教育网域名安全证书服务方案

（Digicert 证书）

赛尔网络有限公司

工程研究中心

2019 年 5 月

目 录

一、 SSL 证书概述

SSL 证书是遵守 TLS/SSL 协议的一种数字证书，用于在 Web 服务器与浏览器以及客户端之间建立加密链接的加密技术，通过配置和应用 SSL 证书来启用 HTTPS 协议，来保证互联网数据传输的安全，实现网站 HTTPS 化，使网站可信，防劫持、防篡改、防监听。

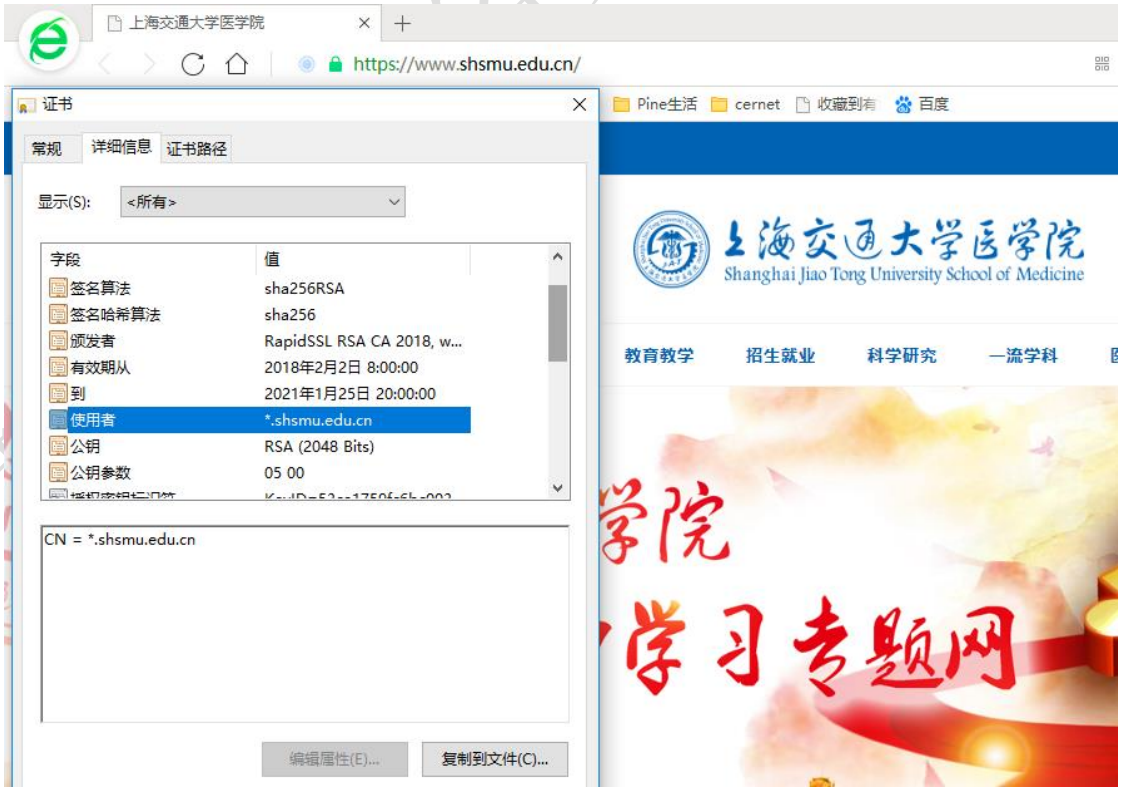
SSL 证书是网络安全的标准，由全球信任的证书颁发机构(CA)验证服务器身份后颁发。将 SSL 证书安装在网站服务器上，可实现网站身份验证和数据加密传输功能。

我们与国际顶级权威 CA 机构合作提供教育网 SSL 证书服务，证书类型丰富，操作流程简单方便，为高校用户提供一站式 HTTPS 安全解决方案。提供 Symantec、GeoTrust、Digicert 多品牌证书的申购、管理、部署等功能，轻松实现网站与 Web 应用的 HTTPS 加密部署。

二、 SSL 证书服务类型

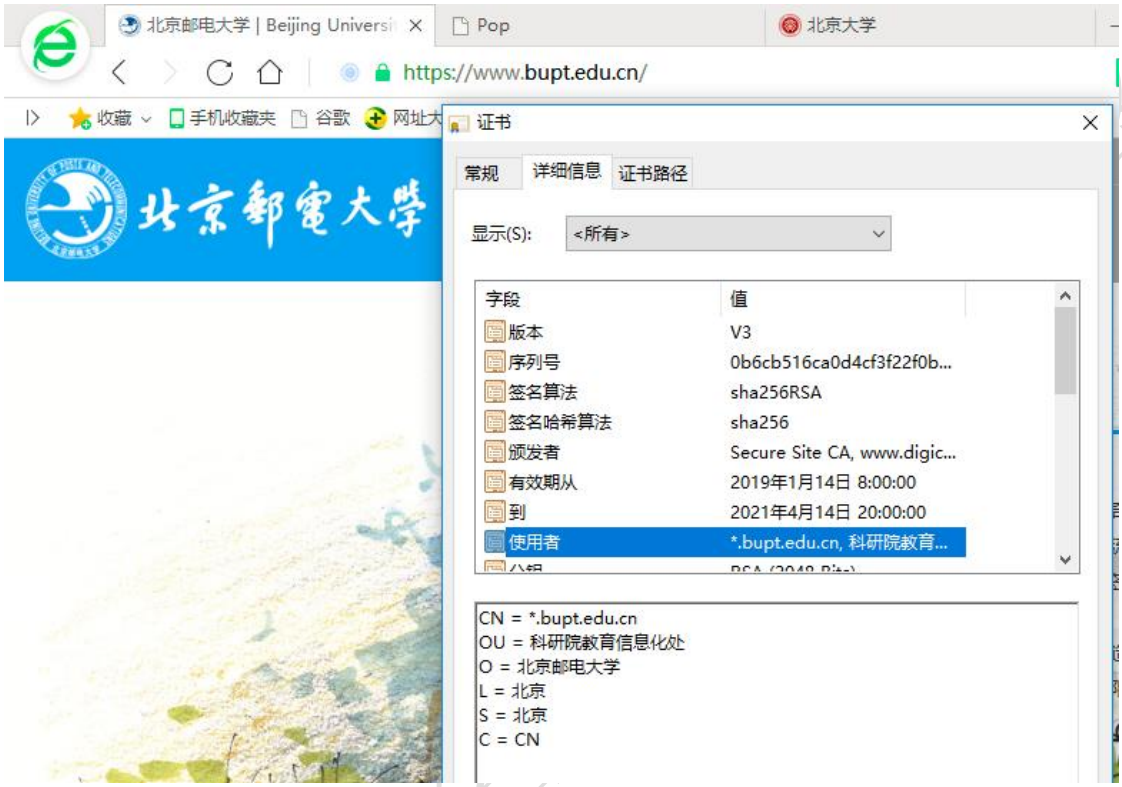
（一）DV 域名验证型

DV SSL 是 Domain Validation SSL Certificate 的缩写，指只验证网站域名所有权的简易型 SSL 证书，证书用于验证一个或多个域名的所有权， DV SSL 证书仅能起到网站机密信息加密的作用，无法向用户证明网站的真实身份。DV SSL 证书不在证书中显示申请单位名称，只显示网站域名。证书签发速度快、价格便宜。DV SSL 证书效果如下图：



（二）OV 机构验证型

OV SSL 是 Organization Validation SSL 的缩写，指需要验证网站所有单位的真实身份的标准型 SSL 证书，通过证书颁发机构审查网站企业身份和域名所有权以证明申请单位是一个合法存在的真实实体，证书用于验证此域名由特定组织所拥有。此类证书不仅能起到网站机密信息加密的作用，而且能向用户证明网站的真实身份。OV SSL 证书效果如下图：



（三）EV 增强验证型

EV SSL 是 Extended Validation SSL 的缩写，指遵循全球统一的严格身份验证标准颁发的 SSL 证书，是目前业界最高安全级别的 SSL 证书。用户访问部署了 EV SSL 证书的网站，不仅浏览器地址栏会显示安全锁标志，而且浏览器地址栏会变成绿色，明确显示网站所属组织机构的名称，从而使访问者更加确信以及更加放心的相信他们所进行交易的网站是真实合法的。EV SSL 证书效果如下图：

三、 SSL 证书保护范围

（一）Single-Domain 单域名

单域名证书仅支持一个完整域名（FQDN），例如 www.alipay.com 或 mail.hust.edu.cn。EV/OV/DV 证书均支持单域名证书。

（二）Multi-Domain 多域名

Multi-Domain 有别于其它证书的是它支持多个主域名，例如 alipay.com 和 tmall.com 同属于一家集团公司，CA 机构只需认证阿里巴巴集团及旗下子公司真实信息即可颁发一张证书，同时能在多个域名的 WEB 应用上部署，Multi-Domain 有效的解决了集团式业务 SSL 加密困扰，大大的提高品牌可信度及用户识别度。又如 pku.edu.cn 和 gotopku.cn 分别是北京大学主网站和北大招生网，因同属于北京大学，所以只需购买多域名证书，就可以解决多个主域名的证书服务需求。具体包括 OV 多域名和 EV 多域名。

（三）Wildcard 通配符（泛域名）

通配符 SSL 证书是 Wildcard SSL Certificate 的缩写，可以保护一个域名以及该域名所有的二级子域名，不限制子域名数量，且添加新的子域名无须重新审核和另外付费。例如，一个单独的通配符证书就可以保护 www.example.com、blog.example.com 和 store.example.com。通配符证书可以保护通用域名和您在提交申请时的所有二级子域名。只需

在通用域名左侧的子域区域添加星号 (*) 即可。具体包括 DV 通配符和 OV 通配符。

四、 教育网域名安全证书服务分类

（一）Secure Site 数字证书（原 Symantec）

1、 功能特性：

1) 每日恶意软件扫描

防护不局限于证书，每个 Secure Site SSL/TLS 证书都可帮助您保护整个网站安全，抵御恶意感染，整个过程全自动进行；

2) Norton 安全认证签章

网站信任从搜索结果页面开始，在搜索结果列表旁边显示全球公认的安全签章，以此证明您的网站经过了认证，让用户放心点击；

3) 浏览器兼容性

一旦看到“安全警示”信息，客户几乎都会放弃请求。我们在现代浏览器中植入根证书，实现 99.75%浏览器的兼容性。

2、 证书类型：

1) Secure Site 单域名 OV

- 保护单个域名，可添加多个 SAN
- 支持 RSA 或 ECC 加密算法
- 最知名的信任标记
- 数据保护 256 /384 位加密
- 1,750,000 美元的 NetSure® 扩充保固
- 网站恶意软件扫描
- 7x24 免费全球客户支持
- 优先级认证支持及技术支持

2) Secure Site 多域名 OV

- 保护 4 个单域名，可扩展更多 SAN，另外增加域名销售优惠价格
- 支持 RSA 或 ECC 加密算法
- 数据保护 256 /384 位加密
- 最知名的信任标记
- 1,750,000 美元的 NetSure® 扩充保固
- 网站恶意软件扫描

- 7x24 免费全球客户支持
- 优先级认证支持及 VIP 技术支持

3) Secure Site 通配符 OV

- 保护多个子域名
- 支持 RSA 或 ECC 加密算法
- 数据保护 256 /384 位加密
- 最知名的信任标记
- 1,750,000 美元的 NetSure® 扩充保固
- 网站恶意软件扫描
- 7x24 免费全球客户支持
- 优先级认证支持及 VIP 技术支持

4) Secure Site 单域名 EV

- 浏览器绿色地址栏
- 对每个子域进行完全身份验证
- 支持 RSA 或 ECC 加密算法
- 数据保护 256 /384 位加密
- 最知名的信任标记
- 1,750,000 美元的 NetSure® 扩充保固
- 网站恶意软件扫描
- 7x24 免费全球客户支持
- 优先级认证支持及 VIP 技术支持

5) Secure Site 多域名 EV

- 浏览器绿色地址栏
- 保护 3 个单域名，另外增加域名销售优惠价格
- 支持 RSA 或 ECC 加密算法
- 数据保护 256 /384 位加密
- 最知名的信任标记
- 1,750,000 美元的 NetSure® 扩充保固
- 网站恶意软件扫描
- 7x24 免费全球客户支持
- 优先级认证支持及 VIP 技术支持

3、 证书区别：

证书特性	单域名 OV	多域名 OV	通配符 OV	单域名 EV	多域名 EV
安全域数	1	4	单个域的所有子域	1	3
诺顿签章	√	√	√	√	√
保护无限子域名			√		
绿色地址栏				√	√
是否显示组织机构				√	√
ECC 公钥加密	√	√	√	√	√
快速检测恶意软件	√	√	√	√	√
24/7 聊天/电子邮件/ 知识库支持	√	√	√	√	√
优先审核和技术支持	√	√	√	√	√
RSA 公钥 SHA-2 算法	√	√	√	√	√
兼容所有主流浏览器和移动设备	√	√	√	√	√

（二）Digicert 数字证书

1、 功能特性

1) 标准 x.509 数字证书
2) 256 位加密

3) RSA 公钥 SHA-2 算法（支持哈希：256，384，512）

4) ECC 公钥密码（支持哈希：256，384）

5) 支持 2048/3072/4096 公钥加密

6) 99.5%客户端兼容性

7) 7/24 全球技术支持

2、 证书类型

1）DigiCert 单域名 OV

- 为一个域提供加密和身份验证
- 当您购买 www.example.com 时，example.com 也是免费保障的
- 无许可费用 - 在多台服务器上安装证书，无需额外费用
- 满足信用卡交易安全的 PCI 要求
- 附带自动真实性检查
- 1,000,000 美元的 NetSure 扩充保固

2）DigiCert 多域名 OV

- 基本价格包括 4 个完全合格的域名（FQDN），另外增加域名销售优惠价格
- 允许您在一个证书上保护多达 250 个网站（FQDN）
- 无许可费用 - 在多台服务器上安装证书，无需额外费用
- 满足信用卡交易安全的 PCI 要求
- 附带自动真实性检查
- 1,000,000 美元的 NetSure 扩充保固

3）DigiCert 通配符 OV

- 基本价格包括 1 个通配符域（* .example.com）及其所有第一级子域
- 基本域也是免费保护的（例如，* .yourdomain.com 保护 yourdomain.com）
- 添加 SAN 以在一个证书上保护多个通配符域（例如，* .example.com，* .secondexample.com 和* .thirdexample.com）
- 允许您在一个证书上保护多达 250 个通配符域
- 无许可费用 - 在多台服务器上安装证书，无需额外费用
- 满足信用卡交易安全的 PCI 要求
- 附带自动真实性检查
- 1,000,000 美元的 NetSure 扩充保固

4）DigiCert 单域名 EV

- 为您的客户提供证明，他们可以在共享敏感信息（例如信用卡号和个人信息）时自信地与您的网站进行互动

- 将访问者转换为销售额，增加收入
- 为一个域提供加密和身份验证
- 当您购买 www.example.com 时，example.com 也是免费保障的
- 无许可费用 - 在多台服务器上安装证书，无需额外费用
- 满足信用卡交易安全的 PCI 要求
- 附带自动真实性检查
- 1,000,000 美元的 NetSure 扩充保固

5）DigiCert 多域名 EV

- 使用一个证书保护多个站点（完全限定的域名）
- 为您提供 SANs 证书的灵活性以及扩展验证带来的额外安全性和用户信心
- 基本价格包括 3 个完全合格的域名（FQDN），另外增加域名销售优惠价格
- 允许您在一个证书上保护多达 250 个网站（FQDN）
- 为您的客户提供证明，他们可以在共享敏感信息（例如信用卡号和个人信息）时自信地与您的网站进行互动
- 无许可费用 - 在多台服务器上安装证书，无需额外费用
- 满足信用卡交易安全的 PCI 要求
- 附带自动真实性检查
- 1,000,000 美元的 NetSure 扩充保固

3、 证书区别

证书特性	单域名 OV	多域名 OV	通配符 OV	单域名 EV	多域名 EV
安全域数	1	4	单个域的所有子域	1	3
保护 www.example.com 和 example.com	√		√	√	
7/24 支持	√	√	√	√	√
兼容所有主流浏览器和移动设备	√	√	√	√	√
保护无限的子域名			√		

显示 EV 绿色地址栏				√	√
是否显示组织机构				√	√

（三）GeoTrust 数字证书

1、功能特性

1）安全性：域控制验证，最高 256 位加密，2048 位根

2）可选购单域名证书或者通配符证书

3）便利性：大多数证书在几分钟内发布，1 - 2 年有效期选项

4）经济高效：无限制的服务器许可证，无限制的免费重发证书有效期

5）普遍性：支持超过 99%的浏览器和大多数移动设备浏览器

2、证书类型

1）GeoTrust DV 证书

- 允许您使用一个证书保护多个域(example.com)和通配符域(*.example.com)
- 在“域名名称”字段中包含一个单域或一个通配符域名
- 添加 SANs 以保护一个证书上的多个域和通配符域(证书订单添加 SANs 可能会产生额外的成本)
- 无限服务器许可证意味着您可以在多个服务器上安装证书而不需要额外的费用
- 受主流浏览器和操作系统的信任
- 使用 RSA 2048+加密或 ECC 256+密钥和 SHA2-256 签名算法保护您的网站
- 满足并符合 TLS 证书的 PCI 要求

2）GeoTrust OV 证书

- 证书让您的客户知道您的站点是值得信任的，并且您足够重视他们的安全性，从而从一个全球可信的证书颁发机构获得您的证书
- 证书信息包含组织名称及信息
- 保护 www.example.com 和 example.com
- 可用的 RSA 和 ECC 算法
- 行业领先的保证-True BusinessID 为您的企业提供 125 万美元的 Netsure 保障
- 可在您的证书中添加多达 250 个主题替代名称(SANs)
- 通配符和 FQDN SANs——只需添加多达 250 个域名，并在您申请 true businessID 证书时指定需要的主题替代名称字段的数量

3）GeoTrust EV 证书

- EV 证书是 GeoTrust 的高级商务级 SSL 安全产品，可以直观地确认 SSL 证书中可用的最高级别的认证
- EV SSL 证书是最高的信任标准
- 保护 www.example.com 和 example.com
- 可用的 RSA 和 ECC 算法
- 技术支持-True Business ID EV 提供优先的技术支持
- 行业领先的保证-True BusinessID 为您的企业提供 125 万美元的 Netsure 保障
- 可在您的证书中添加多达 250 个主题替代名称(SANs)
- 通配符和 FQDN SANs——只需添加多达 250 个域名，并在您申请 true businessID 证书时指定需要的主题替代名称字段的数量

五、 教育网域名安全证书服务内容

1、 提供证书 CSR 文件制作、域名归属权验证和证书安装部署各环节的详细说明文档。

2、 提供 7×24 小时电话技术支持服务，全面解答证书相关问题，指导并配合用户完成数字证书的安装工作，有需要时可提供上门现场技术支持服务，及时为用户解决问题。

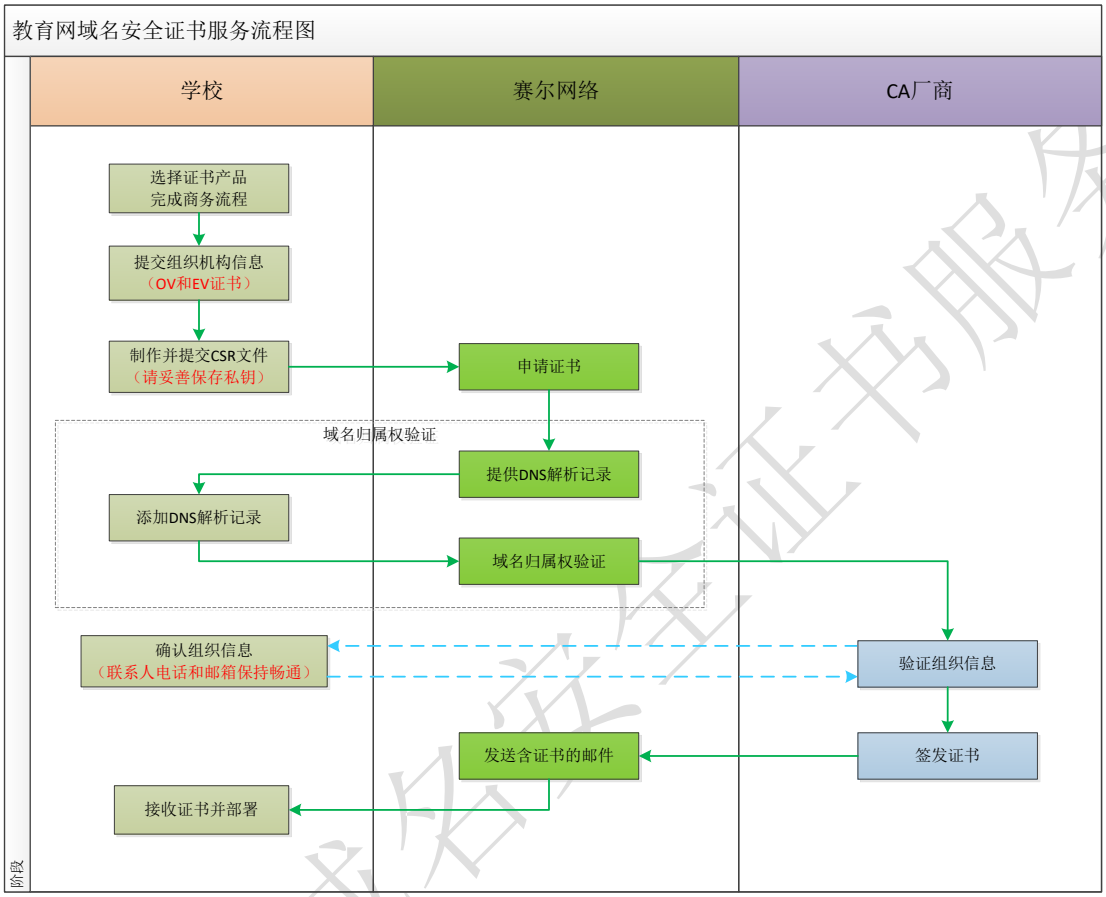
3、 通过电话、邮件、QQ 等工具定期进行回访，了解用户使用情况，及时进行应用培训。

4、 提供完善的证书全生命周期管理服务，及时提醒用户完成更新和续签等工作。

5、 提供完备的售后技术支持服务，为用户网站的安全运营提供有力的保障。

六、 证书申请和网站 HTTPS 升级的基本流程

（一）证书申请流程说明



教育网域名安全证书申请流程图

第一步 选择证书类型，完成商务流程

1、学校选择证书类型，并与赛尔网络有限公司（下称赛尔网络）完成相关商务流程；

2、如申请 OV 或 EV 证书，学校需向赛尔网络提交组织机构信息和联系人信息，内容详见下表一；

组织机构信息	
字段名称	示例
组织机构名称	赛尔网络有限公司
国家	中国
地址	海淀区中关村东路 1 号院清华科技园 8 号楼 B 座赛尔大厦 9 层

省份	北京市
城市	北京市
邮政编码	100084
电话号码	010-62603366
联系人信息	
字段名称	示例
联系人	张三（证书申请人）
联系人职衔	教授
联系邮箱	abc@xyz.com
联系电话	010-62603366

表一

第二步 制作 CSR 文件，提交证书申请

1、学校在申请数字证书之前，需要先在网站 WEB 服务器上制作 CSR 文件（mydomain.csr），然后将 CSR 文件提交给赛尔网络，各种类型 WEB 服务器上生成 CSR 文件的制作说明请参考教育网域名安全证书服务网站的技术服务栏目；

2、赛尔网络向 CA 厂商提交证书申请；

第三步 证书签发验证

1. 进行域名归属权验证（申请 DV 证书只需该环节验证）。验证方法包含：DNS 验证、文件验证、Email 验证三种，推荐使用 DNS 验证方式，验证步骤如下：
   a) 赛尔网络向学校提供 DNS 解析记录字符串；
   b) 学校添加对应的 DNS 解析记录；
   c) 赛尔网络向 CA 厂商提交域名归属权验证。
2. 组织机构验证（申请 OV 或 EV 证书）。

1、CA 厂商与证书申请人电话沟通，确认组织机构信息和证书申请信息；

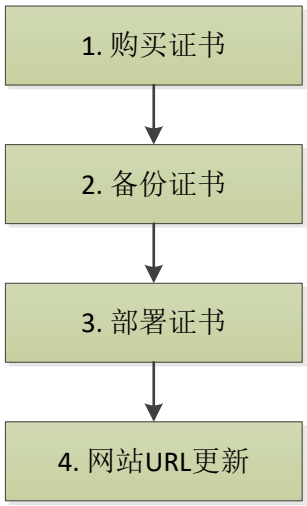
2、CA 厂商还会给组织机构官方联系人邮箱发送确认邮件，要求该联系人回复确认证书申请相关信息。

第四步 证书签发与部署

1、CA 厂商验证域名归属权和组织机构信息通过后签发证书，赛尔网络将证书以邮件方式发送给学校；

2、学校接收邮件下载证书并部署证书。

（二）HTTPS 升级流程说明



Https 升级流程图

第一步 购买证书

1、学校选择适合的证书类型，并与赛尔网络完成相关商务流程；

2、学校制作 CSR 文件，交由赛尔网络向 CA 厂商提交证书申请；

3、CA 厂商验证域名归属权和组织机构后，签发证书；

4、赛尔网络将证书以邮件方式发送给学校；

5、学校接收邮件下载证书。

第二步 备份证书

学校备份证书文件和私钥文件并妥善保管。

第三步 部署证书

学校将证书部署到网站的 Web 服务器或代理服务器上，详细的安装部署文档请参考“教育网域名安全证书服务”网站（https://ssl.cernet.com）技术服务栏目相关说明。

第四步 网站 URL 更新

很多网站的页面会加载一些外部资源，例如图片文件、js 文件、css 文件等，这些外部资源的引用地址需从 http 升级为 https。因为加密网页内如果有非加密的资源，浏览器是不会加载那些资源的。

对于升级后只提供 https 访问的网站，建议更新网站的页面，使其外部资源的引用地址通过 https 访问；为了让用户在浏览器上输入域名的时候从 http 自动跳转到 https，还修改 Web 服务器的配置文件，使用 301 重定向，将 http 协议的访问导向 https 协议。重定向方法如下：

Nginx 的写法。

```
server {
```

```
    listen 80;
    server_name domain.com www.domain.com;
    return 301 https://domain.com$request_uri;
}
```

Apache 的写法（.htaccess 文件）。

```
RewriteEngine On
RewriteCond %{HTTPS} off
RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI} [R=301,L]
```

有些网站升级 https 后，还需保留 http 访问，也建议更新网站的页面，使其外部资源的引用地址通过 https 访问，以保障 https 访问的正常，但不需使用 301 重定向将 http 协议的访问导向 https 协议。

七、 证书所需支持的系统和平台、运行环境说明

目前主流的 WEB 服务器 Nginx 、Apache 、Tomcat 、Lighttpd、IIS7 以及 F5、Haproxy、邮件服务器等等都支持 SSL 协议，SSL 协议版本的选择建议只支持 TLSv1.2，因为 TLSv1.0、TLSv1.1、SSLv2、 SSLv3 容易受到黑客攻击，对于 Java 程序从 JDK1.7 update 96 以后的版本开始支持 TLSv1.2，OpenSSL 从 1.0.0 以后的版本开始支持 TLSv1.2。

SSL 协议的选择建议使用三种配置。根据网站的受众情况选择正确的配置，如果不需要向后兼容性并且仅为现代浏览器客户端服务（Firefox 27 / Chrome 30 等），则使用现代配置（Modern compatibility）。否则使用中间配置（Intermediate compatibility）。仅当有非常老的浏览器客户端（如 Windows XP IE6）访问时，才使用旧的（Old backward compatibility）向后兼容配置。

旧版本的 OpenSSL 可能无法返回完整的算法列表，最新的 AES-GCM 和一些 ECDHE 在 Ubuntu 或 RHEL（CentOS）附带的大多数 OpenSSL 版本中都不存在，如果 OpenSSL 版本较旧，则会自动丢弃不可用的密码，让 OpenSSL 选择它支持的密码套件，始终使用完整的密码套件。**现代兼容（Modern compatibility）：**

对于不需要向后兼容性的服务，密码套件参数的选择提供更高级别的安全性。此配置与 Windows 7，Edge，Opera 17，Safari 9，Android 5.0 和 Java 8 上的 Firefox 27，Chrome 30，IE 11 兼容。

SSL 协议版本选择：TLSv1.2。

中间兼容（Intermediate compatibility）：

对于不需要与旧版客户端兼容的服务（主要是 WinXP），但仍需要支持各种浏览器客户端，建议使用此配置。它与 Firefox 1，Chrome 1，IE 7，Opera 5 和 Safari 1 兼容。

SSL 协议版本选择：TLSv1.2，TLSv1.1，TLSv1。

旧的向后兼容（Old backward compatibility）：

可以与所有浏览器客户端一起使用，例如 Windows XP / IE6。SSL 协议版本选择：TLSv1.2，TLSv1.1，TLSv1，SSLv3。

八、 技术实现案例

（一）使用 OpenSSL 工具生成 CSR 文件

在用户的 WEB 服务器上，执行如下命令（请提前安装 openssl）：

openssl req -new -nodes -sha256 -newkey rsa:2048 -keyout myprivate.key -out mydomain.csr

-new 指定生成一个新的 CSR

-nodes 指定私钥文件不被加密

-sha256 指定摘要算法

-keyout 生成私钥

-newkey rsa:2048 指定私钥类型和长度

-out 最终生成 CSR 文件 mydomain.csr

需要输入的信息说明如下：

字段	说明	示例
Country Name	ISO 国家代码（两位字符）	CN
State or Province Name	所在省份	Beijing
Locality Name	所在城市	Beijing
Organization Name	公司名称	Cernet, Inc.
Organizational Unit Name	部门名称	IT Dept.
Common Name	申请证书的域名	www.example.com
Email Address	不需要输入	
A challenge password	不需要输入	

完成命令提示的输入后，会在当前目录下生成 myprivate.key（私钥文件）和 mydomain.csr（CSR，证书请求文件）两个文件。

注意事项：

1、CSR 的密钥长度有严格要求，要求是 2048 位，密钥类型必须为 RSA。

2、如果申请证书是多域名或者通配子域名，在“Common Name”字段只需要输入一个域名即可(通配子域名可以输入“*.example.com”)。

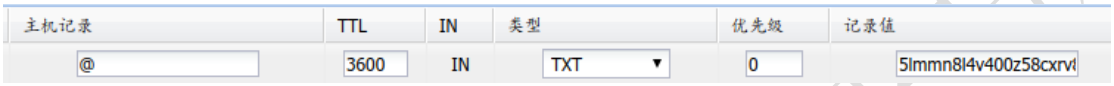
（二）使用 DNS TXT 方式验证域名归属权

1、赛尔网络向 CA 厂商获取域名归属权 DNS TXT 验证随机字符串；

字符串示例：5lmmn8l4v400z58cxrv8xnv8vkcdmdz7

2、赛尔网络将验证字符串提供给用户；

3、用户在域名的解析管理系统里增加 TXT 解析记录，如下图所示；



图一

A、主机记录处填 “@”到输入框内；

B、记录类型为 TXT

C、记录值填写赛尔网络提供的验证字符串

D、优先级不需要填写，默认 0 即可

E、TTL 填写默认值接口，例如 3600 秒（TTL 为缓存时间，数值越小，修改记录生效时间越快）

用户通知赛尔网络已设置完成，赛尔网络向 CA 厂商提交域名归属权验证请求；

CA 厂商验证通过后，签发证书（如用户申请的是 OV 或 EV 证书，还需进行组织机构验证）。

（三）Apache 服务器安装部署证书

1、确认 mod_ssl.so 模块是否安装

首先打开 apache 配置文件，确认是否安装 mod_ssl.so 模块,由于 apache 各个版本的配置略有不同，mod_ssl.so 所在位置也不同。基本在以下两个文件中：

```
/etc/httpd/conf/httpd.conf
/etc/httpd/conf.modules.d/00-ssl.conf
```

分别编辑两个文件：

```
#   vi   /etc/httpd/conf/httpd.conf
```

```
#   vi   /etc/httpd/conf.modules.d/00-ssl.conf
```

查看是否有下边三行，如果有注释 # 的话把 # 删除。

```
LoadModule ssl_module modules/mod_ssl.so
Include conf.modules.d/*.conf
IncludeOptional conf.d/*.conf
```

默认的 apache 安装是不安装 mod_ssl.so 模块的，需要我们通过 yum 方式安装。

```
#    yum install -y   mod_ssl
```

安装完后/etc/httpd/conf.d 目录下会出现一个 ssl.conf 文件（/etc/httpd/conf/httpd.conf 文件中需要 IncludeOptional conf.d/*.conf 或者 Include conf.d/*.conf ，ssl.conf 的配置才生效）。

2、ssl.conf 基本配置

```
# vi   /etc/httpd/conf.d/ssl.conf
```

主要关注以下几行：

```
SSLEngine on
SSLProtocol all -SSLv2 -SSLv3
SSLCipherSuite
HIGH:3DES:!aNULL:!MD5:!SEED:!IDEA:!RC4:!eNULL:!NULL:!DH:!EDH:!EXP
:+MEDIUM
SSLHonorCipherOrder on
SSLCertificateFile /etc/httpd/conf.d/server.crt
SSLCertificateKeyFile /etc/httpd/conf.d/server.key
```

证书的位置为 /etc/httpd/conf.d,也可以放在其他位置，记得修改路径。

3、测试配置是否正确

使用命令 services httpd configtest 或者 apachectl configtest 测试一下配置是否存在错误，没有错误 ok。

```
# apachectl configtest
```

```
[root@localhost conf.d]# apachectl configtest
Syntax OK
```

测试没有问题，重启 httpd 服务器

```
# service httpd force-reload
```

```
[root@localhost ~]# service httpd force-reload
Redirecting to /bin/systemctl force-reload  httpd.service
```

4、301 重定向

在实际使用中，多数访问 http 的访问被重定向到 https,就需要在 http 的配置增加如下红色文字的内容：

```
#   vi /etc/httpd/conf.d/http-vhost.conf
```

```
<VirtualHost *:80>
    ServerAdmin admin@domain.com
    DocumentRoot "/var/www/html"
    ServerName     www.domain.com

    RewriteEngine on
    RewriteCond     %{HTTPS} !=on
    RewriteRule     ^(.*)    https://%{SERVER_NAME}$1 [L,R]

    DirectoryIndex index.htm
    ErrorLog "/var/log/httpd/error_log"
    CustomLog "/var/log/httpd/access_log" combined
    <Directory "/var/www/html">
        Options -Indexes +FollowSymlinks
        AllowOverride All
        Require all granted
    </Directory>
</VirtualHost>
```

保存配置文件后，测试配置是否正确，然后重启 httpd 服务器使配置生效。

（四）Tomcat 服务器安装部署证书

编辑 /usr/local/apache-tomcat-7.0.94/conf/server.xml

（/usr/local/apache-tomcat-7.0.94/为 tomcat 安装目录，请使用实际安装路径替代）

```
# vi /usr/local/apache-tomcat-7.0.94/conf/server.xml
```

定位到下面的内容：

```
<!--
<Connector port="8443"
protocol="org.apache.coyote.http11.Http11Protocol"
maxThreads="150" SSLEnabled="true" scheme="https"
secure="true"
clientAuth="false" sslProtocol="TLS" />
-->
```

取消注释符号 <!-- 和 -->,并修改为如下内容：

```
<Connector port="443"
protocol="org.apache.coyote.http11.Http11NioProtocol"
maxThreads="150"
SSLEnabled="true"
scheme="https"
secure="true"
keystoreFile="/usr/local/apache-tomcat-7.0.94/keystore.jks"
keystorePass="password"
clientAuth="false"
sslProtocol="TLSv1.2"
ciphers="TLS_RSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
SSL_RSA_WITH_3DES_EDE_CBC_SHA,
```

```
                TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA"
        />
```

定位到下面的内容：

```
        <!-- Define an AJP 1.3 Connector on port 8009 -->
        <Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
```

修改为如下内容：

```
        <!-- Define an AJP 1.3 Connector on port 8009 -->
        <Connector port="8009" protocol="AJP/1.3" redirectPort="443" />
```

说明：

keystoreFile="/usr/local/apache-tomcat-7.0.94/keystore.jks" 是证书文件放置的具体位置

keystorePass="password" 是证书读取需要的密码

配置保存后，需要重新启动 tomcat 服务。

关闭 Tomcat 服务：

```
        # /usr/local/apache-tomcat-7.0.94/bin/shutdown.sh
```

或者

```
        # kill -9 PID
```

(PID 为 tomcat 的进程 ID 号可以用命令： ps -ef |grep java |grep -v grep 获得)

启动 Tomcat 服务：

```
        # /usr/local/apache-tomcat-7.0.94/bin/startup.sh
```

查看 Tomcat 日志有无错误提示：

```
        # tail -f /usr/local/apache-tomcat-7.0.94/logs/cataina.out
```

Tomcat 服务正常启动后可以通过浏览器访问 https://www.domain.com 看到正常显示的页面。

九、 教育网域名安全证书服务选型指南

单个网站，建议购买一张单域名 EV 证书。

门户、招生、宣传网站，建议打包购买一张多域名 EV 证书。

保护学院全部二级域名，建议购买一张通配符 OV 证书。

最佳组合： 一张多域名 EV 证书 + 一张通配符 OV 证书。

十、 销售服务渠道和联系人

服务网站：HTTPS://SSL.CERNET.COM

联系电话：

010-62603952（用户支持） 010-62603854（证书咨询）

工作时间：

法定工作日 8:30-17:30 (紧急联系电话：13552939468)

E-mail：ssl@cernet.com

高校用户可以联系赛尔网络有限公司各省分公司