密钥管理

1. 服务器端生成新密钥——下发。
2. 服务器——TBOX的安全通信
3. TBOX下发新密钥至各个ECU，ECU成功接受后返回ACK
4. HSM：公私钥生成、管理功能；非对称加解密
5. OTA安全机制、云端密钥安全管理

密钥的安全管理通常采用层次化的保护方式，一般情况下分为三层加密（根密钥、密钥加密密钥、工作密钥）和两层加密（根密钥、工作密钥）。

1. 根密钥的加、解密运算复杂  
   更换根密钥时，大量工作密钥的解、加密运算会造成巨大的运算开销
2. 工作密钥需要频繁变更  
   工作密钥频繁变更，解、加密运算会造成巨大的运算开销
3. 工作密钥数量巨大且相互独立  
   所有工作密钥都用根密钥加密，一旦根密钥被攻破则所有工作密钥均被攻破。

密钥分配：

公钥：（1）广播式，

（2）目录式：可信机构建立目录<用户，公钥>，

（3）公开密钥证书分配：在前者基础上，公钥证书上有用户身份公钥和一些其他的，这样认证证书即可知道一切。

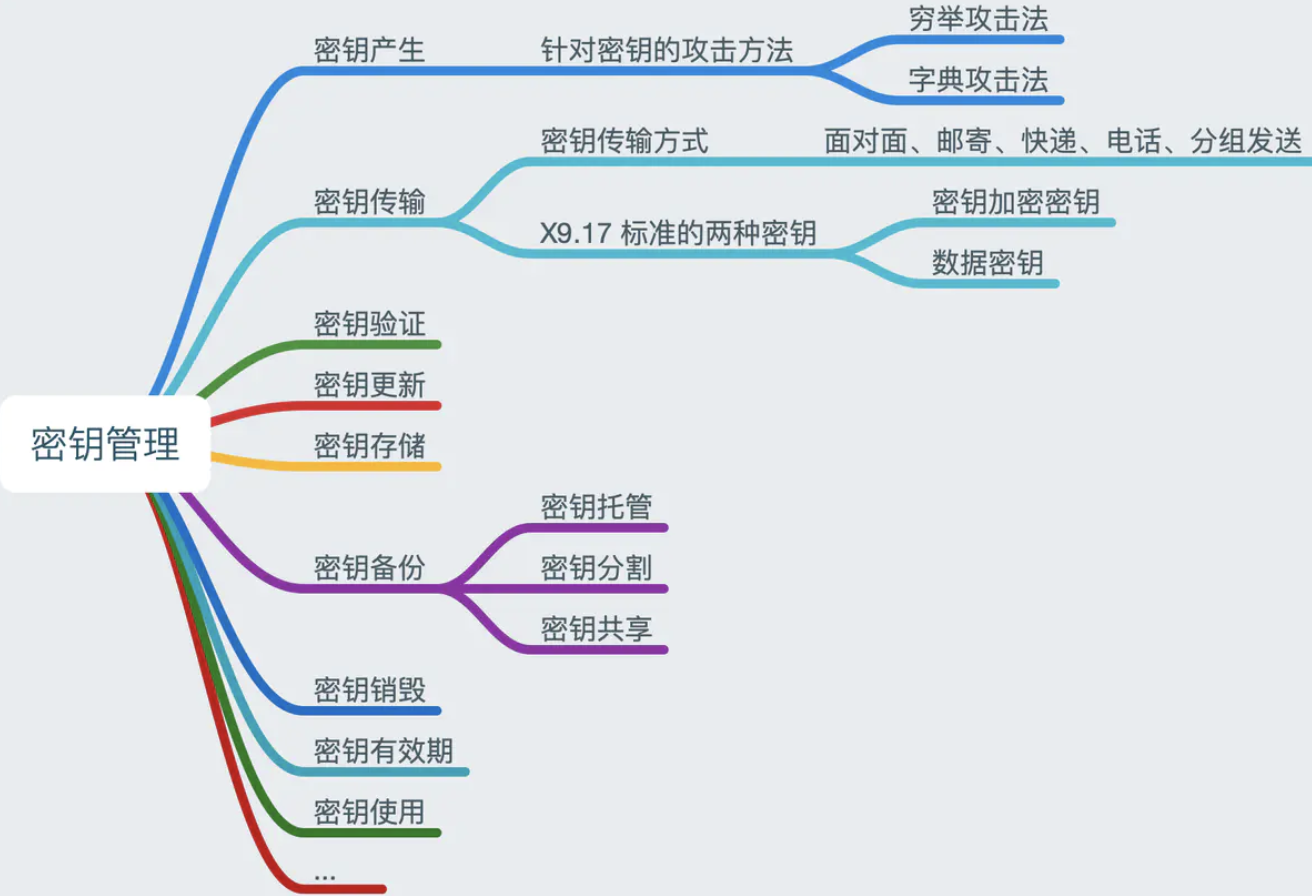
私密密钥分配：

1. 无中心：

* 有共享密钥：即密钥加密密钥
* 无共享密钥：三次握手，没有身份认证

            （2）有中心：  NS密钥分配协议：密钥分配中心C，A，B通信。

                        A有KAC，B有KBC ，A想通信B，C就给A一个会话密钥KAB和一个证书：E-KBC(IDA,KAB)，然后A把证书给B，B一解密就得到会话密钥了。



密钥更新：由TBOX发起，非对称加密传输密钥。

每个ECU由自己的公钥和私钥，每次更新密钥时，TBOX使用各ECU的公钥加密更新后的SM4密钥，向各个ECU发放。

密钥更新流程：

1. 各个ECU更新自己的公钥-私钥对
2. 各个ECU向CA中心申请证书，并将证书发送至TBOX
3. TBOX收到证书，验证真伪后，获取其中各ECU的公钥
4. TBOX使用各ECU的公钥加密更新后的SM4密钥，并向各ECU发放（截断完整密钥发放），并用自己私钥对其进行数字签名
5. 各个ECU使用自己的私钥解密TBOX发送的密文
6. 执行密钥验证，验证不通过则再次申请密钥更新
7. 通过密钥验证后，各更新对称密钥
8. 销毁旧密钥

密钥验证流程：

ECU进行验证通信，即发送验证报文（明文），并对验证报文生成MAC。接收方使用收到验证报文（明文）及新对称密钥，生成MAC验证值，与接受到的MAC值比对，验证新对称密钥的一致性。