

(3) Gesteigerte Beweiskraft durch E-Mail-Signatur? (agitos.de)

Sender-Authentifizierung und
Nachrichtensignatur per DKIM
auf ISP-Ebene



ca.tld, a trusted entity that
saves public keys in
the long-term.

Send new public keys
to ca.tld if necessary,
private keys remain
at the mailservers

Check validity of the email
if needed (long-term)



User `alice@domain.tld`
sends an email to Bob



Alice's mailservers add
a DKIM signature with
`d=domain.tld` and
`i=alice@domain.tld`



Bob's mailservers add an own
signature for a long-term
verification with (1) `d=ca.tld` and
(2) opt. `i=<alice@domain.tld>@ca.tld`
if the incoming DKIM signature is valid.



Bob's mailclient may visualize
(1) that Alice signed her email
(2) that the message has long-
term authenticity