Internet X.509公用密钥机制
操作协议:FTP和HTTP

本备忘录的状态

本文档讲述了一种Internet community的Internet标准跟踪协议，它需要进一步进行讨论和建议以得到改进。请参考最新版的“Internet正式协议标准” (STD1)来获得本协议的标准化程度和状态。发布本备忘录不受限制。

版权声明

概要

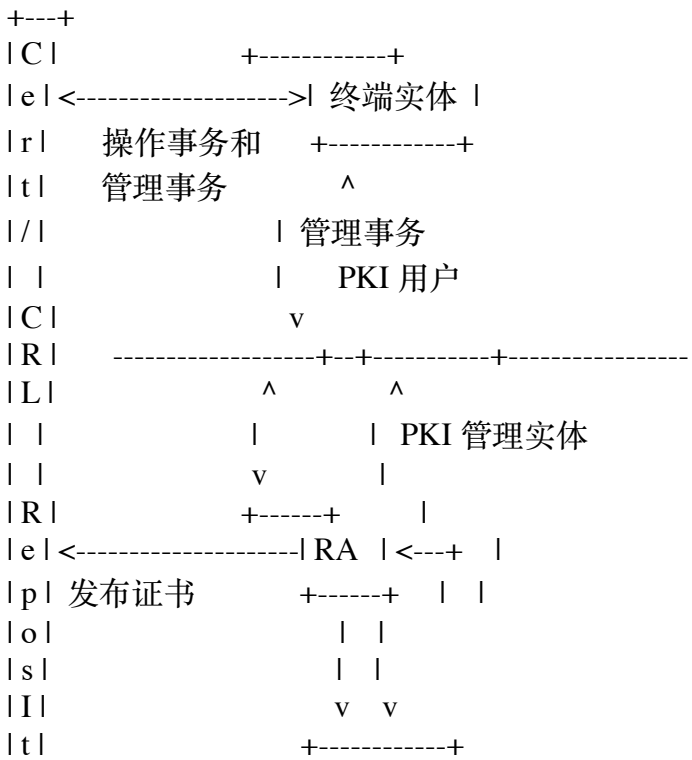
本文档中描述的协议约定满足Internet公用密钥机制(PKI)中的许多可操作的需求。本文档同时讲述了一些使用文件传输协议(FTP)和超文本传输协议(HTTP)来从PKI仓库中获取证书和证书撤消列表(CRLs)的协定。附加的描述访问PKIX仓库机制的可操作的需求在另外的文档中说明。

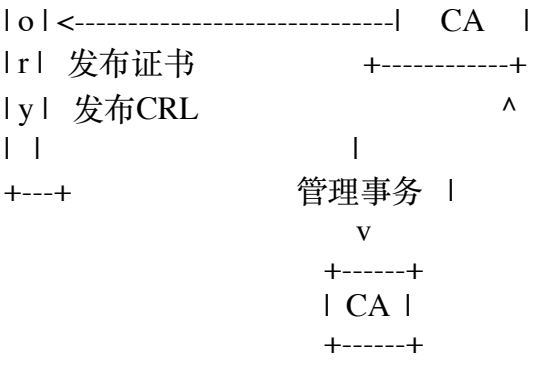
1 介绍

本说明是使用X.509证书和证书撤消列表(CRLs)的Internet公用密钥机制(PKI)多个标准的一部分。本文档同时讲述了一些使用文件传输协议(FTP)和超文本传输协议(HTTP)来从PKI仓库中获取证书和CRLs的协定。附加的描述访问PKI仓库的机制在另外的文档中说明。

1.1 模型

下面是由Internet PKI规范中假定的结构模型的简单视图。





这个模型中的构成是:

终端实体：PKI证书用户及/或者作为证书主题的终端用户系统;

CA：证书授权机构;

RA：登记机构。例如，CA可以把某些管理功能委托给一个操作系统;

仓库：一个保存证书和CRLs的系统或分布系统的集合，并且是一个适合发放证书和CRLs到终端用户的方法。

1.2 证书和CRL仓库

许多CA要求使用在线的校验服务，而其他分布式的CRL允许证书用户自己去实施证书的校验。通常，CA通过把CRL发布到目录中，使得证书用户就可以使用了。目录也是一种正规的证书分配机制。不过，到目前Internet的许多方面还没有提供目录服务。 RFC 959中定义的文件传输协议(FTP)和RFC 2068中定义的超文本传输协议(HTTP)提供了分配证书和CRL的候选方法。

终端实体和CA都可以使用FTP或HTTP协议从仓库中检索证书和CRLs。终端实体可以使用FTP或HTTP来发布自己的证书到仓库中，RA和CA也可以使用FTP或HTTP发布证书和CRLs到仓库中。

2 FTP约定

在证书扩展和CRL扩展中，全名(GeneralName)的URI形式是用来指明证书发行者和可以得到CRLs的位置。例如，一个指定证书标题的URI应该用subjectAltName证书扩展名来传送。一个IA5String描述了如何用匿名FTP方式去获取证书和CRL的信息。例如:

ftp://ftp.netcom.com/sp/spyrus/housley.cer
ftp://ftp.your.org/pki/id48.cer
ftp://ftp.your.org/pki/id48.no42.crl

Internet用户可以在他的商业名片上发布一个指向包含他的证书文件的URI引用。这种方法，在该用户没有目录服务入口时非常有效。FTP已被广泛应用，匿名FTP也已经被许多防火墙所接受，FTP是通过目录存取协议来进行证书和CRL分配的一种有吸引力的可选方法。尽管这种服务能够满足检索已通过URI指定的证书的相关信息的要求，但是它却无法解决在知道一个用户的其他信息，如电子邮件地址或公司的联系地址等情况下，查找该用户证书这样更为一般的问题。

为了方便起见，包含证书的文件应该有一个.cer后缀。每一个“.cer”文件恰好包含了一个以DER格式编码的证书。同样地，包含CRLs的文件应该有一个.crl后缀. 每一个“.crl”文件恰好包含了一个以DER格式编码的CRL。

3 HTTP约定

在证书扩展和CRL扩展中，全名(GeneralName)的URI形式是用来指明证书发行者和可以得到CRLs的位置。例如，一个指定证书标题的URI应该用subjectAltName证书扩展名来传送。一个IA5String描述了如何用匿名HTTP方式去获取证书和CRL的信息。例如:

http://www.netcom.com/sp/spyrus/housley.cer
http://www.your.org/pki/id48.cer
http://www.your.org/pki/id48.no42.crl

Internet用户可以在他的商业名片上发布一个指向包含他的证书文件的URI引用。这种方法，在该用户没有目录服务人口时非常有效。HTTP已被广泛应用，HTTP也已经被许多防火墙所接受。因此，HTTP是通过目录存取协议来进行证书和CRL分配的一种有吸引力的可选方法。 尽管这种服务能够满足检索已通过URI指定的证书的相关信息的要求，但是它却无法解决在知道一个用户的其他信息，如电子邮件地址或公司的联系地址等的情况下，查找该用户证书这样更为一般的问题。

为了方便起见，包含证书的文件应该有一个后缀:.cer。每一个"cer"文件恰好包含了一个以DER格式编码的证书。同样，包含CRL的文件应该有一个后缀:.crl. 每一个"crl"文件恰好包含了一个以DER格式编码的CRL。

4 MIME登记

为支持证书和CRLs的传输，定义了两种MIME类型，它们是:
application/pkix-cert
application/pkix-crl

4.1 申请/pkix-cert

发送到: ietf-types@iana.org
主题: Registration of MIME media type application/pkix-cert
MIME媒介类型名称: 申请
MIME 子类型名称: pkix-cert
需要的参数: 无
可选参数: 版本 (缺省值为 “1”)
编码方面的考虑:不应是8位传输，应是7位传输或SMTP中的Base64码。
安全性方面的考虑:带有加密的证书
互用性方面的考虑:无
发布规范:draft-ietf-pkix-ipki-part1
申请将会使用的媒介类型:所有MIME兼容的传输
附加信息:

变数:无
文件扩展名: .CER
Macintosh文件类型码:无

如果需要更多的信息，请与该E-MAIL联系:

Russ Housley <housley@spyrus.com>

Intended usage: COMMON
Author/Change controller:
Russ Housley <housley@spyrus.com>

4.2 申请/pkix-crl

发送到: ietf-types@iana.org
主题: Registration of MIME media type application/pkix-crl
MIME媒介类型名称: 应用
MIME 子类型名称: pkix-crl
需要的参数: 无
可选参数: 版本 (缺省为 “1”)
编码方面的考虑: 不应是8位传输,应是7位传输或SMTP中的Base64码。
安全性方面的考虑:带有加密的证书撤消列表
互用性方面的考虑:无
发布规范:draft-ietf-pkix-ipki-part1
申请将会使用的媒介类型:所有MIME兼容的传输
附加信息:
变数:无
文件扩展名: .CRL
Macintosh文件类型码:无

如果需要更多的信息，请与以下E-MAIL联系:
Russ Housley <housley@spyrus.com>
Intended usage: COMMON
Author/Change controller:
Russ Housley <housley@spyrus.com>

参考资料

[RFC 959]
Postel，J. and J. Reynolds，“文件传输协议(FTP)”STD 5，RFC 959，1985年10月
[RFC 1738]
Berners-Lee，T.， Masinter，L. and M. McCahill，“通用资源定位(URL)” RFC 1738，1994年12月.
[RFC 2068]
Fielding，R.，Gettys，J.，Mogul，J.，Frystyk，H. and T. Berners-Lee; “超文本传输协议 -- HTTP/1.1”， RFC 2068， 1997年1月.

安全方面的考虑

因为证书和CRL是数字签名的，因此并不需要附加的完整性服务.证书和CRL都不需要秘密地保存，对证书和CRL的匿名访问通常也可接受.因此，并不需要秘密的服务。

在Internet上，HTTP缓存代理很普遍，许多代理并不检查一个对象的最新版本的正确性。如果一个证书或CRL的HTTP请求通过了一个配置不当或忽然中断的代

理，该代理可能会返回一个已超期的响应。

FTP站点和WWW服务器的操作者应该对像的CA和RA这样发布证书和CRLs的终端实体进行认证。但是，不需要对检索证书和CRL进行认证。

作者地址

（略——译者注）

完整的版权声明

（略——译者注）

感谢

（略——译者注）

原文：RFC 2585 《Internet X.509 Public Key Infrastructure Operational Protocols:FTP and HTTP》

译者：张偶 2002年4月