テクニカル・ホワイトペーパー

NOK NOK LABS MULTIFACTOR AUTHENTICATION

Any device.
Any application.
Any authenticator.

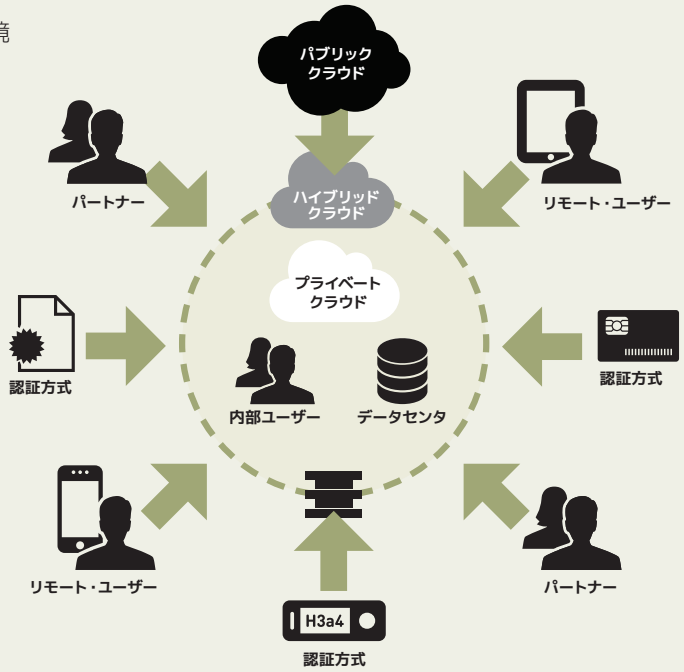
Nok Nok
LABS

本書の内容

Nok Nok
LABS

はじめに

図1
現在の複雑な認証環境



かつて認証はシンプルでした。標準のデスクトップからログインするユーザーは、限られた数のアプリケーションへのアクセスのみを必要としていました。アプリケーションは社内のデータセンターに配置され、ネットワークを境界としてファイアウォールで保護されていました。認証のために、パスワードは十分であり、便利でした。それらはシンプルで、安価で、どこでも使用可能でした。

ある重要なアプリケーションで、より強力な認証形式が必要となる場合、ハードウェア・トークンや公開鍵インフラ（PKI）を利用しました。そのような強度の高い認証方式は企業内での特定の利用場面やインターネット・バンキングでの使用に限られていたため、煩わしく、高価ですが、このような不便さを受け入れて付き合ってきました。　そのため、セキュリティ・アーキテクチャーや認証システムは比較的シンプルかつ静的な環境に適するように構築されていました。

しかし、ここ数年のうちに、環境は急激に変化しました。（図1参照）　ユーザーは標準化されたPCの環境から多種多様なスマートフォンやタブレットの世界へ移ってきました。ユーザーは移動中でもデバイスを切り替えながら、リモートから作業をするようになってきました。アプリケーションもモバイル化してきました。もはや、それらは集中管理されているデータセンターだけに配置されているということはありません。クラウド上に散在したり、パートナーによってホストされたり、モバイル・デバイス上にあります。標準で静的な環境を念頭において構築された認証システムは、このような複雑で異種混在する使用場面に対応できなくなっているのです。

組織は複数の認証スタックの導入を経験し、それぞれ特定の使用場面に対応してきています。しかし、それらのスタックはインテグレーションされていないので、個別に認証のしくみを導入し、展開し、管理しなければなりません。異なる使用場面が増加すると、認証スタックも複数並行して存在することになり、コストがかかり、複雑で、管理の困難な認証インフラができあがってしまいます。段階的に強力な認証のアプローチを取ることも、最低限の共通基準であるパスワードによるアプローチを取ることも、今日の組織やユーザーのニーズにマッチしていません。

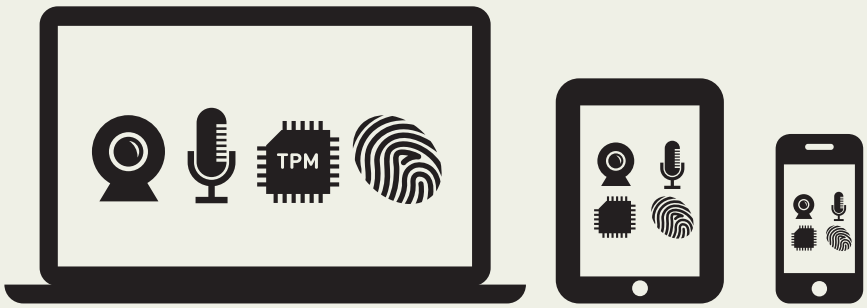
ユーザーも認証には苦労しています。標準的なユーザーによって利用されるサービスの数が増加しているため、ユーザーが記憶する必要のあるユーザー名とパスワードの数も増加しています。このような状況に対し、ユーザーは共通のパスワードや記憶しやすいパスワードを使っているのが現状です。しかし、そのようなパスワードは攻撃に対して脆弱で、セキュリティを低下させます。この状況に対応するため、オンラインやモバイルのアプリケーション・プロバイダ（Relying Partyと呼ばれる）は大文字のアルファベット、特殊文字や数字を追加することでパスワードが複雑になるように推進しています。パスワードは思い

出すのがより困難になるのと同時に、モバイル・デバイスでは一般的な小さく扱いにくいキーボードからの入力を難しくしています。このような状況からユーザーは一つのパスワードを記憶して、同じパスワードを使い回すので、セキュリティが低下するというたちの悪い状況が続いています。
その結果、侵害は、別の侵害を次々と誘発しているので、ドミノ効果の様相を呈しているのです。

幸いなことに、多くのデバイスはすでにユーザーに優しく、低コストで強力な認証を実現可能なテクノロジーを搭載しています。（図2参照） 例えば、ノートPCやデスクトップPCはTrusted Platform Modules(TPMs)が搭載されて久しく、指紋センサーを搭載しているケースさえあります。スマートフォンやタブレットはパワフルなカメラや感度の高いマイクロフォンを搭載しています。これらは生体認証に利用可能です。最近出てきたデバイスには指紋センサーや虹彩認識さえ搭載されています。製造メーカーは重要なデータや操作をハードウェア・レベルで保護することが可能な組み込み機能、Trusted Execution Environments(TEEs)やSecure Elements(SEs)を搭載し始めています。現在のデバイスはパワフルなマルチコア・プロセッサや数ギガバイトのメモリを搭載しており、高い計算能力を必要とする認証アルゴリズムの利用を可能にしています。

今日のデバイスは強力な認証のためのビルディング・ブロックを持っていますが、アプリケーションは、これらのメカニズムの利点を生かせる標準化された方法を持っていません。スマートフォンはカメラを搭載していますが、顔認証のためのソフトウェアを搭載している機種は少しです。例えば、顔によるバイオメトリクス認証アプリケーションがFacebookのモバイル・アプリケーションに組み込まれていないので、スマートフォンのカメラを使ってユーザーがFacebookへの認証を行うのは不可能です。この認証の問題を解決する必要なインテグレーションはこれまで存在しませんでした。この非常に重要な課題に対応するため、Nok Nok Labsではソリューションを開発したのです。

図2
デバイス上で利用可能な認証メカニズム



認証基盤の統一

Nok Nok Labs（以下NNL）はどんなデバイスであっても、そのデバイス上に存在するあらゆる認証方式をアプリケーションが活用可能とするために不可欠なソフトウェアとインテグレーションを提供しています。実際、NNLのソリューションはアプリケーションがすでに出荷済みの数十億ものデバイスが持つセキュリティ機能を活用し、強力な認証を実現することを可能にします。
それはFast IDentity Online（FIDO） Alliance*[1]によって定義されたUniversal Authentication Framework(UAF)に基づいた標準ベースのエンドツーエンド・プラットフォームにこれらの機能を組み込むことで達成されます。

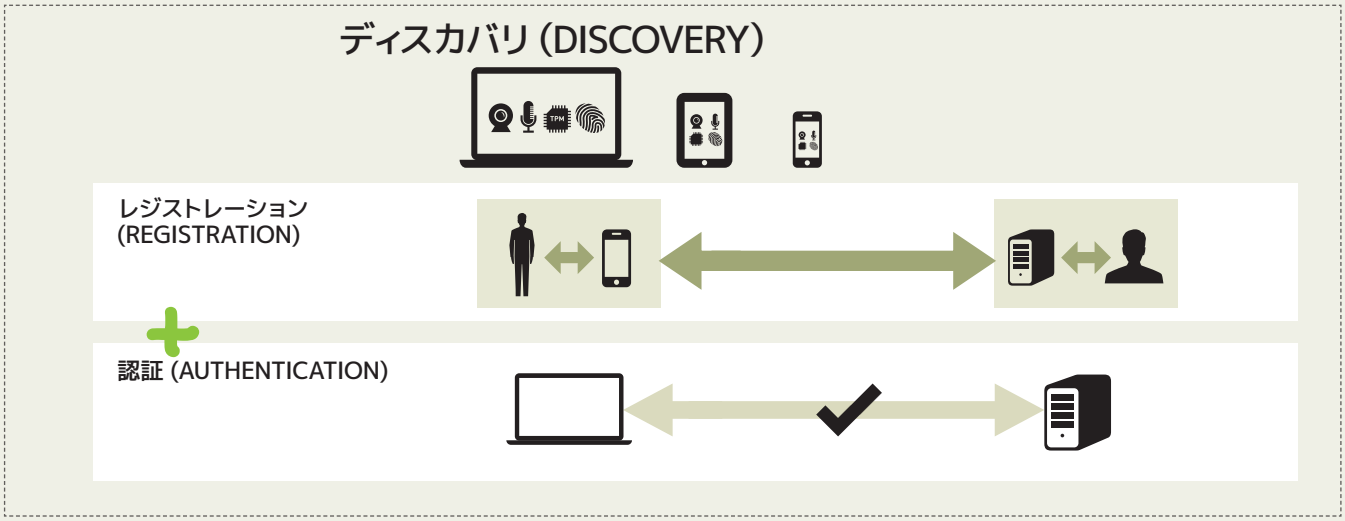
NNLは組織がすべての認証ニーズに対応するシングルの統一されたシステムを導入することを可能にします。パスワードの必要性を最小化することにより、パスワードが持つ、ユーザーの使い勝手に関する弱点を克服しています。どんなデバイスのどんな認証方式もサポートする統一されたモジュール型の認証基盤をつくることにより、今日の認証強化ソリューションが個別に並列して存在し、連携していない状況に対応します。さらに新しい認証方式が将来利用可能になった場合でも容易にサポートできるようになっています。NNLのソリューションはReplying Partyのアプリケーションとインテグレーションされる認証サーバーと、モバイル・アプリケーションでUAF認証を可能にするアプリケーションSDKで構成されています。

このような環境を可能にするのがFIDO Universal Authentication Framework(UAF)プロトコルです。これはモジュール型かつ拡張可能な業界標準のプロトコルであり、どんな認証方式やオーセンティケータであっても実質的に認証を実現できます。UAFは個々のオーセンティケータを抽象化し、認証サーバーとオーセンティケータの相互運用性を実現します。クライアントとサーバー間のすべての通信はセキュアなTransport Layer Security(TLS)チャネルで実行されます。 データベースへの暗号化

1. www.fidoalliance.orgを参照

UNIVERSAL AUTHENTICATION FRAMEWORKプロトコル

図3
UAFオペレーション

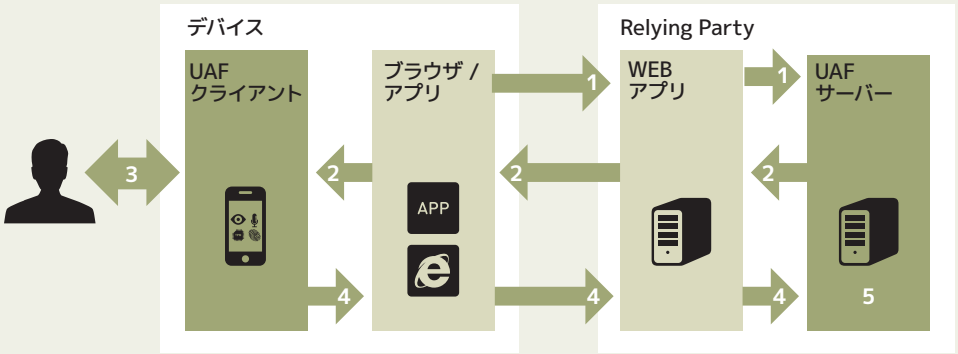


UAFは2つのオペレーションをサポートしています。すなわち、レジストレーション（Registration）と認証（Authentication）であり、これらのオペレーションは両方ともディスカバリ（Discovery）部分を伴っています。（図3参照）

ディスカバリ（Discovery）

ディスカバリ部分は、UAFの能力の核心部分を司っており、エンドツーエンドの認証フレームワークに対し、どのようなオーセンティケータでも仮想的にインテグレーション可能となっています。UAFはポリシー・ベースのディスカバリ・メカニズムを使い、オペレーションで利用される適切な認証方式をネゴシエーションします。それぞれのオペレーションの最中に、サーバーはクライアントに対し、どの認証方式を受け入れることが可能かを伝達します。クライアントはデバイス上で利用可能なポリシー・オプションをユーザーに提示し、ユーザーはその中から特定のRelying　Party用に認証方式を選択することになります。サーバーに対して、デバイスが持つ機能リストを明示することなしに、デバイスの機能を利用可能にするため、このアプローチではプライバシーの問題を回避できるのです。

図4
UAFにおけるレジストレーション



1 レジストレーション開始

2 ポリシーを含む
レジストレーション要求

3 示されたポリシーに従い選択されたオーセンティケータにユーザを登録し、新たに鍵のペアを生成

4 公開鍵を含むレジストレーション応答を送信

5 トラスト・ストアを使用して、（証明：Attestationを含む）レジストレーション応答の有効性を検証

レジストレーション(REGISTRATION)

レジストレーション（登録）オペレーション（図4参照）の間、クライアントはサーバーによって提示された受け入れ可能なオーセンティケータのリストをもとに、1つもしくはそれ以上のオーセンティケータを持つデバイスをユーザーに登録させます。クライアントはユーザー、オーセンティケータ、RELYING PARTYに対し、ユニークな認証鍵（AUTHENTICATION KEY）のペアを生成します。公開鍵はサーバーに送られ、秘密鍵はクライアント上にセキュアにストアされます。

サーバーはこのプロセスの一部として、事前に確立済みの証明鍵（ATTESTATION KEY）を使って、オーセンティケータが本物であることを検証します。これにより、偽のオーセンティケータを利用する攻撃者のリスクを低減します。

レジストレーションではユーザーに対し、オーセンティケータ固有のアクションを要求します。例えば、ユーザーは自身の指紋を登録するために、指紋センサーに指を何度か滑らせることが求められます。ユーザーのレジストレーションが成功したら、新たな鍵のペアが生成されます。この後の他のRELYING PARTYとのレジストレーションのオペレーションでは、ユーザーは指を一度だけ滑らせて、既存のバイオメトリクス・データと新規のアカウントをリンクさせるのです。

ユーザーのプライバシーを保護するため、バイオメトリクス・データはサーバーには送られません。その代わりに、そのデータから生成された再生不可能なテンプレート*[2]をローカルでセキュアにストアし、認証の際に認証用の秘密鍵の解錠を指示するのに使われます。

認証(Authentication)

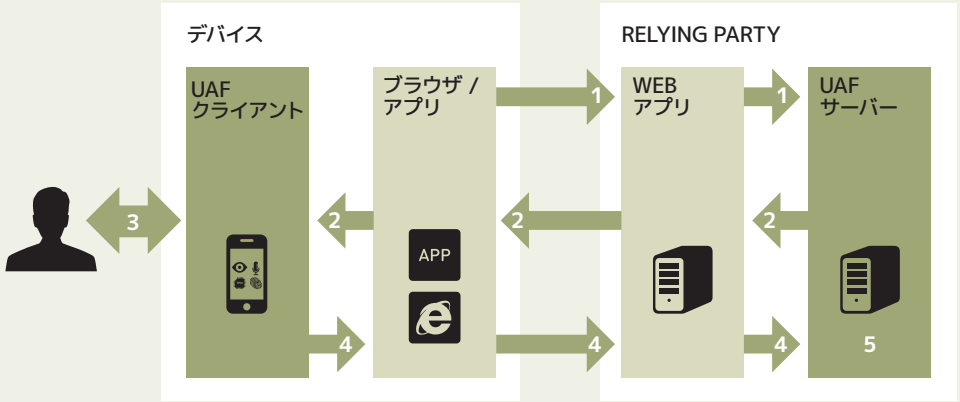
UAF認証は2つのパートで構成されています。

1. クライアントに対するユーザーのローカル認証
2. クライアントのサーバーでの認証

サーバーへの認証はチャレンジ・レスポンス・プロトコルを使って実行されます。サーバーがチャレンジを生成し、認証要求にそれを含めてクライアントに送信します。サーバーは要求メッセージに、そのセッションで受け入れ可能なオーセンティケータの選択肢を示します。クライアントはそれらのオーセンティケータを選択し、特定のオーセンティケータのモダリティ（様式）によって要求されるアクションをユーザーに指示します。例えば、声によるバイオメトリクスのオーセンティケータであれば、ユーザーに声のサンプルを要求します。ユーザーがローカルで認証されれば、クライアントはチャレンジに対するレスポンスをレジストレーションの際の認証鍵を使って計算し、レスポンスをサーバーに返します。レスポンスを検証することによって、サーバーはユーザーが認証鍵のコントロールを持つことを認証します。デバイスの能力によって、認証のレスポンスの計算はソフトウェアで実行されたり、セキュアなハードウェアで実行されたりします。

UAFは認証のステップの一部として、認証を使って、ユーザーによるトランザクションの確認を獲得する機能を提供しています。ユーザーの確認を得るためにトランザクションの詳細が示されます。ユーザーはデバイスへの認証によって、トランザクションを承認することになります。このアプローチではRelying Partyに対し、トランザクションを開始するのに使用したデバイスとは異なるモバイル・デバイスのような2つ目のデバイスをトランザクションの確認用端末として使うことも認めています。

図 5
UAFにおける認証



1 認証開始
2 認証ポリシーとチャレンジを含む認証ページを送信
3 示されたポリシーに従い選択されたオーセンティケータを使って、ユーザを認証
4 認証応答をWEBアプリに送信
5 公開鍵を利用して、認証応答の有効性を検証

THE S3 AUTHENTICATION SUITE

NNL™ S3 Authentication Suiteは、シンプルで、強度のあるスケーラブルな認証を提供しています。FIDO Certified™ のS3 Authentication Suiteは以下の要素で構成されます。

- The Nok Nok Authentication Server
- The Nok Nok App SDK（Androidデバイス用、iOSデバイス用）
- The Nok Nok Authenticator SDK（Androidデバイス用、iOSデバイス用）

2. テンプレートの詳細は使用するAUTHENTICATORにより変わります。

NOK NOK APP SDK

The Nok Nok App SDKは、モバイル・アプリケーションにUAFクライアントを組み込み、新しいSamsung社製Galaxy®、Samsung Note®、Samsung Tab®、富士通Arrows NX、シャープAQUOS Zetaや他のデバイスに搭載された指紋センサー等のデバイスのネイティブなUAF機能認証のために使います。The Nok Nok App SDKはiOSデバイス上のTouch IDと直接インテグレーションも可能であり、古いiOSデバイスではオーセンティケータとしてデバイスのパスコードを利用することも可能です。

認証プロセスの間、The Nok Nok App SDKはサーバーによって指定された1つもしくはそれ以上のオーセンティケータを使って、ユーザーをローカルで認証します。ローカル認証に成功すると、サーバーでのユーザー認証のために使われるRelying Party向けの認証鍵を取り出します。このメカニズムには2つの利点があります。

1. サーバーに対してローカル認証の詳細は抽象化されます。これにより、どんな認証方式でも使えます。
2. センシティブなバイオメトリクス情報はサーバーには送られず、ユーザーのプライバシーは保護されます。

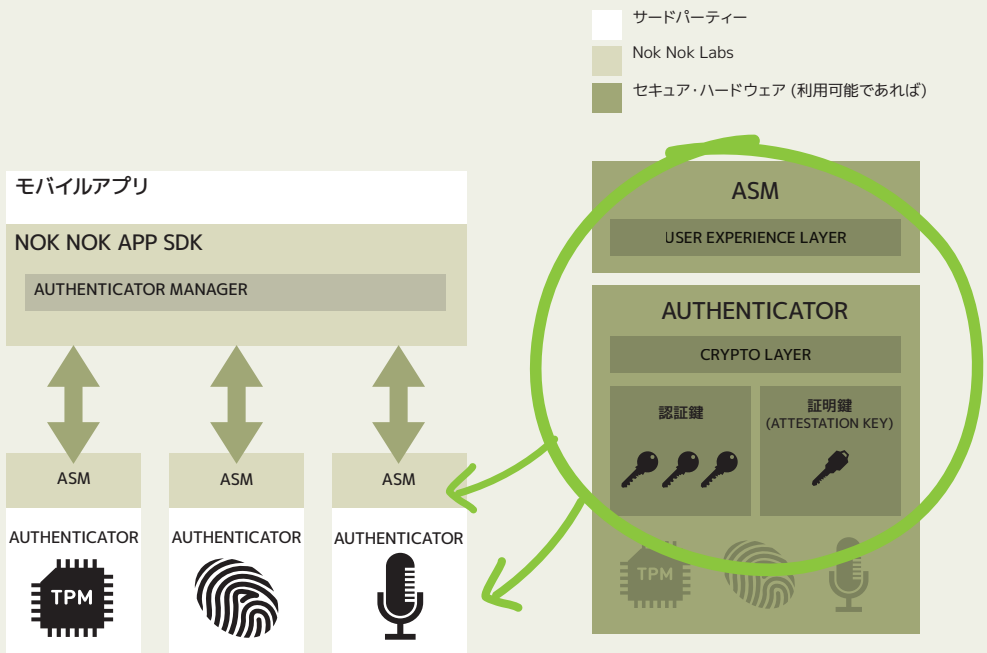
The Nok Nok App SDKは高い拡張性のあるアーキテクチャーを持っています。このデザインにより、モバイル・アプリケーションに直接UAFオーセンティケーター組み込んだり、デバイス上にすでに存在している機能を活用したりできます。The Nok Nok App SDKはThe Nok Nok Authentication Serverから受け取ったUAFリクエストを処理し、サーバーによって指定されたポリシーに基づいてオーセンティケータを起動します。The Nok Nok App SDKは以下に示すコンポーネントで構成されています。

Authenticator Manager：デバイス上に存在するオーセンティケータの機能への統一されたアクセス方法を提供します。Authenticator Managerはオーセンティケータの様々な管理機能、例えばオーセンティケータの発見や追跡を実行します。

Authenticator Specific Module(ASM)：オーセンティケータの詳細と認証プロセスを抽象化します。ASMはオーセンティケータとデバイス上のUAF対応のアプリケーションの接続レイヤとして機能します。

Nok Nok LabsではThe Nok Nok Authenitcator SDKを提供し、オーセンティケータのベンダーがその既存製品向けに容易にUAF ASMを構築することが可能になります。

図 6
Nok Nok App SDKのアーキテクチャ



ASMは下記のコンポーネントを含んでいます。

User Experience Layer：認証プロセスの間、認証対象となるユーザーのエクスペリエンスをサポートします。例えば、指紋用ASMは指紋センサーに対しユーザーに指を擦るようにガイドを表示し、QRコード用ASMはユーザーに対し、ユーザーのモバイルフォンでコンピュータ・スクリーンに写真を取るようにガイドします。

Authenticator: ローカル認証を実行し、認証鍵を取り出し、The Nok Nok Authentication Serverから受け取った認証チャレンジに対し、その鍵で署名をします。オーセンティケータは主に（バイオメトリクス・オーセンティケータ向けには）バイオメトリクスの照合アルゴリズム実装し、UAFで要求される署名アルゴリズムを実装します。オーセンティケータはNok Nok Labsによって提供されたり、サードパーティによって提供されたり、OEMによってデバイスに組み込まれて提供されたりします。

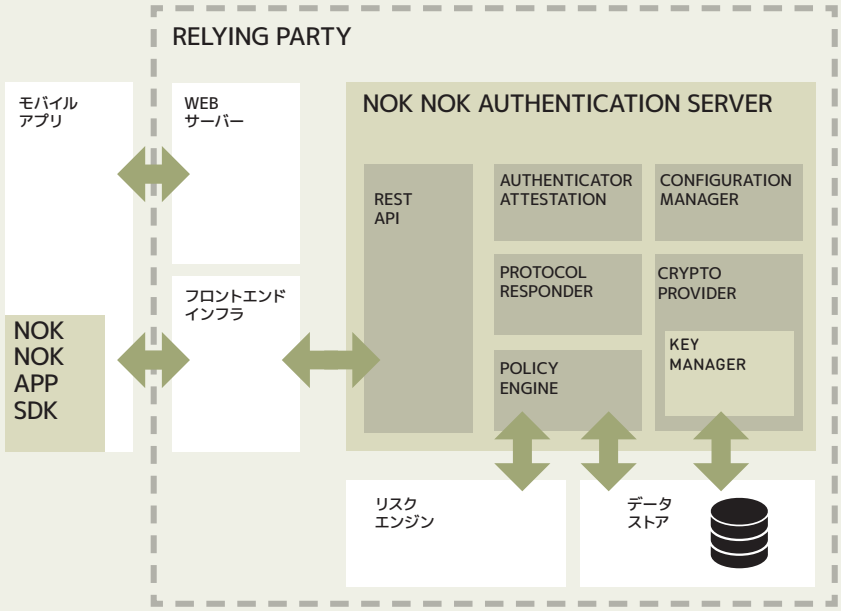
オーセンティケータは認証用の秘密鍵を保護する責任を持っており、その目的のためにTEEのようなセキュアなハードウェアを利用することもあります。それぞれのオーセンティケータは登録のレスポンスに署名するために使われる証明鍵（Attestation Key）を持っています。この鍵はユーザーを検証するのにどのオーセンティケータが使われたかを暗号法的にサーバーが検証するのに使われます。

NOK NOK AUTHENTICATION SERVER

The Nok Nok Authentication Serverは、Relying PartyのWebアプリケーションやモバイル・アプリケーションへの認証サービスを提供するUAFサーバーの役割を果たしています。The Nok Nok Authentication Serverとのシンプルなインテグレーションにより、Relying Partyのアプリケーション・バックエンドに標準ベースの事前構築された認証スタックを組み込み、ユーザーのデバイスで利用可能なあらゆる認証方式を使うことができます。（図7参照）

The Nok Nok Authentication Serverは認証チャレンジを生成し、クライアントからのレスポンスを検証することによって、クライアントを認証します。レジストレーション（登録）の段階でクライアントとの間で確立された鍵を使って、この検証は実行されます。The Nok Nok Authentication Serverは証明プロセスを通じてクライアントによって使われているオーセンティケータが本物かどうかを保証する役割も担っています。ユーザーのプライバシーを保護するためにバイオメトリクス情報はThe Nok Nok Authentication Serverには送られません。

図 7
Nok Nok Authentication Serverのアーキテクチャ



The Nok Nok Authentication Serverは次の要素で構成されます。

REST API：The Nok Nok App SDKがThe Nok Nok Authentication Serverの残りの要素とコミュニケーションするためのインターフェイスです。RESTful APIを使いセキュアなTLS接続上でコミュニケーションが行われます。The Nok Nok Server APIはRelying Partyのアプリケーションとのインテグレーションを容易にするのに必要なデザインが為されています。

Protocol Responder：The Nok Nok Server APIコンポーネントからUAFメッセージを受け取り、内部コマンドに変換し、その処理を開始させます。逆方向に対しては、Protocol Responderは他のコンポーネントからのコマンドをUAFメッセージに変換し、The Nok Nok Server APIコンポーネントを使い、クライアントに送信します。

Crypto Provider：暗号アルゴリズムやThe Nok Nok Authentication Serverによって使われる認証プロトコルを実装します。Crypto Providerはアルゴリズムで使われる鍵をセキュアに管理します。

Authentication Attestation Manager：ユーザーの認証が実行される前に、オーセンティケータのアイデンティティと、関連するオーセンティケータの証明鍵を検証する役割を担います。

Policy Engine：The Nok Nok Authentication Serverのアドミニストレーターによって設定されたポリシーによって、特定のトランザクションにおいて、どのオーセンティケータを使うかを決定するためのインテリジェンスを実装します。Policy Engineを使って、組織はトランザクションにおけるリスクの大きさに対し、リスクに応じて適した認証方式を使って認証を実行可能です。例えば、インターネット・バンキングでユーザーが口座残高をチェックする場合はシンプルに顔認証を実施し、外部への振替や送金を実施する場合は、さらに指紋照合を実行するといった具合です。

Configuration Manager：Relying Partyによって受け入れ可能な認証タイプのようなThe Nok Nok Authentication Serverの様々な設定を管理します。The Nok Nok Authentication Serverは既知のオーセンティケータと、そのセキュリティ属性のデータベースをメンテナンスします。ストアされる情報はオーセンティケータのメーカーやモデル、鍵をストアする能力があるか、セキュア・ハードウェアでのオペレーションを実行する能力があるか、関連する証明鍵を含みます。この情報は複数の目的で使われます。

- オーセンティケータの証明プロセスで、オーセンティケータが本物かどうかを検証します。
- オーセンティケータの既知のセキュリティ属性を決定します。
- Policy ManagerやRelying Partyのアプリケーションが、トランザクションに伴うリスクにマッチする認証方式を持つトランザクションに適切なオーセンティケータを選択することを可能にします。

OUT-OF-BAND認証

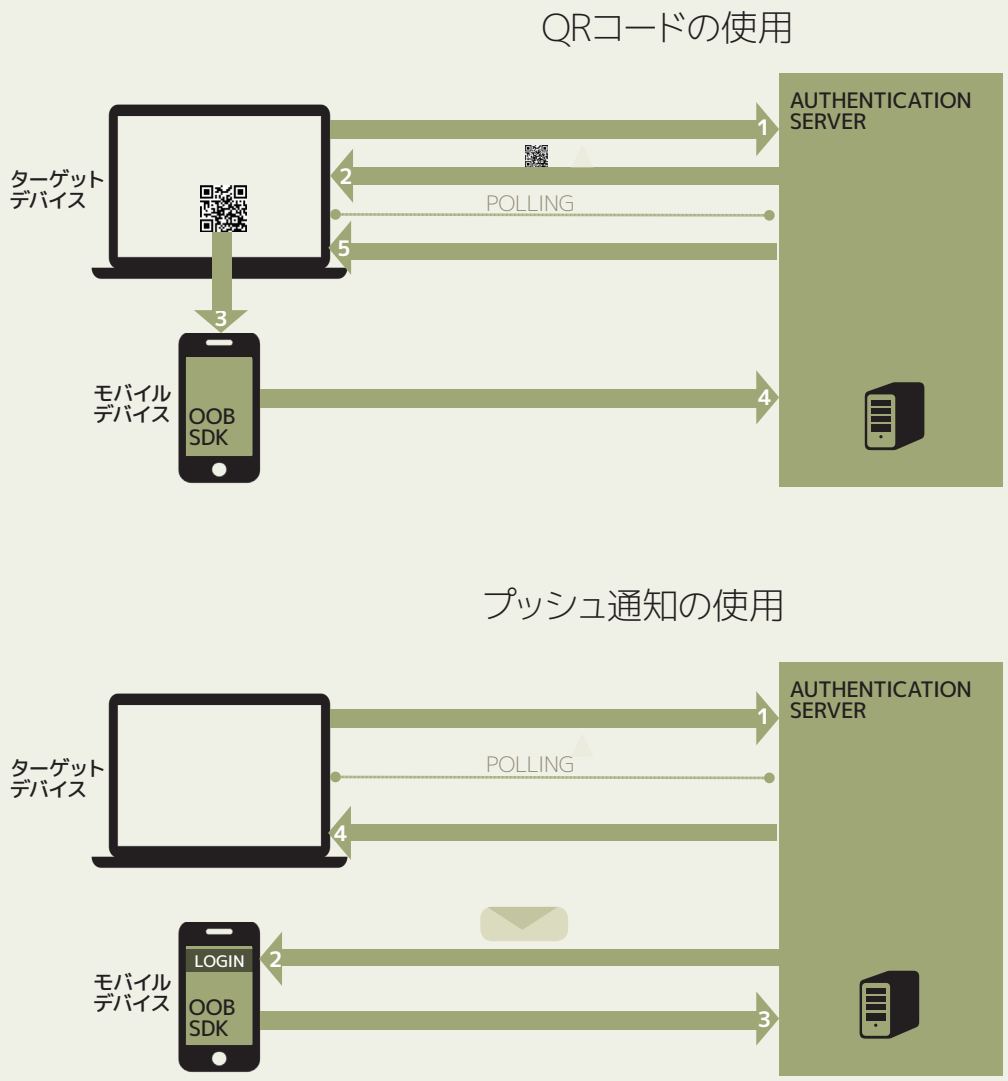
Nok Nok LabsのOut-of-Band(OOB) SDKによって、UAFクライアントを持たないデバイスでもFIDO UAF認証が可能になります。OOB SDKはUAFクライアントを持たない他のシステムで実行中のアプリケーションに対してもUAFベースの認証を拡張します。ユーザーは自身のモバイル・デバイスを使って、ノートブックPC、スマートTV、ATMやKIOSK端末や他の多くのデバイスのようなターゲット・システムに対する認証を可能にします。OOB認証により、UAFプロトコルを別のチャネルで使うことが可能になるので、セキュリティの追加レイヤを提供することになります。OOBは以下の2つのメカニズムを使って、ターゲット・システム上で実行中のアプリケーションとユーザーのモバイル・デバイス上の認証オペレーションを関連付けします。

- QRコード (Quick Response Code)
- プッシュ通知(Push Notification)

QRコード: QRコードは、ユーザーを登録または認証する際に使うことができます。レジストレーションはQRコードを表示しているターゲット・システムで実行されます。ユーザーはモバイル・デバイス上でRelying Partyのアプリケーションを起動し、QRコードをスキャンします。The OOB SDKはQRコードをデコードし、ペアとなっているコードへアクセスします。このコードは、モバイル・デバイス上の1つ以上のオーセンティケータを使ってUAFのレジストレーション・オペレーションを開始するのに使われます。QRコードを使ったOOB認証もレジストレーションと似たようなプロセスに従います。ユーザーがログイン・ボタンをクリックすると、ターゲット・デバイスはサーバーから送られたQRコードを表示します。ユーザーはRelying Partyのモバイル・アプリケーションを使って、モバイル・デバイス上にスキャンします。QRコードにエンコードされている情報を使って、事前に登録されたオーセンティケータでUAF認証オペレーションを実行します。ユーザーがThe Nok Nok Authentication Serverへの認証に成功したら、アプリケーションのバックエンドにこれを通知し、ユーザーにユーザー・データへのアクセスを許可します。

プッシュ通知：ユーザーが登録されたら、ユーザーのモバイル・デバイス上でUAF認証のオペレーションを開始するのに、プッシュ通知を使うことができます。ユーザーがターゲット・デバイス上のFIDOログイン・ボタンをクリックすると、認証サーバーはターゲット・デバイス上のアプリケーションとユーザーのモバイル・デバイスの関連付けを行うのに使うペアとなるコードを生成します。AppleもしくはGoogleのプッシュ通知サーバーを使って、このコードはモバイル・デバイスにプッシュ通知によって送られます。ユーザーがその通知をタップすると、Relying Partyのアプリケーションが起動し、デバイスと認証サーバー間でUAF認証を開始します。ユーザーの認証が成功した後に、認証サーバーはアプリケーションにアクセス許可を通知します。

図 8
OUT-OF-BAND認証



セキュリティ面で優れている点

Nok Nok LabsはUAFプロトコルとS3 Authentication Suiteの多くのセキュリティの特徴を通じて、ハイレベルのエンドツーエンドのセキュリティを提供しています。セキュリティに対するさらなる重要な貢献は全体的なアーキテクチャーが拡張可能かつモジュール化されていることです。この拡張性によって、将来的に使い勝手が良く、よりセキュアなオーセンティケータが利用可能になった際に追加のシステムを導入することなしにスムーズな移行が可能となっているのです。

プロトコルのセキュリティの特徴

UAFプロトコルのユニークなデザインが提供するセーフガードによって、数種類の攻撃に対する保護を実現しています。

パスワード使用を最小限にします：パスワードの代わりに、UAFはユーザーに見えない強力な暗号鍵を利用しています。このことにより、ショルダーサーフィン、キーボードの撮影、キーストロークの記録といった物理的な監視系の攻撃に対する耐性が提供されます。鍵をユーザーに明かさないことで、（パスワードを開示するようにユーザーを騙すような）フィッシング攻撃に対する保護を実現します。高いエントロピーを持つ鍵（128ビット以上）を使って、一般的に使われるパスワードを推測するような攻撃を軽減します。

鍵を送信しません：UAFはチャレンジ・レスポンス型の認証プロトコルなので、認証鍵はデバイスの外に出て行くことはありません。これにより、盗聴攻撃への耐性を提供します。さらにクライアントとサーバー間のすべての通信はTLS接続を使用して保護されています。

リスクの分割：UAFの鍵はユーザー・アカウント、デバイス、Relying Partyの組み合わせごとにユニークなものとなるので、リスクを分割できます。3つの要素のうち、どれか1つが窃取されても、侵害はその要素だけに限定されるのです。例えば、攻撃者がセキュアなハードウェアを持たないデバイスを盗み、そのデバイスから鍵を復元できたとしても、そのユーザーが持つ他のデバイスは侵害を免れます。Relying Partyやユーザーは単に盗まれたデバイスから侵害を試みるアクセスを無効にすれば良いのです。これにより、他のシステムへの攻撃の拡散を防ぐことができます。

NOK NOK APP SDKのセキュリティの特徴

ハードウェア保護：Nok Nok App SDKはデバイスの持つ既存のハードウェア・セキュリティ機能を活かせるようにデザインされています。クライアント・プラットフォームの特定の能力によって、異なるレベルの拡張されたセキュリティの実装が可能になります。

- ハードウェアにストアされた認証鍵
- TEE(Trusted Execution Environment) やSE(Secure Element)のハードウェア機能を利用した署名や検証
- バイオメトリクスの照合はTEE内または特別なチップ上に実現可能
- トランザクションの情報はセキュアなディスプレイで表示可能

ソフトウェア保護：ユーザーのデバイス上にセキュアなハードウェアがあるかどうかに拘らず、Nok Nok App SDKは以下に示すようにクライアントを強固にする数種類のテクニックを使う。

- 認証クレデンシャルと暗号秘密鍵はクリアな状態ではストアされない。
- 実行コードに対しては複数のコードのインテグリティ・チェックが実行される。

NOK NOK AUTHENTICATION SERVERのセキュリティの特徴

Nok Nok Authentication Serverは広範なセキュリティのセーフガードにより、システムとサーバーにストアされたクレデンシャルを保護する。

- クライアントの鍵をサーバーの鍵と暗号的に切り離している。仮に攻撃者が1つのNokNokAuthentication Server上にストアされたユーザーのクレデンシャルへの不正アクセスに成功しても、攻撃者は侵害したサーバーや他のNok Nok Authentication Serverでユーザーになりすますことはできません。
- Nok Nok Authentication Serverのデータベースにおける鍵の暗号化ストレージ[*3]。これには、既存の鍵管理システム(KMS)とインテグレーションされたサーバー側の鍵ストレージと、ユーザーとシステム鍵を保護する関連するハードウェア・セキュリティ・モジュール（HSM）が含まれます。
- 特定のオーセンティケータによってサポートされる時に、認証の証明鍵を経由してクライアントによって使われるオーセンティケータを検証
- 既存のリスク・エンジンからのリスク・スコアを使うことによる、それぞれのオーセンティケータへのダイナミックな信頼レベルの属性付け

認証エコシステムに適したNOK NOK LABSの製品群

The S3 Suiteは認証の「ファースト・マイル」問題、すなわちユーザーと最初のRelying Party間で発生する問題に対応します。ファースト・マイルの認証は、いったん認証されたユーザーが、そのユーザーのアイデンティティを複数のアプリケーションで再利用することを可能にするシングル・サイン・オン（SSO）とフェデレーションと補完関係にあります。そのようなソリューションは、認証点における侵害が複数のサービスを危険に晒すことに繋がるので、リスクが集中することになります。それらのソリューションと相互連携することと、それらに対してユーザーをセキュアに認証可能となることにより、Nok Nok Labsはすべての認証チェーンの全体的なセキュリティを強化します。

Nok Nok Authentication Serverはリスクベース認証(RBA)ソリューションとも連携し、その効果を強化することができます。ユーザーのデバイス、オーセンティケータのメーカーやモデル、ハードウェアの鍵ストレージ機能といったNok Nok Authentication Serverが利用可能な情報はRBAシステムで従来使われる他の情報と併用することで、ユーザーのよりクリアな状況を示すことができます。RBAシステムはNok Nok Authentication Serverのポリシー・エンジンと連携し、特定のトランザクションにおいて受け入れ可能な認証方式を決定します。

拡張可能なデザインを持つThe S3 Suiteは、将来に渡る保証を組織にもたらし、新たなデバイスやオーセンティケータをサポート可能にします。UAF標準をサポートする新たなデバイスはOEMsによって製造時に事前インストールされたクライアントを含んでいます。UAFをサポートする新たなオーセンティケータはオーセンティケータ・ベンダが供給するASMsを伴い、デバイスOEMsによってインテグレーションされます。このことで、Relying Partyは単純にNok Nok Authentication Serverの既知のオーセンティケータのリストと追加されたポリシー・ルールにより、新しいオーセンティケータのサポートを可能にします。さらに言えば、組織によって使われているオーセンティケータのインテグリティを侵害するような特定のオーセンティケータへの攻撃が発生した際には、組織はユーザーのデバイスで利用可能な他のオーセンティケータへの切り替えを容易に実施できます。Nok Nok Labsは組織が変化する認証環境に伴って、その環境を進化させることを可能にしています。

3. 暗号鍵ストレージ、KMS、HSM の統合はサポートされていますが、必須ではありません。

結論

モバイル・デバイスの最近の爆発的な普及や、クラウドの利用はアプリケーションのデザインや提供方法を劇的に変化させてきました。これらの変化によって、パスワード・ベースの認証や既存の認証強化の方式が今日の組織やユーザーのニーズに適切でないことが明らかになってきています。多様なデバイスや、それらのデバイスの多様な使い方によって性格付けられる大規模で異なるユーザー群に対し、組織はサービスを提供する必要があります。適切な認証ソリューションがないことで、ユーザーはフラストレーションを感じています。Nok Nok Labsはデバイスの持つ既存のセキュリティ機能の利点を取り入れることによって、これらの問題に対応します。このことにより、どのような認証方式を使うどのようなデバイス上のアプリケーションに対しても、拡張可能で統一されたインフラストラクチャを生成し、認証を提供できます。UAFプロトコルのFIDO Certified準拠によって、ソリューションは抽象化の原則に基づいて動作し、あらゆるアプリケーションとあらゆる認証方式の間の相互運用を可能にします。

Nok Nok LabsのApp SDKとAuthenticator SDKは標準化されたエンドツーエンドのフレームワークに組み込むことによって、数十億のデバイスのセキュリティ能力を引き出すことができます。UAFはローカル認証で認証鍵を取り出し、その認証鍵をサーバーに対する認証に使用します。

The Nok Nok Authentication ServerはRelying Partyのサーバー・アプリケーションとインテグレーションし、認証サービスを提供します。 Nok Nok Authentication Serverは証明鍵を使ってクライアント・デバイス上のオーセンティケータが正規のものかを検証します。ユーザーを認証する際に、Nok Nok Authentication Serverはチャレンジ・ストリングを生成し、クライアントからのレスポンスを検証します。Nok Nok Authentication Serverによって、組織はトランザクションに伴うリスクに適したポリシーを認証方式に設定することができます。The Out-Of-Band SDKによって、UAFクライアントがインストールされていないデバイスに対しても、UAFを適用可能にします。

Nok Nok Labsのアプローチによる利点を以下に示します。

- 現在の認証サイロ状態（複数の認証システムが並列して存在している状態）を統一し、認証の実装における複雑さを解消します。
- パスワードの使用を最小化し、顔や声といったユーザーが使い易いバイオメトリクス認証を可能にすることで、ユーザーにとって認証が煩わしものではなく、使いやすいものに改善します。
- リスクを分割し、セキュア・ハードウェアの能力を利用することで、よりセキュアな認証を提供します。
- この先の将来も、単にポリシーを設定することで、組織が新たなデバイス上の新たな認証方式を容易に利用可能です。

NOK NOK LABSについて
セキュリティ業界に長年貢献してきたPGP、NETSCAPE、PAYPALやPHOENIXからのエキスパート達がチームを組むことにより、NOK NOK LABSはインターネット・スケールのセキュリティ・プロトコルと製品群を構築するのに十分な経験を持っております。NOK NOK LABSが目指すのは、認証を標準のプロトコルに統一することにより、認証を根本的に変換することであり、これにより企業や組織がクラウド、ビッグデータ、モバイルやオンライン上のビジネスがもたらすパワーを最大限に活用することを可能にすることです。

Nok Nok Labs
4151 Middlefield Road, Suite 200
Palo Alto, CA 94303 USA

www.noknok.com

NOK NOK LABSの詳細は弊社ウェブサイトをご参照されるか、info-j@noknok.comまでお問い合わせください。

Nok Nok
LABS