Smartro

결제모듈연동안내

문서번호 Ver.1.0 [2020.06]

“본 자료는 ㈜스마트로의 서면동의 없이는

제 3 자에게 어떤 방식으로든 공개할 수 없습니다."

개 정 이 력

버전	변경일	변경 내용	작성자	승인자
1.0	20.04.14	[최초작성] - 가맹점연동안내 문서 최초 작성	장신아	
1.1	20.06.09	- 연동 규격서 표준화 작업	장신아	

목 차

1. 스마트로 온라인 PG 결제모듈

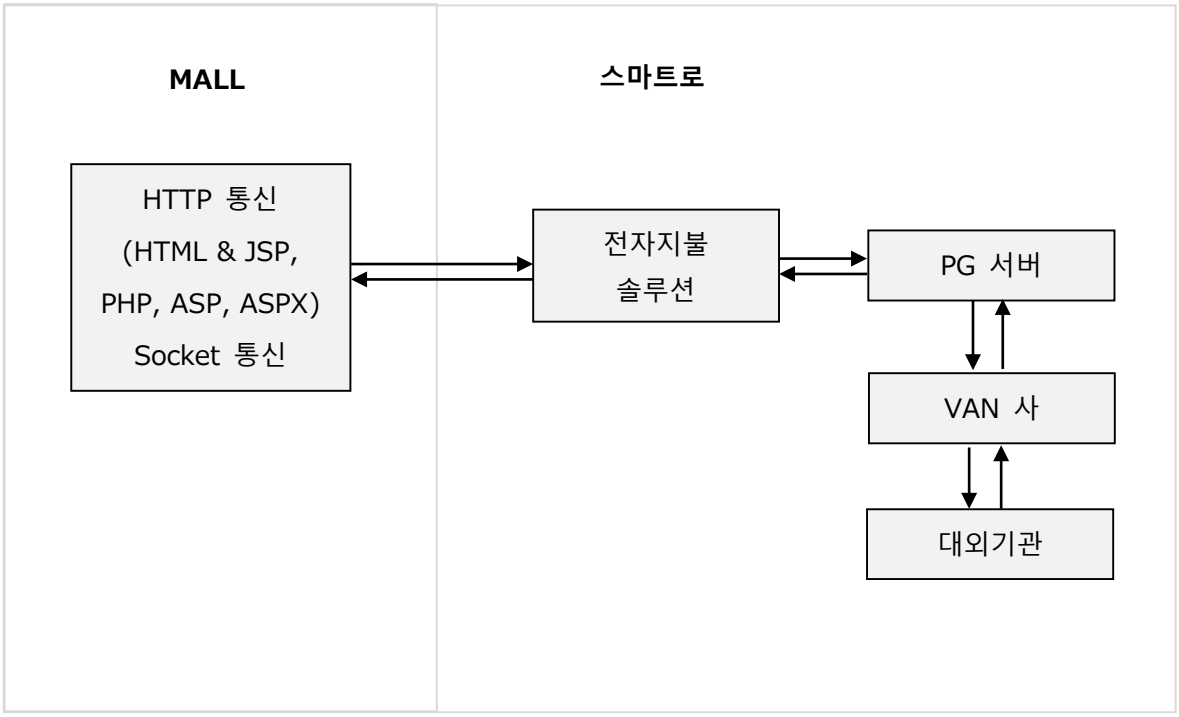
SMARTROPAY 웹 기반 전자 지불 결제 시스템은 안전하고 신뢰성 있는 인터넷 쇼핑을 도와주는 인터넷 전자 지불 솔루션 입니다.

스마트로 온라인 PG 서비스를 이용하고자 하는 가맹점은 스마트로 결제모듈을 가맹점 시스템(ex. 쇼핑몰)에 연동하여 결제 서비스를 이용합니다.

> **※ Note**
> 스마트로에서 제공하는 샘플파일은 연동 가이드 입니다.
> 가맹점에서는 자체 개발환경에 따라 Customizing (ex. 예외처리, DB 처리 등) 하여 연동하시는 것을 권장 드립니다.
> (샘플파일을 그대로 사용하시는 것은 권장 드리지 않습니다.)

1.1. 결제 처리 구성도

① SMARTROPAY 에서 결제 요청 하는 WEB PAGE 를 이용하여 상점 측 결제 요청 페이지 작성
② SMARTROPAY 전자지불 솔루션 연동 페이지 호출
③ PG 서버를 통해 VAN 사 및 대외기관을 연결하여 결제 결과를 상점으로 전송



1.2. 결제 관련 용어

구분	내용
GID (Group ID)	- 회원사를 구분하는 ID 인 MID 를 발급하는 경우, 해당 MID 는 GID 와 多:1(= MID:GID)형태로 연결되어 있습니다. - MID 를 다수 발급하는 경우, MID 를 결제수단 및 사용용도에 따라 그룹별로 관리하기 위해 MID 를 GID 로 그룹화하여 관리하기 위해 사용합니다.
MID (Merchant ID)	- 회원사에 영문과 숫자로 이루어진 10 자리의 상점 ID 를 발급합니다. - 회원사는 ID 로 상점을 구분하여 거래를 처리하므로, 반드시 ID 를 발급받아 SMILEPAY 전자결제 서비스를 등록해야 합니다. - 최초 설치 시 ID 는 테스트용으로 설정된 상태이므로 운영 전환 시 반드시 실제 발급받은 MID 를 사용해야 정상적인 서비스가 가능합니다.
MOID	- 회원사 판매 상품에 대한 주문(order) ID
TID	- 결제 시 생성되는 거래(transaction) 고유 ID 입니다. - 결제 테스트 진행 후 TID 를 별도로 기록하여 관리하시고, 결제 취소 테스트 시 사용하면 됩니다.
상점 서명키 (MerchantKey)	- 상점 서명키는 결제 데이터의 위·변조를 방지하기 위해 MID 발급시에 설정되는 키입니다. - 서명키는 https://www.smilepay.co.kr 사이트(가맹점 > 가맹점정보 > KEY 관리 메뉴)에서 확인할 수 있습니다. ※ 상점 서명키는 패스워드와 같은 중요한 정보이므로, 가맹점에서는 발급받은 상점 서명키를 안전하게 관리하는 것을 권장합니다.
인증 / 비인증	- 인증 : 신용카드 결제 시, 카드사 자체 인증 페이지를 띄우고, 추가 인증 절차를 거쳐 카드사 승인을 받는 형식 - 비인증 : 신용카드번호와 유효기간 등의 정보로 카드사 승인을 받는 형식
MallUserId	- 고객 구분을 위한 고유한 ID 정보
SspMallId	- 신용카드 빌링, 간편결제에서 사용하는 상점 전용 Mall ID 정보 - 통합 간편결제 서비스인 신용카드 빌링, 간편결제 서비스는 동일한 SspMallId 를 사용하는 MID 를 통해 회원정보 공유가 가능합니다.

1.3. 결제 서비스의 특징

서비스	특징
신용카드	인터넷 쇼핑몰에서 상품을 구매하거나 서비스를 이용할 때 결제 대금으로 신용카드를 이용하여 결제하는 서비스입니다.
신용카드 ISP (인터넷안전결제)	신용카드를 이용하여 쇼핑몰에서 상품을 구매할 때, 신용카드 결제 정보에 대한 보안과 인증 기능이 포함된 신용카드 결제 서비스입니다. (비씨카드, 국민카드)

신용카드 빌링 (Billing Key)	고객이 정기적으로 납부하는 금액을 고객에게 발급된 빌링키를 이용하여 정기적으로 과금 처리하는 결제 서비스 입니다.
신용카드 안심클릭	신용카드 결제 시 VISA 에서 제공하는 3D 인증 및 보안 기능이 추가된 신용카드 결제 서비스입니다.
계좌이체	은행 계좌이체를 통합하여 각종 쇼핑몰에서 상품을 구매하거나 서비스를 이용할 때 결제 대금을 계좌이체를 통해 결제하는 서비스입니다. 인터넷 뱅킹과 관련된 파일, 인증서 등이 설치된 PC 에서 인터넷 뱅킹 시스템을 이용하여 계좌이체로 지불하는 방식이며, 이용금액은 고객의 계좌에서 실시간으로 차감됩니다
가상계좌	고객이 은행 별 가상계좌를 이용하여 인터넷 쇼핑몰에서 물품 대금 결제 시 대금입금을 위한 은행계좌번호를 부여 받은 후 해당 가상계좌로 물품대금을 무통장 입금하거나 폰 뱅킹, PC 뱅킹 또는 인터넷 뱅킹 등을 이용하여 온라인으로 입금하는 서비스입니다.
휴대폰	고객이 상품구매 및 서비스 이용 시 결제 대금을 고객이 소유한 휴대폰을 이용하여 결제하는 서비스입니다. 결제된 금액은 고객의 휴대폰 요금에 합산되어 청구됩니다.
문화상품권	고객이 상품구매 및 서비스 이용 시 컬쳐랜드에서 충전한 컬쳐캐쉬를 이용하여 결제를 하는 서비스 입니다. 상품권 번호를 직접 입력하여 결제하는 방식도 가능합니다.
에스크로 (결제대금예치제)	에스크로(escrow)는 상거래 시에, 판매자와 구매자의 사이를 중개하여 물품을 거래하는 결제서비스입니다.
간편결제	고객은 최초 1 회 본인인증 및 신용카드와 결제 비밀번호를 등록하여 간단히 비밀번호를 입력 후 결제하는 간편결제 서비스입니다.

1.4. 결제 서비스 이용 절차

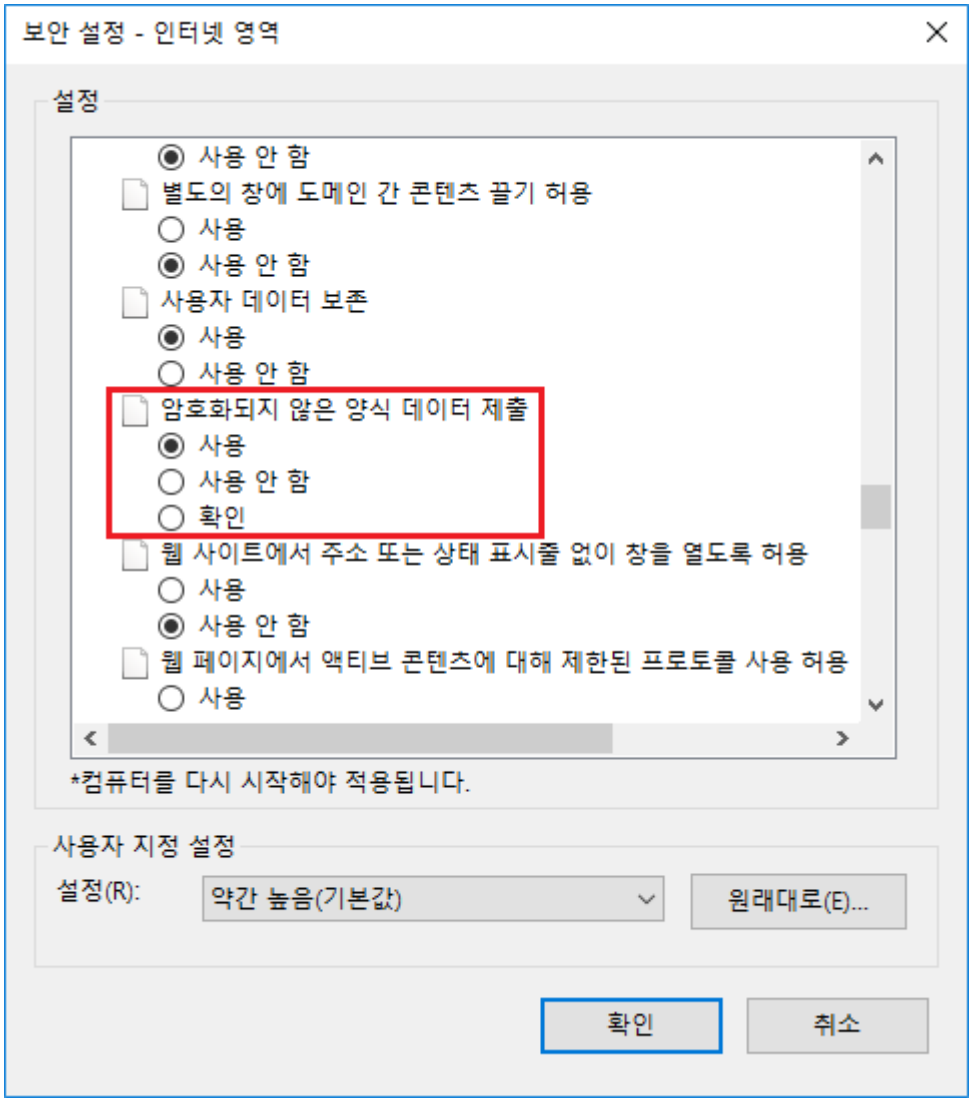
구분	내용
회원사 등록 신청	- 결제 서비스를 이용하기 위해 회원사 등록 및 ID 발급을 신청합니다.
프로그램 및 설치 매뉴얼 다운로드	- 결제 페이지 구성을 위해 용도별 해당 프로그램 다운로드 및 설치 매뉴얼을 다운로드 합니다. (JSP, PHP, ASP, ASP.NET 용)
서명키 확인	- 결제 데이터의 위·변조 방지를 위해 회원사 서명키를 회원사 관리자 페이지에서 확인하여 결제요청 시 해당키를 사용합니다.
설치 프로그램 수정	- 결제 서비스 연동을 위해 해당 설치 프로그램을 수정합니다.
설치 프로그램 테스트	- 프로그램의 정상 동작을 확인하기 위해 결제 테스트를 진행합니다.

2. 결제 브라우저 환경설정 안내

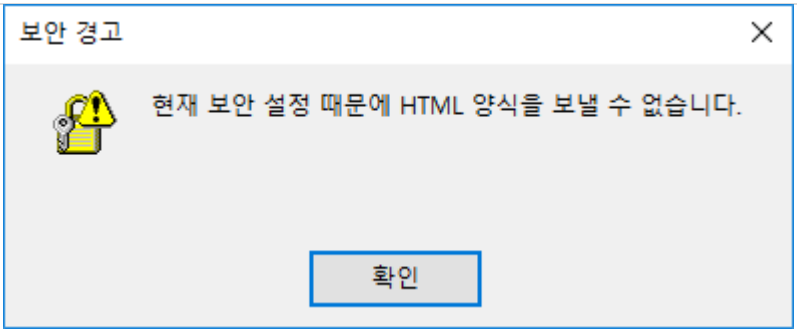
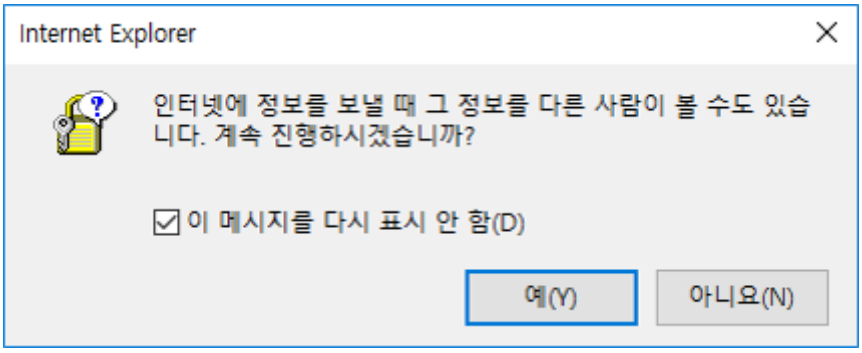
2.1. 사용자 PC 브라우저 환경설정 관련 안내

가맹점에서 도메인 URL 을 HTTP 프로토콜을 사용하는 경우, HTTPS 에서 HTTP 로 전환 시, 사용자 브라우저의 환경설정에 따라 최종 결제 결과(ReturnURL)를 수신할 때, 브라우저 내부 확인 창이 호출됩니다. 이 점에 대하여 미리 가맹점에 안내를 드립니다.

*** 인터넷 옵션 > 보안 탭 > 사용자 지정 수준 > 암호화되지 않은 양식 데이터 제출**



구분	내용
사용	보안경고팝업 미 노출, 정상적인 결제진행 가능합니다. -> 가맹점 ReturnURL 로 결제결과 전달 가능.
사용 안 함	

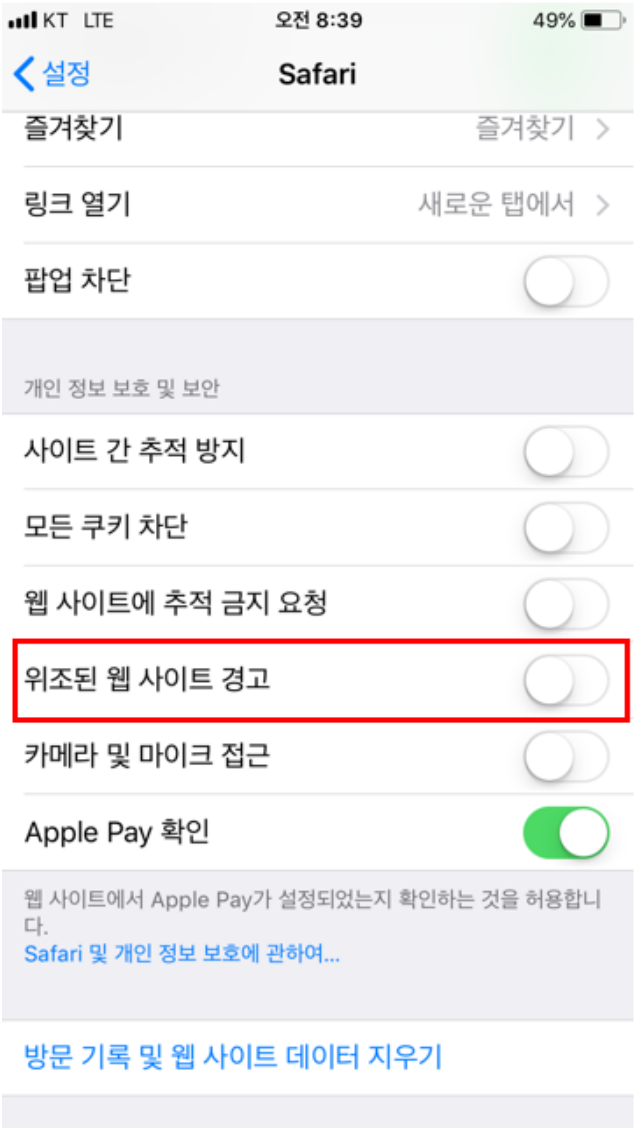
	 위와 같은 보안경고팝업 노출 후, 정상적인 결제진행 불가능합니다. -> 가맹점 ReturnURL 로 결제결과 전달 불가능.
확인	 위와 같은 보안경고팝업 노출 후, - "예" 선택 시, 정상적인 결제진행 가능합니다. -> 가맹점 ReturnURL 로 결제결과 전달 가능. - "아니오" 선택 시, 정상적인 결제진행 불가능합니다. -> 가맹점 ReturnURL 로 결제결과 전달 불가능.

2.2. 모바일 Safari 브라우저 결제결과 수신 관련 특이사항

가맹점에서 도메인 URL 을 HTTP 프로토콜을 사용하는 경우, HTTPS 에서 HTTP 로 전환 시, 최종 결제 결과를 수신할 때, Safari 브라우저에서 내부 확인 창이 호출됩니다.
이 점에 대하여 미리 가맹점에 안내를 드립니다.

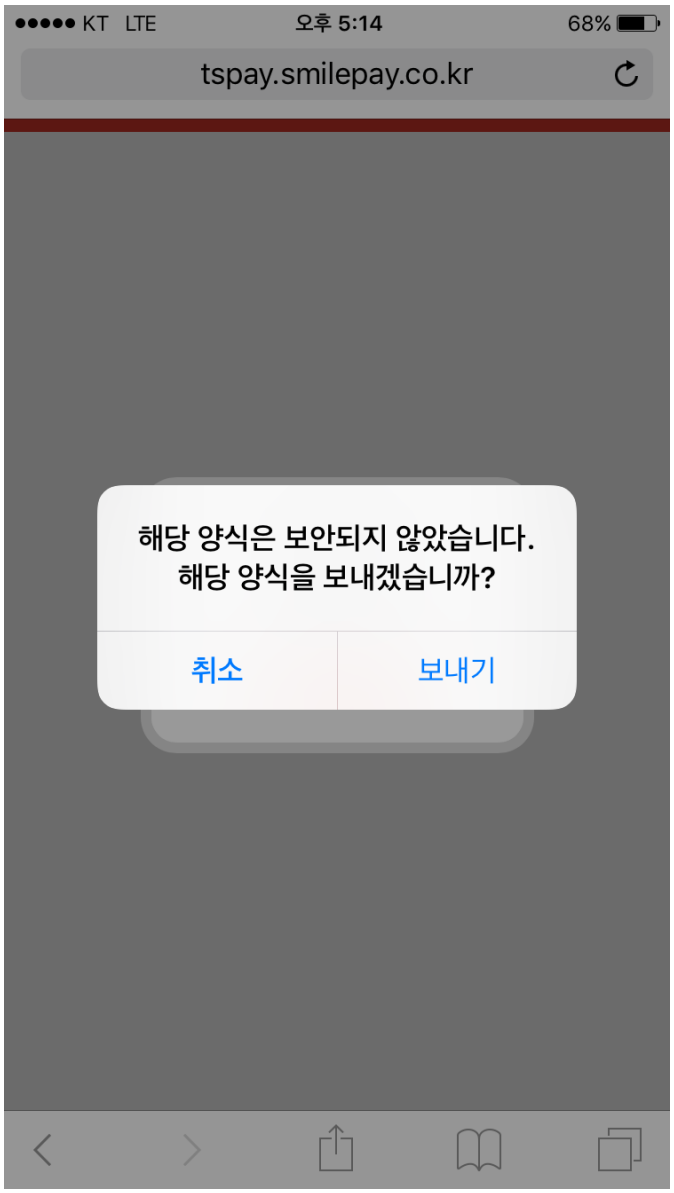
2.2.1. Safari 브라우저 설정 권장 사항

Safari 브라우저 설정의 위조된 웹 사이트 경고 해제를 권장 드립니다.



2.2.2. Safari 브라우저 내부 확인 창

가맹점이 HTTP 프로토콜을 사용할 경우, 위의 Safari 브라우저 설정 사항을 적용하셔야 결제결과 수신이 가능합니다.



구분	내용
취소	정상적인 결제진행이 불가능합니다. -> 가맹점 ReturnURL 로 결제결과 전달 불가능.
보내기	정상적인 결제진행이 가능합니다. -> 가맹점 ReturnURL 로 결제결과 전달 가능.

3. 결제 테스트 안내

- 설치 후 상점 프로세스와의 연동이나 실제 서비스 전환 등을 시행하기 이전에 개발 및 운영 서버에서 반드시 테스트가 필요하며, 테스트가 진행되지 않는 경우 당사로 문의 부탁 드립니다.
- 테스트 서버 (https://tpay.smilepay.co.kr) 에서 승인된 결제는 당사 취소모듈을 통해 직접 취소하시기 바랍니다.

> **※ Note**
> 결제 테스트를 위해 가맹점에서는 스마트로 영업 담당자를 통해 당사 테스트 서버에서 사용 가능한 MID 및 MerchantKey(가맹점키) 정보를 안내 받으시길 바랍니다.

3.1. 스마트로 결제모듈 데모

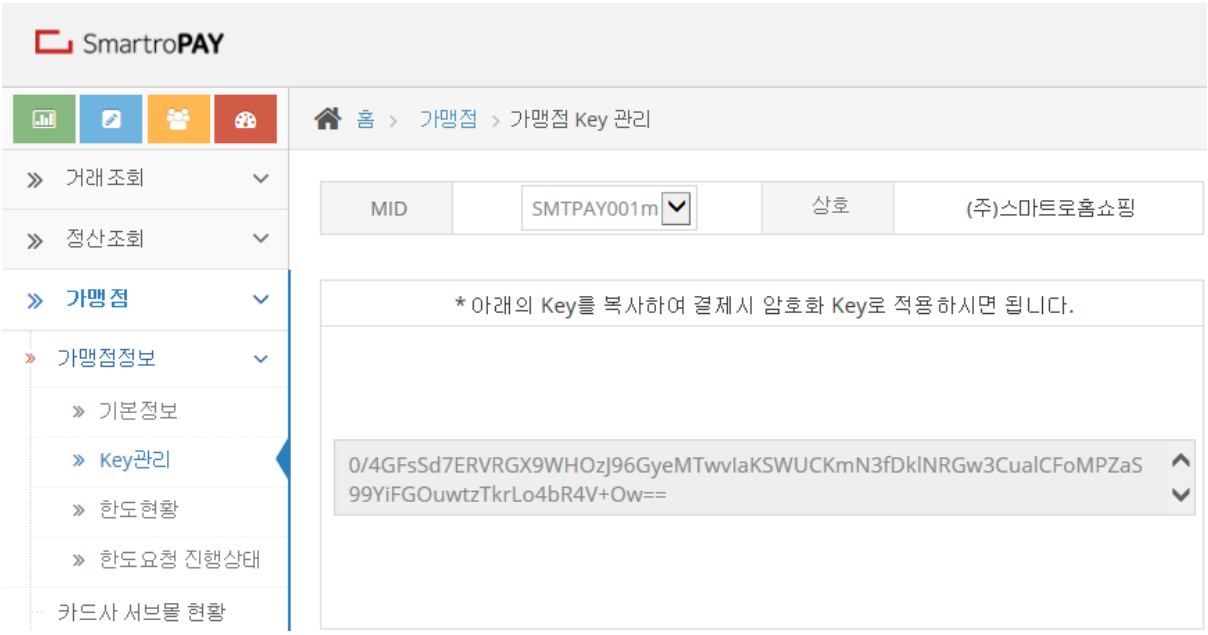
스마트로 PG 홈페이지의 [기술지원 > 결제 미리보기] 메뉴에서 WEBLink 방식의 결제모듈 데모 버전 이용 가능합니다.

접속 URL
https://pg.smartro.co.kr/

3.2. 상점키 안내

스마트로 담당자를 통해 신규 발급된 운영 MID 에 대한 상점키(merchantKey)는 스마트로 가맹점 관리자 페이지의 [가맹점 > 가맹점정보 > Key 관리] 메뉴에서 확인 가능합니다.

접속 URL
https://www.smilepay.co.kr/



> **※ Note**
> - 상점에서는 실 서비스 오픈 시 스마트로 담당자를 통해 발급받은 MID 의 상점키(merchantKey)를 설정 후 당사 운영서버로 결제모듈을 연동합니다.

3.3. 결제서비스 URL

구분	서비스	접속 URL
PC	Test	https://tpay.smilepay.co.kr
	Real	https://pay.smilepay.co.kr
Mobile	Test	https://tspay.smilepay.co.kr
	Real	https://smpay.smilepay.co.kr

3.4. 가상계좌 강제입금 통보 테스트 URL

아래의 가상계좌 강제입금 통보 테스트 URL 은 개발 서버에서만 테스트 가능합니다.

서비스	접속 URL
개발 URL	https://tpay.smilepay.co.kr/payTest/vbank_deposit_notice.jsp

3.5. 계좌이체 결제 테스트 안내

계좌이체 테스트 거래는 아래의 테스트 결제정보로 테스트 가능하십니다.
금융결제원 BankPay 결제 페이지에서 테스트 거래는 보안매체선택(보안카드, OTP)과 같은 보안절차를 생략하며, 일반결제만 테스트 가능합니다.

3.5.1. 예금주실명번호

BankPay 테스트시스템에 개인정보가 저장되지 않도록, 금융결제원에서 제공하는 테스트 예금주실명번호를 입력하여 계좌이체 테스트를 진행 합니다.

전자지갑내 입력항목	정보입력방법	
예금주실명번호	법인 (사업자등록번호)	128-75-17955
	개인 (주민등록번호)	631206-1277229
금융기관	임의의 금융기관 선택	
계좌번호	'000' 으로 시작하는 임의의 번호 입력 (계좌번호자리수 : 8~14 자리)	
계좌 비밀번호	'000' 으로 시작하는 임의의 번호 입력 (계좌 비밀번호 자리수 : 4 자리)	

3.6. 신용카드 결제 테스트 안내

- 신용카드 결제는 체크카드가 아닌, 신용카드로만 테스트를 권장 드립니다.

4. 방화벽 설정

가맹점 서버에 방화벽이 설정되어 있다면 이용할 결제 서비스 별 PG 서버의 IP / Port 정보를 확인하여 가맹점 측 방화벽에 등록하시기 바랍니다.

1. Adaptor 방식 (Socket 통신 방식)

연결대상	포트	프로토콜	연결방향
211.193.35.7 (test)	9001	TCP	OUTBOUND
211.193.35.215 (real)	9001	TCP	OUTBOUND

2. WEBLink 방식

연결대상	포트	프로토콜
211.193.35.7 (test)	443	HTTPS
211.193.35.16 (real)	443	HTTPS

3. 결제 데이터 통보 (재통보 서비스)

연결대상	포트	프로토콜	연결방향
211.193.35.7 (test)	80/443	HTTP/HTTPS	INBOUND
211.193.35.216 (real) 211.193.35.217 (real)	80/443	HTTP/HTTPS	INBOUND

※ Note

결제 데이터 통보 URL 은 80/443 Port 만 이용 가능하며, 타 Port 를 이용할 경우 스마트로 영업담당자를 통해 방화벽 허용 요청이 필요합니다.

타 Port 개방을 위한 스마트로 서버 방화벽 작업에 따라 수 일의 시간이 소요될 수 있습니다.

5. 가맹점 연동문의 지원

- 스마트로 결제모듈 담당자는 SMARTROPAY 결제모듈을 연동하는 가맹점의 개발 및 현업 담당자에게 기술&연동문의를 지원하고 있습니다.
결제모듈 관련 기술&연동문의시 결제모듈타입, 디바이스 등을 고려하여 문의사항에 대한 피드백을 진행해야 하므로, 아래의 내용을 별도로 확인해야 합니다.

① 결제모듈 타입
- WEBLink (HTTP 통신) 혹은 Adaptor (Socket 통신)
② 디바이스
- PC, Mobile, Mobile Native App, Server to Server
③ 결제수단
- 신용카드, 계좌이체, 가상계좌, 휴대폰결제 등
④ 결제방식
- 인증결제, 비인증결제
⑤ 결제모듈 버전
- 가맹점 결제모듈 배포 버전 확인

> **※ Note**
> 가맹점 결제모듈 시스템의 배포내역을 통해 연동문의 가맹점의 결제모듈 타입, 디바이스, 결제수단, 결제방식 및 버전을 확인합니다.

6. 자주하는 기술문의 Q&A 질의 및 답변

- 스마트로 결제모듈 연동 시 자주 발생하는 현상 및 기술문의에 대한 질의 문답을 참고 바랍니다.

6.1. PG Plug-in 결제결과 창 Skip 문의

스마트로 PC Plug-in 에서는 스마트로 결제확인 화면 > 결제결과 화면 > 가맹점 ReturnURL 페이지 호출 형태로 결제 프로세스가 진행됩니다.
PG 결제결과 화면 Skip 여부는 결제요청파라미터 MallResultFWD 를 통해 설정 가능하며 MallResultFWD=Y(권장사항) 로 설정 후 결제를 진행하시면 됩니다.

6.2. PC Plug-in 화면에서 한글 깨짐 현상 관련 문의

스마트로 PC Plug-in 서버는 EUC-KR 기반으로 구성되어 있으며, 가맹점 서버가 UTF-8 환경일 경우, 한글 데이터는 EUC-KR 로 별도 인코딩 처리가 필요합니다.

6.3. Mobile Plug-in 화면에서 한글 깨짐 현상 관련 문의

스마트로 Mobile Plug-in 서버는 UTF-8 기반으로 구성되어 있으며, 가맹점 서버가 EUC-KR 환경일 경우, 한글 데이터는 UTF-8 로 별도 인코딩 처리가 필요합니다.

6.4. PC Plug-in 결제결과 데이터 인코딩 처리 문의

가맹점페이지의 인코딩 방식이 "UTF-8"인 경우, 결제 요청 파라미터 URLEncode="Y", EncodingType="utf8"로 설정하여 결제요청을 하시면, 가맹점에서 결제요청결과 응답시 한글 데이터를 "UTF-8"로 인코딩 처리된 데이터를 응답 받을 수 있습니다.

> **※ Note**
> 당사 서버에서는 결제결과 form 의 accept-charset 을 가맹점이 설정한 EncodingType 으로 설정 후 returnURL 로 응답 데이터를 전달합니다.
> <form name="tranMgr" method="post" action="" accept-charset="UTF-8">

6.5. 결제요청 시 "The requested URL was rejected. ~" 노출 (거래불가)

결제요청 인입 데이터 중 특정 파라미터의 value 값이 방화벽에서 blocking 된 경우, 해당 현상이 발생할 수 있습니다.
가맹점에서는 스마트로 기술 담당자를 통해 blocking 된 사유를 확인하여 결제요청 정보의 형식 확인 및 수정이 필요합니다.

6.6. 각 카드사 별 인증 페이지에서 가능한 결제방식이 상이합니다.

가맹점이 카드사 계약 시 카드사에서는 각 가맹점 고유의 가맹점번호를 발급하여 관리합니다.

당사에서는 각 카드사 별 인증 페이지를 연동하여 호출하고 있으며 카드사에서는 계약된 가맹점 정보를 기반으로 인증 페이지를 노출합니다.
이처럼 각 카드사 별 계약 내용 및 가맹점 성격 (ex.환금성가맹점) 에 따라, 카드사 인증 화면에 노출되는 결제방식이 상이할 수 있으며, 자세한 문의는 해당 카드사를 통해 확인이 필요합니다.

6.7. 위·변조 검증값 오류 관련 문의

스마트로에서는 HTTP 통신시 결제데이터의 위조 및 변조 여부를 검증하기 위해 해쉬값(EncryptData, SignValue) 유효성 검증을 수행하고 있습니다.
위·변조 검증값(HASH 유효성 확인 실패) 오류는 위·변조 데이터 검증에 실패했을 경우 발생하며, 가맹점에서는 해쉬값 생성 규칙 및 해쉬 데이터 생성 문자열에 대한 확인이 필요합니다.

> **※ Note**
> 결제요청 시 가맹점에서 생성 후 전달한 위·변조 데이터와 서버에서 생성한 데이터의 값이 일치하지 않을 경우, HASH 유효성 확인 실패 오류가 발생합니다.

6.8. 스마트로 PG Plug-in 화면 로고 변경 문의

스마트로 PG Plug-in 결제 화면에서는 기본 스마트로 로고가 노출됩니다.
가맹점 자체 로고를 사용하려면, 스마트로 영업 담당자를 통해 가맹점 서버 로고 이미지를 전달하여 상점 ID(MID) 기준정보에 로고 이미지 등록을 합니다.
등록 완료 후 해당 MID 로 결제시도 시 PC, Mobile Plug-in 화면에서 가맹점 자체 로고가 노출됩니다.

6.9. 가맹점 개발환경이 Native App 일 경우 추가 개발사항 문의

가맹점 개발환경이 Native App 일 경우, Hybrid 결제모듈 연동 작업이 추가로 필요합니다.
Hybrid 결제모듈을 통해 인증 App 설치 및 호출, 인증 정보 전달 등의 인증 관련 절차의 구현이 필요하므로, 일반 WEBLink 및 Adaptor 결제모듈과 Hybrid 결제모듈을 함께 연동하시기 바랍니다.

> **※ Note**
> Hybrid 결제모듈의 경우, 결제요청 파라미터 clientType 를 "HYB"로 설정하여 연동합니다.

6.10. 모바일 Hybrid 결제모듈 연동시 인증완료 후 가맹점 App 재호출 여부 문의

ISP 결제인 경우, 결제요청 파라미터 urlScheme 에 가맹점 App 의 URL 스키마를 설정하는 것으로 인증 완료 후 가맹점 App 재호출 가능하나, ISP 외의 인증 App 의 경우 모바일 OS 별 차이가 있습니다.
- Android 인 경우, 인증단계에서 스마트로 PG Plug-in 을 통해 인증 App 을 호출하여 인증이 완료되면 Backgroud 에 있던 가맹점 App 이 재로딩됩니다.

- IOS 인 경우, 인증이 완료되면 Backgroud 에 있던 가맹점 App 이 재로딩되지 않습니다.
따라서, IOS 의 환경에서는 고객이 인증완료 후 기존 PG Plug-in 화면으로 이동하는 Action 이 필요합니다.

6.11. 모바일 Plug-in 결제모듈 연동 시 인증완료 후 기존 브라우저 호출

고객이 각 카드사 인증 App 에서 인증 완료 후, 기존 스마트로 PG Plug-in 화면으로 이동하기 위해 브라우저 호출시 고객의 기본 브라우저 설정 값에 따라 기존 결제를 진행하던 브라우저의 종류가 아닌 기본 브라우저가 호출될 수 있습니다.
이와 같은 경우, 기존 결제를 진행하던 브라우저로 직접 이동하는 Action 을 통해 결제를 계속하여 진행하실 수 있습니다.

6.12. 현금 영수증 발급 문의

계좌이체 및 가상계좌 결제 시 스마트로 PG Plug-in 화면에서 현금영수증 발급 정보를 입력하는 화면이 노출됩니다.
발급정보를 입력 후 결제를 진행하면 해당 결제 건에 대해 현금영수증 발급이 가능하며, 추후 해당 결제를 취소할 경우, 현금 영수증 발급도 취소 됩니다.

가맹점에서 단독 현금영수증을 발급을 원하는 경우, 아래와 같은 방법으로 이용이 가능합니다.

1. 당사 가맹점 관리자 페이지의 현금 영수증 발급 메뉴를 통해 수기로 현금 영수증 발급
2. 현금 영수증 결제모듈 연동을 통해 현금 영수증 발급 (가맹점 추가 개발 필요)

> **※ Note**
> 현금 영수증 발급 정보 입력 화면이 노출되지 않을 경우, 스마트로 영업 담당자를 통해 MID 기준정보에 현금 영수증 사용 설정을 요청하시기 바랍니다.

6.13. 가맹점 서버가 HTTP 프로토콜을 이용하는 경우 특이사항

당사 스마트로 PG 서버는 HTTPS 프로토콜을 사용합니다.
가맹점 서버에서 HTTP 프로토콜을 사용하는 경우, 최종 결제 결과를 수신할 때 HTTPS(스마트로 PG 서버)에서 HTTP(가맹점서버)로 전환되면서 브라우저 설정 값에 따라, 최종 결제결과 수신이 어려울 수 있습니다.
해당 내용 관련해서는 연동 규격서의 [사용자 브라우저 환경설정 관련 안내]를 참고해주시고 안내 내용에 따라 브라우저 환경설정 후 결제 진행 시 결제결과를 정상적으로 수신할 수 있습니다.

6.14. 결제 Plug-in 화면 카드사 노출 여부 관련 문의

신용카드 결제 시 Plug-in 화면의 노출되는 카드사 종류는 발급받은 가맹점 MID 의 기준정보 설정 값에 따릅니다. 특정 카드사 사용 및 노출 유무 설정 관련 내용은 스마트로 영업 담당자를 통해 요청 바랍니다.

6.15. WEBLink 방식 결제모듈 연동 시 가맹점 방화벽 설정 관련 문의

WEBLink 방식 결제모듈을 사용하는 가맹점에서 방화벽 설정이 필요한 경우, 아래의 IP/Port 정보를 방화벽에 등록하여 연동하시기 바랍니다.

- 운영 서버 IP : 211.193.35.16 / Port : 443
- 테스트 서버 IP : 211.193.35.7 / Port : 443

6.16. 고객 결제 도중 사용자 취소 시 이동 페이지 관련 문의

Mobile 버전에서 고객이 결제 취소할 경우, stopURL (가맹점 결제중지 페이지) 로 이동하며, PC 버전에서는 returnURL (가맹점 결제결과 페이지) 로 이동합니다.

6.17. 모바일 ISP 인증 결제 시 오류 발생 문의

모바일 ISP 인증 결제시 인증 App 구동 및 인증완료 단계에서 결제요청 파라미터를 기준으로 당사 서버에서 별도 내부 처리를 하고 있습니다. 이러한 인증 단계에서 가맹점에서 전달한 결제요청 파라미터의 특정 값이 연동 규격을 준수하지 않은 경우, 오류가 발생할 수 있습니다. 가맹점에서는 해당 오류 발생 건에 대한 결제요청 파라미터의 연동 규격 확인이 필요합니다.

> **※ Note**
> Ex. 모바일 ISP 인증 결제 시 결제요청파라미터 GoodsName 의 값이 정의된 길이(80Byte) 보다 초과된 경우라면, (그 외 결제요청 파라미터 동일) 인증 단계에서 오류가 발생할 수 있습니다.

6.18. 모바일 WEBLink 방식 iframe 사용 관련 문의

일반 WEBLink 방식일 경우 결제모듈 연동 시 IOS 버전에서 iframe 사용은 권장사항이 아닙니다. (iframe 사용불가)

6.19. Adaptor 방식과 WEBLink 방식의 차이점 문의

- WEBLink 방식은 인증과 승인이 하나의 프로세스로 구성된 HTTP 통신 방식입니다.
- Adaptor 방식은 인증과 승인이 분리된 형태의 Socket 통신 방식입니다.

6.20. 스마트로 PG 데모 이용 문의

스마트로 PG 홈페이지에서 WEBLink 방식의 결제모듈 데모 버전을 제공하고 있으며 접속 URL 은 아래와 같습니다.

- https://pg.smartro.co.kr [기술지원 > 결제 미리보기 메뉴 > PC / Mobile 결제데모 이용]

6.21. Smartro PG 결제내역 확인 문의

가맹점 관리자 사이트를 통해 결제내역 확인 및 출력이 가능하며, 고객은 당사 PG 홈페이지를 통해 결제내역 확인이 가능합니다.

(1) 스마트로 PG 홈페이지 [고객센터 > 결재내역조회] 서비스 이용

- https://pg.smartro.co.kr/

(2) 스마트로 결제내역 API 연동

 # 직접 거래내역서를 호출할 수 있는 URL 을 통해 결제내역 확인이 가능합니다.

구분	URL 예시
Test	https://test.smilepay.co.kr/issue/IssueLoader.jsp?TID=smartro01m01011507291348513881&type=0
Real	https://www.smilepay.co.kr/issue/IssueLoader.jsp?TID=smartro01m01011507291348513881&type=0
연동 방식	
https://www.smilepay.co.kr/issue/IssueLoader.jsp?TID=[TID 설정]&type=[type 설정] (1) TID : 스마트로 거래 ID (2) type : 지불수단 타입 0 - 각 지불 수단(신용카드,휴대폰결제,계좌이체... 등)일 경우 2 - 현금영수증 (type = 0 혹은 2 값 누락 시 오류페이지 이동)	

(3) 가맹점 관리자 페이지를 통해 결재내역 확인

-> 가맹점 관리자 페이지는 운용 계정을 발급 받으신 후, 이용이 가능합니다.

6.22. 가맹점 추가정보 필드 문의

가맹점에서 추가정보 필드 요청이 있을 경우, 상점예비정보 필드를 추가로 안내하고 있습니다.

결제 요청시, 연동 규격서에 안내된 결제 요청 파라미터 설정 [mainPay.jsp/php/asp/aspx] 의 파라미터와 함께 아래의 상점예비정보를 전달해주시면 됩니다.

파라미터	파라미터 내용	길이	필수	비고
MallReserved	상점예비정보	char(500)	선택	한글입력 시 Base64 사용

- 상점예비정보 예시 : {Form 변수}={Form 값}&{Form 변수}={Form 값}&{Form 변수}={Form 값}& ...
응답 값의 인코딩 처리가 필요합니다.

*** 주의사항**

(1) 상점예비정보 필드는 위와 같이 크기에 제한이 있으므로, 전달 받으려는 데이터를 MallReserved 파라미터에 모두 설정하는 방법이 아닌, MallReserved 에 전달 받고자 하는 데이터의 Key 값을 설정하고 Key 값에 해당되는 실제 Value 데이터를 Session 이나, 데이터베이스에 저장하여 가맹점에서 별도로 처리하는 것을 권장합니다.

(2) 전달 받으려는 데이터를 MallReserved 파라미터에 모두 설정하여 사용하신다면, 한글 데이터가 깨질 수 있으므로 Base64Encoding 의 별도 처리가 필요합니다.

6.23. 결제결과데이터 통보 (재통보 서비스) 방화벽 관련 문의

당사(src)에서 가맹점(dst)으로 나가는 outbound 는 80/443 port 하에 Any 로 열려 있으며 80/443 port 가 아닌 특정 포트로 재통보 서비스를 이용하려면, 추가 등록 절차가 필요합니다.

가맹점에서 따로 방화벽으로 차단하고 있지 않는다면, 당사 운영서버에서 전달되는 결제데이터 통보를 가맹점이 설정한 RetryUrl 로 수신이 가능합니다.

6.24. 결제결과데이터 통보 (재통보 서비스) 프로세스 문의

결제가 완료된 건에 대해 가맹점이 설정한 재통보 URL 을 HTTP 통신으로 호출하여 결제결과 정보를 재전달하고 있으며, 이때, 재통보는 가맹점 관리자를 통해 설정한 재통보 간격 및 횟수를 기반으로 처리됩니다.
가맹점이 설정한 재통보 URL 을 호출 후 HTTP 상태코드 및 가맹점 응답코드(OK)를 통해 재통보 성공 여부를 판단하고 있습니다.

6.25. 결제결과데이터 통보 (재통보 서비스) 설정 후 미통보 오류 문의

결제결과데이터 통보 설정 후로부터 발생한 결제 건에 한하여 재통보가 처리됩니다.

6.26. 스마트로 PG 매입전/후 취소(전취소/후취소) 관련 문의

스마트로 PG 서비스의 결제취소는 카드사 매입 전 취소와 매입 후 취소로 구분됩니다.
매입 전 취소는 당일에만 가능하며, 카드사로 직접 결제취소 요청 후 취소 처리가 가능합니다.
매입 후 취소(결제 당일 이후 취소)는 카드사 결제취소 요청이 아닌, 취소일자 이후 매입 건에 취소거래를 반영하여 카드사로 매입을 진행하게 됩니다.
따라서, 후취소의 경우 카드 결제 내역에 취소 상태가 반영되기 까지 일정시간이 소요될 수 있으며 결제취소에서 매입 전, 매입 후 취소는 카드사 요청 여부에 따라 취소 결과 응답 값이 상이할 수 있습니다.

6.27. 가상계좌 입금 완료 후 결제취소 관련 문의

가상계좌 채번 후에 고객이 해당 가상계좌로 입금을 완료한 경우, 해당 결제 건에 대한 취소는 환불 거래로 진행해야 합니다.

해당 결제 건에 대한 환불처리는 가맹점에서 별도로 환불을 진행하거나, 스마트로 환불 서비스를 이용하는 방법이 있습니다.

6.28. 승인 TID 중복 오류 문의

승인 TID 중복 오류는 최초 승인완료 이후,
당사 승인요청 페이지에서 새로 고침을 하거나, 사용자가 Back 키를 눌러 이전 페이지 이동 후 해당 페이지로 재 진입을 하여 빈번하게 발생되는 현상입니다.
최초 승인완료 후 위와 같은 조작을 통해 기존 승인된 TID 에 대해 당사 서버로 중복 승인요청이 발생할 수 있습니다.

> **※ Note**
> 스마트로에서는 TID 중복 승인 건에 대해 임의로 결제취소를 진행하지 않습니다.

6.29. MID 및 MerchantKey 관련 문의

발급받은 MID 와 MerchantKey 는 ID / Password 과 같은 개념으로, MID : MerchantKey 가 1:1 로 매칭됩니다.
상점 서명키 (MerchantKey) 는 패스워드와 같은 중요한 정보이므로, 가맹점에서는 상점 서명키를 안전하게 관리하는 것을 권장합니다.

6.30. 부분취소 관련 문의

부분취소 요청시 취소 금액(CancelAmt)에 원 거래에 대해 취소할 금액을 설정합니다.
원 거래 승인금액이 11,000 인 건에 대해 1,000 원 부분취소를 진행한다면, 거래 잔액은 10,000 원이 됩니다.

6.31. 정기결제 (빌링키) 프로세스 문의

빌링키 결제는 아래와 같은 프로세스로 진행됩니다.

(1) 회원등록 및 카드등록 (빌링키 발급)
최초 등록인 경우 고객은 회원등록(본인인증) 절차를 거치며, 회원등록 후 카드번호를 등록하여 빌링키를 발급합니다.
-> 빌링키 발급 요청 파라미터의 가맹점 ReturnURL 로 빌링키 발급 결과를 수신 (발급받은 빌링키 정보)
(2) 빌링키 결제승인 요청
앞서 발급받은 고객의 빌링키를 통해 당사 결제서버로 승인 요청하여 실시간 빌링 승인 서비스를 구현합니다. (ex. 정기결제)

6.32. 정기결제 연동시 본인인증 관련 문의

정기결제 연동시 고객이 최초 회원등록일 경우, 본인인증 절차가 필요합니다.

결제정보등록 요청 파라미터 중 고유 고객 구분 정보인 "MallUserID"(회원사 고객 ID) 로 회원등록 여부를 판단합니다.