

# Datatrans E-Com

Technical Implementation Guide

for

# Universal Payment Page

# (UPP)

April 2007 / Version 3.0.4

## Revision Control

Version	Date	Changed by	Comments / nature of change
3.0.0 (doc) 1.4 (SW)	01.11.2005	Urs Kipfer	Complete revision
3.0.1 (doc) 1.4 (SW)	30.12.2005	Urs Kipfer	2.1.1 / 2.2.1: URL for ISO encoding
3.0.2 (doc) 1.4 (SW)	12.01.2006	Urs Kipfer	2.3.3: Anti fraud data management 2.4.2: Payment page response codes
3.0.3 1.4 (SW)	07.07.2006	Urs Kipfer	1.2.4: Click & Buy 2.2.1: Click & Buy 2.3.2: Digital signature, "sign2"; "2sign" for XML settlement
3.0.4	20.04.2007	Urs Kipfer	2.2.1: EasyPay removed from document; PayPal added as payment method

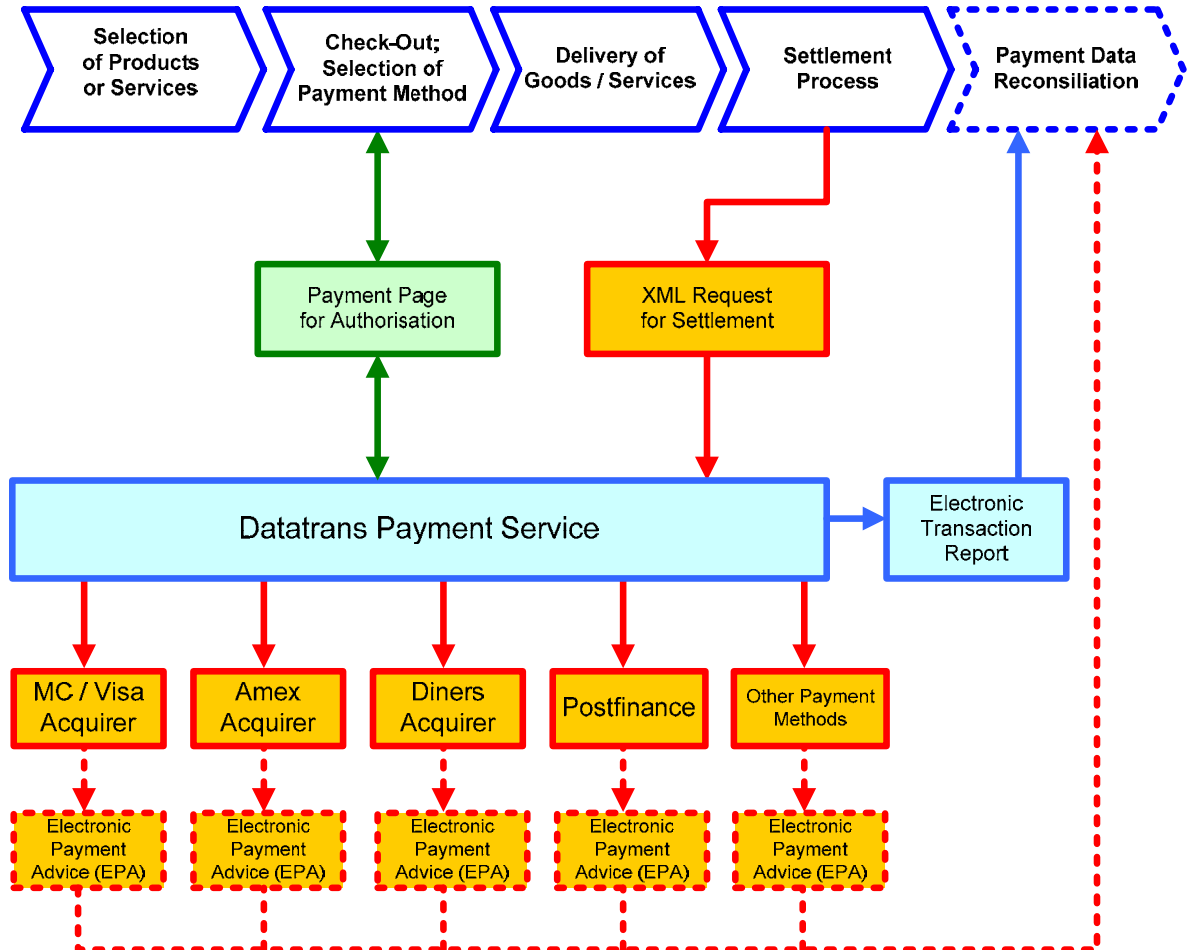
## Table of contents

<b>1. INTRODUCTION</b>	<b>5</b>
<b>1.1. Datatrans Payment Process</b>	<b>5</b>
1.1.1. Role of the PSP	5
1.1.2. Authorisation	6
1.1.3. Settlement	6
1.1.4. Reconciliation / data consolidation	6
<b>1.2. Payment Methods</b>	<b>7</b>
1.2.1. Credit Cards	7
1.2.2. Swiss Postfinance	8
1.2.3. Loyalty Cards	8
1.2.4. Swisscom Click & Buy	8
<b>1.3. Planning / Concept of Payment Integration</b>	<b>9</b>
1.3.1. Which payment methods do I want to offer to my customers?	9
1.3.2. Which acquirer contract types do I need?	9
1.3.3. Do I want to offer local currencies to my customers?	9
1.3.4. How do I avoid fraud?	9
1.3.5. How do I avoid erroneous transactions, i.e. double bookings?	9
1.3.6. How will I match the bank payments with my receivables?	10
1.3.7. Do I need 3D Secure?	10
1.3.8. What is the difference between standard- and hidden mode?	10
1.3.9. What is the CC Alias feature, and why could I need it?	10
1.3.10. How can I process deferred settlement?	10
1.3.11. What is the Post URL?	10
1.3.12. What are merchant specific parameters?	10
<b>1.4. Prerequisites and Restrictions</b>	<b>11</b>
1.4.1. Supported browsers	11
1.4.2. Prerequisites	11
1.4.3. Requirements / restrictions	11
<b>2. TECHNICAL IMPLEMENTATION</b>	<b>12</b>
<b>2.1. Standard Mode</b>	<b>12</b>
2.1.1. Payment page standard mode	12
2.1.2. Response	13
2.1.3. Deferred settlement	13
<b>2.2. Hidden Mode</b>	<b>14</b>
2.2.1. Payment page hidden mode	14
2.2.2. Response	16
2.2.3. Deferred settlement	16
<b>2.3. Security Options</b>	<b>17</b>
2.3.1. Data transfer encryption	17
2.3.2. Digital signature	17
2.3.3. Anti Fraud Data Management	18
<b>2.4. Transaction Response</b>	<b>19</b>
2.4.1. Return parameters	19
2.4.2. Payment page response codes	22
<b>2.5. XML Settlement</b>	<b>23</b>
2.5.1. XML settlement debit / credit request	23
2.5.2. XML settlement response	24

2.5.3.	XML message samples .....	24
2.5.4.	DTD .....	26
<b>3.</b>	<b>TEST PROCEDURE.....</b>	<b>27</b>
<b>3.1.</b>	<b>Offline Authorisation .....</b>	<b>27</b>
<b>4.</b>	<b>INDEX.....</b>	<b>28</b>

## 1. Introduction

### 1.1. Datatrans Payment Process



#### 1.1.1. Role of the PSP

In order to offer to the customer one or more payment methods e-commerce merchants need to choose a PSP. The assignment of a PSP is required for the following reasons:

A PSP...

- ...enables the processing of various payment methods with one unified e-commerce shop interface
- ...provides reporting tools for payment data analysis and reconciliation
- ...ensures that the e-commerce merchant complies with the security regulations of the major credit card organisations

The payment interface by Datatrans supports all levels of complexity an e-commerce business can possibly comprehend.

## 1.1.2. Authorisation

Datatrans offers the following authorisation interfaces:

- **Datatrans Mail / Phone Tool** ([www.datatrans.biz/pronto](http://www.datatrans.biz/pronto)); for mail / phone order business only; does only support credit cards
- **Datatrans E-Com [Payment Page](#)**; for standard and secure e-commerce contracts
- **Datatrans E-Com XML authorisation**; for phone / mail order business only; does only support credit cards; for details please contact the Datarans support team.

All authorisation interfaces offer as an option direct debit functionality. In this case transactions are automatically settled after the successful authorisation process.

## 1.1.3. Settlement

The settlement process is only required if the merchant chooses deferred settlement. Only successfully authorised transactions can be settled. Datatrans offers the following settlement interfaces:

- **Datatrans Back Office Tool**
- **Datatrans E-Com [XML Settlement](#)**

Both interfaces support all payment methods and contract types offered by Datatrans.

## 1.1.4. Reconciliation / data consolidation

We suggest to use the following tools and reports for payment **reconciliation**:

- **Electronic Transaction Report**; offered by Datatrans; available by e-mail or FTP; for details please refer to the Datatrans support team
- **Summarised or itemised payment statement**; offered by all acquirers; available on paper or as PDF file by e-mail
- **Electronic Payment Advice (EPA)**; offered by most of the credit card acquirers; fixed length text files downloadable via FTP; for details please refer to your acquirer
- **Matchbox**; tool for automated matching of EPA files with the merchants receivables; this tool is offered by Treibauf AG; for details please refer to [www.treibauf.ch](http://www.treibauf.ch).

## 1.2. Payment Methods

### 1.2.1. Credit Cards

#### Credit card brands and acquirers

Credit Cards are the most popular of all payment methods in the Internet. Datatrans supports the following credit card brands and acquirers:

Brand	Acquirers supported by Datatrans
Mastercard	Telekurs Multipay (CH), Aduno (CH), B+S Card Services (DE), ConCardis (DE)
Visa	Telekurs Multipay (CH), Aduno (CH), B+S Card Services (DE), ConCardis (DE)
American Express	Swisscard AECS (CH), American Express (DE)
Diners	Diners Club (CH)
JCB	JCB (CH)
Visa Purchasing	UBS Card Center (CH)

For contact details of the acquirer banks mentioned above please refer to [www.datatrans.ch](http://www.datatrans.ch) → "Partners" → "Financial Institutions".

#### Credit card contract types

In order to be able to process credit card transactions a merchant first of all needs a credit card contract with one or more **acquirer banks** (in this document referred to as **acquirer**). The acquirer is the link between the merchant's bank account and the **credit card issuer** (in this document referred to as **issuer**). The acquirers offer the following contract types:

- **Card Present**; used in shops with physical Point of Sales (POS) systems; the card has to be read with a card reader, the cardholder has to sign the credit card slip; good protection against **charge-back**; the issuer has the liability.
- **Mail / Phone Order (MPO)**; used for mail-order business (order by phone, mail or fax. ; limited charge-back protection; the acquirer has the liability
- **Standard Internet (IET)**; used for e-commerce; limited charge-back protection; the acquirer has the liability
- **3D Secure (SEC)**; used for e-commerce; good protection against charge-back; the issuer has the liability

#### Payment process

Basically, credit card transactions are always split into **authorisation** and **settlement**. The following parameters are checked with the authorisation:

- **BIN** and checksum (**LUHN check**)
- status of the card (ok or blocked)
- monthly allowance of the cardholder (monthly limit)
- CVV or CVC (Card Verification Code or Card Verification Value); last three digits in the signature field on the back of the credit card

With the authorisation the monthly allowance of the cardholder is reduced by the authorised amount, no matter whether the transaction will be settled later on or not. The authorised amount is reserved for the merchant and should be settled within 10 days. The issuer returns an authorisation code which serves as the reference of the authorisation.

Once a transaction has been successfully authorised it can be settled. *Important: the cardholder will not be charged without **settlement!*** Authorisation and settlement can be processed in one step (direct debit) or as two separate tasks (deferred settlement).

## 3D Secure (Verified by Visa, MasterCard SecureCode)

3D Secure is a security standard introduced by Visa and Mastercard in order to protect cardholders and merchants against any kind unauthorised use of credit cards. If a merchant has a 3D Secure (SEC) contract the liability shifts from the acquirer to the issuer, no matter if the cardholder is 3D secure enrolled or not. If the cardholder is 3D secure enrolled he is redirected to a dedicated web page of his issuer where he has to enter a password for authentication. For more details please refer to one of the following links:

Verified by Visa: [www.verifiedbyvisa.com](http://www.verifiedbyvisa.com)  
MasterCard SecureCode: [www.mastercardmerchant.com/securecode/](http://www.mastercardmerchant.com/securecode/).

## Security regulations (AIS / SDP)

Visa and Mastercard do no longer allow the storage of credit card details by merchants or **payment service providers** (PSP) unless they pass an extensive security assessment. For details please refer to [www.visaeurope.com/acceptingvisa/ais.html](http://www.visaeurope.com/acceptingvisa/ais.html).

## **1.2.2. Swiss Postfinance**

### Payment methods

Postfinance offers the following payment methods:

- **Debit Direct** (Postcard)
- **Yellownet**
- Yellowbill

For details about these payment methods please refer to [www.yellowpay.ch](http://www.yellowpay.ch).

The Datatrans payment interface offers Debit Direct and Yellownet. The Postfinance payment methods can be processed like credit cards. Authorisation and settlement can either be split, or they can be done in one single step. Both, Debit Direct and Yellownet, offer guaranteed payment upon successful authorisation.

For signing up a Postfinance contract please send an e-mail to [merchanthelp@postfinance.ch](mailto:merchanthelp@postfinance.ch).

## **1.2.3. Loyalty Cards**

The Datatrans payment application supports **Jelmoli Bonus Card** and **Manor MyOne Card**. These payment methods can be processed like credit cards. Loyalty Cards can only be accepted by partners of Jelmoli or Manor.

## **1.2.4. Swisscom Click & Buy**

“Click & Buy” offers invoicing to the monthly phone bill by Swisscom Fixnet. It is currently only available with “rectype” CAA (direct debit). Deferred settlement will be available in Q4 2006.

## **1.3. Planning / Concept of Payment Integration**

The planning of the payment process should start by answering the following questions:

### **1.3.1. Which payment methods do I want to offer to my customers?**

The most common payment method in the e-commerce world is the credit card. It is appropriate for medium and high amounts. For the Swiss local market the Swiss Postfinance payment methods are very popular, too. For transactions with small amounts (**micro billing**) we recommend Swisscom Click & Buy

### **1.3.2. Which acquirer contract types do I need?**

If I am only selling via the Internet I just need a Secure E-Commerce Contract (SEC). Important: SEC contracts require that the merchant is present during the transaction because he might have to enter his 3D Secure password. Therefore, if I also accept orders by mail or phone, or if I do recurring billing, I need Mail / Phone contracts (MPO), too.

### **1.3.3. Do I want to offer local currencies to my customers?**

If yes, please arrange according contracts with your acquirers. Datatrans supports all currencies offered by the acquirers.

### **1.3.4. How do I avoid fraud?**

If I accept Visa and Mastercard, fraud is no longer an issue like it was in the past because the merchants normally have 3D Secure contracts nowadays. Nevertheless, we strongly recommend to check the CVV code, too, because many card issuers and acquirers do no longer authorise transactions without it. As with all other credit card brands the liability shift does not apply, fraud prevention should be taken into consideration. We recommend the following fraud prevention measures:

- check of CVV / CVC
- limitation of maximum amount and / or maximum transactions per day and cardholder (offered by Datatrans)
- limitation of maximum amount and / or maximum transactions per day and IP address (will be offered by Datatrans soon)
- limitation of maximum amount and / or maximum transactions per day and origin IP address (will be offered by Datatrans soon)
- Black list with credit card number ranges and individual card numbers (will be offered by Datatrans soon)

### **1.3.5. How do I avoid erroneous transactions, i.e. double bookings?**

The most common case of erroneous transactions are double bookings. As the e-commerce shop application is forwarding the customer to the payment page of Datatrans it loses control about the payment process. If the customer's browser session stops or hangs for any reason during the payment it can occur that his credit card is charged, but the e-shop does not get the success message and therefore, the merchant does not fulfil the order. Another case could be that a smart customer sends a fake HTTPS post form to Datatrans with an invalid amount. This kind of problems can be avoided as follows:

- split of authorisation and settlement (deferred settlement)
- storing / registration of the order before the start of the payment process; generation of a discrepancy report with all transactions which did not complete the payment process
- use of the "sign" parameter (see [technical specifications](#) for details); avoids modified or fake HTTPS post forms
- use of the [Post URL](#); provides feedback from the Datatrans payment gateway even if the customer's browser session has been terminated
- daily check / match of processed transactions (see chapter "Reconciliation")

## 1.3.6. How will I match the bank payments with my receivables?

As a merchant I have to decide how I will compare the bank payments with the actually processed transactions. This task is absolutely essential, and it has to be done on daily bases. It helps to discover missing or erroneous transactions in time, and it can prevent major damage in the beginning.

For details please refer to the chapter "Reconciliation / Data Consolidation".

## 1.3.7. Do I need 3D Secure?

Datatrans features a certified 3D Secure interface which is fully included into the payment process. It is available in standard- and hidden mode. There is no additional implementation work required. Our payment application automatically determines whether the customer has a 3D Secure enrolled card or not. If yes, the payment application automatically opens the 3D Secure authentication page of the card issuer.

## 1.3.8. What is the difference between standard- and hidden mode?

In [standard mode](#) the consumer is forwarded to the Datatrans payment page. There he selects the payment method and enters his card or account details.

In [hidden mode](#) most of the payment details including credit card number are collected with a form which is part of the e-shop's checkout page. The Datatrans payment page is not visible. Only the Datatrans process page is visible during the authorisation and, if applicable, the 3D Secure authentication. However, the process page is fully customisable. In hidden mode, the consumer is not aware that he is redirected to the Datatrans host.

## 1.3.9. What is the CC Alias feature, and why could I need it?

With the Datatrans payment application the merchant has the option to add credit card information to his customer profiles without offending against the data security regulations of Mastercard and Visa (PCI). This can be achieved by using the credit card alias ([CC Alias](#)) feature offered by Datatrans. The CC Alias is generated with the authorisation process. The e-commerce application of the merchant submits the card number and gets back a numeric value which can be added to the customer profile.

## 1.3.10. How can I process deferred settlement?

As mentioned earlier in this document [authorisation](#) and [settlement](#) can be processed separately. The authorisation has to be submitted to the payment page. With deferred settlement the transactions can be submitted for payment (settled) manually with the Datatrans back office tool ([www.datatrans.biz/pronto](http://www.datatrans.biz/pronto)) or automatically with the [XML interface](#). For details about the XML settlement please refer to the detailed specifications later in this document.

**Note: Transactions have to be settled within 30 days after the authorisation**

## 1.3.11. What is the Post URL?

This feature guaranties that the shop application gets the actual status of all transactions even if the consumer cancels the browser session while the payment process is running. For details about the Post URL please refer to the detailed specifications in chapter "[Technical Implementation](#)".

## 1.3.12. What are merchant specific parameters?

The merchant can invent and submit own parameters. These parameters are returned to the Success-, Error- and Post URL.

## **1.4. Prerequisites and Restrictions**

### **1.4.1. Supported browsers**

"E-Com" supports all common browsers; Exception: The Postfinance payment methods can't be processed with Opera

### **1.4.2. Prerequisites**

The following is required for payment processing with Datatrans "E-Com":

- Valid contracts with one or more acquirers
- Processing contract with Datatrans (for details please refer to [www.datatrans.ch](http://www.datatrans.ch))

### **1.4.3. Requirements / restrictions**

- Datatrans reserves the right to add new return parameters and response codes without notification; any merchant application has to ignore undocumented fields and response codes; Existing parameters and response codes will not be changed
- For hidden mode only: valid SSL certificate issued by a trusted authority
- The XML authorisation interface must not be used for e-commerce; it does not support 3D Secure, and it is not compliant with the security regulations for e-commerce by Mastercard and Visa
- The payment methods by Swiss Postfinance as well as Swisscom Click & Buy and PayPal can be processed in hidden mode, too; however, the payment details have to be entered into a popup window from the provider of the payment method.
- Authorised transactions have to be settled within 30 days
- If the payment page is launched in a frame the minimum size must be 390 by 400 pixels in order to show the 3D Secure password entry screen

## 2. Technical Implementation

### 2.1. Standard Mode

#### 2.1.1. Payment page standard mode

##### Authorisation

The UPP interface directs the consumer to the URL of the service provider and posts the parameters. The final payment transaction response reaches the merchant in two ways:

- The consumer is directed (with posted parameters) back to the merchant (to the URL of his choice).
- Parallel to the call of merchant's web page, the transaction response is directly sent to the server application of the merchant (to the URL of his choice, see parameter "Post URL").

Starting the payment service, the merchant's application directs the consumer to the service URL (e.g. form action) and passes all mandatory and selected optional parameters to the service.

Example:

```
<FORM NAME="myform" ACTION="https://www.datatrans.biz/upp/jsp/upStart.jsp" METHOD="post">

<INPUT TYPE=HIDDEN NAME="merchantId" VALUE="999999999">
<INPUT TYPE=HIDDEN NAME="refno" VALUE="123456">

etc.
```

Once the transaction is completed, the consumer is directed back to the **return address** of the shop application.

##### **Service URLs:**

- UTF-8 encoding: <https://www.datatrans.biz/upp/jsp/upStart.jsp>
- ISO encoding: <https://www.datatrans.biz/upp/jsp/upStartIso.jsp>

##### *Description of payment interface parameters*

Note: all parameters are case specific

**Mandatory parameters** to be submitted with each transaction::

- **merchantId** (AN 18)  
Unique Merchant Identifier  
(assigned by Datatrans)
- **amount** (N 15)  
Transaction amount in cents
- **currency** (A 3)  
Transaction currency – ISO Character Code (CHF, USD, EUR etc.)
- **refno** (AN 18)  
Merchant reference number

## Other mandatory parameters:

The following parameters have to be either submitted with each transaction or configured / preset in the merchant administration tool [www.datatrans.biz/upp](http://www.datatrans.biz/upp):

Return addresses

- **successUrl**  
This parameter represents the URL of the merchant's shop application, where the consumer should be redirected to after a successful transaction
- **errorUrl**  
This parameter represents the URL of the merchant's shop application, where the consumer should be redirected to after a failed transaction
- **cancelUrl**  
This parameter represents the URL of the merchant's shop application, where the consumer should be redirected to after canceling the payment dialog

## Optional parameters:

- **language** (AN 2)  
This parameter specifies the language (language code) in which the payment page should be presented to the cardholder.  
The following ISO-639 2 character language codes are supported:
  - de (German)
  - en (English)
  - fr (French)
- **reqtype**  
The request type specifies whether the transaction has to be immediately **settled** or **authorised** only. There are two request types available:
  - NOA        authorisation only
  - CAA        authorisation with immediate settlement, if the transaction is authorised
- **sign**  
This parameter may be used according to the merchant's security level settings. For details please refer to the chapter "Security Option".
- **PostURL**  
This parameter can't be passed with the HTTPS Post message; it has to be configured in [www.datatrans.biz/upp](http://www.datatrans.biz/upp). For further details please refer to chapter "[Post URL Feedback](#)".
- **Merchant Specific Parameters**  
The merchant can invent and submit any number of own parameters. These parameters are returned to the Success-, Error- and Post URL.  
Restrictions:
  - The maximum length is limited to 300 characters
  - Line brakes are not allowed
  - Merchant specific parameters are not returned to the Post URL with Postfinance transactions

## 2.1.2. Response

Please refer to chapter "[Transaction response](#)"

## 2.1.3. Deferred settlement

Please refer to chapter "[XML Settlement](#)"

## 2.2. Hidden Mode

### 2.2.1. Payment page hidden mode

#### Authorisation

The UPP interface directs the consumer to the URL of the service provider and posts the parameters. The final payment transaction response reaches the merchant in two ways:

- The consumer is directed (with posted parameters) back to the merchant (to the URL of his choice).
- Parallel to the call of merchant's web page, the transaction response is directly sent to the server application of the merchant (to the URL of his choice, see parameter "Post URL").

Starting the payment service, the merchant's application directs the consumer to the service URL /upp/jsp/pStart.jsp (e.g. form action) and passes all mandatory and selected optional parameters to the service.

Example:

```
<FORM NAME="myform" ACTION="https://www.datatrans.biz/upp/jsp/upStart.jsp" METHOD="post">

<INPUT TYPE=HIDDEN NAME="merchantId" VALUE="99999999">
<INPUT TYPE=HIDDEN NAME="refno" VALUE="123456">

etc.
```

Once the transaction is completed, the consumer is directed back to the **return address** of the shop application.

**Important: In hidden mode the payment process has to be started from a visible frame!**

#### Service URLs:

- UTF-8 encoding: <https://www.datatrans.biz/upp/jsp/upStart.jsp>
- ISO encoding: <https://www.datatrans.biz/upp/jsp/upStartIso.jsp>

#### *Description of payment interface parameters*

Note: all parameters are case specific

Mandatory parameters to be submitted with each transaction::

- **merchantId** (AN 18)  
Unique Merchant Identifier  
(assigned by Datatrans)
- **amount** (N 15)  
Transaction amount in cents
- **currency** (A 3)  
Transaction currency – ISO Character Code (CHF, USD, EUR etc.)
- **refno** (AN 18)  
Merchant reference number

Other mandatory parameters:

The following parameters have to be either submitted with each transaction or configured / preset in the merchant administration tool [www.datatrans.biz/upp](http://www.datatrans.biz/upp):

- **successUrl**  
This parameter represents the URL of the merchant's shop application, where the consumer should be redirected to after a successful transaction
- **errorUrl**  
This parameter represents the URL of the merchant's shop application, where the consumer should be redirected to after a failed transaction
- **cancelUrl**  
This parameter represents the URL of the merchant's shop application, where the consumer should be redirected to after canceling the payment dialog

Parameters required for Hidden Mode:

- **paymentmethod**  
Parameter Values:  
VIS - VISA  
ECA - Mastercard  
AMX - American Express  
DIN - Diners Club  
POS - Swiss Post Yellow Account  
CLB - Swisscom Click & Buy (currently "reqtype" CAA only)  
PAP - PayPal
- **cardno** or **aliasCC**  
Credit card number or credit card number alias; required for credit card transactions only
- **expm** (MM)  
Expiry month of the card; required for credit card transactions only
- **expy** (YY)  
Expiry year of the card; required for credit card transactions only

Optional parameters:

- **cvv** (N3)  
CVV Code  
Important: in hidden mode the CVV has to be disabled in the payment page admin tool ([www.datatrans.biz/upp](http://www.datatrans.biz/upp)) even if it is submitted! It will be validated online anyway.
- **useAlias**  
Requests the CC Alias; this option needs to be activated by Datatrans; value: yes
- **testOnly**  
Values:  
- yes (loop-back mode)  
- no (production, same meaning as no parameter)  
This parameter should only be used for presentation purposes as it avoids the validation of the input data. For details please refer to chapter "[Test Procedures](#)"
- **language** (AN 2)  
This parameter specifies the language (language code) in which the payment page should be presented to the cardholder.  
The following ISO-639 2 character language codes are supported:  
- de (German)  
- en (English)  
- fr (French)

- **reqtype**  
The request type specifies whether the transaction has to be immediately **settled** or **authorised** only. There are two request types available:
  - NOA           authorisation only
  - CAA           authorisation with immediate settlement, if the transaction is authorised
- **sign**  
This parameter may be used according to the merchant's security level settings. For details please refer to the chapter "Security Option".

## **2.2.2. Response**

Please refer to chapter "[Transaction response](#)"

## **2.2.3. Deferred settlement**

Please refer to chapter "[XML Settlement](#)"

## 2.3. Security Options

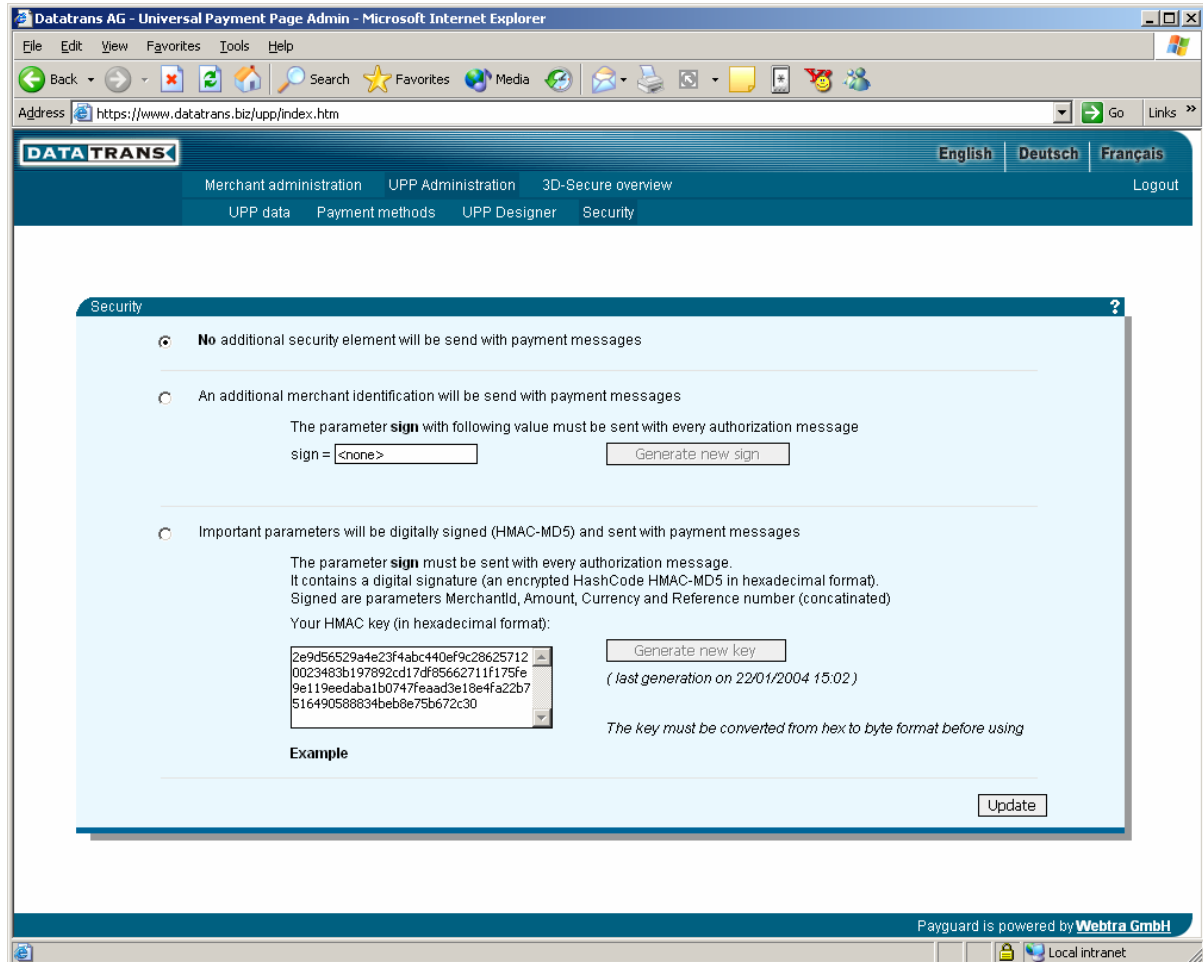
### 2.3.1. Data transfer encryption

The entire data transfer between the merchant's shop application and the Datatrans payment application is secured by the secure SSL protocol.

### 2.3.2. Digital signature

The security elements are described on [www.datatrans.biz/upp](http://www.datatrans.biz/upp). However, this description is only visible if the parameter "sign" has been enabled by Datatrans.

Web page (part of administration tool, if enabled) with description of security features:



Note: With the activation of the security feature the request parameter "sign" becomes mandatory!

#### Security level 0

The data transmission is not secured.

#### Security level 1

The data transmission is secured by sending of the parameter sign, which must contain a merchant-specific control value (constant). This value is generated in the merchant administration tool [www.datatrans.biz/upp](http://www.datatrans.biz/upp). Note that with every change of this value (which is possible at any time), the interface accepts the current value only!

## Security level 2

The data transmission is secured by sending the parameter sign, which must contain a digital signature generated by a standard HMAC-MD5 hash procedure and using a merchant-specific encryption key. The HMAC key is generated by the system and can be changed at any time in the merchant administration tool [www.datatrans.biz/upp](http://www.datatrans.biz/upp). Note that with every change of the key, the interface accepts signature based on the current key only!

Note too that the key is delivered in hexadecimal format, and it should also be stored in this format. But before its usage the key must be translated into byte format!

Creation of the digital signature (value of parameter sign) in the request:

- translate HMAC key from hex to byte format
- create string to be signed by concatenating of parameters merchantId + amount + currency + refno, in exactly this order and without separators
- sign the string using HMAC-MD5 procedure based on merchant's HMAC key
- translate signature from byte to hex format and associate it as value with parameter sign

The system signs the response similarly to the way the merchant does. It passes the signature back to the merchant in parameter "sign2", which is created in the same way as the parameter sign. There is one difference: the signed string contains the parameter "uppTransactionId" instead of the reference number "refno". We recommend to check the response signature.

For an even higher security level, it's now also possible to generate **an alternative key for the "sign2" parameter**. With this feature "sign2" is created with a different parameter. To enable it the option "Use another key for sign2 generation" has to be activated in UPP Admin under "Security".

As an option it is now also possible **to sign XML settlements**. To enable this feature in UPP Admin, go to "Security" and activate "Use signature also with settlements". IMPORTANT: Once the signature validation for settlement is activated, the parameter "sign" will be validated with each XML settlement request.

### 2.3.3. Anti Fraud Data Management

Datatrans offers various fraud prevention options:

- **Exclusion of card numbers or card number ranges;** to be configured in [www.datatrans.biz/upp](http://www.datatrans.biz/upp) under "UPP Administration" / "Anti Fraud Data Management"; card numbers or card number ranges can be entered manually or imported from a text file.  
Text file format: [CC\_from]; [CC\_to]; [Description]
- **Exclusion of IP addresses or IP address ranges;** to be configured in [www.datatrans.biz/upp](http://www.datatrans.biz/upp) under "UPP Administration" / "Anti Fraud Data Management"; IP addresses or IP address ranges can be entered manually or imported from a text file.  
Text file format: [CC\_from]; [CC\_to]; [Description]
- **Maximum settlement amount per card number, merchant, and day;** available upon request to [support@datatrans.ch](mailto:support@datatrans.ch)
- **Maximum number of transactions per card number, merchant, and day;** available upon request to [support@datatrans.ch](mailto:support@datatrans.ch)

## 2.4. Transaction Response

### 2.4.1. Return parameters

#### Successful Authorisation (Direct debit)

This response is sent concurrently to the successUrl and the postUrl, which are provided by the merchant.

- **uppTransactionId**  
Unique transaction identifier (N-18)
- **authorizationCode**  
Transaction authorization code (N-9)
- **responseMessage**  
Response message text (e.g. TRX AUTHORISED) (AN-100)
- **refno**  
Merchant unique order reference number (AN-18)
- **amount**  
Transaction amount in units/cents (123.50 = 12350) (N-15)
- **currency**  
Transaction currency (AN-3)
- **pmethod**  
The payment method by which the transaction has been made (e.g. VIS, ECA,...) (AN-10)
- **reqtype**  
NOA or CAA (AN-5)
- **acqAuthorizationCode**  
Authorization code returned by credit card issuing bank (AN 7)
- **status**  
success
- **uppMsgType**  
Web
- **aliasCC (hidden mode only)**  
alias of Credit Card Number (N-18) - optional
- **maskedCC (hidden mode only)**  
masked Credit Card Number – optional
- **sign2 (only if "sign" has been submitted with authorisation)**  
(see chapter "Security Options")

The service also returns all other merchant parameters sent along with the request.

#### Failed / Unsuccessful Authorisation or Direct debit

This response is sent to errorUrl and postUrl provided by merchant.

- **uppTransactionId**  
Unique transaction identifier (N-18)
- **errorCode**  
Error code (N-4)
- **errorMessage**  
Error response message text (e.g. CARD NUMBER NOT VALID) (AN-100)
- **errorDetail**  
(AN-100)

- **refno**  
Merchant unique order reference number (AN-18)
- **amount**  
transaction amount in units/cents (123.50 = 12350) (N-15)
- **currency**  
Transaction currency (AN-3)
- **pmethod**  
The payment method by which the transaction has been made (e.g. VIS, ECA,...) (AN-10)
- **reqtype**  
NOA or CAA (AN-5)
- **status**  
error
- **uppMsgType**  
Web

The service also returns all other merchant parameters sent along with the request.

## Cancelled Payment Procedure

If the cardholder decides to cancel the payment process and to return to the shop without payment, the response is sent back to cancelUrl.

- **uppTransactionId**  
Unique transaction identifier (N-18)
- **refno**  
Merchant unique order reference number (AN-18)
- **amount**  
Transaction amount in units/cents (123.50 = 12350) (N-15)
- **currency**  
Transaction currency (AN-3)
- **status**  
cancel
- **uppMsgType**  
Web

## PostURL Feedback

A merchant can collect all transactions (either successful or failed) on data-oriented PostURL. This PostURL is used for faceless (server to server) data communication. Note that for security reasons the Post URL cannot be submitted as a parameter. It has to be configured in the merchant's administration tool ([www.datatrans.biz/upp](http://www.datatrans.biz/upp)).

The Merchant can choose one of the following options (according to the PostType setting in [www.datatrans.biz/upp](http://www.datatrans.biz/upp)):

- Get pure XML data
- Get posted HTML form with all necessary parameters posted into the request.

Returned parameters:

- **uppTransactionId**  
Transaction ID
- **amount**  
Amount
- **currency**  
Currency
- **refno**  
Reference number
- **pmethod**  
Payment method
- **reqtype**  
Request type
- **language**  
Language
- **status**  
Status
- **uppMsgType**  
Type of message (post)

Success case only:

- **responseMessage**  
Response message
- **authorizationCode**  
Authorization Code
- **acqAuthorizationCode**  
Acquirer Authorization Code

Error case only:

- **errorCode**  
Error Code
- **errorMessage**  
Error Message
- **errorDetail**  
Error Detail

Optional:

- **aliasCC**  
Alias of CC Number
- **maskedCC**  
Masked CC Number
- **Merchant specific parameters**  
all parameters that were included in the initial request

## 2.4.2. Payment page response codes

Error Code	Code Message	Error Detail:
1001	Missing required parameter	Name of missing parameter
1002	Not valid parameter format	Name of wrong parameter
1003	Value of parameter not found	Name of field for which there is no record in UPP system (e.g. unknown merchantId)
1201	System error	Detail specification
1400	Invalid card number	Detail specification
1401	Invalid expiration date	Detail specification
1402	Expired card	Detail specification
1403	Transaction declined by card issuer	Detail specification
1404	Card blocked	Detail specification
1405	Amount exceeded	Detail specification
-888	CC-alias error	CC-alias not found
3000	Denied by fraud management	Card or IP address blocked by merchant

## 2.5. XML Settlement

### 2.5.1. XML settlement debit / credit request

#### Process overview

This interface can be used for the settlement of authorised transactions and for credit notes of settled debit transactions. Transactions due for settlement can be sent as a formatted XML message via an https request to the Datatrans payment application. After the validation of the XML message the merchant application receives back a status response. The settlement procedure is then performed by the payment application. The merchant gets back an XML-formatted message containing all necessary data about the settled transactions.

#### XML connection

The merchant application directly connects (server to server via standard socket) to the service URL [http://www.datatrans.biz/upp/jsp/XML\\_processor.jsp](http://www.datatrans.biz/upp/jsp/XML_processor.jsp), writes the XML document into this connection and reads the XML response documents from there.

#### Mandatory parameters

- **merchantId**  
Unique Merchant Identifier (allocated by Datatrans at merchant registration process) (AN-18)
- **amount**  
Transaction amount in cents (123.50 = 12350) (N-15)  
*Must not exceed the authorised amount!*
- **currency**  
Transaction currency - ISO character code (CHF) (A-3)
- **refno**  
Merchant unique order reference number (AN-18)  
*Must be the same value as submitted with the authorisation request!*
- **authorizationCode**  
Unique authorization code returned by the Datatrans payment application during authorization procedure (N-18)  
*Must be the same value as submitted with the authorisation request!*
- **pmethod**  
required for PostFinance (value POS) settlement request only (optional for all other payment methods)

#### Optional Parameters

- **reqtype**  
Supported values:  
COA - Settlement debit (transtype 05 required) DEFAULT  
COA - Settlement credit (transtype 06 required)  
STA - Transaction status request  
  
STAReturns status of specified transaction. Required parameters are the same as in case of settlement request. See response codes below.
- **transtype**  
Supported values:  
05 - debit transaction (DEFAULT)  
06 - credit transaction

Note that all parameters marked as DEFAULT are set with the corresponding default value if they are not present or no value is set.

## 2.5.2. XML settlement response

### XML Settlement response parameters

The response XML document contains the same parameters as the request document.

Additional parameters returned upon successful authorisation:

- **responseCode**  
Settlement response code
- **responseMessage**  
Settlement response message text
- **uppTransactionId**  
Original trxId (only for credit transactions)
- **authorizationCode**  
Original authorisation code (only for credit transactions)
- **acqAuthorizationCode**  
Original acquirer's authorisation code returned by acquirer (only for credit transactions)

### XML settlement restrictions:

#### **PostFinance**

(Payment method=POS); Credit transactions are not supported

### XML settlement error codes

Error Code	Code Message	In parameter Error Detail see for:
2001	Input document missing	Name of missing element
2002	Error building document	Document is not well formed XML document
2011	Root element invalid	Unexpected root element of XML document
2012	Body element missing	
2013	merchantId missing	Attribute 'merchantId' in body element missing
2021	Missing value	Name of element, where value is missing
2022	Invalid value	Name of element that contains invalid value

### XML status request (STA) response codes

Response Code	Description
1	Trx ready for settlement (trx authorized)
2	Trx debit waiting for daily settlement process
3	Trx credit waiting for daily settlement process
4	Trx declined or other error
5	Trx in referral status
9	Out of Life Span, Trx in Status 1,5,6,7,8 are automatically archived after 30 days
20	UPP Record not found
21	Trx already settled, return \$BAN = BatchNumber;\$BAD = BatchDate

## 2.5.3. XML message samples

### Settlement request

```
<?xml version="1.0" encoding="UTF-8" ?>
<paymentService version="1">
```

```
<body merchantId="1000011011" testOnly="yes">
  <transaction refno="1234987">
    <request>
      <amount>100</amount>
      <currency>CHF</currency>
      <authorizationCode>332441357</authorizationCode>
    </request>
  </transaction>
</body>
</paymentService>
```

## Settlement response

```
<paymentService version="1">
  <body merchantId="1000011011" testOnly="yes" status="accepted">
    <transaction refno="1234987" trxStatus="response">
      <request>
        <amount>100</amount>
        <currency>CHF</currency>
        <authorizationCode>332441357</authorizationCode>
        <reqtype>COA</reqtype>
        <transtype>05</transtype>
      </request>
      <response>
        <responseCode>01</responseCode>
        <responseMessage>TRX ACCEPTED</responseMessage>
      </response>
    </transaction>
  </body>
</paymentService>
```

## 2.5.4. DTD

### Settlement request

```
<!-- UPP settlement request -->
<!ELEMENT paymentService (body)>
<!ATTLIST paymentService version NMTOKEN #REQUIRED>
<!ELEMENT body (transaction+)>
<!ATTLIST body merchantId NMTOKEN #REQUIRED testOnly (yes|no) "no">
<!ELEMENT transaction (request)>
<!ATTLIST transaction refno NMTOKEN #REQUIRED>
<!ELEMENT request (amount, currency, authorizationCode, reqtype?, transtype?, pmethod?)>
<!ELEMENT amount (#PCDATA)>
<!ELEMENT currency (#PCDATA)>
<!ELEMENT authorizationCode (#PCDATA)>
<!ELEMENT reqtype (#PCDATA)>
<!ELEMENT transtype (#PCDATA)>
<!ELEMENT pmethod (#PCDATA)>
```

### Settlement response

```
<!-- UPP settlement response -->
<!ELEMENT paymentService (body)>
<!ATTLIST paymentService version NMTOKEN #REQUIRED>
<!ELEMENT body (transaction+,error?)>
<!ATTLIST body merchantId NMTOKEN #REQUIRED testOnly (yes|no) "no" status (accepted|error) #REQUIRED>
<!ELEMENT transaction (request,(response|error?))>
<!ATTLIST transaction refno NMTOKEN #REQUIRED trxStatus (response|error) #REQUIRED>
<!ELEMENT request (amount,currency,authorizationCode,reqtype?,transtype?,pmethod?)>
<!ELEMENT amount (#PCDATA)>
<!ELEMENT currency (#PCDATA)>
<!ELEMENT authorizationCode (#PCDATA)>
<!ELEMENT reqtype (#PCDATA)>
<!ELEMENT transtype (#PCDATA)>
<!ELEMENT pmethod (#PCDATA)>
<!ELEMENT response (responseCode,responseMessage,uppTransactionId?,authorizationCode?,
    acqAuthorizationCode?)>
<!ELEMENT responseCode (#PCDATA)>
<!ELEMENT responseMessage (#PCDATA)>
<!ELEMENT uppTransactionId (#PCDATA)>
<!ELEMENT authorizationCode (#PCDATA)>
<!ELEMENT acqAuthorizationCode (#PCDATA)>
<!ELEMENT error (errorCode, errorMessage, errorDetail)>
<!ELEMENT errorCode (#PCDATA)>
<!ELEMENT errorMessage (#PCDATA)>
<!ELEMENT errorDetail (#PCDATA)>
```

### 3. Test Procedure

#### 3.1. Offline Authorisation

##### Description, purpose

The offline authorisation allows a full test of all parameters and functionalities. Transactions can be authorised via UPP and settled via the XML interface. All payment information is visible in [www.datatrans.biz/pronto](http://www.datatrans.biz/pronto). However, as the default test merchant ID 1000011011 is shared by all developers in test stage it is important to use a unique reference number ("refno"). This allows to identify the transaction later. In order to test the error handling of the e-shop application the developer has to use our test card numbers which create dedicated error message depending on the authorized amount:

- Amex: 3758 1111 1111 115
- EC/MC: 5404 0000 0000 0001
- Visa: 4242 4242 4242 4242

Error messages based on transaction amounts:

Amount / amount range	Error message
< 90.--	Transaction authorised
90.-- - 100.--	Transaction declined (i.e. insufficient limit, bad expiry Date)
> 100.00	Card blocked (lost or stolen)

An error can also be created by using an expiry date which is more than 2 years in the past.

The following cards generate the message "Transaction authorised" without verification of the amount:

- Amex: 3750 0000 0000 007
- EC/MC: 5200 0000 0000 0007
- Visa: 4900 0000 0000 0003

The expiry date of all test cards must be in the presence or future.

**Note that these card numbers only work in our test environment! Productive cards can no longer be processed on the test account.**

##### Configuration

- don't use parameter "testOnly"
- merchant ID must be set to 1000011011 (test merchant)

##### Restrictions

The following features can't be tested or simulated using the default test merchant ID 1000011011:

- Post URL
- "sign" parameter
- Individual design of the payment- or process page

These features require access to the technical administration tool [www.datatrans.biz/upp](http://www.datatrans.biz/upp). If you need to implement one of the features which are unavailable on the default test merchant ID please apply for a dedicated test account at [support@datatrans.ch](mailto:support@datatrans.ch). Datatrans will then provide a merchant ID which is dedicated to the merchant for 3 months.

## 4. Index

3D Secure.....	3, 7, 8, 9, 11, 12	Merchant specific parameters .....	14, 23
acquirer.....	3, 6, 7, 8, 9, 25	parameters .....	3, 7, 11, 12, 13, 14, 15, 16, 19, 20, 21, 22, 23, 24, 25, 28
Acquirer .....	23	Parameters .....	14, 16, 24
Alias .....	3, 11, 16, 23	Payment Page.....	1, 6
Click & Buy .....	2, 3, 8, 16	Post URL .....	3, 9, 11, 13, 14, 15, 22, 28
Credit Cards .....	3, 7	Postfinance .....	3, 8, 9, 12, 14
currencies.....	3, 9	PSP .....	3, 5, 8
deferred settlement.....	3, 6, 7, 9, 11	Reconciliation.....	3, 6, 9, 10
Deferred settlement.....	3, 8, 14, 17, 25	Requirements / restrictions .....	3, 12
Digital signature .....	2, 3, 18	response codes .....	2, 3, 12, 23, 24, 25
DTD.....	4, 27	Service URLs .....	13, 15
EasyPay .....	3, 8, 9	Settlement.....	3, 6, 14, 17, 24, 25, 26, 27
erroneous transactions .....	3, 9, 10	sign .....	7, 9, 14, 17, 18, 19, 20, 28
fraud .....	2, 3, 9, 19, 23	standard mode .....	3, 11, 13
Fraud.....	3, 19	Test .....	4, 16, 28
hidden mode.....	3, 11, 12, 15, 16, 20	Transaction response .....	14, 17
ISO encoding.....	2, 13, 15	UTF-8 encoding.....	13, 15
Loyalty Cards.....	3, 8	Visa .....	7, 8, 9, 11, 12, 28
Mail / Phone Tool.....	6	XML.....	2, 3, 4, 6, 11, 12, 14, 17, 19, 22, 24, 25, 26, 28
Mastercard.....	7, 8, 9, 11, 12, 16		
merchant specific parameters .....	3, 11		