

Survivable, Real Time Network Services

Final Technical Report

Defense Advanced Research Projects Agency
Contract F30602-98-1-0225, DARPA Order G409/J175

David L. Mills
University of Delaware

1 April 2003

Abstract

This document is the Final Technical Report on Contract F30602-98-1-0225, DARPA Order G409/J175. It contains material reformatted from the web pages that are the intended final product of this project. The web pages contain an extensive network of links embedding them not only in the framework of this project, but in the framework of other related projects and reference material. The links are not available in this published document.

The text in this document is generally taken verbatim from the web pages with certain minor changes to enhance readability in paper medium. The figures are taken directly from the pages, but rendered in greyscale. The equations have been redone to conform to software publishing requirements. The reference and bibliography material has been moved to the end of the base document.

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

Table of Contents

1.	Introduction.....	1
1.1	Research Plan.....	1
1.2	Approach.....	2
1.3	Deliverables	3
1.4	Statement of Work	4
2.	Autonomous Authentication	4
2.1	Brief Description of Work and Results	5
2.2	Leapseconds Table	6
2.3	Present Status	6
2.4	Future Plans	6
3.	Autokey Protocol	6
3.1	Certificate Trails	7
3.2	Secure Groups.....	9
3.3	Identity Schemes.....	10
3.4	Key Management.....	13
4.	Identity Schemes.....	13
4.1	Schnorr (IFF) Cryptosystem	14
4.2	Guillou-Quisquater (GQ) Cryptosystem.....	15
4.3	Mu-Varadharajan (MV) Cryptosystem	16
5.	References and Bibliography.....	19
A.	Program Manual Page: Authentication Support	21
A.1	Symmetric Key Cryptography	22
A.2	Public Key Cryptography	22
A.3	Operation	23
A.4	Key Management.....	24
A.5	Authentication Commands	24
A.6	Error Codes.....	26
A.7	Files.....	27
A.8	Leapseconds Table	27
B.	Program Manual Page: ntp-keygen Program.....	29
B.1	Synopsis	29
B.2	Description.....	29
B.3	Running the program	30
B.4	Trusted Hosts and Groups.....	31
B.5	Identity Schemes.....	31
B.6	Command Line Options.....	33
B.7	Random Seed File.....	34

B.8	Cryptographic Data Files	34
B.9	Bugs	35
C.	Autokey Protocol Specification	36
C.1	NTP Security Model	37
C.2	Approach.....	39
C.3	Autokey Cryptography	40
C.4	Autokey Operations	42
C.5	Public Key Signatures and Timestamps.....	45
C.6	Autokey Protocol Overview	46
C.7	Autokey State Machine.....	47
C.8	Status Word.....	47
C.8.1	Host State Variables	49
C.8.2	Client State Variables (all modes).....	51
C.9	Autokey Messages	52
C.9.1	Association Message (ASSOC)	52
C.9.2	Certificate Message (CERT).....	52
C.9.3	Cookie Message (COOKIE).....	53
C.9.4	Autokey Message (AUTO).....	53
C.9.5	Leapseconds Table Message (LEAP)	53
C.9.6	Sign Message (SIGN).....	53
C.9.7	Identity Messages (IFF, GQ, MV)	53
C.10	Protocol State Transitions	53
C.10.1	Server Dance.....	54
C.10.2	Broadcast Dance	54
C.10.3	Symmetric Dance.....	55
C.11	Error Recovery.....	56
C.12	References.....	58
D.	Packet Formats.....	60
D.1	Header Field Format	60
D.2	Extension Field Format.....	60
E.	Cryptographic Key and Certificate Management	63
F.	Autokey Error Checking	65
F.1	Packet Processing Rules	65
F.2	Timestamps, Filestamps and Partial Ordering	66
G.	Security Analysis	68
G.1	Protocol Vulnerability.....	68
G.2	Clogging Vulnerability	69
H.	Identity Schemes.....	71

H.1	Certificates	71
	H.1.1 Basic Constraints	71
	H.1.2 Key Usage.....	72
	H.1.3 Extended Key Usage.....	72
	H.1.4 Subject Key Identifier:	72
H.2	Private Certificate (PC) Scheme	72
H.3	Trusted Certificate (TC) Scheme	73
H.4	Schnorr (IFF) Scheme.....	73
H.5	Guillard-Quisquater (GQ) Scheme	75
H.6	Mu-Varadharajan (MV) Identity Scheme	76
H.7	Interoperability Issues.....	79
I.	File Examples	81
	I.1 RSA-MD5cert File and ASN.1 Encoding.....	81
	I.2 RSAkey File and ASN.1 Encoding.....	82
	I.3 IFFpar File and ASN.1 Encoding	82
J.	ASN.1 Encoding Rules	84
	J.1 COOKIE request, IFF response, GQ response, MV response.....	84
	J.2 CERT response, SIGN request and response.....	84

List of Figures

Figure 1.	NTP Secure Group.....	8
Figure 2.	Nested Secure Groups.....	9
Figure 3.	Multiple Secure Groups	10
Figure 4.	PC Identity Scheme	11
Figure 5.	Certificate Trail.....	11
Figure 6.	IFF Identity Scheme.....	12
Figure 7.	GQ Identity Scheme.....	12
Figure 8.	MV Identity Scheme.....	12
Figure 9.	Client-Server Message Exchange	13
Figure 10.	IFF Protocol	15
Figure 11.	GQ Protocol	16
Figure 12.	MV Protocol	17
Figure 13.	Receiving Messages.....	40
Figure 14.	NTPv4 Autokey	41
Figure 15.	Constructing Key List.....	42
Figure 16.	Transmitting Messages	42
Figure 17.	Status Word.....	47
Figure 18.	NTP Header Format.....	60
Figure 19.	NTP Extension Field Format	61
Figure 20.	Private Certificate (PC)Identity Scheme.....	72
Figure 21.	Trusted Certificate (TC) Identity Scheme.....	73
Figure 22.	Schnorr (IFF) Identity Scheme	74
Figure 23.	Guillard-Quisquater (GQ) Identity Scheme.....	75
Figure 24.	Mu-Varadharajan (MV) Identity Scheme	77

List of Tables

Table 1.	IFF Cuckoo Structure.....	15
Table 2.	GQ Cuckoo Structure.....	16
Table 3.	MV Server Cuckoo Structure	17
Table 4.	MV Client Cuckoo Structure	17
Table 5.	IFF Identity Scheme Parameters.....	74
Table 6.	GQ Identity Scheme Parameters.....	76
Table 7.	MV Scheme Server Parameters	77
Table 8.	MV Scheme Client Parameters.....	77