ICT&L REVENUE

Revenue
Cáin agus Custaim na hÉireann
Irish Tax and Customs

PAYE Modernisation

SOAP Web Service Integration Guide

Contents

Version **1.0 Release Candidate 2**
Version Date **19/06/2017**

Version History			
Version	**Change Date**	**Section**	**Change Description**
1.0 Milestone 1	17/11/2017	All	Document published.
			Audience and **Document Context** sections added.
			Document links sources changed
		4.2.2 Timestamp	Added "maximum time" line
1.0 Release Candidate 2	17/05/2018		Version updated to **1.0 Release Candidate 2**
	19/06/2018	All	'payslip' changed to 'submission item'
		4.2.3.1	SHA1 changed to SHA512withRSA

Document References	
Reference	**Document Link**
1. Documents Homepage	Documents Homepage

Audience

This document is for any software provider who has chosen to build or update their products to allow for PAYE Modernisation.

Document context

This document provides a technical overview of how to integrate with Revenue's SOAP web services including how to sign requests validly. This document is designed to be read in conjunction with the four SOAP/XML example files as well as the rest of the Revenue Commissioners' PAYE Modernisation documentation suite including the relevant technical documents.

1. Introduction

This document details the XML PAYE Modernisation web services specification for the following web services:

- Lookup Revenue Payroll Notification (RPN) web service
- New RPN web service
- Payroll Submission web service
- Check Payroll Submission web service
- Check Payroll Run web service

The Documents Homepage specified in Document References is the home to all technical documentation, specification, and examples for the above web services which has been made available to enable payroll software developers' to update their software packages to be compatible with PAYE reporting obligations from January 2019. Path locations specified in this document are relative to this Homepage.

This document assumes familiarity with the XML web services above. A full description of each of these can be found in the Web Service Overview Document under 'PAYE Web Service Examples' on the Documents Homepage. The Web Service Description Language (WSDL) files for the above web services can be found under 'PAYE Web Service Specifications'.

WSDL is a W3C standard for describing web services. Further details of each web service can be found in the supporting WSDL file. Each file references the necessary schemas and indicates the URL where the services may be accessed. The URL for each web service will use the HTTPS protocol to ensure the privacy of all communication between ROS and the web service client.

2. Calling the Services

The web services for the PAYE Modernisation messages are described through WSDL files and the schema for each message.

Further details of the web services can be found in the published PAYE Modernisation WSDL files.

The WSDL, SOAP and WS Security version specifications we are following include:

WSDL 1.2: WSDL 1.2

SOAP 1.2: SOAP 1.2

WS Security 1.1.1: WS Security 1.1.1

2.1. Namespaces, Schemas and Locations

The PAYE Modernisation web services use namespaces which are detailed below.

2.1.1 Lookup Revenue Payroll Notification (RPN) Web Service

The namespace defining all elements related to this web service is outlined in the following table:

Description	Namespace	Relative Location
Lookup RPN Web Service	N/A	../resources/paye_modernisation/rpn.wsdl
Lookup RPN Request & Response Schema	http://www.ros.ie/schemas/paye/rpn/	../resources/paye_modernisation/rpn/v1/rpn-schema.xsd

2.1.2 New RPN Web Service

The namespace defining all elements related to this web service is outlined in the following table:

Description	Namespace	Relative Location
New RPN Web Service	N/A	../resources/paye_modernisation/rpn.wsdl
New RPN Request & Response Schema	http://www.ros.ie/schemas/paye/rpn/	../resources/paye_modernisation/rpn/v1/rpn-schema.xsd

2.1.3 Payroll Submission Web Service

The namespace defining all elements related to this web service is outlined in the following table:

Description	Namespace	Relative Location
Payroll Submission Web Service	N/A	../resources/paye_modernisation/payroll.wsdl
Payroll Submission Request & Response Schema	http://www.ros.ie/schemas/paye/payroll/	../resources/paye_modernisation/payroll/v1/payroll-schema.xsd

2.1.4 Check Payroll Submission Web Service

The namespace defining all elements related to this web service is outlined in the following table:

Description	Namespace	Relative Location
Check Payroll Submission Web Service	N/A	../resources/paye_modernisation/payroll.wsdl
Check Payroll Submission Request & Response Schema	http://www.ros.ie/schemas/paye/payroll/	../resources/paye_modernisation/payroll/v1/payroll-schema.xsd

2.1.5 Check Payroll Run Web Service

The namespace defining all elements related to this web service is outlined in the following table:

Description	Namespace	Relative Location
Check Payroll Run Web Service	N/A	../resources/paye_modernisation/payroll.wsdl
Check Payroll Run Request & Response Schema	http://www.ros.ie/schemas/paye/payroll/	../resources/paye_modernisation/payroll/v1/payroll-schema.xsd

2.2. Digital Signatures

The PAYE Modernisation web services will require a digital signature. This will be the digital signature of the declarant.

3. Interpreting the Responses

Each web service will return a response message to the client as outlined below.

3.1. Validation Errors

3.1.1 SOAP Faults

When a request is made to a PAYE Modernisation web service three checks are carried out before any processing can occur. These include:

1. Authentication
2. Authorisation
3. Schema validation

The message is first checked that it is signed with a valid digital signature, the credentials are authorised and then the message is validated against the schema.

If there is any errors encountered carrying out the above processes then a SOAP fault with a HTTP status code of 500 adhering to https://www.w3.org/TR/soap12-part1/#faultcodeelement will be returned to the client. The fault string will provide more information on the details of the problem. Where a SOAP fault is returned to the client, no processing will occur for that message.

3.1.2 Line Item Validation

Once the message passes schema validation, authentication, and authorisation then lower level line item validation is carried out on the following requests:

- Lookup RPN
- New RPN
- Payroll Submission Request

A successful response is sent back to the client detailing any validation errors that occurred on the request, if any. The code i.e. the technical error code used for mapping to the error message, the path to the error in the schema and the description of the error is detailed in the response.

A list of all validation rules carried out for each request can be found in the Validation Rules document on the Documents Homepage under 'Supporting Documentation'.

3.2. Lookup Revenue Payroll Notification (RPN) Web Service

The Employer's Lookup RPN Response will return the most up to date RPN details for those employees listed in the request who have an RPN associated with the employer. The employees who do not have

an RPN associated with the employer are returned in the response with no RPN details. A New RPN needs to be requested for these employees using the New RPN Request Web Service.

A list of validation errors (if any) on the Lookup RPN Request is also included in the response. Please refer back to Section 3.1 for more information on Validation Errors.

3.3. New RPN Web Service

The Employer's New RPN response will return new RPN details for the employees requested. PPSN and Employment ID of employees are returned with no RPN details where new RPN details could not be created.

A list of validation errors (if any) on the New RPN Request is also included in the response.

3.4. Payroll Submission Web Service

The Payroll Submission response returns an acknowledgement status for the Employer's PAYE Payroll Submission Request.

If validation failed a list of the Submission validation errors are returned in this response.

3.5. Check Payroll Submission Web Service

Check Payroll Submission will return the current status of an employer's PAYE payroll submission. The possible status values are Pending or Completed.

If the status is completed, the response includes summary totals of valid submission items. If the status is pending the response does not contain any summary totals. Validation errors for any invalid submission items are listed as well as any validation errors on the Check Payroll Submission Request. Invalid submission items are not saved therefore their amounts do not feed into the employer liability.

3.6. Check Payroll Run Web Service

Check Payroll Run will return the current status of an Employer's PAYE payroll run. The possible status values are Pending or Processed. If any submissions making up the payroll run are at a status of Pending then the status of the payroll run response will also be at Pending.

If the status is Processed the response includes a list of submissions that make up the payroll run and includes summary details of all processed submissions.

A list of validation errors (if any) on the Check Payroll Run Request is also included in the response.

4. Digital Signatures

Any ROS web service request that either returns confidential information or accepts submission of information must be digitally signed. This must be done using a digital certificate that has been previously retrieved from ROS.

The digital signature must be applied to the message in accordance with the WS-Security specification as specified in Section 4.1.

The digital signature ensures the integrity of the document. By signing the document we can ensure that no malicious intruder has altered the document in any way. It can also be used for non-repudiation purposes.

If a valid digital signature is not attached, a SOAP Fault will be returned. The fault string will provide more information on the details of the problem.

4.1. Namespaces

The valid approach for this is using Oasis standards:

- The WS-Security namespace should be:
  http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd
- The WSU namespace should be:
  http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd
- All Id references should now be of the form wsu:Id e.g. `<x:myElement wsu:Id="ID1" xmlns="…" xmlns:wsu="…"/>`
- The XML Digital Signature namespace should be:
  http://www.w3.org/2000/09/xmldsig#

4.2. Security

The security header contains three elements:

1. The Binary Security Token
2. The Timestamp
3. The Signature.

4.2.1 Binary Security Token

The X509 certificate used to sign the message should be included in the message as a Base64 encoded BinarySecurityToken element (`Envelope/Header/Security/BinarySecurityToken`).

The EncodingType attribute of the BinarySecurityToken should have a value of http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soapmessage-security-1.0#Base64Binary.

The ValueType attribute should have a value of http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-tokenprofile-1.0#X509v3.

4.2.2 Timestamp

The timestamp element (`Envelope/Header/Security/Timestamp`) must contain:

1. The Created date
2. The Expired date.

Both dates must conform to the following Oasis standard: https://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-errata-os-SOAPMessageSecurity.htm#_Toc118717167 and the expired date must be after the created date.

For SOAP requests the maximum time between timestamp creation and expiration is 60 seconds. Please see sample Payroll Submission Valid Request Example.

4.2.3 Signature

This is the signature that is calculated using your ROS digital certificates private key. The signature contains three elements:

1. The SignedInfo element
2. The SignatureValue element
3. The KeyInfo element.

4.2.3.1 SignedInfo

The SignedInfo element contains a CanonicalizationMethod, SignatureMethod and two Reference elements.

XML Canonicalization is used to format the XML before calculating the digest values. The SHA512withRSA algorithm is used for signing the message.

Canonicalization: The Canonicalization Algorithm should be XML-EXC-C14N (Exclusive Canonicalization) - Canonicalization Algorithm

Signature Algorithm: The Signature Algorithm should be SHA512withRSA - http://www.w3.org/2001/04/xmldsig-more#rsa-sha512

This type of message is known as a detached signature.

Oasis Standards References: There must be two Reference elements (`Envelope/Header/Security/Signature/SignedInfo/Reference`) in the SignedInfo element.

- One Reference element should correspond to the signed Body element within the message. The Reference corresponding to the Body should have an id attribute whose value is the same as the Id attribute of the SOAP `<body>` element.
- The other Reference corresponds to the Timestamp. The Reference corresponding to the Timestamp should have an id attribute whose value is the same as the Id attribute of the SOAP `<Timestamp>` element.

Both References should have a single transform – Exclusive Canonicalization (see the URI above). The Digest Algorithm should be SHA512 - http://www.w3.org/2001/04/xmlenc#sha512.

4.2.3.2 SignatureValue

For the SignatureValue (`Envelope/Header/Security/Signature/SignatureValue`) extract the private key from the .p12 file. Please see Appendix A – Extracting from a .p12 File for instructions on how to do this.

4.2.3.3 KeyInfo

The KeyInfo contains a SecurityTokenReference element which contains a Reference corresponding to the BinarySecurityToken from Section 4.2.1 (`Envelope/Header/Security/Signature/KeyInfo/SecurityTokenReference/Reference`).

The `URI` attribute of the Reference should reference the Id attribute of the BinarySecurityToken element. For example, if the Id attribute of the BinarySecurityToken is “X509Token”, the URI attribute of the Reference subelement should be “#X509Token”.

5. Example Messages

There is an adjoining Zip file containing SOAP XML examples that have been discussed in this document.

Monetary figures in all examples are for illustrative purposes only.

Appendix A – Extracting from a .p12 File

Each customer of ROS will have a digital certificate and private key stored in an industry standard PKCS#12 file.

In order to create a digital signature, the private key of the customer must be accessed. A password is required to retrieve the private key from the P12 file. This password can be obtained by prompting the user for their password.

The password on the P12 is not the same as the password entered by the customer. It is in fact the MD5 hash of that password, followed by the Base64-encoding of the resultant bytes.

To calculate the hashed password, follow these steps:

1. First get the bytes of the original password, assuming a "Latin-1" encoding. For the password "Baltimore1," these bytes are: 66 97 108 116 105 109 111 114 101 49 44 (i.e. the value of "B" is 66, "a" is 97, etc.).
2. Then get the MD5 hash of these bytes. MD5 is a standard, public algorithm. Once again, for the password "Baltimore1," these bytes work out as: 223 238 161 24 62 121 39 143 115 167 51 163 245 231 226 94.
3. Finally, create the new password by Base64-encoding the bytes from the previous step. For example, the password, "Baltimore1," this is “3+6hGD55J49zpzOj9efiXg==”.

This new password can then be used to open a standard ROS P12 file.