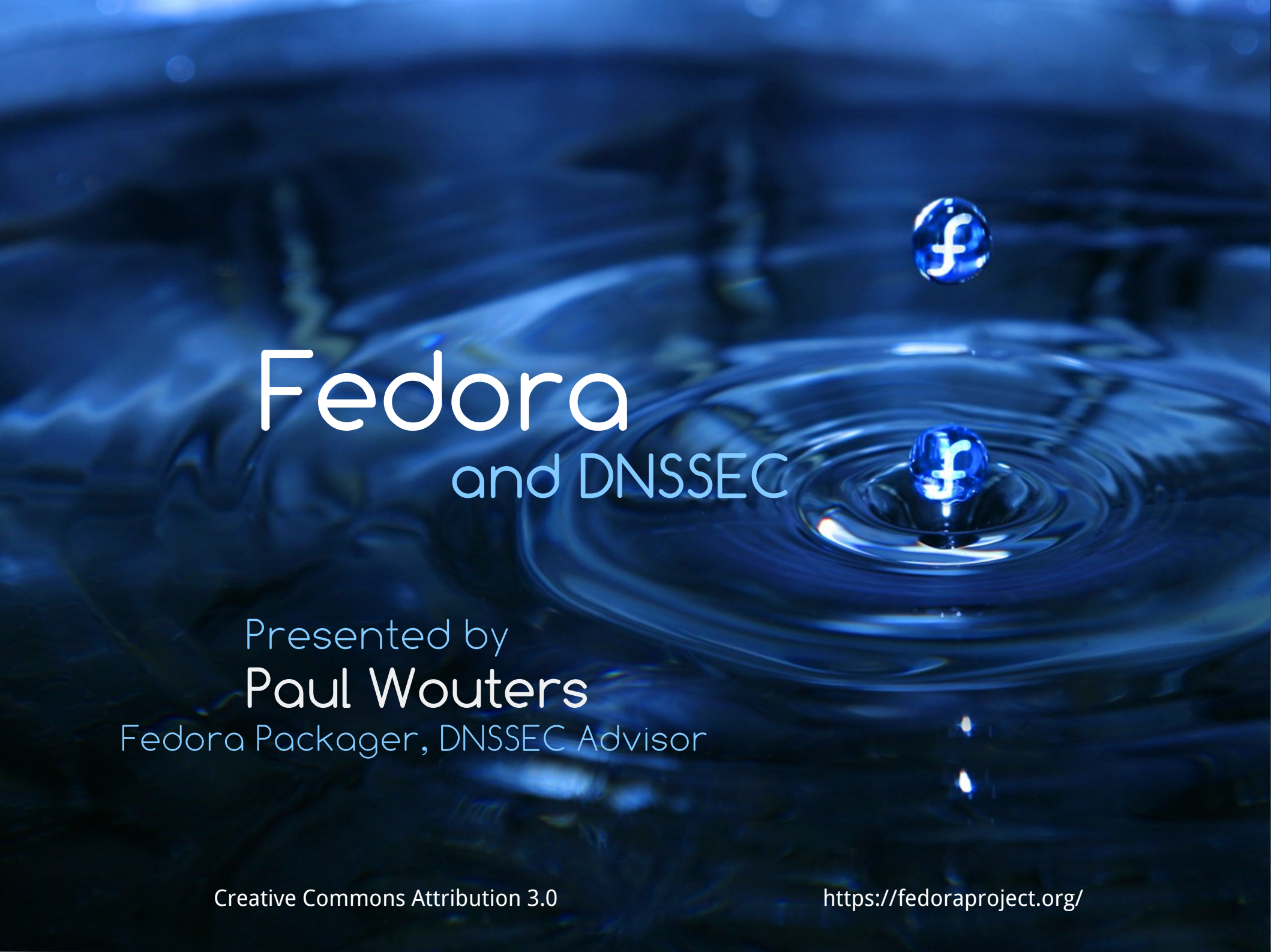

https://fedoraproject.org/

What is Fedora

- Fedora is a fast, stable, and powerful operating system for everyday use built by a worldwide community of friends.
- It's completely free to use, share, modify
- Innovative, Cutting edge, Leading
- 25,000 packages, 250,000 contributors

- Forms the basis for Red Hat Enterprise Linux (RHEL) but also CentOS, OLPC, Moblin, etc

fedora™

DNSSEC packages in Fedora

- Servers: bind9, nsd, unbound, powerdns
- Tools: ldns, libunbound, dnssec-tools, sshfp, autotrust, bind-pkcs11, OpenCryptoki, perl-Net-DNS-SEC

Non-Fedora addons:

- Sun SCA 6000 HSM drivers for Linux kernel
- Firefox DNSSEC labs.nic.cz (Tools->Extensions)
- SPARTA patches for native DNSSEC in
  - Firefox,Postfix, Sendmail, ejabberd, gaim,etc

fedora

DNSSEC with Fedora

- March 2009: unbound and bind ship with TLD trust anchors and DNSSEC & DLV validation enabled **per default** (Fedora 11)
- February 2010: RIPE DDoS incident in some branches of Fedora due to stale RIPE keys (AKA “Rollover or die” incident)
- December 2010: Ship DNSSEC root key for bind and unbound. Phased out all shipped TLD trust anchors and stopped using dnssec-conf. DLV still enabled.

fedora™

DNSSEC with Fedora

- Fedora domains signed with DNSSEC since March 12, 2010
  - (fedoraproject.org, fedorahosted.org, etc)
- Signing using custom script based on bind's dnssec-signzone, keys restricted to ops
- DNSSEC keys are published in the DLV
- DS record support from Fedora's domain Registrar is expected soon
- Two auth name servers sign zones, with different Bind Views for GEO-IPS

fedora

DNSSEC developments

- DNSSEC resolving for all Fedora installs
  - NetworkManager integration, compatible with virt-manager/KVM (currently dnsmasq)
  - Should use DHCP obtained caching name server as forwarder (only unbound can do this – not bind)
  - What to do when ISP DNS is broken?
- TLSA / HASTLS support tool (IETF DANE)
  - SSL certificate validation via DNSSEC (without CAs)
- opendnssec support (dependancy packaging)
- fix ssh client VerifyHostKeyDNS=ask

fedora

Questions?

Contact: Paul Wouters

pwouters@fedoraproject.org
paul@xelerance.com