技术概要：InterSystems 公钥基础设施 (PKI)

版本 2021.1
2021-07-21

技术概要：InterSystems 公钥基础设施 (PKI)

InterSystems IRIS 数据平台 版本 2021.1 2021-07-21

有关 InterSystems 产品的技术支持问题，请联系：

InterSystems 全球响应中心（WRC）

Tel: +1-617-621-0700
Tel: +44 (0) 844 854 2917
Email: support@InterSystems.com

目录

技术概要：InterSystems 公钥基础设施（PKI）

本文档介绍了 InterSystems 公钥基础设施（PKI），它可以在开发组织的安全策略中发挥重要作用。它提供有关公钥加密、证书颁发机构和 PKI 的信息。然后介绍一些与使用 InterSystems PKI 相关的初始任务。完成本指南后，您将有能力创建一个证书颁发机构（CA），然后向 CA 客户端请求并接收证书。

虽然 InterSystems PKI 不用于生产系统，但您可以用它来熟悉 PKI 工具和安全基础设施。作为设计和探索过程的一部分，这对于创建全面的安全方法特别有帮助。

本指南使用 InterSystems IRIS®数据平台的默认设置，这使您能够熟悉 PKI 的基本原理，而不必处理其他在执行实现时很重要的细节问题。有关数据库加密的完整文档，请参见 The InterSystems Public Key Infrastructure（《InterSystems 公钥基础设施》）。

要浏览所有的技术概要（First Look），包括可以在 InterSystems IRIS 免费的评估实例上执行的那些，请参见 InterSystems First Looks（《InterSystems 技术概要》）。

1 为什么 PKI 很重要

在许多企业中，关于安全漏洞的新闻频繁出现，这表明有必要保护他们的通信安全。企业需要保护从一个站点到另一个站点的数据，或者当需要某种可验证的、具有法律约束力的数字签名时。解决这些和其他需求的强大、有效和普遍的工具是*公钥加密（public-key cryptography）*和*公钥基础设施（PKI）*。

公钥加密（Public-key cryptography）能够对数据进行加密和解密。这提供了一种执行与保护数据相关的各种操作的方法。这包括保护在不安全的网络（如 Internet）上传输的数据或确定文档的来源。因此，它启用了关键技术，如传输层安全（Transport Layer Security，TLS），这是浏览器保护我们与网站连接的手段。

公钥加密（Public-key cryptography）对不同实体控制的数据进行操作，这些实体可以是人、应用程序、组织等。但是，仅公钥加密（Public-key cryptography）并不能为这些实体在活动中的身份提供足够的信心，特别是在它们彼此不认识的情况下。为了达到这种信任水平，需要有一个更大的结构，同时为所涉及的实体提供值得信赖和可验证的标识信息。这样一个结构被称为 PKI（公钥基础设施）。

PKI 为实体建立了一种对彼此的身份有信心的方法，即使彼此没有任何直接的个人了解或接触。这要求每个实体信任第三方——*证书颁发机构（CA）*——为其他实体（也称为其他*对等方*）的身份提供担保。通过 PKI，实体可以进行有意义的、具有法律约束力的加密操作，其中包括加密、解密、数字签名和签名验证。

InterSystems 提供了一个公钥基础设施（PKI），它使用 InterSystems IRIS 的实例作为 CA，允许您创建密钥对，并允许您创建与这些密钥对有关的证书。InterSystems CA 适合在组织内部和非生产环境中使用。不建议将其作为生产或商业 CA 使用；虽然它的证书在加密上是可靠的，但商业 CA 除了技术基础设施外，还需要一定程度的组织和法律基础设施。

使用 PKI 的公钥加密支持许多的安全活动：

- 对电子文档进行数字签名
- 验证电子文档的签名
- 加密各方之间的通信
- 加密文档

1.1 公钥加密和证书颁发机构（CA）如何协同工作的基本原理

在使用公钥加密时，每个实体都有一个严格保密的*私钥（private key）*，以及一个广泛使用的*公钥（public key）*。如果您使用其中一个密钥执行一个操作，您可以使用另一个密钥执行互补的操作；例如，如果您用私钥加密数据，那么只有您的公钥可以解密该数据。如果别人用您的公钥对内容进行加密，只有您的私钥——因此也只有您——能够解密。这意味着公钥加密为两个实体之间的安全和私人通信提供了一种方法。

为了使公钥加密在互不相识且不能轻易验证对方身份的实体之间发挥作用，需要有一个双方实体都信任的第三方。这个第三方是证书颁发机构（CA）。证书颁发机构创建证书，这些证书是将公钥绑定到公钥持有者的一组标识信息的数字文档。由于公钥和私钥不可分割地相互绑定，证书也将标识信息绑定到私钥上。一些企业有内部的 CA，它们用来支持内部活动；其他 CA 作为独立的组织运作，通常作为商业服务提供证书。商业 CA 通常在不同程度的身份验证基础上提供证书；在充分验证的情况下，证书可以在组织或个人和公私密钥对之间建立起具有法律约束力的联系。CA 的使用使处于不安全环境中的实体有足够的信心以有意义的和具有法律约束力的方式使用公钥加密。

互相通信的实体不需要使用相同的 CA。相反，每一个人只需要信任对方的 CA。这种信任 CA 的关系通常是在没有任何用户干预的情况下建立的，例如让浏览器附带一组预先批准的 CA 证书。事实上，一个实体可以信任一个 CA，因为它有第二个 CA 的证书，而这个 CA 已经被信任了；在这种情况下，第一个 CA 被称为中间 CA——而且可以有多个中间 CA。

当一个实体从一个 CA 获得证书时，会发生许多事情——经常对用户不可见。首先，CA 客户端使用算法来生成密钥对；然后 CA 客户端获得必要的信息来描述使用该密钥对的实体，这与实体的位置、组织等有关。总的来说，这个标识信息包括一个*专有名称（distinguished name，DN）*。该实体以*证书签名请求（certificate signing request，CSR）*的形式向 CA 提供公钥和 DN 信息；它不提供私钥，因为这是严格保密的。

CA 收到 CSR，然后根据其程序进行处理。然后，CA 签署一份文档，将公钥绑定到 DN 信息，从而创建一个证书（具体来说，就是符合 X.509 标准的证书）。最后，CA 客户端从 CA 获得证书，然后可以将它用于各种活动，如建立 TLS 连接。

当两个实体需要相互认证时，它们使用它们的证书和 CA 对它们的信任关系。因此，当 Alice 和 Bob 试图通过 TLS 进行通信时，TLS 握手会对他们每个人执行如下身份验证：

- Alice 最终得到了 Bob 的证书。Alice 可以信任这个证书，因为 Bob 的 CA 已经对它进行了签名，而且 Bob 的 CA 是受信任的 CA。
- 持有 Alice 证书的 Bob 也是如此。

2 有关 InterSystems PKI

总的来说，CA 和公钥加密的活动是所谓的*公钥基础设施（public key infrastructure，PKI*）的一部分。因此，PKI 提供了一种创建和管理密钥对和证书的方法，并可以支持加密操作，包括加密、解密、数字签名和签名验证。InterSystems IRIS 包含 PKI。

使用 InterSystems PKI，您可以设置一个证书颁发机构（CA），一个 CA 客户端，并开始在用户之间发送安全数据，只需几个步骤。

当 InterSystems IRIS 的一个实例充当CA 时，它被称为 CA 服务器；当实例使用 CA 的服务时，它被称为CA 客户端。一个实例既可以是 CA 服务器，也可以是CA 客户端。

在将自己建立为 CA 服务器时，InterSystems IRIS 的实例要么创建一个密钥对，然后将公钥嵌入到自签名的 X.509 证书中，要么使用外部CA 签名的私钥和 X.509 证书。X.509 是一种行业标准证书结构，它将公钥与专有名称（Distinguished Name， DN）关联起来。

3 亲自尝试 InterSystems PKI

设置和使用 InterSystems PKI 很容易。在这个示例中，您将使用 InterSystems IRIS 的两个实例。您将使用实例 #1 作为CA（这里主要称为CA 服务器）和实例 #2 作为CA 客户端进行一系列的初始操作。这些步骤是：

1. 将实例 #1 配置为CA 服务器
2. 将实例 #2 配置为CA 客户端
3. 在 CA 客户端上，向 CA 服务器提交证书签名请求（CSR）
4. 在 CA 服务器上，处理 CSR
5. 在 CA 客户端上，从 CA 服务器下载它的证书和 CA 服务器证书

重要提示： InterSystems PKI *不*用于生产系统。

此外，本文档中的示例以不适合使用任何PKI 的生产系统的方式简化了设置和使用 CA 的过程。例如，它提供一个建议密码，用于加密和解密CA 服务器的私钥。在生产系统（或除演示系统以外的任何系统）上，*永远不要*使用公开的已知密码，因为这可能会危及您的CA 的私钥的安全，从而危及您的整个PKI；如果这个密钥被泄露或破解，那么*所有*CA 的证书都变得不可信了。

类似地，证书颁发机构的证书和私钥文件的目录与您在本文档练习中使用的InterSystems IRIS 实例在同一台机器上。对于生产系统来说，这个目录应该总是在一个外部设备上（不是本地硬盘驱动器或网络服务器），最好是在一个加密的外部设备上。这是因为该目录持有CA 的私钥。

如果您创建了一个生产系统，请按照 PKI 供应商的说明操作。有关在开发或测试系统中使用 InterSystems PKI 的更多详细信息，请参见 The InterSystems Public Key Infrastructure（《InterSystems 公钥基础设施》）。

3.1 用前须知

要使用这个程序，您需要两个正在运行的InterSystems IRIS 实例。这些实例可以在相同或不同的主机上，但必须相互有网络访问权限。

您对 InterSystems IRIS 的选择包括多种类型的已授权的和免费的评估实例；该实例不需要由您正在工作的系统托管（尽管它们必须相互具有网络访问权限）。关于如何部署每种类型的实例的信息（如果您还没有可使用的实例），请参见 *InterSystems IRIS Basics:Connecting an IDE*（《*InterSystems IRIS 基础：连接一个IDE*》）中的 Deploying InterSystems IRIS（部署 InterSystems IRIS）。

3.2 将实例 #1 配置为 CA 服务器

要将实例#1 配置为CA 服务器：

1. 使用 *InterSystems IRIS Basics: Connecting an IDE*（《*InterSystems IRIS 基础：连接一个IDE*》）中URL described for your instance（为您的实例描述的URL），在您的浏览器中打开实例的管理门户（Management Portal）。
2. 进入 **Public Key Infrastructure（公钥基础设施）**页面(**System Administration（系统管理）** > **Security（安全）** > **Public Key Infrastructure（公钥基础设施）**)。
3. 在 **Public Key Infrastructure（公钥基础设施）**页面上，在**Certificate Authority Server（证书颁发机构服务器）**下，选择 **Configure Local Certificate Authority server（配置本地证书颁发机构服务器）**。这将显示两个字段：
   - **File name root for Certificate Authority’s Certificate and Private Key files（证书颁发机构的证书和私钥文件的文件名根）(没有扩展名)**——输入 `FLCA` (技术概要证书颁发机构（First Look Certificate Authority）)。此处使用 `FLCA` 作为私钥文件和证书文件的名称，所以私钥是在 FLCA.key 中，而证书则在 FLCA.cer 中。
   - **Directory for Certificate Authority’s Certificate and Private Key files（证书颁发机构的证书和私钥文件的目录）**——输入 `flca`。这将在 *install-dir*\mgr\下创建 flca 目录（*install-dir* 是实例的安装目录)，并将 FLCA CA 证书和私钥文件放在那里。您也可以点击**Browse（浏览）**来选择一个不同的位置；当你这样做时，目录选择（Directory Selection）对话框会打开到*install-dir*\mgr\。
4. 点击 **Next（下一步）**继续。
5. 在出现的字段中，输入以下值：
   - **Password to Certificate Authority's Private Key file（证书颁发机构私钥文件的密码）**和 **Confirm Password（确认密码）** — 输入密码以加密和解密 CA 的私钥文件。我们建议您使用 `myflcapw`，这样您在这里就有一份密码的副本。
   - 在 **Certificate Authority Subject Distinguished Name（证书颁发机构主体专有名称）**下，在 **Common Name（通用名称）**中 — 输入标识此CA 的 `First Look CA`。

   如果您使用 InterSystems PKI 进行更深入的测试和实验，当您配置 CA 服务器时，您将完成本节的字段，以包括负责签署CA 请求的用户的电子邮件帐户。对于这个技术概要（First Look），您可以跳过它。
6. 点击 **Save（保存）**。InterSystems IRIS 显示如下信息，表示成功：

```
Certificate Authority server successfully configured.
Created new files: C:\InterSystems\MYIRIS1\mgr\flca\FLCA.cer .key, and .srl.
Certificate Authority Certificate SHA-1 fingerprint:
E3:FB:30:09:53:90:9A:31:30:D3:F0:07:8F:64:65:CD:11:0A:1A:A2
```

这表明InterSystems IRIS 已经执行了以下操作：

- 创建一个密钥对。
- 将私钥保存到您指定的文件位置，并使用您指定的根名称。
- 创建一个包含公钥的自签名CA 证书。

- 将证书保存到您指定的文件位置，并使用您指定的根名称。
- 创建一个颁发的证书数量的计数器，并将其存储在与证书和私钥相同目录中的 SRL（序列）文件中。（每次 CA 颁发新的证书时，InterSystems IRIS 都会根据这个计数器给证书一个唯一的序列号，然后增加 SRL 文件中的值）。

3.3 将实例 #2 配置为 CA 客户端

要将实例#2 配置为CA 客户端：

1. 使用为您的实例描述的URL，在您的浏览器中打开实例的管理门户（Management Portal）。
2. 进入 **Public Key Infrastructure（公钥基础设施）**页面(**System Administration（系统管理）**>**Security（安全）**>**Public Key Infrastructure（公钥基础设施）**)。
3. 在 **Certificate Authority Client（证书颁发机构客户端）**下，选择 **Configure Local Certificate Authority Client（配置本地证书颁发机构客户端）**，这会在此页面上显示多个字段。
4. 填写以下字段，其他字段留空或使用默认值。在上一节中，您使用了实例#1 的主机标识符和web 服务器端口，您必须在这里输入。在其管理门户（Management Portal） URL 中。
   - **Certificate Authority server hostname（证书颁发机构服务器主机名）**——运行 CA 服务器的主机的 IP 地址或 DNS 名称，即实例 #1 的主机。
   - **Certificate Authority WebServer port number（证书颁发机构网络服务器端口号）**——作为 CA 服务器的实例的 web 服务器端口号，也就是实例#1。
   - 在 **Local technical contact（本地技术联系人）**部分，**Name（名称）**——任何值。(这个字段是必需的，因为CA 服务器必须有设置CA 客户端的人的联系信息。因为您既要配置 CA 客户端，又要配置CA 服务器，所以您是它们的本地技术联系人。）

   注意： 在生产环境中，PKI 可能需要带外联系信息，如在 **Local technical contact（本地技术联系人）**区域。这些信息是为了身份验证，客户端需要提供联系人信息以开始这一过程。
5. 点击 **Save（保存）**。

InterSystems IRIS 通过诸如"成功配置证书颁发机构（Certificate Authority，CA）客户端"的信息来确认成功。

3.4 在实例 #2 上，向 CA 服务器提交证书签名请求（CSR）

接下来，在实例#2 上，向 CA 服务器提交一个证书签名请求（CSR）：

1. 仍然在 **Public Key Infrastructure（公钥基础设施）**页面(**System Administration（系统管理）**>**Security（安全）**>**Public Key Infrastructure（公钥基础设施）**)，在 **Certificate Authority Client（证书颁发机构客户端）**下，选择 **Submit Certificate Signing Request to Certificate Authority Server（向证书颁发机构服务器提交证书签名请求）**，这将显示几个新的字段。
2. 按以下方式填写它们，其他字段留空或使用默认值：
   - **File name root for local Certificate and Private Key files（本地证书和私钥文件的文件名根）（没有扩展名）**——输入 `FLCAclient` (技术概要证书颁发机构客户端（First Look Certificate Authority client）)。这使用了 `FLCAclient` 作为私钥文件和证书文件的名称，因此私钥在 FLCAclient.key 中，而证书将很快出现在 FLCAclient.cer 中。
   - 在 **Subject Distinguished Name（主体专有名称）**下，在 **Common Name（通用名称）**字段中——输入 `FL CA client`。
3. 按要求完成这些字段，并点击 **Save（保存）**。如果成功，InterSystems IRIS 将显示如下信息：

```
Certificate Signing Request FLCAclient successfully submitted to the Certificate Authority
at instance MYIRIS1 on node FLCATEST.COM.
SHA-1 Fingerprint: C2:B0:D6:0D:D6:AB:43:DF:7F:B1:22:AE:14:D7:45:FF:CC:0C:20:D0
```

4. 此时，您已经使用InterSystems IRIS 创建并提交了CSR。

3.5 在实例 #1 上，处理 CSR

在实例#1（CA服务器）上，处理CSR，将其转换为证书：

1. 在管理门户（Management Portal）中，进入 **Public Key Infrastructure（公钥基础设施）**页面(**System Administration（系统管理）**>**Security（安全）**>**Public Key Infrastructure（公钥基础设施）**)。
2. 在 **Public Key Infrastructure（公钥基础设施）**页面上，在**Certificate Authority Server（证书颁发机构服务器）**下，选择 **Process pending Certificate Signing Requests（处理待处理的证书签名请求）**，它显示来自CA客户端的待处理 CSR。
3. 点击CSR右侧的 **Process（处理）**，显示CSR的内容，显示CSR的处理字段。有关这些字段的几个要点：
   - 因为您要为可以使用InterSystems IRIS中安全功能的CA客户端颁发证书，所以在 **Certificate Usage（证书使用）**下，您可以保留默认的**TLS/SSL，XML encryption and signature verification（TLS/SSL、XML 加密和签名验证）**。
   - 在生产环境中，您需要验证CA客户端的身份。因此，本节演示如何执行这一行为；例如，在**Request Content（请求内容）**下，显示CA客户端的电话号码和电子邮件。这将允许您通过电话或亲自联系他们并验证他们的身份。
4. 点击 **Issue Certificate（颁发证书）**，这将导致页面显示**Password for Certificate Authority's Private Key file（证书颁发机构私钥文件的密码）**字段。
5. 在 **Password for Certificate Authority's Private Key file（证书颁发机构私钥文件的密码）**字段中，输入 `myflcapw`，这是您在配置CA服务器时创建的密码。
6. 点击 **Finish（完成）**来创建证书。IRIS显示一条信息，如

```
Certificate number 2 issued for Certificate Signing Request FLCAclient
```

InterSystems IRIS现在已经创建了证书。如果CA客户端列出了其技术联系人的电子邮件地址，该地址还会收到证书可供下载的通知。

3.6 在实例 #2 上，从 CA 服务器下载它的证书和 CA 服务器证书

下一步也是最后一步是CA客户端从CA服务器下载CA服务器的证书和它自己的证书：

1. 在管理门户（Management Portal）中，在实例#2上，进入 **Public Key Infrastructure（公钥基础设施）**页面(**System Administration（系统管理）**>**Security（安全）**>**Public Key Infrastructure（公钥基础设施）**)。
2. 在 **Public Key Infrastructure（公钥基础设施）**页面上，在**Certificate Authority Client（证书颁发机构客户端）**下，点击 **Get Certificate(s) from Certificate Authority server（从证书颁发机构服务器获取证书）**。
3. 在显示的字段中，有一个 **Get Certificate Authority Certificate（获取证书颁发机构证书）**按钮。点击它，会下载CA服务器的证书，并显示一条信息，如：

```
Certificate Authority Certificate
(SHA-1 Fingerprint: 8A:38:C9:06:50:A0:4F:71:86:2B:69:4C:A2:42:E0:43:28:C8:70:EB)
saved in file "c:\intersystems\MYIRIS2\mgr\FLCA.cer"
```

4. 再一次点击 **Get Certificate(s) from Certificate Authority server（从证书颁发机构服务器获取证书）**。

5. 已颁发证书表列出了CA客户端的证书。点击行旁边的**Get（获取）**按钮。这就下载了CA客户端的证书，并显示一条信息，如：

```
Certificate number 2
(SHA-1 Fingerprint: 2E:82:27:73:72:38:BC:71:36:70:DC:9E:0D:EF:E6:BC:0D:A9:95:CD)
saved in file "c:\intersystems\MYIRIS2\mgr\FLCAclient.cer"
```

3.7 总结和下一步

您现在有：

1. 将 InterSystems IRIS 的一个实例配置为CA服务器
2. 将 InterSystems IRIS 的另一个实例配置为CA客户端
3. 从 CA客户端向CA服务器提交证书签名请求（CSR）
4. 在 CA服务器上处理CSR
5. 将 CA服务器的证书和CA客户端自己的CA证书从CA服务器下载到CA客户端

这意味着您现在有一个InterSystems IRIS 实例是一个正常运行的CA服务器，另一个InterSystems IRIS 实例是一个正常运行的CA客户端。如果您在另一个InterSystems IRIS 实例上设置CA客户端，并为每个实例创建TLS配置，两个客户端可以交换加密的信息。这为各种安全活动提供了基础。

注意： 最后提醒一下：这个示例系统并不能帮助建立一个安全的环境，因为CA的私钥已经在本文档中公开发布。妥善保护生产系统中的所有私钥是至关重要的，而保护CA的私钥则是*最*重要的。泄露在生产系统中使用的私钥，会导致安全漏洞、数据泄露、财务损失和法律漏洞。除了让您了解InterSystems IRIS 功能之外，请不要使用此文档的CA服务器私钥进行其他任何操作。

4 了解有关InterSystems PKI 的更多信息

有关InterSystems PKI 的完整文档，请参见The InterSystems Public Key Infrastructure（《InterSystems 公钥基础设施》）。