E-mailové reputační systémy

Ondřej Caletka, CESNET

21. dubna 2017

Elektronická pošta se často stává terčem nejrůznějších kampaní, šířících spam nebo phishing. Navíc obecně umožňuje komukoli vydávat se za kohokoli. V tomto příspěvku shrneme techniky, které se používají k prokazování autenticity zpráv a potažmo také možnosti, jak neautentické zprávy detekovat a filtrovat.

1 Sender Policy Framework

Principem SPF (původně zkratka znamenala *Sender Permitted From*) je dát možnost vlastníkovi DNS domény deklarovat, které servery jsou oprávněny odesílat e-mailové zprávy jménem domény. Příjemce pošty pak může validovat, zda poštu od dané domény dostává z autorizovaného serveru a podle toho zohlednit další nakládání se zprávou.

Majitel domény `example.com` může například specifikovat politiku, že poštu z adres `@example.com` mohou předávat pouze servery z adresního rozsahu 192.0.2.0/24 takovýmto DNS záznamem:

```
example.com   IN  TXT  "v=spf1 ip4:192.0.2.0/24 -all"
```

1.1 Pass, neutral, fail, softfail

Obsah `TXT` záznamu obsahuje vždy povinné záhlaví `v=spf1` následované mezerou oddělenými slovy, která definují povolené, nebo naopak zakázané rozsahy adres. Každé slovo může být uvozeno kvalifikátorem, jejichž význam shrnuje tabulka 1.

Tabulka 1: Význam kvalifikátorů SPF

znak	**název**	**význam**
+	pass	daný rozsah adres vyhovuje politice (výchozí)
?	neutral	pro daný rozsah adres politika neexistuje
-	fail	daný rozsah adres nevyhovuje politice
∼	softfail	daný rozsah adres spíše nevyhovuje politice

Jako rozsah adres pak mohou být kromě výše uvedeného příkladu se slovy `all` pro všechny adresy a `ip4` pro daný rozsah adres použita také klíčová slova `a` a `mx`, která doplní IP adresu získanou DNS dotazem na příslušný typ doménového záznamu. Nejlepší současná praxe ale doporučuje se takovýmto zřetězením vyhnout za účelem snížení počtu DNS dotazů, které musí validátor vykonat.

Pravidla se při validaci vyhodnocují v pořadí, v jakém jsou zapsána, po nalezení první shody se další nezkoumají. Neexistující politika vrací stav *neutral*, je tedy ekvivalentní existenci záznamu:

```
example.com   IN  TXT  "v=spf1 ?all"
```

Příjemce pošty, který SPF záznam validuje, tak činí ideálně ještě v průběhu SMTP komunikace. Nejprve by měl pomocí SPF validovat jméno hostitele, kterým se představí klient v SMTP příkazu `HELO/EHLO`, následně validuje adresu domény, uvedenou v příkazu `MAIL FROM`. Pokud na základě vyhodnocení SPF rozhodnuto o nepřijetí zprávy, měla by být odmítnuta již během SMTP komunikace.

1.2 TXT nebo SPF?

SPF je jedním z protokolů, jehož vývoj probíhal ve spěchu a tak trochu mimo půdu IETF. Jedním z důsledků kvapného zavádění je způsob, jakým protokol SPF přikládá význam DNS záznamům typu `TXT`. Ty byly původně určeny pro nestrukturované textové informace. SPF těmto informacím přikládá speciální význam a dopouští se tak klasické chyby známé ve světě databází jako *metadata v datech*.

Na půdě IETF proto kdysi vznikla snaha situaci napravit zavedením nového typu DNS záznamu `SPF`, který bude mít stejný význam jako záznam typu `TXT`, bude však určen jen pro potřebu SPF. Tato snaha ovšem dopadla fiaskem; než se podpora pro nový typ DNS záznamu dostala do DNS serverů a jejich uživatelských rozhraní, bylo SPF již velmi rozvinuto. Validátory tak musely kontrolovat dva různé DNS záznamy a řešit případně rozpory. Přítrž tomu učinil nejnovější standard RFC 7208, který záznam typu `SPF` rezervuje pro budoucí revize standardu, zatímco pro aktuální verzi 1 nařizuje – v souladu se současnou praxí – použití záznamu typu `TXT`.

1.3 Problém s přeposíláním pošty

Mnohem zásadnější je ale koncepční problém s přeposíláním pošty na straně příjemce. Mějme příklad se třemi entitami:

- $\mathbb{A}$ publikuje SPF politiku, obsahující tvrdé selhání pro nepovolené adresy
- $\mathbb{B}$ nemá s SPF nic společného, jen provozuje e-mailové schránky a nabízí svým uživatelům přesměrování pošty na jinou adresu

- $\mathbb{C}$ validuje SPF politiku a poštu, u které SPF selhává, tvrdě odmítá

Problém nastane ve chvíli, kdy uživatel schránky u $\mathbb{B}$ nastaví přesměrování všech nebo vybraných zpráv od $\mathbb{A}$ na adresu u $\mathbb{C}$. K $\mathbb{C}$ se totiž v okamžiku přeposílání připojí server entity $\mathbb{B}$ a bude se snažit doručit zprávu, která bude v SMTP komunikaci `MAIL FROM` označena jako přicházející od $\mathbb{A}$. To $\mathbb{C}$ vyhodnotí jako porušení politiky a zprávu odmítne.

Zpráva se tedy nedoručí a není to ničí vina. Každá z entit však může nějakým způsobem proces ovlivnit s cílem snížit riziko takového nedoručení. Entita $\mathbb{A}$ má možnost použít kvalifikátor *softfail* namísto *fail* (tedy zakončit definici politiky `~all` namísto `-all`). Dává tím najevo, že si sice nepřeje, aby jiné adresy odesílaly poštu jejím jménem, ale nepřeje si tvrdé odmítnutí takových zpráv. Stejně tak entita $\mathbb{C}$ může nastavit svůj systém tak, aby i zprávy, jejichž SPF kontrola selže, podrobila pouze důkladnější kontrole, ale neodmítala. Standard definující SPF totiž záměrně nechává volnost v tom, co se má se zprávou na základě výsledku kontroly stát.

I entita $\mathbb{B}$ může přeposílání upravit tak, aby k porušování SPF politiky nedocházelo. Zdaleka nejjednodušší, nikoli však správné řešení, je přeposílání zpráv s prázdnou obálkovou adresou odesílatele. Negativním efektem takového řešení je, že odesílatel původní zprávy $\mathbb{A}$ se nedozví o případných problémech s doručením zprávy od $\mathbb{B}$ k $\mathbb{C}$. Další, spíše teoretickou možností, kterou připouští SPF standard, je odmítnutí zprávy, jejíž přeposlání by porušilo SPF politiku, návratovým kódem `551, User not local` spolu s uvedením adresy, na kterou má být zpráva odeslána přímo původním odesílatelem.

1.4 Přepisování adresy odesílatele podle SRS

Poslední možností, jak může entita $\mathbb{B}$ zabránit porušování SPF politiky, je systematické přepisování obálkové adresy odesílatele během přeposílání tak, aby případné informace o průběhu doručování k $\mathbb{C}$ bylo možné předat zpět odesílateli. Nelze to však udělat jednoduchým přepisem; takové řešení by ze serveru $\mathbb{B}$ efektivně vytvářelo *open relay*, který by mohl být zneužit k rozesílání spamu. Metoda zvaná *Sender Rewriting Scheme* přepisované adresy proti zneužití zabezpečuje buď kryptograficky, nebo použitím databáze.

V prvním případě je pro odesílatele `user@A.org`, posílajícího zprávu na server `B.org` tímto serverem při přeposílání vytvořena následující obálková adresa odesílatele:

```
SRS0=HHH=TT=A.org=user@B.org
```

Písmena `TT` jsou nahrazena časovou značkou, kdy byla přepsaná adresa použita, písmena `HHH` pak jsou nahrazena částí hashe, na jehož vstupu je adresa odesílatele, časový kód a náhodné tajemství, známé pouze serverům, které generují a validují přepsané adresy.

Protože zpráva ze serveru entity $\mathbb{B}$ přichází s obálkovou adresou entity $\mathbb{B}$, nepředstavuje její doručení žádný problém v SPF. Pokud dojde k problému s doručením přeposlané zprávy, je informace o problému poslána na výše uvedenou speciální adresu. Server $\mathbb{B}$ ze speciální adresy extrahuje původní adresu `user@A.org`, ověří, zda souhlasí hash a zda od časové značky neuplynula příliš dlouhá doba, a pokud vše souhlasí, zprávu předá původnímu odesílateli.

Takovýto přepis má jistá úskalí, související především s maximální povolenou délkou uživatelské části e-mailové adresy, kterou RFC 5321 stanovuje na 64 znaků. Zejména pak v případě, kdy k přeposílání a SRS přepisu dojde víc než jedenkrát. Z toho důvodu je pro takové případy definován zjednodušený formát:

```
SRS1=KKK=B.org==HHH=TT=A.org=user@B2.org
```

Písmena `KKK` představují nový hash, který vytvoří server `B2.org`. Při třetím a dalším přeposlání se již formát přepsané adresy nemění – případné zprávy jsou přeposlány přímo serveru, který provedl první přepis a od něj původnímu odesílateli.

Jinou možností přepisu adres je použití databáze. Každá adresa odesílatele se uloží do databáze pod náhodně vygenerovaným klíčem. Adresa se pak přepíše do tvaru:

```
SRS0=<klíč>@B.org
```

Při doručení zprávy na takovou adresu se skutečná identita odesílatele zjistí z databáze. Položky se z databáze se po určité době vyčistí, aby nebylo možné jednou naučenou adresu používat trvale. Výhodou použití databáze je hlavně omezení problémů s délkou uživatelské části e-mailové adresy. Nevýhodou naopak nutnost databázi synchronizovat a sdílet mezi všemi poštovními servery organizace.

Je zřejmé, že SRS je vcelku komplexní služba, která navíc není nativně podporována většinou poštovních serverů. O jejím nasazení se však vyplatí uvažovat zejména u nejrůznějších školních či univerzitních schránek, kde je míra přeposílání pošty velká.

2 DomainKeys Identified Mail

Systém DKIM slouží zabezpečení obsahu e-mailových zpráv před změnou prostřednictvím elektronického podpisu. Od zavedených systémů jako jsou PGP a S/MIME se liší především tím, že podepisování může provádět kterýkoli článek e-mailové infrastruktury, takže není nutné vyžadovat používání této technologie po uživatelích. Samotný podpis pak putuje se zprávou jako přídavná hlavička, například takováto:

```
DKIM-Signature: v=1; a=rsa-sha256; d=example.com; bh=3yZ…h2=;
 c=relaxed/relaxed; s=dep1; h=Date:From:To:Subject:From;
 b=Wo/qoyff…M0yBh5UqQ=
```

Hodnota `v=1` určuje verzi, `a=` použitý algoritmus podpisu, `d=` je identifikátorem domény, která podepisuje, `bh=` je hash těla zprávy a `b=` vlastní hodnota elektronického podpisu. Binární hodnoty jsou uloženy v kódování Base64.

K ověření podpisu se nepoužívá ani hierarchie veřejných klíčů, ani síť důvěry; veřejný klíč potřebný k ověření podpisu se jednoduše umístí do DNS v podobě `TXT` záznamu, opět v Base64 kódování. Ačkoli se zde také používá obecný typ záznamu `TXT`, kolizi s jinými účely se brání předepsaným prefixem `_domainkey`, za který je připojena doména, která má být zdrojem podpisu. Aby bylo možné klíče hladce měnit a/nebo používat různé klíče v různých částech organizace, je každý DNS záznam s klíčem uvozen tzv. *selektorem* (volba `s=`), což může být naprosto libovolný řetězec, splňující požadavky na platné DNS jméno.

2.1 Nejde o náhradu SPF

Ačkoli se zdá, že účel, ke kterému DKIM existuje, je podobný účelu SPF, není tomu tak. Připomeňme, že SPF řeší pouze autorizaci e-mailového serveru, či obálkové adresy odesílatele, která je předávána v průběhu SMTP komunikace. SPF nijak nezkoumá ani hlavičky, ani vlastní obsah e-mailové zprávy. Proti šíření nejrůznějších podvržených zpráv, sloužících nejčastěji phishingu, které mají v pořádku obálkovou adresu odesílatele, žádným způsobem nepomáhá.

DKIM naopak autorizuje **obsah zprávy**, zcela bez ohledu na to, jakým způsobem byla zpráva doručena. Samotný standard DKIM také na rozdíl od SPF nepředepisuje vůbec žádnou politiku, která by stanovovala, co se má stát se zprávami, jejichž elektronický podpis nevyhoví. Dokonce jeden z cílů DKIMu vyžaduje, aby zprávy s nevalidním DKIM podpisem byly hodnoceny stejně jako zprávy bez jakéhokoli podpisu. To umožňuje DKIM podepisování nasadit beze strachu ze zhoršení spolehlivosti e-mailového systému.

2.2 Kanonizace a přepodepisování hlaviček

Při konfiguraci podepisovacího softwaru jsou k dispozici volby, které by neměly uniknout administrátorově pozornosti. Tou první je kanonizace, tedy jakási předúprava hlaviček a těla zprávy před provedením vlastního elektronického podpisu. Výchozí hodnota `c=simple/simple`, žádnou úpravu neprovádí a tak k poškození elektronického podpisu dojde i sémanticky nevýznamnou změnou hlaviček (úprava velikosti písmen názvů hlaviček) či obsahu (přidání či odebrání bílých mezer). Ačkoli asi panuje všeobecná shoda na tom, že systémy předávající poštu by takové úpravy dělat neměly, není

Tabulka 2: Přehled ADSP politik

název	**význam**
`dkim=unknown`	politika neexistuje (výchozí)
`dkim=all`	všechny zprávy mají být podepsány autorovou doménou
`dkim=discardable`	zprávy, jejichž validace selže, mají být zahozeny

od věci zabezpečit DKIM tak, aby i takto upravená zpráva byla validovatelná. K tomu slouží nastavení kanonizace na `c=relaxed/relaxed`. První hodnota se vztahuje k hlavičkám, druhá k tělu zprávy.

Další zajímavou volbou je vynucené podepsání některých hlaviček, byť ve zprávě nejsou přítomny. Vzhledem k tomu, že hlavičky se během cesty zprávy sítí přidávají, nepodepisuje DKIM všechny, ale pouze ty, které byly vyjmenovány ve volbě `h=` v samotném DKIM podpisu. Typicky bude obsahovat něco jako:

```
h=Date:From:To:Subject:From;
```

Vyskytuje-li se hlavička vícekrát, musí ji i metadata podpisu obsahovat vícekrát; při validaci se přibírají hlavičky postupně odspodu. Hlavičky, které nejsou v seznamu uvedeny, případně další výskyty uvedených hlaviček, nejsou do podpisu zahrnuty. Pokud v nastavení podepisovacího nástroje zapneme *přepodepisování* hlavičky `From`, bude do podpisu zahrnuta i neexistující druhá hlavička `From`. Díky tomu případný útočník nemůže do zprávy dodatečně vložit druhou hlavičku From, která by nebyla DKIMem kryta a mohla tak příjemce zprávy uvést v omyl, kdo je skutečným autorem zprávy. Stejný princip je možné použít například také pro hlavičku `Reply-To`, čímž lze útočníkovi zabránit nedetekovatelně odklonit odpovědi na zprávu na jinou adresu.

2.3 Politika podepisování ADSP

Samotný DKIM nijak nestanovuje, co se má stát se zprávami, které podepsané nejsou, ani to, jakou váhu má DKIM podpis od jiné domény než té, která je uvedena v adrese odesílatele. Aby mohl DKIM opravdu pomoci proti šíření podvržených zpráv, definuje RFC 5617 politiku *Author Domain Signing Practices*. Jedná se o další DNS záznam typu `TXT` na pevně dané subdoméně `_adsp._domainkey`, který může definovat jednu ze tří politik. Ty shrnuje tabulka 2.

Nejpřísnější politika `discardable` je určena výhradně pro domény, které odesílají strojem generované e-maily, u kterých je důležitý boj proti podvrženým zprávám, například automatická sdělení bankovních institucí, případně pro domény, které vůbec nejsou určeny pro e-mail. Tato volba **není určena** pro domény, ve kterých mají schránky uživatelé. To proto, že existuje několik málo legitimních služeb, případně služeb *na hraně legitimity*, které přísnou podmínku podepsání nesplní, ale je žádoucí, aby byly přesto

doručeny. Takovou službou může být posílání e-pohlednic či článků e-mailem, nebo mnohem častěji e-mailové konference.

2.4 Problém ADSP s e-mailovými konferencemi

Elektronický podpis, který DKIM používá, chrání zprávu a několik jejích hlaviček před modifikací a je tedy neslučitelný s většinou systémů, které zprávy modifikují. Pokud tedy máte ve své síti antivir, který s oblibou do všech zpráv připíše *„Odchozí zpráva neobsahuje viry, zkontrolováno nejlepším antivirem na světě“*, případně vás právní oddělení donutilo ke každému e-mailu připsat *právní doložku* nutící nahodilé příjemce zprávu okamžitě smazat a všechno, co v ní bylo napsáno, zapomenout, je nutné takové systémy buď nepoužívat, nebo zařadit ještě před vytvoření DKIM podpisu.

Zařízení, která legitimně zprávu modifikují, jsou i e-mailové konference. U nich je žádoucí, aby zpráva přeposlaná od konference převzala identitu toho, kdo ji do konference odeslal. Zároveň ale konference zprávu často modifikuje způsobem, který není slučitelný s DKIM podpisem:

1. odstraňuje nevhodné přílohy
2. přidává patičku s informacemi o konferenci
3. přidává název konference do předmětu zprávy
4. přidává hlavičku `Reply-To` na adresu konference

Problém je poměrně obsáhlý a nemá jediné vždy správné řešení. Věnuje se mu celé RFC 6377, publikované též jako BCP 167. Jedním z navržených postupů, jak se má konference chovat k podepsaným zprávám, které modifikuje, je následující:

1. validovat všechny DKIM podpisy
2. výsledek validace uložit do hlavičky `Authentication-Results` při současném odstranení všech předchozích hlaviček tohoto typu
3. odstranit ze zprávy všechny hlavičky s DKIM podpisy
4. podepsat zprávu vlastním klíčem, do podepsaných hlaviček přitom zahrnout i hlavičku `Authentication-Results`

Konference, která zprávy modifikuje, by také měla odmítat příspěvky a pokusy o přihlášení od adres v doménách, jejichž ADSP politika je stanovena na `discardable`. Takové zprávy by totiž po modifikaci konferencí byly nejspíše odmítnuty, což by konference mohla nesprávně vyhodnotit jako nefunkční schránku a respondenta odhlásit.

3 Domain-based Message Authentication, Reporting, and Conformance

Standard zvaný jako DMARC byl publikován v RFC 7489 v březnu 2015. Představuje jakési zobecnění ADSP politiky tak, aby kromě DKIM pokrývala i SPF a to s jediným cílem: zaručit, že adresa v hlavičce `From` je autentická. Zkoumá se tedy, zda dopis přišel z IP adresy, kterou doména odesílatele označuje v SPF záznamu jako povolenou a zda souhlasí podpis DMARC z odesílatelovy, případně přidružené domény. Chování DMARC validátorů by také mělo být konzistentní – specifikace nabízí výrazně méně prostoru pro lokální nastavení. Z toho důvodu by uplatnění DMARC politiky mělo mít přednost před uplatňováním SPF či ADSP politik.

Standard přidává také možnost reportování, které umožňuje držiteli odesílající domény získat automatizovaně informace o porušení politiky. Administrátor tak může odhalit například zaměstnance, kteří v rozporu s firemní SPF politikou posílají poštu přes cizí SMTP server.

3.1 DMARC záznam

Politika DMARC je specifikována opět v DNS záznamu typu `TXT` na pevně dané subdoméně `_dmarc`. Standard předepisuje, že záznam musí být nejvýše jeden. Příklad minimalistického záznamu, který obsahuje obě povinné volby, ale nemá žádný význam, vypadá takto:

```
_dmarc.example.com. IN TXT "v=DMARC1; p=none"
```

Volba `v=` určuje verzi politiky. Volba `p=` určuje vlastní politiku. Kromě hodnoty `none` může nabývat také hodnot `quarantine`, pro umístnění neověřitelných zpráv do karantény a `reject` pro úplné odmítnutí zpráv, které neprošly SPF a DKIM autentizací. Subdomény mohou používat samostatnou politiku definovanou buď v nezávislém DNS záznamu, nebo ve volbě `sp=`.

Číselná volba `pct=` může obsahovat procento zpráv, které DMARC validátorem analyzováno – tím je možné v případě velkých provozovatelů politiku postupně zavádět. Volby `adkim=` a `aspf=` nastavují, jak přísně bude porovnávána doména použitá v DKIM, resp. SPF validaci s doménou v hlavičce `From` e-mailové zprávy. Ve výchozím nastavení `r` je porovnávání uvolněné, vyhoví tedy i DKIM podpis/SPF záznam subdomény. Volbou `s` vynutíme striktní režim, kdy se doménové jméno musí shodovat přesně.

3.2 Hlášení o problémech

Pro nastavení reportování o problémech s validací slouží volby `rua=` a `ruf=`. První z nich slouží k odesílání agregovaných reportů, které typicky jednou denně shrnují počet úspěšně a neúspěšně ověřených zpráv, druhá slouží pro

okamžité reportování každé neúspěšně doručované zprávy. Jediným standardizovaným prostředkem přenosu je prozatím e-mail. Hlášení chodí ve formátu XML, který je komprimován gzipem a přiložen k e-mailové zprávě. Držitel záznamu může při specifikaci omezit maximální velikost zpráv, třeba na 10 MB:

```
rua=mailto:dmarc-rua@example.com!10m
```

Aby se zabránilo nevyžádanému zaplavování cizích e-mailových schránek DMARC reporty, není úplně snadné posílat reporty na e-mailovou adresu v jiné doméně. V takovém případě odesílatel reportu ověří, zda dal adresát dané doméně souhlas. Pokud bude chtít například držitel domény `example.com` posílat hlášení na adresu v doméně `@example.org`, musí k tomu majitel domény `example.org` dát souhlas vystavením následujícího DNS záznamu:

```
example.com._report._dmarc.example.org. IN TXT "v=DMARC1"
```

3.3 Problém s e-mailovými konferencemi

DMARC využívá k ověření autenticity odesílatele jako SPF, tak i DKIM, přičemž k úspěšnému ověření stačí splnit alespoň jednu z podmínek. Tím se eliminuje problém s přeposíláním pošty, neboť taková pošta sice poruší SPF, ale nepoškodí DKIM podpis. Problém s e-mailovými konferencemi však zůstává. Taková konference sice neporušuje SPF pravidla, nicméně posílá zprávy z typicky zcela jiné domény, takže pozitivní výsledek SPF autentizace je pro DMARC nepoužitelný.

V zásadě jediné funkční řešení spočívá v úpravě nastavení konference tak, aby posílala e-maily ze své adresy a adresu skutečného respondenta vkládala do hlavičky `Reply-To`. Takové chování sice eliminuje porušení DMARC politik, ale zase činí problém při validaci elektronicky podepsané zprávy ať už pomocí S/MIME nebo PGP.

4 Shrnutí

S trochou nadsázky to s odstupem času vypadá, že standard SPF řeší zhruba stejné množství problémů, jako sám vytváří. Je to nejspíš důsledek jeho překotného vývoje stylem *nejdřív nasadit – pak standardizovat*. Velcí e-mailoví hráči ho však vzali za svůj, a tak zbytku správců nezbývá než se přizpůsobit. Máte-li v plánu SPF zavést pro svoji doménu, začněte nejdříve průzkumem, kudy uživatelé e-mailových schránek odesílají svou poštu a případně nápravou špatného stavu. Stále totiž existuje nemalé procento lidí, kteří odesílají poštu pochybnými cestami začínajícími obvykle u SMTP serveru internetového poskytovatele. Situace se ale pomalu zlepšuje, i velcí freemailoví poskytovatelé nabízejí autentizované předávání pošty k tomu určenou službou Submission (TCP/587). Vzhledem k problému s přeposíláním rozhodně

nelze doporučit zavádět tvrdé `-all` a doufat, že problém bude vyřešen na jiné straně spojení. Volba *softfail* se jeví jako nanejvýš vhodná.

Standard DKIM byl primárně vyvinut jako vylepšení stávajícího systému s důrazem na možnost postupného nasazení bez rizika poškození funkčnosti stávající e-mailové infrastruktury. Postupně zprávy podepsané DKIMem začaly být zvýhodňovány velkými hráči na poli elektronické pošty – Google například v DKIMem podepsaných e-mailech automaticky zobrazuje obrázky – což zvýšilo zájem o technologii, zejména mezi rozesílateli hromadné obchodní korespondence.

Politika ADSP, jejímž cílem je použít DKIM k vynucení jistého standardu v doručování zpráv, již tak úspěšná nebyla, zejména s ohledem na e-mailové konference. Dalšími problémy bylo ne zcela přesně specifikované očekávané chování příjemce zpráv a nemožnost detekovat, že k porušení politiky došlo.

Standard DMARC se snaží vyřešit neduhy jak SPF tak ADSP a přijít s řešením, které umožní nakládat konzistentně s e-maily, které falšují adresu odesílatele. Takové chování je však bohužel běžné u e-mailových konferencí, které je potřeba nastavit tak, aby nepřeposílaly zprávy s původní adresou uživatele v hlavičce `From`. Díky možnosti hlášení je také možné odhalit legitimní poštu, která by byla zahozena, ještě před skutečným uplatněním politiky.