使用硬件安全模块（Hardware Security Module，HSM）

你可以使用硬件安全模块（HSM）来生成和存储 Fabric 节点使用的私钥。HSM 可以保护你的私钥并处理密码学操作，它可以让 Peer 节点和排序节点在不暴露私钥的情况下进行签名和背书。 如果您需要符合政策标准，如FIPS 140-2，您可以有多种经过认证的硬件安全模块可以选择。

目前，Fabric 只支持按照 PKCS11 标准和 HSM 进行通信。

配置 HSM

要在 Fabric 节点中使用 HSM，你需要在节点配置文件（比如 core.yaml 或者 orderer.yaml）中更新 BCCSP （Crypto Service Provider，加密服务提供者）部分。在 BCCSP 部分中，你需要选择 PKCS11 作为提供者，并且要选择你要使用的 PKCS11 库所在的路径。你还需要提供你创建秘钥文件的 label 和 pin。你可以使用一个秘钥生成和保存多个秘钥。

预编译的 Hyperledger Fabric Docker 镜像不支持使用 PKCS11。如果你使用 docker 部署 Fabric，你需要重新编译镜像并启用 PKCS11，编译命令如下：

```
make docker GO_TAGS=pkcs11
```

你需要确保 PKCS11 库可用，你可以在节点上安装它，也可以把它挂载到容器里。

示例

下边的示例演示了如何配置 Fabric 节点使用 HSM。

首先，你需要安装 PKCS11 接口的实现。本示例使用开源实现 softhsm。下载并配置 softhsm 之后，你需要将环境变量 SOFTHSM2_CONF 设置为 softhsm2 的配置文件。

然后你就可以使用 softhsm 来创建秘钥并在 Fabric 节点内部的 HSM slot 中处理密码学操作。在本示例中，我们创建了一个标记为 “fabric” 并把 pin 设置为 “71811222” 的秘钥。你创建秘钥之后，将配置文件修改为使用 PKCS11 和你的秘钥作为加密服务提供者。下边是一个 BCCSP 部分的示例：

```
##############################################################################
# BCCSP (BlockChain Crypto Service Provider) section is used to select which
# crypto library implementation to use
##############################################################################
bccsp:
  default: PKCS11
  pkcs11:
    Library: /etc/hyperledger/fabric/libsofthsm2.so
    Pin: "71811222"
    Label: fabric
    hash: SHA2
    security: 256
    Immutable: false
```

默认情况下，当使用HSM生成私钥时，私钥是可变的，这意味着生成密钥后可以更改PKCS11私钥属性。将`Immutable`设置为`true`意味着在生成密钥后不能更改私钥属性。在使用`Immutable: true`配置为不可变更之前，请保证HMS支持PKCS11的对象副本。

你也可以使用环境变量覆盖配置文件中相关字段。如果你使用 Fabric CA 服务端链接 HSM，你需要设置如下环境变量或者直接在CA服务器配置文件中设置相应的值：

```
FABRIC_CA_SERVER_BCCSP_DEFAULT=PKCS11
FABRIC_CA_SERVER_BCCSP_PKCS11_LIBRARY=/etc/hyperledger/fabric/libsofthsm2.so
FABRIC_CA_SERVER_BCCSP_PKCS11_PIN=71811222
FABRIC_CA_SERVER_BCCSP_PKCS11_LABEL=fabric
```

如果您使用Fabric节点连接到softhsm2，您可以使用如下环境变量或直接在节点配置文件中设置相应的值：

```
CORE_PEER_BCCSP_DEFAULT=PKCS11
CORE_PEER_BCCSP_PKCS11_LIBRARY=/etc/hyperledger/fabric/libsofthsm2.so
CORE_PEER_BCCSP_PKCS11_PIN=71811222
CORE_PEER_BCCSP_PKCS11_LABEL=fabric
```

如果您使用Fabric Orderer连接到softhsm2，您可以使用如下环境变量或直接在Orderer配置文件中设置相应的值：

```
ORDERER_GENERAL_BCCSP_DEFAULT=PKCS11
ORDERER_GENERAL_BCCSP_PKCS11_LIBRARY=/etc/hyperledger/fabric/libsofthsm2.so
ORDERER_GENERAL_BCCSP_PKCS11_PIN=71811222
ORDERER_GENERAL_BCCSP_PKCS11_LABEL=fabric
```

如果你编译了 docker 镜像并使用 docker compose 部署节点，你可以修改 docker compose 配置文件的 volumes 部分来挂载 softhsm 库和配置文件。下边的示例演示了如何在docker compose 配置文件中设置环境变量和卷：

```
  environment:
     - SOFTHSM2_CONF=/etc/hyperledger/fabric/config.file
  volumes:
     - /home/softhsm/config.file:/etc/hyperledger/fabric/config.file
     - /usr/local/Cellar/softhsm/2.1.0/lib/softhsm/libsofthsm2.so:/etc/hyperledger/fabric/libsoft
```

设置一个使用 HSM 的网络

如果你使用 HSM 部署 Fabric 节点，你需要在 HSM 中生成私钥而不是在节点本地 MSP 目录的`keystore`目录中。MSP 的`keystore`目录置空。另外，Fabric 节点会使用`signcerts`目录中签名证书的主体密钥标识符（subject key identifier）来检索 HSM 中的私钥。根据你使用 Fabric CA（Certificate Authority）还是你自己的 CA 的情况，创建 MSP 目录的操作是不一样的。

开始之前

在使用HSM配置Fabric节点之前，您需要完成如下步骤：

1. 在HSM服务器上创建一个分区并记录下分区的`Label`和`PIN`.
2. 按照HSM提供商提供的文档中的说明配置与HSM服务器通信的HSM客户端。

使用带有 HSM 的 Fabric CA

你可以像 Peer 节点或者排序节点一样，通过修改配置文件让 Fabric CA 使用 HSM。因为你可以使用 Fabric CA 在 HSM 内部生成秘钥，所以创建本地 MSP 目录的过程就很简单。按照下边的步骤：

1. 修改Fabric CA server配置文件的`bccsp`部分，并指向为HSM创建的`Label`和`PIN`。当Fabric CA服务器启动时，私钥被生成并存储在HSM中。如果您不想公开CA签名证书，可以跳过此步骤，仅为您的peer或ordering配置HSM，如下所述。
2. 使用 Fabrci CA 客户端，用你的 CA 来注册 Peer 节点或者排序节点的身份。
3. 在您部署一个支持HSM的peer或ordering节点，您需要将节点的私钥存储在HSM里以提供节点证明。编辑Fabric CA 客户端配置文件中的`bccsp`章节或使用对应的环境变量来为您的peer或ordering节点指明HSM的配置文件。在Fabric CA客户端配置文件中,将默认`SW`配置替换为`PKCS11`并为您的HSM提供值。

```
bccsp:
  default: PKCS11
  pkcs11:
    Library: /etc/hyperledger/fabric/libsofthsm2.so
    Pin: "71811222"
    Label: fabric
    hash: SHA2
    security: 256
    Immutable: false
```

然后，对于每个节点，使用Fabric CA客户端根据在步骤2中注册的节点标识注册，从而生成peer或ordering节点的MSP文件夹。enroll命令不是将私钥存储在相关MSP的`keystore`文件夹中，而是使用节点的HSM生成和存储peer或ordering节点的私钥。`keystore`文件夹仍为空。

1. 要将peer或ordering节点配置为使用HSM，同样的更新peer或orderer的配置文件中`bccsp`章节，使用PKCS11并提供`Label`和`PIN`。另外，编辑`mspConfigPath`（对于peer节点）或者`LocalMSPDir`（对于ordering节点）的值，指向在上一步中使用Fabric CA客户端生成的MSP文件夹。既然您已将peer或ordering节点配置为使用HSM，当您重启节点时，它将可以使用HSM保护的私钥对交易进行签名或背书。

在你自己的 CA 上使用 HSM

如果你使用你自己的 CA 来部署 Fabric 组件，你可以按如下步骤使用 HSM：

1. 将您的CA配置使用PKCS11来与HSM进行通信，并创建`Label`和`PIN`。然后使用CA为每个节点生成私钥和签名证书，私钥在HSM内部生成。
2. 使用你的 CA 构建节点 MSP 目录。将第 1 步生成的签名证书放入`signcerts`目录。你也可以让`keystore`目录为空。
3. 要将peer或ordering节点配置为使用HSM，同样的更新peer或orderer的配置文件中`bccsp`章节，使用PKCS11并提供`Label`和`PIN`。另外，编辑`mspConfigPath`（对于peer节点）或者`LocalMSPDir`（对于ordering节点）的值，指向在上一步中使用Fabric CA客户端生成的MSP文件夹。既然您已将

peer或ordering节点配置为使用HSM，当您重启节点时，它将可以使用HSM保护的私钥对交易进行签名或背书。