

Binding Identities and Attributes Using Digitally Signed Certificates

Joon S. Park, NRL/ITT
Ravi Sandhu, George Mason Univ.

Related Work

- X.509 Certificates
- Attribute Certificates
- SPKI (Simple Public Key Infrastructure)
- PGP (Pretty Good Privacy)
- Smart Certificates

Introduction

- In this paper, we
 - Analyze the basic structure of digital certificates and classify the nature of the information.
 - Identify 3 different binders.
 - Describe each binder and compare with others.

Basic Structure of Certificates



Digital Certificate

- What is it?
 - Signed by a CA to confirm that the information in it is valid and belong to the subject.
- Purpose?
 - To provide the integrity of the information (e.g., identities or attributes) in the certificates.

Basic Structure of Certificates

- We classify the nature of information in certificates into blocks.
- The content of each block depends on applications and policies.
- ID certificates should contain authentication information.
- Attribute certificates should link to ID certificates.

Binders

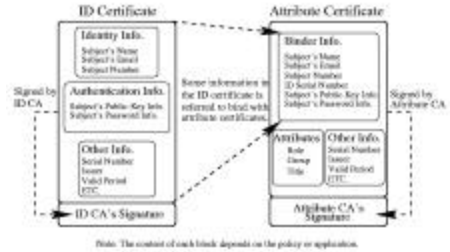
- What is a binder?
 - A mechanism to link attributes to proper identities
- Factors
 - Different CAs
 - Different lifetimes
 - Strength
- To satisfy the requirements, we identify
 - Monolithic Signature
 - Autonomic Signature
 - Chained Signature

Joon S. Park

INFS 767

7

Autonomic Signature



Joon S. Park

INFS 767

10

Monolithic Signature



Joon S. Park

INFS 767

8

Autonomic Signature

- Supports multiple CAs and different lifetimes.
- Binding some information (e.g., subject's name) in ID certificates and attribute certificates.
- Identity and attributes are *loosely-coupled*.

Joon S. Park

INFS 767

11

Monolithic Signature

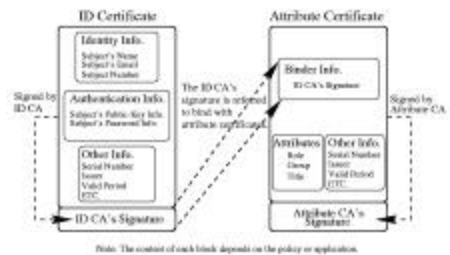
- The simplest binding mechanism.
- Identity and attributes are *tightly-coupled*.
- Problems
 - Multiple CAs, Different Lifetimes

Joon S. Park

INFS 767

9

Chained Signature



Joon S. Park

INFS 767

12

Chained Signature

- Supports multiple CAs and different lifetimes.
- Binding ID CA's signatures in ID certificates and attribute certificates.

A Comparison

| | Monolithic | Autonomic | Chained |
|-----------------------|-----------------|-----------------|-----------|
| CAs | Single | Multiple | Multiple |
| Lifetimes | Same | Different | Different |
| Binding Strength | Tightly-Coupled | Loosely-Coupled | Medium |
| Reusability | Low | High | Medium |
| Certificate Discovery | Easy | Medium | Difficult |

Conclusions

- In this paper
 - We analyzed the basic structure of digital certificates and classified the nature of the information.
 - We identified 3 different binders.
 - We described each binder and compared with others.