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.

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.

Related Work

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

### Monolithic Signature

- The simplest binding mechanism.
- Identity and attributes are tightly-coupled.

### Problems
- Multiple CAs, Different Lifetimes

### 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.

### Chained Signature

- The identity and attributes are linked through a chain of certificates.
- Each certificate confirms the authenticity of the previous one.

Note: The content of each block depends on the policy or application.
Chained Signature

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

A Comparison

<table>
<thead>
<tr>
<th></th>
<th>Monolithic</th>
<th>Autonomic</th>
<th>Chained</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAs</td>
<td>Single</td>
<td>Multiple</td>
<td>Multiple</td>
</tr>
<tr>
<td>Lifetimes</td>
<td>Same</td>
<td>Different</td>
<td>Different</td>
</tr>
<tr>
<td>Binding Strength</td>
<td>Tightly Coupled</td>
<td>Loosely Coupled</td>
<td>Medium</td>
</tr>
<tr>
<td>Reusability</td>
<td>Low</td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>Certificate</td>
<td>Easy</td>
<td>Medium</td>
<td>Difficult</td>
</tr>
<tr>
<td>Discovery</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.