DNSSEC

Polityka i Zasady Postępowania

1. Wprowadzenie

Niniejszy dokument DNSSEC Polityka i Zasady Postępowania (dalej: „**DPS**", z ang. *DNSSEC Policy & Practice Statement*) określa politykę bezpieczeństwa i zasady postępowania Naukowej i Akademickiej Sieci Komputerowej Państwowego - Instytutu Badawczego (dalej: „**NASK**" lub „**Rejestr**") względem strefy domeny krajowej .pl zabezpieczonej DNSSEC.

Niniejszy dokument został opracowany w oparciu o zalecenia określone w opublikowanym przez Internet Engineering Task Force IETF dokumencie: RFC-6841 A Framework for DNSSEC Policies and DNSSEC Practice Statements.

1.1. Wstęp

DNSSEC (Domain Name System Security Extensions) stanowi rozwiązanie zwiększające bezpieczeństwo DNS (Domain Name System). DNSSEC wprowadza do DNS elementy kryptografii (mechanizm kluczy asymetrycznych), która daje możliwość uwierzytelnienia danych otrzymanych w procesie rozwiązywania nazw domen internetowych na adresy IP (Internet Protocol). Proces uwierzytelniania opiera się o tzw. „łańcuch zaufania", co wymaga poprawnego podpisania poszczególnych poziomów stref domen zgodnie z hierarchiczną strukturą DNS. Oznacza to, że aby zabezpieczyć nazwę domeny należy podpisać strefę tej domeny i opublikować rekord DS (jest to kryptograficzny skrót z części publicznej klucza podpisującego strefę) w strefie domeny nadrzędnej. Następnie Rekord DS w strefie domeny nadrzędnej jest podpisywany kluczem prywatnym, a skrót części publicznej klucza podpisującego zostaje przekazany w analogiczny sposób do kolejnej strefy nadrzędnej. W ten sposób łańcuch budowany jest do strefy Root (najwyższy poziom w hierarchii DNS), gdzie znajduje się klucz określany jako „Trust Anchor", który powszechnie przyjmuje się, że jest zaufany.

DPS jest opisem polityki i zasad stosowanych przez rejestr strefy domeny .pl oraz stref drugiego poziomu, dla których NASK jest rejestrem, np.: .gov.pl, .com.pl, .org.pl, .net.pl, .waw.pl (dalej łącznie „**strefy NASK**"). Pełna lista stref NASK dostępna jest na stronie internetowej www.dns.pl.

DPS ma zastosowanie wyłącznie do stref NASK. Każda strefa leżąca poniżej stref NASK w łańcuchu zaufania tworzonym przez DNSSEC może mieć inne wymogi względem bezpieczeństwa i dopuszczać inny poziom akceptacji ryzyka. Abonent nazwy domeny powinien w ramach dostępnych środków zapewnić odpowiedni poziom bezpieczeństwa zarządzanej przez siebie strefie.

1.2. Nazwa i oznaczenie dokumentu

Tytuł dokumentu: DNSSEC Polityka i Zasady Postępowania

Wersja: 2.0

Data publikacji: 12-03-2020

Data ostatniej modyfikacji: 12-03-2020

1.3. Strony i środowisko działania

1.3.1. Rejestr

NASK prowadzi rejestr nazw domeny krajowej najwyższego poziomu .pl oraz rejestr nazw domeny .gov.pl przeznaczonej dla instytucji państwowych.

Po stronie Rejestru leży odpowiedzialność za podpisywanie stref NASK oraz przekazywanie rekordu DS ze strefy .pl do strefy Root. Rekordy DS ze stref drugiego poziomu przekazywane są do strefy .pl.

1.3.2. Partner

Partner (rejestrator), podmiot związany z NASK *Porozumieniem w sprawie współpracy dotyczącej nazw domen internetowych* (dalej Porozumienie). Na stronie www.dns.pl, NASK publikuje aktualną listę rejestratorów wraz ze świadczonymi przez nich usługami DNS, w tym usługą DNSSEC.

Partner, w imieniu Abonenta, za pomocą protokołu EPP, dokonuje w rejestrze domeny .pl rejestracji oraz obsługi nazw w strefach NASK, w tym wprowadzenia lub usunięcia rekordu DS.

1.3.3. Abonent

Abonent jest to podmiot, który w oparciu o *Regulamin nazw domeny .pl* lub *Regulamin nazw w domenie .gov.pl*, zawarł z NASK umowę o utrzymywanie nazwy domeny należącej do stref NASK.

Abonent za pośrednictwem Partnera przekazuje do NASK zmiany wpisów dotyczących rekordów DS.

W przypadku strefy .gov.pl Abonent przekazuje w/w zmiany bezpośrednio do NASK.

1.3.4. Użytkownik DNSSEC

Użytkownik DNSSEC jest to podmiot wykorzystujący odpowiedzi DNS zabezpieczone DNSSEC, który odpowiada samodzielnie za należytą konfigurację własnych urządzeń i dokonywanie aktualizacji związanych z prawidłowym walidowaniem łańcucha zaufania aż do „Trust Anchor".

1.4. Zasady administrowania dokumentem

W przypadku zaistnienia zmian związanych z obsługą DNSSEC w strefach NASK, DPS podlega aktualizacji w zakresie tych zmian.

1.4.1. Organizacja zarządzająca dokumentem

Naukowa i Akademicka Sieć Komputerowa - Państwowy Instytut Badawczy

1.4.2. Dane kontaktowe

NASK - Państwowy Instytut Badawczy

Dział Domen
ul. Kolska 12
01-045 Warszawa
Telefon: +48 22 380 82 00
Faks: +48 22 380 83 01
Email: info@dns.pl

1.4.3. Procedury wprowadzania zmian

Zmiany w DPS wprowadzane są w formie poprawek i publikowane jako nowa wersja dokumentu. Nowa wersja DPS uchyla wcześniejsze wersje DPS.

2. Publikacja i repozytoria

2.1. Miejsce publikacji DPS

Obowiązująca wersja DPS publikowana jest w witrynie NASK www.dns.pl.

2.2. Publikacja kluczy publicznych

NASK publikuje w postaci rekordu DS skrót z klucza KSK:

- dla strefy .pl w strefie Root,

- dla stref drugiego poziomu zarządzanych przez NASK, w tym strefy .gov.pl, w strefie .pl.

3. Wymagania operacyjne

3.1. Znaczenie nazwy domeny

System rozwiązywania nazw domen internetowych na numery IP komputerów (DNS) pozwala w zrozumiały i łatwy sposób połączyć się użytkownikowi z wybranymi usługami typu: www, poczta elektroniczna, telefonia IP. Nazwa domeny to unikalny wpis w rejestrze tej domeny (strefie wyższego poziomu). Rejestr nazw domeny .pl przyjmuje wpisy dotyczące nazw pierwszego poziomu w stosunku do domeny .pl np. dns.pl i drugiego poziomu np. nask.com.pl, nask.waw.pl. Warunki dotyczące rejestracji nazw w strefach NASK określone zostały w witrynie internetowej NASK. NASK dokonuje rejestracji na zasadzie „first come, first served".

DNSSEC zapewnia mechanizmy gwarantujące, że pochodzenie danych uzyskanych za pomocą protokołu DNS jest zgodne z informacjami zawartymi w rejestrze. Nie potwierdza natomiast informacji o Abonencie ani o prawach do wykorzystywania nazwy domeny.

3.2. Aktywacja DNSSEC dla strefy podrzędnej względem strefy NASK

Aktywacja DNSSEC dla strefy podrzędnej odbywa się poprzez wprowadzenie przez Partnera lub NASK do strefy NASK za pomocą protokołu EPP rekordu DS i opublikowanie go w podpisanej strefie nadrzędnej. NASK zakłada, że otrzymany rekord jest poprawny i nie wykonuje jego weryfikacji.

Wyjątek stanowi strefa .gov.pl. Dla domen z tej strefy NASK sprawdza poprawność konfiguracji na autorytatywnym serwerze DNS.

3.3. Identyfikacja i uwierzytelnienie zarządzającego strefą podrzędną

Zarządzającym strefą podrzędną względem stref NASK jest Abonent nazwy domeny należącej do jednej ze stref NASK.

Zgodnie z Porozumieniem, NASK przyjmuje, że Partner posiada zgodę Abonenta na obsługę nazwy domeny .pl, w tym wprowadzanie, modyfikowanie i usuwanie rekordów DS związanych ze strefą danej domeny, a tym samym identyfikuje Abonenta.

W przypadku nazw w strefach NASK obsługiwanych bezpośrednio przez NASK identyfikacji Abonenta dokonuje NASK.

3.4. Rejestracja rekordów DS

Rekordy DS wprowadzane są do strefy nadrzędnej przez system teleinformatyczny Registry (dalej: Registry), w którym są przechowywane informacje dotyczące nazw domeny .pl utrzymywanych przez NASK. Registry przyjmuje od Partnerów i NASK za pomocą protokołu EPP rekordy DS zgodne ze standardem opisanym w dokumencie RFC 5910. Jednej nazwie domeny można przypisać maksymalnie 6 rekordów DS.

3.5. Metody potwierdzania posiadania klucza prywatnego

Rejestr nie prowadzi kontroli poprawności podpisania strefy podrzędnej, dlatego też nie wymaga od Abonenta strefy podrzędnej potwierdzania, że jest w posiadaniu klucza prywatnego podpisującego strefę. Zapewnienie odpowiedniego poziomu bezpieczeństwa leży po stronie Abonenta.

3.6. Usuwanie rekordów DS

3.6.1. Uprawniony do usunięcia rekordów DS

Rekord DS nazwy domeny może zostać usunięty ze strefy NASK przez uprawnionego Partnera lub NASK.

3.6.2. Procedura usuwania rekordów DS

Po usunięciu rekordów DS z Registry w strefie NASK nastąpią zmiany najpóźniej z kolejnym poprawnym pełnym przeładowaniem strefy. Aktualna informacja o godzinach przeładowania stref publikowana jest w witrynie NASK www.dns.pl.

3.6.3. Sytuacja nadzwyczajna

W sytuacji braku kontaktu z Partnerem Abonent może samodzielnie wnioskować o usunięcie rekordu DS. NASK wykona takie usunięcie, o ile w sposób niebudzący wątpliwości wnioskujący potwierdzi na piśmie, iż jest Abonentem nazwy domeny .pl.

4. Funkcje zarządcze i kontrolne

4.1. Zabezpieczenia fizyczne

NASK zapewnia odpowiedni poziom bezpieczeństwa fizycznego zgodnego z wymogami DPS.

4.1.1. Lokalizacja

Rejestr domeny .pl wykorzystuje dla potrzeb DNSSEC dwie lokalizacje: główną oraz centrum zapasowe. Obiekty wykorzystywane dla potrzeb DNSSEC posiadają wielostopniowy system ochrony fizycznej i kontroli dostępu.

4.1.2. Dostęp fizyczny

Wejścia do obiektów oraz teren wokół monitorowane są przez 24 godziny na dobę. Teren obiektów chroniony jest przez system telewizji przemysłowej oraz inne rozwiązania technologiczne

zapewniające brak dostępu osobom nieupoważnionym. Dostęp do urządzeń biorących udział w procedurach DNSSEC jest ograniczony do osób upoważnionych.

4.1.3. Zasilanie i klimatyzacja

Na zasilanie składają się: dwie niezależne linie zasilające z dwóch niezależnych podstacji transformatorowych, dwa zasilacze bezprzerwowe (UPS), agregat prądotwórczy uruchamiany automatycznie oraz zdalny monitoring zasilania energetycznego.

W pomieszczeniach zapewnione są stabilne warunki środowiskowe umożliwiające nieprzerwaną pracę urządzeń. Pomieszczenia wyposażone są w redundantny system klimatyzacji.

4.1.4. Zagrożenie zalaniem i powodzią

Obiekty z urządzeniami wykorzystywanymi do DNSSEC znajdują się na terenach niezagrożonych powodzią. Obiekty utrzymywane są w należytym stanie technicznym i urządzeniom nie grozi zalanie.

4.1.5. Ochrona przeciwpożarowa

Bezpieczeństwo przeciwpożarowe zapewnia system detekcji i sygnalizacji pożaru oraz automatyczny system gaśniczy.

4.1.6. Przechowywanie danych i postępowanie z nośnikami

Dane są klasyfikowane, oznaczane i przechowywane zgodnie z regulacjami wewnętrznymi obowiązującymi w NASK określającymi właściwy poziom bezpieczeństwa przetwarzania tych danych.

4.1.7. Postępowanie ze zbędnymi danymi

Zbędne nośniki, dokumenty i materiały zawierające dane chronione przez NASK są usuwane bądź niszczone w sposób uniemożliwiający ich odtworzenie lub ponowne użycie.

4.1.8. Kopia zapasowa

Kopia zapasowa systemu i danych przechowywana jest w bezpiecznym miejscu poza główną lokalizacją NASK. Dostęp do kopii ograniczony jest do osób upoważnionych.

4.2. Zabezpieczenia proceduralne

4.2.1. Role

Aby zapewnić prawidłową kompartmentalizację uprawnień oraz odpowiedzialności, użytkownikom systemu DNSSEC zostają przydzielone odpowiednie role. Role – to grupy osób z odpowiednim zestawem uprawnień. Zestaw przydzielonych uprawnień pozwala przypisać danej osobie konkretną rolę w procedurach DNSSEC. Szczegółowy zakres obowiązków poszczególnych ról opisują wewnętrzne procedury NASK.

4.2.2. Liczba osób i ról wymaganych do realizacji poszczególnych zadań

Przyjęto zasadę, że do każdej roli przypisana jest ilość osób zapewniająca wysoki poziom redundancji uprawnień.

Do każdej z wykonywanych czynności operacyjnych lub administracyjnych, niezbędne są osoby autoryzujące dostęp oraz osoby uczestniczące w wykonywaniu procedur DNSSEC.

4.2.3. Identyfikacja i uwierzytelnianie osób do pełnienia poszczególnych ról

Role w procedurach DNSSEC mogą pełnić wyłącznie osoby, które zostały wyznaczone przez NASK oraz spełniają kryteria opisane w pkt. **Błąd! Nie można odnaleźć źródła odwołania.**.

4.2.4. Zasada rozdzielenia obowiązków

W procedurach DNSSEC stosowana jest separacja obowiązków. Ograniczenia wprowadzono w odniesieniu do możliwości łączenia ról. Ponadto wybrane role mogą być przypisywane do osób należących do określonych komórek organizacyjnych NASK.

4.3. Bezpieczeństwo osobowe

4.3.1. Wymagania odnośnie kwalifikacji, doświadczenia i posiadanych pozwoleń

Każda osoba, która pełni rolę w procedurach DNSSEC powinna spełniać następujące warunki:

- być zatrudniona w NASK co najmniej rok,
- być zatrudniona na umowę o pracę na czas nieoznaczony lub umowę o pracę na czas oznaczony, który upływa nie wcześniej niż 12 miesięcy od dnia kwalifikacji do pełnienia danej roli,
- nie być w okresie wypowiedzenia,
- posiadać zgodę swojego bezpośredniego przełożonego na wykonywanie obowiązków wynikających z procedur DNSSEC,
- zostać przeszkolona w zakresie stosowania procedur DNSSEC (patrz pkt. 4.3.3).

4.3.2. Postępowanie sprawdzające

NASK w procedurze rekrutacji nie prowadzi dodatkowych sprawdzeń pod kątem pełnienia roli w operacjach DNSSEC. Nowo zatrudniane osoby zgodnie z pkt 4.3.1 nie mogą pełnić ról procedurach DNSSEC.

4.3.3. Wymagania dotyczące szkoleń

Każda osoba pełniąca rolę w procedurach DNSSEC musi przejść szkolenie obejmujące:

- obsługę urządzeń, z których będzie korzystała,
- zakres zadań i odpowiedzialności związanej z pełnioną rolą,
- postępowanie w przypadku wykrycia incydentów naruszenia bezpieczeństwa, kompromitacji kluczy i disaster recovery.

4.3.4. Częstotliwość szkoleń

Przed dopuszczeniem do realizacji procedur DNSSEC, każda osoba, która pełni jedną z ról , o których mowa w pkt. 4.2.1 musi przejść szkolenie określone w pkt. 4.3.3 . Ponowne szkolenie muszą odbyć wszystkie osoby po każdorazowej zmianie procedur DNSSEC oraz te osoby, które nie wykonywały procedur DNSSEC przez okres dłuższy niż 18 miesięcy.

4.3.5. Sankcje w wyniku nieuprawnionego działania

Sankcje wobec osób pełniących role określone w pkt. 4.2.1, które dokonały nieuprawnionego działania, wynikają ze stosunku pracy pomiędzy NASK a tymi osobami.

4.3.6. Wymagania wobec osób niezatrudnionych (wykonawców, zleceniobiorców)

Osoby nie związane z NASK umową o pracę nie mogą być nominowane do ról DNSESC.

W sytuacjach awaryjnych, w przypadku konieczności konsultacji z osobami trzecimi (dostawca urządzeń lub oprogramowania obsługujących DNSSEC), osoby pełniące role DNSSEC mają obowiązek zapewnić poufność danych oraz zadbać o respektowanie niniejszych zasad przez osoby trzecie.

4.3.7. Udostępnienie dokumentacji personelowi

Osoby pełniące poszczególne role mają zapewniony dostęp do procedur wewnętrznych dotyczących wszystkich operacji realizowanych przez te role.

4.4. Procedury rejestrowania zdarzeń

4.4.1. Rodzaje rejestrowanych zdarzeń

Wszystkie operacje wykonywane przy użyciu urządzeń biorących udział w podpisywaniu stref NASK są rejestrowane.

4.4.2. Częstotliwość kontroli zebranych informacji

Administratorzy Rejestru monitorują rejestrowane operacje oraz zdarzenia i co najmniej raz w tygodniu dokonują ich kontroli. W przypadku wykrycia anomalii Administratorzy reagują bez zbędnej zwłoki.

4.4.3. Czas przechowywania logów

Rejestry zebranych operacji i zdarzeń są archiwizowane i przechowywane przez co najmniej 6 miesięcy.

4.4.4. Ochrona logów

Dostęp do rejestrów operacji i zdarzeń jest ograniczony do osób uprawnionych. Rejestry zdarzeń są przechowywane na dwóch niezależnych urządzeniach.

4.4.5. Informowanie użytkowników o rejestrowaniu zdarzeń

Osoby pełniące określone role w systemie DNSSEC w trakcie szkolenia są informowane o rejestrowaniu działań opisanych w pkt. 4.4.1.

4.4.6. Ocena podatności

Wszystkie zapisy niestandardowych operacji i zdarzeń są poddawane analizie na wypadek wykrycia potencjalnej próby złamania zabezpieczeń.

4.5. Kompromitacja kluczy prywatnych i disaster recovery

4.5.1. Obsługa incydentów

Obsługą incydentów zagrożenia bezpieczeństwa związanych z systemem DNSSEC zajmuje się wyznaczony zespół w strukturze organizacyjnej NASK. W zależności od rodzaju incydentu (utrata bądź uszkodzenie danych, kompromitacja kluczy prywatnych, kompromitacja serwera, na którym podpisywane są strefy NASK), podejmowane są odpowiednie działania opisane w procedurach wewnętrznych NASK.

Decyzję o wykonaniu konkretnego działania podejmuje kierownik wyznaczonego zespołu w strukturze organizacyjnej NASK informując o podjętych działaniach swojego zwierzchnika.

4.5.2. Procedury na wypadek uszkodzenia danych, oprogramowania lub sprzętu

Materiał kryptograficzny w postaci kluczy prywatnych przechowywany jest na więcej niż jednym urządzeniu.

W sytuacji awarii wszystkich urządzeń DNSSEC w lokalizacji podstawowej istnieje możliwość przekierowania ruchu i korzystania z urządzeń znajdujących się w lokalizacji zapasowej.

W sytuacji awarii urządzeń DNSSEC powodującej:

- brak możliwości podpisywania nowych rekordów umieszczanych w strefie NASK,

- oraz brak możliwości ponownego podpisywania rekordów z upływającym czasem ważności,

rekord DS zostanie niezwłocznie usunięty ze strefy nadrzędnej a strefa NASK zostanie opublikowana w postaci niepodpisanej.

NASK posiada procedurę wewnętrzną opisującą usunięcie rekordu DS ze strefy nadrzędnej.

4.5.3. Procedury na wypadek kompromitacji klucza prywatnego

Informacje wskazujące na skompromitowanie kluczy DNSSEC stref NASK skutkuje uruchomieniem procedury awaryjnej.
Każde podejrzenie kompromitacji urządzeń wykorzystywanych do podpisywania stref NASK skutkuje m.in. utworzeniem kopii aktualnego stanu systemów na potrzeby analizy zagrożenia, nową instalacją systemów i wymianą awaryjną kluczy. NASK posiada procedury wewnętrzne opisujące szczegółowo sposób postępowania na wypadek podejrzenia kompromitacji klucza prywatnego.

4.5.4. Plan zachowania ciągłości

W celu zapewnienia ciągłości działania usługi DNSSEC, NASK utrzymuje centrum zapasowe dla infrastruktury systemu DNSSEC oraz posiada wdrożone plany awaryjne pozwalające na przywrócenie działania usługi w zaplanowanym czasie. Wszelkie instrukcje, materiał kryptograficzny oraz inne niezbędne informacje posiadają kopie bezpieczeństwa i przechowywane są w sposób minimalizujący ryzyko ich utraty i kompromitacji.

5. Kontrola bezpieczeństwa technicznego

5.1. Generowanie i instalowanie pary kluczy

5.1.1. Generowanie pary kluczy

Klucze generowane są w module bezpieczeństwa zarządzanym przez role określone w procedurach wewnętrznych NASK. Wszystkie czynności realizowane są w obecności określonej liczby uprawnionych osób, tak aby zminimalizować ryzyko błędów ludzkich i nadużyć.
Procedura generowania kluczy opisana jest w dokumentacji wewnętrznej NASK.

5.1.2. Publikacja części publicznej klucza KSK

Część publiczna klucza KSK jest publikowana w sposób bezpieczny zgodnie informacją w punkcie 2.2.

5.1.3. Parametry klucza publicznego i kontrola jakości

Parametry klucza publicznego oraz zasady i sposoby ich kontroli zostały określone w dokumencie wewnętrznym NASK.

5.1.4. Wykorzystanie kluczy

Klucze generowane w procedurach DNSSEC mogą być wykorzystane tylko podczas cyklu ich ważności i nie mogą być użyte do innych celów niż podpisanie stref NASK.

5.2. Ochrona klucza prywatnego i inżynieria modułu kryptograficznego

Wszystkie operacje kryptograficzne dotyczące kluczy prywatnych wykonywane są przez urządzenia DNSSEC, a klucze prywatne nie mogą znaleźć się w formie niezabezpieczonej poza tymi urządzeniami.

5.2.1. Wieloosobowa kontrola klucza prywatnego

Wieloosobowy dostęp do kluczy opisany został w punkcie 4.2.

5.2.2. Depozyt kluczy prywatnych

NASK nie przekazuje kluczy prywatnych do depozytu.

5.2.3. Kopia bezpieczeństwa

Klucze są archiwizowane w zaszyfrowanej postaci i przechowywane w bezpiecznym miejscu. Do odtworzenia kopii w sytuacji uszkodzenia danych stosuje się identyczne procedury bezpieczeństwa jak w procedurze generowania kluczy DNSSEC.

5.2.4. Przechowywanie klucza prywatnego przez moduł kryptograficzny

Klucze prywatne przechowywane są w urządzeniu DNSSEC w postaci zaszyfrowanej specjalnym kluczem.

5.2.5. Archiwizacja klucza prywatnego

Klucz prywatny, który nie jest używany archiwizowany jest wyłącznie w formie kopii zapasowej.

5.2.6. Transfer klucza prywatnego z i do modułu kryptograficznego.

Transfer klucza prywatnego z i do urządzenia DNSSEC odbywa się tylko w postaci kopii zapasowej. Instrukcja tworzenia i przywracania kopii zapasowej jest opisana w procedurach wewnętrznych NASK.

5.2.7. Metoda aktywacji klucza prywatnego

Klucze prywatne są aktywowane automatycznie za pomocą oprogramowania podpisującego.

5.2.8. Metoda dezaktywacji klucza prywatnego

Klucze prywatne są dezaktywowane automatycznie po wygaśnięciu.

5.2.9. Metoda niszczenia klucza prywatnego

Nieużywane klucze prywatne są usuwane z urządzeń DNSSEC manualnie zgodnie z wewnętrznymi procedurami NASK.

5.3. Aktywacja danych autoryzacyjnych

Każda z ról biorących udział w procedurach DNSSEC posiada klucz dostępu.

5.3.1. Aktywacja danych

Każdej roli w DNSSEC zostaje wygenerowany i przypisany klucz dostępu.

5.3.2. Ochrona danych autoryzacyjnych

Każda osoba pełniąca rolę w procedurach DNSSEC zobowiązana jest do ochrony danych autoryzacyjnych. W sytuacji utraty klucza dostępu jego użytkownik zobowiązany jest do natychmiastowego zgłoszenia tego zgodnie z wewnętrznymi procedurami NASK.

5.3.3. Inne aspekty danych autoryzacyjnych

Rejestr nie będzie przechowywał kopii danych autoryzacyjnych.

Przypisywane klucze dostępu nie maja terminu dezaktywacji. Wymiana kluczy dostępu powinna mieć miejsce nie rzadziej niż raz na 2 lata.

W przypadku utraty klucza dostępu lub zmiany składu osobowego w danej roli, następuje niezwłoczne unieważnienie klucza, a następnie wygenerowanie nowego klucza dostępowego i przypisanie go do danej roli.

5.4. Zabezpieczenie urządzeń

Krytyczne elementy systemu DNSSEC zostały odseparowane i znajdują się w odpowiednio zabezpieczonej lokalizacji (punkt **Błąd! Nie można odnaleźć źródła odwołania.**). Dostęp do urządzeń jest ograniczony, a wszystkie operacje przeprowadzane na nich są rejestrowane i poddawane kontroli (punkt 4.4).

5.5. Zabezpieczenie sieci

Sieć NASK zbudowana jest w sposób zapewniający odpowiedni poziom bezpieczeństwa w poszczególnych jej segmentach. Wszystkie chronione informacje są szyfrowane.

5.6. Rejestracja znaczników czasu

System DNSSEC jest zsynchronizowany z serwerem czasu.

5.7. Bezpieczeństwo w procesach utrzymania i rozwoju oprogramowania

5.7.1. Kontrola rozwoju systemu

Do zarządzania rozwojem oprogramowania Rejestr korzysta z systemu wersjonowania kodu. Repozytoria znajdują się na wydzielonym serwerze zarządzanym przez zespół wyznaczony w strukturze organizacyjnej NASK.

5.7.2. Kontrola zarządzania bezpieczeństwem

Rejestr regularnie przeprowadza kontrole bezpieczeństwa, szacuje ryzyko oraz zleca audyty bezpieczeństwa systemu DNSSEC.

6. Podpisywanie strefy

6.1. Długość i algorytm klucza

W przypadku kluczy KSK stosowany jest algorytm RSA o długości klucza 4096 bitów, zaś w przypadku kluczy ZSK o długości 2048 bitów.

6.2. Poświadczanie statusu NXDOMAIN

Rejestr korzysta ze standardu NSEC3 określonego przez RFC 5155. Wszystkie strefy NASK są podpisane w trybie OPT-OUT.

6.3. Format podpisów

Podpisy generowane są za pomocą operacji kryptograficznych RSA przy użyciu SHA256 (RSA/SHA256, RFC 5702).

6.4. Wymiana kluczy ZSK

Wymiana kluczy ZSK przeprowadzona jest co 6 miesiące.

6.5. Wymiana kluczy KSK

Wymiana kluczy KSK przeprowadzona jest co 12 miesięcy.

6.6. Czas życia i częstotliwość wymiany podpisów

Zestawy rekordów podpisane są kluczem ZSK na okres 30 dni (+/- 1 dzień). Nowe rekordy podpisywane są na bieżąco mechanizmem dynamicznych aktualizacji. Całościowy eksport strefy NASK i wygenerowanie podpisów odbywa się co najmniej raz na 7 dni.

6.7. Weryfikacja kluczy podpisujących strefę

Weryfikacja kluczy podpisujących strefę odbywa się poprzez sprawdzenie łańcucha zaufania dla rekordu SOA dla każdej strefy.

6.8. Weryfikacja zestawów rekordów

Rejestr weryfikuje poprawność podpisanych rekordów w sposób automatyczny przy pomocy dostępnych narzędzi i własnych skryptów zgodnie z istniejącymi standardami.

6.9. Parametr TTL dla zestawów rekordów

TTL globalny dla stref = 86400 sekund.
TTL dla DNSKEY = 3600 sekund.
TTL rekordu RRSIG określa TTL rekordu, którego ten podpis dotyczy.

7. Audyt

W celu zapewnienia odpowiedniego poziomu bezpieczeństwa systemu DNSSEC wymagane jest przeprowadzanie audytów bezpieczeństwa.

Audyt ma na celu sprawdzenie zgodności działania Rejestru z wymogami opisanymi w DPS.

7.1. Częstotliwość audytu

Audyt jest przeprowadzany zgodnie z planami audytu NASK, lecz nie rzadziej niż raz na 3 lata. Audyt częściowy poza planem audytu przeprowadzany powinien być w przypadku:

- znaczących zmian w procesach, infrastrukturze lub organizacji związanych z DNSSEC,
- wykrycia istotnych nieprawidłowości w działaniu systemu i procedur związanych z zabezpieczonymi DNSSEC strefami NASK.

7.2. Kwalifikacje audytora

Audytor powinien mieć co najmniej dwuletnie doświadczenie w przeprowadzaniu wewnętrznych audytów bezpieczeństwa informacji, posiadać znajomość standardów i norm bezpieczeństwa IT, języków skryptowych oraz wiedzę z dziedziny bezpieczeństwa protokołu DNS i wykorzystania w nim algorytmów szyfrujących.

7.3. Związek audytora z badanym obszarem

Audytor nie może pełnić żadnej z ról określonych w punkcie 4.2.1. Audytor może być ekspertem zatrudnionym przez NASK do wykonania tego zadania.

7.4. Zakres audytu

Audyt obejmuje zgodność działań systemu DNSSEC z procedurami i wymogami opisanymi w DPS jak i z procedurami wewnętrznymi, których ze względów bezpieczeństwa nie można ujawnić w tym dokumencie.
W przypadku, gdy decyzja o audycie wynika z wprowadzenia zmian w procesach, infrastrukturze lub organizacji lub z wykrycia istotnych nieprawidłowości w działaniu Rejestru i procedur związanych z zabezpieczonymi DNSSEC strefami NASK, audyt może dotyczyć tylko tych zagadnień lub obszarów

DPS, w których wprowadzono zmiany lub wystąpiły nieprawidłowości. Taki audyt jest nazywany audytem częściowym.

7.5. Eliminowanie niezgodności

W przypadku wykrycia niezgodności w działaniu systemu DNSSEC, w wyniku przeprowadzonego audytu, informacje o nich przekazywane są do kierownictwa Rejestru. Kierownictwo Rejestru podejmuje decyzję o dalszym postępowaniu z wykrytą niezgodnością. Działania te są dokumentowane.

7.6. Informowanie o wynikach

Audytor jest zobowiązany do przekazania wyników audytu w formie pisemnej w terminie uzgodnionym z kierownictwem Rejestru.

8. Kwestie prawne

8.1. Ochrona danych osobowych

Dane osobowe przechowywane, przetwarzane i udostępniane są zgodnie z polskim prawem, a w szczególności z Ustawą o ochronie danych osobowych.

8.2. Odpowiedzialność i umowy o zachowaniu poufności

Odpowiedzialność Partnerów i zobowiązanie do zachowania poufności względem NASK jak i NASK względem Partnerów określone są w *Porozumieniu w sprawie współpracy dotyczącej nazw domen internetowych*.
Odpowiedzialność NASK względem Abonentów i Abonentów względem NASK określa *Regulamin nazw domeny .pl* oraz *Regulamin nazw w domenie .gov.pl*.

8.3. Termin obowiązywania DPS

Niniejszy DPS obowiązuje do momentu zastąpienia go nową wersją wprowadzoną zgodnie z procedurą opisaną w pkt. 1.4 lub do odwołania przez Rejestr.

8.4. Obowiązujące prawo

W sprawach nieuregulowanych w DPS, *Porozumieniu w sprawie współpracy dotyczącej nazw domen internetowych, Regulaminie nazw domeny .pl i Regulaminie nazw w domenie .gov.pl* mają zastosowanie przepisy polskiego prawa.