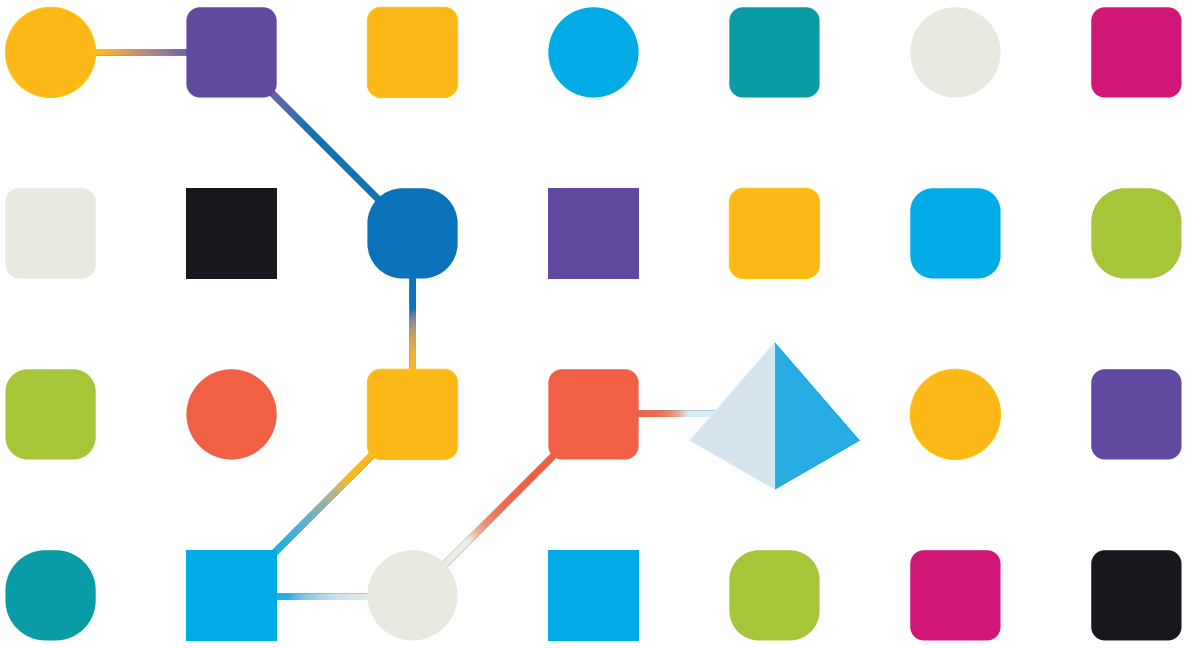
blueprism®

Hub and Interact 4.5

Guide de référence de sécurité

Révision des documents : 1.0



Marques déposées et droits d'auteur

Blue Prism Limited, 2 Cinnamon Park, Crab Lane, Warrington, WA2 0XP, United Kingdom. Enregistré en Angleterre : numéro d'enregistrement 4260035. Tél. : +44 370 879 3000. Web : www.blueprism.com

Contenu

Sécurité de Blue Prism Interact

Ce document fournit un point de référence fonctionnel et technique pour répondre aux préoccupations des clients, aux questions de conformité et aux appels d'offres (Request for Proposals, RFP) concernant la sécurité. Ce guide couvre les points suivants :

- Cryptage
- Authentification
- Connectivité réseau
- Logging

Cryptage

Blue Prism Interact utilise les méthodes de chiffrement suivantes :

Algorithme	Description
Chiffrement du trafic	Activer la communication HTTPS uniquement pour la production. Oblige les clients à fournir des certificats TLS pour toutes les applications Web et tous les canaux de communication doivent être sécurisés. Pour plus d'informations sur la configuration des certificats, consultez l'aide en ligne.
Protection des données	Le programme d'installation de Hub génère un certificat PFX et l'enregistre dans les autorités de certificat racine de confiance. Toutes les applications l'utilisent pour chiffrer les données sensibles, telles que les chaînes de connexion dans le fichier appsettings.json. La protection des données utilise les algorithmes par défaut suivants : • L'algorithme de chiffrement est AES-256-CBC • L'algorithme de validation est HMACSHA256 La clé fait 2 048 bits.
Signature de jeton JWT	Le programme d'installation de Hub génère un certificat PFX et l'enregistre dans les autorités de certificat racine de confiance. Le serveur d'identité l'utilise pour chiffrer le jeton JWT et valider le fichier de licence. Le jeton JWT est chiffré par l'algorithme RSA-SHA-256 et la clé fait 2 048 bits.
Authentication Server	Il s'agit du serveur d'autorisation. Les utilisateurs se connectent via Authentication Server, ce qui détermine les composants auxquels ils ont accès. Le serveur d'authentification utilise SHA-256 pour hacher le secret client et l'ID client.
Stockage du mot de passe	La bibliothèque AspNetIdentity est utilisée pour le hachage de mot de passe et utilise les algorithmes suivants : • PBKDF2 avec HMAC-SHA256 • Salt 128 bits • Sous-clé 256 bits • 10 000 itérations

La clé de licence est chiffrée par l'algorithme RSA-SHA-512.

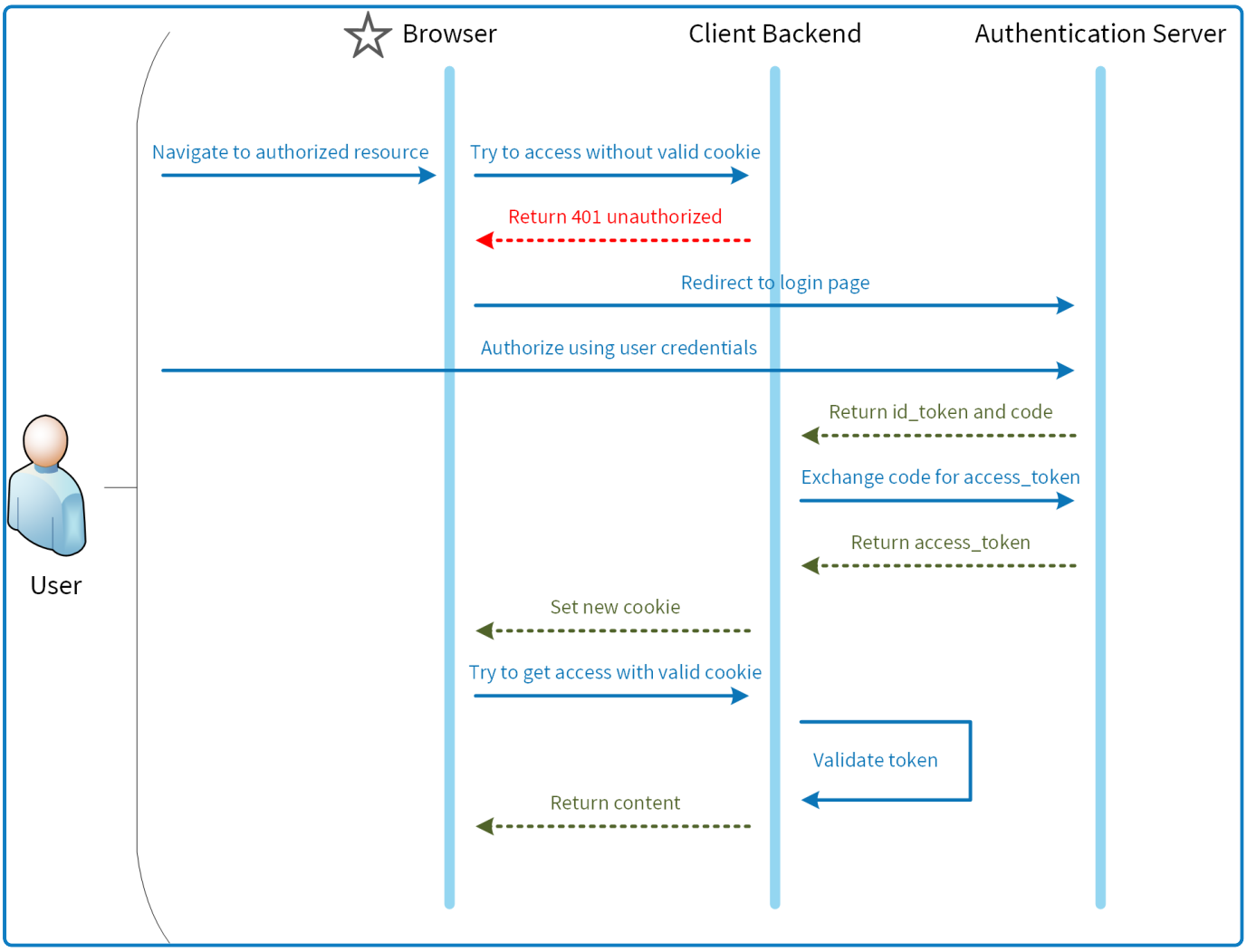
Le chiffrement de base de données peut être fourni par le mécanisme de chiffrement Microsoft (Transparent Data Encryption, TDE) mais doit être implémenté manuellement sur chaque base de données. Pour plus d'informations, voir docs.microsoft.com.

Par défaut, TLS utilise la configuration du système d'exploitation hôte pour les communications TCP et HTTP, en sélectionnant le meilleur protocole et la meilleure version de sécurité. Les protocoles et les chiffrements disponibles sont gérés par l'utilisateur final ou automatiquement via les mises à jour de sécurité Microsoft.

Authentification

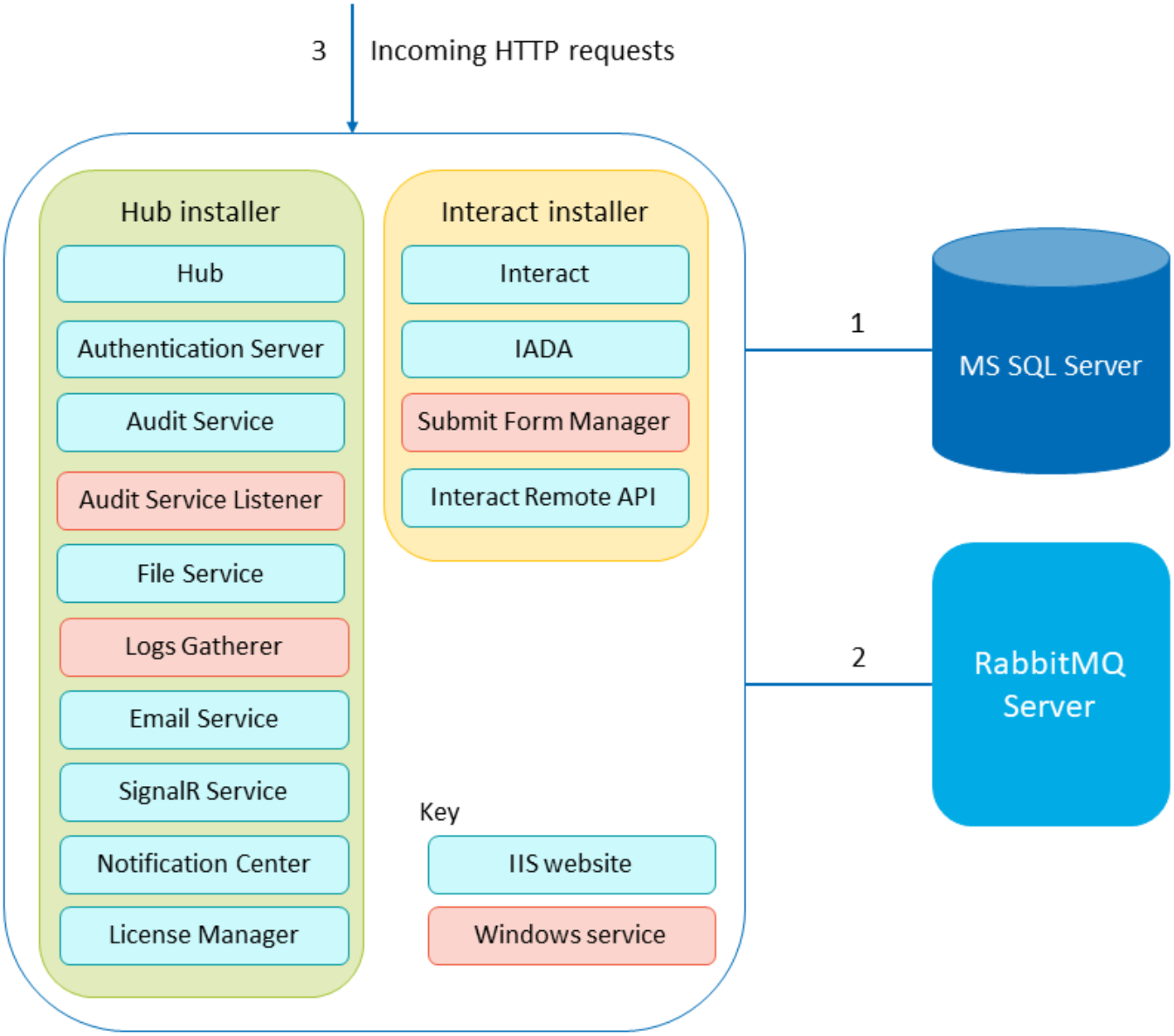
L'authentification dans Interact est décrite ci-dessous :

- Un serveur Authentication Server est fourni et implémenté par le protocole OpenId Connect.
- Tous les appels d'API des utilisateurs sont autorisés.
- Tous les appels d'API entre les applications sont autorisés.
- Le jeton d'accès est stocké dans les cookies HTTPS uniquement, ce qui ne peut pas être intercepté ou modifié.



Connectivité réseau

Le diagramme fournit un aperçu de la communication commune qui se produit avec la plateforme Interact.



1. Sécurisé par TLS : le chiffrement basé sur les certificats est pris en charge en exploitant la fonctionnalité SQL Server qui peut générer automatiquement des certificats autosignés ou exploiter un certificat vérifiable existant.
2. Utilisation du protocole AMQP.
3. La connexion est sécurisée via HTTPS par défaut.

Logging

Le logging de Blue Prism Interact effectué dans Interact est décrit ci-dessous :

- Les logs sont enregistrés dans des fichiers TXT dans des emplacements configurables par l'utilisateur. L'emplacement par défaut est dans le dossier Blue Prism > Interact dans le répertoire d'installation, mais cela peut être configuré en modifiant la valeur de la ligne suivante dans le fichier nlog.configfile, situé dans le dossier Interact du répertoire d'installation :

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

  Où `.\` est le répertoire d'installation Interact. Par défaut, il s'agit de C:\Program Files (x86)\Blue Prism\Interact\

  Une fois la valeur mise à jour, redémarrez IIS.

- Le niveau de logging par défaut peut être configuré dans le fichier appsettings.json :
  - Par défaut : Informations
  - Système : Avertissement
  - Microsoft : Avertissement

  Les niveaux de logging suivants peuvent être appliqués : Critique, Débogage, Erreur, Informations, Aucun, Trace, Avertissement. Pour plus d'informations sur ces niveaux de logging, voir docs.microsoft.com.

  Le fichier est situé dans le dossier Blue Prism > Interact du répertoire d'installation. Modifiez le fichier pour modifier les niveaux de logging. Après une mise à jour du niveau de logging, le service World Wide Web Publishing doit être redémarré pour que la modification prenne effet.

- Les logs sont archivés dans des fichiers zip chaque mois pour réduire le volume de fichiers.
- Les logs ne contiennent aucune information personnelle ou sensible.