Electrical Engineering Department University of Delaware
Technical Report 03-2-1 February 2003

# The Autokey Security Architecture, Protocol and Algorithms

David L. Mills


## Abstract

This document describes the Autokey security model for authenticating servers to clients using the Network Time Protocol (NTP) and public key cryptography. its design is based on the premise that IPSEC schemes cannot be adopted intact, since that would preclude stateless servers and severely compromise timekeeping accuracy. In addition, PKI schemes presume authenticated time values are always available to enforce certificate lifetimes; however, cryptographically verified timestamps require interaction between the timekeeping function and authentication function in ways not yet considered by the IETF.

This Document includes the Autokey requirements analysis, design principles and protocol specification. A detailed description of the protocol states, events and transition functions is included. A prototype of the Autokey design based on this document has been implemented, tested and documented in the NTP Version 4 (NTPv4) software distribution for Unix, Windows and VMS at http://www.ntp.org.


Keywords: network security, public-key infrastructure, digital signatures, computer time synchronization

Sponsored by: DARPA Information Technology Office Order G409, Contract F30602-98-1-0225, and Digital Equipment Corporation Research Agreement 1417.

Table of Contents


1. Introduction ..... 1
2. NTP Security Model ..... 2
3. Approach ..... 4
4. Autokey Cryptography ..... 5
5. Autokey Operations ..... 7
6. Public Key Signatures and Timestamps ..... 10
7. Autokey Protocol Overview ..... 11
8. Autokey State Machine ..... 12
   - 8.1 Status Word ..... 12
   - 8.2 Host State Variables ..... 14
   - 8.3 Client State Variables (all modes) ..... 16
   - 8.4 Server State Variables (broadcast and symmetric modes) ..... 17
   - 8.5 Autokey Messages ..... 17
     - 8.5.1 Association Message (ASSOC) ..... 17
     - 8.5.2 Certificate Message (CERT) ..... 17
     - 8.5.3 Cookie Message (COOKIE) ..... 18
     - 8.5.4 Autokey Message (AUTO) ..... 18
     - 8.5.5 Leapseconds Table Message (LEAP) ..... 18
     - 8.5.6 Sign Message (SIGN) ..... 18
     - 8.5.7 Identity Messages (IFF, GQ, MV) ..... 18
   - 8.6 Protocol State Transitions ..... 18
     - 8.6.1 Server Dance ..... 19
     - 8.6.2 Broadcast Dance ..... 19
     - 8.6.3 Symmetric Dance ..... 20
9. Error Recovery ..... 21
10. References ..... 23
A. Packet Formats ..... 25
   - A.1 Header Field Format ..... 25
   - A.2 Extension Field Format ..... 25
B. Cryptographic Key and Certificate Management ..... 28
C. Autokey Error Checking ..... 30
   - C.1 Packet Processing Rules ..... 30
   - C.2 Timestamps, Filestamps and Partial Ordering ..... 31
D. Security Analysis ..... 33
   - D.1 Protocol Vulnerability ..... 33
   - D.2 Clogging Vulnerability ..... 34
E. Identity Schemes ..... 36

E.1 Certificates ..... 36
E.1.1 Basic Constraints ..... 36
E.1.2 Key Usage ..... 37
E.1.3 Extended Key Usage ..... 37
E.1.4 Subject Key Identifier: ..... 37
E.2 Private Certificate (PC) Scheme ..... 37
E.3 Trusted Certificate (TC) Scheme ..... 38
E.4 Schnorr (IFF) Scheme ..... 38
E.5 Guillard-Quisquater (GQ) Scheme ..... 40
E.6 Mu-Varadharajan (MV) Identity Scheme ..... 41
E.7 Interoperability Issues ..... 44
F. File Examples ..... 46
F.1 RSA-MD5cert File and ASN.1 Encoding ..... 46
F.2 RSAkey File and ASN.1 Encoding ..... 47
F.3 IFFpar File and ASN.1 Encoding ..... 47
G. ASN.1 Encoding Rules ..... 49
G.1 COOKIE request, IFF response, GQ response, MV response ..... 49
G.2 CERT response, SIGN request and response ..... 49

List of Figures

Figure 1. Receiving Messages....5
Figure 2. NTPv4 Autokey....6
Figure 3. Constructing Key List....7
Figure 4. Transmitting Messages....7
Figure 5. Status Word....12
Figure 6. NTP Header Format....25
Figure 7. NTP Extension Field Format....26
Figure 8. Private Certificate (PC)Identity Scheme....37
Figure 9. Trusted Certificate (TC) Identity Scheme....38
Figure 10. Schnorr (IFF) Identity Scheme....39
Figure 11. Guillard-Quisquater (GQ) Identity Scheme....40
Figure 12. Mu-Varadharajan (MV) Identity Scheme....42

## List of Tables

Table 1. IFF Identity Scheme Parameters ..... 39
Table 2. GQ Identity Scheme Parameters ..... 41
Table 3. MV Scheme Server Parameters ..... 42
Table 4. MV Scheme Client Parameters ..... 42