

# Implementation of software tools for the medium-size Certification Authority — X.509 Authentication Services

By Wenming Zhao – wzhao@gmu.edu

## 1. Introduction:

Security, authentication and access control are the vital features that must be present in any communication network. The problem of designing correct protocols for Authentication and Key management is particularly difficult to solve in any environment.

X.509 defines a framework for the provision of authentication services by the X.500 directory, based on the use of public-key cryptography and digital signatures. The directory is, in effect, a server or distributed set of servers that maintains a database of information about users,

X.509 is an important standard because the X.509 certificate format is used in variety context, such as S/MIME, IP Security, and SSL/TLS and SET.

## 2. Objective

Implementing the software applications to generate certificates by the client's request to provide services for the following environment:

- 1) Require that client systems authenticate themselves to servers, but trust the client system concerning the identity of its user;
- 2) Require the user to prove identity for each service invoked. Also require that servers prove their identity to clients.

## 3. Language, platform, and compiler used for a primary implementation. The program portability to other platforms

This software tool will be implemented by JAVA programming language and database, either SQL Server 2000 or Access. Web technology, which includes ASP, HTML and/or XML, is included to implement the distributed system services. The platform, I preferred, is Microsoft Windows 2000/XP.

Compiler: JAVA jdk 1.4.2, Microsoft IE, as well as gnu C/C++ (if needed) under Windows platform.

Additional software may be required (e.g., a library of arithmetic operations on large numbers, RSA Reference Library, etc.), determined in the progress.

## 4. Detailed specification of the input and output of the program(s), including the exact format of input/output files.

This software application implements following functions for the medium-size Certification Authority (CA):

- 1) The initial Certificate Revocation List (CRL) is produced;
- 2) Login on the CA web site;
- 3) Generate certificate requests;
- 4) CA generates certificates, as well as initial Certificate Revocation List;
- 5) Online validation of certificates
- 6) Download client certificates, as well as CRL

**5. Brief description of the function performed by the program(s), including any specific references to standards and detailed descriptions of algorithms in the literature.**

Based on the X.509 standard, the separate basic function should be performed. Such as:

- 1) Generating RSA key;
- 2) Hashing message by hash function;
- 3) Generating certificate;
- 4) Encryption;
- 5) Decryption;
- 6) Verify certificate;

**6. Procedures for testing the functionality and performance of the program(s). The source of test vectors.**

- 1) Performing the following function tests:
- 2) Login on CA web site and send request for certificate;
- 3) Download certificates;
- 4) Validating the certificates

Theoretical testing techniques will be performed, such as unit testing, system testing (black box testing).

**7. Plan of experiments to be performed using the program(s).**

Using one and/or two computers to perform the system experiments on the platform of MS Windows operating system.

**8. A list of possible areas, where the specification can change depending on the progress of the project.**

Analysis on protocols and performance will be hopefully done.

**9. List of literature.**

- 1) Lecture notes on ECE 646.
- 2) William Stallings, Cryptography and Network Security: Principles and Practice.

- 3) Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, Handbook of Applied Cryptography
- 4) Bryant, W. Designing an Authentication System: A Dialogue in Four Scenes
- 5) Kohl, J.; Neuman, B.; and Ts'o, T. "The Evolution of the Kerberos Authentication Service." In Brazier, F., and Johansen, D. Distributed Open Systems. Los Alamitos, CA: IEEE Computer Society Press, 1994.
- 6) Tung, B. Kerberos: A Network Authentication System. Reading, MA: Addison-Wesley, 1999
- 7) <http://web.mit.edu/kerberos/>
- 8) <http://web.mit.edu/kerberos/www/papers.html>
- 9) <http://www.ietf.org-ids.by.wg-pkix.html>
- 10) <http://www.pyca.de/>
- 11) <http://www.leg.state.nv.us/NRS/NRS-720.html>
- 12) relevant web site on procedure of implementation

Note that the above list is not exhaustive and more will be added as required.