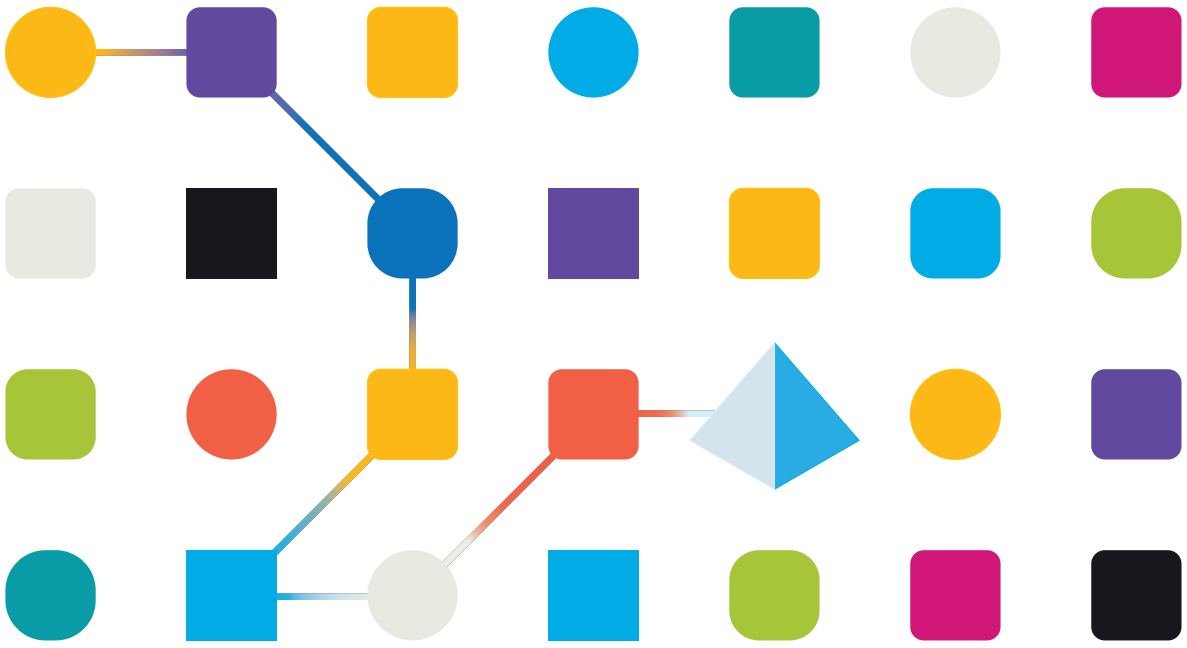
blueprism®

Hub and Interact 4.1

セキュリティリファレンスガイド

Document Revision: 1.0



商標および著作権

Blue Prism Limited, 2 Cinnamon Park, Crab Lane, Warrington, WA2 0XP, United Kingdom。
英国で登録：登録番号4260035。電話：+44 370 879 3000。Web：www.blueprism.com

内容

Blue Prism Interactセキュリティ

本書は、セキュリティに関する顧客の懸念、コンプライアンスに関する問い合わせ、および提案依頼書(RFP)を受けたときに役立つ、機能的および技術的なリファレンスを提供します。このガイドでは、以下について説明します。

- 暗号化
- 認証
- ネットワークコネクティビティ
- ロギング

暗号化

Blue Prism Interactでは、次の暗号化方法を使用します。

アルゴリズム	説明
トラフィック暗号化	本番環境にHTTPSのみの通信を有効にします。すべてのWebアプリケーションに対してTLS証明書を提供することを顧客に要求し、すべての通信チャネルをセキュリティで保護する必要があります。 証明書の構成についての詳細はオンラインヘルプの「」を参照してください。
データ保護	Hubインストーラーは PFX証明書を生成し、信頼されたルート証明局に保存します。すべてのアプリケーションは、appsettings.jsonファイル内の接続文字列など、秘密データを暗号化するために使用されます。 データ保護では、次のデフォルトのアルゴリズムを使用します。 • 暗号化アルゴリズムはAES-256-CBC • 検証アルゴリズムはHMACSHA256 キーサイズは2048ビットです。
JWTトークン署名	Hubインストーラーは PFX証明書を生成し、信頼されたルート証明局に保存します。IDサーバーは、その証明書を使用してJWTトークンを暗号化し、ライセンスファイルを検証します。 JWTトークンはRSA-SHA-256アルゴリズムによって暗号化され、キーサイズは2048ビットです。
ID管理サーバー(IMS)	これは認証サーバーです。IMS を介してユーザーがログインし、アクセスできるコンポーネントを決定します。 IDサーバーはSHA-256を使用してクライアントシークレットとクライアントIDをハッシュ化します。
パスワードのストレージ	AspNetIdentityライブラリは、パスワードハッシュに使用され、次のアルゴリズムを使用します。 • PBKDF2、HMAC-SHA256使用 • 128ビットソルト • 256ビットサブキー • 10000回の反復

ライセンスキーはRSA-SHA-512アルゴリズムによって暗号化されます。

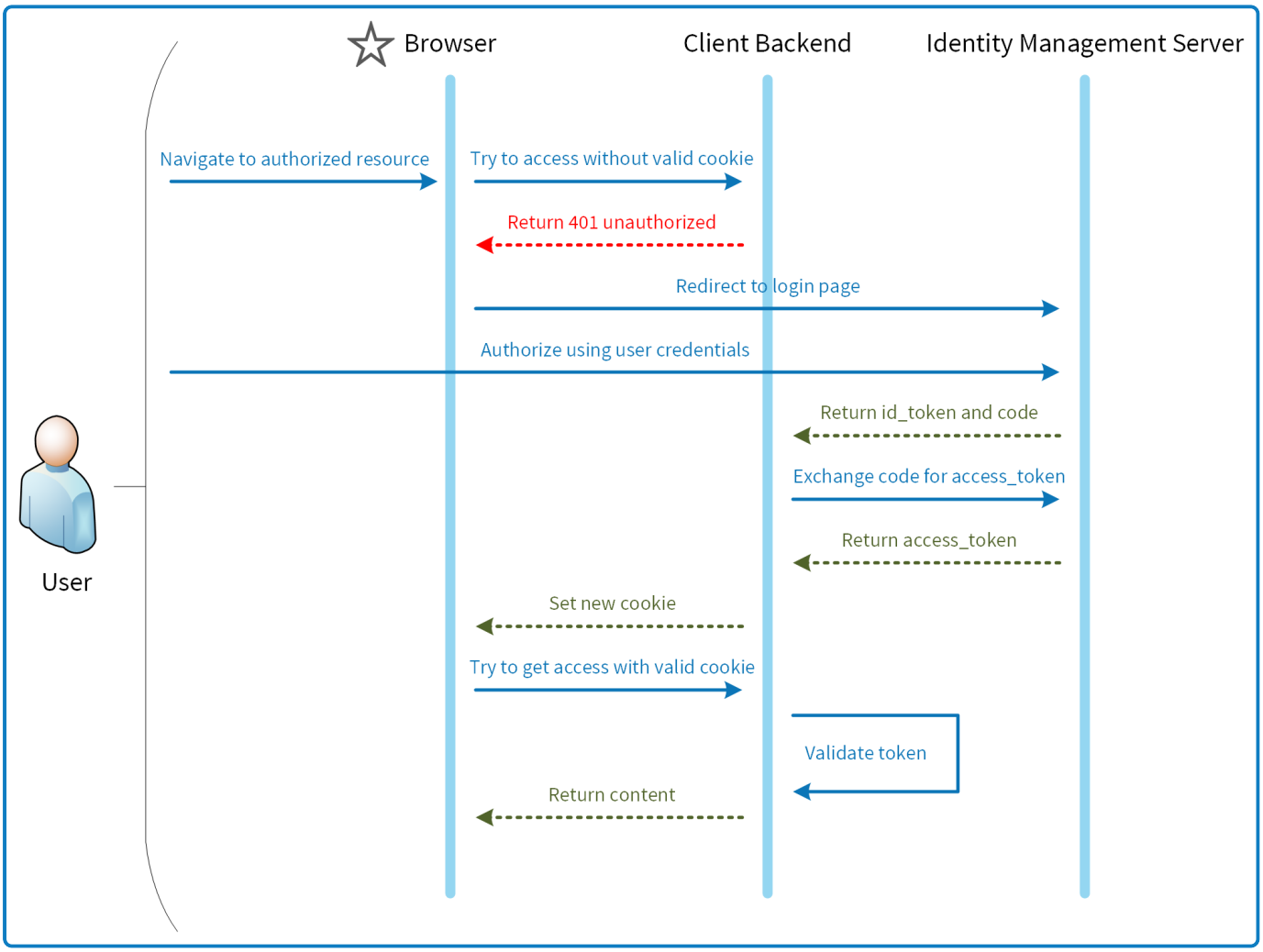
データベースの暗号化は、Microsoftの暗号化メカニズム(Transparent Data Encryption - TDE) によって提供できますが、各データベースに手動で実装する必要があります。詳細については、docs.microsoft.comを参照してください。

TLSは、TCPおよびHTTP通信の両方のホストオペレーティングシステム構成にデフォルト設定され、最適なセキュリティプロトコルとバージョンを選択します。利用可能なプロトコルと暗号は、エンドユーザーによって管理されるか、Microsoftのセキュリティ更新によって自動的に処理されます。

認証

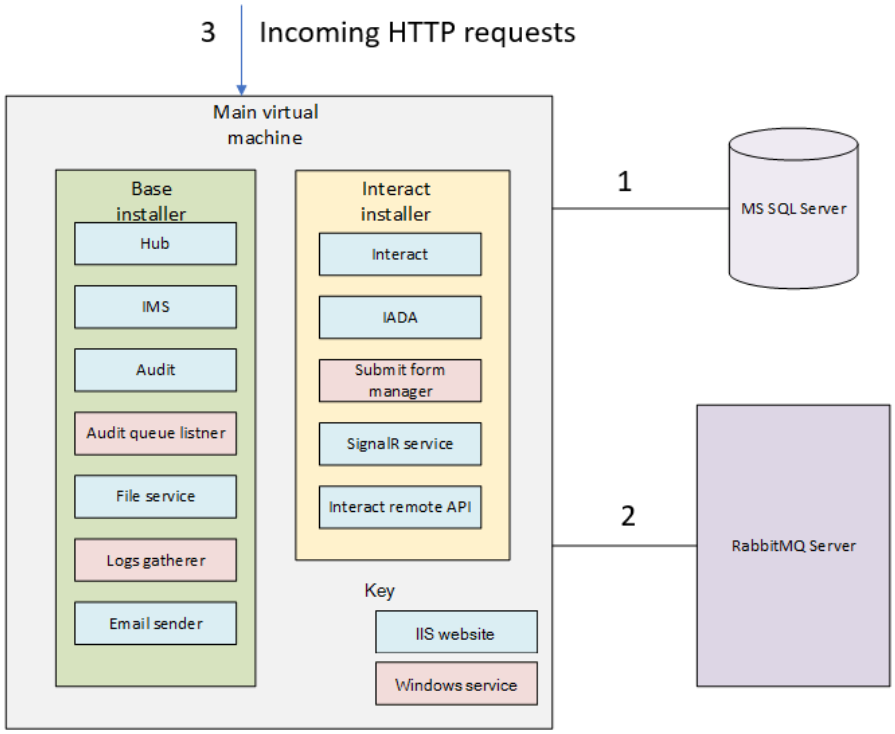
Interactでの認証の概要は以下のとおりです。

- OpenId Connectプロトコルによって実装されるID Serverが提供されます。
- すべてのユーザーのAPI呼び出しが許可されます。
- アプリケーション間のすべてのAPI呼び出しが許可されます。
- アクセストークンは、傍受または変更できないHTTPSクッキーにのみ保存されます。



ネットワークコネクティビティ

この図は、Interactプラットフォームで発生する一般的な通信の概要を示しています。



1. TLSによる保護 - 証明書ベースの暗号化は、自己署名証明書を自動生成したり、既存の検証可能な証明書を活用したりできるSQL Server機能を利用することでサポートされています。
2. AMQPプロトコルを使用しています。
3. 接続は、デフォルトではHTTPSを介して保護されます。

ロギング

Interactで実行されるBlue Prism Interactのロギングの概要を以下に示します。

- ログは、ユーザーが設定可能な場所にTXTファイルで保存されます。デフォルトの場所はインストールディレクトリ内のBlue Prism > Interactフォルダーですが、これはインストールディレクトリのInteractフォルダーにあるnlog.configfileの次の行の値を編集することで設定できます。

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

  ここで、.\はInteractのインストールディレクトリです。デフォルトでは、これはC:\Program Files (x86)\Blue Prism\Interact\です。

  更新が完了したら、IISを再起動します。
- デフォルトのロギングレベルは、appsettings.jsonファイルで設定できます。
  - デフォルト：Information
  - システム：Warning
  - Microsoft：Warning

  次のロギングレベルを適用できます。Critical、Debug、Error、Information、None、Trace、Warning。これらのロギングレベルの詳細については、docs.microsoft.comを参照してください。

  ファイルは、インストールディレクトリ内のBlue Prism > Interactフォルダーにあります。ファイルを編集してロギングレベルを変更します。ロギングレベルの更新後、変更を有効にするには、World Wide Web Publishingサービスを再起動する必要があります。
- ログは、ファイルサイズのボリュームを縮小するため、毎月zipファイルにアーカイブされます。
- ログには、個人情報や秘密情報は一切含まれません。