**问题描述**

Azure Key Vault支持上传PEM格式的证书，但是要求PEM证书的格式必须符合PKCS#8规范，但我们在使用openssl等工具生成证书时，默认会生成PKCS#1编码的key，如果直接将PKCS#1编码的key导入Key Vault时，会返回错误：PEM is unexpected format，导致无法正常导入。

**问题分析：**

将PKCS#1的证书转换为PKCS#8格式，然后在上传至Azure Key Vault，我们可以借助openssl工具或者使用代码进行转换。

首先，介绍下PKCS#8和PKCS#1的区别，PKCS#1是RSA加密标准，PKCS#1定义了RSA公钥函数的基本格式标准，特别是数字签名。而PKCS#8 是更为通用的非对称加密私钥语法标准。两者的格式区别

PKCS#1的格式如下，通常使用BEGIN RSA PRIVATE KEY和BEGIN RSA ENCRYPTED PRIVATE KEY 来包裹key信息。

-----BEGIN RSA PRIVATE KEY-----

...

-----END RSA PRIVATE KEY-----

PKCS#8的格式如下，通常使用BEGIN PRIVATE KEY和BEGIN ENCRYPTED PRIVATE KEY 来包裹key信息。

-----BEGIN PRIVATE KEY-----

...

-----END PRIVATE KEY-----

-----BEGIN CERTIFICATE-----

...

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

...

-----END CERTIFICATE-----

如果Private Key使用加密格式，那么private Key的格式如下：

-----BEGIN ENCRYPTED PRIVATE KEY-----

...

-----END ENCRYPTED PRIVATE KEY-----

**解决方法：**

接下来，我们进行PKCS#1和PKCS#8的转换

**使用openssl工具将PKCS#1私钥转换为PKCS#8格式**

执行命令如下，输入为PKCS#1 Key，输出PKCS#8 Key

openssl pkcs8 -topk8 -inform PEM -in pkcs1.key -outform pem -nocrypt -out pkcs8.pem

**使用代码方式进行转换**

我们可以使用代码解析PKCS#1格式的私钥，并将其按照PCKS#8的编码规范输出。示例代码，请参考以下代码片段文档

[https://gist.github.com/chenrui1988/6b104a010172786dbcbc0aafc466d291#file-rsakeyutils-cs-L78](https://na01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fgist.github.com%2Fchenrui1988%2F6b104a010172786dbcbc0aafc466d291%23file-rsakeyutils-cs-L78&data=02%7C01%7Clutia%40microsoft.com%7C5caa12dda0814703d56708d4b9425be1%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C636337142073838628&sdata=c%2BhSWxwZzFDJsAMNiDM7a3k7Ka5akQO2i8MYfRR1zhI%3D&reserved=0)

转换之后，我们就可以正常将证书进行上传！

**参考文档：**

[https://stackoverflow.com/questions/23852221/converting-privatekey-to-pem-string-without-using-bouncycastle/23864945#comment36753748\_23864945](https://na01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fstackoverflow.com%2Fquestions%2F23852221%2Fconverting-privatekey-to-pem-string-without-using-bouncycastle%2F23864945%23comment36753748_23864945&data=02%7C01%7Clutia%40microsoft.com%7C5caa12dda0814703d56708d4b9425be1%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C636337142073838628&sdata=kfxhlPBytwxcF5SFEyCYkKY08nPihqNuvxyxh8QJhcw%3D&reserved=0)

<https://gist.github.com/chenrui1988/6b104a010172786dbcbc0aafc466d291>

[https://docs.microsoft.com/en-us/rest/api/keyvault/about-keys--secrets-and-certificates?redirectedfrom=MSDN#key-vault-certificates](https://na01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Frest%2Fapi%2Fkeyvault%2Fabout-keys--secrets-and-certificates%3Fredirectedfrom%3DMSDN%23key-vault-certificates&data=02%7C01%7Clutia%40microsoft.com%7Ce282a37408734ae8bc0808d4b78665c1%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C636335235270302581&sdata=3hZ3FpJ4clpieCFp20WOMIiSYX5a5TcoqY9KCTEO0Pw%3D&reserved=0)

[https://docs.microsoft.com/en-us/rest/api/keyvault/importcertificate](https://na01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Frest%2Fapi%2Fkeyvault%2Fimportcertificate&data=02%7C01%7Clutia%40microsoft.com%7Ce282a37408734ae8bc0808d4b78665c1%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C636335235270302581&sdata=dQFZffWPWES0lmNmImWdalfDUGRX6dakSulGKbNID3A%3D&reserved=0)