

Attribute Revocation, Audit

Santosh Chokhani
28 September 2009

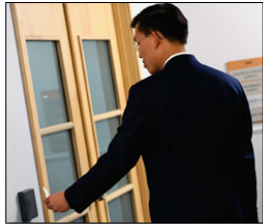
- **Attribute Promulgation Methods**
- **Revocation**
 - **Considerations**
 - **How to revoke based on attribute promulgation methods**
 - **Pros and cons**
- **Audit**
 - **Events**
 - **Other Considerations**
 - **Pros and cons based on attribute promulgation methods**

Attributes Promulgation

- **Public Key Certificate**
 - Subject Directory Attribute Extension
 - Implicit in Name
- **Attribute Certificate**
- **SAML Authorization Attribute Server**
- **Database Server**
- **Application Database**

Public Key Certificate

Claimant



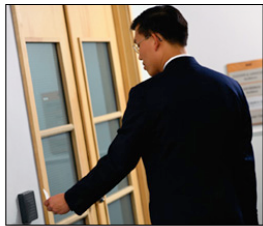
Relying
Party
System



- Certificate has attributes
- Certificate Revocation can be checked by relying party
- Claimant uses private key in a secure cryptographic protocol to prove to be subject of the certificate
- Relying party associates attributes in the certificate with the subject of certificate (subject DN or SAN)

Attribute Certificate

Claimant



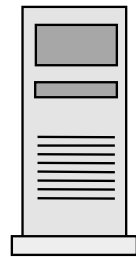
Relying
Party
System



- Claimant uses private key in a secure cryptographic protocol to prove to be subject of PKC and AC
- PKC and AC bound by name or key or key hash in AC
- Relying party associates attributes in the AC with the subject of AC and PKC (subject DN or SAN)

SAML Assertion

- Authorization Server could rely on other mechanisms (PKC, AC, DB, etc.) to obtain the attributes



Authorization Server



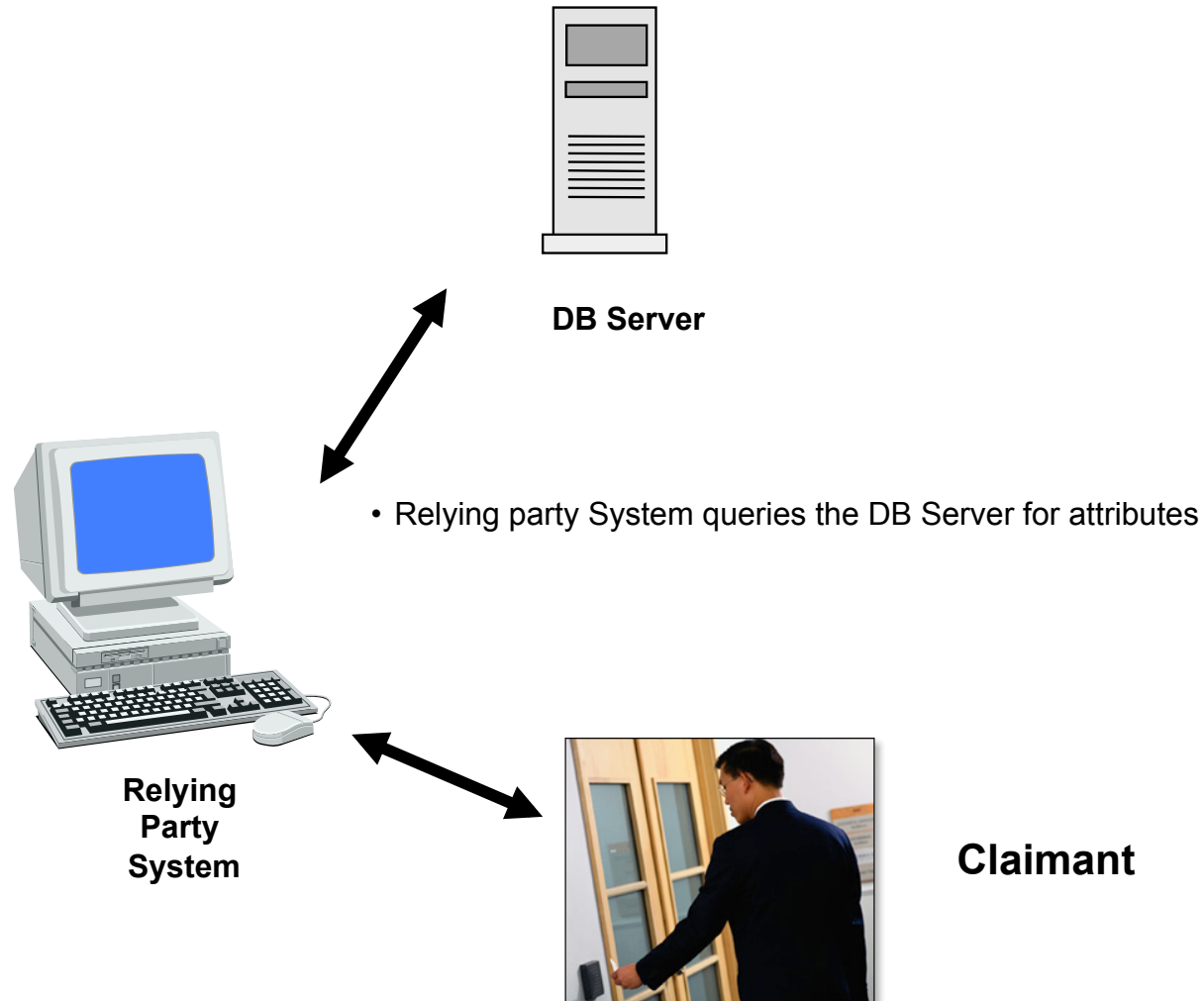
Relying Party System

- Claimant identity is verified and attribute are provided in SAML authorization assertion



Claimant

Database Server

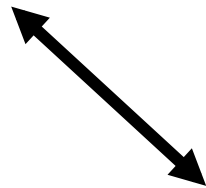


Application Database



Application

- Application uses attributes based on authenticated identity of the claimant



Claimant

Revocation: Considerations

- **Speed of Revocation**
- **Latency for Relying Parties**
- **Authentication and Authorization Balance**
 - Safer to revoke than not to revoke
 - Relying party denial of service due to rogue person revocation
- **Synchronization of distributed databases**

Revocation Methods

- **Public Key Certificate**
 - CRL, OCSP, Proprietary Micali Scheme to revoke specific attribute without revoking certificate
- **Attribute Certificate**
 - ACRL, Proprietary Micali Scheme to revoke specific attribute without revoking certificate
- **SAML**
 - None; Assertions are short-lived
 - Authorization Server creates SAML assertions using other methods listed here. Thus, revocation is effected using other methods
- **Database**
 - Database update

Pros and Cons

	Speed	Latency	Balance	Sync
Public Key Certificate				
Attribute Certificate				
SAML				
Database Server				
App Database				

- **Bestowal of attribute**
- **Withdrawal of attribute**
- **Modification of attribute**

- **Log size**
- **Amenability to processing**
 - Good, old needle in haystack
- **Integrity**
- **Privacy/Confidentiality**
- **Aggregation problem**
 - Rich dataset more sensitive than sum of individual parts

Audit: Pros and Cons

	Log Size	Proc.	Integrity	Privacy/ Conf.	Aggr.
PKC					
AC					
SAML					
DB Server					
App					

What Did I Miss?

