Two Worlds, One Smart Card: An Integrated Solution for Physical Access and Logical Security Using PKI on a Single Smart Card*

Jaap-Henk Hoepman[1,2] and Geert Kleinhuis[1]

[1] TNO Information and Communication Technology
P.O. Box 1416, 9701 BK Groningen, The Netherlands
jaap-henk.hoepman@tno.nl, geert.kleinhuis@tno.nl
[2] Institute for Computing and Information Sciences
Radboud University Nijmegen
P.O. Box 9010, 6500 GL Nijmegen, The Netherlands
jhh@cs.ru.nl

Abstract. We present a use case of the introduction of a large scale Public Key Infrastructure (PKI) environment in an incumbent telecommunications company in The Netherlands. The main characteristics of the case are the integration of an existing physical access facility with a PKI environment for logical security of the company ICT infrastructure. In fact, both are accessed using a single (smart) company card. The purpose was to implement a high level of security, within the practical constraints at hand, and to reach a level of *reduced sign-on* for company employees. This integration poses numerous challenges. In this article we describe how PKI is actually introduced to support authentication, signing and encryption services for its employees.

18.000 personalised smart cards with PKI were issued, controlling access to over 1500 buildings, fitted with in total more than 6000 smart card readers. The smart cards also controlled access to 14.000 personal workstations both desktops and laptops (each fitted with a contact smart card reader), with access to over a 1000 different applications.

Keywords: PKI, Access control, smart card, reduced sign-on.

1 Introduction

To grant their employees access to office buildings and plants, companies these days issue their employees a (smart) card that is both an identity card as well as an electronic key. Usually, this key can be used without any further authentication to enter the premises. Few companies would require their employees to enter a PIN code as well as presenting their card to open a door, for instance. Such a system for access control to physical objects has been known and in use for quite some time. It grants or denies access to office buildings and sectors within such buildings in a convenient and uniform manner.

* Id: pki-geert.tex,v 1.7 2007/04/16 11:56:59 jhh Exp.

J. Lopez, P. Samarati, and J.L. Ferrer (Eds.): EuroPKI 2007, LNCS 4582, pp. 236–247, 2007.

However, access control to objects in the digital domain (like computing systems, company applications and information) is usually not handled in the same uniform manner. They often have their own access control mechanism. This is a burden on employees. Consider, for example, the multitude of user names and passwords an office worker may have to enter during the course of a single working week.

This difference can be explained partially by the fact that implementing access control for digital objects is considered more difficult than implementing access control for physical objects. It is also caused by the fact that no single system for uniformly handling authentication and access control is in widespread use today. This is true because Kerberos[NT94], and other methods of single sign-on, largely remain academic exercises, even though (a variant of) Kerberos is part of the Microsoft code base.

This paper describes a use case where all employees of a large telecommunications company in the Netherlands were issued with a *single* smart card to obtain access to both physical and digital objects. Security, authentication and access control in the digital domain is based on a Public Key Infrastructure (PKI) (cf. [AL99, RFC 3280, ES00]).

There were three reasons to use a single smart card for access control in the digital as well as the physical domain.

1. There were high security requirements concerning the general handling of digital information, as well as the authentication of the actor in a workflow.
2. The aim was to arrive at a more user-friendly system of *reduced sign-on*.
3. It was desirable to reduce cost through a simpler and unified access control management organisation.

The latter point could only be achieved through a scalable solution that was usable for a large population of workers with varying skills and technical background. This solution is documented in this paper.

The remainder of this paper is structured as follows. We first discuss the issue of how many keys are needed for physical and logical access control. Section 3 describes the functional architecture. Details on the use case are presented in Section 4. The concrete architecture is given after that. We finish with an example of how an employee is entered into the system (section 6) and conclude with user experience, security issues and conclusions.

2 How Many Keys Do We Need?

A number of international information security organisations have studied the trend that security increasingly crosses the confines of individual objects, towards a more holistic, integrated, approach. They concluded that the convergence of security within (large) enterprises is rapidly emerging and enterprises need to adapt accordingly [Ham05]. In fact, this convergence may cover all the objects within a value chain, and extends through physical as well as informational goods.