draft-fuller-lisp-ddt-01
DDT Security

V. Fuller, D. Lewis, V. Ermagan

Presenter: Vina Ermagan

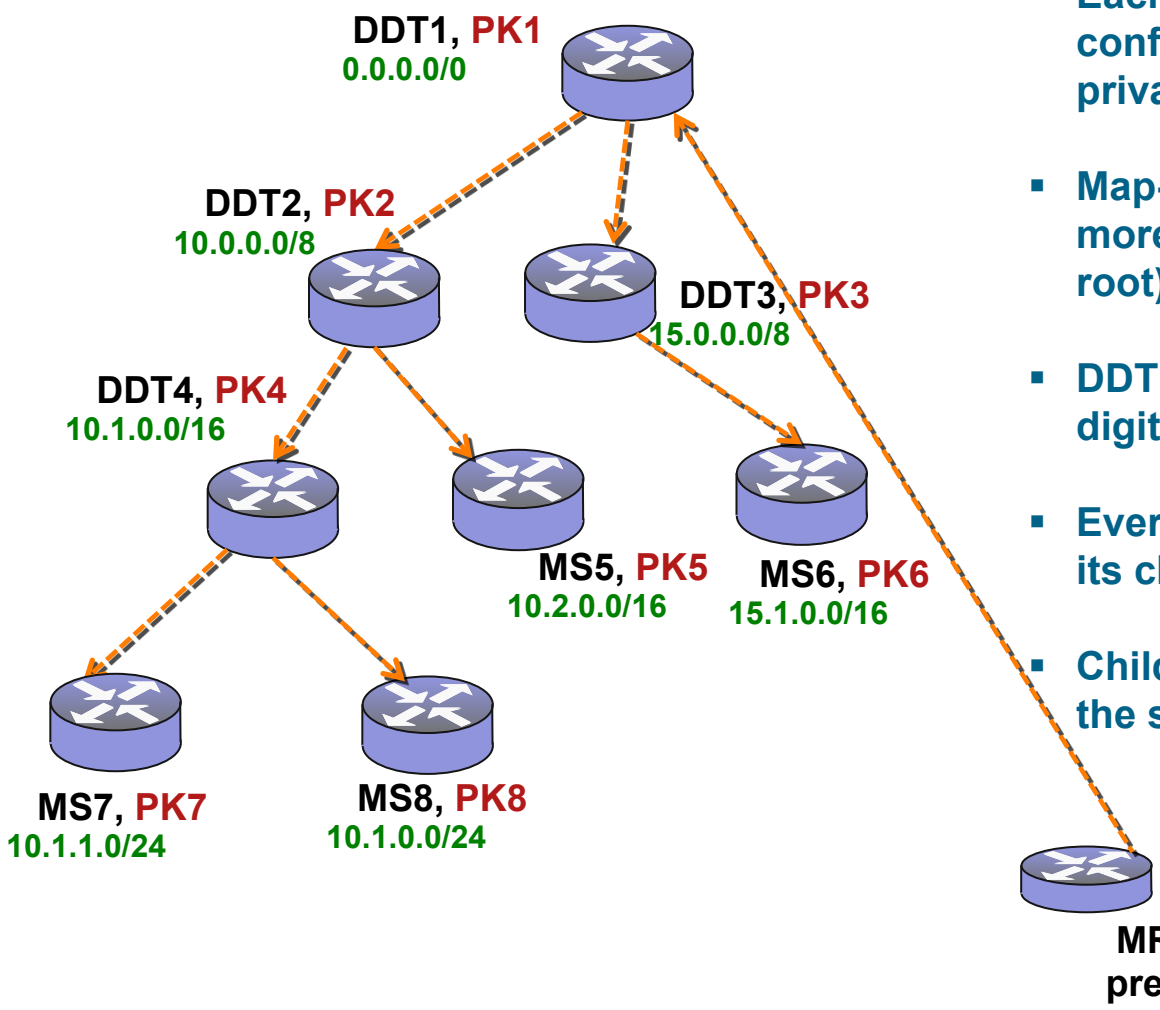
IETF 83, Paris – March 2012

Goals and Scope

- Provide the following for the DDT lookup process
  - Data origin authentication
  - Data integrity protection
  - XEID-prefix delegation

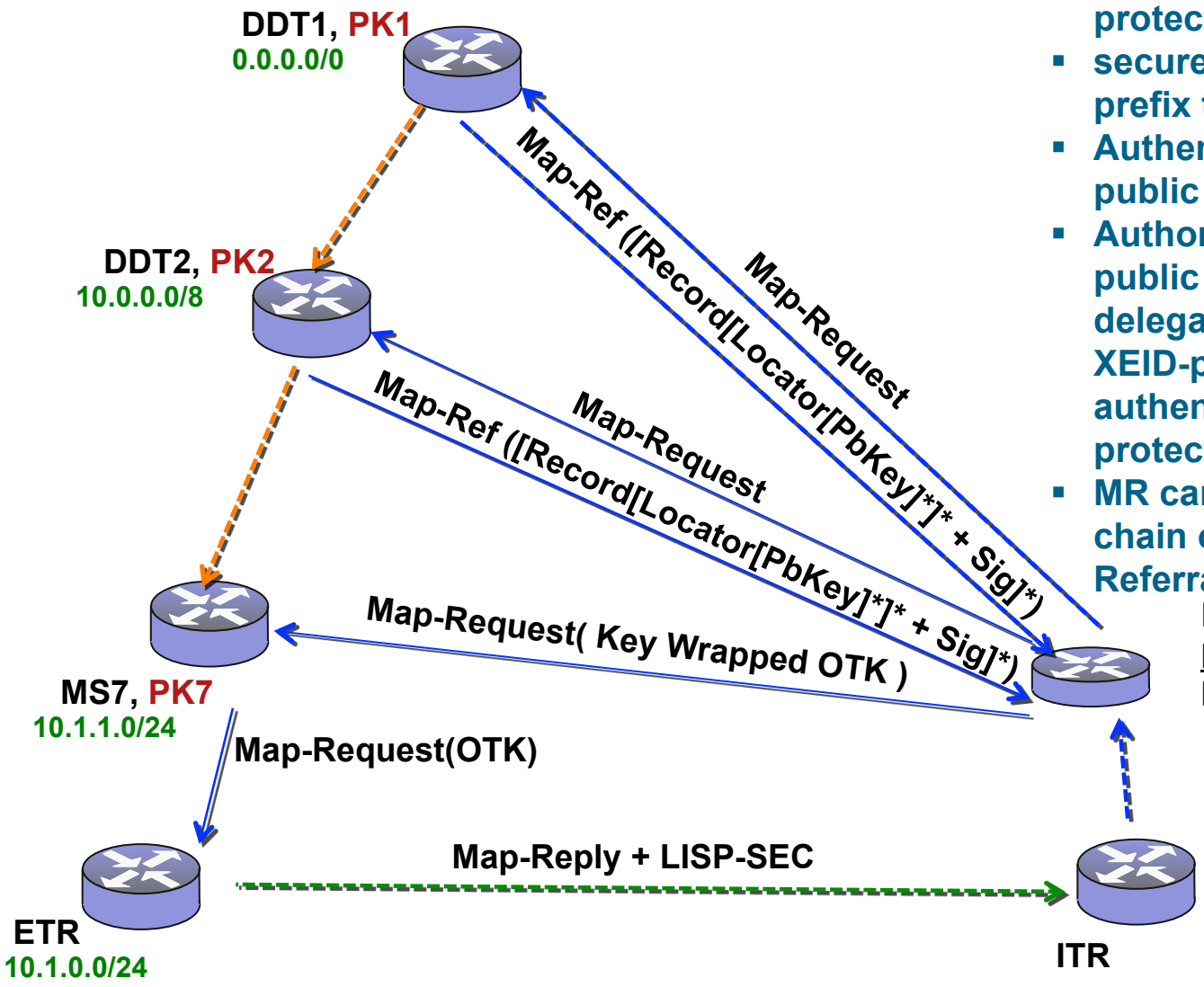
- Out of scope:
  - Global XEID prefix authorization

Security Architecture Overview



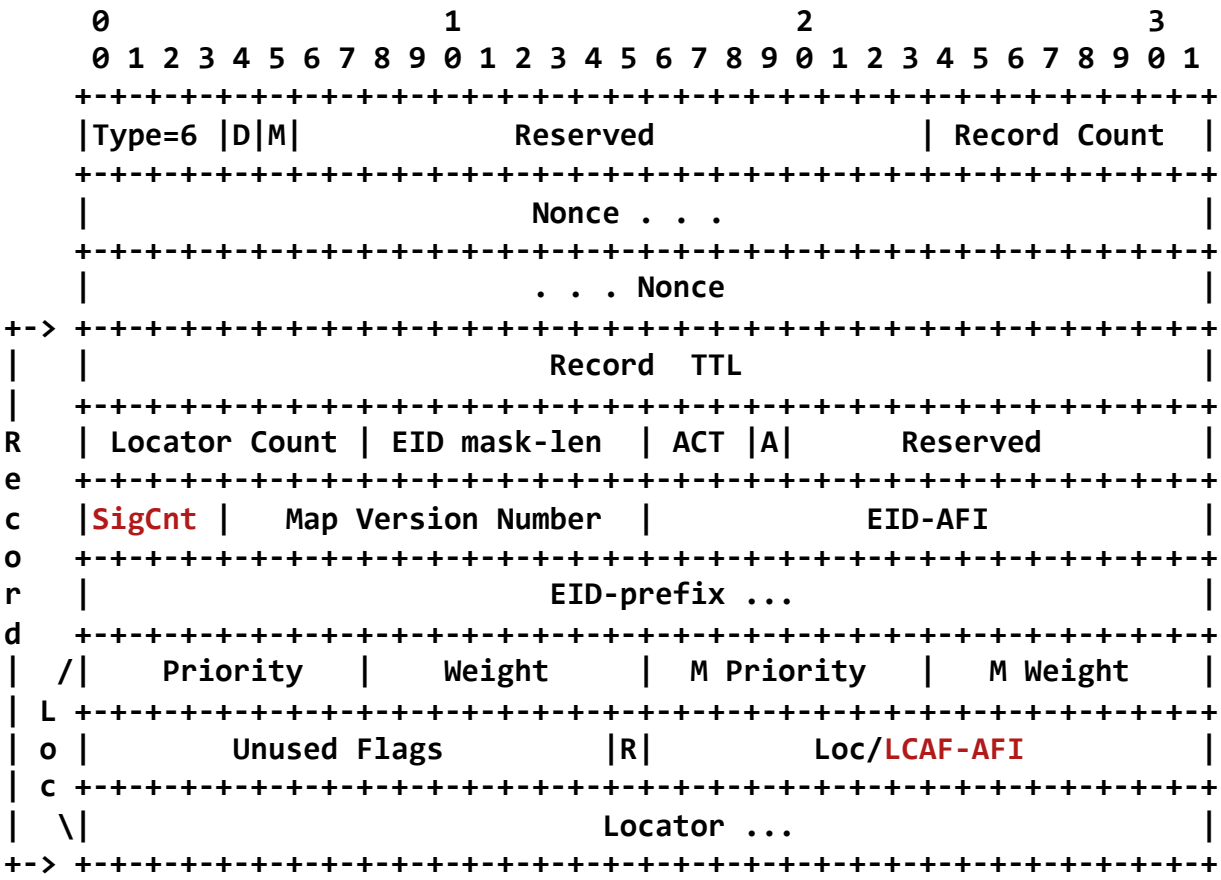
- Each DDT node, and Map-Server configured with one or more Public/ private key pair(s)
- Map-Resolvers configured with one or more trusted public keys (usually the root)
- DDT node private keys are used to digitally sign Map-Referral Records
- Every DDT node also configured with its children's Public Keys
- Children public keys are included in the signed Map-Referral records

Signing Referral Records

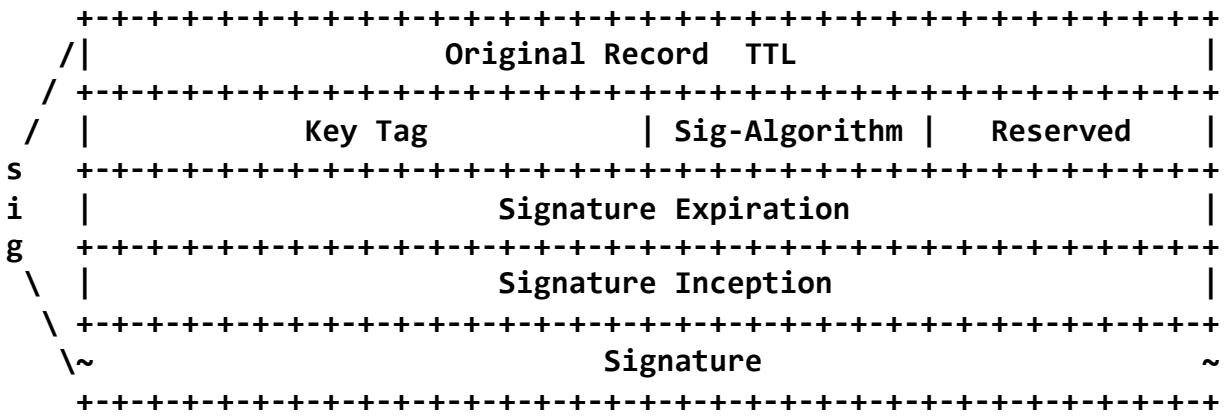


- Provides origin auth and integrity protection for the record data
- securely delegates a sub XEID-prefix to a child DDT node
- Authenticates the child DDT public keys
- Authorizes the child DDT node's public key to provide further delegation of the associated XEID-prefix (including origin authentication and integrity protection)
- MR can form an authentication chain of Pub keys to verify Map-Referrals

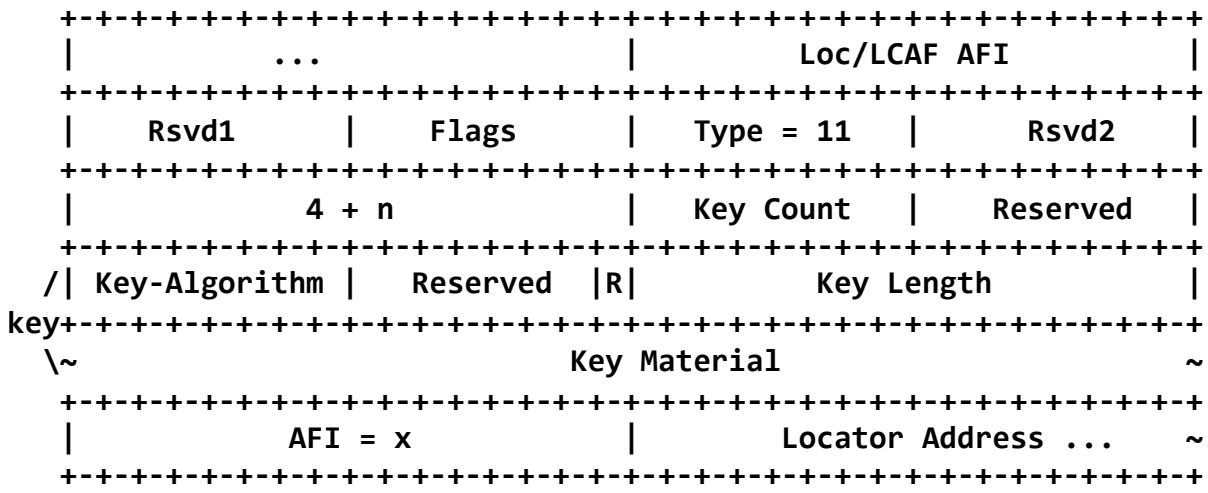
Map-Referral Format



Signature Format



Including Keys in referrals



Q&A

- Thanks to Noel Chiappa for his major contribution to DDT Security design.