

Taking the laptop shouldn't mean taking the keys.



monban

One authentication. From power-on to work.

A guardian crest for Monban: two defensive walls flank an angular M and protected opening. A separate diamond represents the user-held cryptographic contribution outside the laptop.

Distinctive, compact, and reproducible in a single colour. The mark connects the identity to the product's threat model: device possession should not be enough to recover the disk key.

Identity proposal v0.2 - 5 October 2026. Monban is in development. This guide describes intended behavior, not a shipping guarantee or certification.

Four reasons for Monban.

01 / PHYSICAL ACCESS

Even TPM + PIN depends on the TPM.

TPM + PIN adds protection, but vulnerable TPM implementations can permit secret extraction and bypass hardware anti-hammering, leaving a PIN to offline guessing. Monban's goal is an external cryptographic dependency that stays with the user.

02 / LESS FRICTION

One authentication. From power-on to work.

Unify pre-boot authentication, Windows sign-in, and network access through a secure handoff. Strong authentication need not mean two separate login ceremonies.

03 / CLOUD INDEPENDENCE

Passkeys for AD. Without Entra.

Target native passkey Windows sign-in and on-premises AD authentication without a cloud identity provider. Local domain controllers remain the authentication authority.

04 / EXISTING AVAILABILITY

Your DCs authenticate. Your HA carries on.

Run authentication on existing domain controllers, with their replication and redundancy. No separate Monban appliance or vendor-hosted service is intended in the online login path.

Security claims that hold up.

BITLOCKER TPM + PIN

The important distinction is the protection of key material, not a claim that AES is broken. BitLocker does not simply leave an unprotected plaintext disk key in the TPM. In the implementation studied by faultTPM, a PIN-derived encryption layer remains after TPM state compromise, but hardware rate limits can be bypassed and PIN guesses tested offline. A strong enhanced PIN can retain substantial protection.

FIPS 140-2 LEVEL 2

Level 2 adds tamper evidence. That rating alone does not guarantee resistance to invasive key extraction; higher physical-security levels add stronger protection. Do not claim "no physical protection at all" or that "most TPMs" have a particular rating without model-specific evidence. Overall certification level, physical-security rating, and other evaluations must be distinguished.

THE EXTERNAL-SECRET COMMITMENT

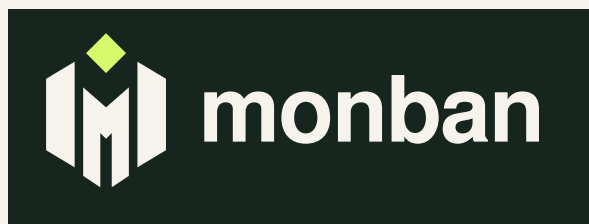
TPM compromise is explicitly in Monban's target threat model. Modes advertised as resisting TPM extraction must require cryptographic material from a separate authenticator, such as supported PRF-based derivation. TPM-policy-only token gating does not provide the same property. Recovery protectors must preserve the intended security boundary.

SCOPE & AVAILABILITY

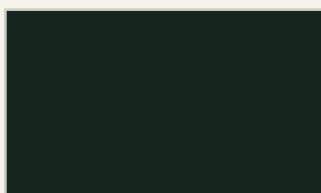
Focus on properly configured, powered-off or supported hibernated devices. An already-unlocked running system and in-memory disk keys have different risks. The intended DC-based login path adds no separate central vendor dependency, but still depends on AD, DNS, networks, and deployed Monban components. Cached/offline and revocation behavior need explicit supported-mode documentation.

No absolute attack-proof claims, NCSC/NIST endorsement, or production-readiness claims. These are design commitments pending product validation.

The identity system.

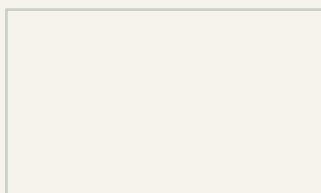


Mark: guardian walls, protected M/gateway, separate key diamond. Use the mark alone for favicons and constrained spaces. Use the complete horizontal lockup for the primary product signature.



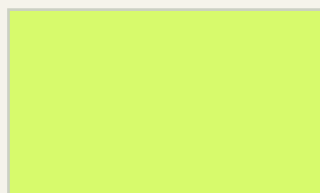
Ink

#17251F



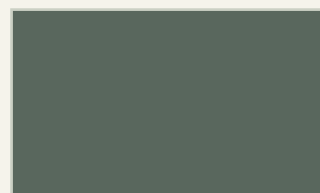
Ivory

#F5F3EB



Lime

#D7FA6C



Muted

#59675D

Nimbus Sans: regular display headlines and body; bold wordmark and emphasis. Nimbus Mono PS: component identifiers and short technical labels. Self-hosted font files and licence are included. SVG wordmarks are outlined; this PDF uses embedded DejaVu as a document substitute.

Ink and ivory are the foundation; lime highlights key actions and the separate-key diamond. Use ink text on lime. Use a monochrome logo where colour contrast or reproduction quality is limited.

Clear space: at least one quarter of the mark's height on every side. Recommended minimums: 28 px high for the full crest and 140 px wide for the lockup. At smaller sizes, use the simplified favicon. Do not stretch, rotate, add effects, or alter the geometry.

Screen RGB: ink 23/37/31; ivory 245/243/235; lime 215/250/108; muted 89/103/93. Print CMYK approximations: 38/0/16/85; 0/1/4/4; 14/0/57/2; 14/0/10/60. Proof colour with your printer.

Ready-to-use words.

ELEVATOR PITCH

Monban is building passkey security for Windows and on-premises Active Directory. Its goal is to protect a lost laptop even when an attacker can compromise its TPM, by retaining a cryptographic dependency on a separate user-held authenticator. One pre-boot authentication carries users into Windows and network access. Domain controllers do the authentication, using existing AD redundancy, without Entra or a separate vendor appliance in the login path.

SHORT DESCRIPTION

Monban is a security suite in development for passkey-controlled disk unlock, Windows sign-in, and on-premises AD authentication. It combines a physical-access threat model with one authentication experience and a DC-based architecture.

HEADLINE & SUPPORT

One authentication. From power-on to work.

Taking the laptop shouldn't mean taking the keys.

VOICE & CALL TO ACTION

Calm, direct, technically precise. State the threat and the architectural response. Use "building", "goal", and "designed to" while product validation is pending.

CTA: Register interest.

Supporting copy: Product updates and early-access news.

Registration does not guarantee an early-access place.

Company legal details, privacy contact, press contact, launch date, and supported configurations remain to be confirmed before public launch.

The suite & source notes.

Pre-boot

`monbase-preboot`

Rust UEFI application: slot/TPM/FIDO logic and pre-boot provisioning helpers.

Login

`monbase-login`

Rust Windows provider, broker/service, enrollment, pre-boot handoff consumer, supported authentication integration.

Enterprise

`monbase-enterprise`

Rust AD/DC issuer and integration, enrollment, replication and revocation behavior.

Proposed public labels: Monban Pre-boot, Monban Login, Monban Enterprise. Preserve the exact `monbase-*` identifiers in technical material.

SOURCES / REVIEWED 5 OCTOBER 2026

NCSC: Windows guidance - TPM + PIN recommendation

NIST SP 800-111, section 4.2 - multi-factor enterprise authentication

NIST FIPS 140-2, sections 1.2 and 4.5 - physical security levels

faultPM, sections V-C and V-D - BitLocker TPM + PIN analysis

Microsoft: FIDO2 Windows sign-in - unsupported on-premises-only AD

Microsoft: BitLocker countermeasures - physical-access threat classes

Source labels are clickable. These sources establish context, not Monban certification or endorsement. Microsoft, Windows, and Active Directory are integration targets.