A

WIPO
المنظمة العالمية
للملكية الفكرية

1 أكتوبر 2021

خدمات لاهاي الإلكترونية

المحتويات

المقدمة

النطاق

هذه الوثيقة عبارة عن مقدمة لخدمات لاهاي الإلكترونية، وهي واجهة للتواصل بين الأجهزة (M2M) خاصة بنظام لاهاي.

نظرة عامة

خدمات لاهاي الإلكترونية هي بروتوكول آمن، ويمكن النفاذ إليه بسهولة، وموثوق، وهو بروتوكول قائم على واجهة برمجة التطبيقات التي تستخدم بروتوكول نقل النص التشعبي الآمن (HTTPS)/نقل الحالة التمثيلية (REST) لتبادل البيانات مع نظام لاهاي. ويمكن استخدامها لإرسال أو استقبال البيانات.

ويمكن استخدام خدمات لاهاي الإلكترونية من أجل:

- إرسال قرارات أو طلبات غير مباشرة
- التحقق من حالة استيراد السندات
- حالة معالجة الاستعلام
- الحصول على نشرات لاهاي
- الحصول على النسخ السرية (مكاتب الملكية الفكرية التي لها صفة الفحص فقط).

خدمات لاهاي الإلكترونية هي قناة نظام لاهاي المفضلة لتبادل البيانات. لذلك، تُشجع مكاتب الملكية الفكرية بشدة على استخدام تلك الخدمات من البداية. كما تُشجع المكاتب التي تتبادل البيانات بالفعل مع نظام لاهاي عبر التبادل الإلكتروني للبيانات/الورق/القنوات الأخرى على الانتقال إلى نظام خدمات لاهاي الإلكترونية.

المصادقة والأمان

أمان واجهة برمجة التطبيقات

صُممت واجهة برمجة التطبيقات الخاصة بخدمات لاهاي الإلكترونية للتواصل بين الأجهزة باستخدام حمولات سرية.

تعتمد المصادقة على توقيع مفتاح غير متماثل يعد جزءًا من النسخة 1.0 من نمط أمان واجهة برمجة التطبيقات من الدرجة المالية. (Financial-grade API Security Profile 1.0) ويمكن تطبيق نمط أمان لواجهة برمجة التطبيقات من الدرجة المالية على واجهات برمجة التطبيقات في أي مجال سوقي يتطلب مستوى أمان أعلى من الذي يوفره بروتوكول OAuth القياسي أو أداة التحقق من المستخدم النهائي OpenID Connect، وهذا يعني أنه يحتوي على نمط أمان متطور من بروتوكول OAuth المناسب لحماية واجهات برمجة التطبيقات المتضمنة لمخاطر متأصلة عالية.

إنشاء الأزواج الرئيسية وإسناد المعرفات للعملاء

يوضح الرسم البياني أدناه العملية الشاملة لتسجيل معرف عملاء واجهة برمجة التطبيقات والمفتاح العام للويبو بالإضافة إلى عنوان بروتوكول الإنترنت (IP address) العام لطلب العميل.

إجراءات المكتب:

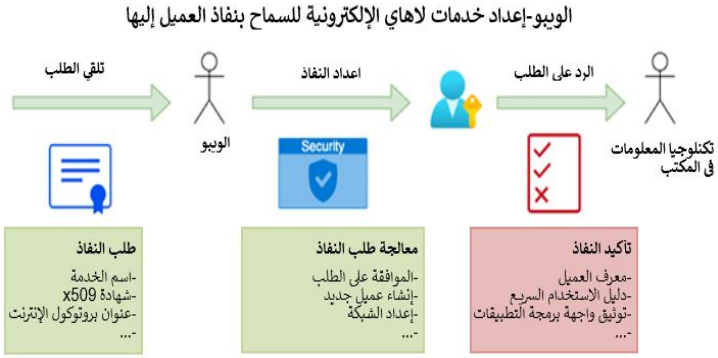
1. إنشاء زوج من المفاتيح العامة والخاصة (انظر الملحق ألف: إنشاء العميل زوج من المفاتيح على نظام OpenSSL).
2. إصدار الشهادة x509 باستخدام المفتاح العام.
3. طلب النفاذ إلى خدمات لاهاي الإلكترونية عن طريق إرسال بريد إلكتروني إلى hague.it@wipo.int يشمل:

   (أ) ملء استمارة الويبو (انظر الملحق باء: استمارة طلب النفاذ إلى واجهة برمجة التطبيقات لتكنولوجيا المعلومات والاتصالات الخاصة بالويبو)؛

   (ب) الشهادة X509.

إجراءات الويبو:

1. بعد استلام ما ورد أعلاه، تُنشئ معرّف العميل.
2. إسناد/ربط المفتاح العام بمعرف العميل.
3. إضافة عنوان بروتوكول الإنترنت إلى القائمة البيضاء.
4. إعداد خدمات لاهاي الإلكترونية من أجل السماح لمعرف العميل القيام بالطلبات.
5. تأكيد معرف العميل لمكتب الملكية الفكرية.

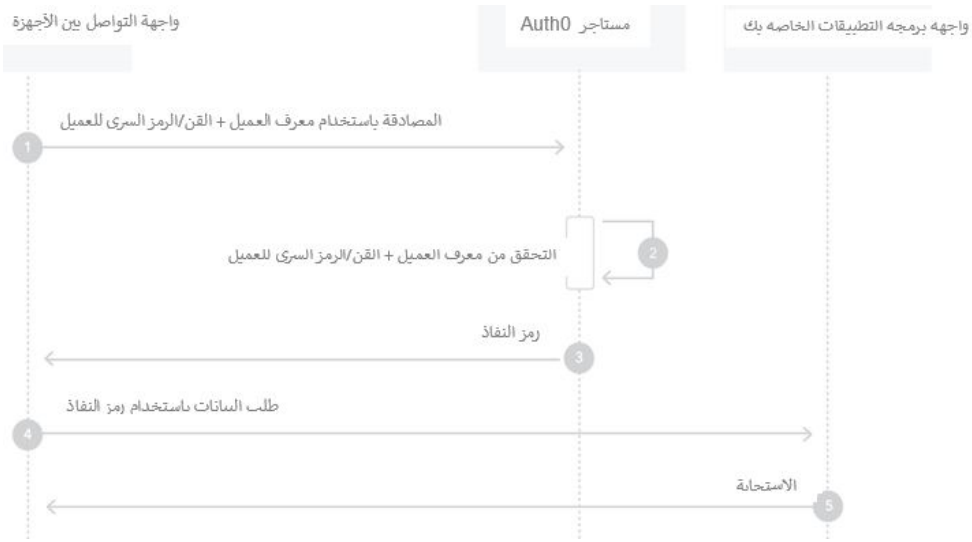


المصادقة على خدمات لاهاي الإلكترونية

بمجرد تسجيل معرف العميل والمفتاح العام وعنوان بروتوكول الإنترنت العام في الويبو، وإعداد خدمات لاهاي الإلكترونية، يصبح مكتب الملكية الفكرية جاهزًا لاستخدام واجهة برمجة التطبيقات.

ويوضح الرسم البياني أدناه الكيفية التي يتم بها التفاعل مع واجهة الخدمات:

1. طلب HTTPS إلى مستأجر Auth0 معرّف العميل ورمز JWT
2. التشفير بواسطة المفتاح الخاص. ملاحظة: **يجب** أن يأتي الطلب من عنوان بروتوكول الإنترنت المدرج في القائمة البيضاء.
3. يتم التحقق من صحة طلب HTTPS ويُنشأ رمز JWT لإتاحة النفاذ.
4. عند نجاح العملية، يتم إرجاع رمز النفاذ JWT مع انتهاء صلاحيته بعد ساعة واحدة.
5. يمكن إجراء استدعاءات نقاط نهاية HTTPS الموالية في نافذة انتهاء الصلاحية باستخدام رمز النفاذ JWT نفسه.



وصف واجهة برمجة التطبيقات

تنفذ واجهة برمجة التطبيقات الخاصة بخدمات لاهاي الإلكترونية نقاط نهاية REST التالية:

1. إرسال الطلبات والقرارات غير المباشرة إلى نظام لاهاي (POST/request).
2. التحقق من حالة استيراد سندات طلب غير مباشر أو قرار تم إرساله (GET/request/import).
3. الاستعلام عن حالة طلب خدمة معينة (GET /request/{serviceRequestId}).
4. الحصول على النشرة المتضمنة للمعلومات (GET /publication/bulletin/{weekId})
5. الحصول على النسخة السرية (GET /publication/copy/confidential/{weekId})

ويمكن الاطلاع على التفاصيل الكاملة حول واجهة برمجة التطبيقات الخاصة بخدمات لاهاي الإلكترونية (المعلمات والاستجابات وما إلى ذلك) في الملحق دال: واجهة برمجة التطبيقات للمنصة العامة لنظام لاهاي.

وتستند جميع الحمولات إلى معيار XML المستخدم في الويبو، وهو المعيار ST.96. ويمكن الاطلاع على التفاصيل الكاملة حول الإصدار 0.4 من المعيار ST.96 وعلى مخططات لغة الترميز الموسعة (XSDs) على الرابط https://www.wipo.int/standards/en/st96/v4-0/. وتوجد الأنساق الثانوية المطلوبة على وجه التحديد في الخدمات الإلكترونية في طور التوحيد القياسي.

ملاحظة: هناك نقطة نهاية تسمى pingMe يمكن استخدامها للتحقق من الاتصال من جهة العميل وجهة خدمات لاهاي الإلكترونية. وليست لهذه النقطة أية وظيفة، ولكنها متاحة لأغراض إجراء الاختبار التقني وعمليات التحقق.

إرسال الطلبات والقرارات غير المباشرة إلى نظام لاهاي (POST/request).

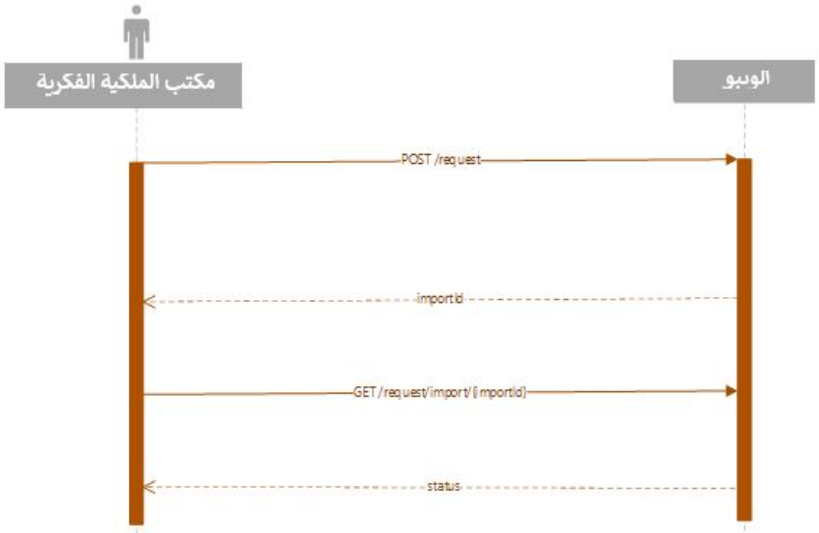
يتم إرسال الطلبات والقرارات إلى نظام لاهاي من خلال طلب POST، حيث تكون الحمولة هي حزمة مستندات الاستيراد (انظر أدناه).

ويتم توليد معرف استيراد لكل حزمة عند نجاح عملية الإرسال، مما يعني أنه تم استلام حزمة مستندات الاستيراد وسيقوم المكتب الدولي بمعالجتها.

ويمكن استخدام معرف استيراد الحزمة هذا لاحقًا للحصول على رقم طلب الخدمة (GET request/import)، وبالتالي يمكن استخدام رقم طلب الخدمة للحصول على حالة الطلب (طلب GET).

وحمولة الطلب المودع وطلب القرار هي ملف مضغوط واحد يحتوي على المعيار ST.96 بنسق XML ومستندات وصور.

- يجب وضع هذه الملفات في المسار النسبي كما هو موضح في مخطط XML.
- يجب أن يحتوي الملف المضغوط (وبالتالي حمولة الطلب) على طلب واحد فقط أو قرار واحد.
- لا يمكن أن تحتوي الحمولة على أكثر من ملف XML واحد.
- يمكن الاطلاع على أمثلة على المسار ftp://ftpird.wipo.int/ST96_V_4_0_test/import-packages-4.0.zip.



الاستعلام عن حالة طلب خدمة معينة (GET /request/{serviceRequestId})

بعد استيراد نظام لاهاي الحزمة، يُطلق على المعاملة اسم طلب الخدمة (SR) ويُسند لها رقم يُسمى رقم طلب الخدمة (SRN). ويمكن الحصول على هذا الرقم من خلال نقطة النهاية GET request/import (انظر أعلاه).

وبمجرد توفر رقم طلب الخدمة، يمكن الحصول على حالة الطلب باستخدام نقطة نهاية الطلب.

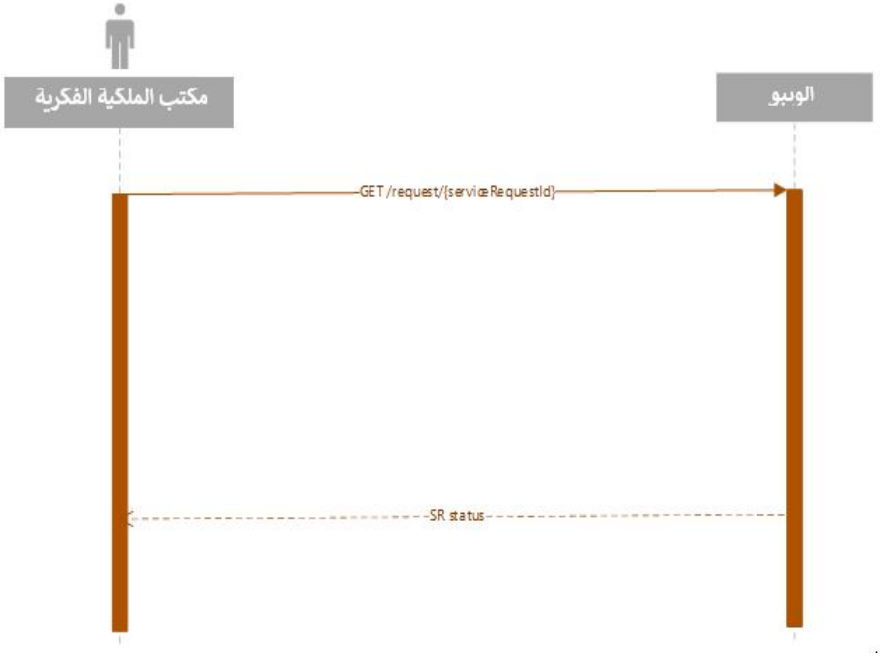
وتتمثل أنواع الحالة التي سيُتحصل عليها:

- غير محدد
- قيد المعالجة
- في انتظار التسوية
- مسجل
- مهجور
- ملغى

وردًا على الاستعلام عن حالة طلب الخدمة، ترسل خدمات لاهاي الإلكترونية حمولة بموجب المعيار ST.96 تشمل:

- معرف الطلب
- حالة المعالجة

- رقم طلب الخدمة
- رقم التسجيل الدولي (IRN)
- عند الاقتضاء، تاريخ النشر المتوقع.



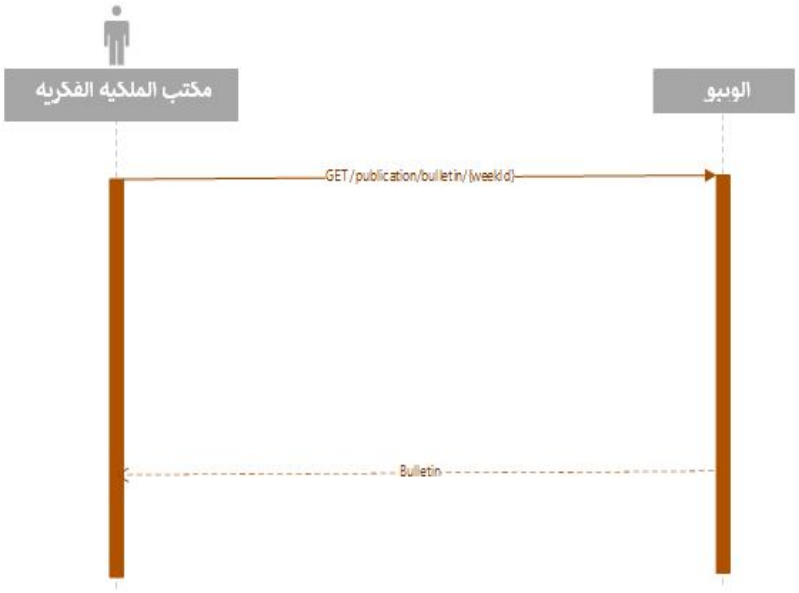
الحصول على النشرة المتضمنة للمعلومات (GET /publication/bulletin/{weekId})

يصدر المكتب الدولي النشرات أسبوعيا، عادةً في ليلة الجمعة (توقيت وسط أوروبا). ويمكن طلبها في أي وقت بعد إنشائها. ويكون نسق معلمة weekId هو yyyyww.

وتضم حمولة الاستجابة على ملف مضغوط بالمحتويات التالية:

- البيانات الببليوغرافية للنشرة كملف المعيار ST.96؛
- مجلدات الصور المتعلقة بالتسجيلات المشمولة أو الصور التي أُجريت عليها التصويبات.

على سبيل المثال، يمكن الاطلاع على حمولات النشرات (النسخ السرية لها نفس البنية) على المسار ftp://ftpird.wipo.int / ST96_V_4_0.



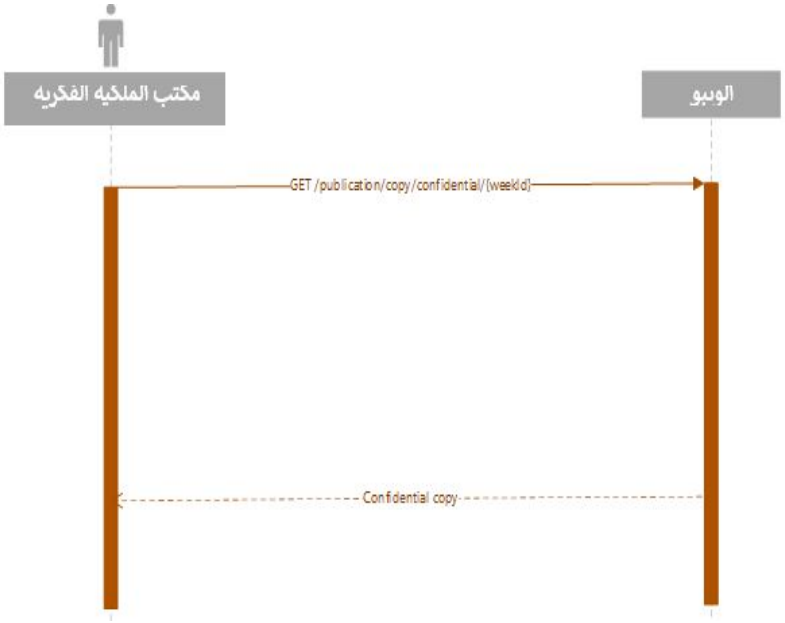
الحصول على النسخة السرية (GET /publication/copy/confidential/{weekId})

للنسخ السرية نفس بنية النشرات.

يصدر المكتب الدولي النسخ السرية أسبوعيا، عادةً في ليلة الجمعة (توقيت وسط أوروبا). ويمكن طلبها في أي وقت بعد إنشائها. ويكون نسق معلمة weekId هو yyyyww.

وتضم حمولة الاستجابة على ملف مضغوط بالمحتويات التالية:

- البيانات الببليوغرافية من النسخة السرية كملف المعيار ST.96؛
- مجلدات الصور المتعلقة بالتسجيلات المشمولة أو الصور التي أُجريت عليها التصويبات.



الملحق ألف: إنشاء العميل زوج من المفاتيح على نظام OPENSSL

قم بإنشاء زوج من المفاتيح الخاصة/العامة غير متماثل وشهادة x509 للتسجيل من خلال التواصل بين الأجهزة في الويبو.

إنشاء عناصر التسجيل في أداة الويبو للتحقق من المستخدم النهائي OpenID Connect (OIDC)

```
#!/bin/bash

# Set the environment
PRIVATE_KEY_ES256=hague4offices_private.pem
PUBLIC_KEY_ES256=hague4offices_public.pem
CLIENT_NAME=DAS

# Generates the ES256 keys
openssl ecparam -genkey -name prime256v1 -noout -out "${PRIVATE_KEY_ES256}"

# Extracts the public key
openssl ec -in "${PRIVATE_KEY_ES256}" -pubout -out "${PUBLIC_KEY_ES256}"

# Generates an x509 certificate
CERT_KEY_ES256=es256_cert.pem
OPENSSL_CONF=./openssl.cnf
CERT_CN="${CLIENT_NAME} private_key_jwt authentication"

# Build the certificate config file
printf '[ req ]\n' > "${OPENSSL_CONF}"
printf 'prompt = no\n' >> "${OPENSSL_CONF}"
printf 'distinguished_name = req_distinguished_name\n' >> "${OPENSSL_CONF}"
printf '[ req_distinguished_name ]\n' >> "${OPENSSL_CONF}"
printf 'CN = %s\n' "${CERT_CN}" >> "${OPENSSL_CONF}"

# Creates the x509 certificate
openssl req -x509 -new -config "${OPENSSL_CONF}" -key "${PRIVATE_KEY_ES256}" -out
"${CERT_KEY_ES256}"
```

1. أرسل **es256_cert.pem** إلى الويبو لإعداد النفاذ إلى خدمات لاهاي الإلكترونية (يجب أن تظل **hague4offices_private.pem** دائمًا سرية وألا تتم مشاركتها مطلقًا أحد).
2. انتظر حتى توفر لك الويبو **معرف العميل** و**النطاق** بعد عملية الإعداد.
3. اختبر الاتصال باستخدام طلب تجريبي بموجب نظام لاهاي مخصص للعميل (سيؤكد الرابط لاحقا).

الملحق باء: استمارة طلب النفاذ إلى واجهة برمجة التطبيقات لتكنولوجيا المعلومات والاتصالات الخاصة بالويبو

الاستمارات أدناه هي مجرد مسودات اعدتها من الويبو. وتجدر الإشارة إلى أن النسخة النهائية من تلك الاستمارات معلقة وستؤكد لاحقا. (2021/09/01).

يُرجى ملء هذا الاستمارة لتقديم معلومات عامة حول السياق.

معلومات عامة	
نوع الطلب؟	طلب إنشاء الطلب ☐ تحديث الطلب ☐
صف المعلومات المحدثة[1]	معلومات الاتصال ☐ نطاق عنوان بروتوكول الإنترنت الخاص بالعميل ☐ الشهادة ☐ النطاقات ☐
البيئة[2]	الإصدار
اسم الطلب على واجهة برمجة التطبيقات	
وصف الطلب	
العنوان الشبكي (العناوين الشبكية) لواجهة برمجة التطبيقات	
صاحب الطلب	
العنوان البريدي لصاحب الطلب[3]	
اسم جهة الاتصال التقنية المعنية بالطلب	
البريد الإلكتروني لجهة الاتصال التقنية المعنية بالطلب[4]	
من الذي سيَنْفُذ إلى الطلب؟	الأشخاص الداخليون ☐ الأشخاص الخارجيون ☐
كيف تتم حماية واجهة برمجة التطبيقات؟	استخدام رمز النفاذ الذي تم الحصول عليه عبر بروتوكول Oauth 2 الخاص بتدفق بيانات نفاذ العميل

[1] يرجى تقديم هذه المعلومات فقط في حالة الطلب التحديث.
[2] يُرجى اختيار البيئة.
[3] سيُستخدم للإخطار عند التخطيط لنشر مكون مقدم بروتوكول Oauth2 في عملية الإنتاج ويمكن أن يكون له تأثير على الطلب.
[4] سيُستخدم للإخطار عند التخطيط لنشر مكون مقدم بروتوكول Oauth2 في عملية الإنتاج ويمكن أن يكون له تأثير على الطلب.

يُرجى ملء هذا الاستمارة لتقديم معلومات عامة حول السياق.

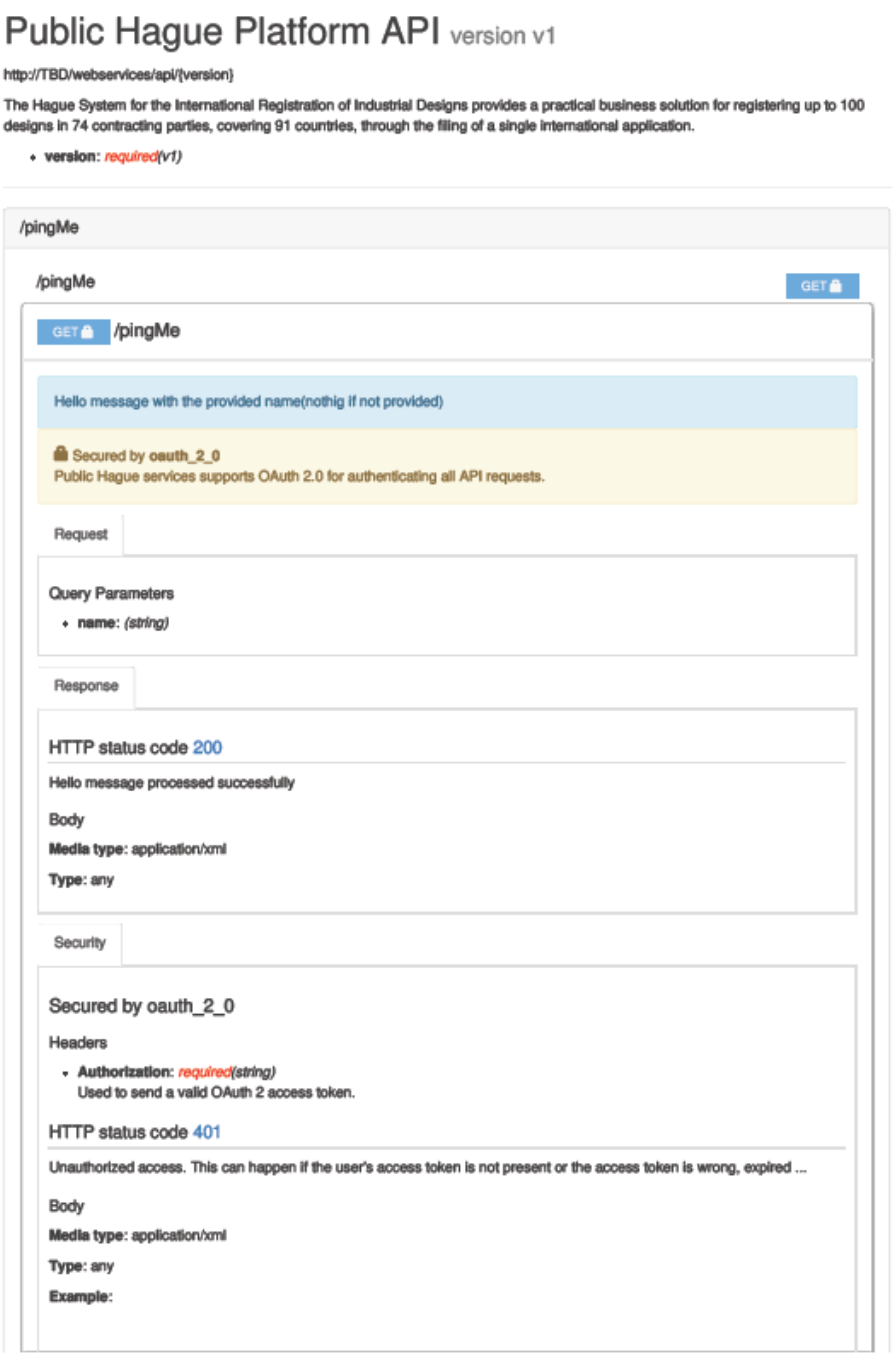
حماية واجهة برمجة التطبيقات باستخدام البروتوكول OAuth2	
معرف العميل	ستوفره الويبو
نوع العميل	سري
النطاقات المدعومة (اختياري)	حسب الأنماط التلقائية
الشهادة (X509V3 - ES256)	
نطاق عنوان بروتوكول الإنترنت الخاص بالعميل	
طريقة مصادقة العميل	الرمز الخاص JWT (يرسل العميل بيانات نفاذه باستخدام JWT)

الملحق جيم: مقتطف للحصول على رمز النفاذ من منصة إدارة الهوية والنفاذ وتشفير البيانات (OPENAM) في الويبو

يعد نص باش (script bash) أدناه مثالاً لطلب مصادقة الويبو باستخدام المفتاح الخاص لمكتب الملكية الفكرية:

```
#!/bin/bash
PRIVATE_KEY_ES256=es256_private.pem
CLIENT_ID=das-api-auth
SCOPE="das-api/das-access"
ISSUER="https://logindev.wipo.int/am/oauth2"

# https://logindev.wipo.int/am/oauth2/.well-known/openid-configuration
OIDC_CONFIG_JSON=$(curl -k "${ISSUER}/.well-known/openid-configuration")

# Generic way to obtain the token endpoint
TOKEN_ENDPOINT=$(printf '%s' ${OIDC_CONFIG_JSON} | jq -r ".token_endpoint")
UTC_TIME=$(date -u +%s)
EXP_TIME=$(expr "$UTC_TIME" + 10)
JWT_ID=Un1qu3i0

JSON='{'
JSON=${JSON}$(printf '"iss":"%s"' ${CLIENT_ID})
JSON=${JSON}$(printf ',"sub":"%s"' ${CLIENT_ID})
JSON=${JSON}$(printf ',"aud":"%s"' ${TOKEN_ENDPOINT})
JSON=${JSON}$(printf ',"exp":%s' ${EXP_TIME})
JSON=${JSON}'}'

JSON_HEADER_B64=$(printf '{"alg":"ES256","typ":"JWT"}' | jq -cj | base64 -w0 | tr -d
'\n=' | tr '+/' '-_')

JSON_PAYLOAD_B64=$(printf $JSON | jq -cj | base64 -w0 | tr -d '\n=' | tr '+/' '-_')

JSON_SIGNATURE_ASN1_B64=$(printf '%s.%s' $JSON_HEADER_B64 $JSON_PAYLOAD_B64 | openssl
dgst -sha256 -sign"${PRIVATE_KEY_ES256}" | openssl asn1parse -inform DER | base64 -w0)
JSON_SIGNATURE_HEX=$(printf $JSON_SIGNATURE_ASN1_B64 | base64 -d | sed -n '/INTEGER/p'
| sed 's/.*INTEGER\s*://g' | sed -z 's/[^0-9A-F]//g')
JSON_SIGNATURE_B64=$(printf $JSON_SIGNATURE_HEX | xxd -p -r | base64 -w0 | tr -d '\n='
| tr '+/' '-_')

JWT_ASSERTION=$(printf '%s.%s.%s' $JSON_HEADER_B64 $JSON_PAYLOAD_B64
$JSON_SIGNATURE_B64)

# echo $JWT_ASSERTION
# Access token private_key_jwt
# --insecure is only needed when testing within WIPO premises (because of the
proxy...)
curl \
  --header "Content-Type: application/x-www-form-urlencoded" \
  --data-urlencode "grant_type=client_credentials" \
  --data-urlencode scope="${SCOPE}" \
  --data-urlencode "client_assertion_type=urn:ietf:params:oauth:client-assertion-
type:jwt-bearer" \
  --data-urlencode "client_assertion=${JWT_ASSERTION}" \
  --url "${TOKEN_ENDPOINT}"
```

الملحق دال: واجهة برمجة التطبيقات للمنصة العامة لنظام لاهاي



Public Hague Platform API version v1

http://TBD/webservices/api/{version}

The Hague System for the International Registration of Industrial Designs provides a practical business solution for registering up to 100 designs in 74 contracting parties, covering 91 countries, through the filing of a single international application.

- **version:** *required(v1)*

/pingMe

/pingMe GET

GET /pingMe

Hello message with the provided name(nothig if not provided)

Secured by oauth_2_0
Public Hague services supports OAuth 2.0 for authenticating all API requests.

Request

Query Parameters

- **name:** *(string)*

Response

HTTP status code 200

Hello message processed successfully

Body

Media type: application/xml

Type: any

Security

Secured by oauth_2_0

Headers

- **Authorization:** *required(string)*
  Used to send a valid OAuth 2 access token.

HTTP status code 401

Unauthorized access. This can happen if the user's access token is not present or the access token is wrong, expired ...

Body

Media type: application/xml

Type: any

Example:

ملاحظة: ستُدرج معلومات إضافية في الإصدارات اللاحقة من هذه الوثيقة.