# 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 instytutu badawczego (dalej: „NASK" lub „Rejestr") względem strefy domeny krajowej .pl zabezpieczonej DNSSEC.

Niniejszy dokument jest zgodny z wymogami określonymi w projekcie organizacji IETF: RFC-draft DNSSEC Policy & Practice Statement Framework.

## 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 wprowadzić specjalny kryptograficzny skrót z części publicznej klucza podpisującego strefę (rekord DS, delegation signer) do strefy domeny nadrzędnej w hierarchii DNS, w której nazwa domeny podlegająca zabezpieczeniu została zarejestrowana. Tu z kolei wspomniany skrót powinien zostać podpisany kluczem prywatnym, a jego skrót przekazany w analogiczny sposób do strefy nadrzędnej. Taki łańcuch budowany jest aż 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 zabezpieczonej DNSSEC oraz innych stref, 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 http://www.dns.pl.

## 1.2. Nazwa i oznaczenie dokumentu

Tytuł dokumentu: DNSSEC Polityka i Zasady Postępowania

Wersja: 1.3

Data publikacji: 13-12-2011

Data modyfikacji: 03-07-2018

## 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 podpisanie stref NASK oraz przekazanie 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), to przedsiębiorca, który zawarł z NASK *Porozumienie w sprawie współpracy dotyczącej nazw domen internetowych* („*Porozumienie*") i uzyskał zgodę Abonenta nazwy domeny .pl na reprezentowanie wobec NASK.

Partner, w imieniu Abonenta, za pomocą protokołu EPP, bezpośrednio w rejestrze domeny .pl, dokonuje rejestracji i obsługi nazw w strefach NASK w tym wprowadzenia lub usunięcia rekordu DS. Zasady dokonywania takich wpisów, obowiązki i prawa Partnera oraz jego odpowiedzialność reguluje *Porozumienie*.

*1.3.3. Abonent*

Abonent jest to podmiot albo jednostka organizacyjna nieposiadająca osobowości prawnej, który w oparciu o *Regulamin nazw domeny .pl* lub *Regulamin nazw w domenie .gov.pl* opublikowany na stronie internetowej http://www.dns.pl, zawarł z NASK umowę o utrzymywanie nazwy domeny należącej do strefy NASK. Jeżeli przedmiotem takiej umowy została objęta również obsługa administracyjna i techniczna w rozumieniu umowy, Abonent przekazuje bezpośrednio NASK zmiany wpisów dotyczących nazwy domeny, w tym rekordu DS.

W przypadku zawarcia umowy za pośrednictwem Partnera, wpisów dotyczących rekordu DS w strefach NASK dokonuje Partner.

*1.3.4. Użytkownik DNSSEC*

Użytkownik DNSSEC jest to podmiot albo jednostka organizacyjna nieposiadająca osobowości prawnej 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".

*1.3.5. Zastosowanie*

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 ryzyka. Abonent nazwy domeny powinien w ramach dostępnych środków zapewnić odpowiedni poziom bezpieczeństwa zarządzanej przez siebie strefie.

### 1.4. Zasady administrowania dokumentem

DPS powinien zostać zaktualizowany w przypadku zaistnienia zmian związanych z obsługą DNSSEC w strefach NASK mających bezpośrednie przełożenie na jego treść.

*1.4.1. Organizacja zarządzająca dokumentem*

Naukowa i Akademicka Sieć Komputerowa instytut badawczy

*1.4.2. Dane kontaktowe*

Naukowa i Akademicka Sieć Komputerowa 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

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

## 2.2. Publikacja KSK

NASK publikuje w postaci rekordu DS skrót z klucza KSK podpisującego:

- strefę .pl w strefie Root,

- strefy drugiego poziomu zarządzane przez NASK, w tym strefę .gov.pl, w strefie .pl.

## 2.3. Kontrola dostępu

DPS publikowany jest w witrynie NASK, w formie zabezpieczonej przed nieuprawnionym usunięciem i modyfikacją, poprzez protokół HTTPS.

# 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 wybraną usługą, 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 będzie wykonywał jego weryfikacji.

## 3.3. Identyfikacja i uwierzytelnienie zarządzającego strefą podrzędną

Zarządzającym strefą podrzędną względem strefy NASK jest Abonent nazwy domeny należącej do strefy NASK.

Zgodnie z Porozumieniem, NASK przyjmuje, że Partner posiada zgodę Abonenta na obsługę nazwy domeny .pl w tym wprowadzania, modyfikowania i usuwania rekordów DS związanych ze strefą danej nazwy domeny .pl, 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 Registry – system elektroniczny, w którym są przechowywane informacje na temat 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, czyli całościowym eksportem bazy danych Registry do postaci plików stref. Aktualna informacja o godzinach przeładowania stref publikowana jest w witrynie NASK https://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. Kontrola fizyczna

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 przypadku awarii jednej ze stacji następuje automatyczne przełączenie źródeł zasilania.

W pomieszczeniach zapewnione są stabilne warunki środowiskowe umożliwiające nieprzerwaną pracę urządzeń, zarówno serwerów, jak również urządzeń sieciowych. Pomieszczenia wyposażone są w redundantny system klimatyzacji precyzyjnej kontrolujący i utrzymujący stałą temperaturę i wilgotność powietrza.

### *4.1.4. Zagrożenie zalaniem i powodzią*

Obiekty utrzymywane są w należytym stanie technicznym i urządzeniom nie grozi zalanie. Pomieszczenia z urządzeniami wykorzystywanymi do DNSSEC znajdują się najniżej na pierwszym piętrze, dlatego nie są zagrożone powodzią.

### *4.1.5. Ochrona przeciwpożarowa*

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

### *4.1.6. Przechowywanie*

Poufne dane przechowywane są zgodnie z instrukcjami i zaleceniami wewnętrznymi obowiązującymi w NASK.

*4.1.7. Postępowanie z „odpadami"*

Dokumenty i materiały zawierające dane poufne są niszczone w sposób uniemożliwiający ich odtworzenie.

*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. Nadzór proceduralny

*4.2.1. Role*

Role – to grupy osób z odpowiednim zestawem uprawnień.
Zestaw przydzielonych uprawnień pozwala przypisać danej osobie konkretną rolę w procedurach administracyjnych DNSSEC.
NASK określił na potrzeby DNSSEC następujące role:

- *Administrator HSM*
- *Administrator klucza MBK*
- *Administrator z uprawnieniami do generowania kluczy*

*4.2.2. Liczba osób i ról wymaganych do realizacji poszczególnych zadań*

Każdą rolę pełni kilka osób. Przyjęto zasadę, że do każdej roli przypisana jest ilość osób zapewniająca wysoki poziom redundancji uprawnień.
Wymagane jest, aby do wykonania zadania w procedurach DNSSEC rola była reprezentowana zawsze przez tę samą liczbę osób, minimum 3 ($n \geq 3$).
Procedury wewnętrzne NASK określają szczegółowo wymaganą liczbę osób i ról w procedurach DNSSEC.

*4.2.3. Identyfikacja i uwierzytelnianie osób do pełnienia poszczególnych ról*

Pełnić określone role w procedurach DNSSEC mogą wyłącznie osoby, które zostały wyznaczone na piśmie przez NASK oraz spełniają kryteria opisane w pkt. 4.3.

*4.2.4. Zadania wymagające rozdzielenia obowiązków*

*Administratorzy HSM* jako użytkownicy o nieograniczonych uprawnieniach dostępowych nie powinni pełnić żadnej dodatkowej roli.

## 4.3. Nadzór nad personelem

*4.3.1. Wymogi względem personelu*

Każda osoba, która pełni jedną z ról wymienionych pkt. 4.2.1 powinna spełniać następujące wymogi:

- 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 po upływie 24 miesięcy od dnia kwalifikacji do pełnienia danej roli,
- posiadać zgodę swojego bezpośredniego przełożonego na wykonywanie obowiązków wynikających z procedur DNSSEC.

*4.3.2. Postępowanie sprawdzające*

Przełożony osoby ubiegającej się lub biorącej udział w procedurach DNSSEC potwierdza raz na dwa lata kierownikowi wyznaczonego zespołu w strukturze organizacyjnej NASK spełnienie przez tę osobę wymogów określonych w pkt. 4.3.1.

*4.3.3. Wymagania dotyczące szkoleń*

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

- obsługi urządzeń, z których będzie korzystała,
- zakresu zadań i odpowiedzialności związanej z pełnioną rolą,
- swojego udziału w procedurach stosowanych w przypadku wykrycia incydentów naruszenia bezpieczeństwa, kompromitacji kluczy i disaster recovery.

*4.3.4. Częstotliwość szkoleń*

Każda osoba, która pełni jedną z ról określonych w pkt. 4.2.1 musi przejść szkolenie określone w pkt. 4.3.3 w okresie do miesiąca od momentu uzyskania uprawnień. Ponadto osoby pełniące rolę *Administratorów HSM* oraz *Administratorów z uprawnieniami do generowania kluczy* powinny uczestniczyć w procedurze generowania kluczy określonej w pkt. 5.1 co najmniej raz na rok.

*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 personelu*

Nikt poza osobami pełniącymi role określone w pkt. 4.2.1 nie może mieć dostępu do systemu zarządzającego kluczami i nie może dokonywać w nim zmian. W wyjątkowej sytuacji osoba pełniąca daną rolę może wykonywać swoje czynności w konsultacji z dostawcą urządzeń lub oprogramowania, przy czym nie może dojść w takiej sytuacji do ujawnienia danych poufnych lub innego naruszenia bezpieczeństwa, a w tym do kompromitacji kluczy.

*4.3.7. Udostępnienie dokumentacji personelowi*

Osoby pełniące poszczególne role mają dostęp do procedur wewnętrznych dotyczących wymiany klucza, tworzenia i przywracania kopii zapasowej. O każdej zmianie w ww. procedurach osoby te są na bieżąco informowane.

## 4.4. Procedury rejestrowania zdarzeń

### *4.4.1. Rejestrowane zdarzenia*

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

### *4.4.2. Częstotliwości kontroli zebranych informacji*

Administratorzy Rejestru monitorują rejestrowane operacje oraz zdarzenia i co najmniej raz dziennie dokonują ich kontroli.

### *4.4.3. Czas przechowywania*

Rejestry zebranych operacji i zdarzeń są archiwizowane i przechowywane przez co najmniej 3 lata.

### *4.4.4. Ochrona*

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 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 i disaster recovery

### *4.5.1. Obsługa incydentów*

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

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

*4.5.2. Uszkodzenie danych, oprogramowania lub sprzętu*

Materiał kryptograficzny w postaci kluczy prywatnych przechowywany jest na więcej niż jednym urządzeniu HSM (Hardware Security Module).

W sytuacji awarii wszystkich urządzeń HSM w głównej lokalizacji istnieje możliwość przekierowania ruchu i korzystania z urządzeń HSM znajdujących się w lokalizacji zapasowej bez konieczności przełączania całej infrastruktury Registry.

W sytuacji awarii wszystkich urządzeń HSM niemożliwe stanie się podpisywanie nowych rekordów umieszczanych w strefie NASK. Niemożliwe stanie się również ponowne podpisanie istniejących rekordów jeżeli czas ważności ich podpisów wygaśnie. Wówczas w trybie awaryjnym zostanie usunięty rekord DS ze strefy nadrzędnej oraz opublikowana na serwerach DNS strefa NASK w postaci niepodpisanej. NASK posiada procedurę wewnętrzną opisującą usunięcie rekordu DS ze strefy nadrzędnej.

*4.5.3. Kompromitacja 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. Contingency plan*

Utrzymywania jest stała gotowość do przełączenia systemu Registry do lokalizacji zapasowej. Dodatkowo wszelkie instrukcje, procedury oraz materiał kryptograficzny przechowywane są w miejscu bezpiecznym poza lokalizacją główną.

Decyzję o przełączeniu do lokalizacji zapasowej podejmuje kierownik wyznaczonego zespołu w strukturze organizacyjnej NASK informując o swojej decyzji swojego zwierzchnika.

# 5. Kontrola bezpieczeństwa technicznego

## 5.1. Generowanie i instalowanie pary kluczy

### *5.1.1. Generowanie pary kluczy*

Klucze generowane są w sprzętowym module bezpieczeństwa (HSM) zarządzanym przez osoby pełniące rolę *Administratorów HSM*. Wszystkie czynności wykonywane na urządzeniu HSM odbywają się przy obecności co najmniej trzech *Administratorów HSM*.
Do wygenerowania kluczy, potrzebna jest dodatkowa obecność 3 osób z grupy *Administratorów z uprawnieniami do generowania kluczy*. Procedura generowania kluczy opisana jest w dokumentacji wewnętrznej NASK. Przyjęte przez Rejestr procedury wymuszają rozpoczęcie niezwłocznie po generowaniu klucza procedury synchronizacji urządzeń HSM.

### *5.1.2. Publikacja klucza publicznego KSK*

Klucz publiczny w sposób bezpieczny pobierany jest przez *Administratorów HSM* i publikowany zgodnie informacją w punkcie 2.2.

### *5.1.3. Parametry klucza publicznego i kontrola jakości*

Parametry klucza publicznego oraz zasady i sposoby ich kontroli określone zostały 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 inżynierii modułu kryptograficznego

Wszystkie operacje kryptograficzne dotyczące kluczy prywatnych wykonywane są w urządzeniu HSM, a klucze prywatne nie mogą znaleźć się w formie niezabezpieczonej poza tym urządzeniem.

### *5.2.1. Normy i kontrola modułu kryptograficznego*

Kryptograficzny moduł sprzętowy wykorzystywany przez NASK musi posiadać odpowiedni certyfikat.

### *5.2.2. Wieloosobowa kontrola klucza prywatnego*

Wieloosobowy dostęp do kluczy opisany został w punkcie 4.2.

### *5.2.3. Depozyt kluczy prywatnych*

NASK nie przekazuje kluczy prywatnych do depozytu.

*5.2.4. Kopia bezpieczeństwa*

Klucze są archiwizowane w formie zaszyfrowanej kluczem Master Backup Key (MBK), która przechowywana jest w bezpiecznym miejscu. Do stworzenia kopii potrzebne są osoby reprezentujące rolę *Administratorów HSM,* natomiast do odtworzenia kopii w sytuacji uszkodzenia danych na urządzeniu HSM potrzebne są osoby reprezentujące dwie role *Administratorzy HSM* oraz *Administratorzy klucza MBK*.

*5.2.5. Przechowywanie klucza prywatnego na HSM*

Klucze prywatne przechowywane są w urządzeniu HSM w postaci zaszyfrowanej specjalnym kluczem pozostającym tylko i wyłączenie w urządzeniu HSM. W sytuacji naruszenia integralności urządzenia poprzez atak fizyczny na urządzenie, klucz zostaje trwale usunięty z urządzenia HSM. Efektem jest brak możliwości odszyfrowania materiału kryptograficznego.

*5.2.6. Archiwizacja klucza prywatnego*

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

*5.2.7. Transfer klucza prywatnego z i do modułu kryptograficznego.*

Transfer klucza prywatnego z i do urządzenia HSM odbywa się tylko w postaci kopii zapasowej i przywrócenia jej na innym urządzeniu HSM. Instrukcja tworzenia i przywracania kopii zapasowej jest opisana w procedurach wewnętrznych NASK.

*5.2.8. Metoda aktywacji klucza prywatnego*

Klucze prywatne są aktywowane za pomocą oprogramowania podpisującego przy obecności osób pełniących role *Administratorów HSM* oraz *Administratorów z uprawnienia do generowania kluczy*.

*5.2.9. Metoda dezaktywacji klucza prywatnego*

Klucze prywatne są dezaktywowane za pomocą oprogramowania podpisującego przy obecności osób pełniących rolę *Administratorów HSM* .

*5.2.10. Metoda niszczenia klucza prywatnego*

Nieużywane klucze prywatne są usuwane z systemu związanego z zabezpieczaną strefą NASK. Klucze usuwane są przez *Administratorów HSM*.

### 5.3. Pozostałe aspekty zarządzania parą kluczy

*5.3.1. Archiwizacja kluczy publicznych*

Klucze publiczne archiwizowane są na serwerze backupowym podłączonym do systemu backupu centralnego. Serwer backupowy pozostaje pod kontrolą wyznaczonego zespołu w strukturze organizacyjnej NASK.

*5.3.2. Czas użycia kluczy*

Klucze przestają być ważne z momentem zaprzestania ich produkcyjnego wykorzystania. Klucze nie mogą być ponownie wykorzystywane.

## 5.4. Aktywacja danych autoryzacyjnych

Każda z osób biorących udział w procedurach DNSSEC posiada indywidualny klucz dostępu. Każdy klucz dostępu przypisany jest tylko i wyłącznie do jednej osoby.

Dane do logowania nie powielają się i są znane tylko jednej osobie.

*5.4.1. Aktywacja danych*

Każdej osobie pełniącej rolę w procesie DNSSEC zostaje wygenerowany i przypisany indywidualny klucz dostępu. Generowanie kluczy dostępowych odbywa się w obecności *Administratorów HSM*.

*5.4.2. Ochrona danych autoryzacyjnych*

Każda osoba pełniąca rolę w procedurach DNSSEC zobowiązana jest do ochrony danych autoryzacyjnych w postaci klucza dostępu. W sytuacji utraty klucza dostępu jego użytkownik zobowiązany jest do natychmiastowego powiadomienia o tym fakcie osób pełniących rolę *Administratorów HSM*.

*5.4.3. Inne aspekty danych autoryzacyjnych*

Rejestr nie będzie przechowywał kopi 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 następuje niezwłoczne unieważnienie tego klucza, a następnie wygenerowanie nowego klucza dostępowego i przypisanie go osobie pełniącej daną rolę.

## 5.5. Kontrola bezpieczeństwa urządzeń

Krytyczne elementy systemu Registry zostały odseparowane i znajdują się w odpowiednio zabezpieczonej lokalizacji (punkt 4.1). Dostęp do urządzeń jest ograniczonych, a sposób wykorzystania urządzeń rejestrowany i poddawany kontroli (punkt 4.4).

## 5.6. Kontrola bezpieczeństwa sieci

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

## 5.7. Timestamping

System Registry jest zsynchronizowany z serwerem czasu utrzymywanym przez NASK.

## 5.8. Cykle kontroli technicznej

### *5.8.1. Kontrola rozwoju systemu*

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

### *5.8.2. Kontrola zarządzania bezpieczeństwem*

Rejestr przeprowadza systematyczne kontrole bezpieczeństwa i ocen ryzyk dla systemu jak również poddaje się cyklicznym audytom bezpieczeństwa systemu.

### *5.8.3. Zarządzanie zmianą*

Rejestr stosuje System Zarządzania Zmianą do zarządzania oprogramowaniem odpowiedzialnym za operacje DNSSEC.

# 6. Podpisywanie strefy

## 6.1. Długość i algorytm klucza

W przypadku kluczy KSK stosowany jest algorytm RSA o długości klucza 2048 bitów, zaś w przypadku kluczy ZSK o długości 1024 bitów.

## 6.2. Uwierzytelnianie nieistniejących rekordów

Rejestr korzysta ze standardów NSEC3 określonych 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 3 miesiące.

## 6.5. Wymiana kluczy KSK

Wymiana kluczy KSK przeprowadzona jest co 6 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 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

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

## 7.1. Częstotliwość audytu

O konieczności przeprowadzenia audytu decyduje NASK. Audyt całościowy przeprowadzany jest nie rzadziej niż raz na dwa lata. Częściej niż co dwa lata może być przeprowadzany audyt częściowy. Podstawowe przesłanki do przeprowadzania audytu częściowego zgodności z DPS:

- znaczące zmiany wprowadzone w procesach, infrastrukturze lub organizacji,
- zauważone istotne 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, posiadać znajomość standardów i norm bezpieczeństwa IT, oprogramowania BIND, 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 jednej z ról określonych w punkcie 4.2.1. Audytor może być ekspertem zatrudnionym przez NASK do wykonania tego zadania.

## 7.4. Zakres audytu

Audyt całościowy obejmuje zgodność działania Rejestru z procedurami i wymogami opisanymi w DPS jak i z procedurami wewnętrznymi, których ze względów bezpieczeństwa nie można ujawnić w tym dokumencie, a których istnienie wynika z wymogów DPS.
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/obszarów DPS, w których wprowadzono zmiany lub wystąpiły nieprawidłowości. Taki audyt jest nazywany audytem częściowym. O audycie audytowani powinni być poinformowani z odpowiednim wyprzedzeniem.

## 7.5. Eliminowanie rozbieżności

Audytor w momencie wykrycia nieprawidłowości w działaniu Rejestru i procedur związanych z zabezpieczonymi DNSSEC strefami NASK informuje o nich osoby audytowane oraz kierownictwo Rejestru, które podejmie działania naprawcze oraz zapobiegawcze, gdy jest to niezbędne.

## 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*.
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.

## 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.