

UPU-IP

UPU-IP EAP Get API Integration Guide

Author: Marie Fourny | ARP | Technical Account Manager

Used by: Status: CLASSIFICATION: Created on: ARP Version-1.0 **PUBLIC** 2023/06/20

PostalTechnologyCentre



Version	Date	Author	Organization	Comments
1.0	2023.06.20	M. Fourny	DPTC	Initial document

Document history and version tracking

Referenced documents (optional)

Document	Version	Description
<u>www.upu.int/api</u>		Detailed description UPU-IP EAP Get API

Table of contents

1	Over	<i>r</i> iew
1	.1	About this document: intended audience
1	.2	Terminology and acronyms
1	.3	Introduction
2	EAP G	Set API Web Service4
2	.1	Security - Transport Level Security4
2	.2	Connecting to the EAP Get API with certificate in Microsoft Windows Certificate Stores4
	2.2.1	Create client certificate request and obtain client certificate4
	2.2.2	Verify the certificates installation from Windows server4
	2.2.3	How a certificate is validated6
2	.3	Connecting to the EAP Get API with Java key store or manual certificate request7
	2.3.1	Create manual client certificate request and obtain client certificate7
2	.4	Generating a Web Service proxy client10
2	.5	Methods



1 Overview

1.1 About this document: intended audience

This document is intended for system developers or IT staff of postal organizations and their subsidiaries who are building Web Service client applications to connect their national system to the Electronic Advance PosTransfer (EAP) Get API, which is an independent component of the UPU Interconnection Platform (UPU-IP).

1.2 Terminology and acronyms

Term - acronym	Description
Business partner	Refers to organizations, Designated Operators (DOs), or third-party commercial entities that connect or use UPU-IP to exchange payment and payment-related messages with other business partners. A business partner is designed as sending or receiving partner for various EAPs.
ΕΑΡ	Electronic Advance PosTransfer, information regarding potential postal payment, which has been captured thanks to the PosTransfer app and which will become a real postal payment when customer come to the post office with cash and identity document. UPU-IP EAP component is the central repository to hold EAPs data in independent database (not related to UPU-IP).
Postal payment	A wide range of payment services and instructions, used instead of "money order"
PosTransfer	UPU trademark for postal payment and name of the mobile application presenting the brand and allowing customers to prepare international cash transfers from home.
UPU-IP	UPU Interconnection Platform, central system storing postal payment and exposing APIs to operate on postal payments.
WS	Web Service

1.3 Introduction

The UPU-IP EAP is the central repository for the Electronic Advance PosTransfers (EAP), draft as captured by customer in the PosTransfer app. The UPU-IP EAP is an independent component of the UPU-IP.

Business partner can publish the PosTransfer app to provide their customers with the ability to prepare international cash transfers from home. At the end of the data capture process, end-customers will obtain a temporary number. This is a reference to a pre-filled PosTransfer stored in the central repository UPU-IP EAP.

At the time, customers are ready to issue international cash postal payment and come to the post office, this temporary number will be necessary at the counter for the postal staff to retrieve the data already stored into UPU-IP EAP. The system used by postal staff may be business partner's national system or future versions of IFS Cloud system connecting to the EAP Get API.



2 EAP Get API Web Service

The UPU-IP EAP has a Web Service Interface, which is exposed to business partners. Using the exposed Web Service (WS), business partners are able to build their own web client applications to retrieve the prefilled EAP data, which was captured by their customer thanks to the PosTransfer app.

Business partners integrating with the EAP Get API can retrieve all the PosTransfer EAP data based on the PosTransfer code, including pictures of identity documents. They can speed up PosTransfer emission time at the counter (no paper form filling, no identity documents' scanning) and improve compliance of recorded data as it has already be prevalidated against bilateral agreement in the PosTransfer app.

2.1 Security - Transport Level Security

Transport Level Security (TLS) is an evolved version of Secure Socket Layer (SSL). Using x.509 certificate, TLS ensures end-to-end security of data sent between applications, avoiding possible eavesdropping or alteration of the content being transported.

Web service requests and responses to and from EAP Get API are authenticated with x.509 certificates and encrypted.

2.2 Connecting to the EAP Get API with certificate in Microsoft Windows Certificate Stores

2.2.1 Create client certificate request and obtain client certificate

Before access to the Web Service Interface is granted, business partners must first generate a Certificate Signing Request (CSR) on the machine hosting the WS client. The CSR must be sent to the UPU for it to be signed then returned to business partners. In addition to the signed certificate, the PTC root Certificate Authority (CA) and sub-CA certificates provided by the PTC must be installed to ensure the chain of trust with the PTC root CA. Once the certificates are installed, business partners can access the EAP Get API.

Refer to the <u>PTC Enroll Client tool and its documentation</u> to perform the following tasks: create the certificate request and submit it to the PTC, install CA and sub-CA certificates, retrieve signed certificate for the machine and install it, and test the SSL connection.

To get a copy of the PTC Enroll Client tool, you can enter your service request at <u>https://support.upu.int</u>

2.2.2 Verify the certificates installation from Windows server



- 1. Open the Microsoft Management Console (MMC) by clicking Start then typing mmc in the Search field. The MMC window opens.
- 2. Add Snap-in to manage Certificates for Computer account:

Console1 - [Console Root]			- 🗆 ×
🚡 Fi 🚺 tion View Favor	ites Window Helj		- 8 ×
🔶 New	Ctrl+N		
Copen	Ctrl+O	Name	Actions
Save	Ctrl+S		Console Root
Save As		There are no items to show in this view.	Mare Artices
Add/Remove Span-in	2 trl+M		More Actions
Ontions		Add or Remove Snap-ins	×
opuonisii		Ver and select many ine for this seconds from these statistics as any second sections. We calculated at af some ine way	
1 compregnt		rou can select snap-ins for one consider non-chose available on your computer and computer the selected set or snap-ins. For extensible snap-ins, you can configure which extensions are enabled.	
2 wf		Available snap-ins: Selected snap-ins:	
3 devrogmt		Snan-in Vendor A Console Root Edit Extensions	
Exit		ActiveX Control Microsoft Cor	
		Authorization Manager Microsoft Cor	
		Certificates 3 Microsoft Cor	
		Component Services Microsoft Cor Move Up	
		Move Down	
		Disk Management Microsoft and Add > 4	
		Event Viewer Microsoft Cor	
		Folder Microsoft Cor	
		Totemet Information. Microsoft Cor	
		BP Security Monitor Microsoft Cor	
		B IP Security Policy M Microsoft Cor	
			-
		Description:	_
		The Certificates snap-in allows you to provise the contents of the certificate stores for yourself, a service, or a computer.	
		OK Cancel	
Enables you to add snap-ins to or	remove them from th	snap-in console.	
		Certificates span-in	×
		Connexted shipp in	~
		This snap-in will always manage certificates for:	
		O my user account	
		O Service account	
		Computer account	
		< Back Next > Cancel	
		Caller	

3. Open the signed certificate you have installed and check the Certification Path tab. If all certificates are installed properly, your window will show the correct installation paths, as in the example below.

General Details	Certification Path
Certification pa	th
PTC CA o	n Dev





Confidence Format User Confidence Format User Confidence Format User Confidence Confiden	n rite Aluuni view Pavorites Window Hei 🕨 🔿 📶 🛍 🙆 🔂 🔢	þ								- 6
	Concrete Rest Concrete User Concret	Itsuet To Client of Client of PTC St	Issued By PTC Enrollment Sub CA PreProd ertificate with private key ate Authority certificate. P ubordinate CA certificate	Expiration Date 11/15/2016	Intended Purpose	Friendly Name chiene>	Status	Certi	Actions Certificates More Actions	

4. You can also verify whether the certificate you have installed has a private key. Open the certificate then click the **General** tab.

	Certificate Information
Thi	 scertificate is intended for the following purpose(s): Ensures the identity of a remote computer
	Issued to: INT-WRK-01.internal.ptc-prod.net
	Issued by: PTC Enrolment Sub CA INTERN-IFS-30
?	Valid from 3/ 16/ 2017 to 3/ 16/ 2022 You have a private key that corresponds to this certificate.

2.2.3 How a certificate is validated

Each time a business partner's WS client application makes a call to the EAP Get API, the certificate is validated against the UPU-IP's PTC root CA for authenticity and trustworthiness.



2.3 Connecting to the EAP Get API with Java key store or manual certificate request

2.3.1 Create manual client certificate request and obtain client certificate

PTC's Enroll Client tool is based on the Windows solution and may not be compatible with non-Windows based servers or integration based on Java Key Stores. In such situation, the partner may have to generate a standard client certificate and submit a service request to the UPU via our ticketing system to get a certificate.

This document describes the process and the requirements to generate and retrieve a valid request for a client certificate connecting to EAP Get API.

Requesting a client certificate from a non-Windows-based OS

Follow the procedure below to obtain a client certificate to connect to the UPU-IP API from a non-Windows-based operating system:

1. Collect the certificate files for the PTC Certificate Authority and PTC Enrollment subordinate certificate authority, which may have to be installed on the non-Windows server.

Certificate	Platform	URL
PTC Certificate Authority	Production	n/a yet, provided as attachment for the moment
PTC Certificate Authority	Pre-production	n/a yet, provided as attachment for the moment
PTC Enrollment Sub CA	Production	n/a yet, provided as attachment for the moment
PTC Enrollment Sub CA	Pre-production	n/a yet, provided as attachment for the moment

2. Generate a standard PKCS #10 client certificate request that meets the following requirements:

Request property	Expectation
Request format	PKCS #10
Friendly name	The title given to a certificate
CN -Common name attribute in Subject	The public URL of the server, for example, yoursite.com
SAN - Subject Alternative Name	The domain names and IP addresses of the server requesting the certificate. This is an optional attribute. However, since the development of the security protocols requires SAN specifications, it is recommended to specify at least the public URL of the server as done in the common name attribute of the subject. E.g. DNS Name=yoursite.com
E - Email attribute in Subject	The email address of the contact handling certificate request and renewal for this certificate
L - Locality attribute in Subject	The locality in which the certificate to be generated will reside based on this certificate request
S - State attribute in Subject	The state or province in which the certificate to be generated will reside based on this certificate request
C - Country attribute in Subject	The two-letter code of the country where your organization is located
O - Organization attribute in	The organization code for which the certificate will be produced, such as the
Subject	Spanish organization code J1CESA. This information is essential since it can be used to confirm validate that the EAP Get API caller is authorized to retrieve data related to this organization
OU - Organization Unit attribute in Subject	Server





Request property	Expectation
Key usage	Data encipherment
	Digital signature
	Key encipherment
Extended Key Usage	Client Authentication
(application policies)	
Key size	2048
Hash algorithm	Sha256
File export format of	Base 64 file
the certificate request	
file	

Alternative option to produce the client certificate with Java SDK and OpenSSL:

<u>Prerequisites</u>

- EAP-GET Package from UPU
- Java JDK installed on the machine
- OpenSSL

Steps

Prepare client certificate key and request

- Copy EAP-Get Package on the server to be enrolled
- Run the EAP-GetPackage\1_CreatePrivateKeyAndCertificateRequest.bat script
 It prompts for details to be included in the certificate request and openSSL executable path.
 It generates a file with ".key" extension (file with client certificate key) and ".csr" extension (file with client certificate request).

Submit client certificate request to obtain client certificate

PTC Enroll tool can be used to submit the csr file, but if the PTC Enroll tool cannot be installed on the server, follow these steps

- Raise a service request: Log into UPU's ticketing system <u>https://support.upu.int</u>.
- Go to the Service Catalog, click on Services for Postal Operations and, under the Postal Payment Services category, raise a new request for Post*Net Finance. Attach the client certificate request (.csr) file to the ticket and indicate whether the request is for a pre-production or production environment.
- While handling the service request, PTC will use the PTC enroll tool on its servers to submit the request, approved it and provide the issued certificate as an attachment to the ticket. The provided file will be a .cer file Base 64 exported file (converted from the PTC Enroll tool to the Base 64 with full CA chain).



← → C ①	5f5f1bef55715							Q p2	* 2 *	- n n
Official PTC Tools Translation Documents	ation 📙 IPS 📒 CSS	📒 QualityOfService 📒 UPU-IP	Reuters	IFS Cloud	PTC Enrolment	IFS 4.50	eCompendium	UVUX Materials	DPS	RefData
SERVICE DESK	HOME	SERVICE CATALOG		Ţ 9	()**	ି		E	FOURNY ma	rie 🕒
News Welcome to the UPU Service	Desk									
		SE	RVICE CAT	TALOG						
Catalog	Search for a s	ervice								q
IB Services										
Services for postal operations										
UPU Members and Delegates Services										
Category					IFS INANCIAL	IONAL.	P	OST*Ne	t Fina	nce
Compendia								•		
Customs		Eurogiro Interconnection		175	- International Financ	e System		Past*Ne	Finance	_
Mail			i							
Postal Payment Services										
PTC Hosted Cloud Services		PosTransfer 5 App		PPS *	Clearin	G SERVICES CLEANING	INT		R	
Security & Access										
Other Services							_			
		PosTransfer App			PPS+Clearing					

Convert the client certificate to a java key store

- Copy the Base 64 client certificate into the EAP-Get Package folder
- Run the EAP-GetPackage\4_CreateJavaKeyStore.bat script

It prompts for details of the client certificate, Password to use during the java key store creation, openSSL and java Runtime executable paths.

The script generate the java private key (p12 file) and the java key store which will contain the java private key, client certificate and full CA chain in one store file (.jks).

It prompts several times for the password to protect the private key and java key store (always use the same value).

The generated jks file can be used in Java application with the specified password.



2.4 Generating a Web Service proxy client

To build your WS proxy client application, EAP Get API endpoints and documentation is available online at the following URLs, to be used with proper client certificate:

Pre-production (for integration and test activities): <u>http://eap.preprod.upu.org/eap.api/</u>

Production : <u>http://eap.ptc.post/EAP.API/</u>

Contact the PTC Service Desk at <u>https://support.upu.int</u> if you encounter difficulties connecting.

2.5 Methods

For a complete list of the methods that the Web Service Interface exposes, see the EAP Get API documentation at www.upu.int/api