EDSR -02

Tommy Jensen, Microsoft
Corey Mosher, Innate
John Todd, Quad9
Two major changes since -01

• Split into two separate modes of redirection:
  • Strict Origin Redirection
  • Overlapping Origin Redirection
• Special consideration for DDR-discovered resolvers
Strict Origin Redirection

• This is exactly what it sounds like
  • Clients are required to support SOR (EDSR default mode)
  • No matter how long the chain of redirections, every step must maintain the same domain name as the original resolver
Strict Origin Redirection + Delegated Credentials

• But what if the server operator wants to redirect to a third party who does not have a cert for the name?
  • Text now recommends use of Delegated Credentials
  • Still Strict Origin, but destination does not have to have access to the name’s private key
  • Yay RFC reuse!
Overlapping Origin Redirection

• An alternative to using delegated credentials
  • Destination server can have a new domain name it is referred to as long as its TLS cert is valid for both the old and new domain names
  • Entirely optional mode of redirection for clients given the additional security considerations it introduces
Overlapping Origin Redirection

• Intended for edge cases where client policy is in play
  • Clients should not generally support this for all names
  • Servers must accommodate clients refusing OOR the same way they must accommodate clients refusing redirection generally
Overlapping Origin Redirection

- This makes EDSR more flexible
  - Unblocks providers whose partners, clients, or TLS dependencies do not have support for delegated credentials
  - Text includes a breakdown of when it could be useful but how SOR + DC is preferable
About DDR-discovered resolvers

• EDSR identifies servers by name, but DDR identifies servers only by an IP address
  • Well-established security model point from DDR WGLC
  • This means EDSR by domain name must not be used with DDR-discovered resolvers (there is no *trustworthy* name known to the client)
About DDR-discovered resolvers

- When using EDSR with DDR-discovered resolvers, the IP address is used as the identity, not the name
  - SOR: redirections MUST all pass the original IP addr validation
  - OOR: not supported at all
Next steps

• Does this satisfy the security concerns from the -01 reviews?
• Are we ready to adopt so we can refine as a WG?