SOLUTION BRIEF

IoT SDK SOLUTIONS BRIEF

BUSINESS CHALLENGES

International Data Corporation (IDC) estimates that there will be 41.6 billion connected IoT devices, or "things," generating 79.4 zettabytes (ZB) of data by 2025. This data holds valuable information about entry/egress times of employees at work, heart rate, car location, who is at the front door, transactions made through smart home speakers and more – all of which need strong security in a connected IoT device world.

Securing connected devices opens up new opportunities to provide privileged user access to devices of all sorts. Vending machines, ATMs, Connected Cars and more can all be transformed into new lines of revenue-generating services.

Secure router authentication unlocks the potential to turn a smart home into a platform for remote monitoring and services. Secure remote access to home networks permits a greater range of opportunities to serve your customers.

Highlights

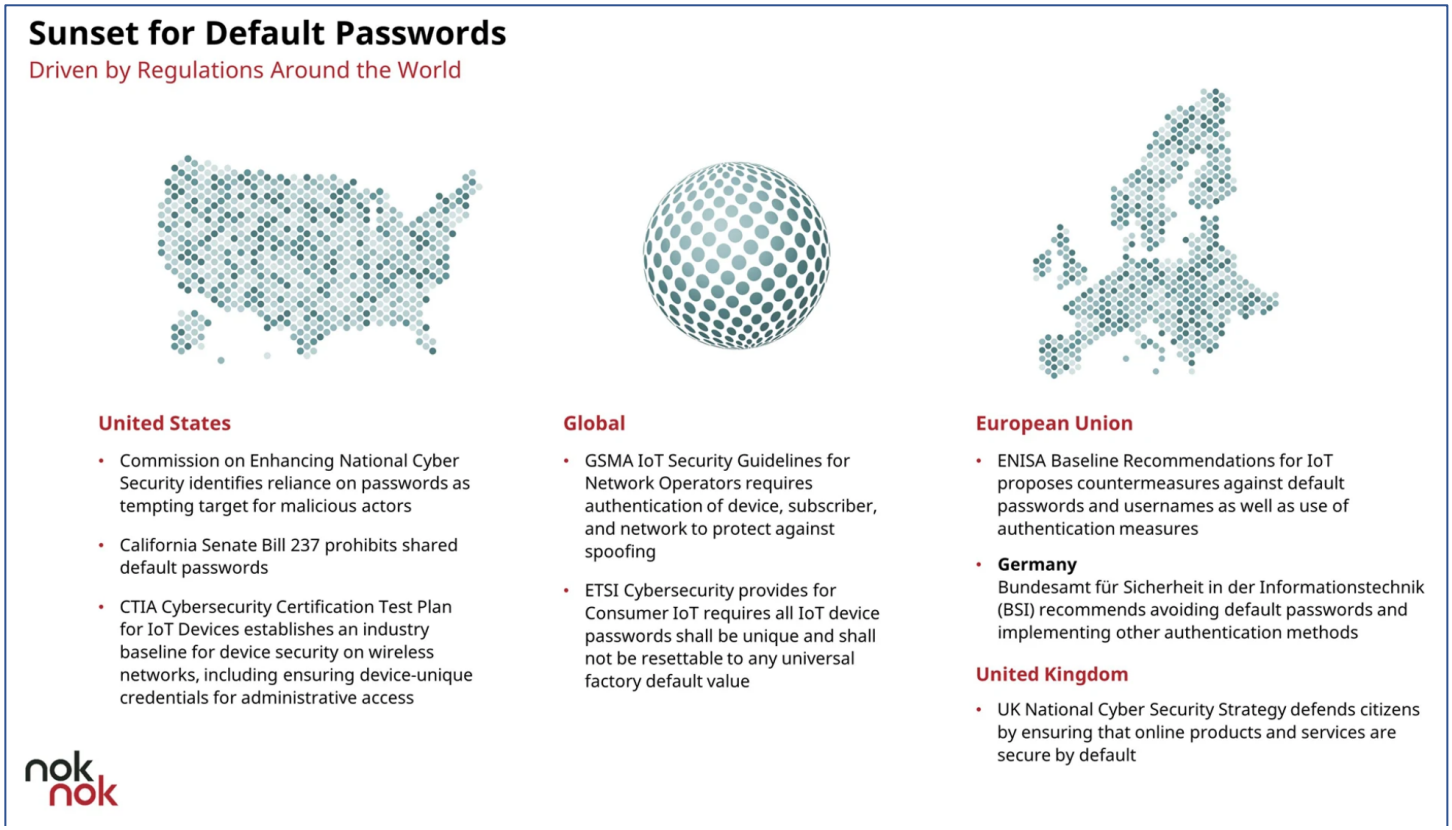
- IoT device attestation and authentication
- Easily runs on existing microcontroller units (MCUs)
- Automated onboarding and biding of users and applications to IoT devices
- Supports security industry standards, governmental standards and global regulatory requirements that specify *"NO (shared) or default passwords"*
- Multi-factor authentication (MFA) that is faster, more secure and more convenient than username/password
- Supports both standalone and cloud-connected devices
- Interoperability between service providers and IoT devices
- Supports all biometric modalities

Secure router authentication unlocks the potential to turn a smart home into a platform for remote monitoring and services. Secure remote access to home networks permits a greater range of opportunities to serve your customers.

FIDO Standards based interoperability, able to standardize user-to-device, and device-to-device authentication across the industry and ecosystem with modular simplicity and ease of use.

The Nok Nok IoT SDK Applies to a Wide Variety of Use Cases.

1. **Simple to Use:** The Nok Nok IoT SDK supports both cloud-connected and stand-alone devices. Manufacturers and service providers can end their reliance on weak password-based security. Built with flexible scaling in mind, the Nok Nok IoT SDK provides strong, multi-factor authentication while improving security and simplifying both the management and user experience.
2. **Simple to Secure** A Nok Nok IoT SDK enabled device becomes a zero-trust entity for network security. Security is no longer dependent on a secure perimeter. By eliminating the broken legacy of passwords, Nok Nok secured devices can avoid the overhead for complex and maintenance intense
3. **Simple to Comply:** Manufacturers are being pressured to end their reliance on shared default passwords for user-to-device authentication. The Nok Nok IoT SDK provides a simple answer to these pressures by implementing a unique - yet scalable - authentication scheme for IoT devices. Various regulatory and standards bodies have embraced FIDO protocols to satisfy their authentication requirements.



4. **Simple to Deploy:** The Nok Nok IoT SDK was designed with existing microcontroller units (MCUs) in mind. No new or dedicated hardware is required. Manufacturers and service providers can improve their security posture without the need to replace or re-issue hardware.

5. **Simple to Dispose:** The Nok Nok IoT SDK does not store any secrets on the device. When a wave of devices reach their end-of-life and need to be replaced, security experts can be assured that no secret user credentials can be revealed with the disposed devices. This decreases maintenance costs while improving the security footing of deploying organizations.
6. **Simple to Integrate:** The Nok Nok IoT SDK can interact with any FIDO certified authenticator or server. In the fragmented IoT industry, such interoperability is key for wide ranging integration and deployment so that the IoT market at large can focus efforts on expanding use cases and providing more value to their users.
7. **Simple to Deploy:** The Nok Nok IoT SDK was designed with existing microcontroller units (MCUs) in mind. No new or dedicated hardware is required. Manufacturers and service providers can improve their security posture without the need to replace or re-issue hardware.
8. **Simple to Upgrade:** As new IoT devices are introduced, the Nok Nok authentication infrastructure lowers the cost and complexity of integrating new devices and modes of authentication. A single developer API gives organizations the power to address all of their authentication needs with ease. Mobile, web and desktop applications can be upgraded at the same time as wearables and other IoT devices. New modes of authentication can be incorporated seamlessly.

FIND OUT MORE

For more information about the Nok Nok S3 Authentication Suite, please visit https://noknok.com/products/s3-authentication-suite/. Nok Nok provides a variety of trial options for the S3 Authentication Suite including Software-as-a-Service, container image and installable software. To try Nok Nok's solutions, please visit https://www.noknok.com/trynow.

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