Opowieść

Historia domen, rejestrów i uwierzytelniania poczty oraz mapa książki.

- Domena i DNS publiczny: od HOSTS.TXT do DMARC

Domena i DNS publiczny: od HOSTS.TXT do DMARC

Poziom: podstawy

Dotyczy: domeny internetowe, rejestry i rejestratorzy (NASK dla .pl), DNS publiczny, DNSSEC, CAA, SPF, DKIM, DMARC (RFC 9989), MTA-STS i TLS-RPT, stan na 26 października 2026

Czas: ~15 min

Ta strona otwiera książkę o nazwie, pod którą Zielona istnieje w internecie: kto ją wydaje, kto ją trzyma, kto odpowiada światu na pytanie „gdzie jest poczta Zielonej” i jak udowodnić, że wiadomość z adresu `@zielona.example` naprawdę wysłała Zielona. Wracamy tu, gdy ktoś pyta, czyja jest domena, kiedy wygasa i dlaczego faktury lądują w spamie.

Skróty użyte na tej stronie (14)

Skrót	Co znaczy
CAA	Certification Authority Authorization: rekord DNS, który mówi, które urzędy certyfikacji mogą wystawiać certyfikaty dla domeny
DKIM	DomainKeys Identified Mail: cyfrowy podpis wiadomości e-mail
DMARC	Domain-based Message Authentication, Reporting and Conformance: reguła domeny mówiąca, co robić z mailem, który nie przeszedł SPF i DKIM
DNS	Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP
DNSSEC	DNS Security Extensions: podpisy cyfrowe w DNS, dzięki którym można sprawdzić, że odpowiedź nie została po drodze podmieniona
HOSTS.TXT	centralny plik z nazwami i adresami wszystkich komputerów wczesnego internetu, poprzednik DNS
IANA	Internet Assigned Numbers Authority: funkcja prowadząca strefę główną DNS i listę końcówek domen oraz rejestry numerów protokołów
ICANN	Internet Corporation for Assigned Names and Numbers: organizacja założona w 1998 roku, która ustala zasady dla domen globalnych i akredytuje rejestratorów
MTA-STS	Mail Transfer Agent Strict Transport Security: zasada opublikowana przez domenę, że poczta do niej ma być wysyłana wyłącznie szyfrowanym połączeniem z serwerem o ustalonej nazwie
MX	Mail Exchanger: rekord DNS wskazujący serwer poczty domeny

Skrót	Co znaczy
NASK	Naukowa i Akademicka Sieć Komputerowa: państwowy instytut badawczy, który prowadzi rejestr domen .pl i przyjmuje zgłoszenia przez rejestratorów (partnerów)
RFC	Request for Comments: oficjalny dokument opisujący standard internetowy, na przykład sposób działania danego protokołu; w ITIL także Request for Change, czyli wniosek o zmianę
SPF	Sender Policy Framework: rekord DNS mówiący, które serwery mogą wysyłać pocztę domeny
TLS-RPT	SMTP TLS Reporting: rekord _smtp._tls z adresem, na który serwery nadawców wysyłają raz na dobę raport o udanych i nieudanych szyfrowanych połączeniach z naszymi serwerami poczty (RFC 8460)

Skąd się wzięło

Początki nazw w internecie, plik HOSTS.TXT i narodziny DNS w RFC 882 i 883 z 1983 roku opisuje już Active Directory, DNS i DHCP: od X.500 i HOSTS.TXT do Entra ID. Tu zaczynamy w chwili, gdy nazwy stały się towarem. 15 marca 1985 roku zarejestrowano pierwszą domenę w `.com`, `symbolics.com`, a w 1998 roku powstał ICANN, który miał uporządkować rynek i otworzyć go dla wielu firm sprzedających domeny.

> **Pojęcie: rejestr i rejestrator.** Rejestr prowadzi bazę wszystkich domen w jednej końcówce (na przykład `.pl`) i jej serwery nazw. Rejestrator to firma, u której kupujemy domenę: zgłasza ją do rejestru, przyjmuje opłaty i daje nam panel. My jesteśmy abonentem, czyli właścicielem prawa do nazwy na czas opłacony.

Końcówkę `.pl` wpisano do bazy IANA 30 lipca 1990 roku. Domeną opiekował się najpierw zespół na Uniwersytecie Warszawskim, a od grudnia 1993 roku NASK. W grudniu 2002 roku NASK uruchomił program partnerski, czyli model z rejestratorami, a od marca 2017 roku każdy abonent `.pl` jest obsługiwany przez rejestratora, nie bezpośrednio przez rejestr. Strefa `.pl` daje domeny z DNSSEC od grudnia 2011 roku, a usługę Registry Lock, blokadę zmian na poziomie rejestru, od marca 2019 roku.

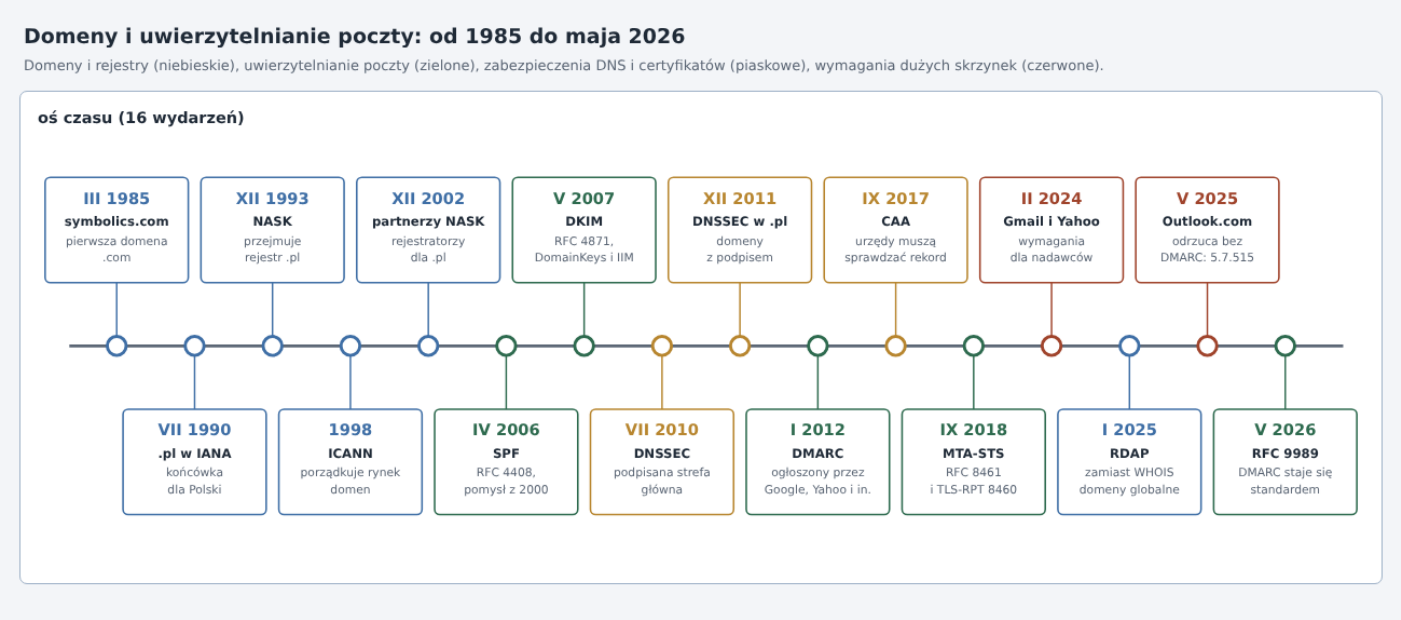
Druga połowa historii to poczta, w której pole „Od” przez lata można było wpisać dowolnie.

Mechanizmy obrony objaśnia Jak działa poczta: MTA, MDA, MUA, SMTP, kolejka, a tu tylko daty.

Mechanizm	Pierwsze kroki	Norma	Stan w 2026
SPF	pomysł w 2000, nazwa w 2003	RFC 4408 (2006), RFC 7208 (2014)	standard
DKIM	DomainKeys Yahoo i Identified Internet Mail Cisco, 2004	RFC 4871 (2007), RFC 6376 (2011)	standard

Mechanizm	Pierwsze kroki	Norma	Stan w 2026
DMARC	ogłoszony 30 stycznia 2012 przez Google, Yahoo, Microsoft, PayPal i innych	RFC 7489 (2015, dokument informacyjny)	w maju 2026 zastąpiony przez RFC 9989, 9990 i 9991
MTA-STS i TLS-RPT	szyfrowanie między serwerami pocztowymi	RFC 8461 i 8460 (wrzesień 2018)	standard
CAA	lista urzędów, które mogą wystawić certyfikat dla domeny	RFC 6844 (2013), RFC 8659 (2019)	sprawdzanie obowiązkowe dla urzędów od 8 września 2017

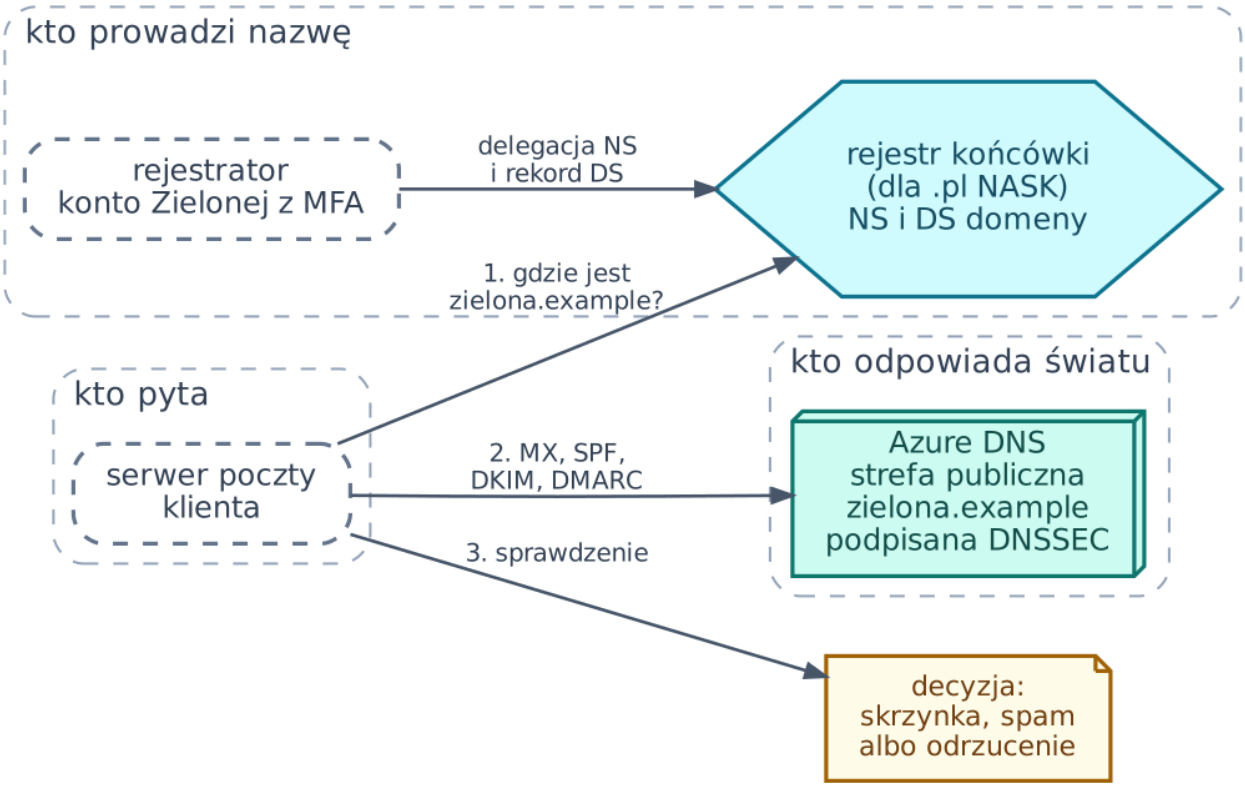
Od 1 lutego 2024 roku Gmail i Yahoo, a od 5 maja 2025 roku Outlook.com wymagają SPF, DKIM i DMARC od nadawców masowych, a Gmail i Yahoo od wszystkich przynajmniej SPF albo DKIM. Domena przestała być wizytówką, a stała się dowodem tożsamości firmy w poczcie.



Rysunek 1. Oś czasu domen i uwierzytelniania poczty: od pierwszej domeny .com w 1985 roku, przez domenę .pl, ICANN, SPF, DKIM, DMARC, podpisanie strefy głównej i CAA, po wymagania Gmaila i Outlooka oraz DMARC w RFC 9989 w 2026 roku (kliknięcie otwiera pełny rozmiar)

Jak to działa w jednym obrazku

Gdy serwer klienta dostaje wiadomość od pani Haliny, pyta rejestr końcówki, gdzie leży strefa Zielonej, a potem jej serwery nazw o rekordy MX, SPF, DKIM i DMARC. Podpis DNSSEC pozwala mu sprawdzić, że nikt nie podmienił odpowiedzi po drodze.



Rysunek 2. Kto odpowiada za nazwę zielona.example: rejestrator zgłasza domenę i rekord DS do rejestru, rejestr wskazuje serwery nazw dostawcy DNS, a serwer odbiorcy pyta je o MX, SPF, DKIM i DMARC, zanim zdecyduje, co zrobić z wiadomością (kliknięcie otwiera pełny rozmiar)

Dlaczego Zielona

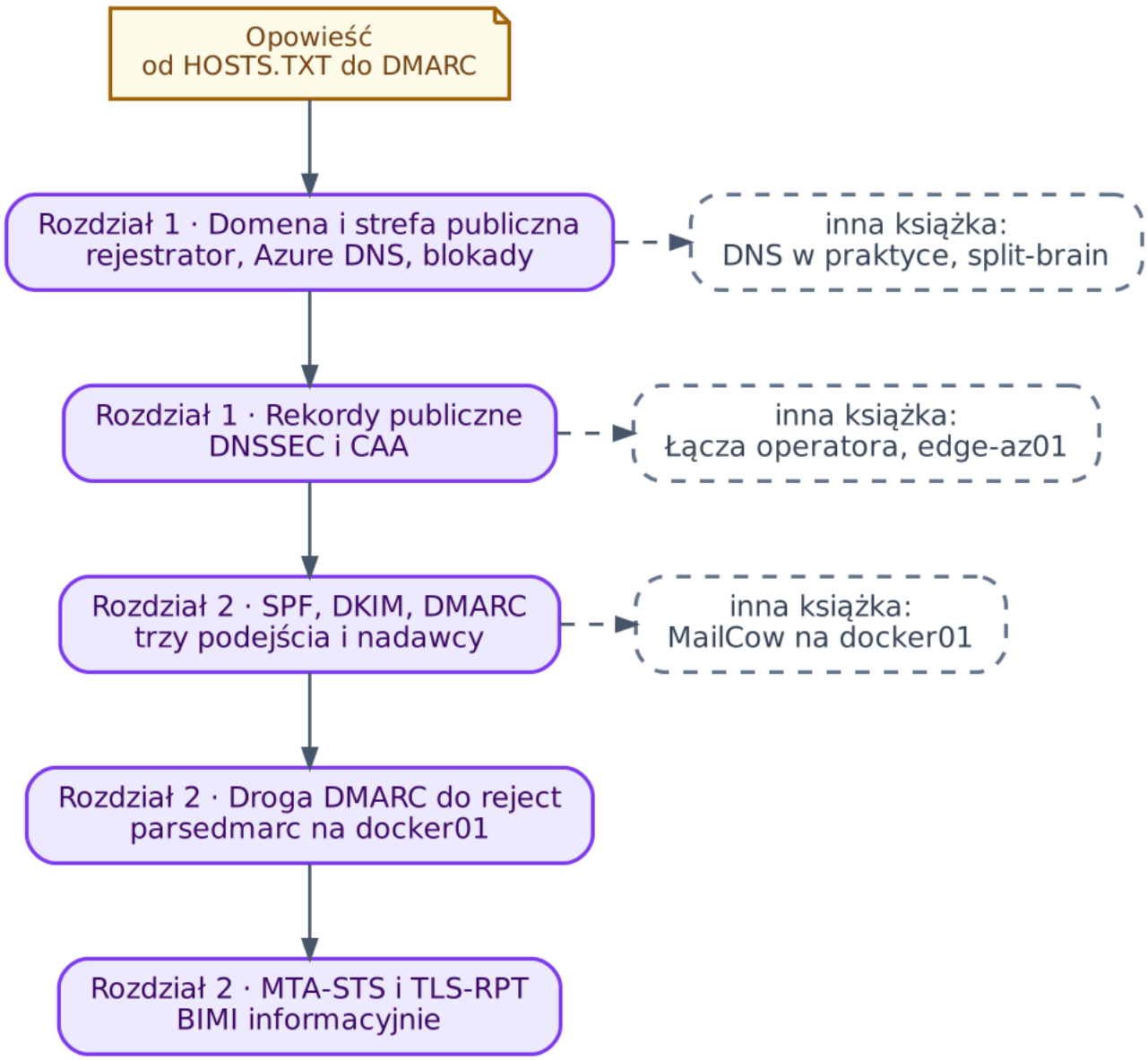
> **Z ŻYCIA WZIĘTE**
>
> Poniedziałek, 8:05. Biuro rachunkowe dzwoni do pani Haliny, że faktury z Zielonej od tygodnia lądują w spamie, a jedna wróciła z błędem `550 5.7.515` z Outlooka. W tym samym czasie pan Zbigniew przekazuje Tomkowi wiadomość od rejestratora, przysłaną na prywatny adres byłego informatyka: domena wygasa za dziewięć dni. Pan Wojtek, który akurat robi audyt, zadaje pytanie, na które nikt nie umie odpowiedzieć od razu: kto jest właścicielem domeny i gdzie jest hasło do konta u rejestratora?

Domena `zielona.example` jest fikcyjna: końcówkę `.example` zarezerwowało RFC 2606 do przykładów, więc żadne polecenie z tej książki nie zadziała na nią w prawdziwym internecie. W poleceniach do skopiowania piszemy `NazwaDomeny`, a w wynikach i tabelach stoi świat Zielonej.

Problemy z tej scenki są organizacyjne: konto u rejestratora na prywatnym adresie, brak rejestru dat i DMARC ustawiony raz, bez czytania raportów. Książka idzie od domeny jako zasobu firmy, przez strefę i jej rekordy, do poczty w trzech równorzędnych podejściach: MailCow na `docker01`, Microsoft 365 z Exchange Online i Google Workspace z Gmailem.

Mapa tej książki

Książka ma sześć stron w trzech rozdziałach.



Rysunek 3. Mapa książki: Opowieść, rozdział o domenie i strefie publicznej oraz rozdział o uwierzytelnianiu poczty, z odsyłaczami do książek o poczcie, Active Directory i łączach (kliknięcie

otwiera pełny rozmiar)

Strona	Na jakie pytanie odpowiada
Domena i DNS publiczny: od HOSTS.TXT do DMARC	Skąd wzięły się domeny, rejestratorzy i uwierzytelnianie poczty
Domena i strefa publiczna: rejestrator, dostawca DNS, odnowienia i blokady	Czyja jest domena, gdzie trzymamy strefę `zielona.example` i jak jej nie zgubić
Rekordy publiczne Zielonej, DNSSEC i CAA	Jakie rekordy ma strefa publiczna, jak ją podpisać i kto może wystawić certyfikat
SPF, DKIM i DMARC: trzy podejścia do poczty i systemy wysyłające w imieniu domeny	Jakie rekordy ustawić dla MailCow, Microsoft 365 i Google Workspace, co z Optimą, skanerami i sklepem i czego wymagają Gmail, Yahoo i Outlook
Droga DMARC od p=none do p=reject z raportami parsedmarc na docker01	Jak przejść do odrzucania podszytej poczty bez gubienia własnej
MTA-STS i TLS-RPT: szyfrowanie poczty między serwerami, a BIMI informacyjnie	Jak wymusić szyfrowanie poczty przychodzącej i czy warto mieć logo w skrzynce odbiorcy

Strefę wewnętrzną i split-brain opisuje DNS w praktyce: strefy w AD, przekazywanie warunkowe, scavenging i split-brain, przełączanie rekordów przy awarii łącza Łącza operatora: światłowód, radiolinia, LTE i 5G oraz przełączanie na FortiGate, a pocztę na `docker01` MailCow: serwer pocztowy w kontenerach, który Zielona wybrała zamiast Zimbry.

Źródła (odczyt 26 października 2026): dns.pl, historia rejestru i „30 lat domeny .pl” (1990, NASK od grudnia 1993, program partnerski 2002, DNSSEC 2011, Registry Lock 2019, model z rejestratorami od 2017) · betanews.com, 15 marca 2025 (40 lat `symbolics.com`) · en.wikipedia.org, Sender Policy Framework (2000, 2003, RFC 4408, RFC 7208) · dmarc.org, historia DMARC (30 stycznia 2012) · rfc-editor.org: RFC 6376, 7489, 8460, 8461, 8659, 9989 (maj 2026, zastępuje RFC 7489 i 9091) · archive.cabforum.org, Ballot 187 (CAA od 8 września 2017) · support.google.com, Email sender guidelines (1 lutego 2024) · senders.yahooinc.com, best practices · mailgun.com i uriports.com o wymaganiach Outlooka (5 maja 2025, `550 5.7.515`). Ilustracje własne.