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

List of Figures

List of Tables