RSA AUTHENTICATION FOR MOBILE
RSA ADAPTIVE AUTHENTICATION MOBILE SDK

THE LANDSCAPE

- Proliferation of mobile devices brings risk as well as opportunity
- Mobile devices are increasingly used for fraud
- Mobile devices have embedded functionalities such as fingerprint sensors, cameras and microphones that can be leveraged to enhance security and end user convenience
- Consumers expect frictionless authentication from any device they are using

AA MOBILE SDK FOR SECURITY AND CONVENIENCE

- RSA Adaptive Authentication can be embedded in mobile apps via the Mobile SDK
- Consumers can authenticate themselves with biometrics when challenged for a step up in a mobile app that embeds the AA Mobile SDK
- Mobile applications that directly integrate RSA Adaptive Authentication protect consumer accounts from unauthorized access—without adversely impacting end user access or usability

CONTACT US
To learn more about how EMC products, services, and solutions can help solve your business and IT challenges, contact your local representative or authorized reseller or visit us at www.EMC.com/rsa.

MOBILE RISKS AND OPPORTUNITIES
In order to meet consumer demand for convenience, organizations continue to extend product and service offerings as well as account access into both web and mobile channels. Consumers demand access to their information and accounts when and where the want it, more often than not from the mobile device they are connected to 24x7. At the same time, cybercriminals continue to evolve, leveraging Phishing, Man in the Middle (MITM), Man in the Browser (MITB), and other tactics to gain unauthorized access to funds, data and accounts.

Where legitimate businesses go, fraudsters follow. The mobile channel is increasingly being used in attacks targeting legitimate users who bank, shop and communicate via their mobile device.

RSA ADAPTIVE AUTHENTICATION MOBILE SDK
The proliferation of mobile devices brings opportunity as well as risk however. Mobile applications that directly integrate Adaptive Authentication can protect consumers against unauthorized access with minimal impact to the end user.

Adaptive Authentication has a dedicated mobile risk model that includes capabilities such as location awareness and mobile device identification. The location of a device is detected using a series of time and geography based algorithms and can access location data gathered through Wi-Fi, cell-tower triangulation, and GPS. Device identification captures characteristics such as device model, language, and screen size. Anomalies such as locations or devices which are new to the user are deemed high risk.

Adaptive Authentication’s mobile capabilities also include identification of compromised devices (i.e., those that have been jail broken or rooted) and mobile emulation detection.

In addition to enhanced fraud detection in the mobile channel, the AA Mobile SDK also enables organizations to provide consumers with a seamless mobile experience.

In addition to a more traditional range of step up options including One Time Password, the Mobile SDK leverages embedded functionalities such as fingerprint sensors, cameras and microphones to enhance both security and end user convenience. When challenged to authenticate during a higher-risk login or transaction, consumers can be offered the opportunity to use a biometric (fingerprint or eye vein).

OFFERING SECURITY AND CONVENIENCE
RSA’s vision for mobile risk-based authentication solutions is to minimally impact the mobile user experience while still maintaining strong authentication by leveraging the RSA® Risk Engine to analyze risk indicators including device identification, geo-location, behavioral profiling, and real-time fraud data from the RSA eFraudNetwork™ community.