# RSA® ADAPTIVE AUTHENTICATION

## A comprehensive authentication and risk management platform

**As more organizations seek to migrate customers, members and partners to the cost-effective online channel, the need to instill confidence and implement stronger security measures becomes critical. In addition, online threats such as phishing, man-in-the-middle attacks, and Trojans are constantly evolving and organizations need to be concerned about deploying a long-term solution that can readily adapt to changes.**

**Achieving the right balance of authentication security without compromising the user experience or straining the budget is a challenge for many organizations. Even so, strong authentication is key to protecting sensitive data and increasing adoption of online channel usage. And, as most users now experience the implementation of stronger authentication when banking online, they have come to expect that same level of protection when accessing sensitive information at any site.**

### THE RIGHT CHOICE FOR AUTHENTICATION

RSA® Adaptive Authentication is a comprehensive authentication and risk management platform providing cost-effective protection for an entire user base. Adaptive Authentication monitors and authenticates user activities based on risk levels, institutional policies and customer segmentation and can be implemented with most existing authentication methods including:

- **Invisible authentication**. Device identification and profiling
- **Out-of-band authentication**. Phone call, SMS or e-mail
- **Challenge questions**. Question- or knowledge-based authentication
- **Multi-credential framework.** For those 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.** Assuring users that 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 intelligently support most existing authentication technologies, organizations that use Adaptive Authentication can be flexible in:

– How strongly they authenticate end users,

– How they distinguish between new and existing end users,

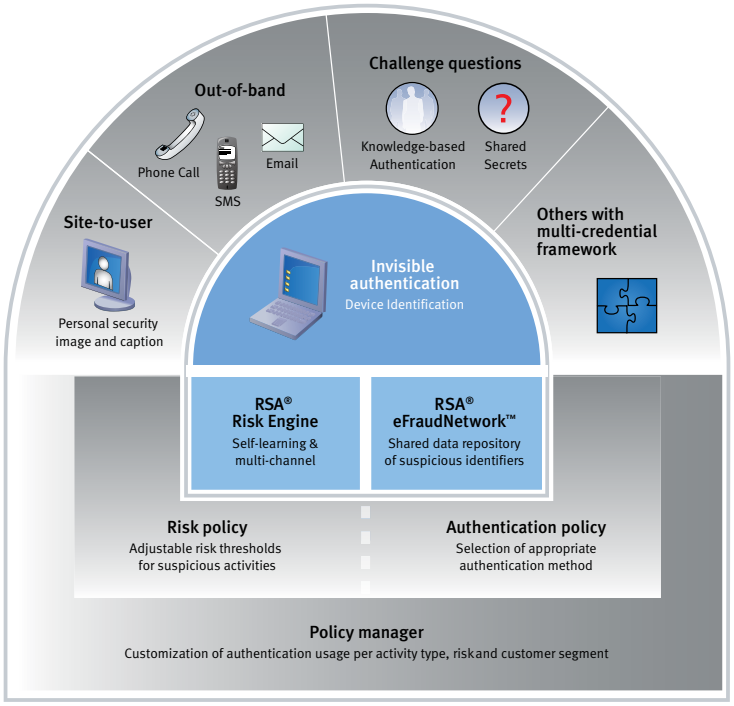
– What areas of the business to protect with strong authentication,

– How to comply with changing regulations,

– What they are willing to accept in terms of risk levels, and

– How to comply with the various requirements of the regions and countries where they operate.

**Adaptive Authentication is capable of supporting most existing authentication technologies.**




RSA risk-based authentication technology measures a series of risk indicators behind-the-scenes to assure user identities

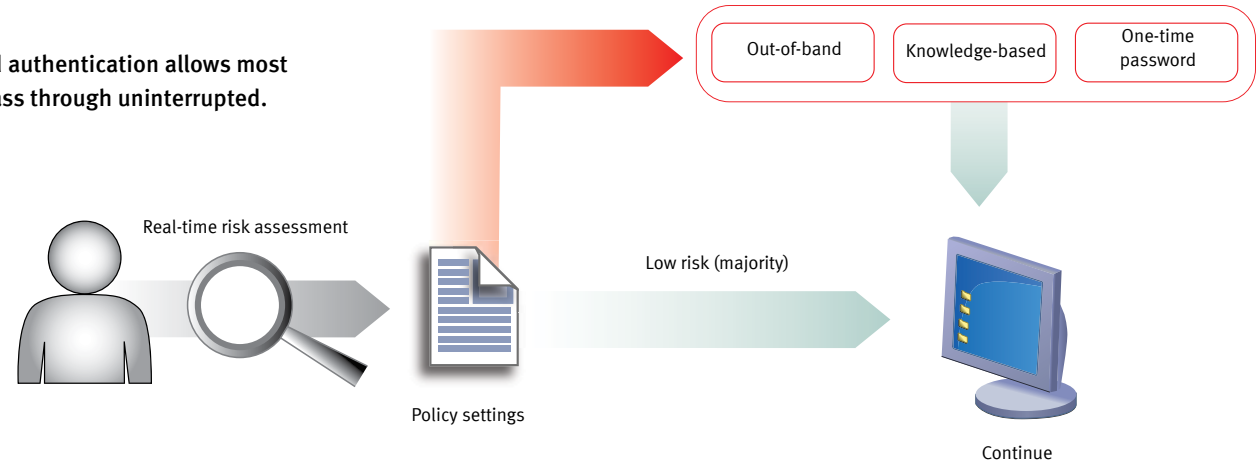
## THE DYNAMICS OF RISK-BASED AUTHENTICATION

Adaptive Authentication is powered by RSA risk-based authentication technology, a sophisticated system that measures a series of risk indicators behind-the-scenes to assure user identities. This transparent authentication provides for a superior user experience as users are only challenged in the highest risk scenarios or when an institutional policy has been violated. In addition, risk-based authentication is self-learning to help protect against Trojans, man-in-the-middle attacks and other forms of malware threats.

RSA risk-based authentication is powered by a series of core technologies – RSA device identification, the RSA® Risk Engine, the RSA eFraudNetwork™, the RSA® Policy Manager, and the RSA Multi-credential Framework.

RSA Device Identification helps enable transparent authentication for the vast majority of users by analyzing the device profile (the device from which the user accesses the server or network) and the behavioral profile (what activities the user typically performs), and matching the current activity against these profiles.

**Risk-based authentication allows most users to pass through uninterrupted.**




The RSA Risk Engine is 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 and 1000, is generated for each activity. The higher the risk score, the greater the likelihood is that an activity is fraudulent.

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 is used to translate organizational risk policy into decisions and actions through the use of a comprehensive rules framework that can be configured in real-time.

The RSA Risk Engine is self-learning technology that evaluates each online activity in real-time, tracking over one hundred indicators in order to detect fraudulent activity.

The RSA eFraudNetwork is a cross-organization database of fraud patterns gleaned from RSA's extensive network of customers, ISPs and third party contributors across the globe. When a fraud pattern is identified, the fraud data, transaction profile and device fingerprints are moved to a shared data repository. The eFraudNetwork provides direct feeds to the Risk Engine so that when a transaction or activity is attempted from a device or IP that appears in the eFraudNetwork data repository, it will be deemed high-risk and prompt a request for additional authentication.

The RSA Multi-credential Framework 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.

## FLEXIBLE DEPLOYMENT AND CONFIGURATION OPTIONS

RSA recognizes that no two businesses share the exact same user authentication needs – which is why RSA offers a wide array of authentication, deployment and customization options. Adaptive Authentication can be deployed, configured and used in a number of ways to meet the needs of an organization and its end users.

### *Visible or Invisible Deployment*

Adaptive Authentication can be deployed visibly or invisibly, depending on organizational needs and end user convenience. Some organizations prefer visible authentication to make their users visually aware they are being protected and to comply with regulations. Also, the use of visible authentication may lead some to believe that organizational and customer information is being protected more strongly.

On the other hand, some organizations prefer to use invisible authentication to monitor online activity in an effort to not disrupt or change the user experience, to avoid alerting fraudsters to the fact that a new security system is in place or as an additional protective layer against advanced threats.

### *On-premise or ASP/Hosted Deployment*

Organizations worldwide currently deploy Adaptive Authentication in two ways – as an on-premise installation that uses existing IT infrastructure or as a hosted (ASP) authentication service.

### *Multiple Configuration Options*

Adaptive Authentication can be configured in a number of ways to balance security and risk without compromising the user experience. For instance, 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 (i.e., hardware or software tokens for individuals that conduct high-risk activities on a regular basis). Most token form factors can be custom branded, providing an opportunity for organizations to align their brand with safety and security in order to remind their users of the value placed in their online protection.

## 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 financial services, healthcare and government. It is currently being used to protect over 200 million online users and has processed and protected over 20 billion transactions to date.

## ABOUT RSA

RSA is the premier provider of security, risk and compliance solutions, helping the world's leading organizations succeed by solving their most complex and sensitive security challenges. These challenges include managing organizational risk, safeguarding mobile access and collaboration, proving compliance, and securing virtual and cloud environments.

Combining business-critical controls in identity assurance, data loss prevention, encryption and tokenization, fraud protection and SIEM with industry leading eGRC capabilities and consulting services, RSA brings trust and visibility to millions of user identities, the transactions that they perform and the data that is generated.



AA DS 0511