1. Introduction

Abusive email often includes unauthorized and deceptive use of a domain name in the RFC5322.From header field. The domain typically belongs to an organization expected to be known to – and presumably trusted by – the recipient. The Sender Policy Framework ([RFC7208]) and DomainKeys Identified Mail ([RFC6376]) protocols provide domain-level authentication, but are not directly associated with the From: domain. DMARC leverages them, so that Domain Owners publish a DNS record indicating their From: field:

* Email authentication policies
* Level of concern for mail that fails authentication checks
* Desire for reports about email use of the domain name

DMARC can cover non-existent sub-domains, below the “Organizational Domain”, as well as domains at the top of the name hierarchy, controlled by Public Suffix Operators (PSOs).

As with SPF and DKIM, DMARC classes results as "pass" or "fail".  A pass from either SPF or DKIM is required. Also the passed domain must be “aligned” with the RFC5322.From domain.  Domains are said to be "in alignment" if they have the same Organizational Domain, which is at the top of the domain hierarchy, while having the same administrative authority as the From: field domain.

A DMARC pass indicates only that the From: domain has been authenticated for that message. Of course, authentication does not carry an explicit or implicit value assertion about that message or about the Domain Owner. Indeed, a mail-receiving organization performing DMARC validation can choose to follow the Domain Owner’s requested disposition for authentication failures, and to inform the Domain Owner of the mail handling decision for that message. It also might choose different actions.

For a mail-receiving organization supporting DMARC, a message that passes validation is part of a message stream that is reliably associated with the From: field Domain Owner.  Therefore, reputation assessment of that stream by the mail-receiving organization is not encumbered by accounting for unauthorized use of that domain in the From: field.  A message that fails this validation is not necessarily associated with the Domain Owner's domain and its reputation.

DMARC, in the associated [DMARC-Aggregate-Reporting] and [DMARC-Failure-Reporting] documents, also specifies a reporting framework. Using it, a mail-receiving domain can generate regular reports about messages that claim to be from a domain publishing DMARC policies, sending the reports to the addresses specified by the Domain Owner.

Use of DMARC creates some interoperability challenges that require due consideration before deployment, particularly with configurations that can cause mail to be rejected.  These are discussed in Section 9.