Multi-Factor Authentication (MFA)

Improve workflows, reduce operating costs, and deploy new services faster with automation

MULTI-FACTOR AUTHENTICATION INTRODUCTION

Multi-factor authentication serves a vital function within any organization -securing access to corporate networks, protecting the identities of users, and ensuring that a user is who he claims to be.

Evolving business needs around cloud applications and mobile devices, combined with rising threats, and the need to reduce costs, require entirely new considerations for access control.

THE NEED FOR MULTI-FACTOR AUTHENTICATION

New threats, risks, and vulnerabilities as well as evolving business requirements underscore to the need for a strong authentication approach based on simple service delivery, choice, and future-forward scalability.

TODAY, ORGANIZATIONS ARE ASKING:

- Can I address new demands of my business - like cloud and mobile devices?
- How do I map access control methods to business risk and the needs of my users?
- Can I centrally manage, control and administer all my users and endpoints?
- Who controls my user data?
- How can I incorporate additional security layers to help me further fortify against threats?
- And how do I keep it all practical and cost-effective?

More than ever, customers are looking for identity and access management solutions that deliver simplicity, automation, reduced TCO and choice.

TODAY, ORGANIZATIONS ARE ASKING:

Multi-factor authentication ensures that a user is who they claim to be. The more factors used to determine a person's identity, the greater the trust of authenticity.

THALES

For all the benefits of this product and more visit RjRinnovations.com

RJR innovations™
609 - 1420 Blair Towers Place, Ottawa, ON Canada K1J
800-232-8457 info@rjrinnovations.com

MFA CAN BE ACHIEVED USING A COMBINATION OF THE FOLLOWING FACTORS:

- Something You Know – password or PIN
- Something You Have – token or smart card (two-factor authentication)
- Something You Are – biometrics, such as a ngerprint (three-factor authentication)

Because multi-factor authentication security requires multiple means of identi cation at login, it is widely recognized as the most secure method for authenticating access to data and applications.

SAFENET MFA PRODUCTS:

Authentication as a Service (AaaS)

More and more businesses embrace the bene ts that derive from managing their data and applications in the cloud. As users access sensitive assets from a greater variety of devices and locations, organizations become vulnerable to new threats. AaaS enables organizations to easily apply strong authentication onto multiple access points.

SafeNet AaaS Products:

- SafeNet Authentication Service (SAS): Delivers AaaS with exible token options, enabling a quick cloud migration and protecting data from any source – from cloud-based and on-premise applications to networks, users, and devices.

Authentication Management

SafeNet offers the most comprehensive identity access and management systems to administer, monitor, and manage strong authentication deployments across the organization.

SafeNet Management Platforms:

- SafeNet Authentication Manager: A comprehensive server for securing local and remote access to numerous corporate resources using a single authentication back end.
- SafeNet Authentication Manager Express: A one-time password (OTP) solution that enables secure remote access to online resources.
- MyID Card Management System: A Web-based management solution used to issue, manage, and support SafeNet smart cards and USB tokens.

Authenticators – Tokens, Smart Cards & Other Form Factors

Offering the broadest range of methods and form factors, SafeNet allows customers to address numerous use cases, assurance levels, and threat vectors with unified, centrally managed policies-managed from one authentication back end delivered in the cloud or on premise.

SafeNet Authenticators:

OTP Authenticators: Generate dynamic one-time passwords (OTPs) for properly authenticating users to critical applications and data, whether on a token, mobile device, or grid-based authentication.

For all the benefits of this product and more visit RjRinnovations.com

609 - 1420 Blair Towers Place, Ottawa, ON Canada K1J
800-232-8457 info@rjrinnovations.com

Certificate-Based USB Tokens:
Provide secure remote access as well as other advanced applications, including digital signing, password management, network logon, and combined physical/logical access.

Certificate-Based Smart Cards:
Strong multi-factor authentication in traditional credit card form factors that enable organizations to address their PKI security and access control needs.

Hybrid Tokens:
Authenticators that combine one-time password, encrypted ash memory or certi cate-based technology on the same strong authentication device.

Mobile Phone- and Software-Based Authentication:
Save on hardware and deployment costs, while users bene t by not having to carry an additional hardware token around with them.

SECURITY APPLICATIONS

SafeNet's security applications consist of middleware and password management software that enable users to securely store and manage user credentials.

SafeNet Authentication Client:
A middleware client that manages SafeNet's extensive portfolio of certi cate-based smart cards, USB tokens, and software-based devices.

eToken Network Logon:
A token-based solution for securing your employees' PCs and preventing unauthorized access to your corporate network.

THALES

We provide innovative, customized business process consulting, software implementation services and Level 1 bilingual support for multiple ITSM and DEM solutions and add-ons. We understand that in today's day and age, technology leaders are focused on transforming how IT operates. Digital transformation and automation are key elements in ensuring that most organizations keep up with how fast-paced both technology and information are consumed and delivered – at work and at home; on premise and in the cloud.

RJR innovations
609 - 1420 Blair Towers Place, Ottawa, ON Canada K1J
800-232-8457 info@rjrinnovations.com