m-Commerce 서비스를 위한 지불 및 보안 기술 동향

SK텔레콤(주) 최준원 · 김지희 · 임재철

1. 무선 보안 및 기술 동향

무선 보안 기술에 대해서 Security Infrastructure (WPKI) 구성과 WAP Forum, IETF에서 다루어지고 있는 무선 보안 관련 기술 동향을 소개한다.

WPKI

아래의 그림은 WPKI Configuration 및 각 Entity 간의 동작을 간략하게 나타낸 것이다.

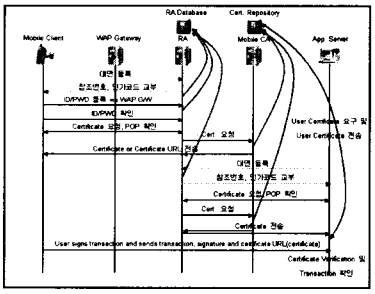


그림 1 WPKI Configuration

WPKI에서 사용되는 보안 Algorithm Set의 다음과 같이 구성 될 수 있다.

표 1 WPKI Algorithm Set
(M : Mandatory, O : Optional,
R: Recommend, N/A : Not Assigned)

알고리즘		Server	Mobile	비고
Symmetric Algorithm	3DES(168) CBC	M	M	
	Seed(128) CBC	M	M	
	AES(128) CBC	N/A	N/A	
Signature Algorithm	RSA	M (생성) M (확인)	O (생성) M (확인)	Mobile Client은 반드시 알고리즘 중 하나는 반드시 지원
	KCDSA	O	O	
	ECDSA	O (생성) M (확인)	M (생성) R (확인)	
Key Agreement Algorithm	ECDH	M	R	Mobile Client은 반드시 알고리즘 중 하나는 반드시 지원
Key Transport Algorithm	RSA	M	R	
Hash Algorithm	MD5	O	O	If KCDSA supported
	SHA-1	M	M	
	HAS-160	O(M-비고)	O(M-비고)	

WPKI를 지원하는 각 Entity의 Certificate Format은 아래 표와 같이 구성 될 수 있다

(N/A : Not Assigned)

표 2 Certificate Format

인증서 형식	서버 인식/처리	Mobile Client 인식/처리
WTLSCertificate	Mandatory	Mandatory
무선용 X.509 v3 인증서	Mandatory	Strong Recommended
X.509 v3 인증서 (RFC 2459)	Mandatory	N/A

Trusted CA Information Handling을 위해 Signature Verification Method과 Out of band hash verification method를 지원할 수 있으며, Mobile Client으로의 인증서 전송은 인증서가 정상적으로 발생되었다는 메시지와 함께 인증서의 URL을 전송 (application/vnd.wap.cert-response Content Type) 하는 것으로 처리할 수 있다.

WMLScript-CryptoEx Functions

WAP Application Layer에서 보안/인증 서비스를 제공하기 위한 것으로. End to End Security 보장하기 위해 다음과 같은 signTextEx 및 encryptTextEx을 사용할 수 있다.

signedString=CryptoEx.signTextEx(stringToSign, options, keyIdType, keyId)

wapEnvelopedData=CryptoEx.encryptTextEx (flag, dataToEncrypt, recipientPublicKey, keyMegementAlgorithm, contentEncryptionAlgorithms, rid_type, rid)

WAP Forum, IETF에서 다루어지고 있는 무선 보안 관련 주요 무선보안 관련기술은 TLS(Transport Layer Security) and TLS Extensions, Certificate Revocation Checking Mechanism / OCSP, Piggy backing, XML 기반 보안기술 등이다.

```
Simplified OCSP :
   SimplifiedOCSPRequest ::= SEQUENCE {
     tbsRequest            TBSRequest,
      ... -- RFU
   }TBSRequest ::= SEQUENCE {
     version               [0] Version DEFAULT v1,
     requestList           SEQUENCE SIZE (1..ub_requests) OF Request
   }Version ::= INTEGER  { v1(0) }Request ::= SEQUENCE {
     reqCert               CertID,
     ... -- RFU
   }CertID ::= SEQUENCE {
     hashAlgorithm         AlgorithmIdentifier{{OCSPHashAlgorithms}},
     issuerNameHash        OCTET STRING (SIZE(8..MAX)),
     issuerKeyHash         OCTET STRING (SIZE(8..MAX)),
     serialNumber          INTEGER (1..MAX)
   }
SimplifiedOCSPResponse ::= SEQUENCE {
     responseStatus        OCSPResponseStatus,
     responseBytes         [0] ResponseBytes OPTIONAL
   }ResponseBytes ::= SEQUENCE {
     responseType          OCSP-RESPONSE.&id ({OCSPResponses}),
     response  OCTET STRING
     -- response는 responseType에 의해 확인되는
     -- Extension Object에 대한 &ResponseType의 DER 값이다.
   }BasicOCSPResponse ::= SEQUENCE {
     tbsResponseData       ResponseData,
     signatureAlgorithm    AlgorithmIdentifier {{OCSPSignatureAlgorithms}},
     signature             BIT STRING,
     ... -- RFU
   }
ResponseData ::= SEQUENCE {
     version               [0] Version DEFAULT v1,
     responderID           ResponderID,
     producedAt            GeneralizedTime,
     responses SEQUENCE SIZE(1..ub_responses) OF SingleResponse,
     ... --RFU
   }
SingleResponse ::= SEQUENCE {
     certID                CertID,
     certStatus            CertStatus,
     thisUpdate            GeneralizedTime,
     nextUpdate            [0] GeneralizedTime OPTIONAL,
     ... --RFU
   }
```

TLS(Transport Layer Security) and TLS Extensions

전송계층보안 기술인 TLS (RFC 2246)는 기본적으로 SSL v3에서 발전한 기술이며 이미 많은 웹서버 및 클라이언트 환경에 적용되어 있다. "TLS Extensions" 은 기존 TLS 규격에서 6가지 확장 필드를 추가한 규격이며 확장필드는 다음과 같다. Virtual Hosting 지원을 위한 dns_name, Record Size Negotiation을 위한 max_record_size, 클라이언트 인증서 URL 전송을 위한 certificate_url, 서버의

신뢰된 CA 정보 전송을 위한 trusted_ca_keys, HMAC Size를 줄이기 위한 truncated_hmac, 서버 인증서 Revocation 확인을 위한 status_request

Certificate Revocation Checking Mechanism

무선 환경에서 Certificate Revocation Checking 메커니즘으로는 OCSP(On line Certificate Status Protocol, RFC 2560) 또는 Piggybacking 방식이 논의되고 있다. Certificate Revocation Checking 메커니즘으로 OCSP를 기반으로 Piggybacking 방식(예:TLS 및 Signed Data의 전송 시)도 일부 적용될 수 있다. OCSP의 경우 RFC 2560 전체를 적용하는 방안보다는 RFC 2560의 무선 적용 버전인 Simplified OCSP 형태가 적용될 수 있으며, Simplified OCSP 및 Piggybacking 방식을 간단히 설명하였다(page 7 참조).

XML 기반 보안 기술

XML 기반 전자서명(X Signature)의 경우 W3C 및 IETF를 중심으로 상당수준 표준화가 진행되었으며 XML 기반 암호(X Encryption) 및 키 관리(XKMS) 등 표준화가 진행중이다. XML 기반 보안 기술의 경우 다소 메시지 크기가 길어지는 문제점에도 불구하고 XML 자체가 가지는 많은 장점 및 무선 클라이언트의 ASN.1의 Encoding/Decoding의 처리의 제약으로 인해 향후 무선 환경에서 무선보안기술로써 XML 기반 보안기술은 지속적으로 활발한 논의가 예상된다.

2. 무선 지불 결제 및 기술 동향

무선 컨텐츠 전자 지불, Shopping Mall의 전자 지불 결제와 같이 상품 및 컨텐츠를 제공하는 CP들은 지불 결제를 대행해 주는 Payment Gateway와 같은 전문 지불 대행 업체를 활용하고 있으며, 무선 WAP 단말, PDA등의 다양한 사용자 무선 환경 플랫폼에서의 보안 Protocol 및 지불 결제용 전자지갑(e-Wallet) 구현에 대한 부담을 해소함과 동시에, 지불 결제 수단별로 가맹점 계약 및 정산 관리를 해야 하는 불편함도 줄 일 수 있다. 무선 환경에서 사용자 편의성을 위한 다양한 지불 결제 수단을 제공하며, CP들에게 단일한 정산 채널을 제공하기 위한 통합 지불 결제 서비스에 대한 수요는 계속 증가될 것이며, Smart Card 기반의 e-Wallet은 사용자에게 안전하고 편리한 지불 수단을 제공할 것이다.

Smart Card 기반의 VSDC Payment

무선 환경에서 Payment Server와 Smart Card 기반의 e-Wallet을 이용한 VSDC Purchase Transaction Flow는 아래와 같다.

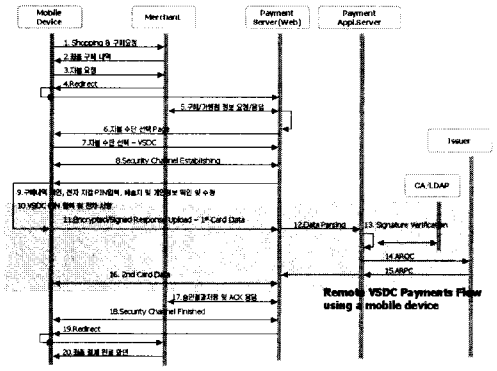


그림 2 Remote VSDC Payment Flow using a mobile device

VSDC의 무선 거래 시, Offline Data Authentication (SDA or DDA)는 실행하지 않으며, CVM을 실행 한 후, 3DES algorithm 방식의 ARQC를 포함한 Online Transaction Processing을 진행한다. Visa 회원사의 IC Card Data 처리 가능 여부에 따라 VisaNet과 Issuer 간 Earl Option 또는 Full Option으로의 Online Transaction을 실행한다. Cardholder Verification은 offline PIN을 통하여 카드 소지자 검증과 카드 분실, 도난 카드 사용 방지를 위한 것으로 향후 Visa 3-D Secure에서의 Payer Authentication으로 구현될 수 있다.

3-D Secure

3-D Secure는 SSL 기반의 Authenticated Payment Protocol로 Online 상에서 Payment Authorization Request Processing 진행 전에 Issuer로부터 사용자 인증을 받는 과정으로 Cardholder의 Authentication은 Password 방식 이 외에, SIM Toolkit, WPKI, VSDC 등을 활용 할 수 있다. 현재, 3-D Secure Protocol은 Mobile Internet Device용 Extension 규격을 제공하고 있으나, 각 Issuer의 ACS와 모든 가맹점의 MPI가 다양한 Mobile Device Platform 환경에서 Cardholder Authentication을 구현하는데 PARes를 Reconstructing 해야 하며, 무선 구간에서의 Redirect 횟수가 늘어나는 등 어려움이

예상된다.

3-D Secure Mobile Extension, using e-wallet and Payment Server

Payment Server와 e-Wallet을 이용하여, 향후 중요한 지불 수단이 될 Smart Card 기반의 VSDC Purchase Transaction에 대한 무선 환경에서의 3-D Secure 구현을 아래와 같이 제안한다.

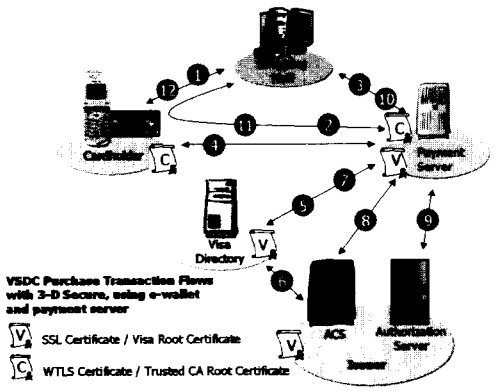


그림 3 VSDC Purchase Transaction Flows with 3-D Secure

위 그림에 대한 단계별 설명은 아래 표와 같다.

표 3 Purchase Transaction Description

Step	Description	Note
1	사용자가 Shopping Mall에서 구매물품을 장바구니에 담고 결제를 진행 함.	
2	사용자의 Payer Authentication 및 Payment Authorization을 위해 Payment Server로 Redirection 됨.	
3	사용자의 구매 내역 요청하며, Payment Server로 전송 함.	
4	사용자의 구매 내역을 확인하고, 전자 지갑 비밀번호 입력 후, 개인 정보, 배송지 정보, 비자 안전 지불 비밀번호를 확인 및 수정함. 개인 인증서가 있는 경우, 전자서명을 이어 VSDC 결제 진행을 함.	3-D Secure (Password Auth.)
5	Payment Server는 Visa Directory에 PAN을 전송 함.	3-D Secure
6	Visa Directory는 Card Range 검사 후, PAN이 등록되어 있는 ACS를 검색 하며, 해당 ACS는 회신 함.	3-D Secure
7	Visa Directory는 PG Server의 MPI로 ACS의 URL정보와 함께 VERes를 회신 함.	3-D Secure
8	Payment Server는 해당 ACS에 Payer Authentication을 요청 하며, ACS는 PARes를 Payment Server에 회신하며, Authentication History에 결과를 저장 함.	3-D Secure
9	MPI는 PARes의 Signature를 Verification한 후, EMV Payment Authorization Process를 진행 함.	3-D Secure
10	Payment Server는 승인 결과를 Shopping Mall에 전송 함.	
11	결제 처리 완료 메시지와 함께 Shopping Mall로 Redirection 함.	
12	사용자에게 최종 처리 결과를 전송 함.	

Payer Authentication은 Password를 통하여 할 수 있으며, Chip Card를 이용할 수도 있다. Password의 경우, 사용자 단말의 e-Wallet에 미리 저장하여, Payer Authentication 진행 시 Password를 확인 후, Payment Server를 통해 ACS에 인증을 요청한다. Chip Card의 경우, VSDC Authentication Process를 Payment Server를 통해 Issuer의 ACS와 진행한다. Server Authentication을 위해서는 미리 등록된 PAM을 사용자에게 Display 하는 대신, Server Certificate의 DN Attributes를 이용하여 Trusted한 Server임을 증명할 수 있다.

Payment Server가 Payer Authentication을 중계하기 때문에, PARes의 Validation을 위해 아래의 Signature Syntax에 대한 Reconstructing을 하지 않아도 되며, 무선 망 구간을 통한 Redirect 및 통신 횟수를 줄임으로써, 전체 Transaction Process 소요시간 단축과 거래 완료 신뢰성을 높일 수 있다.

```
XML-Signature Syntax
<ThreeDSecure>
  <Message>
    <PARes id=" PARes12345" >...</PARes>
      <Signature>
        <SignedInfo>
          <Reference URI=" #PARes12345" >
          ...
          </Reference>
        </SignedInfo>
      </Signature>
  </Message>
</ThreeDSecure>
```

3-D Secure Core Funcions v1.0.1 이후의 향후 방향은 PAReq와 VEReq에 대해서 가맹점의 signature를 이용한 Merchant Authentication을 포함한다.

3. Off-line Access 기술 및 동향

3.1 바코드 및 쿠폰 응용 서비스 및 기술 동향

제품의 표면, 카드, 표지판 등 다양한 사물의 표면에 부착된 바코드를 판독하여 Mobile Device 사용자에게 해당 사물에 연계된 정보를 제공하거나, 특정 기능을 수행시킬 수 있는 On/Offline 통합 서비스이다. 1차원 바코드 응용 서비스로는 Mobile Phone에 바코드를 다운로드 받아 오프라인 가맹점 POS의 스캐너로 해독, 가입자 인증을 거쳐 상품 제조사의 할

인품목을 일괄적으로 자동 할인 또는 포인트 적립을 받게 되는 Mobile 전자 쿠폰 서비스가 있다. 바코드의 전송규격은 WBMP(Wireless BMP)나 동영상 압축 전송 솔루션으로 폭넓게 활용되고 있는 SIS(Simple Image Service)규격을 사용한다.

1차원 바코드에 비하여 향후 다양한 서비스의 기본 플랫폼으로 자리 매김 할 것으로 예상되는 2차원 바코드로는 DATA MATRIX CODE, QRCODE CODE, MAXICODE CODE, CODEONE CODE, PDF-417 CODE, CODE49 CODE 등이 있으며, 2차원 바코드의 적용 사례로 2차원 코드 전자영수증 발행 서비스, 2차원 코드 고지 서비스, 모바일 폰 2차원 코드 전자고지 시스템, 2차원 코드의 압축.복원 기술 및 위.변조방지 시스템, 2차원 코드 전자문서 네트워크 솔루션, 2차원 코드 인력관리 시스템, 2차원 코드 물류관리 시스템등에 활용 될 수 있다.

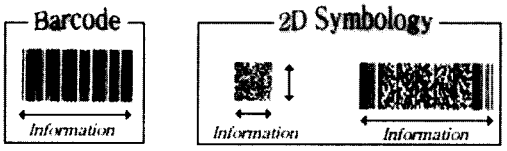


그림 4 1D, 2D Barcodes

표 4 Barcode 비교표

코드 종류	1차원 바코드	2차원 바코드
데이터 형식	알파벳, 숫자	알파벳, 숫자, 특수문자, Binary 숫자, 다국적 언어
데이터 저장 용량	약 20자 내외	약 2000자 내외
데이터 밀도	1	20-100
데이터 복구 가능성	NO	YES

3.2 IrDA, RF, Bluetooth

RF, IrDA, Bluetooth와 같은 근접 통신을 통한 휴대폰의 Off-line Access 지불 서비스가 상용화 되고 있다. RF 방식은 단순한 통신이 가능하며, IrDA 방식은 'Point and Shoot' 의 지향성을 갖으며, IrFM을 통한 Financial Transaction에 대한 프로토콜이 구현된다. Bluetooth 방식은 'Select and Connect' 으로 무지향성으로 프로토콜 구현에 제한이 없는 것이 장점이다.

IrFM의 구성은 IrDA를 기반으로 하여 Client-Server Mode의 형태를 가지도록 되어 있으며, 다음 그림은 IrFM의 구성에 대한 개념을 나타낸다.

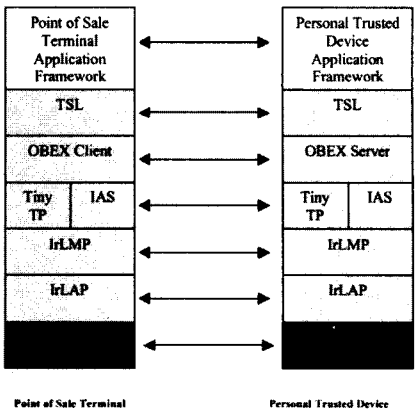


그림 5 IrFM Architecture

위에서 IrDA 하드웨어부터 OBEX 까지는 IrDA 규격을 그대로 따르며, IrDA의 위에 TSL (Transaction Service Layer)을 도입하였다. TSL은 OBEX 함수들을 이용해서 구현되는 primitive들로 구성이 된다. 다음의 그림은 IrFM에 기반한 off-line access를 통한 EMV 결제 거래 Flow를 나타낸다. IrFM을 통하여 PTD와 POS Terminal간 Data Process가 진행되며, Cardholder Verification은 PTD에서 이루어지며, POS Terminal에서 DDA 또는 SDA의 off-line authentication processing과 on-line processing은 Terminal Action Analysis에 따라 수행 될 수 있다.

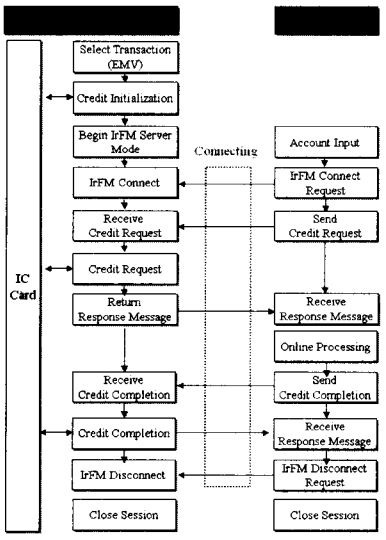


그림 6 EMV Transaction Flow based on IrFM

참고문헌

[1] EMV2000 Integrated Circuit Card Spec for Payment Systems - Book1~4.

[2] Visa Smart Debit/Credit ? System Technical Letter

[3] Visa Integrated Circuit Card (ICC) Specification, v1.3.1

[4] 3-D Secure Protocol Specification v 1.0, May 2001.

[5] 3-D Secure Protocol Specification Mobile Extension for Internet Devices, Draft v 0.1 May 2001.

[6] "WML Script Crypto API," WAP Forum, November 1999.

[7] "WMLScript Language Specification," WAP Forum, November 1999.

[8] "Wireless Transport Layer Security Specification," WAP Forum, November 1999.

[9] "WAP Architecture Specification," WAP Forum, April 1998.

[10] "WAP Public Key Infrastructure Definition", WAP Forum, July 2000.

[11] "The LDAP URL Format," IETF RFC 2255, T. Howes. M. Smith, December 1997.

[12] IETF RFC 2246 : TLS Specification

[13] IETF RFC 2459 : PKIX Certificate & CRL Profiles

[14] IETF RFC 2560 : OCSP

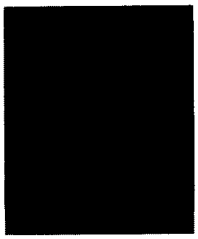
[15] IETF Security Area Draft : TLS Extensions

[16] http://www.NeSign.co.kr

[17] http://www.NePay.co.kr

[18] http://www.moneta.co.kr

최 준 원



1995 고려대학교 전기공학과 졸업

2000년 영국 University of Manchester Institute of Science and Technology(UMIST) 전기전자공학과 통신공학 석사 졸업. 현재 SK Telecom 무선 전자지불 결제, 전자화폐 충전 시스템 및 Payment 규격 담당.

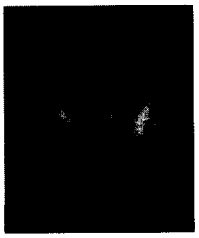
E-mail:jerry@sktelecom.com

김 지 희

1997 이화여자대학교 컴퓨터학과 졸업, 현재 SK Telecom WPKI 시스템 담당.

E-mail:poem24@sktelecom.com

임 재 철



1994 서울대학교 전자공학과 졸업, 현재 규격 담당.

E-mail:jchullim@sktelecom.com