RSA® ADAPTIVE AUTHENTICATION

Protecting Mobile Transactions

Solution Brief
THE MOBILE LANDSCAPE

Even though accessing products and services remotely is not a new concept, advances in technology continue to create new opportunities – and new channels – for consumers to communicate, transact and work. Today, the mobile channel is a prime example. Particularly suited for an on-the-move society that demands convenience, mobile devices – including laptops, mobile phones, smart phones, tablets and PDAs – free consumers from the confines of traditional storefronts and geography by providing anywhere-anytime access on a 24x7 basis.

Organizations are responding by moving products and services to the mobile channel, delivering specialized small-screen adaptations for web browsing, and developing apps that supply mobile functionality and brand-based services. As of August 2015, over 40% of all transactions originated from a mobile device – nearly a 35% growth year over year¹.

Despite the convenience offered to end users, the mobile channel continues to be vulnerable to a myriad of threats similar to those witnessed in the online channel such as phishing and malware. Cybercriminals are paying attention to the transaction growth in the mobile channel and creating opportunity for themselves. In fact, today approximately 54% of all fraudulent transactions originated from the mobile channel compared to less than 10% just three years ago². It is vital, therefore, for organizations to instill trust and confidence in the mobile channel by applying the same level of protection their customers have come to expect when conducting transactions in the online channel.

RSA ADAPTIVE AUTHENTICATION FOR MOBILE

RSA Adaptive Authentication is a comprehensive, risk-based authentication and fraud-detection platform that provides cost-effective protection for an entire user base. The Mobile Protection module is an extension of RSA Adaptive Authentication technology, allowing new or existing customers to easily extend strong risk-based authentication to secure transactions in the mobile channel. RSA Adaptive Authentication protects multiple types of mobile channels including mobile browsers, WAP browsers and the more sophisticated, mobile-specific functionality of mobile applications.

The RSA Risk Engine is at the heart of the RSA Adaptive Authentication Mobile Protection module. The Risk Engine has a mobile-dedicated risk model that silently analyzes a variety of indicators to determine risk level. Once the transaction details are analyzed, the Risk Engine generates a score between 0 and 1000, which represents the level of confidence associated with the legitimacy of the user and the transaction. Indicators the Risk Engine considers include:

- **Mobile device identifiers.** These include device model, language, screen size, system version and many more. This allows the risk engine to build a profile of the device and flag devices not associated with that user.

- **Location.** Location is identified through Wi-Fi, cell-tower triangulation and GPS. Location is used to identify high risk or atypical locations or illogical ground speeds.

- **Behavioral profile.** This includes an analysis of the transaction being conducted including the amount and payee and whether or not it is typical behavior for the user.

- **RSA® eFraudNetwork™** The eFON is a repository of fraud patterns, IPs, device IDs and account numbers shared by RSA’s network of customers, partners and third-party contributors worldwide. The service provides direct feeds to the Risk Engine. Transactions or activities attempted from a device or to an account that appears in the eFraudNetwork have a higher risk indicator.

In addition, jail broken, rooted and mobile-emulated devices are identified to provide additional context for better risk assessment.

---

¹ RSA AFCC
² Ibid

*Current Trends in Mobile Transactions and Banking*

In the second half of 2015:
- Over 40% of all transactions originated from a mobile device*
- 32% of all fraudulent transaction originated from a mobile device*

In 2013, there were 145K +new mobile malware strains vs. 40K in 2012; 98% of malware targeting Android OS**

*RSA AFCC
**Kaspersky Labs
The Adaptive Authentication Mobile Protection module allows existing customers to easily extend the same protection they offer their web users to their mobile users.

RSA Adaptive Authentication also considers an organization’s risk tolerance in determining the level of risk associated with the user or transaction – thresholds for challenges, approvals and denials can be set based on an organization’s risk tolerance. In addition, organizations can use the RSA Policy Manager to set custom risk policies for challenging, denying or allowing users and transactions via a comprehensive rules framework that can be configured in real-time. The Policy Manager allows organizations to develop a true cross-channel strategy by applying risk policies and acceptable risk levels across the multiple channels where user access is enabled. For example, an organization might set a lower risk threshold for the online channel when considering it is common for users to access their account from multiple computers yet set a higher risk threshold for mobile devices as users are most likely to access an account from the same mobile device all the time.

In most situations, users are authenticated invisibly, eliminating the impact on user experience. Only high-risk and unusual scenarios that fall outside a user’s normal pattern of behavior will be challenged. In these cases and depending on the organization’s policy, users can be challenged with a variety of step-up authentication methods such as classic challenge questions, one-time-password or biometric (fingerprint or eyeprint). In addition, the RSA Multi-Credential Framework allows organizations to customize their Adaptive Authentication deployment with additional authentication methods to meet the needs and risk level of all users via RSA Professional Services, “in-house” or through third parties.

Adaptive Authentication offers integration through a web services call and a Software Development Kit (SDK) that allows developers to embed data collection and authentication directly into their mobile applications. Supported platforms include Apple iOS, Android OS, Windows and Blackberry OS.

Developers of mobile applications for business, banking, e-commerce and data access can increase security and confidence by integrating strong risk-based authentication in their mobile offerings with the AA mobile SDK.

**EXTEND YOUR EXISTING INVESTMENT TO MOBILE**

RSA Adaptive Authentication is used today by over 8,000 organizations across multiple industries to protect more than 450 million user identities and 50 billion transactions worldwide. In addition to proven results, RSA Adaptive Authentication is flexible and can be deployed in two ways – as an on-premise installation that uses existing IT infrastructure or as a software-as-a-service model.

As more organizations move products and services to the mobile channel, protecting against fraud and advanced threats will be important to build customer trust. The RSA Adaptive Authentication Mobile Protection module gives organizations the ability to authenticate end-users in different ways, depending on their activity type, transactional details and mobile device being used. RSA Adaptive Authentication also enables organizations to set unique risk policies for other channels as well – such as the Web channel – and realize the unique benefits of a true multi-channel fraud protection strategy.