Key Management with Policy-based Access Control

Christian Cachin* Divay Bansal† Günter Karjoth*

27 April 2012

A key management system performs vital functions for the secure operation of cryptographic systems, in particular for governing the lifecycle of cryptographic credentials. Although usually proprietary today and tied to particular hardware incarnations, such key-management systems are expected become network-enabled, open, and standard-based in the future. They will address the needs of cryptographically protected cloud computing services; more importantly, the key-management systems of the future will operate from the cloud.

Open key-management systems need a common language. The recently developed OASIS Key Management Interoperability Protocol (KMIP) standard establishes a single, comprehensive protocol for the communication between enterprise key-management systems and cryptographic services. It was created by an industry group with the goal of simplifying key-management processes and reducing the associated operational costs. Products of several vendors support KMIP as of today.

Access control plays a crucial role for the security of network-based key management. Modern access-control systems are policy-based and permit a variety of operational modes and deployment models; for enterprise-wide deployment a careful separation of policy administration, access-control decision, and policy enforcement is important. This has been recognized in the work leading to the XACML standard (eXtensible Access Control Markup Language). XACML defines a declarative access control policy language implemented in XML, together with a processing model that describes how to evaluate authorization requests according to the rules defined in policies.

In this presentation we discuss how to integrate a policy-based access control system using XACML with a KMIP-based key management server. We formulate an access-control model for KMIP and discuss the semantics of various KMIP operations. Based on these findings, we present formal policies and their implementation in XACML.

We have also realized a prototype system that integrates key management with policy-based access control according to the SOA (service-oriented architecture) paradigm. The prototype evaluates and enforces XACML-based policy for key management on a KMIP key-management server. We discuss the design of the authorization mechanism and its integration with KMIP.

*IBM Research - Zurich, CH-8803 Rüschlikon, Switzerland. {cca,gka}@zurich.ibm.com

†Adnovum Informatik AG, CH-8005 Zurich. divay.bansal@adnovum.ch. Work done at IBM Research - Zurich in collaboration with ETH Zurich.