# e-비지니스 환경에서 메시지 보안을 고려한 웹 서비스 와 CBD 통합에 관한 연구

하 얀*
*경인여자대학 정보미디어학부
e-mail:white@kic.ac.kr

# A Study on Integration of Web Service considering Message Security and CBD for e-business environment

Yan Ha*
*School of Information & Media, Kyungin Women's College

## 요 약

본 연구는 메시지 보안을 고려한 웹 서비스와 컴포넌트 개발 방법론의 통합에 관한 것으로, 컴포넌트 저장소에 있는 컴포넌트들을 검색하여 동적으로 웹 서비스를 제공하는 시스템을 기반으로 안전한 웹 서비스를 위해 메시지 보안 요소를 지원하기 위한 것이다. 이질적인 컴포넌트들로부터 통합된 프레임워크를 제공하고, 이들로부터 동적으로 웹 서비스를 생성하는 과정에서 웹 서비스의 보안을 개선시키고자 한다. 이를 위해 XML 기반 보안 및 전자서명 인증 기술의 포함으로 메시지 내용의 무결성과 기밀성을 보장하는 것을 목표로 한다.

키워드 : Message Security, Web Service, e-business environment, CBD

## I. 서론

웹 서비스 메시지 보안 기술인 WS-Security는 웹 서비스의 메시지 교환 프로토콜인 SOAP을 기반으로 하여, 인증, 무결성, 부인봉쇄, 기밀성 등의 보안 기능을 확장하여 제공하는 웹 서비스의 보안의 핵심이 되는 기술로 2004년 OASIS에서 표준으로 채택된 기술로 W3C의 XML 전자서명 및 XML 암호를 확장하여 다양한 보안 모델과 암호화 기술을 적용해 안전한 웹 서비스 애플리케이션을 지원하는 것이다[1].

본 연구는 메시지 보안을 고려한 웹 서비스와 컴포넌트 기반 개발을 통합하기 위한 연구로 사용자로부터 컴포넌트들 검색을 요청받아 컴포넌트 저장소로부터 컴포넌트를 검색하고 탐색된 컴포넌트를 웹 서비스를 통해 제공하는 시스템에서 안전한 웹 서비스 제공을 위한 보안 요소 적용을 위한 것이다. WS-Security 는 이질적인 시스템 간의 보안 정보 교환을 위한 상호 운용성 보장을 목적으로 하므로 본 연구에서는 이를 이용하여 안전한 웹 서비스를 목적으로 하며, 이질적인 컴포넌트 통합 및 웹 서비스 생성을 하고자 한다. 본 연구의 의의는 e-비지니스 환경에서 이질적인 컴포넌트 활용성을 향상시키며, 안전하게 웹 서비스를 제공하는 것을 그 목표로 한다.

## II. 관련 연구

본 연구는 크게 2가지 분야의 관련 연구를 포함한다. 첫째, 웹 서비스 보안이다. 웹 서비스 보안과 관련된 표준으로는 XML Signature, XML Encryption, WS-Security, XKMS, SAML, XACML, WS-Trust, WS-policy 등이 있다[2][3]. 특히, WS-Security는 기본적으로 XML 서명과 암호화를 사용하여 안전한 웹 서비스를 구축할 때 사용되는 무결성과 기밀성을 구현하기 위해 SOAP 확장의 표준 세

트를 제공하는 것으로, 보안 토큰 확산 등의 메커니즘을 제공한다. WS-policy는 웹 서비스 네트워크에서 사용할 보안 토큰의 종류, 지원하는 알고리즘 등 보안 정책에 관련된 정보들을 표준적으로 교환하고 해석할 수 있도록 하는 표준이다. WS-Trust는 웹 서비스가 안전하게 작동할 수 있도록 학기 위한 신뢰모델에 대한 표준이다. WS-Federation은 다양한 환경에서 신뢰관계를 어떻게 관리하고 중개할 것인가에 대한 표준이다. WS-SecureConversation은 통신 당사자 간에 보안 문맥을 어떻게 관리하고 교환할 것인가에 대한 표준이다[4]. 이외에도 웹 서비스 네트워크에서 보다 개선된 보안을 위해 여러 가지 표준 제정 작업이 이루어지고 있다.

둘째, 컴포넌트개발 방법론과 웹 서비스를 통합에 관한 연구로 이질적인 컴포넌트들로부터 동적 웹 서비스 생성에 관한 연구이다. [5]는 컴포넌트의 재사용성을 위해 이질적인 컴포넌트로부터 웹 서비스를 동적으로 생성하는 연구를 했다. 이에 [6]은 온톨로지 기반 시맨틱 웹 서비스 생성을 위한 연구를 진행한 바 있다. 그러나 이들 연구에서 보안과 관련된 요소는 언급되지 않아 안전한 웹 서비스를 위한 보안 요소의 적용이 필요하다.

## III. 본론

### 1. 웹 서비스 보안

웹 서비스는 사용자의 인증정보 및 속성 등의 보안 정보를 전달하는 방법을 요구하고 보안 정보가 여러 경유지를 거쳐 최종 목적지에 전달되는 동안 무결성과 기밀성을 보장할 것을 요구하는데, 보안 정보를 전달하는 방법은 SOAP(Simple Object Access Protocol)이다. 이 같은 메시지 수준의 보안은 다음과 같은 특징을 갖는다[7]. 기본적인 전송 메커니즘으로부터 독립적이며, 이기종 보안 구조에 사용할 수 있으며, 종단간 보안을 제공한다. 그리고, 여러 암호화 기술을 지원하며, 부인방지 기능을 제공한다. 여기서 부인방지는 송신자는 데이터 전송에 대해 부인할 수 없는 것이다.

일반적으로 XML 암호화 기술은 XML 문서의 부분적 요소에 대한 암호화와 복호화를 지원하는 것으로 기밀성 서비스를 제공한다. 〈표 1〉은 XML 암호화 구조를 나타낸 것이다[한국전산원].

그리고, XML 서명은 XML 문서에 대해 XML 형태의 서명을 생성하고 검증할 수 있는 서명 기법이며, 전자문서에 대해 인증(authentication), 무결성(integrity), 부인방지(non-repudiation) 등의 정보보호 서비스를 제공한다. 인증은 입증된 ID를 가진 누구나 서비스에 접근하는 것이고, 무결성은 송신자와 수신자 간에 전송되는 데이터는 변경되지 않는 것이다.

〈표 1〉 XML 암호화 구조

```
<EncryptedData Id? Type?>
  <EncryptionMethod/>
  <ds:KeyInfo>
      <EncryptedKey>?
      <AgreementMethod>?
      <ds:KeyName>?
      <ds:RetrivalMethod>?
      <ds:*>?
   </ds:KeyInfo>?
  <CiperData>
     <CiperValue>?
     <CiperReference URI?>?
  </CiperData>
</EncryptedData>
```

〈표 2〉 XML 서명 구조

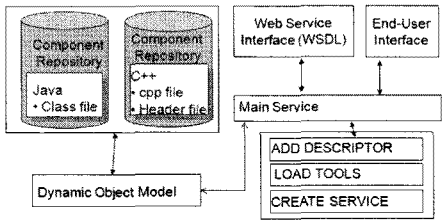
```
<Signature>
  <SignedInfo>
     (CanonicalizationMethod)
     (SignatureMethod)
     (<Reference URL=)? >
       (Transforms)?
       (DigestMethod)
       (DigestValue)
       </Reference>)+
      <SignedInfor>
      (KeyInfo)?
      (Object)*
   </Signature>
```

〈표 2〉는 XML 서명 구조이며, 여기서 발생지시자 '?'은 0번 혹은 1번, '+'는 1번 이상, 그리고 '*'는 0번 이상을 나타낸다[조광문].

본 연구에서 적용하는 WS Security는 XML 문서 암호화와 서명을 포함하는 것으로, 보안 토큰을 포함하여 보안 솔루션을 제공한다는 점이 XML 암호화와 서명과 다른 점이다. 여기서, 보안 토근이란 요청의 모음을 나타내는 것으로 디지털 서명된 보안 토큰은 특정 인증 기관에서 암호화하여 승인된 보안 토큰(예, X.509)을 의미한다. 또한, 소유 증명 토큰은 송신측이 소유 증명을 나타내기 위해 사용할 수 있는 데이터가 들어 있는 것을 의미한다.

### 2. 웹 서비스 동적 생성

웹 서비스를 동적으로 생성하기 위해서는 클라이언트가 서비스를 필요로 할 때 실행 시간에 웹 서비스로 변환되어야 한다. 컴포넌트로부터 웹 서비스의 동적 생성은 컴포넌트의 본질에 의존하고 적당한 도구와 기법은 동적으로 웹 서비스를 생성하기 위해 사용된다. 동적으로 컴포넌트를 배치시키는 그림은 〈그림 1〉과 같다.

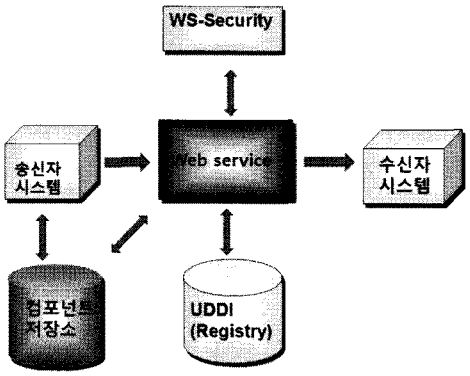



〈그림 1〉 컴포넌트로부터 웹 서비스 생성

〈그림 1〉에서 컴포넌트는 자바와 C++컴포넌트를 사용하며, 자바 컴포넌트를 동적으로 배치하기 위해 Apache SOAP의 형태를 이용하고 C++ 컴포넌트는 C++를 위한 WASP Server 도구를 이용하여 웹 서비스로 변환한다.

## 3. 전체 시스템

WS-Security를 포함한 웹 서비스와 컴포넌트 기반 개발을 통합한 전체 시스템은 〈그림 2〉와 같다. 각 구성 요소는 크게 송신자 시스템, 수신자 시스템, 컴포넌트 저장소, UDDI Registry, 웹 서비스 그리고, WS-Security 이다.




〈그림 2〉 전체 시스템 구성 요소

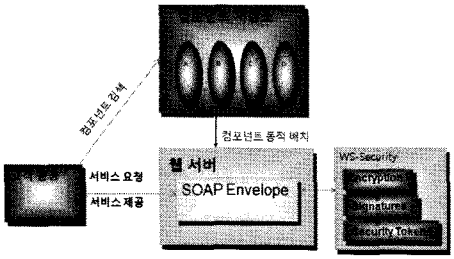
〈그림 2〉의 각 구성요소의 기능은 다음과 같다.

송신자 시스템는 이기종의 컴포넌트들을 제공하는 것으로 컴포넌트 개발자 등이 컴포넌트를 수시로 업로드시키게 된다. 해당 송신자 시스템은 컴포넌트를 위한 웹 서비스를 만들고, 레지스트리에서 웹 서비스를 기록한다. 수신자 시스템은 고객이 요청에 맞는 컴포넌트 탐색을 위해 웹 서비스에 접근하며, 고객 응용에 적합한 서비스를 요청한다. 이때, 서비스를 위한 WSDL 파일은 수신자에게 반환되고 수신자는 WSDL로부터 웹 서비스의 위치를 읽어들이고 이에 대한 웹 서비스를 호출한다. 컴포넌트 저장소는 컴포넌트가 실제로 저장될 뿐만 아니라 컴포넌트의 속성이 저장된 DB를 갖는다. 그 외, UDDI Registry는 웹 서비스의 레지스트리로서, 서비스를 위한 WSDL은 UDDI에서 기록되고, 고객은 SOAP 프로토콜을 이용하여 레지스트리에 접근한다. 웹 서버는 웹 서비스를 수행하고 컴포넌트 저장소에 접근한다. WS-Security는 XML 암호화를 사용하여 메시지 기밀성을 제공하고, XML 서명으로 메시지 무결성과 보안 토큰을 제공해 안전한 웹 서비스의 보안 솔루션을 제공한다.

다시 말해, 고객 요청에서 고객 탐색 기준을 만족하는 컴포넌트 저장소를 탐색하고 동적으로 컴포넌트를 위한 웹 서비스를 생성하고, 이 때, XML 암호화와 서명, 보안 토큰을 사용하여 안전한 웹 서비스를 제공한다.

## 4. WS-Security가 포함된 웹 서비스

WS-Security를 이용하여 서명과 암호화를 수행하는 일반적인 SOAP의 형태를 나타내고 있다. 여러 형태의 보안 토큰이 보안 헤더에 블록 안에 존재할 수 있고, 전송하려는 대칭키와 같은 보안 토큰은 암호화할 수 있다. 디지털 서명은 보안 헤더 블록 내에 있지만 SOAP 내의 어느 부분에서라도 참조하게 된다. 〈그림 3〉은 WS-Security가 포함된 웹 서비스 생성 과정을 나타낸 것이다.




〈그림 3〉 WS-Security가 포함된 웹 서비스 생성

〈그림 3〉에서 보안 요소를 고려한 웹 서비스 생성 과정을 단계별로 나타내면 다음과 같다.

1단계: 보안 토큰을 생성한다.
2단계: 웹 서비스 프록시의 인스턴스를 생성한다.
3단계: 요청 컨텍스트에 토큰을 추가한다.
4단계: 서명 개체를 이용하여 메시지에 서명한다.
5단계: 서명 개체를 사용하여 메시지를 암호화한다.
6단계: 웹 서비스 요청자의 디지털 인증을 허가한다.
7단계: 웹 서비스를 호출한다.
8단계: 컴포넌트 저장소를 검색한다.
9단계: 해당 컴포넌트를 웹 서비스로 변환한다.

위 단계에 의해 지원되는 웹 서비스 보안 기술 지원 범위를 로 나타내면 다음과 같다.

〈표 3〉 보안 기술 지원 범위

| 보안기술 | XML Encryption | XML Signature | WS-Security |
|---|---|---|---|
| 기밀성 | O | | O |
| 무결성 | | O | O |
| 인증 | | | O |
| 부인방지 | | O | O |

〈표 3〉의 각 보안 기술은 각 위험 요소에 대한 방안으로 적용되고 있다. 기밀성은 메시지 도청, 무결성은 메시지 변조, 인증은 메시지 위조, 그리고, 부인방지는 메시지 송신 및 부인 방지를 지원한다. WS-Security는 이들 보안 기술을 지원 가능하다.

## V. 결론

본 연구는 메시지 보안 요소를 고려한 웹 서비스로 이질적인 컴포넌트들을 탐색하여 동적으로 웹 서비스를 제공하는 것이다. 현재까지 개발된 기존 연구가 컴포넌트로부터 웹 서비스를 동적으로 생성하는 연구에 초점을 맞춘데 비해, 본 연구는 WS-Security 표준에 따라 XML 서명, 암호 인증 등을 통해 기밀성과 무결성을 보장하여, 안전한 웹 서비스를 제공하는 시스템을 설계하였다. 이는 안전한 웹 서비스 제공과 컴포넌트 재사용성 향상 측면에서 의의가 있다. 앞으로 본 연구는 웹 서비스의 보안 표준을 반영한 시스템 개발을 목표로 하며, 각 보안 요소가 적용된 시스템들의 정량적인 평가를 해야 할 것이다. 이를 위해, 관련 연구들 간의 성능평가를 위한 항목 추출 및 평가도구 개발 등의 꾸준한 연구가 필요하다.

## 참고문헌


[1] 김주한 외 7인, "웹 서비스 보안 기술의 표준화 및 시장동향", 전자통신동향분석, 제20권 제1호, 2005년 2월.

[2] 한국전산원, " e-비지니스를 위한 웹 서비스 메시징 보안 방안 연구", 2004년 12월.

[3] Marc Clasnliau, Web Services Security, Oracle, Oct 2006.

[4] 강장묵, "시맨틱 웹과 웹 서비스 보안에 관한 소고(온톨로지를 중심으로", e-비지니스 연구, 제8권 제2호, 2007년 6월.

[5] Roger Lee, Ashok hariknumar, Chia-chu Chiang, Hae-Sool Yang, Haeng-Kon Kim, Byeongdo Kang, "A Framework for Dynamiccally Converting Components to Web Services", Proceedings 3rd ACIS International Conference on Software Engineering Research, Management & Application(SERA2005), Aug 2005, pp.431~437.

[6] 하 얀, "CBD에 의한 온톨로지 기반 시맨틱 웹 서비스 생성", 정보처리학회 논문지 D, 제 14권-D권 제4호, 2007년 6월.

[7] 문기영 외 4인, "안전한 XML 기반 웹서비스를 위한 웹 애플리케이션 보안 프레임워크", 정보보호학회지, 제13권 제5호, 2003년 12월.

[8] Don Smith, "Web Services Enhancements 2.0에서의 WS-Security 연습", 2003.8. http://tong.nate.com/astonisha/31627727

[9] 조광문, "전자상거래에서 안전한 정보교환을 위한 웹 서비스 기반의 XML 보안 모델," 한국 컴퓨터 교육학회 논문지, 제7권 제5호, 2004년 9월.