mementom

PUBLIC WHITE PAPER

Anonymous Customers. Accountable Companies.

Private permission for apps, software, services, websites, marketplaces, and consumer-directed exchange - without an identity profile

---

Your memory holds the key to what's next.

Patent pending | Public edition | August 2026

mementom.app | mementom.net

EXECUTIVE SUMMARY

The internet can recognize a customer without learning a life story

Most internet relationships begin by demanding an email address. An email is more than a communication channel: it is a durable address that can be tracked, breached, enriched, and correlated with other accounts. Changing a password changes the lock; it does not move the address or remove the target.

Mementom begins with a narrower question: is this the same private returning customer, and may this exact action happen now? A consumer creates one global Mementom account without giving Mementom a civil name, email address, phone number, social-login identity, or biometric identity. Each participating vendor receives a different stable random pairwise relationship and no global identifier.

THE PROPOSITION Anonymous customers. Accountable companies. Private permission. A photo and a phrase open the door - without asking who you are.

Why this matters

Continuity and identity are different needs. A marketplace may need to recognize the same seller, an app may need to restore a subscription, and a service may need to authorize a booking change without requiring Mementom to know who the consumer is. A vendor may still know its own customer when shipping, tax, payment, licensing, or regulation requires it; that separate identity never becomes a Mementom identity assertion.

01	02	03
Reusable	**Pairwise**	**Live**
One private account can connect to many participating products.	Every vendor receives a different relationship identifier.	Every consequential action is decided against current rights.

The commercial opening

Mementom is a private recognition and authorization marketplace for software, apps, online services, websites, and marketplaces. It also enables consumer-to-business-to-consumer, or C2B2C, exchange. A qualified broker may move data, insight, intent, and value under terms chosen by the consumer. Mementom clears the permission without receiving the exchanged data or enriching the anonymous account into identity.

1 / THE CONCEPT

A private credential relationship built from memory

The name Mementom blends memento with momentum. A memento preserves meaning. Momentum carries a person or system toward what comes next. The product joins those ideas: a memory becomes a key, and the key moves a permitted action forward.

The matching pair

PHOTO	PHRASE	MEMKEY
Something held	**Something recalled**	**One private pair**
A particular source image kept under the holder's control.	A private phrase connected to the meaning of that image.	The managed image and private phrase become one memkey.

The photo is not used to identify a face or subject. It is credential material. A landscape, garden gate, drawing, or another personally meaningful image can serve. The phrase is not a public caption or security question. Together the photo and phrase become a mementom key - a memkey for short. Neither element works alone.

One account, two through seven memkeys

A single master credential concentrates risk. Mementom maintains a private inventory of two through seven active memkeys. A participating product declares an assurance minimum. A new consumer creates that number; an existing consumer creates only the exact deficit. The consumer does not label which memkey serves which product right, and the vendor never sees or chooses the assignment.

Property	Meaning
Private recognition	The same vendor-local relationship returns without a civil identity assertion.
Two-part	The photo and phrase are verified as a matching pair.
Privately assigned	Mementom maps eligible memkeys to vendor-local challenge tags.
Replaceable	The consumer can rotate a memkey while Mementom preserves applicable tag coverage.
Live	Rights, lifecycle, risk, epochs, and operation bindings are checked for every challenge.

2 / OPERATING MODEL

Each participant owns a different part of the decision

Mementom separates consumer-held proof, vendor-defined business meaning, and live policy evaluation. This separation prevents a vendor operator from resetting a private memkey and then impersonating the consumer, while still letting the vendor change product rights immediately.

Role	Responsibility
Consumer	Keeps managed images and private phrases, approves vendor connections, and initiates rotation or disconnection.
Mementom	Owns the memkey relationships, private tag assignments, challenge selection, proof verification, risk state, and go/no-go decision delivery.
Participating vendor	Defines product rights, visible consequences, assurance policy, applications, and the business action enforced after a valid result.
Vendor backend	Creates signed requests, keeps response private keys, decrypts and verifies decisions, consumes them once, and performs the bound action.
Vendor application	Starts a connection or challenge and returns the consumer to the approved product destination; it never handles memkey proof.
Security operator	Investigates privacy-minimized events and changes rights or risk controls without learning the consumer's memkeys.

Separation of duties

The vendor knows that its pairwise subject has a named right but not which memkey implements that right. Mementom knows the private assignment but not the consumer's civil identity or the vendor's customer record. The consumer holds the two proof artifacts but does not know which product right maps to which memkey. The vendor's response private key remains only in its backend KMS or HSM.

DESIGN PRINCIPLE Mementom owns the memkey and the go/no-go decision delivery. The consumer controls the proof artifacts. The vendor controls the business right and enforces the exact result.

3 / ENROLLMENT

Connect once; add only what the product needs

A product begins with a short-lived, signed connection request. Mementom shows the verified product, purpose, requested rights, consequence, expiry, and approved return target before asking for proof. The consumer can create a private Mementom account or choose Already use Mementom and return through an existing memkey.

1. **Verify the product request.** Reject an expired, substituted, unregistered, or return-target-mismatched request before any proof screen appears.
2. **Create or reuse.** A new consumer creates the required two through seven memkeys. An existing consumer proves one memkey and adds only the exact policy deficit.
3. **Prepare the managed image.** Selection, drag, paste, or camera input is processed locally. The source image bytes never enter the API.
4. **Pair a private phrase.** The phrase is entered only inside Mementom and is deliberately excluded from password-manager capture.
5. **Assign coverage privately.** Mementom randomly maps eligible memkeys to product-local challenge tags. Neither the consumer nor vendor chooses or sees the mapping.
6. **Complete the pairwise connection.** The vendor receives only its random pairwise subject after the consumer confirms connection and required Account Key custody.

Managed images remain consumer-held

Every enrolled source becomes a managed color JPEG with a neutral random filename, a cryptographically random opaque pixel locator, and disposable Account Key search metadata. Exact managed-copy recognition is strongest; tolerant recognition is an optional, separately validated policy. The original untagged photo is not itself enrolled.

PRIVACY BOUNDARY Products never receive photos, phrases, Account Keys, global account IDs, memkey identifiers, or private tag assignments.

4 / LOGIN AND RECOVERY

Image-first access; guarded recovery when risk appears

Ordinary access starts with one managed memkey image. Its opaque locator scopes the account and one exact memkey; only then does Mementom request the matching private phrase. The Account Key is a photo-search and recovery aid, not a login field, authenticator, identity, or authority token.

1. **Present an image.** Local processing extracts strong image evidence without uploading original photo bytes.
2. **Request only its phrase.** Mementom never exposes a phrase hint, inventory count, Account Key, or which half of a failed pair was wrong.
3. **Check current state.** The service evaluates memkey status, account attempt timing, active IP block, risk, epochs, and the requested right.
4. **Open a scoped session.** Correct proof establishes the private Mementom account or product-local relationship, not a civil identity.

Suspicion changes the proof contract

A failed phrase after strong image identification flags that memkey and activates an account-wide image-attempt timing gate; it does not permanently lock correct proof. Unattempted, unflagged memkeys are requested first. A correct full pair begins only a provisional recovery session, followed by the required number of consecutive, distinct full memkey proofs - never fewer than two. Any failure ends that recovery sequence.

VERIFIED-OWNER RESPONSE If the consumer says a suspicious attempt was not theirs, the implicated memkey must be replaced while Mementom preserves or atomically rebalances its challenge-tag coverage.

5 / CONTINUOUS AUTHORIZATION

A live challenge gate around any consequential action

Login proves continuity, but it does not pre-authorize every future action. A product creates challenge tags for rights such as accept offer, restore subscription, change recovery settings, administer workspace, confirm booking, use admission, publish, license, pay out, or consent. Mementom makes a new current decision at the moment of consequence.

Example: accept one high-value offer

1. **Request.** The product backend sends an opaque request ID, tag, action, resource digest, visible offer summary, consequence, expiry, and approved return target.
2. **Show.** Mementom shows the exact $4,800 offer and settlement consequence before proof.
3. **Challenge.** Mementom randomly selects an eligible private assignment, displays its phrase, and asks for the matching managed image.
4. **Decide.** The service checks proof, live right, versions, epochs, risk, optional geofence, operation bindings, expiry, and one-use status.
5. **Enforce.** The vendor backend retrieves and decrypts the opaque result, verifies Mementom's signature and every binding, atomically consumes it, then performs the action.

The response is encrypted to the current challenge-tag public key and useful only to the vendor backend that holds its private key. It carries the vendor's pairwise subject, specific yes/no decision, action and resource bindings, versions, epochs, expiry, and one-use nonce - never a reusable binary login answer.

DYNAMIC PROOF The same action may request a different phrase-and-image relationship next time. Even the same memkey can be challenged again and receive no when the live right has changed.

6 / CHANGE MANAGEMENT

Memkeys change. Rights stay live.

Credential and product-right lifecycles are separate. The consumer controls replacement of held proof. The vendor can grant or remove a right for its pairwise subject without knowing which memkeys cover it. Mementom changes private assignments and returns current decisions without reissuing application credentials or rebuilding a product.

Change	Live effect
Grant or remove right	The next challenge uses the new entitlement version; no cache preserves the old answer.
Force challenge	A challenge epoch advances so affected sessions must prove again at the next gate.
Voluntary rotation	A different active memkey authorizes replacement; private coverage follows atomically.
Compromise replacement	The suspect memkey retires while affected tag coverage is preserved or rebalanced.
Tag-key rotation	New decisions use the current key version under fixed in-flight overlap rules.
Disconnect product	The vendor-local subject ends without deleting the consumer's private account.

No operator impersonation

A vendor operator can change a business right but cannot see a phrase, select or reset a memkey, or manufacture consumer proof. Mementom verifies replacement with a different active memkey and the recovery contract, activates the new pair, retires the old one, advances versions, and invalidates incompatible challenges.

Changes take effect now

Rights, connections, response keys, memkeys, and forced-challenge epochs are checked again at challenge and result consumption. A state change can invalidate an earlier decision before the vendor action executes.

7 / ADAPTIVE PROTECTION

Network context informs policy; it does not become identity

Mementom does not collect IP data during ordinary successful access or non-geofenced challenges. It permits IP handling in only two bounded cases: when a challenge tag explicitly enables geofencing, or after a failed initial account-access attempt. An IP address is never a memkey, identity, presence proof, or authorization factor.

Geofencing as a policy boundary

Zone	Policy response
Allowed	Continue only when a valid memkey, current right, and every other gate also pass.
Step-up	Require a different memkey, additional round, or current stronger assurance.
Restricted	Permit low-risk access while hiding or blocking sensitive actions.
Denied	Return the tag-specific no decision without exposing which policy element failed.
Uncertain	Fail closed or step up under the challenge tag's explicit confidence policy.

For a geofenced challenge, raw IP may exist only in volatile processing. The durable decision contains a coarse policy result, policy version, observation time, confidence class, and nonreversible context digest - not raw IP or precise location. When geofencing is off, no geolocation, ASN, proxy classification, pseudonymization, analytics, trace, or access-log copy is created.

FAILED-LOGIN EXCEPTION After failed initial access, Mementom keeps the trusted exact source IP in a restricted, short-lived timed-block record. The block has bounded escalation and deletion - never a permanent denylist or shared identity.

8 / ABNORMAL-USE RESPONSE

Slow the attack without locking out the owner

Knowing an Account Key, finding searchable image metadata, grouping photos in an obviously named Mementom album, or stealing a phrase sheet must not grant access. Those clues may help an attacker assemble an image or phrase inventory, so the online protocol limits how quickly that inventory can be tested and never reveals the correct correlation.

Observed event	Mementom response
Unknown image	Return a neutral no. Do not confirm an account, flag a memkey, or collect IP unless this is failed initial access.
Strong image + wrong phrase	Flag the identified memkey, record the incident, start bounded account attempt timing, and create a short IP block for failed login.
Further public attempt	Ask for an image first, pace the global account, and prefer memkeys not yet attempted.
Correct flagged pair	Open provisional recovery only; require the contract's additional distinct full proofs.
Verified compromise	Require atomic replacement and preserve or rebalance the affected challenge-tag coverage.

Recovery is sequential and reserved

After the first correct pair, Mementom reserves the recovery sequence to a signed recovery-session handle so unrelated public attempts cannot continually push the real owner behind the attacker's timing. Every required match must succeed consecutively with a distinct complete pair. Incident review appears only after verified recovery and asks whether each suspicious attempt belonged to the consumer.

The system reports no phrase, image hint, memkey identity, remaining attempt count, account existence, or inventory detail to an unauthenticated presenter. A risk flag and a credential lifecycle lock are separate states: the legitimate consumer retains a controlled proof and recovery path.

9 / SECURITY AND PRIVACY

Protect the relationship, including from the endpoint

Mementom reduces identity exposure, but it does not pretend that an unlocked, fully compromised device is safe. A local administrator, malware, accessibility controller, or AI agent with broad file and screen access may enumerate images and phrase material or operate the browser as the consumer. The architecture narrows opportunity and contains misuse; it cannot guarantee secrecy after endpoint compromise.

Control area	Production expectation
Photo handling	Process locally, request one image at a time, upload no originals, release previews promptly, and use neutral random managed filenames.
Phrase handling	Exclude phrase fields from password managers, clipboard convenience, logs, storage, analytics, and product surfaces.
Account Key custody	Offer an origin-scoped password-manager or encrypted-vault secret, with explicit consumer verification and a physical fallback.
Decision security	Use TLS plus tag-specific response encryption, Mementom signatures, exact operation bindings, short expiry, and atomic one-use consumption.
Automation resistance	Use one-attempt challenges, account timing, failed-login IP blocks, replay protection, risk flags, forced challenges, and guarded recovery.
Endpoint hardening	Limit AI-agent file permissions and Full Disk Access; optionally bind high-assurance flows to an isolated device key or passkey.

Assurance should be stated precisely

Manual photo-and-phrase proof should not be called automatically phishing-resistant. NIST reserves that assurance for cryptographic methods that prevent useful authenticator output from reaching an impostor verifier. High-assurance deployments can bind Mementom to a protected channel, passkey, or hardware-backed device key.

Tolerant image matching expands attack surface and remains off by default in public deployment until representative physical and digital transfer corpora pass false-accept, false-reject, collision, transplant, spoofing, and adversarial evaluation.

Mementom has no identity to surrender

Mementom cannot directly reveal a civil identity it never collects. If compelled or breached, it can expose only the anonymous account, pairwise relationships, and limited records it retains. This is a strong non-possession boundary, not universal unlinkability: payment, vendor, device, network, surveillance, or timing evidence may let an outside party correlate a relationship with a known person.

10 / PARTNER ADOPTION

Private permission for products and C2B2C exchange

Mementom gives apps, software, services, websites, and marketplaces returning-consumer continuity and fresh authority without another identity profile. The hosted ceremony remains separate from backend enforcement, so a modified browser cannot turn a visual success state into permission. Consumers remain unidentified; participating companies remain qualified, contract-bound, and accountable.

Product surface	Illustrative challenge gate
Marketplace	Accept one exact offer, release settlement, publish a listing, or authorize payout.
Consumer app	Restore a paid subscription, connect a device, or change recovery settings.
Website	Return to a private relationship or approve a consequential account change.
Software / SaaS	Administer a workspace, export data, change policy, or authorize an AI-agent action.
Online service	Confirm one booking, transfer, cancellation, or resource change.
Event network	Consume one admission without turning a temporary ticket into a permanent identity account.
C2B2C data marketplace	Offer one named insight to one buyer for a visible purpose, period, price, and returned value.

C2B2C changes who directs the data economy

The problem is not data brokerage as a category. The problem is invisible identity extraction. In C2B2C, the consumer chooses what data, insight, or intent to offer, the buyer and purpose, the permitted use period, the consequence, and the value returned. A qualified broker such as nCent may match, price, deliver, account for, and settle that exchange. nCent brokers data and value; Mementom privately clears permission.

PROHIBITED ENRICHMENT No broker or buyer receives a key into the global Mementom account. Pairwise subjects cannot be joined across companies, and Mementom's authorization graph and challenge history cannot become identity-enrichment products.

Small integration, firm enforcement boundary

A product registers its vendor and applications, approved return targets, challenge tags, assurance policies, webhooks, and response-encryption public keys. Its backend creates signed connection and challenge requests. The hosted Mementom ceremony collects private proof. The server SDK retrieves the opaque

result, decrypts it with the product's private key, verifies signature, tag, subject, action, resource, versions, epochs, expiry, and nonce, then consumes it atomically before executing.

Evidence before scale

Near-term proof should validate managed-image usability across devices and transfer paths, password-manager Account Key custody, pairwise isolation, key rotation, rights invalidation, one-use consumption, guarded recovery, failed-access pacing, geofence privacy, and false-accept or denial-of-service resistance. Vendor qualification should be risk-tiered: automated baseline checks for ordinary products, enhanced diligence for sensitive uses, and prohibition of covert surveillance, discriminatory enforcement, identity enrichment, or other abusive integrations.

Accountability belongs to the company

Mementom can leave consumer identity out of permission while requiring every participating company to be known and responsible. Qualification verifies the legal operator, approved products and destinations, declared purpose, data handling, complaint path, incident response, and accountable contact. The burden rises with risk instead of imposing one expensive process on every integration.

Qualification tier	Company obligation
Baseline product	Verify the legal operator, domain and app control, security contact, public terms, and prohibited-use acceptance.
Sensitive challenge	Add enhanced diligence, least-authority review, human appeal, auditability, and tested incident response.
C2B2C broker or buyer	Bind the exact offer, purpose, use period, value returned, downstream handling, revocation effect, and no-enrichment promise.
Excluded use	Reject covert surveillance, stalking, discriminatory enforcement, unlawful or illicit trade, cross-vendor linkage, and identity enrichment.

ACCOUNTABILITY BOUNDARY The consumer is anonymous to Mementom. The participating company is not.

11 / INTELLECTUAL PROPERTY

A layered protection strategy

Mementom is patent pending. The filing strategy is intended to protect the broad system rather than one screen or implementation detail: private consumer recognition, pairwise vendor relationships, multiple consumer-held memkeys, managed-image recognition, private challenge-tag assignment, dynamic challenge choreography, encrypted action-scoped decisions, guarded recovery, adaptive policy, abnormal-use controls, and replaceable lifecycle management.

Broad provisional posture

A useful provisional record describes the current implementation and practical alternatives, including media types, managed representations, locators, matching methods, proof directions, pairwise subjects, challenge-tag and key versions, recovery contracts, rights, epochs, deployment models, and enforcement paths. Necessary drawings, sequences, state transitions, and failures should support the system as a whole. The USPTO states that a provisional must contain a written description satisfying 35 U.S.C. 112(a) and that a corresponding nonprovisional generally must be filed within the provisional's 12-month pendency to preserve the benefit of that filing date.

Protection beyond patents

Layer	Commercial purpose
Patent	Protect novel systems, workflows, matching controls, challenge protocols, and action-scoped authorization.
Trademark	Protect the Mementom name and the photo-phrase key mark for the relevant goods and services.
Copyright	Protect original source code, documentation, diagrams, site copy, and artwork.
Trade secret	Protect tuning, fraud logic, operational methods, compatibility knowledge, and partner economics.
Contract	Define ownership, licensing, confidentiality, improvements, telemetry, security, and termination rights.
Domains	Maintain mementom.app and mementom.net as commercial destinations and renewal-controlled assets.

Public material should explain the value and operating model without publishing unnecessary enabling detail. Patent scope, inventorship, ownership, foreign strategy, trademark clearance, and filing deadlines remain matters for qualified counsel. The commercial goal is a licensable package that combines protected claims, working software, brand assets, integration patterns, and retained operational know-how.

12 / BRAND

Memory plus momentum

The brand translates a technical product into human terms. Memento supplies memory and personal meaning. Momentum supplies direction. The invented word Mementom holds both ideas in one name.

BRAND PROMISE Your memory holds the key to what's next.

The mark

The logo joins a minimal photo frame, the phrase beneath it, and a forward-facing key. The key continues from the frame so the negative space reads as one object: memory becoming authority. The photo content uses a mountain and sun rather than a person. The phrase blocks remain visible because the words are essential to the credential. The key has recognizable one-sided teeth and points forward.

Visual character

Deep ink communicates seriousness. Muted blue carries trust and movement. Warm white adds humanity. The lowercase wordmark is approachable rather than institutional. The system avoids faces, fingerprints, surveillance imagery, shields, and generic padlocks because the product is not built around identifying a person. It is built around proving a right.

Public language

The clearest explanation remains the simplest: a photo and a phrase open the door without asking who you are. After the term is introduced, each credential is a memkey. Mementom names the service, SDK, policy, Marketplace, and broader system. Technical language belongs behind the human proposition, where product teams can evaluate architecture and enforcement without losing the memory idea that makes Mementom memorable.

CONCLUSION

Recognition without identity; permission without extraction

Mementom changes the starting point for an internet relationship. Instead of sharing enough information to identify or globally correlate a person, it asks whether this is the same returning consumer for one product and whether that vendor-local subject holds this exact right now. The consumer keeps the memkeys. Mementom keeps their private assignments. The product receives only its pairwise relationship and a live, bound decision.

The same model can restore a subscription, protect account recovery, gate administration, approve an offer, confirm a booking, retrieve a movie ticket, consume admission, or authorize a consumer-directed nCent data exchange. Rights can change immediately. Memkeys can be replaced without severing vendor connections. Risk can trigger stronger proof and recovery without giving an attacker a permanent lockout lever.

MARKETPLACE PROPOSITION Anonymous customers. Accountable companies. Private permission. The internet should not have to know your life story to be useful to you.

Selected standards and public guidance

1. **NIST SP 800-63-4, Digital Identity Guidelines.** https://pages.nist.gov/800-63-4/
2. **NIST SP 800-63B-4, Authenticator and Verifier Requirements.** https://pages.nist.gov/800-63-4/sp800-63b/authenticators/
3. **NIST SP 800-63C-4, Federation and Assertions.** https://pages.nist.gov/800-63-4/sp800-63c/federation/
4. **NIST SP 800-207, Zero Trust Architecture.** https://csrc.nist.gov/pubs/sp/800/207/final
5. **OWASP Transaction Authorization Cheat Sheet.** https://cheatsheetseries.owasp.org/cheatsheets/Transaction_Authorization_Cheat_Sheet.html
6. **USPTO, Provisional Application for Patent.** https://www.uspto.gov/patents/basics/apply/provisional-application

This public paper describes Mementom's product model and intended architecture at a high level. Specific assurance, compliance, patent scope, and deployment obligations depend on the implementation and the relying service.