Lotus Domino 系统构筑安全电子商务网站

杨海涛 (广州 广东省建设工程交易中心 510630)

摘要：本文论述了中小企业自建安全电子商务网站的Lotus Domino群件解决方案，提出了适应不同需求层次的安全性策略，并阐述了具体实施过程的相关问题。

关键词：HTTPS SSL 身份验证 CA 第三方CA 授权加密 X.509证书 PKCS Active X控件 HTML OBJECT标记 KEYGEN标记 安全性 计费

1 前言

随着网上电子商务迅猛发展，网上商务活动的安全性日益引人关注。网上电子商务(这里主要是指电子交易)可划分为三个阶段：前交易阶段，主要是信息的发布和获取此类活动；交易中阶段，主要是进行商品选购、价格洽定、合同签订等交易磋商确认活动；后交易阶段，主要是完成交易有关的款项支付、货物承运、凭证发放及签收等活动。但通常对中小企业来说，其所构筑电子商务网站功能主要是着眼于前二阶段，而“后交易阶段”的功能则通过外部电子协作或传统商务方式实现。

无论那个阶段，网站的经营者都必须提供适当的安全性保障，并承担相应的责任。在电子商务中，网站的经营者所承担的责任与各交易方在交易中的责任是不同的：网站必须提供技术措施，保障交易中的私密信息的私密性、交易信息的完整性及不可否认性，对受限制的信息资源实现访问控制(常用在实施会员制商务活动中)，归纳起来就是提供客户的身份认证及通信保密服务，将责任敏感信息与信息提供者和有权使用者对应起来；而各交易方的责任则是：对所提供的信息承当责任(合法性、准确性、时效性等)，对所进行的操作行为负责。要实现此类保障就必须构筑好企业的Internet通信基础设施(指“消息传递、电子邮件处理系统/平台”)，配备具有基于Internet标准的内置认证及安全保密功能的Web应用服务器，并且要求该服务器平台必须是一个适用于交互式Web商业应用的应用程序开发和实施环境。对于中小型企业来说，选择Internet/Extranet网络应用开发平台还必须充分考虑到开发成本相对低廉、实施速度较快等方面因素(在美国、CA企业级服务器价值可达110，000美元)，而Lotus Domino则是具备这样条件的适用于构筑Extranet和Internet站点的功能强大、可伸缩性强而且经济的服务器系统。此外，Lotus Domino群件系统是跨操作系统平台的，在Windows NT操作系统平台上所作的开发几乎可直接向大型Unix主机系统或IBM大型主机系统迁移，这点对做大企业尤为重要。

2 安全性策略

Web用户的安全性限制取决于Web应用信息的公布范围，谁可参与交互操作及其参与程度如何。此外还应考虑用户使用的易用性及安全管理的可行性，不能因为说明繁复、使用不便、使用环境特殊而赶走客户，或者维护管理容易出纰漏留有隐患。现在大多数Web站点的安全特性是按单一层次进行设计的：对Web用户或者要求电子证书(X.509证书)，或者要求“用户名/口令”；对网站资源对象只能整体设定开放，不能只对其中的部分内容(如某字段)的访问进行控制，或者不能按应用对其进行精确的访问角度控制(如通常只划分对get、post两种操作角色)。利用Lotus Domino系统的虚拟Web主机及重定向设置，可在单一台服务器上建立“电子证书”验证及“用户名/口令”验证(指身份鉴证)并存的Web站点，可按“不能访问”、“投稿者”、“读者”、“作者”、“编辑”等精确划分Web用户的操作角色，以个人、个人组、服务器、服务器组、混合组等为单位进行授权管理。此外对浏览器的每次启动(于新过程中浏览)，一次用户验证在同一会话期间对站点任何资源的访问均有效。网站可按不同类型的用户：资源所有者(公司)的雇员、最佳客户、未来主题、非主顾、会员、合作伙伴和竞争对手等区别对待，并依据对安全性要

求的程度，对受控资源设定身份验证的种类：对安全性要求高的，要求用户提供“电子证书”，对安全性要求不高的，为方便用户使用及系统管理，只要求用户提供“用户名/口令”进行身份认证。建议所有身份验证均通过加密手段进行，本文推荐用SSL安全通道技术。

3 构筑安全电子商务网站

中小企业通常只设一个网站，因此要求企业的所有Internet/Extranet业务统一在同一的门户下。

在通信方面，根据内容的安全性及响应性能要求，对初步的或与站点信任无关的信息链接不使用加密协议(如HTTP)，而对需要加密传输的、与站点信任有关的链接要用SSL加密通道进行(如HTTPS)。为防止用户尝试用HTTP代替HTTPS发出URL请求，在Domino Web服务器的Web配置中，对所有指向安全资源的URL设定从HTTP到HTTPS的URL重定向(不能使用映射，映射只能在同一协议间进行)。

在用户身份验证方面，如要限定对站点某些资源的访问仅仅在提供X.509证书的前提下方可进行，则必须在Domino Web服务器上建立虚拟的“纯安全Web站点”，并对该虚拟Web站点设置成仅要求SSL验证，然后使用HTTPS指向该“纯安全Web站点”资源，将所有实际指向该资源的其他非纯安全Web站点的URL重定向至该“纯安全Web站点”的URL(HTTPS)，并在资源的访问控制列表上对用户群进行授权管理，并可通过对该资源的编程来(在取得证书用户的信息后)细化对用户的请求的处理。下面介绍在Domino上构筑安全站点的步骤。

3.1 构建CA权威机构和配置CA服务器

(1) 建立CA(Certificate Authority)权威管理应用程序(在Domino系统中为数据库对象，以下简称CA管理程序)：生成包含X.509电子证书信息的CA密钥集文件(记载用口令加密后的“RSA公用/私用密钥对”信息，并与CA的说明性信息联系起来)。该根证书由其公用密钥(public key)、公开密钥算法(public-key algorithm)、报文摘要算法标识符和参数、CA实体身份的说明性信息及数字签名(在求得MD5报文摘要后，用CA私用密钥进行)组成。

(2) 将站点的Domino Web服务器配置成CA服务器：用CA管理程序生成CA服务器的密钥集文件(含未验证的服务器证书)，由系统自动产生申请CA服务器证书验证的请求，经过验证(CA数字签名)该服务器证书的步骤，最后在该服务器密钥集文件中存储了(其密钥集所对应的)经CA验证的CA服务器电子证书信息、该CA机构根证书以及系统默认的其他CA机构根证书。在设置站点时通过对密钥集文件的引用来使用服务器证书。

(3) 在对应的Domino Web服务器(由CA说明信息的内容指定)的安全配置中，指定SSL所用的密钥集文件名，启用SSL验证。

经过上述步骤即建立起企业本身的CA服务器。

3.2 配置虚拟Web服务器用作纯安全Web站点

(1) 建立并配置“服务器证书管理”应用程序：为虚拟Web服务器生成服务器密钥集文件(记载用口令加密后的“RSA公用/私用密钥对”信息及证书信息)。

(2) 将虚拟Web服务器设置成信任上面所建立的CA权威：首先在CA应用程序中提取CA根证书，然后在服务器证书管理应用程序中，将所提取的CA根证书合并到虚拟Web服务器密钥集文件中，作为服务器的信任根之一。

(3) 向所建立的CA权威机构提交申请服务器证书验证的请求，在CA审批后，将CA签发的已验证服务器证书添加到Web服务器中。具体做法是：在提交服务器证书申请后，首先在CA管理程序中审批该CA服务器证书的请求(给出有效目期，用CA的私用密钥进行数字签名，每个请求对应一个ID)，然后在CA管理程序中提取Web服务器证书(按ID)，最后在Web“服务器证书管理”应用程序中，将所提取的已验证Web服务器证书保存到虚拟Web服务器的密钥集文件中。

(4) 在虚拟Domino Web服务器的安全配置中，指定SSL所用的密钥集文件名，启用SSL验证。将客户端安全验证设置成仅要求X.509证书验证。

3.3 提供X.509证书服务

(1) 在主页上提供下载“根证书”的链接。为了证实根证书的真实性，可应Web用户要求出具传统书面签章的关于“根证书”的证明(将“主题”—Subject，“指印”—公用密钥—等予以签章)。

(2) 提供通过SSL(在信任“根证书”的前提下)申请客户端证书的HTTPS网页链接。对于IE浏览器，所下载的申请客户端证书的网页提供ActiveX控件的CEnroll OBJECT(Certificate Enrollment Control Object—包含在Xenroll.dll中)对象来产生符合PKCS#6标准(它是X.509证书的超集)的证书(未被CA签发的)，生成并传送该证书的“公用/私用”密钥对、客户实体描述串等信息(用户必须提供准确身份信息，特别是准备用于安全电子邮件

的邮箱名—发送数字签名邮件时其邮箱名必须与证书所载的相匹配)；对Netscape浏览器，所下载的申请客户端证书的网页在HTML form中提供〈KEYGEN〉标记以实现生成符合PKCS标准的客户端证书的功能。

(3) CA管理员在客户提交证书申请后，欲予以批准，则要为该客户在站点Domino目录上创建个人文档(存放证书的公开信息)，并根据要求提供的服务对其授权：在其可访问的资源上增加其相应的操作权限。本文建议，在站点上为所有注册的证书用户建立电子邮箱(用作证书中指定的邮箱地址，供用户接收S/MIME加密邮件)。

(4) CA服务器在CA管理员审批客户端证书后，自动产生含有供申请者提取电子证书的https链接的电子邮件通知。CA管理员亦可通过电话或网站公告栏告知申请者有关证书的ID号(证书审批编号)，以便申请者通过网站网页的“提取电子证书的链接”来提取电子证书。所有提取操作均必须在原申请电子证书的Web客户机(浏览器)上进行。

[说明] 要使在IE浏览器中申请的证书的私用密钥能导出原申请浏览器外使用(Netscape浏览器产生的个人证书通常是可导出的)，CEnroll Object的GenkeyFlags属性必须设置成CRYPT_EXPORTABLE(缺省为0，不可导出)。使个人证书的私用密钥可导出虽然带来了方便，但亦带来了安全的隐患：当用户导出个人证书(包括私用密钥)到其他计算机的4.X以下版本IE浏览器中使用后，其个人证书(包括私用密钥)将在该浏览器中留置下来(因为4.X以下版本的IE浏览器不提供“删除”个人证书的功能)；而在5.0以上版本IE浏览器或Netscape浏览器中则无此问题，因为都提供“删除”个人证书(包括私用密钥)的操作功能。必须注意到，符合PKCS#12(个人信息交换语法)标准的证书文件可用在IE与Netscape浏览器间交换(导出及导入)证书的私用密钥。

3.4 提供基于会话的“用户名/口令”验证服务

目前绝大多数站点均提供有“用户名/口令”验证服务，但大抵只对访问某个资源起作用，如要访问同一站点的其他资源则又要再验证用户的身份，既不方便用户又不能使用户在同一次打开浏览器的会话(又称“过程”)中的先后访问保持关联。通常这种用户先后访问的关联是要通过开发cookie应用程序来实现的，但在Lotus Domino系统里这种前后访问的跟踪已有系统级实现，只需适当配置(启用会话验证)即可。

由于前面已配置Domino Web服务器使用X.509证书，即可通过加密的https通道来传输“用户名/口令”进行验证，以增强安全性。值得注意的是，现在许多站点的“用户名/口令”传送仍然是通过常规http链接进行明文传输，如常见的电讯和Internet服务的资费操作及密码(口令)更改等大都如此。

本文认为在“交易前”的信息发布及查询应在保持一定的安全性的前提下，以方便网站注册客户为主，身份验证通常采用基于会话的“用户名/口令”验证(通过https进行)手段即可。

3.5 有偿服务的计费

商务网站是以商务为目的，同时为平衡交易各方(同是网站的客户)权利与义务，通常都在部分项目上实行有偿服务。这就涉及到如何对部分注册用户的进行计费的问题。一般计费有两种方式：一是计时记费，二是包时段制，三是计数记费，四是成交额计费。“计时记费”主要用在接入服务、信息(如广告等)刊登服务的计费上。但对内容服务来说，在不区分所访问资源时，其实现较为简单，若要在区分免费资源和计费资源的条件下进行计费则其处理是相当繁复的(当免费和计费资源同属一数据库时，甚至难以实现)，而且无论哪种情况，其系统开销是相当大，因此对提供内容有偿服务来说，特别是在同时提供免费和计费资源(内容)服务时是不宜采取“计时记费”的。而“包时段制”则无论是技术实现，还是资费管理都是较为简便的，应当为商业内容服务的首要计费方式。至于“计数记费”则主要应用在广告刊登的计费上，或小额商品成交收费上。如用在内容服务收费上则对用户来说是很不合理的(比如对信息供应来说，不论是该用户阅览一次还是十次，服务提供者就是有义务保障用户得到应当知悉的信息)。而“成交额计费”则主要应用在“后交易”阶段的大宗成交交易的服务费计费上。

目前，中小企业商务网站的有偿收费绝大部分来源于广告和信息刊登及内容服务方面，而主要的收费处理工作则是关于内容服务方面的。就电子证书用户而言，是不容易发生客户串用(共用)电子证书的(用途较敏感、易引起责任纠纷，加上操作上的限制)。对“用户名/口令”验证则因其安全性较低而应用于责任不大、用途不敏感方面的业务，容易出现多人共用(特别是同一单位的人员)同一帐户(用户名/口令)从而影响网站经营者权益的现象。为抑止这样的情况出现，应在主页的显眼位置设置“更改密码”的便利操作(最好跟“用户登录”在一起)，方便用户随时更改密码(口令)，这样使“口令”的共用者面临风险：其“口令”的更改很可能是不可控制的。并且，为审计跟踪起见，同时记录“注册用户”对其“口令”进行更改操作的历史(含客户的主机名及IP地址)。■