

Forrester Consulting

MAKING LEADERS SUCCESSFUL EVERY DAY

March 20, 2009

Authentication-As-A-Service

A commissioned study conducted by Forrester Consulting on behalf of VeriSign

FORRESTER®



Headquarters

Forrester Research, Inc., 400 Technology Square, Cambridge, MA 02139 USA
Tel: +1 617.613.6000 • Fax: +1 617.613.5000 • www.forrester.com

TABLE OF CONTENTS

Executive Summary	3
Key Findings	3
What Is Consumer Two-Factor Authentication And How Does It Relate To Trust?	4
Authentication-As-A-Service Provides Security In The Cloud	4
Authentication Is Key To Customer Trust	5
Mounting Pressures On Current Authentication Processes	5
Exploring Authentication-As-A-Service.....	8
Businesses Expect Benefits From Authentication-As-A-Service	9
The Authentication-As-A-Service Decision-Making Process	10
Expediting AaaS Adoption In Your Organization	12
Appendix A: Research Methodology	13
Appendix B: Related Forrester Research.....	13

© 2009, Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. For additional information, go to www.forrester.com.

Executive Summary

A user name and password have traditionally been used to authenticate Web users, either to log them onto an application or grant them access to a resource. This approach provides a relatively low level of trust for consumers: Passwords can be easy to guess, too short, and difficult to manage. Adding a second factor credential (typically a one-time password or security code on a credential such as hardware tokens/cards, mobile phones, etc.) to the authentication process helps to address these challenges with passwords. Commonly referred to as two-factor authentication (2FA), 2FA adds additional security to authentication and represents a higher level of trust between consumers and online businesses.

One 2FA solution is authentication-as-a-service (AaaS). AaaS is an Internet-based service that offers an on-demand verification of one-time password tokens to consumers and businesses.

To understand the market context of authentication-as-a-service, VeriSign commissioned Forrester Consulting to evaluate the current approaches to authentication, the challenges companies face in regards to authentication, and their perceptions of AaaS.

Key Findings

In conducting in-depth online surveys with 324 global IT security decision-makers in November and December 2008, Forrester found that:

- **Authentication is a key to gaining customer trust, although providing secure authentication is a daunting process.** Businesses are faced with a large volume of Web site hits for which authentication is necessary. Seventy percent of those surveyed report that their current authentication methods directly influence their customers' perception of trust. Needing to provide secure authentication in an environment with increasing regulations, rising online fraud, and escalating costs creates challenges for companies that see customer trust as a business priority.
- **Authentication-as-a-service offers many benefits to these organizations.** Companies are interested in AaaS, and expect benefits related to improved reliability, reduced fraud, and reduced identify theft. Companies also felt that AaaS could offer improved scalability.
- **Companies understand that upgrades are necessary to provide truly secure authentication and are exploring authentication-as-a-service.** Seventy-five percent of organizations surveyed have budgeted for or are considering an upgrade to their current authentication process or technology within the next year. The survey also found that many line-of-business owners and C-level executives will be involved with this decision-making process. Given their focus on maintaining customer trust, it is not surprising that these business managers will be most interested in the level of customer privacy and the reputation of the service provider.
- **Companies are concerned about the costs of authentication-as-a-service.** In these difficult economic times, it's understandable that the flag is dropped at the mention of purchasing new technologies or services. To understand the actual value, it's important to create a cost model that looks at the cost of handling authentication in-house compared with "as a service". This business case will be necessary to convince executive stakeholders that AaaS is a credible, viable solution to the authentication problem.

What Is Consumer Two-Factor Authentication And How Does It Relate To Trust?

When authenticating customers on their Web sites, businesses have traditionally used the user name and password combination with which we are all familiar. Unfortunately this approach provides a relatively low level of security for consumers: Passwords can be easy to guess, too short, and difficult to manage. These challenges with passwords are well-known to consumers and lead to a lower level of trust among online customers. Adding a second factor, e.g., combining what a user knows (user name/password) with what he has (typically a one-time password or security code on a credential such as hardware token, mobile phone, etc.) to the authentication process can help to address these issues. Commonly referred to as two-factor authentication (2FA), 2FA adds additional security to authentication and raises the level of trust between consumers and online businesses.

Various organizations, such as retail and investment banks, retailers, and others have implemented 2FA using hardware or software credentials that generates a one-time password, or by generating the one-time password through a non-Web channel (typically a short text message to a mobile phone). The validation of the second factor can be done either in-premise or over the cloud. Some of the challenges of in-premise validations are the high cost of capital expenditure to source the hardware needed, issues with reliability and scalability, and lastly, the time needed to implement such a solution.

Outsourcing 2FA authentication can help address the above challenges in the following ways:

- Organizations do not need to invest in building and operating a 2FA authentication infrastructure, which is especially enticing for small and mid-sized businesses.
- Reliability and scalability of the service is the responsibility of the trusted provider.
- Quick time-to-market.
- Outsourcing 2FA converts the capital expenditure to an operational expenditure, which is a significant value proposition in a down economy.

Authentication-As-A-Service Provides Security In The Cloud

One 2FA solution is authentication-as-a-service (AaaS). AaaS is an Internet-based service that offers an on-demand verification of the second factor to consumers and businesses. It relies on two-factor authentication that is offered on-demand from an “in the cloud” provider to seamlessly authenticate online customers.

Authentication-as-a-service has the benefit of improving reliability for organizations that currently rely on internal systems that may experience downtime or slow response times. It also helps to quickly market the solutions and reduces costs for providing the service by converting CAPEX to OPEX.

With all of these benefits, moving to authentication-as-a-service would require a change in how enterprises approach their authentication strategy. To better understand global businesses' current

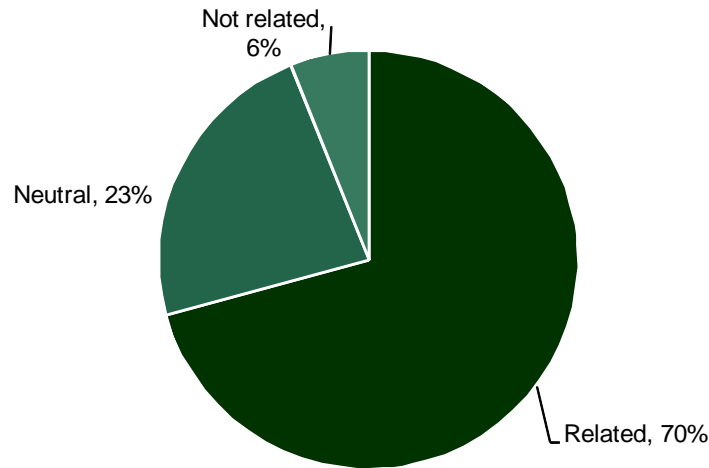
approaches to authentication and their perceptions of authentication-as-a-service, VeriSign commissioned a survey conducted by Forrester Consulting of 324 global IT security decision-makers. This paper provides an overview of the findings of this research.

Authentication Is Key To Customer Trust

In this survey of 324 global IT security decision-makers, 70% reported that their current authentication methods are related to their customers' degree of trust in their offerings (see Figure 1). Eighty percent of respondents said that line-of-business managers believe that the establishment and retention of customer trust is a business requirement. Given the importance placed on securing trust, it is not surprising that 60% of those surveyed reported that this objective was supported with a specific technology or policy implementation. These investments included everything from: "[A] more user friendly and robust front-end application," to "New server, and overhaul of databases," and "Customer education and usage safety ethics," as well as "Easier-to-use authentication processes."

Figure 1: Authentication Drives Customer Trust

"How strongly do you believe that your current customer authentication methods are related to your customers' degree of trust in the security of your offering?"



Base: 324 global IT security decision-makers
(percentages do not total 100 due to rounding)

Source: "Authentication As-A-Service Study," a commissioned study conducted by Forrester Consulting on behalf of VeriSign, December 2008

Mounting Pressures On Current Authentication Processes

Despite its importance in maintaining customer trust, authentication is a challenge that confronts the majority of businesses that have an online presence. According to our survey, more than 80% of respondents reported that at least half of their Web site users need to be authenticated. With 59% of respondents receiving at least 500 customer visits daily, the volume of authentication is daunting.

Traditional approaches to this online customer authentication process require each enterprise to independently establish an acceptable level of trust between the customer and the enterprise and then provide and manage a method to invoke that trust relationship online on demand. Nearly two-thirds (65%) of those surveyed rely on security to maintain a database of customer information to support this verification process. However, this approach is being squeezed by:

- Escalating online fraud.** More than half of respondents (52%) agreed that online fraud due to customer authentication issues is a challenge. Among German respondents, 64% believed this was true for their enterprises. Nearly a quarter (24%) of respondents reported that their current method of authentication is inadequate in reducing fraud. Given the increasing consumer sophistication, it is not surprising that organizations are focused on making sure their customers feel secure transacting with them online.
- Increasing costs of authentication.** One of the obstacles reported by nearly half (48%) of survey respondents is the cost of administering the authentication system (see Figure 2). An additional 41% of respondents were concerned about the cost of deploying additional authentication factors. In the US, these costs are an even greater concern, with 52% citing this as a challenge. Most organizations consider the expenses associated with deploying and administering their identity management systems as the cost of doing business, but the investment level is becoming a concern for many organizations.
- Growing regulatory burdens.** Sixty-eight percent of survey respondents reported that transborder regulations affect their authentication process (see Figure 3). This is true in all global regions, but especially in Germany, where 80% of respondents are affected. These concerns are likely to grow, with 62% of all respondents agreeing that government regulation is expected to require stronger authentication in the future.

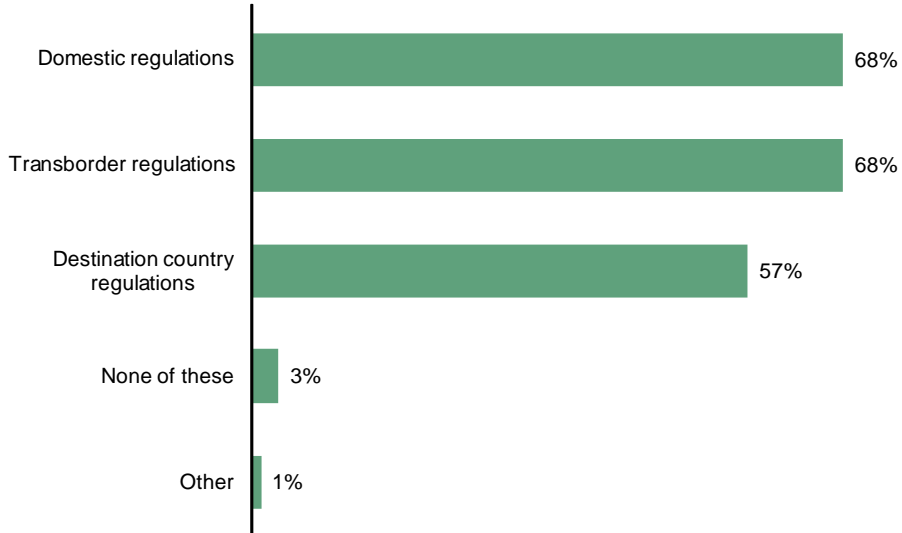
Figure 2: Cost Of System Administration Is The Greatest Challenge Enterprises Face



Base: 324 global IT security decision-makers (multiple responses accepted)

Source: “Authentication-As-A-Service Study,” a commissioned study conducted by Forrester Consulting on behalf of VeriSign, December 2008

Figure 3: Most Respondents Are Affected By International Authentication Regulations
“Which of the following types of regulations affect your organization’s approach to Web site authentication? Please select all that apply.”



Base: 324 global IT security decision-makers
(multiple responses accepted)

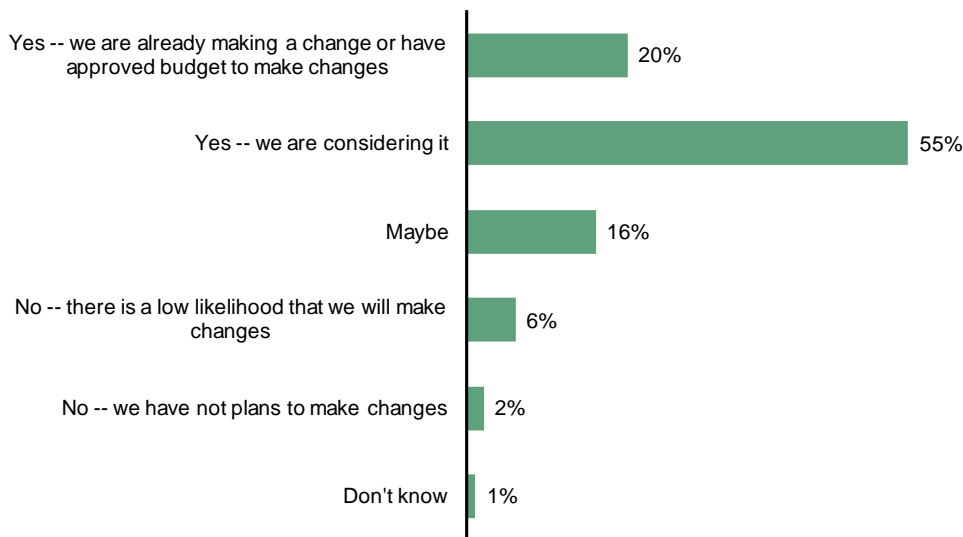
Source: “Authentication-As-A-Service Study,” a commissioned study conducted by Forrester Consulting on behalf of VeriSign, December 2008

Exploring Authentication-As-A-Service

With this business focus on customer trust and increasing authentication challenges, it's not surprising that 75% of respondents have either budgeted for or are considering an upgrade to their Web site authentication process or technology over the next 12 months (see Figure 4).

Figure 4: Three-Quarters Of Respondents Are Planning Or Considering Authentication Changes

“Does your organization plan to change or upgrade its Web site authentication process or technology over the next 12 months?”



Base: 324 global IT security decision-makers

Source: “Authentication-As-A-Service Study,” a commissioned study conducted by Forrester Consulting on behalf of VeriSign, December 2008

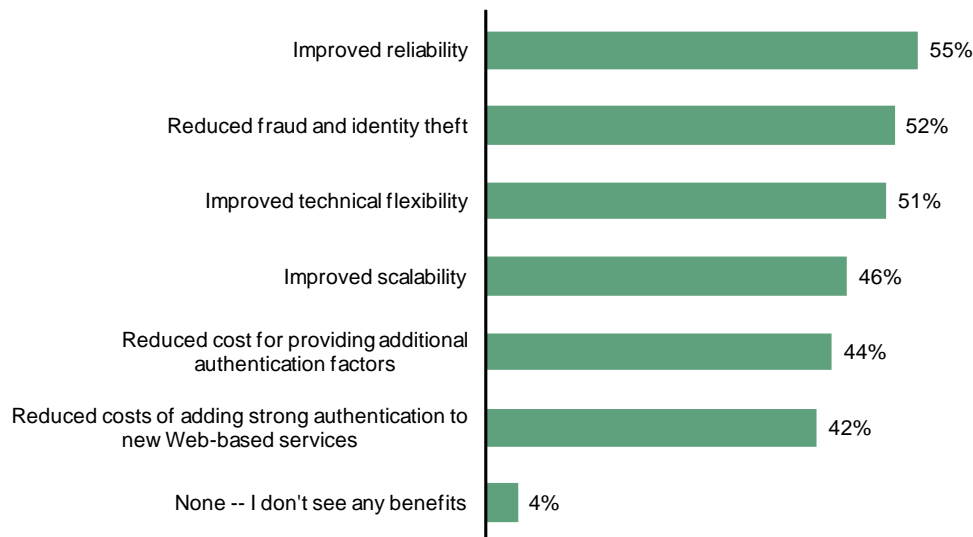
Businesses Expect Benefits From Authentication-As-A-Service

Nearly three-quarters (72%) of global respondents expressed an interest in authentication-as-a-service. IT decision-makers in the emerging markets of India and Brazil were the most interested in AaaS at 86% and 79%, respectively, while just over half of respondents from the UK (52%) indicated interest in AaaS.

Those surveyed cited improved reliability and reduced fraud and identity theft as the primary benefits they would expect to accrue for their organizations (see Figure 5). Seventy-one percent of those surveyed in India anticipated better reliability. In addition, many respondents (46%) expected to benefit from improved scalability. In fact, 55% of respondents agreed that authentication-as-a-service sounded much more economically and operationally scalable than internally managed customer authentication.

Figure 5: Improved Reliability Leads The List Of Benefits

“Thinking about authentication-as-a-service, what are some of the benefits that you could foresee for your organization?”



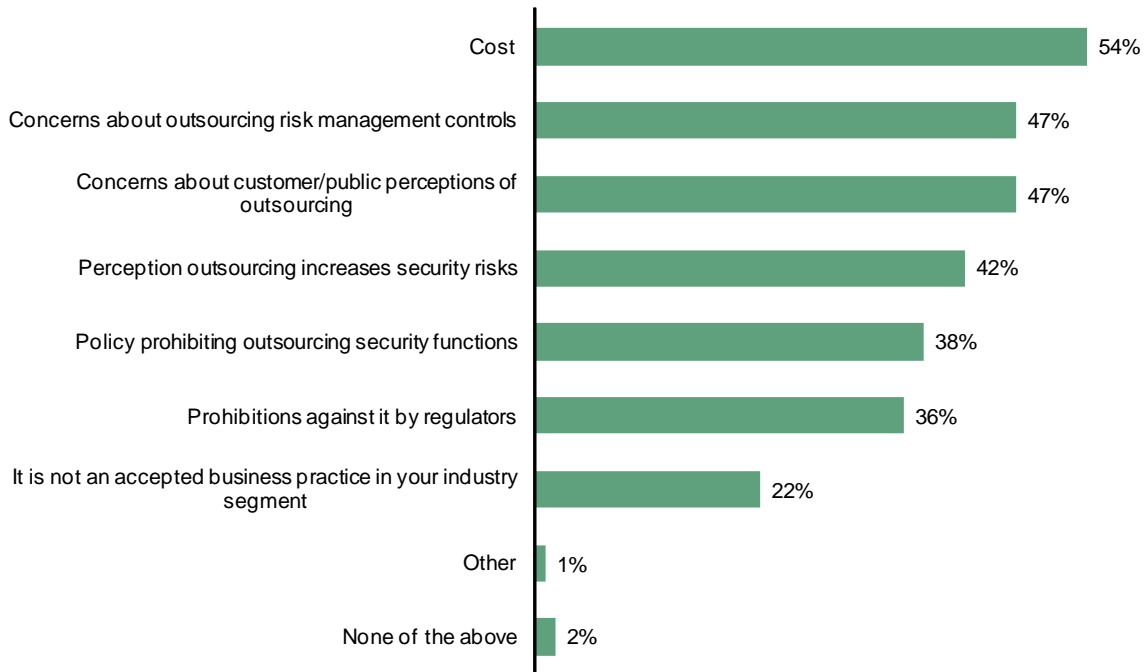
Base: 324 global IT security decision-makers
(multiple responses accepted)

Source: “Authentication-As-A-Service Study,” a commissioned study conducted by Forrester Consulting on behalf of VeriSign, December 2008

The major concerns expressed about adopting authentication-as-a-service centered on cost (see Figure 6). This hesitation is understandable, given the current economic climate — any new technology investments are heavily scrutinized to ensure a quick return. Respondents also expressed concern about the idea of outsourcing such vital risk management controls. This was coupled with a wariness of how consumers would perceive the security of an outsourced service versus an internally managed one. Fifty-nine percent of Indian respondents said that the number of participating customers was a concern. Seventy-four percent of UK respondents were concerned about policies prohibiting outsourcing.

Figure 6: Cost And Perceptions Of Outsourcing Are The Leading Concerns About AaaS

“Which of the following would be major considerations when making a decision whether to use authentication-as-a-service?”



Base: 324 global IT security decision-makers (multiple responses accepted)

Source: “Authentication-As-A-Service Study,” a commissioned study conducted by Forrester Consulting on behalf of VeriSign, December 2008

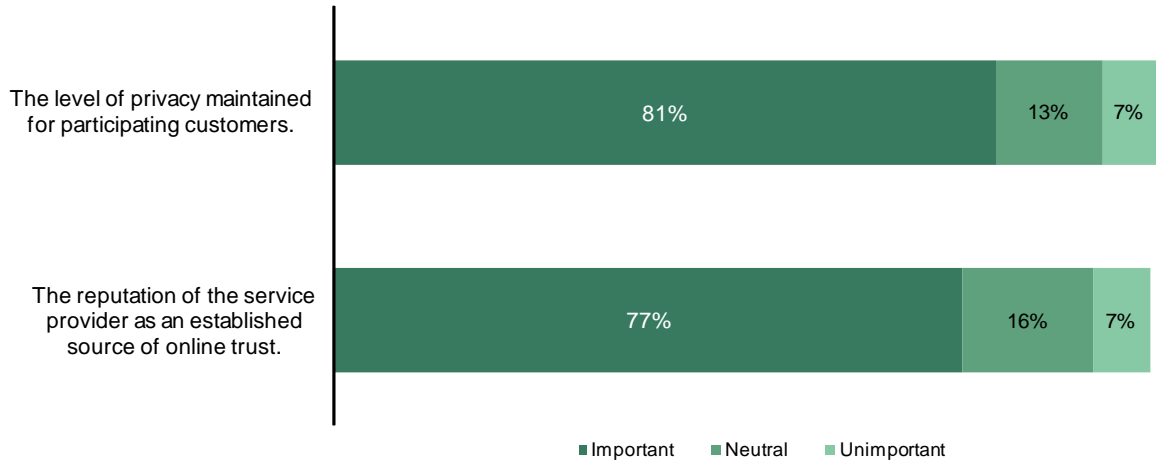
The Authentication-As-A-Service Decision-Making Process

As with most technology decisions, the managers involved in the decision of whether to adopt AaaS include the head of IT (69%) and the head of IT security (45%). But 44% of the global survey respondents indicated that the final decision about whether to implement AaaS rests with a non-IT executive — either a business decision-maker outside of IT (16%) or C-level executives outside of IT (28%). Given the business focus on authentication as a key link in the chain of customer trust, it is not surprising that line-of-business owners and C-level executives would place a priority on evaluating changes to these technologies and processes.

When asked how these executives would evaluate the usefulness of AaaS for their organizations, the survey respondents reported that the level of customer privacy and the reputation of the service provider would be important (see Figure 7). Both of these elements are essential to securing and maintaining customer trust and would be vital for companies considering using an outside service for this functionality.

Figure 7: Customer Privacy And Service Provider Reputation Are The Keys To Success

“Please rate the importance of each of the following factors in a decision to adopt authentication-as-a-service.”



Base: 324 global IT security decision-makers
(percentages do not total 100 due to rounding)

Source: “Authentication-As-A-Service-Study,” a commissioned study conducted by Forrester Consulting on behalf of VeriSign, December 2008

Expediting AaaS Adoption In Your Organization

Given the benefits that many global IT security decision-makers see in turning to authentication-as-a-service, it is worthwhile to explore steps that organizations can take to move toward AaaS.

Forrester recommends that organizations that are considering this transition:

- **Look for a trusted name in an AaaS provider.** Since authentication is part of your organization's mission-critical infrastructure, it is very important to look only at AaaS providers with proven trusted business models, security, and SLA track records. Using a trusted provider of AaaS is important: 70% of the business decision-makers in our survey indicated that superior authentication is strongly related to the trust of their customers in the company — and thus ultimately, their business success. This is important based on respondents' strong agreement with the requirement that the AaaS provider should be an established and trusted provider of online trust.
- **Standardize on security — in a framework outside of applications.** Many organizations spend a lot of effort on maintaining applications, each with its own security model (different user IDs, passwords, password policies, and password reset features). This model is not only expensive, but it also demands a lot of bandwidth from application developers. Forrester found that organizations that move to a standard, centralized authentication framework (e.g., Web single sign-on, etc.) and integrate AaaS with the model are in a position to produce a greater return on AaaS.
- **Work with business SaaS providers to adopt AaaS.** Software-as-a-service business applications are usually easier to integrate into an AaaS model, as they are technically segregated from the IT organization's in-house hosted applications and represent a smaller integration challenge. In many cases, SaaS providers already accept AaaS, which makes integration easier. This reduces the cost of implementing 2FA, since some of the costs related to 2FA are borne by the SaaS provider. The SaaS provider can also use AaaS to accept 2FA authentication from other clients thus enhancing security in their application.
- **Create a comparative cost model.** Business justification in times of an economic downturn is a key to convince executive stakeholders about the credibility of AaaS. IT buyers need to create parallel cost models for procuring and operating authentication systems in-house versus using AaaS. Cost items related to an in-house authentication system should include licenses, maintenance, operations (to maintain required service levels), hardware, and all costs around managing tokens: procurement, provisioning, distribution, and exception process management. On the other hand, AaaS costs include initial setup and integration, fixed monthly fees, and per-authentication transaction costs.

Appendix A: Research Methodology

In this study, Forrester conducted an online survey of 324 decision-makers in the United States, Brazil, Germany, India, and the UK to evaluate current approaches to authentication, the challenges companies face in regards to authentication, and their perceptions of AaaS. Survey participants included managers who are personally involved in decisions related enterprise security solutions. Respondents represented a mix of industries with a focus on public sector, media entertainment, healthcare, financial services, eCommerce (retail). Respondents were offered a monetary incentive or a prize as a thank you for time spent on the survey. The study began in November 2008 and was completed in December 2008.

Appendix B: Related Forrester Research

“Identity And Access Management Mitigates Risks During Economic Uncertainty: Using Identity And Access Management To Protect Your Business” by Andras Cser, January 26, 2009

“Market Overview: Strong Authentication For Enterprises In 2008: Securing The Doors To Your IT Environment” by Bill Nagel, July 16, 2008

“Countering Online Fraud Globally: Strategies For Breaking Free Of The Cat And Mouse Game” by Geoffrey Turner, February 20, 2008

“Mobile Authentication Marries Security With Convenience: A Token-Killing Form Factor For Secure Consumer Online Banking” by Bill Nagel, November 16, 2007