Policy Discovery and Related Alignment Issues

- Related tickets: 24, 34, 46, 58, 59, 60, 68, 108, 111, 112, 121
- Lively mailing list discussion seems to have coalesced around the idea of replacing current two query method (RFC5322.From and Organizational Domain) with a DNS tree walk
    - Walk will be limited in scope (see next slide)

Proposed Text Changes for DNS Tree Walk

policy_discovery_7489	policy_discovery_no_psl
skipping to change at *line 20*	skipping to change at *line 20*
allowing subdomain policy overrides, and limiting DNS query load, the following DNS lookup scheme is employed:	allowing subdomain policy overrides, and limiting DNS query load, the following DNS lookup scheme is employed:
1. Mail Receivers MUST query the DNS for a DMARC TXT record at the DNS domain matching the one found in the RFC5322.From domain in the message. A possibly empty set of records is returned.	1. Mail Receivers MUST query the DNS for a DMARC TXT record at the DNS domain matching the one found in the RFC5322.From domain in the message. A possibly empty set of records is returned.
2. Records that do not start with a "v=" tag that identifies the current version of DMARC are discarded.	2. Records that do not start with a "v=" tag that identifies the current version of DMARC are discarded.
3. If the set is now empty, the Mail Receiver MUST query the DNS for a DMARC TXT record at the DNS domain matching the Organizational Domain in place of the RFC5322.From domain in the message (if different). This record can contain policy to be asserted for subdomains of the Organizational Domain. A possibly empty set of records is returned.	3. If the set is now empty, the Mail Receiver determines the target for additional queries.
4. Records that do not start with a "v=" tag that identifies the current version of DMARC are discarded.	4. Break the subject DNS domain name into a set of "n" ordered labels. Number these labels from right to left; e.g., for "example.com", "com" would be label 1 and "example" would be label 2. 5. Count the number of labels found in the subject DNS domain. Let that number be "x". If x <5, remove one label from the subject domain. If x >= 5, then remove labels from the subject domain until 4 labels remain. The resulting DNS domain name is the new target for subsequent lookups. 6. The Mail Receiver MUST query the DNS for a DMARC TXT record at the DNS domain matching this new target in place of the RFC5322.From domain in the message. This record can contain policy to be asserted for subdomains of the target. A possibly empty set of records is returned. 7. Records that do not start with a "v=" tag that identifies the current version of DMARC are discarded.
5. If the remaining set contains multiple records or no records, policy discovery terminates and DMARC processing is not applied to this message.	8. If the set is now empty, the Mail Receiver determines the target for additional queries by removing a single label from the target domain and repeating steps 6 and 7 until there are no more labels remaining. 9. If the remaining set contains multiple records or no records, policy discovery terminates and DMARC processing is not applied to this message.
End of changes. 3 change blocks.	
8 lines changed or deleted	*25 lines changed or added*

Tree Walk Requires Change to Identifying Org Domains

- Discussion of PSD domains including flag in _dmarc records identifying themselves as PSD domains
  - If implemented, two domains will be in relaxed alignment if both end in names that are not PSDs
- Consensus not reached on this concept as of yet