RSA ADAPTIVE AUTHENTICATION TO MEET PCI DSS REQUIREMENTS FOR STRONG AUTHENTICATION
As merchants worldwide become more familiar with the Payment Card Industry Data Security Standard (PCI DSS), there is a move to explore how various technologies may be applied within a PCI environment. This certainly holds true in the context of PCI DSS requirement 8: “Assign a unique ID to each person with computer access.”

More specifically, PCI DSS requirement 8.3 calls for organizations to “incorporate two-factor authentication for remote access to the network by employees, administrators, and third parties.” For merchants, this means demonstrating – often to a PCI Qualified Security Assessor (QSA) – that individuals accessing the cardholder network remotely are verified via “both a password and an additional authentication item.”

Two-factor authentication, also commonly referred to as multi-factor authentication, alludes to the fact that there is more than one factor, or proof, needed in order for a successful authentication to be made. Multi-factor authentication consists of a combination of two or more of the following factors:

- **Personal factors (something you know):** This category refers to things that the user knows such as a password or challenge questions.
- **Technical factors (something you have):** This category refers to things that are physical such as a token or something embedded on a computer or other device, such as a digital certificate or flash shared object, which can be used to uniquely identify the user.
- **Human factors (something you are or do):** This category refers to things that are physically or mentally unique and attributable to an individual. This might include a biometric identifier such as a fingerprint or patterns of behavior.

### RISK-BASED AUTHENTICATION TO MEET MULTI-FACTOR REQUIREMENTS

RSA Adaptive Authentication is a multi-factor authentication and risk management platform providing cost-effective protection for large user populations. Adaptive Authentication works with leading SSL VPN and web access management (WAM) providers to enable strong authentication for enterprise applications and provides a web services (SOAP) interface performing risk-based authentication for users attempting to access protected applications.

Adaptive Authentication is powered by RSA’s risk-based authentication technology, a sophisticated system that measures a series of risk indicators behind-the-scenes to assure user identities. Adaptive Authentication uses a combination of device profiling, behavior profiling and RSA eFraudNetwork™ checks to meet the requirements for multi-factor authentication in terms of something the user has and something the user is.

**Device profiling: something the user has**

Adaptive Authentication uses device profiling to meet the technical factor requirement for multi-factor authentication in terms of something the user has. Device profiling enables the vast majority of users to be authenticated by analyzing the device profile, for the physical laptop, PC, tablet or mobile device from which the user accesses the website or application on a regular basis, and whether the device is known as having been previously used by the user. Device profiling is used for maintaining the different devices related data facts. For the web channel data includes:

- HTTP headers, operating system versions and patch levels,
- Browser type and version, software versions, display parameters (size and color depth), languages, time zone, etc.
- IP address, extracted IP geo location details and additional information on the ISP, IP owner, connection type, etc.
For mobile devices, the device profile contains additional device identifiers such as the IMEI, the ICCID, and more. In addition, the geo-location of smart mobile devices is not based solely on the IP, but also on information that can be collected directly from the mobile device itself.

The device profile is used to determine whether the current device is one from which the user usually accesses (data/information). The RE also checks if a device is from former fraudulent or genuine activities in the employee or consumer population as well as across activities in other RSA customers.

Behavior Profiling: Something the User Is/Does

Adaptive Authentication uses behavioral profiling to meet the technical factor requirement for multi-factor authentication in terms of something the user is or does. Behavioral profiling is used to identify high-risk login or activity attempts by measuring elements such as velocity checking, IP address information, and time of day comparisons. For example, if a user normally logs in during normal business hours from New York City and suddenly attempts to login from Moscow in the middle of the night, the system might consider this unusual behavior. However, if the user travels frequently and logs in at various hours from different locations worldwide, then this may not be considered unusual behavior.

THE DYNAMICS OF RISK-BASED AUTHENTICATION

Adaptive Authentication is powered by the RSA Risk Engine. The Risk Engine measures a series of indicators behind-the-scenes to validate user identities and behaviors. The majority of logins are “invisibly” authenticated by using analytics. This transparent authentication creates a superior user experience as users are only challenged in the highest risk scenarios. In addition, RSA Adaptive Authentication is self-learning and thus constantly improves detection accuracy.

The RSA Risk Engine measures over 100 different risk indicators for every log on or transaction performed. These risk indicators typically involve device identification, behavioral profile, and a check against the RSA eFraudNetwork.

RSA Risk Engine

The RSA® Risk Engine (RE) is a core technology of Adaptive Authentication. Combining both online data and traditional offline data, the Risk Engine evaluates each attempted login and activity in real-time, tracking over one hundred indicators in order to detect a
login attempt or activity that is suspicious or high-risk. The RE reduces the risk of privacy and compliance exposure, lowers the level of fraud, detects possible impersonators and identifies new fraud trends as they develop.

RSA eFraudNetwork matching – The performance of the Risk Engine in detecting potential cases of unauthorized access is directly enhanced by feeds from the RSA eFraudNetwork data repository. The eFraudNetwork contains information on IP addresses and device fingerprints that have been used to commit cybercrime in the past. The information from each login attempt is matched against information contained within the eFraudNetwork repository. If a match is identified, the eFraudNetwork input is then sent back to the Risk Engine which combines it with the hard rules and Bayesian model in generating a final risk score.

From all of these parameters, a risk score between 0 and 1000 is generated; the higher the score, the greater the risk the activity poses to the organization. Policies are established by each organization according to their risk threshold and depending on the score generated, the system can block an activity or prompt an additional authentication challenge. Organizations implementing RSA Adaptive Authentication in a PCI environment can work with their QSA or internal security team to determine the level of risk that is appropriate.

RSA eFraudNetwork

The RSA eFraudNetwork is a cross-organization data repository of fraud patterns gleaned from RSA’s worldwide network of customers, end users, ISPs, and third party contributors. When a fraud pattern is identified, the IP address and device fingerprints are moved to a shared data repository.

The RSA eFraudNetwork list of known fraudulent entities is constantly being generated and is collected through direct and indirect process.

A direct collection process gathers known fraudulent entities that are:

- Reported as confirmed fraud through the RSA eFraudNetwork Case Management tool; or
- Deemed “high-risk” by the RSA Risk Engine (activities that have triggered additional authentication and where the user has failed to complete that authentication).

The eFraudNetwork is further enriched by using an indirect process called “coloring.” IPs can be related to each other if they have similar characteristics such as the same device ID. For example, if IP 1.2.3.4 has been marked as having been used to commit fraud and is known to be reaching from device A, then IP 5.6.7.8, also reaching from device A, is “colored.” Thus, IP 5.6.7.8 is marked as high-risk, even if it hasn’t been directly confirmed as an IP that has been used to commit fraud.

RSA Policy Manager: Defining Risk Policy

The RSA Policy Manager allows customization of authentication policies based on organizational risk policy and end user segmentation. For example, a “privileged” user, such as an administrator, that has access to the most highly sensitive data may be automatically prompted to undergo an additional authentication challenge when logging in from an unknown device before access is granted.

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 production implementation. Adaptive Authentication employs a flexible and extensible Multi-Credential Framework (MCF) that enables multiple authentication options to be governed by the Policy Manager.
RSA Multi-Credential Framework

The Multi-Credential Framework provides an abstraction layer that enables one software platform to support multiple authentication methods (based on end user segmentation 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 applications, and different risk levels.

ADDITIONAL AUTHENTICATION FOR HIGH-RISK SCENARIOS

RSA Adaptive Authentication can invoke additional authentication methods in the event a login or activity is deemed high-risk. This is especially important for situations where a remote user is logging in from a device that is not recognized and has not been previously used to access the network. Adaptive Authentication challenges the end user to reconfirm that they are who they claim by offering multiple options. Challenge questions, dynamic knowledge-based authentication, OTPs and out-of-band authentications can be easily deployed to protect high risk transactions.

Out-of-Band Authentication

The Adaptive Authentication Out-of-band (OOB) Phone, SMS and email Authentication module is one of the strongest additional authentication options because it leverages a means to communicate with the user that circumvents the online environment.

Out-of-band authentication occurs either when a high-risk activity (identified as such by the RSA Risk Engine) occurs or when an organizational policy (e.g. “Challenge all activities originating in Country X or Country Y”) triggers it. When either or both of these scenarios occur, out-of-band authentication provides many obvious benefits. First, it meets the demands by customers for a secure solution that is easy to use and understand. Second, it does not require users to buy new hardware or download software and relies on common, accessible communication channel: a landline or mobile phone call, SMS or email. Finally, the widespread availability and flexibility of these communication channels meets the organizational need for a global solution that will work seamlessly across diverse geographies.

RSA Adaptive Authentication leverages out-of-band phone, SMS and email authentication to verify transactions in cases where a transaction has been deemed high-risk and the user has been challenged. A communication is sent to the customer either through a phone call, SMS message or email. Then a secure, onetime password will be used to authenticate the genuine user’s transaction when verified by RSA’s Adaptive Authentication.

Dynamic Knowledge Based Authentication and Challenge Questions

Challenge questions (sometimes called “shared secrets”) are questions which an online user enrolls in and is then prompted to answer when additional authentication is required. Enrollment in challenge questions occurs when the user signs up for stronger authentication. This typically occurs either when a new user initially enrolls into an application or when an organization chooses to roll out multi-factor authentication to their users.

Dynamic Knowledge Based Authentication (KBA): KBA, like Challenge Questions, presents consumers with a series of dynamic questions that the consumer must answer in order to complete login or complete a transaction. The difference between KBA and Challenge questions is that KBA questions are not pre-selected by the consumer. KBA questions are culled from public and private databases.

1 Merchants pursuing an Adaptive Authentication deployment within the context of a PCI compliance project should work with their security teams and QSAs to evaluate the level of risk that should trigger additional authentication.
Knowledge-based authentication questions are often referred to as “out-of-wallet” questions because the knowledge needed to answer the questions (for instance, “What street did you live on at your previous residence?”) is not held in a wallet and therefore, is very difficult for anyone other than the genuine user to know – or guess.

An example might be “what color was the Ford Escort you owned in 1998?” These questions are presented to the end-user, and a pass/fail result is provided.

**CONCLUSION**

RSA Adaptive Authentication provides strong multi-factor authentication by providing a layer of security in addition to something the user knows – their username and password. It addresses PCI DSS requirement 8.3 which calls for organizations to implement two-factor authentication for remote users. Even though a majority of authentication requests are conducted transparently to the user, Adaptive Authentication still provides multi-factor authentication based on device profiling which determines what the user has (their device) and behavioral profiling which determines what a user is or does.

In addition, Adaptive Authentication addresses the challenge of authenticating remote users that are logging in from a device that is not recognized by prompting a user to complete an out-of-band authentication or answer challenge questions in order to assure their identity. The combination of these factors creates an ideal multi-factor solution to help organizations comply with PCI requirements.