

모바일OK기반 상거래 기술

(주)페이게이트

2010.2.3

페이게이트 이야기

- 주력서비스 : 해외결제
 - 해외발행카드결제, 달러결제
 - 일본계좌이체, 중국CUP, Alipay
- 경쟁업체 : PayPal, WorldPay
- 국제적 보안(PCIDSS), 웹표준

모바일OK

- 웹사이트 또는 웹 응용에 유무선 단말의 종류에 구애받지 않고 이용할 수 있는 웹 표준 기술
- History
 - 2009년 3월 MOK표준기반 결제시스템 제안/채택
 - 2009년 11월 개발완료
- 소개동영상

MOK 웹표준기반 결제시스템 구현가능한가?

- 전자인증
 - 여신전문금융업 감독규정 제24조의 6
- 기술적 침해대응
 - 전자금융감독규정 시행세칙 제29조
- 30만원이상 공인인증 적용
 - 전자금융감독규정 시행세칙 제31조

전자인증방안

- 카드비밀번호 인증
- 안심클릭 인증
- 모바일ISP
- 금액인증
- 기타

카드 비밀번호 인증

- 카드번호 + 유효기간 + 카드비번
- 소액에 한정
- 국내 한정

안심클릭 인증

- 스펙상 가능성 있음
- 전카드 미지원
- 국내전용, 일부 해외
- 팝업구조
- 탭자가 되버린 현실

모바일 ISP

- App 기반
- 일부카드사 한정
- 국내전용

금액인증

AA, Amount Authentication

금액인증 개념

- 신용카드 승인금액을 OTP로 이용
- 절차
 - 20만원짜리 상품구매 가정
 - 소비자에게서 카드정보 받아 20만원 미만의 Random한 금액(AA) 생성
 - AA금액으로 승인획득후 소비자에게 본인의 카드발행사에 문의하여 승인금액 확인하도록 요청
 - 소비자는 카드사전달 SMS등을 통해 금액확인
 - 소비자 입력 금액이 AA금액과 일치하면 거래취소후 원거래금액으로 재승인

승인금액 확인방식

- 카드사 제공 SMS, E-Mail
- 카드사 웹사이트 방문
- 카드사 전화문의
- 카드사 고객센터 방문
- 기타 카드사와 카드소지자간의 약정된 안전한 개인정보 제공방식 이용

금액인증 옵션

- 프로파일DB (한번인증받은 유저가 동일 카드로 재결제시 절차생략)
- 금액인증 시작 최저금액 설정
- Timeout
- 세션저장

해외사업자와 비교

- PayPal

- 세계1위 결제업체
- 승인시 가맹점 이름 앞에 Random한 코드 추가
- 소비자가 알아서 Random code 확인하여 인증코드로 사용

- Alipay

- 중국1위업체
- 소비자 계좌로 소액을 2회 이체
- 소비자가 알아서 이체금액 확인하여 인증코드로 사용

MOK 웹표준기반 결제시스템 구현가능한가?

- 전자인증방안
 - 여신전문금융업 감독규정 제24조의 6
- 기술적 침해대응방안
 - 전자금융감독규정 시행세칙 제29조
- 30만원이상 공인인증 적용방안
 - 전자금융감독규정 시행세칙 제31조

기술적 침해 대응방안

- 종단간 암호화
- 입력정보 보호대책
- 악성코드 예방대책

종단간 암호화

- SSLv3 / TLSv1
- Server Proxy 배제

입력정보 보호대책

- Javascript Screen Keyboard
 - 키배열 Randomize, Masking
- Javascript Security
 - 무결성 검증, 동적로딩, 난독화, Caja

악성코드 예방대책

- platform Detect하여 안전한 platform만 허용
- DNS 정보변조 검증
- 그림문자(Captcha)이용 로봇결제 방지
- OWASP 10대 보안취약점 방어적용
- 웹방화벽 설치
- 정기적 침투시험
- 이용자 보안권고 및 인지동의

MOK 웹표준기반 결제시스템 구현가능한가?

- 전자인증방안
 - 여신전문금융업 감독규정 제24조의 6
- 기술적 침해대응방안
 - 전자금융감독규정 시행세칙 제29조
- 30만원이상 공인인증 적용방안
 - 전자금융감독규정 시행세칙 제31조

공인인증 적용방안

- 공인인증 사용예외
- SSL Client Certificate Authentication

공인인증 사용예외

- 전자금융거래법 시행세칙 31조
 - 본인계좌에 대한 조회
 - 전화, CD/ATM등과 같이 공인인증서의 설치 운용이 불가능한 수단을 이용한 전자금융거래
 - 등록금, 원서접수비 등 본인확인이 가능하고 입금계좌가 지정되어 있는 경우
 - 전자상거래에서 지급결제로서 30만원 미만의 신용카드 결제 또는 온라인 계좌이체
 - 전자화폐, 선불전자지급수단을 온라인상에서 사용하는 경우
 - 금융기관등이 범위를 정하여 공인인증서 적용을 제외할것을 감독원장에게 요청하고 감독원장이 이를 승인하는 경우

공인인증서를 사용할 수 없는 기술환경

- 다양한 Device나 Platform이 시장에 나오고 있음.
- 공인인증서를 사용할 수 없는 기술환경은 항상 존재함
- 이러한 간극은 영원히 지속
- 한번에 해결할 해법은 없는가?

오픈웹 대법원 판결

- 공인인증기관은 Firefox유저에 대한 가입 사설비제공 의무 없음
- Firefox == Non-IE
- 공인인증기관 : 의무(X)
- 민간사업자 : 의무(?)

공인인증 해법

- 공인인증기관이 가입자설비를 제공하는 기술환경
 - 의무사용 (공인인증기관이 제공범위 확대할수록 의무사용범위 증가)
- 그외 기술환경
 - 민간사업자 자율에 맞겨야
 - 자율(보안업체 솔루션 구매, 직접제작, 사용안할수도)

SSL Client Auth

- 선택한 자율적 해법
- 대부분 Browser에서 SSL Client Authentication 지원
- 웹표준 환경에서 동작

App기반 인프라 구성 의 위험성

- 스마트폰 App에 기반하여 국가 전자상거래 인프라 구성하는것은 매우 위험
- 해외 벤더의 승인과정
 - 승인을 잘 안해줌, 승인했다가 취소하기도
- 일개 해외벤더의 정책등에 따라 국가 전자상거래 인프라가 무너질 위험성 존재
- 지속가능한 기술환경에 기반한 인프라 구축이 필요

확산

- 제도적 확산 : 금감원 보안성 심의
- 기술적 확산 : KECIS

KECIS

- 한국형 전자상거래 서비스 제공자간 상호연동 표준안(*)
- Korea Electronic Commerce Interoperability Standard

KECIS에서 무엇을 표준화하자는지인지?

- 주고받는 데이터 구조를 표준화 => IETF ECML
- 주고받는 방법을 표준화 => OASIS SAML 응용
 - 서비스 “요청”과 “응답”방식을 표준화
- 효과
 - 서비스 제공자는 자신의 고유한 구조나 방법을 유지하되 KECIS구조를 “추가”
 - 서비스 자체가 제3자 웹서비스에 결합될 수 있는 표준화된 Application Interface를 갖추게 됨

KECIS 시연

References

- KECIS
<http://mountieit.blogspot.com/2009/12/kecis.html>
- 스마트폰기반 카드결제서비스
http://docs.google.com/View?id=dhm28v4q_125dtq92qct

Contact

- 발표자 : 이동산 (Mountie Lee)
- Web : <http://paygate.net>
- Tel : 02-2140-2700
- Email : mountie@paygate.net
- Twitter : mountielee