# Tools for Securely Getting DNSSEC Root Trust Anchors

Paul Hoffman, ICANN

Jakob Schlyter, Kirei

OARC 25, Dallas, October 2016

v1

# Tool overview

- Many programs, particularly validating recursive resolvers, need to get and validate the DNSSEC root trust anchors (“the XML file”)
- The `get_trust_anchor.py` tool does that with minimal installation requirements
- Fits in a niche similar to `unbound_anchor`, but has a different deployment footprint

# Design goals

- Must have minimal deployment requirements: Python 2.7 or 3.x with **no additional libraries**, plus OpenSSL command line
- Make the code trivial to read so that someone else can replicate it in whatever language they want
  - Show our steps as pseudocode
- Only rely on **ICANN CA for validation**
  - Use, but don’t rely on, HTTPS to get files
- Another platform for testing the trust anchor management for the upcoming KSK roll

# Really? Just Python and OpenSSL?

- **Yes**. It kept being tempting to add libraries to Python to make the code cleaner, but we kept to the design goal.
- Python comes with lots of **built-in libraries**; we used:
  - argparse, base64, codecs, datetime, hashlib, json, os, pprint, re, struct, subprocess, sys, tempfile, and xml.etree.ElementTree
- OpenSSL is **used just once**, in step 3, to validate the S/MIME signature on the trust anchor file

# Steps

1. Fetch the trust anchor file from IANA using HTTPS
2. Fetch the S/MIME signature for the trust anchor file from IANA using HTTPS
3. Validate the signature on the trust anchor file using a built-in IANA CA key
4. Extract the trust anchor key digests from the trust anchor file
5. Check the validity period for each digest
6. Verify that the trust anchors match the KSK in the root zone file
7. Write out the trust anchors as a DNSKEY and DS records

# Some possibly-useful features

- Can use a **local file** instead of getting the trust anchor from the URL
- Can save the temporary files for doing post-mortems
- Follows **PEP 8**

# Other tools

- Code in BIND
- unbound_anchor
- Probably lots of others

# Getting `get_trust_anchor.py`

- https://github.com/kirei/dnssec-ta-tools
  - In the `get_trust_anchor` subdirectory
  - This repo also contains other trust anchor tools
- Pull requests and issues **are welcome**