

FS-TR02-01, June 18, 2002 (40 pages)

Technical Report

PMI: Privilege Management Infrastructure

3 1009-1

8

e-mail : mhkang@future.co.kr

Abstract

(PKI: Public Key Infrastructure)

(Attribute)

가

(PMI: Privilege Management Infrastructure)

가

가

PMI

(Attribute Certificate)

가

PMI

, PMI

Cryptography & Network Security Center, Future Systems, Inc.
(<http://www.future.co.kr>, <http://www.securitytechnet.com>)

1	. PMI	1
1.1		1
1.2		2
1.3	PMI	3
1.3.1	(General Model)	3
1.3.2	(Control Model)	4
1.3.3	(Delegation Model)	5
1.3.4		5
1.4		6
1.5		7
2	.	9
2.1	ITU-T Recommendation X.509 (2001.3): Attribute Certificate Profile	10
2.1.1	X.509	10
2.1.2		10
2.1.3		13
2.1.4	(Role attribute – Attribute Type)	14
2.1.5	(Extensions)	14
2.2	IETF RFC 3281 : Attribute Certificate Profile	23
2.2.1		23
2.2.2		24
2.2.3	(extensions)	26
2.2.4	(Attribute Type)	28
3	. PMI	31
3.1	Baltimore SelectAccess	31
3.2	Entrust GetAccess	32
3.3	Netegrity SiteMinder	33
3.4	TrustedAuthorizer TrustedAuthorizer	35
3.5	RSA ClearTrust	37
		38

1 . PMI

1.1

가

X.509

가

1.

가

1

가

가

가

2.

가

가

(PKI)

가

가

(PMI: Privilege Management Infrastructure)

(Attribute Certificate)

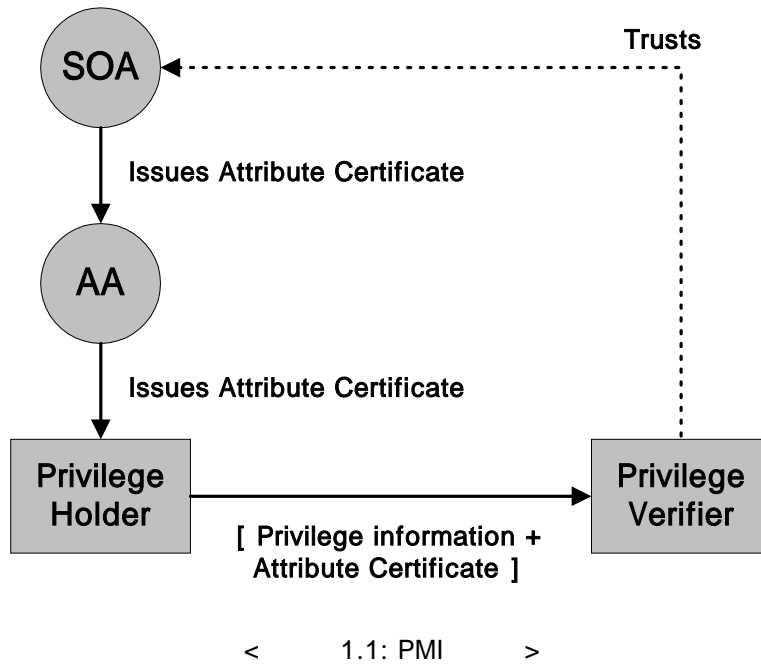
PMI

가 가 가 가

가

가

1.2



< 1.1: PMI >

1.1
SOA(Source Of Authority)
가

(PMI)

CA

AA

AA(Attribute Authority)

SOA

AA

PKI End-entity

(Privilege Verifier)

가

PMI

PKI

PMI Entity	PKI Entity
Source of Authority(SOA)	Root CA
Attribute Authority(AA)	Certificate Authority(CA)
Privilege Holder	Certificate subject
Privilege Verifier	Relying Party

1.3 PMI

ITU-T X.509

(General Model), (Control Model), (Delegation Model),
(Roles Model)

1.3.1 (General Model)

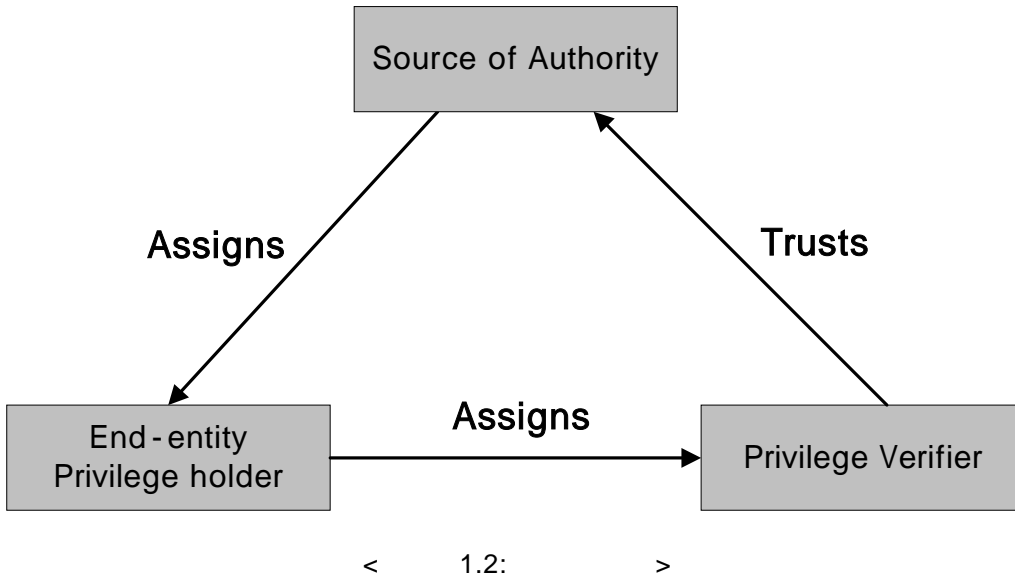
(Object), (Privilege Asserter)
(Privilege Verifier)

가
(Method) 가 , 'Allow Entity' 가
가
가

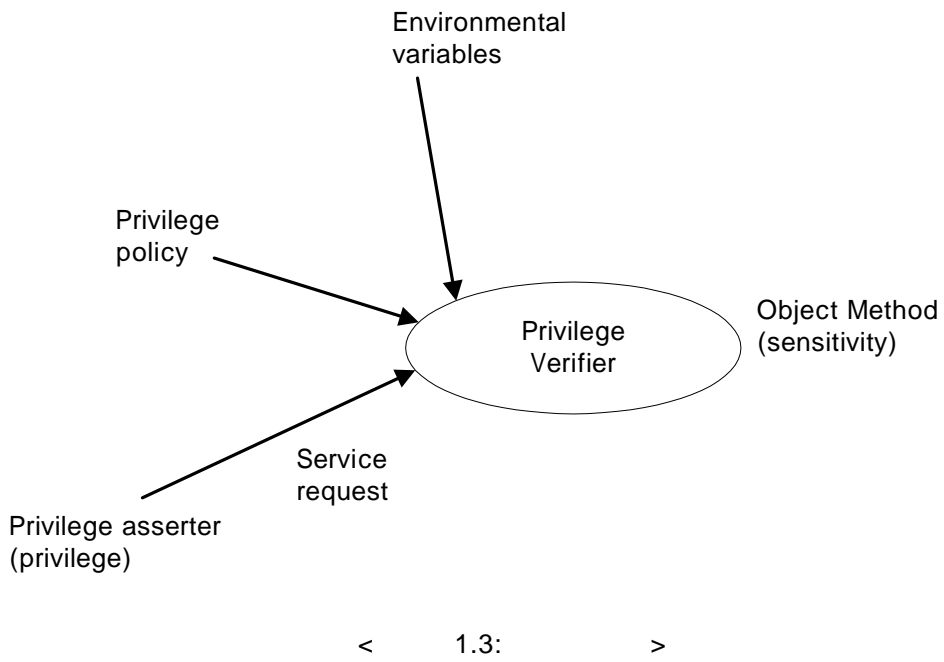
4 가

-
- (privilege policy)
- ,
- (sensitivity)

1.2



1.3.2 (Control Model)



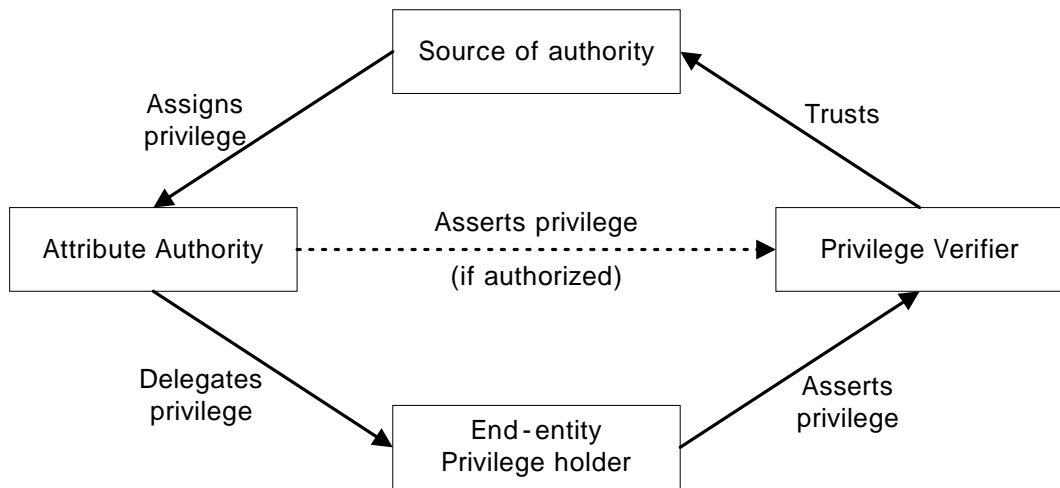
가

1.3

1.3.3 (Delegation Model)

PMI (General Model)

가 , SOA, PMI AA ,
 SOA가 가 AA
 가 가
 AA 가
 End-entity
 SOA AA가 가



< 1.4: >

1.3.4

(Roles)

role

(Role

Specification Certificate)

가

1.4

IETF

•

•

RFC2459

•

•

가

keyUsage 가

가

basicConstraints

CA BOOLEAN

TRUE

•

가

•

•

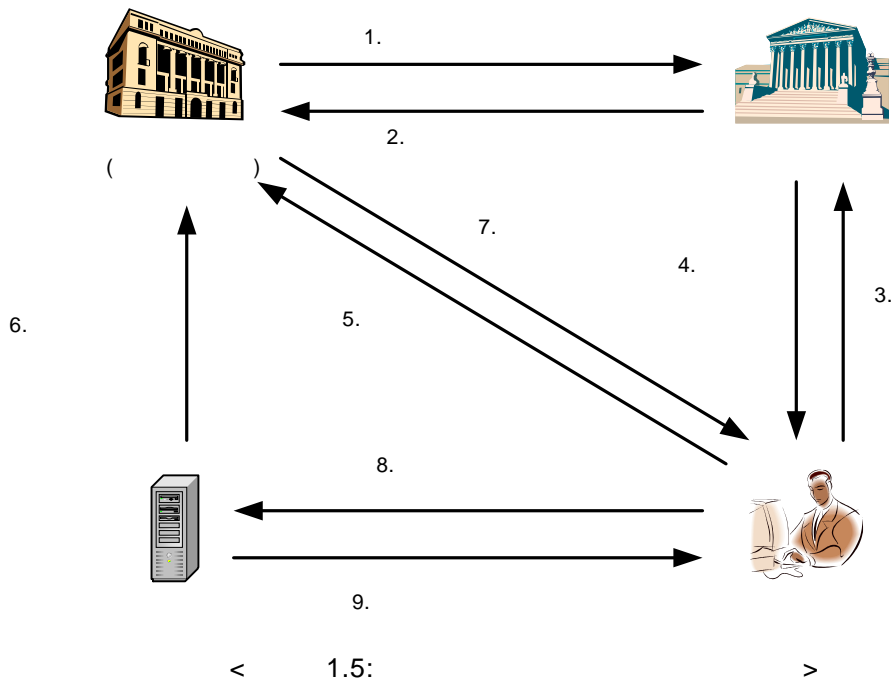
가 Targets

•

critical

가

1.5



1.5

가
가

가

5 7

. 가
가 / 가 가
가 Holder

objectDigestInfo . baseCertificateID, entityName
SEQUENCE .

가
. X.509 2000 ,
RFC 3281 가 .

2 .

PMI IETF
 ITU-T가 . ITU-T ISO/IEC X.509 2000 , IETF
 , RFC 3281 , .
 ITU-T RFC 3281 ,
 version, holder, issuer, signature, serialNumber, attrCertValidityPeriod, attributes,
 issuerUniqueId, extensions . ITU-T , ,
 , 가 PMI
 (Role) .

ITU-T X.509	RFC 3281
Version	version
Holder	holder
Issuer	issuer
Signature	signature
SerialNumber	serialNumber
attrCertValidityPeriod	attrCertValidityPeriod
attributes(1)	attributes(6)
IssuerUniqueId	issuerUniqueId
extensions(13)	extensions(0)

< 2.1: ITU-T RFC 3281 >

2.1 ITU-T Recommendation X.509 (2001.3): Attribute Certificate Profile

2.1.1 X.509

```
AttributeCertificate ::= SIGNED {AttributeCertificateInfo}
```

```
AttributeCertificateInfo ::= SEQUENCE
```

```
{  
    version                AttCertVersion,  
    holder                  Holder,  
    issuer                  AttCertIssuer,  
    signature               AlgorithmIdentifier,  
    serialNumber            CertificateSerialNumber,  
    attCertValidityPeriod  AttCertValidityPeriod,  
    attributes              SEQUENCE OF Attribute,  
    issuerUniqueID          UniqueIdentifier    OPTIONAL,  
    extensions              Extensions         OPTIONAL  
}
```

2.1.2

1) version

```
AttCertVersion ::= INTEGER { v2(1) }
```

2) holder

```
Holder ::= SEQUENCE
```

```
{  
    baseCertificateID      [0] IssuerSerial    OPTIONAL,  
    entityName              [1] GeneralNames   OPTIONAL,  
    objectDigestInfo       [2] ObjectDigestInfo OPTIONAL  
}
```


3) issuer

```
AttCertIssuer ::= [0] SEQUENCE
{
    issuerName          GeneralName          OPTIONAL,
    baseCertificateID   [0] IssuerSerial     OPTIONAL,
    objectDigestInfo    [1] ObjectDigestInfo OPTIONAL
}
```

```
IssuerSerial ::= SEQUENCE
{
    issuer      GeneralNames,
    serial      CertificateSerialNumber,
    issuerID    UniqueIdentifier          OPTIONAL
}
```

- issuerName :
- baseCertificateID : 가 ,
- objectDigestInfo :

4) signature

5) serialNumber

6) attCerValidityPeriod

```

AttCertValidityPeriod ::= SEQUENCE
{
    notBeforeTime    GeneralizedTime,
    notAfterTime     GeneralizedTime
}

```

7) attribute

8) issuerUniqueID

가

9) extensions

가

2.1.3

```

AttributeCertificatePath ::= SEQUENCE
{
    attributeCertificate    AttributeCertificate,
    acPath                  SEQUENCE OF ACPATHData    OPTIONAL
}

```

```

ACPATHData ::= SEQUENCE
{
    certificate            [0]    Certificate            OPTIONAL,
    attributeCertificate   [1]    AttributeCertificate    OPTIONAL
}

```

2.1.4 (Role attribute – Attribute Type)

Role ATTRIBUTE ::=

```
{  
  WITH SYNTAX      RoleSyntax  
  ID                id-at-role  
}
```

RoleSyntax ::= SEQUENCE

```
{  
  roleAuthority    [0]   GeneralNames OPTIONAL,  
  roleName         [1]   GeneralName  
}
```

2.1.5 (Extensions)

- **Basic Privilege Management :**

1) Time Specification Extension

timeSpecification EXTENSTION ::=

```
{  
  SYNTAX           TimeSpecification  
  IDENTIFIED BY   id-ce-timeSpecification  
}
```

- 가
AA
- 가 critical

2) Targeting Information Extension

```
targetingInformation EXTENSION ::=
{
  SYNTAX          SEQUENCE SIZE (1..MAX) OF Targets
  IDENTIFIED BY   id-ce-targetInformation
}
```

```
Targets ::= SEQUENCE SIZE (1..MAX) OF Target
```

```
Target ::= CHOICE
{
  targetName      [0]   GeneralName,
  targetGroup     [1]   GeneralName,
  targetCert      [2]   TargetCert
}
```

```
TargetCert ::= SEQUENCE
{
  targetCertificate      IssuerSerial,
  targetName             GeneralName      OPTIONAL,
  certDigestInfo        ObjectDigestInfo OPTIONAL
}
```

- IETF AC targeting extension
-

3) User Notice Extension

```
userNotice EXTENSION ::=
{
  SYNTAX          SEQUENCE SIZE (1..MAX) OF UserNotice
  IDENTIFIED BY   id-ce-userNotice
}
```

- AA 가 , 가

4) Acceptable privilege policies extension

```
acceptablePrivilegePolicies EXTENSION ::=
```

```
{  
  SYNTAX          AcceptablePrivilegePoliciesSyntax  
  IDENTIFIED BY   id-ce-acceptablePrivilegePolicies  
}
```

```
AcceptablePrivilegePoliciesSyntax ::= SEQUENCE SIZE (1..MAX) OF  
                                       PrivilegePolicy
```

- 가 가 .

- **Privilege Management Certificate Extension :**

1) CRL distribution points extension

```
cRLDistributionPoints EXTENSION ::=
```

```
{  
  SYNTAX          CRLDistPointsSyntax  
  IDENTIFIED BY   id-ce-cRLDistributionPoints  
}
```

```
CRLDistPointsSyntax ::= SEQUENCE SIZE (1..MAX) OF DistributionPoint
```

```
DistributionPoint ::= SEQUENCE {  
  DistributionPoint [0] DistributionPointName OPTIONAL,  
  reasons [1] ReasonFlags OPTIONAL,  
  cRLIssuer [2] GeneralNames OPTIONAL  
}
```

```
DistributionPointName ::= CHOICE {
```


- Source of Authority Extension :

1) SOA Identifier Extension

```

soaIdentifier EXTENSION ::=
{
  SYNTAX          NULL
  IDENTIFIED BY   id-ce-soaIdentifier
}

```

- CA SOA 가
- Certificate Subject가 SOA
- SOA

2) Attribute Descriptor Extension

```

attributeDescriptor EXTENSION ::=
{
  SYNTAX          AttributeDescriptorSyntax
  IDENTIFIED BY   {id-ce-attributeDescriptor }
}

```

```

AttributeDescriptorSyntax ::= SEQUENCE

```

```

{
  identifier          AttributeIdentifier,
  attributeSyntax     OCTET STRING          (SIZE(1..MAX)),
  name                [0] AttributeName     OPTIONAL,
  description         [1] AttributeDescription OPTIONAL,
  dominationRule     PrivilegePolicyIdentifier
}

```

```

AttributeIdentifier ::= ATTRIBUTE.&id({AttributeIDs})

```

```

AttributeIDs ATTRIBUTE ::= {...}

```


-
-
- 가 , 가
(non-critical).
- , 가
,

- **Delegation Extension :**

1) Basic Attribute Constraints Extension

```
basicAttConstraints EXTENSION ::=
{
  SYNTAX          BasicAttConstraintsSyntax
  IDENTIFIED BY  { id-ce-basicAttConstraints }
}
```

```
BasicAttConstraintsSyntax ::= SEQUENCE
{
  authority          BOOLEAN DEFAULT FALSE,
  pathLenConstraint INTEGER (0..MAX) OPTIONAL
}
```

-
- authority : . TRUE holder가
AA , , FALSE holder가 end-entity .
- pathLenConstraint authority가 true . Delegation Path
AA
- pathLenConstraint가 , Delegation Path 가 .

2) Delegated Name Constraints Extension

```
delegatedNameConstraints EXTENSION ::=
{
  SYNTAX          NameConstraintsSyntax
  IDENTIFIED BY   id-ce-delegatedNameConstraints
}
```

- Delegation Path

가

- nameConstraints

3) Acceptable Certificate Policies Extension

```
acceptableCertPolicies EXTENSION ::=
{
  SYNTAX          AcceptableCertPoliciesSyntax
  IDENTIFIED BY   id-ce-acceptableCertPolicies
}
```

AcceptableCertPoliciesSyntax ::= SEQUENCE SIZE (1..MAX) OF CertPolicyId
CertPolicyId ::= OBJECT IDENTIFIER

- 가 ,

가

- ,

- end-entity

4) Authority Attribute Identifier Extension

```
authorityAttributeIdentifier EXTENSION ::=
{
  SYNTAX          AuthorityAttributeIdentifierSyntax
  IDENTIFIED BY   { id-ce-authorityAttributeIdentifier }
}
```

AuthorityAttributeIdentifierSyntax ::= SEQUENCE SIZE (1..MAX)
OF AuthAttId

AuthAttId ::= IssuerSerial

- authority 가 AA privilege 가 ,
- AA AA end-entity
- extension .
- (back pointer) .
- ,
.

2.2 IETF RFC 3281 : Attribute Certificate Profile

2.2.1

```
AttributeCertificate ::= SEQUENCE {  
    acinfo          AttributeCertificateInfo,  
    signatureAlgorithm AlgorithmIdentifier,  
    signatureValue   BIT STRING  
}
```

```
AttributeCertificateInfo ::= SEQUENCE {  
    version          AttCertVersion  
    holder           Holder,  
    issuer           AttCertIssuer,  
    signature        AlgorithmIdentifier,  
    serialNumber     CertificateSerialNumber,  
    attrCertValidityPeriod AttCertValidityPeriod,  
    attributes       SEQUENCE OF Attribute,  
    issuerUniqueID   UniqueIdentifier OPTIONAL,  
    extensions       Extensions OPTIONAL  
}
```

```
Attribute ::= SEQUENCE {  
    type      AttributeType,  
    values    SET OF AttributeValue  
}
```

```
AttributeType ::= OBJECT IDENTIFIER
```

```
AttributeValue ::= ANY DEFINED BY AttributeType
```


7) attribute

가

가

8) issuerUniquelIdentifier

9) extensions

holder

가

(non-critical extension)

)

(

2.2.3 (extensions)

1) Audit Identity

ID

(

/

가

).

name	id-ce-targetInformation
OID	{ id-ce 55 }
Syntax	SEQUENCE OF Targets
Criticality	MUST be TRUE

2) AC targeting

Targets ::= SEQUENCE OF Target

```
Target ::= CHOICE {
    targetName      [0]  GeneralName,
    targetGroup     [1]  GeneralName,
    targetCert      [2]  TargetCert
}
```

```
TargetCert ::= SEQUENCE {
    targetCertificate IssuerSerial,
    targetName        GeneralName      OPTIONAL,
    certDigestInfo    ObjectDigestInfo OPTIONAL
}
```

targeting information target

3) Authority Key Identifier

가

4) Authority Information Access

가

(OCSP protocol) . accessLocation URI URI HTTP
URL .(OCSP)

5) CRL Distribution Points

가

6) No Revocation Available

가

2.2.4 (Attribute Type)

IETF

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

1) Service Authentication Information

가

가

```
SvceAuthInfo ::= SEQUENCE {
    service      GeneralName,
    ident       GeneralName,
    authInfo    OCTET STRING OPTIONAL
}
```

2) Access Identity

(

holder

). authInfo

3) Charging Identity

Charging()

4) Group

5) Role

holder

6) Clearance

```
Clearance ::= SEQUENCE {  
    policyId          [0]  OBJECT IDENTIFIER,  
    classList         [1]  ClassList DEFAULT {unclassified},  
    securityCategories [2]  SET OF SecurityCategory OPTIONAL  
}
```

```
ClassList ::= BIT STRING {  
    unmarked          (0),  
    unclassified      (1),  
    restricted        (2),  
    confidential      (3),  
    secret            (4),  
    topSecret         (5)  
}
```

```
SecurityCategory ::= SEQUENCE {  
    Type          [0]    IMPLICIT OBJECT IDENTIFIER,  
    value         [1]    ANY DEFINED BY type  
}
```

3 . PMI

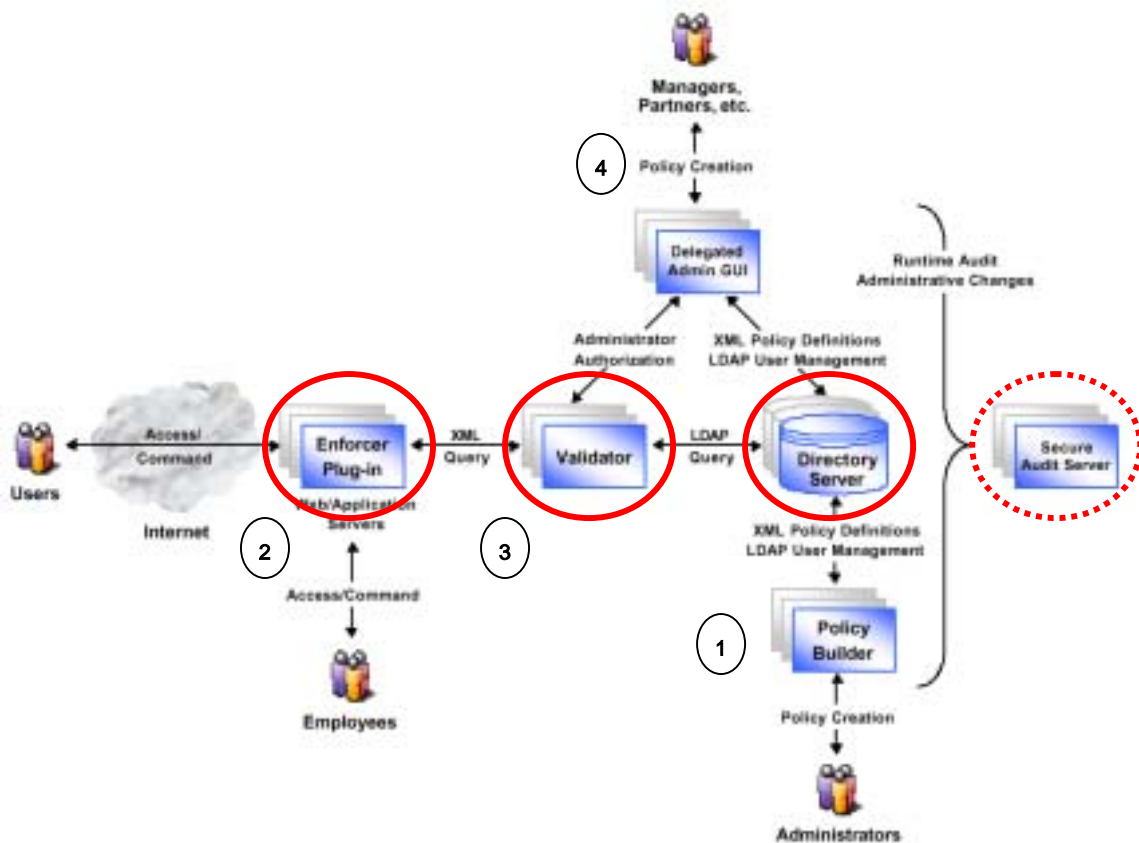
PMI

5

PMI

- Baltimore's SelectAccess
- Entrust's GetAccess
- Netegrity's SiteMinder
- TrustedAuthorizer's TrustedAuthorizer
- RSA's ClearTrust

3.1 Baltimore SelectAccess



< 3.1: SelectAccess >

(authorized)

(4) AccessServer custom navigation

(5) 가 , intercept

(6) , Registry Server (verify)

(7) registry server ID, (preferences), (roles),

(8)

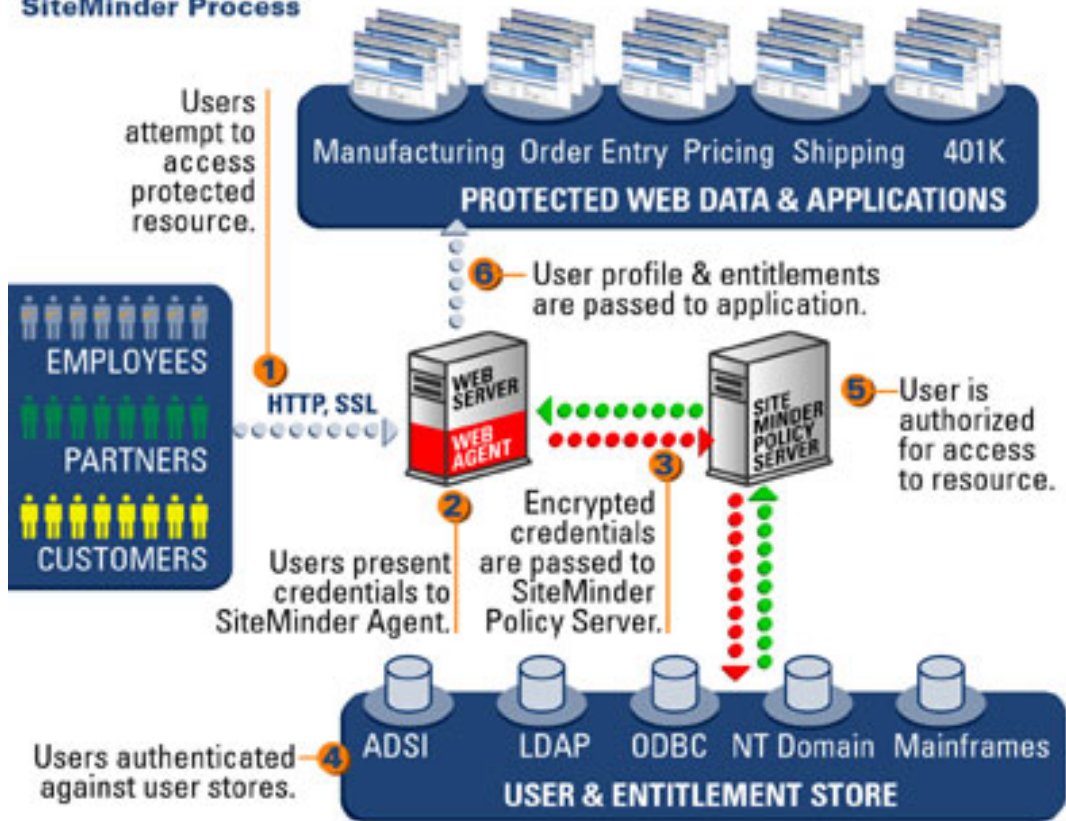
* Mobile Proxy Server wireless device 가

3.3. Netegrity SiteMinder

(1) Resource Protection : Web Agent
SiteMinder policy
database 가

(2) Authentication : SiteMinder가 ,
SiteMinder , Web Agent
Agent / ,
Policy Server 가 Policy Server
Server 가
가 (full) , timestamps SiteMinder
Web seit single
sign-on

SiteMinder Process

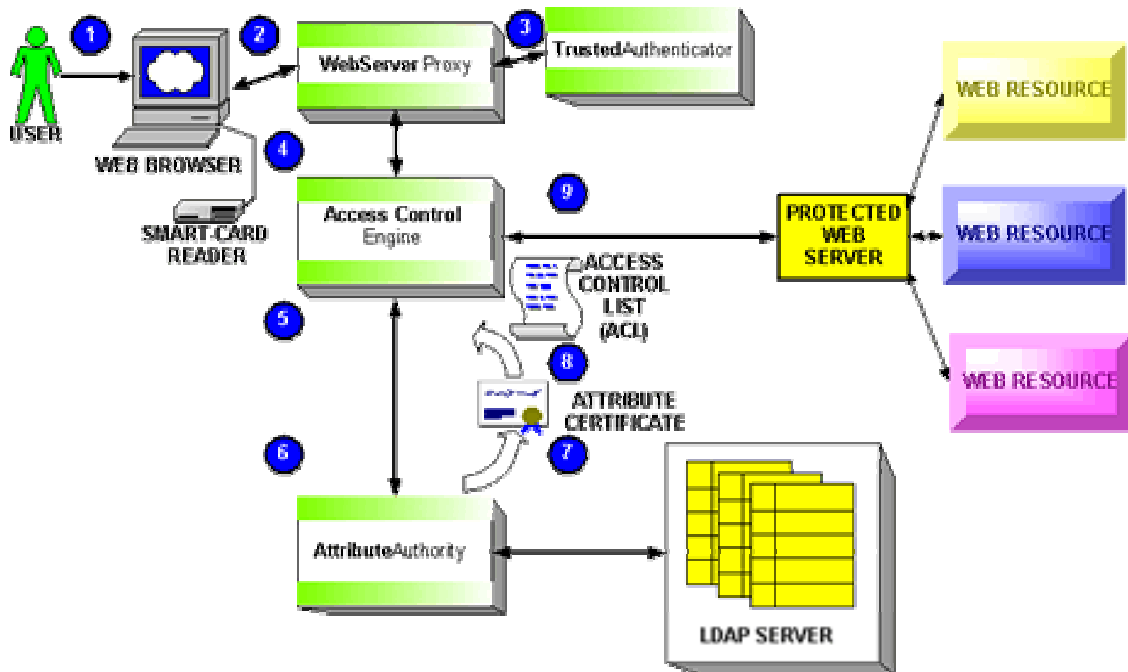


< 3.3: SiteMinder >

(3) Authorization : 가 , SiteMinder
 . Policy Server 가
 Policy Store . Policy Server
 가 가 .
 - common attributes - , SiteMinder
 가

(4) Personalization : SiteMinder
 . ,
 (personalize)
 가
 가 , SiteMinder 가

3.4 TrustedAuthorizer TrustedAuthorizer



< 3.4: TrustedAuthorizer >

(1)

TrustedAuthorizer

(2) TrustedWebServer SSL-enabled Web Server Proxy . TrustedWebServer
 intercept . URL

■ _____ / _____ : TrustedAuthorizer Web
 Server identity . , Access Control Engine
 identifier 'single-sign on' 가
 가 , (authentication) 가

■ _____ /ID : TrustedAuthorizer Web Server
 TrustedAuthenticator
 redirect .

(3) 가 ID , , Trusted
Authenticator 가 . TrustedAuthenticator

identity . single-sign-on
 가 가
 Single sign-on 가 any period

(4) Access Control Engine .

(5) Access Control Engine(ACE) Attribute Authority . ACE
 . ACE
 identity - URL . ACE
 attribute certificate attributes가
 attribute가 , ACE LAAP
 Attribute Authority . * LAAP
 : Lightweight Attribute Certificate Access Protocol

(6) Attribute Authority ACE attribute certificate , Attribute
 Authority identity 가
 가 .

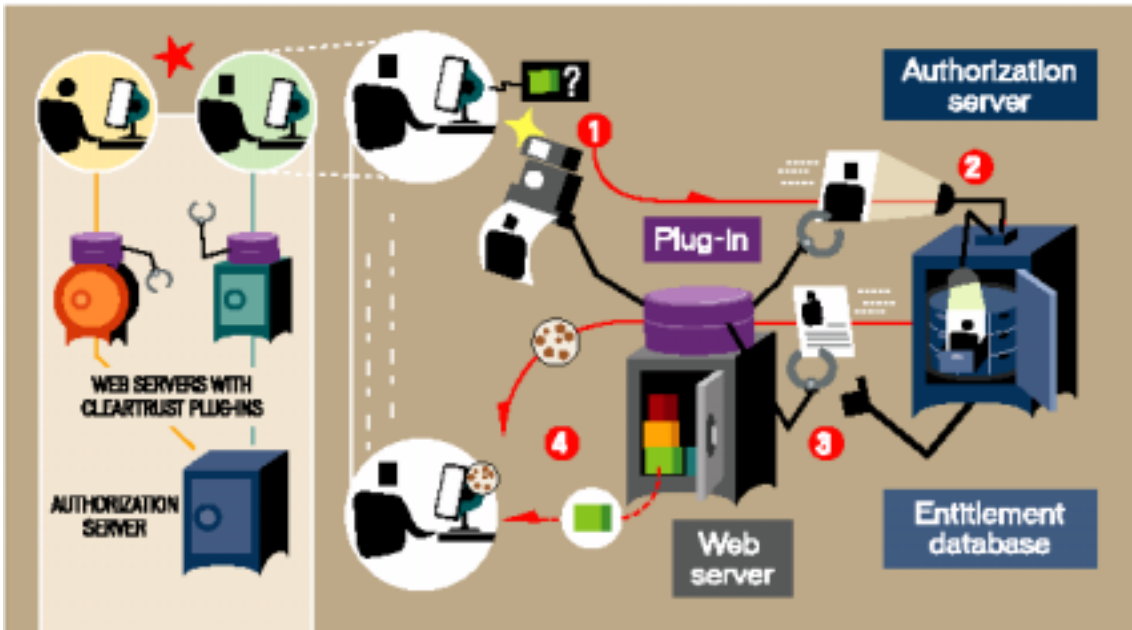
(7) Note. Attribute Authority LDAP

(8) 가 , Attribute Authority Attribute
Certificate ACE . Attribute Certificate
 ACE . Attribute Certificate
 (short lived)

(9) Access Control Engine Attribute Authority Attribute Certificate
ACL(Access Control List) attribute
 Access Control List 가 가
 가
 security attributes,
 action

(10) Access Control List Attribute Certificate 가 , Access Control Engine가 ACL

3.5. RSA ClearTrust



< 3.5: ClearTrust >

Securant (authorization) Web server
integration complexities

가

가

(1) , Web ClearTrust
plug-in (credentials)

(2) authorization server Authorization server Securant
entitlement database 가 plug-in (authorization)

(3) , plug-in

- [1]. American National Standard for Financial Services X9.45, “Enhanced Management Controls Using Digital Signatures and Attribute Certificates”
- [2]. ISO/IEC 9594-8 / ITU-T Recommendation X.509, “Information Technology – Open System Interconnection: The Directory: Authentication Framework”, 1997.
- [3]. S. Farrell and R. Housley, “An Internet Attribute Certificate Profile for Authorization”, RFC 3281, April 2002. available on line at <http://www.ietf.org/rfc/rfc3281.txt>.
- [4]. Joon S. Park and Ravi Sandhu, “Binding Identities and Attributes Using Digitally Signed Certificates”, IEEE Communication Magazine, September, 2000.
- [5]. P. Yee, “Attribute Certificate Management Messages over CMS”, March 2002, draft-ietf-pkix-acmc-01.txt
- [6]. P. Yee, Attribute Certificate Request Message Format, March 2002, draft-ietf-pkix-acrmf-01.txt