Https API接口（用于CDN供应商）

# 概览

## 背景

China CDN 团队会筛选多个CDN供应商以支持Https 功能，此文档为CDN供应商定义了HTTPS接口的要求。

## 术语

|  |  |
| --- | --- |
| 术语 | 描述 |
| SSL证书 | 用户的SSL证书，用来绑定CDN的节点，实现CDN的HTTPS服务 |
| AAD认证证书 | 由CDN供应商提供证书用来设置Azure Active Directory以获取 Azure Key Vault（Azure密钥保管库）的访问权限 |
| 公钥证书 | 仅包含公钥的AAD认证证书 |
| 私钥证书 | 包含私钥的AAD认证证书 |

# 通过 Azure CDN API获取用户SSL证书

## CDN供应商所需要步骤:

* CDN供应商准备一套具有私钥的证书和对应的只包含公钥的证书
* 将公钥证书发送到Azure China CDN团队，CDN 团队提供对应的AAD Client ID
* 实现 Azure中国CDN团队所需的两个API。详见后续3.1章节
* 通过证书的完整路径（API参数中获取），AAD Client ID，以及AAD私钥证书 获取到节点的SSL证书并完成绑定。

# CDN 供应商接口要求

CDN供应商需要实现至少两个API，以便实现Https 节点绑定功能。

## 绑定SSL证书API

|  |  |  |  |
| --- | --- | --- | --- |
| Item | Value | Description | Examples |
| API名称 | BindCertificate | * API由CDN供应商提供 * Invoked by Azure CDN Service 由Azure CDN服务 调用 * CDN provider bind customer's certificate to a CDN custom domain CDN供应商将客户的SSL证书绑定到CDN 客户的域名 | <https://api.mockcdn.cn/bindcertificate> |
| Https方法 | POST |  |  |
| 认证 | 跟随CDN供应商 |  |  |
| 授权 | 跟随CDN供应商 |  |  |
| 参数 | EndpointId：CDN供应商端的节点ID | * CDN供应商端关于某个域名的节点ID * 用来绑定Https证书 * 参数可以在Http Body中，也可以在URL中指定 | 32456 |
| 参数 | Certificate ：Azure密钥保管库上的证书地址 | * Azure密钥保管库上的证书地址 * CDN供应商会被授权来下载此证书 * 参数可以在Http Body中，也可以在URL中指定 | <https://transit-cdn-cert.vault.azure.cn/certificates/cc9706ec-7f99-4df9-83a9-4820931a2552> |
| 参数 | ClientID ：Azure AAD ClientID | * Azure Service提供给供应商用来访问密钥保管库的Client ID * CDN供应商会被授权来下载此证书 * 参数可以在Http Body中，也可以在URL中指定 | 5451E51E-7E8D-481C-BD44-41E25B580F26 |
| 网址格式 | 跟随CDN供应商 | CDN供应商也可以把需要的参数放在URL参数中 | <https://api.mockcdn.cn/bindcertificate> |
| 正文格式 | 跟随CDN供应商 | CDN供应商也可以把需要的参数放在URL参数中 | {  “EndpointId”: “cc9706ec-7f99-4df9-83a9-4820931a2552”,  “Certificate”: “<https://transit-cdn-cert.vault.azure.cn/certificates/cc9706ec-7f99-4df9-83a9-4820931a2552>”  “ClientID”: “5451E51E-7E8D-481C-BD44-41E25B580F26”  } |
| 响应 状态代码 | Https Status Code | * 成功状态码：202 (Accepted) * 非成功状态码：除202 (Accepted)以外的其它状态码 |  |
| 响应 状态代码-成功 | 跟随CDN供应商 | * Http响应状态码应为202（已接受） * 必须 为https证书绑定 异步任务提供TaskID | {  “TaskID”: “97ac6d45-8e89-4e79-b6c0-20f43abcf51f”  } |
| 响应 状态代码-失败 | 跟随CDN供应商 | * Http响应状态码为 非 202的状态 * 必须提供 错误代码 * 必须提供 错误消息 | {  “ErrorCode”: “CertificateNotFound”,  “ErrorMessage”: “Certificate is not found”  } |

## 查询绑定证书任务状态API

|  |  |  |  |
| --- | --- | --- | --- |
| Item | Value | Description | Examples |
| API名称 | QueryTask | * API由CDN提供商提供 * 由Azure CDN服务调用 * CDN供应商将客户的证书绑定到CDN自定义的域名 | <https://api.mockcdn.cn/task/97ac6d45-8e89-4e79-b6c0-20f43abcf51f> |
| Https方法 | GET |  |  |
| 认证 | 跟随CDN供应商 |  |  |
| 授权 | 跟随CDN供应商 |  |  |
| 参数 | TaskID | BindCertificate API返回的TaskID | 97ac6d45-8e89-4e79-b6c0-20f43abcf51f |
| 网址格式 | 跟随CDN供应商 | * 参数TaskID可以在URL中 | <https://api.mockcdn.cn/task/97ac6d45-8e89-4e79-b6c0-20f43abcf51f> |
| 正文格式 | 跟随CDN供应商 | * 参数TaskID可以在URL中 |  |
| 响应状态代码 | 跟随CDN供应商 | * 200（OK） API调用成功 * API调用的非200（OK）失败 |  |
| 响应状态代码-成功 | 跟随CDN供应商 | * Http响应状态码应为200（OK） * 必须至少提供以下任务状态之一： Inprogress，Completed，Failed | {  “Status”: “Inprogress”  } |
| 响应状态代码-失败 | 跟随CDN供应商 | * Http响应状态码为非200（OK）的状态 | {  “ErrorCode”: “NotFound”,  “ErrorMessage”: “TaskID not found”  } |

# Sample Code for CDN Provider

## Retrieve Customer’s SSL Cert in Transit Key Vault

### C# version

<https://github.com/mccdn/ChinaCDNHttpsForProviders/tree/master/ReadSSLCertFromKeyVault-Net>

### Java Version

<https://github.com/mccdn/ChinaCDNHttpsForProviders/tree/master/ReadSSLCertFromKeyVault-Java>

# References

Azure Key Vault REST API: <https://docs.microsoft.com/en-us/rest/api/keyvault/>

Coding with Key Vault: <https://docs.microsoft.com/en-us/azure/key-vault/key-vault-developers-guide#coding-with-key-vault>