cesnet

DKIM VERSUS S/MIME

Jiří Ráž
CESNET

únor 2023
seminář o bezpečnosti sítí a služeb

S/MIME pro uživatele

- Slouží pro identifikaci odesílatele
- Podepisuje tělo zprávy
- Příjemce může snadno ověřit zda nebylo se zprávou manipulováno
- Nastavení a použití je čistě na uživatelské úrovni
- **Asymetrická šifra** (privátní a veřejný klíč, CA)
- Je možné použít pro end to end šifrování
- Veřejný klíč si musí obě strany vyměnit

DKIM pro servery

- **Slouží pro identifikaci odesílajícího serveru**
- **Server (doména) může používat více klíčů**
- **Podepisuje vybrané hlavičky zprávy** (h=Date:From:To:Subject:From;)
- **Ověření provádí přijímací server**
- **Nastavení a použití je na správci e-mailu**
- **Asymetrická šifra** (privátní a veřejný klíč)
- **Veřejný klíč je vystaven v DNS jako txt záznam** (_domainkey)
- **Společně se SPF je součástí DMARC**

S/MIM VS DKIM PŘEHLED

	S/MIME	DKIM
Asymetrická šifra	Ano	Ano
Validace	V poštovním klientu	Na serveru
Veřejný klíč	„Osobně“	V DNS
Podepisuje	Tělo	Hlavičky
Nastavuje	Uživatel	Správce

cesnet

DĚKUJI ZA POZORNOST

MÁTE NĚJAKÉ DOTAZY?