An Overview and Competitive Analysis of the One-Time Password (OTP) Market
Introduction ............................................................................................................................ 3
OTP Market Landscape ......................................................................................................... 4
  Market Drivers .................................................................................................................. 5
Competitive Analysis ............................................................................................................. 7
  RSA, the Security Division of EMC .................................................................................... 7
Key Performance Drivers for RSA ........................................................................................ 8
Conclusion .............................................................................................................................. 9
INTRODUCTION

Over the past year, data breaches have impacted organizations of all types and sizes; from large organizations to small businesses or governmental agencies, nobody is immune. As a result, firms continue to invest in—and prioritize—information security. From an industry perspective, variations are evident. For example, while the financial services, IT and government sectors emphasize security strategy as a high priority, entertainment and travel companies invest less in this area.

With the explosion of smartphone adoption, the number of people making purchases via a mobile device has increased significantly. As eCommerce became m Commerce, payment security became an area of considerable focus. During a “card not present” payment process, a personal account number (PAN), expiration date, and card validation code (CVC) are not enough to completely secure the transaction. However, new mechanisms such as 3D Secure appear to increase the confidence of both consumers and eMerchants.

However, protecting a mobile device itself is necessary to ensure that only the owner is able to use it. Although a simple mechanism such as a personal identification number (PIN) can perform this task, in 2011, more than 60% of smartphone users were not using a PIN to protect their mobile device.

Traditional password protection is not enough. Statistically speaking, well-known passwords such as “1234”, “password” or “love” allow hackers to access personal data in 20% of the cases. If this hacking strategy is coupled with a range of tools to obtain personal data (written piece of software, keylogger, etc.) the chance to break the password could reach 55%.

In order to decrease the number of security breaches due to phishing, keyboard logging, man-in-the-middle attacks or other methods, companies are integrating mobile OTP (one-time password), OTP tokens and USB tokens. The OTP solution adds another level of security protection as the use of a temporary password strongly protects network access and end users.
OTP MARKET LANDSCAPE

Due to the widespread adoption of the Internet and wireless devices, there is a specific need to fully secure digital home networks and associated services. The emergence of mobile payments (online payment by using website platform or specific application) has increased this security need. Strong authentication solutions improve the security level by incorporating another security measure to overcome the weaknesses and limitations of static passwords.

As shown in Figure 2, the global OTP market is growing at a compound annual growth rate (CAGR) of 7.5%. In 2012, the market was valued at $824.7 million and is projected to grow to $1.189 billion by 2017.
OTP market revenue is driven by hardware and the USB Token market. This source of revenue generates 83.7% of the total OTP market. The dominance of these revenue sources is not a surprise, as these solutions are adopted by a significant proportion of companies. This type of additional security measure has prompted rapid development of OTP solutions to deliver a cost-effective solution to corporate clients. Verticals such as physical and logical access, online payment or online gaming are the main areas of development. But the wide distribution of smartphones and tablets, coupled with new usage cases such as BYOD, are further boosting demand for OTP solutions. Both enterprises and financial institutions will be motivated to invest in hardware OTP solutions, even if the software OTP market continues to be attractive. It generated 16.3% of revenue for the total OTP market.

**MARKET DRIVERS**

As the volume of threats and the variety of breaches continue to grow, security protection is a constant battle for companies. This year, a higher level of scale was reached when the US government reported that more than 94 million records (containing personal information) have been exposed since 2009 in the US alone. Nearly 81 million of these were due to the loss or theft of mobile devices. High-profile instances involving major companies have also emerged. For example, Yahoo! was attacked in July 2012, with a reported 400,000 plain-text passwords stolen. Apple also revealed that a million Apple Unique Device Identifiers (UDIDs) were hacked in September 2012. The proliferation of identity theft and data breaches is the result of single-factor methods of authentication or weak passwords. Figure 3 describes the most influential market drivers that increase demand for OTP solutions.

**Figure 3– Total OTP Market: Key Market Drivers (Global), 2013-2018**

<table>
<thead>
<tr>
<th>Market Drivers</th>
<th>1-2 years</th>
<th>3-4 years</th>
<th>5 years</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance with legislations, regulations and standards</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>Need for two-factor authentication</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>Security cost rationalization</td>
<td>H</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td>Proliferation of Identity theft and data breaches</td>
<td>H</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>BYOD and cloud applications promote OTP adoption</td>
<td>H</td>
<td>M</td>
<td>M</td>
</tr>
</tbody>
</table>

*Source: Frost & Sullivan*

- **Compliance with legislations, regulations and standards**: With the recent controversy information regarding NSA activity and the PRISM program, citizens will probably be less reluctant to use strong authentication methods to access the network or their personal data. With data security as a current major focus point, compliance regulations and legislation continue to push organizations to use technology that will effectively ensure the proper handling of sensitive data. This is particularly true for payment and financial purposes with the Federal Financial Institutions Examination Council (FFIEC) and the Payment Card Industry Data Security Standard (PCI-DSS), but is also
needed to protect health data following the Health Information Technology for Economic and Clinical Health (HITECH) act. The emergence of governmental online services such as tax declaration has compelled OTP solution providers to adhere to Identification-Authentication-Signature European Citizen Card (IAS-ECC) in Europe.

- **Need for two-factor authentication**: This authentication method is now the most popular globally and could drastically reduce the incidence of online security breaches. As the name suggests, this solution provides two means of identification: something that the user has (token) and something that the user knows (PIN). This is a minimum requirement for network access or digital identification. Some industries are already looking to stronger authentication methods, such as three-factor authentication, by adding biometric data.

- **Security cost rationalization**: Overcoming legacy hardware token authentication is a challenge for many organizations. Whether it be changing OTP providers or switching to software-based authentication solutions, a change requires IT decision-makers to be open-minded. With further education, decision-makers have come to understand the benefits of software-based authentication and the use of more than a single form factor. OTP vendors are working to change the perception of complex deployments by developing platforms that promote interoperability and multiple forms of two-factor authentication. The multiple network security breaches of 2012 that affected entities such as LinkedIn, Nationwide Insurance and Apple have proven that any organization can be a target, or susceptible to either a highly sophisticated attack or a small vulnerability in an application.

- **Proliferation of identity theft and data breaches**: 2012 was the year of data breach proliferation, not only due to the increasing number of attacks, but also by the emergence of large-scale data breaches. As the total number of Internet/mobile connections and online payments has drastically increased, so has the total number of identity thefts and data breaches. Identity theft gives a really negative influence to the market when it impacts bank accounts security. This influence is lower when it comes from social media accounts security. The emergence of mobile and online payment solutions created a specific need to protect data and deliver enhanced security. The lack of international rules for data protection allows the OTP solution to be seen as a trustable service by providing an easy-to-install security solution.

- **BYOD and cloud applications promote OTP adoption**: The explosion of smartphones and tablets has changed the way people use professional and personal communication devices. The use of professional tablets is minor compared to consumer tablets. Indeed, globally, the average percentage of professional tablets shipped will be 0.8% (2012-2017) when in the same time consumer tablets will reach 92.9% (2012-2017) and E-Readers 6.3% (2012-2017). Finally, Mobile Device Management (MDM), Identity Access Management (IAM) and even NFC payment are moving into the cloud. This trend is the perfect answer to accelerate adoption of services and to decrease total investment costs. However, the security of the cloud should be aligned to company policies. OTP, in that case, is an accurate answer. The solution is accessible at any time, from any device, and anywhere.
COMPETITIVE ANALYSIS

The security industry is evolving rapidly in response to the explosion of mobile devices and the emergence of new usages such as mobile payment and remote access. Only simple solutions coupled with minimal investment will survive in this competitive landscape. The need to have an authentication solution that is easy to use and that can allow a Single Sign On (SSO) element is crucial. But an optimized, secured solution should also reach a high level of security by providing reliable and strong authentication. OTP authentication vendors have understood these market constraints and provided a broad range of authentication solutions in 2012.

Competitive positioning within the global 2012 OTP market is shown in Figure 4. In 2012, RSA confirmed its leadership position with a broad product portfolio and large choice of form factors.

Figure 4–Total OTP Market Competitor Positioning Analysis (Global), 2012

Source: Frost & Sullivan

RSA, THE SECURITY DIVISION OF EMC

RSA has developed a popular set of solutions for authentication. For the enterprise market, the firm is seen as the most secure partner for two-factor authentication. For many years, RSA has created a complete two-factor authentication product portfolio. These solutions can be coupled with RSA’s authentication manager in order to centralize all security tokens and user profiles.
As shown in Figure 5, RSA led the market with 45.1% revenue share within the global OTP market in 2012.

**Figure 5–Total OTP Market Percent of Revenue (Global), 2012**

Today, a static security solution is insufficient, and the need for a real-time and dynamic security solution is clear. Much like banks and financial institutions that are using risk management to optimize payment security levels, RSA has decided to use risk management to enhance its authentication services to better answer specific security requirements.

**KEY PERFORMANCE DRIVERS FOR RSA**

**Wide Range of Innovative Products**

With more than 30 years of experience in the authentication business, RSA has built a solid reputation of reliable authentication solutions by using the latest security standards and strong cryptography mechanisms. Most of these technologies are patented, and as such, guarantee a strong market footprint. Authenticators could be used for authentication management, but also to encipher and protect hard disks or to generate digital signature for emails or during data transactions.

**Personalized and Best-in-Class Solutions**

RSA designed its business strategy by employing a customer-centric approach. Multiple form factors and options (such as authentication manager) are available. For an enterprise or an individual, a customized solution is crucial, as long as it is coupled with a reliable token. RSA has developed convenient products that are aligned with client expectations. Consequently, SMBs are able to find secure solutions to protect their network access. SMBs that were reluctant to deploy authentication solutions because of the high investment cost can now use cost-effective, risk-based and on-demand authentication systems.
**Flexibility**

RSA has designed all of its products in order to facilitate final integration with a minimum of time and money. RSA solutions can be easily installed with more than 400 partner solutions used for network access, VPN or firewall. This strategy offers true benefit, as RSA product deployment does not need specific project or long-term investment. RSA’s OTP products are designed to be compatible with all major physical software platforms or virtual ones such as VMware. The architecture of the solution grants replication and evolution of the entire system.

As a result, RSA’s products offer flexibility and control over total investment.

**CONCLUSION**

The OTP market is evolving from the hardware form factor to solutions answering the need for mobility and flexibility. The shift to more mobile-centric demand is driven by the widespread adoption of mobile devices and mobile payment/banking solutions. Enterprises are looking for specific security solutions in order to avoid data breaches and identity theft. At the same time, new requirements have emerged such as email encryption, digital signature and mobile access. Most OTP vendors have evolved their traditional product portfolio to better answer the changing needs of end users. As a result, the software OTP market is growing and many OTP vendors are providing specific credentials for NFC or Bluetooth purposes. OTP is moving to software-based solutions to leverage mobile devices as trustable identity providers.
ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today’s market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies? Contact Us: Start the Discussion

For information regarding permission, write:
Frost & Sullivan
331 E. Evelyn Ave. Suite 100
Mountain View, CA 94041