HIDEEZ KEY

Hideez bluetooth security key / multi-factor authenticator / password manager. Analysis of NIST 800.63b and FIPS 140-2 compliance.

Version 1.0

Introduction

Effective and usable authentication is an interesting challenge that involves applying various techniques and approaches to achieve the highest degree of certainty when granting access to resources without overburdening the user.

Hideez has a unique approach of securing employees and contractor's access to company computers by storing strong passwords on a secure key, paired up with a 2nd factor, eliminating the need for employees to remember or write down their passwords. (As an added bonus Hideez security key also serves as RFID access card, protecting physical access.)

NIST 800-63b is a "golden standard" when it comes to Digital Identity and Authentication guidelines for the government and commercial sectors. It segments the authentication requirements by authentication assurance layers (AALs) and examines thoroughly all the considerations that go into each requirement. In this white paper we will examine how Hideez key stacks up against these requirements to achieve highest level compliance.

Device overview

- Name of the authenticator: Hideez Key 2
- Hardware Type & Version: flash-based nRF52832 BLE SoC
- Software Platform/OS: “NonOS”, SoftDevice S112 by Nordic Semiconductor for nRF52 series
- Authenticator category: 1

Hideez Key 2 is an electronic device assembled on a simple PCB integrating nRF52832 BLE SoC with appropriate peripheral (see below). The PCB sits in a plastic box 1.3 x 1.3 x 0.4 inch. The whole device weighs 0.3 oz.

The PCB comprises of:

- a buzzer
- a led indicator
- a multifunctional button
- CR2032 battery
- Nordic Semiconductor nRF52832 SoC
- PCB antenna
- A few supporting electronic elements

In the same plastic case with the PCB, there is another independent component - an RFID-device. Nordic nRF52832 does not have access to the RFID-device.

Hideez Key 2 provides a means of strong authentication according to FIDO U2F specification, and it can aggregate and provide other authentication methods implemented as separate modules.

FIPS 140-2 Standard

Organizations use the FIPS 140-2 standard to ensure that the hardware they select meets specific security requirements. The FIPS certification standard defines four increasing, qualitative levels of security:

Level 1: Requires production-grade equipment and externally tested algorithms.

Level 2: Adds requirements for physical tamper-evidence and role-based authentication. Software implementations must run on an Operating System approved to Common Criteria at EAL2.

Level 3: Adds requirements for physical tamper-resistance and identity-based authentication. There must also be physical or logical separation between the interfaces by which “critical security parameters” enter and leave the module. Private keys can only enter or leave in encrypted form.

Level 4: This level makes the physical security requirements more stringent, requiring the ability to be tamper-active, erasing the contents of the device if it detects various forms of environmental attack.

Hideez Key 2 is architecturally compliant with Levels 1-4 of FIPS 140-2 standard given it’s architecture and threat protection methods.

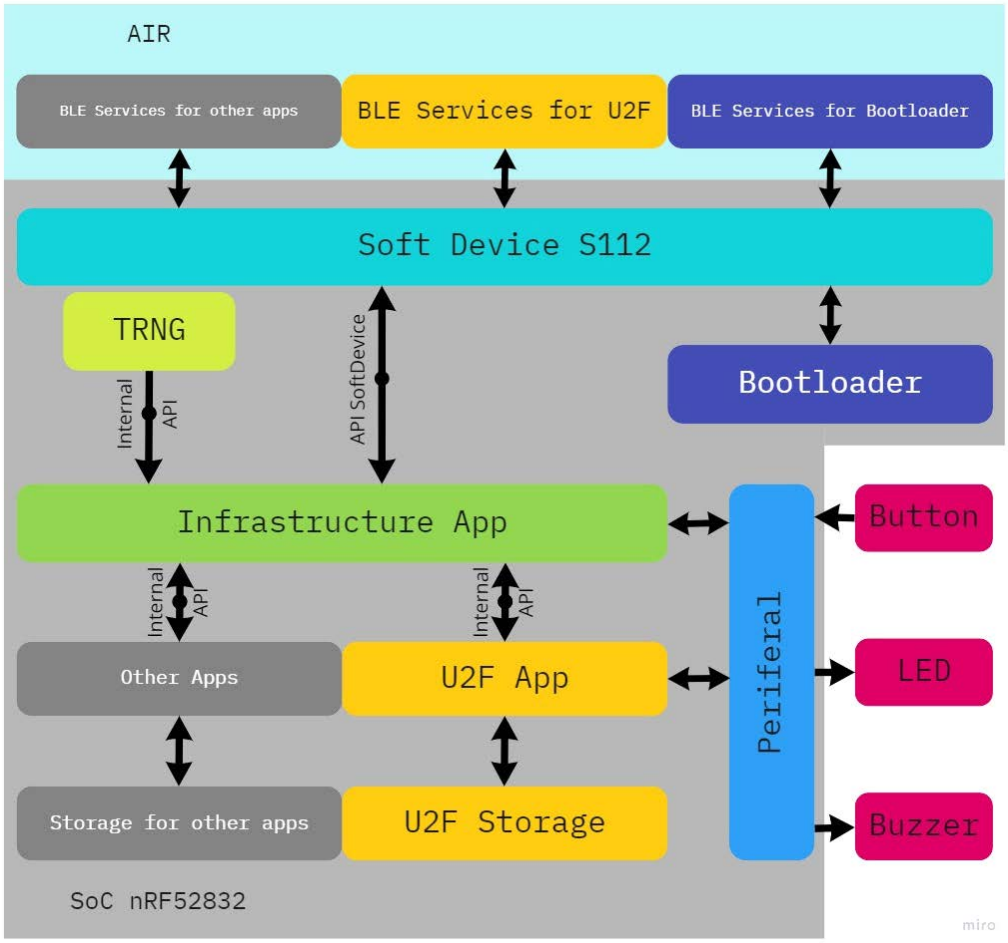
Hideez Key 2 architecture

Hideez Key 2 architecture is an example of a “Non-OS” approach where HLOS (High-Level Operating System) and ROE (Restricted Operating Environment) are one and the same. Hideez provides all the necessary infrastructure software and API, making it possible to run and control software modules like FIDO Authenticator Application.

Hideez Key 2 Authenticator combines FIDO Authenticator Application that implements the authenticator portion of the FIDO U2F protocol, Hideez infrastructure software component that provides the main cycle (including routing between software modules) and required

API, Bootloader Application, Nordic SoftDevice S112 as well as nRF52832-based hardware with peripheral.

The overall structure of the Hideez Key 2 Authenticator is shown in the following figure:



Hideez Key 2 Authenticator includes SoftDevice S112 software modules, Infrastructure App, U2F App, Bootloader, and other apps. All program modules are stored in the nRF52832 internal flash memory and use the nRF52832 internal RAM memory. Hideez Key Authenticator does not have an external Flash or RAM memory. All external interfaces that can be used for Debug (UART, SPI, I2C, etc.) are disabled and are never used during the operation.

All the modules are loaded to the nRF52832 chip during the manufacturing using the contact interface SWD. After a successful module load, the APPROTECT rere level, and SWD gets disabled. After the APPPROTECT installation, any further reload modification and read

of the software modules is impossible without deleting the entire flash memory (EraseAll). It is also not possible to view or modify the contents of RAM nRF52832.

In case there is a need to update software modules, a Bootloader application is used. The Bootloader application works through the custom BLE service Bootloader and client application (web, mobile, or desktop). The ECC256 public key is stored inside the Bootloader applicatioefore loading the modules, the Bootloader application checks the digital signature for the downloaded data using the ECDSA algorithm. If the digital signature is correct, then Bootloader removes all the applications and makes the update.

Hardware and software attacks protection

To protect nRF53832 from unauthorized access, Nordic Semiconductor provides an Access Port Protection (APP).
If the APP has been enabled in the APPROTECT register (0x10001208) of the UICR (User information configuration registers, non-volatile memory (NVM) registers), the debugger's read/write access to all CPU registers and memory-mapped addresses is blocked.

The only way to 'reopen/unlock' the device is to issue an ERASEALL command and a reset through the CTRL-AP access port. It erases the entire code flash and UICR area of the device, in addition to the entire RAM.

The APP is enabled in Hideez Key 2 by default. It is a mandatory step in the manufacturing process of the device and cannot be disabled programmatically without connecting to the hardware port and erasing all the data.

Encryption

ASP	Data	Description	Secret ?	Strength	Where this is stored.	How this is protected.	How this is generated.	Input/ Output	When this is destroyed	Unique or Shared
Private Keys	ECDSA on P-256	Private key used for signing operation	yes	128	Wrapped in the Key Handle	Encrypted-then-HMACed with AES-256 and HMAC-SHA-256	Generated using RNG	During registration and authentication	RP deletes security key	Unique
Key handle	Structure	Contains all information necessary to authenticate a user to the RP	no	128	With relying party	N/A	KeyHandle structure: - Message: AES-256 (Transport Secret, (Nonce, AppIDHash, Counter)) - Tag: HMAC-SHA-256 (Authentication Secret, Message)	During registration and authentication	RP deletes security key	Unique
Device Attestation Key	ECDSA on P-256	Device Private Root Key	yes	128	Storage	Access Port Protection	It is generated once during Hideez Key FIDO attestation certificate generation	Never	Never	shared per a batch of 100000 devices of the model

							with help of Hideez local CA.			
Global Signature Counter	INT	Keeps track of the signature done by the device	yes	N/A	Storage	Access Port Protection	Incremented during registration and authentication	Never	Device Reset	Shared
Master Secret	RNG	Encryption Key is used during deriving Private Keys	yes	256	Storage	Access Port Protection	Generated using RNG during instantiation	Never	Device Reset	Unique
Transport Secret	RNG	Encryption Key to encrypt KeyHandle	yes	256	Storage	Access Port Protection	Generated using RNG during instantiation	Never	Device Reset	Unique
Authentication Secret	RNG	Encryption Key to authenticate KeyHandle	yes	256	Storage	Access Port Protection	Generated using RNG during instantiation	Never	Device Reset	Unique

Summary of NIST 800-63b AAL requirements

Requirement	AAL1	AAL2	AAL3
Permitted Authenticator Types	Memorized Secret; Look-Up Secret; Out-of-Band; SF OTP Device; MF OTP Device; SF Crypto Software; SF Crypto Device; MF Crypto Software; MF Crypto Device	MF OTP Device; MF Crypto Software; MF Crypto Device; or Memorized Secret plus: • Look-Up Secret • Out-of-Band • SF OTP Device • SF Crypto Software • SF Crypto Device	MF Crypto Device; SF Crypto Device plus Memorized Secret; SF OTP Device plus MF Crypto Device or Software; SF OTP Device plus SF Crypto Software plus Memorized Secret
FIPS 140 Verification	Level 1 (Government agency verifiers)	Level 1 (Government agency authenticators and verifiers)	Level 2 overall (MF authenticators) Level 1 overall (verifiers and SF Crypto Devices) Level 3 physical security (all authenticators)
Reauthentication	30 days	12 hours or 30 minutes inactivity; MAY use one authentication factor	12 hours or 15 minutes inactivity; SHALL use both authentication factors
Security Controls	SP 800-53 Low Baseline (or equivalent)	SP 800-53 Moderate Baseline (or equivalent)	SP 800-53 High Baseline (or equivalent)
MitM Resistance	Required	Required	Required
Verifier Impersonation Resistance	Not required	Not required	Required
Verifier Compromise Resistance	Not required	Not required	Required
Replay Resistance	Not required	Not required	Required
Authentication Intent	Not required	Recommended	Required

Records Retention Policy	Required	Required	Required
Privacy Controls	Required	Required	Required

Authenticator Types

Hideez Key is a combination of a FIDO U2F compliant multi-factor cryptographic device, a password manager, OTP generator and RFID access key.

Traditionally, a security key would employ only FIDO U2F authenticator or only OTP with PIN. Hideez key provides a combination of FIDO U2F (or FIDO2) and OTP, with a memorized secret that's stored on the device, protected by a PIN, thus meeting NIST's permitted authenticator type for AAL3.

Of note:

> *The verifier SHALL use approved encryption and an authenticated protected channel when requesting memorized secrets to provide resistance to eavesdropping and MitM attacks.*

Hideez key password manager feature provides a secure channel from the key to the client, to the verifier (which the PC client can ascertain)

Reauthentication

800-63b calls for reauthentication to be an integral part of the secure authentication process.

> *Periodic reauthentication of subscriber sessions SHALL be performed as described in Section 7.2. At AAL2, authentication of the subscriber SHALL be repeated at least once per 12 hours during an extended usage session, regardless of user activity. Reauthentication of the subscriber SHALL be repeated following any*

> *period of inactivity lasting 30 minutes or longer. The session SHALL be terminated (i.e., logged out) when either of these time limits is reached.*
>
> *Reauthentication of a session that has not yet reached its time limit MAY require only a memorized secret or a biometric in conjunction with the still-valid session secret. The verifier MAY prompt the user to cause activity just before the inactivity timeout.*

Typically, reauthentication would be carried out by the verifier, and most authenticator solutions rely on that. Hideez goes couple of steps further and provides its own reauthentication mechanism that can be layered on top of verifier's policies, providing a uniform reauthentication policy implementation.

Hideez's reauthentication features defined via a security profile include a need to perform one of the actions based on session time to live (TTL) or proximity of the key to the host computer.

- PIN code
- Press of a button
- Connection to Hideez Enterprise Server (HES)

In addition, reauthentication can be triggered on bonding (pairing), reconnection, and new session events. Hideez solution also implements proximity based configurable lockouts, further strengthening the reauthentication policies.

Note: FIDO standard doesn't cover session expiration or lock-outs - this functionality is "above and beyond" the base standard.

Verifier Impersonation Resistance

Verifier impersonation is one of the key vectors of attack used by bad actors to intercept the authentication credentials to be able to reuse them later with the legitimate verifier.

> *A verifier impersonation-resistant authentication protocol SHALL establish an authenticated protected channel with the verifier. It SHALL then strongly and*

> *irreversibly bind a channel identifier that was negotiated in establishing the authenticated protected channel to the authenticator output (e.g., by signing the two values together using a private key controlled by the claimant for which the public key is known to the verifier). The verifier SHALL validate the signature or other information used to prove verifier impersonation resistance. This prevents an impostor verifier, even one that has obtained a certificate representing the actual verifier, from replaying that authentication on a different authenticated protected channel.*

Hideez addresses verifier impersonation rather inventively (due to the built-in password manager implementation) by allowing the administrator to main a white list of the url and application resources the user has access to. This provides a solid defense against phishing type attacks or local malware that's made to impersonate legitimate enterprise applications.

Replay Resistance

800-63b calls for replay resistance as a way to prevent attackers from capturing authentication sequences and replaying them:

> *An authentication process resists replay attacks if it is impractical to achieve a successful authentication by recording and replaying a previous authentication message. Replay resistance is in addition to the replay-resistant nature of authenticated protected channel protocols, since the output could be stolen prior to entry into the protected channel. Protocols that use nonces or challenges to prove the "freshness" of the transaction are resistant to replay attacks since the verifier will easily detect when old protocol messages are replayed since they will not contain the appropriate nonces or timeliness data.*

Hideez key implements a three layer encryption in order to protect against replay:

- Host to key (device to device) encryption
- SW client to key storage level encryption
- Server to key storage level encryption, where the SW client acts only as transport

These 3 layers of encryption in combination provide very strong protection against replay attacks.

Authentication Intent

From 800-63b:

> *An authentication process demonstrates intent if it requires the subject to explicitly respond to each authentication or reauthentication request. The goal of authentication intent is to make it more difficult for directly connected physical authenticators (e.g., multi-factor cryptographic devices) to be used without the subject's knowledge, such as by malware on the endpoint.*

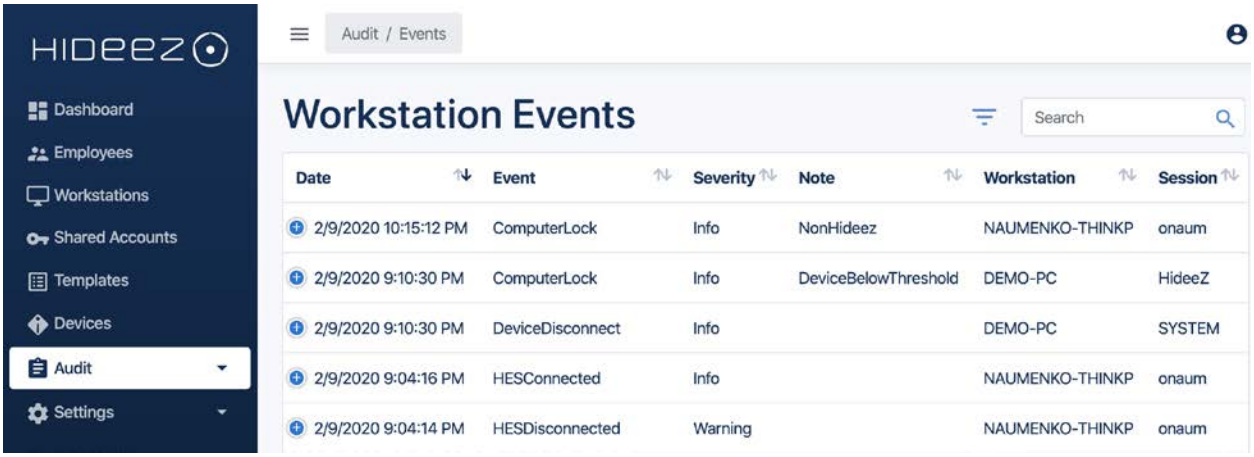
Hideez authenticator device employs two measures to establish the intent:

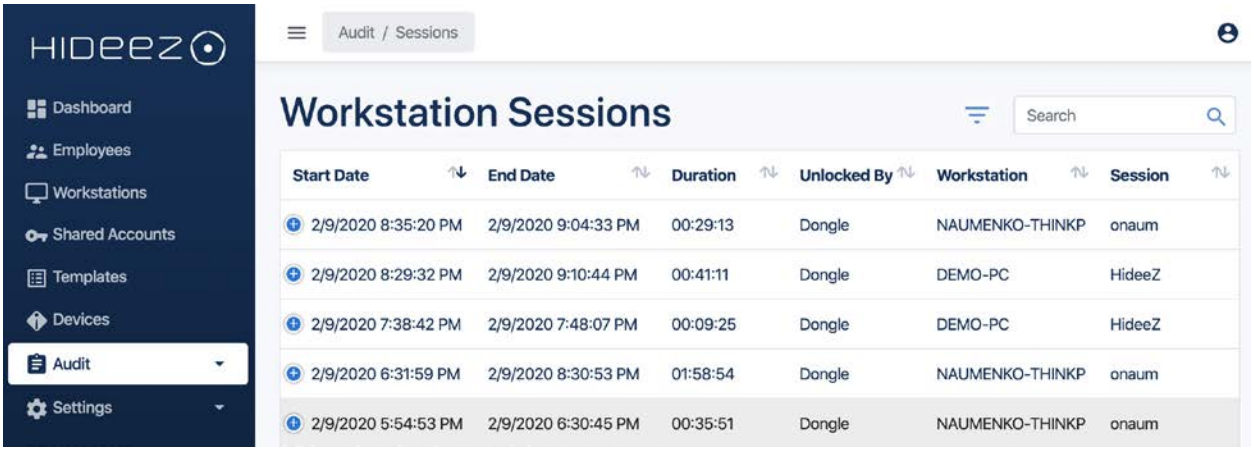
1) It requires the user to press the button on the authenticator device
2) Requires the user to enter a memorized secret (PIN code) on the host client

These measures combine rather well

Logging, Audits, and Records Retention

Logging, auditing, and records represent a significant part of an enterprise-grade authenticator solution. Thanks to its unique combination of the authenticator and password manager functionality, Hideez is able to provide audit data that is well correlated and actionable.





Privacy Controls

The largest vector of attack on user privacy is via the browser's use of cached data (cookies). Hideez's approach of moving the login information outside of browser scope provides the separation requested by NIST and other data privacy standards like HIPAA and GDPR.

Threat Mitigation

NIST 800-63b recommends analysis of the threat mitigation features and measures along the following vectors:

Authenticator Threat / Attack	Remediation
Theft	Hideez employees a 3-way registration process among the host client, server, and the authenticator, which alleviates the threat of binding an authenticator to a new host. Using a stolen authenticator with the host that has been bound is addressed with a memorized secret PIN stored on the device and verified by the software client
Duplication	Authenticator manufacturing process is protected by a unique master key which is assigned at the time of manufacturing to each authenticator
Eavesdropping	The communication channel is triple protected by a three-layer encryption protocol layered over the communication channels. The authentication is negotiated between host software client and the authenticator device. Any updates from the server are point-to-point encrypted, from the database on the server to the storage on the authenticator device.
Offline Cracking	Offline cracking is protected by the retry limit on the host software client and is gated by the code generation speed of the authenticator device
Side channel attack	The cryptographic device is using the chipset designed to resist differential power or timing analysis

Phishing or Pharming	Hideez Enterprise solution is utilizing a whitelist based templating system for resources, which compares the resource that is being accessed to the whitelist, thus effectively resisting the phishing spoofing attempts
Social Engineering	In addition to having to physically possess the authenticator device, it's possible to configure security policy to require the mobile phone to serve as an additional factor establishing the user binding
Online guessing	When the authorized online resource is detected, the host client attempts to take over the input and reports back any failures to trigger server alerts
Endpoint Compromise	Binding of the authenticator device and the SW client on the host is a three way binding with server authorization. It is not possible to maliciously bind an impostor host client with the authenticator device.
Unauthorized binding	The binding is provisioned and monitored by an administrator, restricting ad hoc bindings

Hideez key implements distinct solutions for each one of these risk factors, oven overlapping for further efficiency.

Conclusion

We hope that by describing how Hideez Secure Key for Enterprise solution addresses the requirements set forward by NIST in 800-63b guidelines, we are able to provide transparency and instill confidence in adherence to current standards and best practices. However, this adherence is only part of the story as the solution architecture needs to be flexible to accommodate potential future requirements, and highly usable to ensure user adoption. Hideez's ultimate goal is to provide the perfect trifecta of usability, adaptability, and standards / best practice adherence.