register.si

DNSSEC izjava

o pravilnikih in postopkih

Akademska in raziskovalna mreža Slovenije

Kazalo

1. Uvod

Ta dokument je izjava zavoda **Arnes** o varnostnih ukrepih in postopkih, ki se skupaj z varnostnimi razširitvami sistema imenskih domen (DNSSEC) uporabljajo v slovenski vrhnji domeni **.si**. Dokument je skladen z osnutkom RFC »Izjava o pravilnikih in postopkih za protokol DNSSEC«. DNSSEC izjava je eden od več dokumentov, pomembnih za delovanje območja **.si**.

1.1 Pregled

DNSSEC je nabor zapisov in sprememb protokola, ki omogočajo identifikacijo DNS odgovorov in zagotavljajo, da ostane vsebina med prenosom nespremenjena, vključno z mehanizmi za preverjanje pristnosti zanikanja obstoja. Zapisi DNS, zaščiteni s protokolom DNSSEC, so kriptografsko podpisani in v hierarhijo DNS prinašajo asimetrično kriptografijo.
Zaupanje upošteva enako verigo kot drevo DNS, kar pomeni, da izvira iz korenske domene in se prenaša na enak način kot lastništvo domene.

Namen tega dokumenta je omogočiti lokalni internetni skupnosti, da lahko določi stopnjo zaupanja, ki jo želi dodeliti Arnesu za upravljanje protokola DNSSEC. V dokumentu so podrobno opisani postopki in pravilniki, ki jih Arnes uporablja pri upravljanju storitev DNSSEC za območje .si.

1.2 Ime in identifikacija dokumenta

Naziv dokumenta: DNSSEC izjava o pravilnikih in postopkih

Različica: 1.0

Ustvarjeno: 25. november 2011

Posodobljeno: 25. november 2011

Objavljeno: 1. December 2011

1.3 Skupnost in upoštevnost

Ta dokument velja izključno za vrhnjo domeno .si in opisuje postopke ter varnostne ukrepe, ki jih je treba upoštevati pri upravljanju in uporabi ključev ter podpisov pri Arnesovem podpisovanju območja .si.

Arnes trenutno ne sprejema javnih ključev podrejenih območij v obliki zapisov DS (Delegation Signer) za vključitev v območje .si.

Določene so naslednje vloge in odgovornosti.

1.3.1 Register

Arnes upravlja vrhnjo domeno .si in je odgovoren za delovanje območja .si v internetu.

Arnes je edini register za domeno .si. Odgovornost registra je, da podpisuje območje .si in zagotavlja razpoložljivost javnih ključev (KSK in ZSK) območja za splošno javnost, pri čemer mora zaščititi zaupnost zasebnega dela ključev.

1.3.2 Odvisna stran

Gradivo javnega ključa, ki ga kot sidro zaupanja objavi register, lahko uporablja poljuben uporabnik, ki ga zanima uporaba območij kot varnih vstopnih točk za protokol DNSSEC (npr. rekurzivni strežniki, ki znajo preveriti DNSSEC odgovore). Odvisna stran je odgovorna za konfiguriranje in posodabljanje ustreznih sider zaupanja. Odvisna stran mora biti seznanjena z vsemi pomembnimi dogodki v domeni .si, povezanimi s protokolom DNSSEC.

1.4 Skrbništvo različic

Ta dokument bomo redno pregledovali in po potrebi posodobili.

1.4.1 Organizacija za skrbništvo različic

Arnes (Akademska in raziskovalna mreža Slovenije)

1.4.2 Podatki za stik

Arnes

Poštni naslov

Jamova 39
1000 Ljubljana
Slovenija

Naslov za obisk:

Tehnološki park 18
1000 Ljubljana
Slovenija

Telefon: (+386) (0)1 4798800
Faks: (+386) (0)1 47998899
E-pošta: register@register.si
Spletno mesto: http://www.register.si

1.4.3 Postopki spreminjanja različic

Spremembe tega dokumenta se izvedejo v obliki sprememb obstoječega dokumenta ali kot objava nove različice dokumenta. Ta dokument in njegove spremembe so objavljeni na naslovu http://www.register.si/dnssec/.

Veljavna je samo najnovejša različica tega dokumenta.

2 Objava in skladišča

2.1 Mesto objave

Arnes objavlja informacije v zvezi s protokolom DNSSEC na naslovu http://www.register.si/dnssec/.

Uradna veljavna različica je elektronska različica dokumenta na navedenem naslovu.

2.2 Objavljanje ključev za podpisovanje ključa (KSK)

Arnes objavlja ključe KSK za območje .si samo neposredno v korenskem območju (DS). V uporabi niso nobena druga sidra zaupanja ali skladišča.

3 Operativne zahteve

Arnes trenutno ne sprejema javnih ključev podrejenih območij za vključitev v nadrejeno območje.

4 Objekti, upravljanje in operativni nadzor

4.1 Fizični nadzor

4.1.1 Lokacija

Arnes upravlja dve fizični mesti v Sloveniji, ki vključujeta strežniške sobe in omare v Arnesovih pisarnah v Ljubljani.

4.1.2 Fizični dostop

Dostop do vseh naših prostorov je omejen na pooblaščeno osebje.

4.1.3 Električno napajanje in klimatizacija

Vsi prostori so opremljeni z neprekinjenim napajanjem (UPS) in klimatskimi napravami. Na vseh mestih, vključno s podatkovnim centrom v Arnesovih prostorih, so vzpostavljeni redundantni sistemi za primer izpada napajanja.

4.1.4 Stik z vodo

Zaradi preprečitve stika z vodo je vsa naša oprema nameščena v prostorih, ki so več metrov nad višino tal, in postavljena na dvignjeni pod.

4.1.5 Preprečevanje požarov in požarna zaščita

Vsi prostori so opremljeni z javljalniki požara in gasilnimi aparati.

4.1.6 Shranjevanje nosilcev podatkov

Gradivo ključev KSK DNSSEC je shranjeno v strojnem varnostnem modulu, skladnem s standardom FIPS 140-2 (3. stopnja varnosti).

Do zasebnega dela ključev se dostopa samo med varnostnim kopiranjem.

Izvažanje zasebnih ključev brez zaščite s šifriranjem ni mogoče.

Varnostne kopije gradiva ključev so shranjene šifrirane na izmenljivih nosilcih podatkov v trezorju na varnem mestu.

4.1.7 Odlaganje odpadkov

Dokumente in gradivo z občutljivimi podatki je treba pred odlaganjem razrezati. Nosilce podatkov, ki se uporabljajo za zbiranje ali prenašanje občutljivih podatkov, je treba pred odlaganjem narediti neberljive.

4.1.8 Varnostne kopije na drugem mestu

Varnostne kopije gradiva ključev so shranjene šifrirane na žetonu USB na varnem mestu. Varnostne kopije skrbnika sistema in žetoni varnostnih uradnikov so shranjeni na varnem mestu.

4.2 Postopkovni nadzor

4.2.1 Vloge

4.2.1.1 Zaupanja vredne vloge

Arnes pozna dve različni vlogi, povezani s protokolom DNSSEC:

- skrbnik sistema,
- varnostni uradnik.

4.2.1.2 Druge vloge

Lahko je prisotna priča. Priča nima dostopa do ključev in fizičnega ali logičnega dostopa do operativnih prostorov.

4.2.2 Število oseb, zahtevanih za opravilo

Pri vsakem postopku DNSSEC morata biti fizično prisotna vsaj dva varnostna uradnika.

Spremembe konfiguracije in druga skrbniška opravila v strojnem varnostnem modulu se lahko opravijo samo v prisotnosti dveh varnostnih uradnikov.

Spremembe konfiguracije in druga skrbniška opravila v podpisniku se lahko opravijo samo v prisotnosti dveh varnostnih uradnikov.

4.2.3 Identifikacija in preverjanje pristnosti za vlogo

Vsaka oseba z dodeljeno vlogo v postopku DNSSEC je dodana na seznam članov, vključenih v postopek.

4.2.4 Opravila, ki zahtevajo delitev dolžnosti

Skrbniki sistema so usposobljeno tehnično osebje brez upravljavske funkcije v Arnesu. Brez skrbnika sistema ni mogoče izvesti nobenega postopka DNSSEC. Ne morejo pa začeti postopka DNSSEC, če nimajo pooblastitve varnostnih uradnikov. Skrbnik sistema lahko opravi samo menjave ključev v nujnih primerih.

Varnostni uradniki nimajo tehnične vloge v Arnesu, imajo pa tehnično znanje o protokolih DNS in DNSSEC, nekateri pa imajo tudi višje upravljavske funkcije v Arnesu. Za postopke DNSSEC lahko izdajajo pooblastitve, ne morejo pa jih izvajati. Za pooblastitev mora biti fizično prisoten vsaj en varnostni uradnik, drug varnostni uradnik (iz višje uprave) pa mora postopek pisno odobriti.

4.3 Nadzor osebja

4.3.1 Zahteve za usposobljenost, izkušnje in dovoljenje za dostop do zaupnih podatkov

Vsaka oseba, ki ima vlogo v postopku DNSSEC, mora:

- imeti z Arnesom sklenjeno pogodbo za nedoločen čas,
- delati za Arnes vsaj tri mesece.

4.3.2 Postopki preverjanja preteklosti

Za zaupanja vredne vloge v razdelku 4.3.1 so potrebna ta preverjanja preteklosti:

- življenjepis kandidata,
- prejšnje zaposlitve,
- pregled priporočil.

4.3.3 Zahteve za usposobljenost

Vsaka oseba, ki ima vlogo v postopku DNSSEC, mora opraviti usposabljanje za ta postopek DNSSEC in biti ustrezno usposobljena.

4.3.4 Zahteve za pogodbeno osebje

Osebe, ki nimajo navedenih zaupanja vrednih vlog (4.2.1), ne morejo dobiti dostopa do podpisnih sistemov. Če je treba, lahko zunanji izvajalec sodeluje pri opravilu s svetovanjem. Izvajalec ne sme v nobenem primeru izvajati opravil v sistemu.

4.3.5 Dokumentacija za osebje

Informacije o rednih postopkih za varnostno kopiranje in obnovitev so na voljo vsem sodelujočim osebam. Če so postopki znatno spremenjeni, je osebje ustrezno obveščeno.

4.4 Postopki zapisovanja v dnevnik nadzora

4.4.1 Vrste dogodkov, ki se zapisujejo

Vsi postopki DNSSEC se ročno zapisujejo v dnevnik, shranjen na varnem mestu.

Vsi dostopi do podpisnikov in podpisne programske opreme se zapisujejo v sistemski dnevnik teh sistemov in sistematično preverjajo za morebitne nepravilnosti.

4.4.2 Obdobje hranjenja podatkov v dnevniku nadzora

Dnevniki se hranijo za obdobje trajanja vsaj dveh menjav ključev KSK.

4.5 Grožnje in vnovična vzpostavitev po katastrofi

4.5.1 Postopki obvladovanja dogodkov in groženj

Če dogodek privede ali bi lahko privedel do zaznane varnostne grožnje, je treba izvesti preiskavo o dogodku. Če se domneva, da je dogodek ogrozil zasebni del ključa KSK, je treba izvesti postopek za menjavo ključa KSK v nujnih primerih.

4.5.2 Poškodovana računalniška oprema, programska oprema in/ali podatki

Če pride do zgoraj navedenih poškodb, je treba sprožiti postopke obvladovanja dogodkov in izvesti ustrezne ukrepe.

4.5.3 Postopki v primeru ogrozitve zasebnega ključa entitete

V primeru domnevne ali dejanske ogrozitve ključa KSK je treba izvesti oceno stanja in z odobritvijo varnostnega uradnika ter skrbnika sistema sestaviti in izvesti načrt ukrepanja.

Informacije o nujni menjavi ogroženega ključa so posredovane na način, opisan v poglavju 2.1

4.6 Prenehanje entitete

Če mora register iz katerega koli razloga ukiniti protokol DNSSEC za območje .SI in znova vzpostaviti položaj brez podpisovanja, se to zgodi na urejen način in z ustreznim obveščanjem splošne javnosti.

Če se dejavnost prenese na drugo stranko, mora register s svojim sodelovanjem omogočiti čim bolj nemoten prehod.

5 Tehnični varnostni ukrepi

5.1 Ustvarjanje in namestitev parov ključev

5.1.1 Ustvarjanje parov ključev

Ustvarjanje ključev se izvaja v strojnem varnostnem modulu (HSM), ki ga upravlja usposobljeno in posebej določeno osebje z zaupanja vrednimi vlogami. Te osebe morajo biti prisotne pri celotnem postopku.

Pri prvem ustvarjanju ključev KSK/ZSK se ustvarijo ključi za obdobje 5 let. Postopki ustvarjanja ključev so opisani v »vodniku po postopkih«.

Celoten postopek ustvarjanja ključa se zapisuje v dnevnik, delno elektronsko in delno ročno na papir, za kar skrbi varnostni uradnik.

5.1.2 Objavljanje javnih ključev

Javni ključ je varno pridobljen iz podpisnega sistema in nato objavljen, kot je opisano v razdelku 2.2.

5.1.3 Nameni uporabe ključev

Ključ je dovoljeno uporabiti samo za eno območje. Vnovična uporaba ni mogoča.

5.2 Zaščita zasebnih ključev in tehnični nadzor kriptografskega modula

Vsi kriptografski postopki se izvajajo v strojnem modulu. Zunaj varne podpisne infrastrukture DNS ni nobenih nezaščitenih zasebnih ključev.

5.2.1 Nadzor in standardi za kriptografski modul

Arnes shranjuje ključe DNSSEC v strojnem varnostnem modulu, skladnem s standardom FIPS 140-2 (3. stopnja varnosti).

5.2.2 Nadzor zasebnih ključev (m-od-n) s strani več oseb

V celotnem sistemu ni mogoč dostop do nešifriranih ključev. Dostop do podpisnega sistema je opisan v poglavju »Zaupanja vredne vloge«.

5.2.3 »Escrow« hramba zasebnih ključev

Se ne uporablja.

5.2.4 Varnostno kopiranje zasebnih ključev

Varnostne kopije zasebnih ključev so prenesene na šifrirane nosilce podatkov in shranjene na varnem mestu. Pri varnostnem kopiranju ali obnovitvi varnostne kopije morata biti prisotna varnostni uradnik in skrbnik sistema.

5.2.5 Način aktiviranja zasebnega ključa

Zasebne ključe aktivira podpisna programska oprema. Ključi ZSK se aktivirajo samodejno. Ključi KSK so aktivirani ročno z uporabo postopka za menjavo ključa KSK DNSSEC.

5.2.6 Način dezaktiviranja zasebnega ključa

Zasebne ključe dezaktivira podpisna programska oprema. Ključi ZSK se dezaktivirajo samodejno. Ključi KSK so dezaktivirani ročno z uporabo postopka za menjavo ključa KSK DNSSEC.

5.2.7 Način uničenja zasebnega ključa

Zasebne ključe samodejno uniči strojni varnostni modul na podlagi ukaza podpisne programske opreme, ki je izdan samodejno, ko ključi niso več potrebni.

5.3 Drugi vidiki upravljanja parov ključev

5.3.1 Obdobja uporabe ključev

Ključi KSK se uporabljajo eno do tri leta. Ključi ZSK se uporabljajo 30 dni.

5.4 Podatki za aktiviranje

Med podatke za aktiviranje spadajo kode PIN za različne trezorje in ključi ter gesla PGP. Vsi podatki za aktiviranje se uporabljajo osebno.

5.4.1 Ustvarjanje in namestitev podatkov za aktiviranje

Vsak varnostni uradnik in skrbnik sistema je odgovoren za ustvarjanje lastnih podatkov za aktiviranje v skladu s postopki, opisanimi v »vodniku po postopkih«.

5.4.2 Zaščita podatkov za aktiviranje

Vsak varnostni uradnik in skrbnik sistema je odgovoren za zagotovitev najboljše možne zaščite svojih podatkov za aktiviranje, kot je opisano v »vodniku po postopkih« ali na drugačen način. Če obstaja sum ogrozitve podatkov za aktiviranje, jih mora uporabnik takoj zamenjati.

5.5 Varnostni ukrepi za računalnike

Vsi kritični sestavni deli sistemov registra so nameščeni v varnih prostorih organizacije, kot je opisano v poglavju 4.1. Dostop do operacijskih sistemov strežnikov je omejen na posameznike, ki ga potrebujejo za svoje delo, torej skrbnike sistema. Vsi dostopi se zapisujejo v dnevnik in so sledljivi na ravni posameznika.

5.6 Varnostni ukrepi za omrežja

Omrežja registra so logično razdeljena na različna varnostna območja, med katerimi je vzpostavljena varna komunikacija. Zapisovanje v dnevnik se izvaja v požarnih zidovih. Vsi občutljivi podatki, ki se prenašajo po komunikacijskem omrežju, so vedno zaščiteni z zapletenim šifriranjem.

5.7 Časovno žigosanje

Register uporablja za časovno žigosanje protokol NTP. Časovni žigi se ustvarjajo na podlagi časa UTC in so standardizirani za vse dnevniške podatke in čas veljavnosti za podpise.

5.8 Tehnični nadzor življenjskega cikla

5.8.1 Nadzor razvoja sistema

Podpisni sistem je zasnovan na podlagi arhitekture OpenDNSSEC in programske opreme BIND. Register nadzoruje razvoj dodatnega sistema, potrebnega za delovanje protokola DNSSEC, in sistem pred uvedbo ovrednoti, da se tako zagotovita kakovost in varnost podpisne storitve .si DNSSEC.

5.8.2 Zagotavljanje varnosti

Varnost podpisne storitve .si DNSSEC register zagotavlja z ukrepi, kot so nadzor vstopa/izstopa, nadzor osebja vključno z usposabljanjem, operativni nadzor vključno z nadzorom pooblastil in sistemski nadzor vključno z zaščito pred vdori in virusi.

5.8.3 Varnostni ukrepi za življenjski cikel

Register redno pregleduje, ali nadzor razvoja podpisne storitve .si DNSSEC poteka na predpisan način. Register prav tako zbira informacije o varnosti, raziskuje tehnične trende in ocenjuje/izboljšuje sistem skladno s potrebami.

6 Podpisovanje območja

6.1 Dolžine ključev in algoritmi

Za ključe KSK se trenutno uporabljajo algoritmi RSA z dolžino ključa 2048 bitov, za ključe ZSK pa z dolžino 1024 bitov.

6.2 Zanikanje obstoja s preverjanjem pristnosti

Register uporablja zapise NSEC3 »opt out«, kot določa dokument RFC 5155.

6.3 Oblika podpisa

Podpisi se ustvarjajo z asimetričnim šifriranjem in kriptografskim razpršilnim algoritmom s funkcijo SHA256.

6.4 Menjava ključa za podpisovanje območja

Menjava ključa ZSK se izvede vsakih 30 dni.

6.5 Menjava ključa za podpisovanje ključa

Menjava ključa KSK se izvede enkrat na leto z načinom dvojnega podpisa, opisanim v dokumentu RFC 4641.

6.6 Življenjska doba podpisa in pogostost vnovičnega podpisovanja

Nabori zapisov DNS se podpisujejo s ključi ZSK z obdobjem veljavnosti 14 dni. Vnovič se podpišejo vsake tri dni. Ustvarjanje datoteke območja in podpisovanje novih zapisov se izvaja vsako drugo uro.

6.7 Preverjanje nabora ključev za podpisovanje območja

Za zagotovitev podpisov in obdobja veljavnosti ključev se pred objavljanjem podatkov o območju v internetu izvedejo varnostni ukrepi za zapis DNSKEY. To se naredi tako, da se preveri veriga od zapisa DS v nadrejenem območju do ključa KSK, ZSK in podpisa zapisa SOA .si. Register preveri, ali imajo poslani zapisi DS ustrezne zapise DNSKEY v podrejenem območju, preden jih doda v območje .si.

6.8 Preverjanje zapisov DNS

Register pred razpošiljanjem preveri, ali so vsi zapisi DNS veljavni in skladni z veljavnimi standardi.

6.9 Življenjska doba zapisov DNS

DNSKEY: 3600 sekund
NSEC3: enakovredno najmanjšemu polju zapisa SOA (RFC5155)
RRSIG: enakovredno življenjski dobi nabora zapisov DNS, 7200 v praksi
DS: 7200 sekund
NSEC3PARAM: 3600 sekund