The Three Rules for Protecting Enterprise Identities

An Introduction to SafeNet’s Next-Generation Authentication Solutions
Contents

I. The New IAM Trinity – and the Need to Secure Elastic Enterprise Boundaries ..........3
  The Old IAM Trinity vs. the New IAM Trinity ..........................................................3
  Enterprise Agility and the New IAM Trinity ..........................................................5
  Information Security and the New IAM Trinity ......................................................6
II. Bridging the Authentication Gap – Three Rules for Selecting a Future-ready Solution .7
  Rule 1 – Select for Control and Integrity.................................................................8
  Rule 2 – Seek Smooth Management.......................................................................9
  Rule 3 – Ensure the Ability to Adapt .....................................................................10
  Assessing your Organization's Needs .....................................................................11
III. Next-Generation Authentication from SafeNet ....................................................12
  i. Frictionless Authentication ................................................................................13
     Frictionless Management....................................................................................13
        Automated Lifecycle Administration ..............................................................13
        Management by Exception ..............................................................................13
        Extensive User Self-Service ..........................................................................14
     Frictionless Authentication ................................................................................15
        Native Identity Federation .............................................................................15
        Choice of Delivery Platforms ........................................................................15
        Choice of Authentication methods .............................................................17
        Broad Use Case and Ecosystem Support ........................................................17
  ii. Trust ..................................................................................................................18
     Standards-based Security ....................................................................................18
        Protocols and Algorithms ...............................................................................18
        Security Certifications ....................................................................................18
        Expert Recognition ..........................................................................................18
     Trusted Authentication Environment .................................................................18
        Field-programmable Tokens ..........................................................................18
        Hardware-based Root of Trust ........................................................................18
  iii. Transparency .....................................................................................................19
IV. Conclusion: Embarking on Next-Generation Enterprise Authentication...............20
Once protected by the isolated confines of enterprise IT, business boundaries have been permanently warped by the juggernauts of virtualization and cloud computing. Expected to grow 18 percent year-over-year through 2016, cloud-delivered services such as SaaS, infrastructure-as-a-service (IaaS), and platform-as-a-service (PaaS) have created a new IAM trinity, one that consists of a complex identity management and authentication environment.

Enterprise IT perimeters have changed, giving rise to the New IAM Trinity—one that comprises a “many-to-many” authentication environment—a multitude of identities accessing multiple resources from multiple devices.

The Old IAM Trinity vs. the New IAM Trinity

A single user, authenticating to a single access point, using a single workstation encompasses the simple IAM trinity of yesteryear (Figure 1). Moving from single to multiple authentication environments, enterprise IT perimeters have changed, giving rise to the New IAM Trinity—one that comprises a “many-to-many” authentication environment—a multitude of identities accessing multiple resources from multiple devices (Figure 2).
Enterprise users today have multiple online identities—social, personal, government-issued, or corporate. Some have multiple levels of access privileges; for example, system administrators tasked with ensuring that systems and applications are functioning correctly for users with different levels of permissions, and may therefore authenticate alternately as users, admins, or even ‘super’ admins. Editors of wikis or online publications may view, troubleshoot, and revise web pages using different identities. Users may authenticate with one identity to their consumer-targeted SaaS apps (e.g., file exchange, webmail) but with a different identity to their enterprise-bound cloud services (CRMs, ERPs, IaaS, PaaS, etc.).

To confuse identity management matters even more, users now access the same applications from different devices, corporate-issued or BYOD. These endpoints carry with them different device identifiers—MAC addresses, OSs, browsers, and IP addresses. Moreover, the tipping point is increasingly shifting in favor of mobile devices, with Americans spending longer hours online through their mobile browsers and apps, rather than using their PCs.\(^1\)

Organizations have come to rely on access to a wealth of external resources, which provide critical enterprise data and infrastructure, such as corporate VPNs, global content delivery networks (IaaS), CRMs, ERPs, cloud-computing, and web-hosting platforms (PaaS). How can organizations verify who is accessing their information when this very information is hosted outside their IT perimeter?

---

Enterprise Agility and the New IAM Trinity

How has enterprise agility been affected by the need to manage the New IAM Trinity? Organizations acting conservatively may venture the adoption of a single SaaS application, handing over the task of verifying user identity and access permissions to an external service provider—the SaaS provider.

Some organizations may try to avoid the cloud at all cost, at the price of decelerating their growth, as complex IAM hampers the adoption of SaaS applications, and impedes the adoption of new technology, such as application virtualization and cloud-computing infrastructure. Still others may seek to capitalize on cloud computing technology for the purpose of lowering costs and reducing IT administration overhead, but fear that doing so will completely expose their organizations’ data, documents, and platforms.

According to a SafeNet survey, 73 percent of security and IT professionals seek solutions that support compliance and security when sourcing systems that resolve cloud consolidation issues. Why are these needs so top-of-mind? Simply because, in a complex “many-to-many” environment, the feat of enforcing consistent access controls and auditing access events throughout a fragmented IT environment becomes quite a challenge. In fact, 59 percent of the IT and security professionals surveyed admitted that their current solutions are falling short of auditing requirements.

As if increased day-to-day operational efficiency and convenience, along with cost reduction, were not sufficient incentives to resolve the complexity of the New IAM Trinity, enterprises without advanced IAM schemes inhibit business flexibility—remote network access while on the go, flexible work-from-home arrangements, and ad-hoc access to contractors, freelancers, or offshore personnel—all cannot be securely established in a timely manner without an appropriate IAM scheme that enables simple and quick provisioning, authorization, verification, and access.
Information Security and the New IAM Trinity

Hampering SaaS adoption and efficiency in some organizations, still others may willingly embrace cloud while failing to consider the security implications, such as those that could arise in the event that unauthorized access is gained to critical business information residing in file-sharing or SaaS apps, or in the event that critical web hosting infrastructure is compromised, and subsequently modified or poisoned. Drawing on a wide-scale survey\(^1\) of the authentication landscape in multiple continents, SafeNet found that 52 percent of organizations already use strong two-factor authentication not only for remote network access (VPNs) but for at least one additional application as well.

Complex identity and authentication environments are prone to creating multiple external user stores, such as those created by default when users register to a new web service. On-premises user stores, while forking the audit trail, do offer some visibility into access events (with visibility consolidated through single sign-on), while hosted user stores belonging to cloud applications do not offer any visibility into security events, severing the security audit trail and leaving it incomplete.

Frequently, these assets that reside in the cloud and outside of an organization’s traditional network perimeter are protected only with a password, which is easily compromised by phishing, database hacking, and brute force (or dictionary) attacks.

Adding to the identity entropy, BYOD-support policies—already implemented by 68 percent of organizations in North America and EMEA\(^2\)—often lack a strong authentication component, increasing the risk of unauthorized access originating from these devices.

Cloud applications that cut off the security audit trail, web portals and resources protected only with vulnerable passwords, and personal devices that double as workstations—all of these create a complex IAM environment in which the sum total of risk associated with unauthorized access and data breaches increases.

---


In light of the New IAM Trinity, enterprises are compelled to rethink their IAM strategy and source a solution that will not only bridge identities to the cloud and streamline current identity needs but will also comprise an extensible authentication framework for emerging ones.

To help guide your organization through the decision process of sourcing a solution that will address your access management needs, today and tomorrow, SafeNet has defined three rules to selecting a future-ready authentication solution:

→ Rule 1 – Select for control and integrity
→ Rule 2 – Seek smooth management
→ Rule 3 – Ensure the ability to adapt

More information on each rule is provided in the sections that follow.
Rule 1 – Select for Control and Integrity

Foremost on the prerequisite list is control and integrity.

An authentication solution’s most important functionality is to secure access to resources throughout an organization’s IT ecosystem, to protect identities, and ensure that users are who they claim to be. To this end, a sourced solution should enable strong, multi-factor authentication to resources throughout business boundaries, both on-premises and in the cloud.

To safeguard enterprise security, the solution itself should be scrutinized for technical soundness to ensure that it does not contain security vulnerabilities.

Next, solutions that are standards-based should be preferred, as they provide transparency with regards to their inner clockwork and integrity, and contribute to a solution’s robustness. International standards are continuously tested and reviewed by industry experts, allowing vulnerabilities to be weeded out and the standard to be improved.

Third, solutions that have been certified by independent national, regional, or international standards organizations ensure that best practices are met during the solution’s manufacturing and operation.

Fourth, some organizations may opt to source a solution that allows organizations to store their own authentication data (OTP seeds) in order to reduce the risk inherent to hosting such data by a third party.

Finally, an authentication solution should assist your organization with regulatory compliance, without any additional administration on your part. This consideration can be addressed with robust reporting capabilities, which are simplified when generated from a single authentication interface.

Seek Control and Integrity

Select authentication solutions that:

→ Have been scrutinized for technical soundness
→ Have been certified by regional or international standards organizations
→ Allow organizations to store their own token seed data
→ Facilitate regulatory compliance
Rule 2 – Seek Smooth Management

After checking a solution for control and integrity, verify how complex the solution is to deploy and administer.

- **Provisioning** – How simple is the workflow for provisioning authentication methods (tokens and tokenless) to current users, new users, internal users residing within an enterprise user store, or external users that need to be added ad-hoc? Can users be imported in more than one way, such as imported files, synching with external user stores, etc.?

- **Deployment and maintenance** – Deployment considerations include such factors as time to value, and the ability to integrate with your existing infrastructure and maintain your current security investments. Additional considerations are hardware and software prerequisites, and enterprise priorities that determine whether an optimal solution should be deployed as an on-premises platform or as-a-service delivered from the cloud.

- **Management by exception** – To keep management overhead to a minimum, seek authentication solutions that offer automated alerts in the event that configuration changes are made, certain inventory thresholds are exceeded, or certain actions are not taken, such as the activation of soft tokens by a certain user group.

Seek Smooth Management

**Select authentication solutions that:**

- Facilitate provisioning to both internal and external users
- Offer cost-effective deployment and maintenance
- Enable management by exception
Rule 3 – Ensure the Ability to Adapt

To meet an organization’s current and emerging identity access and management needs, prospective authentication solutions should:

→ **Support all current use cases** – Basic IAM needs include synching with user stores and extending authentication to basic access scenarios, such as remote network access (VPN) and remote access to corporate email. Additional strong authentication scenarios that may be required in high risk environments may be pre-boot/disk encryption and network logon.

→ **Support future use cases** – Application and desktop virtualization, adoption of additional cloud applications, and the adoption of hosted networking and computing resources may all affect the type of solution sought, as the solution in question would be required to accommodate all of these needs.

→ **Offer scalability** – Solutions that easily grow with your organization simplify future access management needs. Mergers and acquisitions may require a multi-tier, multi-tenant solution that can grow with an organization to accommodate shared services, new user groups, and profit-and-loss units. Billing and security audits, in turn, are simplified by reporting generated by a multi-tenant, multi-tier solution.

→ **Accommodate evolving endpoints** – With the consumerization of mobile technology, organizations seek to support mobility policies that enable secure access to sensitive enterprise resources from a range of different devices and endpoints.

Seek the Ability to Adapt

**Select authentication solutions that:**

→ Support all current use cases
→ Support future use cases
→ Offer scalability
→ Accommodate evolving endpoints
Assessing your Organization’s Needs

The New IAM Trinity—resulting from increased enterprise mobility, endpoint evolution, and as-a-service business models—is affecting organizations’ ability to maintain business agility without compromising information security.

Many enterprises are aware of their need to address these challenges but still encounter the same constraints when sourcing an appropriate authentication solution:

→ **Cost** – Specifically, the need to keep TCO down, which is facilitated by opex (operational expenditure) pricing models as opposed to capex (capital expenditure) investments.

→ **Usability** – The need to streamline authentication from an IT deployment and management perspective, while keeping authentication simple for the end user. Factors to consider are implementation and administration overhead with cloud-based as-a-service models.

→ **Risk** – The need to address different levels of risk for different user groups and applications. For example, sys admins and users may require varying levels of identity assurance, depending, in turn, on the sensitivity of the resource accessed.

The three main constraints to sourcing an enterprise authentication solution are:
III. Next-Generation Authentication from SafeNet

Powered by frictionless authentication, SafeNet’s Next-Generation Authentication lets organizations meet their business and security needs to achieve the optimal balance between convenience, risk mitigation, and TCO.

Next-Generation Authentication offers frictionless authentication, combined with transparency, trust, and control, allowing organizations to secure access to diverse applications and meet security regulations in a shifting IT landscape.

Support for a broad IT ecosystem and fully automated authentication lets organizations extend strong authentication to diverse environments and address new use cases while reducing management complexities and costs.

Flexible delivery models, the broadest range of authentication methods and a choice of form factors ensure optimized risk mitigation and user convenience. Extensive reporting capabilities provide the visibility and transparency that is critical for security oversight.

SafeNet’s Next-Generation Authentication Solutions offer:

→ **Frictionless Authentication** for both IT professionals and users

→ **Trust** through standards-based technology and certifications, and a fully trusted authentication environment

→ **Transparency** achieved via a single audit trail spanning an enterprise’s entire IT ecosystem
i. Frictionless Authentication

Fulfilling the promise of Next-Generation Authentication, SafeNet offers frictionless authentication and frictionless management through fully automated workflows and platform agility.

Frictionless Management

SafeNet’s Next-Generation Authentication solutions reduce IT administration overhead through automated token- and user-lifecycle management, real-time threshold- and event-based alerts, and extensive user self-service, drastically reducing the time and cost of configuring and provisioning authentication methods to users, and dramatically reducing the time it takes to identify and handle system events.

Automated Lifecycle Administration

Providing virtually unlimited scalability, and essential for organizations whose user count is in the thousands and tens of thousands, auto-provisioning allows SafeNet’s solutions to create user accounts without manual intervention, and allows 'soft' tokens and tokenless methods to be allocated to predefined user groups and individuals.

Policy-based controls, as defined per group, allow teams, departments, and business units to be allocated specific token configurations, application permissions, and pre-authentication rules. By combining policy-based controls and periodic synching with existing user stores (such as AD, Oracle, SQL, Lotus, Novell, IBM, etc.), SafeNet’s Next-Generation Authentication solutions apply the appropriate access policies and token (or tokenless) configurations to a user’s authentication scheme. Auto-synching and auto-provisioning functionalities enable SafeNet’s solutions to automatically issue tokens to new users, automatically request users to activate their tokens by email, and enable auto-revocation and auto-modification of a user’s access permissions when they are removed from a user store or reassigned to a new user group.

Management by Exception

Streamlining user, token, and solution management, SafeNet’s solutions deliver automated alerts via SMS text messages or email notifications, allowing administrators to manage by exception. These alerts provide real-time red-flag notifications on user, solution, and inventory events that require follow-up action.

Alerts can be configured for various event types, thresholds, and notification recipients to ensure mitigation measures are performed on time. Examples include notifications to users and administrators in the event of account lockout following a predefined number of consecutive failed login attempts. Modification of a key system configuration setting, the absence of user enrollments by a certain date, the near-depletion of token or license inventory, and account status changes are all examples of events that can automatically generate real-time alerts to the appropriate personnel.
Extensive User Self-Service

Users receive enrollment and token activation email notifications, allowing them to activate and administer their own authentication tokens and profiles, helping driving down help desk calls. Activating a token, reporting a token lost and requesting a new one, changing a PIN or password, changing contact details, along with other administrative tasks, can all be completed by users through a dedicated self-service portal. This has extensive implications on a global workforce that may number in the hundreds, thousands, or tens of thousands, and may be distributed among different time zones, as it allows for the automated resolution of numerous simple, yet critical, token- and user-related issues.

SafeNet provides frictionless solution management thanks to its:

→ Fully automated lifecycle administration
→ Management by exception
→ Extensive user self-service
Frictionless Authentication
Support for a broad IT ecosystem lets organizations extend strong authentication to diverse environments and address new use cases while reducing password fatigue, management complexities, and costs. Providing optimal agility, Next-Generation Authentication offers the following:

Native Identity Federation
SafeNet allows organizations to natively extend identities to the cloud and centrally implement and manage strong authentication policies for enterprise and cloud applications from a single authentication back end.

Through support of the SAML Identity Federation protocol, SafeNet authentication platforms serve as the trusted identity provider for cloud applications. With federated login, SafeNet’s platforms allow users to sign in once in order to concurrently gain access to all their cloud applications (including IaaS, Paas, and SaaS).

Periodic synching with user stores and native identity federation enable automated workflows, with user store changes automatically taking effect in the authentication back end; for example, adding, modifying, and removing permissions, tokens, and management roles, to name a few.

Unified access control policies, such as group-based permissions and strong two-factor authentication, help streamline security throughout the IT ecosystem, with native identity federation removing the burden of remembering multiple access credentials.

Choice of Delivery Platforms
Available as a cloud-based service or installed on-premises, SafeNet’s Next-Generation Authentication lets organizations implement strong authentication according to their business and security needs. Cloud-delivered solutions shorten deployment and implementation cycles, and offer organizational efficiencies such as eliminating the need to procure and maintain additional infrastructure.
With federated login, SafeNet’s platforms allow users to sign in once in order to concurrently gain access to all their cloud applications.
Choice of Authentication methods
Offering users frictionless authentication, SafeNet’s Next-Generation Authentication solutions offer the broadest range of authentication methods and form factors. Allowing self-enrollment and self-administration of tokens, SafeNet’s solutions also offer tokenless context-based authentication, and enable federated login.

OTP, OOB, context-based authentication, and pattern-based and certificate-based authentication can be selected based on levels of assurance required for different use cases. Offering unparalleled flexibility, form factors such as smart cards, USB tokens, and software or phone-based tokens may be deployed according to user preference and convenience, while maintaining a lower TCO with central management of all tokens.

Phone tokens and X.509 certificates enable authentication from BYOD devices in the same manner as those that are corporate-issued, while federated login enables users to log in only once, using the same identity used to log on to the network, to concurrently gain access to multiple cloud applications.

Broad Use Case and Ecosystem Support
SafeNet allows organizations to implement strong authentication for numerous use cases, and achieve uniform, centrally managed security policies for a broad IT ecosystem, which may include any combination of the following authentication use cases:

- Remote access (VPN)
- Cloud access
- Local network logon
- VDI and private clouds
- Web-based portals
- PKI support for pre-boot disk encryption
- PKI support for digital signatures

Offering out-of-the-box integrations that easily interlock with your current on-premises, hybrid, or cloud-based ecosystem, SafeNet’s Next-Generation Authentication mitigates risk and allows smooth adoption of new technologies. Uniform access policies can be applied to diverse use cases, with pre-validated integrations offering a lower total cost of ownership.
ii. Trust

SafeNet’s solutions meet stringent international standards and offer a trusted authentication environment, giving organizations the confidence and controls they need to adopt new technologies and secure their IT ecosystems.

**Standards-based Security**

Protocols and Algorithms

Ensuring transparency and business confidence, SafeNet’s solutions employ standards-based authentication protocols and encryption algorithms, which have been vetted by peer reviews and standards organizations. By deploying a solution designed with known protocols and algorithms, organizations gain technical insight and the peace of mind that evolves with industry scrutiny and validation.

**Security Certifications**

Holding its solutions to the highest security standards, SafeNet solutions have been awarded certifications by international and regional industry organizations. These pertain to best practices implemented with respect to as-a-service operations, and product design and performance.

**Expert Recognition**

A recognized market leader, SafeNet has been consistently recognized by industry analysts as the market leader for enterprise authentication. Leading in innovative vision and noted for its execution capabilities, SafeNet’s flexible vanguard solutions provide organizations with the latest authentication technology, without compromising usability and convenience.

**Trusted Authentication Environment**

Field-programmable Tokens

SafeNet’s Next-Generation Authentication provides customers the option to control their own authentication data through field-programmable tokens. By programming tokens at their premises of choice, organizations can maintain stringent control and supervision over their own authentication data, eliminating the need to rely on third-party security practices.

By programming tokens at their premises of choice, organizations can maintain stringent control and supervision over their own authentication data, eliminating the need to rely on third-party security practices.

**Hardware-based Root of Trust**

SafeNet authentication solutions are protected by a hardware-based root of trust, ensuring that authentication data cannot be copied or stolen, and providing resiliency in the event of malicious attacks. Hardware-based roots of trust consist of hardware modules that store encryption keys and cryptographic operations, providing tighter data protection.
iii. Transparency

SafeNet offers extensive and automated reporting, giving CISOs and IT administrators immediate visibility into the daily movements of their authentication activity. Robust reporting capabilities enable security audits and lower costs through transparency and streamlined administration.

CISOs and CIOs whose users access all applications and resources through a single authentication service interface, gain the visibility and transparency they need to get an immediate audit trail of which users are accessing both cloud and enterprise applications at any given time.

With automated reporting, authorized personnel can easily schedule periodically-generated detailed security, compliance, accounting, and inventory reports in whatever format required to comply with all relevant security standards, including SOX, PCI, and HIPAA.

In addition to customary logging functionality, CISOs can benefit from improved visibility and transparency with security policy reports covering such data as alerts history, operator roles and scope, authentication nodes, status of various provisioning tasks, and RADIUS attributes per user or group, to name a few.

Compliance reports, on the other hand, cover user authentication metrics, locked accounts, users secured with only static passwords, administrator logons, critical configuration changes, and other factors relevant to internal and external auditors.

Details on SMS credits, tokens and licenses, among others, can be viewed in accounting reports, while inventory management reports provide detailed information on tokens, token ownership status, and other relevant information.
IV. Conclusion: Embarking on Next-Generation Enterprise Authentication

In a complex and evolving climate of advanced threats, virtualization, regulatory mandates, and mobility, organizations are taking a data-centric approach to protect and control their sensitive information.

By selecting solutions that offer smooth management, control, and integrity, and the ability to adapt to an ever-expanding IT ecosystem, organizations can maintain business agility without compromising information security.

To this end, SafeNet fulfills the promise of Next-Generation Authentication by offering frictionless authentication combined with transparency, trust and control, supplying the only complete portfolio that provides persistent protection of sensitive information at all critical access points.

From the data center to the cloud, SafeNet helps organizations remain protected, compliant, and in control—no matter where their business takes them.

About SafeNet

Founded in 1983, SafeNet, Inc. is one of the largest information security companies in the world, and is trusted to protect the most sensitive data for market-leading organizations around the globe. SafeNet’s data-centric approach focuses on the protection of high value information throughout its lifecycle, from the data center to the cloud. More than 25,000 customers across commercial enterprises and government agencies trust SafeNet to protect and control access to sensitive data, manage risk, ensure compliance, and secure virtual and cloud environments.