Níže uvedená anglická verze textu slouží jen pro základní orientaci v problematice. Vždy je nutné vycházet z oficiálního textu v českém jazyce.

The below English version of the text shall only be used for a basic understanding of the subject matter. The official text in the Czech language is the only binding text.

Elektronická evidence tržeb
Electronic Registration of Sales

Format and structure of registered sale information

Description of the data interface for receipt of registered sale data messages

Version 2.0

Date of last Czech version: 13. 6. 2016

Changes with respect to last published version 1.0)*

Change No	Description
1	A new constraint on financial values was imposed: insignificant leading zeroes and a minus character before zero value are not allowed – see *3.3.3.11 Sale's financial information*
2	A new critical control was added: a maximal size of the registered sale data message (incl. SOAP envelope) cannot exceed 12 kB – see *2.2.3 Critical controls*
3	Two new error messages with codes 7 (the maximal size of the registered sale data message 12 kB was exceeded) and 8 (technical error or data error occured) were added – see *3.5.4 List of error codes and error messages*

)* The table of changes does not describe minor formal text corrections.

Document content

This document provides a description of the data interface for receipt and acknowledgement of data messages containing information on sales which the EET taxpayers are obliged to send for every sale made and subject to registration as per Act no. 112/2016 Coll., on Registration of Sales.

Files containing definition of the XML schema and the Web service (WSDL), which describe the structure of the registered sale data messages and the Web service used to receive them are provided as Annexes to this document.

Table of contents

1 INTRODUCTION

1.1 ABBREVIATIONS

Abbreviation	Definition
BKP	Bezpečnostní kód poplatníka/Taxpayer's Security Code
CRL	Certificate Revocation List
DIČ	Daňové identifikační číslo/Tax identification number
DPH	Daň z přidané hodnoty/Value added tax (VAT)
EET	Elektronická evidence tržeb/Electronic Registration of Sales
FIK	Fiskální identifikační kód/Fiscal Identification Code
GFŘ	Generální finanční ředitelství/General Financial Directorate
PKP	Podpisový kód poplatníka/Taxpayer's Signature Code
SEČ	Central European Time (CET)
SELČ	Central European Summer Time (CEST)
SOAP	Message exchange protocol for XML messages as specified at https://www.w3.org/TR/soap/
WS-security	Web Services Security – extension of the SOAP standard to include WWW services security as specified at http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss
WSDL	Web Services Description Language – a XML-based language for description of functions offered by a WWW service as specified at http://www.w3.org/TR/wsdl
XML Schema	A XML-based language intended for definition of XML document structure as specified at http://www.w3.org/TR/xmlschema11-1/ and https://www.w3.org/TR/xmlschema11-2/
ZoET	Act on Registration of Sales

1.2 TERMINOLOGY

This chapter contains the definition of terminology used in this document.

Term	Definition
Receipt	A receipt is a proof of sale issued (in paper form or electronically) by a taxpayer to a person or entity making a purchase, which contains information on a registered sale defined in the provisions of Section 20 of the Act on Registration of Sales.
E-sale	A data structure in a defined format prescribed by the financial authority, which contains all data on a registered sale as defined in the Act on

Term	Definition
	Registration of Sales and the relevant Ministry of Finance regulations. These are only the data on the sale (SOAP payload), i.e. without the SOAP envelope and its security.
Registered sale data message	A data structure in a defined format prescribed by the financial authority, which contains information about the e-sale and other technical information necessary. This is a complete XML message containing information described in the relevant Web service standards: SOAP/WSDL/WS-Security, etc. A registered sale data message is sent by a cash register to the tax authority's common technical equipment.
Acknowledgement data message	A data structure in a defined format prescribed by the financial authority, which contains the Fiscal Identification Code (FIK) and is used as acknowledgement of receipt and formal correctness)* of the *registered sale data message* sent.
Error data message	A data structure in a defined format prescribed by the financial authority, which contains an error code and its text description as a reaction to *a registered sale data message* received containing critical errors preventing it from being processed, or when another error occurs which prevents the message being processed at the tax authority's side.
Taxpayer's cash register	A device on the taxpayer's side, which sends information on registered sales to the tax authority. This may signify, depending on the context, an end device such as a cash register, or additional SW and HW actually sending the registered sales information. The data messages include an item marked as "Cash register ID", which identifies the end device (cash register). In other parts of the text, this term usually means the end device and the relevant SW and HW sending the data messages.
Registered sale	See Section 4 of the Act on Registration of Sales

)* Formal correctness of a data message means its compliance with the prescribed data structure and fulfilment of all documented critical controls which are a prerequisite for receipt of a registered sale data message, not an actual correctness or accuracy of the relevant registered sale.

2 COMMUNICATION SCENARIO - DATA MESSAGE SENDING

2.1 BASIC COMMUNICATION SCHEME

A cash register device sends individual registered sale data messages to the tax authority's common technical equipment specified by the tax authority. When a registered sale data message sent by the taxpayer's cash register passes the critical controls – see *2.2.3 Critical controls*, the tax authority's common technical equipment immediately creates an *Acknowledgement data message*, which is then sent back to the taxpayer's cash register which sent the original data message.

The communication follows this scenario: *request/response*. The aim of the acknowledgement data message is to acknowledge receipt and formal correctness of the received data message to the taxpayer's cash register. The Acknowledgement data message is linked to the original; data message by the taxpayer's Security Code (BKP) and also by the data message number as assigned by the taxpayer – see 3 *Data message structure* and it also includes the Fiscal Identification Code (FIK), generated by the tax authority's common technical equipment. The FIK is unique for every correctly received registered sale data message.

When a registered sale data message does not pass the critical controls, or a critical fault occurs in the tax authority's common technical equipment which prevents further processing of the message, the taxpayer's cash register which sent the message will be sent am error data message, if that is possible given the fault in question.

The communication scenario is shown on *Fig. 1*.

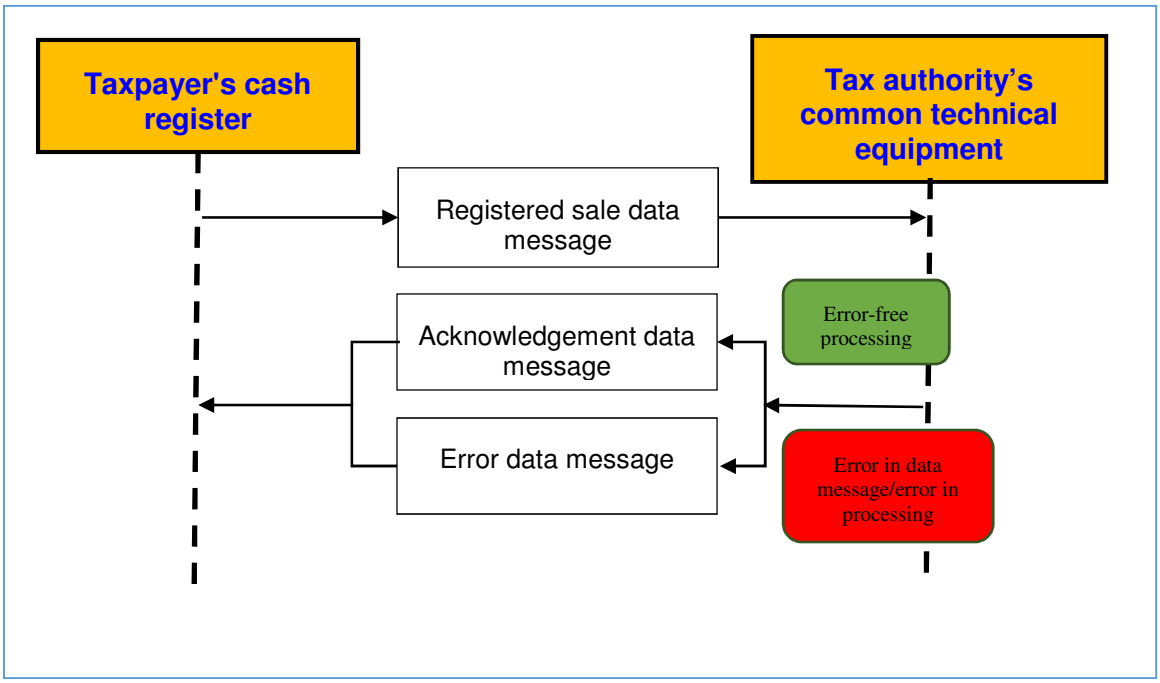

Fig. 1 – Communication scenario

2.2 DATA MESSAGE SENDING MODES, PRODUCTION AND NON-PRODUCTION ENVIRONMENT

2.2.1 Data message sending mode

The EET taxpayers will be able to send a registered sale data message in one of two modes. The required mode is selected by setting the Verification mode flag (*overeni* attribute) in the header of the data message:

- **Operational mode** will be used for regular sending of registered sale data messages and obtaining the FIKs. In the operational mode, the data message's header either does not include the Verification mode of sending flag, or its attribute is set to *false*.

- **Verification mode** will be used by the EET taxpayers to verify correct connection settings and functional connection between the cash register and the EET system. A data message in this mode will include the Verification mode of sending flag with a value of *true*.

2.2.2 Production and non-production environment

The GFŘ will publish Web service addresses for the production environment and one or more non-production environments:

- **Production environment** is intended for the EET taxpayers and will be used for routine operations, i.e. receipt and acknowledgement of data messages containing information on registered sales.

- **Non-production environment (playground)** will be used solely by software developers (developing software for cash registers), not by cash registers' end users. Sending a data message to the non-production environment shall not be considered sending of registered sale information as per Section 18 of the Act on Registration of Sales, i.e. the FIK returned by the non-production environment is not a valid FIK.
  In the non-production environment, digital certificates for cash registers may be issued using a simplified process.

Both environments will be available in operational and verification modes. The following table shows what type of reply will be sent by the EET system based on:

1. The mode in which the data message was sent. The mode is selected by the value of the *overeni* attribute in the *Hlavicka* element in the registered sale data message.

2. The target environment. The environment is selected by the Web service address to which the data message is sent. Addresses for the individual environments will be published by the tax authority.

3. The validity of the data message, i.e. whether or not it contains critical errors.

Registered sale data message mode	Target environment	Use scenario	Validity of the registered sale data message	Response from the EET system
Operational The *Hlavicka* element of the data message **does not** contain the *overeni/verification* attribute, or contains the *overeni="false"* attribute	**Production**	The EET taxpayer uses the data message to send information about a registered sale	Valid	- Acknowledgement data message - The assigned FIK is unique and is a valid FIK - The response contains an electronic signature (signed by a production certificate) - **The registered sale has been received by the EET system)***
			Not valid	- Error data message - Non-zero error code, text description of the error - The response does not contain an electronic signature
	Non-production	A SW developer testing their application in an operational mode	Valid	- Acknowledgement data message - The assigned FIK has a specific value ("-ff" at the end), **but is not valid** - The response includes a non-production environment flag (*test="true"*) - The response contains an electronic signature (signed by a testing certificate)
			Not valid	- Error data message - Non-zero error code, text description of the error - The response includes a non-production environment flag (*test="true"*) - The response does not contain an electronic signature
Verification The *Hlavicka element of the date message* contains the *overeni="true"* attribute	**Production**	The EET taxpayer is verifying the functionality of the connection between their cash register and the EET system	Valid	- Error data message - Error code 0 – i.e. no errors identified - Error description "Datovou zpravu evidovane trzby v overovacim modu se podarilo zpracovat" (The registered sale data message in verification mode was successfully processed) - The response does not contain an electronic signature
			Not valid	- Error data message - Non-zero error code, text description of the error - The response does not contain an electronic signature
	Non-production	A SW developer using their application in the verification mode to test the functionality of the connection between the cash register and the EET system.	Valid	- Error data message - Error code 0 – i.e. no errors identified - Error description "Datovou zpravu evidovane trzby v overovacim modu se podarilo zpracovat" (The registered sale data message in verification mode was successfully processed)The response includes a non-production environment flag (*test="true"*) - The response does not contain an electronic signature
			Not valid	- Error data message - Non-zero error code, text description of the error - The response includes a non-production environment flag (*test="true"*) - The response does not contain an electronic signature
)* in all other cases in this table, the registered sale has not been accepted by the EET system				

Table1: EET system's reply options

2.2.3 Critical controls

Critical controls shall be performed on received registered sales data messages in the EET system. When any of the critical controls return a failure, the registered sale data message shall not be accepted and the FIK shall not be issued.

Upon identifying a critical error, the EET system will return an error data message containing the error's numeric code and its text description – see *3.5.4 List of error codes and error messages*.

When errors which the system can interpret as a cyber attack are identified, the system does not send any response to the client (the taxpayer's cash register).

The critical controls include the following:

- Check of the document's XML formatting – UTF-8 is required
- Check of the individual registered sale data message's XML schema (*.xsd), which contains an exact definition of the data and format structure for the individual data items and a check of presence of individual items
- Check of the size of the registered sale data message (incl. SOAP envelope) which cannot exceed 12 kB
- Check of the data message's electronic signature, including the taxpayer's certificate (the taxpayer's certificate is part of the SOAP envelope of the data message as per the WS-Security standard)
  - Check of the certificate's issuing authority
  - Check of the certificate's validity, including CRL
- Check of the integrity of the tax identification number
- Check of the BKP/PKP compatibility.

3 DATA MESSAGE STRUCTURE

3.1 DATA ITEM CODING

All items in all data messages will only use selected characters encoded as a single byte in a standard decimal ASCII character set. The allowed decimal codes are 9, 10, 13, or 32 to 126.

UTF-8 shall be mandatorily used for encoding the data messages as XML documents, i.e. first line of the XML SOAP envelope will always be:

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

All XML elements of the e-sale are part of the same namespace, specified in the Web service definition (WSDL), i.e:

```
xmlns:eet="http://fs.mfcr.cz/eet/schema/v1"
```

The data format mask for individual items, which is listed along with their detailed description below, is a regular expression in the sense of the XML Schema, which defines the required syntax of the given item. For clarity, the metasign for start of text strings (^) and end of text strings ($) are also used throughout this document.

Hexadecimal numbers larger than 9 ("a" to "f") may be used as lower or upper case letters, i.e. also as "A" to "F".

3.2 DATA MESSAGE STRUCTURE OVERVIEW

All three types of data messages (registered sale data message, acknowledgement data message, error data message) have a common basic data format based on the SOAP (Simple Object Access Protocol) protocol, i.e. application XML data structures are inserted into the body of the SOAP envelope (<SOAP EnvelopeBody>).

The registered sale data message (*Fig. 2*) and the Acknowledgement data message will be signed (*Fig. 3* left), the error data message will not be signed (*Fig. 3* right).

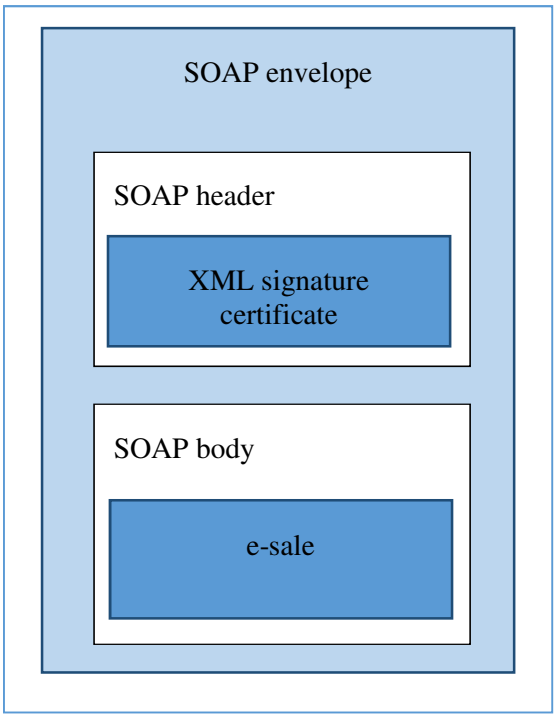

Fig. 2 Registered sale data message structure

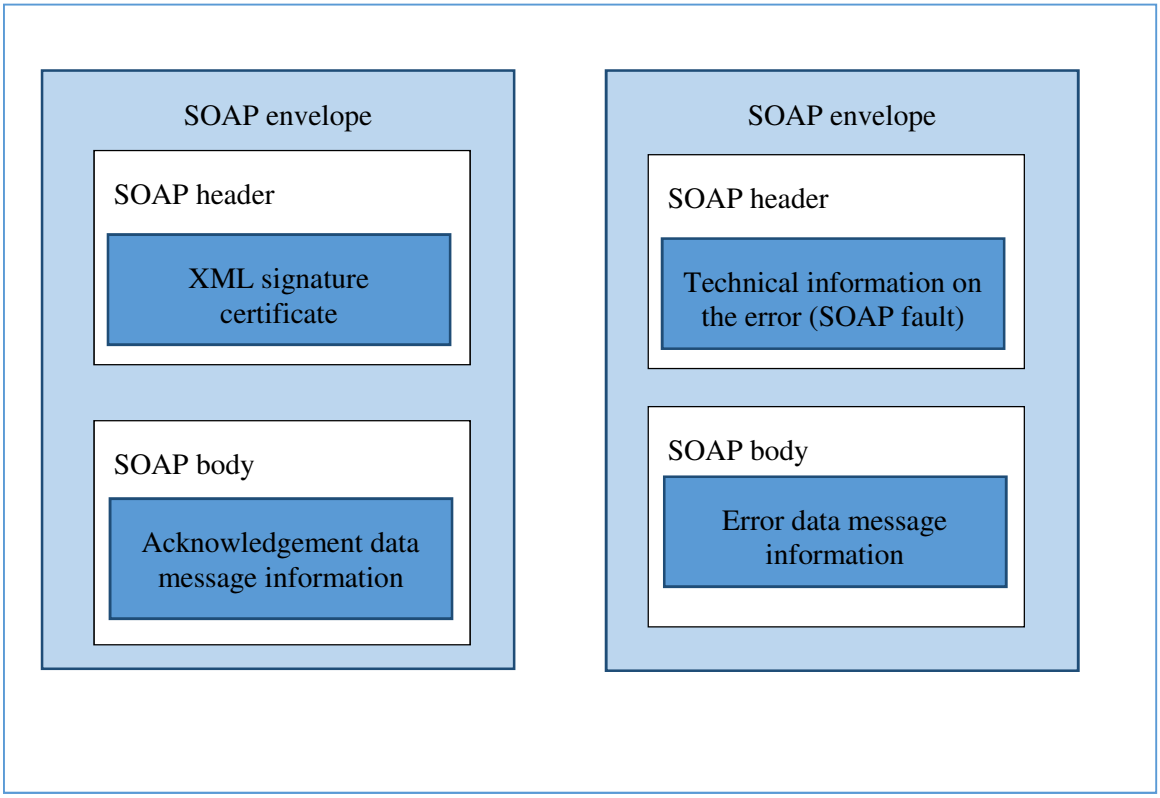

Fig. 3 Acknowledgement and error data message structure

3.3 REGISTERED SALE DATA MESSAGE

Is a data message, including the SOAP envelope, is a SOAP XML structure containing all information specified for the registered sale data message. The registered sale data are saved in an embedded *e-sale* structure (the <Trzba> XML element), which is part of the <SOAP Envelope Body> XML element.

In the <SOAP Envelope Header> XML element, the XML signature and a certificate (whose private key was used to create the XML signature) will be saved. When the key certificate used at the time of issuing the Receipt (i.e. creation of PKP and BKP) is no longer valid at the time of sending of the registered sale data message, the taxpayer may use another valid certificate for the XML signature – see also *4.1 Taxpayer's Signature Code (PKP)*.

The registered sale data message will be described in detail in the definition of the relevant Web service – see 6 *SOAP XML message and its security*.

The *Registered sale data message* itself is stored in the <SOAP Envelope Body> XML element as the <Trzba> element.
This element contains two embedded elements representing the <Hlavicka>, <Chyba> and <KontrolniKody>data areas.
These data areas contain the data items themselves – see *3.3.2 Overview of registered sale data message items*.

3.3.1 E-sale XML format

e-sale XML format overview:

```
<eet:Trzba>
      <eet:Hlavicka atributes ... />
```

```
        <eet:Data atributes ... />
        <eet:KontrolniKody>
                values ...
        </eet:KontrolniKody>
</eet:Trzba>
```

XML elements' attributes and values are described below.

3.3.2 Overview of registered sale data message items

Data area		Item name	Mandatory	XML name)*
Hlavička (Header)	1	Message's UUID	Yes	uuid_zpravy
	2	Date and time of sending	Yes	dat_odesl
	3	First sending of sales information	Yes	prvni_zaslani
	4	Flag of verification sending mode	No	overeni
Data (Data)	5	Tax identification number	Yes	dic_popl
	6	Appointing tax identification number	No	dic_poverujiciho
	7	Business premises ID	Yes	id_provoz
	8	Cash register ID	Yes	id_pokl
	9	Serial number of receipt	Yes	porad_cis
	10	Date and time of sale	Yes	dat_trzby
	11	Total amount of sale	Yes	celk_trzba
	12	Total amount for performance exempted from VAT, other performance	No	zakl_nepodl_dph
	13	Total tax base - basic VAT rate	No	zakl_dan1
	14	Total VAT - basic VAT rate	No	dan1
	15	Total tax base - first reduced VAT rate	No	zakl_dan2
	16	Total VAT - first reduced VAT rate	No	dan2
	17	Total tax base - second reduced VAT rate	No	zakl_dan3
	18	Total VAT - second reduced VAT rate	No	dan3
	19	Total amount under the VAT scheme for travel service	No	cest_sluz
	20	Total amount under the VAT scheme for the sale of used goods - basic VAT rate	No	pouzit_zboz1
	21	Total amount under the VAT scheme for the sale of used goods - first reduced VAT rate	No	pouzit_zboz2
	22	Total amount under the VAT scheme for the sale of used goods - second reduced VAT rate	No	pouzit_zboz3
	23	Total amount of payments intended for subsequent drawing or settlement	No	urceno_cerp_zuct
	24	Total amount of payments which are payments subsequently drawn or settled	No	cerp_zuct
	25	Sale regime	Yes	rezim
Kontrolní kódy (Control codes)	26	Taxpayer's Signature Code (PKP)	Yes	pkp
	27	Taxpayer's Security Code (BKP)	Yes	bkp

)* XML name is the name of a XML element or a XML attribute.

3.3.3 Detailed description of e-sale items

As an example, tax identification number of GFŘ and MFČR are used below.

3.3.3.1 Message's UUID (uuid_zpravy)

Is an attribute of the <Hlavicka> XML element. The UUID (Universally Unique Identifier) of the registered sale data message is generated by the taxpayer's cash register. The UUID shall have the following format as per RFC 4122:

```
xxxxxxxx-xxxx-Mxxx-Nxxx-xxxxxxxxxxxx
```

, where "x", "M" and "N" are hexadecimal numbers. "M" is the version of the UUID and its values are 1 to 5. The value of the two highest bites of N is mandatorily 1 0 (UUID variant), i.e. its allowed hexadecimal values are: 8, 9, A, B.

Data format mask:

```
^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[1-5][0-9a-fA-F]{3}-[89abAB][0-9a-fA-F]{3}-[0-9a-fA-F]{12}$
```

, where the "-" character is a dash (ASCII decimal code 45).

Length: 36 characters.

Example:

```
b3a09b52-7c87-4014-a496-4c7a53cf9125
```

3.3.3.2 Date and time of sending (dat_odesl)

Is an attribute of the <Hlavicka> XML element. The date and time of sending is the moment when the cash register sends the registered sale data message.

The data format is a DateTime type as per ISO 8601, as specified in the relevant W3C specification: https://www.w3.org/TR/xmlschema11-2/#dateTime:

```
rrrr-mm-ddThh:mm:ss±hh:mm
```

, where "*rrrr-mm-dd*" is the date in the "year-month-day" format, "*hh*:*mm*:*ss*" is the time in the "hour:minute:second" format and "*±hh*:*mm*" is the time zone expressed as the difference from UTC/GMT in hours and minutes. The "±" is either a "+" (plus), or a "-" (minus), depending on whether the difference from the UTC/GMT is positive or negative. As a special value, a string of "Z" may be used, whose meaning is "+00:00".

The date and time of sending of a data message is the local time in the given time zone plus the time zone code (mandatory) as per these examples:

- +01:00 for daylight saving time in the Czech Republic – i.e. CET
- +02:00 for summer time in the Czech Republic – i.e. CEST
- +*hh*:*mm*, or –*hh*:*mm, or* Z for other time zones (outside of the Czech Republic).

Length: 25 characters.

Example - daylight saving time:

```
2016-11-09T04:25:28+01:00
```

This is 4 hours, 25 minutes and 28 seconds CET, i.e. 3:25:28 UTC/GMT.

Example - summer time:

```
2017-06-09T05:25:28+02:00
```

This is 5 hours, 25 minutes and 28 seconds CEST, i.e. 3:25:28 UTC/GMT.

3.3.3.3 First sending of sales information (prvni_zaslani)

Is an attribute of the <Hlavicka> XML element. This is a flag with a value of *true* or *false* (or *1*/*0*), which shows whether the communication is the first (*true* or *1*), or repeated (*false* or *0*) sending of the relevant registered sale.

The data format is based on the relevant W3C specification, see: https://www.w3.org/TR/xmlschema11-2/#boolean).

Length: 1 to 5 characters.

Example:

```
true
```

3.3.3.4 Flag of verification sending mode (overeni)

Is an attribute of the <Hlavicka> XML element. This is a flag through which the taxpayer's cash register may set the verification mode for sending of registered sale data messages.

When the flag is present and has a value of *true* (or *1*), the data message is processed in verification mode – see *2.2 Data message sending modes, production and non-production environment*.

When the flag is not present, or when its value is *false* (or *0*), the data message is processed in operational mode.

The data format is based on the relevant W3C specification, see: https://www.w3.org/TR/xmlschema11-2/#boolean).

Length: 1 to 5 characters.

Example:

```
true
```

3.3.3.5 Tax identification number (dic_popl)

Is an attribute of the <Data> XML element. It is the DIČ/tax identification number sending the registered sale data message, valid at the time of accepting the payment, or at the time of making the payment order, when such an order is made in advance. The DIČ shall include the country code: CZ. The attribute value is identical to the DIČ listed in the certificate used for the electronic signature of data messages (the certificate is part of the SOAP envelope of the registered sale data message). The taxpayer whose DIČ changes may send registered sale data messages with their new DIČ in the *dic_popl* attribute, signed by the existing certificate until a new certificate is issued for them.

Data format mask:

```
^CZ[0-9]{8,10}$
```

Length: 10 to 12 characters.

Example: (GFŘ and MF DIČ):

```
CZ72080043
CZ00006947
```

3.3.3.6 Appointing tax identification number (dic_poverujiciho)

Is an attribute of the <Data> XML element. It is the valid DIČ of a taxpayer receiving the sales, who authorised another taxpayer to register the sales. The data format is identical to that of the *tax identification number* attribute.

3.3.3.7 Business premises ID (id_provoz)

Is an attribute of the <Data> XML element. It is a number ID for the business premises, assigned to the taxpayer at the EET Portal.

Data format mask:

```
^[1-9][0-9]{0,5}$
```

Length: 1 to 6 characters, i.e. a range of 1 to 999999.

Example:

```
25
```

3.3.3.8 Cash register ID (id_pokl)

Is an attribute of the <Data> XML element. It is an ID code for the taxpayer's cash register sending the registered sale data message to the tax authority's common technical equipment. The code is created at the taxpayer's side and consists of alphanumeric and selected special characters.

Data format mask:

```
^[0-9a-zA-Z\.,:;/#\-_]{1,20}$
```

, where the last character in the square bracket is a space (the " " character with an ASCII decimal code of 32) and the "-" character is a dash (ASCII decimal code 45).

Length: 1 to 20 characters.

Example:

```
5a/A-q/5:22d_2
```

3.3.3.9 Serial number of receipt (porad_cis)

Is an attribute of the <Data> XML element. It is the serial number of a receipt, created at the taxpayer's side using alphanumeric and selected special characters. The code consists of alphanumeric and selected special characters.

Data format mask:

```
^[0-9a-zA-Z\.,:;/#\-_]{1,20}$
```

, where the last character in the square bracket is a space (the " " character with an ASCII decimal code of 32) and the "-" character is a dash (ASCII decimal code 45).

Length: 1 to 20 characters.

Example:

```
#25/c-12/1A_2/2016
```

3.3.3.10 Date and time of sale (dat_trzby)

Is an attribute of the <Data> XML element. This is the date and time of the registered sale taking place and/or the date and time of making the receipt, when the receipt is made beforehand.

The format is identical to that of the date and time of sending – see *3.3.3.2 Date and time of sending*, i.e. date and time in the local time zone and a mandatory code for the time zone.

3.3.3.11 Sale's financial information

All financial information for a sale are attributes of the <Data> XML element. The following numerical information/items (in this order) are used for the following financial values in CZK:

11	Total amount of sale
12	Total amount for performance exempted from VAT, other performance
13	Total tax base - basic VAT rate
14	Total VAT - basic VAT rate
15	Total tax base - first reduced VAT rate
16	Total VAT - first reduced VAT rate
17	Total tax base - second reduced VAT rate
18	Total VAT - second reduced VAT rate
19	Total amount under the VAT scheme for travel service
20	Total amount under the VAT scheme for the sale of used goods - basic VAT rate
21	Total amount under the VAT scheme for the sale of used goods - first reduced VAT rate
22	Total amount under the VAT scheme for the sale of used goods - second reduced VAT rate
23	Total amount of payments intended for subsequent drawing or settlement
24	Total amount of payments which are payments subsequently drawn or settled

The number values of all amounts shall be provided in decimal numbers with exactly two mandatory decimals and a decimal point as per https://www.w3.org/TR/xmlschema11-2/#decimal. The values may be positive, zero, or negative.

To achieve a one-to-one correspondence between the numerical value of a financial item and the character string of its decimal representation, insignificant leading zeroes and a minus character (a dash character with ASCII decimal code 45) before zero value are forbidden.

Data format mask:

```
^((0|-?[1-9]\d{0,7})\.\d\d|-0\.(0[1-9]|[1-9]\d))$
```

Length:

- for non-negative values: 4 to 11 characters, i.e. minimum non-zero value is CZK 0.00, maximum non-zero value is CZK 99 999 999.99
- for negative values: 5 to 12 characters, i.e. minimum zero value is CZK -99 999 999.99, maximum zero value is CZK -0.01

This means that the financial items are limited in their absolute value to numbers smaller than CZK 100 million.

Examples::

250.00

-187.20

0.56

Examples of wrong character string representations:

Numerical value	Wrong representation	Correct representation
20,45	020.45	20.45
10,25	00010.25	10.25
0	-0.00	0.00
0	-00.00	0.00
0,2	.20	0.20
-100	-00100.00	-100.00

3.3.3.12 Sale regime (rezim)

Is an attribute of the <Data> XML element. The sale regime is either regular, or simplified. The following codes are used:

- 0 regular regime
- 1 simplified regime

Data format mask:

```
^[01]$
```

Length: 1 character.

3.3.3.13 Taxpayer's Signature Code (pkp)

Is a value of the <pkp> XML element, which is part of the <KontrolniKody> XML element. The PKP is an electronic signature for selected e-sale information. The <pkp> element attributes define the following:

- Hash algorithm used (message digest, hash): SHA256
- Electronic signature algorithm used: RSA2048
- PKP coding method used: Base64, i.e. a string of characters: "0" to "9", "a" to "z", "A" to "Z", "/", "+" a "=".

The type is defined as per https://www.w3.org/TR/xmlschema11-2/#base64Binary.

Length: the binary data length is 256 bytes, i.e. the Base64 representation is 344 characters-long.

A detailed description of the generation and resulting format of the PKP is provided in the *4.1 Taxpayer's Signature Code (PKP)* chapter.

3.3.3.14 Taxpayer's Security Code (bkp)

Is a value of the <bkp> XML element, which is part of the <KontrolniKody> XML element. BKP is a hash, or message digest of the PKP code. The <bkp> element attributes define the following:

- Hash algorithm used (message digest, hash): SHA1
- The BKP value encoding method used: Base16, i.e. a string of hexadecimal numbers.

Caution: this is not the regular type (https://www.w3.org/TR/xmlschema11-2/#hexBinary), but a modified value as per specifications below.

Length: binary data length 20 bytes, i.e. 40 hexadecimal numbers. For improved clarity, the hexadecimal numbers in the BKP will be divided by a hash (the "-" character, ASCII decimal code 45) after every eight numbers. The total length of the BKP in text form is therefore 44 characters.

Data format mask:

```
^([0-9a-fA-F]{8}-){4}[0-9a-fA-F]{8}$
```

, where the "-" character is a dash (ASCII decimal code 45).

A detailed description of the generation and resulting format of the BKP is provided in the *4.2 Taxpayer's Security Code (BKP)* chapter.

3.3.4 E-sale example

The following text is an example of the <Trzba> XML element sent in the regular production mode:

```
<eet:Trzba>
      <eet:Hlavicka
            uuid_zpravy="e23e5a5a-08d7-4a08-844d-2b6c6b60621d"
            dat_odesl="2016-12-08T21:19:40+01:00"
            prvni_zaslani="true" />
<eet:Data dic_popl="CZ72080043" dic_poverujiciho="CZ00006947"
      id_provoz="181" id_pokl="00/2535/CN58" porad_cis="0/2482/IE25"
      dat_trzby="2016-12-07T22:01:00+01:00" celk_trzba="87988.00"
      zakl_nepodl_dph="5922.00" zakl_dan1="-7083.74" dan1="-1487.59"
      zakl_dan2="-7605.28" dan2="-1140.79" zakl_dan3="-7172.54"
      dan3="-717.25" cest_sluz="4267.00" pouzit_zboz1="956.00"
      pouzit_zboz2="424.00" pouzit_zboz3="131.00"
      urceno_cerp_zuct="343.00" cerp_zuct="237.00" rezim="1" />
      <eet:KontrolniKody>
      <eet:pkp digest="SHA256" cipher="RSA2048" encoding="base64">
Ca8sTbURReQjjgcy/znXBKjPOnZof3AxWK5WySpyMrUXF0o7cz1BP6adQzktODKh2d8s
oAhn1R/S07lVDTa/6r9xTuI3NBH/+7YfYz/t92eb5Y6aNvLm6tXfOdE3C94EQmT0SEEz
9rInGXXP1whIKYX7K0HgVrxjdxCFkZF8Lt12XbahhAzJ47LcPxuBZZp6U6wJ2sWI5os3
KY9u/ZChzAUaCec7H56QwkMnu3U3Ftwi/YrxSzQZTmPTpFYKXnYanrFaLDJm+1/yg+VQ
ntoByBM+HeDXigBK+SHaxx+Nd0sSmm1Im4v685BRVdUId+4CobcnSQ3CBsjAhqmIrtWT
GQ==
      </eet:pkp>
      <eet:bkp digest="SHA1" encoding="base16">
            03ec1d0e-6d9f77fb-1d798ccb-f4739666-a4069bc3 </eet:bkp>
      </eet:KontrolniKody>
</eet:Trzba>
```

This is an example of the <Trzba> XML element sent in the verification mode:

```
<eet:Trzba>
      <eet:Hlavicka
```

```
            uuid_zpravy="e23e5a5a-08d7-4a08-844d-2b6c6b60621d"
            dat_odesl="2016-12-08T21:19:40+01:00"
            prvni_zaslani="true" overeni="true" />
<eet:Data dic_popl="CZ72080043" dic_poverujiciho="CZ00006947"
      id_provoz="181" id_pokl="00/2535/CN58" porad_cis="0/2482/IE25"
      dat_trzby="2016-12-07T22:01:00+01:00" celk_trzba="87988.00"
      zakl_nepodl_dph="5922.00" zakl_dan1="-7083.74" dan1="-1487.59"
      zakl_dan2="-7605.28" dan2="-1140.79" zakl_dan3="-7172.54"
      dan3="-717.25" cest_sluz="4267.00" pouzit_zboz1="956.00"
      pouzit_zboz2="424.00" pouzit_zboz3="131.00"
      urceno_cerp_zuct="343.00" cerp_zuct="237.00" rezim="1" />
      <eet:KontrolniKody>
      <eet:pkp digest="SHA256" cipher="RSA2048" encoding="base64">
Ca8sTbURReQjjgcy/znXBKjPOnZof3AxWK5WySpyMrUXF0o7cz1BP6adQzktODKh2d8s
oAhn1R/S07lVDTa/6r9xTuI3NBH/+7YfYz/t92eb5Y6aNvLm6tXfOdE3C94EQmT0SEEz
9rInGXXP1whIKYX7K0HgVrxjdxCFkZF8Lt12XbahhAzJ47LcPxuBZZp6U6wJ2sWI5os3
KY9u/ZChzAUaCec7H56QwkMnu3U3Ftwi/YrxSzQZTmPTpFYKXnYanrFaLDJm+1/yg+VQ
ntoByBM+HeDXigBK+SHaxx+Nd0sSmm1Im4v685BRVdUId+4CobcnSQ3CBsjAhqmIrtWT
GQ==
      </eet:pkp>
      <eet:bkp digest="SHA1" encoding="base16">
            03ec1d0e-6d9f77fb-1d798ccb-f4739666-a4069bc3 </eet:bkp>
      </eet:KontrolniKody>
</eet:Trzba>
```

3.4 ACKNOWLEDGEMENT DATA MESSAGE

The *acknowledgement data message* is a SOAP XML structure containing acknowledgement information on the receipt of registered sale by the tax authority's common technical equipment. The acknowledgement data are stored in the <SOAP Envelope Body> XML element.

The <SOAP Envelope Header> XML element will contain a XML signature and a certificate for the tax authority's common technical equipment, whose private key was used to create the XML signature.

The acknowledgement itself is saved in the <SOAP Envelope Body> XML element as the <Odpoved> element. This element contains two embedded elements which represent data areas: <Hlavicka> and <Potvrzeni>. These data areas contain the data items – see *3.4.2 Overview of acknowledgement data items*.

Individual replies of the EET system depending on the mode, validity of the data message and the target environment are provided in *Table1: EET system's reply options*.

3.4.1 Acknowledgement - XML format

The Acknowledgement XML format overview:

```
<eet:Odpoved>
      <eet:Hlavicka atributes ... />
      <eet:Potvrzeni atributes ... />
</eet:Odpoved>
```

The XML element attributes and values are provided below.

3.4.2 Overview of acknowledgement data items

Data area		Item name	Mandatory	XML name)*
Hlavička (Header)	1	Message's UUID	Yes	uuid_zpravy
	2	Date and time of message receipt	Yes	dat_prij
	3	Taxpayer's Security Code	Yes	bkp
Potvrzení (Acknowledgement)	4	Fiscal Identification Code	Yes	fik
	5	Non-production environment flag	No	test

)* XML name is the name of a XML element or a XML attribute.

3.4.2.1 Message's UUID (uuid_zpravy)

Is an attribute of the <Hlavicka> XML element. This is the registered sale data message's UUID for the data message sent by the taxpayer's cash register – see *3.3.3.1 Message's UUID*.

3.4.2.2 Date and time of sale (dat_trzby)

Is an attribute of the <Hlavicka> XML element. The date and time of receipt of the acknowledged message is the time when the tax authority's common technical equipment received the registered sale data message.

The format of this item is identical to that of the date and time of sending – see *3.3.3.2 Date and time of sending*.

3.4.2.3 Taxpayer's Security Code (bkp)

Is an attribute of the <Hlavicka> XML element. This is the registered sale data message's BKP for the data message sent by the taxpayer's cash register – see *3.3.3.14 Taxpayer's Security Code (bkp)*.

3.4.2.4 Fiscal Identification Code (fik)

Is an attribute of the <Potvrzeni> XML element. This is a Fiscal Identification Code (FIK), generated by the tax authority's common technical equipment, which is unique for each acknowledged registered sale data message sent by the taxpayer's cash register.

The FIK data format is as follows:

```
uuid_prijem-Id_zarizeni
```

, where `uuid_prijem` is the UUID number generated by an individual EET system device which received the message and `Id_zarizeni` is a two-digit hexadecimal number of such device.

Data format mask:

```
^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-4[0-9a-fA-F]{3}-[89abAB][0-9a-fA-F]{3}-[0-9a-fA-F]{12}-[0-9a-fA-F]{2}$
```

Length: 39 characters.

Example:

```
b3a09b52-7c87-4014-a496-4c7a53cf9125-03
```

When a FIK is assigned in the non-production environment and is therefore not an actual FIK as per the Act on Registration of Sales, its last two characters have a value of ff (Fictional FIK= ff)

Example:

```
b3a09b52-7c87-4014-a496-4c7a53cf9125-ff
```

3.4.2.5 Non-production environment flag (test)

Is an attribute of the <Potvrzeni> XML element. It is a flag by which the tax authority's common technical equipment informs the taxpayer's cash register whether the registered sale data message has been sent into the production or non-production environment.

When the flag is present and has a value of *true* (or *1*), the data message was received in the non-production environment – see *2.2 Data message sending modes, production and non-production environment.*

When the flag is not present, the data message was received in the production environment.

The data format is based on the relevant W3C specification, see: https://www.w3.org/TR/xmlschema11-2/#boolean).

Length: 1 to 5 characters.

Example:

```
true
```

3.4.3 Example of acknowledgement

The following is an example of the <Odpoved> XML element from the production environment:

```
<eet:Odpoved>
      <eet:Hlavicka uuid_zpravy="123e4567-e89b-42d3-a456-
426655440000"
      dat_prij="2017-03-04T18:25:21+01:00"
      bkp="01234567-89abcdef-01234567-89abcdef-01234567" />
      <eet:Potvrzeni fik="987a6be5-6af5-44f3-b4fc-987654321000-02" />
</eet:Odpoved>
```

This is an example of the <Odpoved> XML element from the non-production environment:

```
<eet:Odpoved>
      <eet:Hlavicka uuid_zpravy="123e4567-e89b-42d3-a456-
426655440000"
      dat_prij="2017-03-04T18:25:21+01:00"
      bkp="01234567-89abcdef-01234567-89abcdef-01234567" />
      <eet:Potvrzeni fik="987a6be5-6af5-44f3-b4fc-987654321000-03"
      test="true" />
</eet:Odpoved>
```

3.5 ERROR DATA MESSAGE

The error data message is a SOAP XML structure containing an error code and an error message text concerning:

1. a critical error in the received registered sale data message, or

2. a temporary technical error in the processing at the tax authority's common technical equipment's side (requires the registered sale data message to be re-sent later).

The error message data are stored in the <SOAP Envelope Body> XML element as the <Odpoved> element. This element contains two embedded elements representing the <Hlavicka> and <Chyba> data areas. These data areas contain the data items themselves – see *3.5.2 Overview of error data items*.

In this instance the <SOAP Envelope> will not contain a XML signature or a certificate.

Individual replies of the EET system depending on the mode, validity of the data message and the target environment are provided in *Table1: EET system's reply options*.

3.5.1 Error - XML format

The Error XML format overview:

```
<eet:Odpoved>
      <eet:Hlavicka atributes ... />
      <eet:Chyba atributes ...>
            values ...
      </eet:Chyba>
</eet:Odpoved>
```

The XML element attributes and values are provided below.

3.5.2 Overview of error data items

Data area		Item name	Mandatory	XML name)*
Hlavička (Header)	1	Message's UUID	No	uuid_zpravy
	2	Date and time of message rejection	No	dat_odmit
	3	Taxpayer's Security Code	No	bkp
Chyba (Error)	4	Error code	Yes	kod
	5	Text description of the error	Yes	Chyba
	6	Non-production environment flag	No	test

)* XML name is the name of a XML element or a XML attribute.

3.5.2.1 Message's UUID (uuid_zpravy)

Is an attribute of the <Hlavicka> XML element. This is the registered sale data message's UUID for the data message sent by the taxpayer's cash register and containing an error – see *3.3.3.1 Message's UUID*.

3.5.2.2 Date and time of sale (dat_trzby)

Is an attribute of the <Hlavicka> XML element. It is the date and time of rejection of a message containing an error, i.e. the time the registered sale data message with an error is processed at the tax authority's common technical equipment.

The format of this item is identical to that of the date and time of sending – see *3.3.3.2 Date and time of sending*.

3.5.2.3 Taxpayer's Security Code (bkp)

Is an attribute of the <Hlavicka> XML element. This is the BKP for a sale sent by the taxpayer's cash register and containing an error – see *3.3.3.14 Taxpayer's Security Code (bkp)*.

3.5.2.4 Error code (kod)

Is an attribute of the <Chyba> XML element. This is a decimal integer with a maximum of three digits, which is assigned to an individual critical error in the defined code-list. The error code values may be positive, zero, or negative.

Data format mask:

```
^-?\d{1,3}$
```

Length:

- for non-negative values: 1 to 3 characters, i.e. minimum non-zero value is 0, maximum non-zero value is 999
- for negative values: 2 to 4 characters, i.e. minimum zero value is -999, maximum zero value is -1

Examples::

10

-1

560

3.5.2.5 Text description of the error (Chyba)

Is a value of the <Chyba> XML element. This is a character string in the Czech language describing the error which occurred during processing of the data message.

To ensure consistency of all data messages, only characters in the lower ASCII set of XML-allowed characters will be used, i.e. characters with decimal codes of 9, 10, 13, or 32 to 126. This means the text description will not use any diacritics.

Max. length: 100 characters.

3.5.2.6 Non-production environment flag (test)

Is an attribute of the <Chyba> XML element. It is a flag by which the tax authority's common technical equipment informs the taxpayer's cash register whether the registered sale data message has been sent into the production or non-production environment.

When the flag is present and has a value of *true* (or *1*), the data message was received in the non-production environment – see *2.2 Data message sending modes, production and non-production environment.*

When the flag is not present, the data message was received in the production environment.

The data format is based on the relevant W3C specification, see: https://www.w3.org/TR/xmlschema11-2/#boolean).

Length: 1 to 5 characters.

Example:

```
true
```

3.5.3 Example of an error

The following are examples of the error reply in the <Odpoved> XML element containing information on the error.

These are production environment reply examples for the <Odpoved> XML element containing information on the error:

Example 1 (the registered sale data message was successfully analysed):

```
<eet:Odpoved>
      <eet:Hlavicka
            uuid_zpravy="123e4567-e89b-42d3-a456-426655440000"
            bkp="01234567-89abcdef-01234567-89abcdef-01234567"
            dat_odmit="2017-03-04T18:25:21+01:00" />
      <eet:Chyba kod="5">
            Neplatny kontrolni bezpecnostni kod poplatnika (BKP)
      </eet:Chyba>
</eet:Odpoved>
```

Example 2 (the registered sale data message could not be analysed):

```
<eet:Odpoved>
      <eet:Hlavicka dat_odmit="2017-03-04T18:25:21+01:00" />
      <eet:Chyba kod="3">
            XML zprava nevyhovela kontrole XML schematu
      </eet:Chyba>
</eet:Odpoved>
```

Example 3 (technical problem with the tax authority's common technical equipment):

```
<eet:Odpoved>
      <eet:Hlavicka dat_odmit="2017-03-04T18:25:21+01:00" />
      <eet:Chyba kod="-1">
            Docasna technicka chyba zpracovani - odeslete prosim
datovou zpravu pozdeji
      </eet:Chyba>
</eet:Odpoved>
```

This is an example of an error message in the <Odpoved> XML element from the non-productive environment:

```
<eet:Odpoved>
      <eet:Hlavicka
            uuid_zpravy="123e4567-e89b-42d3-a456-426655440000"
            bkp="01234567-89abcdef-01234567-89abcdef-01234567"
            dat_odmit="2017-03-04T18:25:21+01:00" />
      <eet:Chyba kod="5" test="true">
            Neplatny kontrolni bezpecnostni kod poplatnika (BKP)
      </eet:Chyba>
</eet:Odpoved>
```

3.5.4 List of error codes and error messages

Code	Error message text)*
-999 – -2	)**
-1	Docasna technicka chyba zpracovani – odeslete prosim datovou zpravu pozdeji (Temporary technical error in processing - please re-send the data message later)
0	Datovou zpravu evidovane trzby v overovacim modu se podarilo zpracovat (The registered sale data message in verification mode was successfully processed)
1	)**
2	Kodovani XML neni platne (The XML encoding is not valid))***
3	XML zprava nevyhovela kontrole XML schematu (The XML message failed the XML schema check)
4	Neplatny podpis SOAP zpravy (Invalid SOAP message signature)
5	Neplatny kontrolni bezpecnostni kod poplatnika (BKP) (Invalid Taxpayer's Security Code (BKP))
6	DIC poplatnika ma chybnou strukturu (Invalid structure of tax identification number)
8	Datova zprava je prilis velka (The data message is too big)
9	Datova zprava nebyla zpracovana kvuli technicke chybe nebo chybe dat (The data message was not processed because of a technical error or a data error)
9 – 999	)**

)* The error message texts shall be without diacritics as all EET system messages – see *3.1 Data item coding*.

)** Reserved for future use.

)*** Depending on the situation, this error may also be reacted to by returning a technical error, i.e. the SOAP fault, or by ignoring the data message when it appears to be a cyber attack.

4 PKP AND BKP CODES

4.1 TAXPAYER'S SIGNATURE CODE (PKP)

The Taxpayer's Signature Code (PKP) is an electronic signature of selected information in the registered sale data message as specified by the tax authority.

Technically speaking, the PKP is an electronic signature of a text string, created in a defined process from selected data items of the e-sale – see 5 *Registered sale identification - PKP items selection*Registered sale identification - PKP. The signature is created by the taxpayer's cash register using its own private key. This private key is uniquely paired to a public key which is part of the X509 certificate inserted in the <SOAP Header> SOAP element of the data message. This means that to create the PKP and XML signature of the data message, the same private key must be used – the only exception is when the certificate of the key used at the time of issue of the Receipt (i.e. used to create the PKP and BKP) is no longer valid at the time of sending of the registered sale data message. In such cases the taxpayer may use another valid certificate to create the XML signature.

The calculation of the PKP in the cash register follows these steps:

1. The text to be signed (`plaintext`) is created by chaining selected items of the <Trzba> elements in ASCII code and with "|" (ASCII decimal code 124) between individual items.

2. Such `plaintext` is then electronically signed by the SHA256withRSA algorithm using the same key and certificate as those used to electronically sign the entire data message. This results in a `rsa_text`.

3. The resulting `rsa_text` signature is then encoded using the Base64 algorithm into a `rsa_text_base64` text string, which is then saved in the data message as the value of the <pkp> XML element in the <Trzba> element. The resulting text string has a length of 344 characters.

4.1.1 Example of a PKP calculation

The following Java code illustrates the calculation of the PKP code. Standard classes which are part of the Java development environment are used in the calculation.

```
import java.security.KeyStore;
import java.security.PrivateKey;
import java.security.Signature;
```

The example of the PKP calculation below uses variables whose values depend on the target environment (i.e. taxpayer's cash register).

```
KeyStore keystore; // key repository for keys containing signature certificate
String alias;      // alias for the certificate in the key repository
String password;   // password for the certificate's private key
```

The calculation example below assumes that the `plaintext` variable will be filled as per definition in *4.1 Taxpayer's Signature Code (PKP)*.

```
String plaintext;       // text being signed
```

The algorithm for chaining items into text being signed depends on the individual implementation of the Web service's client. The resulting text being signed will have the following content (data for the

text were taken from the <Trzba> XML element in the normal production mode in *3.3.4 E-sale example*).

```
"CZ72080043|181|00/2535/CN58|0/2482/IE25|2016-12-07T22:01:00+01:00|87988.00"
```

The first step in the calculation is preparation of the `java.security.Signature` type object with which the PKP will be calculated.

```
Signature signature = Signature.getInstance("SHA256withRSA");
signature.initSign((PrivateKey) keystore
        .getKey(alias, password.toCharArray()));
signature.update(plaintext.getBytes("UTF-8"));
```

In the second step, the calculation of the PKP (electronic signature) will be made.

```
byte[] rsa_text= signature.sign();
```

The `rsa_text` variable after execution of the `sign()` function contains binary data (an octet string) from which the PKP is computed by conversion to Base64 encoding. A particulal API function for conversion into a Base64 encoded string of characters depends on the respective implementation of the Web Service's client.

4.2 TAXPAYER'S SECURITY CODE (BKP)

The Taxpayer's Security Code (BKP) is a hash/message digest of the PKP value, where the PKP is used in the form of a string of octets (see `rsa_text value above`) by the SHA1 algorithm. From this definition it is clear that when the PKP is known, the BKP may be reconstructed at any time.

BKP calculation steps:

1. If the original octet string `rsa_text` is available, we can start at step 2 below;
   if the PKP is available (i.e. a character string in Base64 encoding): `rsa_text_base64`, it is necessary to first decode it to an octet string: `rsa_text`.

2. From the `rsa_text` octet string a hash/message digest is created using the SHA1 algorithm. This creates a `hash_sha1` octet string with a length of 160 bits (20 bytes).

3. The `hash_sha1` octet string is then hexadecimaly encoded into a `hash_sha1_base16` text string.

4. The `hash_sha1_base16` text string is then converted into the target form by inserting between the subsequent hexadecimal numbers:
   8. and 9.
   16. and 17.
   24. and 25.
   32. and 33.
   the dash sign ("-" ASCII decimal code 45), i.e. the 40 hexadecimal numbers in the BKP are divided into 5 five blocks of 8 numbers each.
   This text string is then inserted into the data message as the value of the <bkp> XML element in the <Trzba> element. The resulting text string has a length of 44 characters.

5 REGISTERED SALE IDENTIFICATION - PKP ITEMS SELECTION

A registered sale will be uniquely identified by the BKP code calculated using the algorithm described in 4 *PKP and BKP codes* from the basic data items of the <Data> XML elements of the e-sale as listed (in original order numbers):

Data area		Name of item – basic	Mandatory	XML name
Data	5	Tax identification number	Yes	dic_popl
	7	Business premises ID	Yes	id_provoz
	8	Cash register ID	Yes	id_pokl
	9	Serial number of receipt	Yes	porad_cis
	10	Date and time of sale	Yes	dat_trzby
	11	Total amount of sale	Yes	celk_trzba

The starting text to be signed (`plaintext`) for the calculation of PKP is obtained by concatenation of the above items of the registered sale data message in the given order in the ASCII code with the "|" (ASCII decimal code 124) as a separator between individual items.

Example:

Let the values of the above items be the following:

	Name of item – basic	XML name	Value
5	Tax identification number	dic_popl	`CZ72080043`
7	Business premises ID	id_provoz	`243`
8	Cash register ID	id_pokl	`24/A-6/Brno_2`
9	Serial number of receipt	porad_cis	`#135433c/11/2016`
10	Date and time of sale	dat_trzby	`2016-12-09T16:45:36+01:00`
11	Total amount of sale	celk_trzba	`3264.00`

The text (`plaintext`) from which the PKP will be calculated will then have the value of:

```
CZ72080043|243|24/A-6/Brno_2|#135433c/11/2016|2016-12-
09T16:45:36+01:00|3264.00
```

When a Registered sale data message with the same BKP as a previously-received message is received, the new message will be understood as containing information on the same registered sale.

6 SOAP XML MESSAGE AND ITS SECURITY

The Web service interface is formally defined by the WSDL (Web Services Description Language). The WSDL document links the relevant XML Schema document, which describes the XML structure of the e-sale itself. The XML structure of the e-sale shall be the only content in the <soap:Body> SOAP element.

The XML schema and WSDL files are provided as Annexes to this document.

The Web service security complies with the Web Services Security (WSS) standard in the following areas.

6.1 COMMUNICATION ENCODING USING THE HTTPS PROTOCOL

The tax authority's common technical equipment shall have a SSL server certificate. The cash register shall, as part of the SSL connection initialisation (SSL handshake) with the tax authority's common technical equipment, mandatorily verify the validity of the SSL server certificate (whether it was issued by a trustworthy authority and whether the name for which it was issued corresponds to the common technical equipment's address.

The SSL client (cash register) authentication is not required as part of the SSL handshake.

6.2 SIGNATURE OF REGISTERED SALE DATA MESSAGES

Each registered sale data message shall mandatorily be signed with a key for which a X509 taxpayer's certificate has been issued. The taxpayer's certificate shall be valid at the time of processing of the registered sale data message at the tax authority's common technical equipment's side.

Apart from the situation described in *4.1 Taxpayer's Signature Code (PKP)*, the key and the certificate used for the electronic signature in the data message must be identical to the key and certificate used to calculate the PKP code. In the signature of a SOAP message, only a single element may be included: the <soap:Body> element containing the XML structure of the e-sale (<eet:Trzba>) as per the valid XML Schema. The signature shall comply with the XML Signature Syntax and Processing (Second Edition) standard and the following requirements:

- The WS-Security 1.0 and XML Signature standards are used for the electronic signature
- The X509 certificate belonging to the private key used to implement the electronic signature on the registered sale data message, including the SOAP envelope, shall be attached in the BinarySecurityToken element (http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary) in the X509v3 format (http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3)
- The "Exclusive C14N" XML canonicalization algorithm shall be used (Exclusive XML Canonicalization Version 1.0, https://www.w3.org/TR/xml-exc-c14n/)
- To calculate the hash (digest) of the SOAP message's signature, the SHA256 algorithm shall be used (http://www.w3.org/2001/04/xmlenc#sha256)
- For the SOAP message's electronic signature, the RSA-SHA256 algorithm shall be used (http://www.w3.org/2001/04/xmldsig-more#rsa-sha256)

- The entire <soap:Body> element shall be included in the electronic signature, the message headers are not signed electronically (WS-Addressing or other standards requiring a similar concept are used)
- Other requirements concerning WSS may be provided in the WSDL.

6.3 ELECTRONIC SIGNATURE OF THE ACKNOWLEDGEMENT DATA MESSAGES

Acknowledgement data messages in the SOAP format will include the tax authority's common technical equipment's electronic signature.