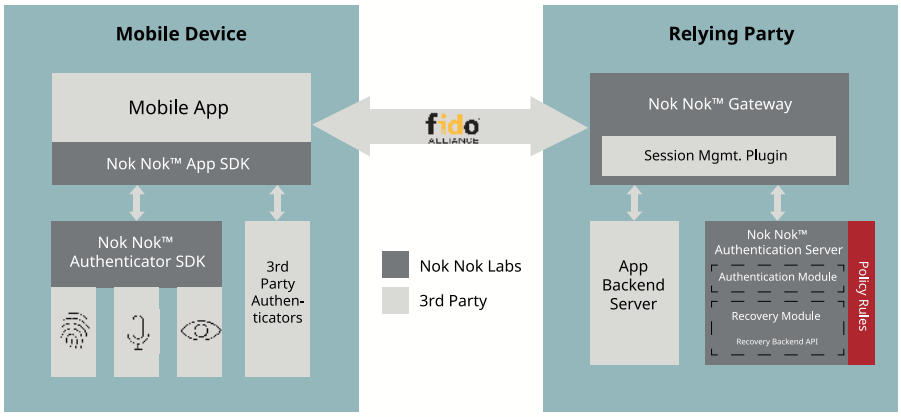
Nok Nok Authentication Server

Introducing Nok Nok Authentication Server



With cloud services, competition is only a click away for your users. Authentication is the front door to access your digital services. An inviting user experience is key to attract and retain users. At the same time, you are faced with increasing security challenges if your front door is not properly "locked". So strong authentication that is secure enough to protect against phishing and other attacks is an additional key requirement. Today's authentication solutions require a separate end-to-end authentication stack for each scenario resulting in high complexity and cost as the number of use cases and scenarios increase.

Nok Nok S3 Authentication Suite Overview

Nok Nok Authentication Server allows organizations to support virtually all authentication use cases and scenarios from a single unified solution, dramatically reducing the cost and complexity of authentication.

Nok Nok Authentication Server leverages the security capabilities already present on a user's device in order to bring strong authentication to any application, supporting any authentication method and on any device. The Authentication Server plugs security capabilities of billions of existing devices into a server with support for all FIDO Alliance Protocols (UAF, U2F and FIDO2), and allows any application to take advantage of these capabilities. FIDO2 supports native authentication through web browsers that implement Web Authentication APIs. In addition, users can also authenticate to web applications through any web browser using Nok Nok's Out-Of-Band authentication from their mobile devices.

The Authentication Server features an extensible design that ensures new authenticators and modalities can be easily supported. By integrating with Nok Nok Authentication Server just once, server applications can support virtually any of the authentication methods available on a wide range of devices such as laptops, smartphones and tablets. Organizations can dynamically allow or disallow any authentication method based on security requirements and the transaction risk.

Key Benefits

User Experience

Nok Nok Authentication Server minimizes the need for users to remember account specific passwords by allowing them to authenticate using more user-friendly authentication methods such as fingerprint biometrics, voice biometrics, face biometrics, authenticator specific PINs, and many more.

Cost

Authentication Server allows organizations to consolidate multiple authentication stacks into a simple unified, extensible solution that significantly reduces deployment and ongoing costs.

Flexibility

Organizations have the ability to easily adapt to the changing security landscape. By simply configuring policy rules, organizations can enable strong authentication support for a new device or authentication method, or disallow untrustworthy authentication methods.

Key Features

Scalable Account Recovery Platform - The Nok Nok Authentication Server provides a flexible policy-based platform for identity proofing and account recovery. It supports a variety of methods including email ID, phone number, and scan of government issued Photo ID and a live picture. The server provides APIs to easily add any additional recovery method.

Out Of Band Authentication - Out-of-Band (OOB) authentication allows users to use a mobile device to authenticate from other devices such as desktop application, web browsers, Kiosk-PCs, IVR, or ATMs. The user binds the browser session or transaction to his or her mobile device by scanning a QR code using the mobile device or by triggering a push notification. The user then performs FIDO-based authentication on an out-of-band channel between the mobile device and the Nok Nok Authentication Server.

New Device Activation - New Device Activation is a QR code-based mechanism that allows the user to initiate authenticator registration on a new device by using a previously registered device. This eliminates the inconvenience and security risk when a user is forced to recall and enter a password multiple times. With New Device Activation, a user simply uses their new device to capture a QR code displayed on an existing device. This feature makes it practical for users to register multiple authenticators. This reduces the likelihood of requiring account recovery when an authenticator gets lost.

Authenticator Policy - Authenticator policy is used to provide the choice of authenticators to the end users. This feature uses rules to evaluate the relative risk presented by a particular authentication method and offers a simple way to take specific actions. In other words, the policy can be configured with different rules to ensure that each transaction runs through a set of checks before being approved or denied. Authenticator policies help app developers to select the right authenticators in order to comply with certain requirements of government regulations, such as PSD2.

Administration Console - The Nok Nok Authentication Server Administration Console is a web-based UI for managing the Authentication Server. This feature allows administrators to configure policies, change properties, and review server analytics details.

Reporting and Analytics - The Nok Nok Authentication Server analytics and reporting feature lets you view, generate, and download statistical data and reports. This dashboard provides insights into the user base by providing a count for unique users, registrations, authentications, transactions and deregistration over a specified time period. These numbers can be further examined in the context of location, devices and platforms.

Carrier Grade - The Nok Nok Authentication Server is a carrier grade solution that is commercially deployed and in production by leading companies supporting tens of millions of users across the globe. It supports hundreds to thousands transactions (Registration, Authentication, Deregistration and Transaction Confirmation) per second. The server can be deployed in a cluster to support high availability requirements.

FIDO Metadata Service Integration - New FIDO certified authenticators are introduced in the market quite frequently. The FIDO Alliance runs a Metadata Service for the Relying Parties (RP) to receive information about new authenticators - called Metadata Statements. The Nok Nok Authentication Server provides a direct integration with this Metadata Service, resulting in an easy way for RPs to get up-to-date information about authenticators, allowing them to accept and support authenticators from any vendor that meet specified requirements.

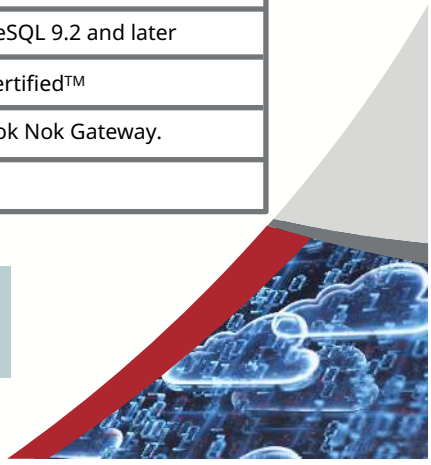
Container Support - The Nok Nok Authentication Server supports deployment on Docker containers. This container support further simplifies server deployment and maintenance updates for both on-premise and public-cloud.

Technical Specifications:

	Authentication Server Requirement
Operating Systems	Red Hat® Enterprise Linux 7 / CentOS 7
Java	Oracle JDK 8
Application Server	Apache™ Tomcat 8.0 and 8.5
Database	Oracle 12c Release 1, MySQL 5.7.10 and later, PostgreSQL 9.2 and later
FIDO Protocols	FIDO UAF Certified™, FIDO U2F Certified™ , FIDO2 Certified™
Federation Connectors	Federation Connectors are integrated through the Nok Nok Gateway.
Container Support	Docker

ABOUT NOK NOK LABS

Nok Nok empowers global organizations to improve the user experience to access digital services, while meeting the most advanced privacy and regulatory requirements. Nok Nok Labs and its industry leading customers and partners include Fujitsu Limited, Ericsson, Hitachi, Lenovo, NTT DATA, NTT DOCOMO, OneSpan and Samsung. For more information, visit www.noknok.com.



Nok Nok Labs, 2890 Zanker Road, Suite 203 San Jose, CA 95134 USA