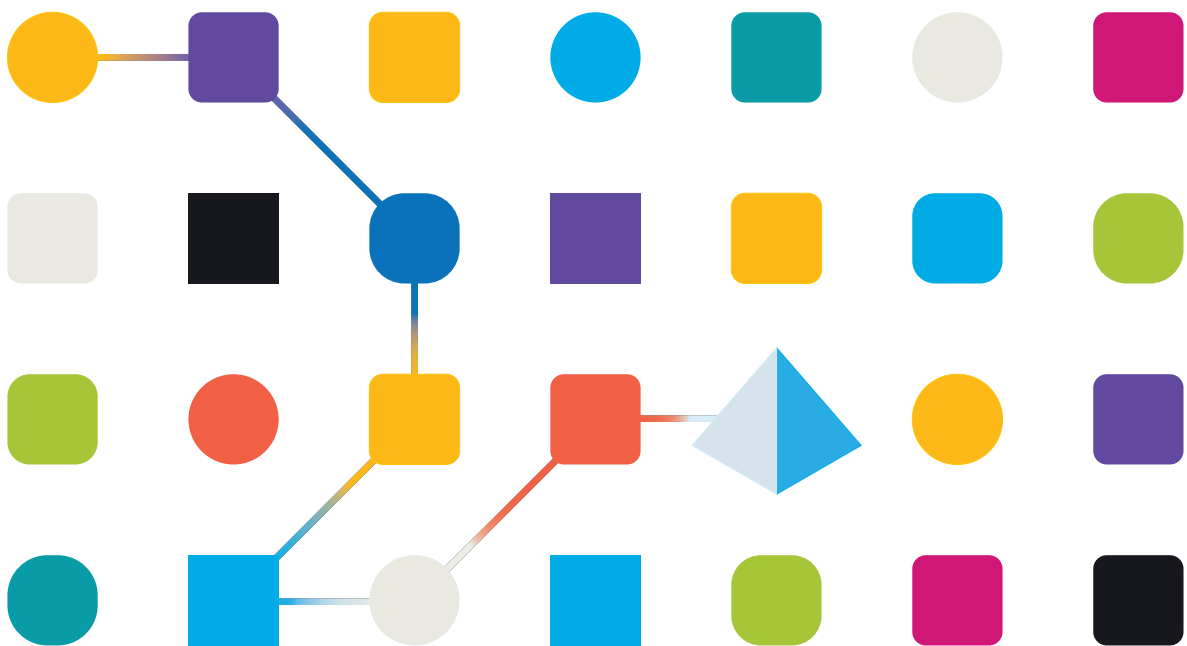


# blueprism<sup>®</sup>

## Hub and Interact 4.6

### 安全参考指南

文档修订版:1.0



## 商标和版权

本指南中包含的信息是 Blue Prism Limited 和/或附属公司的专有和机密信息，未经获授权的 Blue Prism 代表的书面同意，不得披露给第三方。未经 Blue Prism Limited 或其附属公司的书面同意，不得以任何形式或通过任何手段(电子或实物形式，包括复制)翻印或传输本文档中的任何部分。

### © Blue Prism Limited 2001—2022

“Blue Prism”、“Blue Prism”徽标和 Prism 设备是 Blue Prism Limited 及其附属公司的商标或注册商标。保留所有权利。

其他所有商标在本指南中的使用均得到认可，并用于各自所属方的利益。

Blue Prism Limited 及其附属公司对本指南中引用的外部网站的内容概不负责。

Blue Prism Limited, 2 Cinnamon Park, Crab Lane, Warrington, WA2 0XP, 英国。

在英国境内注册:注册编号:4260035。电话:+44 370 879 3000。网站:[www.blueprism.com](http://www.blueprism.com)

## 目录

Blue Prism Interact 安全 .....	4
加密 .....	5
身份验证 .....	6
网络连接 .....	7
日志记录 .....	8

## Blue Prism Interact 安全

本文档提供功能和技术参考点，帮助解决客户疑虑、合规性查询以及有关安全的传入提案请求 (RFP)。本指南涵盖以下内容：

- 加密
- 身份验证
- 网络连接
- 日志记录

## 加密

Blue Prism Interact 使用以下加密方法：

算法	描述
流量加密	为生产启用仅限 HTTPS 的通信。要求客户为所有 Web 应用程序提供 TLS 证书，并且所有通信信道都受到保护。 有关配置证书的更多信息，请参阅 <a href="#">在线帮助</a> 。
数据保护	Hub 安装程序会生成 PFX 证书并将其保存到受信任的根证书颁发机构。所有应用程序均借此加密敏感数据，例如 appsettings.json 文件中的连接字符串。 数据保护使用以下默认算法： <ul style="list-style-type: none"> <li>• 加密算法为 AES-256-CBC</li> <li>• 验证算法为 HMACSHA256</li> </ul> 密钥大小为 2048 位。
JSON Web 令牌签名	Hub 安装程序会生成 PFX 证书并将其保存到受信任的根证书颁发机构。Identity Server 借此加密 JSON Web 令牌并验证许可证文件。 JSON Web 令牌通过 RSA-SHA-256 算法加密，密钥大小为 2048 位。
Authentication Server	这是授权服务器—用户通过 Authentication Server 登录，该服务器决定了他们有权访问的组件。 Authentication Server 使用 SHA-256 对客户端密钥和客户端 ID 进行哈希处理。
密码存储	AspNetIdentity 库用于密码哈希，并使用以下算法： <ul style="list-style-type: none"> <li>• PBKDF2 与 HMAC-SHA256</li> <li>• 128 位 salt</li> <li>• 256 位子密钥</li> <li>• 10000 次迭代</li> </ul>

许可证密钥通过 RSA-SHA-512 算法加密。

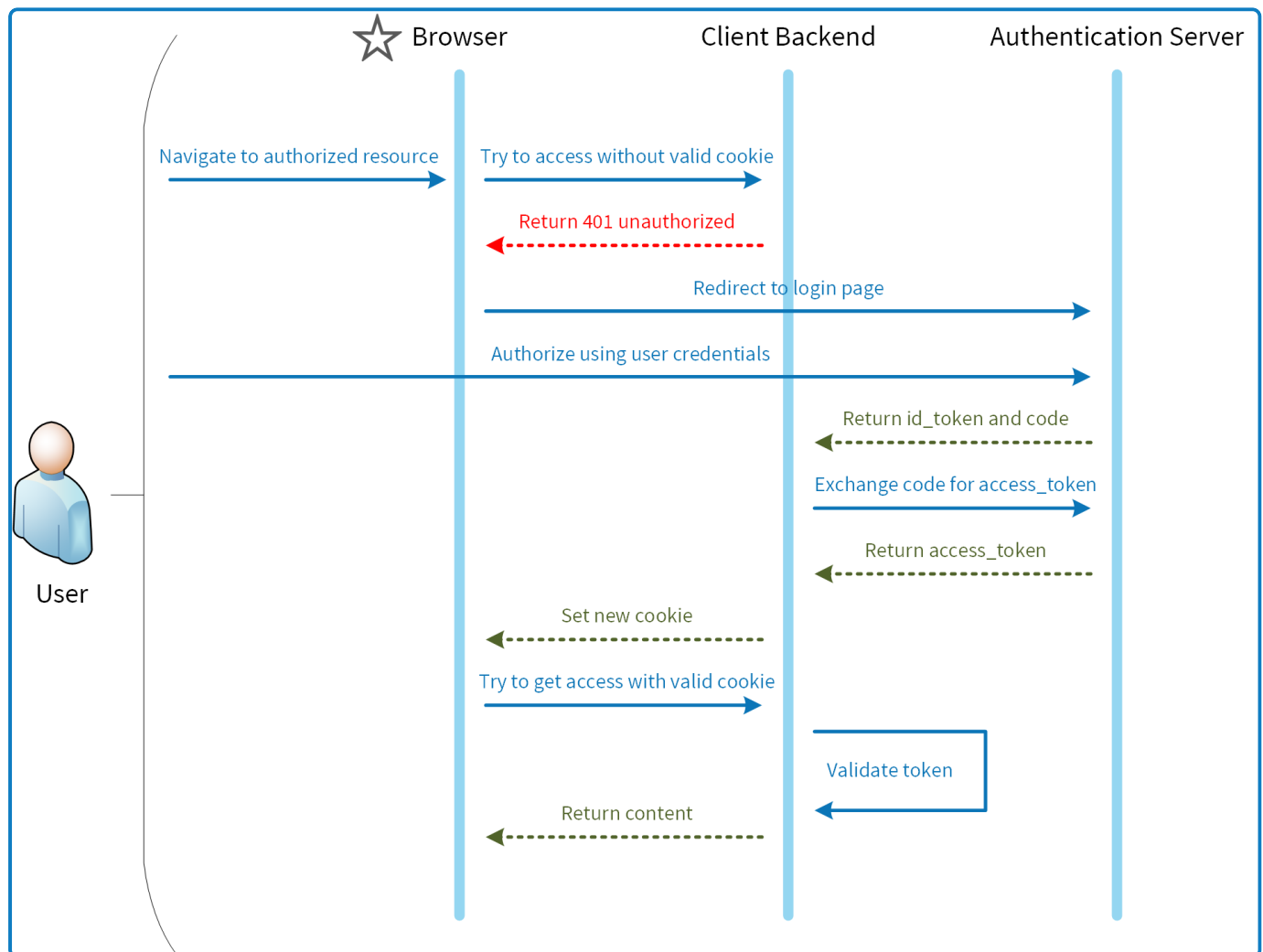
数据库加密可以由 Microsoft 加密机制(透明数据加密—TDE)提供，但必须在每个数据库上手动实施。有关更多信息，请访问：[docs.microsoft.com](https://docs.microsoft.com)。

TLS 默认为 TCP 和 HTTP 通信的主机操作系统配置，选择最佳的安全协议和版本。可用的协议和密码由最终用户管理，或通过 Microsoft 安全更新自动处理。

## 身份验证

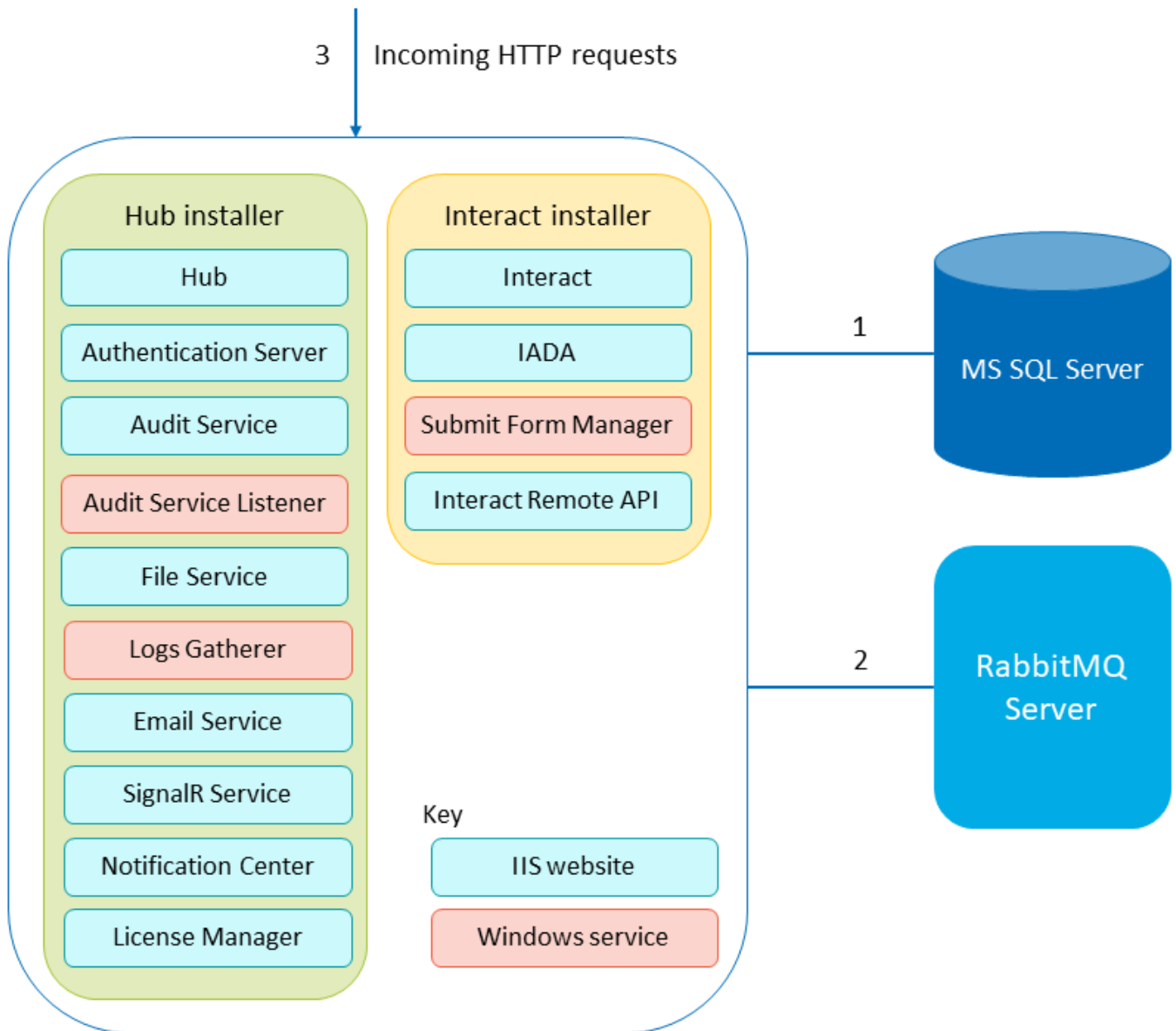
Interact 中的身份验证概述如下：

- 提供 Authentication Server, 由 OpenId Connect 协议实施。
- 所有用户的 API 调用均获得授权。
- 应用程序之间的所有 API 调用均获得授权。
- 访问令牌仅在 HTTPS Cookie 中存储, 无法拦截或修改。



## 网络连接

该图概述了通过 Interact 平台进行的常见通信。



1. 由 TLS 保护—利用 SQL Server 功能自动生成自签名证书或利用现有的可验证证书, 从而支持基于证书的加密。
2. 使用 AMQP 协议。
3. 默认情况下, 通过 HTTPS 保护连接。

## 日志记录

在 Interact 中执行的 Blue Prism Interact 日志记录概述如下：

- 日志在用户可配置位置保存为 TXT 文件—默认位置位于安装目录内的 Blue Prism > Interact 文件夹, 但是通过编辑 nlog.configfile(位于安装目录的 Interact 文件夹中) 内以下行的值, 可以对位置进行配置：

```
<variable name="logsFolder" value=".\\Logs_Interact"/>
```

其中 .\ 是 Interact 安装目录。默认情况下, 此目录为 C:\Program Files (x86)\Blue Prism\Interact\ 更新后, 重新启动 IIS。

- 默认日志记录级别可在 appsettings.json 文件中进行配置：
  - 默认: 信息
  - 系统: 警告
  - Microsoft: 警告

有以下日志记录级别可应用: 严重、调试、错误、信息、无、跟踪、警告。有关这些日志记录级别的更多信息, 请参阅 [docs.microsoft.com](https://docs.microsoft.com)。

该文件位于安装目录内的 Blue Prism > Interact 文件夹—编辑该文件可更改日志记录级别。更新日志级别后, 必须重新启动 World Wide Web Publishing 服务, 才能使更改生效。

- 日志每月会存档到 Zip 文件, 以减少文件大小。
- 日志不包含任何个人信息或敏感信息。