

Strong User Authentication

Best-in-Class Performance at Assuring Identities

March 2008



Executive Summary

This research benchmark provides insight and recommendations for all organizations that are interested in decreasing their reliance on username and passwords for user authentication and learning more about the benefits of deploying **strong user authentication** solutions. Strong user authentication can be used to increase the level of assurance for online identities as part of an overall approach to securing access to information and managing risk.

Best-in-Class Performance

To distinguish Best-in-Class companies from Industry Average and Laggard organizations, Aberdeen used the year-over-year changes in the following performance criteria:

- Number of security-related incidents
- Number of non-compliance incidents (e.g., failed audits)
- Amount of human error related to security
- Number of help desk calls related to user authentication
- Total management costs related to user authentication

Companies with top performance based on these criteria earned Best-in-Class status.

Competitive Maturity Assessment

Survey results show that the firms enjoying Best-in-Class performance shared several common characteristics, including the following:

- Deployment of one or more methods of user authentication other than username / password (80%)
- Consistent user authentication policies as a function of information assets (76%), supported applications (76%), and supported access methods (60%); and consistent authorization policies (access privileges) as a function of identity (76%)
- Formalized workflow for authorizing the provisioning of user authentication credentials (58%)
- Responsible executive or team with primary ownership for user authentication policy (68%) and credential lifecycle management (52%)

Recommended Actions

In addition to the specific recommendations in Chapter Three of this report, to achieve Best-in-Class performance companies should select and deploy strong user authentication solutions based on their assessment of the optimal balance between security, total cost of ownership, and alignment with the end-user populations and applications being supported.

Research Benchmark

Aberdeen's Research Benchmarks provide an in-depth look into process, procedure, methodologies, and technologies; identify best practices; and make actionable recommendations

"We struggled for a long time with giving top priority to the inevitable replacement of passwords with strong authentication. In a smaller company, security does not typically make the list of the top five things we need to do this month. The risks and benefits [of strong authentication] were reasonably clear, but security was always one of those issues we said we would worry about later. It's not viewed as important ... until it breaks, and then it's a crisis. This will sound funny, but the impetus to move literally came to me in a fortune cookie: 'The expedient thing and the right thing are seldom the same thing.'"

~CEO,
Small Enterprise

Send to a Friend 

Table of Contents

| | |
|---|----|
| Executive Summary..... | 2 |
| Best-in-Class Performance..... | 2 |
| Competitive Maturity Assessment..... | 2 |
| Recommended Actions..... | 2 |
| Chapter One: Benchmarking the Best-in-Class..... | 5 |
| Business Context - The Problems with Passwords..... | 5 |
| Aberdeen's Maturity Class Framework..... | 7 |
| Best-in-Class PACE Model..... | 8 |
| Best-in-Class Strategies..... | 9 |
| Chapter Two: Benchmarking Requirements for Success..... | 13 |
| Competitive Assessment..... | 14 |
| Capabilities and Enablers..... | 15 |
| Chapter Three: Recommended Actions..... | 25 |
| Laggard Steps to Success..... | 25 |
| Industry Average Steps to Success..... | 25 |
| Best-in-Class Steps to Success..... | 26 |
| Appendix A: Research Methodology..... | 27 |
| Appendix B: Related Aberdeen Research..... | 29 |

Figures

| | |
|---|----|
| Figure 1: Current Password Practices..... | 5 |
| Figure 2: Leading Drivers for Strong User Authentication Initiatives by Best-in-Class Organizations..... | 6 |
| Figure 3: Best-in-Class Strategies Driving Current Investments..... | 10 |
| Figure 4: Top Performers Have Deployed Strong Authentication..... | 10 |
| Figure 5: Abundant Choice - Current Use and Planned / Evaluating..... | 11 |
| Figure 6: Consistent Policies for Authentication and Authorization..... | 16 |
| Figure 7: Consistent Approach to Rollout, Analysis, Audit, Reporting, and Exception-Handling for User Authentication..... | 17 |
| Figure 8: Organizational Ownership and End-User Awareness..... | 18 |
| Figure 9: Discovery and Classification as Prelude to Policy..... | 19 |
| Figure 10: Reporting and Management Visibility, Post-Deployment..... | 20 |
| Figure 11: Credential Lifecycle Management (Provisioning)..... | 21 |
| Figure 12: Credential Lifecycle Management (End-User Support)..... | 21 |
| Figure 13: Credential Lifecycle Management (De-provisioning)..... | 22 |
| Figure 14: Credential Lifecycle Management (Operations / Mgmt)..... | 23 |
| Figure 15: Performance Management..... | 23 |

Tables

| | |
|--|---|
| Table 1: Top Performers Earn Best-in-Class Status..... | 7 |
| Table 2: The Best-in-Class PACE Framework..... | 8 |

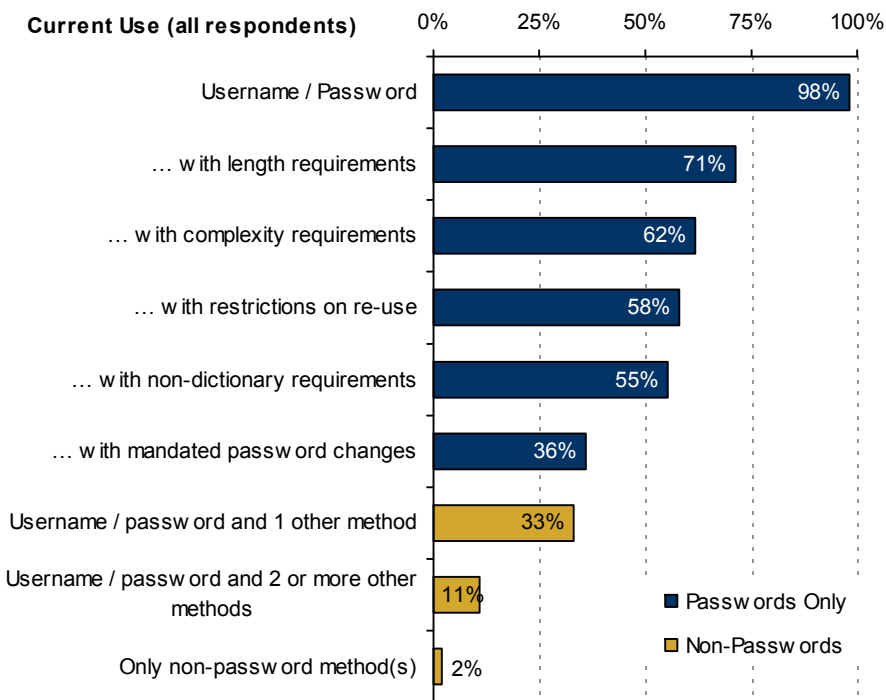
Table 3: Competitive Framework 14
Table 4: PACE Framework Key 28
Table 5: Competitive Framework Key 28
Table 6: Relationship Between PACE and the Competitive Framework 28

Chapter One: Benchmarking the Best-in-Class

Business Context - The Problems with Passwords

Aberdeen's research indicates that virtually all organizations surveyed (98%) indicate continued reliance on username and passwords for authenticating end users to control access to systems, networks, data, and applications. Nearly half (48%) of all respondents, however, have also deployed at least one stronger, non-password method of user authentication (Figure 1).

Figure 1: Current Password Practices



Source: Aberdeen Group, March 2008

A majority of all respondents have taken steps to strengthen the security of passwords, for example:

- Requirements for length (71%), complexity (62%), and frequency of change (36%)
- Restrictions on re-use (58%)
- Exclusion of standard dictionary terms (55%)

All of these steps enhance the security of passwords, but at the same time they make passwords more cumbersome for end users. Passwords that are more difficult to guess are also more difficult to remember. Natural coping mechanisms include writing them down (which weakens security) and

Fast Facts

For respondents in this study:

- ✓ 88% of all enterprise users have multiple work-related passwords
- ✓ The average number of work-related passwords per user is between five and six

relying on calls to the help desk (which increases cost). Shockingly, nearly two-thirds of all respondents (64%) currently do not even require passwords to be changed. It should go without saying that none of the resulting risks, costs, and inconveniences were the formal intent of management in establishing current user authentication policies based on passwords.

The sheer number of passwords amplifies the problem. In a typical day in the life of an average enterprise knowledge worker, she may be required to use a half-dozen passwords or more in the normal course of Windows logon, data encryption, remote access (e.g., VPN or SSL VPN), WiFi access, e-mail, web-based applications or portals, and back-office applications (e.g., HR or ERP). In addition, smaller subsets of users may use passwords to access privileged accounts (i.e., administrative functions) or to execute high-value transactions. The current research indicates that about nine out of 10 (88%) enterprise users have multiple work-related passwords.

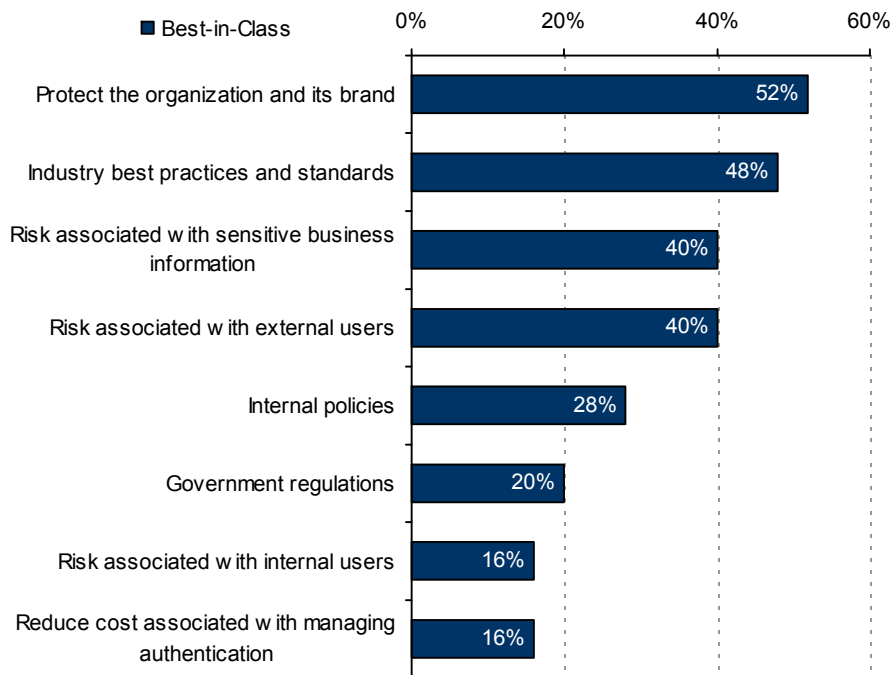
The top pressures driving organizations to focus resources on evaluating and implementing stronger, non-password forms of user authentication are those Aberdeen has seen in virtually all security benchmark studies over the past year (Figure 2). Risks, regulations, internal policies, and industry best practices and standards continue to be the leading market drivers, along with "protecting the organization and its brand."

Fast Facts

Among Best-in-Class organizations in this study, over the last 12 months:

- ✓ 52% have increased the number of network users
- ✓ 48% have increased the number of remote users
- ✓ 44% have increased the number of wireless users
- ✓ 32% have increased the number of guest (non-permanent) users

Figure 2: Leading Drivers for Strong User Authentication Initiatives by Best-in-Class Organizations



Source: Aberdeen Group, March 2008

"It's already game over ... we can't roll the rock back in front of the cave. Our customers are now our weakest link in terms of security. Establishing higher assurance for user identities is one of the most obvious places you can start."

~CISO,
Web Portal

“Reduce cost” is a more recently emerging theme seen in Aberdeen’s security research, but worthy of special note as a driver for investments in strong user authentication given the common (mis)perception that passwords are “free.” Our November 2007 report on [Security Governance and Risk Management](#) first showed that Best-in-Class organizations have begun to develop security Governance, Risk management and Compliance (GRC) processes to more effectively allocate their finite IT resources and activities based on their business objectives and on acceptable levels of risk.

Also noteworthy in Figure 2 is the relative importance of risk from external users (40%) versus risk from internal users (16%) as a driver for current investments in strong user authentication. The relentless trends towards de-perimeterization have required organizations to provide more end user populations with expanded access, to a broader set of data and applications, over a wider range of access methods. For companies with top performance, providing higher levels of assurance for the identities of these end users is a critical element of a deliberate security GRC infrastructure.

Fast Facts

Percentage of Best-in-Class organizations in this study that have increased the use of strong user authentication over the last 12 months, by end-user population:

- √ 48% all employees
- √ 44% mobile / remote employees
- √ 32% privileged users (admins)
- √ 32% contractors
- √ 20% business partners
- √ 20% customers

Aberdeen's Maturity Class Framework

To distinguish Best-in-Class companies from Industry Average and Laggard organizations with respect to user authentication, Aberdeen used the year-over-year changes in the following performance criteria:

- Number of security-related incidents
- Number of non-compliance incidents (e.g., failed audits)
- Amount of human error related to security
- Number of help desk calls related to user authentication
- Total management costs related to user authentication

"We are struggling to take the precious IT resources we have today - most of which are spent on routine operations - and transfer a greater portion of those resources to an innovation bucket."

~CIO,
High-Tech Industry

Companies with top performance based on these criteria earned Best-in-Class status, as described in Table I. (For additional details on the Aberdeen Maturity Class Framework, see Table 5 in Appendix A.) Survey responses from nearly 150 organizations representing a diverse set of industries are included in this study.

Table I: Top Performers Earn Best-in-Class Status

| Definition of Maturity Class | Mean Class Performance |
|---|--|
| <p>Best-in-Class: Top 20% of aggregate performance scorers</p> | <ul style="list-style-type: none"> ▪ 52% decreased the number of actual security-related incidents ▪ 44% decreased the number of non-compliance incidents (e.g., failed audits) ▪ 80% decreased the amount of human error related to security ▪ 44% decreased the number of help desk calls related to user authentication ▪ 36% decreased the total management costs related to user authentication |

| Definition of Maturity Class | Mean Class Performance |
|---|--|
| Industry Average: Middle 50% of aggregate performance scorers | <ul style="list-style-type: none"> ▪ 3% decreased the number of actual security-related incidents ▪ 3% increased the number of non-compliance incidents (e.g., failed audits) ▪ 2% decreased the amount of human error related to security ▪ 6% increased the number of help desk calls related to user authentication ▪ 5% increased the total management costs related to user authentication |
| Laggard: Bottom 30% of aggregate performance scorers | <ul style="list-style-type: none"> ▪ 31% increased the number of actual security-related incidents ▪ 33% increased the number of non-compliance incidents (e.g., failed audits) ▪ 31% increased the amount of human error related to security ▪ 39% increased the number of help desk calls related to user authentication ▪ 31% increased the total management costs related to user authentication |

Note: Percentages shown are the net of "increased," "stayed the same," and "decreased"
Source: Aberdeen Group, March 2008

Best-in-Class PACE Model

Using strong user authentication to increase the level of assurance for online identities requires a combination of strategic actions, organizational capabilities, and enabling technologies – referred to by Aberdeen as the Best-in-Class PACE Framework (for a description of the Aberdeen PACE Framework, see Table 4 in Appendix A). The characteristics exhibited by Best-in-Class organizations in this study are summarized in Table 2.

Table 2: The Best-in-Class PACE Framework

| Pressures | Actions | Capabilities | Enablers |
|---|--|---|--|
| <ul style="list-style-type: none"> ▪ Protect the organization and its brand ▪ Industry best practices and standards | <ul style="list-style-type: none"> ▪ Establish and enforce consistent policies and procedures for user authentication ▪ Strive toward a common user authentication "platform" that can manage multiple authentication methods ▪ Reduce the total cost of managing user authentication credentials | <ul style="list-style-type: none"> ▪ Consistent user authentication policies – by classification of information assets, by supported applications, and by supported access methods ▪ Consistent authorization policies ▪ Systematic implementation / rollout ▪ Formalized workflow for authorizing provisioning / management of user authentication credentials ▪ Consistent policies for emergency access (e.g., lost / stolen / forgotten) ▪ Standardized audit, analysis, and reporting ▪ Regular review and analysis of audit and reporting data from user authentication management systems ▪ Standardized response for exceptions, security events, or incidents of non-compliance, and systematic elimination of root causes | <ul style="list-style-type: none"> ▪ One-time passwords ▪ Digital certificates (X.509) ▪ Biometrics (fingerprint) ▪ Smart cards (ISO 7816) ▪ Converged logical / physical access cards ▪ Knowledge-based authentication (e.g., security questions) ▪ Identity and access management ▪ User provisioning ▪ Web access management |

Source: Aberdeen Group, March 2008

Best-in-Class Strategies

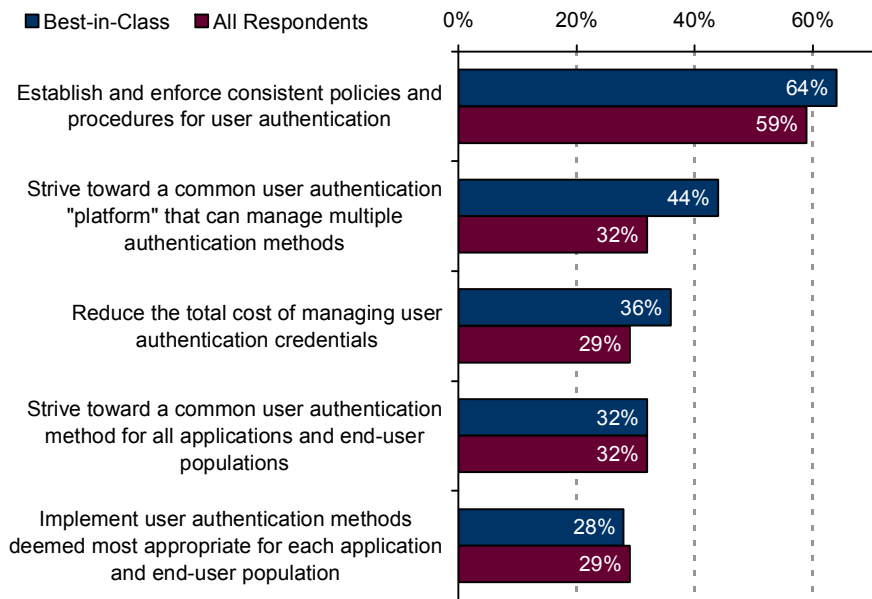
Strategies which are based on establishing and enforcing consistent policies for user authentication correlate most highly (64% of Best-in-Class organizations) with current investments in strong user authentication (Figure 3). In addition, the research shows that the top performers were 24% more likely to identify an explicit strategy to reduce the total cost of managing user authentication credentials as a driver for current investment.

With respect to selecting and implementing specific strong user authentication methods, the data reveals three distinct strategic approaches:

- **The right tool for the job.** The first approach is to implement user authentication methods that are deemed most appropriate for each application and end-user population. For example, an organization might use hardware tokens for administrative access to privileged accounts, digital certificates for employee remote access over VPN, and heuristic, risk-based scoring for online access by external customers. In this approach, management of these systems would traditionally be done independently. The Best-in-Class were marginally less likely than all respondents (28% versus 29%) to identify this as their strategic approach.
- **One for all.** A second approach is to strive towards a common user authentication method for all applications and end-user populations. An example of this is a US federal government agency that issues smart cards in compliance with HSPD-12, as described in the December 2007 [Logical / Physical Security Convergence: Is It in the Cards?](#) benchmark report. The Best-in-Class were equally as likely as all respondents (32%) to identify this as their user authentication strategy.
- **Common platform.** A third approach is to move towards a common user authentication infrastructure that can manage multiple user authentication methods. The same example can be used of a company that deploys hardware tokens, digital certificates, and heuristic, risk-based scoring for different populations and purposes. The difference in this case is that the company would strive to implement a common back-end to create and enforce policies and to manage authentications credentials more consistently over their lifecycle. Best-in-Class organizations were 31% more likely than all respondents to identify this as the strategy which is driving current investments in user authentication.

We have seen, as a consistent theme across multiple studies, a strong correlation between top performance and a deliberate shift away from tactical, siloed deployments towards a more centralized infrastructure for sustainable, "continuous" security GRC. While these capabilities are still nascent, even among the Best-in-Class, we clearly see them here once again in the context of providing higher assurance for user identities through the deployment of strong user authentication.

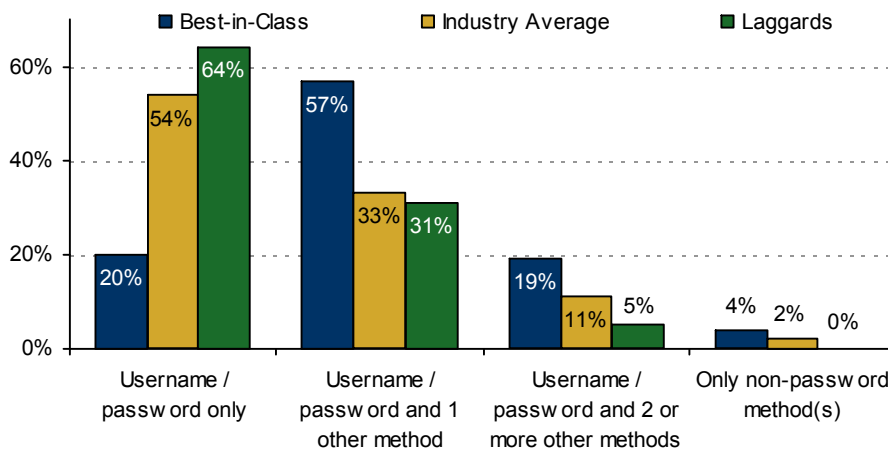
Figure 3: Best-in-Class Strategies Driving Current Investments



Source: Aberdeen Group, March 2008

The common platform strategy is well-aligned with the motivation to reduce the cost of managing existing strong authentication deployments: four out of five Best-in-Class organizations have currently deployed at least one strong user authentication method in addition to username / password, and about two out of five have deployed two or more strong authentication methods (Figure 4). Replacing existing solutions with interoperable, more cost-effective alternatives is another example of cost reduction surfaced through direct interviews.

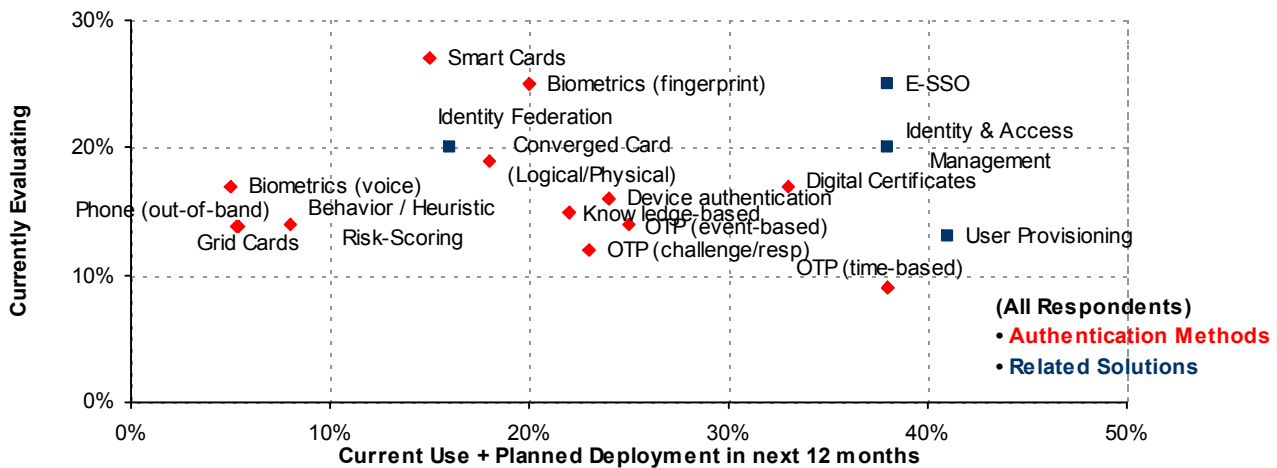
Figure 4: Top Performers Have Deployed Strong Authentication



Source: Aberdeen Group, March 2008

Figure 5 illustrates the rich diversity of strong authentication methods that have been deployed and which are currently being evaluated. Twelve selected non-password user authentication methods are plotted in two dimensions, designed to give insight into current and near-term deployments (on the x-axis) versus current evaluations (on the y-axis). For example, looking along the x-axis shows that current deployments are dominated by one-time passwords, digital certificates, and knowledge-based authentication (i.e., secret questions). Looking along the y-axis shows that methods currently under evaluation are led by smart cards, fingerprint biometrics, and converged cards (for both logical access and physical access). This diversity, of both authentication methods and of buyer interest, underscores the unique balance of solution attributes and organizational preferences that make up the selection criteria for each deployment. It also underscores the strategic value of solutions that can effectively deploy and manage multiple authentication methods.

Figure 5: Abundant Choice - Current Use and Planned / Evaluating



Source: Aberdeen Group, March 2008

In addition, the research identifies a diversity of both availability and interest in terms of the many form factors which can be used as physical "containers" for certain user authentication credentials. For example, purpose-built hardware tokens dominate for current use and near-term deployments, while current evaluations are highest for cards, USB thumb drives, smart phones and PDAs, and other USB devices. Once again, this data serves to underscore the general market shift towards flexibility and choice with respect to strong user authentication, as opposed to one-size-fits-all.

Best-in-Class organizations in this study were determined by their improvements in security and compliance, and by their improvements in key elements of cost (human error, help desk costs, and total management costs) related to user authentication. In the next chapter, we will see what the top performers are doing to achieve these gains.

Aberdeen Insights – Strategy

The ultimate choice of specific strong user authentication method(s) is a unique balance of solution attributes and organizational attributes that make up the selection criteria for every use case within each organization. In the current study, Aberdeen collected information about perceptions and priorities based on four high-level categories:

- **Total Cost of Ownership (TCO)** including acquisition cost; deployment cost; and ongoing cost of operations and management
- **Fit for end-users** including ease of learning (first time); ease of use (on an ongoing basis); whether or not the solution is visible / tangible to end-users; acceptability by end-users; convenience of form factor (if applicable); portability (e.g., can be used from work, home, or while traveling); and multi-purpose (e.g., can be used for both logical access and physical access)
- **Fit for the organization** including strength of authentication; security of implementation; adequacy for the resources / operations / transactions being protected; adequacy for minimum compliance requirements; integration / interoperability with existing infrastructure, applications, and solution providers
- **Strategic fit** including the degree to which the solution provider is a "specialist" versus providing a "platform;" support for multiple authentication methods; support for directory integration, web access management, enterprise single sign-on, or identity federation; vendor reputation; vendor support

Based on the richness of the current dataset, additional insights on buyer perceptions and preferences for several specific strong user authentication methods – one-time passwords (both hardware and software versions); digital certificates (X.509); biometrics (fingerprint); and smart cards (ISO 7816) – may be published as supplementary Research Briefs on this topic.

If anything, the research demonstrates that passwords continue to be a problem, and that a rich diversity of strong authentication alternatives will continue to be available in the market. Organizations that deploy at least one strong authentication method should make an informed choice based on their own unique balance of preferences and solution attributes. In addition, they should give deliberate thought to the strategic choice they are making, between a variety of methods each with their own back-end; versus a single method for all users; versus a variety of methods with a common back-end. Solutions providers will likely evolve into "authentication specialists" who innovate around specific methods, and "authentication platforms" which can enable common support and lifecycle management for multiple methods.

Chapter Two: Benchmarking Requirements for Success

The perceived balance of security, total cost of ownership, and fit for end-users and applications ultimately leads to the selection of one or more specific strong user authentication methods to replace passwords and provide higher assurance for identities. These choices, along with the policy, planning, process, and organizational elements of implementation, are critical success factors in the ability to realize the business benefits of better security, sustained compliance, reduced human error, reduced help desk calls, and lower total cost of management.

Case Study – Leading US Bank

One of the world's largest financial institutions, serving nearly 60 million consumers in the US, currently supports 24 million active online banking users. The company is a good example of providing higher assurance for user identities through the deployment of a spectrum of security technologies, including strong user authentication. "We constantly strive to strike the optimal balance between leading edge security technologies on the one hand, while still providing our online customers with the access and convenience they have come to expect," says the bank's director of customer service. "We achieve this through a flexible, multi-layered approach to security."

The standard online banking login is based on strong user authentication, also known as "two-factor" authentication, with the first factor being the user's card number and the second factor being the user's PIN. These are the same card and PIN used at the ATM or at the point of sale. This provides a visible layer of authentication to the end-user, and provides the convenience of using the same method across multiple channels.

Another visible security layer is an image and a user-selected phrase that is always displayed before users are asked to enter their PIN. The solution also enables the bank to transparently evaluate certain aspects of the user's computer, providing additional assurance of identity. In addition, it provides the user with a visual cue that they are visiting a bona fide bank site. "We tell our online banking customers that once they've signed up for the free service, they only have to remember one thing," he notes. "Never enter sensitive information, such as your PIN, if you don't see the image and phrase you selected."

Still another layer of identity assurance is achieved through the use of knowledge-based authentication, which refers to the familiar "security questions" that are pre-established between the user and the bank. When the bank's systems evaluate a risk score for a given transaction that exceeds its policy-based threshold, these security questions may be asked to provide a higher degree of assurance of the user's identity for that particular transaction.

continued

Fast Facts

Best-in-Class strategic approach to current investments in strong user authentication:

- √ 44% common authentication platform, supporting multiple methods
- √ 32% common authentication method for all users and applications
- √ 28% multiple authentication methods deployed and managed separately

Case Study – Leading US Bank

Most recently, the bank is offering its online customers another optional free service, which sends a text message containing a one-time passcode to the user's pre-registered mobile phone number, for authenticating funds transfers. This too is two-factor user authentication, with one factor being the customer's phone and the second factor being the one-time password. "This is yet another added layer of protection," he notes, "to give our online banking customers confidence that they are the only ones who can authorize a transfer of funds, within or outside the bank."

Competitive Assessment

Aberdeen Group analyzed the aggregated metrics of surveyed companies to determine whether their performance ranked as Best-in-Class, Industry Average, or Laggard. In addition to having common performance levels, each class also shared characteristics in five key categories: (1) **process** (the approaches taken to execute daily operations); (2) **organization** (corporate focus and collaboration among stakeholders); (3) **knowledge management** (putting data in context and exposing it to key stakeholders); (4) **technology** (the selection of appropriate tools, and the effective deployment of those tools); and (5) **performance management** (the ability of the organization to measure results to improve the business). These characteristics, identified in Table 3, serve as a guideline for best practices, and correlate directly with Best-in-Class performance across the associated metrics.

Table 3: Competitive Framework

| | Best-in-Class | Industry Average | Laggards |
|---|---|-------------------------|-----------------|
| Process | Consistent user authentication policies based on classification of information assets | | |
| | 76% | 62% | 36% |
| | Consistent user authentication policies for all supported applications | | |
| | 76% | 58% | 36% |
| | Consistent authentication policies for all supported access methods (e.g., wired, wireless, VPN, web) | | |
| | 60% | 55% | 49% |
| | Consistent authorization policies (e.g., access privileges) | | |
| | 76% | 58% | 44% |
| | Regular review and analysis of audit and reporting data from user authentication management systems | | |
| | 60% | 27% | 18% |
| Formalized workflow for authorizing the provisioning of user authentication credentials | | | |
| 58% | 48% | 18% | |

| | Best-in-Class | Industry Average | Laggards |
|-------------------------------|--|--|--|
| Organization | Responsible executive or team with primary ownership for user authentication policy | | |
| | 68% | 65% | 54% |
| | Responsible executive or team with primary ownership for credential lifecycle management | | |
| | 52% | 50% | 31% |
| | End-user awareness and training programs around user authentication | | |
| | 52% | 42% | 31% |
| Knowledge Management | Discovery and classification of information assets | | |
| | 52% | 39% | 28% |
| | Inventory and classification of supported applications | | |
| | 60% | 35% | 26% |
| | Identification and classification of supported access methods | | |
| | 60% | 35% | 26% |
| Technology | Systematic implementation and rollout capabilities for user authentication solutions | | |
| | 56% | 44% | 33% |
| | Security technologies currently in use (also see Figure 5) | | |
| | <ul style="list-style-type: none"> ▪ Username / password 96% ▪ Username / password and one other method 57% ▪ Username / Password and two 2 or more other methods 19% ▪ Only non-password methods 4% | <ul style="list-style-type: none"> ▪ Username / password 98% ▪ Username / password and one other method 33% ▪ Username / Password and two or more other methods 11% ▪ Only non-password methods 2% | <ul style="list-style-type: none"> ▪ Username / password 100% ▪ Username / password and one other method 31% ▪ Username / Password and two or more other methods 5% ▪ Only non-password methods 0% |
| | | | |
| Performance Management | Identification of all information required for auditing and reporting | | |
| | 40% | 32% | 28% |
| | Identification of required frequency for auditing and reporting | | |
| | 40% | 27% | 23% |
| | Measurement of the total costs associated with managing user authentication | | |
| | 20% | 17% | 13% |

Source: Aberdeen Group, March 2008

Capabilities and Enablers

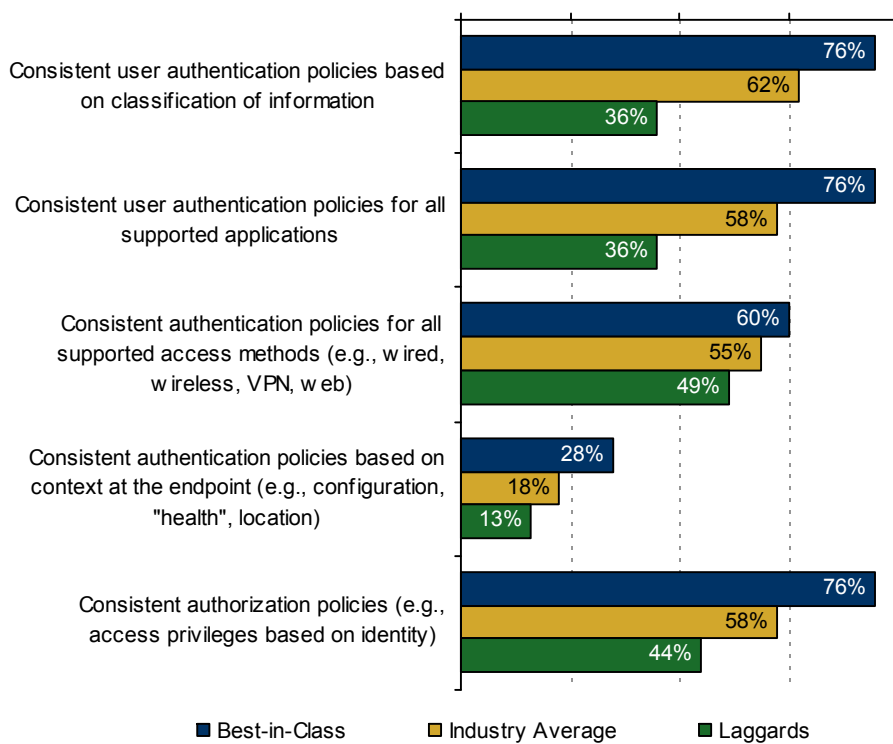
Based on the comparisons within the Competitive Framework and interviews with select respondents, analysis of the Best-in-Class highlights the degree to which they have developed their authentication-related business processes beyond those of their Industry Average and Laggard counterparts.

Process

Policies for user authentication are inherently a function of several factors, including the type of information being accessed, the nature of the applications being accessed, and the method of access (e.g., wired, wireless, VPN, or web-based). Best-in-Class organizations have developed more consistent authentication policies in each of these dimensions, in some cases by a factor of more than two-times compared to their Industry Average and Laggard counterparts (Figure 6). Best-in-Class companies are also more than two-times more likely to use current context at the endpoint (such as compliance with policies for configuration, posture or "health") as a factor for establishing user authentication policies, although at only 28% this is still an emerging trend.

In addition, more than three-fourths (76%) of the Best-in-Class have also developed consistent policies for authorization (access privileges) as a function of identity, compared to less than half (44%) of Laggards. In simple terms, "who you are" impacts "what you may do." Making authorization decisions in the context of a flexible, dynamic authentication environment is a more advanced capability, but one that is likely to be increasingly important as companies strive to address business requirements for mobility and expanded access, while simultaneously enhancing security and sustaining compliance.

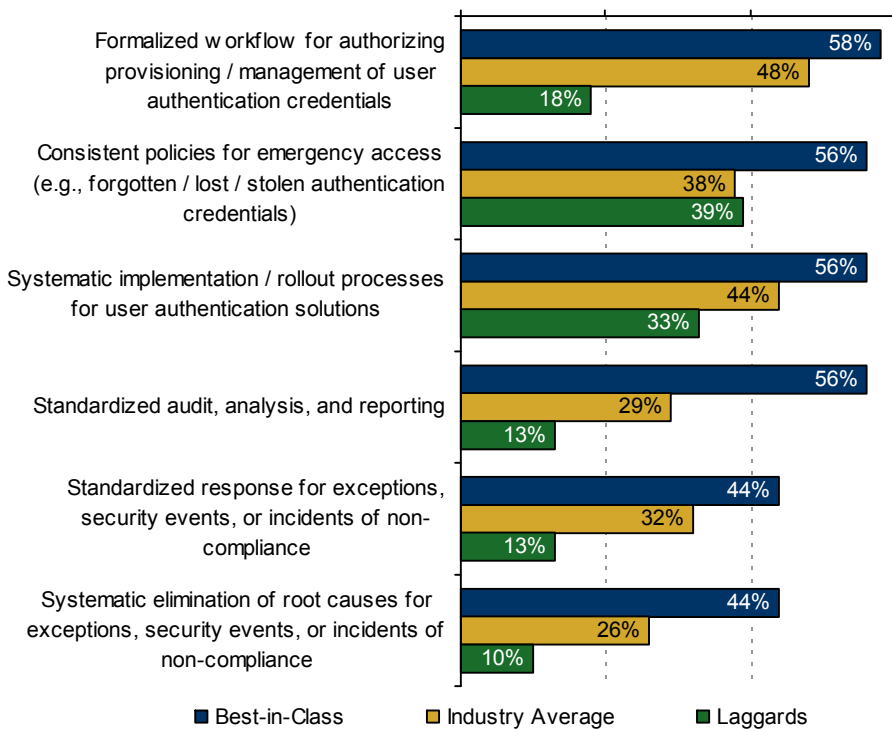
Figure 6: Consistent Policies for Authentication and Authorization



Source: Aberdeen Group, March 2008

Compared to the other maturity classes, the Best-in-Class in this study have also developed more systematic, sustainable business processes for user authentication rollout, analysis, audit, reporting, and exception-handling (Figure 7). The Best-in-Class were three-times to five-times more likely than Laggards to identify standardized responses for exceptions and systematic elimination of root causes for exceptions as current capabilities, though these capabilities too are still emerging. The overall trend is toward a more consistent, repeatable user authentication management infrastructure, independent of the particular authentication method(s).

Figure 7: Consistent Approach to Rollout, Analysis, Audit, Reporting, and Exception-Handling for User Authentication



Source: Aberdeen Group, March 2008

Figure 7 also illustrates that Best-in-Class organizations are more likely to have developed consistent policies for critical user-facing elements of the credential lifecycle, such as the initial provisioning of credentials, and emergency access in the event of forgotten, lost, or stolen credentials. For example, the Best-in-Class are more than three-times more likely (58% versus 18%) than Laggards to have formalized the workflow for authorizing and provisioning credentials for new users.

Note: Figure 11, Figure 12, Figure 13 and Figure 14 provide additional insight into top performance across all elements of managing user authentication credentials throughout their lifecycle.

Organization

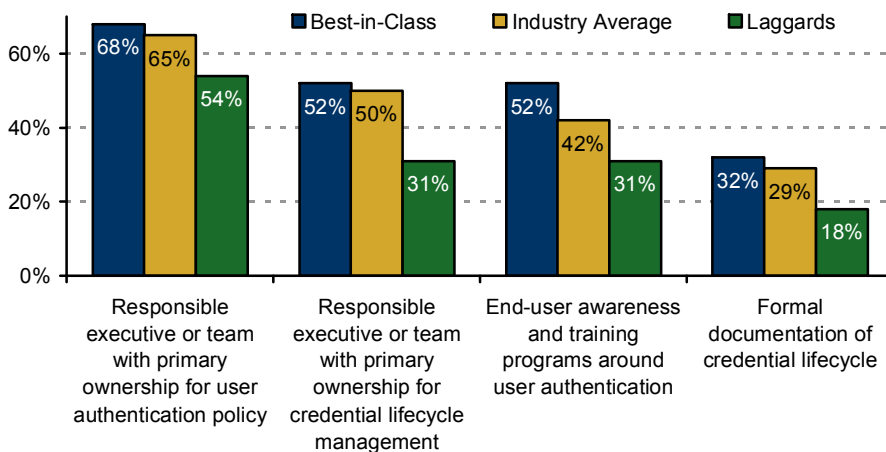
While top performers are 26% more likely than lagging performers to have clear ownership for user authentication *policy*, they are 68% more likely to have clear ownership for credential lifecycle *management* (Figure 8). This highlights one of the consistent themes seen across Aberdeen's recent research, in which the security team is typically responsible for establishing policy but is usually reliant upon the network and IT operations teams for implementation, management, and enforcement. Regardless of whether ownership for policy and ownership for execution are combined or separate, primary ownership of each by a responsible executive or team is strongly correlated with the achievement of top results. Surprisingly, however, only a third (32%) of the Best-in-Class indicated that they have formally documented all aspects of the credential lifecycle.

"The CSO, as quickly as he can, is trying to move all of the operational responsibility back to the CIO. He wants to keep all of the strategic activities, i.e., policy, but not the operational responsibility – that's back to IT."

~ IT Project Leader,
 Financial Services industry

End-user awareness and training around user authentication is also a distinguishing characteristic of Best-in-Class organizations, higher by a factor of 68% compared to Laggards. The consistent policies and processes established by top performers, as discussed earlier, certainly make it more straightforward to educate end-users on expected and acceptable behavior regarding authentication.

Figure 8: Organizational Ownership and End-User Awareness



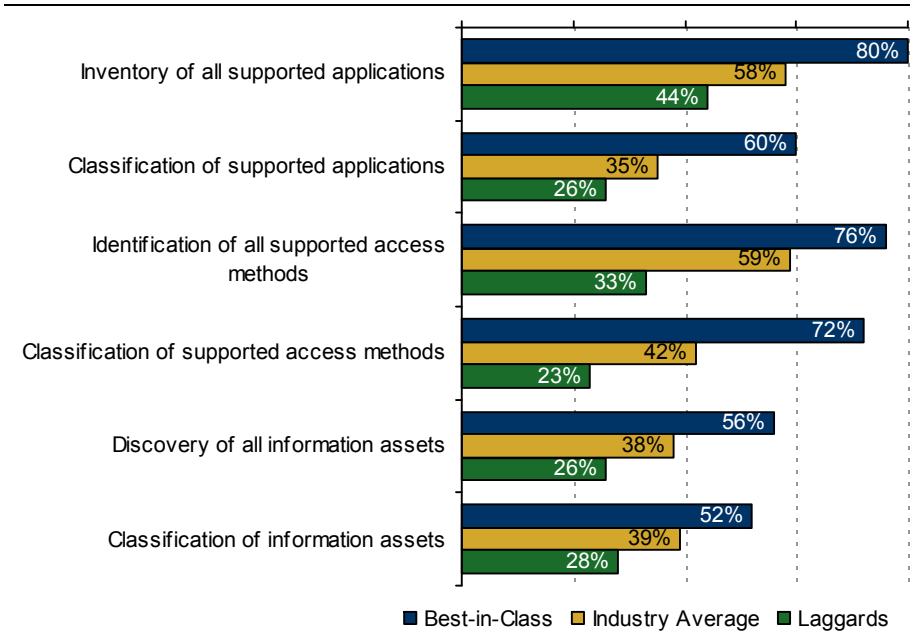
Source: Aberdeen Group, March 2008

Knowledge Management

As discussed earlier, Best-in-Class organizations are more likely to have developed consistent user authentication policies as a function of several important factors, including the type of information being accessed, the nature of the applications being accessed, and the method of access. Figure 9 illustrates the degree to which the Best-in-Class have identified and classified the information required to establish and enforce their authentication policies. The most challenging area – discovery and classification of information assets – tends to be discussed primarily in the

context of protecting against data loss, but as seen in Figure 9 it is also a distinguishing characteristic of top performance in user authentication. If the general principle is to invest in protecting only that which is worth protecting, then it is easy to see why identification and classification of data, applications, and access methods are foundational elements for establishing a sound and consistent user authentication policy.

Figure 9: Discovery and Classification as Prelude to Policy

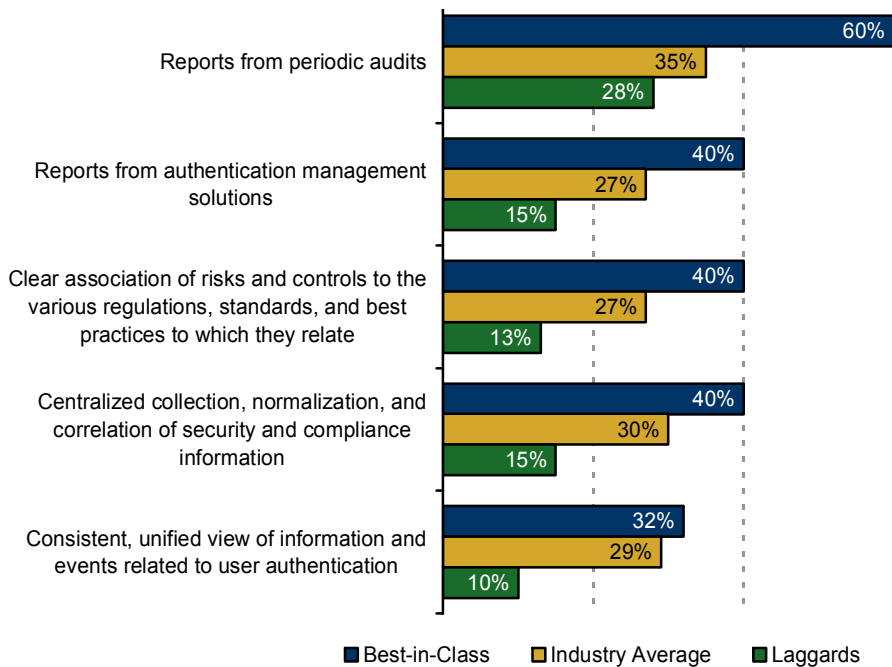


Source: Aberdeen Group, March 2008

Figure 10 provides interesting insights into post-deployment information that also helps to distinguish the top performers in managing user authentication. For example, Best-in-Class organizations are three-times better than Laggards at associating security risks and user authentication controls to the various regulations, standards, and best practices to which they relate. At just 40%, however, much improvement is still needed to keep pace with a complex and changing regulatory environment.

In addition, Figure 10 shows that Best-in-Class organizations are 50% more likely (60% versus 40%) to obtain user authentication reporting information from periodic *audits* than directly from their authentication management solutions, while only one-third (32%) indicate having a consistent, unified view of information and events related to user authentication. This indicates a strong opportunity for solutions providers to help their customers improve overall management visibility, both by improving the audit and reporting capabilities of their standalone authentication management solutions, and by improving the level of integration with centralized authentication "platforms" and / or security information and event management systems.

Figure 10: Reporting and Management Visibility, Post-Deployment



Source: Aberdeen Group, March 2008

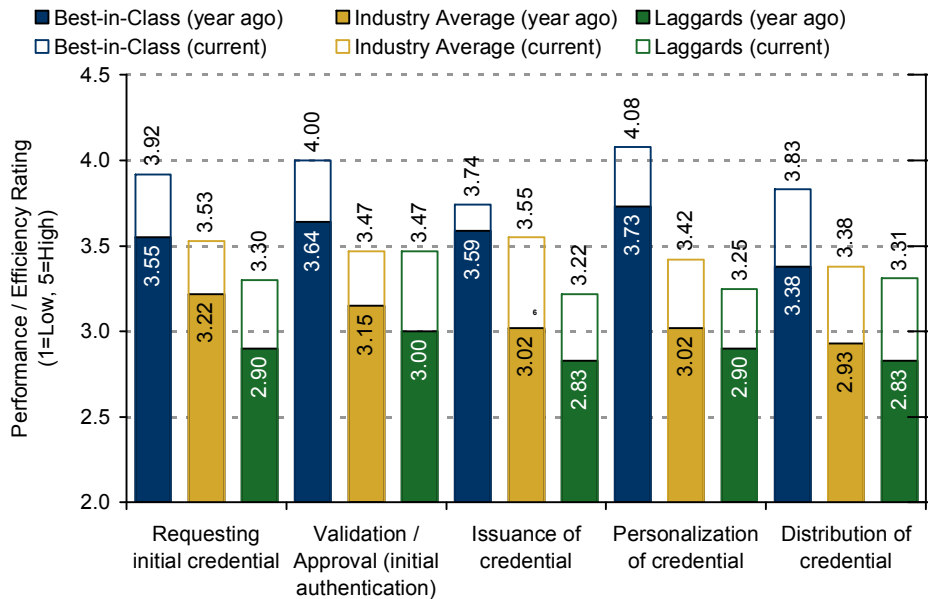
Technology

Independent of the user authentication method, Best-in-Class organizations excel relative to the other maturity classes in managing authentication credentials throughout most aspects of their natural lifecycle, which for purposes of this analysis are divided into the following categories:

- **Provisioning.** The initial request for credential; validation / approval (initial authentication of user identity); issuance; personalization; and distribution (Figure 11)
- **User support.** Emergency access (e.g., for forgotten, lost, or stolen credentials); user self-service (password reset); user self-service (other); and help desk support (Figure 12)
- **De-provisioning.** Replacement, renewal, suspension, and revocation of credentials (Figure 13)
- **Operations / management.** Ongoing (real-time) authentication; audit and reporting of credential usage (Figure 14)

Respondents in the study were asked to rank their performance / efficiency for each element of the credential lifecycle on a scale of 1 (lowest) to 5 (highest), both currently and for one year ago. Figure 11 through Figure 14 show the respective results for the four categories of provisioning, user support, de-provisioning, and operations / management.

Figure 11: Credential Lifecycle Management (Provisioning)



Source: Aberdeen Group, March 2008

Across these four high-level categories, the highest performance rating is in provisioning (Figure 11). In other words, companies feel that their level of performance and efficiency is highest in the up-front aspects of requesting, approving, issuing, personalizing, and distributing an authentication credential.

Fast Facts

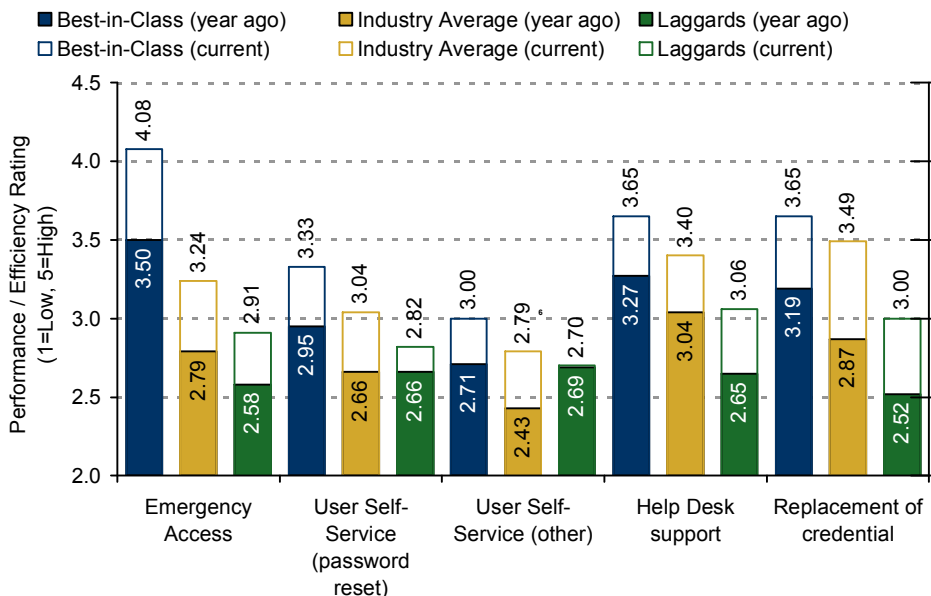
Percentage of password / PIN resets serviced in one hour or less:

- ✓ Best-in-Class 71%
- ✓ Industry Average 62%
- ✓ Laggards 47%

Percentage of emergency access requests serviced in one hour or less:

- ✓ Best-in-Class 65%
- ✓ Industry Average 46%
- ✓ Laggards 31%

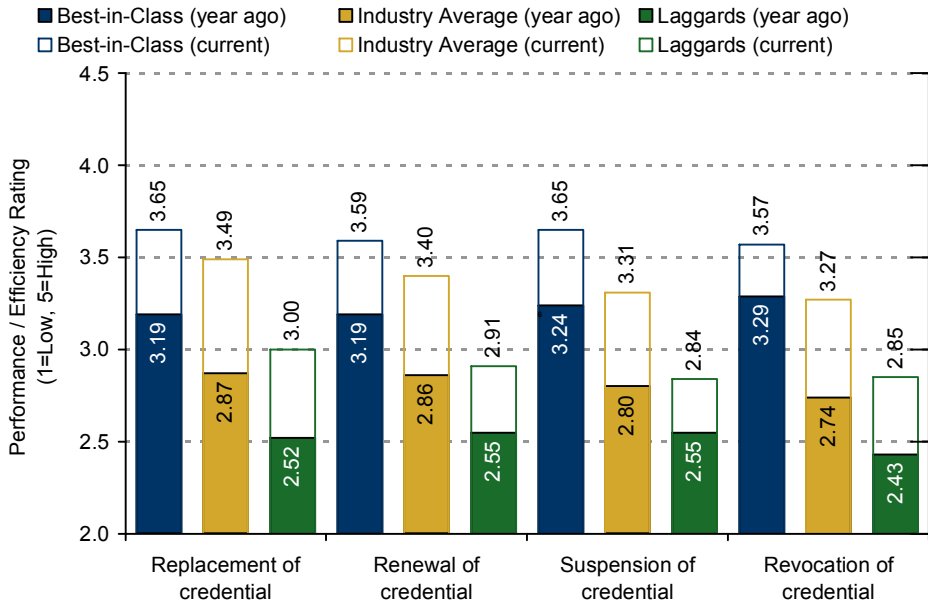
Figure 12: Credential Lifecycle Management (End-User Support)



Source: Aberdeen Group, March 2008

Contrast this to the second category, end-user support, where with the exception of emergency access, the average performance rating by the Best-in-Class is about 15% lower than for the provisioning category. Across the board, user self-service is clearly a major opportunity for operational improvement (Figure 12).

Figure 13: Credential Lifecycle Management (De-provisioning)



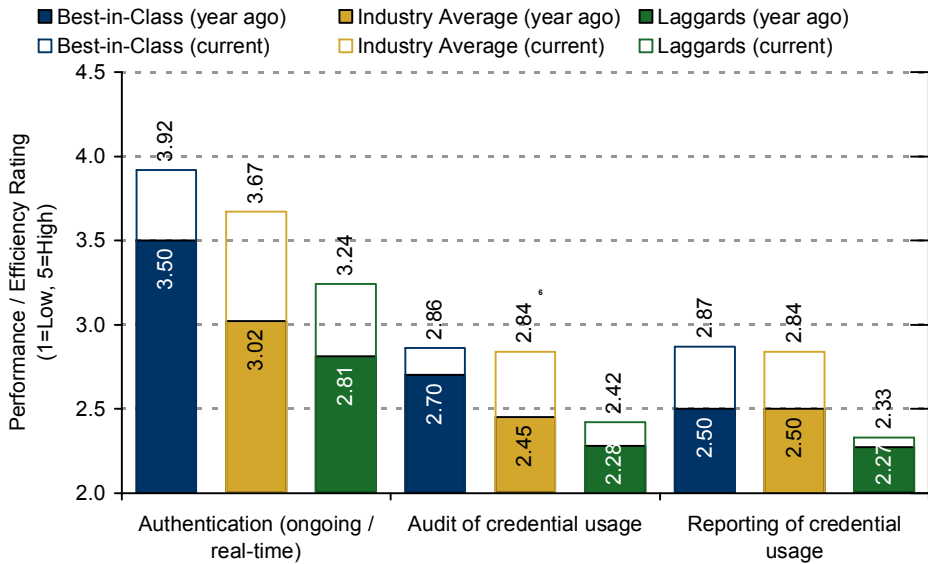
Source: Aberdeen Group, March 2008

Figure 13 shows the results for the de-provisioning category, i.e., the back-end of the credential lifecycle which includes the replacement, renewal, suspension, and revocation of user authentication credentials. On average, the Best-in-Class rate their current performance and efficiency at de-provisioning about 10% lower than that for provisioning. Anecdotal evidence for enterprise scenarios suggests that more attention is given to the front end of the lifecycle (incoming users) than to the back end (outgoing users) because IT resources are limited and "the squeakiest wheels always get the grease." Previous Aberdeen research has shown that both ends of the lifecycle have significant cost implications for poor performance, however. No one wants to keep on-boarding users sitting idle and unable to work or transact, but at the same time there are significant risks of access remaining open long after accounts have been "orphaned" due to employee turnover or customer defection.

Finally, Figure 14 shows the performance ratings for the operational and management aspects of credential lifecycle management. With respect to the ongoing / real-time aspects of authenticating users, the Best-in-Class reported high marks. As previously discussed, however, auditing and reporting of credential usage is a significant opportunity for operational

improvement, with the top performers rating their current performance at 27% lower than that for provisioning.

Figure 14: Credential Lifecycle Management (Operations / Mgmt)

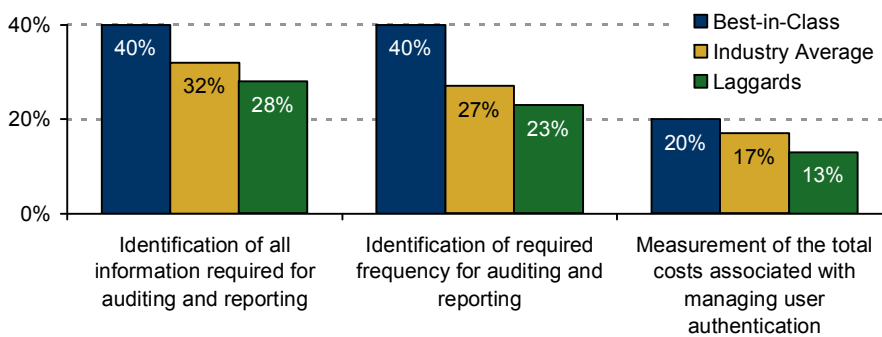


Source: Aberdeen Group, March 2008

Performance Management

Consistent with the preceding analysis and discussion, Best-in-Class organizations do a better job than their counterparts at identifying both the *content* and the *frequency* required for auditing and reporting, though at just 40% large improvements are possible (Figure 15). The most challenging aspect of managing performance for user authentication is in the area of measuring the total cost of ownership. Only one in five of Best-in-Class organizations in this study indicated measurement of the total cost of managing user authentication as a current capability. The implication is that companies have the strategic intent, but do not yet have the tools.

Figure 15: Performance Management



Source: Aberdeen Group, March 2008

A significant problem created by this last point is that absent any meaningful insight into the actual cost of deploying and managing user authentication solutions, many organizations default to acquisition cost alone for evaluating and selecting strong user authentication methods. This tends to favor the pointless perpetuation of passwords, which are "free" to acquire, but are costly in terms of management and productivity. Increased visibility into these real but hidden costs can help to support the business case for strong user authentication. In turn, strong user authentication helps to unlock the business benefits realized by the Best-in-Class organizations in this study, which include better security, sustained compliance, reduced human error, and lower total costs.

Aberdeen Insights — Technology

We have seen that the market presents organizations with a bountiful bouquet of alternatives for strong user authentication, each with its own unique balance of attributes. Marketing messages can sometimes take on a near-religious flavor, as specialist vendors promote the advantages of their own method or attack the disadvantages of an alternative method. The four high-level categories of TCO, fit for end-users, fit for the organization, and strategic fit provide a useful framework for comparing and contrasting one strong authentication method to another. Tradeoffs are, and will continue to be, the name of the game for their ultimate selection. The good news for buyers is that the general trend is towards continued variety, flexibility, and choice with respect to user authentication method.

Independent of which user authentication method(s) are deployed, however, Best-in-Class organizations have excelled relative to their Industry Average and Laggard counterparts at managing user authentication credentials throughout their natural lifecycle. In some cases, this will favor a more ecumenical, platform-oriented approach. Among the four high-level categories of provisioning, user support, de-provisioning, and operations / management, research shows that the best performance overall is currently in the front-end aspects of provisioning. The biggest opportunities for improvement are currently in the areas of end-user self-service, and management and reporting on credential usage.

Consistent policies for user authentication and authorization, along with clear accountability and ownership for both policy and credential lifecycle management, are the foundation for the results achieved by top performers. The overall context is to incorporate strong user authentication, where appropriate, to provide higher assurance for user identities as part of protecting information and managing risk.

Chapter Three: Recommended Actions

Whether a company is trying to move its performance in trusted computing from Laggard to Industry Average, or Industry Average to Best-in-Class, the following actions will help drive the necessary performance improvements:

Laggard Steps to Success

- **Lay the groundwork for policy.** Identification and classification of relevant information, applications, and access methods are foundational elements for establishing sound and consistent user authentication policies. Just over one-quarter of Laggards report such identification and classification as current capabilities.
- **Establish consistent policies for user authentication and access privileges.** Just one-third to one-half of Laggards currently report consistent policies in these areas. Policies should be a function of several factors, including the type of information being accessed, the nature of the applications being accessed, the method of access, and the profile of the end user populations.
- **Establish formal workflow for credential lifecycle management, starting with the provisioning of user authentication credentials.** Less than one in five Laggard organizations report having formal workflow to authorize the provisioning of new user authentication credentials – this is unacceptably lax for the root of assurance for user identities.

Industry Average Steps to Success

- **Lay the groundwork for policy.** Between 35% and 40% of Industry Average organizations reported current capabilities for identification and classification of information, applications, and access methods. Taking these steps establishes the foundation for establishing solid and consistent user authentication and authorization policies.
- **Establish consistent policies for user authentication and access privileges.** Between one-half and two-thirds of the Industry Average currently report having consistent policies in these areas, compared to up to three-quarters of Best-in-Class organizations. Having them in place will streamline the selection of specific strong user authentication solutions where they are most appropriate.
- **Be more proactive about user authentication management.** Only one-quarter of the Industry Average regularly review and analyze the audit and reporting data from their user authentication management systems, less than half the rate reported by the Best-in-Class. Merely having the information is necessary, but not sufficient, for achieving top results.

Fast Facts

Strong user authentication technologies currently deployed by Best-in-Class organizations in this study include:

- √ 56% one-time passwords (time-based)
- √ 28% digital certificates
- √ 28% fingerprint biometrics
- √ 24% converged logical / physical access cards

Best-in-Class Steps to Success

- **Lay the groundwork for policy.** Even the Best-in-Class organizations can improve with respect to the identification and classification of information, applications, and access methods. Just 50% to 60% of the Best-in-Class reported current capabilities in these areas.
- **Increase the accountability for both policy and management of user authentication.** More than two-thirds of Best-in-Class organizations have clear ownership for security policy, while slightly more than half have clear ownership for credential lifecycle management. Regardless of whether ownership for policy and ownership for execution are combined or separate on the org chart, primary ownership of each by a responsible executive or team is strongly correlated with the achievement of top results.
- **Improve visibility; measure total costs.** Only one in five of the Best-in-Class organizations in this study indicated measurement of the total cost of managing user authentication as a current capability. Increased visibility into the real, but hidden, management and support costs of existing authentication systems (including passwords) can help to support the business case for strong user authentication and higher assurance of identities.

Aberdeen Insights — Summary

The "right" strong user authentication is not something to make a decision about by listening to the loudest marketing messages, but instead by finding the unique balance of solution attributes and organizational attributes that make up the selection criteria for your use case and your organization. Providing higher assurance for identities through strong user authentication is an important element of protecting information and managing risk. It should be based on consistent policies for authentication and authorization, and there should be clear ownership for both policy and management of user authentication credentials over their lifecycle.

Two broad classes of solution providers will play important roles in strong user authentication. The first, "authentication specialists," will continue to innovate as they always have around specific methods. The second, "identity assurance platforms," will enable support and management for multiple methods from a common infrastructure. Organizations should look both to expand the deployment of strong user authentication and to improve credential lifecycle management for their unique environments.

Send to a Friend 

Appendix A: Research Methodology

In March 2008, Aberdeen examined the range of approaches currently being taken in the deployment of "strong" user authentication methods, i.e., methods other than traditional username and password. The experiences and intentions of nearly 150 organizations from a diverse set of industries are represented in this study. Aberdeen supplemented this online survey effort with interviews with select survey respondents, gathering additional information on user authentication strategies, experiences, and results.

Responding organizations had the following demographics:

- *Job title / function:* The research sample included respondents with the following job titles: C-level (23%); Vice President (5%); Director (19%); Manager (22%); Staff / Consultant (25%); and Other (6%). The largest segment by functional responsibility was IT, representing 48% of the sample.
- *Industry:* The research sample included respondents from a wide range of industries. The largest segments were financial (15%), high tech (24%), government / defense (5%), education (5%).
- *Geography:* A slight majority of respondents (51%) were from North America. Remaining respondents were from the Asia-Pacific region (16%) and Europe / Middle East / Africa (33%).
- *Company size:* Twenty-eight percent (28%) of respondents were from large enterprises (annual revenues above US \$1 billion); 28% were from midsize enterprises (annual revenues between \$50 million and \$1 billion); and 44% of respondents were from small businesses (annual revenues of \$50 million or less).

Solution providers recognized as sponsors were solicited after the fact and had no substantive influence on the direction of this report. Their sponsorship has made it possible for Aberdeen Group to make these findings available to readers at no charge.

Table 4: PACE Framework Key

| Overview |
|--|
| <p>Aberdeen applies a methodology to benchmark research that evaluates the business pressures, actions, capabilities, and enablers (PACE) that indicate corporate behavior in specific business processes. These terms are defined as follows:</p> <p>Pressures – external forces that impact an organization’s market position, competitiveness, or business operations (e.g., economic, political and regulatory, technology, changing customer preferences, competitive)</p> <p>Actions – the strategic approaches that an organization takes in response to industry pressures (e.g., align the corporate business model to leverage industry opportunities, such as product / service strategy, target markets, financial strategy, go-to-market, and sales strategy)</p> <p>Capabilities – the business process competencies required to execute corporate strategy (e.g., skilled people, brand, market positioning, viable products / services, ecosystem partners, financing)</p> <p>Enablers – the key functionality of technology solutions required to support the organization’s enabling business practices (e.g., development platform, applications, network connectivity, user interface, training and support, partner interfaces, data cleansing, and management)</p> |

Source: Aberdeen Group, March 2008

Table 5: Competitive Framework Key

| Overview | |
|--|---|
| <p>The Aberdeen Competitive Framework defines enterprises as falling into one of the following three levels of practices and performance:</p> <p>Best-in-Class (20%) – Practices that are the best currently being employed and are significantly superior to the Industry Average, and result in the top industry performance.</p> <p>Industry Average (50%) – Practices that represent the average or norm, and result in average industry performance.</p> <p>Laggards (30%) – Practices that are significantly behind the average of the industry, and result in below average performance.</p> | <p>In the following categories:</p> <p>Process – What is the scope of process standardization? What is the efficiency and effectiveness of this process?</p> <p>Organization – How is your company currently organized to manage and optimize this particular process?</p> <p>Knowledge – What visibility do you have into key data and intelligence required to manage this process?</p> <p>Technology – What level of automation have you used to support this process? How is this automation integrated and aligned?</p> <p>Performance – What do you measure? How frequently? What’s your actual performance?</p> |

Source: Aberdeen Group, March 2008

Table 6: Relationship Between PACE and the Competitive Framework

| PACE and the Competitive Framework – How They Interact |
|--|
| <p>Aberdeen research indicates that companies that identify the most influential pressures and take the most transformational and effective actions are most likely to achieve superior performance. The level of competitive performance that a company achieves is strongly determined by the PACE choices that they make and how well they execute those decisions.</p> |

Source: Aberdeen Group, March 2008

Appendix B: Related Aberdeen Research

Aberdeen research that forms a companion or reference to this benchmark report includes the following:

- [*Trusted Computing: Tune In, Turn It On*](#); February 2008
- [*Trusted Computing and User Authentication*](#); February 2008
- [*Logical / Physical Security Convergence: Is It in the Cards?*](#); December 2007
- [*Security Governance and Risk Management*](#); November 2007
- [*Sustaining Compliance*](#); September 2007

Information on these and any other Aberdeen publications can be found at www.Aberdeen.com.

Author: Derek E. Brink, Vice President and Research Director, IT Security,
Derek.Brink@aberdeen.com

Since 1988, Aberdeen's research has been helping corporations worldwide become Best-in-Class. Having benchmarked the performance of more than 644,000 companies, Aberdeen is uniquely positioned to provide organizations with the facts that matter — the facts that enable companies to get ahead and drive results. That's why our research is relied on by more than 2.2 million readers in over 40 countries, 90% of the Fortune 1,000, and 93% of the Technology 500.

As a Harte-Hanks Company, Aberdeen plays a key role of putting content in context for the global direct and targeted marketing company. Aberdeen's analytical and independent view of the "customer optimization" process of Harte-Hanks (Information – Opportunity – Insight – Engagement – Interaction) extends the client value and accentuates the strategic role Harte-Hanks brings to the market. For additional information, visit Aberdeen <http://www.aberdeen.com> or call (617) 723-7890, or to learn more about Harte-Hanks, call (800) 456-9748 or go to <http://www.harte-hanks.com>

This document is the result of primary research performed by Aberdeen Group. Aberdeen Group's methodologies provide for objective fact-based research and represent the best analysis available at the time of publication. Unless otherwise noted, the entire contents of this publication are copyrighted by Aberdeen Group, Inc. and may not be reproduced, distributed, archived, or transmitted in any form or by any means without prior written consent by Aberdeen Group, Inc.

010908a