syncsort

PRODUCT SHEET

# Cilasoft Reinforced Authentication Manager for i (RAMi)

## Strengthen Password Security with Multi-Factor Authentication

As stories of data breaches caused by exploited credentials continue to make headlines, it is clear that basic password protection mechanisms are no longer good enough. Organizations require an additional layer of protection that is also easy to use and doesn't impose an additional burden on administrators.

Multi-factor authentication, also referred to as two-factor authentication, has become a popular method for strengthening security since it requires a user to authenticate in two ways prior to accessing a system, an application or its data. These factors can include something they **know** (user id, password, PIN), something they **have** (email account, smart phone, token device) or something they **are** (finger print, iris scan).

Syncsort's Cilasoft Reinforced Authentication Manager for i, or RAMi, improves the security of your IBM i system and core business applications with multi-factor authentication, self-service password control, and support for the "four eyes principle" of supervised changes to sensitive data. With RAMi, you can:

- Add an authentication layer beyond memorized or written passwords
- Meet audit and regulatory requirements and recommendations in PCI DSS 3.2, HIPAA, Swift Alliance Access and other regulations
- Invoke rules-based multi-factor authentication only for users or specific situations that require it
- Lower the risk of unauthorized access to systems, applications and data
- Reduce the risk of data theft and its costs and consequences
- Audit multi-factor authentication failures from an existing SIEM server

**Passwords alone are weak. The frequency of breaches due to stolen or guessed passwords and brute-force attacks requires an additional layer of user authentication security.**

## Powerful, Flexible Multi-Factor Authentication

RAMi provides peace of mind by ensuring only authorized individuals obtain access to your systems and sensitive data, and delivers the flexibility to meet the needs of your environment and business. RAMi enables you to integrate multi-factor authentication into the IBM i 5250 signon screen, or invoke the process on demand.

When integrated with the signon screen, you can choose between single-step or two-step authentication. Single-step authentication requires both the user's password and a token for authentication. The user is not told which one failed if either is incorrect, delivering true multi-factor authentication. With the two-step process, a token screen is presented after the IBM i signon.

RAMi's rules engine makes it easy to configure the solution to invoke multi-factor authentication screens only for the users or specific situations that require it. Several pre-defined rules are provided to help you get started quickly. Rules criteria are available to specify which users should authenticate through RAMi based on whether they:

- are registered or unregistered
- are limited capability users
- are a member of specific group profiles
- possess special authorities
- are using a specific device
- are authenticating from a specific subsystem or iASP
- have a particular IP address
- are authenticating at a certain date or time.

If RAMi is invoked on demand, either manually or in a program, the calling program can also be specified as a criterion.

With RAMi, you also have a choice of authentication methods:

- **Cilasoft** - RAMi transmits a token by email and/or popup using Cilasoft technology. This method is recommended for less demanding environments that require no additional cost or effort.
- **RADIUS** – RAMi contains a RADIUS client that runs natively on IBM i for organizations that wish to use an existing RADIUS-based authenticator or build their own RADIUS server.
- **RSA** – RAMi is certified by RSA as compliant with SecureID® to serve the most demanding environments through integration with RSA RADIUS servers and RSA RADIUS cloud services. RSA cloud services support biometrics, such as a finger print or facial image from a mobile phone, in addition to traditional voice mail token, SMS token, and push approval methods.

Authentication failures through RAMi can be audited using your existing SIEM server.

## Self-Service User Re-enablement and Password Changes

RAMi's on-demand authentication capabilities can also be used to grant users the ability to re-enable their profiles or change their passwords if forgotten. If configured, users can answer pre-configured security questions and/or receive a single-use token via pop-up, email or RSA SecurID device before performing changes to their profiles.

## Four Eyes Principle for Supervised Changes to Sensitive Data

For operations that could have significant impact on the server, or for data changes that are so sensitive they must be supervised by a second pair of eyes, RAMi can be used to enforce a four eyes policy. When a user wishes to perform such a change or operation, a designated administrator receives an email with a single-use token along with information on the identity of the user making the request and the job number. The administrator can then enter the single-use token into the user's screen and observe the change while it is made.

## Supported Platforms

- IBM i OS versions 6.1 to 7.3
- All hardware platforms that support those operating system versions

## RSA Certification

Visit https://community.rsa.com/docs/DOC-92160 to view the RSA SecurID Access Implementation Guide for RAMi.