Secure Split Key (SSK)

No single key. No single point of compromise.

NewCore's patent-pending approach to cryptographic signing authority. The key that signs your workforce's access into every SAML and OIDC application is split between NewCore and your environment, so neither side can sign alone.

HOW SSK WORKS

One signature, two parties.

- **Split cryptographic signing key.** The private key that authorizes every authentication token is split in two. NewCore holds one half, your organization holds the other, and NewCore never sees your half.
- **The customer share stays in your environment.** Delivered through a managed browser extension, MDM, or the NewCore mobile app. Every sign-in requires your share to complete, so tokens cannot be forged from outside your environment.
- **Nothing changes for users or downstream apps.** Every connected application receives a standard, spec-compliant SAML assertion or OIDC token. The only application-side change is pointing it at the SSK metadata or issuer.

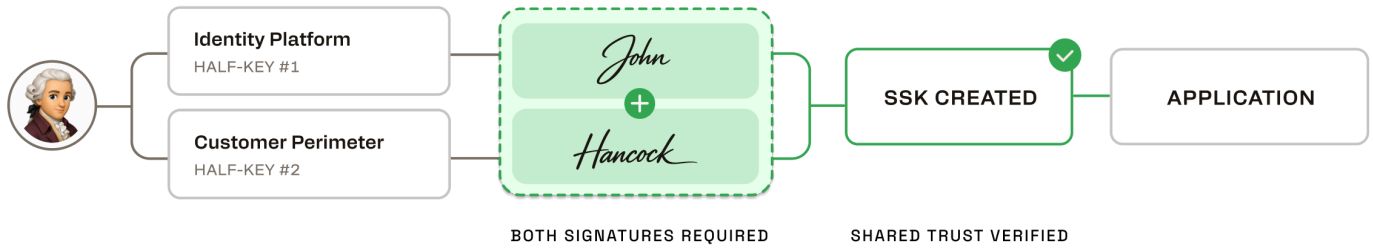
KEY BENEFITS

- **Stolen credentials stop short.**
  Even with a username, password, and OTP, an attacker cannot complete a sign-in without the customer share on an enrolled device.
- **Vendor breach, contained.**
  A compromise of NewCore exposes one share, which cannot forge a token any application will accept. Your share never reaches our servers.
- **Low operational lift.**
  One key ceremony per tenant, one extension deployment, then a toggle per application.

BEFORE AND AFTER

LEGACY One vendor signs every token

WITH SSK Signing requires both halves



See SSK in a 30-minute demo.

NewCore is the next-gen IdP for humans and AI agents, built from the ground up to address the architectural failures legacy IdPs cannot fix.

Request a Demo →