mementom

PUBLIC WHITE PAPER

Memory as a Key to Authority

An identity-independent system for authentication, account recovery, delegated rights, and protected actions

---

Your memory holds the key to what's next.

Patent pending | Public edition | July 2026

mementom.app | mementom.net

EXECUTIVE SUMMARY

Prove the right without making identity the key

Most authentication systems begin by collecting identity: a name, an email address, a phone number, a face, or an account tied to another provider. Mementom begins with a narrower question: does this holder possess the private credential assigned to this right?

A Mementom combines a specific user-held photo with a phrase created for that photo. The pair can open an account, restore an anonymous session, delegate limited access, or approve a protected operation. Neither element is sufficient alone. The right can be replaced without changing a permanent human trait, and one account can maintain several Mementoms for different levels of authority.

THE PROPOSITION A photo and a phrase open the door - without asking who you are.

Why this matters

The credential itself does not need to carry a biography. That creates a practical privacy advantage for pseudonymous services, shared households, care networks, partner portals, private recovery, and any workflow where the system needs to verify authority without turning identity data into the price of entry.

01	02	03
Memorable	**Scoped**	**Replaceable**
The holder chooses material with personal meaning.	Each Mementom is tied to a defined right or action.	Rights continue while credentials can change.

The commercial opening

Mementom can be offered as a hosted verification service, an integration SDK, a dedicated tenant, or an enterprise-controlled deployment. The platform value is not limited to login. It sits at the intersection of account recovery, continuous authorization, privacy-preserving access, delegated control, adaptive security, and human approval for consequential actions.

1 / THE CONCEPT

A credential 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	RIGHT
Something held	**Something recalled**	**Something permitted**
A particular source image kept under the holder's control.	A private phrase connected to the meaning of that image.	The account, resource, role, or action assigned to the pair.

The photo is not used to identify a face or subject. It is credential material. A landscape, a garden gate, a drawing, or another personally meaningful image can serve the purpose. The phrase is not a public caption or a conventional security question. It is the private connection between the holder and that specific image.

One account, several keys

A single master credential concentrates risk. Mementom is designed as a portfolio of rights. An account may use one Mementom for recovery, another for owner administration, another for a family member, and another for a particular transaction. The owner can distribute limited authority without distributing every privilege.

Property	Meaning
Identity-independent	The credential proves configured authority; it does not establish civil identity.
Two-part	The photo and phrase are verified as a matching pair.
Action-aware	A verifier may request a different Mementom for a different operation.
Lifecycle-controlled	Credentials can be activated, restricted, suspended, replaced, or revoked.
Policy-driven	Risk, geography, role, and transaction context can change the required proof.

2 / OPERATING MODEL

Roles describe authority, not biography

Mementom separates the person who controls policy from the credential that proves a right. A partner may know the people involved, or may know none of them. The authorization model remains the same because it is expressed through opaque accounts, defined roles, and scoped credentials.

Role	Responsibility
Rights owner	Creates policy and assigns, replaces, suspends, or revokes Mementoms.
Holder	Keeps the matching photo and phrase and responds to authorized challenges.
Delegate	Uses a Mementom limited by resource, duration, geography, or action.
Relying service	Requests proof for a specific account, resource, or operation and enforces the result.
Mementom verifier	Manages challenges, validates proofs, applies lifecycle state, and issues scoped results.
Security operator	Investigates abnormal use and contains affected sessions or credentials.

Separation of duties

For sensitive systems, no single administrator should be able to create a powerful credential, expand its authority, weaken its controls, and erase the evidence. Mementom policies can require distinct owner and operator approvals, preserve immutable lifecycle events, and keep ordinary recovery credentials separate from administrative keys.

DESIGN PRINCIPLE Possession of a shared recovery key should not automatically confer authority to delete data, transfer ownership, or rewrite security policy.

3 / ENROLLMENT

Creating a Mementom

Enrollment creates the relationship among a photo, its private phrase, and the right the pair will protect. The source photo remains with the holder in the recommended profile. The verifier retains only the protected material needed to recognize a later presentation.

1. **Open a protected enrollment session.** The service identifies the opaque account, resource, and authority allowed to create the credential.
2. **Choose a meaningful photo.** The holder selects a source image that can be retained and found again. The interface makes clear whether the deployment requires the exact original file.
3. **Create a private phrase.** The holder writes a phrase linked to the image's personal meaning rather than visible content or common biographical facts.
4. **Derive the enrollment record.** The client creates a non-reconstructive representation locally and withholds the source photo from the verifier.
5. **Assign rights and policy.** The owner defines whether the Mementom is for recovery, routine access, delegation, administration, or a protected action.
6. **Confirm and activate.** A fresh test proves that the holder can reproduce the pair before the credential becomes active.

A practical recovery set

An account can enroll several Mementoms. For example, one photo might be paired with the phrase "Sunrise beyond the blue ridge" and another with "Rain on the old garden gate." The images are visibly different, the phrases are not interchangeable, and either pair can be assigned a distinct role in the policy.

PRIVACY BOUNDARY The recommended architecture keeps source photos and raw phrases out of routine server storage and keeps risk telemetry separate from the credential core.

4 / LOGIN AND RECOVERY

Restoring access without restoring identity

Mementom can restore a pseudonymous account even when no email address, phone number, or external identity provider exists. The holder presents one enrolled photo. Once that photo is recognized, the system requests the phrase associated with it. A correct pair returns the pre-existing account rights rather than creating a new identity.

1. **Request access.** The service creates a fresh, expiring challenge for the account or resource.
2. **Present the source photo.** The client derives the comparison material locally and submits only the proof required by the verifier.
3. **Complete the phrase.** The holder supplies the phrase associated with that exact enrolled image.
4. **Apply policy.** The verifier checks freshness, credential status, rate limits, and the right requested.
5. **Return scoped authority.** Successful proof restores the existing account or opens a narrowly defined session.

Logging out changes the visible state

A clear logout matters in an identity-independent system. After the recovery keys are saved, logout removes the local bearer state and the project disappears from that browser. Recovery is therefore demonstrable: the matching photo and phrase do not merely pass a test; they return the same project and its rights.

CORE INVARIANT The photo alone does not open the account. The phrase alone does not open the account. Only the enrolled pair, accepted under a fresh challenge, restores the right.

5 / CONTINUOUS AUTHORIZATION

A key for the action, not only the door

Login begins a session. It should not grant permanent authority over every operation that follows. Mementom supports step-up challenges that are bound to the action being attempted, so the system can ask for stronger proof at the moment of consequence.

Example: removing a protected Space

1. **Attempt.** A holder tries to remove the Bedroom Space from a project.
2. **Describe.** The service identifies the action and target clearly: Remove Bedroom.
3. **Challenge.** The verifier presents the phrase "Sunrise beyond the blue ridge" and asks for the matching enrolled photo.
4. **Bind.** A successful response creates a short-lived approval limited to that action, project, and Space.
5. **Enforce.** The destructive endpoint checks and consumes that approval before committing the removal.

If the holder changes the target or action, the approval no longer applies. If the proof fails, the service can deny the operation without necessarily locking every other right. This keeps containment proportional and preserves ordinary access when policy allows.

TRANSACTION INTEGRITY The holder should see what is being approved. The proof should be fresh, short-lived, single-use, and bound to the material action.

6 / CHANGE MANAGEMENT

Rights can persist while credentials change

A permanent biometric cannot be reissued after disclosure. A Mementom can. Replacement creates a new credential version, proves the new pair, and then retires the old authority according to policy. The account, resource, and role do not need to change.

Lifecycle state	Effect
Pending	Created but not yet possession-tested or approved.
Active	Eligible to authorize within its assigned policy.
Restricted	Temporarily limited while lower-risk access may remain.
Suspended	Stopped reversibly during investigation or owner review.
Revoked	Permanently terminated.
Superseded	Replaced by a newer version and retained only for history.

Safe replacement

The owner authorizes the change with an existing administrative Mementom or an independent approval path. The replacement is enrolled as a new version, tested before cutover, and assigned an explicit activation policy. The prior version is then superseded or revoked, affected sessions are ended, and outstanding challenges are invalidated.

Delegation without credential sharing

When another person needs access, the safer pattern is to create a separate delegated Mementom instead of sharing an owner credential. The delegated right can carry its own expiration, geographic boundary, transaction ceiling, and revocation path. Ending the delegation does not disrupt the owner's credential.

7 / ADAPTIVE PROTECTION

Network context informs policy; it does not become identity

A verifier can observe an Internet Protocol address and derive limited security context such as network provider, hosting classification, country or broad region, reputation, and access velocity. Those signals can reveal anomalies, but they are not reliable proof of who is present. Mobile routing, corporate networks, shared addresses, VPNs, and inaccurate geolocation all limit certainty.

Geofencing as a policy boundary

Zone	Policy response
Allowed	Continue when the requested Mementom and other controls pass.
Step-up	Require a different Mementom, additional round, or owner approval.
Restricted	Permit low-risk access while hiding or blocking sensitive actions.
Denied	Refuse the request under owner, contractual, or legal policy.
Travel exception	Apply a time-limited owner-approved override without creating permanent trust.

Raw network addresses should be minimized, access-controlled, and retained only for a documented security purpose. Approximate region can support a decision, but location should not silently become a durable identity profile. This approach is consistent with zero-trust guidance that rejects network location as a sufficient basis for implicit trust.

TERMINOLOGY In this section, IP means Internet Protocol address. Intellectual-property protection is addressed separately.

8 / ABNORMAL-USE RESPONSE

Respond to the event without over-collecting the person

Abnormal use is evaluated through the combination of proof outcome and context. A new device, rapid geography change, repeated failures, unusual time, proxy infrastructure, or an unexpected destructive action can increase risk. None of these facts alone should be treated as a final determination.

Risk band	Illustrative response
Low	Allow the scoped session and continue ordinary monitoring.
Guarded	Request a fresh Mementom and shorten the session.
Elevated	Request a different Mementom and block sensitive actions pending proof.
High	Contain the session, suspend the implicated credential, and alert the owner.
Critical	Deny, revoke affected rights, preserve evidence, and begin incident response.

The response sequence

Contain the pending operation first. Challenge with an independent Mementom rather than repeating the suspected credential. Suspend the narrowest affected right that addresses the risk. Notify through a previously approved channel without disclosing the source image or phrase. Investigate the opaque account, session, network, policy, and transaction events. Restore only the necessary rights, rotate compromised credentials, and document the decision.

The system should avoid indiscriminate account-wide lockout when a credential-specific response is sufficient. This reduces denial-of-service risk and preserves a path for legitimate recovery.

9 / SECURITY AND PRIVACY

Explicit boundaries, standard controls

Mementom's value comes from reducing identity dependence, separating rights, requiring a matching pair, and making credentials replaceable. Those properties complement, rather than replace, established security engineering.

Control area	Production expectation
Transport	Authenticated encrypted channels for enrollment, challenge, and verification.
Freshness	A new nonce or challenge with a short expiry for every proof.
Replay control	Single-use, transaction-bound outputs that cannot authorize another session or action.
Verifier security	Protected secrets, tenant isolation, least privilege, rotation, and independent review.
Rate control	Credential, account, device, and network budgets designed to resist guessing and denial of service.
Audit	Tamper-evident lifecycle and decision records that exclude photos, phrases, and unnecessary network detail.

Assurance should be stated precisely

A manually entered photo-and-phrase flow should not be described as automatically phishing-resistant. NIST defines phishing resistance through cryptographic mechanisms that prevent useful authenticator outputs from being disclosed to an impostor verifier. Deployments that require recognized phishing resistance can bind Mementom to a verifier, protected channel, passkey, or hardware-backed device key.

Likewise, fuzzy photo matching introduces a useful tolerance but also an attack surface. Comparison should be rate-limited, short-lived, capability-controlled, and reviewed against false acceptance and false rejection. The public proposition remains simple; the production system must be disciplined.

10 / PARTNER ADOPTION

A platform for narrowly defined authority

Mementom is applicable wherever a system needs proof of a right and conventional identity collection is unnecessary, undesirable, incomplete, or too rigid. The first commercial deployments should be bounded enough to measure reliability and safe enough to preserve a fallback.

Market	Potential entry point
Privacy-first consumer services	Anonymous account recovery without email or phone dependency.
Households and care networks	Shared access with owner-only administrative keys.
Partner and operations portals	Step-up approval for exports, policy changes, and transfers.
Education and youth services	Rights-based access without unnecessary contact identifiers.
Physical and local access	Short-lived authority for a door, facility, device, or offline resource.
Autonomous systems	Human approval bound to an agent's consequential action and parameters.

Deployment paths

A hosted service can provide enrollment, challenge, policy, lifecycle, and assertion APIs. A dedicated tenant can isolate keys, telemetry, retention, and audit policy. An enterprise-controlled option can place verifier components inside the partner's environment. Each model preserves the same product contract: source media remains under holder control, rights remain explicit, and results are scoped to the relying party's action.

Evidence before scale

The near-term proof plan is straightforward: validate exact-photo usability across common devices and transport paths; test enrollment and recovery completion; commission protocol and application-security review; measure false rejection and support burden; and run a design-partner pilot around one protected workflow. Expansion should follow evidence, not precede it.

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 one implementation detail: enrollment of multiple user-held memory keys, privacy-preserving recognition, challenge choreography, action-scoped authority, recovery and administrative roles, adaptive policy, abnormal-use controls, and replaceable lifecycle management.

Broad provisional posture

A useful provisional record describes the current implementation and practical alternatives, including different media types, representations, matching methods, proof directions, key classes, challenge depths, deployment models, and action policies. Necessary drawings, sequence diagrams, state transitions, and failure paths 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. Technical language belongs behind that proposition, where partners can evaluate architecture, policy, and deployment fit without losing the human idea that makes Mementom memorable.

CONCLUSION

A narrower proof with broader possibilities

Mementom changes the starting point for authentication. Instead of collecting enough information to identify a person, it asks whether the holder possesses the private key assigned to a particular right. That key is memorable, divisible across roles, replaceable over time, and available again when an anonymous account must be restored.

The same model can protect a login, a recovery path, a delegated resource, a destructive operation, or a transaction. Context can increase the required proof without becoming identity. Abnormal use can be contained without exposing the photo or phrase. Owners can change credentials without changing themselves.

PARTNER PROPOSITION Give people a credential they can remember, owners a right they can change, and services a proof they can verify.

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 800-207, Zero Trust Architecture.** https://csrc.nist.gov/pubs/sp/800/207/final
4. **OWASP Authentication Cheat Sheet.** https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html
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.