



# **NTP Extension Field Cleanup for NTS ARIN Community Grant: Interim Report**



# History

NTPv3: 1992-1998

NTPv4: 1997-Present. Major releases and Events:

Aug 2001: ntp-4.1.0

Feb 2002: ntp-4.1.1

Jul 2003: ntp-4.1.2

Oct 2003: ntp-4.2.0

Jul 2005: draft-ietf-ntp-ntp4-00

Jun 2006: ntp-4.2.2

Dec 2006: ntp-4.2.4

Sep 2007: draft-ietf-ntp-autokey-00



# NTPv4: 2009-Present

Dec 2009: ntp-4.2.6 (with 5 update releases)  
Jun 2010: RFC5905 and RFC5906 published  
Dec 2014: ntp-4.2.6 (with 15 update releases)  
ntp-4.2.6p16 due out soon  
ntp-4.4 could be out this year

Q3/97: NTPv4 code first came out  
Q2/05: First NTPv4 draft standard came out  
Q2/10: NTPv4 Standards published



# NTP v3/v4 Differences

At the protocol level, the only difference between v3 and v4 is that v4 supports an Extension Field (EF), at the end of the packet.

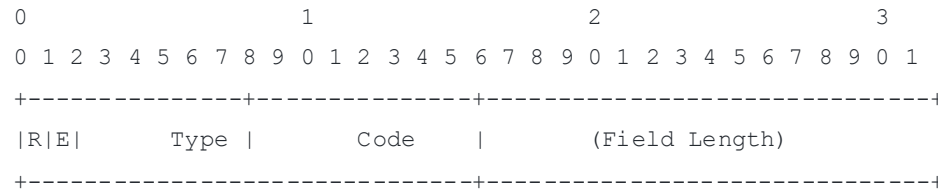
From 1997-2015, the only use-case for an EF was the Autokey protocol, specified by RFC5906.

Starting in ~2015, several other EFs were being worked on.

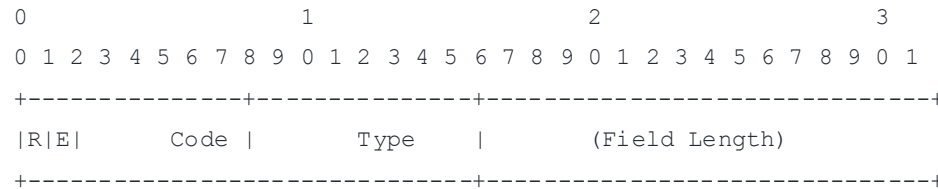


# NTP EF Formats

The 1997 V1 Extension field header:



RFC5906 used the V2 Extension Field header:



This is trickier than just swapping the `Code` and `Type` fields, and both formats must be supported.



# How we got here

NTPv3 (and earlier) had private key authentication.

Prof. Mills was discussing specific use-cases for public key authentication and NTP, and designed Autokey for these situations. This code was first deployed in 1997, using the V1 EF structure. Sometime before RFC5906 was finalized in 2010, the IETF spec'd the V2 EF structure. But since there were active Autokey users and no other EFs contemplated, Dave never updated the code.



# Why this effort is Good

With the advent of NTS, the IETF NTP Working Group's design for an ephemeral public key authentication system, new players implemented NTS and that's when it became clear that the NTP Project's implementation needed to support the V2 (published) EF spec, to interoperate with others.

Since there are *still* users of Autokey out there, we need to be able to support both the V1 and V2 Extension Field formats.



# Status

We're about half-way through the code conversion.

The changes affect many lines of code in several of the longer code files. Several new files have been added to the codebase.

Still need to spec out the `ntp.conf` file syntax to ensure each association gets the right EF format.

We are on-track with the implementation schedule.





# In conclusion...

We greatly appreciate receiving an ARIN Community Grant to help NTF, the NTP Project, and all who use our software to help us take the next step in deploying NTS in our NTP software.