# 面向 PKI 第三方应用程序的 RSA Keon 就绪实施指南

最后修订：6/1/2004

## 1. 合作伙伴信息

| | |
|---|---|
| 合作伙伴名称 | IBM |
| 网站 | http://www.ibm.com/software/cn/websphere/datapower/ |
| 产品名称 | XS40 XML Security Gateway |
| 版本 & 平台 | Release 3 |
| 产品说明 | 特制的 1 U 机架式网络设备，提供了全面的 XML 安全功能集合，功能包括：XML 加密、XML/SOAP 防火墙过滤、XML 数字签名；XML 架构验证；SSL；XML 访问控制。 |
| 产品分类 | Web 服务 |
| 与 RSA Keon 整合 | 证书授权 |

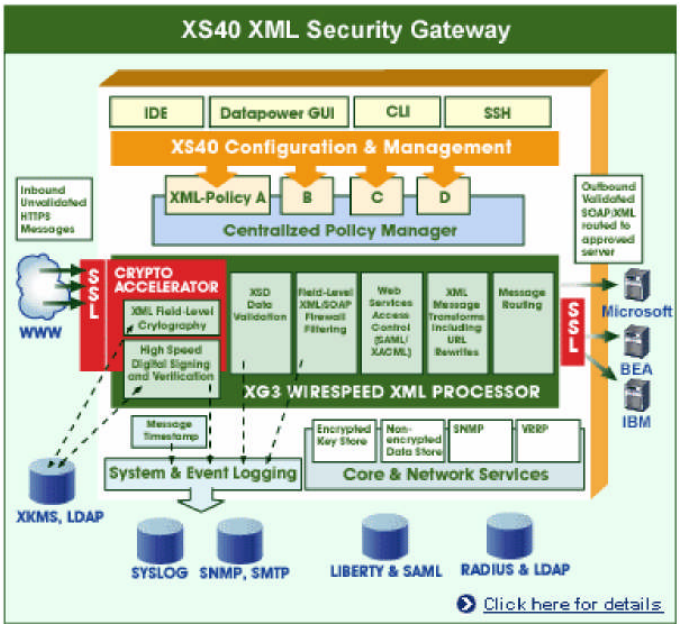
## 2. 联系人信息

| | 销售联系人 | 支持联系人 |
|---|---|---|
| | 李宗灿 | 崔鹏 |
| 电子邮箱 | johnlee@cn.ibm.com | cuipeng@cn.ibm.com |
| 电话 | (86-10)63618826 | (86-10)63612176 |
| 网站 | http://www.ibm.com/software/cn/websphere/datapower/ | http://www.ibm.com/software/cn/websphere/datapower/ |

## 3. 产品需求

### 硬件和软件需求

| 组件名称：**XS40** 设备 | |
|---|---|
| DataPower 固件 | Release 3 （或更新版本） |
| OpenSSL | 用于将 base64 转换为 DER（任何等效工具均适用） |
| | |

## 4. 产品配置

### 互操作性所需的 RSA Keon CA 的*可安装*要素。

1. 已针对 Keon 6.5.1 进行测试；不需特殊权限。

### 互操作性所需的 RSA Keon CA 的*可配置*要素

1. CRL 发布的配置：标准。
2. OCSP 响应程序的配置：标准。
3. 证书发布的配置：已针对内部 LDAP 服务器进行测试，但任何 LDAP 服务器均应有效。

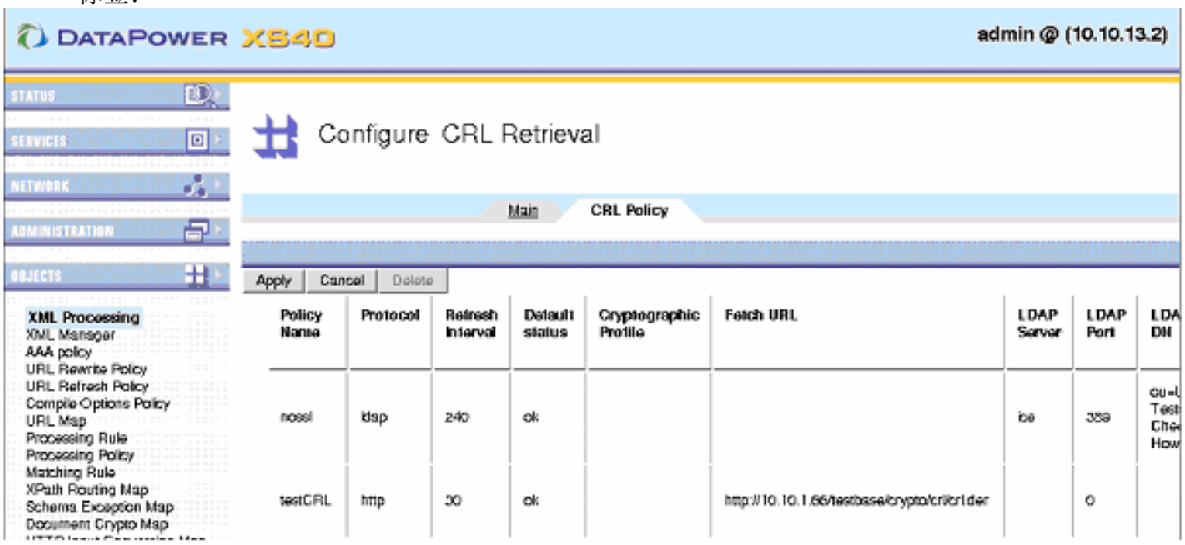
### 互操作性所需的合作伙伴产品的*可安装*要素

1. 固件版本 3.0 或更新版本的 XS40 的标准安装。

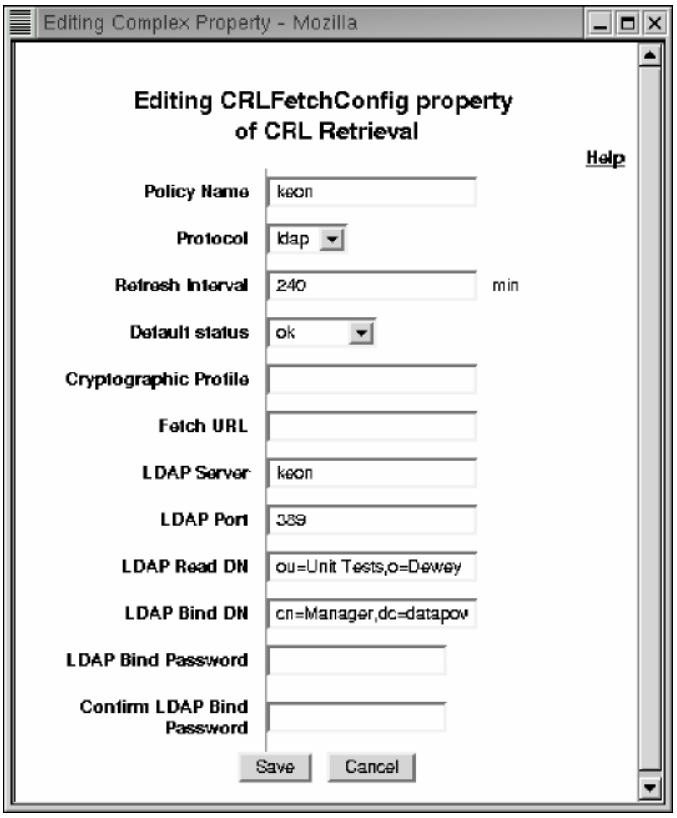
## 互操作性所需的合作伙伴产品的*可配置*要素

1. CRL 校验机制：完成以下步骤来配置 XS40，以适当时间间隔抓取 CRL。

   在 WebGUI 中，打开 **Objects** 菜单，在 Crypto 部分中单击 **CRL Retrieval**，并选择 **CRL Policy** 标签：



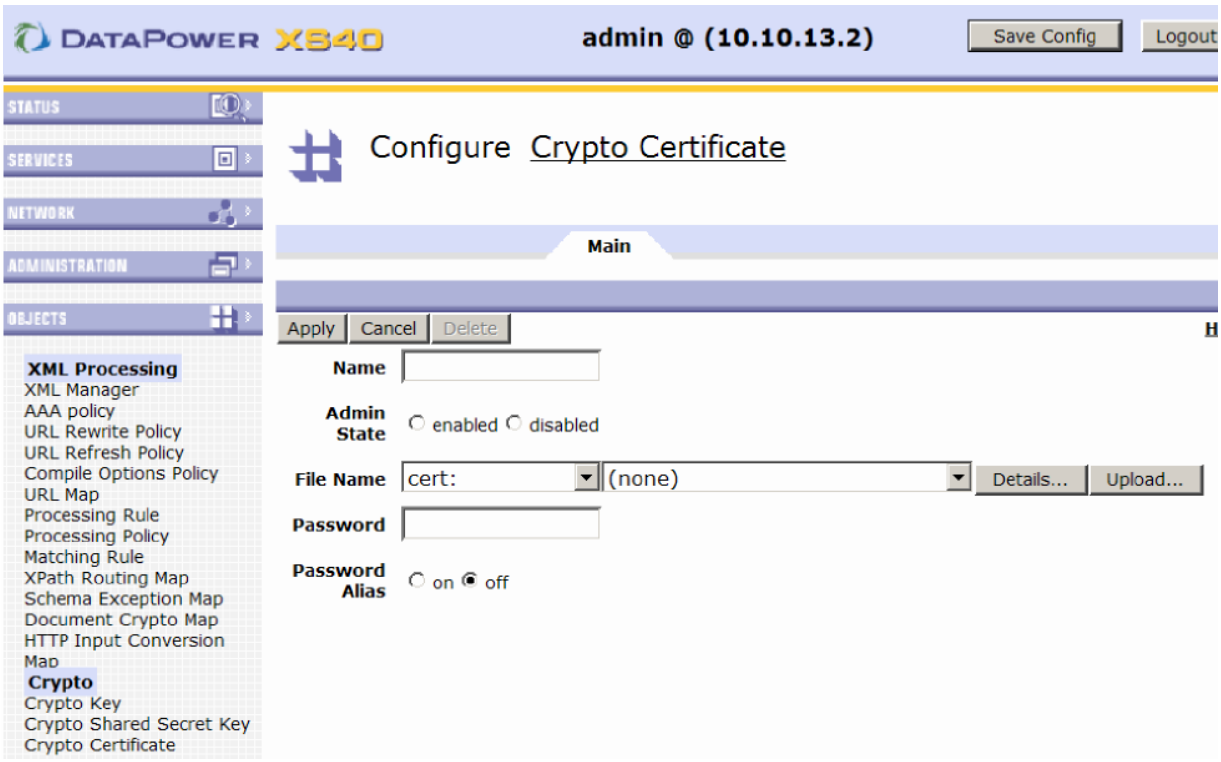

   然后添加一条新策略以从 Keon CA 中抓取 CRL：



2. OCSP 校验机制：针对未来版本计划，当前不可实现。

3. 信任验证：在 XS40 设备上载入 Keon CA 证书。可接受任何标准输出格式。参见下例，它使用了 keon.pem 文件。

   首先使用 XS40 的 WebGUI，打开左侧的 **Objects** 菜单，单击 **Crypto Certificate**。然后单击 **Add**。你会看到如下界面。接着单击 **Upload...**




在 File Management 弹出框中，输入 **keon.pem** 文件路径，然后单击 **Upload**。


填写加密认证表格剩下的部分，单击 Apply 以创建新加密密钥。

现在，当您通过在 Object 菜单选择 **Crypto Validation Credential** 以创建新验证凭据时，应该能够看到并使用 keon 证书。

4. 注册：参看 DataPower 管理文档，获得关于为服务器使用 **keygen** 功能生成公/私钥和证书签发请求（CSR）的指导。

## 5. 产品操作

**注意：***欲获取如何在 DataPower XS40 中使用证书的完整说明，请参考标准 DataPower 文档。*

### RSA Keon CA 的操作要素

1. 证书生成：标准安装 CA 6.5.1，Rev. A7，2003 年 9 月。
2. 证书更新：标准安装
3. 证书吊销：标准安装

### 合作伙伴产品操作要素

1. 注册
   通过 RSA Keon 注册界面完成注册。
2. 输入证书

   参看上页屏幕截图。
3. 证书使用的标准配置，参看标准 DataPower 文档。
4. LDAP 支持　能与 LDAP 绑定以查找名称。

   可使用样式表进行证书检索。请联系 DataPower 以获取适当的样式表。
5. 状态机制
   CRL – LDAP
6. 状态检查
   几乎在未来版本中加入 OCSP 验证
7. RSA Keon Web 护照支持
   N/A
8. RSA SecurID 节支持
   N/A

## 6. 第三方应用程序验证清单

**测试日期：2004 年 5 月 1 日**

| 产品 | 已测试版本 |
|---|---|
| RSA Keon Certificate Authority | Release 6.5.1 |
| RSA Keon Web 护照 | N/A |
| XS40 | Release 3.0 |

| 测试用例 | | | 结果 |
|---|---|---|---|
| **证书注册** | | | |
| PKCS#1 0 证书请求 | | | P |
| 正确安装的 PKCS#7 响应 | | | P |
| CMP 证书请求 | | | N/A |
| 正确安装的 CMP 响应 | | | N/A |
| SCEP 证书请求 | | | N/A |
| 正确安装的 SCEP 响应 | | | N/A |
| **导入证书** | | | |
| 导入 PKCS#12 信封 | | | P |
| 通过剪切/粘贴（到文件，然后上传文件）导入 | | | P |
| 通过剪切/粘贴（到文件，然后上传文件）安装根证书 | | | P |
| 通过剪切/粘贴（到文件，然后上传文件）安装 SubCA 证书 | | | P |
| 通过 SCEP 安装根证书 | | | N/A |
| 通过 SCEP 安装 SubCA 证书 | | | N/A |
| 检查是否已安装证书链 | | | P |
| **证书使用** | **签名** | **加密** | **SSL** |
| S/MIME | N/A | N/A | |
| 文档和文件 | N/A | N/A | |
| SSL 客户机身份验证 | | | P |
| **LDAP 支持** | | | |
| 名称查找 | | | P |
| 证书检索 | | | P |
| **证书状态检查** | **OCSP** | **CRL- LDAP** | **其他** |
| 有效证书的成功状态 | N/A | P | N/A |
| 已吊销证书的失败状态 | N/A | P | N/A |
| 挂起证书的失败状态 | N/A | P | N/A |
| 恢复证书的通过状态 | N/A | P | N/A |
| **RSA Keon Web 护照 / RSA SecurID 节支持** | | **通道** | **KWP** |
| 通过 MS CAPI (Internet Explorer)访问证书 | | N/A | N/A |
| 通过 PKCS#11 (Netscape)访问证书 | | N/A | N/A |

*JEC*

*P=“通过”或“是” F=“失败” N/A=不可用功能

## 7. 已知问题

无。