



## Account Information System (AIS) Program

# 자주하는 질문(FAQ)

### Q AIS가 무엇입니까?

A 카드정보보안(AIS, Account Information Security)은 비자의 리스크 관리 프로그램으로 카드 정보 및 거래 정보 보호를 목표로 합니다. 이에 의거하여 카드 정보 및 거래 정보를 처리, 저장, 전송하는 모든 기관은 반드시 PCI 보안표준협회(PCI SSC)의 PCI 카드 보안 표준(PCI DSS, Payment Card Industry Data Security Standards)을 준수해야 합니다.

주요 5대 카드브랜드사는 지난 2006년 표준 감독을 위해 PCI 보안 표준 협회(PCI Security Standards Council)를 설립하였으나, 각각의 카드사는 인증 조건, 마감일, 벌금 개요에 대한 별개의 고유 프로그램을 유지하고 있습니다.

PCI DSS 와 PCI SSC 에 대한 자세한 정보를 보시려면, PCI SSC 웹사이트 [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org) 를 방문하십시오.

### Q 누가 PCI DSS 를 준수해야 합니까?

A 카드 사용자의 자료를 저장, 처리, 전송하는 모든 기관 즉, 가맹점, 서비스 제공업체 (예. 지불중계(PG), IPSP, 프로세서), 매입사, 발행사 모두 PCI DSS 를 반드시 준수해야 합니다. 이 조건은 모든 소매업체(기존 전통기업), 우편, 전화주문(MOTO), 전자상거래를 포함한 모든 수납 채널에 적용됩니다.

### Q 제 3 기관에게 카드 사용자 정보의 처리, 전송, 저장을 아웃소싱하는 경우에는 어떻게 됩니까?

A 발행은행, 매입은행 모두 반드시 PCI 카드 보안 표준을 준수하는 서비스 공급업체를 이용해야 하며, 은행은 각자의 가맹점도 이들을 이용하도록 할 책임이 있습니다. 비록 가맹점의 서비스 공급업체와 매입사가 직접적인 계약관계가 없더라도, 비자 매입사들은 비준수로 야기된 결과에 대한 책임이 있습니다.

### Q 어떻게 PCI DSS 준수 인증을 받을 수 있습니까?

A 가맹점 및 서비스 공급업체에 대한 인증 조건은 각 기관의 연평균 카드 사용자 처리 규모에 기반을 두고 있습니다. 가맹점 및 서비스 공급업체의 수준과 조건은 [www.visa-asia.com/secured](http://www.visa-asia.com/secured) 을 참조하십시오.

인증 방법:

- PCI SSC 인증 보완 감사원 (QSA)가 실시한 연간 현장 PCI 데이터 보안 평가
- PCI SSC 인증 스캐닝 벤더(ASC)가 실시하는 분기별 취약성 스캔
- PCI DSS 연간 자가 평가 질문지(SAQ)를 사용한 연간 자가 평가

QSA, ASV, SAQ 명단을 보려면, [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org) 를 방문하십시오.

**Q PCI 자가평가결문지(SAQ)가 무엇입니까?**

A PCI 자가평가결문지(SAQ, Self-Assessment Questionnaire)는 가맹점과 서비스 제공업체가 자신의 PCI DSS 준수 상태를 스스로 평가해 볼 수 있는 인증 도구입니다. SAQ 는 [www.pcisecuritystandards.org/saq/instructions.shtml](http://www.pcisecuritystandards.org/saq/instructions.shtml) 에서 다운로드 할 수 있습니다.

**Q 취약성 스캔이 무엇입니까?**

A 취약성 스캔은 인터넷에서 자신의 네트워크를 평가하는 자동 원격 스캔으로 인증되지 않거나 악의적인 사용자가 네트워크에 접근해 잠재적으로 카드사용자의 데이터를 위협할 만한 취약점이나 결함이 있는지를 체크하는 것입니다.

**Q PCI DSS 준수성은 한번만 충족시키면 됩니까?**

A 아니요. PCI DSS 준수는 지속적으로 진행됩니다. 인증 활동이 실제 거래량과 연간 기관 프로세스에 따라 달라지는 만큼, 모든가맹점과 서비스 공급업체는 항상 PCI DSS 를 준수해야 합니다.

**Q 마감기한이 있습니까?**

A 네. 마감기한은 다음과 같습니다:

**레벨 1** 가맹점

- 금지 데이터 저장 삭제의 마감일자는 **2009년 9월 30일**입니다.
- PCI DSS 준수 마감일자는 **2010년 9월 30일**입니다.

**레벨 2** 가맹점

- 금지 데이터 저장 삭제의 마감일자는 **2009년 9월 30일**입니다.

**서비스 공급업체**

- PCI DSS 준수 마감일자는 **2008년 12월 31일**입니다.

**Q 가맹점 레벨은 어떻게 결정되며 인증 조건은 무엇입니까?**

A PCI DSS 의 준수는 의무사항입니다. 비자는 거래량, 잠재 리스크, 비자 시스템에 대한 노출 정도에 따라 준수 인증 레벨을 규정합니다. 비자는 연간 PCI DSS 준수 인증을 위한 전세계가 동일하게 적용하는 가맹점의 레벨 결정 방법과 인증 조건을 마련하였으며 내용은 다음과 같습니다.

레벨	가맹점 기준	인증 조건
1	연간 6 백만 건 이상(모든 채널)의 비자 거래를 처리하는가맹점또는 지역 비자가 레벨 1 으로 인정된 글로벌가맹점	<ul style="list-style-type: none"> <li>▪ 인증 보완 감사원("QSA")가 실시한 연간 준수 보고서("ROC")</li> <li>▪ 인증 스캔 벤더 ("ASV")의 분기별 네트워크 스캔</li> <li>▪ 준수 증명서 양식</li> </ul>

레벨	가맹점 기준	인증 조건
2	연간 백만~6 백만 건 이상(모든 채널)의 비자 거래를 처리하는가맹점	<ul style="list-style-type: none"> <li>연간자가 평가 질문지("SAQ")</li> <li>ASV 의 분기별 네트워크 스캔</li> <li>준수 증명서 양식</li> </ul>
3	연간 2 만~백만 건의 비자 전자 상거래를 처리하는가맹점	<ul style="list-style-type: none"> <li>연간 SAQ</li> <li>ASV 의 분기별 네트워크 스캔</li> <li>준수 증명서 양식</li> </ul>
4	연간 2 만 건 미만의 비자 전자상거래를 처리하는가맹점 및 연간 백만 건의 비자 거래를 처리하는가맹점	<ul style="list-style-type: none"> <li>연간 SAQ 권장</li> <li>적용 가능 시, ASV 의 분기별 네트워크 스캔</li> <li>매입사가 설정한 준수 인증 조건 준수</li> </ul>

\* 위 네 가지 레벨 중 하나에 해당하는 모든가맹점은 12개월간의 비자 거래량에 기준합니다. 거래량은가맹점의 사업 분야 설명(“DBA”)으로부터의 총 비자 거래 수(신용, 현금, 선불 포함)에 기반을 두고 있습니다. 가맹점 기업이 하나 이상의 DBA를 지닐 경우, 인증 레벨 규정을 위해 고객은 반드시 기업이 저장, 처리, 전송한 총 거래 규모를 고려해야 합니다. 데이터를 총계하지 않을 경우, 기업이 여러 개의 DBA를 대표하여 카드 사용자의 데이터를 저장, 처리, 전송하지 않을 경우, 회원들은 위와 같은 인증 레벨 결정 시 DBA의 개별 거래량을 계속 고려해야 합니다.

**Q 가맹점 레벨은 어떻게 결정되며 인증 조건은 무엇입니까?**

A 비자는 서비스 제공업체의 연간 PCI DSS 준수 인증을 위한 글로벌 제휴 레벨 및 인증 조건을 마련하였으며 내용은 다음과 같습니다.

레벨	모든 지역	인증 조건
1	연간 30 만 건 이상의 거래를 저장, 처리, 전송하는 비자넷(VisaNet) 프로세서 또는 서비스 공급업체	<ul style="list-style-type: none"> <li>QSA 의 연간 ROC</li> <li>ASV 의 분기별 네트워크 스캔</li> <li>준수 증명서 양식</li> </ul>
2	연간 30 만 건 미만의 거래를 저장, 처리, 전송하는 서비스 공급업체	<ul style="list-style-type: none"> <li>연간 SAQ</li> <li>ASV 의 분기별 네트워크 스캔</li> <li>준수 증명서 양식</li> </ul>

**Q AIS 프로그램에 참여하지 않으면 어떻게 됩니까?**

A 전 세계 모든 비자 발행은행, 매입은행과 거래관계에 있는 업체(가맹점, 서비스 공급업체 등)는 반드시 AIS 프로그램에 참여 해야 합니다.발행사나 매입사와 거래관계에 있는 업체가 AIS 프로그램의 요구조건을 준수하지 않을 경우, 발행사나 매입사는 비자에 의해 패널티가 적용될 수 있습니다. 궁극적으로 비자 카드를 취급하기 위해서는 모든가맹점과 서비스 업체는 반드시 AIS 조건을 준수해야 합니다.

**Q. AIS 프로그램에 대한 문의사항이 있을 경우 어떻게 합니까?**

A 귀사의 매입은행에 문의하거나 AIS 웹사이트 [www.visa-asia.com/secured](http://www.visa-asia.com/secured) 를 방문하십시오. PCI DSS 및 관련 정보에 대한 문의사항이 있으시면

[www.pcisecuritystandards.org/about/contact](http://www.pcisecuritystandards.org/about/contact) 의 PCI SSC 에게 문의하십시오.

## 지불 어플리케이션

### Q PA DSS 가 무엇입니까?

A 지불 어플리케이션 데이터 보안 표준 (PA-DSS)은 비자의 PABP 에 기반한 업계 표준으로써, PCI DSS 를 지원하고 소프트웨어 벤더 및 다른 이들의 안전한 지불 어플리케이션 개발을 돕기 위해 고안되었습니다. 안전한 지불 어플리케이션이란 전체 마그네틱 띠 및 기타 민감한 인증 데이터, PIN 데이터 등과 같은 금지 데이터의 저장을 방지하는 것을 뜻합니다. PA-DSS 은 PCI 보안 표준 협의회 (PCI SSC) 및 PCI DSS, PCI PED 등의 기타 업계 표준에 의해 관리되며 모든 주요 카드 브랜드사에게 적용하고 있는 국제 표준입니다.

PCI DSS 준수 조건에 대한 자세한 정보를 보시려면, [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org) 를 방문하십시오.

### Q PA-DSS 조건을 따르는 지불 어플리케이션의 종류는 무엇입니까?

A PA-DSS 는 소프트웨어 벤더 및 인증, 결산에 필요한 카드 사용자의 정보를 저장, 처리, 전송하는 지불 어플리케이션 개발업체에게 적용됩니다. 또한 이 지불 어플리케이션을 가맹점과 서비스 공급업체에게 판매, 유통, 혹은 인가하는 업체들도 이에 적용됩니다.

PA-DSS 에 따라 인증된 지불 어플리케이션이 PCI-DSS 준수 환경에서 시행되면 전체 마그네틱 띠/트랙, 카드 인증 코드(CAV2, CID, CVC2, CVV2), PIN, PIN 블록 등과 같은 보안 침해 및 이로 인한 사기 피해를 최소화할 수 있습니다.

### Q PA-DSS 조건을 따르지 않는 지불 어플리케이션의 종류는 무엇입니까?

- A
1. 단일 고객만을 위해 개발, 판매된 지불 어플리케이션은 PA-DSS 에 적용 되지 않습니다. 그러나, 고객의 PCI DSS 평가시 평가 범위에 적용됩니다.
  2. 가맹점이나 서비스 개발업체가 사내용(in-house)으로 개발하고 제 3 자에게 판매되지 않은 지불 어플리케이션은 PA-DSS 에 적용 되지 않습니다. 그러나, 가맹점과 서비스 개발업체의 PCI DSS 평가시 평가 범위에 적용됩니다.
  3. Standalone POS 터미널의 지불 어플리케이션은 PA-DSS 에 적용되지 않습니다.
  4. 다음의 어플리케이션은 PA-DSS 범위에 포함되지 않는 대표적 지불 어플리케이션들입니다. 지불 어플리케이션이 설치된 운영 시스템(예. 윈도우, 유닉스), 카드 사용자 데이터를 저장하는 데이터베이스 시스템(예. 오라클), 카드 사용자의 자료를 저장하는 백오피스 시스템(예. 보고 또는 고객 서비스 목적).

### Q PCI SSC 는 기존의 비자 PABP 프로그램 하에서 인증된 어플리케이션도 인정합니까?

A PCI SSC 는 PABP 인증 지불 어플리케이션을 인정하며 적합한 PABP 버전과 함께 게재합니다. 세부 사항은 하단의 표를 참고하십시오.

		만료 전 PCI SSC 리스트		만료 후 PCI SSC 리스트	
버전	만료일	인증 노트	배치 노트	인증 노트	배치 노트
PABP 1.4	24 개월	PABP 에 따라 인증	신규배치 수락가능	PABP 에 따라 인증	신규배치 수락 불가능
PABP 1.3	18 개월	PABP 에 따라 인증	신규배치 수락가능	PABP 에 따라 인증	신규배치 수락 불가능
PABP 1.3 이전	12 개월	Pre-PCI 어플리케이션	신규 배치 권장하지 않음	Pre-PCI 어플리케이션	신규배치 수락 불가능
PA-DSS 1.1	표준 변경 3년 후	PA-DSS 에 따라 인증	신규배치 수락가능	PA-DSS 에 따라 인증	신규배치 수락 불가능

**Q PA-DSS 가 고객에게 주는 영향은 무엇입니까?**

A 안전한 지불 어플리케이션을 통해 고객의 PCI DSS 준수가 용이해집니다. DSS 준수 환경이 시행되면, PA-DSS 인증 지불 어플리케이션으로 인해 전체 마그네틱 띠 데이터, 카드 인증 코드 및 가치(CAV2, CID, CVC2, CVV2), PIN, PIN 블록 등과 같은 보안 침해 위험성을 최소화할 수 있습니다.

**Q 누가 PA-DSS 평가를 시행합니까?**

A PCI SSC 가 인증한 지불 어플리케이션 보완 감사원(PA-QSA)만이 지불 어플리케이션 검사를 시행할 수 있습니다. 모든 QSA 가 PA-QSA 는 아님을 참고하십시오. QSA 가 추가 평가 조건에 부합해야만 PA-QSA 가 될 수 있습니다. PA-QSA 의 명단은 PCI SSC 웹사이트에 공개되어 있습니다.

**Q PA DSS 인증 비용은 얼마입니까?**

A 수반되는 인증 비용은 소프트웨어 벤더가 지불해야 합니다. PA-DSS 인증은 지불 어플리케이션의 복잡성과 규모, 검사 소요 시간, PA-QSA 비용에 따라 인증비용이 결정됩니다.