Executive Summary
Change can bring both opportunities and threats to any organisation, and there's been no shortage of change for the resellers and distributors offering security solutions in EMEA today. How will current changes affect your business? This paper reports on findings from a survey of SafeNet’s EMEA channel on some of the significant dynamics affecting the two-factor authentication market currently, and offers some insights into how those realities are expected to change in the coming years.

Introduction
Throughout EMEA, security teams have been relying on multi-factor authentication for quite some time. Today, however, the nature of authentication is changing in some fundamental ways:

- **Expanding usage.** Demand for authentication continues to grow. In the past, authentication was often deployed within an enterprise to address specific groups and use cases, such as VPN access. Now, there is a trend toward making authentication standard operating procedure for a much broader set of users and uses, such as safeguarding access to collaboration portals and cloud-based services.

- **Increasing urgency.** The need to leverage multi-factor authentication continues to grow increasingly urgent. This urgency is being driven both by traditional demands to mitigate risk and address compliance mandates, and to sustain security in the midst of such emerging trends as the proliferation of cloud services, collaboration tools, and bring your own device (BYOD) initiatives. For example, in cloud environments, multiple tiers and types of administrators may have access to infrastructure and assets, so leveraging multi-factor authentication to prevent unauthorized access and create unified access policies is vital.

- **Evolving technology.** Given the shifts in the technological environment brought about by cloud services and mobile device proliferation, there has been a fundamental evolution in terms of how authentication is used and implemented. For example, the increased use of smart phones in an enterprise means that more people are using their mobile devices to access corporate resources. Likewise, the distribution and decentralization of data and applications across the enterprise and the cloud means that users have to authenticate to more resources.
These trends are presenting significant implications for enterprises—and opportunities for the channel that serves these organisations. To provide a sense of the scope of these opportunities, SafeNet conducted an extensive survey of enterprise IT and security professionals, and the survey amply illustrated that virtually all organisations are employing multi-factor authentication today. However, the percentage of users within each organization using multi-factor authentication varies substantially. Across the board, adoption among users is expected to grow. Currently, 32.4% of respondents indicated that less than 10% of the workforce is using multi-factor authentication. But in two years, 50% of respondents expect that at least half of all employees will be using two-factor authentication.

To provide more context around the experiences and opportunities presented to those in the channel, SafeNet conducted a survey of channel representatives from across the EMEA region. This paper draws on the findings of this survey to provide a current look at the authentication market and offer SafeNet channel partners insights into where it is headed.

Summary of Top Findings
Following are a few of the survey’s top findings:

- **The promise of the cloud.** Cloud-based services are widely seen as an opportunity—with a resounding 72% indicating they see the cloud as offering their business potential to grow. In addition, when the channel sells a third-party cloud service, the vast majority, almost 80%, see their cost of delivering services drop, and over 17% see costs drop by 30% or more.

- **The increased cloud-readiness of customers.** Today, channel respondents stated that they feel customers will increasingly be open to a cloud-based two-factor authentication service if it offers compelling economics. About 60% indicated that more than 20% of their customers would be open to a cloud solution today, more than 80% expect that to be the case in two years.

- **The rise of mobile phone authentication.** While hardware tokens are the dominant form factor currently, respondents expect that the use of mobile phones for multi-factor authentication is expected to be the most common approach in the future. Respondents anticipate the percentage of users relying on mobile phone authentication to grow from 23% currently to 40% in two years.

- **The rising use of multiple tokens.** To support BYOD trends and the expansion of multi-factor authentication use cases, IT organisations are increasingly going to be issuing multiple tokens to employees. While 47% currently say more than 20% of users have multiple tokens currently, more than 70% expect that to be the case in two years.

- **The expansion of tokens beyond employees.** Enterprises will increasingly be purchasing tokens, not just to secure employee access, but the access of contractors, suppliers, and customers as well. Currently, about 31% say that more than 20% of their accounts are purchasing tokens for non-employees, but 50% predict that will be the case in two years.

Selling Cloud-based Services
The survey looked at the prospects offered by the cloud in several different ways. Survey results revealed that the channel absolutely sees the cloud as an opportunity for business growth, and that selling third-party cloud services reduces the cost of service delivery. There was also broad consensus that offering professional services along with cloud offerings was important. Respondents also indicated that many customers are open to cloud-based two-factor authentication, and anticipate that number to grow substantially in the next couple of years.

---

1 For the authentication survey and trends please refer to the document, Multi-factor Authentication: Current Usage and Trends. Contact your local marketing representative to receive this document.
Cloud Broadly Expected to Foster Growth
Respondents were asked whether they saw the cloud as offering the potential for business growth, and the answer was a resounding one. About 72% of respondents said they thought the cloud could help their business grow. By contrast, about 13% said they didn’t think that was the case, and under 15% said they expected growth associated with the cloud to remain about the same.

The Cloud Reduces Service Delivery Costs
Respondents were queried about the cost reductions associated with selling third-party cloud services. Almost 80% of respondents indicated that they see a reduction in the cost of service delivery when selling cloud services. The highest percentage, 38%, reported enjoying cost reductions of 10 to 30%. 16% of respondents said they saw cost reductions of greater than 30%.

When Selling Cloud-based Solutions, Offering Professional Services is Key
The survey asked respondents how important it is to offer customers professional services when selling cloud-based solutions, and there was very clear consensus in this area. Over 65% of respondents said it was important or very important—while no one said “not at all important”.

Customer Openness to Cloud-based Two-factor Authentication
When channel sales representatives try to sell cloud-based authentication services, how receptive are customers? To gauge this, the survey asked respondents whether their prospects would be willing to choose a cloud-based authentication solution if it provided significant cost savings over a traditional offering. Responses were fairly evenly split across different percentage groups, but the majority, 57%, indicated that between 20 and 60% of customers would consider a cloud-based authentication solution. Among response options, the highest amount, about 1/3, said between 20 and 40% would opt for a cloud option today.

In addition, we asked how respondents anticipated customer receptiveness would change in the next couple of years. Over that time, respondents expect the numbers to shift pretty substantially. While almost 15% said less than 10% would choose the cloud currently, less than 5% of respondents thought that would be the case in two years. 68% said they anticipated that between 20 and 60% of customers would opt for the cloud alternative. Further, over 16% anticipated that more than 60% of their customers would opt for the cloud in two years.

Evolving Token Usage
Like virtually every area of security and IT, mobility will have a fundamental impact on multi-factor authentication. Respondents seem to expect that mobile phone tokens will become the dominant form factor. Further, respondents report that they expect their clients to expand the number of employees that use multiple tokens, and that they’re going to increasingly buy tokens, not just for employees, but partners, contractors, and customers as well. The following sections offer more details on these trends.

Token Form Factor: Going Mobile
Today, hardware-based tokens are the dominant form factor for two-factor authentication deployments. Almost 50% of respondents said they saw hardware tokens in their customer environments. Mobile phone tokens, which represented the second most common category, received a 23% response. In the future, respondents expect those numbers to change dramatically. Respondents predict that the adoption of mobile phone tokens will grow to over 40%, while hardware usage will slip to 25%.

Interestingly, these numbers are aligned with the survey SafeNet ran with respondents from within end user organisations. The survey found that respondents expect that their adoption of mobile authentication will grow substantially, from 27.6% to 44.87%.
Employees to Increasingly Use Multiple Tokens
Given the broader trends in IT and security, it is clear that the demand for multi-factor authentication will continue to grow. This is borne out by the survey, which looked at the topic of users employing more than one token. The highest percentage of respondents, over 50%, say that less than 20% of employees in their accounts currently use more than one token. When asked about the rate of multiple token usage in two years, the percentage of those pointing to that “less than 20%” figure drops from 50% to 29%. About 1/3 say between 20 and 40% will use more than one token in two years, and more than 37% expect the figure to be 40% or more.

Tokens Not Just for Employees
Another way to quantify the increased demand for tokens is to assess the breadth of usage. While tokens in many organisations were initially used solely to secure employee access, that has started to change. Respondents were asked about current rates of token usage in their opportunities by non-employees, such as suppliers, customers, and contractors. Currently, 37% of respondents indicated that less than 10% of accounts are purchasing tokens for non-employees. About 25% said between 20 and 40% of opportunities were using tokens in this way. In two years, only 15% expect it will be less than 10% of accounts that are purchasing tokens for non-employees. On the other hand, about 38% expect between 20% and 40% of accounts will be taking this approach.

Leveraging New Technologies to Build Your Business
For SafeNet channel partners, the significant growth projected in authentication deployments, coupled with the high costs associated with traditional authentication platforms, present a compelling sales opportunity. Even if a customer has a competitive solution in place today, a SafeNet solution can present a compelling alternative—SafeNet Authentication Service. SafeNet Authentication Service makes strong authentication easy to implement and manage, and the solution makes it easy to migrate from alternative authentication platforms. By leveraging SafeNet Authentication Service, channel partners can deliver high-value offerings that meet a real demand in the marketplace, helping organizations address the increasing demand for multi-factor authentication, while realizing significant cost savings over traditional approaches.

With SafeNet Authentication Service, resellers and distributors can deliver a compelling offering that can help them boost their margins and market share. In addition to offering direct revenue growth opportunities, SafeNet Authentication Service allows organizations to be at the forefront of security innovation and offer a high-value service, either under their own brand or in a sell-through model. SafeNet Authentication Service enables channel partners to strengthen their market position by aligning with the recognized leader in authentication. By adopting SafeNet Authentication Service, organizations can:

- Boost customer retention as clients look to migrate to a service-based authentication offering.
- Leverage cross-sell opportunities, so they can increase average revenue per user.
- Capitalize on the increase in customers looking to move to the cloud.
- Enhance competitive differentiation by offering customers new ways to adopt authentication.
- Simplify the way they manage their authentication business.
Q1. Do you see Cloud services offering your business the potential to grow?

Q2. When thinking of the opportunities you see for two factor authentication what percentage of users use each token type now?

Q3. When thinking of the opportunities you see for two factor authentication what percentage of users do you think will use these in the future?

Q4. With increasing employee usage of multiple devices to access corporate resources including BYOD, what percentage of users require or use more than one token now?

Q5. With increasing employee usage of multiple devices to access the corporate network including mobile devices, tablets and BYOD, what percentage of users will require or use more than one token in two years time?

Q6. When you sell a third party cloud service how much does it reduce your cost of delivering services?

Q7. When selling a cloud based solution how important is it for you to also offer professional services?

Q8. Based on the opportunities you see, what percentage of them currently include tokens that are not for your customers employees (ie tokens for your customers suppliers or customers or contractors)?
Q9 Based on the opportunities you see, what percentage of them currently include tokens that are not for your customers' employees (i.e., tokens for your customers' suppliers or customers or contractors)?

Q10 If a cloud-based two-factor authentication solution offered a significant saving against a traditional self-managed solution, what percentage of the customers you work with would choose the cloud solution today?

Q11 If a cloud-based two-factor authentication solution offered a significant saving against a traditional self-managed solution, what percentage of the customers you work with would choose the cloud solution in two years time?
Conclusion
Trends and market dynamics all point to this being a promising time to be in the security channel. Given the heightened security threats your accounts are contending with, the demand for multi-factor authentication solutions will only grow. Further, given the evolution of mobile technologies and cloud-based services, the channel can leverage an increasingly broad array of options to deliver services to customers. By tracking and responding to the trends outlined in this paper, resellers and distributors can begin to more fully exploit the opportunities available.

About the Survey
During fall 2012, SafeNet conducted a survey of more than 50 respondents who work in the channel. Respondents from across the Europe, Middle East, and Africa region participated.

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