TLS-RPT & MTA-STS – Modernisering av e-postskyddet

Denna övergripande guide beskriver hur du **säkrar** din e-postleverans mot avlyssning och nedgraderingsattacker genom att aktivera internetstandarderna **TLS-RPT** och **MTA-STS**.

Exemplen i guiden utgår från domänen **workgroup.se** och hur konfigurationen görs i kontrollpanelen hos **one.com** efter migreringen 2026-10-22.

Genom att kombinera dessa två tekniker säkerställer du att omvärldens e-postservrar alltid kommunicerar med dina servrar över krypterade tunnlar, **vilket skyddar mot så kallade ”man in the middle”-attacker.**

Översikt

För att göra implementeringen så pedagogisk som möjligt delar vi upp den i två logiska delar, där vi börjar med det enklaste rapporteringsskyddet.

Standard / Teknik	Funktion & Syfte	Svårighetsgrad
🟢 **Del 1: TLS-RPT** *(RFC 8460)*	**SMTP TLS Reporting.** Domänen signalerar till omvärlden att den vill ha automatiska rapporter om krypteringen (TLS) misslyckas vid e-postöverföring.	**Enkel** 🟢 *(Kräver endast en DNS-post och separat e-postadress)*
🟡 **Del 2: MTA-STS** *(RFC 8461)*	**SMTP MTA Strict Transport Security.** Tvingar fram säker, krypterad e-postöverföring via TLS och förhindrar avlyssning samt så kallade *Man-in-the-middle*-attacker.	**Måttlig** 🟡 *(Kräver en webbfil i en specifik underkatalog under en subdomän och en DNS-post)*

🟢 Del 1: Kom i gång med TLS-RPT (RFC 8460)

Innan vi publicerar instruktionen i DNS måste vi ha en separat e-postadress för de automatiska rapporterna. Vi rekommenderar att du alltid använder en separat brevlåda eftersom rapporterna skickas som maskinläsbara XML/JSON-filer i bakgrunden. Detta underlättar även om du vill sätta upp en automatisk vidarebefordran eller läsa in filerna i ett externt rapportsystem.

Förutsättning: Skapa en e-postadress i din kontrollpanel, exempelvis: tlsrpt@workgroup.se.

När e-postadressen är aktiv är vi redo att aktivera rapporteringen genom att lägga till följande TXT-post i DNS-inställningarna hos one.com:

TXT-post i DNS:

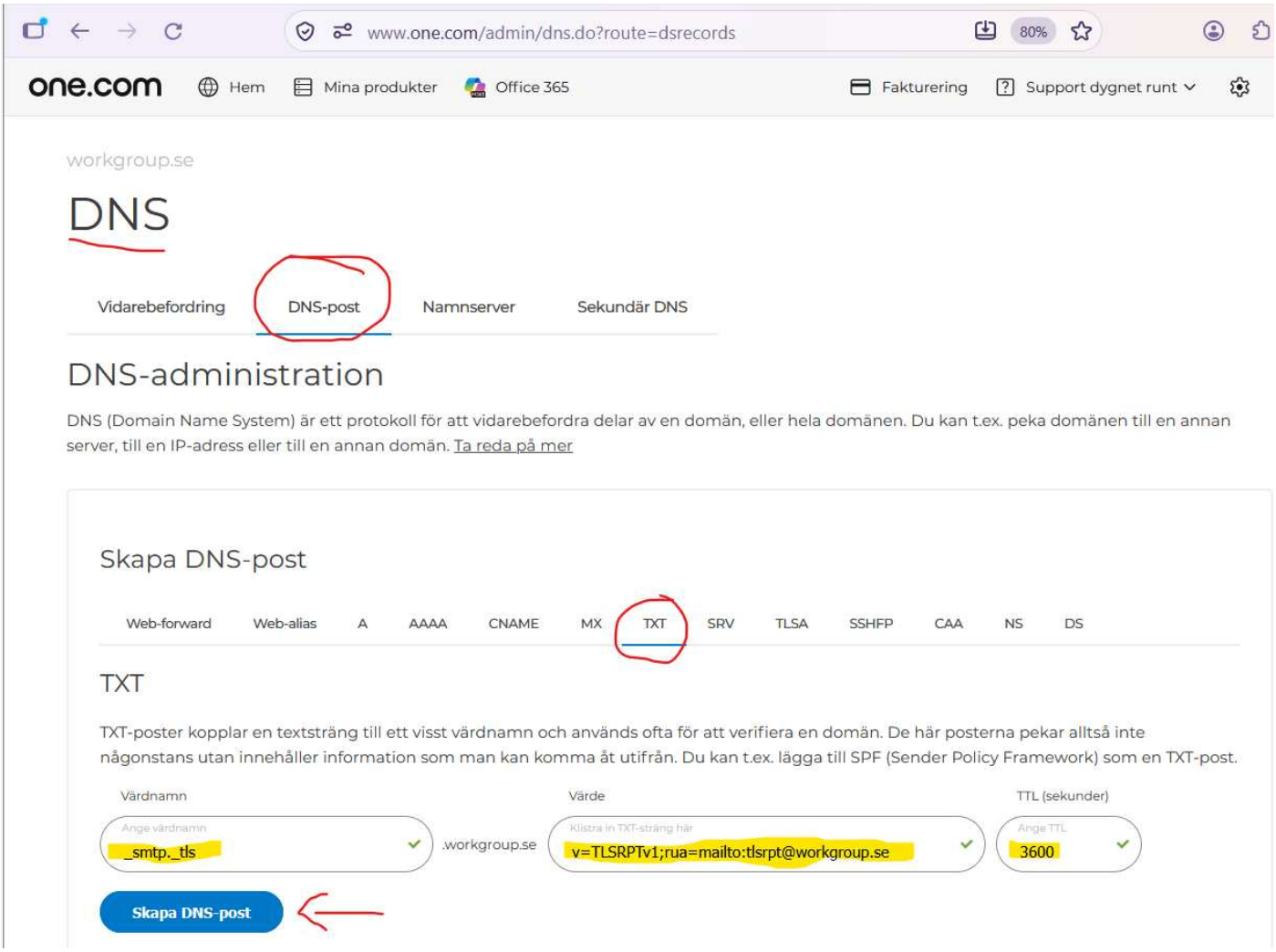
Host: **_smtp._tls**

Value: **v=TLSRPTv1;rua=mailto:tlsrpt@workgroup.se**

TTL: **3600**

Nedan visas ett skärmklipp från one.com med DNS-inställningen för TLS-RPT

one.com: Kontrollpanelen / Domän / DNS-inställningar



🟡 Del 2: Kom i gång med MTA-STS (RFC 8461)

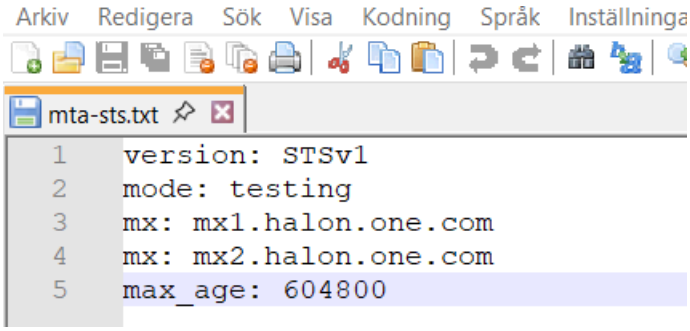
Till skillnad från TLS-RPT räcker det inte med att bara lägga till en DNS-post för MTA-STS.
Denna standard kräver att du publicerar en specifik textfil på en krypterad subdomän (HTTPS) i en specifik underkatalog. Mottagande e-postservrar kommer att besöka denna webbadress för att läsa in din säkerhetspolicy.

🟡 Steg 1: Skapa textfilen **mta-sts.txt**

För att skapa filen fungerar vanliga Anteckningar (Notepad) i Windows utmärkt, men i detta exempel använder vi Notepad++.

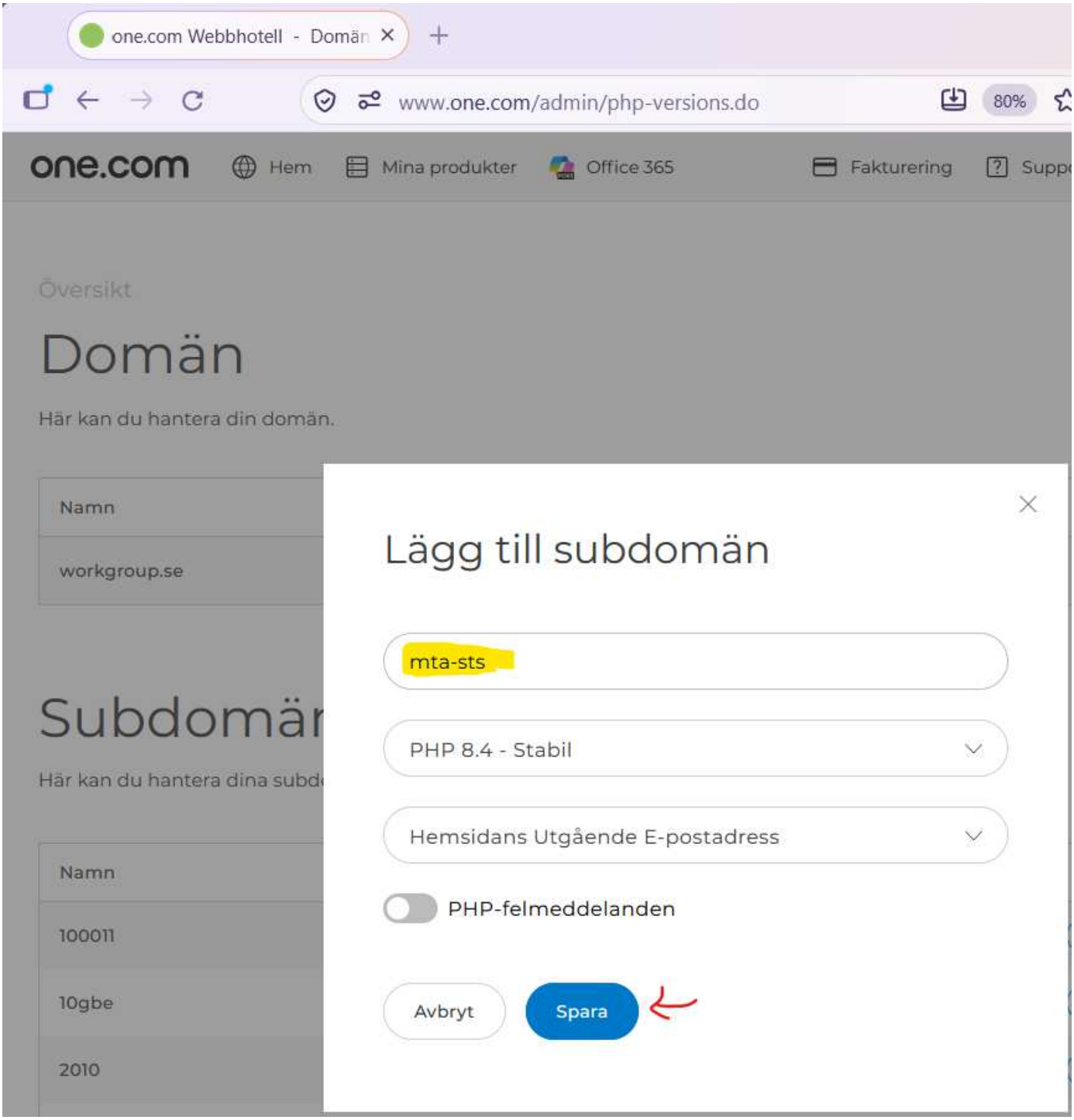
version: STSv1
mode: testing
mx: mx1.halon.one.com
mx: mx2.halon.one.com
max_age: 604800

Skärmklipp nedan från Notepad++

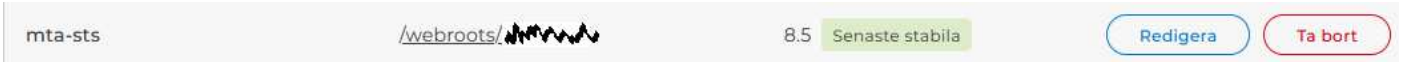


🟡 Steg 2: Lägg till subdomänen mta-sts

one.com: Kontrollpanelen / Domän / Underdomäner



När subdomänen skapats är det viktigt att du noterar var den ligger dvs under /webroots/**XXXXXXXX**



🟡 Steg 3: Anslut med SFTP till ditt konto

För att kunna skapa kataloger samt ladda upp vår textfil mta-sts.txt behöver vi numera ansluta via SFTP och något lämpligt program exempelvis Filezilla, WinSCP eller för macOS Transmit.
(innan kunde man skapa katalog i roten på domänen men nu säkras subdomäner lite extra)

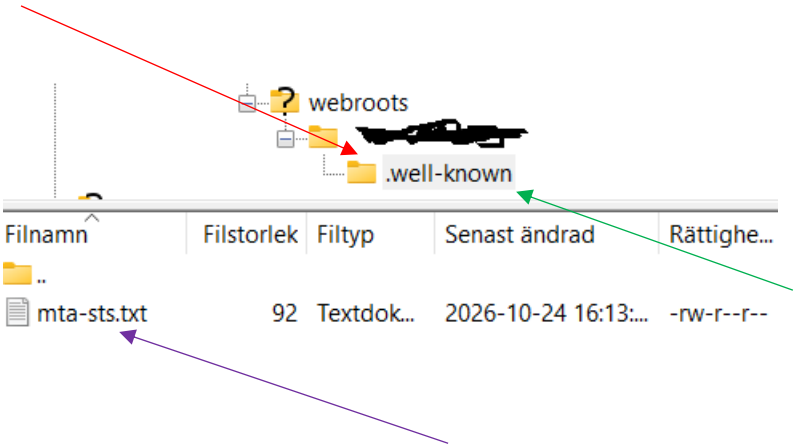
Besök nedan om du inte har inloggningsuppgifter eller behöver nollställa lösenord.

one.com: Kontrollpanelen / Hosting Inställningar / SSH & SFTP

Jag använder FileZilla, och tips om hur du hämtar programmet utan reklam finns under referenser i slutet av dokumentet.

Med FileZilla loggar jag in med SFTP och väljer rätt katalog för subdomänen. Vilken katalog som är den rätta ser du under den webroots/**XXXXXX**-sökväg vi noterade innan.

Därefter **högerklickar vi och väljer skapa katalog ".well-known"**. Det är mycket viktigt att du får med **punkten i början**.



Tryck sedan på katalogen **.well-known**

Slutligen drar vi in den skapade filen **mta-sts.txt** i katalogen **.well-known**

🟡 Steg 4: Lägga till DNS-poster för MTA-STS

Nästa steg i testläget (mode: testing) är att lägga upp TXT i DNS:en på samma sätt som för TLS-RPT.

Id kan vara vad som helst men jag rekommenderar datum plus klockslag ÅÅÅÅMMDDHHMM, vilket är "best practice" enligt RFC 8461.

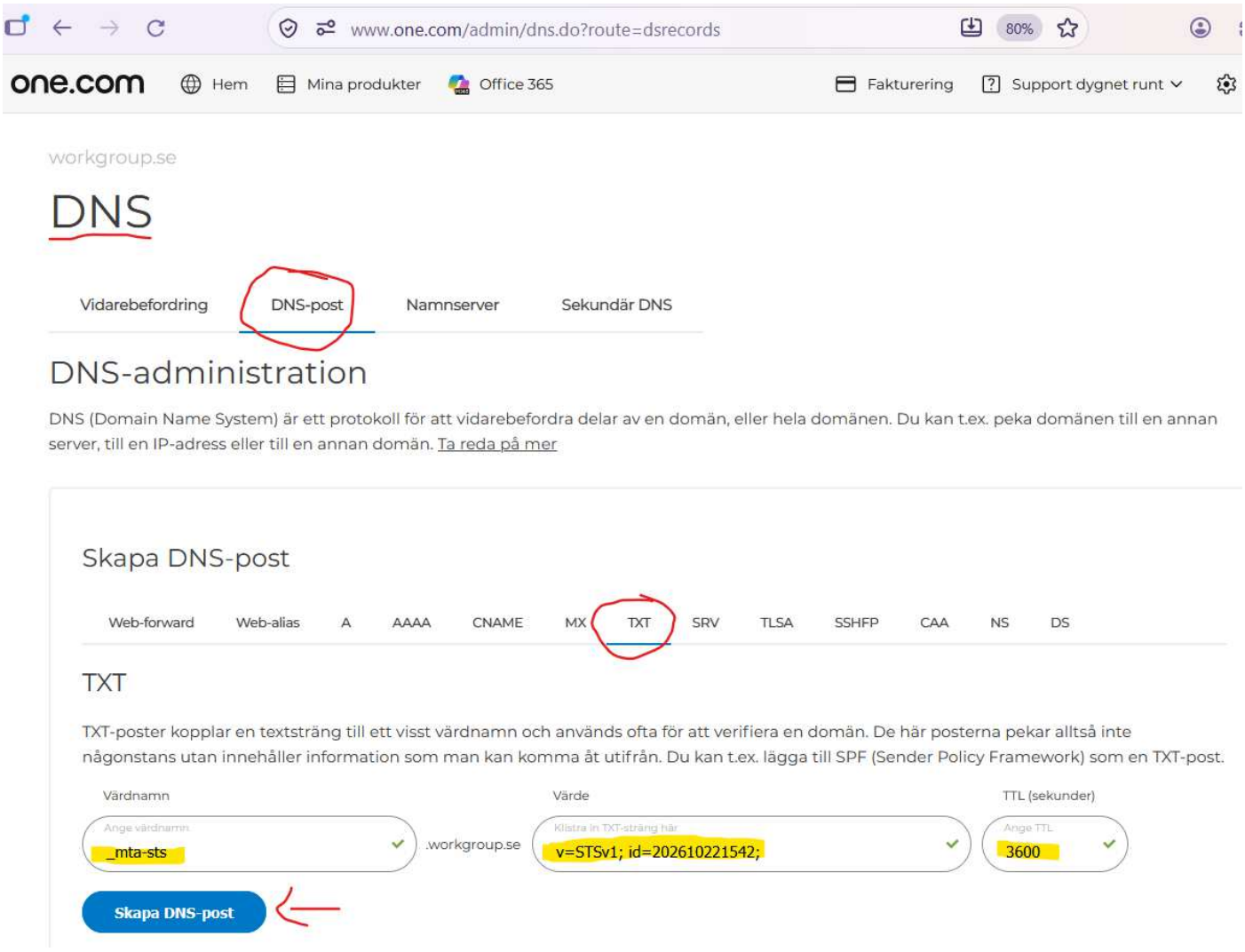
TXT-post i DNS:

Host: **_mta-sts**

Value: **v=STSv1; id=202610221542;**

TTL: **3600**

one.com: Kontrollpanelen / Domän / DNS-inställningar



🟡 Steg 5: Fungerar det och hur man ändrar från testläge (testing) till skarpt (enforce)

Referenser & Slutkontroll

När DNS-posterna har spridit sig (TTL 3600 sekunder blir en timme) kan du göra en fullständig extern validering för att säkerställa att din domän nu har ett fullgott betyg under sektionerna för både krypteringsintegritet och rapportering.

Efter att ha kontrollerat vad som loggas, samt även undersökt att det kommer in rapporter till e-postadressen tlsrpt@workgroup.se, är nästa steg att aktivera skyddet fullt ut. Detta görs lämpligen efter några dagar eller veckor.

Ändra i textfilen **mta-sts.txt**

Ersätt mode: testing med mode: enforce och ladda slutligen upp filen via SFTP för att ersätta den gamla versionen.

OBS! Kom ihåg att alltid uppdatera värdet för id= i DNS-posten _mta-sts varje gång du gör ändringar i textfilen.

v=STSv1; id=202610221542; (Ändra id= till dagens datum och klockslag)

Du bör kunna kontrollera att filen är publicerad i en vanlig webbläsare via:
https://mta-sts.dindomän.se/.well-known/mta-sts.txt

I vårt exempel:
https://mta-sts.workgroup.se/.well-known/mta-sts.txt

Kontroll-sidor:
https://www.uriports.com/tools/mtasts-validator?domain=workgroup.se
https://easydmarc.com/tools/mta-sts-check?domain=workgroup.se
https://www.mailhardener.com/tools/mta-sts-validator?domain=workgroup.se

Om du ändrar något i textfilen mta-sts.txt **MÅSTE** du uppdatera id-numret ovan i DNS:en.

Identifiera din DKIM-selektor via brevhuvudet
Det finns olika externa testprogram där man ibland manuellt får lägga till sin DKIM-selektor.
Denna listas som **s=** i meddelandets brevhuvud (*e-postheader*).

Öppna ett e-postmeddelande som du har skickat till dig själv och välj att visa meddelandeinformationen (*message header*).

Sök efter texten **s=**. Det kan se ut ungefär så här:

”DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; t=1790004239; x=1790609039; d=workgroup.se; ***s=rsa1****;”*

Det värde som du ska ange manuellt i testprogrammet för DKIM i detta fall är alltså: **rsa1**

Referenser (fungerande 2026-10-22)

MTA-STS (Wikipedia)
https://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol#SMTP_MTA_Strict_Transport_Security

Microsoft: Enhance mail flow with MTA-STS
https://learn.microsoft.com/en-us/exchange/security-and-compliance/enhance-mail-flow-using-strict-transport-security

Google MTA-STS och TLS-rapportering
https://knowledge.workspace.google.com/admin/gmail/advanced/about-mta-sts-and-tls-reporting?hl=sv

FileZilla – The free FTP solution
https://filezilla-project.org/ https://filezilla-project.org/download.php?show_all=1
💡 Tips: Klicka på den lilla länken under knappen där det står "**Show additional download options**".
Välj filen som heter FileZilla_X.YY.Z_win64-setup.exe (i stället for den som heter _sponsored-setup.exe).

Notepad++ - is a free source code editor and Notepad replacement.
https://notepad-plus-plus.org/

För dig som vill läsa de ursprungliga och exakta tekniska specifikationerna direkt från internets standardiseringsorgan.

RFC 8460 (SMTP TLS Reporting)
https://www.rfc-editor.org/info/rfc8460/

RFC 8461 (SMTP MTA Strict Transport Security)
https://www.rfc-editor.org/info/rfc8461/

Dokumentlagring

- Senaste version av detta dokument finns sparat under https://workgroup.se/pdf/
- Direktlänk till senaste versionen (PDF/A) https://workgroup.se/pdf/nutidssakring-epost-tlsrpt-mta-sts.pdf

Workgroup DreamTeam 2026