如何使用密钥管理库导入PEM格式的证书

通过 Azure 密钥保管库，Azure 用户能够保护和控制云应用程序和服务使用的加密密钥和其他机密。密钥保管库在设计上确保了微软无法看到或提取用户的密钥，通过加密密钥存储在云中，能提高云应用程序的性能并减少延迟。

**问题描述：**

我们在使用密钥管理库上传证书时，根据不同的情况需要上传不同格式的证书，例如PFX、PEM等等。有时用户开发应用在调用密钥管理时，上传PEM格式证书时，会返回错误：PEM is unexpected format，因此无法成功导入PEM格式的证书。

**问题分析：**

我们以.net应用开发为例，可以通过调用方法[ImportCertificateAsync(IKeyVaultClient, String, String, String, String, CertificatePolicy, CertificateAttributes, IDictionary<String,String>, CancellationToken)](https://na01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Fdotnet%2Fapi%2Fmicrosoft.azure.keyvault.keyvaultclientextensions.importcertificateasync%3Fview%3Dazurekeyvault-2.0.6%23Microsoft_Azure_KeyVault_KeyVaultClientExtensions_ImportCertificateAsync_Microsoft_Azure_KeyVault_IKeyVaultClient_System_String_System_String_System_String_System_String_Microsoft_Azure_KeyVault_Models_CertificatePolicy_Microsoft_Azure_KeyVault_Models_CertificateAttributes_System_Collections_Generic_IDictionary_System_String_System_String__System_Threading_CancellationToken_&data=02%7C01%7Clutia%40microsoft.com%7C2bc76272dbd347ba3af808d4912d98cd%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C636293072460583104&sdata=AH50m0S%2BUroTimZxp3tUkatlT%2FgV9Md1UqgO0EMvq9U%3D&reserved=0)来导入PEM格式的证书，更多的说明可以参考[官方链接](https://na01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Fdotnet%2Fapi%2Fmicrosoft.azure.keyvault.keyvaultclientextensions.importcertificateasync%3Fview%3Dazurekeyvault-2.0.6&data=02%7C01%7Clutia%40microsoft.com%7C2bc76272dbd347ba3af808d4912d98cd%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C636293072460583104&sdata=GzsEmL9z6W1xZJn1BnJhydWTJkt%2FNkbGju8cjfYy9mw%3D&reserved=0)。

但是当我们调用上述方法上传PEM格式证书时会有一些特殊的要求（需要注意的是，这些要求同样适用于使用CLI以及各种其他语言的SDK）。

具体的要求如下：

1. 在创建/导入PEM格式证书时，CertificatePolicy中secret的ContentType的值需要设定为application/x-pem-file；如果是PFX的话，ContentType的值为CertificateContentType.Pfx。

PEM可以通过下面的格式定义CertificatePolicy：

var policy = new CertificatePolicy

{

KeyProperties = new KeyProperties

{

Exportable = true,

KeyType = "RSA"

},

SecretProperties = new SecretProperties

{

ContentType = "application/x-pem-file" // PEM certificate

//ContentType = CertificateContentType.Pfx // PFX certificate

}

};

1. 需要导入的PEM格式的证书需要是下面格式之一，这意味着:

* 传递给ImportCertificateAsync的参数也要包括“-----”等特殊字符。
* 同时也要保证传递过来的字符串包含换行符从而保证是下面要求的格式。
* 导入的证书最少是一个，最多整个字符串长度不可超过25K。
* 关于密钥管理库可以接受的PEM格式文件的说明，可以参考[链接](http://how2ssl.com/articles/working_with_pem_files/)。

|  |  |
| --- | --- |
| **Pem with unencrypted pkcs#8 Key** | **Pem with encrypted pkcs#8 Key** |
| -----BEGIN PRIVATE KEY-----  …………………  -----END PRIVATE KEY-----    -----BEGIN CERTIFICATE-----  ……….  -----END CERTIFICATE-----    -----BEGIN CERTIFICATE-----  ……….  -----END CERTIFICATE----- | -----BEGIN ENCRYPTED PRIVATE KEY-----  …………………  -----END ENCRYPTED PRIVATE KEY-----    -----BEGIN CERTIFICATE-----  ……….  -----END CERTIFICATE----- |

.net中的参数定义如下：

base64X509 = "-----BEGIN PRIVATE KEY-----\nMIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDkZlh01m5vpwFvFaffSHzcJRl8mZtLpo4K4p8Hed+QH/………LyVcynibPKezupYJ1wg\n-----END PRIVATE KEY-----\n-----BEGIN CERTIFICATE-----\nMIIDNDCCAhygAwIBAgIQBdSVCj/ TnN09N6jDqgmOtpUUhWwrn5………7quTVwcUEAjwrPDx3s=\n-----END CERTIFICATE-----";

最后，关于导入PEM 证书，您可以通过[链接](https://mileytest.blob.core.chinacloudapi.cn/videofile/HelloKeyVault.rar)下载demo程序，您需要替换App.config中的参数为您自己的密钥管理的值。这方面的信息，我们即将在[官方链接](https://na01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Fdotnet%2Fapi%2Fmicrosoft.azure.keyvault.keyvaultclientextensions.importcertificateasync%3Fview%3Dazurekeyvault-2.0.6&data=02%7C01%7Clutia%40microsoft.com%7C2bc76272dbd347ba3af808d4912d98cd%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C636293072460583104&sdata=GzsEmL9z6W1xZJn1BnJhydWTJkt%2FNkbGju8cjfYy9mw%3D&reserved=0)中更新，请您关注我们的网站，了解更多详细的信息。