A thesis submitted for a master of science degree in computer security of ENST (Telecom Paris)

IMPLEMENTING AN INTERNAL PUBLIC KEY INFRASTRUCTURE WITHIN NATEXIS BANQUES POPULAIRES

Constantin Yamkoudougou, Security Engineer

23 novembre 2002

1 Aknowledgements

I specially want to adress my heartfelt thanks to :
Bernard LE FEBVRE DE NAILLY, Director of Natexis Architecture Services who accepted my application for an intership focussing on an internal public key infrastructure .
Céline PEROT, she is responsible of the security team called ATIA-sécurité within Natexis and in spite of important responsabilities did get a bit time to organize my internship.
I also want to thank Vincent REY the project manager with whom I have worked on ACI for so much advices on how to choose a suitable solution..
Special thanks to Arnault MICHEL, a software architecture ; he is also expert on java and was really helpfull when I needed to get started with the working environnement and was a tips' supplier when I was ready to develop a suitable solution according to the Natexis requirements.
Endly, I want to thank all the members of Natexis security team for their precious help during all the internship.

2 Introduction

The familly of TCP/IP protocols was originally designed to meet the needs for communication without worrying about problems of security. Several protocol layers were developed thereafter to patch its many break-ins. As an example I can quote SSL, IPsec and S/MIME. The whole of all these additive stacks ensure the security of the communications in term of authenticity, confidentiality, integrity, and non-repudiation on the basis of public key cryptography. Thus, the security of these protocols depends now on the security of certificates provider which is the public key infrastructure. As a result, public key infrastructure became a leading entity in the heart of computer security.

This document is about the implementation of such infrastructure for internal uses at NATEXIS. It was written as a thesis to validate a Master of science degree in computer and network security at the National School of telecommunications of Paris (ENST - Telecom Paris). The purpose of the given public key infrastructure was to issue certificates for a java-based production environment servers involved in a important project.

The first part of this report is devoted to the presentation of the company within which this work took place : Natexis Banques Populaires which counts in this moment more than 11000 collaborators. This part describes in addition to its current activities, the organization of the security service and is completed by the definition of the needs which led to the implementation of an internal infrastructure of public key.

The second part deepens the training context and approaches the technology of the public key infrastructure by explaining the reader the basic concepts of cryptography with public key and the role of its various components.

The given public key infrastructure projet was in fact a part of a great one about many type of x509 standard certificates issueing. The functional specifications of this great projects are described here. Chapter 9 tells you what kind of scenario has been emphasized.

Note : For reason of confidentiality of an important part of my job, I don't go further in details in this public report. I apologize for people in need of what can be a suitable technology or organization for them and I am inviting them to send me a message to this given address : constantin.yamknaz at free.fr).