전자문서 표준 컨테이너(DDC)의 권한 관리 방안에 대한 연구

국상진*, 허승호*, 장혜란*, 원준열*, 원동호**
*(주)한국무역정보통신
**성균관대학교 정보통신공학부
e-mail : twister@ktnet.com

Research on the privilege management of Digital Document Container

Sangjin Kook*, Seung ho Huh*,
Hyeran Jang*, Jun yol Won*, Dong-Ho Won**
*IT-Reaserch, Korea Trade Network
**School of Information and Communication Eng.,
Sungkyunkwan University

요 약

전자문서보관소와 같이 대규모의 전자문서가 저장되는 시스템은 어떤 특정한 방법을 기준으로 해당 데이터를 저장한다. 이는 데이터의 저장, 검색, 송수신, 보안 요소 등 여러 가지 요구사항에서 기인하며, 이를 근거로 설계 되어야 한다. 본고에서는 현재 이슈가 되고 있는 전자문서보관소의 적합한 데이터 저장 방법에 대하여 알아보고 이를 안전하게 관리하기 위한 방법을 접근제어 측면에서 생각하여 보기로 한다.

1. 서론

최근 정부의 주도로 전자문서 보관소의 구축 움직임이 활발히 이루어지고 있다. 이는 종이문서에 대한 불편함과 이로 기인하는 물적, 인적 자원 낭비 등을 줄여 보자는 강한 의지이다. 종이문서를 전자문서로 바꾸어 활용하는 일은 우리 생활을 더욱 편리하게 만들 것이며, 이를 위한 선행 과제로 전자문서를 어떻게 잘 보관하고 사용할 것인가에 대하여 생각해 보아야 할 것이다. 본고 에서는 전자문서를 보관하고 있는 전자문서 보관소의 데이터 저장 방안과 이를 안전하고 쉽게 이용할 수 있도록 하는 권한 부여에 대하여 고려사항 및 방안을 제안한다.

2. DDC

2.1 DDC

DDC(Digital Data Container)[1]는 디지털 데이터를 저장하기 위한 디지털 컨테이너로 전자문서 보관소(TDA, Trust Document Authority)와 같은 디지털 데이터의 보관을 목적으로 하는 곳에서 에서 사용 가능하도록 설계 되었다.

2.2 DDC의 유용성

DDC는 TDA가 디지털 문서를 효율적으로 그리고 안전하게 보관하고, 관리하고, 분배할 수 있도록 도와준다. DDC는 다음과 같은 요구사항을 가지고 있으며, 이는 TDA가 가져야 할 가장 중요한 요소이다.

- 전자문서의 효율적으로 관리
- 높은 수준의 보안 제공
- 전자문서의 장기보존
- 기술 중립성
- 검색 가능성
- 전자문서의 접근 통제

2.3 DDC의 보안 요소

DDC가 요구하는 보안 요소는 <표 1>과 같다. 일반적인 전자 문서나 디지털 데이터의 요구사항과 다르지 않다.

<표 1> DDC의 보안 기술 요소

요 구 사 항		관 련 기 술
무결성		HASH, MAC
프라이버시	기밀성	암호화
	원본성	전자 서명
증명		X.509 Certificate
인가		역할 기반 접근 통제
감사		로그 기록
부인방지		증명, 전자 서명
검증		X.509 Certificate

2.4 DDC의 사례

DDC에 대한 개념은 다음과 같은 프로젝트 또는 완성품으로 제안 되어 왔다.

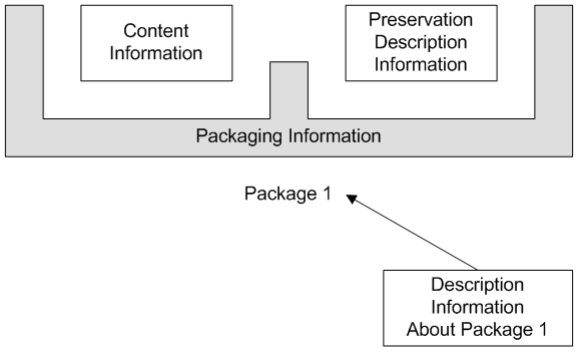
2.4.1 OAIS(Open Archival Information System)

OAIS[2][3]는 ISO의 요청으로 국제 협력체인 CCSDS(Consultative Committee for Space Data System)에서 개발 하였다. 이는 미국의 NASA, 일본의 NASDA, 러시아의 RSA등이 주체가 되었다.

OAIS의 목적은 정보를 보관하는 책임을 수행하는 기록 보존 모델의 연구이며, 주로 데이터의 장기 보관 기술 및 프로세스의 개발 등에 있다.

OAIS의 모델 중 DDC와 비슷한 개념은 정보 묶음(Information Package)으로 나타난다.

· OAIS의 Information Package



(그림 1) Information Package의 개념과 관계

- 패키지(컨테이너) = CI + PDI + PI
- Content Information (CI) : 정보의 집합
- Preservation Description Information (PDI) : CI를 보존하는데 필요한 정보, 4가지로 구성
- Packaging Information (PI) : CI와 PDI를 캡슐화하고 구별할 수 있도록 보여줌, CI와 PDI를 제한, 묶음

· PDI에 대한 요구사항

OAIS는 CI를 보존하는데 필요한 PDI 4가지 정보를 다음과 같이 정의 하였다.

- Provenance Information(출처 정보) : 출처, 보관, 알고리즘, 이력
- Context Information(관계 정보) : 환경에 대하여 갖는 관계
- Reference Information(식별 정보) : 식별정보를 제공 (URLs, handles, service IDs)
- Fixity Information(고정정보) : 수정하지 못하는 정보 (checksums)

2.4.2 PKCS#7

RSA Security에서 개발한 PKCS 문서는 현재 가장 널리 사용되고 있는 보안 표준 문서 중의 하나이다. 현재 PKCS#7은 IETF의 SMIME 워킹그룹에서 CMS(Cryptographic Message Syntax)라는 이름으로 계승 되고 있다. 가장 빈번하게 사용되는 표준 중의 하나인 PKCS#7은 보안 메시지 구문에 대하여 기술하고 있다.

PKCS#7은 다음과 같은 형식을 정의 하고 있으며, 원하는 보안 요소에 따라서 각각의 Content 타입을 사용한다.

<표 2> CMS의 데이터 타입

Content Type
1. Data
2. Signed-data
3. Enveloped-data
4. Digested-data
5. Encrypted-data
6. Authenticated-data

PKCS#7은 다양한 속성 값을 적용하는 데에는 문제점이 있으나, 간단한 시간 값과 같은 속성들은 적용 가능하다.

3. 접근 통제 방안

TDA와 같은 서비스 시스템을 구축하여 운영한다면, 저장된 데이터에 대한 접근 통제 방안은 크게 두 가지 방식에서 접근 가능하다. 이는 전체의 시스템 관점에서 접근 통제 관리를 수행하는 방법과, 각각의 데이터 관점에서의 접근 통제 관리를 수행하는 방법에 해당한다.

3.1 접근 통제 메커니즘

일반적으로 흔히 언급 되고 있는 시스템 접근 통제 기술로는 MAC(Mandatory Access Control-강제적 접근 제어), DAC(Discretionary Access Control-임의적 접근 제어), RBAC(Role-based Access Control-역할 기반 접근 제어) 방식이 존재 한다.

시스템 관점에서의 접근 통제는 보다 일관된 접근 통제를 수행 가능하다는 장점이 있다.

3.2 PMI

데이터 관점의 접근 통제에는 PMI(Privilege Mangement Infrastructure)라는 기술이 적용 가능하다. PMI는 PKI(공개키 기반구조)를 이용하여 보다 안전하고 명확한 권한 부여가 가능한 장점을 가지고 있다. PMI는 ITU-T의 X.509 문서에서 표준화를 진행 중에 있으며, IETF의 PKIX 워킹그룹에서 RFC 3281[4]으로 표준화를 이루었다.

4. 권한 정보 적용 방안

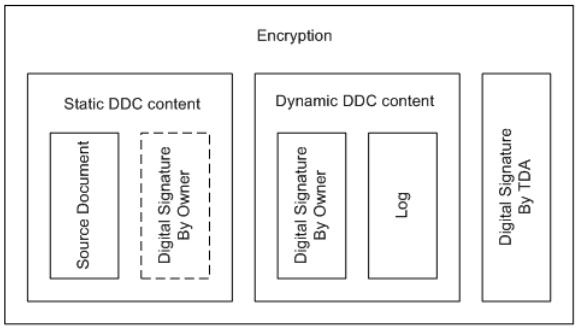
4.1 일반적 TDA의 권한 관리 방안

효과적인 권한관리 방안에 가장 먼저 필요한 것은 보안 정책의 수립이다. TDA는 다루어지는 모든 문서에 대하여 권한을 부여하는 정책을 성립하고 이를 운영하는 독립된 시스템을 구축한다.

DDC와 같은 컨텐트 기반의 권한 관리를 위하여 TDA는 보다 복잡한 정책, 표준, 가이드라인 및 프로시저를 준용 한다.

4.2 DDC의 권한 정보 적용 시 고려 사항

DDC의 주요 구성 요소는 다음과 같다.



(그림 2) DDC의 구조

- Static DDC : 일반적으로 빈번하지 않게 그리고 수동으로 업데이트 되는 데이터에 해당 한다. static DDC 내용은 컨테이너 데이터와 보호된 소스 전자문서를 포함 한다.

- Dynamic DDC : 지속적으로, 자동적으로 전자문서보관소에 의해 업데이트 되는 데이터에 해당 한다. 다이내믹 DDC 내용은 전자서명과 로그를 포함 한다.

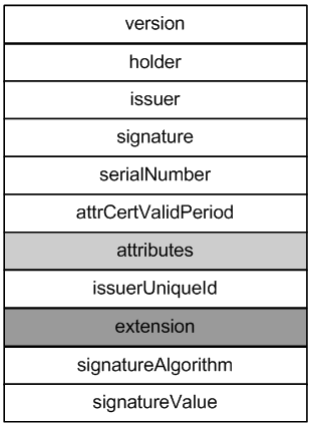
<표 3> 이용 가능한 신원 정보

정 보	내 용
Identifier	DDC의 이름
creater	문서 생성자
publisher	DDC 생성 TDA 이름
type	DDC의 종류
rights	DDC의 권리
...	...

권한 부여를 위하여 이용 가능한 DDC 정보는 주로 신원 정보이다. 이용 가능한 신원 정보는 <표 3>과 같다.

4.3 AC의 생성

RFC 3281의 속성인증서는 (그림 3)과 같은 구조를 갖는다. 이때 DDC와의 연동을 위하여 속성인증서(AC, Attribute Certificate)의 속성을 이용한다.



(그림 3) AC의 구조

<표 5> AC의 주요 attribute structure (RFC3281)

```
IetfAttrSyntax ::= SEQUENCE {
   policyAuthority [0] GeneralNames
                          OPTIONAL,
   values      SEQUENCE OF CHOICE {
       octets  OCTET   STRING,
       oid     OBJECT  IDENTIFIER,
       string  UTF8String }    }
SvceAuthInfo ::=    SEQUENCE {
       service   GeneralName,
       ident     GeneralName,
       authInfo OCTET STRING OPTIONAL}
```

AC의 Attribute은 DDC에 적합하도록 설계되어야 하며, PKC 및 DDC와의 강력한 연결이 필요하다. <표 5>는 RFC3281에 기술되어 있는 주요 속성 메시지 구조이다.

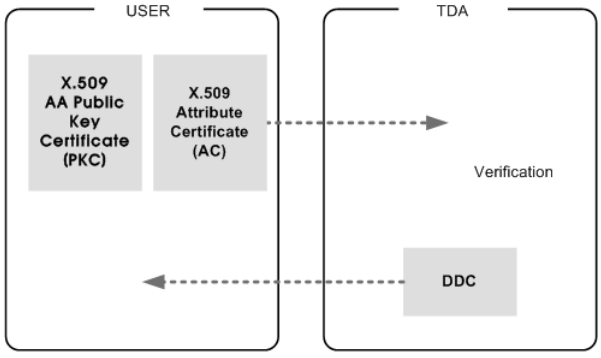
DDC에 사용할 수 있는 속성은 다음의 <표 6>에 나타내었다. DDC는 안전한 보관, 송수신, 증명을 위하여 TDA만이 만들기 때문에 AC의 Attribute에 생성한 TDA의 이름, 정확한 속성 정책, 대상 DDC의 포인터, 그리고 속성 값을 포함한다. DDC에 대한 포인터는 DDC의 생성 정책에 맞추어 적용 한다.

<표 6> DDC용 Attribute

```
DDCAttributeSyntax ::= SEQUENCE {
   TDA     [0] GeneralNames OPTIONAL,
   attributeIdentifier OBJECT IDENTIFIER,
   targetDDC   OCTET   STRING,
   values  SEQUENCE OF CHOICE {
       octets OCTET   STRING,
       oid    OBJECT  IDENTIFIER,
       string UTF8String     }      }
```

4.4 적용 프로세스

- 사용자는 TDA의 권한 관리 시스템으로부터 문서 접근 권한에 대한 AC를 발급 받는다.
- 사용자는 TDA로부터 원하는 Data를 얻기 위하여 문서 요청을 한다.
- TDA는 사용자의 요청에 대하여 권한 정보를 가진 AC와 유효성 확인을 위한 검증을 수행한다.
- 요청에 대한 DDC를 사용자에게 전달한다. 이때 사용자가 가진 속성에 따라서 DDC를 생성하거나, 기존의 DDC를 검색하여 전달한다.



(그림 4) PKC, AC검증 및 DDC 전달

4.5 주요 고려 사항

AC가 가지고 있는 속성은 특정한 DDC에 해당하는 정보를 가지고 있다. AA는 적절히 AC를 발급하고 있는지 다른 DDC의 접근 권한까지 부여하는지에 대하여 항상 관리 감독하여야 한다.

문서의 가치에 따라서 특정 DDC 하나만을 지정하는 방식을 사용하는 것이 보안 측면에서 유리하나, 일반적인 접근제어 방식과 동시에 사용하는 것이 비용 측면에서 유리하다.

TDA는 AA와 DDC 생성 및 서비스 검증 주체간의 적절한 정책과 표준 및 프로세스를 설정하여 운영 하여야 한다.

5. 결론

본고에서는 전자문서보관소에서 사용가능한 DDC에 대하여 알아보고, DDC를 사용하기 위하여 필요한 권한 관리 방안과, 이를 적용하기 위한 방안에 대하여 논 하였다. 이와 같은 방법이 적용 된다면 정책적인 면과 기술적 측면의 적절한 조화가 필요하게 되며, 이는 안전한 문서보관의 시작이 될 수 있을 것이다.

대부분의 기업과 기관들이 장기적인 문서 보관[5]에 어려움을 겪고 있다. 또한, 이러한 회사들의 대부분이 자신의 문서를 제3의 보관 장소에 보관하는 것도 꺼리고 있다. 이는 보안상의 위험이 여전히 존재하기 때문이며, 이러한 위험을 줄이는 것이 전자문서 보관소의 목표이기도 하다. 권한 관리와 같은 적절한 보안 기술의 사용이 안전한 전자문서의 보관 방안에 가장 중요한 요소가 될 것이다.

참고문헌

[1] KTNET-CMU electronic commerce practicum team, "Digital Document Container (DDC) Technical Design", 2005

[2] CCSDS, "Reference Model for an Open Archival Information System(OAIS)", http://www.ccsds.org/, 2002

[3] 이소연, "디지털 아카이빙의 표준화와 OAIS 참조모형", 정보관리연구학회지, Vol 33, P44-68, 2002

[4] S. Farrell, R. Housley "An Internet Attribute Certificate Profile for Authorization", RFC 3281, April 2002.

[5] 한국정보보호진흥원, "전자서명장기검증기술 개발", 2004. 12