



Adaptive Authentication in Healthcare Environments

The Growth of Healthcare Portals

Physician and patient portals to facilitate information exchange are becoming an important part of healthcare organizations' patient care delivery, marketing, and administration workflow. Healthcare organizations of all sizes are responding to the demands of patients, physicians, payers, and employees for better access to information and services. Portal implementations are thereby viewed as a cost-effective, productivity tool and a means of increasing revenue and providing safer patient care.

Portals provide access to patient information, clinical and business applications, processes, and resources throughout the organization. Physicians use web portals as a productivity tool to streamline clinical workflow and increase billable services. Patients use web portals to register and schedule appointments, communicate securely with physicians, check account status, make online bill payments, store their health history, and participate in e-visits. And payers may use web portals to help submit and settle claims, communicate Explanation-of-Benefits (EOBs), and membership changes. As more healthcare organizations deploy web-based portals, they must implement stronger security measures in order to protect against unauthorized access to sensitive patient data and meet regulatory compliance demands.

The Need for Secure Remote Access

Today, it is widely recognized that the use of password-only protection as the sole method of assuring the identities of remote users through infrastructure such as virtual private networks (VPNs) and web access management (WAM) applications represents a significant security threat to organizations. Single-factor protection provides one central point of attack for a hacker and, once defeated, can result in incidents such as a security breach, financial loss, or loss of patient data or personally identifiable information (PII).

Concurrently, many IT departments are grappling with business requirements to extend the accessibility of enterprise applications to an even broader audience – including vendors, suppliers, partners and even customers. Doing so could place demands on already strained IT budgets and head count to effectively manage endpoints over which the organization may have little or no control.

The Right Choice for Authentication

Whether your healthcare organization is concerned with securing portal access or remote application access, a solution that is proven, offers a method of strong two-factor authentication and is cost-effective for an entire user population is what will meet the guidelines.

RSA® Adaptive Authentication is a comprehensive authentication and fraud detection platform providing cost-effective protection for your entire user base. It monitors and authenticates activities based on risk, policies, and users by



The Security Division of EMC

Is Risk-Based Authentication (RBA) Really Secure?

In order to compromise Risk-Based Authentication technology, a criminal would need to have access to four different types of information: (1) the username and password, (2) the device identifiers, (3) the forensic device information and (4) the IP information for imitating the user's behavior.

Moreover, each of these categories consists of many elements. Consider the forensic information which contains several dozen data points that would be extremely difficult to mimic precisely. To steal forensic information, a criminal would need to change the form submissions on every post. Or to steal IP information, a criminal would need to put a proxy on the legitimate device which, while possible, is an extremely difficult task.

correlating device identification profiles, behavioral patterning profiles, RSA® eFraudNetwork™ feeds, user profiles, and fraud intelligence.

A variety of authentication methods exist that can be used on top of the Adaptive Authentication platform including:

- **Invisible authentication.** Device identification and profiling
- **Out-of-band authentication.** Phone call, SMS, or e-mail
- **Challenge questions.** Challenge questions or knowledge-based authentication (KBA)
- **Multi-Credential Framework.** For organizations wanting more choices, Adaptive Authentication is designed to easily integrate with a large selection of other authentication methods. The Multi-Credential Framework allows organizations to develop authentication methods via RSA Professional Services, “in-house” or through third parties to customize Adaptive Authentication.
- **Site-to-user authentication.** Site-to-user authentication assures users they are transacting with a legitimate website by displaying a personal security image and caption that has been pre-selected by the user at login.

By having the ability to support most existing authentication technologies, healthcare organizations that use Adaptive Authentication can be flexible in:

- How strongly they authenticate end users
- How they distinguish between new and existing end users
- What areas of the business to protect with strong authentication
- How to comply with changing regulations
- What they are willing to accept in terms of risk levels
- How to comply with the various requirements of the regions and countries where they operate

The Dynamics of Risk-based Authentication

Adaptive Authentication is powered by Risk-Based Authentication (RBA), a risk assessment and authentication technology that operates transparently and classifies all users by measuring a series of risk indicators. This transparent authentication for the majority of users provides for a convenient online experience as users are only challenged when suspicious activities are identified and/or an organizational policy is violated.

Risk-Based Authentication assesses the risk of each online activity and assigns a risk score based on the likelihood of that activity being legitimate. When an activity is identified as high-risk, a user can be challenged with a secondary form of visible “step-up” authentication such as a series of challenge questions. Finally, Risk-Based Authentication inspires user confidence in the online channel while enabling organizations to improve security beyond simple user names and passwords.

RSA's Risk-Based Authentication is powered by a series of core technologies – device profiling, behavioral profiling, the RSA® Risk Engine, the RSA® eFraudNetwork™, the RSA® Policy Manager, and the RSA® Multi-credential Framework.

Device Profiling

Profiling enables Adaptive Authentication to assure the identities of the vast majority of users transparently by comparing the profile of a given activity with their typical profile patterns. Device Profiling analyzes the device profile (the physical laptop/PC from which the user accesses the



website or application) and determines if the device is known as having been previously used by this user. The two main components of Device Profiling are Unique Device Identification and Statistical Device Identification.

Unique Device Identification distinguishes a device through the use of two main elements embedded on the user's laptop/PC –secure first party cookies and flash shared objects (sometimes referred to as “Flash cookies”). Statistical Device Identification is a technology that analyzes the characteristics of a device to statistically identify a user's device.

Behavioral Profiling

Risk-Based Authentication also uses behavioral analysis to identify high-risk authentication attempts. Some parameters that are measured include velocity checking, IP address information, and time of day comparisons. Behavioral Profiling analysis complements Device Profiling with user behavior to offer a form of multi-factor authentication that includes something you have (the device) and something you do (behavior).

RSA Risk Engine

The RSA® Risk Engine is a proven, self-learning technology that evaluates each online activity in real-time, tracking over one hundred indicators in order to detect fraudulent activity. A unique risk score, between 0 – 1000, is generated for each activity. The higher the risk score, the greater the likelihood is that an activity is fraudulent.

RSA Policy Manager

The RSA® Policy Manager enables organizations to instantly react to emerging localized fraud patterns and effectively investigate activities flagged as high-risk. The Policy Manager translates organizational risk policy into decisions and actions through the use of a web-based Rules Management application, comprehensive rules framework, real-time configuration, and Performance Simulator for testing prior to being put into production.

RSA eFraudNetwork

The RSA® eFraudNetwork™ is a cross-organization, cross-industry data repository of fraud patterns gleaned from RSA's worldwide network of customers, end users, ISPs, and third party contributors. The eFraudNetwork community is dedicated to sharing and disseminating information on fraudulent activity to help keep its members one step ahead of fraudsters. When a fraud pattern is identified, the fraud

data, activity profile, and device fingerprints are moved to a shared data repository. The eFraudNetwork enables real-time proactive protection to hundreds of millions of online users worldwide that are actively connected to the network and is one of the many sources that feeds the Risk Engine in determining risk.

RSA Multi-credential Framework (MCF)

The RSA Multi-credential Framework (MCF) provides an abstraction layer that enables one software platform to support multiple authentication methods (based on end user segment and risk assessment) in a single deployment. With the Multi-credential Framework, different authentication methods are leveraged through policy settings to accommodate different end user populations, different online products, and different risk levels.

On-Premise or SaaS / Hosted Deployment Options

Organizations worldwide currently deploy Adaptive Authentication in two ways – as an on-premise installation that uses existing IT infrastructure or as a hosted authentication service that helps to manage the end user lifecycle.

Is Risk-Based Authentication (RBA) Really Multi-factor Authentication (MFA)?

Risk-Based Authentication (RBA) is a definitive form of multi-factor authentication and uses multiple layers to achieve this.

- RBA is always applied on top of username and password (something you know: first factor)
- RBA always examines characteristics of the device (something you have: second factor)
- RBA always examines various user behaviors (something you do)

In addition to these three factors, “step-up authentication” can be invoked in the form of something you know (challenge questions) or something you have (out-of-band phone authentication) when an activity is determined to be high-risk or an organizational policy is violated.



Recognizing that no two organizations share the exact same user authentication needs, RSA offers the widest possible range of authentication, deployment, and customization options.

RSA has one of the world's largest security Software-as-a-Service (SaaS) practices, with more than 3,700 organizations relying on RSA Hosted Operations for a variety of our products that offer this delivery model. RSA Hosted Operations has been providing SaaS products for more than seven years in the areas of card authentication, web authentication, and identity verification.

Multiple Configuration Options

Adaptive Authentication can be configured in a number of ways to balance security and risk without compromising the user experience. Many organizations currently provide risk-

based authentication for their entire user base and allow the RSA Risk Engine to determine those individuals that require additional protection. Other organizations choose an appropriate supplemental form factor based on a user's preference or the types of activities they conduct.

A Proven Solution

RSA Adaptive Authentication is a proven solution that is currently deployed at over 8,000 organizations worldwide and across multiple industries including healthcare, financial services, government, insurance, automotive, real estate, manufacturing, and pharmaceuticals. It is currently being used to protect over 200 million online users and has processed and protected over 20 billion transactions to date.

RSA is your trusted partner

RSA, The Security Division of EMC, is the expert in information-centric security, enabling the protection of information throughout its lifecycle. RSA enables customers to cost-effectively secure critical information assets and online identities wherever they live and at every step of the way, and manage security information and events to ease the burden of compliance.

RSA offers industry-leading solutions in identity assurance & access control, 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.

©2009 RSA Security Inc. All Rights Reserved.

RSA, RSA Security, and the RSA logo are 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.

AAHC DS 0309



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