LIBRARY, ICT SERVICES & ARCHIVE

Status: Definitief
Approved MT-LISA: 23-06-2023
Reviewed:27-06-2023
Author: Peter Peters

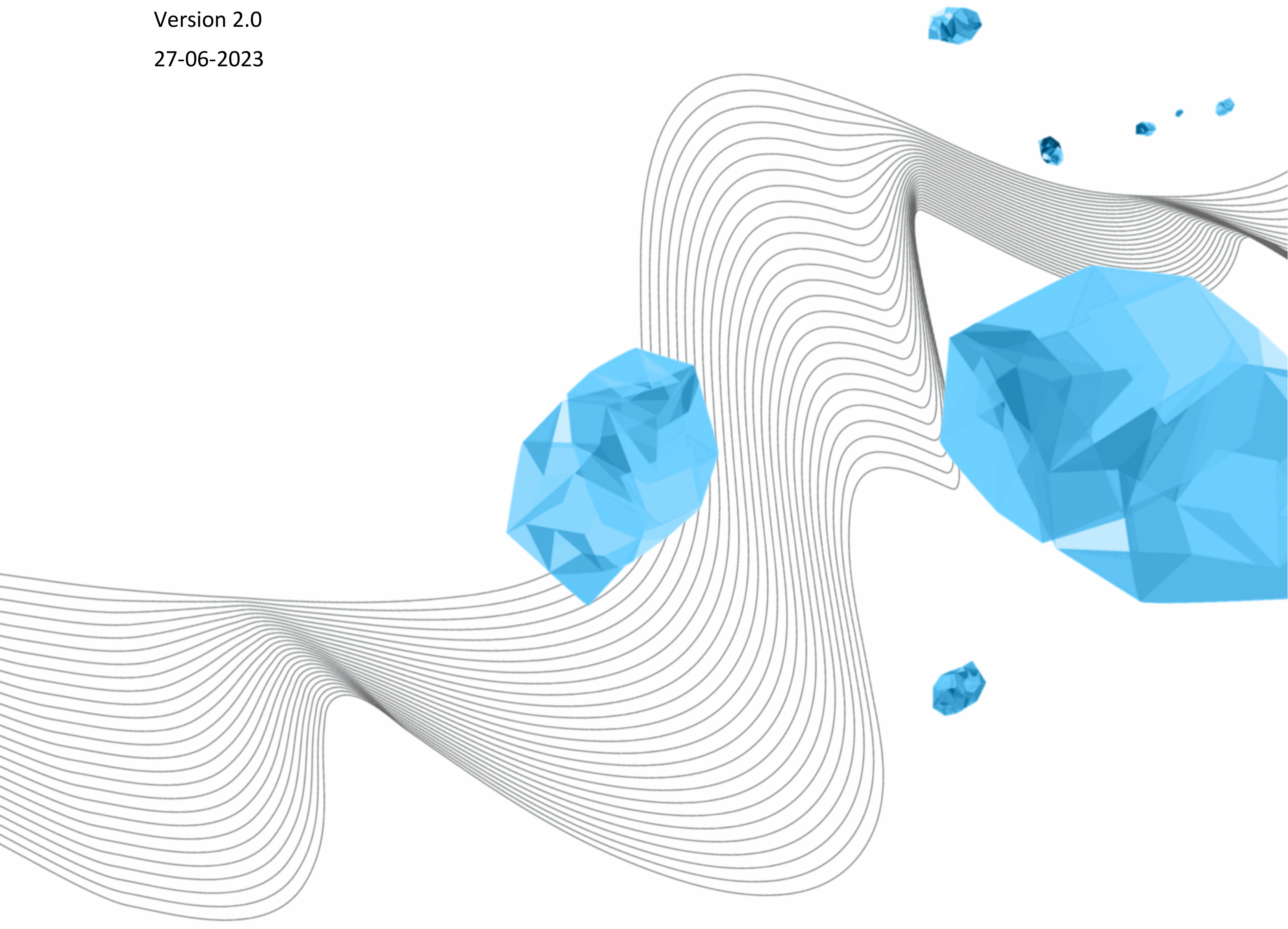
GUIDELINES ON EMAIL MESSAGE AUTHENTICATION

SPF, DMARC AND DKIM

LISA

Version 2.0

27-06-2023



UNIVERSITY OF TWENTE.

COLOPHON

ORGANISATION
Library, ICT Services & Archive

TITLE
Guidelines on Email Message Authentication

REFERENCE
LISA-0388

VERSION (STATUS)
2.0

DATE
27-06-2023

AUTOR(S)
Peter Peters

COPYRIGHT

© Universiteit Twente, Nederland.
All rights reserved. No part of this publication may be reproduced, stored in an automated database, or made public in any form or by any means, whether electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of the University of Twente.

DOCUMENT HISTORY

VERSION	DATE	AUTOR(S)	REMARKS
1.0	01-04-2020	P.G.M. Peters	Official version
2.0	15-06-2023	P.G.M. Peters	Added DMARC Changed SPF to include Microsoft Exchange Online

DISTRIBUTION LIST

VERSION	DATE	AUTOR(S)	DISTRIBUTED TO
1.0	01-04-2020	P.G.M. Peters	Published on Cyber Safety website
2.0	27-6-2023	P.G.M. Peters	CISO, ter vaststelling

REFERENCES

VERSION	DATE	AUTOR(S)	TITLE

CONTENT

1 INTRODUCTION

As an email sender, you've always been told that following email best practices is essential to get the best results from your email. One of these best practices is ensuring you're properly authenticating your email messages. Implementing these practices is hard for the regular user. Therefore the University of Twente has implemented several measures to support and promote safe email message authentication.

These guidelines describe how the university implements SPF, DMARC and DKIM, the pillars of email message authentication. SPF and DKIM describe ways to check for legitimate email messages. DMARC tells the receiving mail server what the university thinks should be done with messages that do not pass the SPF and DKIM checks.

2 WAYS THE UNIVERSITY USES SPF, DKIM AND DMARC

The university will publish DMARC information advising the receiving servers to drop messages that do not pass the checks for SPF or DKIM. If either indicates the email message does not arrive from a legitimate source, it can not be a message that originated from the university.

Below are guidelines on how the university (students and employees) and the university's suppliers should implement and use SPF and DKIM. The university controls DMARC.

3 CONSIDERATIONS

The guidelines defined in chapter 4 are based on a number of considerations that govern or limit the use of SPF, DMARC and DKIM. These considerations are explained in this chapter.

3.1 SPF LIMITATIONS

SPF has some limitations[1] in its use. An SPF RR has a practical limit of 255 characters. This limit means we are limited to the number of entries, either host names or IP addresses, we can include. SPF offers a solution by referring to other SPF RRs. If they are in the same domain, both SPF RRs added together should not exceed roughly 460 characters. The third and most dangerous limit is the number of requests a mail server should need to resolve the SPF RR. That number is ten (10).

While we can control the first two limitations, the latter is hardly manageable if we refer to external SPF records, like when using cloud service providers who want to send email messages with our addresses. Look, for instance, at the SPF RR for student.utwente.nl:

v=spf1 include:_spf.google.com include:_spf.snt.utwente.nl -all

This simple SPF RR only has two referrers, but still, the receiving mail server has to perform eight queries to decide whether the sending server is allowed to. Adding one or two extra referrers results in an email server being unable to complete a query, and the server will most probably refuse to accept the email.

[1] https://www.socketlabs.com/blog/best-practices-sender-policy-framework-spf/

If a SaaS provider wants to send email messages with our addresses, they always ask us to add their servers to our SPF RR.

v=spf1 include:_spf.example.com -all

That doesn't seem so bad, except when another SaaS provider has the same request.

v=spf1 include:_spf.example.com include:_spf.example.nl -all

Because we don't know how many referrers those companies use in their SPF RR, we have no idea if or when the limit of ten queries is reached.

3.2 MAIL SERVER OUTSIDE UT CONTROL

Another reason we do not allow entries for SaaS providers is that the university has no control over the servers the provider uses. A SaaS provider may use Amazon and ask us to add Amazon SES to our SPF RR.

v=spf1 include:_spf.amazonses.com -all

Because the SaaS provider does not know on what machine their software is running. It's the cloud, after all. They can't narrow it down any further. So by using this entry in our SPF RR, all Amazon SES customers could send messages using our email addresses. Even though we trust Amazon, we can not trust its customers, as is also the case with Azure and Google Cloud.

In some cases, creating a separate domain where the SaaS provider can define the SPF RR is possible. See Rule 6 in the policy below.

3.3 DOMAINS WITHOUT EMAIL

The university's email policy restricts email to only a few domains. Other domains should not be used to send or receive email. To prevent criminals from using these domains for phishing, we should publish an SPF RR indicating that any email from these domains should be treated as phishing.

This can include domains outside of utwente.nl.

3.4 DOMAINS FOR STUDENT ASSOCIATIONS AND THIRD PARTIES

Student associations and other third parties have domains under utwente.nl or separately. They are responsible for their own email and anti-phishing protection. The university will help them set up the proper protection. If they choose otherwise, we should take measures to prevent their measures from interfering with ours.

4 GUIDELINES

The above considerations result in the below rules for SPF RR entries.

1. For utwente.nl, only the official mail servers will be included in the SPF RR.
   v=spf1 mx a:smtppool.utwente.nl a:edgepool.ad.utwente.nl include:spf.protection.outlook.com include:_spfout.mf.surf.net include:_spf.surfmailfilter.nl -all
2. The university uses DKIM for outgoing messages for all @utwente.nl addresses.

3. The university will configure DMARC to enforce the SPF and DKIM checks for all their domains.
   v=DMARC1; p=reject; sp=none; fo=s; ri=3600; rua=mailto:dmarc@utwente.nl; ruf=mailto:dmarc+ruf@utwente.nl
4. Sub-domains for student associations and third parties can use whatever SPF or DKIM configuration they want. We urge them to adhere to these guidelines as much as possible.
5. If a SaaS provider needs to send email messages using our addresses, we urge them to use our SMTP server to send email. These messages will then fall under the central SPF and DKIM configuration.
6. If a SaaS provider can not send email messages through our servers and wants to use SPF, a separate email domain will be configured with the requested SPF RR.
   v=spf1 include:_spf.example.com -all
   The SaaS provider is responsible for adhering to the limits imposed on SPF RRs for this domain. They should also configure DKIM for that domain.
7. Email messages with addresses including other subdomains, e.g. for departments, are not allowed. The same goes for other domains under the responsibility of the university. An SPF RR to indicate that must be configured for each (sub)domain.
   v=spf1 -all
8. The university is responsible for all its domains. Therefore the university will keep control of the information published through their nameservers. This allows the university to change any published SPF, DKIM or DMARC information. The university will do so when abuse is detected or for any other reason.

5 REVIEW OF THESE GUIDELINES

These Guidelines will be reviewed at least every three years. The following review will be mid-2026. There may be grounds for an interim evaluation of these guidelines. If that evaluation gives cause to do so, the guidelines will be adjusted sooner.

Security management of the University of Twente is responsible for these guidelines.

The CISO determines these guidelines.