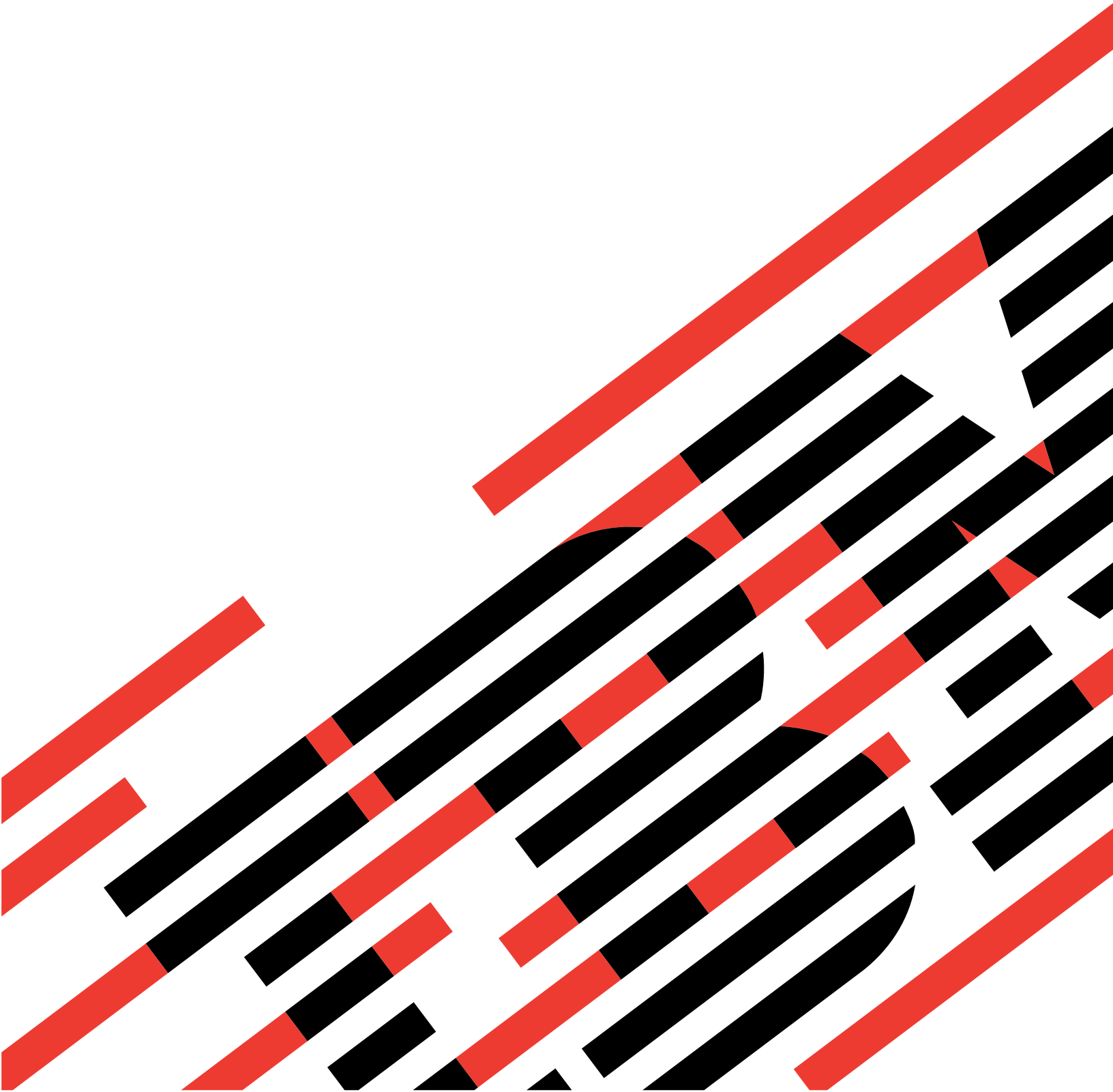
IBM

eserver

iSeries

对象签署和签名验证



IBM

@server

iSeries

对象签署和签名验证

目录

对象签署和签名验证

对象签署和签名验证是一些安全性功能，可使用它们来验证多种 iSeries™ 对象的完整性。使用数字证书的专用密钥签署对象，并使用证书（它包含相应的公用密钥）验证数字签名。数字签名确保要签署对象的时间和内容的完整性。签名是可靠性和权限的不可否认的证据。它可用于显示来源的证据并检测来源是否篡改。通过签署对象，可识别对象的源并提供检测对象是否更改的手段。在验证对象的签名时，可确定自对象签署以来是否对其内容进行了更改。还可验证签名的源以确保对象来源的可靠性。

可通过以下途径实现 iSeries 对象签署和签名验证:

- 使用 API 以程序化方式签署对象及验证对象的签名。
- 使用“数字证书管理器”签署对象及查看或验证对象的签名。
- “iSeries 导航器中央管理”将对象作为分发软件包的一部分签署以供其它系统使用。
- 使用 CL 命令，如“检查对象完整性”（CHKOBJITG）来验证签名。

要了解更多有关这些签署对象的方法以及签署对象可如何增强当前的安全性策略，请查看以下主题:

V5R2 的新增功能
使用此信息了解有关新的 iSeries 对象签署和签名验证功能，以及对此发行版文档所做的更改。

打印此主题
使用此信息将整个主题打印为 PDF 文件。

对象签署方案
使用此信息查看方案，这些方案演示了一些使用 iSeries 对象签署和签名验证功能的典型情况。每个方案还提供了必须执行以实现所描述方案的配置任务。

对象签署概念
使用此概念和参考信息可了解有关数字签名、对象签署和签名验证过程工作的更多信息。

对象签署和签名验证的先决条件
使用此信息了解配置的先决条件，以及签署对象和验证签名的其它规划注意事项。

管理已签署对象
使用此信息了解可用于处理已签署对象的 iSeries 命令和系统值，以及已签署对象如何影响备份和恢复过程。

对对象签署和签名验证进行故障诊断
使用此信息了解如何解决在签署对象和验证签名时可能遇到的问题和错误。

对象签署和签名验证的相关信息
使用此信息查找到其它资源的链接，以了解有关签署对象和验证对象签名的更多信息。

V5R2 的新增功能

在 V5R1 中首次引入了 iSeries 的对象签署和签名验证功能。然而，V5R2 中有一些新的功能和增强。

新的或增强的对象签署和签名验证功能包括:

- **“iSeries 导航器中央管理”对象签署功能**
  现在，可使用“中央管理产品定义”向导签署为分发到 iSeries 端点系统而封装的对象。

- **签署命令（*CMD）对象**
  现在可签署命令（*CMD）对象。可选择是要签署整个 *CMD 对象还是只签署 *CMD 对象的核心组件。
- **新的签署和验证 API**
  可使用三个新的 API 以程序化方式利用增强的 OS/400® 签署与验证功能:
  - 签署缓冲区（QYDOSGNB，QydoSignBuffer）API
    此 API 允许本地系统数字化地签署缓冲区以确保它是可信任的。在签署缓冲区后，系统将数字签名返回给该 API 的调用者。例如，可使用此 API 签署 XML 文件的一部分，而将签名存储在 XML 文件的另一部分。或者，可将数据库文件记录读入缓冲区并使用 API 签署它们。
  - 验证缓冲区（QYDOVFYB，QydoVerifyBuffer）
    此 API 允许本地系统验证先前签署的缓冲区的数字签名。
  - 添加验证方（QYDOADDV，QydoAddVerifier）API
    此 API 向系统的 *SIGNATUREVERIFICATION 证书存储库添加证书。然后，系统可使用添加的证书验证该证书创建的对象签名。验证签名允许系统验证已签署对象的完整性以确保它们自签署以来没被更改。如果该证书存储库不存在，则此 API 在添加证书时创建它。

    注: 由于安全性原因，此 API 不允许将“认证中心”（CA）证书插入 *SIGNATUREVERIFICATION 证书存储库。向证书存储库添加 CA 证书时，系统将该 CA 看作可信的证书源。因此，系统就认为该 CA 发出的证书来自可信的源。所以，不能使用该 API 创建安装出口程序将 CA 证书插入证书存储库。必须使用“数字证书管理器”向证书存储库添加 CA 证书以确保必须特定并人为控制系统信任哪些 CA。这样将防止发生系统从管理员没有特意指定为可信的源导入证书的可能。

    如果要防止任何人在您不知道的情况下使用此 API 向 *SIGNATUREVERIFICATION 证书存储库添加验证证书，则应该考虑在您的系统上禁用此 API。可通过使用“系统服务工具”（SST）禁止更改与安全性相关的系统值完成此操作。

先前，有关 iSeries 对象签署和签名验证功能的信息是“数字证书管理信息中心”主题的一部分。现在，可使用其它方法签署对象和验证签名。因此，通过提供有关使用这些功能的集中的信息，这个新的“信息中心”主题可让使用对象签署和签名验证功能更加容易。该主题提供增强的和更完整的信息（如方案），帮助您确定何时及如何使用这些功能来补充安全性策略。

此主题新的或增强的信息包括:

- 方案，可用于帮助您确定如何最好地使用对象签署和签名验证功能以补充安全性策略。
- 描述可用于管理系统上已签署对象的命令和系统值的新章节。
- 描述签署对象和验证签名的规划及其它概念性信息的新章节。

要查找有关此发行版的新增功能或更改的其它信息，参阅用户备忘录 。

打印本主题

要查看或下载 PDF 版本，选择对象签署和签名验证 （文件大小 350 kb 或大约 44 页）。

要在工作站上保存 PDF 供查看或打印:

1. 在浏览器中打开该 PDF（单击上面的链接）。
2. 在浏览器的菜单中，单击**文件**。
3. 单击**另存为...**
4. 浏览至希望在其中保存该 PDF 的目录。

5. 单击**保存**。

如果需要 Adobe Acrobat Reader 来查看或打印该 PDF，可从 Adobe Web 站点（www.adobe.com/prodindex/acrobat/readstep.html）  下载一个副本。

对象签署方案

iSeries 服务器提供几种不同的方法来签署对象和验证对象的签名。如何选择签署对象及如何处理签署对象，因您的业务和安全性需要及目的而异。在一些情况下，可能只需要验证系统上的对象签名以确保对象的完整性。在其它情况下，可能选择签署分发给其他人的对象。签署对象允许其他人识别对象的来源并检查对象的完整性。

选择使用哪种方法取决于各种因素。本主题中提供的方案描述典型业务环境中一些更常用的对象签署和签名验证目的。每个方案还描述要实现所描述方案的先决条件和必须执行的任务。查看这些方案以帮助您确定如何以最适于您的业务和安全性需要的途径来使用 iSeries 对象签署功能:

方案: 使用“数字证书管理器”签署对象和验证签名
此方案描述某个公司希望在其公共 Web 服务器上签署易受攻击的应用程序对象。他们希望能更容易地确定何时存在对这些对象的未授权更改。根据该公司的业务需要和安全性目标，此方案描述如何使用“数字证书管理器”（DCM）作为签署对象和验证对象签名的主要方法。

方案: 使用 API 签署对象及验证签名
此方案描述某应用程序开发公司希望以程序化方式签署其销售的应用程序。他们希望能够使客户确信应用程序来自他们公司，并向他们提供在安装时检测应用程序未授权更改的手段。根据该公司的业务需要和安全性目标，此方案描述如何使用“签署对象”API 和“添加验证方”API 以签署对象并启用签名验证。

方案: 使用“中央管理”签署对象
此方案描述某公司希望签署其封装并分发给多个 iSeries 服务器的对象。根据该公司的业务需要和安全性目标，此方案描述如何使用“iSeries 导航器中央管理”功能封装并签署它们分发到其它 iSeries 服务器的对象。

方案: 使用 DCM 签署对象和验证签名

情况

作为 MyCo 公司的 iSeries 管理员，您负责管理公司的两台 iSeries 服务器。其中一台 iSeries 服务器提供公司的公共 Web 站点。您使用公司的内部生产 iSeries 服务器开发此公共 Web 站点的内容，经测试后将文件和程序对象传送到公共 Web 服务器。

公司的公共 Web 服务器提供一般的公司信息 Web 站点。该 Web 站点还提供各种表单供客户填写以注册产品及请求产品信息、产品更新布告、产品分发位置等等。您关心的薄弱环节是提供这些表单的 cgi-bin 程序；您知道它们可能被修改。因此，您希望能检查这些程序对象的完整性并检测何时对其进行了未授权的更改。所以，您决定数字化签署这些对象以实现这个安全性目标。

您研究了 OS/400 对象签署功能并了解到有几种方法可用于签署对象和验证对象签名。因为您负责管理的 iSeries 服务器数量少并且认为不必经常签署对象，所以您决定使用“数字证书管理器”（DCM）执行这些任务。您还决定创建“本地认证中心”（CA）并使用专用证书签署对象。使用“本地 CA”发出的专用证书对对象进行签署可减少使用此安全性技术的花费，因为您不必从知名的公共 CA 购买证书。

此示例介绍了希望在少量 iSeries 服务器上签署对象时设置和使用对象签署过程中所涉及的步骤。

方案的优点

此方案有以下优点:

- 签署对象提供检查易受攻击对象的完整性以及更加容易地确定对象在签署以后是否被更改。这样可减少将来可能会发生的查找应用程序和其它系统问题的某些故障诊断。
- 使用 DCM 的图形用户界面（GUI）签署对象和验证对象签名允许您及公司其他人快捷地执行这些任务。
- 使用 DCM 签署对象和验证对象签名减少了理解对象签署和将对象签署用作安全性策略的一部分所必须花的时间量。
- 使用“本地认证中心”（CA）发出的证书使签署对象以更少的花费实现。

目的

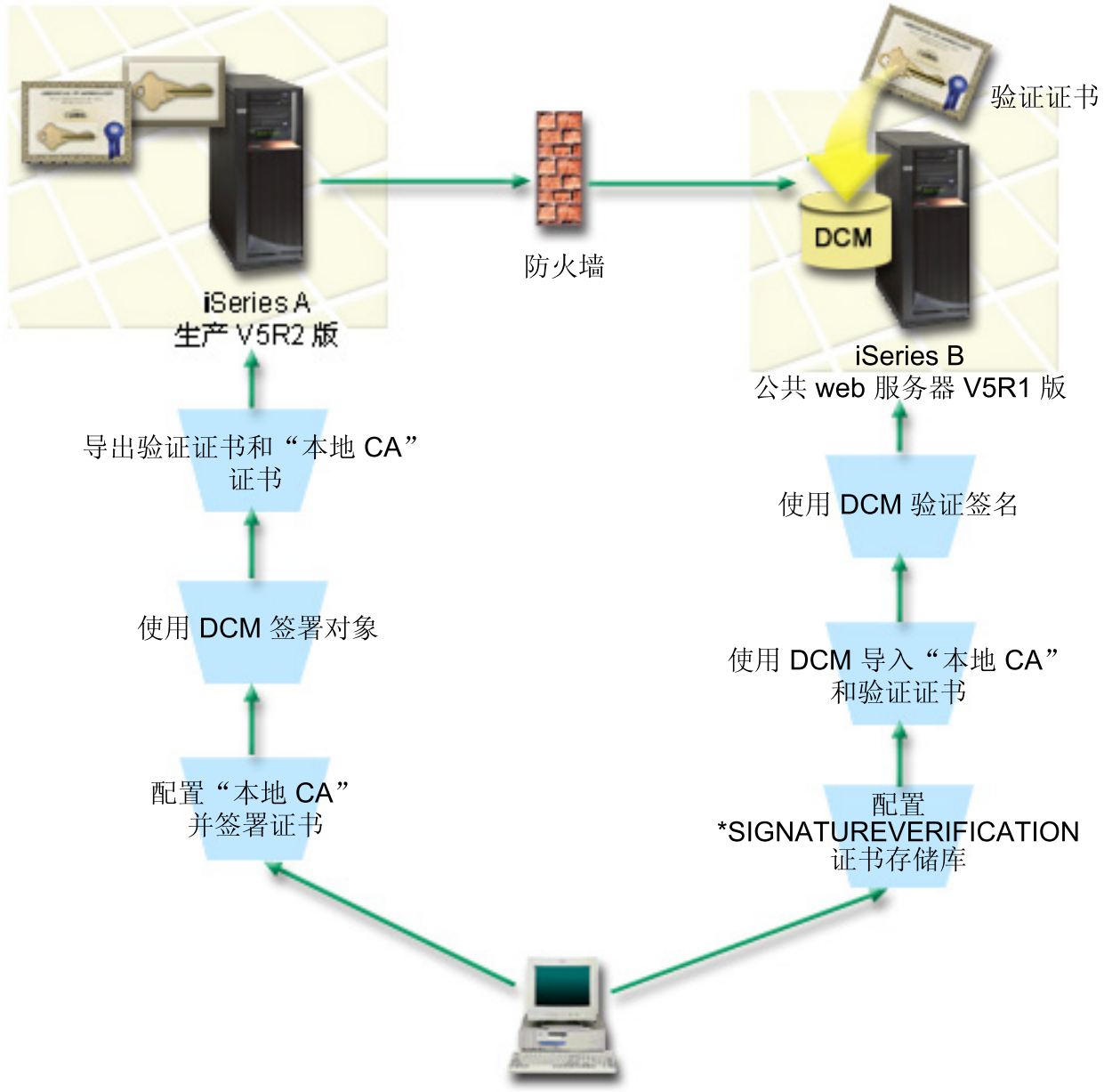
在此方案中，您希望数字化签署公司的公共 iSeries 服务器上易受攻击的对象（如生成表单的 cgi-bin 程序）。作为 MyCo 公司的系统管理员，您希望使用“数字证书管理器”（DCM）签署这些对象并验证对象的签名。

此方案的目的如下所述:

- 必须以来自“本地 CA”的证书签署公共 Web 服务器（iSeries B）上的公司应用程序和其它易受攻击的对象以限制签署应用程序的成本。
- 系统管理员和其它指定的用户必须能容易地验证 iSeries 服务器的数字签名以验证公司已签署对象的源和可靠性。为实现此目标，在每个服务器的 *SIGNATUREVERIFICATION 证书存储库中，每个 iSeries 服务器必须同时拥有公司签名验证证书和“本地认证中心”（CA）证书的副本。
- 通过验证公司应用程序和其它对象的签名，iSeries 管理员和其他人可检测自对象签署以来其内容是否被更改过。
- 系统管理员必须使用 DCM 签署对象；系统管理员和其他人必须能够使用 DCM 验证对象签名。

详细信息

下图演示实现此方案的对象签署和签名验证过程:



该图演示与此方案相关的以下几点:

iSeries A

- iSeries A 运行 OS/400 版本 5 发行版 2（V5R2）。
- iSeries A 是公司的内部生产服务器和公共 iSeries Web 服务器（iSeries B）的开发平台。
- iSeries A 安装了 Cryptographic Access Provider 128-bit for iSeries（5722–AC3）。
- iSeries A 安装并配置了“数字证书管理器”（OS/400 选项 34）和 IBM® HTTP Server（5722–DG1）。
- iSeries A 充当“本地认证中心”（CA），且对象签署证书驻留在此系统上。
- iSeries A 使用 DCM 签署对象，并且是公司公共应用程序和其它对象的主要对象签署系统。
- iSeries A 配置为启用签名验证。

iSeries B

- iSeries B 运行 OS/400 版本 5 发行版 1（V5R1）。
- iSeries B 是公司防火墙之外的公司外部公共 Web 服务器。
- iSeries B 安装了 Cryptographic Access Provider 128-bit（5722–AC3）。
- iSeries B 安装并配置了“数字证书管理器”（OS/400 选项 34）和 IBM HTTP Server（5722–DG1）。
- iSeries B 不运行“本地 CA”，也不签署对象。
- iSeries B 配置为可通过使用 DCM 创建 *SIGNATUREVERIFICATION 证书存储库并导入必需的验证和“本地 CA”证书启用签名验证。
- 使用 DCM 验证对象签名。

先决条件和假设

此方案取决于以下的先决条件和假设:

1. 所有 iSeries 服务器都满足安装和使用“数字证书管理器”（DCM）的要求。
2. 在任何一台 iSeries 服务器上，先前没有人配置或使用过 DCM。
3. 所有 iSeries 服务器都安装了最高级别的 Cryptographic Access Provider 128-bit 许可程序（5722-AC3）。
4. 在所有方案 iSeries 服务器上恢复（QVFYOBJRST）系统值期间，验证对象签名的缺省设置为 3，且此设置未被更改。该缺省设置确保服务器在恢复已签署对象时可验证对象签名。
5. iSeries A 的系统管理员必须具有 *ALLOBJ 特权以签署对象，或者必须将该用户概要文件授权给对象签署应用程序。
6. 系统管理员或在 DCM 中创建证书存储库的任何其他人都必须具有 *SECADM 和 *ALLOBJ 特权。
7. 系统管理员或所有其它 iSeries 服务器上的其他人必须具有 *AUDIT 特权才能验证对象签名。

任务步骤

有两组任务，必须完成才能实现此方案: 一组任务允许将 iSeries A 配置为“本地认证中心”（CA）并且签署及验证对象签名。第二组任务允许配置 iSeries B 以验证 iSeries A 创建的对象签名。

iSeries A 任务步骤

必须在 iSeries A 上完成以下任务的每一项才能创建专用“本地 CA”以及签署对象和验证对象签名，如此方案所述:

1. 完成所有先决条件的步骤以安装及配置所有必需的 iSeries 产品。
2. 使用“数字证书管理器”（DCM）创建“本地认证中心”（CA）以发出对象签署证书。
3. 使用 DCM 创建应用程序定义。
4. 使用 DCM 指定证书给对象签署应用程序定义。
5. 使用 DCM 签署 cgi-bin 程序对象。
6. 使用 DCM 导出证书，这些证书是其它系统验证对象签名必须使用的证书。必须将“本地 CA”证书的副本和对象签署证书的副本作为签名验证证书导出到文件中。
7. 传送证书文件到公司的公共 iSeries 服务器（iSeries B），以便您及其他人可验证 iSeries A 创建的签名。

iSeries B 任务步骤

如果打算恢复在此方案中传送到公共 Web 服务器（iSeries B）的已签署对象，在传送已签署对象之前应在 iSeries B 上完成这些签名验证配置任务。必须先完成签名验证配置，才能在公共 Web 服务器上恢复已签署对象时成功地验证签名。

在 iSeries B 上，必须如此方案所述完成以下验证对象签名的任务:

8. 使用“数字证书管理器”（DCM）创建 *SIGNATUREVERIFICATION 证书存储库。
9. 使用 DCM 导入“本地 CA”证书和签名验证证书。
10. 使用 DCM 对传送的对象验证签名。

配置详细信息

如此方案所述完成以下任务步骤，配置并使用“数字证书管理器”以签署对象。

步骤 1: 完成所有先决条件的步骤

必须完成所有先决条件任务以安装和配置所有必需的 iSeries 产品，才能执行实现此方案的特定配置任务。

步骤 2: 创建“本地认证中心”以发出专用对象签署证书

使用“数字证书管理器”（DCM）创建“本地认证中心”（CA）时，该过程要求您完成一系列表单。这些表单指导您完成创建 CA 的过程以及完成其它任务的过程，其它任务是开始将数字证书用于“安全套接字层”（SSL）、对象签署和签名验证所必需的过程。虽然在此方案中不必对 SSL 配置证书，但必须完成此任务中的所有表单以配置系统签署对象。

要使用 DCM 创建并操作“本地 CA”，执行以下步骤:

1. 启动 DCM。
2. 在 DCM 的导航框架中，选择**创建认证中心（CA）**以显示一系列表单。

   注: 如果对完成此指导任务中的特定表单有疑问，请选择此页面顶部的问号（**?**）按钮以访问联机帮助。
3. 完成此指导任务的所有表单。执行此任务时，务必执行以下操作:
   a. 提供“本地 CA”的标识信息。
   b. 在浏览器中安装“本地 CA”证书以便软件可识别“本地 CA”并确认该“本地 CA”发出的证书。
   c. 指定“本地 CA”的策略数据。
   d. 使用新的“本地 CA”发出应用程序可用于 SSL 连接的服务器或客户机证书。

      注: 虽然此方案没有使用此证书，但必须先创建它才能使用“本地 CA”发出所需的对象签署证书。如果取消任务而不创建此证书，必须分别创建对象签署证书及存储该证书的 *OBJECTSIGNING 证书存储库。
   e. 选择可以使用服务器或客户机证书的应用程序以进行 SSL 连接。

      注: 对于此方案，不要选择任何应用程序，单击**继续**以显示下一个表单。
   f. 使用新的“本地 CA”发出应用程序可用于数字化签署对象的对象签署证书。此子任务创建 *OBJECTSIGNING 证书存储库。它是用于管理对象签署证书的证书存储库。
   g. 选择应信任“本地 CA”的应用程序。

      注: 对于此方案，不要选择任何应用程序，单击**继续**以完成任务。

创建了“本地 CA”和对象签署证书后，必须先定义对象签署应用程序来使用该证书，才能签署对象。

步骤 3: 创建对象签署应用程序定义

创建对象签署证书后，必须使用“数字证书管理器”（DCM）定义可用于签署对象的对象签署应用程序。应用程序定义不需要引用实际的应用程序；创建的应用程序定义应描述要签署的对象的类型或组。需要该定义以便将应用程序标识与该证书关联从而启用签署过程。

要使用 DCM 创建对象签署应用程序定义，请遵循以下步骤:

1. 在导航框架中，单击**选择证书存储库**并选择 ***OBJECTSIGNING** 作为要打开的证书存储库。
2. 在显示“证书存储库和密码”页面时，提供在创建证书存储库时为其指定的密码并单击**继续**。
3. 在导航框架中，选择**管理应用程序**显示任务列表。
4. 从任务列表选择**添加应用程序**显示定义应用程序的表单。
5. 完成该表单并单击**添加**。

现在必须为创建的应用程序指定对象签署证书。

步骤 4: 为对象签署应用程序定义指定证书

要为对象签署应用程序指定证书，请遵循以下步骤:

1. 在 DCM 导航框架中，选择**管理证书**显示任务列表。
2. 从任务列表中，选择**指定证书**显示当前证书存储库的证书列表。
3. 从该列表选择证书，单击**指定给应用程序**显示当前证书存储库的应用程序定义列表。
4. 从列表选择一个或多个应用程序，单击**继续**。显示一个消息页面，确认证书指定，或者如果发生问题则提供错误信息。

完成此任务时，已准备好使用 DCM 签署公司的公共 Web 服务器（iSeries B）将使用的程序对象。

步骤 5: 签署程序对象

要使用 DCM 签署程序对象以在公司公共 Web 服务器（iSeries B）上使用，请遵循以下步骤:

1. 在导航框架中，单击**选择证书存储库**并选择 ***OBJECTSIGNING** 作为要打开的证书存储库。
2. 输入 *OBJECTSIGNING 证书存储库的密码，然后单击**继续**。
3. 导航框架刷新之后，选择**管理可签署的对象**显示任务列表。
4. 从任务列表中，选择**签署对象**显示可用于签署对象的应用程序定义列表。
5. 选择在上一步骤中定义的应用程序并单击**签署对象**。显示供您指定要签署的对象的位置的表单。
6. 在提供的字段中，输入要签署的对象的全限定路径和对象的文件名或目录，然后单击**继续**。或者输入目录位置，然后单击**浏览**查看该目录的内容以选择对象进行签署。

   注: 对象名称必须以前导斜杠开始，否则会发生错误。也可使用某些通配符来描述希望签署的部分目录。这些通配符有星号（*****），它指定*任意数量的字符*，和问号（**?**），它指定*任意一个字符*。例如，要签署特定目录中的所有对象，可输入 `/mydirectory/*`；要签署特定库中的所有程序，可输入 `/QSYS.LIB/QGPL.LIB/*.PGM`。只能在路径名称的最后一部分中使用这些通配符；例如，`/mydirectory*/filename` 将导致错误消息。如果希望使用“浏览”功能查看库列表或目录内容，应输入通配符作为路径名称的一部分，然后单击**浏览**。
7. 选择希望用于签署所选对象的处理选项，然后单击**继续**。

注: 如果选择等待作业结果，则在浏览器中直接显示结果文件。当前作业的结果附加到结果文件的末尾。因此，除当前作业的结果外，该文件可包含任何先前作业的结果。可使用该文件中的日期字段确定该文件中哪些行适用于当前作业。日期字段为 YYYYMMDD 格式。该文件的第一个字段可能是消息标识（如果处理该对象期间发生错误的话）或日期字段（指示处理该作业的日期）。

8. 指定全限定路径和文件名以用于存储对象签署操作的作业结果，然后单击**继续**。或者，输入目录位置，然后单击**浏览**查看该目录的内容以选择存储该作业结果的文件。显示消息指示已提交该作业以签署对象。要查看作业结果，参阅作业记录中的作业 **QOBJSGNBAT**。

为确保您及其他人能验证签名，必须将必要的证书导出到文件并将该证书文件传送到 iSeries B。还必须在 iSeries B 上完成所有签名验证配置任务，才能将已签署程序对象传送到 iSeries B。必须完成签名验证配置才能在 iSeries B 上恢复已签署对象时成功验证签名。

步骤 6: 导出证书以在 iSeries B 上启用签名验证

签署对象以保护内容的完整性要求您及其他人都有验证签名的可靠性的手段。要在签署对象的同一系统（iSeries A）上验证对象签名，必须使用 DCM 创建 *SIGNATUREVERIFICATION 证书存储库。此证书存储库必须同时包含该对象签署证书的副本和发出该签署证书的 CA 的 CA 证书的副本。

要允许其他人验证签名，必须向其提供签署该对象的证书的副本。使用“本地认证中心”（CA）发出证书时，还必须为其提供“本地 CA”证书的副本。

要使用 DCM 以便可在签署对象的同一系统上验证签名（在此方案中为 iSeries A），请遵循以下步骤:

1. 在导航框架中，选择**创建新的证书存储库**并选择 ***SIGNATUREVERIFICATION** 作为要创建的证书存储库。
2. 选择**是**以将现有对象签署证书作为签名验证证书复制到新的证书存储库。
3. 为新的证书存储库指定密码，然后单击**继续**以创建证书存储库。现在可在用于签署对象的同一系统上使用 DCM 验证对象签名。

要使用 DCM 导出“本地 CA”证书的副本及对象签署证书的副本作为签名验证证书以便可在其它系统（iSeries B）上验证对象签名，请遵循以下步骤:

1. 在导航框架中，选择**管理证书**，然后，选择**导出证书**任务。
2. 选择**认证中心（CA）**，单击**继续**显示可导出的 CA 证书的列表。
3. 从列表选择较早时创建的“本地 CA”证书，单击**导出**。
4. 指定**文件**作为导出目标，单击**继续**。
5. 指定导出的“本地 CA”证书的全限定路径和文件名，单击**继续**以导出证书。
6. 单击**确定**以退出“导出确认”页面。现在可导出对象签署证书的副本。
7. 重新选择**导出证书**任务。
8. 选择**对象签署**以显示可导出的对象签署证书的列表。
9. 从列表选择相应的对象签署证书，单击**导出**。
10. 选择**文件**，**作为签名验证证书**为目的，单击**继续**。
11. 指定导出的签名验证证书的全限定路径和文件名，单击**继续**以导出证书。

现在可将这些文件传送到 iSeries 端点系统，将要在该端点系统上验证用该证书创建的签名。

步骤 7: 将证书文件传送到公司公共服务器 iSeries B

必须先将在 iSeries A 上创建的证书文件传送到 iSeries B（在此方案中为公司的公共 Web 服务器），才能配置它们以验证您签署的对象。可使用几种不同的方法传送证书文件。例如，可使用“文件传输协议”（FTP）或“中央管理”软件包分发来传送文件。

步骤 8: 签名验证任务: 创建 *SIGNATUREVERIFICATION 证书存储库

要在 iSeries B（公司的公共 Web 服务器）上验证对象签名，iSeries B 必须在 *SIGNATUREVERIFICATION 证书存储库中有相应的签名验证证书的副本。因为使用了“本地 CA”发出的证书签署对象，所以此证书存储库还必须包含“本地 CA”证书的副本。

要创建 *SIGNATUREVERIFICATION 证书存储库，请遵循以下步骤:

1. 启动 DCM。
2. 在“数字证书管理器”（DCM）导航框架中，选择**创建新的证书存储库**并选择 ***SIGNATUREVERIFICATION** 作为要创建的证书存储库。

   注: 如果在使用 DCM 时对如何完成特定的表单有疑问，请选择页面顶部的问号（**?**）以访问联机帮助。
3. 为新的证书存储库指定密码，单击**继续**以创建证书存储库。现在可将证书导入存储库并用其验证对象签名。

步骤 9: 签名验证任务: 导入证书

要验证对象的签名，*SIGNATUREVERIFICATION 存储库必须包含签名验证证书的副本。如果签署证书是专用的，此证书存储库还必须有发出该签署证书的“本地认证中心”（CA）证书的副本。在此方案中，已将两个证书都导出到文件中，并将该文件传送到每个 iSeries 端点系统。

要将这些证书导入 *SIGNATUREVERIFICATION 存储库中，请遵循以下步骤:

1. 在 DCM 导航框架中，单击**选择证书存储库**，并选择 ***SIGNATUREVERIFICATION** 作为要打开的证书存储库。
2. 显示“证书存储库和密码”页面时，提供在创建证书存储库时为其指定的密码并单击**继续**。
3. 导航框架刷新之后，选择**管理证书**以显示任务列表。
4. 从任务列表中，选择**导入证书**。
5. 选择**认证中心（CA）**作为证书类型并单击**继续**。

   注: 导入专用签名验证证书之前必须先导入“本地 CA”证书，否则，签名验证证书的导入过程将失败。
6. 指定 CA 证书文件的全限定路径和文件名，单击**继续**。显示一个消息，确认导入过程成功，或者如果该过程失败则提供错误信息。
7. 重新选择**导入证书**任务。
8. 选择**签名验证**作为要导入的证书类型，单击**继续**。
9. 指定签名验证证书文件的全限定路径和文件名，单击**继续**。显示一个消息，确认导入过程成功，或者如果该过程失败则提供错误信息。

现在可在 iSeries B 上使用 DCM 来验证在 iSeries A 上使用相应的签署证书创建的对象签名。

步骤 10: 签名验证任务: 验证程序对象签名

要使用 DCM 验证已传送的程序对象的签名，请遵循以下步骤:

1. 在导航框架中，单击**选择证书存储库**，并选择 ***SIGNATUREVERIFICATION** 作为要打开的证书存储库。

2. 输入 *SIGNATUREVERIFICATION 证书存储库的密码，单击**继续**。
3. 导航框架刷新之后，选择**管理可签署的对象**以显示任务列表。
4. 从任务列表中，选择**验证对象签名**以指定希望验证其签名的对象的位置。
5. 在提供的字段中，输入希望验证其签名的对象的全限定路径和对象的文件名或目录，单击**继续**。或者，输入目录位置，单击**浏览**以查看该目录的内容来选择对象进行签名验证。

   注: 还可使用某些通配符来描述要验证的目录部分。这些通配符有星号（*****），它指定*任意个数的字符*；和问号（**?**），它指定*任意一个字符*。例如，要签署特定目录中的所有对象，可输入 `/mydirectory/*`；要签署特定库中的所有程序，可输入 `/QSYS.LIB/QGPL.LIB/*.PGM`。只能在路径名称的最后一部分中使用这些通配符，例如 `/mydirectory*/filename` 将导致出现错误消息。如果希望使用“浏览”功能查看库列表或目录内容，应先将通配符作为路径名的一部分输入，然后单击**浏览**。
6. 选择希望用于验证所选对象签名的处理选项，单击**继续**。

   注: 如果选择等待作业结果，则结果文件直接显示在浏览器中。当前作业的结果附加到结果文件的末尾。因此，除当前作业的那些结果外，该文件可包含任何先前作业的结果。可使用该文件中的日期字段来确定该文件中哪些行适用于当前作业。日期字段为 YYYYMMDD 格式。该文件的第一个字段可能是消息标识（如果处理该对象期间发生错误的话）或日期字段（指示处理该作业的日期）。
7. 指定用于存储签名验证操作的作业结果的全限定路径和文件名，单击**继续**。或者，输入目录位置，单击**浏览**以查看该目录的内容来选择文件存储该作业结果。显示一个消息指示已提交该作业以验证对象签名。要查看作业结果，参阅作业记录中的作业 **QOBJSGNBAT**。

方案: 使用 API 签署对象和验证对象签名

情况

您的公司（MyCo 公司）是一家为客户开发应用程序的 iSeries 业务伙伴。作为公司的软件开发者，您负责封装这些应用程序以用于客户分发。您当前使用程序来封装应用程序。客户可订购压缩光盘（CD-ROM）或者他们可访问您的 Web 站点并下载应用程序。

您一直很关注最新的业界新闻，尤其是安全性新闻。因此，您知道客户理所当然地关心他们接收的或下载的程序的源和内容。有几次客户原以为他们接收的或下载的产品是来自可信的源，但结果却不是真正的产品源。这种混乱的情况有时导致客户安装了他们不希望安装的产品。有时所安装的产品竟然是恶意程序或者被修改过且对系统造成了损害。

虽然这类问题对于 iSeries 客户并不常见，但您希望使客户确信他们从您那里获得的应用程序确实是来自于您的公司。您还希望为客户提供检查应用程序完整性的方法，以便客户在安装这些应用程序之前就可确定它们是否被修改过。

通过研究，您决定使用 OS/400 对象签署功能来实现您的安全性目标。数字化签署应用程序允许客户验证您的公司是其接收或下载的应用程序的合法源。因为您当前以程序化方式封装应用程序，所以您决定使用 API，这样可以轻易地向现有封装过程添加对象签署。您还决定使用公共证书签署对象，以便在安装产品时可使签名验证过程对客户透明。

将用于签署对象的数字证书的副本作为应用程序软件包的一部分。客户获得应用程序软件包时，可使用证书的公用密钥验证应用程序签名。此过程允许客户识别并验证应用程序的源，并确保应用程序对象的内容自签署以来未被修改。

此示例介绍如何以程序化方式签署用于您开发并封装供其他人使用的应用程序的对象。

方案的优点

此方案有以下优点:

- 使用 API 以程序化方式封装并签署对象将减少实现此安全性所必须花费的时间。
- 在封装时使用 API 签署对象将减少要签署对象必须执行的步骤数，因为签署过程是封装过程的一部分。
- 签署对象的软件包允许您更容易地确定对象自签署以来是否被更改过。这样可减少将来为客户找出应用程序问题时的一些故障诊断过程。
- 使用知名的公共“认证中心”（CA）的证书签署对象，可让您在产品安装程序中将“添加验证方 API”用作出口程序的一部分。使用此 API 允许将用于签署应用程序的公共证书自动添加到客户系统。这样确保签名验证对客户透明。

目的

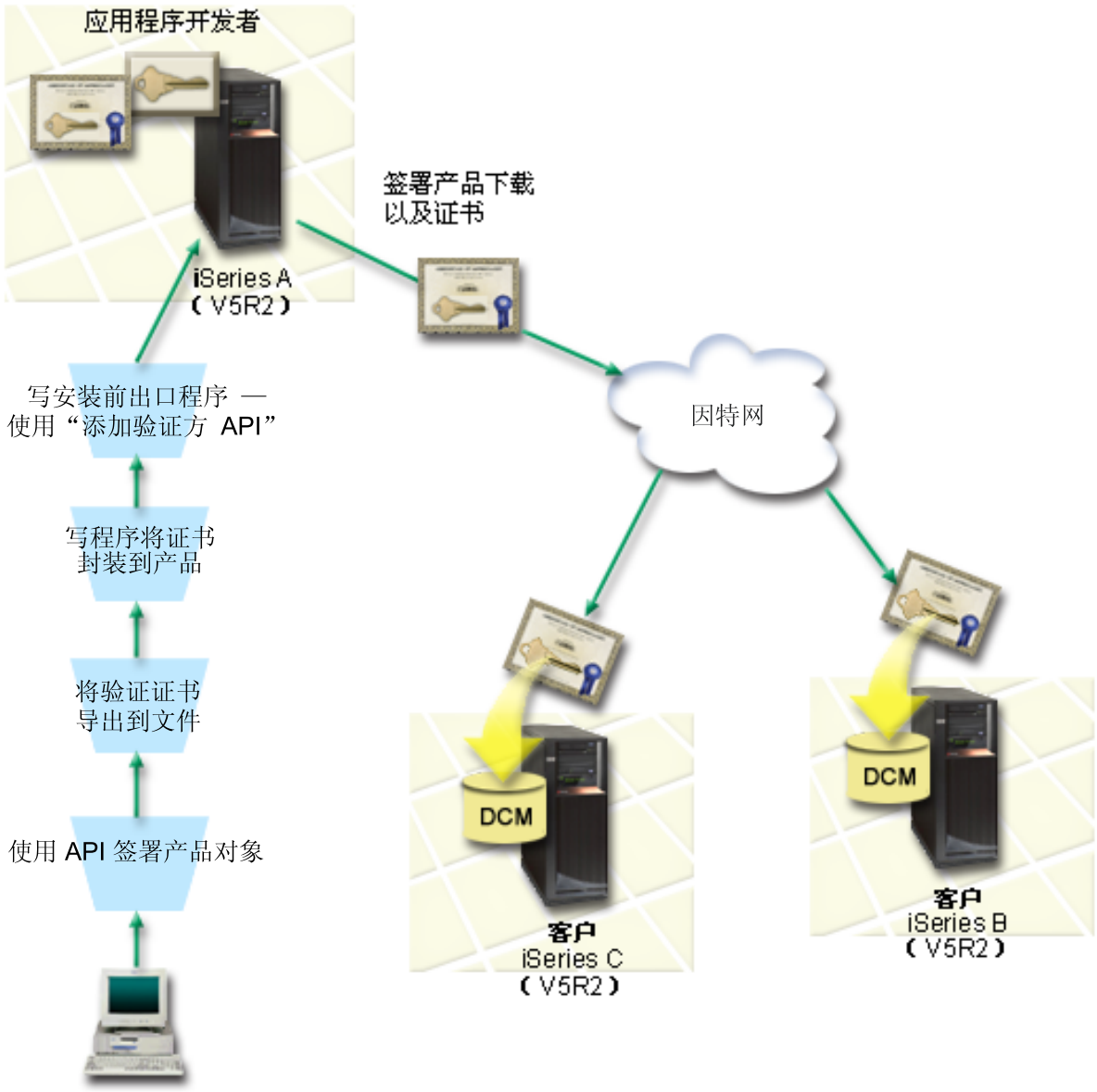
在此方案中，MyCo 公司希望以程序化方式签署它封装并分发给其客户的应用程序。作为 MyCo 公司的应用程序的生产开发者，您当前以程序化方式封装公司的应用程序以分发给客户。因此，您希望使用 iSeries API 签署应用程序并让客户的 iSeries 在产品安装期间以程序化方式验证签名。

此方案的目的如下所述:

- 公司生产开发者必须能通过将“签署对象 API”用作现有程序化应用程序封装过程的一部分来签署对象。
- 必须用公共证书签署公司应用程序，以确保在应用程序产品安装过程期间签名验证过程对客户透明。
- 公司必须能使用 iSeries API 以程序化方式将必需的签名验证证书添加到客户的 iSeries 服务器 *SIGNATUREVERIFICATION 证书存储库。如果此证书存储库尚不存在，公司必须能以程序化方式在客户的 iSeries 服务器上作为产品安装过程的一部分创建此证书存储库。
- 产品安装之后，客户必须能够较容易地验证公司应用程序的数字签名。客户必须能够验证签名，以便他们可确定该已签署应用程序的源和可靠性，并确定该应用程序自签署以来是否被更改过。

详细信息

下图演示实现此方案的对象签署和签名验证过程:



该图演示与此方案相关的以下几点:

中央系统（iSeries A）

- iSeries A 运行 OS/400 版本 5 发行版 2（V5R2）。
- iSeries A 运行应用开发者的产品封装程序。
- iSeries A 安装了 Cryptographic Access Provider 128-bit for iSeries（5722–AC3）。
- iSeries A 安装并配置了“数字证书管理器”（OS/400 选项 34）和 IBM HTTP Server（5722–DG1）。
- iSeries A 是公司应用程序产品的主要对象签署系统。在 iSeries A 上通过执行以下任务来完成客户分发的产品对象签署:
  1. 使用 API 签署公司应用程序产品。
  2. 使用 DCM 将签名验证证书导出到文件，以便客户可验证已签署对象。
  3. 编写程序以将验证证书添加到已签署应用程序产品。

4. 为使用 “添加验证方 API” 的产品编写安装前出口程序。此 API 允许产品安装过程以程序化方式将验证证书添加到客户的 iSeries 服务器（iSeries B 和 C）上的 *SIGNATUREVERIFICATION 证书存储库。

客户 iSeries 服务器 B 和 C

- iSeries B 运行 OS/400 版本 5 发行版 2（V5R2）。
- iSeries C 运行 OS/400 版本 5 发行版 2（V5R2）。
- iSeries B 和 C 安装并配置了 “数字证书管理器”（选项 34）和 IBM HTTP Server（5722–DG1）。
- iSeries B 和 C 从应用程序开发公司（该公司拥有 iSeries A）的 Web 站点购买和下载应用程序。
- MyCo 的应用程序安装过程在这些客户的每台 iSeries 服务器上创建 *SIGNATUREVERIFICATION 证书存储库时，iSeries B 和 C 获得 MyCo 的签名验证证书的副本。

先决条件和假设

此方案取决于以下的先决条件和假设:

1. 所有 iSeries 服务器都满足安装和使用 “数字证书管理器”（DCM）的要求。

   注: 满足安装和使用 DCM 的先决条件对于客户（此方案中为 iSeries B 和 C）是一个可选的要求。虽然 “添加验证方 API” 根据需要作为产品安装过程的一部分可创建 *SIGNATUREVERIFICATION 证书存储库，但 “添加验证方 API” 使用缺省密码创建该证书存储库。客户需要使用 DCM 更改缺省密码以保护此证书存储库免受未授权的访问。
2. 在任何一台 iSeries 服务器上，先前没有人配置或使用过 DCM。
3. 所有 iSeries 服务器都安装了最高级别的 Cryptographic Access Provider 128-bit 许可程序（5722-AC3）。
4. 在所有方案中的 iSeries 服务器上恢复（QVFYOBJRST）系统值期间验证对象签名的缺省设置为 3，且此设置未被更改。缺省设置确保在恢复已签署对象时服务器可验证对象签名。
5. iSeries A 的网络管理员必须具有 *ALLOBJ 用户概要文件特权以签署对象，或者必须将该用户概要文件授权给对象签署应用程序。
6. 系统管理员或在 DCM 中创建证书存储库的任何其他人（包括程序）都必须具有 *SECADM 和 *ALLOBJ 用户概要文件特权。
7. 系统管理员或所有其它 iSeries 服务器上的其他人必须具有 *AUDIT 用户概要文件特权才能验证对象签名。

任务步骤

必须在 iSeries A 上完成以下任务的每一项才能签署对象，如此方案所述:

1. 完成所有先决条件的步骤以安装并配置所有必需的 iSeries 产品。
2. 使用 DCM 创建证书请求以从知名的公共 “认证中心”（CA）获得对象签署证书。
3. 使用 DCM 创建对象签署应用程序定义。
4. 使用 DCM 导入已签署对象签署证书并将其指定给对象签署应用程序定义。
5. 使用 DCM 导出对象签署证书作为签名验证证书，以便客户可用它验证应用程序对象的签名。
6. 重新编写应用程序封装程序以包括签名验证证书文件，将其作为产品的一部分，并在封装它分发给客户时使用 “签署对象 API” 签署应用程序。
7. 创建安装前出口程序，该安装前出口程序使用 “添加验证方 API” 作为应用程序封装过程的一部分。此出口程序允许在产品安装期间创建 *SIGNATUREVERIFICATION 证书存储库，并向客户的 iSeries 服务器添加必需的签名验证证书。
8. 让客户在其 iSeries 服务器上使用 DCM 对 *SIGNATUREVERIFICATION 证书存储库重新设置缺省密码。

配置详细信息

如此方案所述，完成以下任务步骤以使用 OS/400 API 签署对象。

步骤 1: 完成所有先决条件的步骤

必须先完成所有先决条件任务以安装并配置所有必需的 iSeries 产品，才能执行实现此方案的特定配置任务。

步骤 2: 使用 DCM 从知名的公共 CA 获取证书

此方案假设您先前没有使用过“数字证书管理器”（DCM）来创建和管理证书。因此，必须创建 *OBJECTSIGNING 证书存储库作为创建对象签署证书过程的一部分。创建此证书存储库时，它提供创建和管理对象签署证书所需的任务。要从知名的公共“认证中心”（CA）获取证书，使用 DCM 为该证书创建标识信息和公用 — 专用密钥对，并将此信息提交到 CA 以获取证书。

要创建需要提供给知名的公共 CA 的证书请求信息，以便可获取对象签署证书，完成以下步骤:

1. 启动 DCM。
2. 在 DCM 的导航框架中，选择**创建新的证书存储库**以启动指导任务并完成一系列表单。这些表单指导您完成创建证书存储库及可用于签署对象的证书的过程。

   注: 如果对完成此指导任务中的特定表单有疑问，请选择此页面顶部的问号（**?**）以访问联机帮助。
3. 选择 ***OBJECTSIGNING** 作为要创建的证书存储库，单击**继续**。
4. 选择**是**创建证书以作为创建 *OBJECTSIGNING 证书存储库的一部分，单击**继续**。
5. 选择 **VeriSign 或其它因特网“认证中心”（CA）**作为新证书的签发者，单击**继续**以显示一个表单，供您提供该新证书的标识信息。
6. 完成该表单并单击**继续**以显示确认页面。此确认页面显示证书请求数据，您必须将其提供给将向您发出证书的公共“认证中心”（CA）。“证书签署请求”（CSR）数据包含公用密钥和为新证书指定的其它信息。
7. 仔细将 CSR 数据复制并粘贴到证书申请表或单独的文件中，申请证书时需要将其提供给公共 CA。必须使用所有 CSR 数据，包括“新证书申请”的“第一行”和“最后一行”。退出此页面时，数据将丢失且无法恢复。
8. 将应用程序的表单或文件发送给您选择的要向您发出或签署证书的 CA。
9. 等到 CA 返回了已签署的完成的证书后，继续本方案的下一个任务步骤。

步骤 3: 创建对象签署应用程序定义

将证书申请发送到知名的公共 CA 后，可使用 DCM 定义可用于签署对象的对象签署应用程序。应用程序定义不需要引用实际的应用程序；创建的应用程序定义应描述打算签署的对象的类型或组。需要该定义以便将应用程序标识与该证书关联从而启用签署过程。

要使用 DCM 创建对象签署应用程序定义，请遵循以下步骤:

1. 在导航框架中，单击**选择证书存储库**并选择 ***OBJECTSIGNING** 作为要打开的证书存储库。
2. 显示“证书存储库和密码”页面时，提供在创建证书存储库时为其指定的密码并单击**继续**。
3. 在导航框架中，选择**管理应用程序**以显示任务列表。
4. 从任务列表选择**添加应用程序**以显示用于定义应用程序的表单。
5. 完成该表单并单击**添加**。

收到从 CA 返回的已签署的证书后，可将该证书指定给创建的应用程序。

步骤 4: 导入已签署的公共证书并将其指定给对象签署应用程序

要导入证书并将其指定给应用程序以启用对象签署，请遵循以下步骤:

1. 启动 DCM。
2. 在导航框架中，单击**选择证书存储库**并选择 ***OBJECTSIGNING** 作为要打开的证书存储库。
3. 显示“证书存储库和密码”页面时，提供在创建证书存储库时为其指定的密码并单击**继续**。
4. 导航框架刷新之后，选择**管理证书**以显示任务列表。
5. 从任务列表中，选择**导入证书**以开始将已签署的证书导入至证书存储库的过程。

   注: 如果对完成此指导任务中的特定表单有疑问，请选择此页面顶部的问号（**?**）以访问联机帮助。
6. 从**管理证书**任务列表选择**指定证书**以显示当前证书存储库的证书列表。
7. 从该列表选择证书，然后单击**指定给应用程序**以显示当前证书存储库的应用程序定义列表。
8. 从该列表选择应用程序，单击**继续**。显示一个页面，它显示指定选择的确认消息，或者如果发生问题则显示错误消息。

完成此任务后，已准备好通过使用 OS/400 API 签署应用程序和其它对象。然而，为确保您及其他人能验证签名，必须将必要的证书导出到文件，并将其传送到任何安装了已签署应用程序的 iSeries 服务器。然后，客户 iSeries 服务器在安装您的应用程序时必须能使用该证书验证应用程序的签名。可使用“添加验证方 API”作为应用程序安装程序的一部分对客户执行必要的签名验证配置。例如，可创建调用“添加验证方API”的安装前出口程序以配置客户的 iSeries 服务器。

步骤 5: 导出证书以便能在其它 iSeries 服务器上启用签名验证

签署对象要求您和其他人具有一种验证签名的可靠性的手段，可使用这种手段确定是否对已签署对象进行了更改。要在签署对象的同一系统上验证对象签名，必须使用 DCM 创建 *SIGNATUREVERIFICATION 证书存储库。此证书存储库必须同时包含该对象签署证书的副本和发出该签署证书的 CA 的 CA 证书的副本。

要允许其他人验证签名，必须向其提供签署该对象的证书的副本。使用“本地认证中心”（CA）发出证书时，还必须向其提供“本地 CA”证书的副本。

要使用 DCM 以便可在签署对象的同一系统上验证签名（在此方案中为 iSeries A），请遵循以下步骤:

1. 在导航框架中，选择**创建新的证书存储库**并选择 ***SIGNATUREVERIFICATION** 作为要创建的证书存储库。
2. 选择**是**将现有对象签署证书作为签名验证证书复制到新的证书存储库中。
3. 为新的证书存储库指定密码，单击**继续**以创建证书存储库。现在可在用于签署对象的同一系统上使用 DCM 验证对象签名。

要使用 DCM 导出对象签署证书的一个副本作为签名验证证书，以便其他人可验证您的对象签名，请遵循以下步骤:

1. 在导航框架中，选择**管理证书**，然后选择**导出证书**任务。
2. 选择**对象签署**以显示可导出的对象签署证书列表。
3. 从列表选择相应的对象签署证书，单击**导出**。
4. 选择**文件，作为签名验证证书**作为目的，单击**继续**。
5. 指定导出的签名验证证书的全限定路径和文件名，单击**继续**以导出证书。

现在可将此文件添加到为产品创建的应用程序安装软件包。通过将“添加验证方 API”用作安装程序的一部分，可将此证书添加到客户的 *SIGNATUREVERIFICATION 证书存储库。如果此证书存储库尚不存在，则该 API 还将创建证书存储库。然后，在客户的 iSeries 服务器上恢复应用程序对象时产品安装程序可验证其签名。

步骤 6: 更新应用程序封装程序以使用 iSeries API 签署应用程序

将签名验证证书文件添加到应用程序软件包后，在将产品库封装以用于客户分发时可使用“签署对象 API”编写或编辑现有的应用程序以对产品库进行签署。

为帮助您更深入地了解如何将“签署对象 API”用作应用程序封装程序的一部分，查看以下代码示例。此示例代码片断以 C 编写，它不是完整的签署和封装程序，而是调用该“签署对象 API”的程序的部分示例。如果选择使用此程序示例，请更改它以符合您的特定需要。由于安全性的原因，IBM 建议您将程序示例个性化，而不要使用提供的缺省值。

注: IBM 授予您使用所有编程代码示例的非专有版权许可证，您可由此生成相似的定制功能以满足您特定的需要。IBM 提供所有样本代码只是出于解释的目的。并未在所有环境下完全测试这些示例。因此，IBM 不保证或暗示这些程序的可靠性、可服务性和功能。本文档中包含的所有程序是以“按现状”的基础提供的，不附有任何形式的保证。明示的不保证声明包括非侵权性、适销性和适用于某特定用途的默示保证。

更改此代码片断以符合您的需要，以将“签署对象 API”用作应用程序产品封装程序的一部分。需要将两个参数发送到此程序: 要签署的库的名称和对象签署应用程序标识的名称; 应用程序标识区分大小写，库名称不区分大小写。如果将几个库用作要签署的产品的一部分，您编写的程序可数次调用此片段。

```
/* ------------------------------------------------------------ */
/*                                                              */
/* COPYRIGHT (C) IBM CORP. 2002                                 */
/*                                                              */
/* Use Sign Object API to sign one or more libraries            */
/*                                                              */
/* The API will digitally sign all objects in a specified library   */
/*                                                              */
/*                                                              */
/*                                                              */
/* This material contains programming source code for your      */
/* consideration.  This example has not been thoroughly         */
/* tested under all conditions.  IBM, therefore, cannot         */
/* guarantee or imply reliability, serviceability, or function  */
/* of these programs.  All programs contained herein are        */
/* provided to you "AS IS".  THE IMPLIED WARRANTIES OF          */
/* MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE     */
/* ARE EXPRESSLY DISCLAIMED.  IBM provides no program services for  */
/* these programs and files.                                    */
/*                                                              */
/*                                                              */
/*                                                              */
/* The parameters are:                                          */
/*                                                              */
/*  char *   name of the library to sign                        */
/*  char *   name of the application ID                         */
/*                                                              */

#include <qydosgno.h>
#include <stdlib.h>
#include <stdio.h>
#include <string.h>

int main (int argc, char *argv[])
{

    /* parameters:
```

```
   char * library to sign objects in,
   char * application identifier to sign with

 */

int         lib_length, applid_length, path_length, multiobj_length;
Qus_EC_t    error_code;
char        libname[11];
char        path_name[256];

Qydo_Multi_Objects_T * multi_objects = NULL;
multiobj_length = 0;
error_code.Bytes_Provided = 0;    /* return exceptions for any errors */


/* ------------------------------------ */
/* construct path name given library name */
/* ------------------------------------ */
memset(libname, '\00', 11); /* initialize library name */
for(lib_length = 0;
    ((*(argv[1] + lib_length) != ' ') &&
     (*(argv[1] + lib_length) != '\00'));
    lib_length++);
memcpy(argv[1], libname, lib_length); /* fill in library name */

/* build path name parm for API call */
sprintf(path_name, "/QSYS.LIB/%s.LIB/*", libname);
path_length = strlen(path_name);

/* ---------------------------- */
/* find length of application id */
/* ---------------------------- */
for(applid_length = 0;
    ((*(argv[2] + applid_length) != ' ') &&
     (*(argv[2] + applid_length) != '\00'));
    applid_length++);

/* ------------------------------- */
/* sign all objects in this library */
/* ------------------------------- */
QYDOSGNO  (path_name,             /* path name to object         */
           &path_length,          /* length of path name         */
           "OBJN0100",            /* format name                 */
           argv[2],               /* application identifier (ID) */
           &applid_length,        /* length of  application ID   */
           "1",                   /* replace duplicate signature */
           multi_objects,         /* how to handle multiple
                                        objects                */
           &multiobj_length,      /* length of multiple objects
                                     structure to use
                                    (0=no mult.object structure)*/
           &error_code);          /* error code                  */



   return 0;

}
```

步骤 7: 创建使用“添加验证方 API”的安装前出口程序

有了签署应用程序的程序化过程后，可将“添加验证方 API”用作安装程序的一部分来创建最终产品以供分发。例如，可将“添加验证方 API”用作安装前出口程序的一部分以确保在恢复已签署应用程序对象之前将证书添加到证书存储库。它允许在客户的 iSeries 服务器上恢复应用程序对象时，安装程序验证应用程序对象的签名。

注: 由于安全性原因，此 API 不允许将“认证中心”（CA）证书插入 *SIGNATUREVERIFICATION 证书存储库。向证书存储库添加 CA 证书时，系统将该 CA 看作可信的证书源。因此，系统认为该 CA 发出的证书来自可信的源。所以，不能使用该 API 创建安装出口程序将 CA 证书插入证书存储库。必须使用“数字证书管理器”向证书存储库添加 CA 证书以确保他人必须专门并手工控制系统信任哪些 CA。这样将防止发生系统从管理员没有特意指定为可信的源导入证书的可能性。

如果要防止任何人在您不知道的情况下使用此 API 向 *SIGNATUREVERIFICATION 证书存储库添加验证证书，则您应考虑在系统上禁用此 API。可通过使用“系统服务工具”（SST）禁止更改与安全性相关的系统值来完成此操作。

为帮助您更深入地了解如何将“添加验证方 API”用作应用程序安装程序的一部分，查看以下安装前出口程序代码示例。此示例代码片断以 C 编写，它不是完整的安装前出口程序，而是调用该“添加验证方 API”的程序的部分示例。如果选择使用此程序示例，则更改它以符合您的特定需要。由于安全性原因，IBM 建议您个性化程序示例，而不要使用提供的缺省值。

注: IBM 授予您使用所有编程代码示例的非专有版权许可证的权利，您可由此生成相似的定制功能以满足您特定的需要。IBM 提供所有样本代码只是出于解释的目的。并未在所有环境下完全测试这些示例。因此，IBM 不保证或暗示这些程序的可靠性、可服务性或者功能。本文档中包含的所有程序是以“按现状”的基础提供的，不附有任何形式的保证。明示的不保证声明包括非侵权性、适销性和适用于某特定用途的默示保证。

更改此代码片断以符合将“添加验证方 API”用作安装前出口程序的一部分的需要，以在他们安装产品时将必需的签名验证证书添加到客户的 iSeries 服务器。

```
/* ---------------------------------------------------------------- */
/*                                                                  */
/* COPYRIGHT (C) IBM CORP. 2002                                     */
/*                                                                  */
/* Use Add Verifier API to add a certificate in the specified       */
/* IFS file to the *SIGNATUREVERIFICATION certificate store.        */
/*                                                                  */
/* The API will create the certificate store if it does not exist.  */
/* If the certificate store is created it will be given a default   */
/* password that should be changed using DCM as soon as possible.   */
/* This warning needs to be given to the owners of the system that  */
/* use this program.                                                */
/*                                                                  */
/*                                                                  */
/*                                                                  */
/* This material contains programming source code for your          */
/* consideration.  This example has not been thoroughly             */
/* tested under all conditions.  IBM, therefore, cannot             */
/* guarantee or imply reliability, serviceability, or function      */
/* of these programs.  All programs contained herein are            */
/* provided to you "AS IS".  THE IMPLIED WARRANTIES OF              */
/* MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE         */
/* ARE EXPRESSLY DISCLAIMED.  IBM provides no program services for  */
/* these programs and files.                                        */
/*                                                                  */
/*                                                                  */
/*                                                                  */
/* The parameters are:                                              */
/*                                                                  */
/*  char *   path name to IFS file that holds the certificate       */
/*  char *   certificate label to give certificate                  */
/*                                                                  */
/*                                                                  */
/*                                                                  */
/* ---------------------------------------------------------------- */
```

```
#include <qydoadd1.h>
#include <stdlib.h>
#include <string.h>

int main (int argc, char *argv[])
{

    int         pathname_length, cert_label_length;
    Qus_EC_t    error_code;
    char      * pathname = argv[1];
    char      * certlabel = argv[2];

    /* find length of path name */
    for(pathname_length = 0;
        ((*(pathname + pathname_length) != ' ') &&
         (*(pathname + pathname_length) != '\00'));
        pathname_length++);

    /* find length of certificate label */
    for(cert_label_length = 0;
        ((*(certlabel + cert_label_length) != ' ') &&
         (*(certlabel + cert_label_length) != '\00'));
        cert_label_length++);


    error_code.Bytes_Provided = 0;     /* return exceptions for any errors  */

    QydoAddVerifier (pathname,         /* path name to file with certificate*/
                     &pathname_length, /* length of path name               */
                     "OBJN0100",       /* format name                       */
                     certlabel,        /* certificate label                 */
                     &cert_label_length, /* length of certificate label     */
                     &error_code);     /* error code                        */

    return 0;
}
```

完成这些任务后，可封装应用程序并将其分发给客户。客户安装应用程序时，将已签署应用程序对象作为安装过程的一部分对它进行验证。以后，客户可使用“数字证书管理器”（DCM）验证应用程序对象签名。它允许客户确定应用程序的源是否可信，并确定应用程序自签署以来是否被更改过。

注：安装程序可能已为客户用缺省密码创建了 *SIGNATUREVERIFICATION 证书存储库。您应建议客户应尽快使用 DCM 重新设置证书存储库的密码以保护证书存储库不受未经授权的访问。

步骤 8：让客户重新设置 *SIGNATUREVERIFICATION 证书存储库的缺省密码

“添加验证方 API”可能已在客户的 iSeries 服务器上创建了 *SIGNATUREVERIFICATION 证书存储库作为产品安装过程的一部分。如果该 API 创建了证书存储库，则它也创建了证书存储库的缺省密码。因此，应建议客户使用 DCM 重新设置此密码以保护证书存储库不受未授权的访问。

让客户完成以下步骤以重新设置 *SIGNATUREVERIFICATION 证书存储库密码:

1. 启动 DCM。
2. 在导航框架中，单击**选择证书存储库**，并选择 ***SIGNATUREVERIFICATION** 作为要打开的证书存储库。
3. 显示“证书存储库和密码”页面时，单击**重新设置密码**以显示“重新设置证书存储库密码”页面。

   注：如果对完成此指导任务中的特定表单有疑问，请选择该页面顶部的问号（**?**）以访问联机帮助。
4. 为存储库指定新密码、重新输入以确认新密码以及选择证书存储库的密码到期策略，单击**继续**。

方案: 使用“中央管理”签署对象

情况

您的公司（MyCo 公司）开发应用程序，分发到公司内多个位置的多台 iSeries 服务器。作为网络管理员，您负责确保在公司的所有 iSeries 服务器上安装和更新这些应用程序。您目前使用“iSeries 导航器”的中央管理功能以便更容易地封装并分发这些应用程序，以及执行您负责的其它管理任务。然而，您查找并更正这些应用程序问题所花费的时间比预想的要多得多，因为存在对这些对象的未授权更改。因此，您希望通过数字化签署这些对象以更好地保护它们的完整性。

您研究了 OS/400 对象签署功能，并了解到从 V5R2 开始，“中央管理”允许在封装和分发对象时签署对象。通过使用“中央管理”，可有效并相对容易地达到公司的安全性目标。您还决定创建“本地认证中心”（CA），并使用它发出签署对象的证书。使用“本地 CA”发出的证书进行对象签署可减少使用此安全性技术的花费，因为不必从知名的公共 CA 购买证书。

此示例介绍对分发到公司多台 iSeries 服务器的应用程序配置和使用对象签署时涉及的步骤。

方案的优点

此方案具有以下优点:

- 使用“中央管理”封装并签署对象，可减少将已签署对象分发到公司的 iSeries 服务器必须花费的时间。
- 使用“中央管理”签署软件包中的对象可减少签署对象必须执行的步骤，因为签署过程是封装过程的一部分。
- 签署对象软件包允许您更容易地确定对象自签署以来是否被更改过。这样可减少将来为查找应用程序问题而需要做的一些故障诊断。
- 使用“本地认证中心”（CA）发出的证书签署对象，使签署对象以更低的成本实现。

目的

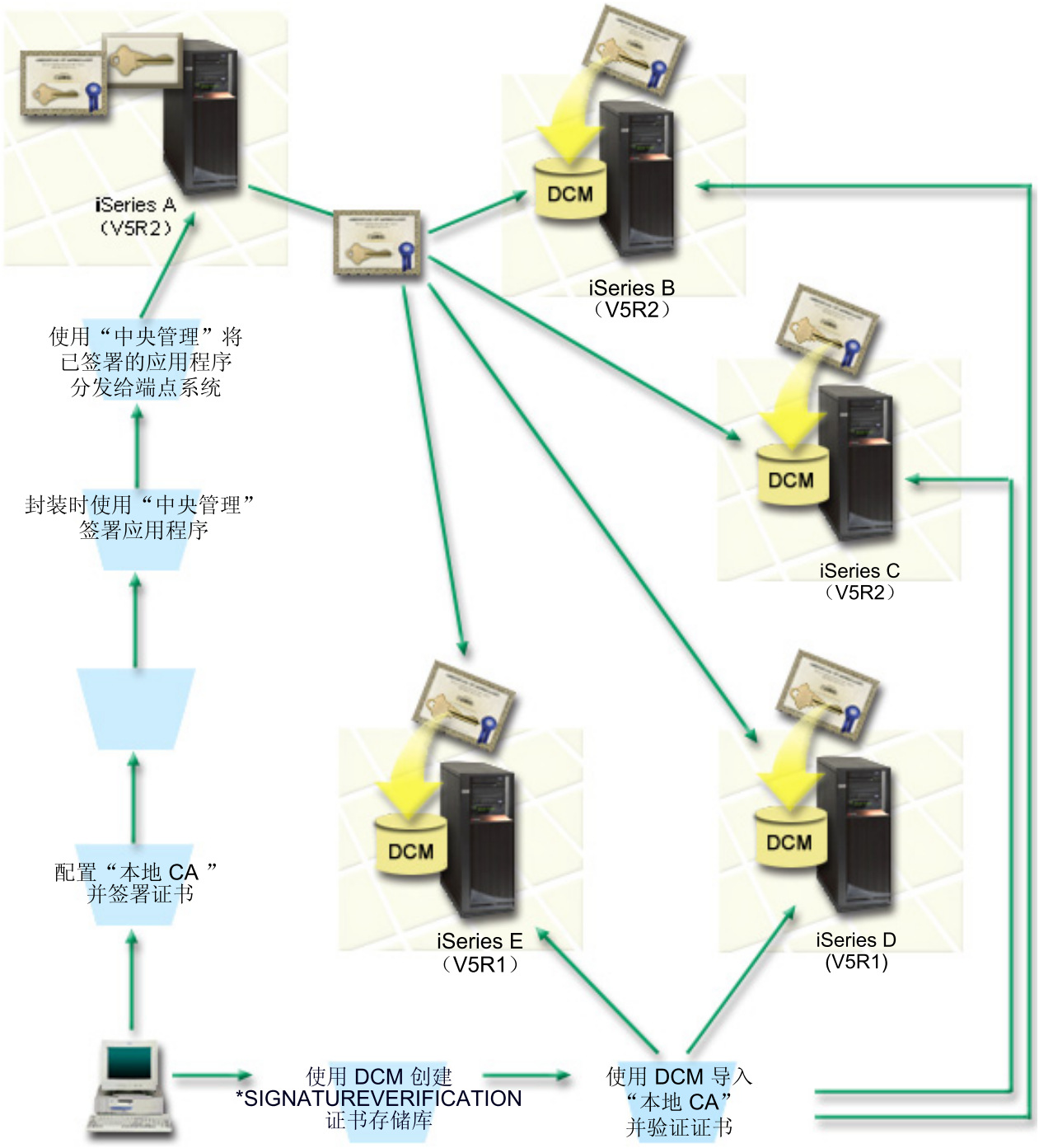
在此方案中，MyCo 公司希望数字化签署将分发到公司内多台 iSeries 服务器的应用程序。作为 MyCo 公司的网络管理员，您已经对许多 iSeries 管理任务使用“中央管理”。因此，您希望将“中央管理”当前的使用延伸到签署分发给其它 iSeries 服务器的公司应用程序。

此方案的目的如下所述:

- 必须用“本地 CA”发出的证书签署公司应用程序以限制签署应用程序的成本。
- 系统管理员和其他指定的用户必须能够较容易地在所有 iSeries 服务器上验证数字签名，以验证公司已签署对象的源及其可靠性。为实现此目标，在每个服务器的 *SIGNATUREVERIFICATION 证书存储库中，每个 iSeries 服务器必须同时拥有公司签名验证证书和“本地认证中心”（CA）证书的副本。
- 验证公司应用程序签名允许 iSeries 管理员和其他人检测自对象签署以来其内容是否被更改。
- 管理员必须能使用“中央管理”封装、签署他们的应用程序，然后将这些应用程序分发给其 iSeries 服务器。

详细信息

下图演示实现此方案的对象签署和签名验证过程:



该图演示与此方案相关的以下几点:

中央系统（iSeries A）

- iSeries A 运行 OS/400 版本 5 发行版 2（V5R2）。
- iSeries A 用作运行“中央管理”功能的中央系统，包括封装和分发公司应用程序。
- iSeries A 安装了 Cryptographic Access Provider 128-bit for iSeries（5722–AC3）。
- iSeries A 安装并配置了“数字证书管理器”（OS/400 选项 34）和 IBM HTTP Server（5722–DG1）。
- iSeries A 充当“本地认证中心”（CA），且对象签署证书驻留在此系统上。

- iSeries A 是公司应用程序的主要对象签署系统。在 iSeries A 上通过执行以下任务完成对客户分发的产品对象签署:
  1. 使用 DCM 创建“本地 CA”并使用“本地 CA”创建对象签署证书。
  2. 使用 DCM 将“本地 CA”证书的副本和签名验证证书导出到文件中，以便端点系统（iSeries B、C、D 和 E）可验证已签署对象。
  3. 使用“中央管理”签署应用程序对象并将其与验证证书文件封装在一起。
  4. 使用“中央管理”将已签署应用程序和证书文件分发给端点系统。

端点系统（iSeries 服务器 B、C、D 和 E）

- iSeries B 和 C 运行 OS/400 版本 5 发行版 2（V5R2）。
- iSeries D 和 E 运行 OS/400 版本 5 发行版 1（V5R1）。
- iSeries B、C、D 和 E 安装并配置了“数字证书证书管理器”（选项 34）和 IBM HTTP Server（5722–DG1）。
- iSeries B、C、D 和 E 在系统接收已签署应用程序时从中央系统（iSeries A）接收公司的签名验证证书和“本地 CA”的一个副本。
- 使用 DCM 创建 *SIGNATUREVERIFICATION 证书存储库并将“本地 CA”和验证证书导入此证书存储库中。

先决条件和假设

此方案取决于以下的先决条件和假设:

1. 所有 iSeries 服务器都满足安装和使用“数字证书管理器”（DCM）的要求。
2. 在任何一台 iSeries 服务器上，先前没有人配置或使用过 DCM。
3. iSeries A 满足安装和使用“iSeries 导航器”和“中央管理”的要求。
4. 所有 iSeries 端点系统必须运行“中央管理”服务器。
5. 所有 iSeries 服务器都安装了最高级别的 Cryptographic Access Provider 128-bit 许可程序（5722-AC3）。
6. 在所有方案 iSeries 服务器上恢复（QVFYOBJRST）系统值期间验证对象签名的缺省设置为 3，且此设置未被更改。缺省设置确保服务器在恢复已签署对象时可验证对象签名。
7. iSeries A 的网络管理员必须具有 *ALLOBJ 用户概要文件特权来签署对象，或者必须将该用户概要文件授权给对象签署应用程序。
8. 网络管理员或在 DCM 中创建证书存储库的任何其他人必须具有 *SECADM 和 *ALLOBJ 用户概要文件特权。
9. 系统管理员或所有其它 iSeries 服务器上的其他人必须具有 *AUDIT 用户概要文件特权才能验证对象签名。

任务步骤

有两组任务，必须完成才能实现此方案: 一组任务允许设置 iSeries A 以使用“中央管理”签署和分发应用程序。另一组任务允许系统管理员和其他人在所有其它 iSeries 服务器上验证这些应用程序的签名。

对象签署任务步骤

必须在 iSeries A 上完成这些任务中的每一个任务才能签署对象，如此方案所述:

1. 完成所有先决条件的步骤以安装并配置所有必需的 iSeries 产品。
2. 使用“数字证书管理器”（DCM）创建“本地认证中心”（CA）以发出专用对象签署证书。

3. 使用 DCM 创建应用程序定义。
4. 使用 DCM 指定证书给对象签署应用程序定义。
5. 使用 DCM 导出证书，这些证书是其它系统验证对象签名必须使用的证书。必须同时将“本地 CA”证书的副本和对象签署证书的副本作为签名验证证书导出到文件中。
6. 传送证书文件至打算在其上验证签名的每个 iSeries 端点系统。
7. 使用“中央管理”签署应用程序对象。

签名验证任务步骤

应在每个 iSeries 端点系统上先完成这些签名验证配置任务，才能使用“中央管理”将已签署应用程序对象传送给它们。必须先完成签名验证配置，才能在端点系统上恢复已签署对象时成功地验证签名。

在每个 iSeries 端点系统上，必须完成这些任务才能验证对象签名，如此方案所述:

8. 使用“数字证书管理器”（DCM）创建 *SIGNATUREVERIFICATION 证书存储库。
9. 使用 DCM 导入“本地 CA”证书和签名验证证书。

配置详细信息

如此方案所述，完成以下任务步骤来配置“中央管理”用于对象签署。

步骤 1: 完成所有先决条件的步骤

必须完成所有先决条件任务以安装并配置所有必需的 iSeries 产品，才能执行实现此方案的特定配置任务。

步骤 2: 创建“本地认证中心”以发出专用对象签署证书

使用“数字证书管理器”（DCM）创建“本地认证中心”（CA）时，该过程需要您完成一系列表单。这些表单可指导您完成创建 CA 的过程以及完成开始将数字证书用于“安全套接字层”（SSL）、对象签署和签名验证所必需的其它任务的过程。虽然在此方案中不必对 SSL 配置证书，但必须完成该项任务中的所有表单来配置系统用于签署对象。

要使用 DCM 创建并操作“本地 CA”，请遵循以下步骤:

1. 启动 DCM。
2. 在 DCM 的导航框架中，选择**创建认证中心（CA）**以显示一系列表单。

   注: 如果对完成此指导任务中的特定表单有疑问，选择此页面顶部的问号（**?**）按钮以访问联机帮助。
3. 完成此指导任务的所有表单。执行此任务时，务必执行以下操作:
   a. 提供“本地 CA”的标识信息。
   b. 在浏览器中安装“本地 CA”证书以便软件可识别“本地 CA”并确认该“本地 CA”发出的证书。
   c. 指定“本地 CA”的策略数据。
   d. 使用新的“本地 CA”发出应用程序可用于 SSL 连接的服务器或客户机证书。

      注: 虽然此方案没有使用此证书，但必须创建它才能使用“本地 CA”发出所需的对象签署证书。如果取消任务而不创建此证书，必须分别创建对象签署证书及存储该证书的 *OBJECTSIGNING 证书存储库。
   e. 选择可使用服务器或客户机证书进行 SSL 连接的应用程序。

      注: 对于此方案，不要选择任何应用程序，单击**继续**以显示下一个表单。

f. 使用新的“本地 CA”发出应用程序可用于数字化签署对象的对象签署证书。此子任务创建 *OBJECTSIGNING 证书存储库。它是用于管理对象签署证书的证书存储库。

g. 选择应信任“本地 CA”的应用程序。

注: 对于此方案，不要选择任何应用程序，单击**继续**以完成任务。

创建了“本地 CA”和对象签署证书后，必须定义使用该证书的对象签署应用程序才能签署对象。

步骤 3: 创建对象签署应用程序定义

创建对象签署证书之后，必须使用“数字证书管理器”（DCM）定义可用于签署对象的对象签署应用程序。应用程序定义不需要引用实际的应用程序；创建的应用程序定义应描述打算签署的对象的类型或组。需要该定义以便将应用程序标识与该证书关联从而启用签署过程。

要使用 DCM 创建对象签署应用程序定义，执行以下步骤:

1. 在导航框架中，单击**选择证书存储库**并选择 ***OBJECTSIGNING** 作为要打开的证书存储库。
2. 显示“证书存储库和密码”页面时，提供在创建证书存储库时为其指定的密码并单击**继续**。
3. 在导航框架中，选择**管理应用程序**显示任务列表。
4. 从任务列表选择**添加应用程序**以显示定义应用程序的表单。
5. 完成该表单并单击**添加**。

现在必须为创建的应用程序指定对象签署证书。

步骤 4: 为对象签署应用程序定义指定证书

要为对象签署应用程序指定证书，请遵循以下步骤:

1. 在 DCM 导航框架中，选择**管理证书**以显示任务列表。
2. 从任务列表中，选择**指定证书**以显示当前证书存储库的证书列表。
3. 从该列表选择证书，然后单击**指定给应用程序**以显示当前证书存储库的应用程序定义列表。
4. 从列表选择一个或多个应用程序，单击**继续**。显示一个消息页面，确认证书指定，或者如果发生问题则提供错误信息。

完成此任务后，已准备好在封装和分发对象时使用“中央管理”签署对象。然而，为确保您及其他人能验证签名，必须将必要的证书导出到文件，并将其传送至所有 iSeries 端点系统。还必须先在每个 iSeries 端点系统上完成所有签名验证配置任务，才能使用“中央管理”将已签署应用程序对象传送给它们。必须先完成签名验证配置，才能在端点系统上恢复已签署对象时成功地验证签名。

步骤 5: 导出证书以便可在其它 iSeries 系统上验证签名

为保护内容的完整性签署对象需要您及其他人都具有验证签名的可靠性的手段。要在签署对象的同一系统上验证对象签名，必须使用 DCM 创建 *SIGNATUREVERIFICATION 证书存储库。此证书存储库必须同时包含该对象签署证书的副本和发出该签署证书的 CA 的 CA 证书的副本。

要允许其他人验证签名，必须向其提供签署该对象的证书的副本。使用“本地认证中心”（CA）发出证书时，还必须为其提供“本地 CA”证书的副本。

要使用 DCM 以便可在签署对象的同一系统（在此方案中为 iSeries A）上验证签名，请遵循以下步骤:

1. 在导航框架中，选择**创建新的证书存储库**并选择 ***SIGNATUREVERIFICATION** 作为要创建的证书存储库。

2. 选择**是**将现有对象签署证书作为签名验证证书复制到新的证书存储库。
3. 为新的证书存储库指定密码，单击**继续**以创建证书存储库。现在可在用于签署对象的同一系统上使用 DCM 验证对象签名。

要使用 DCM 导出“本地 CA”证书的副本及对象签署证书的副本作为签名验证证书，以便可在其它系统上验证对象签名，请遵循以下步骤:

1. 在导航框架中，选择**管理证书**，然后选择**导出证书**任务。
2. 选择**认证中心（CA）**，单击**继续**以显示可导出的 CA 证书的列表。
3. 从列表选择较早时创建的“本地 CA”证书，单击**导出**。
4. 指定**文件**作为导出目的，单击**继续**。
5. 指定导出的“本地 CA”证书的全限定路径和文件名，单击**继续**以导出证书。
6. 单击**确定**以退出“导出确认”页面。现在可导出对象签署证书的副本。
7. 重新选择**导出证书**任务。
8. 选择**对象签署**以显示可导出的对象签署证书列表。
9. 从列表选择相应的对象签署证书，单击**导出**。
10. 选择**文件，作为签名验证证书**作为目的，单击**继续**。
11. 指定导出的签名验证证书的全限定路径和文件名，单击**继续**导出证书。

现在可将这些文件传送到打算在其上验证用该证书创建的签名的 iSeries 端点系统。

步骤 6: 将证书文件传送至 iSeries 端点系统

必须将在 iSeries A 上创建的证书文件传送至此方案中的 iSeries 端点系统，才能配置它们以验证您签署的对象。可使用几种不同的方法传送证书文件。例如，可使用“文件传输协议”（FTP）或“中央管理”软件包分发来传送文件。

步骤 7: 使用“中央管理”签署对象

“中央管理”的对象签署过程是软件封装分发过程的一部分。必须在每个 iSeries 端点系统上先完成所有签名验证配置任务，才能使用“中央管理”将已签署应用程序对象传送给它们。必须先完成签名验证配置，才能在端点系统上恢复已签署对象时成功地验证签名。

要如此方案所述，签署分发至 iSeries 端点系统的应用程序，请遵循以下步骤:

1. 使用“中央管理”封装和分发软件产品。
2. 进入**产品定义**向导的**标识**面板时，单击**高级**显示**高级标识**面板。
3. 在**数字签署**字段中，输入较早时创建的对象签署应用程序的应用程序标识，单击**确定**。
4. 完成向导并继续到该过程以使用“中央管理”封装和分发软件产品。

步骤 8: 签名验证任务: 在 iSeries 端点系统上创建 *SIGNATUREVERIFICATION 证书存储库

要在此方案中的 iSeries 端点系统上验证对象签名，每个系统在 *SIGNATUREVERIFICATION 证书存储库中必须有相应的签名验证证书的副本。如果专用证书签署了对象，此证书存储库中也必须包含“本地 CA”证书的副本。

要创建 *SIGNATUREVERIFICATION 证书存储库，请遵循以下步骤:

1. 启动 DCM。
2. 在“数字证书管理器”（DCM）导航框架中，选择**创建新的证书存储库**并选择 ***SIGNATUREVERIFICATION** 作为要创建的证书存储库。

   注: 如果对完成此指导任务中的特定表单有疑问，请选择此页面顶部的问号（**?**）以访问联机帮助。
3. 为新的证书存储库指定密码，单击**继续**创建证书存储库。现在可将证书导入存储库并使用其验证对象签名。

步骤 9: 签名验证任务: 导入证书

要验证对象的签名，*SIGNATUREVERIFICATION 存储库必须包含签名验证证书的副本。如果签署证书是专用的，此证书存储库还必须有发出该签署证书的“本地认证中心”（CA）证书的副本。在此方案中，已将两个证书都导出到一个文件中，并将该文件传送到每个 iSeries 端点系统。

要将这些证书导入 *SIGNATUREVERIFICATION 存储库中，请遵循以下步骤:

1. 在 DCM 导航框架中，单击**选择证书存储库**，并选择 ***SIGNATUREVERIFICATION** 作为要打开的证书。
2. 显示“证书存储库和密码”页面时，提供在创建证书存储库时为其指定的密码并单击**继续**。
3. 导航框架刷新之后，选择**管理证书**显示任务列表。
4. 从任务列表中，选择**导入证书**。
5. 选择**认证中心（CA）**作为证书类型，单击**继续**。

   注: 在导入专用签名验证证书之前必须先导入“本地 CA”证书；否则签名验证证书的导入过程将失败。
6. 指定 CA 证书文件的全限定路径和文件名，单击**继续**。显示一个消息，确认导入过程成功，或者如果该过程失败则提供错误信息。
7. 重新选择**导入证书**任务。
8. 选择**签名验证**作为要导入的证书类型，单击**继续**。
9. 指定签名验证证书文件的全限定路径和文件名，单击**继续**。显示一个消息，确认导入过程成功，或者如果该过程失败则提供错误信息。

您的 iSeries 系统现在可在恢复已签署对象时验证用相应的签署证书创建的对象签名。

对象签署概念

开始使用 iSeries 对象签署和签名验证功能之前，您可能会发现查看以下一些概念很有帮助:

数字签名
了解什么是数字签名以及它们可提供哪些保护。

可签署的对象
了解可签署哪些 iSeries 对象以及有关命令（*CMD）对象签名选项。

对象签署处理
了解签署对象过程如何工作以及可为该过程设置哪些参数。

签名验证处理
了解验证对象签名的工作过程以及可为该过程设置哪些参数。

数字签名

OS/400 提供对使用数字证书数字化地“签署”对象的支持。对象的数字签名使用某种形式的密码术创建，它象书面文档上的个人签名。数字签名提供对象来源的证明以及用以验证对象完整性的手段。数字证书的所有者使用该证书的专用密钥“签署”对象。该对象的接收方使用证书的相应公用密钥解密签名，这样将验证已签署对象的完整性并验证发送方是不是对象的源。

对象签署支持增加了传统的 iSeries 服务器工具以控制谁能更改对象。传统的控制不能保护对象通过因特网或其它不可信任的网络传送时不受未授权的篡改。因为您可检测自对象签署以来其内容是否被更改过，万一遇到此类情况您可以更容易地确定是否信任所获得的对象。

数字签名是对象中数据的加密数学摘要。数字签名并不将对象及其内容加密并使其成为专用；然而，该摘要自身是加密的，以防止对其进行未授权的更改。希望确保对象在传送过程中没有被更改及对象源自可接受的合法源的任何人，都可使用签署证书的公用密钥验证原始数字签名。如果签名不再匹配，则数据可能已被修改。在这种情况下，接收方可以避免使用该对象，并联系签发者以获得已签署对象的另一个副本。

对象签名代表签署该对象的系统，而不是该系统上的特定用户（虽然用户必须具有适当的权限才能使用证书签署对象）。

如果决定使用数字签名来满足您的安全性需要和策略，应评估应使用公共证书还是发出本地证书。如果打算将对象分发给一般公众用户，应考虑使用知名的公共“认证中心”（CA）的证书来签署对象。使用公共证书确保其他人能容易且廉价地验证您在分发给他们的对象上的签名。然而，如果打算只在您的组织内分发对象，应使用数字证书管理器（DCM）来操作您自己的“本地 CA”以发出签署对象的证书。使用“本地 CA”的专用证书签署对象比从知名的公共 CA 购买证书花费要少。

数字签名类型

从 V5R2 开始，可签署命令（*CMD）对象；也可选择 *CMD 对象的两种类型签名中的一种：核心对象签名或全部对象签名。

- **全部对象签名**
  此类型的签名涉及除对象的少数不必要的字节以外的所有内容。
- **核心对象签名**
  此类型的签名涉及 *CMD 对象的基本字节。然而，签名不涉及那些较频繁更改的字节。此类型的签名允许对命令进行一些更改而不会使签名无效。核心对象签名不涉及哪些字节根据特定的 *CMD 对象而异；例如，核心签名不涉及 *CMD 对象的参数缺省值。不会使核心对象签名无效的更改的示例包括:
  - 更改命令缺省值。
  - 向没有有效性检查程序的命令添加有效性检查程序。
  - 更改“允许运行的位置”参数。
  - 更改“允许有限的用户”参数。

要了解有关可签署哪些 iSeries 对象以及核心对象签名涉及 *CMD 对象的哪些字节的更多信息，参阅可签署的对象。

可签署的对象

您可数字化地签署多种 OS/400 对象类型，而不管签署它们所使用的方法。可签署在系统的集成文件系统中存储的任何对象（*STMF），存储在库中的对象除外。如果对象有附加的 Java™ 程序，则也将签署该程序。只能签署 QSYS.LIB 文件系统中的这些对象：程序（*PGM）、服务程序（*SRVPGM）、模块（*MODULE）、SQL 程序包（*SQLPKG）、*FILE（仅保存文件）和命令（*CMD）。

要签署对象，它必须驻留在本地系统上。例如，如果在 Integrated xSeries Server for iSeries 上操作 Windows® 2000 服务器，应在集成文件系统中使 QNTC 文件系统可用。认为此文件系统中的目录不是本地的，因为它们包含属于 Windows 2000 操作系统的文件。另外，不能签署空对象或为 V5R1 之前的发行版编译的对象。

命令（*CMD）对象签名

签署 *CMD 对象时，可选择两种签名类型中的一种应用于该 *CMD 对象。可选择任一个签署整个对象，或者只签署对象的核心部分。选择签署整个对象时，该签名应用于该对象的所有字节，少数不必要的字节除外。全部对象签名涉及核心对象签名中包含的项。

在选择只签署核心对象时，签名将保护必要的字节，而不签署较经常更改的字节。不签署哪些字节根据 *CMD 对象而异，但可包括这样一些字节，它们确定对象有效的方式或确定允许对象在哪里运行，以及其它。例如，核心签名不涉及 *CMD 对象的参数缺省值。此类型的签名允许对命令进行一些更改而不会使签名无效。有关不会使这些类型的签名无效的更改的示例包括:

- 更改命令缺省值。
- 向没有有效性检验程序的命令添加有效性检验程序。
- 更改“允许运行的位置”参数。
- 更改“允许有限的用户”参数。

下表准确描述了将 *CMD 对象中哪些字节包括为核心对象签名的一部分。

*CMD 对象的核心对象签名的组合

对象的一部分	与核心对象签名的关系
由 CHGCMDDFT 更改的命令缺省值	不是核心对象签名的一部分
处理命令和库的程序	总是包括为核心对象签名的一部分
REXX 源文件和库	如果在签署时对该命令指定则包括，否则不是核心对象签名的一部分
REXX 源成员	如果在签署时对该命令指定则包括，否则不是核心对象签名的一部分
REXX 命令环境和库	如果在签署时对该命令指定则包括，否则不是核心对象签名的一部分
REXX 出口程序名称、库和出口代码	如果在签署时对该命令指定则包括，否则不是核心对象签名的一部分
有效性检验程序和库	如果在签署时对该命令指定则包括，否则不是核心对象签名的一部分
有效的方式	不是核心对象签名的一部分
允许运行的位置	不是核心对象签名的一部分
允许有限的用户	不是核心对象签名的一部分
帮助书架	如果在签署时对该命令指定则包括，否则不是核心对象签名的一部分
帮助屏面组和库	如果在签署时对该命令指定则包括，否则不是核心对象签名的一部分
帮助标识符	如果在签署时对该命令指定则包括，否则不是核心对象签名的一部分
帮助搜索索引和库	如果在签署时对该命令指定则包括，否则不是核心对象签名的一部分

对象的一部分	与核心对象签名的关系
当前库	如果在签署时对该命令指定则包括，否则不是核心对象签名的一部分
产品库	如果在签署时对该命令指定则包括，否则不是核心对象签名的一部分
提示覆盖程序和库	如果在签署时对该命令指定则包括，否则不是核心对象签名的一部分
文本（描述）	不属于核心对象签名或全部对象签名的一部分，因为它没有存储在对象中
启用图形用户界面（GUI）	不是核心对象签名的一部分

对象签署处理

签署对象时可对对象签署处理指定以下选项。

- **错误处理**
  可指定在对多个对象创建签名时应用程序应使用哪种类型的错误处理。可指定在错误发生时应用程序是停止签署对象还是继续签署该过程中的任何其它对象。
- **重复对象签名**
  可指定在应用程序重新签署对象时应如何处理签署过程。可指定是保留原始的签名不变，还是用新的签名替换原始的签名。
- **子目录中的对象**
  可指定应用程序应如何处理子目录中的签署对象。可指定应用程序签署任何子目录中的个别对象，或者指定应用程序只签署主目录中的那些对象而忽略所有子目录。
- **对象签名的作用域**
  在签署 *CMD 对象时，可指定是签署整个对象还是只签署对象的核心部分。

签名验证处理

可为签名验证处理指定以下选项。

- **错误处理**
  可指定在验证多个对象的签名时应用程序应使用哪种类型的错误处理。可指定在错误发生时应用程序是停止验证签名，还是继续验证该过程中的任何其它对象的签名。
- **子目录中的对象**
  可指定应用程序应如何处理子目录对象的验证签名。可指定应用程序验证任何子目录中的个别对象的签名，或者应用程序只验证主目录内的那些对象的签名而忽略所有子目录。
- **核心签名验证与整个签名验证**
  有一些系统规则确定在验证过程期间系统应如何处理对象的核心签名与整个签名。这些规则如下所述:
  - 如果对象没有签名，则验证过程报告对象未签署，并继续验证该过程中的任何其它对象。
  - 如果对象由系统可信的源（IBM）签署，则签名必须匹配，否则验证过程失败。如果签名匹配，则验证过程继续。签名是对象中数据的加密数学摘要；因此，如果验证期间对象中的数据与签署时对象中的数据相匹配，则认为签名匹配。
  - 如果对象有任何可信的全部对象签名（根据 *SIGNATUREVERIFICATION 证书存储库中包含的证书），这些签名中必须至少有一个签名匹配，否则验证过程将失败。如果至少有一个全部对象签名匹配，验证过程将继续。

– 如果该对象有任何可信的核心对象签名，这些签名中必须至少有一个签名与 *SIGNATUREVERIFICATION 证书存储库中的证书相匹配，否则验证过程将失败。如果至少有一个核心对象签名匹配，验证过程将继续。

对象签署和签名验证的先决条件

OS/400 对象签署和签名验证功能提供控制 iSeries 服务器上的对象的附加且强大的手段。要利用这些功能，必须满足使用它们的先决条件。

对象签署的先决条件

取决于您的业务和安全性需要，有许多方法可用来签署对象:

- 可使用“数字证书管理器”（DCM）。
- 可编写使用“签署对象 API”的程序。
- 可使用“iSeries 导航器”的“中央管理”功能在封装对象以分发给端点 iSeries 系统时签署对象。

选择用哪个方法来签署对象取决于您的业务和安全性需要。不管计划使用什么方法签署对象，必须确保满足一定的先决条件:

- 必须满足安装和使用“数字证书管理器”（DCM）的先决条件。
  - 必须使用 DCM 创建 *OBJECTSIGNING 证书存储库。作为创建“本地认证中心”（CA）过程的一部分，或者作为管理公共因特网 CA 对象签署证书过程的一部分来创建此证书存储库。
  - *OBJECTSIGNING 证书存储库必须包含至少一个证书，该证书可以通过使用“本地 CA”创建或者从公共因特网 CA 获得。
  - 必须使用 DCM 创建至少一个对象签署应用程序定义以用于签署对象。
  - 必须使用 DCM 将特定的证书指定给对象签署应用程序定义。
- 签署对象的 iSeries 用户概要文件必须具有 *ALLOBJ 特权。创建 *SIGNATUREVERIFICATION 证书存储库的 iSeries 用户概要文件必须具有 *SECADM 和 *ALLOBJ 特权。

签名验证的先决条件

有许多方法可用来验证对象签名:

- 可使用“数字证书管理器”（DCM）。
- 可编写使用“验证对象（QYDOVFYO）API”的程序。
- 可使用多个命令中的其中一个命令（如“检查对象完整性”（CHKOBJITG）命令）。

选择用哪种方法来验证签名取决于您的业务和安全性需要。不管计划使用什么方法，必须确保满足一定的先决条件:

- 必须满足安装和使用“数字证书管理器”（DCM）的先决条件。
- 必须创建 *SIGNATUREVERIFICATION 证书存储库。取决于您的需要，用两种方法中的一种创建此证书存储库。可通过使用“数字证书管理器”（DCM）来创建它以管理签名验证证书。或者，如果使用公共证书签署对象，可通过编写使用“添加验证方（QYDOADDV）API”的程序来创建此证书存储库。

  注: “添加验证方 API”使用缺省密码创建证书存储库。需要使用 DCM 选择一个密码来重新设置此缺省密码以防止未授权访问该证书存储库。
- *SIGNATUREVERIFICATION 证书存储库必须包含已签署对象的证书的副本。可用两种方法中的一种将此证书添加到证书存储库。可在签署系统上使用 DCM 将证书导出到文件，然后，在目标验证系统上使用 DCM

将证书导入 *SIGNATUREVERIFICATION 证书存储库。或者，如果使用公共证书签署对象，可通过编写使用“添加验证方 API”的程序将证书添加到目标验证系统的证书存储库。

- *SIGNATUREVERIFICATION 证书存储库必须包含发出签署对象的证书的 CA 证书的副本。如果使用公共证书签署对象，则目标验证系统上的证书存储库应该已经拥有所需 CA 证书的副本。然而，如果使用由“本地 CA”发出的证书签署对象，则必须使用 DCM 将“本地 CA”证书的副本添加到目标验证系统上的证书存储库。

  注：由于安全性原因，“添加验证方 API”不允许将“认证中心”（CA）证书插入 *SIGNATUREVERIFICATION 证书存储库。向证书存储库添加 CA 证书时，系统将该 CA 看作可信的证书源。因此，系统认为该 CA 发出的证书来自可信的源。所以，不能使用该 API 创建安装出口程序将 CA 证书插入证书存储库。必须使用“数字证书管理器”向证书存储库添加 CA 证书以确保他人必须专门并手工控制系统信任哪些 CA。这样将防止发生系统从管理员没有特意指定为可信的源导入证书的可能性。

  如果使用由“本地 CA”发出的证书签署对象，必须在“本地 CA”主机 iSeries 服务器上使用 DCM 将“本地 CA”证书的副本导出到文件。然后，可在目标验证 iSeries 服务器上使用 DCM 将“本地 CA”证书导入 *SIGNATUREVERIFICATION 证书存储库中。为防止可能会发生的错误，必须先将“本地 CA”证书导入此证书存储库中，然后再使用“添加验证方 API”添加签名验证证书。因此，如果您使用由“本地 CA”发出的证书，会发现使用 DCM 将 CA 证书和验证证书同时导入证书存储库更加容易。

  如果希望防止任何人在您不知道的情况下使用此 API 向 *SIGNATUREVERIFICATION 证书存储库添加验证证书，则应考虑在您的系统上禁用此 API。可通过使用“系统服务工具”（SST）禁止更改与安全性相关的系统值来完成此操作。
- 验证签名的 iSeries 用户概要文件必须具有 *AUDIT 特权。创建 *SIGNATUREVERIFICATION 证书存储库或更改其密码的 iSeries 用户概要文件必须具有 *SECADM 和 *ALLOBJ 特权。

管理已签署对象

从 V5R1 开始，IBM 开始签署 OS/400 许可程序和 PTF，作为将操作系统正式标记为 IBM 开发的一种方式，也作为检测何时对系统对象进行了未授权更改的一种手段。业务伙伴和其它供应商同样也可能签署您购买的应用程序。因此，即使您自己没有签署对象，也需要了解如何处理已签署对象，以及这些已签署对象如何影响系统管理任务的例程。

已签署对象主要影响备份与恢复任务，尤其是如何保存对象及将对象恢复到系统上。

影响已签署对象的系统值和命令
了解可用来管理已签署对象的系统值和命令，或者运行时影响已签署对象的系统值和命令。

已签署对象的保存与恢复注意事项
了解已签署对象如何影响对系统执行保存与恢复任务。

确保签名完整性的代码检查程序命令
了解有关使用命令验证对象签名以确定对象完整性的详细信息。

影响已签署对象的系统值和命令

要有效地管理已签署对象，需要了解系统值和命令如何影响已签署对象。**在恢复期间验证对象签名**（QVFYOBJRST）系统值确定某些恢复命令如何影响已签署对象，以及在恢复操作期间系统如何处理已签署

对象。没有专门设计用于在 iSeries 系统上处理已签署对象的 CL 命令。然而，有很多常用的 CL 命令可用来管理已签署对象（或管理使对象可签署的基础结构对象）。通过从对象除去签名从而取消签名所提供的保护，其它命令对系统上的已签署对象会有消极影响。

影响已签署对象的系统值

在恢复期间验证对象签名（QVFYOBJRST）系统值，是 OS/400 系统值的恢复类成员，它确定命令如何影响系统上的已签署对象。此系统值可通过 “iSeries 导航器”获得，它控制系统在恢复操作期间处理签名验证的方式。用于此系统值的设置和两个其它系统值设置一起，影响系统的恢复操作。取决于为此值选择的设置，根据其签名状态（例如，对象是否未签署、签名是否无效以及是否由可信的源签署等等。）可允许或禁止恢复对象。此系统值的缺省设置不但允许恢复未签署的对象，而且确保仅当已签署对象具有有效的签名时才能恢复。仅当某个对象具有系统信任的签名时系统才将该对象定义为已签署；系统忽略其它 “不可信的”对象签名并将其作为未签署的对象对待。

有几个值可用作 QVFYOBJRST 系统值，对于系统存储的所有对象，其范围为从忽略所有签名到要求有效签名。此系统值仅影响要恢复的可执行对象（如程序（*PGM）、命令（*CMD）、服务程序（*SRVPGM）、SQL 程序包（*SQLPKG）和模块（*MODULE））。它也适用于流文件（*STMP）对象，这些对象具有由 “创建 Java 程序”（CRTJVAPGM）命令创建的关联的 Java 程序。它不适用于保存（*SAV）文件或 IFS 文件。

要了解有关使用此系统值和其它系统值的更多信息，参阅 “信息中心”中的系统值查找程序。

影响已签署对象的 CL 命令

有几个 CL 命令允许处理已签署对象或影响 iSeries 服务器上的已签署对象。可使用多种命令查看对象的签名信息、验证对象签名以及保存和恢复验证签名所需的安全性对象。另外，有一组命令在运行时可除去对象的签名且取消签名所提供的安全性。

查看对象签名信息的命令

- “显示对象描述”（DSPOBJD）命令。
  此命令显示在指定的库或在线程库列表的库中指定的对象的名称和属性。可使用此命令确定对象是否已签署及查看有关签名的信息。
- “显示对象链接”（DSPLNK）和 “处理对象链接”（WRKLNK）集成文件系统命令。
  可使用这两个命令中的任何一个显示集成文件系统中的对象的签名信息。

验证对象签名的命令

- “检查对象完整性”（CHKOBJITG）命令。
  此命令允许确定系统上的对象是否破坏了完整性。可使用此命令验证签名，这和使用病毒检查程序确定病毒何时毁坏了系统上的文件或其它对象的方法很相似。要了解有关将此命令用于已签署和可签署的对象的更多信息，参阅确保签名完整性的代码检查程序命令。
- “检查产品选项”（CHKPRDOPT）命令。
  此命令报告软件产品正确结构和实际结构之间的差异。例如，如果从已安装的产品删除了对象，该命令将报告错误。可使用 CKHSIG 参数指定命令应如何处理和报告产品的可能的签名问题。要了解有关将此命令用于已签署和可签署的对象的更多信息，参阅确保签名完整性的代码检查程序命令。
- “保存许可程序”（SAVLICPGM）命令。
  此命令保存组成许可程序的对象的副本。它以可由 “恢复许可程序”（RSTLICPGM）命令恢复的形式保存许可程序。可使用 CKHSIG 参数指定命令应如何处理和报告产品的可能的签名问题。要了解有关将此命令用于已签署和可签署的对象的更多信息，参阅确保签名完整性的代码检查程序命令。

- “恢复”（RST）命令。
  此命令恢复在集成文件系统（IFS）中可以使用的一个或多个对象的副本。此命令还允许在系统上恢复证书存储库及其内容。然而，不能使用此命令来恢复 *SIGNATUREVERIFICATION 证书存储库。恢复命令如何处理已签署和可签署的对象由在恢复（QVFYOBJRST）系统值期间“验证对象签名”的设置确定。
- “恢复库”（RSTLIB）命令。
  此命令恢复由“保存库”（SAVLIB）命令保存的一个库或一组库。RSTLIB 命令恢复整个库，包括库描述、对象描述和库中对象的内容。此命令如何处理已签署和可签署的对象由在恢复（QVFYOBJRST）系统值期间“验证对象签名”的设置确定。
- “恢复许可程序”（RSTLICPGM）命令。
  此命令装入或恢复初始安装或新发行版安装的许可程序。此命令如何处理已签署和可签署的对象由在恢复（QVFYOBJRST）系统值期间“验证对象签名”的设置确定。
- “恢复对象”（RSTOBJ）命令。
  此命令恢复使用单个命令保存在软盘、磁带、光学卷或保存文件中的单个库中的一个或多个对象。此命令如何处理已签署和可签署的对象由在恢复（QVFYOBJRST）系统值期间“验证对象签名”的设置确定。

保存和恢复证书存储库的命令

- “保存”（SAV）命令。
  此命令允许保存可用于集成文件系统（包括证书存储库）中的一个或多个对象的副本。然而，不能使用此命令保存 *SIGNATUREVERIFICATION 证书存储库。
- “保存安全性数据”（SAVSECDTA）命令。
  此命令允许保存不要求系统处于受限制状态时的所有安全性信息。使用此命令允许保存 *SIGNATUREVERIFICATION 证书存储库及证书存储库所包含的证书。此命令不保存任何其它的证书存储库。
- “保存系统”（SAVSYS）命令。
  此命令允许使用与 iSeries 服务器安装兼容的格式保存许可内码的副本和 QSYS 库的副本。它不从任何其它库保存对象。另外，它允许保存安全性和配置对象，这些安全性和配置对象也可通过使用 SAVSECDTA 和 SAVCFG 命令来保存。使用此命令允许保存 *SIGNATUREVERIFICATION 证书存储库及证书存储库所包含的证书。
- “恢复”（RST）命令。
  此命令允许在系统上恢复证书存储库及其内容。然而，不能使用此命令恢复 *SIGNATUREVERIFICATION 证书存储库。
- “恢复用户概要文件”（RSTUSRPRF）命令。
  此命令允许恢复用“保存系统”（SAVSYS）或“保存安全性数据”（SAVSECDTA）命令保存的一个或一组用户概要文件的基本部分。可使用此命令恢复 *SIGNATUREVERIFICATION 证书存储库、此证书存储库的隐藏密码及所有其它证书存储库的隐藏密码。通过将 *DCM 指定为 SCEDTA 参数的值并将 *NONE 指定为 USRPRF 参数的值，可恢复 *SIGNATUREVERIFICATION 证书存储库而不恢复用户概要文件信息。要使用此命令恢复用户概要文件信息和证书存储库及其密码，则将 *ALL 指定为 USRPRF 参数的值。

可除去或丢弃对象签名的命令

对已签署对象使用以下命令时，可以通过除去或丢弃对象签名的方式来完成。除去签名可能会导致受影响的对象出现问题。至少，将再也不能验证对象的源是否可信，并且再也不能验证签名来检测是否对对象进行了更改。应只将这些命令用于您创建的那些已签署对象（相对于从其它源如 IBM 或供应商获得的已签署对象）。如果关心该命令是否除去或丢弃了对象的签名，可使用“显示对象描述”（DSPOBJD）命令查看签名是否还在，并且如果有必要可重新签署它。

注: 要验证“保存”命令是否丢弃了对象的签名，必须将对象恢复到保存该对象的库之外的库中（例如，QTEMP）。然后，可使用 DSPOBJD 命令来确定保存介质上的对象是否丢弃了其签名。

- “更改程序”（CHGPGM）命令。
  此命令更改程序的属性，而不要求重新编译它。另外，即使指定的属性与当前的属性相同，也可使用此命令强制重新创建程序。
- “更改服务程序”（CHGSRVPGM）命令。
  此命令更改服务程序的属性，而不要求重新编译它。另外，即使指定的属性与当前的属性相同，也可使用此命令强制重新创建服务程序。
- “清除保存文件”（CLRSAVF）命令。
  此命令清除保存文件的内容；它清除保存文件的所有现有的记录并减少该文件使用的存储量。
- “保存”（SAV）命令。
  此命令保存可用于集成文件系统中的一个或多个对象的副本。— 使用此命令时，如果为 TGTRLS 参数指定一个比 V5R2M0 更早的值，则会从保存介质上的命令（*CMD）对象丢弃签名。因为不能在 V5R2 之前的发行版中签署命令对象，所以签名将丢弃。
- “保存库”（SAVLIB）命令。
  此命令允许保存一个或多个库的副本。使用此命令时，如果为 TGTRLS 参数指定比 V5R2M0 更早的值，则会从保存介质上的命令（*CMD）对象丢弃签名。因为不能在 V5R2 之前的发行版中签署命令对象，所以签名将丢弃。
- “保存对象”（SAVOBJ）命令。
  此命令保存位于同一库中的单个对象或一组对象的副本。使用此命令时，如果为 TGTRLS 参数指定比 V5R2M0 更早的值，则会从保存介质上的命令（*CMD）对象丢弃签名。因为不能在 V5R2 之前的发行版中签署命令对象，所以签名将丢弃。

已签署对象的保存与恢复注意事项

在 iSeries 服务器上，有几个系统值会影响恢复操作。这些系统值中只有一个值，**在恢复期间验证对象签名（QVFYOBJRST）**系统值，确定在恢复对象时系统如何处理已签署对象。为此系统值选择的设置让您确定恢复过程如何处理没有签名或者带无效签名的对象的验证。

一些保存和恢复命令影响已签署对象，或者确定在保存和恢复操作期间系统如何处理已签署和未签署的对象。应了解这些命令及其对已签署对象的影响，以便可更好地管理系统并避免可能发生的潜在问题。

这些命令在保存和恢复操作期间可验证对象签名:

- “保存许可程序”（SAVLICPGM）命令。
- “恢复”（RST）命令。
- “恢复库”（RSTLIB）命令。
- “恢复许可程序”（RSTLICPGM）命令。
- “恢复对象”（RSTOBJ）命令。

这些命令允许您保存并恢复证书存储库；证书存储库是安全性敏感的对象，它包含用于签署对象和验证签名的证书:

- “保存”（SAV）命令。
- “保存安全性数据”（SAVSECDTA）命令。
- “保存系统”（SAVSYS）命令。
- “恢复”（RST）命令。
- “恢复用户概要文件”（RSTUSRPRF）命令。

取决于所使用的参数值，一些保存命令可能会丢弃保存介质上的对象的签名，从而取消签名所提供的安全性。例如，如果*任何*保存操作引用的命令（*CMD）对象的目标发行版早于 V5R2M0，将导致不带签名而保存命令。

除去签名可能会导致受影响的对象出现问题。至少，将再也不能验证对象的源是否可信，并且再也不能验证签名来检测是否对对象进行了更改。应只将这些命令用于您创建的那些已签署对象（相对于从其它源如 IBM 或供应商获得的已签署对象）。

注: 要验证“保存”命令是否丢弃了对象的签名，必须将对象恢复到保存该对象的库之外的库中（例如，QTEMP）。然后，可使用 DSPOBJD 命令来确定保存介质上的对象是否丢弃了其签名。

应知道以下特定保存命令以及一般保存命令的这种潜在的问题:

- “保存”（SAV）命令。
- “保存库”（SAVLIB）命令。
- “保存对象”（SAVOBJ）命令。

有关在保存和恢复操作期间这些命令如何影响已签署对象和对象签名的更多信息，参阅影响已签署对象的系统值和命令。

确保签名完整性的代码检查程序命令

可使用“数字证书管理器”（DCM）或 API 来验证对象签名。也可使用几个命令来检查签名。使用这些命令允许您验证签名，这和使用病毒检查程序确定病毒是否毁坏系统的文件或其它对象的方法很相似。在将对象恢复或安装到系统（例如通过使用 RSTLIB 命令）时，检查大多数签名。

可选择使用三个命令中的其中一个检查已经在系统上的对象的签名。这些命令中，“检查对象完整性”（CHKOBJITG）命令专门设计用于验证对象签名。对于这些命令的每个命令签名检查都受 CHKSIG 参数的控制。此参数允许您检查对其签名的所有可签署的对象类型、忽略所有签名或只检查有签名的对象。最后这个选项是该参数的缺省值。

“检查对象完整性”（CHKOBJITG）命令

“检查对象完整性”（CHKOBJITG）命令允许确定系统上的对象是否破坏完整性。可使用此命令检查特定用户概要文件拥有的对象、匹配特定路径名的对象或者系统上的所有对象是否破坏完整性。满足以下条件其中之一时，就会产生一个破坏完整性记录项:

- 命令、程序、模块对象或库的属性已被更改。
- 对象的数字签名被确定为无效。签名是对象中数据的加密数学摘要；因此，如果验证期间对象中的数据与签署时对象中的数据相匹配，则认为签名匹配且有效。无效的签名是根据两种加密数学摘要的比较来确定的，这两种加密数学摘要分别是在签署对象时创建的及在签名验证期间完成的。签名验证过程对这两个摘要值进行比较。如果两值不同，则对象自签署以来其内容已被更改且认为签名为无效签名。
- 该对象类型的对象有不正确的域属性。
-

如果该命令检测到对象破坏了完整性，则它将对象名、库名称（或路径名）、对象类型、对象所有者和失败类型添加到数据库日志文件。该命令在某些其它情况下也创建记录项，虽然这些情况没有破坏完整性。例如，该命令对以下这些对象创建记录项: 可签署但没有数字签名的对象、不能检查的对象和处于要求更改以便在当前系统实现（从 IMPI 转换至 RISC）上使用的格式的对象。

CHKSIG 参数值控制命令如何处理对象的数字签名。可为此参数指定以下三个值之一:

- *SIGNED — 指定此值时，该命令检查带有数字签名的对象。该命令对有无效签名的任何对象创建记录项。它是缺省值。

- *ALL — 指定此值时，该命令检查所有可签署的对象以确定它们是否有签名。该命令将对任何可签署但没有签名的对象和任何有无效签名的对象创建记录项。
- *NONE — 指定此值时，该命令不检查对象的数字签名。

“检查产品选项”（CHKPRDOPT）命令

“检查产品选项”（CHKPRDOPT）命令报告软件产品的正确结构和实际结构之间的差异。例如，如果从已安装的产品删除了对象，该命令将报告错误。

CHKSIG 参数值控制命令如何处理对象的数字签名。可为此参数指定以下三个值之一:

- *SIGNED — 指定此值时，该命令检查带有数字签名的对象。该命令验证任何已签署对象的签名。如果命令确定对象的签名无效，则该命令就向作业记录发送一个消息，并将该产品标识为处于错误的状态。它是缺省值。
- *ALL — 指定此值时，命令检查所有可签署的对象以确定这些对象是否有签名并验证其签名。对于没有签名的任何可签署对象，该命令向作业记录发送一个消息；然而，该命令不将产品标识为错误。如果命令确定对象的签名无效，该命令向作业记录发送一个消息并将产品设置为错误。
- *NONE — 指定此值时，命令不检查产品对象的数字签名。

“保存许可程序”（SAVLICPGM）命令

“保存许可程序”（SAVLICPGM）命令允许保存组成许可程序的对象的副本。它以可由“恢复许可程序”（RSTLICPGM）命令恢复的格式保存许可程序。

CHKSIG 参数值控制命令如何处理对象的数字签名。可为此参数指定以下三个值之一:

- *SIGNED — 指定此值时，该命令检查带有数字签名的对象。该命令验证任何已签署对象的签名但不检查未签署的对象。如果命令确定对象的签名无效，则它向作业记录发送一条标识该对象的消息，且保存将失败。它是缺省值。
- *ALL — 指定此值时，命令检查所有可签署的对象以确定这些对象是否有签名并验证其签名。对于没有签名的任何可签署对象，该命令向作业记录发送一个消息；然而，保存过程将不会终止。如果命令确定对象的签名无效，它向作业记录发送一个消息，且保存将失败。
- *NONE — 指定此值时，命令不检查产品对象的数字签名。

对已签署对象进行故障诊断

可使用以下表格查找信息以帮助您诊断一些较常见的问题，这些问题在使用 iSeries 对象签署和签名验证功能时会遇到。

常见对象签署问题

问题	可能的解决方法
使用“签署对象 API”签署目标发行版为 V4R5 或更早版本的对象时，签署过程失败且不签署对象（错误消息 CPFB721）。	对于 V5R1 之前的版本，iSeries 不提供对象签署支持。对于那些返回错误消息 CPFB721 的对象，必须使用 V5R1 或更高的目标发行版重新创建那些程序以便签署这些对象。

常见签名验证问题

问题	可能的解决方法
对于没有签名的对象，恢复过程将失败。	如果不关心是否缺少签名，请检查 QVFYOBJRST 系统值是否设置为 5。值 5 指定不能恢复未签署的对象。将该值更改为 3 并再试恢复。
对于有签名的对象，恢复过程将失败。	如果将 *SIGNATUREVERIFICATION 证书存储库传送至系统且没有使用 DCM 更改其密码，则可能发生恢复过程失败的问题。在这种情况下，在恢复过程期间不能使用存储库包含的证书验证签名。使用 DCM 更改证书存储库的密码。如果您不知道密码，则必须删除该证书存储库，然后重新创建它并使用 DCM 更改密码。
恢复或安装产品时，由于无法验证签名而发生错误。	对象签名无法正确验证时，可能表明对象自签署以来被更改过。如果是对象完整性的问题，则不应更改 QVFYOBJRST 系统值或执行允许有问题的对象恢复的其它操作。这样做会绕过签名验证所提供的安全性并允许有害的对象进入系统。而应该与对象签发者联系以确定解决该问题应采取的适当措施。

对象签署和签名验证的相关信息

对象签署和签名验证是相对较新的安全性技术。如果您有兴趣希望更广泛地了解这些技术及它们如何工作，此处是其它资源的一个简单列表，您会发现它们很有用:

- **VeriSign Help Desk Web 站点**
  VeriSign Web 站点提供了一个有关数字证书主题（如对象签署），以及许多其它因特网安全性主题的内容广泛的库。
- **IBM eServer iSeries Wired Network Security: OS/400 V5R1 DCM and Cryptographic Enhancements SG24-6168**
  此 IBM 红皮书集中论述 V5R1 网络安全性增强。此红皮书涉及许多主题，包括如何使用 iSeries 对象签署功能以及“数字证书管理器”（DCM）等等。

中国印刷