

# ALTO Server Discovery

IETF#87, Berlin, 2013-07-29

Sebastian Kiesel

[sebastian.kiesel@izus.uni-stuttgart.de](mailto:sebastian.kiesel@izus.uni-stuttgart.de)

# Recap

## One architecture, two drafts

- Step 1
    - DHCP → draft-ietf-alto-server-discovery-08
    - Manual Input → draft-ietf-alto-server-discovery-08
    - Reverse-DNS → draft-kist-alto-3pdisc-04
  - Step 2
    - U-NAPTR Lookup → draft-kiesel-alto-3pdisc-impl-00
- 
- The diagram illustrates the flow of draft information. Red arrows point from 'DHCP' and 'Manual Input' to 'draft-ietf-alto-server-discovery-08'. A green arrow points from 'Reverse-DNS' to 'draft-kist-alto-3pdisc-04'. A dashed green arrow points from 'U-NAPTR Lookup' to 'draft-kiesel-alto-3pdisc-impl-00'.

# draft-ietf-alto-server-discovery

IETF#87, Berlin, 2013-07-29

Sebastian Kiesel

sebastian.kiesel@izus.uni-stuttgart.de

# draft-ietf-alto-server-discovery

- **IETF Last Call** on -08 2013-06-06 .. 2013-06-20
- Thanks for feedback to
  - Meral Shirazipour (Gen-ART): Typos
  - Tina Tsou (Secdir):
    - Inconsistency in order DHCP vs. manual input
    - Security considerations in general
    - Typos
- **New version -09** submitted today!
  - Delayed due to submission cutoff
  - Tina has reviewed a preview version and says her issues are resolved

# draft-ietf-alto-server-discovery

## Diffs -08 to -09

- It has always been intended that manual input serves as a fallback if DHCP is not available  
AND to override DHCP if the user wants to
- Clarify that presence of a manual configuration has to be checked *before* trying DHCP – otherwise overriding won't work

# draft-ietf-alto-server-discovery

- Security Considerations section nearly re-written from scratch
  - Now matches the high quality of other ALTO documents 😊
- Discussion of four protection goals
  - Integrity of the ALTO Server's URI
    - probably the most serious security concern related to ALTO server discovery
    - Possible attack vectors: manual c., DHCP, DNS – follow BCPs for securing DHCP, DNS
    - Note: if DHCP or DNS are compromised, much worse things can happen
    - Note: TLS cert will auth. The IRD URI, not the U-NAPTR input domain name
  - Availability of the ALTO Server Discovery Procedure
    - Undesirable, but not extremely critical (apps should be able to handle unavailability)
    - Follow BCPs for securing DHCP and DNS
  - Confidentiality of the ALTO Server's URI
    - Not a threat in the deployment scenarios discussed so far – re-evaluate if necessary
  - Privacy for ALTO Clients
    - Not a threat in the deployment scenarios discussed so far – re-evaluate if necessary

# draft-ietf-alto-server-discovery

## Next steps

- Ready for publication!
- Thanks to all contributors & reviewers!

draft-kist-alto-3pdisc

IETF#87, Berlin, 2013-07-29

Sebastian Kiesel

sebastian.kiesel@izus.uni-stuttgart.de



# draft-kist-alto-3pdisc

- The “missing piece” document
  - Support for 3pdisc is a requirement (AR-33 in RFC 6708)
  - May also be useful\* if DHCP is not available and manual configuration is undesirable (i.e., if the other draft does not work)

\* various footnotes on UNSAF and other deployment issues apply

# draft-kist-alto-3pdisc

## Since last meeting

- -03 (2013-05-16) adds lots of clarifications and deployment considerations, but does not change the algorithm
- -04 (2013-06-15) change to the algorithm, still ongoing discussion with DNS directorate
  - Store NAPTR records directly in “reverse tree”
  - Proof-of-concept implementation changed and verified to work, but new version not published yet

# draft-kist-alto-3pdisc

## Discussions with the DNS directorate

- Thanks to Olafur Gudmundsson for extensive discussions
- Discussions are still ongoing, focusing on details
- So far, we did not receive a written certificate that the DNS directorate thinks that this is a really good idea
- But, we did not receive a “oh no! – the Internet will melt down if you do that!” either 😊

# draft-kist-alto-3pdisc

## Next Steps

- Continue discussions with DNS folks
- Publish updated implementation and testbed
- Adopt as a WG item?