SOLUTION BRIEF

RSA My Page | ID Verification and Secure Enrollment

Identity assurance at enrollment, at recovery, and at every sensitive workflow

Credentials can be stolen. Identities can be faked. An attacker who convinces your help desk they're a legitimate employee—or who slips through onboarding under a false identity—can operate inside your environment for months before detection. ID verification closes that gap by confirming not just that someone has the right credentials, but that they are the person entitled to have them.

Where ID verification matters most

ID verification is most critical at high-risk points in the identity lifecycle—when a new user is being onboarded, or when an existing user needs to recover access. These are the moments attackers target.

- **Credential enrollment**: New users verify their identity digitally—using biometrics, a government-issued ID, or other verification methods—before birthright credentials are issued. Remote workers can complete the process without appearing in person.
- **Credential recovery**: When a user needs to reset or recover credentials, RSA My Page requires proof of identity before access is restored. This stops the social engineering technique used in attacks like the ALPHV ransomware campaigns, where attackers called help desks claiming to have forgotten passwords.

How RSA ID verification works

RSA My Page integrates ID Dataweb's verification workflows through RSA's OpenID Connect (OIDC) connector. Administrators configure and deploy ID verification workflows without custom coding. The process begins with an initial authentication step, followed by the ID Dataweb verification workflow. Each interaction is logged for audit and compliance reporting. Available verification templates through ID Dataweb:

- **MobileMatch**: Verifies identity through phone possession, ownership, and credit bureau data.
- **BioGovID**: Employs a live selfie and government ID match for high-assurance verification.
- **DynamicKBA**: Confirms identity using dynamic knowledge-based questions.

Extended coverage: verifying users without a registered authenticator

ID verification is also available through RSA Help Desk Live Verify, extending the same identity proofing to contractors, partners, temporary employees and users without a registered authenticator through government-issued identification. These users have historically represented a gap in verification coverage.

The RSA Help Desk Live Verify workflow confirms both the user's and the agent's identities without either side sharing a PIN, password, or personal detail. Administrators configure which user populations are routed to authenticator-based verification versus ID Verification through the same RSA ID Plus policy framework.

Built for the organizations with the most to lose

RSA ID Verification is designed for organizations where identity assurance is not optional:

Financial institutions where fraudulent insider access and help desk social engineering directly translate to financial loss.

Government agencies with strict identity requirements at access boundaries that extend to contractors and partners.

High-assurance organizations where onboarding an imposter—or allowing an attacker to recover someone else's credentials—represents an unacceptable risk.

Beyond enrollment: any sensitive workflow

The same verification engine that secures credential enrollment and recovery can protect any workflow where identity assurance is required before a sensitive action is taken:

- Wire transfer authorization and high-value transaction approval in financial services.
- Privilege escalation requests and VPN recovery.
- HR actions involving sensitive employee data.
- Access request approvals at identity boundaries that extend to contractors and partners.

Built for regulated, high-assurance environments

RSA ID verification is designed for organizations where identity assurance requirements are not optional:

- Financial institutions where fraudulent insider access and help desk social engineering directly translate to financial loss.
- Government agencies with strict identity requirements at access boundaries that extend to contractors and partners.
- High-assurance organizations where onboarding an imposter—or allowing an attacker to recover someone else's credentials—represents an unacceptable risk.

Powered by ID Dataweb

RSA's ID verification capability is powered by ID Dataweb, a leading provider of real-time identity verification, fraud prevention, and risk management. The integration embeds ID Dataweb's verification workflows into RSA My Page and RSA Help Desk Live Verify with no custom coding required, available to all RSA ID Plus E2 and E3 subscribers.

Get started

Contact us to learn more about ID verification and secure enrollment with RSA ID Plus.

About RSA

RSA is the identity standard for government agencies, finance, and high assurance organizations. RSA provides the identity intelligence, authentication, access, governance, and lifecycle capabilities needed to prevent threats, secure access, maintain operations, and surpass compliance. More than 9,000 security-first organizations trust RSA to manage more than 60 million identities across on-premises, hybrid, and multi-cloud environments. For additional information, visit our website to **contact sales**, **find a partner**, or **learn more** about RSA.

About ID Dataweb

ID Dataweb™ helps enterprises stay ahead of identity fraud and account-related threats with real-time detection and mitigation while maintaining a seamless experience for their workforce, third parties, and customers. The ID Dataweb SaaS platform combines adaptive identity verification methods, behavioral analytics, device and credential intelligence, and risk scoring. Backed by AI and expert insights, these capabilities proactively stop identity-based attacks, protect revenue, and strengthen compliance. Unlike static legacy identity tools, ID Dataweb delivers dynamic, multi-layered risk orchestration that adapts to evolving threats. Its low-code, cloud-native services deploy quickly, integrate seamlessly with existing IAM systems, and align with each customer's policies. For more information, please visit **www.iddataweb.com**.