

November 15-18, 2010



Santa Clara Marriott  
Santa Clara, CA

# **Standardization and open source implementation of integrated access control policy management**

Ryuichi Ogawa, Masayuki Nakae

Service Platforms Res. Labs.

NEC Corporation

**NEC**

# Disclaimer

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.

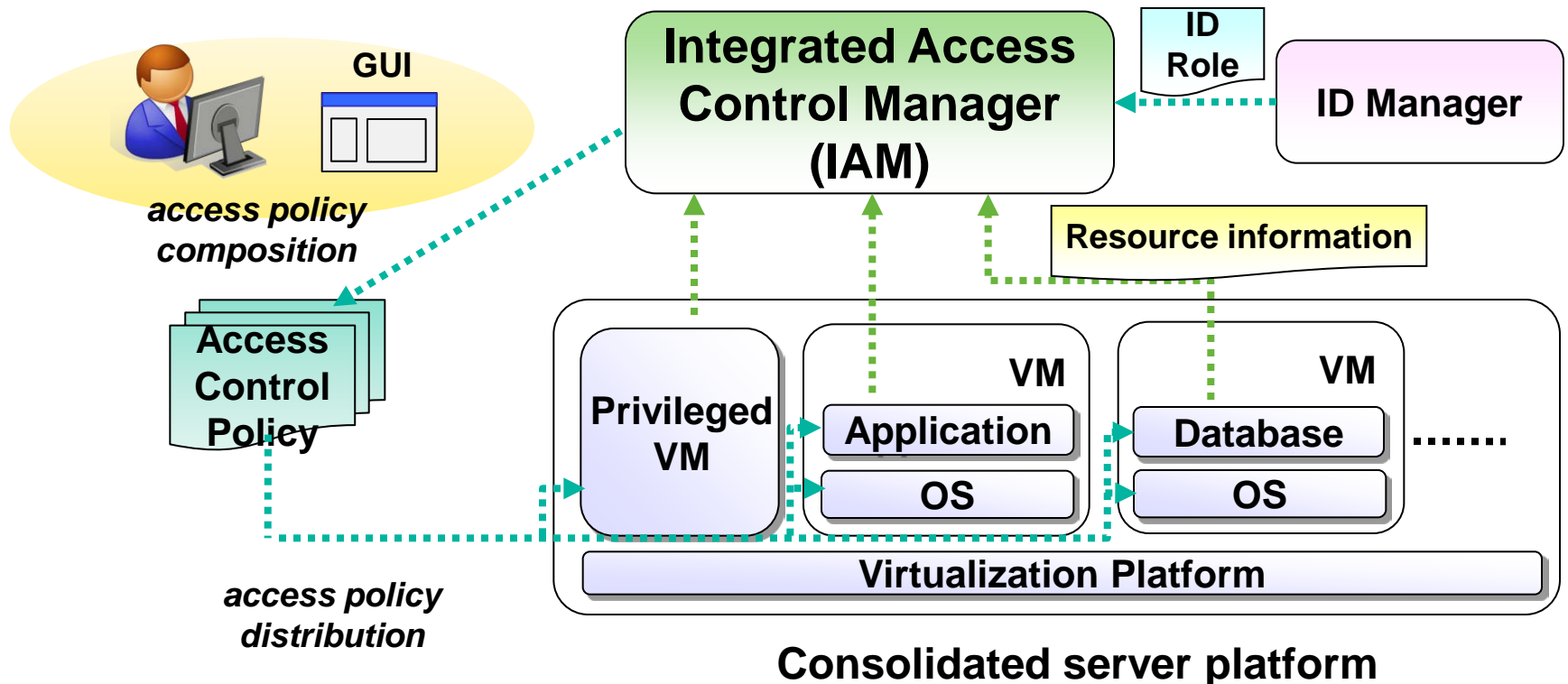
<http://www.dmtf.org/standards/cdm>



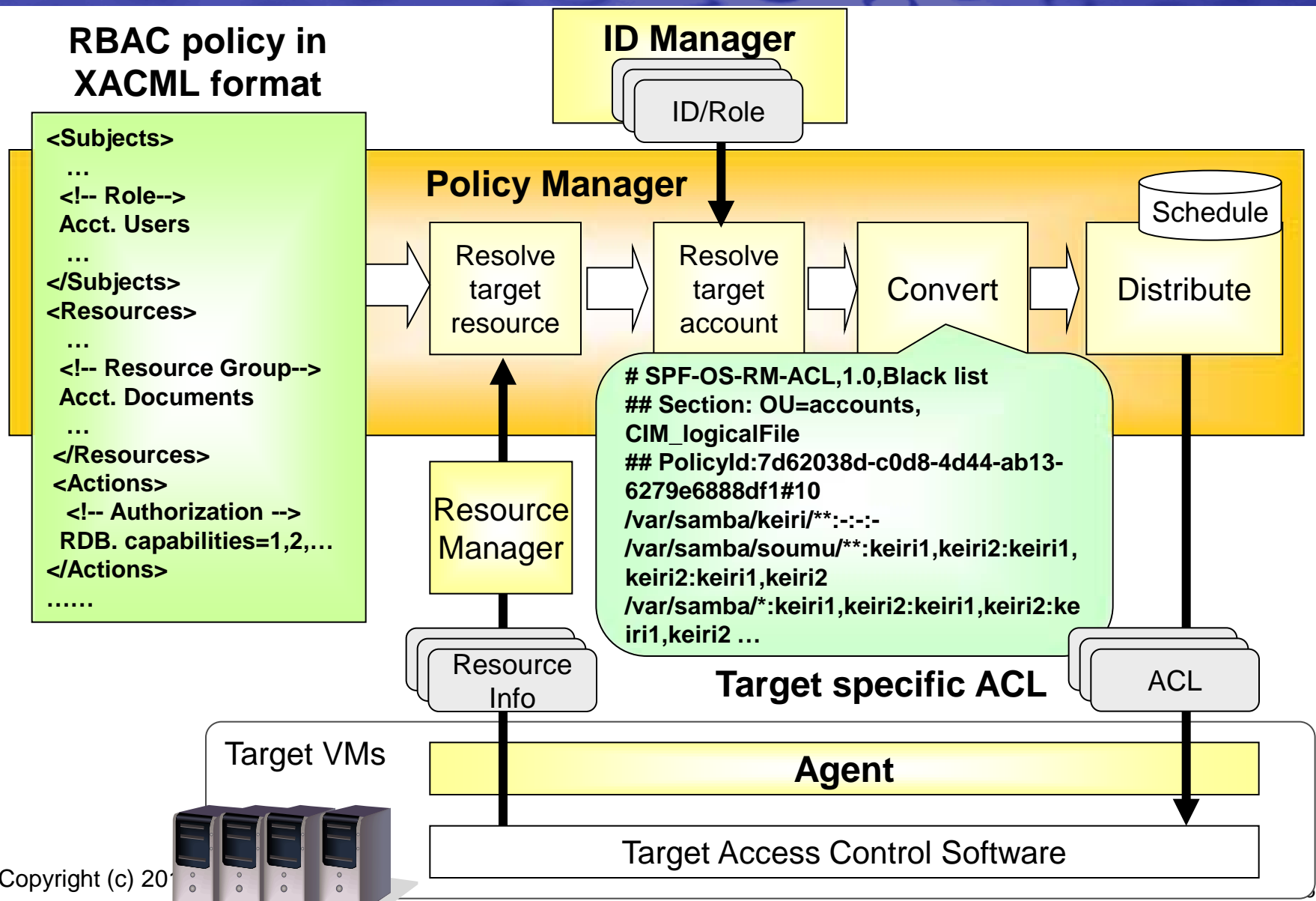
- Introduction
- Proposal of IAM profile
  - Model
  - Use case
- Profile implementation
  - ETRI collaboration
- Demonstration
- Future work

# Introduction: Secure Platform overview

- Secure Platform (SPF) is an architecture of security measures and management for consolidated server environment.
- Integrated Access Manager (IAM) is a core building block of SPF-based security management, which allows us to manage a number of ACLs with a common set of Role-Based Access Control (RBAC) policies.



# How IAM actually works

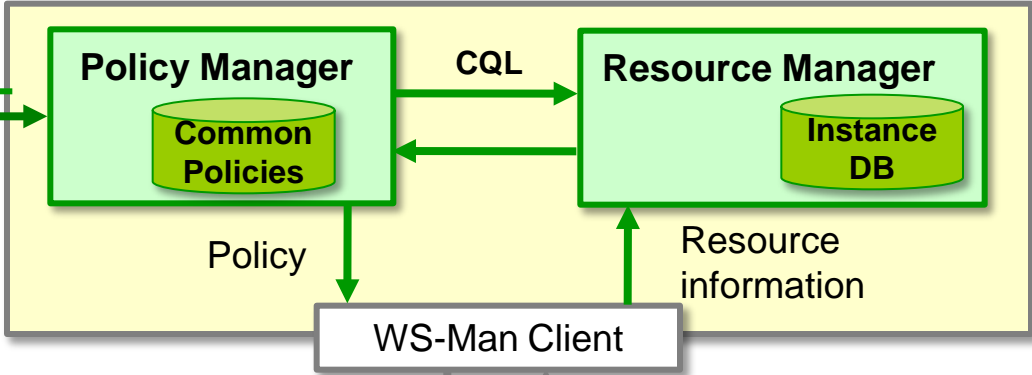


# CIM-based architecture

Security Manager



*Integrated Access Control Manager*

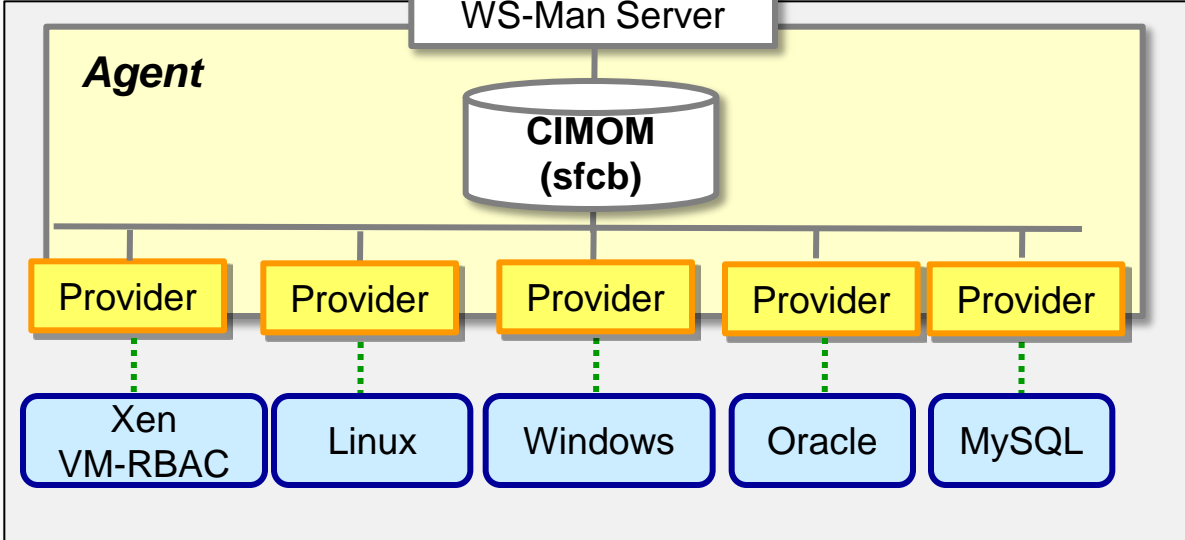


WS-Transfer (Put)

WS-Transfer (Get)  
WS-Enumeration

WS-Man Server

Target server



# Related profiles

- CIM-SPL
  - Specifies CIM-based policy language for policy-driven management of distributed objects. Its RBAC extension is proposed.
- RBAC profile
  - Specifies role-based access control functionality targeted to managed objects

## Issue

- We need a new profile that can handle access policy composition and distribution for different types of resources/operations in an integrated manner.

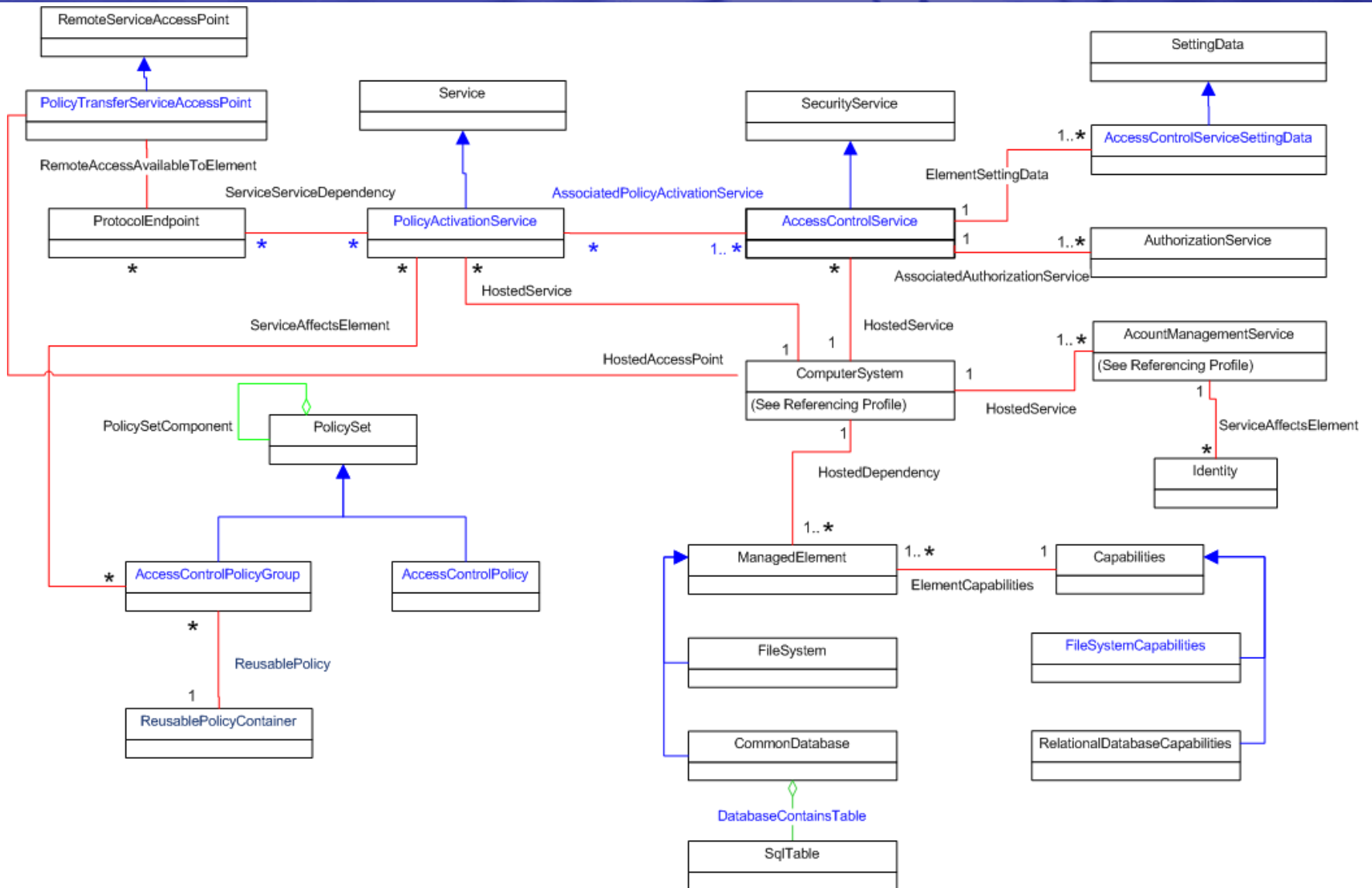
# Proposal of IAM profile

- A profile for integrated management of access control policies has been proposed
  - Modeling access control modules and their access control types
  - Defining methods for distributing and activating access control policies
- Work in Progress profile is available from DMTF site
  - DSP1106 1.0.0 Integrated Access Control Policy Management Profile

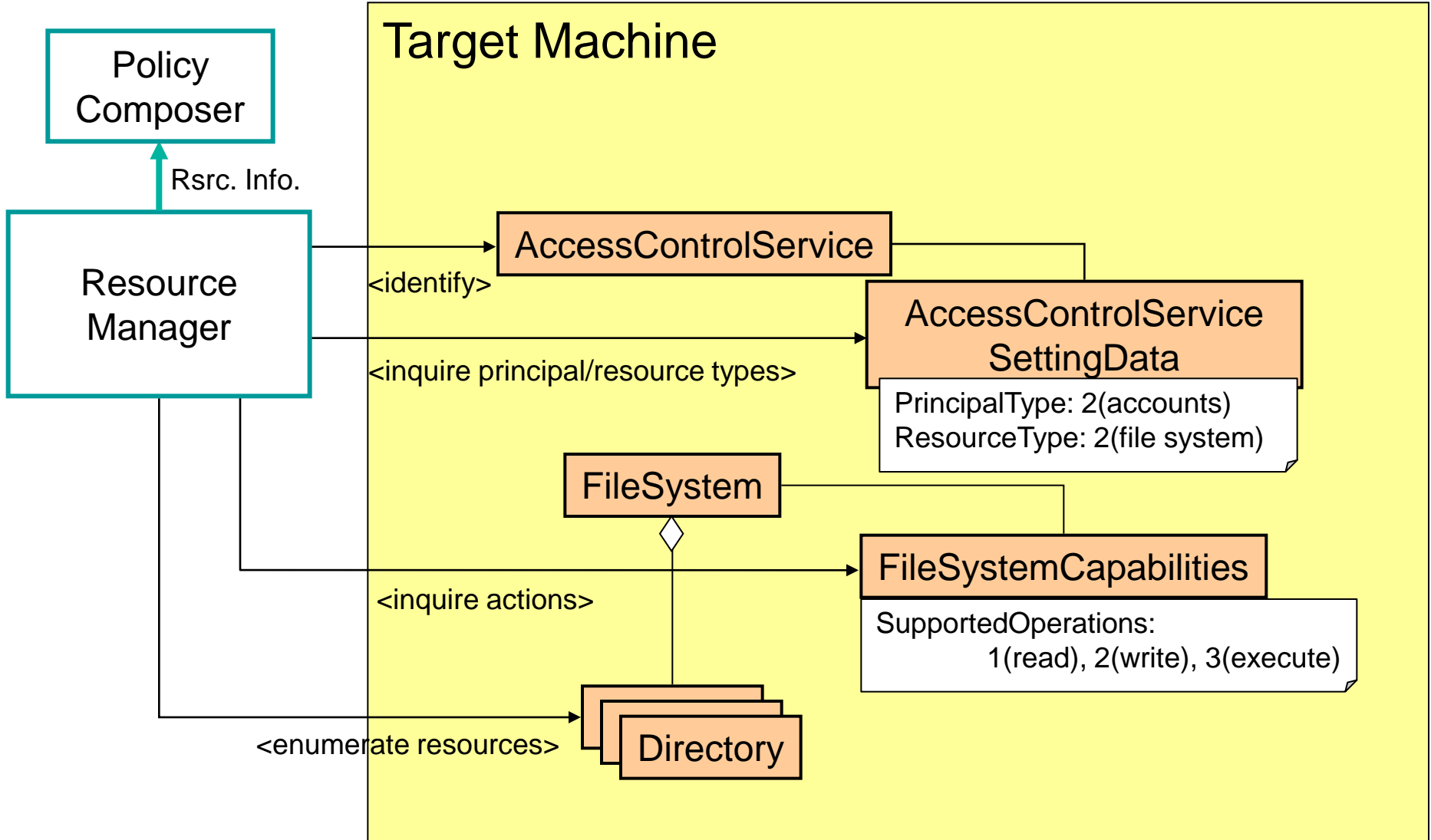
# Proposed model components

- CIM\_AccessControlService
  - Represents access control policy enforcement point
- CIM\_AccessControlServiceSettingData
  - Represents granularity of access control at the point
- CIM\_xxxCapabilities
  - Represents operation types of targeted resource xxx  
e.g. CIM\_FileSystemCapabilities
- CIM\_PolicyTransferService
- CIM\_TransferServiceAccessPoint
- CIM\_PolicyActivationService
- CIM\_AccessControlPolicy

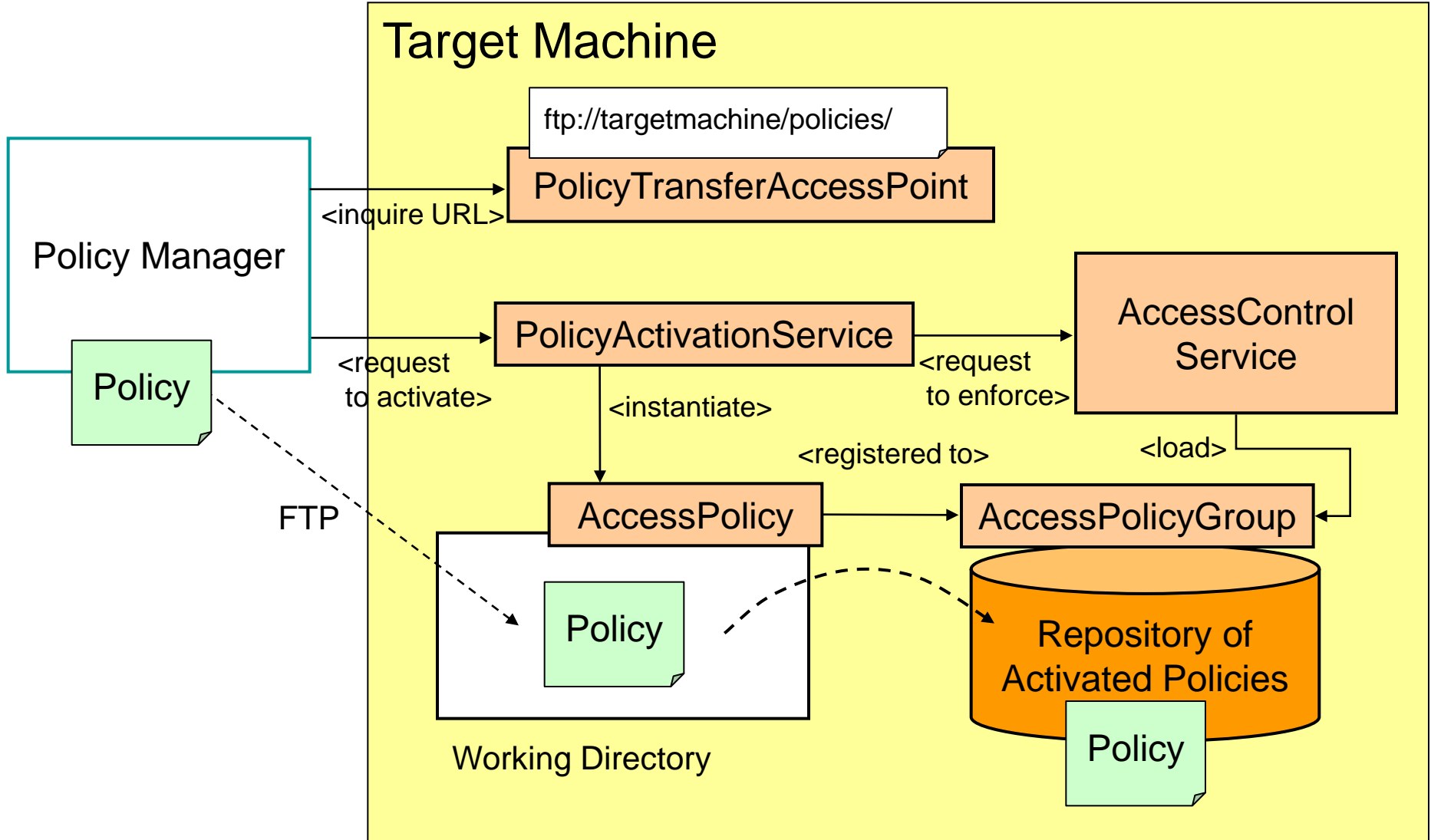
# CIM schema of IAM Profile



# Use case: Resource information collection



# Use case: Distribution and activation of access control policies



# Standardization status

- The CIM schema proposed in the profile has been revised, and now in review of Sub-schema Committee.
- Key issues:
  - Remodeling for more generality:  
Original: CIM\_ReferenceMonitor (captured only software modules)  
Revised: CIM\_AccessControlService (captures hardware modules as well)
  - Resolving ambiguities:  
Original: CIM\_PolicyTransferService (seemed to represent both a URL and a network service)  
Revised: CIM\_PolicyTransferServiceAccessPoint (represents a URL of policy distribution only)

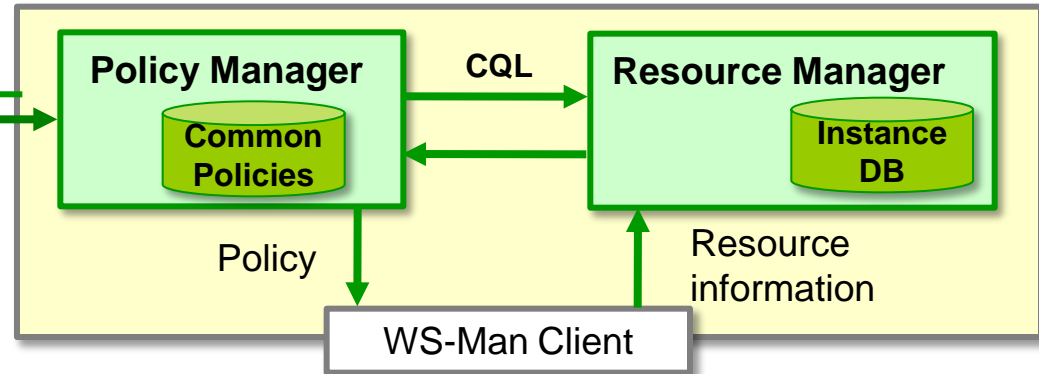
# Profile implementation

# IAM profile implementation

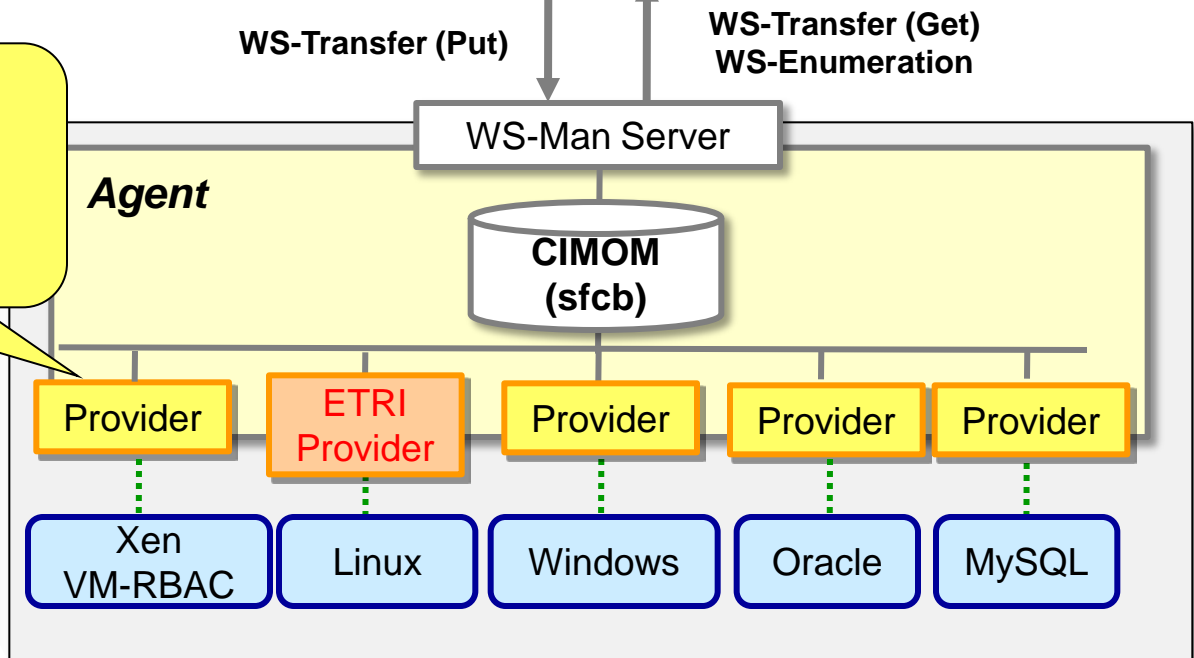
Security Manager



*Integrated Access Control Manager*



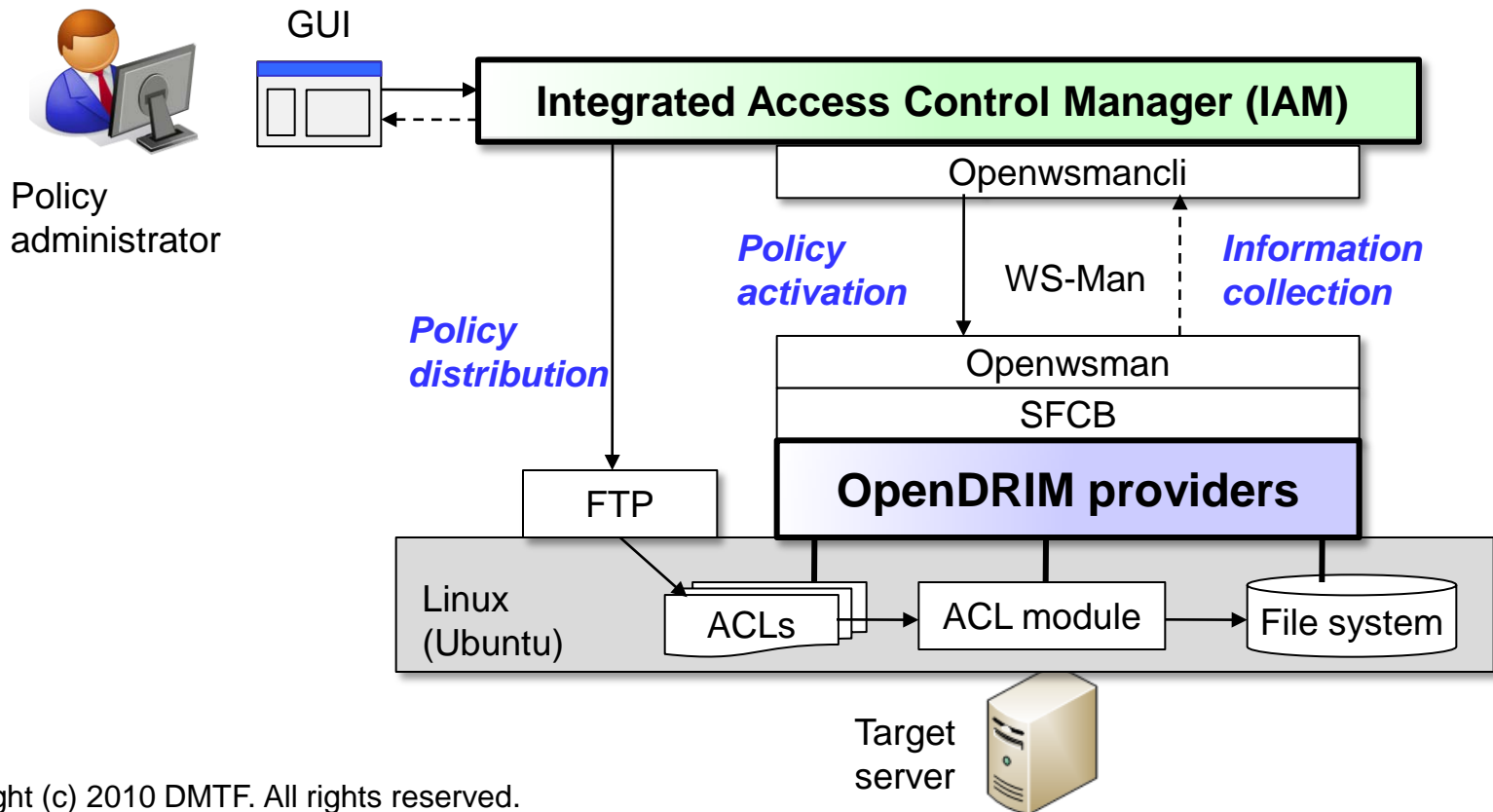
**Provider enhancement for access policy setting**



# Collaboration with ETRI

- Experimental implementation of IAM Profile has been done by ETRI\* as a part of OpenDRIM providers, handling POSIX 1.e file ACLs.

\*Electronics and Telecommunications Research Institute



# What is OpenDRIM Project?

- Research Goals:
  - Develop distributed resource information management technologies & environment based on CIM/WBEM standards of DMTF.
  - Promote CIM-based open source software in Northeast Asia. Achievements are available at: <http://sourceforge.net/projects/opendrim/>

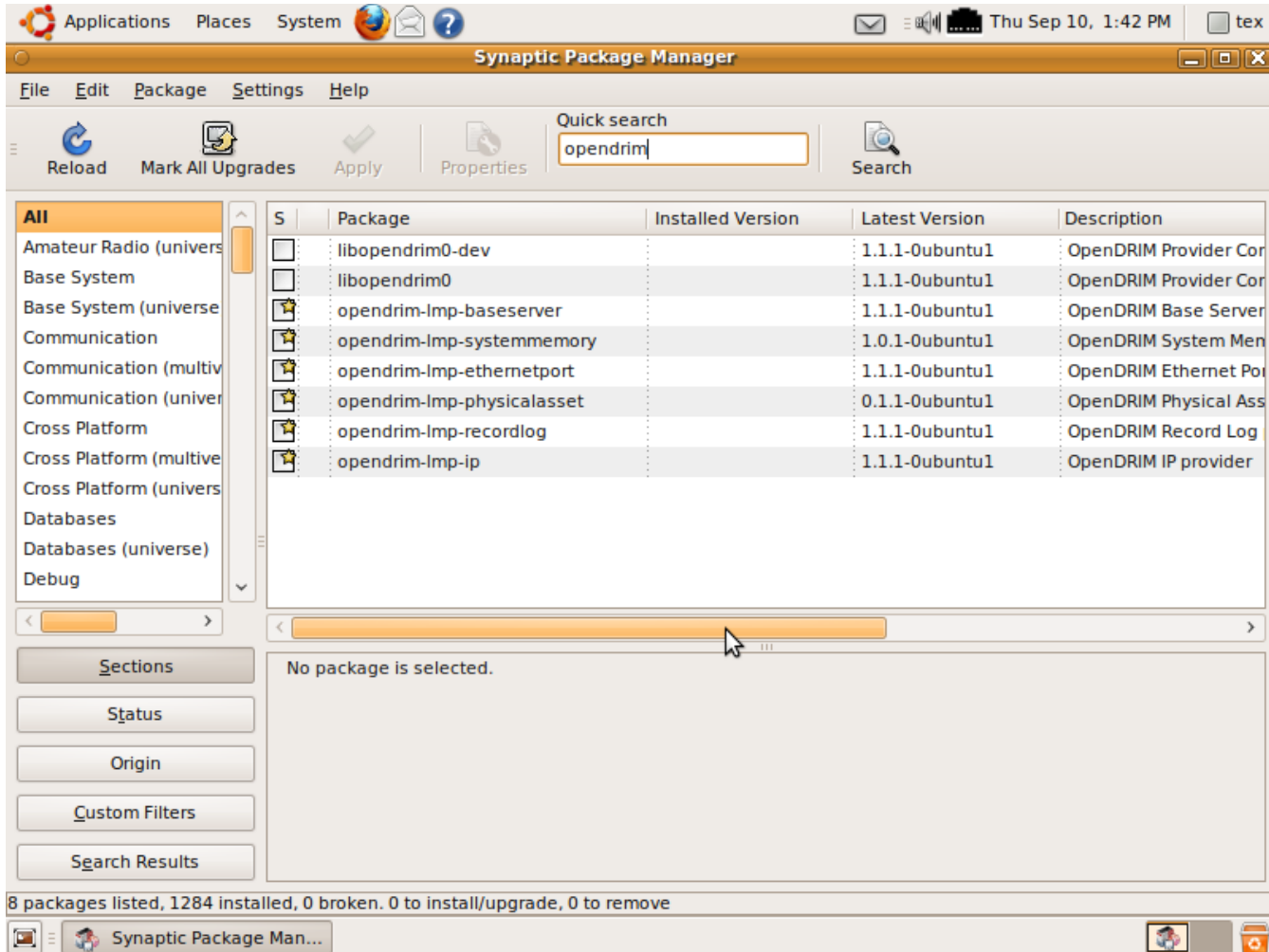


# Implementation status

- Finished implementing the WIP version of IAM Profile.
- Remote access test from IAM server in Kawasaki, Japan to targeted Linux server in Daejeon, Korea has been done successfully.
- The Linux IAM provider will be available as a part of OpenDRIM 2010 version.

# OpenDRIM in Ubuntu

- Ubuntu Karmic ('09.10) adopted OpenDRIM results



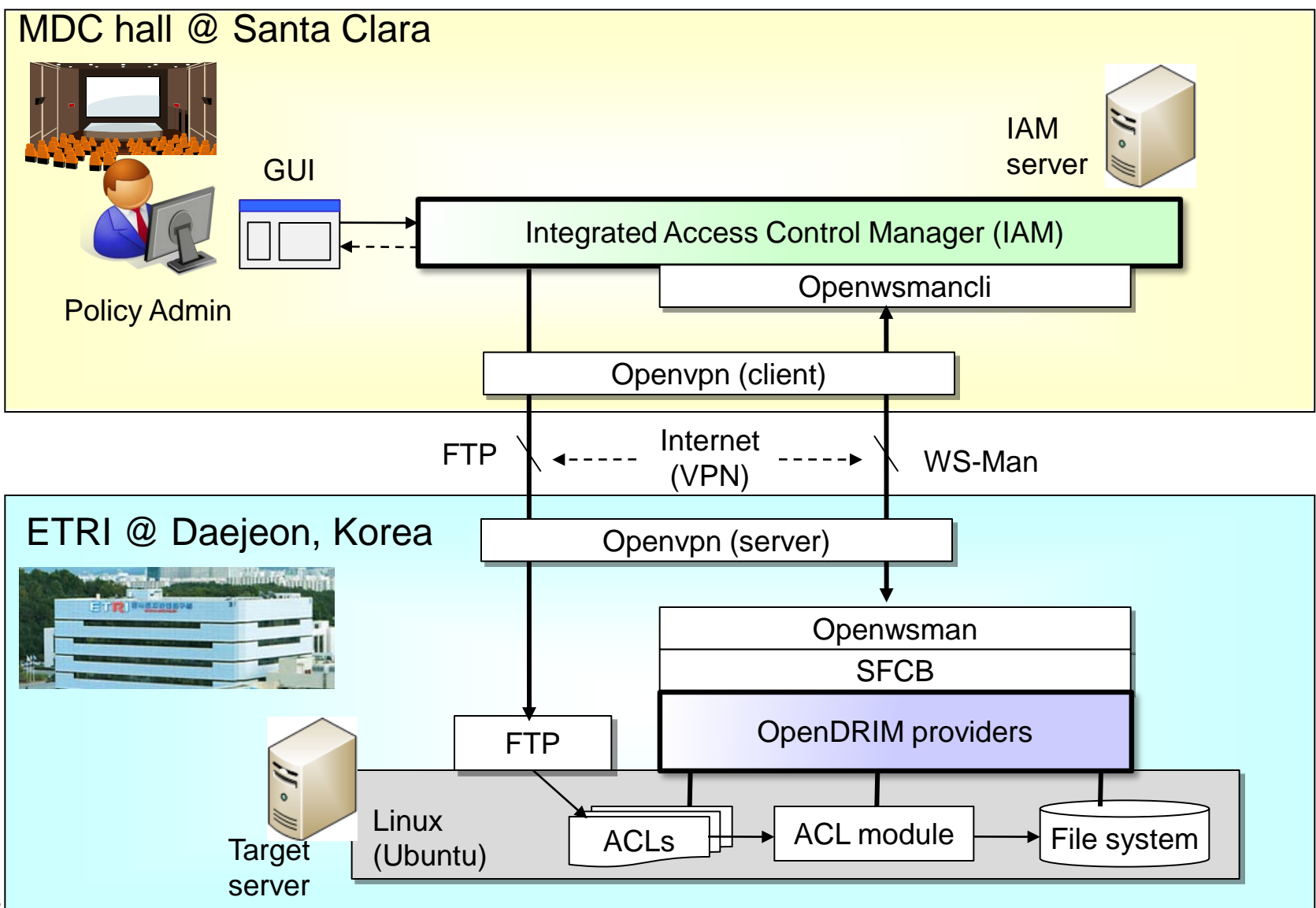
The screenshot shows the Synaptic Package Manager window with a search for 'opendrim'. The search results table is as follows:

S	Package	Installed Version	Latest Version	Description
<input type="checkbox"/>	libopendrim0-dev		1.1.1-0ubuntu1	OpenDRIM Provider Cor
<input type="checkbox"/>	libopendrim0		1.1.1-0ubuntu1	OpenDRIM Provider Cor
<input checked="" type="checkbox"/>	opendrim-imp-baseserver		1.1.1-0ubuntu1	OpenDRIM Base Server
<input checked="" type="checkbox"/>	opendrim-imp-systemmemory		1.0.1-0ubuntu1	OpenDRIM System Men
<input checked="" type="checkbox"/>	opendrim-imp-ethernetport		1.1.1-0ubuntu1	OpenDRIM Ethernet Po
<input checked="" type="checkbox"/>	opendrim-imp-physicalasset		0.1.1-0ubuntu1	OpenDRIM Physical Ass
<input checked="" type="checkbox"/>	opendrim-imp-recordlog		1.1.1-0ubuntu1	OpenDRIM Record Log
<input checked="" type="checkbox"/>	opendrim-imp-ip		1.1.1-0ubuntu1	OpenDRIM IP provider

8 packages listed, 1284 installed, 0 broken, 0 to install/upgrade, 0 to remove

# Demonstration

# Demo system configuration



# Future work

- Continue final standardization work
  - Update the profile according to Schema Subcommittee comments and review it again in Policy WG.
- Model upgrade to get related to other standards
  - CIM-SPL based policies
  - ID Management Profile
  - Policy distribution via OVF metadata
  - Cloud service provider interface

# Acknowledgement

- IAM implementation work is a part of the Secure Platform project supported by Japanese ministry of Economy, Trade and Industry, and Association for Super-Advanced Electronics Technologies.
- The IAM architecture and reference monitor models were developed with much help of T. Hatakeyama, I. Igarashi, Y. Ezaki, T. Aizawa, and S. Onzuka, of Fujitsu Limited.
- The implementation of OpenDRIM providers was done by C. Ahn of ETRI and G. Bottex of UX Systems.

# Q/A Session

Thank you!