

An Overview and Competitive Analysis of the One-Time Password (OTP) Market



A Frost & Sullivan White Paper
Prepared by Martha Vazquez,
Research Analyst

TABLE OF CONTENTS

Introduction	3
Brief Overview of the OTP Market	3
Market Drivers	4
Competitive Analysis	5
RSA, The Security Division of EMC	6
Key Performance Drivers for RSA	7
<i>Strength of Security</i>	7
<i>Interoperability</i>	7
<i>Worldwide Well-Known Brand Name</i>	8
Conclusions	8
About Frost & Sullivan	9

INTRODUCTION

Attackers continue to be bolder, more creative, and technically savvy with regards to gaining pertinent user passwords. End-users increasingly divulge sensitive information on social networks, information that cyber criminals can use in order to guess end-user passwords. As the usage of social networks continues to increase, the need for stronger protection is more important than ever before.

In addition to weak password protection, the workforce is drastically changing and more employees are working remotely, driving the need for strengthened password protection solutions. In order to ensure the best information security possible, it is crucial that a password be regularly modified since weak passwords and Personal Identification Numbers (PINs) are the primary reasons for security breaches.

The hardware and software authentication devices market is witnessing increasing growth in revenues. Companies integrating mobile OTP, OTP tokens and USB tokens into their networks decrease the risks of data breach and improve their overall security posture. As the authentication market progresses, organizations will look at purchasing advanced security technology that will protect their information and that of their clients by requiring a user to have multiple factors of identification before gaining access to a workstation or network device. This significantly reduces the possibility of theft and prevents the compromise of an entire system due to a compromised password.

BRIEF OVERVIEW OF THE OTP MARKET

As shown in Figure 1, the World OTP Market was valued at \$461 million in 2009, and the revenues are likely to increase to \$741.5 million by 2017, at a compound annual growth rate (CAGR) of 6.2 percent over the period 2009 to 2017.

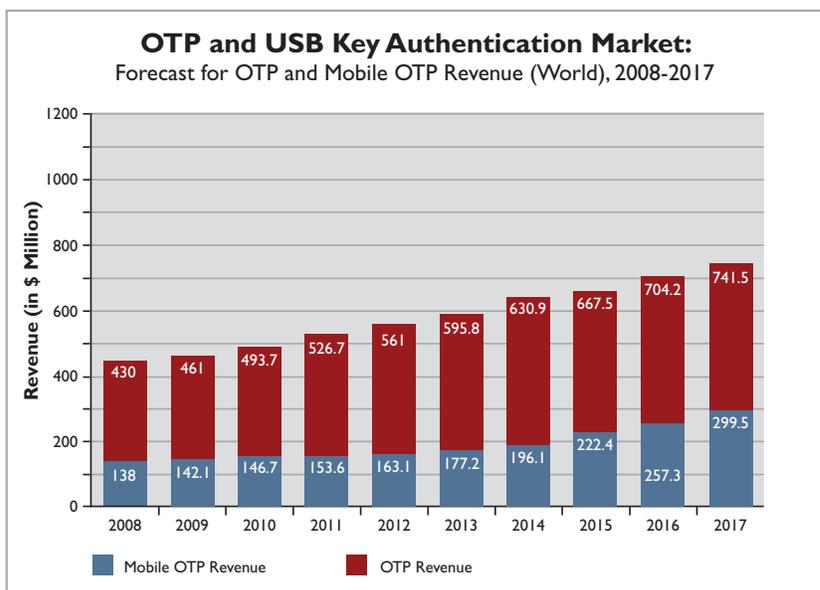


Figure 1—OTP and USB Key Authentication Market: OTP Tokens Revenue (World), 2008–2017

The OTP token segment will continue to dominate the hardware authentication device market, segments such as USBs and mobile OTPs will slowly represent less of the OTP token market. In addition, USB tokens are gaining in popularity, as they have the ability to merge the functions of both OTP and smart cards in a hybrid USB token.

Almost all of the competitors in the market have an OTP token offering, and some of the same companies are offering USB tokens, smart cards, mobile OTP and authentication management systems. Companies such as RSA understand that authentication is no longer composed of only one hardware device, but from myriad authentication methods to meet the needs of a wider user base and new authentication requirements. This approach made most vendors develop products adapted to specific needs as well as a robust management system that can manage all products and services relating to authentication and more complex deployment environments.

Many vendors in the OTP market are trying to differentiate themselves from the competition. Vendors are not only looking at offering a large spectrum of authentication solutions, but are also trying to focus their efforts on developing and upgrading the authentication management systems.

MARKET DRIVERS

The protection of network systems and personal identification has become a critical solution for businesses to adopt. Table I lists the most influential drivers for the global OTP and USB authentication market. These drivers include the weakness of passwords, compliance, and the need to secure remote users.

Rank	Drivers	1-2 Years	3-4 Years	5-7 Years
1	Weakness of Passwords	High	High	High
2	Compliance with Legislations, Regulations and Standards	High	High	High
3	Need to Authenticate and Secure Remote Access Users	High	High	High
4	Identity Theft and Phishing Attacks	Medium	Medium	Medium
5	Cost of Supporting Passwords	Medium	Medium	High
6	Efficency of Digital Signature Laws and PKI	Medium	Medium	High
7	Ease of Use of Tokens	High	Medium	Medium

Table I—One-Time Password and USB Key Authentication Markets: Drivers Ranked in Order of Impact, (World) 2009-2017

The top driver for this market is the inherent weakness of user passwords. Users are typically required to log in to workstations using the combination of a user name and password. Since most users will typically choose an easy password combination, it is likely the user password can be obtained through social engineering, physical force or guessing. As a result, organizations have adopted more complex password policies. Since these

policies are typically expensive to maintain due to systems administration costs, solutions such as single sign-on (SSO) systems significantly reduce password management problems for the end-user. However, they can be expensive and complicated to deploy, and do not address the fundamental problem of the ease with which passwords can be compromised. For these reasons, organizations now turn to mobile OTP, OTP and USB authentication solutions.

Maintaining compliance due to legislation, regulations and standards is another strong driver for enterprises in implementing stronger authentication solutions. The business paradigm for workers and consumers has changed significantly over the years. Now more than ever, employees are working outside of the office. In addition, consumers and small businesses are conducting work from home or when traveling. As online services are booming, solutions such as IPSEC and SSL VPNs are the most popular and secure solutions for remote access. However, in such instances, the verification of remote access users is essential. Today, authentication vendors can promote increased network security by selling mobile OTP, OTP and USB devices separately or as an integrated solution into a Virtual Private Network.

As shown above, there are other drivers in this market, but all the drivers revolve around the increased risk that organizations take on if end-user passwords are not secured.

COMPETITIVE ANALYSIS

OTP authentication vendors have two key challenges to contend with: the challenge of interoperability and the need for a new approach to the consumer hardware authentication device market. The requirement for interoperability implies that OTP tokens have to be designed to interface with existing networks, no matter the specifications, multiple protocol standards, or products from other vendors. However, the typical customer network contains various generations of products added over time as the network grew. To meet these requirements, OTP tokens are thus expected to interoperate with most, if not all, of the products within these networks.

There is also a need for a new approach to the consumer hardware authentication device market. The consumer market has the potential to be much larger than the enterprise market. This makes the consumer market an attractive market for vendors. Today, the available hardware authentication solutions do not yet meet the needs of the consumer in terms of cost, manageability, deployment mechanisms, privacy concerns, and so on. Consequently, another challenge for the industry is to develop technologies and products that address the needs of the consumer identity market, taking advantage of the market opportunities therein.

In 2009, Frost & Sullivan tracked 15 vendors participating in the hardware authentication devices market. Established vendors such as RSA and VASCO remain the overall leaders in the market with a combined 79.3 percent market share. However, it is important to note that RSA is the dominant player in this market, with 62.7 percent of the market share.

Figure 2 shows the competitive landscape of the OTP market. Frost & Sullivan believes RSA will remain the market leader with a dominating percentage of market shares in the near future. RSA, like most OTP vendors, understands the current trends in the strong authentication market and has added security solutions to its portfolio, including knowledge-based authentication, software tokens and risk-based authentication. Most vendors are already offering solutions that fit the current trends and are competing for market share in the new strong authentication market.

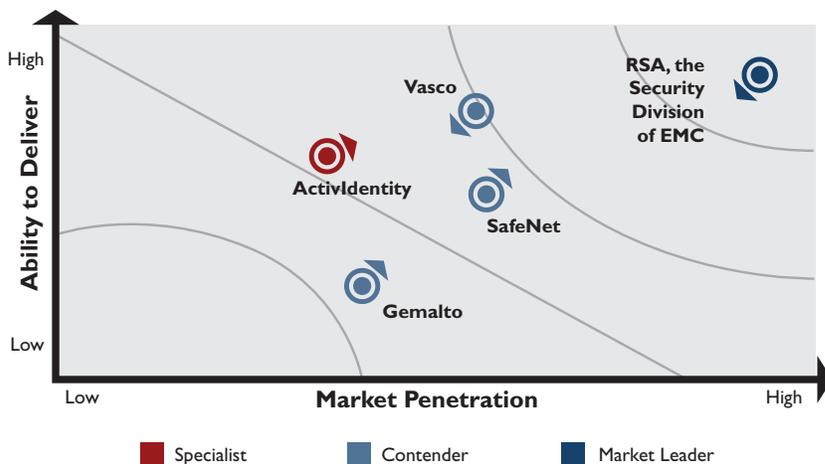


Figure 2—Competitive Landscape for OTP Market

RSA, THE SECURITY DIVISION OF EMC

As shown in Figure 3, RSA held 62.7 percent market share in the OTP token segment in 2009.

World OTP Key Market Share Distribution
Market Share by Vendor (2009)

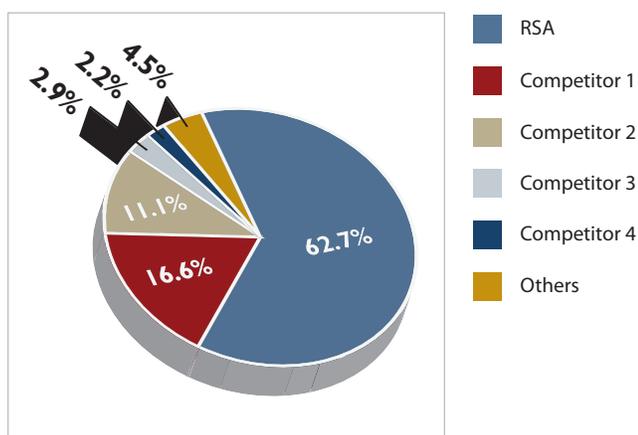


Figure 3—World OTP Market Share Distribution by Vendor (2009)

RSA, OVERALL AUTHENTICATION MARKET

As shown in Figure 4, RSA held 51.3 percent market share in the total overall authentication segment in 2009.

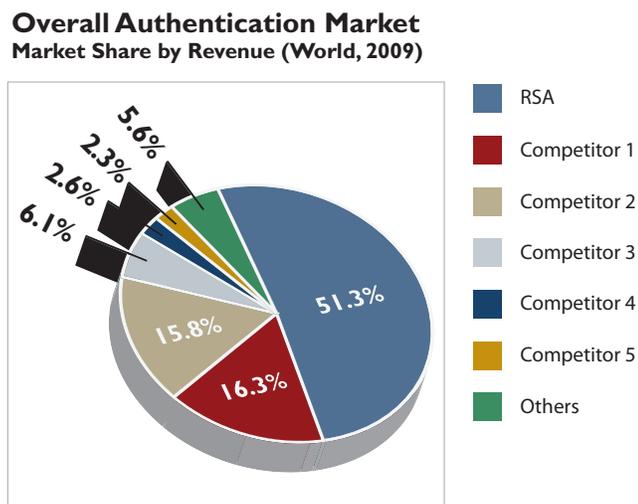


Figure 4—Overall Authentication Market Market Shares by Revenue, World 2009

RSA provides a broad range of offerings for guarding the integrity and confidentiality of information, including identity assurance and access control, data loss prevention, encryption and key management, compliance and security information management, and fraud protection. Authentication remains a priority for RSA, where it maintains leadership in OTP and risk-based authentication. RSA continues to expand and innovate the SecurID OTP portfolio to include mobile software tokens, SMS authentication, hybrid authenticators and virtual credentials. Additionally, RSA provides biometric and USB Flash solutions, through partnerships, allowing organizations to choose the solution that best meets their user, risk, and security requirements.

RSA's SecurID product dominates the market and is in many ways synonymous with hardware authentication. A two-factor authentication solution, SecurID provides a reliable level of authentication thanks to the combination of a PIN and an authenticator that has a one-time password changing every 60 seconds. Consequently, SecurID offers safer authentication protocol than reusable passwords and event-based OTPs.

RSA continues to expand the RSA SecurID portfolio to include mobile OTP software tokens, SMS authentication, as well as hybrid USB authenticators. Offering these innovative solutions allows organizations to choose the solution that best meets their user, risk and security requirements. Recently, RSA delivered a new mobile authenticator for iPhone, a secure token application. RSA also differentiates itself from its competitors with investments in the Authentication Manager server. The Authentication Manager server allows for robust administration, credential lifecycle management and end-user self-service,

allowing organizations to manage support costs, a major cost factor in authentication solutions. The combination of SecurID and RSA's offerings in risk-based and knowledge-based authentication provides companies with the tools they need to create the most appropriate layered solution for their organization.

KEY PERFORMANCE DRIVERS FOR RSA

Strength of Security

The RSA SecurID product is a two-factor authentication solution. SecurID provides a reliable level of authentication thanks to the combination of a PIN and an authenticator that has a one-time password that changes every 60 seconds. SecurID provides users highly secure anytime, anywhere access to VPNs, wireless access points, Web applications, network operating systems and more, thanks to a password combination nearly impossible to hack or guess. SecurID offers safer authentication protocol than reusable passwords and event-based OTPs.

Interoperability

RSA's OTP Authenticators are designed to suit as many customers' existing networks as possible, no matter the specifications, multiple protocol standards or products from other vendors deployed. RSA Authentication Manager is interoperable with many of the major network infrastructure and operating system products on the market. More than 400 products from more than 200 vendors are interoperable with RSA OTP tokens. Consequently, RSA's products contribute to an organization's greatest flexibility and investment protection.

Worldwide Well-Known Brand Name

RSA has established itself as an incontrovertible OTP tokens vendor. In order to secure its leadership position, RSA has entered markets worldwide to the extent that it is now present in more than 50 countries. Concentrating its activities in the American continent and in Europe, Middle East and Africa (EMEA), RSA is now entering emerging markets such as China, Singapore and Latin America. It has also diversified its vertical market penetration and, although the financial sector remains its field of predilection, it is also present in markets such as the government, defense, retail, manufacturing, telecommunication, transportation, and consulting. RSA is dedicated to developing closer relationships with its clients. As such, both a high degree of market penetration and loyal consumer behavior ensure RSA's leadership in the OTP token market.

CONCLUSIONS

The landscape of the OTP market is changing as more organizations are searching for convenient solutions such as mobile authenticators. Growth in the market will center on providing these types of alternative mobile solutions for end-users. The increasing popularity of remote workers and mobile employees represents an opportunity for OTP vendors to increase their user base. As a result, industry participants are likely to develop competitive advantages around superior service-orientated propositions—diversifying authentication methods and management systems.

CONTACT US

Auckland
Bangkok
Beijing
Bengaluru
Bogotá
Buenos Aires
Cape Town
Chennai
Colombo
Delhi / NCR
Dhaka
Dubai
Frankfurt
Hong Kong
Istanbul
Jakarta
Kolkata
Kuala Lumpur
London
Mexico City
Milan
Moscow
Mumbai
Manhattan
Oxford
Paris
Rockville Centre
San Antonio
São Paulo
Seoul
Shanghai
Silicon Valley
Singapore
Sophia Antipolis
Sydney
Taipei
Tel Aviv
Tokyo
Toronto
Warsaw

Silicon Valley
331 E. Evelyn Ave. Suite 100
Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10, Suite 400,
San Antonio, Texas 78229-5616
Tel 210.348.1000
Fax 210.348.1003

London
4, Grosvenor Gardens,
London SW1W 0DH, UK
Tel 44(0)20 7730 3438
Fax 44(0)20 7730 3343

877.GoFrost
myfrost@frost.com
<http://www.frost.com>

ABOUT FROST & SULLIVAN

Based in Mountain View, California, Frost & Sullivan is a global leader in strategic growth consulting. This white paper is part of Frost & Sullivan's ongoing strategic research into the Information Technology industries. Frost & Sullivan regularly publishes strategic analyses of the major markets for products that encompass storage, management, and security of data. Frost & Sullivan also provides custom growth consulting to a variety of national and international companies.

The information presented in this publication is based on research and interviews conducted solely by Frost & Sullivan and, therefore, is subject to fluctuation. Frost & Sullivan takes no responsibility for any incorrect information supplied to us by manufacturers or end-users. All copyright and other proprietary notices must be retained. No license to publish, communicate, modify, commercialize or alter this document is granted.

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