



AION Protocol Platform

Executive Report — Integrated Build v1.1

What Has Improved, What We Now Have, and Why It Matters

GRMG LLC — Global Resources Management Group

Prepared for Executive & Partner Review

Confidential — June 2026

Contents

Contents

2

1. Executive Summary

7

The AION Protocol Platform has advanced from a working demonstration into a hardened, deployable product ready for vendor evaluation and licensing. This report documents the improvements delivered in the integrated v1.1 build, what the platform now provides end to end, and why each change strengthens our position with banks, defense-oriented buyers, and other security-conscious institutions.

7

Three themes define this release. First, security was hardened where it mattered most — password protection was rebuilt, and per-message forward secrecy was added so that a future key compromise cannot unlock past communications. Second, the platform became durable and operable — all data now survives restarts, the system is licensed and self-managing, and vendors can deploy it with a single click. Third, everything is proven, not asserted — 75 automated tests, including real browser tests of the in-browser encryption, confirm the platform behaves as described.

7

Bottom line: AION is now something we can put in front of a hostile technical reviewer with confidence. Each claim is backed by working, tested code, and the scope of what is live versus planned is stated honestly — which is itself a credibility asset in front of the audiences we are selling to.

7

2. Where We Started

7

The prior build was an honest, well-structured demonstration of the AION concept: real X25519 and AES-256-GCM encryption, a local-entropy key path with no dependence on public data feeds, a hash-chained integrity ledger, and an administrator approval portal. It proved the idea and was clean enough to show to partners such as the Tucson Embedded Systems and Zoho discussions.

7

However, a candid review identified gaps that a professional evaluator would flag in the first hour — not flaws in the concept, but the difference between a demonstration and a product. The platform's own capabilities page already named two of them. Addressing these gaps was the purpose of this release.

8

Gaps identified before this release

8

3. What We Improved

9

Each gap above has been closed. The table below summarizes the before-and-after; the sections that follow explain why each improvement matters to a buyer.

9

4. What We Now Have — and Why It Is Good

10

4.1 Hardened security that survives scrutiny

10

Stronger password protection. Passwords are now protected with scrypt, a deliberately slow, memory-hard algorithm that makes large-scale password cracking economically impractical. Existing accounts upgrade automatically the next time a user logs in, so the improvement requires no disruption. Why it is good: this is the single most common finding in a security review of a login system; closing it removes an easy criticism and protects our users' credentials.

10

Per-message forward secrecy. Each message can now be locked with a one-time key that is discarded after use. Even if someone later steals a user's long-term keys, they cannot read past messages. Why it is good: forward secrecy is the standard expected of any serious secure-messaging product, and it directly answers the "what if keys are stolen later" question every security buyer asks.

10

Honest, named scope. The platform provides forward secrecy today; the more advanced "self-healing" property of a full ratchet is named as a roadmap item rather than implied. Why it is good: stating limits plainly

builds trust with technical reviewers far more effectively than overclaiming, which is quickly exposed.

10

4.2 A durable, tamper-evident system

10

Everything now persists. Messages, the integrity ledger, user accounts, licensing state, and connection settings are all stored durably and survive restarts. The integrity ledger — our tamper-evidence mechanism — now persists across reboots and refuses to start if its chain has been altered. Why it is good: a tamper-evident log that resets on every restart is the first thing a reviewer dismisses. A log that survives and self-verifies is a genuine assurance feature we can demonstrate live.

10

4.3 A licensable, self-managing product

10

Self-expiring 90-day evaluations. Each vendor receives a cryptographically signed license. A beta evaluation runs for 90 days from first launch and then expires on its own, with no action required from us, and without deleting any of the vendor's data. Why it is good: it lets us run controlled trials at scale without manual oversight, and protects our intellectual property.

10

Seamless upgrade to a paid license. When a vendor decides to buy, installing the full license unlocks the product in place — all of their contacts, message history, and audit records carry over automatically, with no migration. Why it is good: the path from trial to paying customer has zero friction and zero data loss, removing a common reason deals stall.

10

4.4 Easy to deploy, easy to support

11

One-click start. Vendors launch the platform by double-clicking a single icon carrying the GRMG mark; it starts the system and opens the console automatically, on Windows, macOS, or Linux. Why it is good: it removes the technical barrier to evaluation — a non-specialist can be running AION in under a minute.

11

Built-in support channel. A Contact-GRMG button lets any user or vendor send us a question; messages are saved immediately and delivered by both email and text, so nothing is lost even if a channel is temporarily down. Why it is good: it shortens our feedback loop during trials and signals a supported, professional product.

11

Distribute to a whole team in one step. From the console, a vendor can build a one-click package for their own testers, and we can stamp out a customized, branded build for each client from a single configuration file. Why it is good: it turns onboarding a new evaluator from an IT project into a download.

11

4.5 AION as a secure front for a vendor's own systems

11

An authenticated, audited gateway. Vendors can place their own back-end services behind AION. Every request is then authenticated and recorded in the tamper-evident ledger before it reaches their system. Critically, the product ships with no GRMG endpoints or ports of any kind — that information stays confidential by design. Why it is good: it lets AION become a protective layer over a customer's existing infrastructure — a much larger role than messaging alone — while keeping our own systems private.

11

5. Proof: Tested, Not Asserted

12

A central principle of this release is that every claim is backed by working code that is automatically tested. The platform now ships with 75 automated checks across three layers, all passing:

12

Why it is good: the live browser tests are especially significant — they confirm that encryption happens on the user's device and that our servers never see readable content. This is a claim we can now prove on demand, which is exactly what a security-conscious buyer needs to see.

12

6. Capability Snapshot

12

Live today

12

On the roadmap (named honestly)

12

7. Why This Matters for GRMG

14

The audiences we are selling to — banks, defense-oriented buyers, and regulated institutions — do not buy on promises. They buy on demonstrable security, operational maturity, and the credibility of the team behind the product. This release moves AION decisively toward all three.

14

1. Executive Summary

The AION Protocol Platform has advanced from a working demonstration into a hardened, deployable product ready for vendor evaluation and licensing. This report documents the improvements delivered in the integrated v1.1 build, what the platform now provides end to end, and why each change strengthens our position with banks, defense-oriented buyers, and other security-conscious institutions.

Three themes define this release. First, security was hardened where it mattered most — password protection was rebuilt, and per-message forward secrecy was added so that a future key compromise cannot unlock past communications. Second, the platform became durable and operable — all data now survives restarts, the system is licensed and self-managing, and vendors can deploy it with a single click. Third, everything is proven, not asserted — 75 automated tests, including real browser tests of the in-browser encryption, confirm the platform behaves as described.

Bottom line: AION is now something we can put in front of a hostile technical reviewer with confidence. Each claim is backed by working, tested code, and the scope of what is live versus planned is stated honestly — which is itself a credibility asset in front of the audiences we are selling to.

2. Where We Started

The prior build was an honest, well-structured demonstration of the AION concept: real X25519 and AES-256-GCM encryption, a local-entropy key path with no dependence on public data feeds, a hash-chained integrity ledger, and an administrator approval portal. It proved the idea and was clean enough to show to partners such as the Tucson Embedded Systems and Zoho discussions.

However, a candid review identified gaps that a professional evaluator would flag in the first hour — not flaws in the concept, but the difference between a demonstration and a product. The platform's own capabilities page already named two of them. Addressing these gaps was the purpose of this release.

Gaps identified before this release

Area	The gap
Password protection	User passwords were protected with a single, fast hash — vulnerable to brute-force cracking on modern hardware.
Data durability	Messages and the integrity ledger lived only in memory; a restart erased them, resetting the tamper-evident log to zero.
Forward secrecy	A future compromise of a stored key could expose past messages — the capabilities page flagged this openly.
Fixed key salt	A demo used a hardcoded cryptographic salt, also flagged on the capabilities page.
Licensing & lifecycle	No mechanism to license the product, enforce a trial period, or upgrade a vendor without losing their data.
Deployment & support	No one-click start for non-technical users, no built-in support channel, and no way to safely place a vendor's own systems behind AION.

3. What We Improved

Each gap above has been closed. The table below summarizes the before-and-after; the sections that follow explain why each improvement matters to a buyer.

Capability	Before	Now
Password security	Fast single-pass hash	scrypt (memory-hard); old accounts auto-upgrade on next login
Persistence	In-memory; lost on restart	Durable database; messages, ledger, peers, and settings survive restarts
Forward secrecy	Not present (flagged)	Per-message forward secrecy via one-time prekeys
Key salt	Fixed demo salt (flagged)	Random per-operation salts throughout
Tamper evidence	Reset on restart	Ledger persists and refuses to start on a broken chain
Licensing	None	90-day self-expiring trial; in-place upgrade with no data loss
Support channel	None	In-app Contact-GRMG (email + SMS), nothing lost if offline
Vendor integration	None	Authenticated, audited gateway fronting a vendor's own systems
Deployment	Manual	One-click launchers (Windows/macOS/Linux) with the GRMG logo
Distribution	Manual	Per-client package builder and a one-click tester bundle
Assurance	Manual checks	75 automated tests incl. real in-browser encryption tests

4. What We Now Have — and Why It Is Good

4.1 Hardened security that survives scrutiny

Stronger password protection. Passwords are now protected with scrypt, a deliberately slow, memory-hard algorithm that makes large-scale password cracking economically impractical. Existing accounts upgrade automatically the next time a user logs in, so the improvement requires no disruption. **Why it is good:** this is the single most common finding in a security review of a login system; closing it removes an easy criticism and protects our users' credentials.

Per-message forward secrecy. Each message can now be locked with a one-time key that is discarded after use. Even if someone later steals a user's long-term keys, they cannot read past messages. **Why it is good:** forward secrecy is the standard expected of any serious secure-messaging product, and it directly answers the "what if keys are stolen later" question every security buyer asks.

Honest, named scope. The platform provides forward secrecy today; the more advanced "self-healing" property of a full ratchet is named as a roadmap item rather than implied. **Why it is good:** stating limits plainly builds trust with technical reviewers far more effectively than overclaiming, which is quickly exposed.

4.2 A durable, tamper-evident system

Everything now persists. Messages, the integrity ledger, user accounts, licensing state, and connection settings are all stored durably and survive restarts. The integrity ledger — our tamper-evidence mechanism — now persists across reboots and refuses to start if its chain has been altered. **Why it is good:** a tamper-evident log that resets on every restart is the first thing a reviewer dismisses. A log that survives and self-verifies is a genuine assurance feature we can demonstrate live.

4.3 A licensable, self-managing product

Self-expiring 90-day evaluations. Each vendor receives a cryptographically signed license. A beta evaluation runs for 90 days from first launch and then expires on its own, with no action required from us, and without deleting any of the vendor's data. **Why it is good:** it lets us run controlled trials at scale without manual oversight, and protects our intellectual property.

Seamless upgrade to a paid license. When a vendor decides to buy, installing the full license unlocks the product in place — all of their contacts, message history, and audit records carry over automatically, with no migration. **Why it is**

good: the path from trial to paying customer has zero friction and zero data loss, removing a common reason deals stall.

4.4 Easy to deploy, easy to support

One-click start. Vendors launch the platform by double-clicking a single icon carrying the GRMG mark; it starts the system and opens the console automatically, on Windows, macOS, or Linux. **Why it is good:** it removes the technical barrier to evaluation — a non-specialist can be running AION in under a minute.

Built-in support channel. A Contact-GRMG button lets any user or vendor send us a question; messages are saved immediately and delivered by both email and text, so nothing is lost even if a channel is temporarily down. **Why it is good:** it shortens our feedback loop during trials and signals a supported, professional product.

Distribute to a whole team in one step. From the console, a vendor can build a one-click package for their own testers, and we can stamp out a customized, branded build for each client from a single configuration file. **Why it is good:** it turns onboarding a new evaluator from an IT project into a download.

4.5 AION as a secure front for a vendor's own systems

An authenticated, audited gateway. Vendors can place their own back-end services behind AION. Every request is then authenticated and recorded in the tamper-evident ledger before it reaches their system. Critically, the product ships with no GRMG endpoints or ports of any kind — that information stays confidential by design. **Why it is good:** it lets AION become a protective layer over a customer's existing infrastructure — a much larger role than messaging alone — while keeping our own systems private.

5. Proof: Tested, Not Asserted

A central principle of this release is that every claim is backed by working code that is automatically tested. The platform now ships with 75 automated checks across three layers, all passing:

Test layer	Checks	What it proves
Server integration	25	Login, approvals, forward-secrecy key exchange, durable inbox, support channel, gateway, ledger integrity, and survival across restarts.
Live browser tests	11	Two real browser sessions perform the actual in-browser encryption: keys publish, a message is sent with forward secrecy and decrypted by the recipient, and a compressed file transfers — while the server only ever holds scrambled ciphertext.
Component tests	39	Licensing expiry and upgrade, tamper detection, support-channel delivery and retry, and the packaging builder.

Why it is good: the live browser tests are especially significant — they confirm that encryption happens on the user's device and that our servers never see readable content. This is a claim we can now prove on demand, which is exactly what a security-conscious buyer needs to see.

6. Capability Snapshot

Live today

- **Secure messaging** — encrypted on the user's device; the server relays scrambled ciphertext only.
- **Per-message forward secrecy** — past messages stay protected even if keys are later compromised.
- **Hardened login** — bcrypt password protection with automatic upgrade of older accounts.
- **Tamper-evident audit ledger** — persists across restarts and self-verifies on startup.
- **Encrypted file transfer** — files are intelligently compressed, then encrypted.
- **1-to-1 voice and video** — end-to-end encrypted media, authenticated by the same identities.
- **90-day self-expiring licensing** — with seamless, no-data-loss upgrade to a paid license.
- **In-app GRMG support channel** — delivered by email and SMS, with nothing lost if offline.
- **Authenticated connections gateway** — AION as an audited front over a vendor's own systems.
- **One-click deployment and tester packaging** — branded with the GRMG mark.

On the roadmap (named honestly)

- **Full ratchet messaging** — adds self-healing security after a compromise, on top of today's forward secrecy.
- **Group voice and video** — secure multi-party calls.

- **Post-quantum key exchange** — the upgrade path is already built into the design.
- **Online license check-in** — for stronger enforcement where required.

7. Why This Matters for GRMG

The audiences we are selling to — banks, defense-oriented buyers, and regulated institutions — do not buy on promises. They buy on demonstrable security, operational maturity, and the credibility of the team behind the product. This release moves AION decisively toward all three.

- **Credibility under review:** the security improvements close the findings a professional reviewer looks for first, and add forward secrecy, a baseline expectation for the category.
- **Operational maturity:** durable storage, licensing, one-click deployment, and a support channel are the difference between a demo and a product an institution can actually run.
- **A repeatable sales motion:** the per-client builder, self-expiring trials, and seamless upgrade let us run many evaluations at once and convert them without friction.
- **Defensible honesty:** naming our limitations plainly, and backing every claim with automated tests, is precisely the posture that earns trust in rooms full of skeptics.

In short: we now have a secure, durable, licensable AION platform that a non-technical evaluator can launch in one click, that a hostile technical reviewer can inspect without finding the obvious gaps, and that we can distribute, support, and convert to paid licensing at scale. That is a materially stronger commercial asset than we held a release ago.

Prepared by GRMG LLC — Global Resources Management Group

AION Protocol Platform · Integrated Build v1.1 · Confidential