GUIA API IMERCADO CONCILIAÇÃO

SasToken para download do arquivo IMBARQ via API

Sumário

1. HISTÓRICO DE REVISÃO

Data	Versão	Descrição
28/03/2022	1.0	Versão Inicial
30/05/2022	1.1	Informações dos endpoints de CERT e PROD. Informação do Host. Inclusão do Fluxo de solicitação de autenticação e solicitação do SASTOKEN.

2. INTRODUÇÃO

Este documento descreve o conjunto de definições de APIs desenvolvidas pela B3 que serão utilizadas no fluxo de download de arquivos IMBARQs via API. Esse documento trata-se especificamente da interface de comunicação API Web (REST) que viabiliza acesso ao Azure Blob Storage (sistema de armazenamento de objetos altamente escalonáveis e seguro para arquivos) para captura e download dos arquivos IMBARQs.

As APIs (Application Programming Interface) WEB possibilitam aos participantes do iMercado Conciliação desenvolverem aplicações para automatizar processos de comunicação, com aplicações machine-to-machine, para participantes que não possuem acesso as redes RCCF e RCB.

3. AUTENTICAÇÃO

Neste capítulo temos as informações relacionadas à Segurança da Informação.

A B3 definiu como modelo de segurança para as APIs expostas o uso de Mutual SSL (Two Way SSL) com pinagem de certificado e tokens JWT obtidos com padrão OAuth 2.0.

3.1 Mutual SSL (Two Way SSL)

Para que o canal de comunicação entre cliente e servidor seja seguro, para todas as APIs do iMercado, é utilizado protocolo HTTPS (Hyper Text Transfer Protocol Secure), o que implica a apresentação de certificado pelo servidor para garantir sua autenticidade e criptografia dos dados trafegados.

Com o uso do Mutual SSL (Two Way SSL) o cliente também deverá apresentar certificado ao servidor durante o handshake SSL, garantindo assim mútua autenticidade.

O certificado de cliente será fornecido pela B3 juntamente com a senha utilizada para proteger a chave privada.

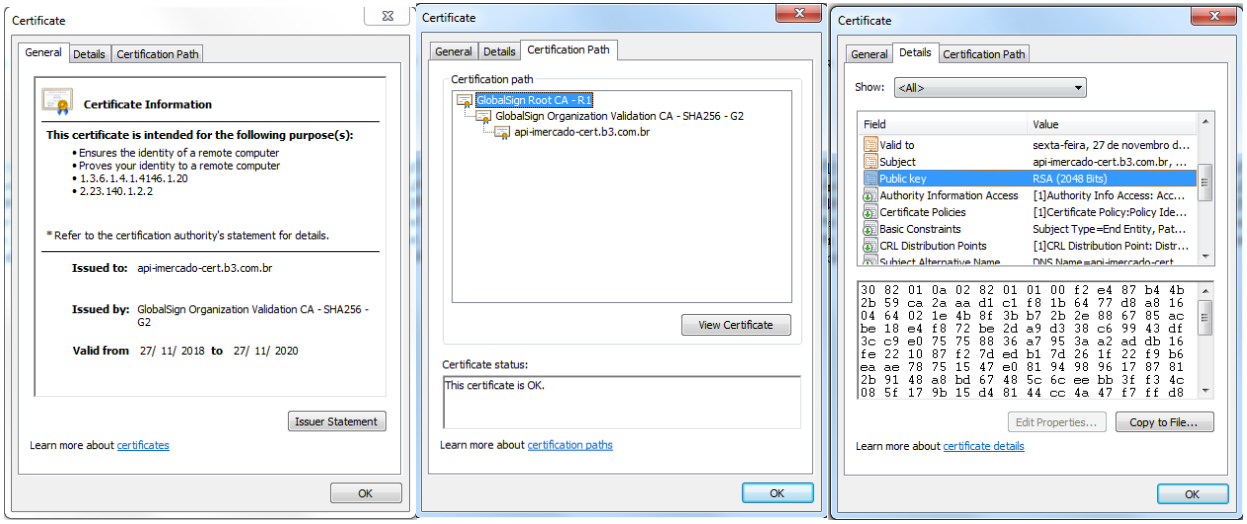
Abaixo exemplo se conexão utilizando mutual SSL com o comando curl:

```
curl --cert ./client.cer:senhafornecidapelaB3 --key client.key \

--request GET https://api-cip-cert.b3.com.br/healthcheck
```

3.2 Pinagem de Certificado

Os clientes que irão consumir as APIs deverão implementar a pinagem do certificado raiz do endereço de conexão. As imagens abaixo ilustram como obter as informações para implementação da pinagem de certificado.



3.3 Token JWT no padrão OAuth 2.0

Para consumir a API, o usuário deverá realizar uma requisição de um token JWT - ele garante que o usuário está autorizado a seguir. Ele precisará informar as seguintes informações na requisição do token JWT no padrão OAuth 2.0:

HTTP: POST

HOST: https://api-listados-cert.b3.com.br

Caminho: /api/oauth/token

Cabeçalho: Content-Type: application/x-www-form-urlencoded

Parâmetros do Corpo:

grant_type = client_credentials (Esse valor é fixo - igual para todas as requisições)

client_id = c96rr10-dcf5-4231-ertert-cf886b8318fa (Aqui vai o client id que o usuário recebeu no pacote de acesso)

client_secret = wertwert-68cf-4a59-b51b-67ee6f820a77 (Aqui vai o client secret que o usuário recebeu no pacote de acesso)

O usuário deverá informar o certificado digital que recebeu no pacote de acesso, utilizando a técnica de Mutual SSL Abaixo veja um exemplo de requisição completa de token JWT com Mutual SSL utilizando CURL - entretanto, a requisição pode ser implementada em outra linguagem desejada:

```
curl --cert ./certificado.cer:senhadocertificado --key chave.key \

--insecure --header "Content-Type: application/x-www-form-urlencoded" \

-d "grant_type=client_credentials&client_id=dc96rr10-dcf5-4231-ertert-cf886b8318fa&client_secret=wertwert-68cf-4a59-b51b-67ee6f820a77" \
```

-X POST https://api-listados-cert.b3.com.br/api/oauth/token

A resposta da requisição será:

{
"access_token":"eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiI5OTkiLCAiZXhwIjoiMTU2MDAwNzgyOSIsICJpc3MiOiJDTj1JbnRlcm1lZCBDZXJ0aWZpY2F0ZSAtIEpXVCxPVT1HQ01DLE89QjMgU0EsTD1TYW8gUGF1bG8sUz1TUCxDPUJSIn0.JSWxLOVX6xWmeLAhwdTP2xKt2eK3JAJ2oB6lYn06PROQdpaCk8E_CaS-xGc2xz9iBEnLTxZTrfdhyYstkBv90fLXVQnhEVFhfXLq2Ov-xWAO_DFPeGLXzy5_7WOpbZ3oKbjJ1XVxbCZnoDIt3VRZGNHAyiS8dZJzxV0n9D8qa_HhtZhOJNbH0ynhPyoE8qMULvgJQ5DzjXIvk2mP-KWIfhoY9CQnGseqTjrqWOj2kmYsQ9yCgAW6DRxB7LvTOavUk/vjOga7hmeXk9-kunaqcu5EMpWzHeiFNGFhY1U4XhFtPZSIWzu23d6wDq5U0ZAWoV3Sw396d-hA3_cah9_hKQw",

"token_type": "Bearer",

"expires_in": "8640",

"scope": "resource.WRITE resource.READ"

}

Os campos são:

− access_token: é o token JWT. Ele deverá ser informado no cabeçalho das requisições às APIs.

− expires_in: a validade do token é de 120 minutos. Após esse tempo, o token JWT não será mais válido, e o usuário deverá requisitar um novo token para consumir as APIs.

− token_type: especifica o authentication schema utilizado pela API, por exemplo, Basic, Bearer, AWS, entre outros. Para as APIs de ofertas e negócios, será utilizado sempre o schema Bearer, conforme RFC:

https://tools.ietf.org/html/rfc6750

Para consumir a API, o access_token deve ser enviado no padrão Bearer, através de um cabeçalho Authorization. Exemplo de chamada:

HTTP: GET

HOST: https://api-listados-cert.b3.com.br

Caminho: /api/cip/v1/sas-tokens

Cabeçalho: Authorization: Bearer {{access_token}}

Fluxo de solicitação de autenticação e solicitação do SASTOKEN:

4. VERBOS HTTP

Para a API SASTOKEN será utilizado somente o verbo GET. Os demais verbos HTTP não são suportados.

5. ENDPOINT

URI base (todas as URIs iniciam com): /api/cip/v1
Exemplo de uma URL completa, para o ambiente de produção, referente ao recurso /sas-tokens

https://api-listados.b3.com.br/api/cip/v1/sas-tokens

6. ENDEREÇOS API

A B3 possui dois ambientes, um dedicado a certificação dos participantes e outro é o ambiente produtivo.
Seguem os endereços para conexão referente cada ambiente:

- Certificação: https://api-listados-cert.b3.com.br/
- Produção: https://api-listados.b3.com.br/

7. SWAGGER

A documentação técnica detalhada da **API SASTOKEN** está disponível no Swagger em:

https://clientes.b3.com.br/pt_br/roadmap/sobre/imercado-arquivos-imbarq-consumo-por-api.htm

Ver Item: “Material de apoio”.

8. MÉTODOS / TAXONOMIA

Os itens abaixo têm como objetivo apresentar a taxonomia (estruturas, nomes, tipos, descrição, valores disponíveis etc.) dos dados que compõem os recursos da API SASToken – IMercado conciliação.

Essas informações poderão ser atualizadas conforme a necessidade de ajustes ou manutenções/melhorias que possam surgir e sempre que ocorrer versionamento ou inclusão de novas funcionalidades na API.

Método	Endpoint	Descrição
GET	/api/cip/v1/sas-tokens	Retorna uma URI de acesso ao StorageAccount da Azure.

8.1 Portfolio – Consulta de posições

GET - /api/ api/cip/v1/sas-tokens

Esse método é responsável por realizar consulta e retornar uma URL de acesso ao StoregeAccount da Azure.

Este recurso tem como característica os seguintes itens:

Json de saída

```
{
  "data": {
    "sasToken": "https://azrstcorimbarqn.blob.core.windows.net/999-1?sv=2020-08-04&se=2021-10-
25T17%3A48%3A26Z&sr=c&sp=rl&sig=POglDoYxsDkfW81xwUvtEDk4r90vqN7xxfqb9wR636E%3D"
  },
  "links": {
    "self": null,
    "first": null,
    "prev": null,
    "next": null,
    "last": null
  }
}
```

Parâmetros de Entrada

N/A.

Parâmetros de Saída

Índice	Campo	Card.	Tipo de Dado	Detalhe do Tipo de Dado	Descrição
1.0	x-v	1..1	string		Versão da API. Ex: 1.0.0
2.0	data				
2.1	sasToken	1..1	string	MaxLength=2000	URI de acesso ao StorageAccount da Azure.
3.0	links				
3.1	self	1..1	string	MaxLength=2000	Current page link
3.2	first	0..1	string	MaxLength=2000	First page link
3.3	prev	0..1	string	MaxLength=2000	Next page link
3.4	next	0..1	string	MaxLength=2000	Next page link
3.5	last	0..1	string	MaxLength=2000	Last page link
4.0	errors				
4.1	code	1..1	string	MaxLength=10	Código do erro
4.2	title	1..1	string	MaxLength=100	Mensagem do erro
4.3	detail	1..1	string	MaxLength=2000	Informações complementares sobre o erro

9. RESPONSE CODE

A B3 usa códigos de resposta HTTP normais para indicar o sucesso ou falha de uma solicitação da API. Um código de resposta de 200, por exemplo, significa sucesso, enquanto os códigos no intervalo 4xx indicam um erro em relação às informações fornecidas. Já os códigos no intervalo 5xx apontam um erro de comunicação com os nossos servidores. Confira quais são os códigos de erro utilizados pelos recursos da SASTOKEN.

Http codes retornados

Código	Código Retorno	Mensagem	Descrição
200	200	Ok	Indica que a requisição foi recebida e executada com sucesso.
201	201	Created.	Indica que a requisição foi bem sucedida e que um novo recurso foi criado.
204	204	No Content.	Operação de exclusão ou alteração concluída com sucesso.
400	400	Bad Request	Indica que a requisição não foi executada porque está mal formada.
401	401	Unauthorized	O servidor não pôde verificar se você está autorizado a acessar o documento solicitado. As credenciais fornecidas estão erradas (por exemplo, senha incorreta) ou seu navegador não sabe como fornecer as credenciais necessárias.
403	403	Forbidden	Indica que o servidor entendeu o pedido, mas se recusa a autorizá-lo. Esse status é semelhante ao 401, mas neste caso a re-autenticação não fará diferença. O acesso é permanentemente proibido e vinculado à lógica da aplicação (como uma senha incorreta).
404	404	Not Found	O erro 404 é um código de resposta HTTP que indica que o cliente não pôde comunicar com o servidor, ou o servidor não pôde encontrar o que foi pedido, ou foi configurado para não cumprir o pedido e não revelar a razão ou a página não existe mais.
422	422	Unprocessable Entity.	Indica que solicitação foi bem formada, mas não pôde ser processada devido à lógica de negócios específica da solicitação. Podem retornar objeto errors ou erros.
500	500	Internal Server Error.	Indica que a operação falhou. Ocorreu um erro no gateway da API ou no microsserviço.