



December 3-6, 2007, Santa Clara Marriott, Santa Clara, CA

Security Management

Scope

Disclaimer



The DMTF was formed to lead the development, adoption and unification of management standards and initiatives for desktop, enterprise and internet environments

- The information in this presentation represents a snapshot of work in progress within the DMTF.
- This information is subject to change. The Standard Specifications remain the normative reference for all information.
- For additional information, see the Distributed Management Task Force (DMTF) Web site.
<http://www.dmtf.org>.

Presentation Goal

- Describe why and when DMTF security management profiles are useful, and perhaps as importantly what they do not cover.
- Discuss the relationship of these profiles to other management profiles and how these security profiles should be integrated into the implementation of a CIM Server.

Purpose of Security Mgmt profiles

- Security management profiles:
 - Specify the service interfaces used to manage the security related aspects of a system or separately managed subsystem
 - Define how to impose security policies, but do choose specific security policies
 - Specific security policies are imposed by management profiles that define the overall system or subsystem behavior

Current Security Mgmt profiles

- Simple Identity Management
- Role Based Access
- Credential Management

Simple Identity Management

- Specifies the interfaces required to:
 - Manage local accounts
 - Manage principals authenticated locally
 - Manage principals authenticated remotely
 - Scope authentication of principals to specified ingress points, systems, services, or other contexts
 - Manage groups of principals
- Does NOT specify authentication interfaces or mechanisms

Role Based Access

- Interfaces to manage:
 - Roles and the privileges that they grant
 - Assignment of principals to roles
 - Ability to restrict the use of a role to at most one principal

- Future extensions:
 - Additions to manage extended information related to roles

Credential Management

- Management of keys and certificates
- Import/Export of keys and certificates
- Managing certificate revocation lists
- Interface for signing certificates

Future Security Mgmt profiles

- Identity Management
 - Base for Simple Identity Management
 - Generic behavioral interfaces for all types of principals
- Authorization Management
 - Interfaces to manage ACL based privileges
 - Interfaces to manage resource ownership
- Security Service Management
 - Manage security services on the local system, including their use of 3rd party services
- Security Policy Management
 - Interfaces to manage specification of authentication and authorization policies

Relationship to other Profiles

- CLP Service, specifies roles
- Service processor
- Base Server
- Base Desktop Mobile

