Mecanismo de contingencia Triodos Bank

1. Control de versiones

Versión	Fecha	Descripción del cambio	Redactado por	Revisado por
1.0	Julio 2019	Documento inicial		
2.0	01/08/2019	Revisión respuestas json		
3.0	09/08/2019	Revisión respuestas json tras la actualización		

2. Índice

1. CONTROL DE VERSIONES 3
2. ÍNDICE 4
3. INTRODUCCIÓN 5
4. DESCRIPCIÓN 6
5. OBTENCIÓN SELLO 8
6. IDENTIFICACIÓN 9
7. SOLICITUD DE SEGUNDO FACTOR DE AUTENTICACIÓN - LOGIN 11
8. SELECCIÓN DE CONTRATO 12
9. POSICIÓN GLOBAL 13
10. CONSULTA DE MOVIMIENTOS 15
11. CONSULTA DE SALDOS 16
12. CONSULTA DE COMISIONES 18
13. RECUPERACIÓN DE LA MÁSCARA DE FIRMAS 19
14. TRANSFERENCIA 20
15. SOLICITUD DE SEGUNDO FACTOR DE AUTENTICACIÓN - TRANSFERENCIA 21
16. DESCONEXIÓN 22

3. Introducción

Se describe el detalle del mecanismo de contingencia específico para Triodos Bank.

4. Descripción

Los servicios que se documentan son los siguientes:

- Obtención del sello/clave para la identificación
- Identificación (previa obtención del sello/clave con la llamada a sello/clave)
- Solicitud de segundo factor de autenticación - Login
- Selección de contrato.
- Posición global
- Consulta de saldos
- Consulta de movimientos
- Consulta de comisiones
- Recuperación de seguridad (posiciones de la firma)
- Transferencia
- Solicitud de segundo factor de autenticación - Transferencia
- Desconexión

Para simplificar la implantación en las distintas aplicaciones móviles, los servicios se invocan mediante la invocación de un servicio web con protocolo https con envío de parámetros por POST, y devuelven formato json.

Para la invocación de los diferentes servicios, previamente se ha debido abrir sesión con el cliente en la plataforma de banca electrónica.

Cada servicio web está asociado a una operativa del canal específico, que debe haber sido autorizada al PSU en función de su perfil. Si el PSU no está autorizado a realizar determinada operativa los servicios devolverán el error pertinentemente

Todos los servicios se invocarán siguiendo el formato de url, dentro de los parámetros comunes a todas las operaciones el campo IDIOMA es significativo.

- IDIOMA=NN

NN el idiocma utilizado por el cliente, dependiendo de la entidad estarán disponibles uno o varios idiomas.
- 01 Castellano

Cada servicio tiene una respuesta específica en caso de que acabe correctamente. De forma general hay una respuesta de error con el siguiente formato.

```
{
        "result": "ko",
        "texto_error":"Texto de error"
}
```

Cada invocación al servicio debe ser firmada con el certificado QSealC del TPP. EL proceso de firma consistirá en formar una cadena de texto tipo GET con todos los parámetros POST de la invocación más un campo FECHAFIRMA=YYYYMMDDHHMMSS y firmar dicha cadena con la clave privada del certificado.

Por ejemplo, para el siguiente conjunto de parámetros POST

- *CAJA=1491*
- *CAMINO=FLBK*
- *OPERACION=0002*
- *IDIOMA=01*
- *SELLO=2019.07.25.12.50.06*
- *PAN= 1R*
- *PIN=53D2184E4C09191E*
- *BROKER=SI*
- *PINV3=si*

Se formará la cadena de texto.

CAJA=1491 &CAMINO=FLBK&OPERACION=0002&IDIOMA=01&SELLO=2019.07.25.12.50.06&
PAN=1R & PIN=53D2184E4C09191E&BROKER=SI&PINV3=si&FECHAFIRMA=20190726121212

Y el resultado de la firma se enviará como parámetro POST con el nombre FIRMAQSEAL.

Adicionalmente se añadirá como parámetro POST el campo FECHAFIRMA con el valor incluido en el proceso de firma de la url

5. Obtención SELLO

Para poder hacer una identificación, es necesario obtener los parámetros: sesión, sello y clave para enviarlos en el resto de invocaciones. En los epígrafes posteriores se explicará cómo usar estos parámetros.

Llamada:

https://be.ceca.es/BEWeb/1491/FLBK/inicio_identificacion_sello.action

Parámetros*:*

Ninguno

Respuesta*:*

```
{
        "JSESSIONID": "nUn0Ir0QfyNDl5MPaYA-kL8_.desabeweb",
        "clave" : "d14671b5ee8b943287597993bbefd9c9ae208d9e387e3487",
        "sello" : "2019.07.29.17.16.54"
}
```

6. Identificación

El objeto de este servicio es validar los datos de usuario y clave recabados del cliente.

Llamada:

https://be.ceca.es/BEWeb/1491/FLBK/oidc_identificacion.action;jsessionid=PSPRlkSpIBHZ2peGp5iIeNTN.desabeweb

Parámetros:

- *CAJA=1491 (Valor fijo)*
- *CAMINO=FLBK (Valor fijo)*
- *OPERACION=0002 (Valor fijo)*
- *IDIOMA=01 (Valor fijo)*
- *SELLO=2019.09.05.12.33.11 (recibido en la invocación del sello)*
- *PAN=9999991491 (Valor fijo)*
- *PANENTIDAD=* 1R *(nif usuario)*
- *PIN=55B87E8835FCEECF (Pin encriptado con la clave recibida en el sello)*
- *BROKER=SI (Valor fijo)*
- *PINV3=si (Valor fijo)*

Para encriptar el PIN es necesario obtener previamente el parámetro “clave” y usar la función de encriptado pinEncriptado=MOD(clave, pinIntroducido). Para ello es necesario tener incorporados los js: MOD3.js, RSA.js, Barret.js y BigInt.js.

El resultado de esta función es el valor que hay que asignarle al parámetro PIN.

Además habrá que añadir a la url el valor “jsessionid” obtenido del servicio SELLO. Tal y como se muestra en el ejemplo de llamada.

Si la conexión es satisfactoria la respuesta será el siguiente json:


```
{
    "result": "ok",
    "otpFlag": "true ",
    "JSESSIONID": "PSPRlkSpIBHZ2peGp5iIeNTN.desabeweb",
    "LLAMADA": "C4X1A2C02350Z051E057",
    "CLIENTE": "1491000190",
    "USERNAME": "NOMBRE",
    "CONTRATOS": [
        {
            "CONTRATO": "0000612564",
            "TIPO": "P",
```

```
            "DESCRIPCION": "RAZON_SOCIAL_0000612564",
            "RELATIONSHIPTYPE": "7"
        }
    ]
}
```


El parámetro LLAMADA también será necesario para invocar las operaciones que se describen a continuación.

7. Solicitud de segundo factor de autenticación - Login

Es posible que, en base a ciertos criterios, se solicite un segundo factor de autenticación para asegurar que el Login que se está realizando no proviene de un TPP externo. Para ello se recibirá una clave OTP en el número de teléfono registrado por el usuario. Una vez introducida, si la autenticación es exitosa, se continuará con el proceso de Login.

Llamada*:*

https://be.ceca.es/BEWeb/1491/FLBK/not6263_d_0.action;jsessionid=3uz7DruhdBeG5JkOE-wP6bMr.desabeweb

Parámetros*:*

- *USUARIO= 78702963E (Identificación del usuario a autenticar)*
- *OTP= F2D2CD11 (Clave recibida en el teléfono asignado por el usuario)*

Si la conexión es satisfactoria la respuesta será el siguiente json:

```
{
  "resultado": "ok"
}
```

8.Selección de contrato

Se realiza la selección del contrato a partir de los contratos recibidos en la login.

Llamada:

https://be.ceca.es/BEWeb/1491/FLBK/selectCtt_2467_d_d_e2467.action

Parámetros:

- *CAJA=1491 (Valor fijo)*
- *CAMINO=FLBK (Valor fijo)*
- *IDIOMA=01 (Valor fijo)*
- *OPERACION=selectCtt_2467_d_d_e2467 (Valor fijo)*
- *CLIENTE= 1491000190 (Cliente ceca recibido en el nodo CLIENTE al llamar al login "oidc_identificacion.action")*
- *LLAMADA=* C4X1A2C02350Z051E057 *(Llamada recibida en el sello)*
- *contratoSeleccionado= 0000612564 (concatenación de los nodos* CONTRATO+RELATIONSHIPTYPE *al llamar al login "oidc_identificacion.action"* siendo el campo RELATIONSHIPTYPE con formato de 2 dígitos*)*
- *username= NOMBRE (Nombre de usuario recibido en el nodo* USERNAME *al llamar al login "oidc_identificacion.action")*

La estructura del json es:

```
{
    "result": "ok"
}
```

9.Posición global

La Posición global devuelve los datos de las cuentas del usuario identificado en formato json.

Llamada POST:

https://be.ceca.es/BEWeb/1491/FLBK/not6261_d_0.action;jsessionid=3uz7DruhdBeG5JkOE-wP6bMr.desabeweb

Parámetros:

- *IDIOMA=01 (Valor fijo)*
- *LLAMADA=* C4X1A2C02350Z051E057 *(Llamada recibida en el sello)*
- *contratoSeleccionado= 0000612564 (concatenación de los nodos* CONTRATO+RELATIONSHIPTYPE *al llamar al login "oidc_identificacion.action"* siendo el campo RELATIONSHIPTYPE con formato de 2 dígitos*)*
- *CAJA=1491 (Valor fijo)*
- *CAMINO=FLBK (Valor fijo)*

La estructura del json de respuesta es:


```
{
    "BLOQUE": [
        {
            "SIGNO": "+",
            "OFICINA": "0001",
            "TIPO": "01",
            "CUENTA": "0000202115009025",
            "TITULARIDAD": "00",
            "SALDO2": "0000000000000000",
            "SALDO": "6.8783.0000",
            "SALDO1": "0000000687830000",
            "MONEDA": "978",
            "IBAN": "ES5314910199990000202115009025",
            "ALIAS": "",
            "GCUENTA": "14910199990000202115009025",
            "ENTIDAD": "1491",
            "MONEDADES": "",
            "CARGO": "CA"
        },
        {RESTO DE CUENTAS}
    ],
    "operacionOK": "6261",
    "resultado": "OK"
}
```

10. Consulta de movimientos

La consulta de movimientos devuelve los movimientos de la cuenta del usuario en formato json.

Llamada POST:

https://be.ceca.es/BEWeb/1491/FLBK/not6262_d_0.action;jsessionid=3uz7DruhdBeG5JkOE-wP6bMr.desabeweb

Parámetros:

- *CAJA=1491 (Valor fijo)*
- *CAMINO=FLBK (Valor fijo)*
- *IDIOMA=01 (Valor fijo)*
- *LLAMADA=* C4X1A2C02350Z051E057 *(Llamada recibida en el sello)*
- *iban= ES5314919999202115009025 (IBAN a consultar los movimientos)*
- *fecIni=01012019 (Fecha de inicio)*
- *fecFin= 31092019 (Fecha fin)*

La estructura del json es:


```
{
   "paginationKey": "",
   "paginationFlag": "false",
   "bloque1": [
        {
            "id": "0000003473",
            "amount": "-000000000002149.05",
            "valueDate": "01062019",
            "reason": "PAGO PRESTAMO",
            "description": "PR 149199993000089573",
            "currentBalance": "+000000000068783.00",
            "code": "SIND",
            "reference": "2081190860",
            "documentId": "",
            "operationDate": "12062019"
        },
       {RESTO DE MOVIMIENTOS}
    ],

    "resultado": "OK"

}
```

11. Consulta de saldos

La consulta de saldos devuelve los saldos de la cuenta del usuario en formato json.

Llamada POST:

https://be.ceca.es/BEWeb/1491/FLBK/not6264_d_0.action;jsessionid=3uz7DruhdBeG5JkOE-wP6bMr.desabeweb

Parámetros:

- *CAJA=1491 (Valor fijo)*
- *CAMINO=FLBK (fijo)*
- *IDIOMA=01 (fijo)*
- *LLAMADA= C4X1A2C02350Z051E057 (Llamada recibida en el sello)*
- *iban= ES5314919999202115009025 (IBAN de la cuenta a consultar saldos)*

La estructura del json es:


```
{
    "IBANRECIBIDO": "ES5314919999202115009025",
    "BLOQUE": [
        {
            "OFICINA": "0001",
            "SIGNO2": "+",
            "CUENTAASOCIADA": "",
            "TIPO": "01",
            "TIPORELACION": "00",
            "SIGNO3": "+",
            "SIGNO4": "+",
            "SALDO2": "0000000687830000",
            "CUENTA": "202115009025",
            "SALDO1": "0000000687830000",
            "SALDO4": "0000000000000000",
            "SITUACION": "00",
            "SALDO3": "0000000000000000",
            "MONEDA": "978",
            "ALIAS": "",
            "AUTORIZACION": "CA",
            "GCUENTA": "14919999202115009025",
            "FECHACADU": "0000",
            "ENTIDAD": "1491",
            "SIGNO1": "+"
        }
    ],
    "operacionOK": "6264",
    "resultado": "OK"
```

```
}
```

12. Consulta de comisiones

Servicio que recupera las comisiones de una transacción.

Llamada POST:

ttps://be.ceca.es/BEWeb/1491/FLBK/not6278_d_0.action;jsessionid=3uz7DruhdBeG5JkOE-wP6bMr.desabeweb

Parámetros:

- *CAJA=1491 (Valor fijo)*
- *CAMINO=FLBK (fijo)*
- *IDIOMA=01 (fijo)*
- *LLAMADA=C4X1A2C02350Z051E057 (Llamada recibida en el sello)*
- *IBAN= ES5314919999202115009025 (IBAN de la cuenta ordenante)*
- *IMPORTE=0000000687830000 (En formato de 12 enteros y 4 decimales sin separación de decimales)*
- *MONEDA=978*
- *NOMBENEFICIARIO=NOMBRE (Nombre del beneficiario)*
- *IBANBENEFICIARIO=ES6601821606140201559863 (IBAN del beneficiario)*
- *CONCEPTO=Prueba*

La estructura del json es:


```
{
  "resultado": "ok",
  "amount": "+000000000068783.00",
  "fee": "+000000000000001.00",
  "total": "+000000000068784.00"
}
```

13. Recuperación de la máscara de firmas

Este servicio recupera las posiciones de la firma a introducir.

Llamada POST:

https://be.ceca.es/BEWeb/1491/FLBK/not6287_d_0.action;jsessionid=l1Zi5Rtg3jjBYWIQgt7CA1U6.desabeweb

Parámetros:

- *CAJA=1491 (Valor fijo)*
- *CAMINO=FLBK (Valor fijo)*
- *IDIOMA=01 (Valor fijo)*
- *LLAMADA= 21R1C150C6Z0X0524020 (Llamada recibida en el sello)*

La estructura del json es:


```
{
  "resultado": "ok",
  "PosicionesFirma": "2578"
}
```

14. Transferencia

Este servicio envía la información del OTP introducido por el cliente y ejecuta la transferencia.

Tanto el campo TOKENOTP como el campo FIRMA1 va encriptado con la misma clave recibida en el sello.

Llamada POST:

https://be.ceca.es/BEWeb/1491/FLBK/not6284_d_0.action;jsessionid=rphrz05CbRE_begS6HIVcj4T.desabeweb

Parámetros:

- *CAJA=1491 (Valor fijo)*
- *CAMINO=FLBK (Valor fijo)*
- *IDIOMA=01 (Valor fijo)*
- *LLAMADA= 5953H3W04150C0R750C1 (Llamada recibida en el sello)*
- *FIRMA= TIOO (Firma con las posiciones indicadas en servicio de la recuperación de la máscara de firmas)*
- *IBANORDENANTE= ES5314919999202115009025 (IBAN del ordenante)*
- *IBANBENEF= ES6699996061402015598 63 (IBAN del Beneficiario)*
- *IMPORTE=%0000000000000335.00 (Importe de la transacción en formato +00000000000000000.00)*
- *CONCEPTO=Prueba (Concepto de la transferencia)*
- *NOMBENEF=Pedro (Nombre del Beneficiario)*

La estructura del json es:

```
{
  "resultado": "ok",
  "REFERENCIA": "",
  "otpFlag": "true"
}
```

15. Solicitud de segundo factor de autenticación - Transferencia

Es posible que, en base a ciertos criterios, se solicite un segundo factor de autenticación para asegurar que la Transferencia que se está realizando no proviene de un TPP externo. Para ello se recibirá una clave OTP en el número de teléfono registrado por el usuario. Una vez introducida, si la autenticación es exitosa, se continuará con el proceso de Transferencia.

Llamada*:*

https://be.ceca.es/BEWeb/1491/FLBK/not6265_d_0.action;jsessionid=rphrz05CbRE_begS6HIVcj4T.desabeweb

Parámetros*:*

- *USUARIO= 78702963E (Identificación del usuario a autenticar)*
- *OTP= C1CFE124 (Clave recibida en el teléfono asignado por el usuario)*
- *CAJA=1491 (Valor fijo)*
- *CAMINO=FLBK (Valor fijo)*
- *IDIOMA=01 (Valor fijo)*
- *LLAMADA= 5953H3W04150C0R750C1 (Llamada recibida en el sello)*
- *FIRMA= TIOO (Firma con las posiciones indicadas en servicio de la recuperación de la máscara de firmas)*
- *IBANORDENANTE= ES5314919999202115009025 (IBAN del ordenante)*
- *IBANBENEF= ES6699996061402015598 63 (IBAN del Beneficiario)*
- *IMPORTE=%0000000000000335.00 (Importe de la transacción en formato +00000000000000000.00)*
- *CONCEPTO=Prueba (Concepto de la transferencia)*
- *NOMBENEF=Pedro (Nombre del Beneficiario)*

Si la conexión es satisfactoria la respuesta será el siguiente json:

```
{
  "resultado": "ok"
}
```

16. Desconexión

Cierra la sesión del cliente

Llamada:

http://be.ceca.es/BEWeb/1491/FLBK/desconexion.action;jsessionid=DvG6iWLY699uMRfDlQ1khFeN.desabeweb

Parámetros:

- *CAJA=1491 (Valor fijo)*
- *CAMINO=FLBK (Valor fijo)*
- *CLIENTE= 1491000192 (Cliente ceca recibido en el nodo CLIENTE al llamar al login "oidc_identificacion.action")*
- *IDIOMA=01 (Valor fijo)*
- *LLAMADA= F1F2W1Z0X350E041E0C3 (Llamada recibida en el sello)*
- *OPERAC=0000 (Valor fijo)*

La estructura del json es:

```
{
  "result": "ok"
}
```