

# RSA<sup>®</sup> ADAPTIVE AUTHENTICATION FOR ECOMMERCE

## 신용 카드 발급사를 위한 위험 기반 3-D SECURE 솔루션

3-D Secure은 Mastercard, American Express, Visa, JCB International에서 채택한 부정 행위 방지 프로토콜로 온라인 결제에 대한 추가적인 보호를 제공합니다. 3-D Secure 프로토콜에서는 등록된 카드 소유자가 참여하는 판매업체에서 등록된 신용 카드를 사용할 때마다 거래 진행 전 해당 카드 소유자를 인증합니다. 기존 3-D Secure 환경에서 인증은 신용 카드를 등록할 때 카드 소유자가 생성한 암호를 기반으로 하며, 거래가 발생할 때마다 확인을 거쳐야 했습니다.

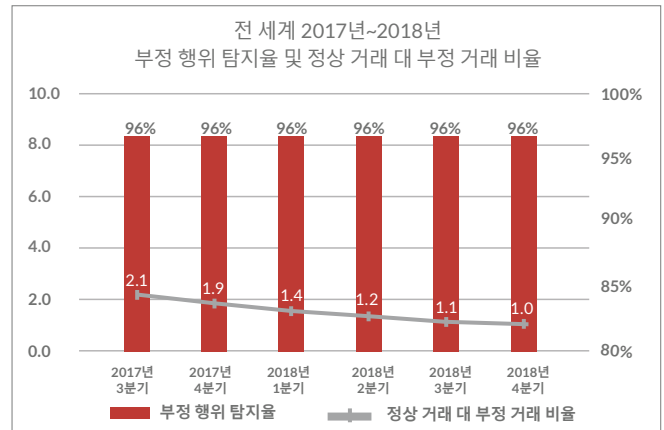
기존 3-D Secure의 100% 본인 확인율은 발급사, 판매업체, 카드 소유자 모두에게 부정적인 영향을 미칩니다. 구매 흐름을 방해하는 모든 활동으로 인해 쇼핑 카트 단계에서 구매를 포기할 확률이 높아지므로 발급사와 판매업체 모두 매출이 감소합니다. 카드 소유자가 암호를 잊어버렸을 경우 발생하는 부정적인 경험 역시 포기 확률을 높이고 특정 카드의 사용을 줄여 발급사의 매출에 영향을 미칩니다.

위험 기반 3-D Secure는 강력한 인증을 통해 높은 부정 행위 탐지율을 제공하며, 카드 소유자가 발급사의 매출에 부정적인 영향을 주는 바람직하지 않은 경험을 가급적 겪지 않도록 방지합니다. 위험 기반 3-D Secure을 통해 신용 카드 발급사는 부정 행위를 줄이고 매출을 보호할 수 있습니다.

### 높은 부정 행위 탐지율, 낮은 개입률

Adaptive Authentication for eCommerce는 신용 카드 발급사와 프로세서를 위한 RSA의 3-D Secure 액세스 제어 서버입니다. 솔루션의 핵심인 RSA 위험 엔진을 통해 Adaptive Authentication for eCommerce가 자동으로 카드 소유자를 인증하며 위험도가 높은 고객(전체 거래의 전 세계 평균 5%)만 본인 확인이 진행됩니다. 높은 정확도의

위험 엔진을 통해 거짓 양성률은 매우 낮게 유지하면서 부정 행위 탐지율은 매우 높일 수 있습니다.



위의 그래프에서 RSA Adaptive Authentication for eCommerce의 평균 부정 행위 탐지율이 96%이며, 정상 거래 대 부정 거래의 비율(확인된 부정 거래 한 건당 본인 확인된 정상 거래의 수)은 낮음을 확인할 수 있습니다. RSA Adaptive Authentication for eCommerce의 경우 매우 적은 수의 합법적인 고객만 확인하면서도 부정 행위로 인한 손실은 크게 감소시킬 수 있습니다. 이를 통해 카드 소유자의 경험을 향상하고 발급사의 매출을 보호하는 것은 물론, 거래 검토와 정상 고객의 문의 처리와 관련된 운영 비용을 절감할 수 있습니다.

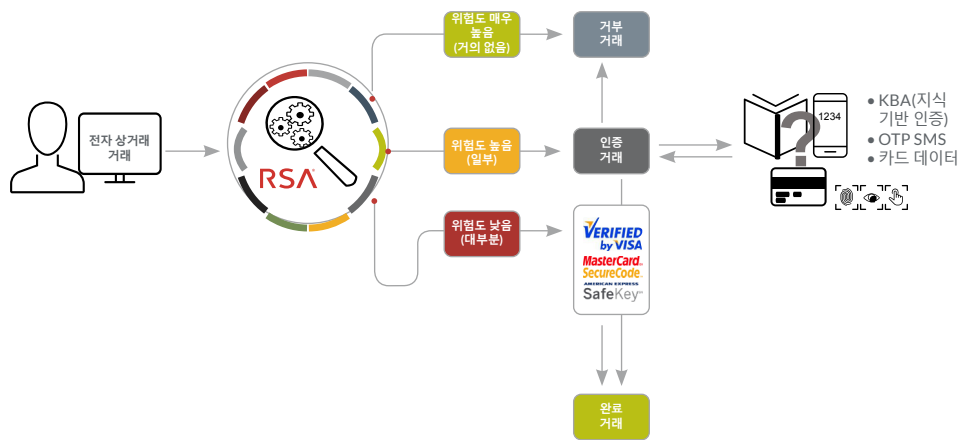
### 중단 없는 인증으로 원활한 카드 소유자 경험을 제공

3-D Secure 프로토콜과 인프라스트럭처, RSA Adaptive Authentication for eCommerce를 활용하여 차지백 손실의 위험을 완화하면서 판매업체와 카드 발급사가 카드 소유자에게 일관성 있고 안전한 온라인 쇼핑 환경을 제공할 수 있도록 합니다.

카드 발급 은행은 RSA Adaptive Authentication for eCommerce를 통해 카드 소유자의 쇼핑 경험에 영향을 미치지 않으면서 VbV(Verified by Visa®), MasterCard SecureCode®와 Identity Check®, American Express SafeKey® 지원을 제공할 수 있습니다. Adaptive Authentication for eCommerce는 RSA 위험 엔진을 사용하여 각 거래를 운영 중단 없이 실시간으로 평가하고 거래가 부정 거래일 확률을 결정합니다. 위험도가 높은 것으로 확인된 거래와 관련된 카드 소유자만 본인 확인이 요구되므로, 참가하는 판매업체의 거래 중 약 95%가 3-D Secure 검증 프로세스에 의해 중단되지 않습니다. 또한 중단 없는 인증 방법 덕분에 발급사가 사전에 전체 카드 BIN 범위를 등록하므로 카드 소유자는 VbV, SecureCode, Identity Check 또는 SafeKey 등록 프로세스를 거칠 필요가 없고, 일회성 비밀번호와 생체 인식을 포함해 다양한 단계별 인증 방법을 사용하므로 암호를 기억할 필요가 없습니다. 이를 통해 정상 카드 소유자는 중단 없이 온라인 거래가 가능합니다.

“ 더 많은 판매를 처리할 수 있고 부정 행위로 인한 손실을 제어할 수 있으며 고객이 솔루션에 만족한 단점에서 솔루션 도입이 성공적이었음을 확인할 수 있었습니다. ”

부사장 겸 부정 행위 위험 제어 관리자대형 은행



## 분석 애플리케이션

RSA Adaptive Authentication for eCommerce의 분석 애플리케이션은 카드 발급사가 3-D Secure 거래 데이터를 완벽하게 파악할 수 있도록 지원합니다. 분석 애플리케이션은 일일 및 월간 모니터링 지표, 부정 행위 탐지율 및 규칙 성능 데이터를 발급사가 즉시 이용할 수 있게 제공하므로 솔루션을 위험 허용 한도와 비즈니스 우선 순위 에 맞게 조정할 수 있습니다.

대시보드는 다음과 같은 보고서로 구성됩니다.

- 동향 및 변칙적 상황을 시각화하고 강조
- 다양한 세분성 수준에서 데이터 확인 가능
- 필요 시 즉각적인 변화를 위한 유연하고 동적인 인터페이스 제공

또한 발급사는 대시보드의 정보를 외부 애플리케이션에서 사용할 수 있는 다양한 형식으로 내보낼 수 있습니다.

분석 애플리케이션은 발급사에게 위험 요소 현황에 대해 더 많은 분석 정보를 제공하므로, 발급사는 정책 관리 규칙, 위험 수치 임계값 및 기타 구성 가능한 변수에 대해 보다 다양한 정보에 입각하여 의사 결정을 내릴 수 있습니다.

## 차세대 3-D SECURE 2.0

3-D Secure 프로토콜은 진화하고 있습니다. 새로운 프로토콜 개발을 전담하는 표준 기관인 EMVCo는 2016년 10월에 차세대 3-D Secure(EMV 3-D Secure, 3-D Secure 2.0 또는 간단히 “3DS 2.0”)을 출시했습니다. 3DS 2.0 프로토콜은 RSA가 2008년에 개척한 접근 방식인 위험 기반 인증 기술을 활용하여 카드 소유자에게 원활한 쇼핑 환경을 제공합니다. RSA는 EMVCo의 기술 제휴업체로서 3DS 2.0에 입력 정보를 제공했으며 이는 사양에 반영되었습니다.

RSA는 플랫폼 내에서 새로운 기능을 지원하기 위해 노력할 것이며, 카드 발급사에 압호 없고 중단 없는 인증을 제공하는 이니셔티브를 수립하기 위해 고객 및 EMVCo와 직접적인 협력을 지속할 것입니다.

## RSA 소개

RSA® Business-Driven Security™ 솔루션은 통합된 가시성, 자동화된 분석 정보 및 조율된 작업에 따라 디지털 위험을 관리하는 통합된 접근 방식을 조직에 제공합니다. RSA 고객은 신속한 감지 및 대응, 사용자 액세스 제어, 소비자 부정 행위 방지 및 통합 위험 관리를 위한 솔루션을 통해 혁신적인 변화를 추진하고 이러한 변화에 지속적으로 적응할 수 있습니다. 자세한 내용은 [rsa.com/ko-kr](https://rsa.com/ko-kr)을 참조하시기 바랍니다.