

Diameter AVP Level Security: Scenarios and Requirements

draft-tschofenig-dime-e2e-sec-req-01.txt

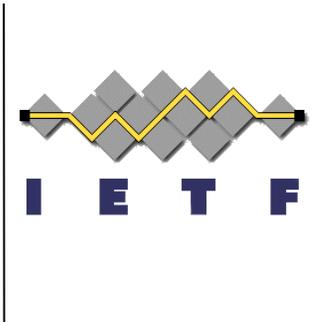
Hannes Tschofenig

DIME WG

IETF 87

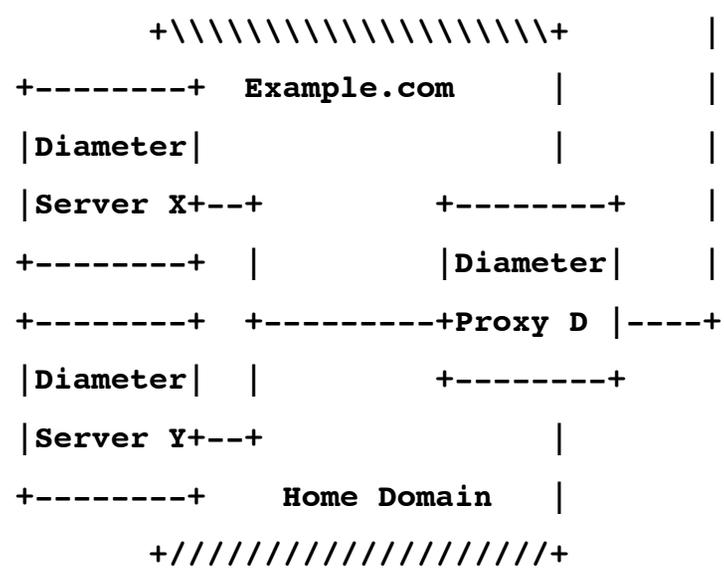
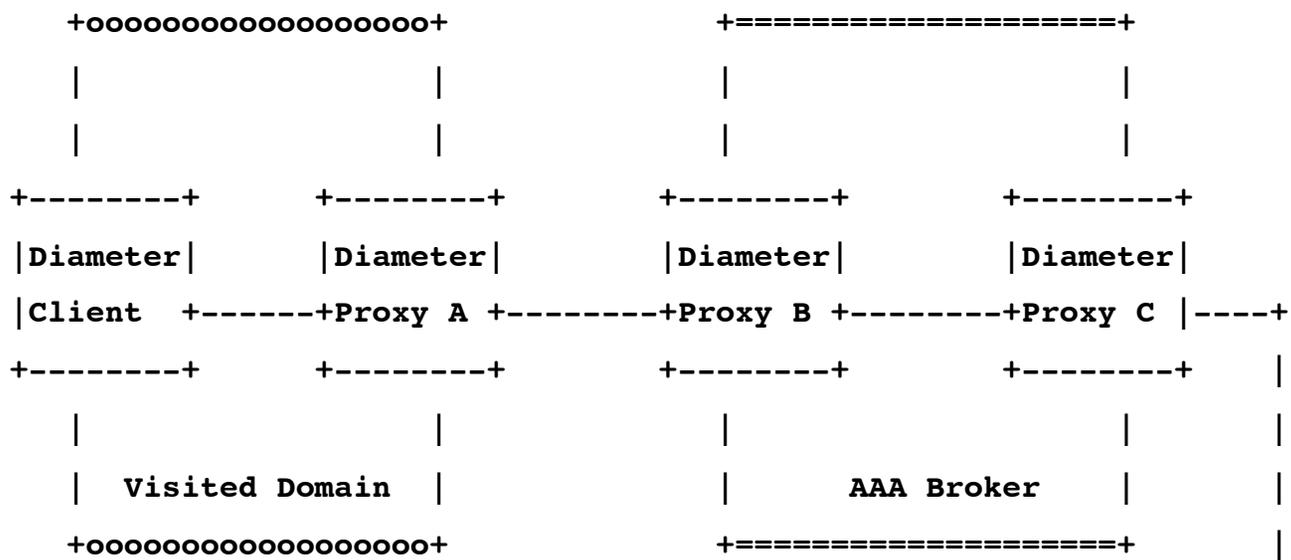
July, 2013

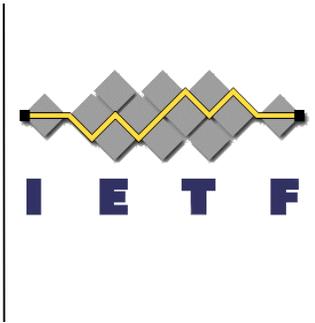




Changes since IETF#86

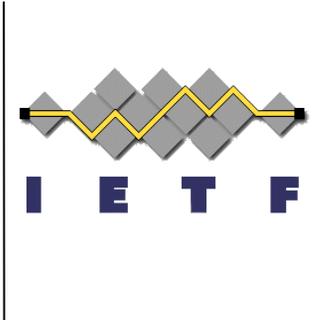
- Added Kervin Pillay as co-author
- Major re-write of the document with
 - Expanded use cases
 - Revised requirements





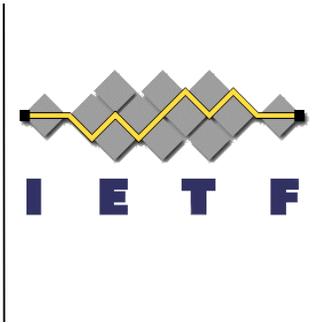
Use Cases

- End-to-End Diameter AVP Security Protection
- Middle-to-End Diameter AVP Security Protection
- End-to-Middle Diameter AVP Security Protection
- Middle-to-Middle Diameter AVP Security Protection



Requirements

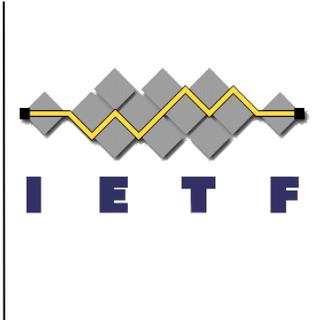
- #1: Solutions **MUST** support an extensible set of cryptographic algorithms.
- #2: Solutions **MUST** support confidentiality, integrity, and data-origin authentication. Solutions for integrity protection **MUST** work in a backwards-compatible way with existing Diameter applications.
- #3: Solutions **MUST** support replay protection.
- #4: Solutions **MUST** support the ability to delegate security functionality to another entity.
- #5: Solutions **MUST** be able to selectively apply their cryptographic protection to certain Diameter AVPs.



Requirements, cont.

- #6: Solutions MUST recommend a mandatory-to-implement cryptographic algorithm.
- #7: Solutions MUST support symmetric keys and asymmetric keys.
- #8: A solution for dynamic key management has to be provided.
- #9: The ability to statically provisioned keys has to be supported to simplify management for small-scale deployments that typically do not have a backend network management infrastructure.
- #10: Capability/Policy Discovery
- #11: Command-Line Support

Next Steps



Is this is a good starting point for a working group document?