G00231072

Magic Quadrant for User Authentication

Published: 7 March 2013

Analyst(s): Ant Allan

The user authentication market is dominated by well-established, wide-focus vendors. Newer wide- and tight-focus vendors continue to offer enterprises sound alternatives across a range of use cases. The Nexus of Forces will shape the market in the midterm.

Strategic Planning Assumptions

By 2017, more than 50% of enterprises will choose cloud-based services as the delivery option for new or refreshed user authentication implementations — up from less than 10% today.

By year-end 2016, more than 30% of enterprises will use contextual authentication for workforce remote access — up from less than 2% today.

Market Definition/Description

A provider in the user authentication market delivers on-premises software/hardware or a cloud-based service that makes real-time authentication decisions for users using any of a variety of endpoint devices (that is, not just Windows PCs) to access one or more applications, systems or services in a variety of use cases. Where appropriate to the authentication methods supported, a provider in the user authentication market also delivers client-side software or hardware used by end users in those real-time authentication decisions.

This market definition does not include providers that deliver only one or more of the following:

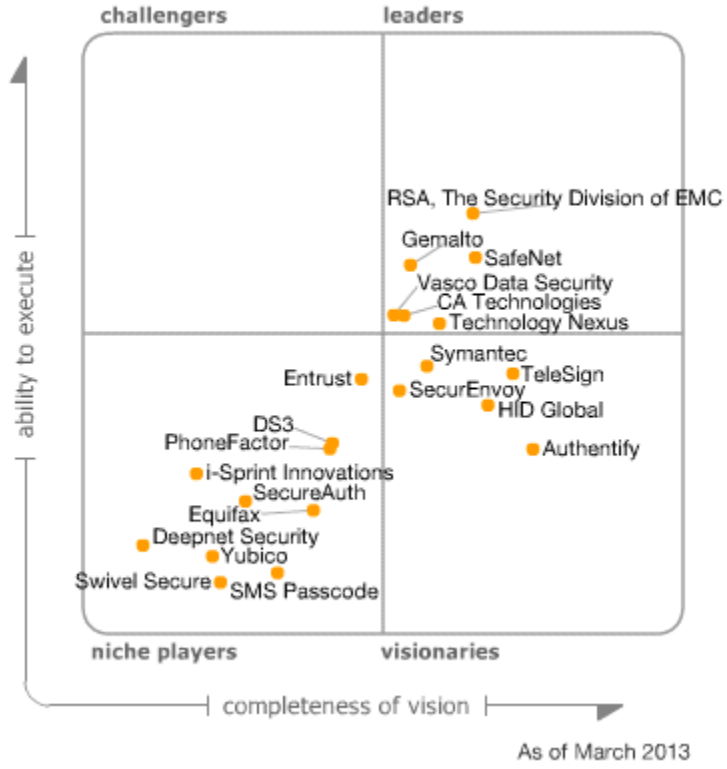
1. Client-side software or hardware, such as PC middleware, smart cards and biometric capture devices (sensors)
2. Software, hardware or a service, such as Web access management (WAM) or Web fraud detection (WFD), that makes a real-time access decision and may interact with discrete third-party user authentication platforms (for example, to provide "step up" authentication)
3. Credential management tools, such as password management tools, card management (CM) tools and public-key infrastructure (PKI) certification authority (CA) and registration authority (RA) tools (including OCSP responders)

4. Software, hardware or services in other markets, such as WAM or VPN, that embed native support for one or many authentication methods

A provider in the user authentication market may, of course, deliver one or more such offerings as part of, or in addition to, its user authentication offering. Note, however, that, for the purposes of this Magic Quadrant, offerings of Types 2, 3 and 4 are not considered to be "user authentication" offerings, and are not included in customer, end-user or revenue figures.

Magic Quadrant

Figure 1. Magic Quadrant for User Authentication



Source: Gartner (March 2013)

Gartner sees user authentication vendors falling into four categories with somewhat indistinct and overlapping boundaries:

1. **Specialist vendors:** A specialist user authentication vendor focuses on a distinctive proprietary authentication method — a unique method or a proprietary instantiation of a common method — and also offers a corresponding infrastructure or a software development kit (SDK) that will allow it to plug into customers' applications or other vendors' extensible infrastructures.

2. **Commodity vendors:** These vendors focus on one or a few well-established authentication methods, such as one-time password (OTP) tokens (hardware or software) and out of band (OOB) authentication methods. A commodity vendor may provide a basic infrastructure to support only those few methods; it will compete on price rather than functionality; and its offerings will primarily interest small or midsize businesses (SMBs) and some small enterprises that still have narrower needs.
3. **Tight-focus vendors:** These are commodity vendors that provide a robust, scalable infrastructure that can meet the needs of larger enterprises and global service providers — and sometimes augment other vendors' portfolios — and that compete primarily on functionality rather than price.
4. **Wide-focus (formerly broad-portfolio) vendors:** The defining characteristic of these vendors is that they offer or support many distinct authentication methods — and, again, compete primarily on functionality rather than price. They will typically offer a versatile, extensible authentication infrastructure that can support a wider range of methods than they offer, which may be sourced through OEM agreements with one or more other vendors in any of these categories, or be left to the enterprise to source directly from those vendors.

The vendors included in this Magic Quadrant fall into the latter two categories, and any vendor may also be a specialist vendor (that is, it may have some unique intellectual property among its portfolios).

The sizes of the vendors included, in terms of numbers of customers and numbers of end users, vary by orders of magnitude. In the Vendor Strengths and Cautions section below, we call out vendors that fall into the following highest and lowest tiers, according to the following order-of-magnitude scheme — "O(N)" should be read as "having the order of magnitude characterized by N":

Number of customers (N):

- Lowest tier:
  - O(100): $56 < N \leq 178$
  - O(320): $178 < N \leq 560$
- Median tier:
  - O(1,000): $560 < N \leq 1{,}780$
  - O(3,200): $1{,}780 < N \leq 5{,}600$
- Highest tier:
  - O(10,000): $5{,}600 < N \leq 17{,}800$
  - O(32,000): $17{,}800 < N \leq 56{,}000$
  - $N > 56{,}000$

Number of end users (N, in millions):

- Lowest tier:
  - O(1): $N \leq 1.78$
  - O(3.2): $1.78 < N \leq 5.6$
- Median tier:
  - O(10): $5.6 < N \leq 17.8$
  - O(32): $17.8 < N \leq 56$
- Highest tier:
  - O(100): $56 < N \leq 178$
  - O(320): $178 < N \leq 560$
  - $N > 560$

Market Size

Gartner's estimate of revenue across all segments of the authentication market for 2012 remains approximately $2 billion. However, the margin of error in this estimate is high, because not all the vendors included in this Magic Quadrant provided revenue data, and because of the "long tail" of the approximately 200 authentication vendors not included in it. Individual vendors included in this Magic Quadrant that did provide revenue data reported year-over-year revenue growth in the range 10% to 150%, with the median being approximately 25% growth. Of those vendors that provided customer numbers, growth was in the range 10% to 300%, with the median being approximately 40% growth.

We estimate the overall customer growth in the market to be approximately 30% year over year. Because of the continued shift toward lower-cost authentication solutions, we estimate the overall revenue growth to be approximately only 15%.

Range of Authentication Methods

Enterprise interest in OTP methods, broadly defined, remains high, with phone-as-a-token methods dominating traditional hardware tokens in new and refreshed deployments (although hardware tokens still have the larger installed base). Wide-focus user authentication vendors offer these and more, and also generally offer or support knowledge-based authentication (KBA) methods or X.509 tokens (such as smart cards). Most of the tight-focus vendors offer just phone-as-a-token methods, especially OOB authentication methods (sometimes incorporating biometric voice recognition as an option), with a few vendors (none of which are included in this Magic Quadrant) offering only KBA or biometric authentication methods.

The vendors included in this Magic Quadrant may offer any of a variety of methods across a range of categories (see "A Taxonomy of Authentication Methods, Update" [Note: This document has been archived; some of its content may not reflect current conditions]). These categories — and,

where appropriate, the corresponding categories from the National Institute of Standards and Technology (NIST) Special Publication 800-63-1 "Electronic Authentication Guideline" (December 2011) — are:

- **Lexical KBA (NIST: "preregistered knowledge token"):** This approach combines improved password methods and Q&A methods. An improved password method allows a user to continue using a familiar password, but provides more secure ways of entering the password or generating unique authentication information from the password. A Q&A method prompts the user to answer one or more questions, with the answers preregistered or based on on-hand workforce or customer data, or on aggregated life history information.
- **Graphical KBA (no corresponding NIST category):** Graphical KBA uses pattern-based OTP methods and image-based methods. A pattern-based OTP method asks the user to remember a fixed, arbitrary pattern of cells in an on-screen grid that is randomly populated for each login, and to construct an OTP from numbers assigned to those cells. An image-based method asks the user to remember a set of images or categories of images, and to identify the appropriate images from random arrays presented at login.
- **OTP token (NIST: "multifactor OTP hardware token," "single-factor OTP token" and "look-up secret token"):** This authentication method uses a specialized device or software application for an existing device, such as a smartphone, that generates an OTP — either continuously (time-synchronous) or on demand (event-synchronous) — which the user enters at login. The token may incorporate a PIN or be used in conjunction with a simple password. This category also includes transaction number (TAN) lists and grid cards for "generating" OTPs. Note that the "OTP" category does not include "OTP by SMS" or similar methods, which Gartner classifies as OOB authentication methods (see below). One of several algorithms may be used:
  - American National Standards Institute (ANSI) X9.9 (time- or event-synchronous, or challenge-response)
  - Initiative for Open Authentication (OATH) HMAC-based OTP (HOTP), time-based OTP (TOTP) or OATH Challenge-Response Algorithms (OCRAs)
  - Europay, MasterCard and Visa (EMV); MasterCard Chip Authentication Program (CAP); or Visa Dynamic Passcode Authentication (DPA), which is also called remote chip authentication (RCA)
  - A proprietary algorithm
- **X.509 token (NIST: "multifactor hardware cryptographic token," "multifactor software cryptographic token" and "single-factor cryptographic token"):** This X.509 PKI-based method uses a specialized hardware device, such as a smart card, or software that holds public-key credentials (keys or certificates) that are used in an automated cryptographic authentication mechanism. The token may be PIN-protected, biometric-enabled or used in conjunction with a simple password.

- **Other token (no corresponding NIST category):** This category of methods embraces any other type of token, such as a magnetic stripe card, an RFID token or a 125kHz proximity card, a CD token, or proprietary software that "tokenizes" a generic device, such as a USB NAND flash drive or an MP3 player.
- **OOB authentication (NIST: "out-of-band token"):** This category of methods uses an OOB channel (for example, SMS or voice telephony) to exchange authentication information (for example, sending the user an OTP that he or she enters via the PC keyboard). It is typically used in conjunction with a simple password. (Some vendors also support OTP delivery via email in a similar way; however, this is not strictly "OOB" because the OTP is sent over the same data channel as the connection to the server.) A few vendors now offer PC and mobile apps that support push notification modes. These are, in principle, distinct from OTP software tokens because the app doesn't generate an OTP, although some vendors offer hybrid apps that provide OTP generation as well as OOB push notification modes.
- **Biological biometric (no corresponding NIST category):** A biological biometric authentication method uses a biological characteristic (such as face topography, iris structure, vein structure of the hand or a fingerprint) as the basis for authentication. It may be used in conjunction with a simple password or some type of token.
- **Behavioral biometric (no corresponding NIST category):** A behavioral biometric authentication method uses a behavioral trait (such as voice and typing rhythm) as the basis for authentication. It may be used in conjunction with a simple password or some type of token.

In the research for this Magic Quadrant, a vendor's range of authentication methods offered and supported was evaluated as part of the assessment of the strength of its product or service offering. Note that tight-focus vendors offer only one or a few authentication methods, but this doesn't necessarily limit their position within the Magic Quadrant. Rather, we assessed a vendor's range of offerings in the context of its demonstrated ability to support enterprise needs across a variety of use cases (see below).

Use Cases for User Authentication

Many enterprises adopt new authentication methods to support one or many use cases, the most common of which are workforce remote access (especially access to corporate networks and applications via a VPN or hosted virtual desktop [HVD]) and external-user remote access (especially retail-customer access to Web applications).

The same new authentication method may be used across one or a few use cases, but the more use cases an enterprise must support, the more likely it needs to support multiple authentication methods to provide a reasonable and appropriate balance of authentication strength, total cost of ownership (TCO) and user experience (UX) in each case (see "Gartner Authentication Method Evaluation Scorecards, 2011: Overview").

A full range of use cases is enumerated below. Vendors included in this Magic Quadrant can typically support multiple use cases, and the positioning reflects that breadth as part of the Ability to Execute.

Not all vendors have equal experience in all use cases; some may have a stronger track record in enterprise use cases, such as workforce remote access, while others may focus on access to retail-customer applications, especially in financial services. Thus, if the focus were on only specific use cases, then the vendor positions would likely look rather different. Especially for the financial services use case, consideration should also be given to vendors' WFD capabilities (see the Information subsection below and "Magic Quadrant for Web Fraud Detection").

Not all the vendors in this Magic Quadrant were able to break down their customer numbers on this basis, and in these cases, we have considered the use cases mentioned in inquiry calls where clients cited those vendors.

Note that stand-alone endpoint access use cases cannot use a vendor's authentication infrastructure because the endpoints are not network-connected at login, but rather demand direct integration of a new authentication method into the client OS. Note also that Microsoft Windows natively supports "interactive smart card login" — that is, X.509 token-based authentication.

The authentication use cases that Gartner considered while preparing this Magic Quadrant (with the relevant subcategories) are:

Endpoint Access

- PC preboot authentication: Preboot access to a stand-alone or networked PC by any user
- PC login: Access to a stand-alone PC by any user
- Mobile device login: Access to a mobile device by any user

Workforce Local Access

- Windows LAN: Access to the Windows network by any workforce user
- Business application: Access to any individual business applications (Web or legacy) by any workforce user
- Cloud applications: Access to cloud applications, such as salesforce.com and Google Apps, by any remote or mobile workforce user
- Server (system administrator): Access to a server (or similar) by a system administrator (or similar)
- Network infrastructure (network administrator): Access to firewalls, routers, switches and so on by a network administrator (or similar) on the corporate network

Workforce Remote Access

- VPN: Access to the corporate network via an IPsec VPN or a Secure Sockets Layer (SSL) VPN by any remote or mobile workforce user

- HVD: Access to the corporate network via a Web-based thin client (for example, Citrix XenDesktop or VMware View) or zero client (for example, Teradici) by any remote or mobile workforce user
- Business Web applications: Access to business Web applications by any workforce user
- Portals: Access to portal applications, such as Outlook Web App and self-service HR portals, by any remote or mobile workforce user
- Cloud applications: Access to cloud apps, such as salesforce.com and Google Apps, by any remote or mobile workforce user

External Users' Remote Access

- VPN: Access to back-end applications via IPsec or SSL VPN by any business partner, supply chain partner or other external user
- HVD: Access to the corporate network via a Web-based thin client (for example, Citrix XenDesktop or VMware View) or zero client (for example, Teradici) by any business partner, supply chain partner or other external user
- Business Web applications: Access to Web applications by any business partner, supply chain partner or other external user (except retail customers)
- Retail customer applications: Access to customer-facing Web applications

For each use case, the enterprise must identify the methods or combinations of methods that fit best, considering at least authentication strength, TCO and UX (see "How to Choose New Authentication Methods" [Note: This document has been archived; some of its content may not reflect current conditions]).

Note that some vendors have a particular focus on one use case or a few use cases, which may limit their vertical position within the Magic Quadrant. Nevertheless, such vendors could offer solutions that are ideally suited to your needs.

Market Trends and the Nexus of Forces

In "The Nexus of Forces: Social, Mobile, Cloud and Information," Gartner noted that a nexus of converging forces — social, mobile, cloud and information — is building on and transforming user behavior while creating new business opportunities.

In the Nexus of Forces, information is the context for delivering enhanced social and mobile experiences. Mobile devices are a platform for effective social networking and new ways of work. Social links people to their work and each other in new and unexpected ways. Cloud enables the delivery of information and functionality to users and systems. The forces of the nexus are intertwined to create a user-driven ecosystem of modern computing.

Looking at the trends in the user authentication market over the past year and into the next few years, it is these four forces that surface as the most significant.

Vendors' market understanding and offering (product) strategy (see the Evaluation Criteria section below) were evaluated against these market trends. This represents a significant change from the 2012 Magic Quadrant research (only cloud was significant in that evaluation); thus, vendors that really "get" the impact of mobile, information and social have tended to shift toward the right (increased Completeness of Vision).

Cloud

Cloud computing is relevant to the user authentication market in two ways:

- It provides a delivery option for vendors' user authentication offerings.
- It is another integration target for vendors' user authentication offerings (however they are delivered).

Several included vendors offer cloud-based user authentication services — traditional managed (hosted) services or new multitenanted cloud-based services — or partner with third-party managed security service providers (MSSPs) ranging from global telcos to smaller, local firms (for example, Sygnify, Tata Communications and Verizon Business).

Historically, cloud-based authentication services have had the most traction among SMBs — companies with fewer than 1,000 employees — and in public-sector vertical industries (government and higher education). Costs, resources and around-the-clock support considerations make a service offering appealing to these customers. Now, we continue to see increasing adoption of cloud-based user authentication services among private-sector enterprises. Several vendors successfully offer only a cloud-based service (or promote such a service over any on-premises offering), and enterprises are choosing such solutions based on their overall value proposition — including, but not limited to, simplicity, flexibility and cost considerations.

We expect further growth in cloud-based user authentication services among enterprises as multitenanted cloud-based services mature, and as cloud computing becomes more widely adopted as a way of delivering business applications and services generally. Gartner predicts that, by 2017, more than 50% of enterprises will choose cloud-based services as the delivery option for new or refreshed user authentication implementations — up from less than 10% today. However, it is likely that on-premises solutions will persist in the longer term, especially in more risk-averse enterprises that want to retain full control of identity administration, credentialing and verification.

To address the need to extend the enterprise's user authentication solution to cloud-based applications, services and infrastructures, user authentication vendors are increasingly supporting SAML-based federation to facilitate integration with these new targets. This approach may be the simplest approach for some enterprises, while others will seek additional identity management capabilities provided by other federation-savvy tools (see "Technology Overview for Federated Identity Management").

In 2012, more than half of the vendors in the Magic Quadrant supported SAML-based federation; this year, about three-quarters have native support, with a few vendors requiring the use of another product in their portfolio or Active Directory Federation Services. However, this still is not a

ubiquitous solution because many cloud targets don't support SAML-based federation themselves. Undoubtedly, federation will become the norm in the midterm to long term, but it is likely that the RESTful "O-protocols" (OAuth and the nascent OpenID Connect) will be preferred by many cloud providers (OAuth now and OpenID Connect within one to three years as it matures), so user authentication vendors (and others) will need to support these in addition to SAML.

Mobile

Mobile computing is relevant to the user authentication market in two ways:

- It provides a new form factor for authentication tokens (phone-as-a-token authentication methods).
- It provides a new kind of endpoint and context in which users must authenticate; either:
  - *To* the endpoint; or
  - *From* the endpoint.

Phone-as-a-token authentication embraces a number of different authentication mechanisms, of which the most widely used are software OTP tokens for smartphones and OOB authentication methods (see the Range of Authentication Methods section above and "Good Authentication Choices: Evaluating Phone-as-a-Token Authentication Methods"). The TCO and UX benefits of phone-as-a-token authentication methods lead enterprises to prefer them to legacy OTP hardware tokens in new and refreshed deployments.

All the vendors in this Magic Quadrant offer at least one phone-as-a-token authentication method (although some don't position these as "primary" authentication options, but rather as backups for other methods), as do many tens of vendors not included here (and this number continues to grow). These methods are increasingly commoditized, and vendors are seeking to differentiate themselves by simplifying provisioning/enrollment and further improving UX.

However, mobile computing erodes the UX and other benefits of phone-as-a-token authentication methods. In fact, the impact of mobile computing extends to the majority of popular methods. Those that are commonly used for workforce remote and local access from PCs — typically OTP hardware tokens and phone-as-a-token authentication methods in the first case, and X.509 smart tokens in the latter — don't migrate well to mobile computing for the following reasons:

- Poor UX in most cases (and users' UX expectations are higher on mobile devices)
- Reduced assurance in the case of phone-as-a-token methods
- Difficulty in, and cost of, technical integration of X.509 smart tokens

Note that these barriers arise however the user is getting access to the downstream systems, and however authentication is integrated: via VPN, HVD or Web app using a mobile browser; via a resident mobile app (with native integration or via a wrapper); or via an application container. However, each of these approaches might, in practice, further constrain what can be used because of which integration points a user authentication vendor supports.

In the absence of widely available and proven "mobile apt" authentication methods, pragmatism is driving enterprises to implement methods that may not be classically "strong," but are technically feasible, lower cost and provide better UX. One example of such a method is the use of power-on passwords with X.509 device credentials (see "Predicts 2013: Mobile, Social and Federation Drive Identity and Access Management").

Where higher-assurance authentication is indicated, users will increasingly resist using a dedicated device for authentication. However, biometric authentication can provide a higher level of assurance with improved UX, and a growing number of vendors (not included in this Magic Quadrant) offer products that exploit the phone as a biometric capture device. (Some vendors support voice verification in conjunction with OOB voice modes, but this isn't quite the same thing.)

Suitable low-friction biometric authentication modes include typing rhythm, voice recognition, and face topography and iris structure (using user-facing cameras). Multiple modes may be combined in a solution to provide broader options, or to support progressive, risk-appropriate authentication. Gartner has predicted increasing use of biometric authentication for access to enterprise networks or high-value Web applications from smartphones or tablets (see "Predicts 2012: A Maturing Competitive Landscape Brings New IAM Opportunities").

We now feel that contextual authentication (see below) will likely also play a significant part in mobile-apt user authentication, especially since the phone itself provides a rich node of identity-relevant contextual data that can be used to increase the confidence in the claimed identity.

We also note that adopting significantly different user authentication methods for different kinds of endpoints will be unsustainable in the midterm to long term because the burden on enterprises and users alike will be too great. Thus, mobile-apt methods must also be "PC apt." Combinations of X.509 credentials on the endpoint, low-friction biometric modes and contextual authentication will likely fit the bill. In cases where PCs lack the right capture devices (such as mikes and cameras), users' phones can be co-opted.

Having said all that, only some of the vendors in this Magic Quadrant have demonstrated awareness of this need, and regrettably few have any way of addressing it.

Information

Information is fundamental to contextual authentication and adaptive access control. The full value of these approaches comes from applying advanced analytical techniques from large aggregations of identity-relevant information ("big identity data").

WFD tools, which are widely deployed in retail banking in the U.S. and elsewhere, established the idea of using contextual data (such as endpoint identity [EPI] and geolocation, typically inferred from the IP address) as a way of corroborating a user's claimed identity (contextual authentication).

These WFD tools have been adopted by a relatively small number of enterprises in other use cases, including remote access by workforce and external users. Some vendors (including RSA, The Security Division of EMC) now target these WFD tools at larger enterprises for remote-access use cases; and some vendors (including a number in this Magic Quadrant, as well as smaller new

entrants, such as Safelayer Secure Communications) have embedded contextual authentication/ adaptive access control capabilities into "pure" user authentication products.

A key benefit of contextual authentication is that it can increase the level of assurance provided by, for example, a password, without requiring users to use a traditional higher-assurance ("two-factor") authentication method. In some use cases with low to medium risk, and for workforces with highly consistent work patterns, password plus contextual authentication may be sufficient.

However, in many use cases, unless the enterprise is willing to block access, it will still be necessary to invoke a higher-assurance method ("step-up" or "progressive" authentication) when the contextual data varies outside of norms (unknown endpoint, unusual location or one that is unreasonably distant from the last known location, and so on), when insufficient contextual data is available or when the user is attempting to access higher-value assets. Nevertheless, the burden of authentication on users is reduced (along with support overheads).

In a banking or similar context, rather than progressive authentication, invoking transaction verification is typically a more appropriate action. In other contexts, it might be appropriate to impose another "obligation," such as switching on more-granular auditing.

Gartner describes the concept that frames these different approaches as adaptive access control (see "Adaptive Access Control Emerges" [Note: This document has been archived; some of its content may not reflect current conditions]). Several vendors use the term "risk-based authentication," but the scope of this approach goes beyond authentication alone; rather, it delivers a more flexible and granular authorization mechanism, and ensures appropriate levels of trust. Note that adaptive access control doesn't demand the use of contextual authentication, but always uses some contextual data about the user, endpoint, transaction or asset to make a risk-based authorization decision; this might be the level of trust in the person (such as strength of identity proofing), the current security state of the endpoint (perhaps based on information from an endpoint protection platform or mobile device management tool), the financial value of a transaction, the sensitivity or criticality of a resource, or the time since the user's entitlements were last certified (attested).

Adoption of contextual authentication in the context of adaptive access control will provide further impetus for the migration from legacy OTP hardware tokens toward "tokenless" solutions. If users will be using a higher-assurance method more rarely, then it becomes harder to justify investing in relatively costly tokens with high logistical overheads. Thus, we expect to see further interest in and adoption of phone-as-a-token authentication methods, as well as phone-based biometric authentication methods (see the Mobile subsection above). Gartner projects that major user authentication vendors will make significant strides in the breadth and depth of these contextual authentication frameworks during the next four years.

The range of contextual data sources used is rapidly expanding (with mobile computing providing a rich seam), and leading business intelligence vendors are exploring how they can leverage their analytics to "feed" contextual authentication frameworks. In this scenario, an authenticated social network identity may be consumed as further corroboration of identity (see the Social subsection below). Use of smartphones, either as endpoints or as active components of user authentication, will potentially make available a further set of identity-relevant information (see the Mobile

subsection above). With increasing numbers of independent sources of contextual data, the confidence this provides increases exponentially because of consilience effects — for example, consistency between IP-based geolocation, GPS and cell tower information. This shift in emphasis will create opportunities for new vendors, and existing user authentication vendors that don't support contextual authentication will increasingly find themselves at a disadvantage in the market (and further to the left in the Magic Quadrant).

Gartner predicts that, by year-end 2016, more than 30% of enterprises will use contextual authentication for workforce remote access — up from less than 2% today. (Note that this 2% doesn't include "simple" context-based access controls, such as denying or restricting an unknown endpoint's access to the network, independent of the user-authentication decision point.)

Social

Social network identities can be used to simplify user registration, subsequent logins or both. Using "Login with Facebook" (or other popular social networks) lowers friction, and thus improves the UX for customer registration and subsequent logins (see "Predicts 2013: Mobile, Social and Federation Drive Identity and Access Management"):

- For registration, required personal information can be imported from users' social profiles, thus reducing — if not eliminating — form filling.
- For login, using the social network identity means that users don't have to remember yet another rarely used password, and they don't have to go through convoluted password reset processes if they forget them.

The challenge for user authentication vendors is to support an authentication workflow wherein an enterprise allows users to log in with their social network identities (that is, when the user is already logged into the social network, without the traditional step of entering a user ID and password), but also wants to invoke explicit authentication for higher assurance. Few of the vendors in this Magic Quadrant showed any awareness of this need.

In addition, in situations where a social network identity is not being used to log in directly, social network identities previously linked with the user's enterprise or customer identity can be used as additional contextual data to increase the confidence in a claimed identity (see above). Multiple authenticated social network identities provide higher confidence — but the authentication engine needs to avoid double counting (that is, using the same social network identity for initial login and corroboration). Relevant identity data from a broader range of social profiles can also be folded into the mix.

Other Considerations

Versatile Authentication Servers and Services (VASs)

A VAS is a single product or service that supports a variety of open and proprietary (including third-party) authentication methods in multiplatform environments.

Wide-focus authentication vendors are typically VAS vendors, and, with few exceptions, VASs are the only authentication infrastructure they offer (although perhaps with different delivery options). Thus, even if a customer is initially adopting only one kind of authentication method from such a vendor, it will be implementing a VAS that gives it the flexibility to change or add methods to support future needs.

Where a wide-focus vendor (such as RSA, The Security Division of EMC) supports only its own proprietary methods or those licensed from another vendor, enterprises must consider the impact of vendor lock-in, particularly when it may restrict the future adoption of fit-for-purpose authentication methods.

X.509 Tokens

Unlike OTP tokens and OOB authentication offerings, "authentication using X.509 tokens" does not represent a complete product of fully integrated components provided by a single vendor, but rather an ensemble of discrete components from two or more vendors. Thus, X.509 token projects can be significantly more complex than they may appear at first. Enterprises must identify combinations of the different components that are interoperable, as demonstrated through true technology partnerships, rather than simply through co-marketing and co-selling agreements, and they should also demand multiple reference implementations.

Among the vendors included in this Magic Quadrant, some (such as Gemalto, HID Global and SafeNet) provide only the smart tokens, middleware and CM tools. Others (such as Symantec) provide only the PKI components. For many enterprises, the PKI tools provided by Active Directory Certificate Services (a standard component in the Standard and Datacenter editions of Active Directory) will be good enough, so any of the vendors that provide only the smart tokens may be sound choices. Where enterprises have a need for richer functionality in their PKI components, both types of vendors are needed.

It is important to note, however, that this "incompleteness" is a market reality for X.509-based authentication, and vendors offering smart tokens and supporting X.509-based authentication in their authentication infrastructure products were not penalized for lacking PKI tools when we were developing this Magic Quadrant. Moreover, X.509-based authentication for Windows PC and network login is natively supported, so it does not need an authentication infrastructure that defines the market covered by this Magic Quadrant (see the Market Definition/Description section above).

Enterprises seeking to support this can consider other vendors that offer smart tokens (for example, G&D, Morpho and Oberthur Technologies), PC middleware (from the smart token vendors or others, such as charismathics) and CM tools (from the smart token vendors or others, such as Bell ID, Intercede and Microsoft [as part of Forefront Identity Manager]).

Pricing Scenarios

For this Magic Quadrant, vendor pricing was evaluated across the following scenarios (unchanged from the 2012 Magic Quadrant):

Scenario 1

Communications (publishing and news media): Small enterprise (3,000 employees) with 3,000 workforce users of "any" kind:

- Usage: Daily, several times per day.
- Endpoints: PC — approximately 60% Windows XP and Vista (Active Directory) and 40% Mac OS X (OpenLDAP).
- Endpoints owned by: Company.
- User location: Corporate LAN.
- Access to: PC and LAN, downstream business and content management applications, mixture of internal and external Web and legacy.
- Sensitivity: Company- and customer-confidential information.
- Notes: The company also plans to refresh its building access systems, and may be receptive to a "common access card" approach.

The average (median) price for this scenario was approximately $154,000 (up from $125,000 in the 2012 Magic Quadrant).

Scenario 2

Retail ("high street" and online store): Large enterprise (10,000 employees) with 50 workforce users, limited to system administrators and other data center staff:

- Usage: Daily, several times per day.
- Endpoints: PC — mixture of Windows XP and Vista.
- Endpoints owned by: Company.
- User location: Corporate LAN.
- Access to: Windows, Unix, and IBM i and z/OS servers, Web and application servers, network infrastructure.
- Sensitivity: Business-critical platforms.
- Notes: Users have personal accounts on all servers, plus the use of shared accounts mediated by a shared account password management (SAPM) tool (for example, Cyber-Ark Software and Quest Software). Users also need contingency access to assets via an SSL VPN from PCs ("any" OS). The company has already deployed 1,500 RSA SecurID hardware tokens for remote access for its mobile workforce. It must comply with the U.S. Sarbanes-Oxley Act, the PCI Data Security Standard (DSS) and other requirements (as appropriate) to the targets accessed.

The average (median) price for this scenario was approximately $7,500 (up from $7,000 in the 2012 Magic Quadrant).

Scenario 3

Healthcare (teaching hospital): Large enterprise (10,000 employees) with 1,000 external users, comprising doctors and other designated staff in doctors' practices:

- Usage: Daily, several times per day.
- Endpoints: PC — mixture of Windows XP and Vista, some Windows 7 and Mac OS X, and maybe others.
- Endpoints owned by: Doctors' practices.
- User location: On LANs in doctors' practices.
- Access to: Electronic health record applications; mixture of Web and legacy (via SSL VPN).
- Sensitivity: Patient records.
- Notes: Enterprise must comply with the U.S. Health Insurance Portability and Accountability Act (HIPAA) and the U.S. Health Information Technology for Economic and Clinical Health (HITECH) Act requirements. PCs may be shared by doctors and other staff members in doctors' practices.

The average (median) price for this scenario was approximately $65,000 (down from $70,000 in the 2012 Magic Quadrant).

Scenario 4

Utilities (power): Large enterprise (20,000 employees) with 5,000 users comprising a traveling workforce and a "roaming" campus workforce:

- Usage: Daily, several times per day to several times per week.
- Endpoints: PC (mainly Windows XP), smartphones (mainly BlackBerry) and some other devices.
- Endpoints owned by: Company.
- User location: Public Internet and corporate wireless LAN (WLAN).
- Access to: Business applications, mixture of internal Web and legacy, via SSL VPN or WLAN.
- Sensitivity: Company- and customer-confidential information, financial systems (some users), information about critical infrastructure (some users).
- Notes: Must comply with U.S. Federal Energy Regulatory Commission (FERC), North American Electric Reliability Corporation (NERC), and other regulatory and legal requirements. The company is also investigating endpoint encryption solutions for its traveling workforce's PCs.

The average (median) price for this scenario was approximately $220,000 (up from $200,000 in the 2012 Magic Quadrant).

Scenario 5

Financial services (retail bank): Large enterprise (20,000 employees) with 1 million external users, all retail banking customers:

- Usage: Variable, up to once every few months.
- Endpoints: PC — mixture of Windows XP and Vista, some Windows 7 and Mac OS X; smartphones (including Android and iOS) and tablets (mainly iOS).
- Endpoints owned by: Customers, Internet cafes and others, possibly also customers' employers.
- User location: Public Internet, sometimes worldwide; possibly corporate LANs.
- Access to: Web application.
- Sensitivity: Personal bank accounts, up to $100,000 per account.
- Notes: Most customers are based in metropolitan and urban areas, but approximately 10% are in areas without mobile network coverage.

The average (median) price for this scenario was approximately $2 million (up from $1.9 million in the 2012 Magic Quadrant).

General Remarks

These pricing scenarios do not reflect any discounts that a vendor may offer particular customers or prospects, nor do they reflect other considerations that contribute to the TCO of a user authentication solution (see "Gartner Authentication Method Evaluation Scorecards, 2011: Total Cost of Ownership").

In each scenario, different vendors may base their pricing on different authentication methods with differential pricing. This may be the case when two vendors have similar ranges of authentication methods, but preferred different methods as the "best" solution on which to base their pricing.

In the Vendor Strengths and Cautions section, we will call out the vendors that fall into the lowest (best) and highest (poorest) "quartiles" — that is, the first and last 25% of the pricing range between the lowest and highest figures provided (not all vendors provided pricing guidance for all scenarios). Vendors are not necessarily evenly distributed between the quartiles; as an extreme example, if all but one vendor had pricing in the region of $10,000, and the one had pricing in the region of $100,000, then the majority would be in the lowest quartile and the one would be in the highest, with none in the intermediate quartiles.

Vendor Strengths and Cautions

Authentify

Authentify, based in Chicago, was established in 1999. It offers OOB authentication services and has multiple OEM relationships (which include other vendors discussed in this Magic Quadrant). Authentify has a strong market focus on financial services, and tailors its offerings to banks' and others' need for layered security and fraud prevention measures.

Authentify's core offering in this market is Authentify Out-of-Band Authentication, which provides OOB authentication via voice modes. This can extended by two additional-cost offerings: Authentify 2CHK, an OOB app for mobile devices and PCs, and Voice Biometric Verification. A small number of customers (such as universities offering remote classes and exams) choose Authentify for voice verification primarily, where "OOB" is relegated to a capture mechanism.

Authentify has moved from the Niche Players quadrant to the Visionaries quadrant in this year's Magic Quadrant, based on a clearly articulated understanding of and vision for this market.

Strengths

- Authentify supports contextual authentication/adaptive access control, including Telephone Data Analytics.
- Although its customer numbers are in the lowest tier, the great majority are large enterprises, and Authentify is among the vendors with the highest number of end users.
- The vendor's pricing for Scenarios 2, 3 and 5 was in the lowest quartile.

Cautions

- While Authentify can integrate with cloud apps, it doesn't support federated single sign-on (SSO) via SAML.
- Authentify focuses on only OOB authentication. However, it has a very strong product and a strong focus on the needs of its target markets, especially in financial services. Several other vendors, including some in this research, license Authentify for voice-based OOB authentication.
- It is most commonly used only for external user remote-access use cases (VPN access for business partners and access to customer-facing Web applications).

CA Technologies

CA Technologies' history dates back to the 1970s, and the company has a history of growth through mergers and acquisitions, as well as internal product development. In 2010, CA Technologies acquired Arcot Systems, with which it already had an important strategic partnership.

CA's core offerings in this market are CA Advanced Authentication (integrating CA AuthMinder, its core authentication product, and CA RiskMinder, its Web fraud detection product), delivered as server software, and CA CloudMinder Advanced Authentication, a multitenanted cloud-based service.

The ex-Arcot portfolio also includes e-payment card authentication, secure electronic notification and delivery, and digital signature integrated with Adobe Acrobat. The acquisition also gave CA Technologies an established cloud services infrastructure and expertise for cloud delivery of its wider portfolio of identity and access management (IAM) offerings.

CA remains a Leader in this market.

Strengths

- CA has very broad target system integration.
- It offers a wide range of authentication methods, with OTP software tokens (for PCs as well as mobile phones) and X.509 software tokens being the most commonly used by its customers. The CA RiskMinder component supports contextual authentication/adaptive access control.
- Although its customer numbers are in the lowest tier, the majority are large enterprises, and CA is among the vendors with the highest number of end users.
- It is commonly used across a wide range of workforce local and remote-access as well as external users' remote-access use cases.
- Reference customers cited pricing model/TCO, functionality, the level of security provided by CA's "Cryptographic Camouflage" and UX as key decision factors. The majority also cited integration with CA SiteMinder, although one reference customer felt that there was still room for improvement with that.
- Reference customers were generally satisfied with CA's customer support.
- The vendor's pricing for Scenario 5 was in the lowest quartile.

Caution

- Reference customers cited a range of issues around designing/developing custom end-user workflows and interfaces as a significant implementation challenge.

Deepnet Security

Deepnet Security, based in London, is a privately owned security software business that was formed in 2003.

Its core user authentication offering is the Deepnet DualShield Unified Authentication Platform. It also offers DualShield VE, a virtual appliance for Linux only.

Deepnet is new in this year's Magic Quadrant. It demonstrated significant growth from previous years, thereby allowing it to meet this year's inclusion criteria.

Strengths

- Deepnet offers a wide range of authentication methods, with OTP apps for mobile phones, OTP hardware tokens and SMS-based OOB authentication being the most commonly used by its customers. It offers an innovative, multimodal biometric authentication option, MultiSense, which combines face recognition and voice verification with speech recognition. It also offers limited contextual authentication with DevicePass (EPI).
- It is commonly used across a range of workforce local and remote-access as well as external users' remote-access use cases.
- Reference customers were extremely satisfied with Deepnet's customer support.
- The vendor's pricing for Scenarios 2, 3 and 5 was in the lowest quartile.

Cautions

- Deepnet lacks a cloud-based service offering.
- Of the vendors included in this research, Deepnet has one of the weakest positions in the enterprise user authentication market. While its customer numbers are moderate, the majority are only SMBs, and its end-user numbers are in the lowest tier of the vendors included in this research.

DS3

Founded in 1998 as RT Systems, this Singapore-based company changed its name to Data Security Systems Solutions (DS3) in 2001 to better reflect its market focus. In 2010, it raised institutional funding to expand and execute on its vision to provide solutions that will meet the user and data authentication requirements for different customer segments, different industries and different use cases. DS3 was acquired by Gemalto in December 2012 (see the discussion below under Gemalto).

DS3's core offering in this market is the DS3 Authentication Server (server software). It also offers a scaled-down version, DS3 Authentication Security Module, targeted at deployments of less than 5,000 users, as well as a virtual appliance, a managed service and an SDK for direct integration into customer-facing applications.

DS3 moved from the Visionaries quadrant to the Niche Players quadrant in this year's Magic Quadrant. It continues to execute well in its core market, but is limited by its target vertical industry and geography in ways that inhibit progress in developing a broader competitive awareness.

Strengths

- DS3 supports a wide range of authentication methods, with OTP hardware tokens and SMS-based OOB authentication being the most commonly used by its customers.
- It is commonly used across a range of workforce local and remote-access as well as external users' remote-access use cases. The majority of DS3's customers are in financial services, using DS3 predominantly for customer authentication.
- Reference customers were extremely satisfied with DS3's customer support.
- The vendor's pricing for Scenarios 4 and 5 was in the lowest quartile, and it presented the lowest pricing for Scenario 1.

Cautions

- DS3 lacks integration with cloud-based applications, which reduces opportunities to sell outside a narrow financial-services vertical industry.
- It does not offer contextual authentication/adaptive access control — a conspicuous lack in its target market (financial services). However, DS3 continues to work with leading WFD vendors to complete the solution to the customer.
- While DS3's customer numbers are in the lowest tier of the vendors included in this research, its end-user numbers are moderate, and almost half of its customers are large enterprises. However, the great majority of them are in Asia/Pacific, and DS3 shows no evidence of significant competitive clout in other geographies, despite its partnership with IBM.

Entrust

Entrust, headquartered in Dallas, is a well-established security vendor offering WAM, WFD, citizen e-ID and data encryption tools, in addition to its authentication portfolio. A public company since 1998, Entrust was taken private in 2009 by the private equity investment firm Thoma Bravo.

Entrust's core offering in this market is IdentityGuard, which is delivered as server software. This supports a much broader range of authentication methods than the OTP grid cards that first bore that name. The vendor also has PKI product and service offerings.

Entrust remains in the Niche Players quadrant in this year's Magic Quadrant, although it has articulated a clearer market understanding and vision.

Strengths

- Entrust has very broad target system integration. Cloud-based application integration (via the additional IdentityGuard Federation Module) supports OpenID as well as SAML.
- Entrust offers a wide range of authentication methods, with OTP hardware tokens still being the most commonly used by its customers. IdentityGuard supports contextual authentication/

adaptive access control via its native "Risk Based" engine. Entrust also offers a WFD tool (TransactionGuard), but the vendor was dropped from the 2012 "Magic Quadrant for Web Fraud Detection" because it was unable to provide three customer references, and Gartner did not see it competing in the WFD market in 2011.

- It is commonly used across a range of workforce local and remote-access as well as external users' remote-access use cases (but see below). Entrust has a flexible offering around common access cards.
- The vendor's pricing for Scenario 5 was in the lowest quartile.

Cautions

- Although business partners use Entrust for external users' remote access, only 5% of the vendor's customers use IdentityGuard for retail customer access (however, this accounts for about 80% of Entrust's end-user numbers).
- Entrust lacks a managed hosted service or cloud-based service user authentication offering, although these are available through partner MSSPs.
- The vendor presented the highest pricing for Scenario 2.

Equifax

Equifax, based in Atlanta, has a long history in identity, going back to 1899. It entered the user authentication market in 2010 with its acquisition of Anakam, a wide-focus authentication vendor with a market focus on healthcare and government.

Equifax's core offering in this market is Anakam.TFA, which is available as server software and as a multitenanted cloud-based service. This is one part of Equifax's range of fraud and identity solutions, which also embraces identity proofing (based on patented technology), professional credential and attribute verification, and business entity verification. This range of offerings reflects Equifax's goal to be a broader identity assurance provider, rather than a direct competitor to Leaders in the market covered by this research.

Equifax remains in the Niche Players quadrant in this year's Magic Quadrant.

Strengths

- Equifax offers a fairly wide range of authentication methods, with SMS-based OOB authentication being the most commonly used by its customers. (This had been extended by licensing technology from Gemalto.) It offers simple contextual authentication/adaptive access control based on EPI and IP-based geolocation.
- Anakam.TFA is used across a range of workforce local and remote-access as well as external users' remote-access use cases.

- The majority of Equifax's customers are large enterprises. However, a greater majority of the customers are in government, with only small numbers in other vertical industries, and the vendor's international presence is relatively small.

Cautions

- Anakam.TFA provides integration to cloud-based applications only via a Web service API rather than via federated SSO.
- Other vendors' reference customers cited lack of integration with CA SiteMinder as a reason for spurning Equifax.
- The vendor's pricing for Scenarios 3 and 4 was in the highest quartile. It did not present pricing for Scenarios 1 and 2, commenting that it would not normally address these use cases.

Gemalto

Amsterdam-based Gemalto, formed in 2006 by the merger of Axalto (formerly the smart card division of Schlumberger) and Gemplus, is a leading smart card vendor with a strong presence in the authentication market. It offers OTP tokens as well as smart tokens. Gemalto has broadened the range of its offerings through a succession of acquisitions. Many of these have had a particular relevance to the financial services industry, which constitutes one of the largest constituencies among Gemalto's customers. Gemalto continued this trend with its acquisition of DS3 in December 2012 (which was announced in January 2013). Going forward, DS3 Authentication Server will become Gemalto's core offering for financial services, with its legacy portfolio being targeted at other vertical industries.

Gemalto's core offering in this market is its IDConfirm 1000 server software. It also offers a managed hosted service (with a multitenanted cloud-based service on its road map for 2013) and an SDK for direct integration into customer-facing applications. In partnership with nAppliance Networks, Gemalto offers a hardware appliance bundling IDConfirm with Microsoft Forefront Identity Manager and DirectAccess.

Gemalto also offers Coesys eGov, which is aimed at e-government applications and combines user authentication and federated SSO.

Gemalto has moved from Niche Player to Leader in this market. It has demonstrated improved overall viability, execution (including competitive pricing), responsiveness and customer experience (the strongest among the vendors in this research), and it has articulated a much clearer market understanding (although its product strategy is not quite in step with this yet).

Strengths

- Gemalto has broad target system integration (but see below).
- Gemalto offers a fairly wide range of authentication methods, with X.509 hardware tokens (smart cards and so on) being the most commonly used by its enterprise customers, ahead of

OTP tokens. Gemalto noted that more of its customers were migrating from OTP tokens to X.509 hardware tokens, citing "several high-profile breaches in the last couple of years." However, its financial services customers are continuing to buy OTP hardware tokens (including RCA readers) in the millions.

- Gemalto's offerings are used across the broadest range of use cases. It has a capable offering around common access cards.
- Reference customers were very or extremely satisfied with Gemalto's customer support.
- Gemalto has one of the strongest positions in the enterprise user authentication market. While its customer numbers are moderate, its end-user numbers are in the highest tier, and the great majority of its customers are large enterprises.
- The vendor's pricing for Scenarios 1, 2 and 3 was in the lowest quartile, and it presented the lowest pricing for Scenario 4. Several reference customers cited pricing model/TCO as a key decision factor in selecting Gemalto.

Cautions

- IDConfirm supports integration with cloud-based applications only via a Google plug-in, not via federated SSO.
- While Gemalto offers a managed service — hosted on Amazon Web Services or in Gemalto's own security operations center — it doesn't yet offer a multitenanted cloud-based service. The vendor tells us this is on the road map for 2013.
- Gemalto lacks any contextual authentication/adaptive access control capability.

HID Global

HID Global, based in Irvine, California, is part of Assa Abloy, which acquired ActivIdentity in December 2010 to form the HID Global Identity Assurance business unit. Like ActivIdentity and its predecessors (ActivCard, Aspace Solutions and Protocom), this unit has a long history in authentication and adjacent markets. Its current focus is on authentication and credential management across multiple market segments.

HID has a variety of authentication offerings, now under the ActivID brand (formerly ActivIdentity 4TRESS): Authentication Server and AAA Server (server software), Authentication Appliance (hardware and virtual), and Authentication SDK (for direct integration into customer-facing applications).

It also offers ActivID Threat Detection Service (TDS), under an OEM license from ThreatMetrix; card management tools (as server software and a hardware appliance) supporting the use of X.509 hardware tokens; and the CoreStreet Validation Suite (for X.509 certificate validation and so on).

HID Global has moved from the Niche Players quadrant to the Visionaries quadrant in this year's Magic Quadrant. It articulated an improved market understanding and vision.

Strengths

- HID has very broad target system integration. All offerings except ActivID AAA Server now support SAML-based federated SSO to cloud-based applications, without the need for a separate product.
- HID offers one of the widest ranges of authentication methods, with OTP hardware tokens being the most commonly used by its customers (although it notes that these are declining in popularity in favor of OTP software tokens). Unsurprisingly for a vendor with a significant presence in the physical access control system (PACS) space, HID supports the use of building access cards (contactless chip cards and RFID cards) via its naviGO product.
- HID's offerings are used across a broad range of use cases, with workforce remote access by VPN being ubiquitous among its customers. HID has a strong offering around common access cards.
- Reference customers cited pricing model/TCO, functionality and expected performance as key decision factors.

Cautions

- HID lacks a managed hosted service or cloud-based service offering, although these are available through partner MSSPs.
- HID supports full contextual authentication/adaptive access control only via ActivID TDS, a separately licensed service. The service is integrated into the ActivID Authentication Appliance and (HID tells us) will be added to the ActivID Authentication Server in 2013.
- The vendor's pricing for Scenario 4 was in the highest quartile.

i-Sprint Innovations

Singapore-based i-Sprint Innovations was founded in 2000 by ex-Citibank security professionals and is backed by global institutional investors. It was acquired in 2011 by Automated Systems Holdings Ltd. (ASL), a subsidiary of Teamsun. Thus, i-Sprint gained access to the Chinese market, given the Multi-Level Protection Scheme (MLPS) in China, which obliges companies to use only domestic security solutions.

i-Sprint's core offering in this market is AccessMatrix Universal Authentication Server (UAS), a server software product. AccessMatrix is an integrated set of IAM technologies; apart from UAS, this includes enterprise SSO (ESSO), WAM and privileged account management capabilities.

i-Sprint moved from the Visionaries quadrant to the Niche Players quadrant in this year's Magic Quadrant. It continues to execute well in its core market, but is limited by its target vertical industry and geography in ways that inhibit progress in developing broader competitive awareness.

Strengths

- i-Sprint has broad target system integration.
- It supports a wide range of authentication methods, with improved passwords, OTP hardware tokens (under license from other vendors) and SMS-based OOB authentication being used by the vast majority of its customers. It offers limited contextual authentication via EPI, with IP-based geolocation available only via custom integration with F5's Global Traffic Manager (GTM).
- i-Sprint is used across a broad range of workforce local and remote-access as well as external users' remote-access use cases. Its strong focus on financial services encompasses the majority of its customers.
- Reference customers were very satisfied with i-Sprint's customer support.
- The vendor's pricing for Scenario 4 was in the lowest quartile. Reference customers cited pricing model/TCO as a key decision factor in selecting i-Sprint.

Cautions

- i-Sprint has no managed hosted service or multitenanted cloud-based service. However, it offers a version of its software specifically for MSSP use, and ASL is planning to launch a cloud-based service in 2013.
- While i-Sprint's customer numbers are in the lowest tier, its end-user numbers are moderate, and about half of its customers are large enterprises. However, a great majority of its customers are in Asia/Pacific, and it seems likely that this restricted geographic presence will persist, given i-Sprint's focus on the Chinese market.
- The vendor's pricing for Scenario 2 was in the highest quartile.

PhoneFactor

PhoneFactor, based in Overland, Kansas, and established in 2001 as Positive Networks, has offered its multitenanted, cloud-based OOB authentication service since 2007. PhoneFactor was acquired by Microsoft in October 2012 (see "PhoneFactor a Puzzling Authentication Choice for Microsoft"), but continues to operate as a fully independent subsidiary. While Gartner views this as positive for PhoneFactor in the short term to midterm, we remain uncertain about the strategic value to Microsoft.

PhoneFactor's core offering in this market is the PhoneFactor multitenanted cloud-based service with on-premises software components (PhoneFactor Agent and PhoneFactor Direct SDK) for target-system integration.

PhoneFactor remains a Niche Player in this market. It has articulated an improved strategy.

Strengths

- PhoneFactor has broad target system integration.

- PhoneFactor is used across a broad range of workforce and external users' remote-access use cases. However, use in workforce local access use cases is limited.
- Reference customers were very or extremely satisfied with PhoneFactor's customer support.
- The vendor's pricing for Scenarios 2, 3 and 5 was in the lowest quartile. Reference customers cited pricing model/TCO as a key decision factor in selecting PhoneFactor — and, in particular, that pricing was based on the number of active users each month, rather than the total number of users.

Cautions

- PhoneFactor offers only phone-as-a-token authentication methods (voice-based and SMS-based OOB authentication and a mobile app that functions as a TOTP OTP token, as well as supports OOB authentication via push notification). However, it supports biometric voice verification (under license from multiple vendors) as an adjunct to the OOB voice modes, and can support other vendors' OATH OTP hardware tokens.
- PhoneFactor doesn't have contextual authentication/adaptive access control capabilities, although it supports IP-address whitelisting and caching as a way of letting customers control the invocation of OOB authentication.
- Although its customer numbers are moderate, PhoneFactor's end-user numbers are in the lowest tier of the vendors included in this research, and the majority of its customers are SMBs. Moreover, the great majority of PhoneFactor's customers are in the U.S. These factors bear significantly on its vertical position in the Magic Quadrant.

RSA, The Security Division of EMC

RSA, The Security Division of EMC, which is based in Bedford, Massachusetts, has a long history in the authentication market. Security Dynamics was founded in 1984 and began shipping its SecurID tokens in 1986. Security Dynamics acquired RSA Data Security in July 1996 and formed RSA Security. In 2006, RSA was acquired by EMC. Other acquisitions have provided RSA with a broad portfolio of access and intelligence products (including RSA Access Manager; see "MarketScope for Web Access Management"). RSA's recent acquisition, Silver Tail Systems, a leader in the WFD market (see "Magic Quadrant for Web Fraud Detection"), will directly strengthen its offerings in the WFD market, and indirectly in this market as well.

RSA's core offering in this market is RSA Authentication Manager (AM), which supports the well-known RSA SecurID OTP tokens (among other methods) and is offered as server software and a hardware appliance. (RSA AM8 will also be offered as a virtual appliance.) RSA SecurID OTP tokens are also supported by RSA SecurID Authentication Engine, an SDK for direct integration into customer-facing applications. In the period covered by this research, the vendor has had RSA Authentication Manager Express (AMX), a hardware appliance, aimed at SMBs, but this will be superseded by RSA AM8.

RSA Adaptive Authentication (AA), RSA's WFD offering (server software and a managed hosted service), is used beyond its initial target market (e-banking), thereby allowing large enterprises in all vertical industries to take advantage of its contextual authentication/adaptive access control capabilities. RSA also offers RSA Identity Verification, a managed service offering that offers identity proofing based on life-history questions, which consumer-facing customers also use for interactive user authentication.

RSA has moved from the Challengers quadrant to the Leaders quadrant in this year's Magic Quadrant. It has moved on from the significant hurdle of the 2011 breach and provided greater transparency regarding its presence in the market and its overall viability. It has demonstrated significantly improved execution and market responsiveness, as well as clearly articulated its market understanding and product strategy.

Strengths

- RSA offers a fairly broad but solely proprietary range of authentication methods, with OTP hardware tokens still being most commonly used by its customers. RSA AMX and RSA AA support contextual authentication/adaptive access control, which was not provided in RSA AM (an omission we have noted since April 2009; see "MarketScope for Enterprise Broad-Portfolio Authentication Vendors" [Note: This document has been archived; some of its content may not reflect current conditions]). However, it will be available, at an additional licensing cost, in RSA AM8, to be released in March 2013. Further enhancing this aspect of RSA's portfolio is a significant part of its vision for the user authentication market.
- RSA offerings are used across a very broad range of workforce remote and local access as well as external users' remote-access use cases.
- RSA has one of the strongest positions in the enterprise user authentication market. Its customer and end-user numbers are in the highest tier.
- Reference customers generally cited industry experience, functional capabilities and expected performance/scalability as key decision factors in selecting RSA. They were very or extremely satisfied with RSA's customer support.
- Despite RSA's reputation for high prices (see below), its pricings were competitive across all scenarios, except No. 4. Its pricing for Scenario 2 was in the lowest quartile, and it presented one of the two lowest pricings for Scenario 5.
- RSA is still the vendor most often cited as the competitor to beat by the others included in this research.

Cautions

- RSA does not offer support for RSA SecurID OTP tokens in a managed hosted or multitenanted cloud-based service. However, such services are provided globally by a wide range of MSSPs.
- RSA AM and RSA Authentication Engine support integration with cloud-based applications only via ancillary products, such as RSA Federated Identity Manager or third-party equivalents. RSA AA supports this only via an API, but RSA AMX doesn't support this at all.

- Some RSA reference customers were critical of the lack of customizable reporting capabilities of RSA AM. (These are unchanged in RSA AM8.)
- While RSA is the vendor most often cited in inquiries, the majority of those inquiries ask about which methods and vendors offer lower TCO and better UX than RSA SecurID hardware tokens. Some of the other vendors' reference customers cited price as a reason for spurning RSA. However, sometimes, clients (including RSA customers) are not aware that RSA offers lower-TCO phone-as-a-token authentication methods.

SafeNet

SafeNet, based in Baltimore, was established in 1983 as Industrial Resource Engineering and changed its name in 2000. In 2007, SafeNet was acquired by Vector Capital, which also acquired Aladdin Knowledge Systems two years later. Both firms now trade under the SafeNet name. SafeNet has successfully integrated a diverse range of user authentication products with different pedigrees, including Aladdin's eToken and Secure Computing's SafeWord (one of the oldest lines of OTP tokens). In March 2012, SafeNet acquired Cryptocard — a vendor in the Visionaries quadrant of the 2012 Magic Quadrant — essentially for its cloud-based user authentication service. SafeNet's other major product lines focus on software rights management and cryptography for data protection, including hardware security modules (HSMs).

SafeNet's core offerings in this market include two server-software products, SafeNet Authentication Manager and SafeNet Authentication Manager Express; SafeNet Authentication Service, a multitenanted cloud-based service (with a special edition aimed at service providers); and SafeNet OTP Authentication Engine (which supports only SafeNet's proprietary OTP tokens), an SDK for direct integration into customer-facing applications.

SafeNet remains in the Leaders quadrant of this year's Magic Quadrant.

Strengths

- SafeNet has very broad target system integration.
- SafeNet offers a very wide range of authentication methods (with SafeNet Authentication Manager supporting the whole range, including X.509 tokens, and SafeNet Authentication Manager Express and SafeNet Authentication Service supporting somewhat narrower ranges). OTP tokens and X.509 tokens are the most widely used among its customers. SafeNet has added support for contextual authentication/adaptive access control to SafeNet Authentication Manager; this includes EPI and IP-based geolocation as well as simple behavioral analytics.
- SafeNet's offerings are used across a very broad range of workforce remote and local access as well as external users' remote-access use cases. SafeNet has a capable offering around common access cards.
- SafeNet has one of the strongest positions in the enterprise user authentication market. Its customer and end-user numbers are in the highest tier.

- Reference customers generally cited functional capabilities as the key decision factor in selecting SafeNet. They were satisfied or very satisfied with SafeNet's customer support.
- The vendor's pricing for Scenarios 1, 2 and 3 was in the lowest quartile.

Caution

- The vendor's pricing for Scenario 5 was in the highest quartile.

SecureAuth

Formed in 2005 as MultiFactor Corporation, this Irvine, California-based vendor changed its name to SecureAuth in 2010.

In our opinion, SecureAuth IdP is primarily a WAM product delivering federated SSO with broad protocol support, strong mobile device support (including an integration toolkit for mobile Web and resident mobile applications) and native support for a range of authentication methods (see "MarketScope for Web Access Management" for further details). SecureAuth's Universal Browser Credential (UBC) does double duty as an X.509 software token and as the anchor for SecureAuth IdP's SSO and authentication workflow. Because of the ease of provisioning and using UBCs, many Gartner clients see SecureAuth IdP as a possible direct replacement for other vendors' "pure" user authentication offerings, quite apart from its WAM capabilities. Hence, its inclusion in this research.

SecureAuth IdP is delivered as a virtual appliance that can be supported in a range of virtualization environments, including Amazon EC2. SecureAuth doesn't offer IdP as a managed hosted service by itself, but rather through a dedicated partnership with Authen2cate.

SecureAuth remains a Niche Player in this market, albeit one differentiated by the extended capabilities of its core offering that fall into an adjacent IAM market.

Strengths

- SecureAuth IdP is focused around X.509 software tokens that are provisioned to users' endpoint devices, but offers a number of other authentication methods, among which OOB authentication methods are most widely used by its customers. SecureAuth IdP can also support a variety of other authentication methods by being able to *consume* identities authenticated by other services, such as Microsoft Active Directory or a social network.
- It is commonly used across a range of workforce local and remote-access as well as external users' remote-access use cases, although less than one-fifth of SecureAuth's customers use it for access to retail-customer applications.
- The vendor's pricing for Scenario 1 was in the lowest quartile.
- The great majority of SecureAuth's customers are large enterprises.
- SecureAuth continues to be the vendor most often cited positively by clients in inquiries about user authentication. Clients call out the ease of implementation and ongoing administration of SecureAuth IdP, as well as the good UX provided by its X.509 software tokens.

Cautions

- While SecureAuth has fairly broad target system integration, it revolves around SecureAuth UBC, which requires a Web interface, so integration to legacy target systems must be proxied through a Web-enabled gateway, such as from Cisco, Citrix, F5 or Juniper Networks.
- Since the 2012 Magic Quadrant, SecureAuth has added support for YubiKey OTP hardware tokens using Yubico's proprietary algorithm. While this research was being prepared, SecureAuth added support for OATH tokens. SecureAuth lacks a contextual authentication/ adaptive access control capability.
- SecureAuth's customer numbers are in the lowest tier of the vendors included in this research, although its end-user numbers are moderate.
- The vendor's pricing for Scenario 5 was in the highest quartile.

SecurEnvoy

U.K.-based SecurEnvoy, formed in 2003, was one of the first vendors to offer OOB authentication solutions.

Its core offering in this market is SecurAccess, which is delivered as server software.

SecurEnvoy has moved from the Niche Players quadrant to the Visionaries quadrant in this year's Magic Quadrant. It has demonstrated continued innovation around phone-as-a-token user authentication methods, including support for new use cases.

Strengths

- SecurEnvoy has fairly broad target system integration, although it lacks native support for federated SSO to cloud-based applications, relying instead on integration with Active Directory Federation Services.
- While SecurEnvoy offers only OOB authentication and OTP software tokens for mobile phones and PCs (with SMS modes and OTP apps being the most widely used among its customers), its implementation of these methods is superior. It provides a range of configuration options for OOB authentication via SMS modes that enable an enterprise to address operational issues (such as latency and lack of signal) and balance UX against a desired level of security.
- SecurEnvoy is used across a very broad range of workforce remote and local access as well as external users' remote-access use cases. Uniquely among phone-as-a-token vendors, it provides preboot authentication via integration with Sophos.
- Reference customers generally cited functional capabilities and pricing model/TCO as the key decision factors in selecting SecurEnvoy. They were extremely satisfied with SecurEnvoy's customer support.
- The vendor's pricing for Scenarios 2, 3 and 5 was in the lowest quartile.

Cautions

- SecurEnvoy doesn't offer a hardware appliance or a managed hosted or multitenanted cloud-based service (although this might be offered by third-party MSSPs).
- SecurEnvoy lacks a contextual authentication/adaptive access control capability.
- Although its customer numbers are moderate, SecurEnvoy's end-user numbers are in the lowest tier of the vendors included in this research.
- The great majority of SecurEnvoy's customers are in EMEA. However, the vendor is growing its presence globally through investments in regional offices and partners.

SMS Passcode

Denmark-based SMS Passcode was established in 1999 as Conecto A/S, a consulting operation implementing mobile solutions. SMS Passcode OOB authentication, which is delivered as server software, was launched in 2005. At the end of 2009, the company sold off its consulting business and adopted the name of the product.

SMS Passcode remains in the Niche Players quadrant of this Magic Quadrant.

Strengths

- SMS Passcode has fairly broad target system integration, although it lacks native support for federated SSO to cloud-based applications, relying instead on integration with Active Directory Federation Services.
- Reference customers generally cited pricing model/TCO as the key decision factor in selecting SMS Passcode, with some also calling out functional capabilities and expected performance/scalability. They were very or extremely satisfied with SMS Passcode's customer support.
- The vendor's pricing for Scenario 2 was in the lowest quartile.

Cautions

- SMS Passcode doesn't offer a hardware or software appliance, a managed hosted service or a multitenanted cloud-based service (although these might be offered by third-party MSSPs).
- SMS Passcode offers OOB authentication, and supports Yubico YubiKey OTP tokens when users don't have or are unable to use OOB authentication. (SMS modes are the most widely used by its customers. Voice modes are also supported via partners such as TeleSign and Twilio.) SMS Passcode offers only coarse-grained adaptive access control based on geolocation.
- It is commonly used across only workforce remote-access use cases.
- Of the vendors included in this research, SMS Passcode has one of the weakest positions in the enterprise user authentication market, although it has a strong presence among SMBs. The great majority of SMS Passcode's customers are in EMEA.

- The vendor's pricing for Scenario 4 was in the highest quartile. It didn't present pricing for Scenario 5, commenting that the use case didn't match its channel-driven "plug and play" go-to-market model.

Swivel Secure

U.K.-based Swivel Secure was established in 2000 and launched its PINsafe product line in 2003.

Swivel Secure's core offering in this market is delivered as server software, or as a hardware or virtual appliance. A Swivel Secure-branded managed (hosted) service is operated by an outsourcing partner.

Swivel Secure remains a Niche Player in this market.

Strengths

- Swivel Secure has fairly broad target system integration, with federated SSO to cloud-based applications via integration with Active Directory Federation Services, or directly via SAML. Notably, Swivel Secure is integrated with Microsoft Office 365 and Business Productivity Online Suite.
- Swivel Secure provides an idiosyncratic range of authentication methods, based around a variety of improved password and pattern-based OTP KBA methods that work with nonce challenges ("Security Strings"), which can be displayed on the login screen in the simplest implementation (which is the most widely used by Swivel Secure's customers). These KBA methods can also be used in conjunction with a highly proprietary app for smartphones that displays pregenerated challenges. In addition, Swivel Secure offers OOB authentication, in which the OOB channel can be used to deliver the challenge or capture the derived OTP; an SMS mode can also deliver a conventional OTP.
- The vendor's pricing for Scenarios 2, 3, 4 and 5 was in the lowest quartile.

Cautions

- Swivel Secure lacks a contextual authentication/adaptive access control capability.
- It is commonly used across only workforce remote-access use cases.
- Although its customer numbers are moderate, Swivel Secure's end-user numbers are in the lowest tier of the vendors included in this research. Nevertheless, a significant proportion of Swivel Secure's revenue comes from enterprise customers. Among its domestic customers, it cites 18 among the FTSE 100.
- The vendor didn't present pricing for Scenario 1, commenting that it couldn't support Mac OS X endpoints.

Symantec

Symantec, based in Mountain View, California, has been a publicly traded company since 1989. This well-established security, storage and system management vendor entered the authentication market in 2010 with the acquisition of VeriSign's Identity and Authentication Services business.

Symantec's core offering in this market is Symantec Validation and ID Protection (VIP) Service, a multitenanted cloud-based service. Symantec also offers an adjacent product, Symantec O_3, a cloud access security broker (see "The Growing Importance of Cloud Access Security Brokers") incorporating federation technology from Symplified that can provide the "glue" when Symantec VIP is deployed to support cloud-based applications.

Symantec has moved from the Niche Players quadrant to the Visionaries quadrant in this Magic Quadrant.

Strengths

- Symantec VIP has broad target system integration, although it lacks native support for federated SSO to cloud-based applications, relying on integration with Symantec O_3 or a third-party federated SSO tool, such as Active Directory Federation Services.
- Symantec offers a fairly wide range of authentication methods, with OTP hardware tokens and OTP software tokens for mobile phones being the most commonly used by its customers. Symantec VIP embeds contextual authentication/adaptive access control under the name "Intelligent Authentication."
- It is commonly used across a wide range of workforce local and remote-access as well as external users' remote-access use cases.
- Reference customers generally cited pricing model/TCO as the key decision factor in selecting Symantec. They were satisfied or very satisfied with Symantec's customer support.
- The vendor's pricing for Scenarios 2 and 3 was in the lowest quartile.

Cautions

- The vendor didn't present pricing for Scenario 5, commenting that the optimal pricing model would be transaction-based rather than user-based, and would be very sensitive to particular customer needs and transaction volumes. It declined to provide an estimate based on typical volumes for the kind of customer described in the scenario.
- Although about half of Symantec VIP customers are in financial services, Symantec no longer has a discrete WFD offering (see "Magic Quadrant for Web Fraud Detection"). While Symantec VIP's Intelligent Authentication carries over some of the WFD functionality, this may not meet customer needs as well as other vendors' full-blown WFD offerings (particularly RSA's, following its acquisition of Silver Tail Systems).

Technology Nexus

Sweden-based Technology Nexus was founded as a management buyout from Saab Technologies in 1984. In 2010, it acquired PortWise, another Swedish company, and added PortWise's authentication portfolio, WAM and identity federation platform, and SSL VPN tool to its own PKI-based authentication and other offerings, giving the merged company a broader portfolio of authentication methods as well as a broader customer base. (PortWise, under its former name of Lemon Planet, was one of the first vendors to offer OOB authentication.) Other relevant Nexus acquisitions have included iD2 Technologies, Blueice Research and vps.

Nexus' core offerings in this market are the PortWise Authentication Server (server software), Nexus Appliance Platform (a virtual appliance based on CentOS), Nexus Managed Service (a managed hosted service), and Nexus Cloud Service (a multitenanted cloud-based service). It also offers Nexus Certificate Manager, a CM tool (with a range of delivery options) and PortWise Signature Gateway, an e-signature offering. Further IAM offerings include PortWise Access Manager (an SSL VPN tool rather than a WAM tool) and Nexus Argus Authentication Server (a federated SSO tool with wide native user authentication support).

Nexus has moved from Challenger to Leader in this market. It has clearly articulated its market understanding, and demonstrated a relatively strong market understanding and strategy.

Strengths

- Nexus' offerings have broad target system integration, although they lack native support for federated SSO to cloud-based applications, relying instead on integration with Nexus Argus Authentication Server, Nexus Hybrid Access Gateway, the upcoming Nexus Identity Gateway or a third-party federated SSO tool.
- Nexus offers one of the widest ranges of authentication methods, with OTP apps for mobile phones and SMS-based OOB authentication being the most commonly used by its customers. It includes biometric authentication (user interactivity) via an OEM agreement with BehavioSec (see "Cool Vendors in Security: Identity and Access Management, 2012"). It also offers simple contextual authentication/adaptive access control based on EPI and IP-based geolocation.
- It is most commonly used across a broad range of workforce and external users' remote-access use cases. Nexus is building up a capable offering around common access cards.
- Although its customer numbers are only moderately good, Nexus' end-user numbers are in the highest tier, and the majority of its customers are large enterprises.
- Reference customers generally cited functional capabilities and understanding of business needs as the key decision factors in selecting Nexus. They were very satisfied with Nexus' customer support.
- The vendor's pricing for Scenarios 2, 3, 4 and 5 was in the lowest quartile.

Cautions

- Nexus has very few customers in vertical industries outside financial services and government.
- Nexus has a very limited presence in North America.

TeleSign

TeleSign, based in Marina del Rey, California, was established in 2005.

TeleSign's core offering, TeleSign 2FA, is a multitenanted cloud-based OOB authentication service. TeleSign also offers TeleSign Verify, which leverages users' phones to protect against online fraud, and PhoneID, which provides a variety of information about a phone number that can be used as an indicator of risk, or to improve quality of service for OOB authentication (for example, identifying phone numbers that can't receive SMS messages). In February 2013, TeleSign announced the acquisition of Routo Telecommunications, which gives TeleSign a global mobile messaging platform and access to network data that will enhance its offerings.

TeleSign remains a Visionary in this market, with some upward movement due to its execution (including competitive pricing) and market responsiveness.

Strengths

- TeleSign 2FA supports contextual authentication/adaptive access control, based in part around its PhoneID offering.
- It is commonly used across a range of workforce local and remote-access use cases, and very commonly used across a number of external users' remote-access use cases.
- Although its customer numbers are only moderately good, TeleSign's end-user numbers are in the highest tier. TeleSign benefits from its strong presence among very large global service providers (including social media), even though the majority of its customers are SMBs (via partners).
- Reference customers generally cited functional capabilities and pricing model/TCO as the key decision factors in selecting TeleSign. They were extremely satisfied with TeleSign's customer support.
- The vendor's pricing for Scenarios 1, 2, 3 and 4 was in the lowest quartile, and it presented one of the two lowest pricings for Scenario 5.

Cautions

- TeleSign has somewhat limited target system integration, relying on partners (including other vendors in this research) for integration with some targets. It doesn't integrate with cloud-based applications via federated SSO.
- TeleSign focuses on only OOB authentication. However, it has a very strong product and a strong focus on its target markets. Several other vendors, including some in this research,

license TeleSign for at least voice-based OOB authentication. TeleSign doesn't support biometric voice verification, citing lack of customer demand to date.

Vasco Data Security

Vasco, based in Chicago, entered the OTP token market in 1996 with the acquisition of Digipass, and it continues to use Digipass branding for its portfolio of authentication products.

Vasco's core authentication offerings include Identikey (server software), Identikey Appliance (a Linux-based hardware appliance), Digipass as a Service and MyDigipass.com (Vasco's service offering in hosted [private cloud] and multitenanted [public cloud] variants), and Vacman Controller, an API-based authentication library for direct integration into customer-facing applications.

Vasco also offers the aXsGUARD Gatekeeper, a range of remote-access hardware appliances aimed at the SMB market.

Vasco has moved from Challenger to Leader in this market, having demonstrated relatively strong market understanding, strategy and innovation.

Strengths

- Identikey and Identikey Appliance have broad target system integration, including federated SSO integration with cloud-based applications via SAML 2.0 and OpenID, as well as via OpenASelect, a Vasco-owned proprietary federation solution. The nascent Digipass as a Service and MyDigipass.com services integrate with only Web/application servers and cloud-based applications.
- Vasco offers one of the widest ranges of authentication methods, with OTP hardware tokens being ubiquitous among its customers. OTP apps for smartphones, contactless X.509 smart tokens and SMS-based OOB authentication are also common. (Note that Identikey and Identikey Appliance don't have native support for X.509 authentication, while Digipass as a Service and MyDigipass.com support a restricted range of methods.)
- Vasco's offerings are commonly used across a broad range of workforce local and remote-access as well as external users' remote-access use cases.
- Vasco has one of the strongest positions in the enterprise user authentication market. Its customer and end-user numbers are in the highest tier.
- Most reference customers were satisfied or very satisfied with Vasco's customer support.
- The vendor's pricing for Scenarios 2 and 5 was in the lowest quartile.

Cautions

- Vasco's products have no contextual authentication/adaptive access control capability.

- The vendor's pricing for Scenarios 3 and 4 was in the highest quartile, and it presented the highest pricing for Scenario 1. Some of the other vendors' reference customers cited price as a reason for spurning Vasco.

Yubico

Yubico, based in Stockholm, Sweden, and Palo Alto, California, was established in 2007.

Yubico's core offerings in this market include the open-source YubiValidation server (server software), YubiRADIUS VA (a virtual appliance) and YubiCloud (a multitenanted cloud-based service). Yubico's server source C-library is available for third-party integrations. It also offers YubiHSM, an HSM that can act as a YubiValidation server for up to 1,000 users.

Yubico remains a Niche Player in this market. While Yubico has significant aspirations for its distinctive OTP, X.509 and Near Field Communication (NFC) hardware tokens, its vision doesn't map well to Gartner's view of the overarching trends in this market.

Strengths

- Several other vendors, including some included in this research, integrate support for Yubico's YubiKey tokens. Notably, we have recently seen Google introduce native support for YubiKey Neo login.
- YubiKey's OTP hardware tokens have a distinctive design and unique features: They are USB tokens with a small, very robust form factor. (YubiKey Nano tokens are even smaller.) They can generate proprietary or OATH-based OTPs, as well as present a static password, at the touch of a button. From the PC's point of view, the token is a keyboard, so it requires no special software to work with any PC OS. YubiKey Neo tokens add an NFC interface, allowing them to work with NFC-enabled endpoint devices, X.509 authentication support, and Mifare support for integration with PACSs.
- It is used across a broad range of all kinds of use cases, although implementation sometimes requires partner or open-source software (for example, AuthLite or Mi-Token for preboot authentication to Windows PCs, and AuthLite or pGina for Windows PC login). Some Linux distros (for example, OpenBSD and Ubuntu) have native support.
- The vendor presented the lowest pricing for Scenarios 1, 2 and 3, and its pricing for Scenario 4 was in the lowest quartile.

Cautions

- Target system integration is restricted compared with other vendors in this research, and is variable across Yubico's offerings (with YubiRADIUS VA having the broadest range). Notably, they lack integration with WAM products. Integration with cloud-based applications requires a proprietary REST-like interface (YubiCloud Connector API) or third-party code, such as SimpleSAMLphp or SAML for Google Apps.

- Yubico has a narrow range of authentication methods, namely the YubiKey OTP tokens (but see above). A particular limitation is that the hardware tokens need a standard Type A USB socket on the endpoint device, thereby restricting their use with many mobile devices (notably Apple iOS devices) unless adapters are used (for example, the iPad Camera Connector Kit). While YubiKey Neo can be used with NFC-enabled phones or tablets, these won't be mainstream before 2015, so most mobile users will need Yubico's OTP app, which is not strongly differentiated from others on the market.
- Of the vendors included in this research, Yubico has one of the weakest positions in the enterprise user authentication market. Although its customer numbers are moderately good, Yubico's end-user numbers are the lowest among the vendors included in this research. However, while the great majority of its customers are SMBs, 40% of Yubico's revenue comes from a handful of Fortune 100 companies.

Vendors Added or Dropped

We review and adjust our inclusion criteria for Magic Quadrants and MarketScopes as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant or MarketScope may change over time. A vendor appearing in a Magic Quadrant or MarketScope one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. This may be a reflection of a change in the market and, therefore, changed evaluation criteria, or a change of focus by a vendor.

Added

- Deepnet Security: A U.K.-based, wide-focus user authentication vendor.

Dropped

The following vendors failed to meet the elevated inclusion criteria for this year's Magic Quadrant:

- McAfee (formerly Nordic Edge)
- Quest Software (now owned by Dell)

In addition, Cryptocard was acquired by SafeNet early in 2012.

The following vendor did not meet the inclusion criteria, but is worthy of note.

- Imprivata, based in Lexington, Massachusetts, and formed in 2002, has been a successful vendor in the ESSO market for several years with its OneSign ESSO appliance (see "Market Overview for Enterprise Single Sign-On Tools"). In the past few years, Imprivata has had a singular focus on and success in the healthcare market. It also offers OneSign Authentication Management (AM), a stand-alone user authentication product, as a hardware or virtual appliance. OneSign AM supports a full range of the authentication methods demanded by its target market, including the use of building access cards (contactless chip cards and RFID cards) and fingerprint biometric authentication, which are commonly used among healthcare

customers in North America, and X.509 hardware tokens, which are widely used among healthcare customers in EMEA. With this target vertical industry, Imprivata is the leading vendor by market share, according to healthcare industry sources. While Imprivata, in our opinion, doesn't fit our market definition for a general user authentication solution, Gartner clients in healthcare will likely find that Imprivata can meet their specific needs ahead of other vendors included in this Magic Quadrant.

Other Changes

- ActivIdentity: Previously an HID Global company, ActivIdentity dropped its own brand in favor of its parent's name.
- DS3: Acquired by Gemalto in December 2012 as this research was being finalized. Because it is too early to determine how this acquisition will impact Gemalto's placement in the Magic Quadrant, we have published our individual evaluations as they were. See Gemalto's entry to read our projections.
- PhoneFactor: Now part of Microsoft, but it continues to do business under its own brand.

Inclusion and Exclusion Criteria

The following inclusion criteria apply:

- **Relevance of offering:** Each core user authentication product or service meets the user authentication market definition detailed above.
- **Longevity of offering:** Each core user authentication product or service has been generally available since at least 1 May 2011, and is in use in customer production environments.
- **Origination of offering:** The offering is manufactured or operated by the vendor, or is a significantly modified version obtained through an OEM relationship. (We discount any software, hardware or service that has merely been obtained without functional modification through a licensing agreement from another vendor — for example, as part of a reseller/partner agreement.)
- **Number of customers and end users (including customers of third-party service providers and their end users):** As of 31 December 2011, the vendor had one of the following:
  - 500 or more active customers using the vendor's authentication offerings in a production environment
  - 125 or more such customers with a total of 5 million or more end users
- **Verifiability:** Customer references must be available. Vendors with minimal or negligible apparent market share among Gartner clients, or with no currently shipping products, may be excluded from the ratings. Products must be deployed in customer production environments.
- Gartner analysts consider that aspects of the company's product, execution or vision are noteworthy.

Evaluation Criteria

Ability to Execute

Gartner analysts evaluate technology providers on the quality and efficacy of the processes, systems, methods or procedures that enable IT provider performance to be competitive, efficient and effective, and to positively impact revenue, retention and reputation. Ultimately, technology providers are judged on their ability and success in capitalizing on their vision.

Product/Service

We evaluate:

- The capabilities, quality and feature sets of one or more on-premises software or hardware products or cloud-based services that make real-time authentication decisions and can be integrated with any of a variety of enterprise systems — as well as the skills necessary to support these offerings. We also evaluate offerings that were generally available as of May 2011.
- The range and variety of user authentication methods offered or supported, along with the client-side software or hardware used by end users in those real-time authentication decisions.
- The applicability and suitability of these offerings to a wide range of use cases across different kinds of users and different enterprise systems.
- The capabilities, quality, and feature sets of ancillary and adjacent products and services relevant to enterprises' user authentication needs.

Overall Viability (Business Unit, Financial, Strategy, Organization)

- We evaluate the vendor's overall financial health, the financial and practical success of the user authentication line of business, and the likelihood that the vendor will continue investing in and advancing the state of the art of the user authentication portfolio — and, if appropriate, the likelihood that the vendor will continue offering the portfolio within its broader product portfolio.

Sales Execution/Pricing

We evaluate:

- The vendor's capabilities in areas such as deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel, including value-added resellers and third-party managed service providers.
- Pricing over a number of different scenarios. Clients are increasingly price-sensitive as they seek the optimal balance of assurance and accountability, UX, and TCO when selecting new user authentication methods.

Market Responsiveness and Track Record

We evaluate:

- The vendor's demonstrated ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change.
- How the vendor has embraced or responded to standards initiatives in the user authentication market and adjacent segments.

Marketing Execution

- We evaluate the clarity, quality, creativity and efficacy of programs designed to deliver the vendor's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This mind share can be driven by a combination of publicity, promotional initiatives, thought leadership, word-of-mouth and sales activities.

Customer Experience

- We evaluate the vendor's relationships and services/programs — such as technical support and professional services — that facilitate customers' successful implementations and use of the vendor's user authentication offerings. We consider Gartner client and reference customer feedback.

Operations

- We evaluate the ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product/Service	High
Overall Viability (Business Unit, Financial, Strategy, Organization)	Standard
Sales Execution/Pricing	High
Market Responsiveness and Track Record	Standard
Marketing Execution	Standard
Customer Experience	Standard
Operations	Low

Source: Gartner (March 2013)

Completeness of Vision

Gartner analysts evaluate technology providers on their ability to convincingly articulate logical statements about current and future market direction, innovation, customer needs and competitive forces, and how well they map to the Gartner position. Ultimately, technology providers are rated on their understanding of how market forces can be exploited to create opportunities for the provider.

Market Understanding

- We evaluate the vendor's understanding of buyers' needs and how it translates these needs into offerings. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those wants and needs with their added vision.

Marketing Strategy

- We evaluate the clarity and differentiation of the vendor's marketing messages, and the consistency of communication throughout the organization — and externally through its website, advertising, customer programs and positioning statements.

Sales Strategy

- We evaluate the vendor's sales strategy for its user authentication offerings, and whether it uses the appropriate network of direct and indirect sales, marketing, service and communication affiliates that extends the scope and depth of market reach, skills, expertise, technologies, services and the customer base. In particular, we evaluate business development, partnerships with system integrators and channel execution.

Offering (Product) Strategy

- We evaluate the vendor's approach to developing and delivering its user authentication offerings, and whether it emphasizes functionality and feature sets as they map to current and future requirements for enterprises across multiple use cases — differentiated not only by level of risk, but also by business needs and technical, logistical and other constraints. We consider support for open standards and extensibility to support proprietary authentication methods offered by other vendors. We also consider support for mobile devices as endpoints, and for access to cloud-based applications and services.

Business Model

- We evaluate the soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy

- We evaluate the vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including SMBs and vertical industries. We consider the vendor's focus on supporting different use cases, and whether and how it can deliver adjacent products and services that are important to different market segments.

Innovation

- We evaluate the vendor's continuing track record in market-leading innovation, including early standards and technology adoption, how well it anticipates and adjusts to changes in market dynamics as well as customer and end-user needs, and the provision of distinctive products, functions, capabilities, pricing models and so on. We evaluate innovations introduced since May 2011, as well as the vendor's road map over the next one to three years.

Geographic Strategy

- We evaluate how the vendor directs resources, skills and offerings to meet the specific needs of geographies outside its home geography — directly or through partners, channels and subsidiaries — as appropriate for each geography and market.

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	High
Marketing Strategy	Standard
Sales Strategy	Standard
Offering (Product) Strategy	High
Business Model	Standard
Vertical/Industry Strategy	Low
Innovation	High
Geographic Strategy	Low

Source: Gartner (March 2013)

Quadrant Descriptions

Leaders

Leaders in this Magic Quadrant are vendors with a solid track record and, typically, a significant presence in the market. They have a clearly articulated vision that is in line with the market trends, and their vision is typically backed by solid technical innovation as well as an understanding of the challenges and opportunities presented by the Nexus of Forces. Leaders' business strategy and execution are very sound. Vendors in this quadrant can provide a strong solution for enterprises in different vertical industries across one or many use cases, typically including emerging needs pertaining to cloud and mobile.

Challengers

Challengers in this Magic Quadrant are vendors with a solid track record and, typically, a significant presence in the market. Their business execution is generally very sound, although their strategy may not be as strong. They may lack, or may not clearly articulate, a vision that is in line with the market trends, although their technical innovation may be sound. Vendors in this quadrant can provide a strong solution for enterprises in different vertical industries across one or many use cases. Their understanding of the challenges and opportunities presented by the Nexus of Forces may be uneven, or have a limited planning horizon.

There are no Challengers in this year's Magic Quadrant.

Visionaries

Visionaries in this Magic Quadrant are vendors with a clearly articulated vision that is in line with the market trends. Their vision is typically backed by technical innovation and an understanding of the challenges and opportunities of the Nexus of Forces, as well as by a solid business strategy. They have a steady track record, an appreciable presence in the market and acceptable business execution. Vendors in this quadrant can typically provide a very satisfactory solution for enterprises across one or many use cases; this typically includes emerging needs pertaining to cloud or mobile, or a strong solution focused on one or a few particular use cases, or a particular vertical industry.

Niche Players

Niche Players in this Magic Quadrant are vendors with a steady track record and an appreciable presence in the market. They may lack, or may not clearly articulate, a vision that is in line with the market trends, although their technical innovation may be sound. Their business strategy and execution are acceptable. Vendors in this quadrant can typically provide a very satisfactory solution for many enterprises across one or often many use cases, or a sound solution focused on one or a few particular use cases, or a particular vertical industry. In this market in particular, it is worth stressing that any Niche Player could offer a solution that is ideally suited to your needs.

Context

Gartner defines "user authentication" as the real-time corroboration of a claimed identity with a specified or understood level of confidence.

This is a foundational IAM function, because without sufficient confidence in users' identities, the value of other IAM functions — for example, authorization and intelligence (audit and analytics) — is eroded.

User authentication is provided by a range of authentication methods (see "A Taxonomy of Authentication Methods, Update" [Note: This document has been archived; some of its content may not reflect current conditions]) and in a variety of ways. It may be natively supported in an OS or application, or in a directory or access management tool, such as a WAM tool, that spans multiple applications. It may also be added to one or more target systems, including OSs and access management tools, via a third-party component (an API or SDK) that allows it to be embedded directly in each system, or a discrete authentication infrastructure — either on-premises software or hardware or a cloud-based service — which can be integrated with multiple target systems via standard protocols (such as LDAP, RADIUS or SAML) or proprietary software agents.

This Magic Quadrant evaluates the major vendors that provide discrete authentication infrastructures. Some of these vendors also provide APIs, SDKs or components (such as smart cards) that can be consumed by natively supported authentication methods. Many enterprises adopt discrete authentication infrastructures to support one or more — and sometimes many — use cases, the most common of which are workforce remote access (especially access to corporate networks and applications via VPN or HVD) and external-user remote access (especially retail customer access to Web applications).

The same new authentication method may be used across one or a few use cases; however, the more use cases an enterprise must support, the more likely it is to need to support multiple authentication methods to provide a reasonable and appropriate balance of authentication strength, TCO and UX in each use case.

Enterprise interest in OTP methods, broadly defined, remains high; however, during the past few years, we have seen a significant shift in preference from traditional hardware tokens to phone-as-a-token authentication methods.

Wide-focus user authentication vendors offer all these approaches and more — typically offering or supporting KBA methods or X.509 tokens (such as smart cards) as well. Most of the tight-focus vendors offer only phone-as-a-token authentication methods, especially OOB authentication methods. The 21 user authentication vendors included in this Magic Quadrant are those that have the largest presence in the market by number of customers or number of end users served.

Gartner is aware of more than 200 user authentication vendors worldwide, but the market is dominated by a far smaller set of vendors. The leading vendors in this Magic Quadrant account for the majority of the market by customer and end-user numbers. Some of the vendors not included in the Magic Quadrant are poised to challenge the major players, but most are essentially "me, too" commodity vendors that offer technically similar solutions and compete more on price than on quality or experience, while others focus on particular market niches or innovative technologies that may be licensed to major vendors.

Market Overview

Customer wants and needs for user authentication continue to mature. Enterprises increasingly recognize the need for authentication with higher assurance than legacy passwords can provide, across a broader range of use cases, and they are addressing that need. Moreover, enterprises are increasingly aware of the need to find a reasonable and appropriate balance of authentication strength (assurance and accountability), TCO and UX in each use case.

These factors are driving the adoption of alternatives to traditional token-based authentication methods that offer higher levels of assurance, but at a higher cost and with relatively poor UX.

Interest in and support for contextual authentication is driven by these factors and continues to grow, but these techniques are not yet mainstream. Mobile use cases will provide further impetus for contextual authentication and "passive" biometric authentication methods that can be supported without additional hardware.

Although some of the growth in these alternative methods arises from enterprises replacing incumbent tokens, many enterprises are implementing such methods in one or many use cases for the first time. Customer wants and needs are also driving the adoption of authentication methods other than the few that are typically natively supported (for example, in OSs, applications and WAM tools), and these methods demand proprietary authentication infrastructures.

Although a majority of enterprises remain focused on one or a few use cases that may be met by a single authentication method from any kind of vendor, we continue to see growth in the number of enterprises taking a strategic view of authentication, and seeking to address a wider range of use cases that demand different authentication methods with a single, versatile, flexible infrastructure.

Support for cloud computing use cases has driven the adoption of SAML-based federation among user authentication vendors.

Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Magic Quadrants and MarketScopes: How Gartner Evaluates Vendors Within a Market"

"The Five Layers of Fraud Prevention and Using Them to Beat Malware"

"Gartner Authentication Method Evaluation Scorecards, 2011: User Experience"

"Gartner Authentication Method Evaluation Scorecards, 2011: Assurance and Accountability"

"Good Authentication Choices for External User Access"

"Good Authentication Choices for Workforce Local Access"

"Good Authentication Choices for Workforce Remote Access"

Acronym Key and Glossary Terms

ANSI	American National Standards Institute
ASL	Automated Systems Holdings Ltd.
CA	certification authority
CAP	Chip Authentication Program
CM	card management
DPA	Dynamic Passcode Authentication (Visa)
DSS	Data Security Standard (PCI)
EMV	Europay, MasterCard and Visa
EPI	endpoint identity
ESSO	enterprise single sign-on
FERC	Federal Energy Regulatory Commission (U.S.)
HIPAA	Health Insurance Portability and Accountability Act (U.S.)
HITECH	Health Information Technology for Economic and Clinical Health (U.S.)
HMAC	Hash-based Message Authentication Code
HOTP	HMAC-based OTP
HSM	hardware security module
HVD	hosted virtual desktop
IAM	identity and access management
KBA	knowledge-based authentication
LDAP	Lightweight Directory Access Protocol
MLPS	Multi-Level Protection Scheme (China)
MSSP	managed security service provider
NERC	North American Electric Reliability Corporation

NFC	Near Field Communication
NIST	National Institute of Standards and Technology
OATH	Initiative for Open Authentication
OCRA	OATH Challenge-Response Algorithm
OOB	out of band
OTP	one-time password
PACS	physical access control system
PKI	public-key infrastructure
RA	registration authority
RCA	remote chip authentication
SaaS	software as a service
SAML	Security Assertion Markup Language
SAPM	shared account password management
SDK	software development kit
SMB	small or midsize business
SSL	Secure Sockets Layer
SSO	single sign-on
TAN	transaction number
TCO	total cost of ownership
TOTP	time-based OTP
UAS	Universal Authentication Server (i-Sprint)
UBC	Universal Browser Credential
UX	user experience
VAS	versatile authentication server or service

VIP	Validation and ID Protection Service
WAM	Web access management
WFD	Web fraud detection
WLAN	wireless LAN

Evaluation Criteria Definitions

Ability to Execute

Product/Service: Core goods and services offered by the vendor that compete in/ serve the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/ partnerships as defined in the market definition and detailed in the subcriteria.

Overall Viability (Business Unit, Financial, Strategy, Organization): Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel.

Market Responsiveness and Track Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word-of-mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp