高性能CA认证解决方案

何国锋 方志 陈荤祺
(上海市电子商务安全证书管理中心有限公司 200040)

摘要: CA认证是安全电子商务解决方案的重要组成部分。如何提供高性能的CA认证是整个解决方案的关键环节。本文就目前CA认证中一些普遍存在的性能问题，如黑名单的效率等提出一种高性能的CA认证解决方案。

关键词: CA认证 高性能 黑名单 证书状态在线查询

1 前言

电子商务是基于电子网络进行操作的交易。它可以使商家与客户不需要面对面即可进行交易，既节约成本，又提高了工作效率。随着Internet的不断推广，电子商务在近几年蓬勃发展。但同时，我们也注意到，由于交易双方不是面对面，彼此的身份是通过电子方式提交给对方，这样使身份的假冒成为可能。同时电子信息本身的可复制性、可篡改性，使电子交易很难具有有效的交易凭据，这些问题都给电子商务的健康发展带来了负面影响。因此电子商务要求在交易中建立起一个可信任的网络环境。一个可信任的网络环境包括：

- 信息的保密性
- 身份认证
- 信息的完整性
- 信息的不可抵赖性

目前，为建立这个可信任的电子商务环境，国际上通常采用CA技术。CA中心是一个公正的第三方，它利用公开密钥技术，为参与交易的各方发放数字证书，同时负有管理证书、维护数字证书状态的任务。CA中心的数据库中始终含有用户数字证书的最新状态，为每个交易提供身份认证。随着电子商务的发展，网上交易也会越来越多，由于每个交易都希望得到安全的保障，需要进行证书的确认，CA认证的性能将成为电子商务的瓶颈。如何提供高性能的CA认证，成为电子商务健康发展的重要议题。

本文将针对CA认证的过程进行描述，分析CA认证中主要的瓶颈并提出解决方案。

2 CA认证的流程

一个验证数字证书的过程如图1所示：

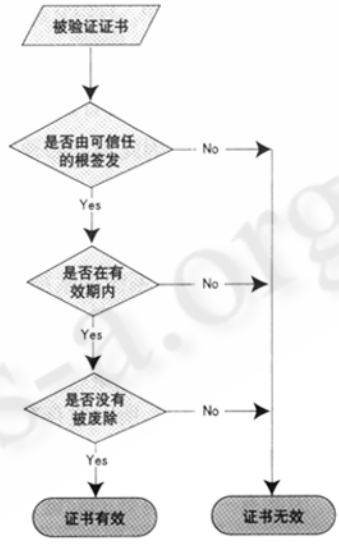

图 1 数字证书验证过程

(1) 验证证书是否由可信赖的CA中心签发；

(2) 检查证书是否在有效期内；

(3) 验证证书是否已被废除。

首先，验证证书是否由可信任的CA中心签发，只需用CA中心的根证书去验证被验证证书中CA的数字签名即可。(具体的验证过程不在这里描述)。可信任的CA中心的根证书一般预置在应用软件中。也可将多个根证书同时预置在一个应用软件中使该软件同时支持多个CA。多级证书的验证则采用证书链的方式进行。如果需要支持交叉认证，则需要特殊的处理方法。(交叉认证的效率问题，

本文不进行详细的描述)。

其次，检查证书是否在有效期中，只需将被验证的证书进行解码，获取证书的有效期，将证书的有效期和本地时间进行比较即可。

最后，验证数字证书是否已被废除。证书废除的原因可能是证书遗失，证书损坏，或证书持有人不再存在或证书持有人不再使用该证书等。数字证书被废除后，就不应继续被信任。

验证证书是否已经废除，目前主要有两种方法。黑名单查询和在线证书状态查询。

黑名单是一个被废除证书的列表（CRL - Certificate Revocation List),它包含了由某根证书签发的所有的在有效期内并且已经被废除了的数字证书的序列号。

黑名单一般每天产生一次(根据不同CA中心的证书操作策略，产生黑名单的时间间隔会有所不同)。黑名单系统将所有被废除证书的序列号组成一个列表文件，并由CA机构对该列表文件进行数字签名，然后通过一定的途径进行发布（如LDAP、FTP、HTTP等)。

黑名单查询是指用户在进行交易时为了确认对方数字证书的有效性，验证对方证书是否被列在黑名单中的过程。由于黑名单定期更新，因此用户必须定期从CA中心获取黑名单，获取的方法由CA中心提供的方法决定。用户在拿到黑名单文件后，首先应该验证黑名单本身的CA签名是否有效，然后，应用系统搜索被验证证书的序列号是否存在于黑名单中，如果存在，说明该证书已经废除，不可信任，反之，证书是有效可信的。

由于黑名单是定时签发的，所以它存在一种缺陷:就是它不能如实地反映待验证书在两次定时签发之间这段时期中的状态。因此有一种更有效的验证方法-在线证书状态查询协议（OCSP-Online Certificate Status Protocol)。

在线证书状态查询是指实时查询证书的状态。它与黑名单一样是为了确认证书是否已经被废除。和黑名单查询相比，在线证书状态查询的优势在于它可以实时的反映证书的当前状态，一般在分钟级。这就避免了使用黑名单查询可能存在的风险。

在线证书状态查询的实现方法主要是在CA中心建立一个动态反映用户数字证书状态的数据库，该数据库采用C/S结构。CA中心建立的服务器等待应用程序发送证书验证请求，在收到验证请求后，从数据库中获得对应证书序列号当前的状态并进行签名，然后返回给客户。既然在线证书状态查询更能反映证书的有效性，为什么还使用黑名单技术呢？黑名单技术由于在两个定时签发期间，黑名单是相同的，只需要下载一次就可以了，有效的避免重复的网络传输。而证书状态在线查询实时反映证书状态，随时可能改变，因此必须有一次认证必须重新传送一次。当然两者的风险是不一样的。因此应用程序需要根据实际的需要进行取舍，一般安全要求比较高，或涉及金额比较大的交易建议使用在线证书状态查询,反之用黑名单查询即可。

验证数字证书是否由可信任的CA签发，是否在有效期内这两项工作都在本地进行，基本上不用考虑性能问题。验证数字证书是否已被废除，需要获得黑名单，或在线进行验证，这都需要考虑网络因素和集中处理，是主要的瓶颈。在此本文主要针对两种验证方式的瓶颈进行分析，并提出解决方案。

3 黑名单验证

黑名单验证过程如下：

(1) 获取黑名单；

(2) 检查黑名单的有效性；

(3) 检查待验数字证书的序列号是否在黑名单中。

其中，后面两步都在本地进行，一般不用考虑性能的问题，主要需考虑获取黑名单这一步的性能。

获取黑名单的方式取决于服务提供商，常见的方式有HTTP、FTP、LDAP或专用程序等等。

传统的做法是某个CA中心将所有废除证书的序列号都列入黑名单内。我们假设一个CA中心的证书数为1,000,000，根据统计，一般废除概率为1%，假设每个证书的序列号位数为20字节。则这个CA的黑名单文件大小大约为1,000,000* 1% * 20 ~= 200K。(此处忽略编码长度)

具此推算，每个黑名单文件将达到200K左右！！！。而且，随着用户的增加和时间的推移，这个文件必将会越来越大。用户在进行交易时，为了确认对方的数字证书是否作废，必须获得该黑名单文件。根据用户的性质不同可以采取不同的方法下载黑名单。如果是服务器程序，一般可采用预先下载的方式,假设黑名单产生的周期是一天一次，则保证每天下载一次即可。对于普通的消费者来说，就必须在用到时进行下载，就目前的网络环境而言，下载一个大小为200K的黑名单文件是需要一段时间的，而实际用到的数据仅占其中很小一部分。那么，如何才能快速地将有效的数据传送给用户呢?

SHECA（上海CA中心）经过多次研究，提出黑名单分段方法。这种方法极大地提高了黑名单查询的效率，既保证黑名单的有效性，又使之适合于网络传送。具体做法如下：

SHECA根据用户的分布特性，采用一定的编组方法将相对一致的用户编成一组，每组都有一个唯一的黑名单文件号与之对应。如果该组中的某个用户证书被废除，它的证书序列号就会出现在该组对应的黑名单文件中，这样就可以通过预先控制组中用户的多少来控制最终黑名单文件的大小。根据统计规律，我们将每个黑名单文件控制在4K以内（相当于1/4个网页大小）。经过这样处理的黑名单就适合于网络实时传送了。

那么对于校验者来说，如何知道某个数字证书对应的黑名单文件号呢？我们在数字证书中利用了一个扩展项：CRL分布点，将分布点进行有效的扩展，来获得该证书对应的黑名单文件号。

比如，一个证书的内容如下：

版本：1

发行者：SHECA

主题：Test

公钥：.....

.....

扩展项：

密钥用途：

CRL分布点：ldap://crl.sheca.com/0001.crl

.....

这就说明该数字证书所在编组所对应的黑名单文件号为0001，如果该证书废除了，则其序列号必然将被列在0001.crl这个黑名单文件中。任何用户在收到Test的证书时，都可以下载0001.crl这个不超过4K的文件来查询该证书是否已被废除。

同时，由于黑名单文件是定期发布的，在前后两次黑名单发布期间，所获取的具有相同文件号的黑名单的内容必然与前次相同，因此可以建立本地黑名单库，进行缓冲，不需要重复下载相同的黑名单文件。SHECA在进行黑名单编组时考虑了用户的相对集中性，这样对于一些专业的系统来说，由于用户本身具有一定的集中性，则到该系统就只需要下载与其有关的有限数量的黑名单文件即可，从而有效地提高了系统的效率。

（SHECA提供的证书应用编程接口已经充分考虑这些特性，应用开发商不需要考虑这些细节。）

在用户较多时，仅仅采用黑名单文件号不能解决所有问题。比如服务器的并发性能，SHECA采用分布式的方法，只需要将CRL分布点的前缀ldap://***.sheca.com中的***更改即可。在将来用户大量增加时，SHECA将启用ldap://crl1.sheca.com,;ldap://crl2.sheca.com等服务器。这种方法同时可以应用于跨地域的CA系统，将数字证书用户按地域进行网络区间划分，使用户数据在各网络区间中有效分布，从而提高网络的效率。比如对北京的用户，我们采用ldap://bjcrl.sheca.com,上海的用户采用ldap://crl.sheca.com的前缀。这样就可以尽可能的实现用户黑名单的就近访问。网络示意图见图2。

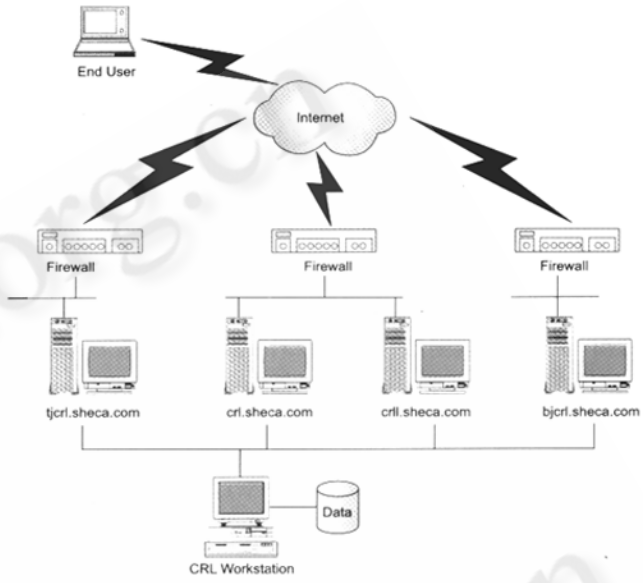

图2 黑名单查询网络示意图

图2中，CRL WorkStation是定期发布黑名单的工作站，将各个黑名单文件分布到各地的CRL服务器中。CRL工作站和各CRL服务器通过内网连接。

4 在线证书状态查询

在线状态查询协议过程如下：

首先，CA中心建立一个该中心签发的所有数字证书状态的数据库，并建立一个OCSP服务器。

当用户在验证一个证书是否已经作废时，他将该证书的序列号发送到OCSP服务器，服务器在接受数据包后，解开序列号，然后到状态数据库中获取该序列号对应的证书状态，成功获取后，将状态数据进行数字签名，发送给用户，用户在验证服务器签名有效后，根据得到的状态判断证书是否可信。

从整个流程看，存在的瓶颈如下：

网络的瓶颈：用户在发送验证请求和服务器返回验证应答都是通过网络进行的，网络的畅通性将直接影响验证的速度。

数据库的瓶颈：服务器为获取数字证书对应的状态，需要对数据库进行操作，在大量并发用户时，数据库的选择和设计尤为重要。

为解决数据库瓶颈，主要对数据库产品进行选择，不同的数据库对并发性有不同的表现。SHECA 采用具有高可靠性，支持高并发的 DB2 进行，可以充分保证数据库的性能。

网络设计也非常重要，SHECA 同样采用分布式的处理方法，将用户相对分开，同时根据用户的地域特性，将用户在地域上进行分离，使数据进行合理的分布，很好的避开骨干网的瓶颈。如图 3 所示：

用户如何知道某个数字证书应到哪个服务器上查询呢?我们同样采用了黑名单分布的办法，利用数字证书扩展项分布 OCSP 查询点。示例如下：

版本： 1

发行者：SHECA

主题： Test

公钥： .....

扩展项：

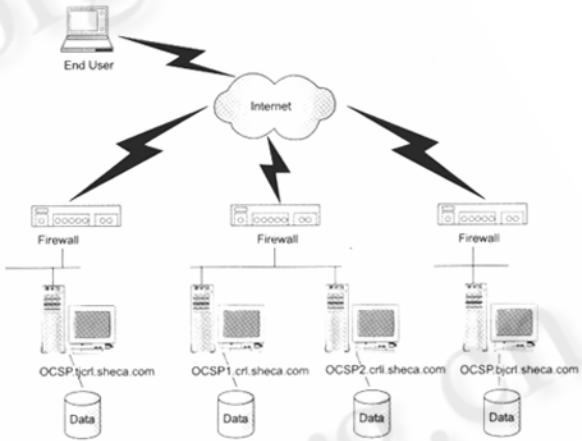

图 3 OCSP 查询网络示意图

密钥用途：

OCSP 分布点： ocsp://ocsp1.sheca.com:8888/

.....

该数字证书说明它的 OCSP 的查询点为 ocsp1.sheca.com:8888，如果用户要验证该数字证书的实时状态，需要用 OCSP 协议实时访问 ocsp1.sheca.com:8888，该服务器会给出该证书的实时状态。■