



The Security Division of EMC

RSA Solution Brief

RSA Adaptive Authentication

Offering Multiple Ways to Provide Strong
Two-Factor Authentication to End Users

The state of passwords today is similar to that of the horse and buggy at the turn of the 19th century. With the advent of the automobile, the reliable and ubiquitous horse and buggy soon became obsolete. Today, the environment is such that organizations are realizing that passwords must also give way to stronger, more effective solutions. In its place, strong authentication is becoming the de facto standard for assuring user identities in the online world. RSA® Adaptive Authentication is at the forefront of this trend by offering a strong authentication solution that not only adds a layer of security on top of existing username and password systems, but does so in a way that is convenient for the end user.

The Basics of Strong Authentication

Strong authentication is also commonly referred to as two-factor authentication or multi-factor authentication. This alludes to the fact that there is more than one factor, or proof, needed in order for an authentication to be made. Some factors include:

- What a user knows (i.e., a password or challenge question)
- What a user has (i.e., a security token or mobile phone)
- What a user is (i.e., a biometric device)
- What a user does (i.e., patterns of behavior)

When only one factor is utilized to authenticate a user, it is considered to be a weak form of authentication. Multi-factor authentication may include multiple types of the same authentication method (for example, two static passwords) but would not necessarily be considered strong authentication.

RSA Adaptive Authentication: Multi-factor Authentication

- Something you have:
Device identification
- Something you are/do:
Behavioral profile
- Something you know:
Username and password
(not managed by RSA
Adaptive Authentication)

The Basics of RSA Adaptive Authentication

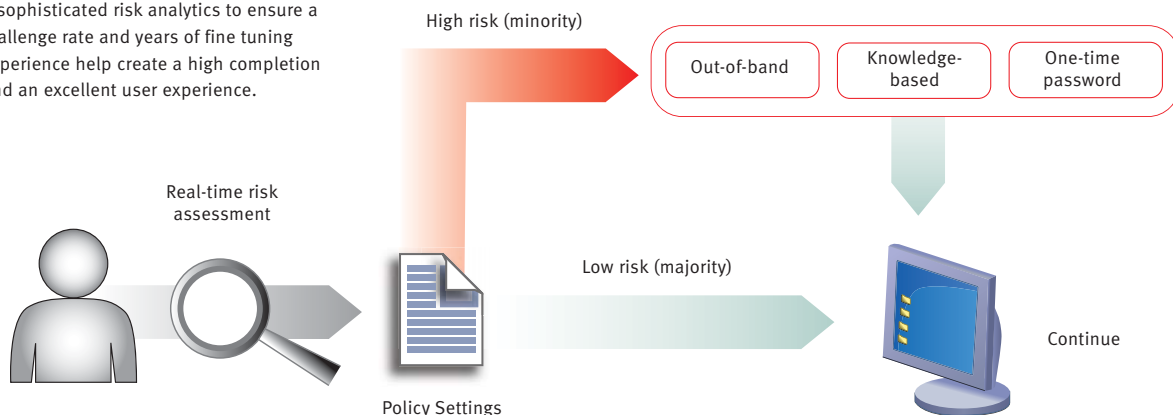
RSA Adaptive Authentication is a comprehensive authentication and risk management platform offering numerous authentication options and providing cost-effective protection for entire groups of users. At its core, Adaptive Authentication is designed to determine when to visibly authenticate users and what type of authentication method to use. These decisions are based on risk levels, institutional policies, and customer segmentation.

Adaptive Authentication combats existing and emerging fraud trends by analyzing device identification data, behavioral profiles, activity patterns, RSA eFraudNetwork™ feeds, multi-channel threat indicators, and fraud intelligence, all integrated into a single platform that is constantly evolving to reflect ongoing changes in the fraud landscape. Adaptive Authentication is currently deployed at over 8,000 organizations worldwide and has processed and protected over 20 billion activities to date.

The key benefits of Adaptive Authentication include:

- Superior user experience (lowest impact on genuine users and highest fraud detection rates)
- Numerous authentication methods with customizable risk and authentication policies
- Strong and convenient protection against malware that can be deployed invisibly and flexibly
- The ability to protect across multiple channels including the online and mobile channels and the IVR/Call Center
- A proven solution deployed at over 8,000 organizations and protecting more than 150 million users worldwide

The RSA Adaptive Authentication solution offers sophisticated risk analytics to ensure a low challenge rate and years of fine tuning and experience help create a high completion rate and an excellent user experience.



Adaptive Authentication Meets the Requirement for Multi-factor Authentication

Traditionally, security solutions meet the requirement for two-factor authentication by requiring users to provide a username and password and an additional credential, such as a one-time password or smart card, every time they access their account information online. However, when using Adaptive Authentication, organizations utilize a risk-based approach that only visibly authenticates users when they exceed a given risk threshold (pre-determined by the organization). If most users are being authenticated behind-the-scenes, does that still meet the standard of strong authentication? The answer is yes.

Something the User Has

RSA Adaptive Authentication always uses a second factor even though the initial authentication is performed transparent to the user. When necessary, RSA performs several authentication procedures behind-the-scenes, including invisible device identification. If a user's device is positively identified and associated with the user (and not with fraudulent use), then the user is considered authenticated. In this case, the device being used to request access is the second factor in strong authentication – “something you have.”

Adaptive Authentication can conduct device identification by fingerprinting the user's device. Device fingerprinting consists of tracking device characteristics that are a natural part of any device such as http headers, operating system versions, browser version, languages, and time zone. Furthermore, device fingerprinting actively introduces additional identifiers with the simple addition of a cookie and/or a flash shared object (also referred to as “flash cookie”) which can then serve as a more unique identifier of the device.

When a user's identity is not positively assured via device authentication, they are challenged using a variety of methods including:

- Challenge questions: Something the user knows
- Knowledge-based questions: Out-of-wallet versions of something the user knows
- Out-of-band phone authentication: Something the user has
- One-time passwords (via SMS, e-mail, token): Something the user has

By authenticating a user with one of these other methods, the device will be established as a “trusted” device in the future.

Something the User Does

When thinking about the factor “something you are,” one usually thinks of biometrical measurements, such as a fingerprint or iris scan, as the authentication method. However, a user’s behavioral pattern – what they typically do – can also be considered a version of “something the user is” or in this case, “something the user does.”

Examining factors such as the type of transaction or online activity, login time, IP-geo location, and transaction volume can help establish a typical behavioral profile for a given user. If something appears to be out of the user’s normal pattern of behavior based on the established profile of past activities, then they can be challenged visibly with methods such as challenge questions or out-of-band phone authentication. However, if the user’s pattern of behavior and device fingerprint match, then authentication will continue behind-the-scenes and the user will continue uninterrupted.

Something the User Knows

Adaptive Authentication is designed to allow for complete anonymity and protect the privacy among the end users being authenticated by the system. The system does not ever know the user’s name or password; this should be asked for and stored by the deploying organization. The username and password combination is the first factor – “what you know” – and becomes multi-factor when combined with Adaptive Authentication.



The Security Division of EMC

RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

©2008 RSA Security Inc. All Rights Reserved.
RSA, RSA Security, eFraudNetwork and the RSA logo are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. EMC is a registered trademark of EMC Corporation. All other products and services mentioned are trademarks of their respective companies.

AATF SB 0808

Conclusion

RSA Adaptive Authentication offers strong authentication by providing a layer of security in addition to something the user knows – their username and password. Even though a majority of authentication requests are conducted transparently to the user, Adaptive Authentication still provides strong multi-factor authentication. Invisible device identification determines what the user has – their device – while behavior analysis determines what a user is or does. The combination of these factors creates a solution that offers strong authentication and maximum convenience to the end user.

RSA is your trusted partner

RSA, The Security Division of EMC, is the premier provider of security solutions for business acceleration, helping the world’s leading organizations succeed by solving their most complex and sensitive security challenges. RSA’s information-centric approach to security guards the integrity and confidentiality of information throughout its lifecycle – no matter where it moves, who accesses it or how it is used.

RSA offers industry-leading solutions in identity assurance & access control, data loss prevention, encryption & key management, compliance & security information management and fraud protection. These solutions bring trust to millions of user identities, the transactions that they perform and the data that is generated. For more information, please visit www.RSA.com and www.EMC.com.