



GOTC 2023 全球开源技术峰会

THE GLOBAL OPENSOURCE TECHNOLOGY CONFERENCE

OPEN SOURCE, INTO THE FUTURE

「Cloud Native Summit」专场

服务网格中工作负载的私钥保护

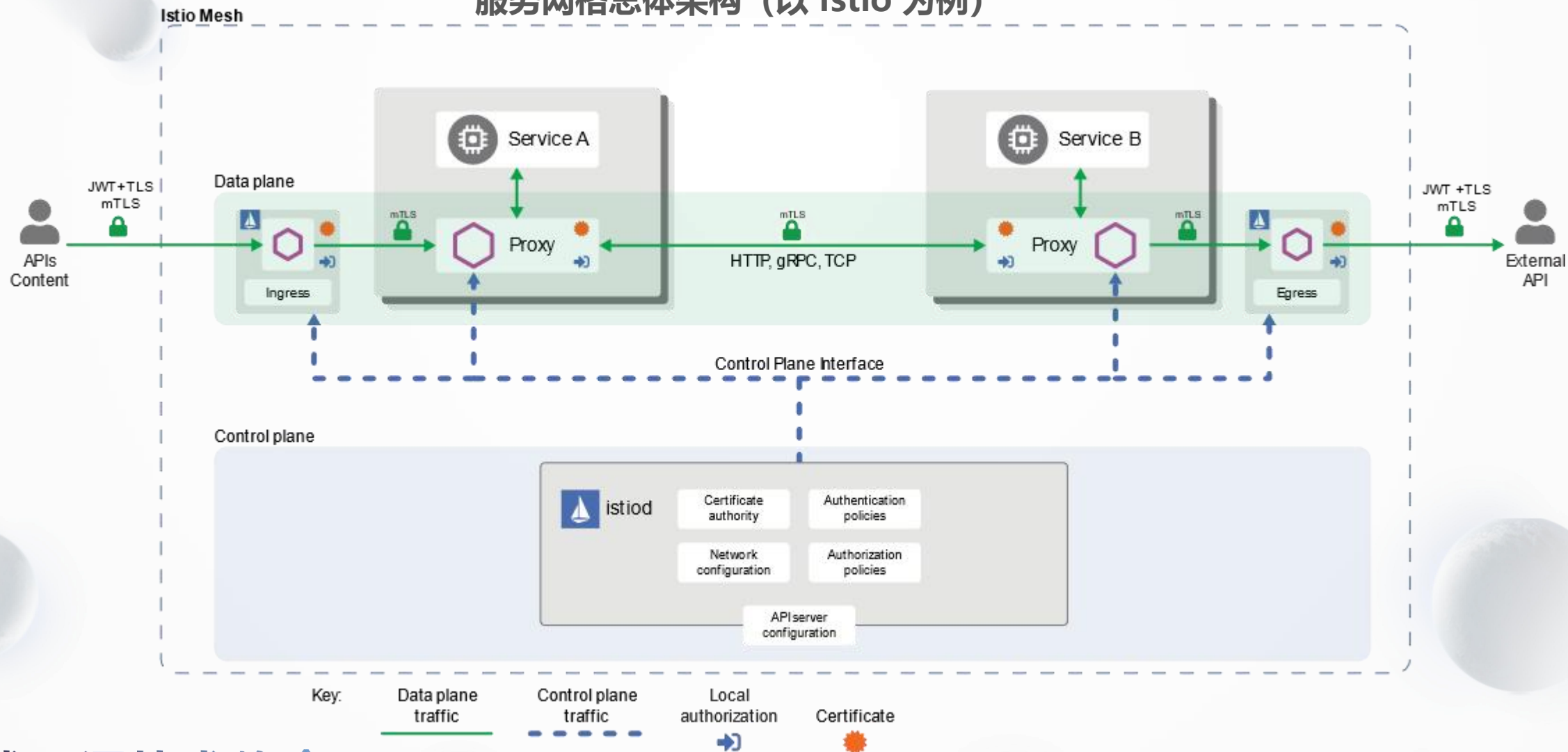
张怀龙 2023年5月28日

非常感谢 丁少君, 刘启明, 陈昕彤, 黄鑫 等同事的共同努力

议程

- 服务网格中工作负载私钥证书现状
- 工作负载私钥在服务网格中面临的风险
- 基于 Intel SGX 的工作负载私钥保护的方案
- 服务网格中工作负载私钥保护 Demo
- 未来计划

服务网格总体架构（以 Istio 为例）



工作负载私钥证书管理的关键组件大致有：

1. CA 服务器 (控制面或第三方 CA 服务器, 如 Istiod 或者 cert-manager)

- 负责签发工作负载证书,
- 将签名后的证书分发给对应工作负载的边车代理 (也可能是第三方 CA 服务器签发后由服务网格控制面完成分发)

2. 密钥发现服务 SDS (数据面 SDS server and API)

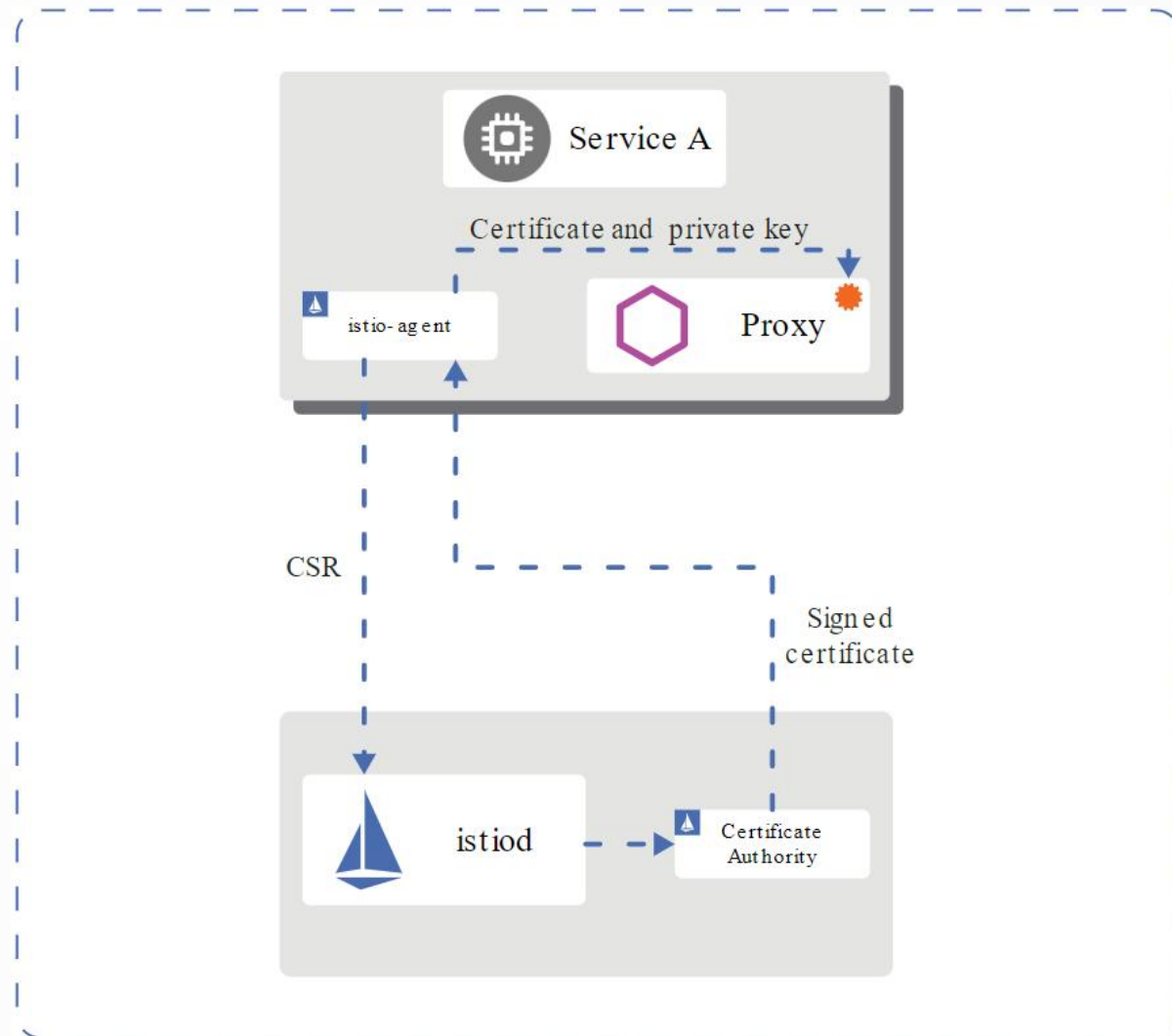
- 负责在运行时动态获取工作负载私钥和签发后的证书

3. 工作负载代理 (数据面, 比如 Istio-agent)

- 生成工作负载的私钥和 CSR
- 通过上一步的 CSR 向 CA 服务器申请证书
- 将工作负载私钥和签发后的证书发送给它对应的边车代理
- 处理工作负载私钥和证书的轮换

以Istio为例，具体的处理流程如下：

1. Istiod 提供 gRPC 服务以接受证书签名请求 (CSRs)
2. 当工作负载启动时，Envoy 通过密钥发现服务 (SDS) API 向同 Pod 内的 Istio-agent 发送证书和密钥请求
3. 在收到 SDS 请求后，Istio-agent 创建私钥和 CSR，然后将 CSR 及其凭据发送到 Istiod CA 进行签名
4. Istiod CA 验证 CSR 中携带的凭据，成功验证后签署 CSR 以生成证书
5. Istio-agent 通过 Envoy SDS API 将私钥和从 Istiod CA 收到的证书发送给 Envoy
6. Istio-agent 会监工作负载证书的有效期。上述 CSR 过程会周期性地重复，以处理证书和密钥轮换

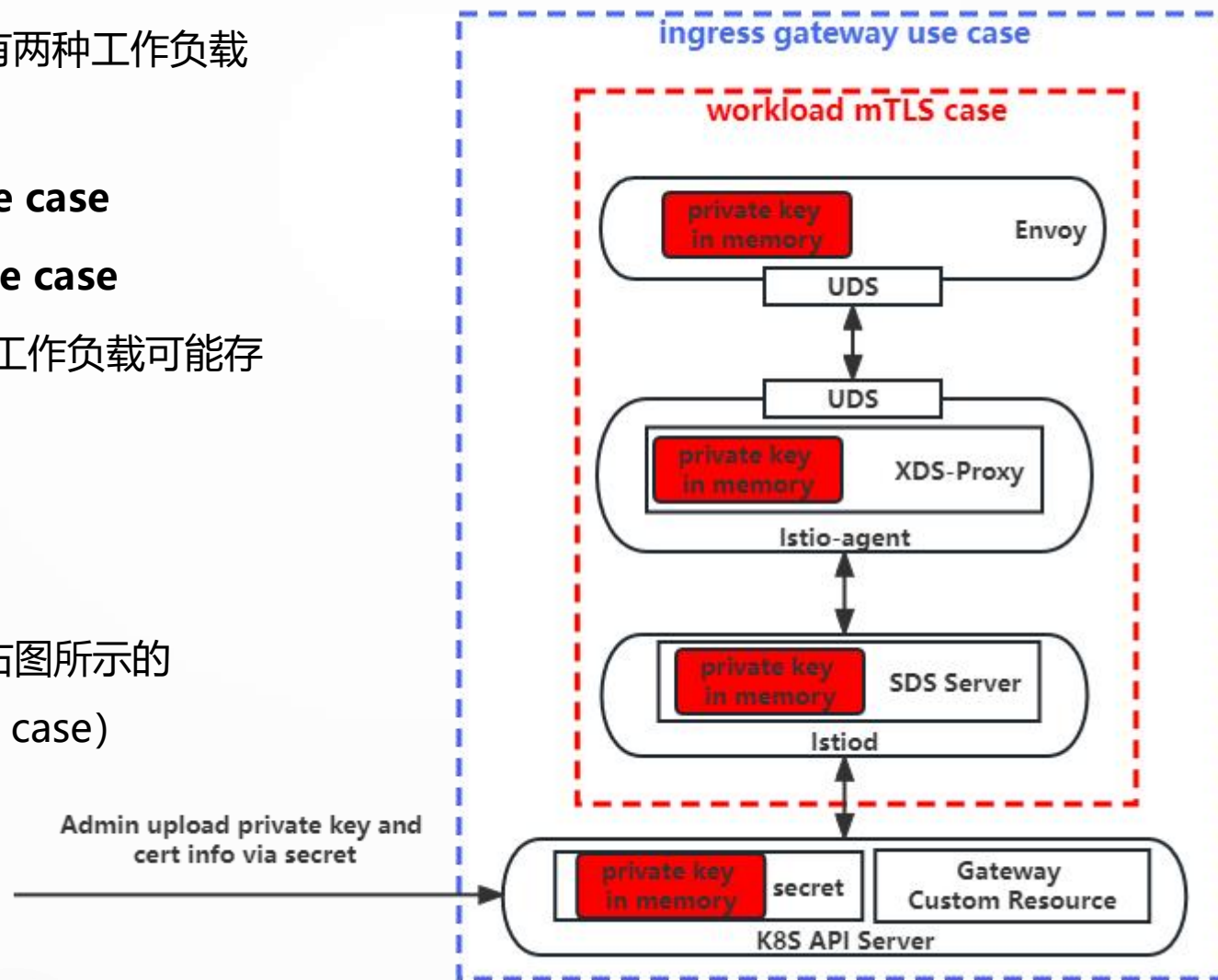


结合上面 Istio 的处理流程，有两种工作负载私钥的生成情况：

- **Workload mTLS use case**
- **Ingress gateway use case**

可以看到目前的服务网格中的工作负载可能存在的风险如下：

- 私钥是明文形式
- 私钥存储在内存中
- 私钥在外部上传（如右图所示的 ingress gateway use case）



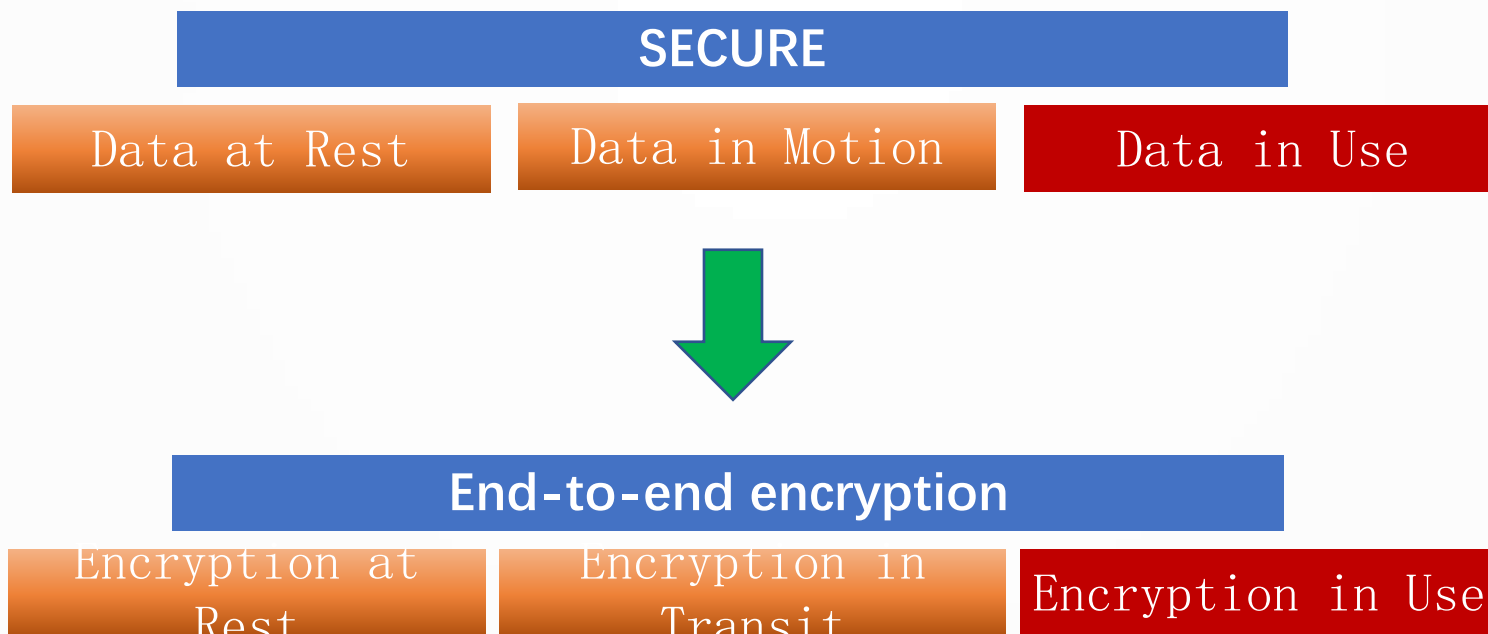
工作负载私钥在Envoy内存中

```
zhlsunshine@zhlsunshine:~/Downloads$ kubectl exec -it httpbin-698cc5f69-ch6qs -c istio-proxy -- bash
istio-proxy@httpbin-698cc5f69-ch6qs:/$
istio-proxy@httpbin-698cc5f69-ch6qs:/$
istio-proxy@httpbin-698cc5f69-ch6qs:/$ curl localhost:15000/config_dump | grep -A 20 -i SecretsConfigDump
% Total    % Received % Xferd  Average Speed   Time    Time     Time    Current
           Dload  Upload   Total     Spent    Left     Speed
100 291k    0 291k    0 27.1M    0 --:--:-- --:--:-- --:--:-- 28.5M
"@type": "type.googleapis.com/envoy.admin.v3.SecretsConfigDump",
"dynamic_active_secrets": [
  {
    "name": "default",
    "last_updated": "2023-04-25T06:13:09.513z",
    "secret": {
      "@type": "type.googleapis.com/envoy.extensions.transport_sockets.tls.v3.Secret",
      "name": "default",
      "tls_certificate": {
        "certificate_chain": {
          "inline_bytes": "LS0tLS1CRUdJTiBDRVJUSUZJQ0FURSB0tLS0tck1JSURQekNDQWl1Z0F3SUJBZ01Qum1iRUpvYXkxYXZsZmE1MMHMwRG9NQTBlh1NjY1NEUUVVCQ3dVQU1CZ3gKRmpBVUJnT1ZCQW9URFd0c2RYTjBawE11Ykc5a11Xd3dIaGNOTWpNd05ESTFNRF14TVRBNVdoY05Nak13TkrJmgnNRF14TxpBNVdqUQFNSU1CSwpBTKJna3Foa21HOXcwQkFRRUZBQ9dQVFE4OU1JSUJDZ0tDQVFFQXFRZHZXeJRxcMo0Y3ZsOHFsamJNL3dsSGxBWEh6a1FvQzd6STJTa2Joc2A2RjZ3SmkvNGpBRUYxadbFpLzVlRHJpWjh1bHJFR3MKbFRpb3pmb1hYQWdyTVY0NGhIWWJlWmJzTXVxSE52SDZ0L3dRMG02Q1Q5V3pLS0Naci92Nk12S3N4Y21TRlDNKwpUU2hKQXNOZkdEumpLTMruNXY0cTQwdkY2WXRwUE15dkRuSUFDbGtJVGRU24OZnr6K1F4VnZncG9wakVBNGI1CjgySTFVR3ZOSGNxeU0VzVxbu5oZDNncExzUFJFbk1tcWFHdmF1b0JQZm1hd2QwNXpnUzNHMmY3OFZoYVYVxcGoKbvpUN0RrNHNabzhtVU9TaX1L TE12aVFKZ11kdGF0bTVBcExxOU83a0JaUzRTK3daYkx0UXpJe1Bpb1VyY0VvNwpZaw1uYXd2NndsadRDd01EQVFBoM80R2RNSUdhTUE0R0ExVWREd0VCL3dRRUF3SUZvREFkQmdOVkhTVUUVGakFVckJnZ3JCZ0VGR1FjREFRWU1Ld1lCQ1FVSEF3SXdeQV1EV1IwVFEFRSC9CQU13QURBZk1nT1ZlU01FR0RBV2dCUW0KWdZ3MVBZW1hc11Z0TZYUctpbHNRSHc3OHpBNKJnT1ZlUkVCOY4RU1EQXVoaXh6Y0dsbVptVTZMeT1qYkhwegpkR1Z5TG14d1kyRnNMMjV6TDJsbFpTRjFiSFF2YzJFdmFIUjBjR0pwYmpBTk1na3Foa21HOXcwQkFRc0ZBQU9dCkFRRUFpcXFrYkpvUTQwOxP5jvcSDMyT1hrMkZ1w1S0j3QNEhql0VRQ3ZjZFE4d2NGMER2WnpYQkkrSm1Ed0EKd296V29rTFczVmxsSFpPSi9raUyVnBTcmFvdFdlR11PbTTFWjk2TmhTST1uL0FSNnBRQ18yd3BNWmNLTTyYkwpJQWdJvJyAyMWNiA3NkaFpYNTQzcWNNYmFhVWVmeFhXakZMDXNjQU1WSUhtZzhGYXFU1pIN3R1SGxBTzFqUFNPNlsegMwWHhJV2h1S2MrN1hYQ0JRUkpVZvd6MkNCUTFWRUVEOX1ani9jMnZtYytVaGs5b1RpR2FFN2FOL05TekEYVBxTDU0QXVZd0gxUEUCT2EywKFCWJzUy8yOvyb2VrWHJreXQ3TWFPt11zTkc0TmPWNz1xekxFNmMyUzRibgozelBibVpubnc2UEtmdwvybu51kytSMXR2UT09ci0tLS0tRU5EIEENFU1RJRk1DQVRFLS0tLS0KL S0tLS1CRUdJTiBDRVJUSUZJQ0FURSB0tLS0tck1JSUMvVENDQWVXZ0F3SUJBZ01SQU0yTXgzUE5MK3Q0EdDwskFBSS9CUEF3RFFZSk1w1w1odmNOQVFFTEJRQXCR0RFV01CUUdBMVVFQ2hNT1kyeDFjM1JsY2k1c2IyTmhiREF1RncweU16QTBVNGt3T0RRNE1UQmFGdzB6TXpBMApNVF13T0RRNE1UQmFNQmd4RmpBVUJnT1ZCQW9URFd0c2RYTjBawE11Ykc5a11Xd3dn20VpTUEwR0NTcudTSW1zckRRRUJBUVVBQTRJQkR3QxdnZ0VLQW9JQkFRRG1uRWRTRms3MD14dStnQzdlSmIvemN0eXZVRDNTQ3RoRWTcUHGKwjJEZ1g3SkpSM002U3N5Ukw3SE9kQ1ZqcXB3cUZRNU1zM1d1UnZLdVhjcF0WwOZzXpNK2dGd0RHEJ5ZDFUwplZ3FYdUozRkxoaThoRmJwYmtEUUVhBbzh1bUZZQk1Y1pocGo3eUy4Mn1wdTJmN1F1akNtRzdBM1crdkhueWE3CmE4WEtUR1hsb01IaxRPY2RJRnVmNHAYsXdrSUXHNWxIYUqV0hXWHFzw9WYjR0TXA0Vm5CVTVvb0100hKt3RjU5T3YmNYeStNTVFKSko2Ttk1VL2tLZEN5SkpTY2TYZ1wNEkvVmcwdfpUQXZoUc8yl2xpa2VmTV1JZcwWQpOMjFZYX1LeEftYy92SGhYTj1JMVm3UzhGd0MwzjVBSjBUUkxkYTFEB2RjVWFkZXJBZ01CQUFH1FqQkFNQTRHCKExVWREd0VCL3dRRUF3SUNCREFQqmdOVkhSTUJBJhFQ1RBREFRSC9NQjBhQTFVZERnUvdCQ1FtWDZ3MVBZW1hKkYXNzWtK2c1ArawxzuUUh3Nzh6QU5CZ2tXagtpRz13MEJBUXNGQUFQ0FRRUfKZzNCYVBZdZdV0VkvL0VrREZYAqpcZ1FEWVRQV1cySmc4UEUveEF1K0thOXROYXRPNMhad2h6cT1Ic11LMGNDNMxrQ1hHRCthL2h1dm1xw1pHQnAXckt6cFpZRFV5T0UyQTUwQkpgSy92S11QK2tLM3QxNjhyTFhLdS8vOudaavk4ZDJPb1Jnu015MG1mc11zaGdvRFkKa24yvytjc3Jxk09xm0ZaNyswUGJ1R2E2bytua1hVemtcMNVUdl1vWU1VUHQ0agXDOUcruitiQk9xZH2mWU9scqpNZjdneFQ1TnNkT0pHd11Ka1ZDZ1Zh13J6Z0phbXRXK2Vpa2JBevpVOG1xe1RPZWV2MHZLYnIzRkxYSmhJWEZTC1Y2djFxdHJwRU9NCURKa2daOV1iMHNZUE9FL0hobytkazM2a5S3cT1tb3VkwjVqbm1jT3M5Qm9hdzVzMWZURjYkT2c9PQotLS0tLUVORCBDRVJUSUZJQ0FURSB0tLS0tck1JSURQekNDQWl1Z0F3SUJBZ01Qum1iRUpvYXkxYXZsZmE1MMHMwRG9NQTBlh1NjY1NEUUVVCQ3dVQU1CZ3gKRmpBVUJnT1ZCQW9URFd0c2RYTjBawE11Ykc5a11Xd3dn20VpTUEwR0NTcudTSW1zckRRRUJBUVVBQTRJQkR3QxdnZ0VLQW9JQkFRRG1uRWRTRms3MD14dStnQzdlSmIvemN0eXZVRDNTQ3RoRWTcUHGKwjJEZ1g3SkpSM002U3N5Ukw3SE9kQ1ZqcXB3cUZRNU1zM1d1UnZLdVhjcF0WwOZzXpNK2dGd0RHEJ5ZDFUwplZ3FYdUozRkxoaThoRmJwYmtEUUVhBbzh1bUZZQk1Y1pocGo3eUy4Mn1wdTJmN1F1akNtRzdBM1crdkhueWE3CmE4WEtUR1hsb01IaxRPY2RJRnVmNHAYsXdrSUXHNWxIYUqV0hXWHFzw9WYjR0TXA0Vm5CVTVvb0100hKt3RjU5T3YmNYeStNTVFKSko2Ttk1VL2tLZEN5SkpTY2TYZ1wNEkvVmcwdfpUQXZoUc8yl2xpa2VmTV1JZcwWQpOMjFZYX1LeEftYy92SGhYTj1JMVm3UzhGd0MwzjVBSjBUUkxkYTFEB2RjVWFkZXJBZ01CQUFH1FqQkFNQTRHCKExVWREd0VCL3dRRUF3SUNCREFQqmdOVkhSTUJBJhFQ1RBREFRSC9NQjBhQTFVZERnUvdCQ1FtWDZ3MVBZW1hKkYXNzWtK2c1ArawxzuUUh3Nzh6QU5CZ2tXagtpRz13MEJBUXNGQUFQ0FRRUfKZzNCYVBZdZdV0VkvL0VrREZYAqpcZ1FEWVRQV1cySmc4UEUveEF1K0thOXROYXRPNMhad2h6cT1Ic11LMGNDNMxrQ1hHRCthL2h1dm1xw1pHQnAXckt6cFpZRFV5T0UyQTUwQkpgSy92S11QK2tLM3QxNjhyTFhLdS8vOudaavk4ZDJPb1Jnu015MG1mc11zaGdvRFkKa24yvytjc3Jxk09xm0ZaNyswUGJ1R2E2bytua1hVemtcMNVUdl1vWU1VUHQ0agXDOUcruitiQk9xZH2mWU9scqpNZjdneFQ1TnNkT0pHd11Ka1ZDZ1Zh13J6Z0phbXRXK2Vpa2JBevpVOG1xe1RPZWV2MHZLYnIzRkxYSmhJWEZTC1Y2djFxdHJwRU9NCURKa2daOV1iMHNZUE9FL0hobytkazM2a5S3cT1tb3VkwjVqbm1jT3M5Qm9hdzVzMWZURjYkT2c9PQotLS0tLUVORCBDRVJUSUZJQ0FURSB0tLS0tck1JSURQekNDQWl1Z0F3SUJBZ01Qum1iRUpvYXkxYXZsZmE1MMHMwRG9NQTBlh1NjY1NEUUVVCQ3dVQU1CZ3gKRmpBVUJnT1ZCQW9URFd0c2RYTjBawE11Ykc5a11Xd3dn20VpTUEwR0NTcudTSW1zckRRRUJBUVVBQTRJQkR3QxdnZ0VLQW9JQkFRRG1uRWRTRms3MD14dStnQzdlSmIvemN0eXZVRDNTQ3RoRWTcUHGKwjJEZ1g3SkpSM002U3N5Ukw3SE9kQ1ZqcXB3cUZRNU1zM1d1UnZLdVhjcF0WwOZzXpNK2dGd0RHEJ5ZDFUwplZ3FYdUozRkxoaThoRmJwYmtEUUVhBbzh1bUZZQk1Y1pocGo3eUy4Mn1wdTJmN1F1akNtRzdBM1crdkhueWE3CmE4WEtUR1hsb01IaxRPY2RJRnVmNHAYsXdrSUXHNWxIYUqV0hXWHFzw9WYjR0TXA0Vm5CVTVvb0100hKt3RjU5T3YmNYeStNTVFKSko2Ttk1VL2tLZEN5SkpTY2TYZ1wNEkvVmcwdfpUQXZoUc8yl2xpa2VmTV1JZcwWQpOMjFZYX1LeEftYy92SGhYTj1JMVm3UzhGd0MwzjVBSjBUUkxkYTFEB2RjVWFkZXJBZ01CQUFH1FqQkFNQTRHCKExVWREd0VCL3dRRUF3SUNCREFQqmdOVkhSTUJBJhFQ1RBREFRSC9NQjBhQTFVZERnUvdCQ1FtWDZ3MVBZW1hKkYXNzWtK2c1ArawxzuUUh3Nzh6QU5CZ2tXagtpRz13MEJBUXNGQUFQ0FRRUfKZzNCYVBZdZdV0VkvL0VrREZYAqpcZ1FEWVRQV1cySmc4UEUveEF1K0thOXROYXRPNMhad2h6cT1Ic11LMGNDNMxrQ1hHRCthL2h1dm1xw1pHQnAXckt6cFpZRFV5T0UyQTUwQkpgSy92S11QK2tLM3QxNjhyTFhLdS8vOudaavk4ZDJPb1Jnu015MG1mc11zaGdvRFkKa24yvytjc3Jxk09xm0ZaNyswUGJ1R2E2bytua1hVemtcMNVUdl1vWU1VUHQ0agXDOUcruitiQk9xZH2mWU9scqpNZjdneFQ1TnNkT0pHd11Ka1ZDZ1Zh13J6Z0phbXRXK2Vpa2JBevpVOG1xe1RPZWV2MHZLYnIzRkxYSmhJWEZTC1Y2djFxdHJwRU9NCURKa2daOV1iMHNZUE9FL0hobytkazM2a5S3cT1tb3VkwjVqbm1jT3M5Qm9hdzVzMWZURjYkT2c9PQotLS0tLUVORCBDRVJUSUZJQ0FURSB0tLS0tck1JSURQekNDQWl1Z0F3SUJBZ01Qum1iRUpvYXkxYXZsZmE1MMHMwRG9NQTBlh1NjY1NEUUVVCQ3dVQU1CZ3gKRmpBVUJnT1ZCQW9URFd0c2RYTjBawE11Ykc5a11Xd3dn20VpTUEwR0NTcudTSW1zckRRRUJBUVVBQTRJQkR3QxdnZ0VLQW9JQkFRRG1uRWRTRms3MD14dStnQzdlSmIvemN0eXZVRDNTQ3RoRWTcUHGKwjJEZ1g3SkpSM002U3N5Ukw3SE9kQ1ZqcXB3cUZRNU1zM1d1UnZLdVhjcF0WwOZzXpNK2dGd0RHEJ5ZDFUwplZ3FYdUozRkxoaThoRmJwYmtEUUVhBbzh1bUZZQk1Y1pocGo3eUy4Mn1wdTJmN1F1akNtRzdBM1crdkhueWE3CmE4WEtUR1hsb01IaxRPY2RJRnVmNHAYsXdrSUXHNWxIYUqV0hXWHFzw9WYjR0TXA0Vm5CVTVvb0100hKt3RjU5T3YmNYeStNTVFKSko2Ttk1VL2tLZEN5SkpTY2TYZ1wNEkvVmcwdfpUQXZoUc8yl2xpa2VmTV1JZcwWQpOMjFZYX1LeEftYy92SGhYTj1JMVm3UzhGd0MwzjVBSjBUUkxkYTFEB2RjVWFkZXJBZ01CQUFH1FqQkFNQTRHCKExVWREd0VCL3dRRUF3SUNCREFQqmdOVkhSTUJBJhFQ1RBREFRSC9NQjBhQTFVZERnUvdCQ1FtWDZ3MVBZW1hKkYXNzWtK2c1ArawxzuUUh3Nzh6QU5CZ2tXagtpRz13MEJBUXNGQUFQ0FRRUfKZzNCYVBZdZdV0VkvL0VrREZYAqpcZ1FEWVRQV1cySmc4UEUveEF1K0thOXROYXRPNMhad2h6cT1Ic11LMGNDNMxrQ1hHRCthL2h1dm1xw1pHQnAXckt6cFpZRFV5T0UyQTUwQkpgSy92S11QK2tLM3QxNjhyTFhLdS8vOudaavk4ZDJPb1Jnu015MG1mc11zaGdvRFkKa24yvytjc3Jxk09xm0ZaNyswUGJ1R2E2bytua1hVemtcMNVUdl1vWU1VUHQ0agXDOUcruitiQk9xZH2mWU9scqpNZjdneFQ1TnNkT0pHd11Ka1ZDZ1Zh13J6Z0phbXRXK2Vpa2JBevpVOG1xe1RPZWV2MHZLYnIzRkxYSmhJWEZTC1Y2djFxdHJwRU9NCURKa2daOV1iMHNZUE9FL0hobytkazM2a5S3cT1tb3VkwjVqbm1jT3M5Qm9hdzVzMWZURjYkT2c9PQotLS0tLUVORCBDRVJUSUZJQ0FURSB0tLS0tck1JSURQekNDQWl1Z0F3SUJBZ01Qum1iRUpvYXkxYXZsZmE1MMHMwRG9NQTBlh1NjY1NEUUVVCQ3dVQU1CZ3gKRmpBVUJnT1ZCQW9URFd0c2RYTjBawE11Ykc5a11Xd3dn20VpTUEwR0NTcudTSW1zckRRRUJBUVVBQTRJQkR3QxdnZ0VLQW9JQkFRRG1uRWRTRms3MD14dStnQzdlSmIvemN0eXZVRDNTQ3RoRWTcUHGKwjJEZ1g3SkpSM002U3N5Ukw3SE9kQ1ZqcXB3cUZRNU1zM1d1UnZLdVhjcF0WwOZzXpNK2dGd0RHEJ5ZDFUwplZ3FYdUozRkxoaThoRmJwYmtEUUVhBbzh1bUZZQk1Y1pocGo3eUy4Mn1wdTJmN1F1akNtRzdBM1crdkhueWE3CmE4WEtUR1hsb01IaxRPY2RJRnVmNHAYsXdrSUXHNWxIYUqV0hXWHFzw9WYjR0TXA0Vm5CVTVvb0100hKt3RjU5T3YmNYeStNTVFKSko2Ttk1VL2tLZEN5SkpTY2TYZ1wNEkvVmcwdfpUQXZoUc8yl2xpa2VmTV1JZcwWQpOMjFZYX1LeEftYy92SGhYTj1JMVm3UzhGd0MwzjVBSjBUUkxkYTFEB2RjVWFkZXJBZ01CQUFH1FqQkFNQTRHCKExVWREd0VCL3dRRUF3SUNCREFQqmdOVkhSTUJBJhFQ1RBREFRSC9NQjBhQTFVZERnUvdCQ1FtWDZ3MVBZW1hKkYXNzWtK2c1ArawxzuUUh3Nzh6QU5CZ2tXagtpRz13MEJBUXNGQUFQ0FRRUfKZzNCYVBZdZdV0VkvL0VrREZYAqpcZ1FEWVRQV1cySmc4UEUveEF1K0thOXROYXRPNMhad2h6cT1Ic11LMGNDNMxrQ1hHRCthL2h1dm1xw1pHQnAXckt6cFpZRFV5T0UyQTUwQkpgSy92S11QK2tLM3QxNjhyTFhLdS8vOudaavk4ZDJPb1Jnu015MG1mc11zaGdvRFkKa24yvytjc3Jxk09xm0ZaNyswUGJ1R2E2bytua1hVemtcMNVUdl1vWU1VUHQ0agXDOUcruitiQk9xZH2mWU9scqpNZjdneFQ1TnNkT0pHd11Ka1ZDZ1Zh13J6Z0phbXRXK2Vpa2JBevpVOG1xe1RPZWV2MHZLYnIzRkxYSmhJWEZTC1Y2djFxdHJwRU9NCURKa2daOV1iMHNZUE9FL0hobytkazM2a5S3cT1tb3VkwjVqbm1jT3M5Qm9hdzVzMWZURjYkT2c9PQotLS0tLUVORCBDRVJUSUZJQ0FURSB0tLS0tck1JSURQekNDQWl1Z0F3SUJBZ01Qum1iRUpvYXkxYXZsZmE1MMHMwRG9NQTBlh1NjY1NEUUVVCQ3dVQU1CZ3gKRmpBVUJnT1ZCQW9URFd0c2RYTjBawE11Ykc5a11Xd3dn20VpTUEwR0NTcudTSW1zckRRRUJBUVVBQTRJQkR3QxdnZ0VLQW9JQkFRRG1uRWRTRms3MD14dStnQzdlSmIvemN0eXZVRDNTQ3RoRWTcUHGKwjJEZ1g3SkpSM002U3N5Ukw3SE9kQ1ZqcXB3cUZRNU1zM1d1UnZLdVhjcF0WwOZzXpNK2dGd0RHEJ5ZDFUwplZ3FYdUozRkxoaThoRmJwYmtEUUVhBbzh1bUZZQk1Y1pocGo3eUy4Mn1wdTJmN1F1akNtRzdBM1crdkhueWE3CmE4WEtUR1hsb01IaxRPY2RJRnVmNHAYsXdrSUXHNWxIYUqV0hXWHFzw9WYjR0TXA0Vm5CVTVvb0100hKt3RjU5T3YmNYeStNTVFKSko2Ttk1VL2tLZEN5SkpTY2TYZ1wNEkvVmcwdfpUQXZoUc8yl2xpa2VmTV1JZcwWQpOMjFZYX1LeEftYy92SGhYTj1JMVm3UzhGd0MwzjVBSjBUUkxkYTFEB2RjVWFkZXJBZ01CQUFH1FqQkFNQTRHCKExVWREd0VCL3dRRUF3SUNCREFQqmdOVkhSTUJBJhFQ1RBREFRSC9NQjBhQTFVZERnUvdCQ1FtWDZ3MVBZW1hKkYXNzWtK2c1ArawxzuUUh3Nzh6QU5CZ2tXagtpRz13MEJBUXNGQUFQ0FRRUfKZzNCYVBZdZdV0VkvL0VrREZYAqpcZ1FEWVRQV1cySmc4UEUveEF1K0thOXROYXRPNMhad2h6cT1Ic11LMGNDNMxrQ1hHRCthL2h1dm1xw1pHQnAXckt6cFpZRFV5T0UyQTUwQkpgSy92S11QK2tLM3QxNjhyTFhLdS8vOudaavk4ZDJPb1Jnu015MG1mc11zaGdvRFkKa24yvytjc3Jxk09xm0ZaNyswUGJ1R2E2bytua1hVemtcMNVUdl1vWU1VUHQ0agXDOUcruitiQk9xZH2mWU9scqpNZjdneFQ1TnNkT0pHd11Ka1ZDZ1Zh13J6Z0phbXRXK2Vpa2JBevpVOG1xe1RPZWV2MHZLYnIzRkxYSmhJWEZTC1Y2djFxdHJwRU9NCURKa2daOV1iMHNZUE9FL0hobytkazM2a5S3cT1tb3VkwjVqbm1jT3M5Qm9hdzVzMWZURjYkT2c9PQotLS0tLUVORCBDRVJUSUZJQ0FURSB0tLS0tck1JSURQekNDQWl1Z0F3SUJBZ01Qum1iRUpvYXkxYXZsZmE1MMHMwRG9NQTBlh1NjY1NEUUVVCQ3dVQU1CZ3gKRmpBVUJnT1ZCQW9URFd0c2RYTjBawE11Ykc5a11Xd3dn20VpTUEwR0NTcudTSW1zckRRRUJBUVVBQTRJQkR3QxdnZ0VLQW9JQkFRRG1uRWRTRms3MD14dStnQzdlSmIvemN0eXZVRDNTQ3RoRWTcUHGKwjJEZ1g3SkpSM002U3N5Ukw3SE9kQ1ZqcXB3cUZRNU1zM1d1UnZLdVhjcF0WwOZzXpNK2dGd0RHEJ5ZDFUwplZ3FYdUozRkxoaThoRmJwYmtEUUVhBbzh1bUZZQk1Y1pocGo3eUy4Mn1wdTJmN1F1akNtRzdBM1crdkhueWE3CmE4WEtUR1hsb01IaxRPY2RJRnVmNHAYsXdrSUXHNWxIYUqV0hXWHFzw9WYjR0TXA0Vm5CVTVvb0100hKt3RjU5T3YmNYeStNTVFKSko2Ttk1VL2tLZEN5SkpTY2TYZ1wNEkvVmcwdfpUQXZoUc8yl2xpa2VmTV1JZcwWQpOMjFZYX1LeEftYy92SGhYTj1JMVm3UzhGd0MwzjVBSjBUUkxkYTFEB2RjVWFkZXJBZ01CQUFH1FqQkFNQTRHCKExVWREd0VCL3dRRUF3SUNCREFQqmdOVkhSTUJBJhFQ1RBREFRSC9NQjBhQTFVZERnUvdCQ1FtWDZ3MVBZW1hKkYXNzWtK2c1ArawxzuUUh3Nzh6QU5CZ2tXagtpRz13MEJBUXNGQUFQ0FRRUfKZzNCYVBZdZdV0VkvL0VrREZYAqpcZ1FEWVRQV1cySmc4UEUveEF1K0thOXROYXRPNMhad2h6cT1Ic11LMGNDNMxrQ1hHRCthL2h1dm1xw1pHQnAXckt6cFpZRFV5T0UyQTUwQkpgSy92S11QK2tLM3QxNjhyTFhLdS8vOudaavk4ZDJPb1Jnu015MG1mc11zaGdvRFkKa24yvytjc3Jxk09xm0ZaNyswUGJ1R2E2bytua1hVemtcMNVUdl1vWU1VUHQ0agXDOUcruitiQk9xZH2mWU9scqpNZjdneFQ1TnNkT0pHd11Ka1ZDZ1Zh13J6Z0phbXRXK2Vpa2JBevpVOG1xe1RPZWV2MHZLYnIzRkxYSmhJWEZTC1Y2djFxdHJwRU9NCURKa2daOV1iMHNZUE9FL0hobytkazM2a5S3cT1tb3VkwjVqbm1jT3M5Qm9hdzVzMWZURjYkT2c9PQotLS0tLUVORCBDRVJUSUZJQ0FURSB0tLS0tck1JSURQekNDQWl1Z0F3SUJBZ01Qum1iRUpvYXkxYXZsZmE1MMHMwRG9NQTBlh1NjY1NEUUVVCQ3dVQU1CZ3gKRmpBVUJnT1ZCQW9URFd0c2RYTjBawE11Ykc5a11Xd3dn20VpTUEwR0NTcudTSW1zckRRRUJBUVVBQTRJQkR3QxdnZ0VLQW9JQkFRRG1uRWRTRms3MD14dStnQzdlSmIvemN0eXZVRDNTQ3RoRWTcUHGKwjJEZ1g3SkpSM002U3N5Ukw3SE9kQ1ZqcXB3cUZRNU1zM1d1UnZLdVhjcF0WwOZzXpNK2dGd0RHEJ5ZDFUwplZ3FYdUozRkxoaThoRmJwYmtEUUVhBbzh1bUZZQk1Y1pocGo3eUy4Mn1wdTJmN1F1akNtRzdBM1crdkhueWE3CmE4WEtUR1hsb01IaxRPY2RJRnVmNHAYsXdrSUXHNWxIYUqV0hXWHFzw9WYjR0TXA0Vm5CVTVvb0100hKt3RjU5T3YmNYeStNTVFKSko2Ttk1VL2tLZEN5SkpTY2TYZ1wNEkvVmcwdfpUQXZoUc8yl2xpa2VmTV1JZcwWQpOMjFZYX1LeEftYy92SGhYTj1JMVm3UzhGd0MwzjVBSjBUUkxkYTFEB2RjVWFkZXJBZ01CQUFH1FqQkFNQTRHCKExVWREd0VCL3dRRUF3SUNCREFQqmdOVkhSTUJBJhFQ1RBREFRSC9NQjBhQTFVZERnUvdCQ1FtWDZ3MVBZW1hKkYXNzWtK2c1ArawxzuUUh3Nzh6QU5CZ2tXagtpRz13MEJBUXNGQUFQ0FRRUfKZzNCYVBZdZdV0VkvL0VrREZYAqpcZ1FEWVRQV1cySmc4UEUveEF1K0thOXROYXRPNMhad2h6cT1Ic11LMGNDNMxrQ1hHRCthL2h1dm1xw1pHQnAXckt6cFpZRFV5T0UyQTUwQkpgSy92S11QK2tLM3QxNjhyTFhLdS8vOudaavk4ZDJPb1Jnu015MG1mc11zaGdvRFkKa24yvytjc3Jxk09xm0ZaNyswUGJ1R2E2bytua1hVemtcMNVUdl1vWU1VUHQ0agXDOUcruitiQk9xZH2mWU9scqpNZjdneFQ1TnNkT0pHd11Ka1ZDZ1Zh13J6Z0phbXRXK2Vpa2JBevpVOG1xe1RPZWV2MHZLYnIzRkxYSmhJWEZTC1Y2djFxdHJwRU9NCURKa2daOV1iMHNZUE9FL0hobytkazM2a5S3cT1tb3VkwjVqbm1jT3M5Qm9hdzVzMWZURjYkT2c9PQotLS0tLUVORCBDRVJUSUZJQ0FURSB0tLS0tck1JSURQekNDQWl1Z0F3SUJBZ01Qum1iRUpvYXkxYXZsZmE1MMHMwRG9NQTBlh1NjY1NEUUVVCQ3dVQU1CZ3gKRmpBVUJnT1ZCQW9URFd0c2RYTjBawE11Ykc5a11Xd3dn20VpTUEwR0NTcudTSW1zckRRRUJBUVVBQTRJQkR3QxdnZ0VLQW9JQkFRRG1uRWRTRms3MD14dStnQzdlSmIvemN0eXZVRDNTQ3RoRWTcUHGKwjJEZ1g3SkpSM002U3N5Ukw3SE9kQ1ZqcXB3cUZRNU1zM1d1UnZLdVhjcF0WwOZzXpNK2dGd0RHEJ5ZDFUwplZ3FYdUozRkxoaThoRmJwYmtEUUVhBbzh1bUZZQk1Y1pocGo3eUy4Mn1wdTJmN1F1akNtRzdBM1crdkhueWE3CmE4WEtUR1hsb01IaxRPY2RJRnVmNHAYsXdrSUXHNWxIYUqV0hXWHFzw9WYjR0TXA0Vm5CVTVvb0100hKt3RjU5T3YmNYeStNTVFKSko2Ttk1VL2tLZEN5SkpTY2TYZ1wNEkvVmcwdfpUQXZoUc8yl2xpa2VmTV1JZcwWQpOMjFZYX1LeEftYy92SGhYTj1JMVm3UzhGd0MwzjVBSjBUUkxkYTFEB2RjVWFkZXJBZ01CQUFH1FqQkFNQTRHCKExVWREd0VCL3dRRUF3SUNCREFQqmdOVkhSTUJBJhFQ1RBREFRSC9NQjBhQTFVZERnUvdCQ1FtWDZ3MVBZW1hKkYXNzWtK2c1ArawxzuUUh3Nzh6QU5CZ2tXagtpRz13MEJBUXNGQUFQ0FRRUfKZzNCYVBZdZdV0VkvL0VrREZYAqpcZ1FEWVRQV1cySmc4UEUveEF1K0thOXROYXRPNMhad2h6cT1Ic11LMGNDNMxrQ1hHRCthL2h1dm1xw1pHQnAXckt6cFpZRFV5T0UyQTUwQkpgSy92S11QK2tLM3QxNjhyTFhLdS8vOudaavk4ZDJPb1Jnu015MG1mc11zaGdvRFkKa24yvytjc3Jxk09xm0ZaNyswUGJ1R2E2bytua1hVemtcMNVUdl1vWU1VUHQ0agXDOUcruitiQk9xZH2mWU9scqpNZjdneFQ1TnNkT0pHd11Ka1ZDZ1Zh13J6Z0phbXRXK2Vpa2JBevpVOG1xe1RPZWV2MHZLYnIzRkxYSmhJWEZTC1Y2djFxdHJwRU9NCURKa2daOV1iMHNZUE9FL0hobytkazM2a5S3cT1tb3VkwjVqbm1jT3M5Qm9hdzVzMWZURjYkT2c9PQotLS0tLUVORCBDRVJUSUZJQ0FURSB0tLS0tck1JSURQekNDQWl1Z0F3SUJBZ01Qum1iRUpvYXkxYXZsZmE1MMHMwRG9NQTBlh1NjY1NEUUVVCQ3dVQU1CZ3gKRmpBVUJnT1ZCQW9URFd0c2RYTjBawE11Ykc5a11Xd3dn20VpTUEwR0NTcudTSW1zckRRRUJBUVVBQTRJQkR3QxdnZ0VLQW9JQkFRRG1uRWRTRms3MD14dStnQzdlSmIvemN0eXZVRDNTQ3RoRWTcUHGKwjJEZ1g3SkpSM002U3N5Ukw3SE9kQ1ZqcXB3cUZRNU1zM1d1UnZLdVhjcF0WwOZzXpNK2dGd0RHEJ5ZDFUwplZ3FYdUozRkxoaThoRmJwYmtEUUVhBbzh1bUZZQk1Y1pocGo3eUy4Mn1wdTJmN1F1akNtRzdBM1crdkhueWE3CmE4WEtUR1hsb01IaxRPY2RJRnVmNHAYsXdrSUXHNWxIYUqV0hXWHFzw9WYjR0TXA0Vm5CVTVvb0100hKt3RjU5T3YmNYeStNTVFKSko2Ttk1VL2tLZEN5SkpTY2TYZ1wNEkvVmcwdfpUQXZoUc8yl2xpa2VmTV1JZcwWQpOMjFZYX1LeEftYy92SGhYTj1JMVm3UzhGd0MwzjVBSjBUUkxkYTFEB2RjVWFkZXJBZ01CQUFH1FqQkFNQTRHCKExVWREd0VCL3dRRUF3SUNCREFQqmdOVkhSTUJBJhFQ1RBREFRSC9NQjBhQTFVZERnUvdCQ1FtWDZ3MVBZW1hKkYXNzWtK2c1ArawxzuUUh3Nzh6QU5CZ2tXagtpRz13MEJBUXNGQUFQ0FRRUfKZzNCYVBZdZdV0VkvL0VrREZYAqpcZ1FEWVRQV1cySmc4UEUveEF1K0thOXROYXRPNMhad2h6cT1Ic11LMGNDNMxrQ1hHRCthL2h1dm1xw1pHQnAXckt6cFpZRFV5T0UyQTUwQkpgSy92S11QK2tLM3QxNjhyTFhLdS8vOudaavk4ZDJPb1Jnu015MG1mc11zaGdvRFkKa24yvytjc3Jxk09xm0ZaNyswUGJ1R2E2bytua1hVemtcMNVUdl1vWU1VUHQ0agXDOUcruitiQk9xZH2mWU9scqpNZjdneFQ1TnNkT0pHd11Ka1ZDZ1Zh13J6Z0phbXRXK2Vpa2JBevpVOG1xe1RPZWV2MHZLYnIzRkxYSmhJWEZTC1Y2djFxdHJwRU9NCURKa2daOV1iMHNZUE9FL0hobytkazM2a5S3cT1tb3VkwjVqbm1jT3M5Qm9hdzVzMWZURjYkT2c9PQotLS0tLUVORCBDRVJUSUZJQ0FURSB0tLS0tck1JSURQekNDQWl1Z0F3SUJBZ01Qum1iRUpvYXkxYXZsZmE1MMHMwRG9NQTBlh1NjY1NEUUVVCQ3dVQU1CZ3gKRmpBVUJnT1ZCQW9URFd0c2RYTjBawE11Ykc5a11Xd3dn20VpTUEwR0NTcudTSW1zckRRRUJBUVVBQTRJQkR3QxdnZ0VLQW9JQkFRRG1uRWRTRms3MD14dStnQzdlSmIvemN0eXZVRDNTQ3RoRWTcUHGKwjJEZ1g3SkpSM002U3N5Ukw3SE9kQ1ZqcXB3cUZRNU1zM1d1UnZLdVhjcF0WwOZzXpNK2dGd0RHEJ5ZDFUwplZ3FYdUozRkxoaThoRmJwYmtEUUVhBbzh1bUZZQk1Y1pocGo3eUy4Mn1wdTJmN1F1akNtRzdBM1crdkhueWE3CmE4WEtUR1hsb01IaxRPY2RJRnVmNHAYsXdrSUXHNWxIYUqV0hXWHFzw9WYjR0TXA0Vm5CVTVvb0100hKt3RjU5T3YmNYeStNTVFKSko2Ttk1VL2tLZEN5SkpTY2TYZ1wNEkvVmcwdfpUQXZoUc8yl2xpa2VmTV1JZcwWQpOMjFZYX1LeEftYy92SGhYTj1JMVm3UzhGd0MwzjVBSjBUUkxkYTFEB2RjVWFkZXJBZ01CQUFH1FqQkFNQTRHCKExVWREd0VCL3dRRUF3SUNCREFQqmdOVkhSTUJBJhFQ1RBREFRSC9NQjBhQTFVZERnUvdCQ1FtWDZ3MVBZW1hKkYXNzWtK2c1ArawxzuUUh3Nzh6QU5CZ2tXagtpRz13MEJBUXNGQUFQ0FRRUfKZzNCYVBZdZdV0VkvL0VrREZYAqpcZ1FEWVRQV1cySmc4UEUveEF1K0thOXROYXRPNMhad2h6cT1Ic11LMGNDNMxrQ1hHRCthL2h1dm1xw1pHQnAXckt6cFpZRFV5T0UyQTUwQkpgSy92S11QK2tLM3QxNjhyTFhLdS8vOudaavk4ZDJPb1Jnu015MG1mc11zaGdvRFkKa24y
```


工作负载私钥在k8s secret中

```
zhlsunshine@zhlsunshine:~/Downloads/istio-1.18.0-alpha.0$ kubectl get secret httpbin-credential -n istio-system -oyaml
apiVersion: v1
data:
  tls.crt: LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUMzakNDQWNZQ0FRQXdEUVJKS29aSWh2Y05BUUVMQlFBd0xURVZNQk1HQTFVRUNnd01awGhoY1hCc1pTQkoKYM1NdU1SUXdFZ11EV1FRERBdGx1R0Z0Y0
  d4bExtTnZiVEFlRncweU16QTBnamd3TwpJNE1ETmFGdzB5TkRBMAppNamN3TwpJNE1ETmFNrDB4SERBYUJnTlZCQU1NRtJomGRIQm1hVzR1w1hoaGJYQnNaUzVqYjIweEhUQWJCZ05wckJBb01GR2gwZehCawFXNGdiM0pulwVc
  1cGvtrjBhvz11TU1JQk1qQ5C22txagtPrz13MEJBUUVGUQFPQ0FROEEKTU1JQkNnS0NBuUvBeU6FNHUXbWVmjN6ZTdjBzZCNC90dU0rQmVtawRyZDV0TzuOEJhdwXtNis3MmtN3Y1IagoXmZdBVnRPMUwrT2tuNcthTuxv
  SH12bw1MY1JHCHBmS0dVNXk4NGVvZmdTL2FkdNvoc1h2aTR2VzcrYXVHOXY2CmdIK3I3Z2k0bzJjcjRNQ1Z4bW5F5RjJtdVo3NTZMUEhYcnFla2YrWTZRNTB1N0hvK1FGYVJo0EpoMTdhs2JyVUMKmjZFK096M084R0h5SDdnw
  W9Nb2NadDzpcUVEwxySwD2S2xubzdxSuhXcw9GUU56NENBa1dJYmtxZ2RLZENHTApRdkFWntJycThkYk1FMEVBA1o2a201cnhUQU1DR1FCYmZHeVU4TU1rOX1EZzhDWGc5TW1LS1FVOFFecWgzNXo5Ck1oazc5dzFyQ1dBRt
  h6UEw4MFpuNVpNCXBuc3J6bnY4MVFJREFRQUJNQTBHQ1NXR1NjYjNEUUVUQ3dVQUE0SUIKQVFBVmtJK2pISFZtUTB0K1U1MjFNZkF3MCszTG8yaHlucR1c1R1TFdxVktPdHUyT0g0UUFNLWG1wVj1CV21BbGpXYU5xRDk4bXJ
  xTFUyT0pEMFVpVWQ3SXVSTmZyW1NBbE51YmEydmlCOSTXRU0zRStVVctUUFZTRzNFBG9TczVfckErcwFDNnpYNkprNFRnRjNRaz1sS3NkNWRtKzdJOG5jTjFvZV1LVjRnUWJ1MU1XcWNPcwUvNkFESVRQWVhR0oKOCtMQ0tD
  b012Uno1OUHQ0tswmdisGFxRwdjSw9EUXZFbX1PSzB2QxpKUFZWMDczN01wdkR3TG1Xvm5hRyswZaAoYzduMnNJK0Jpvk5mRk9HMHRCnw0c3JDUUFyR2xPdEZFNgi1UDN6dFFxdkV6cwVooDB5U2xIYmhnnE0yTFpICndHd
  TgOU3hCYZHRUS9zbHM3Z3Urc3dhNAotLS0tLUVORCBDRVJUSUZJQ0FURS0tLS0tCg==
  tls.key: LS0tLS1CRUdJTiBQVFIETFWStLS0tCk1JSUV2d01CQURBTKJna3Foa21HOXcwQkFRRUZBQVNDQktrd2dnU2xB20VBQW9JQkFRRE1EUGk3V1oyamJmTjckdH1qb0hqKzI0ejRGNutKMnQzbHYzcWZ3Rn
  E2VkyXN3Zhu0J6SnVQWgzZQ1cyTFV2NDZTmo1b3d1Z2ZLK2FZdAp4RwFtbDhVw1RuThponVIRQkw5cDirNkd4ZStMat1idjVxNGIyL3FBZjZ2dUNMawpZaxZnd0pYR1pySVhhYTVuCNzUb3M4ZGV1cDZSLzVqcERUjdZzWo
  1QVZwR0h3bUhYdG9wdXRWN2JvVDQ3UGM3d1lmsWZ1Qm1newh4bTNxS28KU082V3NpQzhxV2VqdW9nZGFxZ1ZBM1BnSUNSwwh1U3FCMHawSV1OQzhCWG5hdXJ4MXNFVFRQ1JucVNibXZGTQpBZ01aQUZ0OGJKVHd3avQzSU9E
  d0p1RDB5SW9sQ1R4QU9xSGZuUDBpR1R2MORXc0Z2QVR6TTh2e1JtZmxreXFTcmV6Yk91L3pwQWdNQkFBRUNnZ0VCOUpRNE1DNNDNcm1ZNUhioFhQMm1NOVRnaDNxOFrMY2k5NEd3ZWNORU92UGoKWdZwb3ZKYzA4RwtNjRjd
  Ep3bwXN3FwSGpnT0RXb1JFR1FHZ2NZNjNvMwpmKzRDTFQ0MwJGRVZsN1Faa10VwpCOWxwBeJpbU12TUVKVEhIR201TGRYRWZUNwtSUZ1CWE15Wn1IWC9aYt1GRyUv2M4ZnhZdeTuSfPnb3NtY1Q0Ckt1d29ZYWRvV3hJTC
  ttMw5aak5CcTdqT0xTQRxc3E10stKzZBCSDAVt1yV2hQOXJKUTBDeKJrZ2hwa0FEaJgKSWk1UFZwbG1JRdG4V1ZuV1hMSktqTW13ak9mbVhML24ra1hwUkd6aJJ3NGFYnW1LZVdISm1XR3NoMmV1dFpHUApPwmNSQjBodHh
  ZVmhGd1pkdWFTUwhnY115TKvNazZ2K0tNeDZZU2t6R3NFQ2dZRUevc2VvU1d0cGJxa1Vud1BXCjFZwJhBRmt1WuX0V1pwWjJUSEnJUXV6c21Udw1xQXNjRE1JWw5Bbi9wa3deTDZmVnBHU00c1JJb2JhRDRZdEUKbVhDwk1n
  U05VN2J1bEhqdUtKdStsMzRrY0d3Swh1U0xPdm9NQVRXemJ4U2p5UTduU050Q09QY3M1by9HUTY5YQpocjh0UVZtMU9GMDN4bmRTVEQYnKhKcVpPeVVDZ11FQX1RSTRVaj1ISTE5RX1HSmNGQZFMcFBmeGJubH11WGROcmlC
  C9wYw9vQ1k5RXFzcHVQY29Gbs9uUE1rag82S1NFSURXcz1HMstaddJnYVYyRVjVZ1NCQ2tIZThkV2FCZzcKY3IzdZFPVmZ5OUPlbjZHODJTWGdxRnA2ZnJ1K0VvZwJtSkJ2bMR2cjVQbkNzMMh1Wxhyd2ZCUM3TC90TU5jLw
  p6ZzZRQnZnc1kvRUNnWUFBbVVPQj1rQ25LK3FLVBSavNCQ2VoNWNVcnh3QzNiT2xwb11Yaw1yoEg1SEFSMVpiCmdWRKJmSn1HL1dLOGgrNXVsb1hQYnBFRk1FS3JFd0swUvPsnmhQdzRDQ1FEWVUXZDk5QTQxdwtMQXBYNm1
  5ncKbG9uVXJ1V2Zdek5mVTVpampqQ1hwZTBMrmFkbm5VL2U5UKFNS1VQTNdCCFRjeEJVY11pd2JJU1RxUUtCZ1FERQpJRGrtQUxuZm1KQXJXT1Z4Rm5Vt1pLTWNZTudRdHhoaw5PVnBkaw9Va2NhMVFrAm9YeHEwQXIybzJV
  QUxwd1h1JckM3ZFmweGNYT1QzVU10dmpZVjFJaytQcV1Tz3M3ec9xsit3NVBna0hiWXRfVudKY0dmb25LZ2tGw1RDOTJYbTMKR1k3aw52ZCs5amVFSit3MUPNN3FzaytzN09ONDJUMDNS3crSUozbmnRS0JnUUMySndwNEZIT
  zhsbmMvs0w5VgpTNTdrR1dtMHFQXSJ1U01av11IRzhHTzR4TmtZRDJrZWixww1mMkJDME94RU1TQThnNXNHU0ZnM1V2OVhrSkN2Cn1RUWN5evhNestVQUNpVT1NRmVxUytTLy8rMzg5Qm1EUUpHSzheUZvNvprNjh5RWwzWi
  9KMzMvZF1YTG5qOGgKQnrc0pOUTRqbU1ONZV1MthOUW9awwhObmc9PQotLS0tLUVORCBQk1WQVRFIEtFWS0tLS0tCg==
kind: Secret
metadata:
  creationTimestamp: "2023-04-28T02:28:40Z"
  name: httpbin-credential
  namespace: istio-system
  resourceVersion: "1723012"
  uid: aef7f880-6139-4d89-bd3e-7cb20a3c5c60
type: kubernetes.io/tls
zhlsunshine@zhlsunshine:~/Downloads/istio-1.18.0-alpha.0$
```

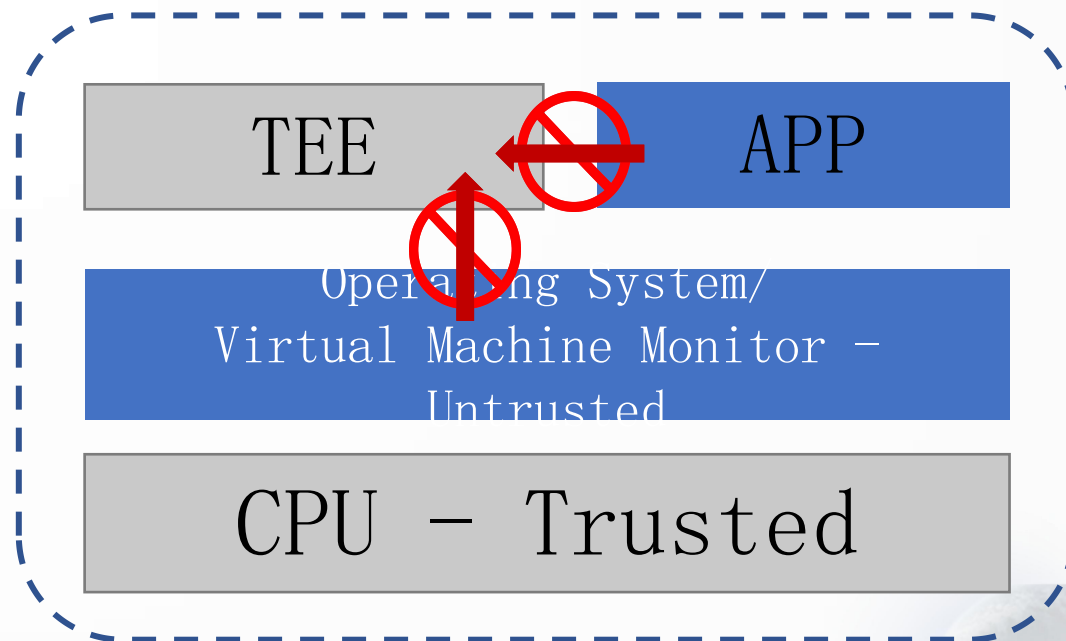
提取此 secret 中 `tls.key` 字段域进行 `base64` 解码即可获得对应的工作负载的私钥。并且通过 `openssl rsa -in private_file_name -text -noout` 即可看到私钥中的明文信息。



可信执行环境：Trusted Execution Environments (TEEs)

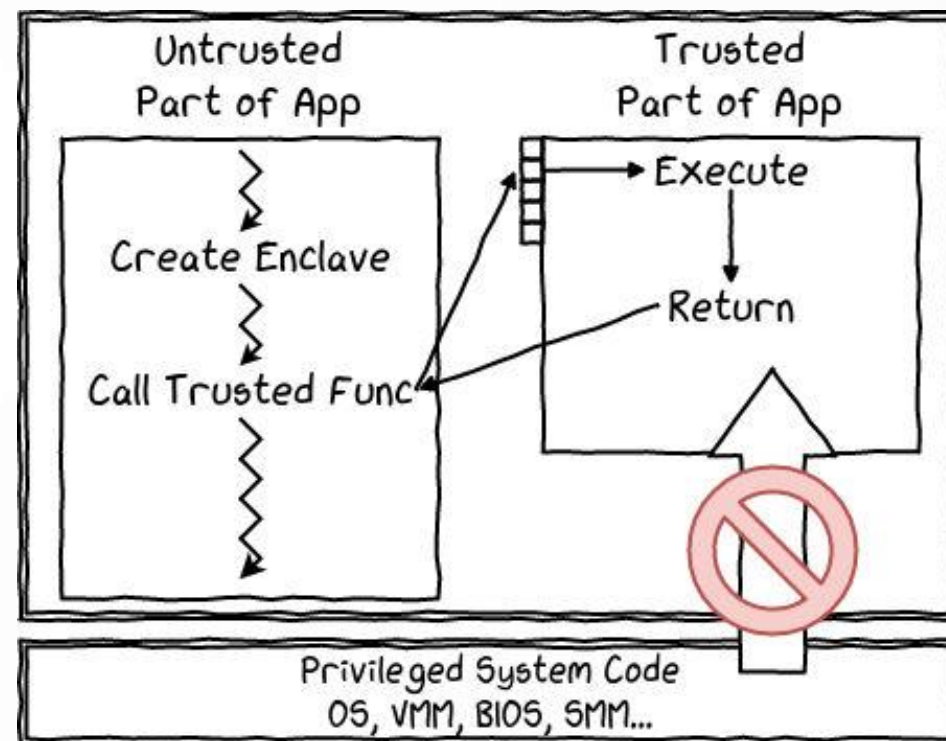
根据 TEEs 的理念，工作负载私钥的保护方案应做到：

- 基于硬件对代码和数据的机密性和完整性的支持
- 即使对 OS, Hypervisor 等特权进程也不能信任
- 信任说明 - quotes and attestation



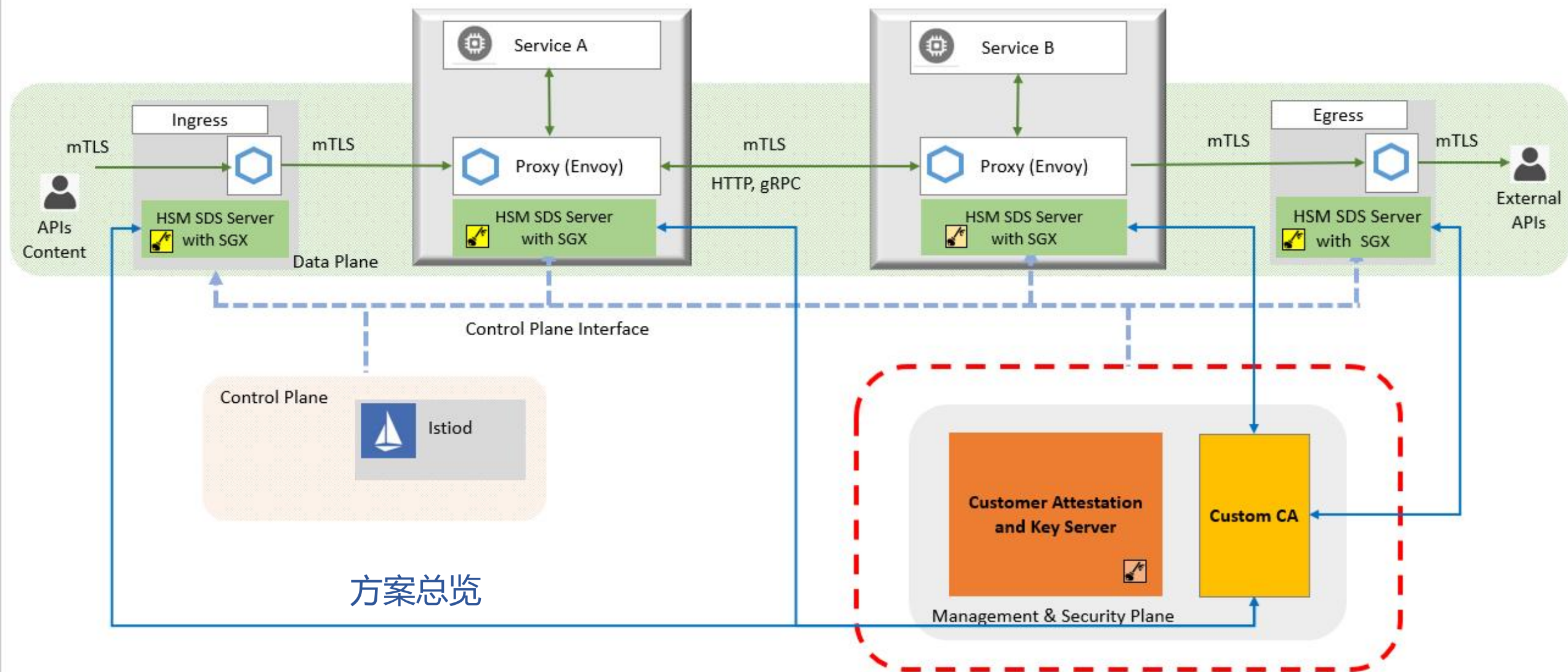


Intel SGX 就是一种**基于进程的可信执行环境**

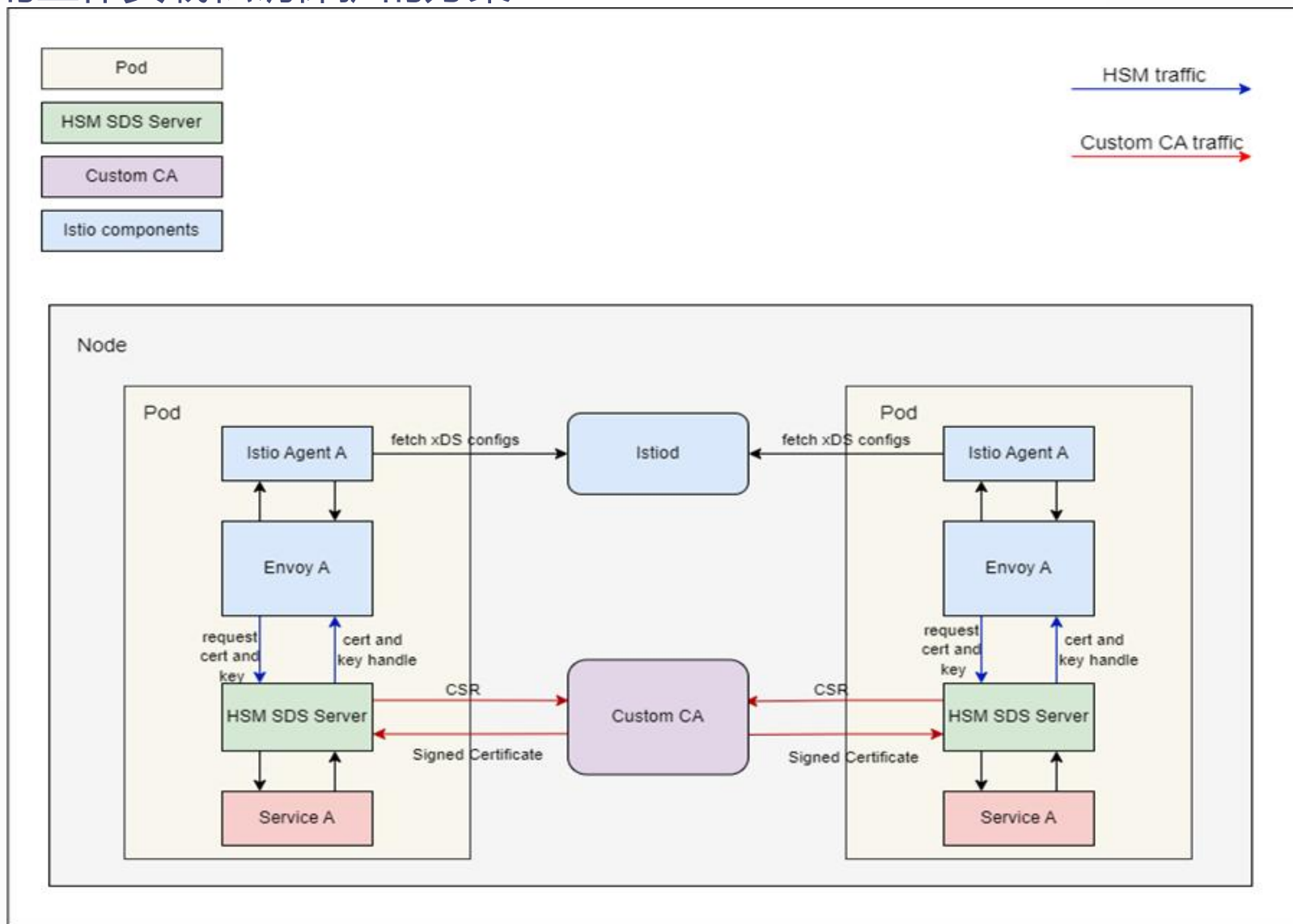


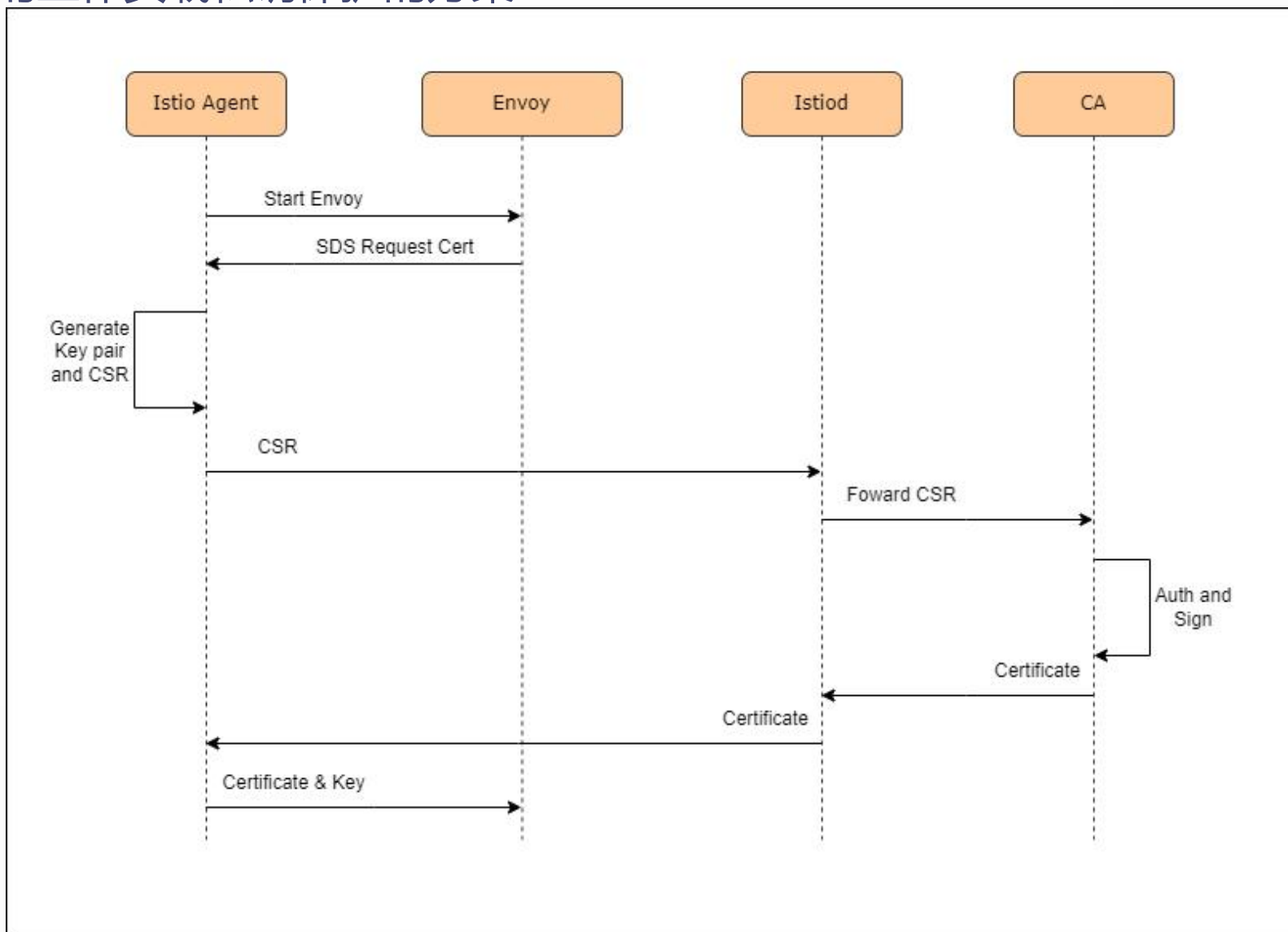
- ☐ 内存加密
- ☐ 访问控制
- ☐ 远程验证
- ☐ 信息密封

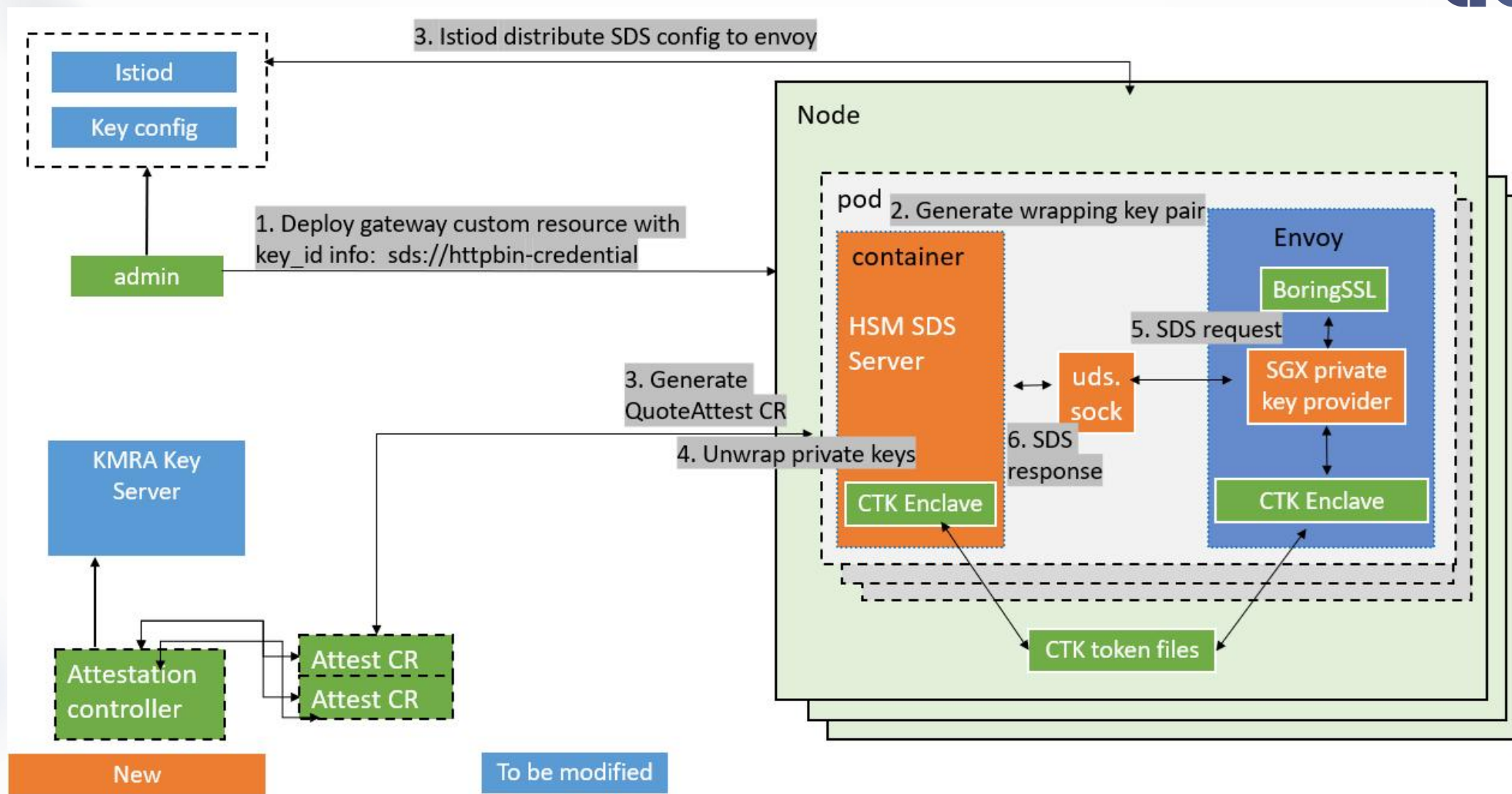
<https://www.intel.com/content/www/us/en/support/articles/000058764/software/intel-security-products.html>



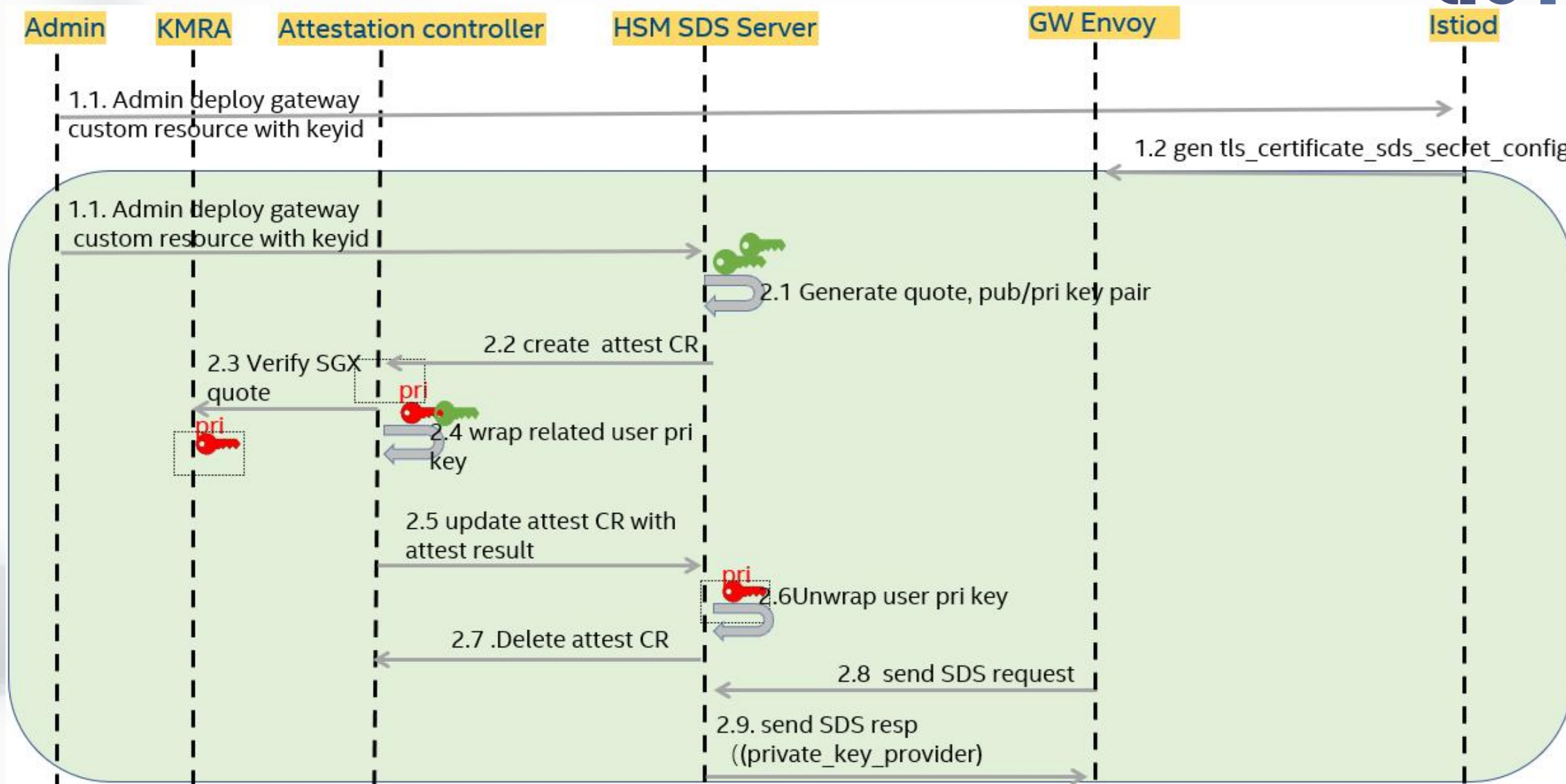
基于 Intel SGX 的工作负载私钥保护的方案







基于 Intel SGX 的工作负载私钥保护的方案




```
root@sgx02:~/huangxin/hsm-sds-server/deployment/istio-configs/gateway-demo#
```

- 希望支持 K8S Gateway API
 - 目前支持 Istio CRD的gateway
- 希望支持通过 ProxyConfig 去动态获取正确的 signer 信息
- 希望支持用户自定义的 CA 和 Attestation 服务
 - 目前 CA 服务支持 cert-manager 和 Intel TCS
 - 目前 Attestation 服务支持 Intel Attestation Service
- 希望支持用户自研的服务网格控制面 + Envoy 数据面
 - 目前支持 Istio 控制面 + Envoy 数据面的服务网格

相关资源:

- <https://github.com/intel/istio>
- <https://github.com/intel/envoy/>
- <https://github.com/istio-ecosystem/hsm-sds-server>
- <https://github.com/intel/trusted-certificate-issuer>
- <https://www.intel.com/content/www/us/en/developer/topic-technology/open/key-management-reference-application/overview.html>
- <https://github.com/intel/trusted-attestation-controller>
- <https://istio.io/latest/docs/tasks/security/cert-management/custom-ca-k8s/>

谢谢大家

Q&A