E-mail standards checklist

Enabling security standards is a great way to protect your e-mail. But where do you begin? This step-by-step guide can help.

We distinguish between outgoing mail (mail you send) and incoming mail (mail you receive). The following table shows the support needed for each standard. A tick means that your mail server software needs to support the standard in order for you to implement it.

	E-mail standard	Outgoing mail support	Incoming mail support
Authentication	SPF	-	√
	DKIM	√	√
	DMARC	-	√
Encryption	STARTTLS	√	√
	DANE	-	√

Example
SPF for outgoing mail is easy to activate without having software that supports SPF on your outbound mail server.
To implement DKIM, on the other hand, you need software support for both outgoing and incoming mail.

Step 1	**SPF sending host**	**DNS**	☐ Modify the DNS. ☐ Use ~all. ☐ Check whether it's working on internet.nl.
Step 2	**DKIM sending host**	**DNS**	☐ Put the public key in the DNS. ☐ Check using dig.
		Mail server	☐ Generate a key pair. ☐ Link the private key to your mail environment. ☐ Configure your mail server to sign outgoing mail using the private key. ☐ Check the digital signature on your outgoing mail using DMARCtester.com or mail-tester.com.
Step 3	**DMARC sending host**	**DNS**	**Immediately** ☐ Set: p=none. ☐ Put the DMARC records in the DNS. ☐ Check the configuration on internet.nl. **Later** ☐ Set: p=quarantine. ☐ Consider using a percentage by setting the pct variable. ☐ Check the configuration on internet.nl. **Objective** ☐ Set: p=reject. ☐ Set percentage to 100%. ☐ Check the result on internet.nl. **Other** We advise using your reporting tools. Tip: use the URIports or DMARC Advisor tool for example.

Step 4	**STARTTLS sending host**	**Mail server**	☐ Configure your mail server. ☐ Arrange certificates. ☐ Put the certificate expiry date on your calendar, with a reminder that gives you plenty of time to renew. ☐ Check the result on internet.nl.
Step 5	**DNSSEC sending host**	**DNS**	☐ Ask your registrar to enable DNSSEC. ☐ Check it's working on internet.nl.
Step 6	**DANE sending host**	**DNS**	For DANE to work, you must first configure DNSSEC and STARTTLS. ☐ Generate a DANE record using the Huque tool. ☐ Check on internet.nl and/or using this DANE checker. ☐ NB: whenever you update your mail server's STARTTLS certificate, you have to reset your DANE record. Once you've successfully configured DANE for outgoing mail, you can set it up for incoming mail.
Step 7	**SPF receiving host**	**Mail server**	☐ Configure your mail server. ☐ Check using your own tools. Want to send yourself test e-mails from an unauthorized IP address? 1. Go to https://emkei.cz/ and send yourself a spoofed email. 2. Check the headers and look for 'Authentication-Results'. If results are given, they should be 'spf=fail' or 'spf=softfail'. 3. In some cases, e.g. if it's an appliance, your mail server will provide handy graphics with data on mail with correct and/or incorrect SPF configurations.
Step 8	**DKIM receiving host**	**Mail server**	☐ Configure your mail server. ☐ Check using your own tools (as per step 7).
Step 9	**DMARC receiving host**	**Mail server**	To set up DMARC, your mail server must support SPF and/or DKIM. ☐ Configure your mail server. ☐ Consider sending RUA reports. ☐ Check using your own tools (step 7) and search for 'dmarc=pass'.
Step 10	**STARTTLS receiving host**	**Mail server**	☐ Check whether your mail software features support (possibly activated in step 4). ☐ Check the configuration on internet.nl.
Step 11	**DNSSEC receiving host**	**DNS**	☐ The sender has to configure this in the DNS.
Step 12	**DANE receiving host**	**Mail server**	To enable DANE, DNSSEC validation must be activated. ☐ Configure validation for DNSSEC. ☐ Configure the software. ☐ Check on havedane.net.
Step 13	**Recommendations**		☐ E-mail standards change all the time, so check every six months that everything's still okay (use internet.nl and other tools). ☐ Record all changes and embed them in your organisation. ☐ Share practical knowledge with colleagues.