Implementing a Standards Based Dynamic Key Framework to Complement PKI

Abstract Prepared for:

Workshop on Cryptography

for Emerging Technologies and Applications

November 7-8, 2011

Information Technology Laboratory

National Institute of Standards and Technology

Response Submitted By:

TecSec Services, Inc.
12950 Worldgate Drive
Suite 100,
Herndon, VA 20170
September 22, 2011

Contact Person:

Ron Parsons
RParsons@tecsec.com
Cell: 301-639-5510

In today's ubiquitously networked world with applications springing up hourly in support of mobile banking, cloud computing, and multiple forms of remote access, the need has never been greater to identify authorized users, protect and control sensitive information assets, and manage access to information, in compliance with privacy statutes and regulations. Securing the Network has limitations; to compensate, securing information that is supported by the Network takes another step when looking at an overall security paradigm. In regards to encryption, this added dimension to protecting information can result in moving us rapidly into the creation and management of an object level, dynamic key solution.

As has historically been the case, key management continues to be a fundamental challenge. There are a variety of key management frameworks. A Public key (static key) framework is well defined for fundamental identity management, and can be used for encryption. A Dynamic key framework can enable active attribute based, differential access to any digital object. Identity can include local rights to access information for which a Dynamic key framework can be considered complimenting Identity and resulting in a complete solution.

The technology is available to create self protecting data objects. Specifically objects that are data label aware; which in turn enables services to be based on that awareness, and also requires a more ubiquitous key management solution. This approach, when widely deployed and appropriately managed, makes transmission a matter of availability and storage a matter of convenience. This approach supports the benefits of cloud computing, but now with security embedded. Self protecting data objects could support multiple levels of information on a common platform and address differential access enforced by encryption to content, information sharing, and multi-user access control.

Static key systems can have scale limitations when applied broadly for the needs of roles, attributes, labels, and permissions. The dynamic key framework to support this level of key distribution and management must have a broader use of scale, and the framework must accommodate rekey which can be an issue for static keys. The goal is to have a framework that is standards-based to maximize interoperability and to be compatible with mobile and cloud markets.

An enterprise can be treated as a unit, and that enterprise will be able to secure all of the information assets whether the data is in transit or at rest. A framework exists that includes a defined collection of NIST encryption standards and has been demonstrated.