Secure Your Domain Name With DNSSEC

DNSSEC @ .MY

Ministry Of Communications And Multimedia Malaysia

.myNIC

Definitions of acronyms used in this publication

Abbreviations	Definition
DNSSEC	Domain Name System Security Extensions
RRSIG	Resource Record Signature
DNSKEY	DNS Public Key
DS	Delegation Signer
NSEC	Next Secure
NSEC3	Next Secure but with hashed next domain name
KSK	Key Signing Key
ZSK	Zone Signing Key

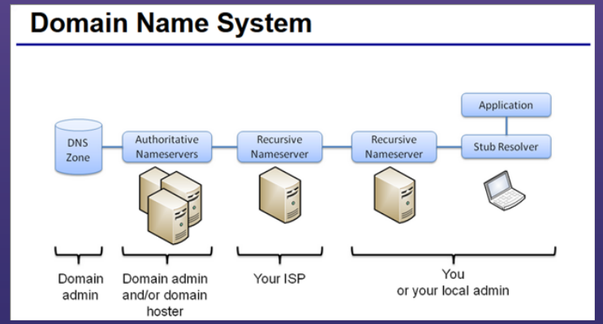
Table of Contents

Introduction to DNSSEC

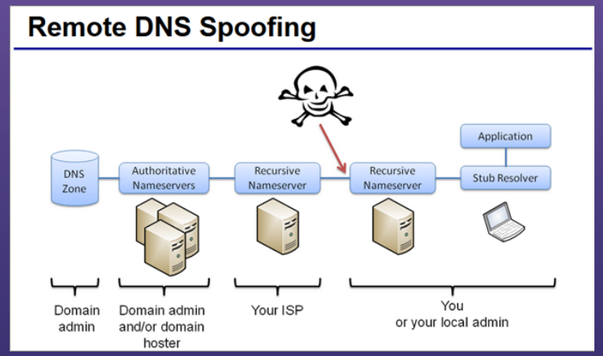
What is DNSSEC?

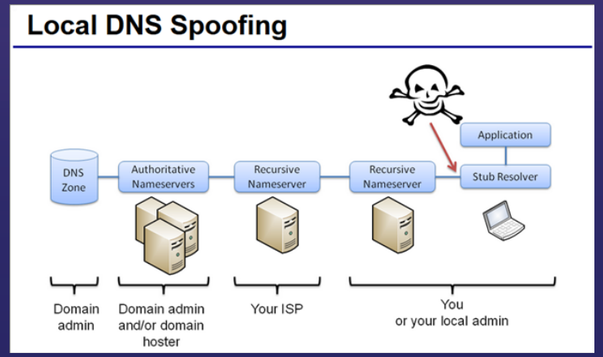
- DNS Security Extensions (DNSSEC) is a security enhancement of Domain Name System.
- DNSSEC is a technology based on an open standard specification designed to protect the name lookups from attacks such as DNS cache poisoning and spoofing.
- DNSSEC provides assurance that a domain name address is correct and can be trusted.
- If there is no DNSSEC, attackers can spoof DNS queries and victims may lead to incorrect sites.

Example of a domain name without DNSSEC signed



Examples of how DNS Spoofing will try and direct client to incorrect or fake website.



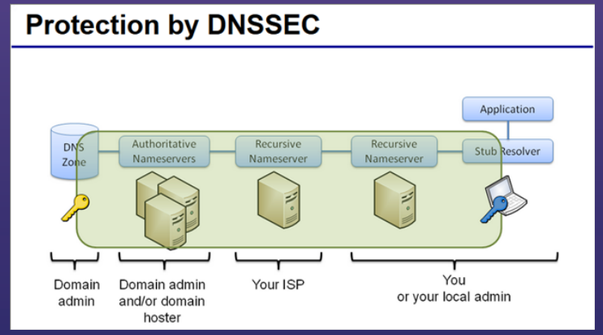


Benefits of DNSSEC

Full deployment of DNSSEC throughout the domain name system ensures:

- That the end user is connecting to the **actual** website or other service corresponding to a particular domain name.
- Protection of a critical piece of the domain name system - the DNS lookup - complementing other technologies such as SSL (https:) that protects the "conversation":
  - authentication, i.e. when a DNS resolver is looking for a domain name, the domain name's name servers help the resolver verify the records returned
- Creation of new service offerings to sign zone for domain owners.

Example of a domain name protected by DNSSEC signed



How DNSSEC Works?

- DNSSEC uses a **"chain of trust"** initiated from the top of the Internet domain name system (the "ROOT") down to the actual domain name being used.
- This "chain of trust" mechanism is used to verify that the requested domain name records are indeed correct and can be trusted.
- DNSSEC extends the existing domain records to include a Delegation Signer (DS) record. The DS is applied to a domain by its owner, which identifies a domain's authenticity so that users may trust it.
- In order to be effective, DNSSEC must be deployed at each step in the domain lookup from root zone to final domain name.

With DNSSEC (.MY Chain of Trust Example)

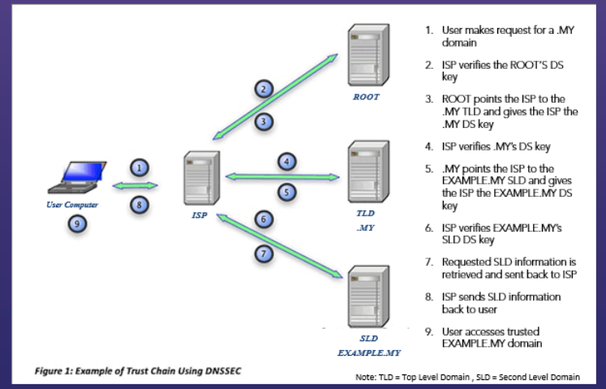


Figure 1: Example of Trust Chain Using DNSSEC

Note: TLD = Top Level Domain , SLD = Second Level Domain

DNSSEC Signing Test

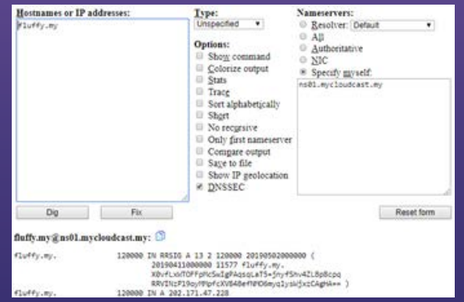
How to check or query whether the DNS Operator/DNS Hosting Provider/Own Authoritative DNS server has signed a domain name with DNSSEC?

There are many ways to check the domain name signing status prior to send the DS key to the Registry/Registrar. One of the web tools to validate the DNSSEC signing status is https://www.digwebinterface.com

1. Browse to https://www.digwebinterface.com
2. Under the Hostname or IP address, enter a domain name with DNSSEC signed
3. Options list. Tick on DNSSEC
4. Nameserver. Choose Specify myself and enter the authoritative DNS server of the domain name
5. Click on Dig button

Example with correct DNSSEC signed

Screenshots on the right are examples of a domain name signed with DNSSEC answered by the authoritative nameservers for the domain name containing the DNSSEC Resource Records **RRSIG, DNSKEY, NSEC and DS**



.MY DNSSEC Activation

DNSSEC CHAIN OF TRUST ESTABLISHED

REGISTRANT (USER)

- Registrant requests to enable DNSSEC for a domain name

DNS OPERATOR/ DNS HOSTING PROVIDER

- Generate and Manage Key
- Publishes all records
- Sign domain

DOMAIN MANAGEMENT SYSTEM

- Accepts DS record
- Update WHOIS
- Sends DS to registry

REGISTRY

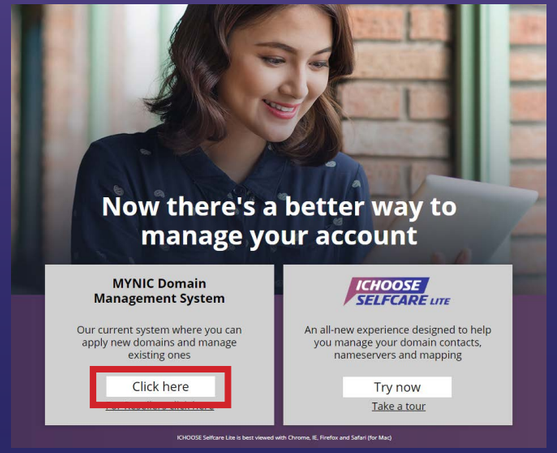
- Sign .MY domain
- Accepts DS record
- Publishes/signs record

Notes: The DNS Operator / DNS Hosting Provider MUST support DNSSEC

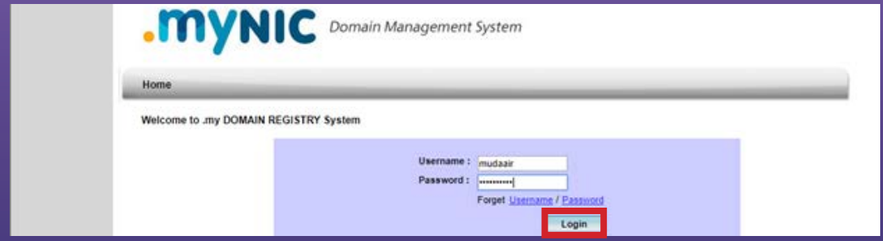
Enabling DNSSEC through MYNIC Domain Management System

1. Log in to Domain Management System (DMS) at www.mynic.my and click **Login** button on top

2. Choose the MYNIC Domain Management System and click the **"Click here"** button

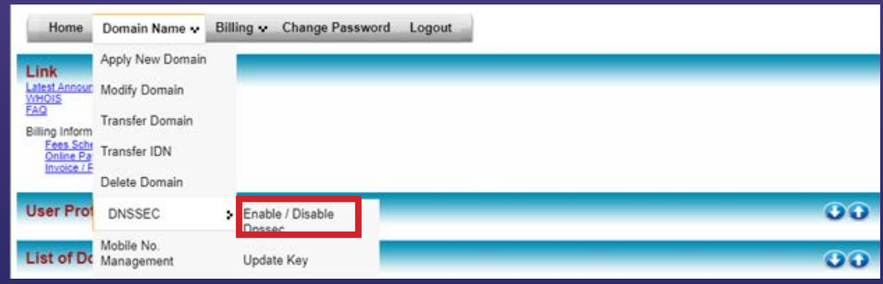


3. Enter the domain name Technical Contact username and password. Then click on **Login** button

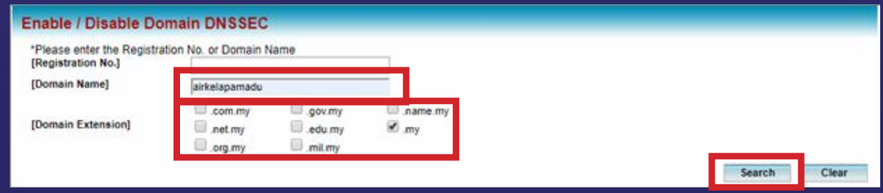


4. To enable DNSSEC

a. Click on Domain Name menu > **DNSSEC** and click on **Enable/Disable DNSSEC**



b. Enter the domain name, select on domain name extension and click on **Search** button

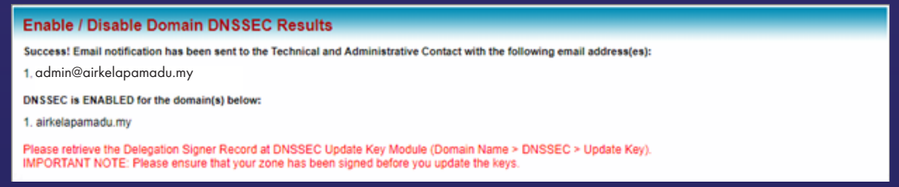


c. Search result of the domain name will be displayed as below

Under the DNSSEC status, click on **Enable**, then **tick** "I hereby.." and click on **Submit** button

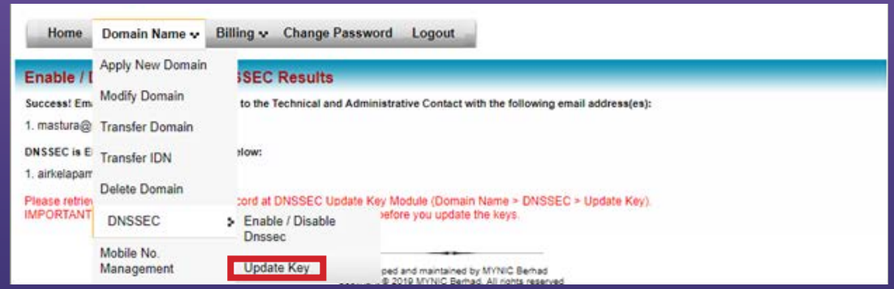
d. Next, click on **Confirm** button

After clicking on **Confirm** button, success notification on enabling the domain name DNSSEC will be displayed below

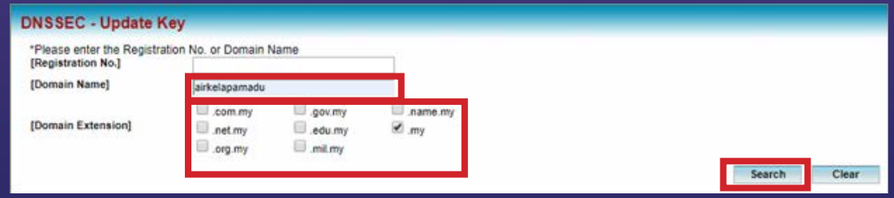


5. Retrieve and Update DNSSEC Key

a. Go back to Domain Name menu > **DNSSEC** and then click on **Update Key**

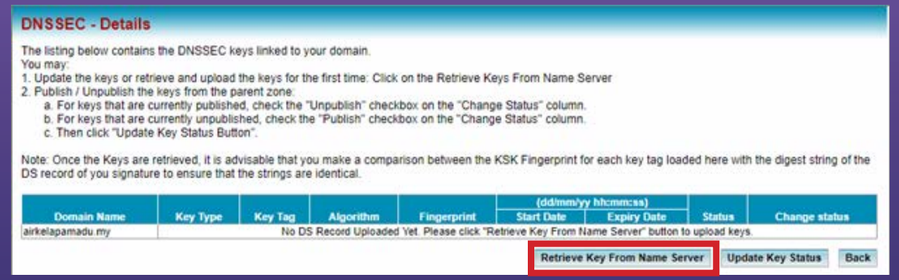


b. Enter the same Domain Name that you had enabled previously. Then click on **Search** button

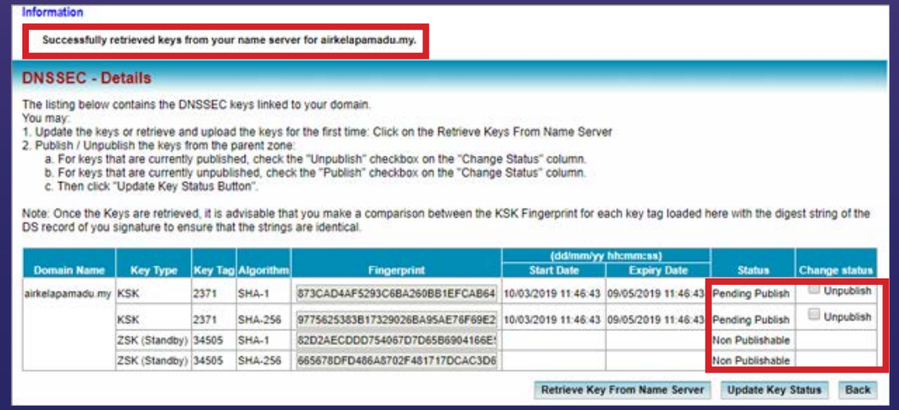


c. Under the Search Results, tick on **Select** and click on **View Details** button

d. On DNSSEC – Details screen, click on **Retrieve Key From**



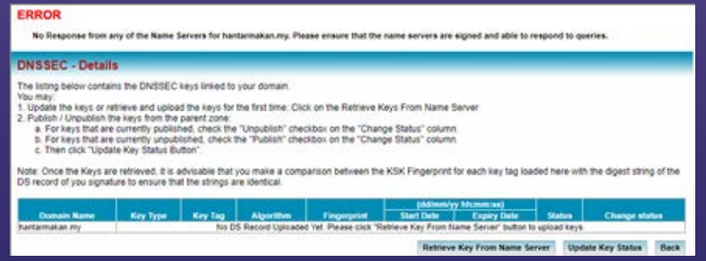
e. Once the keys are successfully retrieved, DNSSEC delegation takes in within 24 hours from this application is submitted



Information:
Below are the definition of "Pending Published", "Unpublished" and "Non Publishable" mean:

- Pending Publish – The DS Records are placed in a queue to be delegated.
- Unpublished – The DS Records has been removed from the file for signing process.
- Non Publishable – This status is only reserved for ZSK. ZSKs are shown only for information sake.

If the Retrieve Key is unsuccessful, an error message will be displayed



Recommendation
After the error has successfully been fixed, the Technical Contact of the domain name can repeat the steps retrieving the keys and ensure the keys are successfully submitted.

Frequently Asked Questions
For more information on DNSSEC, go to wiki.ichoose.my and search for "DNSSEC"

Possible cause of error:

- Nameserver that registered with MYNIC (authoritative name server) might not matched with the nameserver that domain name signed the zone.
- Missing or incorrect RRSIG record on authoritative nameserver
- The domain name has no DNSSEC sign on the authoritative nameserver

Note: The DNS Hosting Provider/DNS Operator/Technical Contact needs to check further on the DNSSEC configurations if the keys are unsuccessful to retrieve through MYNIC Domain Management System.

.MY WHOIS Service

You can view DNSSEC status of your domain name through .my WHOIS Service at https://whois.mynic.my

After your domain name is properly DNSSEC-enabled, the status “DNSSEC Signed-Delegation” will appear in the WHOIS result of the domain name

DNSSSEC Validation

DNSSSEC Validation using DNSViz Tool

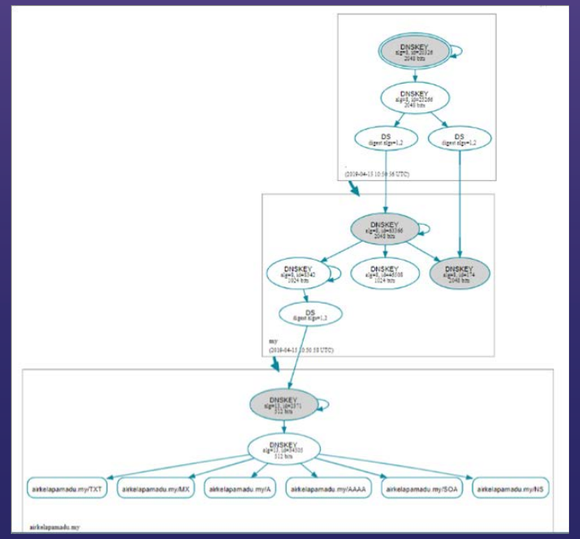
DNSViz is a DNS Visualization Tool to test and analyze of the DNSSEC authentication chain for a domain name.

You can validate the domain name DNSSSEC and view the DNSSEC chain of trust of your domain name with DNViz as per steps below:

1. Browse to http://dnsviz.net
2. Enter a domain name in the text fields that appears and click **Go** button

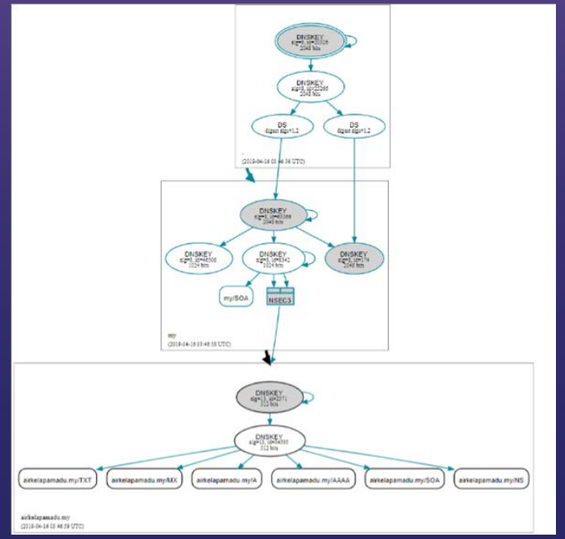
Example with correct DNSSEC

Below is an example of a domain name with functioning DNSSEC records between the Top Level Domain (TLD) nameservers and the authoritative nameservers for airkelapamadu.my



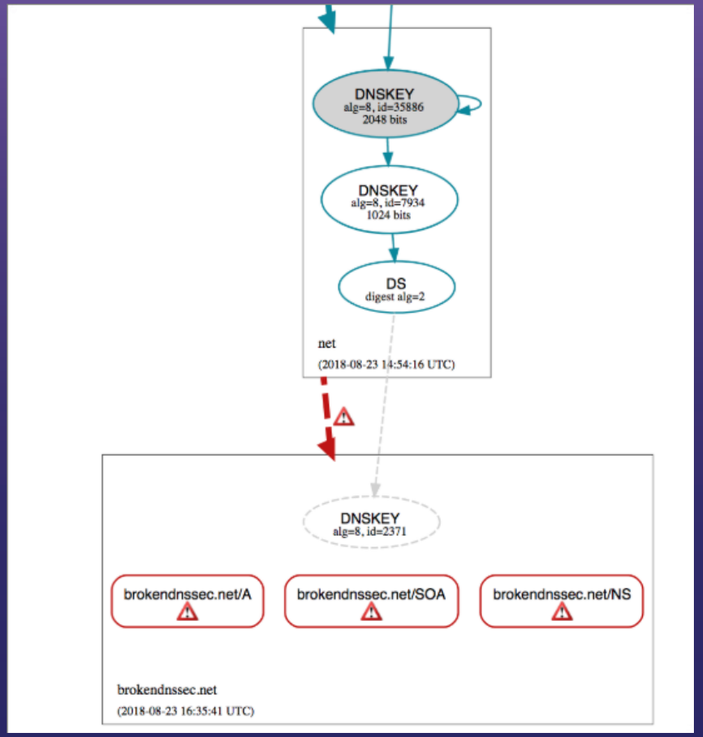
Example without DNSSEC

Below is an example of a working domain name without DNSSEC as diagrammed by DNSViz



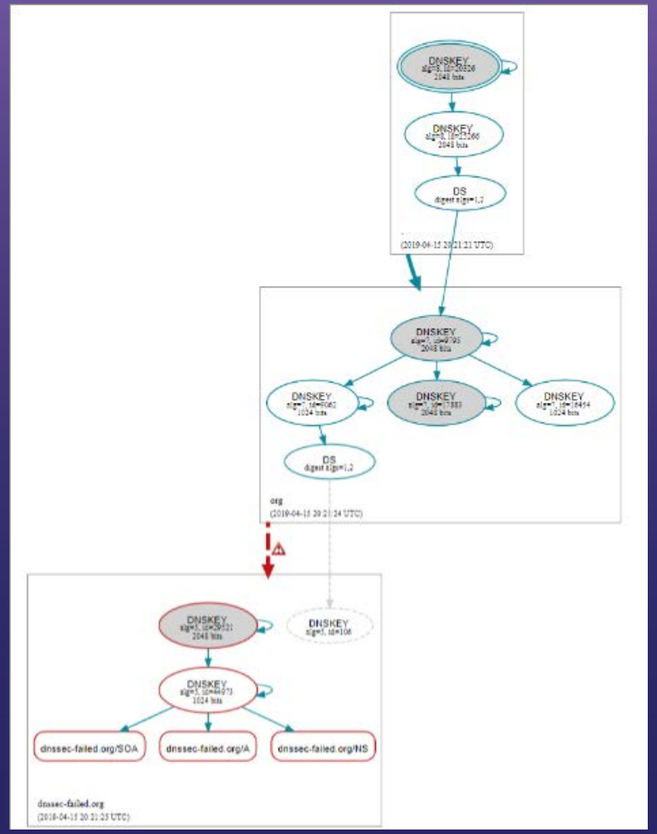
Example with missing or incorrect RRSIG record on authoritative nameserver

The example on the right is how dnsviz.net will display incorrect delegation when no valid DNSKEY records are provided by the authoritative nameserver to match the DS record published by the TLD nameserver:



Example with a broken DNSSEC domain

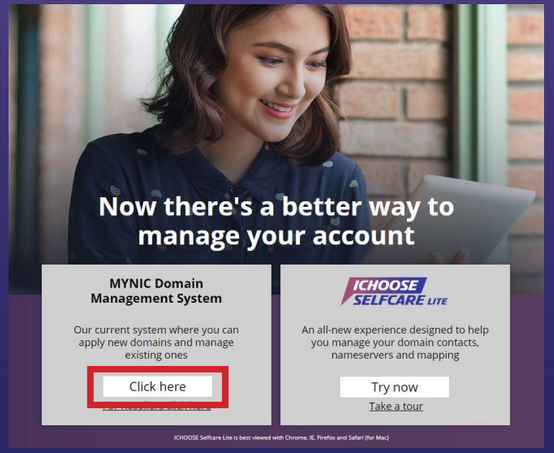
The example on the right is of how dnsviz.net will display a domain that has DNSSEC issues when no valid DS records are provided by the authoritative nameserver to match the DS record published by the TLD nameserver:



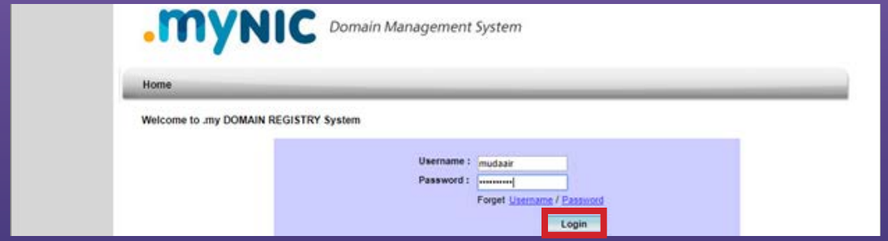
Disabling DNSSEC through MYNIC Domain Management System

1. Log in to Domain Management System (DMS) at www.mynic.my and click **Login** button on top

2. Choose the MYNIC Domain Management System and click the **"Click here"** button



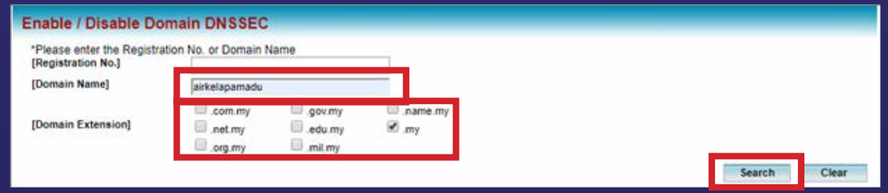
3. Enter the domain name Technical Contact username and password. Then click on **Login** button



4. To disable DNSSEC

a. Click on Domain Name menu > DNSSEC and click on Enable/Disable DNSSEC

b. Enter the domain name, select on domain name extension and click on **Search** button



c. Search result of the domain name will be displayed as below

Under the DNSSEC status, click on **Disable**, then **tick** "I hereby..." and click on **Submit** button

d. Next, click on **Confirm** button

Notification on Disable DNSSEC of the domain name will be displayed as below

MYNIC Berhad @mynicberhad