AAA

J. Scheerder[*] jeroenscheerder@on2it.eu

L.J. Koning[*] lieuwejankoning@on2it.eu

October 25, 2007

1 Introduction

Authentication, authorization and accounting – the so-called triple A services – are gaining ever more prominence in IT security. The holy grail of combining maximal strength on the one hand with minimal user grief on the other has not yet been found however.

2 Goal

Description and proof of concept realization of a practical authentication infrastructure which should ideally be totally platform-independent, but at least deeply platform-agnostic. Particularly interesting points of attention are:

- public key authentication (PKI) and the related technical and organisatorial challenges regarding key distribution and key revocation;
- single sign-on;
- multi-factored authentication, considering not only PKI-based approaches, but also one-time password (OTP) strategies, use of (hardware) tokens as aids for PKI or OTP, integration with existing authentication and directory services, and with potential use of biometry;
- authorization and delegation of authorization, technological and organisational;
- logging and reporting/auditing of access to restricted data.

3 Technology

ON2IT is an IBM ISS– as well as a RSA Security partner. In line with these partnerships IBM's Tivoli Identity Manager and Tivoli Access Manager offer enterprise-level single sign-on and permission control. RSA Security's portfolio comprises integration of directory services and challenge/response-based OTP, using hardware tokens. The entire range of open standards based technology is available as building blocks in addition.

4 Task

Design, describe and implement a platform-insensitive infrastructure foor authentication, delegation, authorization and accounting.

[*] ON2IT b.v., Waardenburg, The Netherlands.