draft-loffredo-regext-epp-over-http-03

M. Loffredo, L. Luconi Trombacchi, M. Martinelli
IIT-CNR/Registro.IT
D. Keathley, J. Gould
VeriSign, Inc
Most relevant changes since version -02

- Has been made fully compliant with RFC 5730
- Aligns with the structure and makeup of EPP over TCP (EoT) in RFC 5734
- Verisign added as co-authors
An EPP client-server connection is mapped onto an HTTP session, which is initiated by the client via sending a GET request to the server.

The EPP server **MUST**:

- include the EPP Greeting in the response
- include the HTTP session ID in the "Set-Cookie" header

The EPP client **MUST**:

- send all subsequent commands as POST requests
- include the HTTP session ID in the "Cookie" header
Security Considerations

• Servers are **REQUIRED** to support TLS 1.2 or higher

• Servers **MUST** implement at least one method of access control that limits server connection access to only authorized clients. Implementation of multiple access control methods is **RECOMMENDED** (Scott’s feedback to be addressed in version -04)

  • IP allow-listing
  
  • identifying clients by its IP address
  
  • locking the session ID to the client's IP address
  
  • require clients to present a valid digital certificate, issued by a recognized Certification Authority (CA)
  
  • require clients to present a secret or a Bearer Token generated out-of-band
Conclusions

• EoH provides an EPP transport choice which is:
  • Cloud-friendly
  • Fully compliant with RFC 5730
  • Fully pluggable transport with EoT
  • Please review the draft and provide feedback on the mailing list
ROW13
4 June 2024
13:00-17:00 UTC
https://regiops.net

A forum for discussion of the technical aspects of registration operations in the domain name system and IP addressing

Submit your proposal by May 10th to: row@cofomo.com