情 報 保 護 學 會 誌
第 12 券 第 5 號, 2002. 10

통합 어플리케이션 정보보호 기반구조

최 대 선*, 진 승 헌*, 정 교 일*

요 약

어플리케이션이나 서비스에서 요구하는 인증, 인가, 감사, 암호화 등의 어플리케이션 정보보호 분야의 현재와 미래의 요구사항을 분석하고 이러한 요구사항에 대응하는 솔루션으로 ETRI에서 개발 중인 통합 어플리케이션 정보보호 기반구조를 소개한다. 어플리케이션 환경을 현재의 현황과 앞으로의 추세를 고려하여 인터넷 서비스 환경, 어플리케이션 통합으로 나누어 분석하여 현재 정보보호의 문제점과 이에 따라 새롭게 요구되는 정보보호서비스를 도출한다. 또한 다양한 정보보호 서비스들의 통합관리의 필요성과 이에 따른 요구사항을 분석한다. 새로운 정보보호 서비스의 제공과 기존 정보보호 솔루션의 통합 및 연동, 관리 요구 사항을 만족시키기 위한 기반구조인 통합 어플리케이션 정보보호 기반구조의 개념과 구조를 소개한다.

I. 서 론

컴퓨터와 인터넷이 급속히 보급되어 모든 분야에 활용됨에 따라 다양한 기능과 형태를 갖는 어플리케이션들이 등장하고 있다. 새로운 형태와 비즈니스 모델을 갖는 닷컴들이 지속적으로 등장하여 불특정 다수의 인터넷 이용자들에게 서비스를 제공한다. 기업의 컴퓨팅 환경에는 이미 수많은 어플리케이션들이 존재하고 있지만 생산성 향상과 비용절감을 가능하게 한다는 기치로 지속적으로 새로운 개념의 어플리케이션들이 등장, 보급되고 있고 이들은 새로운 서비스를 기업 구성원과 관련된 타 기업 및 개인에게 제공한다. 또한 개인들도 개인 홈페이지나 P2P 방식으로 개별적인 서비스를 제공하고 있다. 이러한 어플리케이션들은 정보를 교환하고 상호 서비스를 이용하기 위해 서로 연결되는 추세이다. 이에 따라 사용자가 접근할 수 있는 서비스의 종류는 증가하고 있고 서비스 제공자들은 다양한 접근경로를 갖는 다양한 이용자들을 갖게 된다.

정보보호 분야를 기반구조 정보보호와 어플리케이션 정보보호로 나눌 수 있다. 기반구조 정보보호는 네트워크와 컴퓨터 가용성 유지와 같은 기반구조 자체의 보호와 암호화 채널 형성, 침입차단 등 기반구조 자체에서 제공하는 정보보호를 의미한다. 반면 어플리케이션 정보보호는 서비스 단위로 이루어지는 서비스 이용에 관련된 제어와 서비스에서 요구하는 과금, 감사기록, 암호화, 전자서명 등을 의미한다.

어플리케이션 정보보호는 실제 어플리케이션 구성 환경과 구조 및 서비스 내용에 따라 요구되는 세부사항은 매우 다양하다. 이에 따라 어플리케이션이 요구하는 다양한 정보보호 기술과 솔루션이 개발되었고 현재도 개발되고 있지만 새로이 등장하는 다양한 환경에서의 요구사항에 신속히 대응하지 못하는 상황이다. 새로 등장하는 정보보호 솔루션이나 서비스의 개수도 점점 증가하게 되어 이들의 관리가 복잡한 문제로 대두되고 있다. 또한 다양한 환경의 어플리케이션들이 서로 연동되면서 이들의 정보보호 솔루션이나 서비스들의 연동 또는 통합도 복잡한 문제로 대두되고 있다. 따라서 다양한 요구 사항에 대응하는 정보보호 서비스를 제공하면서 정보보호 서비스들의 연동과 관리를 지원해주는 포괄적인 솔루션이 필요하다.

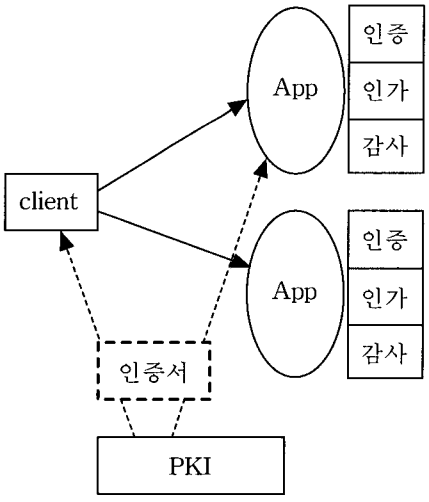
본 논문에서는 현재와 미래에 나타날 다양한 환경하에서 어플리케이션의 정보보호 요구사항을 분석하고 이에 대응하는 포괄적인 솔루션으로 ETRI에서 개발 중인 통합 어플리케이션 정보보호 기반구조를 설명한다. 본 논문은 다음과 같이 구성되어 있다. II장에서는 다양한 어플리케이션 환경에서 발생하는

* 한국전자통신연구원 정보보호연구본부 정보보호기반연구부 ({sunchoi, jinsh, kyoil}@etri.re.kr)

정보보호 요구사항과 이에 대응하기 위해 필요한 솔루션에 대해 기술한다. 기존 솔루션과 기술들 중, 이에 대응하는 것들을 살펴보고 부족한 점을 파악한다. III장에서는 II장에서 살펴본 문제점들을 해결하는 솔루션으로서 ETRI에서 개발 중인 통합 어플리케이션 정보보호 기반 구조를 소개하고, IV장에서 결론을 맺는다.

II. 어플리케이션 환경과 정보보호 요구 사항

그림 1은 현재의 어플리케이션 정보보호 구조를 보여준다. 어플리케이션들은 개별적인 정보보호 요구사항을 갖고 이를 만족시키기 위한 인증, 인가, 감사 등 정보보호 기능을 추가적으로 갖추고 있다. 여기에 PKI와 같은 TTP(Trusted Third Party)가 제공하는 인증서를 이용하고 있지만 TTP는 인증서의 발급과 관리만을 담당할 뿐 실제 인증서를 사용해 인증 등을 수행하는 것은 어플리케이션이다.



〔그림 1〕 현재의 어플리케이션 정보보호 구조

1. 다양한 어플리케이션의 출현

1.1 환경분석

개인 사용자는 인터넷 상에서 수많은 서비스를 이용하고 소속 조직에서도 다양한 어플리케이션들을 이용하고 있다. 사용자가 서비스를 이용하기 위해서는 서비스에 사용자 등록을 하고 자신의 신상정보(profile)를 입력하여 한다. 또한 서비스에 자신을 식별하기 위한 식별자(identifier)를 부여받고 개별적인 인증을 위해 패스워드를 기억해야 한다. 서비스 개수가 늘어남에 따라 사용자가 이러한 정보를 모두 관리하는 것이 점차 불편하고 복잡한 일이 되고 있다. 또한 패스워드 이외의 인증 방법이 사용된 경우, 서비스마다 다른 인증 메커니즘을 클라이언트에 모두 갖고 있어야 한다. 신상정보가 변경되었을 경우, 이를 일일이 갱신하는 것도 매우 어려운 일이 된다. 또한 프라이버시를 위해 자신의 신원을 노출시키지 않고 자신의 어떠한 신상정보(예, 성인 여부)를 입증할 필요성도 있다. 이렇게 자신의 식별자와 신상정보들이 자신의 아이덴터티(identity)를 구성하며 이것을 관리하는 것이 ID 관리(Identity Management)이다. 현재의 어플리케이션 정보보호 구조에서는 ID 관리가 사용자의 수작업에 의존하고 있어 식별자의 분실, 개인 정보의 불일치, 프라이버시의 침해 등의 문제를 일으키는 요인이 되고 있다.

서비스 제공자 입장에서는 사용자 정보의 관리와 인증, 그리고 서비스 요금의 지불 등의 문제가 관리 부담이 될 수도 있다. 물론 가입자 목록 자체가 자산이 되는 경우도 있지만 사용자 정보를 일일이 관리하고 인증, 인가 등의 정보보호 기능과 이용에 따른 과금 기능을 추가하는 것은 어플리케이션 개발에 부가적인 부담이 될 수 있다. 또한 서비스 제공자가 사용자 정보의 확인을 요구하는 경우(예: 실명 확인) 서비스제공자가 이를 직접 수행하는 것은 매우 큰 부담이 된다. 또한 서비스를 위해 제3자가 관리하는 사용자의 속성 정보(예: 신용도)가 필요한 경우도 있다. 제3자가 관리하는 속성 정보를 획득하기 위해서 여러 제공자와 개별적으로 관계를 설정해야 한다. 대규모 사업자는 이러한 과정을 직접 수행할 수 있지만 대다수의 중소규모의 서비스 제공자는 이를 직접 수행하기 어려운 실정이다. 따라서 이들은 안전한 서비스를 위한 정보보호 기능을 충분히 갖추지 못하고 있는 실정이다.

1.2 통합 인증 및 ID 관리 솔루션

이러한 문제점을 해결하는 방법으로 각 어플리케이션에서 수행되던 인증 및 ID관리를 통합하여 대행하는 별도의 서비스를 두는 방법이 있다. 통합 관리 서비스에서 사용자 신상 정보를 관리하고 이를 서비스 제공자에게 제공한다. 또한 사용자 인증을 수행하고 제3자가 제공하는 사용자의 속성 정보도 관리, 제공하게 된다.

인증 및 ID관리를 통합하여 제공하면 사용자는 한 곳에서 신상정보 입력과 관리를 수행할 수 있다. 또한 통합관리서비스에서의 단일 인증으로 모든 서비스를 이용할 수 있으며 인증을 위한 하나의 식별자와 패스워드를 기억하면 된다. 또한 ID관리자가 속성에 대한 증명을 제공함에 따라 신원 노출없는 속성 증명도 가능하다.

서비스 제공자 입장에서는 사용자 관리와 과금, 인증 등을 아웃소싱하므로서 자체적인 구축 및 관리 부담을 덜고 서비스 자체에만 집중할 수 있다. 또한 직접 수행하기 어려운 많은 정보보호 기능들을 이용하여 보다 안전한 서비스를 제공할 수 있다.

이러한 통합 인증 및 ID관리 서비스가 갖추어야 할 기능은 다음과 같다.

- ID(Identifier, profile) 관리
  - 식별자와 신상정보의 관리 및 배포
- 단일 인증(Single Sign On)
- Privacy 보호
  - 신상정보에 대한 접근제어
  - pseudonym/anonym제공
- 제 3자 제공 속성 관리, 제공
- 통합 과금
  - 서비스 제공자에 과금 대행
  - 사용자에게는 통합 과금
- 타 통합 인증 및 ID관리 서비스와의 연합

1.3 관련 기술

통합 인증 및 ID 관리 분야는 최근 크게 이슈화되고 있는 분야이다. Microsoft의 Passport 서비스는 현재 시행되고 있는 통합 인증 및 ID 관리 서비스로 전세계적으로 1억 6천만명의 사용자를 보유하고 있다.[1] 그러나 프라이버시 보호를 위한 pseudonym 또는 anonym 제공 기능과 제3자 제공 속성관리 및 제공 기능이 미흡하다. 가장 중요한 문제는 타 서비스와의 연합을 고려하지 않고 있다. 즉 전세계의 모든 사용자가 Microsoft의 서비스를 거쳐서 전세계 인터넷 서비스를 이용하도록 되어 있는 것이다.

Sun의 Liberty는 통합 인증 및 ID관리를 별도의 서비스가 아닌 기존 인증 및 ID관리 모듈의 연동을 통해 해결하는 방법을 제시하였다.[2] 실제 서비스를 제공하지 않아 서비스 제공자의 부담을 더는 효과는 없으며 통합 과금, 속성 관리/제공 등 별도의 서비스를 필요로 하는 기능을 제공하지 못한다.

2. 어플리케이션 통합 추세

2.1 환경 분석

최근 기업 어플리케이션 발전 동향의 핵심은 통합이다. EAI(Enterprise Application Integration)는 기업 내의 어플리케이션 들의 GUI, 데이터, 프로세스 통합을 통해 관리 비용의 절감 및 비즈니스 프로세스의 자동화를 통한 생산성 향상을 이루려는 개념이다. B2Bi(Business to Business integration)는 기업 간의 어플리케이션 통합으로 구매, 판매, 생산 등에서 관련 기업의 어플리케이션과 연동을 통해 비즈니스 프로세스의 자동화된 통합을 이루어 비용 절감을 달성하려는 시도이다. 이러한 어플리케이션 통합에 따라 기존 정보보호 구조에서는 여러 가지 문제가 발생하고 있다.

조직 내의 다양한 어플리케이션 들의 개별적인 정보보호 기능을 통합하여 관리 비용을 줄이고 조직의 일관된 정보보호 정책을 적용하여 취약요소를 줄이려는 시도는 EAM(Enterprise access management)이라는 개념으로 이미 보급되고 있다. EAI와 같은 어플리케이션 통합을 통해 이러한 조직 내 정보보호 통합의 필요성은 더욱 절실해 진다. 단일 GUI를 사용해 여러 가지 어플리케이션을 사용하면서 개별적으로 ID관리와 인증을 수행하는 것은 문제가 있으므로 통합 인증과 ID관리가 요구된다. 또한 데이터가 통합됨에 따라 어플리케이션 별로 권한 관리가 수행되던 것을 통합하여 수행할 필요가 생긴다. 이러한 통합 권한 관리를 위해서 사용자별로 수행하던 권한 할당 및 관리의 부담을 줄여주는 role이나 group을 이용한 권한관리 기법의 필요성이 더욱 높아지게 되었다.

조직 간의 연동이 되면서 타 조직의 자원 및 서비스에 대한 접근이 필요하게 된다. 이러한 연동을 위해 사용자가 연동하는 모든 조직에 사용자 등록을 하는 것과 관리자가 연동하는 모든 조직의 사용자들을 관리하는 것은 매우 복잡한 일이 된다. 따라서 한 조직의 인증, 인가가 타 조직과 연동되는 것이 필요하다. 신뢰하는 조직을 관리하여 신뢰하는 조직에서 수행한 인증/인가를 인정하는 것이다.

어플리케이션 통합 중에는 프로세스 간의 연동이 있다. 사용자가 어떤 서비스를 요청하면 그 서비스는 서비스 제공을 위해 타 프로세스 서비스를 이용하는 것이다. 서비스의 요청자가 사용자 뿐 아니라 다른 서비스일 수 있는 것이다. 이러한 프로세스 간

의 연동은 새로운 형태의 정보보호 요구 사항을 발생시킨다. 자동화된 연동을 위해서는 우선 단일 인증이 필수적이다. 또한 연동되는 프로세스 간의 권한 관리가 연동되어야 한다. 프로세스 실행 중에 발생되는 정보를 토대로 타 프로세스에 대한 실행 권한을 프로세스가 부여하는 기능도 필요하다. 또한 프로세스의 실행 경로에 따라 달라 질 수 있는 권한 관리가 필요하다. 또한 권한 위임도 필수 적이다. 프로세스가 타 프로세스의 서비스를 호출하는 경우에 처음 자신을 호출한 사용자의 권한을 위임받아야 하는 경우가 있다. 따라서 권한위임에 대한 지원이 필요하다.

2.2 인증, 인가, 감사 통합 및 연동 지원 솔루션

기업 내부 또는 기업간 어플리케이션 통합에 따라 발생하는 여러 가지 요구사항을 만족시키기 위해서는 인증, 인가, 감사를 통합하거나 이들 간의 연동을 지원하는 새로운 솔루션이 필요하다.

이러한 솔루션은 관련 어플리케이션들 또는 관련 조직들간의 중재자적인 지원 역할을 수행하게 된다. 이러한 솔루션이 가져야 하는 기능은 다음과 같다.

- 조직 내 단일 인증
- 조직 내 통합 권한 관리
  - RBAC(Role Based Access Control)
  - Group 기반 권한관리
- 조직 내 통합 감사관리
- 조직 간 인증, 인가의 연동 지원
  - 인증, 인가 정보의 표준화
  - 메커니즘 연동
  - 정책 조율
  - 속성 매핑
  - 메시지 전달
  - Credential 매핑
- 새로운 인증, 인가 기능
  - 위임관리
  - context관리

2.3 관련 기술

2.1 절에서 언급한 바와 같이 조직 내 어플리케이션 정보보호 기능 통합을 주장하는 EAM 개념이 있고 최근 EAM제품들이 많이 출시되고 있다. 대부분의 EAM 제품들은 조직 내부의 단일 인증과 권한 관리 통합 기능을 갖고 있다.[3] 그러나 EAI에서 구현되는 프로세스 통합은 고려하고 있지 않다.

또한 조직 간의 인증, 인가 연동을 위해 인증, 인가 정보를 전달하는 규격으로 SAML이 표준화되어 있다.[4] 그러나 이는 전달 메시지의 표준화일 뿐 조직 간의 연동을 위한 메커니즘 연동, 정책 조율, 속성 매핑에 관한 부분은 여전히 해결되지 못한 상태이다. 이러한 문제가 해결되지 못하면 동일 메커니즘, 정책, 속성을 사용하는 동일 도메인 내에 있는 조직간의 연동 만이 가능하게 되고 Cross 도메인 간의 연동은 불가능하다.

프로세스 연동에 따른 위임관리, context관리같은 문제는 여전히 연구 단계에 있다.[5, 6]

3. 다양한 정보보호 솔루션의 존재

3.1 환경 분석

다양한 종류의 서비스 만큼 다양한 정보보호 기능과 서비스가 존재하고 있다. 상호 연동되기도 하는 이러한 서비스들을 이용하기 위해서 사용자와 어플리케이션 등은 수많은 credential과 식별자, 신상정보를 관리해야 한다. 또한 수많은 정보보호 메커니즘을 구비하여야 한다. 인증에 사용되는 방식이 10가지이면 10가지 모두를 구비하여야 모든 서비스를 이용할 수 있다. 또한 이러한 정보보호 서비스들은 각기 다른 서비스 인터페이스를 갖는다. 이러한 환경은 사용자에게도 큰 부담이 되어 정보보호 서비스의 활성화를 방해하는 요인이 된다.

조직이나 어플리케이션의 정보보호관리 담당자 입장에서는 인증, 인가, 감사, 암호화 등의 다양한 종류의 정보보호 서비스를 관리해야 한다. 각 분야별로 여러 가지 메커니즘이 존재할 수도 있다. 또한 관리 대상도 다양해서 수많은 사용자, 운영자, 어플리케이션, 속성제공자 등을 관리해야 한다. 이러한 관리 대상에 따른 다양한 정책들이 존재하므로 정책 관리도 중요한 업무 중의 하나가 된다. 또한 연동을 위해서는 상충되는 정책의 조율이 필요하다.

3.2 통합 정보보호 서비스 관리

이러한 문제를 해결하기 위해 통합 정보보호 관리 솔루션이 필요하다. 기반구조 보호 분야에서는 이미 통합관제(Enterprise Security Management) 개념이 등장하여 보급되고 있다.[7]

어플리케이션 정보보호 분야에서의 통합관리솔루션은 단일 뷰(View)를 통해 모든 정보보호 서비스와 관련 정보를 관리할 수 있는 관리 도구를 제동해야 한다. 또한 단일 정책 프레임 워크로 모든 서비스 정책을 관리할 수 있어야 한다. 한편 사용자를 위해서는 단일화된 인터페이스로 모든 서비스를 이용할 수 있어야 한다. 또한 이러한 통합관리 솔루션은 기존에 구축된 정보보호 시스템을 포함할 수 있어야 한다.

3.3 관련 기술

앞서 언급한 EAM도 조직 내의 통합 정보보호 관리를 목적으로 하고 있다. 그러나 EAM은 자체의 솔루션으로 모든 정보보호 서비스를 다시 구축해야 한다. 즉 기존에 존재하는 정보보호 서비스를 통합하는 기능은 갖고 있지 않다. 이러한 기능을 갖고 있는 솔루션으로 EASI(Enterprise Application Security Integration)라는 개념이 있다.[8]

EASI는 기존의 정보보호 솔루션에 부가적인 인터페이스를 부착하여 통합 관리구조에 포함시키는 방식을 사용한다. 단일한 정책기반 관리 도구를 갖고 있으며 단일 서비스 제공 인터페이스를 갖고 있다. 그러나 EASI는 사용자를 위한 관리 도구나 관리 서비스를 제공하지 못하고 있다.

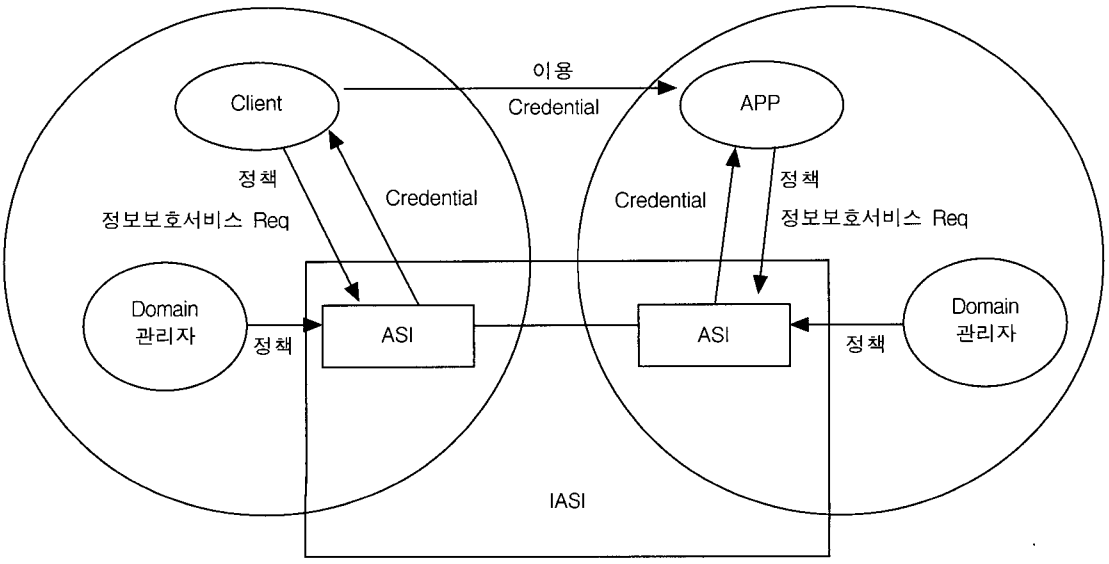
Ⅲ. 통합 어플리케이션 정보보호 기반구조

1. 기본 개념

1.1 기반 구조들의 통합

II장에서는 현재 또는 미래의 어플리케이션 환경과 이에 따라 요구되는 어플리케이션 정보보호 서비스들에 대해 살펴보았다. 이러한 어플리케이션 환경들은 점차 상호 경계가 모호해 지고 상호 간에 연동하고 통합되는 추세이다. 일반 인터넷 환경의 사용자가 EAI 환경의 조직 구성원이나 외부인이 될 수 있다. 닷컴 서비스 제공 어플리케이션 들간에 B2Bi를 통해 연동할 수 있다. 결국 모든 주체와 서비스들이 통합되고 연동되어감에 따라 정보보호 서비스도 모두 통합되고 연동되어야 심리스(seamless) 정보보호가 달성될 수 있다.

사용자나 관리자 입장에서는 단일한 기반구조를 통해 모든 정보보호 서비스를 제공받고 이를 관리하는 것이 바람직하다. 이를 위해 앞서 언급한 정보보호 서비스들이 유기적으로 통합되어 종합적인 서비스를 제공하는 것이 바람직하다. 또한 이러한 서비스들은 단일한 관리 프레임웍을 통해 관리되는 것이 바람직하다.



〔그림 2〕 IASI 기본 개념도

1.2 포괄적인 기반구조

통합 어플리케이션 정보보호 기반구조(IASI, Integrated Application Security Infrastructure)는 현재와 미래에 필요한 모든 종류의 어플리케이션 정보보호 서비스를 제공하는 포괄적인 기반 구조이다.

그림 2에 IASI의 기본 개념이 나타나 있다. IASI는 단일 도메인을 지원하는 ASI들이 모여서 구성된다. 서브넷들이 연결되어 구성되는 인터넷과 유사한 구조이다. 도메인에 속한 사용자, 어플리케이션, 관리자는 자신의 도메인 내부의 ASI를 신뢰하고 모든 어플리케이션 정보보호를 의존한다. ASI가 Domain 간의 신뢰와 통합/연동을 책임진다. 인터넷 사용자들은 서브넷을 이용한다고 생각하지 않고 인터넷을 단일한 기반구조로 보는 것처럼 ASI 이용자들도 하나의 기반구조를 이용한다고 생각한다. 자신의 도메인 내의 ASI를 신뢰하는 것은 서브넷의 게이트웨이를 설정하는 것과 마찬가지가 된다.

사용자, 어플리케이션, 도메인 관리자들은 각각 자신의 정책을 ASI에 통보한다. 사용자와 어플리케이션 들이 필요한 정보보호 서비스를 요청한다. ASI는 credential의 형태를 통해 정보보호 서비스 응답을 제공한다. Credential은 어떠한 종류의 주장(claim)을 담고 있는 정보단위로 인증서나 SAML assertion, kerberos ticket 등 어떤 형태나 될 수 있다.

2. 기본 구조

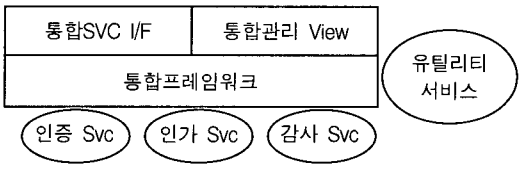
2.1 IASI 자체 요구사항

IASI는 모든 필요한 어플리케이션 정보보호 서비스를 제공, 단일 관리 및 서비스 이용 인터페이스 제공이외에 다음과 같은 자체 요구 사항을 만족 시켜야 한다.

- 기존에 존재하는 정보보호 솔루션 활용
  - 모든 것을 새롭게 만들 수는 없으며 기존에 존재하는 정보보호솔루션들이 최대한 재 사용될 수 있어야 한다.
- 새로 등장하게될 요구 사항을 위한 확장성
  - 새로 등장하게될 어플리케이션 환경과 여기서 발생하는 새로운 요구사항에 대응하기 위한 새로운 정보보호 서비스에 대한 확장성을 제공해야 한다.
- 정보보호 서비스를 위한 추가 비용의 최소화
  - IASI를 도입함에 따라 서비스 속도가 느려져서는 안된다. 또한 IASI 자체의 운영 비용과 많이 발생하면 안된다.

2.2 ASI 프레임워크

IASI 자체 요구사항을 만족시키기 위해서 ASI 프레임워크가 고안되었다. ASI 프레임워크는 기존의 정보보호 솔루션과 신규로 발생될 정보보호 솔루션들을 서비스 형태로 구성하여 이러한 서비스를 통합 서비스 인터페이스와 통합 관리 인터페이스로 이용 및 관리할 수 있도록 하는 프레임워크이다.



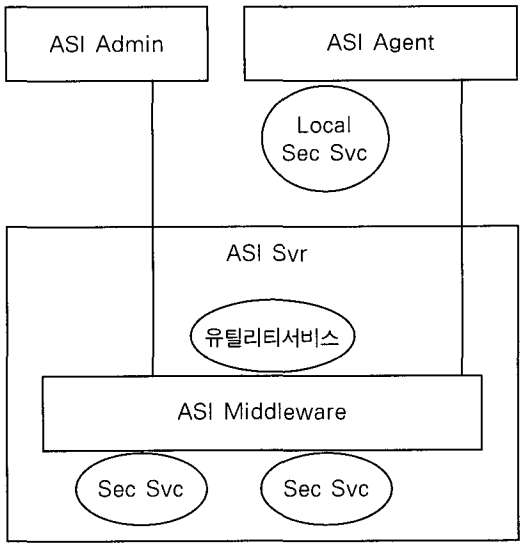
〔그림 3〕 ASI 프레임워크

그림 3에 ASI 프레임워크가 나타나 있다. 통합 프레임워크에 서비스들이 부착되어 있다. 이러한 서비스들에는 기존에 존재하는 정보보호솔루션에 어댑터를 부착한 형태도 있고 추가될 신규 정보보호 서비스를 위해서는 서비스 접속 인터페이스 규격이 마련된다. 통합 프레임워크는 통합 서비스 인터페이스를 통한 서비스의 호출과 통합 관리 인터페이스를 통해 제공되는 정책의 적용을 수행한다. 또한 서비스 간의 연동 및 타 도메인과의 연동도 제공한다. 유틸리티 서비스의 경우는 통합 프레임워크에 포함되지 못하는 서비스 간의 연동 지원 서비스이다.

2.2 IASI 구조

실제 환경에서 IASI는 ASI 단위로 시스템화 된다. 조직을 도메인으로 하고 조직 구성원에게 서비스를 제공하는 ASI 시스템이 있을 수 있고, 일반 인터넷 사용자에게 서비스를 제공하는 공공 ASI 시스템이 있을 수 있다. 이러한 ASI 시스템들이 모여 전체 IASI를 구성하게 된다.

그림 4는 단일 도메인 내에 ASI 시스템 구성을 보여 준다. ASI 서버는 실제 대부분의 ASI서비스를 제공하는 시스템이다.



〔그림 4〕 ASI 구성

ASI 서버는 ASI 프레임워크와 유틸리티 서비스 제공자 및 정보보호 서비스 제공자들을 탑재하고 있다. 부하 분산을 위해 유틸리티 서비스 제공자 및 정보보호 서비스 제공자들은 다른 서버에서 실행될 수도 있다. 이렇게 분산된 서비스들의 호출과 관리를 위해 ASI 프레임워크는 미들웨어의 형태로 구현된다.

ASI Admin은 통합관리 뷰를 제공하고 모든 관리 업무를 수행하는데 사용하는 관리도구이다. ASI Agent는 서비스 이용 인터페이스 역할을 수행한다. 이때 주목할 것은 로컬 정보보호 서비스이다. ASI 서버의 부하를 줄이고 수행시간 단축을 위해 로컬에서 수행될 수 있는 서비스를 ASI서버를 거치지 않고 로컬에서 ASI Agent가 호출하는 것이다. 이러한 로컬 서비스들도 ASI Agent를 통해 ASI 관리 체제에 편입되어 다른 서비스들과 동일하게 관리된다. 원래 로컬에 존재하던 기존 솔루션의 경우에도 이러한 구조를 통해 ASI구조에 편입된다.

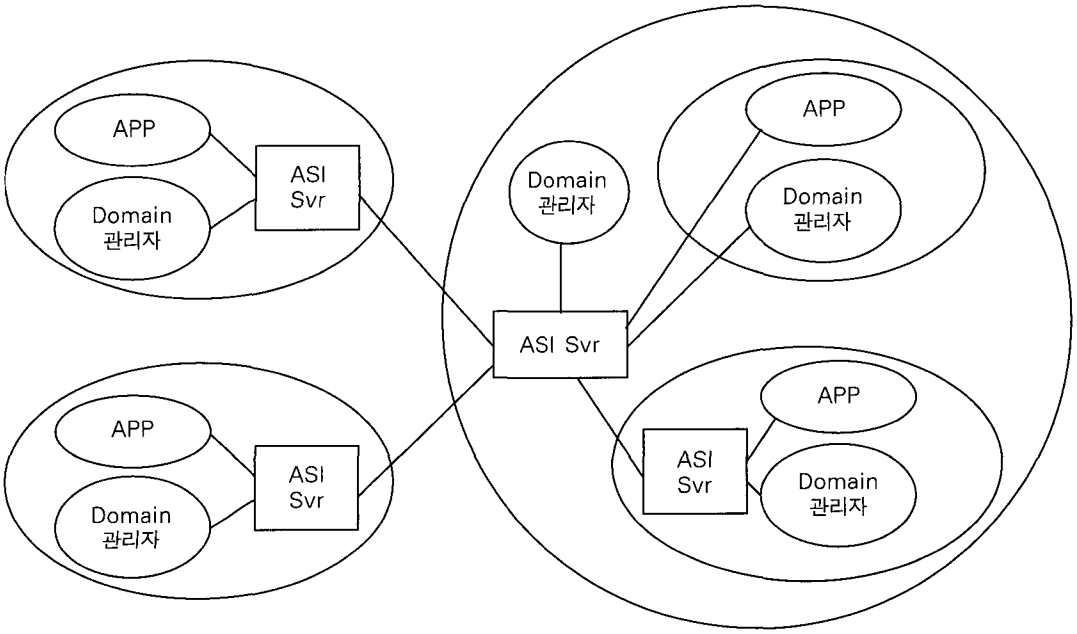
2.2 ASI 도메인 구조

그림 5는 ASI 도메인 구성을 보여준다. 도메인은 개별적으로 독립된 신뢰 단위이다. 도메인 간에 포함관계가 존재할 수 있다.

이 경우 포함하는 도메인을 수퍼 도메인이라하고 포함되는 도메인을 서브도메인이라고 한다.

도메인은 기본적으로 ID 시스템의 범위를 나타내는 ID 도메인이다. 같은 ID시스템 내에서 Sub identifier를 사용하거나 개별적인 인가 도메인을 갖는 경우 서브 도메인을 구성한다.

도메인마다 하나의 ASI 서버가 존재한다. ASI 서버는 도메인의 모든 구성요소로부터 신뢰를 받는다.



〔그림 5〕 IASI 도메인

서브 도메인의 경우에는 별도의 ASI서버를 갖고 있을 수도 있고 수퍼 도메인의 ASI 서버를 공유할 수도 있다. 그러나 서브 도메인의 경우에도 도메인 관리자는 반드시 존재한다.

도메인 간의 연동은 ASI 서버를 경유해서 이루어진다. 두 개의 ASI서버는 연동을 위해 협상, 정책 조율, 속성 매핑과 같은 기능을 수행한다.

V. 결 론

최근의 어플리케이션 환경과 발전 동향을 분석해 볼 때 다양한 종류의 서비스들이 존재하고 발생할 것이며 이들이 서로 통합되어 동작하므로 이러한 환경을 지원하기 위한 새로운 개념의 정보보호서비스가 요구된다고 판단된다. 또한 정보보호 서비스들이 다양해짐에 따라 이들을 통합 관리할 필요성이 증대되고 있다. 이러한 요구 사항에 대응하기 위해 ETRI에서는 통합 어플리케이션 정보보호 기반구조를 개발하고 있다. 통합 어플리케이션 정보보호 기반구조가 개발되면 기존에 불가능하거나 큰 부담이 되었던 여러 가지 정보보호 서비스가 편리하고 저렴하게 제공될 수 있으며 모든 종류의 어플리케이션 정보보호 서비스들을 단일한 인터페이스를 통해 편리하게 이용할 수 있게 되어 지금까지는 정보보호 솔루션 도입과 관리 부담 때문에 안전하지 못한 서비스를 제공하던 서비스 제공자들이 안전한 서비스를 제공할 수 있게 될 것이다.

참고문헌

[1] Geiger, ".Net My Services and .Net Passport User Authentication Overview", Microsoft white paper, september, 2001.

[2] Jeff Hodges, "Liberty Architecture Overview", Liberty Alliance Project documentation, July, 2002.

[3] Russell Jones, "EAM Ain't EASY", Information Security Magazine, January 2002.

[4] "SAML 1.0 Specification Set", OASIS, May 2002.

[5] Longhua Zhang, Gail_Joon Ahn, Bei-Tseng Chu, "A Role-Based Delegation Framework for Healthcare Information systems" SACMAT'02, pp. 125-134, June 2002.

[6] Vijayalakshmi Atluri, Soon Ae Chun, Pietro Mazzoleni, "A Chinese Wall Security Model for Decentralized Workflow Systems", CCS'01, pp. 47-58, November 2001.

[7] Deron Powell, "Enterprise Security Management(ESM): Centralizing Management of Your Security Policy", SANS Institute, December 2000.

[8] Randy Heffner, "Enterprise Application Security Integration", IT Trends 2002, December 2001.

〈著者紹介〉

최 대 선 (Dae-Seon Choi)
정회원

1995년: 동국대학교 전자계산학과 학사
1997년: 포항공과대학교 전자계산학과 석사
1997년 2월~1999년 6월: 현대전자/현대정보기술 정보시스템연구소
1999년 7월~현재: 한국전자통신연구원 정보보호연구본부 인증기반연구팀 연구원
관심분야: 정보보호, 두뇌공학

진 승 헌 (Seung-hun Jin)
정회원

1993년 2월 : 숭실대학교 전자계산 공학과 공학사
1995년 2월 : 숭실대학교 전자계산공학과 공학석사
2000년 3월~현재 : 충남대학교 컴퓨터과학과 박사 과정
1994년 12월~1996년 4월 : 대우통신 종합연구소
1996년 5월~1999년 5월 : 삼성전자 통신연구소
1999년 6월~현재 : 한국전자통신연구원 정보보호연구본부 인증기반연구팀장
관심분야 : 컴퓨터/네트워크 보안, 정보보호(PKI)

정 교 일 (Kyo-il Chung)
정회원
1981년 : 한양대학교 전자공학과 (공학사)
1983년 : 한양대학교 산업대학원 전자계산학과 (공학석사)
1997년 : 한양대학교 대학원 전자공학과 (공학박사)
1982년~현재 : 한국전자통신연구원 정보보호연구본부 정보보호기반연구부장/책임연구원
관심분야 : IC Card, Security, Biometrics, 국가기반보호, 신호처리