Nash Identity Safe

Quantum-Safe Human Authentication for the Post-Web Era

A Public Technical White Paper by Nash 1337, Inc.

Version 1.0 | April 2026

Public-Release Notice. This document describes the public technical philosophy, security objectives, and system architecture of Nash Identity Safe. It intentionally omits proprietary implementation details, including but not limited to hardware layout, firmware internals, biometric feature extraction, model architecture, cryptographic key hierarchy, recovery design, anti-tamper mechanisms, device-pairing protocol, and sensor-fusion thresholds.

Contents

1 Abstract

Nash Identity Safe is a quantum-safe human authentication system designed to verify not merely that a credential is present, but that the authorized human is present, cognitively engaged, and acting within an acceptable local safety state. The system combines hardware-rooted authentication, post-quantum cryptographic communication, color-perception-based cognitive challenge-response, EEG-derived Proof-of-Brain verification, and coercion-aware local risk checks. The result is a new category of security device: not a conventional wallet, key, or passport, but a human authorization safe.

The design responds to three failures in web-era authentication. First, passwords, PINs, push-based MFA, and bearer hardware tokens can be stolen, coerced, phished, or socially engineered. Second, legacy biometrics such as fingerprints, facial recognition, and iris scans create permanent privacy risk because they bind identity to biological traits that cannot be meaningfully revoked. Third, classical public-key infrastructure is entering a post-quantum transition period as organizations prepare to replace cryptographic systems vulnerable to future quantum attacks (Cybersecurity and Infrastructure Security Agency, National Security Agency, and National Institute of Standards and Technology 2023).

Nash Identity Safe is designed around a local-first principle: raw cognitive, EEG, and physiological data remain on device. Relying parties receive cryptographic authorization, attestations, or commitments, not raw brain or body data. The cryptographic layer is designed for quantum-resistant and crypto-agile operation, beginning with Kyber-derived Module-Lattice-Based Key-Encapsulation Mechanism, or ML-KEM, standardized by the National Institute of Standards and Technology in FIPS 203 (National Institute of Standards and Technology 2024b). Future deployments may incorporate post-quantum signature schemes such as ML-DSA and SLH-DSA, standardized in FIPS 204 and FIPS 205 respectively (National Institute of Standards and Technology 2024a, 2024c).

The cognitive authentication layer is informed by Plurigrid's passport.gay technology, which describes Proof of Brain as an identity primitive derived from brainwave entropy, interaction behavior, and revocable commitments rather than centralized biometric templates (Plurigrid 2026b). Nash Identity Safe applies this thesis to a hardware-rooted product architecture, using color perception and local EEG response as a final authentication factor. The device is therefore designed to protect cryptographic authorization, privileged access, AI-agent delegation, digital asset custody, and high-assurance identity workflows in environments where ordinary MFA is insufficient.

2 Executive Summary

Nash Identity Safe is a quantum-safe authentication device for high-value human authorization. Its purpose is to solve a gap left by ordinary multi-factor authentication: most authentication systems can verify a credential, but they cannot reliably verify that the legitimate human user is present, aware, cognitively engaged, and not obviously operating under coercion.

A password verifies knowledge. A hardware token verifies possession. A biometric verifies resemblance to a stored body-derived template. None of these factors alone proves safe, intentional

human authorization. Nash Identity Safe introduces a layered authentication ceremony in which authorization requires device possession, local knowledge, cognitive challenge-response, EEG-derived liveness, and optional distress-aware state evaluation.

The device is designed for a post-quantum and AI-mediated environment. As AI agents increasingly act on behalf of users, organizations will need stronger human checkpoints for high-impact actions. As cryptographically relevant quantum computing advances, organizations must migrate away from vulnerable classical asymmetric systems and toward post-quantum standards. Nash Identity Safe is designed to operate within this transition by using quantum-resistant key establishment and crypto-agile identity architecture.

Nash Identity Safe is not framed as a hardware wallet, although it may protect digital asset operations. It is not framed as a hardware key, although it may protect login flows. It is not framed as a passport, although it may support identity presentation. It is a broader object: a hardware safe for human authorization.

3 Problem: Authentication Without Human Assurance

The dominant forms of authentication were built for an earlier internet. Passwords, one-time codes, SMS, mobile push approvals, and hardware tokens were designed to protect accounts and sessions. They were not designed to answer deeper questions about authorization: Is the right human present? Is the human alive and cognitively engaged? Is the human acting voluntarily? Is the host device trustworthy? Is the cryptographic channel resistant to future quantum attack?

Modern attackers exploit this gap. Credentials are phished. Push notifications are manipulated through fatigue attacks. Tokens are stolen. Phones are seized. Users are coerced into authorizing transfers. Biometric systems can be compelled or spoofed. High-value digital asset holders face physical threats. Enterprise administrators face social engineering. AI-agent workflows introduce new risks in which automated systems may act with delegated authority faster than human users can supervise.

The problem is therefore not simply that authentication needs another factor. The problem is that authentication needs a stronger concept of the human. Nash Identity Safe is designed around that concept: proof of authorized human presence.

4 Design Philosophy

Nash Identity Safe is governed by five design principles.

4.1 Human Authorization Before Credential Release

The device should release cryptographic authorization only after a local ceremony establishes that the user is present, cognitively engaged, and within acceptable safety policy. This is not merely account security. It is authorization security.

4.2 Local-First Cognitive Privacy

Brain and body data are sensitive authentication inputs, not cloud assets. Raw EEG, cognitive-response signals, color-perception profiles, physiological telemetry, and local model parameters should remain on device or within a trusted local environment. Remote systems should receive proofs, commitments, or authorization outcomes rather than raw biometric data.

4.3 Revocability Over Permanent Biometrics

Fingerprints, face geometry, and iris patterns are difficult or impossible to revoke once compromised. Nash Identity Safe avoids reliance on fingerprint or iris authentication. Instead, it uses revocable cognitive challenge-response profiles, including color-perception-based response patterns and EEG-derived Proof-of-Brain verification.

4.4 Quantum-Safe and Crypto-Agile Architecture

Authentication infrastructure must survive the post-quantum migration. Nash Identity Safe is designed to use post-quantum key establishment and to remain crypto-agile as standards mature. ML-KEM is the baseline for lattice-based key establishment under FIPS 203 (National Institute of Standards and Technology 2024b). ML-DSA and SLH-DSA provide standards-track post-quantum signature options for future device attestation, credential signing, and authorization workflows (National Institute of Standards and Technology 2024a, 2024c).

4.5 Coercion-Aware Authorization

Ordinary authentication systems treat coerced compliance as valid authentication. Nash Identity Safe treats coercion as a security condition. The device may incorporate local distress-state signals to delay, deny, modify, or reroute authorization when a request appears inconsistent with normal user state. Such checks are risk signals, not claims of perfect emotion detection.

5 Relationship to Plurigrid and passport.gay

Plurigrid's passport.gay technology provides a public cognitive-identity thesis relevant to Nash Identity Safe. The passport.gay system describes "Proof of Brain" as an identity primitive based on EEG-derived entropy during interactive sessions, with no iris scans, no stored biometric templates, and a commitment-based identity model (Plurigrid 2026b). Its public description includes EEG acquisition, frequency-domain analysis, Shannon entropy, GF(3) state mapping, and decentralized identity commitments (Plurigrid 2026b).

Nash Identity Safe does not treat this thesis as a public biometric database. Instead, it adapts the concept of cognitive participation into a private hardware authentication ceremony. The final authentication factor is not a scan of a permanent body part. It is a live cognitive event: the user perceives color stimuli, responds to a trusted challenge, and produces an EEG-derived response pattern that can be evaluated locally against a revocable profile.

Plurigrid's post-quantum web thesis also informs Nash Identity Safe's cryptographic posture. Plurigrid argues that the weak point in many systems is not only encryption but identity: certificate chains, DNS-bound trust, classical signatures, and asymmetric key exchange remain vulnerable to future quantum attacks (Plurigrid 2026c). Nash Identity Safe adopts the practical implication of this argument by designing identity, pairing, attestation, and authorization flows for post-quantum migration.

6 System Overview

Nash Identity Safe is a multi-factor, state-aware authentication device. Its architecture can be summarized as follows:

1. **Something the user has:** the Nash Identity Safe device and, where enabled, an approved paired biosensor.
2. **Something the user knows:** a local PIN or equivalent device secret.
3. **Something the user cognitively is:** a revocable cognitive-color response profile verified through live color-perception challenge-response.
4. **Something the user's state indicates:** local physiological risk signals that may indicate stress, fear, or coercion.
5. **Something the device proves cryptographically:** a post-quantum-secured authorization, attestation, commitment, or signature.

The system is intended to support protected operations including privileged login, digital asset authorization, secure communications, device unlocking, AI-agent delegation, identity recovery, and high-assurance enterprise approvals.

7 Cognitive-Color Challenge-Response

Color perception provides a rich cognitive surface for human authentication. It is not used as a simple preference quiz, nor as a replacement for cryptographic identity. Instead, color perception is used to generate a live, revocable, user-specific cognitive response ceremony.

During enrollment, the device presents a sequence of calibrated color stimuli through a trusted local display. The user responds to perceived hues, transitions, contrasts, or relationships among stimuli. Simultaneously, the device records local EEG response patterns and interaction timing. A lightweight on-device model learns a user-specific response profile. During later authentication, the device presents shorter challenge sequences and compares live response features against the local profile.

The value of this approach is that it avoids permanent biometric dependency. A fingerprint, face, or iris pattern is bound to the body. A cognitive-color challenge profile can be retrained, rotated, invalidated, or replaced. If a profile is suspected of compromise, the user can perform a new enrollment ceremony with a new challenge set.

The public claim is therefore narrow and precise: Nash Identity Safe uses color-perception-based cognitive challenge-response as a revocable liveness and identity factor within a broader authentication stack.

8 Proof-of-Brain as Final Authentication Factor

Proof-of-Brain is the final local factor in the Nash Identity Safe authentication ceremony. It is derived from live EEG response during cognitive challenge-response, not from a static biometric template.

A typical high-assurance authorization flow proceeds as follows:

1. The user initiates a protected action.
2. Nash Identity Safe wakes a trusted local ceremony.
3. The device verifies possession and local hardware state.
4. The user enters a PIN or local secret.
5. The device presents a color-perception challenge.
6. EEG response is measured locally.
7. The cognitive response profile is evaluated locally.
8. Optional distress-state signals are evaluated under local policy.
9. A post-quantum secure channel is established or resumed.
10. The device releases an authorization proof, attestation, or signature.

The relying party does not receive raw EEG data. It receives a cryptographic output indicating that the local device policy was satisfied.

9 Post-Quantum Cryptographic Architecture

Nash Identity Safe is designed for post-quantum key establishment and crypto-agile authorization.

9.1 ML-KEM Secure Channel

ML-KEM is the Module-Lattice-Based Key-Encapsulation Mechanism standardized by NIST in FIPS 203. NIST states that ML-KEM's security is related to the Module Learning With Errors problem and that the standard is believed to be secure even against adversaries possessing a quantum computer (National Institute of Standards and Technology 2024b). A key-encapsulation mechanism enables parties to establish a shared secret over a public channel, which can then be used with symmetric cryptography for authenticated secure communication (National Institute of Standards and Technology 2024b).

Nash Identity Safe uses ML-KEM-class key establishment as the baseline design direction for secure sessions among the device, companion applications, approved biosensors, and relying-party infrastructure. The purpose is to avoid building a new authentication system around classical key-establishment primitives that are already scheduled for migration.

9.2 Symmetric Encryption and Message Authentication

After post-quantum key establishment, secure sessions can use mature symmetric authenticated-encryption constructions. Plurigrid's post-quantum thesis notes that symmetric and hash primitives such as AES-256, ChaCha20-Poly1305, SHA-256, and BLAKE2 are comparatively more robust against quantum attack than classical asymmetric schemes, although Grover's algorithm changes effective security margins (Plurigrid 2026c). Nash Identity Safe therefore separates key establishment from bulk authenticated encryption and maintains algorithm agility across both layers.

9.3 Post-Quantum Signatures and Attestation

Future versions of Nash Identity Safe may use ML-DSA or SLH-DSA for device attestation, credential signing, firmware verification, or relying-party authorization. ML-DSA, standardized in FIPS 204, is a module-lattice-based digital signature algorithm (National Institute of Standards and Technology 2024a). SLH-DSA, standardized in FIPS 205, is a stateless hash-based digital signature algorithm used to detect unauthorized modification and authenticate a signatory (National Institute of Standards and Technology 2024c). The architecture remains compatible with hybrid classical and post-quantum modes during migration.

9.4 Crypto-Agility

No single post-quantum primitive should be treated as permanent. Nash Identity Safe is designed to support algorithm migration, parameter upgrades, protocol versioning, and future replacement of cryptographic components. This is consistent with national quantum-readiness guidance, which urges organizations to inventory cryptographic dependencies, identify systems with long secrecy lifetimes, and prepare migration roadmaps (Cybersecurity and Infrastructure Security Agency, National Security Agency, and National Institute of Standards and Technology 2023).

10 Coercion-Aware Authentication

Nash Identity Safe treats coercion as a distinct security problem. A user who enters the correct PIN at gunpoint has not safely authorized a transaction. A user who unlocks a device under acute fear has not produced the same security condition as a user acting voluntarily.

The system may incorporate locally evaluated physiological risk signals, such as heart-rate variability deviation or other paired biosensor telemetry. These signals do not define identity. They modulate risk. When local policy detects abnormal distress or coercion risk, the device may delay authorization, require re-verification, refuse a protected action, enter a limited safe mode, or activate a user-configured decoy or recovery path.

The claim is not that a device can perfectly infer emotion. The claim is that distress-aware authentication is superior to authentication systems that ignore coercion entirely. Physiological stress and affect detection are active research areas, and multimodal datasets such as WESAD demonstrate the relevance of wearable signals for stress and affect modeling (Schmidt et al. 2018). Noninvasive cortisol sensing and wearable biochemical sensing are also emerging research areas, with prior work demonstrating molecularly selective wearable cortisol sensing concepts (Parlak et al. 2018). Nash Identity Safe uses these directions as part of a broader coercion-aware security thesis, while preserving local processing and avoiding overclaiming deterministic fear detection.

11 Privacy Architecture

Nash Identity Safe follows a strict privacy model:

1. Raw EEG does not leave the device by default.
2. Color-perception response profiles remain local.
3. Physiological telemetry remains local or within an explicitly paired trusted device.
4. Relying parties receive cryptographic authorization, not raw biometric data.
5. Cognitive profiles are revocable and can be retrained.
6. The system avoids fingerprint and iris dependencies.
7. Cloud services are not required for core authentication.

This architecture aligns with the passport.gay emphasis on no stored biometric templates and commitment-based identity representation (Plurigrid 2026b). It also responds to the central ethical problem of biometric identity systems: permanent exposure. Nash Identity Safe treats the user's brain and body data as private local inputs, not extractable platform assets.

12 Device Architecture

The public reference architecture contains six components.

12.1 Trusted Local Interface

The device includes a trusted interface capable of presenting local authentication challenges. This may include a small screen or equivalent controlled output channel. The purpose is to prevent the host computer or phone from fully controlling the authentication ceremony.

12.2 Cognitive and EEG Input Layer

The device incorporates noninvasive EEG or approved BCI input to measure live cognitive response during challenge-response. Public documentation intentionally omits electrode geometry, signal-processing details, sampling configuration, model architecture, and threshold logic.

12.3 Secure Compute Environment

Sensitive computation occurs in a secure local environment. This includes model inference, cognitive-profile comparison, cryptographic operations, and policy enforcement. The device is designed so that authentication decisions do not require exporting raw signals to a cloud service.

12.4 Post-Quantum Communication Layer

The device communicates with approved host applications, companion sensors, or relying-party infrastructure through authenticated encrypted channels. ML-KEM-class post-quantum key establishment is the baseline design direction for future-resistant session establishment.

12.5 Optional Paired Biosensor Layer

Where enabled, the device may receive local distress-state signals from an approved wearable or companion biosensor. Communication between the paired component and Nash Identity Safe should be encrypted, authenticated, and resistant to replay or unauthorized pairing.

12.6 Revocable Profile Store

The device maintains revocable local profiles for cognitive-color response and related liveness verification. These profiles are not public biometric templates and are not intended to be stored on-chain or in cloud databases.

13 Security Model

Nash Identity Safe is designed to reduce risk from the following threat categories:

- credential theft;
- phishing and push-MFA manipulation;
- stolen hardware tokens;
- coerced authorization;
- session hijacking;
- host-device compromise affecting the user interface;
- biometric replay and static biometric compromise;
- unauthorized AI-agent delegation;
- classical public-key migration risk;
- harvest-now, decrypt-later exposure for long-lifetime secrets.

The system does not claim to eliminate all risk. It is not described as unhackable. It does not fully solve physical coercion, supply-chain compromise, malicious firmware installation, sophisticated side-channel attacks, or all host-malware conditions. It is a defense-in-depth architecture designed to make high-value authorization more human-aware, privacy-preserving, and quantum-safe.

14 Comparison to Existing Authentication Models

Model	Strength	Limitation
Password or PIN	Simple and widely deployed	Phishable, guessable, coerced, and often reused
Authenticator app	Better than password alone	Vulnerable to social engineering and device compromise
Push MFA	Convenient	Vulnerable to fatigue attacks and coerced approval
Hardware security key	Strong possession factor	Can be stolen or used under coercion
Fingerprint or iris biometric	Convenient body-derived signal	Difficult to revoke and privacy-sensitive
FIDO-style passkey	Phishing-resistant public-key authentication (FIDO Alliance 2026)	Does not inherently prove cognitive engagement or absence of duress
Nash Identity Safe	Hardware-rooted, cognitive, post-quantum-ready, and coercion-aware	Requires specialized hardware and careful enrollment

Table 1: Authentication model comparison.

15 Use Cases

15.1 Digital Asset Authorization

Nash Identity Safe can protect high-value digital asset operations by requiring live cognitive verification before approving a transfer, wallet operation, treasury action, or key-release event.

15.2 Enterprise Privileged Access

The device can support privileged access workflows for administrators, executives, engineers, security teams, and operators whose credentials could expose critical systems.

15.3 AI-Agent Delegation

As users delegate tasks to AI agents, Nash Identity Safe can serve as a human checkpoint for high-impact actions. An agent may prepare an action, but the authorized human must cognitively verify and release the final authorization.

15.4 Secure Communications

The device can protect encrypted communication sessions, identity assertions, signing operations, and key-rotation ceremonies.

15.5 Defense and High-Assurance Environments

Nash Identity Safe is suitable for environments where authentication must account for human presence, cryptographic future-resistance, and reduced reliance on phishable credentials.

16 Nash Ecosystem Context

The public Nash portal and the public `nash-portal` repository demonstrate an early ecosystem interface. The repository describes a NASH token terminal user interface in the browser using Ratzilla WebAssembly and GeckoTerminal candlestick data (Plurigrid 2026a). The public Nash portal provides a minimal public interface for the Nash ecosystem (Nash 1337 2026).

Nash Identity Safe is distinct from the public portal. The portal is an interface layer. Nash Identity Safe is a hardware-rooted authentication product category focused on post-quantum identity, cognitive verification, and coercion-resistant authorization.

17 Ethics and Governance

Cognitive authentication requires unusually careful governance. A system that touches brain signals, perception, physiological state, and authorization must be designed around user sovereignty.

Nash Identity Safe is therefore governed by the following ethical commitments:

1. No raw cognitive or physiological cloud extraction for core authentication.
2. No hidden emotion surveillance.
3. No mandatory fingerprint or iris enrollment.
4. No sale of brain or body data.
5. No relying-party access to raw biometric signals.
6. Clear user consent for optional biosensor pairing.
7. Revocable profiles and re-enrollment rights.
8. Transparent safety modes and recovery options.
9. Third-party security and privacy review before sensitive deployments.

The purpose of Nash Identity Safe is to protect human authorization, not to commodify human cognition.

18 Roadmap

18.1 Phase I: Research Prototype

Develop internal prototypes for trusted color challenge-response, local EEG capture, cognitive-profile evaluation, post-quantum session establishment, and secure local policy enforcement.

18.2 Phase II: Security Architecture

Formalize the threat model, enrollment protocol, recovery model, firmware update strategy, anti-tamper posture, and cryptographic protocol suite. Conduct internal red-team review.

18.3 Phase III: Hardware Evaluation

Evaluate device form factors, display mechanisms, dry-electrode feasibility, secure compute options, paired biosensor interfaces, battery constraints, and usability requirements.

18.4 Phase IV: Pilot Deployment

Conduct controlled pilots with consenting users in bounded workflows such as testnet authorization, enterprise login simulation, or high-value approval rehearsal.

18.5 Phase V: External Review

Commission third-party review for cryptography, firmware security, privacy, usability, biometric ethics, and post-quantum migration readiness.

19 Conclusion

Nash Identity Safe is built for a world in which authentication must become more human-aware, more private, and more quantum-safe. Web-era systems verify credentials. Nash Identity Safe verifies authorization.

The system combines hardware-rooted possession, local knowledge, color-perception-based cognitive challenge-response, EEG-derived Proof-of-Brain verification, optional coercion-aware risk checks, and post-quantum cryptographic communication. It avoids fingerprint and iris dependencies. It keeps raw brain and body data local. It supports the migration from classical public-key infrastructure to post-quantum identity systems.

The result is a new class of cybersecurity product: a safe for human authorization.

A Restrictive Technology License Agreement and Terms of Use

A.1 Parties

This Restrictive Technology License Agreement and Terms of Use, the "Agreement," governs access to and use of Nash Identity Safe, related software, firmware, hardware, documentation, prototypes, demonstrations, evaluation units, technical materials, and associated intellectual property, collectively the "Technology," made available by Nash 1337, Inc., the "Company."

By accessing, reviewing, testing, possessing, using, evaluating, or receiving the Technology, the recipient, evaluator, reader, or user, the "Recipient," agrees to be bound by this Agreement.

A.2 License Grant

Subject to full compliance with this Agreement, Nash 1337, Inc. grants the Recipient a limited, revocable, non-exclusive, non-transferable, non-sublicensable license to use the Technology solely for internal, non-commercial, evaluation purposes. No other rights are granted, whether by implication, estoppel, exhaustion, or otherwise.

A.3 Restrictions

The Recipient may not, directly or indirectly:

1. reverse engineer, decompile, disassemble, inspect, image, probe, bypass, extract, or otherwise attempt to derive the source code, firmware, hardware layout, secure-element configuration, cryptographic key hierarchy, model architecture, biometric feature representation, sensor-fusion logic, enrollment protocol, anti-tamper mechanism, or underlying design of the Technology;

2. modify, adapt, translate, improve, emulate, clone, reproduce, or create derivative works based on the Technology;

3. remove, obscure, alter, or falsify any copyright, trademark, patent, confidentiality, attribution, provenance, watermark, device identifier, or proprietary notice;

4. use the Technology to provide services to third parties, including but not limited to authentication-as-a-service, security-as-a-service, SaaS offerings, managed security services, commercial wallet infrastructure, enterprise access-control services, or production cryptographic authorization, without a separate written commercial license from Nash 1337, Inc.;

5. use the Technology in any production, commercial, government, defense, financial, medical, or regulated environment without express written authorization from Nash 1337, Inc.;

6. use the Technology to develop, train, benchmark, validate, or improve a competing product, service, model, device, protocol, patent application, or authentication system;

7. copy or extract any biometric, cognitive, EEG, physiological, cryptographic, or device telemetry except as expressly permitted in writing by Nash 1337, Inc.;

8. attempt to circumvent, disable, or test beyond authorized scope any safety, policy, pairing, authentication, enrollment, recovery, anti-tamper, or access-control mechanism;

9. publish security findings, vulnerability details, benchmarks, teardown information, protocol traces, model behavior, device internals, or performance measurements without prior written consent from Nash 1337, Inc.;

10. transfer, sell, lease, lend, sublicense, disclose, export, or otherwise make available the Technology to any third party without prior written authorization from Nash 1337, Inc.

A.4 Intellectual Property

All rights, title, and interest in and to the Technology, including all patents, patent applications, copyrights, trade secrets, trademarks, mask works, designs, inventions, discoveries, know-how, models, algorithms, datasets, documentation, firmware, software, hardware designs, protocols, and related intellectual property, remain exclusively with Nash 1337, Inc. No ownership rights are transferred under this Agreement.

A.5 Confidentiality

Any non-public information disclosed by Nash 1337, Inc. in connection with the Technology, including technical materials, prototypes, design concepts, security architecture, product plans, business strategy, sensor design, firmware behavior, model logic, cryptographic architecture, and evaluation data, is confidential information. The Recipient shall protect such information using at least reasonable care and shall not disclose it to any third party without prior written authorization from Nash 1337, Inc.

A.6 Feedback

If the Recipient provides suggestions, comments, bug reports, ideas, improvements, analyses, test results, or other feedback regarding the Technology, the Recipient grants Nash 1337, Inc. a perpetual, irrevocable, worldwide, royalty-free, fully paid, transferable, sublicensable license to use, reproduce, modify, commercialize, and otherwise exploit such feedback without restriction or compensation.

A.7 No Warranties

The Technology is provided "AS IS" and "AS AVAILABLE," without warranty of any kind, express, implied, statutory, or otherwise, including but not limited to warranties of merchantability, fitness for a particular purpose, title, non-infringement, accuracy, reliability, security, availability, or uninterrupted operation. Nash 1337, Inc. does not warrant that the Technology will detect all unauthorized access, coercion, distress, biometric spoofing, cryptographic attacks, device compromise, or other security threats.

A.8 Limitation of Liability

To the maximum extent permitted by law, in no event shall Nash 1337, Inc. be liable for any direct, indirect, incidental, special, consequential, exemplary, punitive, or other damages, including but not limited to loss of profits, loss of data, loss of assets, business interruption, personal injury, security breach, unauthorized transaction, device failure, biometric error, false acceptance, false rejection, or other liability arising from or related to the use, inability to use, evaluation, possession, testing, or reliance upon the Technology, even if advised of the possibility of such damages.

A.9 High-Risk Use

The Technology is not authorized for use in life-support systems, emergency response systems, medical diagnosis, weapons systems, nuclear facilities, aviation control, critical infrastructure, or any environment where failure could reasonably lead to death, severe bodily injury, catastrophic loss, or unlawful deprivation of rights, unless Nash 1337, Inc. has entered into a separate written agreement expressly authorizing such use.

A.10 Termination

Nash 1337, Inc. may terminate this Agreement and the license granted herein at any time, with or without cause, upon notice to the Recipient. Upon termination, the Recipient shall immediately cease all use of the Technology and, at Nash 1337, Inc.'s option, return or destroy all copies, prototypes, materials, documentation, and confidential information.

A.11 Reservation of Rights

All rights not expressly granted are reserved by Nash 1337, Inc. Nothing in this Agreement limits Nash 1337, Inc.'s right to develop, license, sell, enforce, protect, modify, or discontinue the Technology.

References

Cybersecurity and Infrastructure Security Agency, National Security Agency, and National Institute of Standards and Technology. 2023. *Quantum-Readiness: Migration to Post-Quantum Cryptography.* Accessed April 24, 2026. https://media.defense.gov/2023/Aug/21/2003284212/-1/-1/0/CSI-QUANTUM-READINESS.PDF.

FIDO Alliance. 2026. "How FIDO Works." Accessed April 24, 2026. https://fidoalliance.org/how-fido-works/.

Nash 1337. 2026. "Nash Portal." Accessed April 24, 2026. https://nash.actor.

National Institute of Standards and Technology. 2024a. *Module-Lattice-Based Digital Signature Standard.* FIPS 204. Accessed April 24, 2026. https://csrc.nist.gov/pubs/fips/204/final.

———. 2024b. *Module-Lattice-Based Key-Encapsulation Mechanism Standard.* FIPS 203. Accessed April 24, 2026. https://csrc.nist.gov/pubs/fips/203/final.

———. 2024c. *Stateless Hash-Based Digital Signature Standard.* FIPS 205. Accessed April 24, 2026. https://csrc.nist.gov/pubs/fips/205/final.

Parlak, Onur, Scott T. Keene, Andrew Marais, Vincenzo F. Curto, and Alberto Salleo. 2018. "Molecularly Selective Nanoporous Membrane-Based Wearable Organic Electrochemical Device for Noninvasive Cortisol Sensing." *Science Advances* 4 (7). https://doi.org/10.1126/sciadv.aar2904.

Plurigrid. 2026a. "nash-portal: NASH Token TUI in the Browser." Accessed April 24, 2026. https://github.com/plurigrid/nash-portal.

———. 2026b. "Passport.gay: Your Brain Is Your Passport." Accessed April 24, 2026. https://plurigrid.com/passport-gay.

———. 2026c. "The Post-Quantum Web / Post-Web Thesis." Accessed April 24, 2026. https://plurigrid.com/pq.

Schmidt, Philip, Attila Reiss, Robert Duerichen, Claus Marberger, and Kristof Van Laerhoven. 2018. "Introducing WESAD, a Multimodal Dataset for Wearable Stress and Affect Detection." *Proceedings of the 20th ACM International Conference on Multimodal Interaction,* 400–408. https://doi.org/10.1145/3242969.3242985.