Autokey Version 2 Specification

draft-sibold-autokey-00

Authors: Dr. D. Sibold – PTB, Stephen Röttger

IETF 85, Atlanta, USA, November 4 – 9, 2012

Introduction

Scope:

Autokey V2 shall provide

- Authenticity of NTP servers and
- Integrity of NTP data packets
- Conformity with the TICTOC Security Requirements

History

IETF 83	Presentation of security issues of RFC 5906 (autokey)
IETF 84	Plan for a new autokey standard was presented
July 30, 2012	00-Version of draft (preliminary)

Document Overview

Section 5 – Autokey Overview

Section 6 – Protocol Sequence

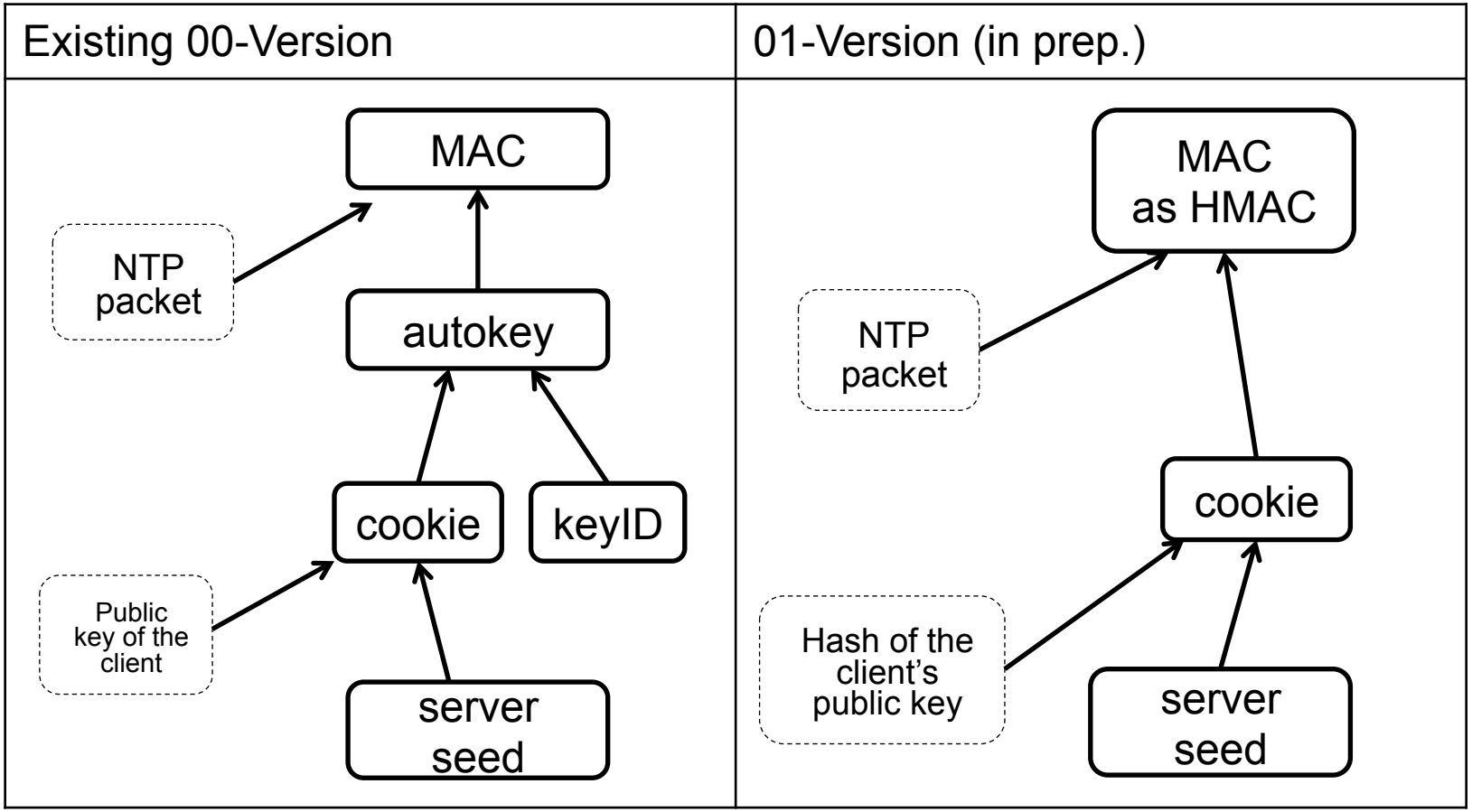
Section 7 – Hash and MAC Algorithms

Section 8 – Server Seed Considerations

…

Appendix A – Check against TICTOC Security Requirements

Section 5 – Autokey Overview



Section 6 – Protocol Sequence

Association Message

NTP packet with extension field of type association.
It contains, inter alia,

- algorithms for signatures,
- agreed hash and MAC algorithms (in 01-version the server has to notify the supported cryptographic hash algorithms).

Certificate Message

- The client verifies the authenticity of the server.
- To this end it request a chain of certificates up to the trusted authority (TA)
- Use of X.509 certificates
- The client needs a list of certificates which are accepted as TAs

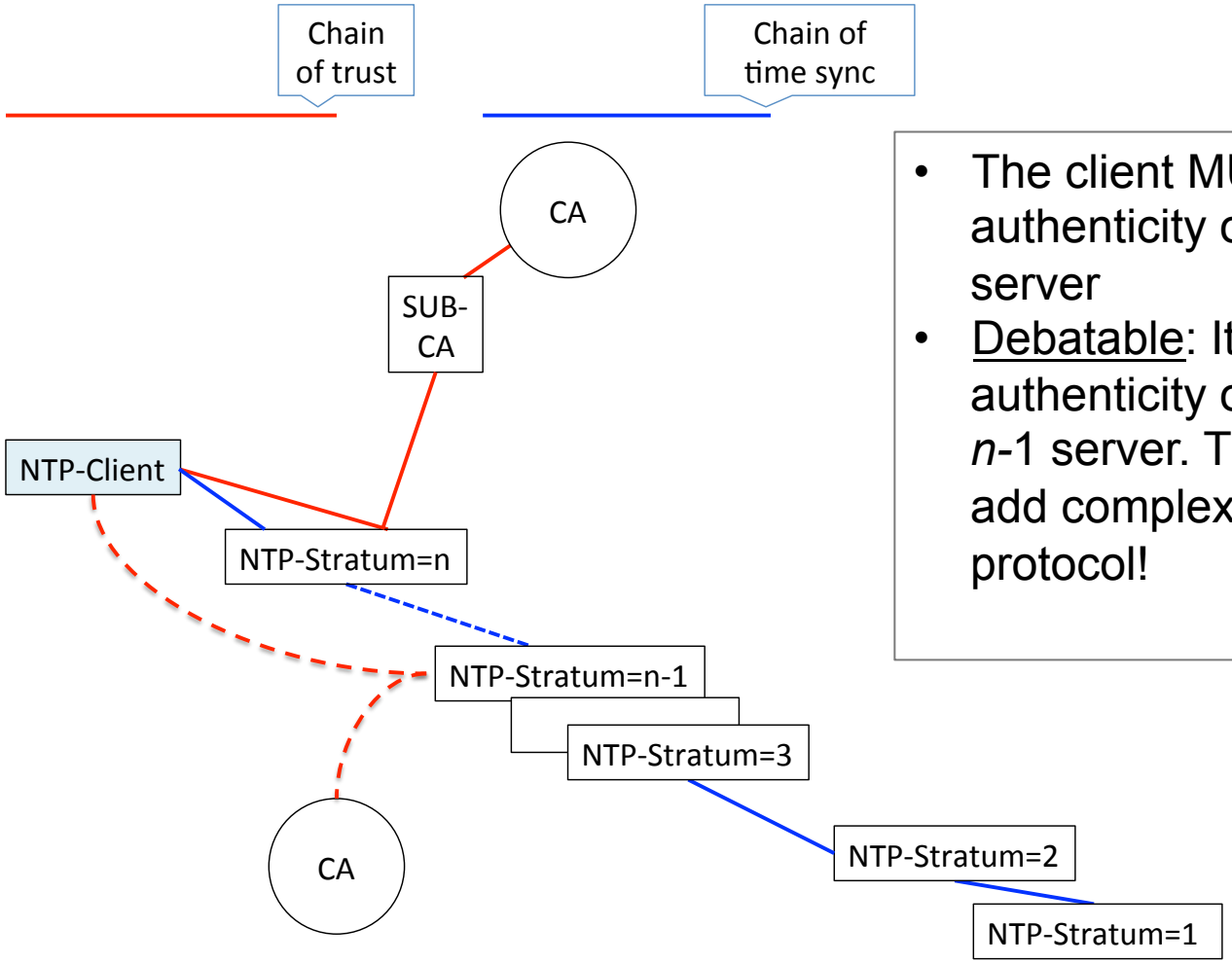
Section 6 – Protocol Sequence (cont …)

Certificate Message (cont. …)

- **Notes**
  - At this stage the client has no reliable time and therefore is not able to verify validity of the certificates. Solutions for an *initial* time stamp:
    - Use of OCSP (Online Certificate Status Protocol, RFC 6277)
    - Use of Time Stamping Authority (TSA) or other reliable sources
    - The validity of certificates is preconditioned (e.g. in corporate networks)
  - TA and Stratum-1 server are not inevitably identical.
    - „Chain of trust“ and „chain of time sync“ are not identical

Section 6 – Protocol Sequence (cont …)

Certificate Message (cont. …)



- The client MUST verify authenticity of stratum *n* server
- Debatable: It may verify authenticity of stratum *n*-1 server. This would add complexity to the protocol!

Section 6 – Protocol Sequence (cont …)

Cookie Message

- The client requests the cookie from the server.
- The request contains its public key (in the 01-version it contains also the hash algorithm selected by the client).
- The response contains the cookie encrypted with the client‘s public key.

Time Request Message

- The client‘s request includes a new extension field „time request“.
- It contains
  - its public key (in the 01-version the hash of the public key) and
  - the hash function which has to be utilized by the server.

Section 7 – Hash and MAC algorithms

	00-Version	01-version (in prep.)
Hash functions for Cookie	• The client MUST request SHA-1 or a stronger • Server MUST provide SHA-256	• The Server supports a list of hash algorithms. • These are notified during association exchange • The server MUST NOT support MD5 or weaker (see also RFC 6151) • Among others, it MUST support SHA-256 or stronger • The client selects one of the notified hash algorithms • This hash algorithm is used for all hashing processes • The MAC is generated via a HMAC
MAC	• The hash function is negotiated between server and client • They SHOULD negotiate a HMAC	
Hash for the public key	• Not applicable	
Hash functions for the Autokeys	• Client MUST request SHA-1 or a stronger • Server MUST provide SHA-256	• Not applicable

Section 8 – Server Seed Considerations

Generation of the seed

Open

Server Seed Live Time

What is a reasonable live time of the seed?

TICTOC Security Requirements

Section	Requirement from I-D tictoc security-requirements-02	Type	Autokey V2
4.1	Authentication of sender.	MUST	OK
	Authentication of master.	MUST	OK
	Recursive authentication	MUST	Open 1)
	Authentication of slaves.	SHOULD	OK
4.2	Integrity protection.	MUST	OK
4.3	Protection against DoS attacks.	MUST	NTP 2)
4.4	Replay protection.	MUST	NTP 2)
4.5	Security association.	MUST	OK
	Unicast and multicast associations.	MUST	OK
	Key freshness.	MUST	OK
4.6	Performance: no degradation in quality of time transfer.	MUST	OK
	Performance: lightweight.	SHOULD	YES
	Performance: storage, bandwidth.	MUST	OK
4.7	Confidentiality protection.	MAY	NO
	Protection against delay attacks.	MAY	NO
4.9	Secure mode.	MUST	NTP? 3)
	Hybrid mode.	MAY	YES

1) But chain of trust not necessarily in line with chain of time sync.
2) Ensured by NTP on-wire protocol
3) This is more a setup/configuration issue

Next steps

- **Finalization of the 01-version of the draft**
- **Inclusion of the NTP development team**
- **Inclusion of IETF's security group**
- **A new name for the protocol (suggestions?)**