapter gives the details of the PSIP-protocol.

5.1 Network Layer.

The network layer is the Internet. This protocol is intended for use on the public Internet. The IPSP must ensure sufficient bandwidth, which allows the running of the PSIP-protocol in real-time with acceptable response times.

The network layer implementation could be based on a standard TCP/IP-stack found in most operating systems - and enhanced with support for Secure Socket Layer.

5.2 SSL Layer

The IPSP must implement a SSL-client using one of the following SSL Cipher-suites:

SSL_RSA_WITH_RC4_128_MD5

SSL_RSA_WITH_RC4_128_SHA

SSL_RSA_WITH_3DES_EDE_CBC_SHA

5.3 Message format and types.

5.3.1 Introduction

As mentioned earlier (see chapter 5), the PSIP-protocol consists of 2 sets of messages:

- PSIP Authorization Request/Response
- PSIP Capture Request/Response

The message format is based on ISO8583-93 and is prefixed with a header defining length, protocol and version.

5.3.4 PSIP header

PSIP header is used to describe the PSIP version, in responses it carries a PBS Payment Gateway response code (PGW response code).

Field	Format	Value
PSIP version	an 7	'PSIP100' - fixed value
PGW response code	an 3	In request: '000' In response - refer to appendix B

The PGW response code defines the status of PBS Payment Gateway (see Appendix B). If the PGW response code indicates that the transaction is "OK", the application should proceed to unpack the PSIP message and verify the actual business response. If the PGW response code indicates "not-OK" no PSIP message is returned

5.3.5 PSIP messages

As mentioned earlier, PSIP is based on ISO8583. The PSIP message is formatted according to ISO 8583. Each ISO 8583 response message includes an action code, specifying the status of the business transaction. This action code reflects the response generated by the card acquirers/issuers, (e.g. "merchant no agreement" / "card blocked").

5.3.6 ISO 8583 v.1

PBS' implementation follows ISO8583 v.1.

The ISO 8583 v.1. standard is using:

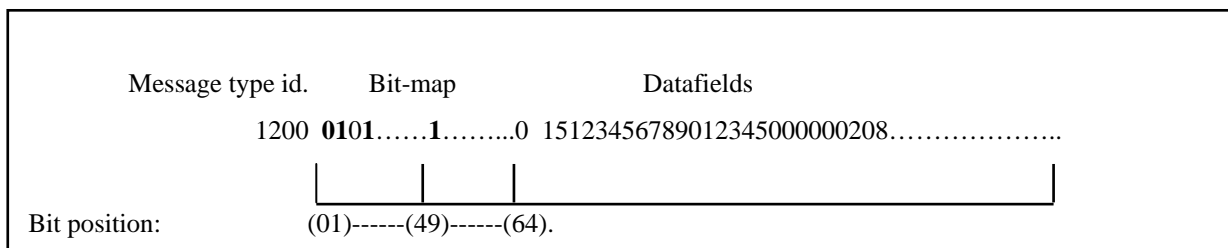
- * Messages of variable length (controlled by bit-map structure - fields may or may not be present)
- * Fields, that may be of variable length, controlled by length fields in front of the field
- * Numeric data, that can be presented as binary data

5.3.6.1 The Basic Features of ISO 8583 v.1.

An ISO 8583 message can contain up to 128 predefined fields. To indicate the presence of a given field, a bit-structure, called a BIT-MAP is included in the ISO 8583 message. Each bit-position in the BIT-MAP can be turned on (1)/off (0), and thereby indicate if a field is present or not.

The BIT-MAP occupies 16 bytes (16 x 8 = 128) if fields above field 64 are present, otherwise the BIT-MAP only occupies 8 bytes. The first bit in the BIT-MAP indicates if an extended BIT-MAP is in use.

The sender and the receiver can compress and expand the message by using the BIT-MAP and the knowledge of each field length definition (fixed or variable)



The above Figure shows how to build a message.

The merchant must be able to handle BIT-MAPS (variable record and variable field length format). Examples of BIT-MAPS for different applications are given in the message descriptions.

New fields in response messages may be added without further notice. Therefore PSIP messages should not be handled as fixed format messages.

5.3.6.2 ISO 8583 - record reading instructions

The record definitions documented in the following chapters are based on the ISO 8583 v.1. definitions.

If a field is present in a message definition, but no definition, format or field value can be found, **the definitions must be looked up in the ISO 8583 v.1.** Standard. For such a field, the complete range of ISO 8583 field values may occur.

PBS may have assigned new values for a field. In that case the values are defined in the ISO 8583 v.1. interval reserved for national use.

For a field where PBS has assigned new values, all the general values defined by ISO 8583 v.1, are still valid, and these are only documented in the ISO 8583 v.1. Standard.

The field format is defined using the **ISO 8583 v.1. Notation** :

a	=	alpha
n	=	numeric
an	=	alphanumeric
ans	=	alphanumeric with special characters
anp	=	alphanumeric and packed data
b	=	binary data

All **printable** alphanumeric characters are supported using the ASCII-character set. Only the Danish Standard version (**codepage 850**) is supported.

Certain fields are defined as **variable length fields**

e.g.: ans..99 LLVAR.

Such a definition means that the field may occupy up to 99 bytes, and there will always be a length field in front, specifying the actual length.

The number of the character "L" specifies how many bytes are used for the length field. The maximal length of the field in the example, including the length field, are then 101 bytes.

The length fields are defined as numeric data, right justified, and must be > '0' (a null value TAG field must not be present..

An expanded ISO 8583 v.1. record will not occupy more than 4K bytes in the PBS interpretation.

Message examples/dumps can be seen in Appendix C

5.3.6.3 Currency codes

Currency codes are defined according to ISO 4217. PBS is always using the alpha 3 byte representation (e.g.: Danish kroner = DKK). The valid codes can be obtained from the national standardisation committees, e.g. "www.ds.dk".

5.3.6.4 Country codes

Country codes are defined according to ISO 3166. PBS is using the numeric 3 byte representation (e.g.: Denmark: 208) except for the country code in field 43, where the alphanumeric 3 byte representation is used (e.g.: Denmark = DNK). The valid codes can be obtained from the national standardisation committees, e.g. "www.ds.dk".

5.3.7 PSIP Authorization Request

ISO 8583 field no.	PSIP field name	PSIP field format	PSIP field definitions and formatting remarks																																																																
N/A	PSIP-HEADER	an 10	'PSIP100000' - fixed value																																																																
	MESSAGE TYPE ID	n 4	<u>Mandatory.</u> '1100' - Authorization Request.																																																																
	BIT MAP	b 8	<p>Mandatory.</p> <p><u>Following are examples, contents may differ due to conditional or optional fields.</u></p> <p>Value in HEX representation (most significant bit first):</p> <p><u>E-commerce using SSL payment or 3-D Secure:</u> '701405C200E28000'</p> <table><tr><td>7</td><td>0</td><td>1</td><td>4</td><td>0</td><td>5</td><td>C</td><td>2</td><td>0</td><td>0</td><td>E</td><td>2</td><td>8</td><td>0</td><td>0</td><td>0</td></tr><tr><td>0111</td><td>0000</td><td>0001</td><td>0100</td><td>0000</td><td>0101</td><td>1100</td><td>0010</td><td>0000</td><td>0000</td><td>1110</td><td>0010</td><td>1000</td><td>0000</td><td>0000</td><td>0000</td></tr></table> <p><u>E-commerce when eDankort:</u> '701405C200E28080'</p> <table><tr><td>7</td><td>0</td><td>1</td><td>4</td><td>0</td><td>5</td><td>C</td><td>2</td><td>0</td><td>0</td><td>E</td><td>2</td><td>8</td><td>0</td><td>8</td><td>0</td></tr><tr><td>0111</td><td>0000</td><td>0001</td><td>0100</td><td>0000</td><td>0101</td><td>1100</td><td>0010</td><td>0000</td><td>0000</td><td>1110</td><td>0010</td><td>1000</td><td>0000</td><td>1000</td><td>0000</td></tr></table>	7	0	1	4	0	5	C	2	0	0	E	2	8	0	0	0	0111	0000	0001	0100	0000	0101	1100	0010	0000	0000	1110	0010	1000	0000	0000	0000	7	0	1	4	0	5	C	2	0	0	E	2	8	0	8	0	0111	0000	0001	0100	0000	0101	1100	0010	0000	0000	1110	0010	1000	0000	1000	0000
7	0	1	4	0	5	C	2	0	0	E	2	8	0	0	0																																																				
0111	0000	0001	0100	0000	0101	1100	0010	0000	0000	1110	0010	1000	0000	0000	0000																																																				
7	0	1	4	0	5	C	2	0	0	E	2	8	0	8	0																																																				
0111	0000	0001	0100	0000	0101	1100	0010	0000	0000	1110	0010	1000	0000	1000	0000																																																				
2	PRIMARY ACCOUNT NUMBER	n ..19 LLVAR	<u>Mandatory.</u> The card number received from the cardholder																																																																
3	PROCESSING CODE	n 6	<u>Mandatory.</u> '000000' - goods and services '110000' - quasi-cash (e.g. gambling)																																																																
4	AMOUNT, TRANSACTION	n 12	<u>Mandatory.</u> Amount approved by the cardholder, and expressed in minor unit of currency – refer to ISO4217 - (e.g. 50 Danish Kroner '5000').																																																																
12	DATE & TIME, LOCAL TRANSACTION	n 12	<u>Mandatory.</u> The current local time at the merchant location. ¹⁰ <u>Format:</u> Yymmddhhmmss																																																																

¹⁰ The local time at the place where the transaction is originated - e.g. on internet it is the current time of the merchant server.

14	DATE, EXPIRATION	n 4	<p><u>Mandatory</u></p> <p>Card expiry date:</p> <p><u>Format:</u> YYMM</p> <p>Please observe special formatting rules regarding the cardholder interface, documented in chapter 8.2.</p> <p>Please observe that in eDankort transactions this field may be zero filled.</p>
22	POINT OF SERVICE DATA CODE	an 12	<p><u>Mandatory.</u></p> <p>Transaction environment:</p> <p>The following applies to Internet Merchants who signed up for 3-D Secure:</p> <p><u>The code must be echoed from 'Authentication Approval' or 'Authentication Decline' field' POSData code'.</u></p> <p>The following applies to Internet Merchants who <i>did not</i> sign up for 3-D Secure(= SSL):</p> <p><u>Internet transactions/electronic commerce - channel encrypted, no authentication e.g. SSL:</u></p> <p>'K00500K00130'</p> <p>Recurring transaction, (the 2nd of n. transactions - the transmission method used for the first transaction depends on how the merchant has obtained the order (see 4.4.5)</p> <p>'K00540K00130'</p> <p><u>Internet transactions/eDankort – Customer authenticated by netbank applications – channel encrypted e.g. SSL:</u></p> <p>'KM0500R00130'</p>
24	FUNCTION CODE	n 3	<p><u>Mandatory.</u></p> <p>'100' original authorization - amount accurate</p> <p>'101' original authorization - amount estimated¹¹</p>

¹¹ This code may be used when the total amount is unknown, e.g. the shipping costs may be estimated.

25	MESSAGE REASON CODE	n 4	<u>Mandatory.</u> Reason for sending this message: '0000' normal transaction '1511' merchant suspicious of fraud
26	CARD ACCEPTOR BUSINESS CODE	n 4	<u>Mandatory.</u> Code identifying the merchant business.
31	ACQUIRER REFERENCE DATA	ans ..20 LLVAR	<u>Mandatory.</u> Order number, generated by merchant, and communicated to cardholder on the receipt. ¹² For cardholders: This number enables the cardholder to identify the payment transaction. The number is carried through to the cardholder on receipts and account statements, (by most card issuers). For merchants This number may be used on the settlement advices from the appropriate acquirer (e.g. PBS or Diners), and may be used by the merchant to reconcile his revenue.
41	CARD ACCEPTOR TERMINAL ID	ans 8	<u>Mandatory.</u> Terminal number (assigned by merchant). Left justified, space filled.
42	CARD ACCEPTOR IDENTIFICATION CODE	ans 15	<u>Mandatory.</u> Merchant number (assigned by the terminal operator). Left justified, space filled.

¹² Processing systems have reduced format and length for this data element. To ensure reference between systems, only the last 5 characters should be used; and only if numeric!

43	CARD ACCEPTOR NAME/LOCATION	an 99 LLVAR	<p><u>Mandatory.</u></p> <p>Merchant name/address as registered by terminal operator.</p> <p><u>Format:</u></p> <p>an 83 <u>Merchant name \ address (street) \ city \</u> - separated by back slash. <i>(mandatory)</i> This field is of variable length.</p> <p>an 10 Card acceptor zipcode (fixed length, left justified, space filled) <i>(mandatory)</i></p> <p>an 3 Card acceptor region (fixed length, left justified, space filled) <i>(optional)</i></p> <p>a 3 Card acceptor country (fixed length, left justified, space filled) <i>(mandatory) (see 5.3.6.4).</i></p>
----	--------------------------------	----------------	---

47	ADDITIONAL DATA NATIONAL	ans..254 LLLVAR	<p>See " 5.3.13 Definition TAG/LENGTH/VALUE data element: "</p> <p>A TAG-GROUP may appear x times in field 47 limited by the total length of field 47.</p> <p>Chapter "5.3.14 Tag definition" contains a list of pre-defined TAG-GROUPs.</p> <p>In this record, the following TAG-ID's are valid¹³:</p> <ul style="list-style-type: none"> • CA: (used in 3-D Secure). The value returned in "Authentication Approval" message field PurchaseXID must be echoed if present. • CB: (used in 3-D Secure). The value returned in "Authentication Approval" message field TXcavv must be echoed if present. • CC: (used in 3-D Secure). The value returned in "Authentication Approval" message field TXcavvAlgoritm must be echoed if present . • CE: (Mandatory when 3-D Secure). The value returned in "Authentication Approval" message field TransactionStatus must be echoed. • P5: (Mandatory for eDankort). The value returned in "Authentication Approval" message must be echoed. • PR: (Conditional when using eDankort). If the tags are present in the "Authentication Approval" message, the tags must be echoed. • S1+S2: (Conditional when eDankort). If the tags are present in the "Authentication Approval" message, the tags must be echoed. • V5: (Mandatory for Dankort & Visa/Dankort) <p>If the field is not supplied by the cardholder do not send the TAG with a 'null value'.</p>
49	CURRENCY CODE TRANSACTION	a 3	<p><u>Mandatory.</u></p> <p>Currency code, defined according to ISO4217 (see 6.3.6.3).</p>

¹³ Note: subfields identified via TAG's do not have a fixed position in the record. When the field is read, you have to "scan" for the desired field; and when writing you always need to "scan" for a free position.

57	Authorization Life Cycle	n 3	<u>Conditional</u> Mandatory in eDankort transactions. The value returned in "Authentication Approval" message must be sent.
----	--------------------------	-----	--

5.3.8 PSIP Authorization Response

ISO 8583 field no.	PSIP field name	PSIP field format	PSIP field definitions and formatting remarks
N/A	PSIP-HEADER	an 10	'PSIP100000' - fixed value
	MESSAGE TYPE ID	n4	<u>Mandatory.</u> '1110' (Authorization Response)
	BIT MAP	b 8	<u>Mandatory.</u> Following are examples, contents may differ due to conditional or optional fields. Value in HEX representation (most significant bit first): <u>Ecommerce using SSL payment or 3-D Secure:</u> '7010000206D08100' <div> <div>7</div><div>0</div><div>1</div><div>0</div><div>0</div><div>0</div><div>0</div><div>0</div><div>2</div><div>0</div><div>6</div><div>D</div><div>0</div><div>8</div><div>1</div><div>0</div><div>0</div> </div> <div> <div>0111</div><div>0000</div><div>0001</div><div>0000</div><div>0000</div><div>0000</div><div>0000</div><div>0000</div><div>0001</div><div>0000</div><div>0111</div><div>1100</div><div>0000</div><div>1000</div><div>0000</div><div>0000</div><div>0000</div> </div> <u>Ecommerce when eDankort.:</u> '7010000206D28180' <div> <div>7</div><div>0</div><div>1</div><div>0</div><div>0</div><div>0</div><div>0</div><div>0</div><div>2</div><div>0</div><div>6</div><div>D</div><div>2</div><div>8</div><div>1</div><div>8</div><div>0</div> </div> <div> <div>0111</div><div>0000</div><div>0001</div><div>0000</div><div>0000</div><div>0000</div><div>0000</div><div>0000</div><div>0001</div><div>0000</div><div>0111</div><div>1100</div><div>0001</div><div>1000</div><div>0000</div><div>1000</div><div>0000</div> </div>
2	PRIMARY ACCOUNT NUMBER	n ..19 LLVAR	<u>Mandatory echo from Authorization Request</u>
3	PROCESSING CODE	n 6	<u>Mandatory echo from Authorization Request.</u>
4	AMOUNT TRANSACTION	n 12	<u>Mandatory.</u> The amount approved by the issuer. which can be less than AMOUNT, TRANSACTION from Authorization Request.
12	DATE & TIME, LOCAL TRANSACTION	n 12	<u>Mandatory echo from Authorization Request.</u>
31	ACQUIRER REFERENCE DATA	ans ..20 LLVAR	<u>Mandatory echo from Authorization Request.</u>
38	APPROVAL CODE	anp 6	<u>Mandatory.</u> Reference code to an approved authorization, generated by issuer if action code is less than 100. If action code is 100 or above, the field will contain 'spaces'.

39	ACTION CODE	n 3	<u>Mandatory.</u> Code indicating the status of the transaction, and the action that must be taken by the merchant. (See Appendix A").
41	CARD ACCEPTOR TERMINAL ID	ans 8	<u>Mandatory echo from Authorization Request.</u>
42	CARD ACCEPTOR IDENTIFICATION CODE	ans 15	<u>Mandatory echo from Authorization Request.</u>
44	ADDITIONAL RESPONSE DATA	ans 99 LLVAR	<u>Conditional</u> For future use. Field, where data elements are written/stored using a "TAG/LENGTH/VALUE" method. <ul style="list-style-type: none"> A TAG/LENGTH/VALUE data element is a constructed data structure, called a TAG-GROUP, and described in "5.3.13 Definition TAG/LENGTH/VALUE data element: "A TAG-GROUP may appear x times in field 44 limited by the total length of field 44. Chapter "5.3.14 Tag definition" contains a list of pre-defined TAG-GROUPs. In this record, the following TAG-ID's are valid¹⁴: A3 A4 A5
47	ADDITIONAL DATA NATIONAL	ans..254 LLLVAR	<u>Conditional</u> See 5.3.13 Definition TAG/LENGTH/VALUE data element: A TAG-GROUP may appear x times in field 47 limited by the total length of field 47. Chapter "5.3.14 Tag definition" contains a list of pre-defined TAG-GROUPs. In this record, the following TAG-ID's are valid ¹⁵ : <ul style="list-style-type: none"> P5: conditional_echo_from Authorization Request; the field must be returned unaltered
49	CURRENCY CODE TRANSACTION	a 3	<u>Mandatory echo from Authorization Request.</u>

¹⁴ Note: subfields identified via TAG's do not have a fixed position in the record. When the field is read, you have to "scan" for the desired field; and when writing you always need to "scan" for a free position.

¹⁵ Note: subfields identified via TAG's do not have a fixed position in the record. When the field is read, you have to "scan" for the desired field; and when writing you always need to "scan" for a free position.

56	AUTH – ORIGINAL DATA ELEMENT (ODE)	b 255 LLLVAR	<u>Mandatory:</u> Data must be presented in the next request message of this business transaction.
57	Authorization Life Cycle	n 3	Mandatory echo from Authorization Request when eDankort

5.3.9 PSIP Reversal Advice

ISO 8583 field no.	PSIP field name	PSIP field format	PSIP field definitions and formatting remarks
N/A	PSIP-HEADER	an 10	'PSIP100000' - fixed value
	MESSAGE TYPE ID	n 4	<u>Mandatory.</u> '1420'
	BIT MAP	b 8	<u>Mandatory.</u> Following are examples, contents may differ due to conditional or optional fields: Value in HEX representation (most significant bit first): 7 0 1 0 0 1 C 2 0 4 E 2 8 1 0 0 011 000 000 000 000 000 110 001 000 010 111 001 100 000 000 000 1 0 1 0 0 1 0 0 0 0 0 0 1 0 0
2	PRIMARY ACCOUNT NUMBER	n..19 LLVAR	<u>Mandatory echo from '1110'</u>
3	PROCESSING CODE	n 6	<u>Mandatory echo from '1100'</u>
4	AMOUNT TRANSACTION	n 12	<u>Mandatory echo from '1100'</u>
12	DATE AND TIME, LOCAL TRANSACTION	n 12	<u>Mandatory:</u> Format: yymmddhhmmss Local time at the merchant location
24	FUNCTION CODE	n 3	<u>Mandatory:</u> Purpose of transaction: '400' Full Reversal, transaction was not completed as approved
25	MESSAGE REASON CODE	n 4	<u>Mandatory:</u> Information for receiver (acquirer) – the reason for sending a message. <u>Value:</u> '4000' customer cancellation '4001' unspecified, no action taken '4002' suspected malfunction
26	CARD ACCEPTOR BUSINESS CODE	n 4	<u>Mandatory echo from '1100'</u>
31	ACQUIRER REFERENCE DATA	ans 23 LLVAR	<u>Mandatory echo from '1100'</u>

38	APPROVAL CODE	anp 6	<u>Mandatory:</u> Echo from '1110'
41	CARD ACCEPTOR TERMINAL ID	ans 8	<u>Conditional echo from '1100'</u>
42	CARD ACCEPTOR IDENTIFICATION CODE	ans 15	<u>Mandatory echo from '1100'</u>
43	CARD ACCEPTOR NAME/LOCATION	n 99 LLVAR	<u>Mandatory echo from '1100'</u>
47	ADDITIONAL DATA NATIONAL	ans..254 LLLVAR	<u>Conditional</u> " A TAG-GROUP may appear x times in field 47 limited by the total length of field 47. Chapter "5.3.14 Tag definition" contains a list of pre-defined TAG-GROUPs. In this record, the following TAG-ID's are valid ¹⁶ : <ul style="list-style-type: none"> P5: . Conditional echo from Authorization Request; the field must be returned unaltered
49	CURRENCY CODE, TRANSACTION	a 3	<u>Mandatory echo from '1100' .</u>
56	AUTH – ORIGINAL DATA ELEMENT (ODE)	b 255 LLLVAR	<u>Mandatory echo from '1110'.</u>
57	Authorization Life Cycle	n 3	Conditional echo from '1110'.

¹⁶ Note: subfields identified via TAG's do not have a fixed position in the record. When the field is read, you have to "scan" for the desired field; and when writing you always need to "scan" for a free position.

5.3.10 PSIP Reversal Advice Response

ISO 8583 field no.	PSIP field name	PSIP field format	PSIP field definitions and formatting remarks																																
N/A	PSIP-HEADER	an 10	'PSIP100000' - fixed value																																
	MESSAGE TYPE ID	n 4	<u>Mandatory.</u> '1430' – Capture Response																																
	BIT MAP	b 8	<u>Mandatory.</u> Present value(might differ in some messages see chapter 5) in HEX representation (most significant bit first): <table><tr><td>7</td><td>0</td><td>1</td><td>0</td><td>0</td><td>1</td><td>C</td><td>2</td><td>0</td><td>2</td><td>C</td><td>2</td><td>8</td><td>1</td><td>0</td><td>0</td></tr><tr><td>0111</td><td>0000</td><td>0001</td><td>0000</td><td>0000</td><td>0001</td><td>1100</td><td>0010</td><td>0000</td><td>0010</td><td>1100</td><td>0010</td><td>1000</td><td>0001</td><td>0000</td><td>0000</td></tr></table>	7	0	1	0	0	1	C	2	0	2	C	2	8	1	0	0	0111	0000	0001	0000	0000	0001	1100	0010	0000	0010	1100	0010	1000	0001	0000	0000
7	0	1	0	0	1	C	2	0	2	C	2	8	1	0	0																				
0111	0000	0001	0000	0000	0001	1100	0010	0000	0010	1100	0010	1000	0001	0000	0000																				
2	PRIMARY ACCOUNT NUMBER	n..19	<u>Mandatory echo from '1420'</u>																																
3	PROCESSING CODE	n 6	<u>Mandatory echo from '1420'</u>																																
4	AMOUNT TRANSACTION	n 12	<u>Mandatory echo from '1420'</u>																																
12	DATE AND TIME, LOCAL TRANSACTION	n 12	<u>Mandatory echo from '1420'</u> .																																
31	ACQUIRER REFERENCE DATA	ans 23 LLVAR	<u>Mandatory echo from '1420'</u>																																
39	ACTION CODE	n 3	<u>Mandatory</u>																																
41	CARD ACCEPTOR TERMINAL ID	ans 8	<u>Mandatory echo from '1420'</u>																																
42	CARD ACCEPTOR IDENTIFICATION CODE	ans..15	<u>Mandatory echo from '1420'</u>																																
49	CURRENCY CODE, TRANSACTION	a3	<u>Mandatory echo from '1420'</u>																																
56	AUTH – ORIGINAL DATA ELEMENT (ODE)	b 255 LLLVAR	<u>Mandatory:</u> Data returned from the PBS SSL Gateway and must be presented in the next request message.																																
57	AUTHORIZATION LIFE CYCLE	n 3	Conditional echo from '1420'.																																

5.3.11 PSIP Capture Request

ISO 8583 field no.	PSIP field name	PSIP field format	PSIP field definitions and formatting remarks
N/A	PSIP-HEADER	an 10	'PSIP100000' - fixed value
	MESSAGE TYPE ID	n 4	<u>Mandatory.</u> '1220' – Capture Request
	BIT MAP	b 8	<u>Mandatory.</u> Following are examples, contents may differ due to conditional or optional fields: Value in HEX representation (most significant bit first): <u>E-commerce using SSL payment or 3-D Secure:</u> : '7014054206E28100' <div> <div>7</div><div>0</div><div>1</div><div>4</div><div>0</div><div>5</div><div>4</div><div>2</div><div>0</div><div>6</div><div>E</div><div>2</div><div>8</div><div>1</div><div>0</div><div>0</div> </div> <div> <div>011</div><div>000</div><div>000</div><div>010</div><div>000</div><div>010</div><div>010</div><div>001</div><div>000</div><div>011</div><div>111</div><div>001</div><div>100</div><div>000</div><div>000</div><div>000</div> </div> <div>1</div> <div>0</div> <div>1</div> <div>0</div> <div>0</div> <div>1</div> <div>0</div> <div>0</div> <div>0</div> <div>0</div> <div>0</div> <div>0</div> <div>0</div> <div>1</div> <div>0</div> <div>0</div>

7

0

1

4

0

5

4

2

0

6

E

2

8

1

8

0

011

000

000

010

000

010

010

001

000

011

111

001

100

000

100

000

1

0

1

0

0

1

0

0

0

0

0

0

0

1

0

0

4	AMOUNT TRANSACTION	n 12	<p><u>Mandatory.</u></p> <p>Amount to be debited to the cardholder account, in the smallest unit of the transaction currency.</p> <p>When <u>debit</u> (PROCESSING CODE = '000000' or '110000'):</p> <p>If 'FUNCTION CODE = '201' (Amount accurate)</p> <ul style="list-style-type: none"> <u>Amount must be echoed from Authorization Response.</u> <p>If 'FUNCTION CODE = '202' (Amount differs)</p> <p>When <u>credit</u> (PROCESSING CODE = '200000'):</p> <p>The <u>amount must not exceed the amount in the original capture.</u></p>
12	DATE & TIME, LOCAL TRANSACTION	n 12	<p><u>Mandatory.</u></p> <p>The current local time at the merchant location.^{17 18}</p> <p>Format: Yymmddhhmmss</p>
14	DATE, EXPIRATION	n 4	<u>Mandatory echo from Authorization Request.</u>
22	POINT OF SERVICE DATA CODE	n 12	<p><u>Mandatory echo from Authorization Request, except for eDankort – where this value must be used:</u></p> <p>_____KM0500RNL130</p>
24	FUNCTION CODE	n 3	<p><u>Mandatory.</u></p> <p>When <u>debit</u> (PROCESSING CODE = '000000' or '110000'):</p> <p>'201' Previously approved authorization, amount same.</p> <p>'202' Previously approved authorization, amount differs.</p> <p>When <u>credit</u> (PROCESSING CODE = '200000'):</p> <p>'200' Original transaction.</p>

¹⁷ The local time at the place where the transaction is executed - e.g. on internet it is the current time of the merchant server.

¹⁸ Please observe, that a credit transaction (PROCESSING CODE = '200000') must not have the same timestamp as the related debit transaction (PROCESSING CODE = '000000').
A credit transaction is a new business transaction and must be stamped with the current local time at the merchant location.

26	CARD ACCEPTOR BUSINESS CODE	n 4	<u>Mandatory.</u> Code identifying the merchant's business as specified in the merchant agreement.
31	ACQUIRER REFERENCE DATA	ans ..20 LLVAR	<u>Mandatory echo from Authorization Request.</u>
38	APPROVAL CODE	anp 6	<u>Mandatory echo from Authorization Response.</u>
39	ACTION CODE	n 3	<u>Mandatory echo from Authorization Response</u>
41	CARD ACCEPTOR TERMINAL ID	ans 8	<u>Mandatory echo from Authorization Request.</u>
42	CARD ACCEPTOR IDENTIFICATION CODE	ans 15	<u>Mandatory echo from Authorization Request.</u>
43	CARD ACCEPTOR NAME/LOCATION	an .. 99 LLVAR	<u>Mandatory echo from Authorization Request.</u>
47	ADDITIONAL DATA NATIONAL	ans..254 LLLVAR	See 5.3.13 Definition TAG/LENGTH/VALUE data element: A TAG-GROUP may appear x times in field 47 limited by the total length of field 47. Chapter "5.3.14 Tag definition" contains a list of pre-defined TAG-GROUPs. In this record, the following TAG-ID's are valid ¹⁹ : <ul style="list-style-type: none"> • P0; (Optional). • P1; (Optional) • P2; (Optional) • P3; (Optional) • P4; (Optional) • P5; <u>Conditional echo from '1110'; the field must be returned unaltered</u>
49	CURRENCY CODE TRANSACTION	a 3	<u>Mandatory.</u> Currency code, defined according to ISO4217 (see 6.3.6.3).
56	AUTH – ORIGINAL DATA ELEMENT (ODE)	b 255 LLLVAR	<u>Mandatory</u> <u>Field echoed from the previous response</u> message of this business transaction.

¹⁹ Note: subfields identified via TAG's do not have a fixed position in the record. When the field is read, you have to "scan" for the desired field; and when writing you always need to "scan" for a free position.

57	Authorization Life Cycle	n 3	Conditional echo from '1110'.
----	--------------------------	-----	-------------------------------

5.3.12 PSIP Capture Response

ISO 8583 field no.	PSIP field name	PSIP field format	PSIP field definitions and formatting remarks
N/A	PSIP-HEADER	an 10	'PSIP100000' - fixed value
	MESSAGE TYPE ID	n 4	<u>Mandatory.</u> '1230' – Capture Response
	BIT MAP	b 8	<u>Mandatory.</u> Present value(may differ in some messages see chapter 5) in HEX representation (most significant bit first): <u>E-commerce using SSL payment.</u> <u>3-D Secure:</u> '7010000206D08100'.
			7010000202C08100
			011000

42	CARD ACCEPTOR IDENTIFICATION CODE	ans 15	<u>Mandatory echo from Capture Request.</u>
44	ADDITIONALRESPONSE DATA	ans 99 LLVAR	<u>Conditional</u> <u>For future use.</u> <p>Field, where data –elements are written/stored using a “TAG/LENGTH/VALUE” method.</p> <p>A TAG/LENGTH/VALUE data –element is a constructed data- structure, called a TAG-GROUP, and described in “5.3.13 Definition TAG/LENGTH/VALUE data element:</p> <p>A TAG-GROUP may appear x times in field 44 limited by the total length of field 44.</p> <p>Chapter “5.3.14 Tag definition” contains a list of pre-defined TAG-GROUPs.</p> <p>In this record, the following TAG-ID’s are valid²⁰:</p> <p>A3</p> <p>A4</p> <p>A5</p>
47	ADDITIONAL DATA NATIONAL	ans..254 LLLVAR	<u>Conditional</u> ²¹ See 5.3.13 Definition TAG/LENGTH/VALUE data element: A TAG-GROUP may appear x times in field 47 limited by the total length of field 47. <p>Chapter “5.3.14 Tag definition” contains a list of pre-defined TAG-GROUPs.</p> <p>In this record, the following TAG-ID’s are valid²²:</p> <ul style="list-style-type: none"> P5: (<u>mandatory for eDankort</u>) <u>Mandatory echo from Capture Response; the field must be returned unaltered.</u>
49	CURRENCY CODE TRANSACTION	a 3	<u>Mandatory echo from Capture Request.</u>
56	AUTH – ORIGINAL DATA ELEMENT (ODE)	b 255 LLLVAR	<u>Mandatory:</u> <p>Data must be presented in the next request message of this business transaction.</p>

²⁰ Note: subfields identified via TAG's do not have a fixed position in the record. When the field is read, you have to “scan” for the desired field; and when writing you always need to “scan” for a free position.

²¹ Some errors occur before conditions can be proved. In such cases only mandatory fields will be present in the message.

²² Note: subfields identified via TAG's do not have a fixed position in the record. When the field is read, you have to “scan” for the desired field; and when writing you always need to “scan” for a free position.

5.3.13 Definition TAG/LENGTH/VALUE data element:

TAG-GROUP		Group containing data defined after a "TAG/LENGTH/ VALUE" principle.
- TAG-ID	an2	Tag identifier Tag-name, which explains what kind of data is contained in field: TAG-VALUE-VAR <ul style="list-style-type: none"> Valid tag identifiers, see "5.3.14 Tag definition".
- TAG-LL	n2	Length field of TAG-VALUE-VAR. Defined as a ISO8583 LL field. Must be > 0.
- TAG-VALUE-VAR	an..99	The content of the field is determined by a tag in the field TAG-ID The field is variable length 1..99.

5.3.14 Tag definition

FORMAT follow the rules in 5.3.6.2ISO 8583 - record reading instructions.

TAG-ID	TAG-NAME	DEFINITION AND FORMAT
A3	RECONCILIATION COUNTER ID	The number of the "reconciliation counter ID" where the amount transaction (field 4) has to be summed up. See example in chapter 5.3.15 . This field is provided for supporting IPSPs' or merchants' ability to automatically generate sums of the turnover on different card schemes. FORMAT: n 3
A4	RECONCILIATION COUNTER NAME	The Name (mnemonic) of the "reconciliation counter" where the amount transaction (field 4) has to be summed up. See example in chapter 5.3.15 . This field is provided for supporting IPSPs' or merchants' ability to automatically generate sums of the turnover on different card schemes FORMAT: ans..16
A5	CARD NAME (FOR PRINTING)	The name of the card product that is to be printed on cardholder receipts . See example in chapter 5.3.15 . FORMAT: ans..16

CA	PurchaseXID	<i>Transaction Identifier</i> Unique transaction identifier determined by MPI. Contains a 20 byte statistically unique value that has been Base64 encoded, giving a 28 byte result. FORMAT: ans 28
CB	TXcavv	<i>Cardholder Authentication Verification Value</i> Determined by ACS. Contains a 20 byte value that has been Base64 encoded, giving a 28 byte result. Required when the value of Transaction Status is "Y" or "A". FORMAT: ans 28
CC	TXcavvAlgorithm	<i>CAVV algorithm</i> A positive integer indicating the algorithm used to generate the Cardholder Authentication Verification Value . Current defined values are: 0 = HMAC (as per SET™ TransStain) (no longer in use for version 1.0.2) 1 = CVV (no longer in use for version 1.0.2) 2 = CVV with ATN 3 = MasterCard SPA algorithm . Required when the value of Transaction Status is "Y" or "A". FORMAT: n 2
CE	TransactionStatus	<i>TransactionStatus</i> Indicates whether a transaction qualifies as an authenticated transaction. Y = Authentication Successful Customer was successfully authenticated. All data needed for clearing, including the Cardholder Authentication Verification Value , is included in the message. N = Authentication Failed Customer failed authentication. U = Authentication Could Not Be Performed Authentication could not be completed, due to technical or other problems. A = Attempts Processing Performed. Authentication could not be completed, but a proof of authentication attempt (CAVV) was generated. Determined by ACS. ' ' = (blank) transaction terminated before authentication was requested (e.g. Issuer is not participating). See <i>appendix F</i> FORMAT: n.. 2

P0	FREE-TEXT-ITEM-DESCRIPTION	<i>Purchase identifier: "Free text item description".</i> FORMAT: an.. 25
P1	TRANSACTION NUMBER	<i>Purchase identifier: "Transaction number".</i> Generated by merchant as an internal system trace number. FORMAT: an.. 25
P2	CUSTOMER-DEFINED DATA	<i>Purchase identifier: "Customer-defined data".</i> FORMAT: an..25
P3	RENTAL AGREEMENT NUMBER	<i>Purchase identifier: "Rental agreement number".</i> FORMAT: an..25
P4	HOTEL FOLIO NUMBER	<i>Purchase identifier: "Hotel folio number".</i> FORMAT: an..25
P5	POSTINGID	<i>Bank generated transaction ID:</i> This transaction ID uniquely identifies the transaction within the financial banking system. The field is present in all subsequent messages related to the financial request. The content of the field is decided by the issuer according to issuer's own needs. FORMAT: ans 26
PR	KEYLABEL	<i>Key label to the key by means of which "SignatureISO9796" must be verified.</i> The field is presently only allowed in Ecommerce environments when the customer is authenticated using eDankort as described in chapter 5.1.3. FORMAT: ans.. 64
S1 + S2	SIGNATUREISO9796	<i>Signature field formatted in accordance with ISO9796.</i> The field is only used for eDankort as described in chapter 5.1.3. FORMAT: (ANS.. 172 – sum of S1 and S2) (the data must be split in the two TAGS . The number of characters in each tag is free except that the maximum number is 99 pr. TAG. The sum of characters in the two TAGs must be <u>exactly</u> 172, e.g. no padding must be

		used).
V5	CARD-VERIFICATION-DATA	<i>Card Verification data:</i> <ul style="list-style-type: none">• VISA CVV-2• MasterCard/Eurocard CVC-2• Dankort Card Verification data (kontrolcifre) FORMAT: n 3

5.3.15 Examples: Reconciliation Counter Id, Reconciliation Counter Name, and Card Name

Table F.80 – Example of Values for Reconciliation Identifiers and Names

Reconciliation Counter Id	Reconciliation Counter Name
001	DANKORT
002	DANSKE EC/MC
003	UDL.EC/MC/VI/JCB
004	AMEX
005	DINERS
006	D KORT BONUS
008	FORBRUGSFORENING
009	ACCEPTCARD
010	SPNKONTOKORT
011	EKSPRESKORT
012	SBVKONTOKORT
013	COMPUTERCITY
014	BG FINANS
015	IKANO FINANS
016	CASTROL CREDIT
019	BG BANK – TAXA

Table F.81 – Example of Values for Card Names to Print

Card Name (for Printing)
ACCEPTCARD
AMEX
BG FINANS
CASTROLCREDIT
COMPUTERCITY
D KORT BONUS
DANKORT
DINERS
EKSPRESKORT
FBF 1886
IKANO FINANS
JCB
MAESTRO
SBVKONTOKORT
SPNKONTOKORT
VISA

Figure 10

5.4 Issuer Authentication (IA) messages extension

The chapter defines data and records used in connection with the "Issuer Authentication" extension as described in chapter 5.1.3.

The messages (HTML form's) must be exchanged before the ISO 8583 messages. Refer to the flow description in 4.4 Detailed description of Shopping and Payment.

5.4.1 Data transport /connection

Data transport between web servers are based on HTML "FORM", method "POST". HTTPS and minimum 128 bit SSL encryption is required.

The Merchant Server must re-direct the customer to the Authentication Router, address information supplied by PBS at time of certification of your payment module.

5.4.2 Data dictionary

All characters in the following fields used in HTML forms are defined according to the ISO 8859-1 character set.²³

Data Name:	Field format	Field definition – when possible based on PSIP/ISO 8583.
AmountTrn	n 12	<p><i>PurchaseAmount:</i> (Supplied by merchant). 12-digit numeric amount in minor units of currency with all punctuation removed. (See ISO 4217) Example: 000000123456</p> <p>This field is equal to ISO 8583 field 4 – "Amount, transaction".</p> <p><i>In the subsequent PSIP ISO 8583 message the content of AmountTrn must be moved to field 4.</i></p>

²³ Please observe that the messages sent to the PGW are defined according to the ASCII character set (see chapter 6.3.6.2)

AuthLifeCycle	n 3	<p><i>Authorization life cycle:</i></p> <p>In 'Authentication Initialization':</p> <p>A time period for which the merchant is <i>requesting</i> guarantee of funds.</p> <p>In 'Authentication Approval' the time period for which the Issuer guarantees funds for a financial transaction which may follow. This field is equal to the ISO 8583 field 57 "Authorization Life Cycle", and defined as follows:</p> <p>Position 1 - time code</p> <table><tr><th><u>Code</u></th><th><u>Description</u></th></tr><tr><td>1</td><td>calendar days²⁴</td></tr><tr><td>2</td><td>hours</td></tr><tr><td>3</td><td>minutes</td></tr></table> <p>Position 2-3 - time interval</p> <table><tr><th><u>Code</u></th><th><u>Description</u></th></tr><tr><td>0-99</td><td>A value of 01 through 99 indicating the number of repetitions indicated in position 1.</td></tr></table> <p><u>Default value:</u> '131' (= 31 calendar days) or according to the merchant agreement.</p> <p><i>In the subsequent PSIP ISO 8583 messages the content of AuthLifeCycle from 'Authentication Approval' must be moved to field 57.</i></p>	<u>Code</u>	<u>Description</u>	1	calendar days ²⁴	2	hours	3	minutes	<u>Code</u>	<u>Description</u>	0-99	A value of 01 through 99 indicating the number of repetitions indicated in position 1.
<u>Code</u>	<u>Description</u>													
1	calendar days ²⁴													
2	hours													
3	minutes													
<u>Code</u>	<u>Description</u>													
0-99	A value of 01 through 99 indicating the number of repetitions indicated in position 1.													
CardLogo	n 1	<p><i>Card logo:</i></p> <p>A value indicating what card type the cardholder has selected on the payment side:</p> <p>'1' Verified-by-Visa (Visa and Visa Electron)</p> <p>'2' SecureCode (MasterCard and Maestro)</p> <p>'3' J/Secure (JCB)</p>												
CurrencyTrn	a 3	<p>PurchaseCurrency (Supplied by merchant).:</p> <p>This field is equal to the currency in ISO 8583 field 49 – "Currency, Transaction".</p>												

²⁴ Calendar days are calculated as:

Date of purchase (date & time, local transaction) e.g:	06 mar01:1601
14 calendar days mean that authorization will expire	20 mar01:2359

		<p>Values defined according to chapter 6.3.6.3.</p> <p><i>In the subsequent PSIP ISO 8583 messages the content of CurrencyTrn must be moved to field 49.</i></p>
DeviceCategory	n 1	<p><i>Device Category</i></p> <p>Indicates the type of cardholder device</p> <p>0 = PC (html) 1 = mobile phone (WML)</p> <p>If no value is provided, the default value is 0 = PC.</p>
ExpirationDate	n 4	<p><i>Card Expiry Date</i></p> <p>This field is equal to the ISO 8583 field 14 – “Date, Expiration”.</p> <p>When eDankort transaction, this field must always be zero-filled.</p> <p><i>In the subsequent PSIP ISO 8583 messages the content of ExpirationDate must be moved to field 14.</i></p>
KeyLabel	anp 33	<p><i>Label to the public key of the banks signature key pair :</i></p> <p>This field is defined as a TAG/LENGTH/VALUE data element, The following TAG-ID has been assigned:</p> <p>⚡ PR (se definition on page 51)</p> <p><i>In the subsequent PSIP ISO 8583 messages the content of KeyLabel must be moved to field 47</i></p>
MerchantAccount	an 15	<p><i>Merchant Account number:</i> (Supplied by merchant).</p> <p>Unique Merchant identification: Merchant number (as specified in merchant agreement/ or assigned by PBS/Terminal Operator).</p> <p><i>In the subsequent PSIP ISO 8583 messages the content of MerchantAccount must be moved to field 42.</i></p>
MerchantAcquirerBIN	n.. 11	Acquirer BIN
Merchantcountry	n 3	<p><i>Merchant Country Code</i> (Determined by merchant).</p> <p>3-digit numeric ISO-3166 Country Code.</p> <p>Determined by Merchant country. (Example: US = 840)</p>
MerchantUrl	[RFC 2396]25	<p><i>Merchant URL</i> (Determined by merchant).</p>

		Fully qualified URL of merchant site
MerchantContinueURL	[RFC 2396]²⁵	<p><i>Merchant Continue URL:</i> (Supplied by merchant).</p> <p>Merchant defined URL address, which is activated when Customer is authenticated in the Netbank.</p>
MerchantDeclineURL	[RFC 2396]²⁵	<p><i>Merchant Decline URL:</i> (Supplied by merchant).</p> <p>Merchant defined URL address, which is activated if the customer is not authenticated/authorized by the netbank, or if the customer rejects the transaction after leaving the merchant application.</p>
MerchantGmtOffset	n 2	<p><i>Merchant Time offset from GMT</i> (Supplied by merchant).</p> <p>Number of hours merchant's local time is offset from Greenwich Mean Time.</p>
MerchantTitle	an..25	<p><i>Merchant Title:</i> (Supplied by merchant).</p> <p>This field is equal to the Merchant name in ISO 8583 field 43 – "Card Acceptor Name location" (the data before the first back-slash).</p> <p>See PSIP Authorization Request for further specification</p> <p><i>In the subsequent PSIP ISO 8583 messages the content of MerchantTitle must be moved to field 43.</i></p>
OrderNo	ans..20	<p><i>Order number:</i> (Supplied by merchant).</p> <p>This field is equal to the Order Number in ISO 8583 field 31 – "Acquirer Reference Data".</p> <p><i>In the subsequent PSIP ISO 8583 messages the content of OrderNo must be moved to field 31.</i></p>
PAN	n..19	<p><i>Primary Account Number</i></p> <p>This field is equal to the ISO 8583 field 2 – "Primary Account Number".</p> <p><i>In the subsequent PSIP ISO 8583 messages the content of PAN must be moved to field 2.</i></p>
POSDatocode	an 12	<p><i>Point of service data code</i></p> <p>This field is equal to the ISO 8583 field 22 –</p>

²⁵ "Uniform Resource Identifiers (URI): Generic Syntax", T. Berners-Lee, R. Fielding, L. Masinter, August 1998. [RFC 2396]

		<p>"Point of service data code".</p> <p><i>In the subsequent PSIP ISO 8583 messages the content of POSDatocode must be moved to field 22, if the Merchant decides to go on with the authorization, see appendix F .</i></p>
PostingID	an 26	<p><i>Bank generated transaction ID:</i></p> <p>This field is defined as a TAG/LENGTH/VALUE data element²⁶, The following TAG-ID has been assigned:</p> <p>⚡ P5 (se definition on page 51)</p> <p><i>In the subsequent PSIP ISO 8583 messages the content of PostingID must be moved to field 47</i></p>
PurchaseAmount	an 13	<p><i>Formatted displayable amount: (Supplied by merchant).</i></p> <p>"ISO 4217 formatted purchase amount. This field should contain a currency symbol, with a thousands separator(s), decimal point and minor units defined for the currency specified in the AmountTrn field.</p> <p>Example: \$1,234.56"</p> <p>Comments:</p> <p>This field is equal to the total amount displayed to the cardholder at the merchant web-site and on merchant generated receipts.</p> <p>Issuer may regard this field as an electronic copy of the amount on the cardholder receipt and use the field in any cardholder dispute cases to determine if cardholder is invoiced another amount than that originally accepted.</p>
PurchaseDate	an 15	<p><i>Purchase date: (Supplied by merchant).</i></p> <p>Date of Purchase (merchant's local date and time, as: YYMMDD HH:MM:SS)</p>
PurchaseDateGMT	an 15	<p><i>Purchase date GMT</i></p> <p>Date of Purchase (expressed date and time, as: YYMMDD HH:MM:SS)</p>
PurchaseDescription	ans... 125	<p>In 3-D Secure the field must contain at least the text 'Order no.: ', followed by the value of the OrderNo field terminated by a period'.'. .</p>

²⁶ TAG/LENGTH/VALUE data-structure described in chapter "6.3.11".

		Ex: Order no.: Az012.
PurchaseExponent	n 1	Currency exponent ref. to ISO 4217
PurchaseInstallment	variable length	Installment Payment data (VISA 3D secure field) (Supplied by merchant).
PurchaseXID	ans 28	Transaction Identifier TAG CA Base 64 encoded
RecurringFrequency	n 3	For future use Min. no. of days between authorizations
RecurringEndrecur	n 8	For future use Format: YYYYMMDD
SignatureISO9796	an 172	Bank generated signature: This field is defined as a TAG/LENGTH/VALUE data element. Since the signature is longer than the length of one TAG, the following two TAG-IDs has been assigned: <ul style="list-style-type: none"> ⌘ S1 (see data dictionary) ⌘ S2 (seedata dictionary) <i>In the subsequent PSIP ISO 8583 messages the content of SignatureISO9796 must be moved to field 47</i>
TestFlg	a 1	Test Flag: (Supplied by merchant). Test Indication – if present the transaction will be performed against netbank test environment. Values _____: 'T' Test 'P' Production

TransactionStatus	a 1	<p><i>Transaction Status (VISA 3D secure field)</i> Indicates whether a transaction qualifies as an authenticated transaction.</p> <p>Y = 'Authentication Successful' Customer was successfully authenticated.</p> <p>U = 'Authentication could not be performed' Authentication could not be completed, due to technical or "not participating Cardholder" or other problems.</p> <p>N = Authentication Failed. Customer failed authentication. Transaction denied.</p> <p>A = Attempts Processing Performed. Authentication could not be completed, but a proof of authentication attempt (CAVV) was generated.</p> <p>' ' Issuer and/or cardholder is not participating.</p>
TXcavv	ans 28	<p><i>Cardholder Authentication Verification Value</i> <i>TAG CB</i></p> <p>Base 64 encoded</p>
TXeci	n 1	<p><i>Electronic Commerce Indicator determines the Point of service data code refer to PSIP Merchant Guide</i></p>
TXcavvAlgorithm	variable length	<p><i>CAVV algorithm</i> <i>TAG CC</i></p>

5.5 Authentication Initialization

"Authentication Initialization" <i>Purpose: The Authentication Initialization message is generated by the Merchant Server and sent to the PBS Authentication router via the cardholder PC connecting the cardholder to his Issuer/Bank.</i>	eDankort Field condition and default value	3-D Secure Field condition and default value
<pre> <form name=AuthenticationRequest action="PBS authentication router URL" method="post" target="_top"²⁷> <input name="MerchantContinueURL" type=hidden value="Merchant authentication Continue URL "> <input name="MerchantDeclineURL" type=hidden value="Merchant Authentication Decline URL "> <input name="MerchantTitle" type=hidden value="Merchant Title"> <input name="OrderNo" type=hidden value="Order number"> <input name="MerchantAccount" type=hidden value="Merchant ID"> <input name="AmountTrn" type=hidden value="PurchaseAmount"> <input name="CurrencyTrn" type=hidden value="PurchaseCurrency"> <input name="AuthLifeCycle" type=hidden value="Authorization life cycle"> <input name="TestFlg" type=hidden value="Test/Prod Flag"> <input name="DeviceCategory" type=hidden value="Device Category"> <input name="MerchantCountry" type=hidden value="Merchant Country Code"> <input name="MerchantGmtoffset" type=hidden value="Merchant Time offset from GMT"> <input name="MerchantUrl" type=hidden value="Merchant URL"> <input name="PAN" type=hidden value="Primary Account Number"> <input name="PurchaseDate" type=hidden value="Purchase date & time"> <input name="PurchaseDateGMT" type=hidden value="Purchase date GMT "> <input name="PurchaseInstallment" type=hidden value="Installment Payment data"> <input name="ExpirationDate" type=hidden value="Card Expiry Date"> <input name="MerchantAcquirerBIN" type=hidden value="Acquirer BIN"> <input name="PurchaseAmount" type=hidden value="Formatted displayable amount"> <input name="PurchaseExponent" type=hidden value="Currency Exponent"> <input name="PurchaseDescription" type=hidden value="Order Description"> <input name="RecurringFrequency" type=hidden value="Recurring Frequency"> <input name="RecurringEndrecur" type=hidden value="Recurring Expiry"> <input name="CardLogo" type=hidden value="Card logo"> </form> </pre>	<p>Mandatory</p> <p>Mandatory</p> <p>Mandatory</p> <p>Mandatory</p> <p>Mandatory</p> <p>Mandatory</p> <p>Mandatory Default value: 'DKK'</p> <p>Optional</p> <p>Mandatory</p> <p>Optional</p> <p>Mandatory</p> <p>Mandatory</p> <p>Mandatory</p> <p>N/A</p> <p>Mandatory</p> <p>N/A</p> <p>N/A</p> <p>Optional</p> <p>N/A</p> <p>N/A</p> <p>Mandatory</p> <p>N/A</p> <p>Optional</p> <p>Optional</p> <p>Optional</p> <p>N/A</p>	<p>Mandatory</p> <p>Mandatory</p> <p>Mandatory</p> <p>Mandatory</p> <p>Mandatory</p> <p>Mandatory</p> <p>Mandatory Default value: 'DKK'</p> <p>N/A</p> <p>Mandatory</p> <p>Optional</p> <p>Mandatory</p> <p>n/a</p> <p>Mandatory</p> <p>Mandatory</p> <p>N/A</p> <p>Mandatory</p> <p>n/a</p> <p>Mandatory</p> <p>Mandatory</p> <p>Conditional</p> <p>Conditional</p> <p>Mandatory</p>

²⁷ The target="_top" option **must** be used

5.6 Authentication Decline

"Authentication Decline" <i>Purpose: The Authentication Decline message is generated by the Netbank Authentication system and sent to the Merchant Server (or PBS eDankort Router) via the cardholder PC in case of transaction decline (Authentication Failed)</i>	eDankort Field condition and default value
<pre> <form name=AuthenticationDecline action="MerchantDeclineURL" method="post" > <input name="OrderNo" type=hidden value="Order number"> <input name="MerchantAccount" type=hidden value="Merchant ID"> <input name="AmountTrn" type=hidden value="PurchaseAmount"> <input name="CurrencyTrn" type=hidden value="PurchaseCurrency"> </form> </pre>	<p>Mandatory <u>echo</u>²⁸</p> <p>Mandatory <u>echo</u></p> <p>Mandatory <u>echo</u></p> <p>Mandatory <u>echo</u></p>

²⁸ "Mandatory Echo" means that the Issuer must return the fields unaltered as received from merchant.

5.7 Authentication Approval

"Authentication Approval" <i>Purpose: The Authentication Approval message is generated by the Issuer Authentication system and sent to the Merchant Server via the cardholder PC.</i>	eDankort Field condition and default value²⁹	3-D Secure Field condition and default value
<pre> <form name=AuthenticationApproval action="MerchantContinueURL " or "MerchantDeclineURL" method="post" > <input name="OrderNo" type=hidden value="Order number"> <input name="MerchantAccount" type=hidden value="Merchant ID"> <input name="AmountTrn" type=hidden value="PurchaseAmount"> <input name="CurrencyTrn" type=hidden value="PurchaseCurrency "> <input name="AuthLifeCycle" type=hidden value="Authorization life cycle"> <input name="PostingID" type=hidden value="Bank generated transaction ID"> <input name="PAN" type=hidden value="Primary Account Number"> <input name="ExpirationDate" type=hidden value="Expiration Date"> <input name="TransactionStatus" type=hidden value="Transaction Status"> <input name="KeyLabel" type=hidden value="Key Label"> <input name="SignatureISO9796" type=hidden value="Signature ISO9796"> <input name="PurchaseAmount" type=hidden value="Displayamount"> </pre>	<p><u>Mandatory echo</u></p> <p><u>Mandatory echo</u></p> <p><u>Mandatory echo</u></p> <p><u>Mandatory echo</u></p> <p><u>Mandatory³⁰</u></p> <p><u>Conditional</u> may be omitted only if Transaction Status indicates "Authenti-cation could not be performed"</p> <p><u>Mandatory</u></p> <p><u>Mandatory When eDankort transaction. this field must be zero-filled.</u></p> <p><u>Mandatory</u> must allways be 'Y'. <u>Conditional</u>, depending on bank implementati on.</p> <p><u>Conditional</u>, depending on bank implementati on.</p> <p><u>Optional echo</u></p> <p>If merchant initiates this field, the bank can</p>	<p><u>Mandatory echo</u></p> <p><u>Mandatory echo</u></p> <p><u>Mandatory echo</u></p> <p><u>Mandatory echo</u></p> <p><u>N/A</u></p> <p><u>N/A</u></p> <p><u>Mandatory</u></p> <p><u>Mandatory</u></p> <p><u>Mandatory</u></p> <p><u>N/A</u></p> <p><u>N/A</u></p> <p><u>N/A</u></p>

²⁹ It is recommended that merchant always validates if "mandatory echo" fields are returned unaltered (e.g. to prevent Cardholders from adjusting the transaction amount or currency code before authentication)

³⁰ If the field is initiated by the merchant, the value may be adjusted by the bank to reflect the guarantee period granted by the bank. Alternatively, the bank must initiate the field according to the bank rules/acquiring agreement.

	choose to forward it or not. ³¹	
<input name="PurchaseInstallment" type=hidden value="Installment Payment data">	<u>Optional echo</u>	<u>Optional echo</u>
<input name="TXcavv " type=hidden value="Cardholder Authentication Verification Value">	<u>N/A</u>	<u>Conditional-mandatory if Transaction status = 'Y' or 'A' and the information is supplied by Issuer</u>
<input name="PurchaseXID " type=hidden value="Transaction Identifier">	<u>N/A</u>	<u>Conditional-mandatory if Transaction status = 'Y' or 'A' and the information is supplied by Issuer</u>
<input name="TXeci" type=hidden value="Electronic Commerce Indicator">	<u>N/A</u>	<u>Conditional - mandatory for Visa transactions</u>
<input name="TXcavvAlgorithm " type=hidden value="CAVV algorithm">	<u>N/A</u>	<u>Conditional-mandatory</u> <u>If Cardholder Authentication Verification Value is present</u>
<input name="CardLogo" type=hidden value="Card logo">	<u>N/A</u>	<u>Mandatory echo</u>
<input name="POSDatacode " type=hidden value="Point of service data code">³²	<u>N/A</u>	<u>Mandatory</u>
</form>		

³¹ PBS will test that this field is filled out in accordance with the field AmountTrn, when certifying the payment modules.

³² If the field has a 'no value', a PSIP Authorization must NOT be sent!

The order can be declined, or another means of payment requested.

6 Security Requirements

6.1 Card Security Programme (The PCI Standard)

In 2005, MasterCard and Visa updated their security standards. All IPSPs must be PCI-compliant in order to be able to handle card data. A number of other card organizations have subsequently joined the programme, including the card organizations represented in the Danish market.

The PCI standard consists of a number of security requirements which are an expansion of the existing security requirements. The security standards are available at <http://www.visaeurope.com/acceptingvisa/securitystandards.html> and https://sdp.mastercardintl.com/serviceproviders/serviceprovider_requirements.shtml

New IPSPs must meet the security requirements, which must be proven by an on-site review by an approved security assessor prior to sending transactions to the PBS system.

All approved IPSPs must have an annual on-site review by an approved security assessor.

Furthermore, a quarterly scan of the IPSPs systems etc. must be performed by an approved scan vendor.

Approved security assessors and scan vendors are available at the following web-sites:

<https://sdp.mastercardintl.com> and www.visaeurope.com/acceptingvisa/ais.html

For further information, please also refer to the IPSP agreement made with PBS A/S.

7 Requirements to cardholder interface in Ecommerce/IA environments

7.1 Order Number

To ensure tracking of a given order, the merchant must generate a unique (within 24 hours) reference: an order number.

The order number must consist of a maximum of 20 visible characters (a-z, 0-9, and special characters , . -).

The merchant must supply the cardholder with the order number in the receipt message. The order number must be forwarded to PBS in the PSIP protocol.

7.2 Expiration Dates

The following should be considered when designing the cardholder interface:

Expiration dates embossed on cards are formatted as MMY (month/year). The PSIP specifies the expiration date as YYMM.

To avoid confusion for the cardholder, it is obvious to make the cardholder key in the expiration date as MMY, and the merchant server must then convert this to the PSIP format.

The merchant server must display a leading text, explaining the format (e.g.: "card expiration date (MMY): ").

7.3 Card Verification Data (CVD)

Card verification data is a number (normally 3 digits) printed on the back of the physical card, right after the card number. The CVD can be found right above or below the signature panel, in the signature panel or in a little box next to the signature panel. The CVD is a number designed to increase security in environments where the magnetic stripe cannot be read.

The CVD cannot be found in the magnetic stripe, and it is not embossed in the plastic, which ensures that it cannot be seen on a credit card paper slip. The CVD enables the merchant to reduce the risk in accepting cards on the internet since the CVD makes it more certain that the physical card is present at the time of purchase. The merchant may demand that the CVD be entered by the cardholder, but if demanded, the merchant server must comply with the rules in Appendix D.

7.4 Cardholder Receipt

When the transaction has been approved, the merchant must transmit a receipt to the cardholder. The receipt must, as a minimum, include the following data (please refer to merchant agreement for further details):

- 1) The name of the merchant (subfield "merchant name" from field 43)
- 2) The merchant's e-mail address
- 3) A description of the goods/services ordered (field 47)
- 4) Order number (field 31)/transaction number (e.g. merchant internal system transaction number (field 47))
- 5) Transaction date (field 12)
- 6) Transaction currency (field 49)
- 7) Transaction amount (field 4)
- 8) Transaction type (debit/credit) (field 4)
- 9) Expected date of delivery
- 10) Status of the transaction (COMPLETED) (field 39 + appendix A)
- 11) Truncated Card number (PAN) (field 2) (see chapter 7.5)

If the transaction is declined, the cardholder receives an error message.

The requirement concerning truncated card number is only applicable to eDankort and Dankort. For other card types such as Eurocard, MasterCard, Visa and JCB, the cardholder receipt should not contain the card number. If the card number is included, it must be truncated, see below.

For requirements to cardholder receipts stipulated by acquirers of other cards, please refer to the acquirer in question.

The amount must not exceed the amount stated on the order form and accepted by the cardholder.

7.5 Truncation of the Card Number (PAN)

To avoid misuse of card numbers, the merchant **MUST** truncate the card number on cardholder receipts.

The card number printed on cardholder receipts enables the cardholder to decide whether the actual cardholder receipt belongs to him/her or not. Therefore, not all digits must be omitted, and the last digits may be used to identify the card used.

Number of digits in the PAN	'Original PAN'	Truncated PAN
7	1234 567	XXXX 567
8	1234 5678	XXXX 5678
9	1234 5678 9	XXXX X678 9
10	1234 5678 90	XXXX XX78 90
11	1234 5678 901	XXXX XXX8 901

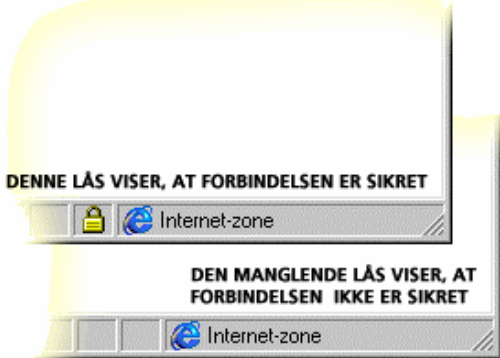
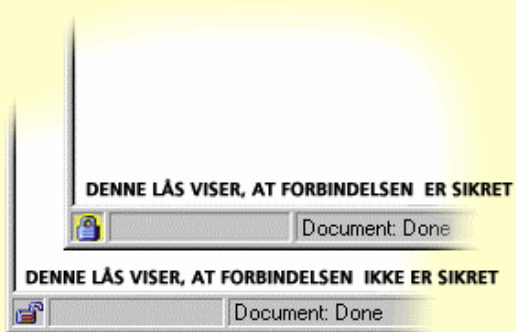
12	1234 5678 9012	XXXX XXXX 9012
13	1234 5678 9012 3	XXXX XXXX X012 3
14	1234 5678 9012 34	XXXX XXXX XX12 34
15	1234 5678 9012 345	XXXX XXXX XXX2 345
16	1234 5678 9012 3456	XXXX XXXX XXXX 3456
17	1234 5678 9012 3456 7	XXXX XXXX XXXX X456 7
18	1234 5678 9012 3456 78	XXXX XXXX XXXX XX56 78
19	1234 5678 9012 3456 789	XXXX XXXX XXXX XXX6 789

7.6 Displaying secure sessions

The merchant system must be designed in a way which enables the different browsers to detect that the session is occurring in a secure SSL environment. The browser must display that the session occurs in a secure SSL session.

The system must be designed in a way that enables the "secure session" symbol (the padlock) to be visible **before** the card number is requested, and the symbol must be visible as long as the SSL session is established.

The system must not store the card number or expiration date on the cardholder PC (in a cookie or by an equivalent technique)

Microsoft Internet Explorer	Netscape Navigator
	

Appendix A Action Code

The Action Codes used are taken from ISO 8583 v.1.

This chapter lists descriptions and interpretation of the most commonly used action codes with an explanation of why a given action code is used. Other action codes can be used, and non-mentioned action codes must be considered as a "decline".

PBS defines some of the below mentioned action codes in the ISO 8583 interval for "national use".

PBS – Action Code

Action Code	Action Code text (for merchant use only)	Action Code text (for use against Cardholder)	Merchant Action
000	Approved	Approved	
001	Honour with identification	Decline ³³	
002	Approved for partial amount	Partly Approved	
060	Approved	Approved	
061	Approved	Approved	
063	Approved	Approved	
100	Do not honour	Decline	
101	Expired Card	Decline/Expired Card	
102	Suspected Fraud	Decline	
103	Card acceptor contact acquirer	Decline	
104	Restricted card	Decline	
105	Card Acceptor call Acquirers security department	Decline	
106	Allowable pin tries exceeded	Decline	
107	Refer to card issuer	Decline ³⁴	
108	Refer to card issuer – special conditions	Decline	
109	Invalid merchant	Decline	
110	Invalid amount	Decline/Amount Error	
111	Invalid card number	Decline	

³³ In essence this transaction is approved, but it is not possible to ask for more identification such as a driver's licence on the internet.

³⁴ The basic meaning of the action code is that the card issuer should be contacted. It is PBS's experience that action code 107 is used as a true decline from issuers outside Denmark, and that authorization will not be granted, even though the card issuer is contacted. If transactions are internet based, and the cardholder initiates the authorization transaction real-time, the action code does not give any meaning

Action Code	Action Code text (for merchant use only)	Action Code text (for use against Cardholder)	Merchant Action
112	Pin data required	Decline	
113	Unacceptable fee	Decline	
114	No account of type requested	Decline	
115	Requested function not supported	Decline	
116	Not sufficient funds	Decline	
117	Incorrect pin	Decline	
118	No card record	Decline	
119	Transaction not permitted to cardholder	Decline/Invalid Transaction	
120	Transaction not permitted to terminal ³⁵	Decline/Invalid Transaction	
121	Exceeds withdrawal amount limit	Decline	
122	Security violation	Decline	
123	Exceeds withdrawal frequency limit	Decline	
124	Violation of law	Decline	
125	Card not effective	Decline	
126	Invalid pin block	Decline	
127	Pin length error	Decline	
128	Pin key synch error	Decline	
129	Suspected counterfeit card	Decline	
160	Invalid date	Decline	
161	Allowable number of pin tries exceeded	Decline	
162	Unable to locate previous message	Decline	
164	Card entry found, below low range	Decline	
165	Pan length not according to table	Decline	
167	Match on previous transaction not allowed	Decline	
200	Do not honour	Decline	
201	Expired card	Decline/Expired Card	
202	Suspected fraud	Decline	

³⁵ Three terminal categories are defined in the card business:

- EFTPOS (Electronic Funds Terminal Point Of Service): Physical terminal installed in a store, operated by merchant.
- ATM (Automated Teller Machine): Cash dispenser, cardholder activated
- NOTA ("paper based"): All transactions where the card number is not read automatically are included in this category. This includes mail-order, phone-order and internet transactions.

Some cards can only be used in a subset of the terminal categories.

Action Code	Action Code text (for merchant use only)	Action Code text (for use against Cardholder)	Merchant Action
203	Card acceptor contact acquirer	Decline	
204	Restricted card	Decline	
205	Card acceptor call acquires security department	Decline	
206	Allowable pin tries exceeded	Decline	
207	Special conditions	Decline	
208	Lost card	Decline	
209	Stolen card	Decline	
210	Suspected counterfeit card	Decline	
900	Advice acknowledged, no financial liability accepted.	Approved	
901	Advice acknowledged, financial liability accepted.	Approved	
902	Invalid transaction	Decline/Invalid Transaction	
903	Re-enter transaction	Decline	
904	Format error	Decline/ System Error	Contact PBS
905	Acquirer not supported by switch	Decline/System Error	
906	Cut over in process	No Reply	Re-submit ³⁶
907	Card issuer or switch inoperative	No Reply	Re-submit
908	Transaction destination cannot find routing	Decline	
909	System malfunction	Decline/ System Error	Contact PBS
910	Card issuer signed off	No Reply	Re-submit
911	Card issuer timed out	No Reply	Re-submit
912	Card issuer unavailable	No Reply	Re-submit
913	Duplicate transmission	Decline/ System Error	Contact PBS
914	Not able to trace back to original transaction	Decline	
915	Reconciliation cut over or checkpoint error	No Reply	Re-submit
916	MAC incorrect	Decline/System Error	
917	MAC key sync error	Decline/System Error	
918	No communication keys available	Decline/System Error	
919	Encryption key error	Decline/System Error	
920	Security software/hardware error – try again	System Error	Re-submit

³⁶ See chapter 5.2

Action Code	Action Code text (for merchant use only)	Action Code text (for use against Cardholder)	Merchant Action
921	Security software/hardware error – no action	System Error	Re-submit
922	Message number out of sequence	System Error	Contact PBS
923	Request in progress	System Error	Re-submit
930	CAVV Incorrect	Decline/ System Error	
940	Invalid date and time, local transaction,	System Error	Correct system date and time on own equipment
945	KIR (PBS host) timeout	No Reply	Re-submit
946	PGW error occurred, unspecified	No Reply	Re-submit
950	Violation of business arrangement	Decline/ System Error	
984	No valid conversion for a field	Decline/ System Error	

Appendix B PGW Response code

PSIP header error codes	PSIP header error codes text (for merchant use only)
000	OK
400	Bad Request
500	Internal server error on PGW
501	Not implemented
503	Service unavailable

Appendix C Message Samples: E-commerce

C.1 Authorization Request

	ASCII
	=====
00CF000052480002200000000000000032RH..2
00000000000000000000000000000000
50534950313030303030313130307014	PSIP1000001100p.
05C200E28000313131323334303432351112340425
37343830303030303030303030303030	7480000000000000
30313230303939303231393134323230	0120099021914220
30303931314B30303530304B30303133	00911K00500K0013
30313030303030303539363430313837	0100000059640187
37372020202020313937383535312020	77 1978551
202020202020343450425320494E5445	44PBS INTE
524E414C20544553545C5C42616C6C65	RNAL TEST\\Balle
7275705C323735302020202020444B	rup\2750 DK
20444E4B3030375635313233444B4B00	DNK007V5123DKK.

C.2 Authorization Response

	ASCII
	=====
00E9000052480002200000000000000032RH..2
00000000000000000000000000000000
50534950313030303030313130307010	PSIP1000001110p.
000206C08100313635303139313233341650191234
30343235373438333030303030303030	0425748300000000
30303030303031323030393930323139	0000001200990219
31343232303030313831343236323830	1422000181426280
30303737372020202020313937383535	00777 197855
312020202020202020444B4B30393030	1 DKK0900
38736F66747761726557347068C20C68	8softwareW4ph..h
1592AC3260205D26D2DAC9D4BB12BBAB	...2`]&.....
7554F356CB15862F2D85EA8A40E7A622	uT.V.../-...@..
B188A2CFCF55464B7AB8EE6DADA6DE61UFKz..m...a
BFFB517534F810D6BBB3E4989C2AF874	..Qu4.....*.t
72E7ACDA95B3E0D4EE00000000000000	r.....

C.3 Capture Request

	ASCII
	=====
014D0000524800022000000000000032	.i..RH..2
000000000000000000000000000000
50534950313030303030313232307014	PSIP1000001220p.
054206E2810031363530313931323334	.B....1650191234
303432353734383330303030303030	0425748300000000
30303030303031323030393930323139	0000001200990219
313432323435303931314B3030353030	1422450911K00500
4B303031333032303135393634303138	K001302015964018
31343236323830303037373720202020	142628000777
203139373835353120202020202020	1978551
343450425320494E5445524E414C2054	44PBS INTERNAL T
4553545C5C42616C6C657275705C3237	EST\\Ballerup\27
3530202020202020444B20444E4B3032	50 DK DNK02
372020202020202020202020202020	7
20202020202020202020202020444B4B30	DKK0
39303038736F66747761726557347068	9008softwareW4ph
C20C681592AC3260205D26D2DAC9D4BB	..h...2`]&.....
12BBAB7554F356CB15862F2D85EA8A40	...uT.V.../-...@
E7A622B188A2CFCF55464B7AB8EE6DAD	.."......UfKz..m.
A6DE61BFFB517534F810D6BBB3E4989C	..a..Qu4.....
2AF87472E7ACDA95B3E0D4EE00000000	*.tr.....

C.4 Capture Response

	ASCII
	=====
00E30000524800022000000000000032RH..2
000000000000000000000000000000
50534950313030303030313233307010	PSIP1000001230p.
000202C08100313635303139313233341650191234
303432353734383330303030303030	0425748300000000
30303030303031323030393930323139	0000001200990219
31343232343530313830303037373720	142245018000777
20202020313937383535312020202020	1978551
202020444B4B3039303038736F667477	DKK09008softw
61726557347068C20C681592AC326020	areW4ph..h...2`
5D26D2DAC9D4BB12BBAB7554F356CB15]&.....uT.V..
862F2D85EA8A40E7A622B13E6D18C62C	./-...@..".>m..
73468CC06ECED20D64D2D366977BAFDA	sF..n...d..f.{..
52500A6F85BC8AAB6AEF65724488E5C9	RP.o....j.erD...
159819000000000000000000000000

Appendix D Rules regarding CVD

The following table shows the card products currently supporting CVD (Card Verification Data).

If the merchant demands that CVD be entered for a card product, the rules stipulated in the following table must be followed.

Please observe that:

- not all card products accepted in the PBS SSL internet solution have CVD, and these card products are therefore not included in the table
- the merchant server must not demand that CVD be entered for card products not included in the table.
- if the merchant has signed a merchant agreement concerning card products that do not have CVD, these cards must be accepted by the merchant server.

D.1 Cards with CVD

Card product name	Prefix range (card numbers starting with:)	Special rules
DINERS	304 - 305 36 38	
JCB	3528 - 3589	
VISA	4000 - 4999	
VISA/DANKORT	4571	As of 01.04.2005 CVD is mandatory
DANKORT	5019	As of 01.04.2005 CVD is mandatory
EUROCARD/ MASTERCARD	5100 - 5599	

Appendix E Authentication processing in 3-D Secure

If the 'Transaction status' value is not 'Y' or 'A' the merchant may decide to complete the transaction as a non-authenticated transaction.

However, the Merchant should be aware that the card schemes have different liability rules. The 'POSDatacode' and 'TransactionStatus' can help in the decision whether to go on with the 'Authorization Request'.

The 'POSDatacode' values indicate:

1. '880500887130' – Authentication of cardholder is proved
2. '880500800130' – Authentication of cardholder could not be proved (e.g. cardholder or issuer not participating)
3. '8805008R0130' – Authentication of cardholder failed. Incorrect cardholder code keyed in or a not foreseen error arose (e.g. communication error).

If 1.: liability always shifts to the Issuer. The Issuer cannot charge back with the reason of an unauthenticated transaction. For Visa and JCB transactions the CAVV is optionally present in Authentication Approval.

If 2.: liability shifts to the Issuer³⁷. The Issuer cannot charge back with the reason of an unauthenticated transaction. No CAVV or AAV is present in Authentication Approval.

If 3.: no liability shift. If in combination with 'TransactionStatus' = 'N', the Cardholder (or a fraud) was not able to supply the right code, the risk of fraud is obvious. Authorization should not be sent.

POSDatacode	TransactionStatus	Send Authorization Request		
		MC	Visa	JCB
'880500887130'	Y	Yes (3D-Secure transaction)	Yes (3D-Secure transaction)	Yes (3D-Secure transaction)
'880500800130'	Y N A U -(blank)	Yes (3D-Secure transaction)	Yes (3D-Secure transaction)	Yes (3D-Secure transaction)
'8805008R0130'	Any value - except N	n/a	Yes (SSL transaction)	Yes (SSL transaction)
<no value> no POSDatacode received in 'Authentication approval'	-	n/a	No decline or ask for another means of payment	No decline or ask for another means of payment

³⁷ This is true except for MasterCard issued in USA, Canada, and Latin America.

Appendix F Implementing own MPI

Merchants or IPSP's who implement their own 3-D Secure authentication server (MPI) must implement the authentication protocol, and follow the rules set up by the card schemes (e.g. Visa).

In addition, they must compose the 'Point of Service data code' field 22 of the PSIP request messages, following the rules pattern of the following table: Deciding the Point of Service Data Code value

Scenario	VEReq status	PAREs status	ECI PAREs MC	ECI PAREs Visa	Point of Service Data Code	
					MC	Visa/JCB
Auth Success	Y	Y	02	5	'880500887130'	'880500887130'
Auth Success (without CAVV/AAV)	Y	Y	02	5	'880500800130'	: '880500887130'
Auth Failure (Password failure)	Y	N	-	n/a	<no value> - decline or use other payment method	<no value> - decline or use other payment method
Auth Failure (Signature verification incorrect)	Y	All	All	-	'880500800130'	'8805008R0130'
Unable to Authenticate	Y	U	-	n/a	'880500800130'	'8805008R0130'
Attempt	Y	A	01	6	'880500800130'	'880500800130'
Attempt (without CAVV/AAV)	Y	A	01	6	'880500800130'	'880500800130'
Cardholder Not Participating	N	-	-	n/a	'880500800130'	'880500800130'
Unable to Authenticate	U	-	-	n/a	'880500800130'	'8805008R0130'
Cardholder Not Participating (via directory cache)	-	-	-	n/a	'880500800130'	'880500800130'
Error on DS	-	-	-	-	'880500800130'	'8805008R0130'
Error on VEReq	-	-	-	-	'880500800130'	'8805008R0130'
Error on VERes	Error	-	-	-	'880500800130'	'8805008R0130'
Error on PAREs	Y	Error	Error	n/a	'880500800130'	'8805008R0130'
Error - other	-	-	-	-	'880500800130'	'8805008R0130'