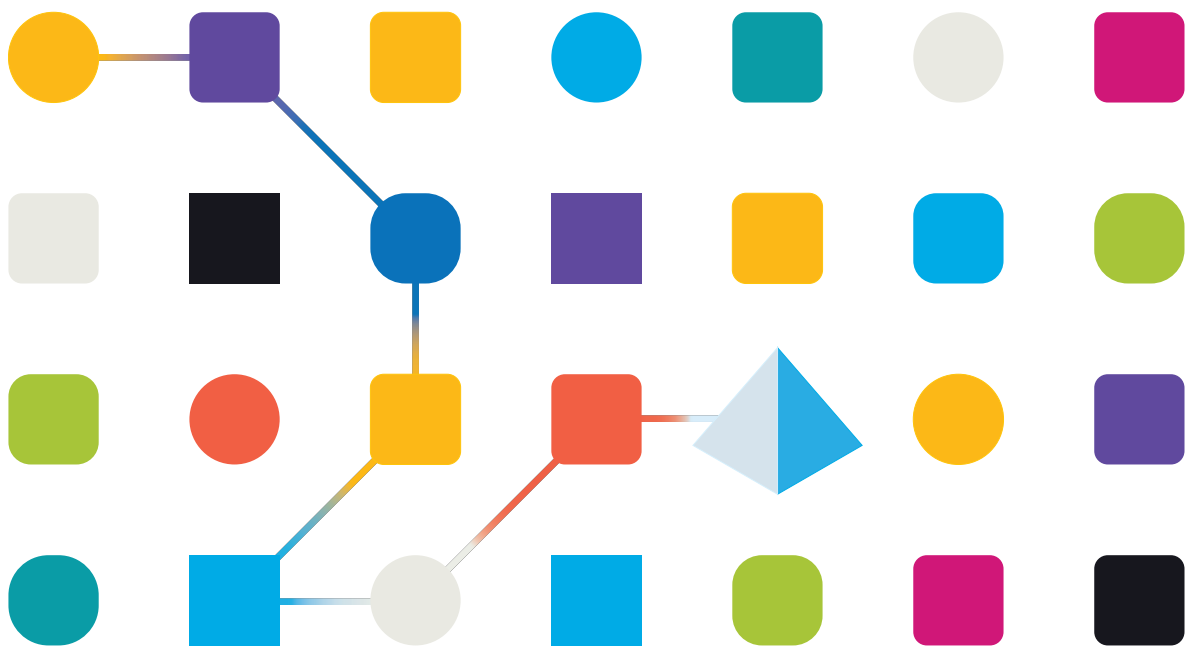


blueprism[®]

Hub and Interact 4.2 Sicherheit – Referenzhandbuch

Dokumentrevision: 1.0



Marken- und Urheberrechtshinweise

Die in diesem Handbuch enthaltenen Informationen sind das Eigentum von Blue Prism Cloud Limited und/oder verbundenen Unternehmen, müssen vertraulich behandelt werden und dürfen ohne schriftliche Genehmigung eines autorisierten Vertreters von Blue Prism nicht an Dritte weitergegeben werden. Ohne die schriftliche Erlaubnis von Blue Prism Cloud Limited oder verbundenen Unternehmen darf kein Teil dieses Dokuments in jeglicher Form oder Weise vervielfältigt oder übertragen werden, sei es elektronisch, mechanisch oder durch Fotokopieren.

© Blue Prism Cloud Limited, 2001 – 2021

„Blue Prism“, das „Blue Prism“ Logo und Prism Device sind Marken oder eingetragene Marken von Blue Prism Limited und seinen Tochtergesellschaften. Alle Rechte vorbehalten.

Alle anderen Warenzeichen werden hiermit anerkannt und werden zum Vorteil ihrer jeweiligen Eigentümer verwendet.

Blue Prism Cloud Limited und seine verbundenen Unternehmen sind nicht für den Inhalt externer Websites verantwortlich, auf die in diesem Handbuch Bezug genommen wird.

Blue Prism Limited, 2 Cinnamon Park, Crab Lane, Warrington, WA2 0XP, United Kingdom.

Registriert in England: Reg.- Nr. 4260035. Tel.: +44 370 879 3000. Web: www.blueprism.com

Inhalt

Blue Prism Interact Sicherheit	4
Verschlüsselung	5
Authentifizierung	6
Netzwerkonnektivität	7
Logging	8

Blue Prism Interact Sicherheit

Dieses Dokument bietet eine funktionale und technische Referenz zur Unterstützung bei Kundenfragen, Compliance-Anfragen und eingehenden Anträgen (Request for Proposals, RFP) rund um die Sicherheit. Dieses Handbuch behandelt folgende Themen:

- Verschlüsselung
- Authentifizierung
- Netzwerkkonnektivität
- Logging

Verschlüsselung

Blue Prism Interact verwendet die folgenden Verschlüsselungsmethoden:

Algorithmus	Beschreibung
Verschlüsselung des Datenverkehrs	<p>Nur HTTPS-Kommunikation für die Produktion aktivieren. Erfordert, dass Kunden TLS-Zertifikate für alle Webanwendungen bereitstellen, und alle Kommunikationskanäle müssen gesichert werden.</p> <p>Weitere Informationen zum Konfigurieren von Zertifikaten finden Sie in der Onlinehilfe.</p>
Datenschutz	<p>Das Hub Installationsprogramm generiert ein PFX-Zertifikat und speichert es bei den vertrauenswürdigen Stammzertifizierungsstellen. Alle Anwendungen verwenden es zur Verschlüsselung vertraulicher Daten, wie z. B. Verbindungszeichenfolgen in der Datei appsettings.json.</p> <p>Der Datenschutz verwendet die folgenden Standardalgorithmen:</p> <ul style="list-style-type: none"> • Der Verschlüsselungsalgorithmus ist AES-256-CBC • Der Validierungsalgorithmus ist HMACSHA256 <p>Die Schlüsselgröße beträgt 2048 Bit.</p>
JWT Token-Unterzeichnung	<p>Das Hub Installationsprogramm generiert ein PFX-Zertifikat und speichert es bei den vertrauenswürdigen Stammzertifizierungsstellen. Der Identity Server verschlüsselt damit das JWT-Token und validiert die Lizenzdatei.</p> <p>Das JWT-Token wird durch den RSA-SHA-256-Algorithmus verschlüsselt und die Schlüsselgröße beträgt 2048 Bit.</p>
Identity Management Server (IMS)	<p>Das ist der Autorisierungsserver – Benutzer melden sich über den IMS an, der die Komponenten bestimmt, auf die sie Zugriff haben.</p> <p>Der Identitätsserver verwendet SHA-256 für die Hashwert-Bildung des Client-Geheimnisses und der Client-ID.</p>
Speicherung des Passworts	<p>Die AspNetIdentity-Bibliothek wird für das Passwort-Hashing verwendet und nutzt die folgenden Algorithmen:</p> <ul style="list-style-type: none"> • PBKDF2 mit HMAC-SHA256 • 128-Bit-Salt • 256-Bit-Unterschlüssel • 10000 Iterationen

Der Lizenzschlüssel wird durch den Algorithmus RSA-SHA-512 verschlüsselt.

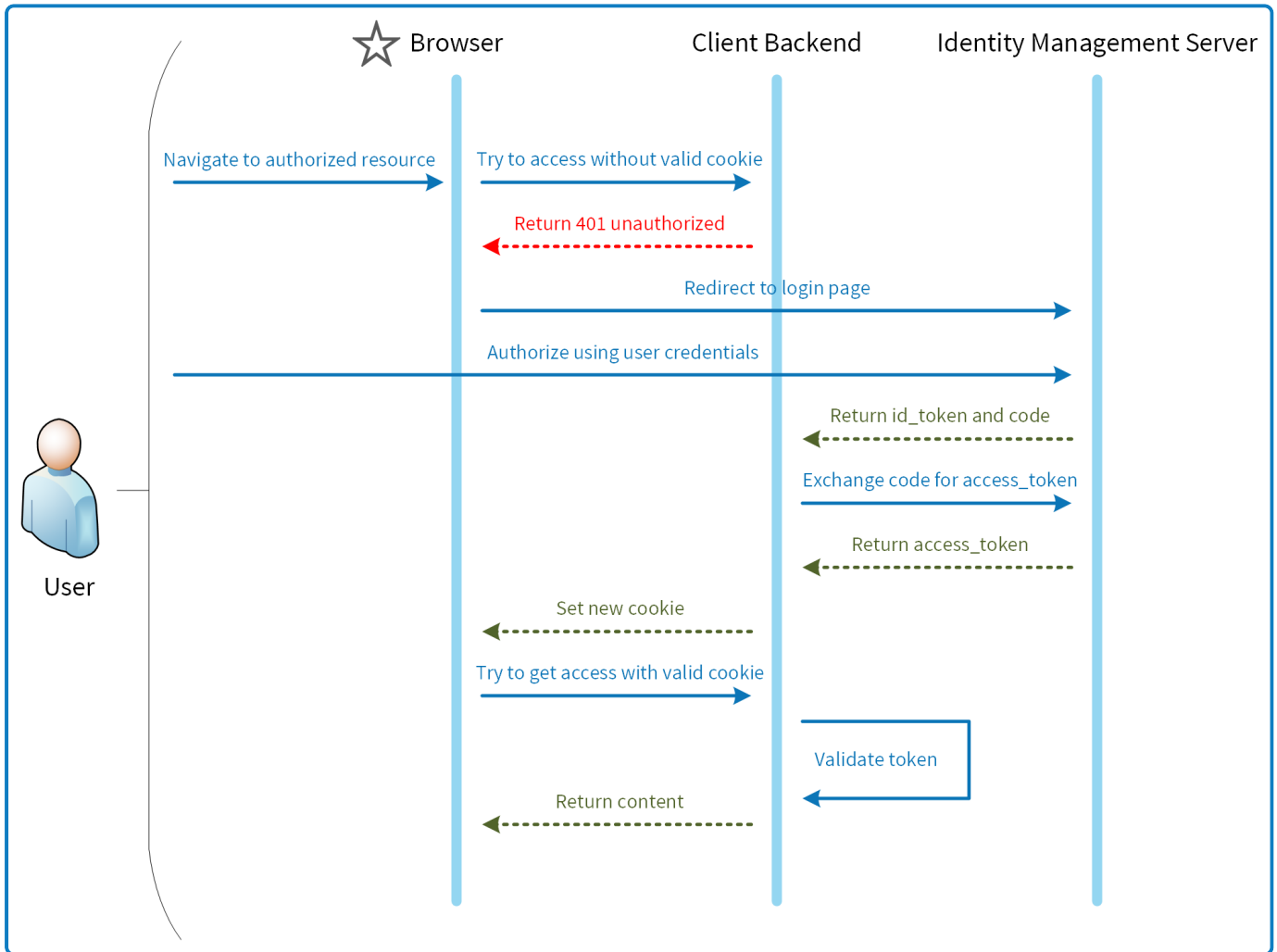
Die Datenbankverschlüsselung ist durch den Microsoft-Verschlüsselungsmechanismus (Transparent Data Encryption – TDE) möglich, muss jedoch manuell in jeder Datenbank implementiert werden. Weitere Informationen finden Sie unter: docs.microsoft.com.

TLS ist standardmäßig auf die Host-Betriebssystemkonfiguration für die TCP- und HTTP-Kommunikation eingestellt und wählt das beste Sicherheitsprotokoll und die beste Version aus. Verfügbare Protokolle und Codierschlüssel werden vom Endbenutzer verwaltet oder automatisch über Microsoft-Sicherheitsupdates gehandhabt.

Authentifizierung

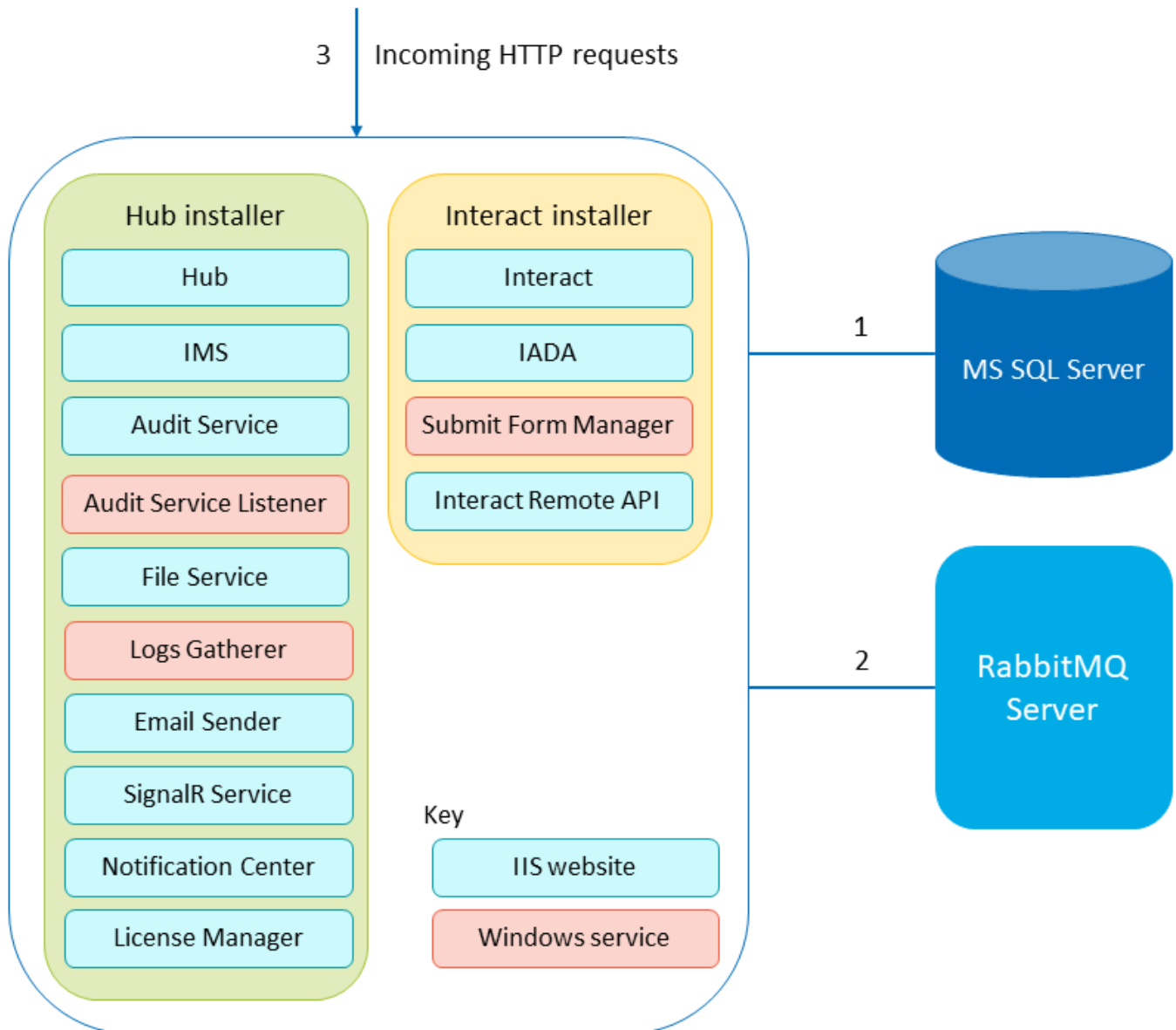
Die Authentifizierung in Interact wird unten beschrieben:

- Es wird ein Identity Server bereitgestellt, der durch das OpenId Connect-Protokoll implementiert wird.
- Die API-Aufrufe aller Benutzer sind autorisiert.
- Alle API-Aufrufe zwischen Anwendungen sind autorisiert.
- Das Zugriffstoken wird nur in HTTPS-Cookies gespeichert, die nicht abgefangen oder modifiziert werden können.



Netzwerkonnektivität

Das Diagramm bietet einen Überblick über die gemeinsame Kommunikation, die auf der Interact Plattform erfolgt.



1. Gesichert durch TLS – Zertifikat-basierte Verschlüsselung wird durch die Nutzung der SQL Server-Funktion unterstützt, die selbstsignierte Zertifikate automatisch generieren oder ein vorhandenes überprüfbares Zertifikat nutzen kann.
2. Verwenden des AMQP-Protokolls.
3. Die Verbindung ist standardmäßig über HTTPS gesichert.

Logging

Blue Prism Interact Logging, das in Interact durchgeführt wird, ist unten beschrieben:

- Logs werden in TXT-Dateien an vom Benutzer konfigurierbaren Speicherorten gespeichert – der Standardspeicherort befindet sich im Ordner Blue Prism > Interact innerhalb des Installationsverzeichnis. Das kann jedoch durch Bearbeiten des Wertes der folgenden Zeile in der Datei nlog.config im Interact Ordner des Installationsverzeichnis konfiguriert werden:

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

Wobei `.\` das Interact Installationsverzeichnis ist. Das Standardverzeichnis ist `C:\Programme (x86)\Blue Prism\Interact\`

Nach der Änderung muss IIS neu gestartet werden.

- Die Standard-Logging-Stufe kann in der Datei appsettings.json konfiguriert werden:
 - Standard: Informationen
 - System: Warnung
 - Microsoft: Warnung

Die folgenden Logging-Stufen können angewendet werden: Kritisch, Debuggen, Fehler, Informationen, Keine, Trace, Warnung. Weitere Informationen über diese Logging-Stufen finden Sie unter docs.microsoft.com.

Die Datei befindet sich im Blue Prism > Interact Ordner im Installationsverzeichnis – bearbeiten Sie die Datei, um die Logging-Stufen zu ändern. Nach einer Aktualisierung der Logging-Stufe muss der World Wide Web Publishing-Dienst neu gestartet werden, damit die Änderung wirksam wird.

- Logs werden jeden Monat in Zip-Dateien archiviert, um die Dateigröße zu reduzieren.
- Logs enthalten keine persönlichen oder vertraulichen Informationen.