DiGiTAL academy

by register.it

Cyber Security

LA "CHAIN OF TRUST" A GARANZIA DELL'AFFIDABILITÀ DEL PROPRIO DOMINIO

Argomenti del corso

- Introduzione e premesse
Il significato della "Chain of Trust " nel mondo dei servizi digitali

- CERTIFICATI SSL

Tipologie di certificati SSL e caratteristiche di sicurezza
A cosa servono, come funzionano e il processo di emissione dei certificati SSL

SSL: Impatti sul GDPR, sanzioni del Garante per la Privacy e penalizzazioni SEO in loro assenza
Cosa si rischia in termini di sanzioni e visibilità del sito/dominio in assenza di certificati SSL

Impatti su score reputazionale del sito web e filtri dei sistemi di EP / EDR.
Scorecard negative e alert dei sistemi di Endpoint Protection e Endpoint Detaction and Response in assenza di certificarti SSL

Esempio d'installazione dei certificati SSL
Breve tutorial su come installare un certificato SSL tramite pannello di controllo di Register.it.

- DNSSEC

In cosa consiste il protocollo DNSSEC e la sua importanza
Autenticità e integrità dei record DNS

Controlli di validità della "Chain of trust"
Il meccanismo di autenticazione a cascata verificato dai resolver

Scenari di attacco verso i quali il DNSSEC è efficace
DNS Cache Poisoning e DNS Spoofing

L'impatto del DNSSEC sullo score reputazionale del dominio
Scorecard del dominio in assenza di DNSSEC

Esempi di configurazione di record DNSSEC sulle zone del dominio
Struttura, informazioni e modalità di configurazione di un record DNSSEC

Implicazioni tecniche nell'utilizzo del DNSSEC
Attenzioni e accorgimenti da adottare quando si configura un record DNS per evitare malfunzionamenti

Esempio di attivazione di DNSSEC da Pannello di Controllo
Breve tutorial su come abilitare il DNSSEC dal Pannello di Controllo di Register.it.

Introduzione e premesse

Nel dinamico mondo dei servizi digitali, di cui i servizi web costituiscono ormai la componente predominante, l'**affidabilità** del servizio è una caratteristica critica per la fiducia e la fidelizzazione dei clienti.

Il concetto di affidabilità e di modalità con cui questa è verificabile dai clienti o potenziali clienti assume una connotazione specifica nel mondo dei servizi digitali.

I criteri di valutazione di un servizio o prodotto erogato o venduto materialmente in un negozio o in un punto vendita e la rintracciabilità "fisica" dell'esercente in caso di problemi non sono direttamente applicabili nel mondo dei servizi digitali, se non ricorrendo a strumenti che permettano di **"derogare" la valutazione dell'affidabilità a soggetti terzi autorevoli o strumenti di verifica a loro volta certificati da soggetti autorevoli.**

Questo è il principio su cui si basa la **"chain of trust" dei servizi digitali**, nelle sue varie modalità di implementazione: derogare ad un soggetto terzo autorevole o a strumenti certificati da soggetti terzi autorevoli la conferma dell'affidabilità del servizio e del soggetto che lo eroga.

CERTIFICATI SSL

Tipologie di certificati SSL e caratteristiche di sicurezza

Facciamo subito un'importante premessa: l'acronimo **SSL** che sta per **Secure Socket Layer** identifica un protocollo crittografico utilizzato per la cifratura di dati in transito su internet e per l'autenticazione della relativa connessione che negli anni si è evoluto, in termini di sicurezza, nel più recente protocollo **TLS Transport Layes Security.**

Nel corso di questo webinar, come d'uso comune, faremo per praticità riferimento ai **Certificati SSL** intendendo **Certificati SSL/TLS.**

Un certificato SSL è uno strumento informatico, costituito da un **certificato digitale**, che permette la crittografia delle comunicazioni tra computer client e il server in cui si trova un sito web e fornisce strumenti per la verifica dell'autenticità di un sito, del relativo dominio e dell'eventuale soggetto proprietario.

Come proprietari o gestori di un sito web non vorreste di certo che i vostri visitatori ricevano l'avviso "La tua connessione non è privata" quando visitano il sito mentre d'altro canto come utenti, quando visitate un sito web, come vi assicurate che sia quello giusto e non uno spoof finalizzato a per rubare o diffondere le vostre informazioni?

La verifica dell'identità è essenziale quando si tratta di sicurezza web, ed è qui che entra in gioco SSL. SSL/TLS verifica l'autenticità dell'identità del server web

L'emissione di un certificato SSL prevede un **processo di verifica** dell'identità e di altre eventuali informazioni e caratteristiche del proprietario del dominio, a livelli differenti a seconda della tipologia di certificato di cui parleremo a seguire.

Tale verifica viene effettuata da un'autorità terza detta **Certification Authority (CA)** che costituisce il soggetto autorevole finale della "chain of trust", cui è delegata la verifica dell'autenticità del dominio.

Lo scopo di un certificato SSL è quindi in sintesi quello di garantire:

- **l'autenticazione del sito web**, domini ed eventuali sottodomini
- **la cifratura e protezione dei dati scambiati** tra il client dell'utente e il webserver

Di seguito verranno decritti i vari livelli di verifiche effettuate dalle Certification Authority per le varie tipologie possibili di certificati SSL

Una volta passate le verifiche necessarie per l'ottenimento di un certificato SSL, questo deve essere installato sul web server che ospita il dominio per il quale è stato emesso.

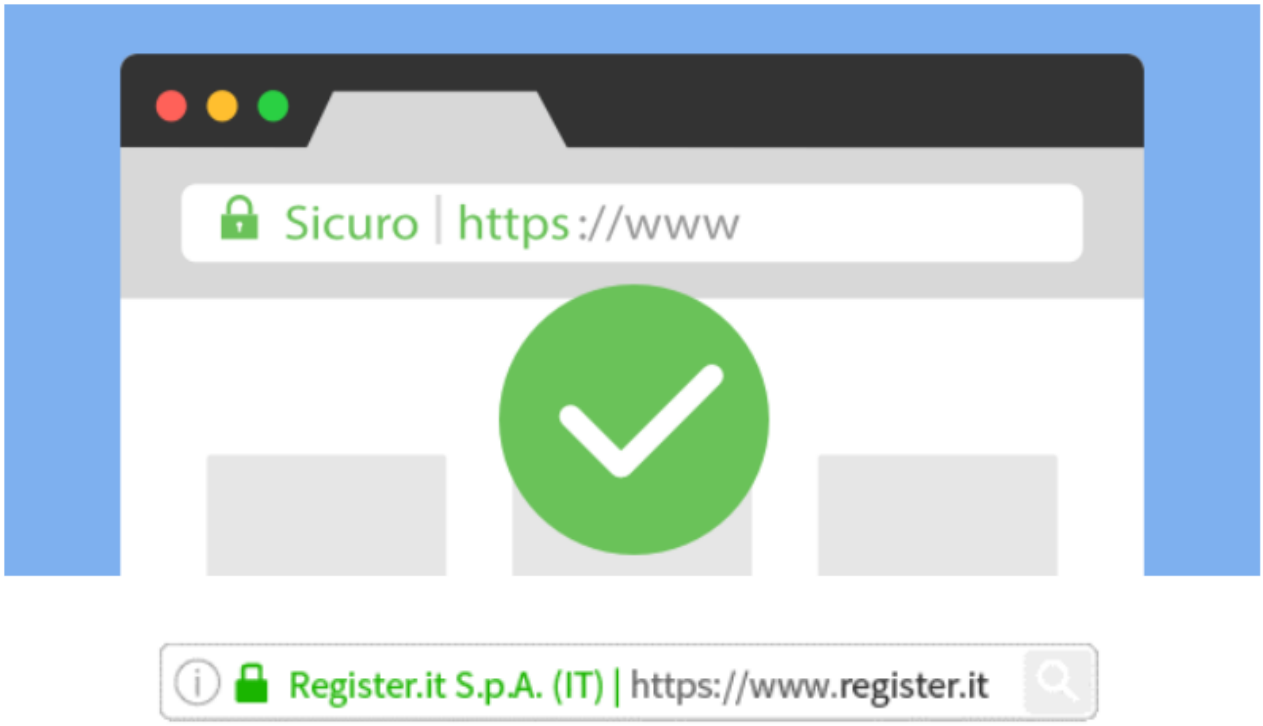
L'installazione del certificato SSL prevede in sintesi la configurazione sul web server della chiave privata e la pubblicazione della chiave pubblica per il successivo utilizzo di un algoritmo di cifratura asimmetrica per lo scambio di dati tra client e web server (protocollo TLS).

Senza entrare troppo nel dettaglio del funzionamento degli algoritmi di crittografia, tema al di fuori dell'obiettivo del presente webinar, si riporta di seguito una rappresentazione logica delle fasi dell'instaurazione di una sessione cifrata tra client e web server tramite certificato SSL, per meglio comprendere l'utilizzo di quest'ultimo a fini crittografici.

Quando un utente visita un sito web, il browser sul suo dispositivo cercherà in prima battuta il certificato SSL/TLS sito. Successivamente il browser eseguirà un "handshake" per verificare la validità del certificato e autenticare il server. Qualora il processo di autenticazione non andasse a buon fine perché il certificato non risulta valido verrebbe restituito l'alert "La connessione non è privata", finalizzato a scoraggiare l'utente dall'utilizzo del sito ritenuto poco affidabile.

Una volta che il browser di un visitatore stabilisce che il vostro certificato è valido e autentica il vostro server, crea un collegamento crittografato con il vostro server per il trasporto sicuro dei dati.

Per installare un certificato SSL, dovete passare attraverso un **processo di verifica dell'identità**. In altre parole, avere un certificato SSL è la prova che il vostro sito web è davvero il vostro sito e non uno contraffatto o una copia di quello della vostra azienda: diventa quindi una barriera efficace contro i siti di phishing.



In sostanza, SSL è un indicatore per i vostri visitatori che possono condividere in modo sicuro informazioni sensibili come numeri di carte di credito, ID, indirizzi email e password sul vostro sito web. Pertanto, SSL rafforza la fiducia tra voi e i vostri clienti/visitatori.

Certificati con convalida del dominio (DV) e con convalida del dominio Wildcard (DVW)

Un sito web protetto con un **certificato DV** mostra un **lucchetto chiuso** (Secure Site Seal) nella barra degli indirizzi. Questo tipo di certificati convalida solo la proprietà del dominio, possono essere acquisiti in modo anonimo e non legano un dominio a una persona, luogo o entità.

La CA controlla il diritto del richiedente di utilizzare un nome di dominio specifico. Nessuna prevedono verifiche su informazione relative al soggetto/azienda proprietario del dominio e nessuna informazione viene visualizzata al di fuori delle informazioni sulla crittografia all'interno del.

Questi certificati vengono rilasciati senza la necessità di inviare documenti aziendali e questo li rende la loro emissione molto pratica le aziende che per i privati. Il servizio di registrazione domini di Register.it prevede l'emissione di certificati *Let's Encript* di tipo DV.

I certificati SSL DV permettono di certificare, oltre al dominio principale, soltanto un sottodominio. Nel caso in cui si voglia utilizzare un certificato SSL di tipo DV ma su più sottodomini sarà necessario richiedere un certificato con **convalida del dominio Wildcard (DVW)** utilizzabile su infiniti sottodomini di terzo livello.

Certificati a convalida estesa (EV)

I **certificati EV** prevedono oltre al controllo del diritto del richiedente sul dominio, controlli incrociati sull'ente proprietario e sull'ubicazione fisica.

La Certificate Authority (CA) verifica il diritto del richiedente di utilizzare il nome a dominio e svolge poi un'accurata verifica sul soggetto/azienda proprietario del dominio, secondo un processo definito da specifiche linee guida del *CA/Browser Forum*.

Questo tipo di verifica viene formalmente documentata dalla CA che può anche essere prodotta in sede giudiziaria in caso di frode durante le transazioni sul sito web.

Nella barra degli indirizzi degli indirizzi web della maggior parte dei principali browser, i certificati SSL di tipo EV mostrano, oltre al lucchetto chiuso (Secure Site Seal), il nome dell'organizzazione e opzionalmente anche l'ID del paese di registrazione.

Una Certificate Authority (CA), prima di emettere un certificato SSL di tipo EV:

- verifica che l'entità abbia il diritto esclusivo di utilizzare il dominio specificato nel certificato
- verifica che l'entità abbia autorizzato correttamente l'emissione del certificato.
- verifica l'esistenza legale, fisica e operativa dell'entità,
- verifica che l'identità dell'entità corrisponda alle registrazioni ufficiali ai corrispettivi registri delle imprese

Certificati con convalida dell'organizzazione (OV)

Per i **certificati OV**, oltre alla proprietà del dominio, viene verificata anche l'organizzazione richiedente e i dettagli del certificato possono essere visualizzati sulla maggior parte dei principali browser web.

La CA, oltre a verificare il diritto del richiedente di utilizzare il nome a dominio, effettua **delle verifiche e valutazioni sull'organizzazione**. Ulteriori informazioni aziendali verificate vengono mostrate ai clienti quando si fa clic sul Sigillo sito sicuro, offrendo una maggiore visibilità in chi si trova dietro il sito e una maggiore fiducia associata. Il nome dell'organizzazione appare anche nel certificato sotto il campo ON.

SSL: Impatti sul GDPR, sanzioni del Garante per la Privacy e penalizzazioni SEO in loro assenza

L'Autorità garante per la protezione dei dati personali si è già espressa con provvedimenti e pubblicazioni sul significato più tecnico di "protezione dei dati personali" ai fini dell'integrità e della riservatezza dei dati, affermando che:
«L'interazione di un utente con un sito web ai fini della trasmissione di dati personali debba essere protetta con protocolli crittografici SSL (Secure Socket Layer), garantendo una migliore sicurezza a fronte dei rischi di furto di identità sempre presenti nell'interazione web con normali protocolli http in chiaro.»

Nell'ottobre 2022 l'Autorità è arrivata a **sanzionare per 15.000 euro** un'azienda che, non utilizzando certificati SSL, non ha di fatto rispettato gli artt. 5, par. 1, lett. f), 25, par. 1, e 32 del GDPR, che prevedono che il titolare del trattamento
«…tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, debba mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso, la cifratura dei dati personali».

Le tecniche di **Search Engine Optimization (SEO)** ovvero l'ottimizzazione dei parametri finalizzata a rendere più facilmente ricercabile un sito web e i suoi contenuti dai motori di ricerca e a migliorarne il posizionamento (ranking) tra i risultati.

I vari motori di ricerca, per determinare la posizione dei siti web nella pagina risultati, considerano vari fattori differenti e molteplici variabili. Un fattore di peso primario per gli algoritmi di ricerca è la sicurezza.

Un motore di ricerca considerato affidabile non posizionerà mai nei primi risultati un sito non sicuro e tenderà anzi a dargli un ranking basso anche in presenza di altri fattori che ne permetterebbero un ranking superiore. Ne va dell'affidabilità percepita del motore di ricerca stesso.

Un sito web che non dispone di un certificato SSL, non potendo garantire né una connessione sicura né tantomeno fornire alcuna credenziale per autenticarne la proprietà del dominio riceverà dai motori di ricerca un **ranking SEO molto basso** e la sua visibilità sul web ne sarà inevitabilmente compromessa.

I motori di ricerca utilizzano strumenti come i web crawler per scansionare la rete, individuare e mappare nei propri database queste parole chiave.

I web crawler però non sono gli unici strumenti adoperati dai motori di ricerca per la creazione e gestione di un ranking tra i diversi siti web.

In questa ricerca, oltre ai web crawler, vengono utilizzati degli algoritmi, più o meno sofisticati a seconda del motore di ricerca, che analizzano diversi fattori per determinare "l'importanza" ed il relativo ranking nella presentazione dei risultati di ricerca di un sito web.

Ogni motore di ricerca considera un differente **insieme di fattori per determinarne il posizionamento dei siti** web nella pagina dei suoi risultati di ricerca. L'algoritmo utilizzato da Google valuta oltre 200 fattori diversi per determinare il ranking di un sito web.

Alcuni dei più importanti fattori valutati sono:

- presenza di certificati SSL
- qualità (verificabile) dei contenuti
- numero di backlink da altri siti Web che si collegano a quel particolare sito o pagina
- affidabilità dei backlink al punto precedente
- posizionamento delle parole chiave all'interno del nome del dominio, dei titoli e dei contenuti;
- velocità del sito e l'ottimizzazione delle immagini.

Impatti su score reputazionale del sito e filtri dei sistemi di EP / EDR.

Sul mercato esistono diversi prodotti o servizi che raccolgono informazioni pubbliche (fonti OSINT), analizzano in modo non invasivo le pagine e le interfacce web e, all'occorrenza, utilizzano anche tecniche più complesse per recuperare informazioni non pubbliche per fornire lo scoring di un servizio web.

Questi strumenti sono in grado di presentare in maniera aggregata o di dettaglio un'analisi su più tipologie di fattori di rischio legati al servizio web.

La complessità di queste valutazioni può essere molto variabile ma in ogni caso un servizio web erogato da un dominio senza certificato SSL riceverà sicuramente da questi strumenti uno scoring complessivamente negativo o comunque insufficiente a garantire un servizio sicuro.

Esempio d'installazione dei certificati SSL

Si riportano di seguito i link a dei pratici tutorial step by step per sia per la richiesta di generazione del file di *Certificate Signing Request* (CSR) per poter associare un certificato SSL al proprio dominio che la successiva installazione del certificato tramite pannello di controllo di Register.it.

https://www.register.it/assistenza/generazione-file-csr-per-il-certificato-ssl/

https://www.register.it/assistenza/installare-certificato-SSL-cpanel/

DNSSEC

In cosa consiste il protocollo DNSSEC e la sua importanza

Un **Domain Name System** è un sistema che ha il compito di "tradurre" o "risolvere" la URL del sito in un indirizzo IP numerico che identifica il sito nel web, permettendo così la visualizzazione dei contenuti del sito web associato a quel nome a dominio.

Le informazioni per effettuare questa mappatura sono contenute nei record DNS. L'affidabilità del DNS dipende, quindi, dall'autenticità e dall'integrità di queste informazioni.

Per progettazione del servizio DNS, un resolver non è in grado di rilevare facilmente una risposta contraffatta a una sua interrogazione. Un aggressore può facilmente mascherarsi come il server autoritativo che un resolver ha originariamente interrogato, creando uno spoofing della risposta che sembra provenire da quel server. In altre parole, un aggressore può reindirizzare un utente a un sito potenzialmente dannoso senza che l'utente se ne accorga.

I resolver ricorsivi memorizzano nella cache i dati DNS che ricevono dai name server autoritativi per accelerare il processo di risoluzione. Se uno stub resolver chiede i dati DNS che il resolver ricorsivo ha nella sua cache, il resolver ricorsivo può rispondere immediatamente senza il ritardo introdotto dalla prima interrogazione di uno o più server autoritativi. Questo affidamento alla cache ha però un lato negativo: se un aggressore invia una risposta DNS contraffatta che viene accettata da un resolver ricorsivo, il risultato è che l'aggressore ha "avvelenato" la cache del resolver ricorsivo che restituirà i dati DNS fraudolenti ad altri dispositivi che li richiedono.

Il **Domain Name System Security Extensions (DNSSEC)** è un protocollo di sicurezza che garantisce e permette di verificare l'autenticità e l'integrità dei record DNS.

Il protocollo DNSSEC rafforza l'autenticazione nel DNS utilizzando firme digitali basate sulla crittografia a chiave pubblica. Con il DNSSEC, non sono le query e le risposte DNS a essere firmate crittograficamente, ma sono i record DNS stessi a essere firmati dal "proprietario" dei dati.

Il protocollo DNSSEC aggiunge in sintesi due importanti funzionalità al protocollo DNS:

- L'**autenticazione** dell'origine dei dati, che consente a un resolver di verificare crittograficamente che i dati ricevuti provengano effettivamente dalla zona da cui si ritiene provengano.

- La protezione dell'**integrità** dei dati, che consente al resolver di sapere che i dati non sono stati modificati durante il transito da quando sono stati originariamente firmati dal proprietario della zona con la chiave privata della zona stessa.

Controlli di validità della "Chain of trust"

La firma digitale dei record DNS prevede innanzitutto che la funzionalità DNSSEC sul DNS generi una **coppia di chiavi** da utilizzare per la **cifratura asimmetrica** che realizza la firma.

- La **chiave privata** è il parametro segreto che rimane interna nel sistema DNS ed è utilizzata per firmare (cifrare) i record DNS della zona.

- La **chiave pubblica** viene pubblicata dal DNS tramite un record apposito, DNSKEY Record, rendendola disponibile per poter decifrare la firma dei record DNS e quindi la loro autenticità e

integrità.

L’affidabilità della chiave pubblicata costituisce il punto critico di tutto l’algoritmo ed è "demandata" ad una "Chain of Trust" di autorità simile alla gerarchia dei DNS utilizzata per la risoluzione dei nomi a dominio.
Il proprietario della zona utilizza la chiave privata della zona per firmare i dati DNS nella zona e generare firme digitali su tali dati.

Ogni resolver ricorsivo che consulta i dati della zona recupera anche la chiave pubblica della zona, che utilizza per convalidare l'autenticità dei dati DNS.

Il resolver ha anche il compito di confermare che la firma digitale sui dati DNS recuperati è valida. In caso affermativo, i dati DNS sono legittimi e vengono restituiti all'utente. Se la firma non è valida, il resolver ipotizza un attacco, scarta i dati e restituisce un errore all'utente.

L’affidabilità della chiave pubblica della zona principale è quindi un importante punto di partenza per la convalida dei dati DNS.

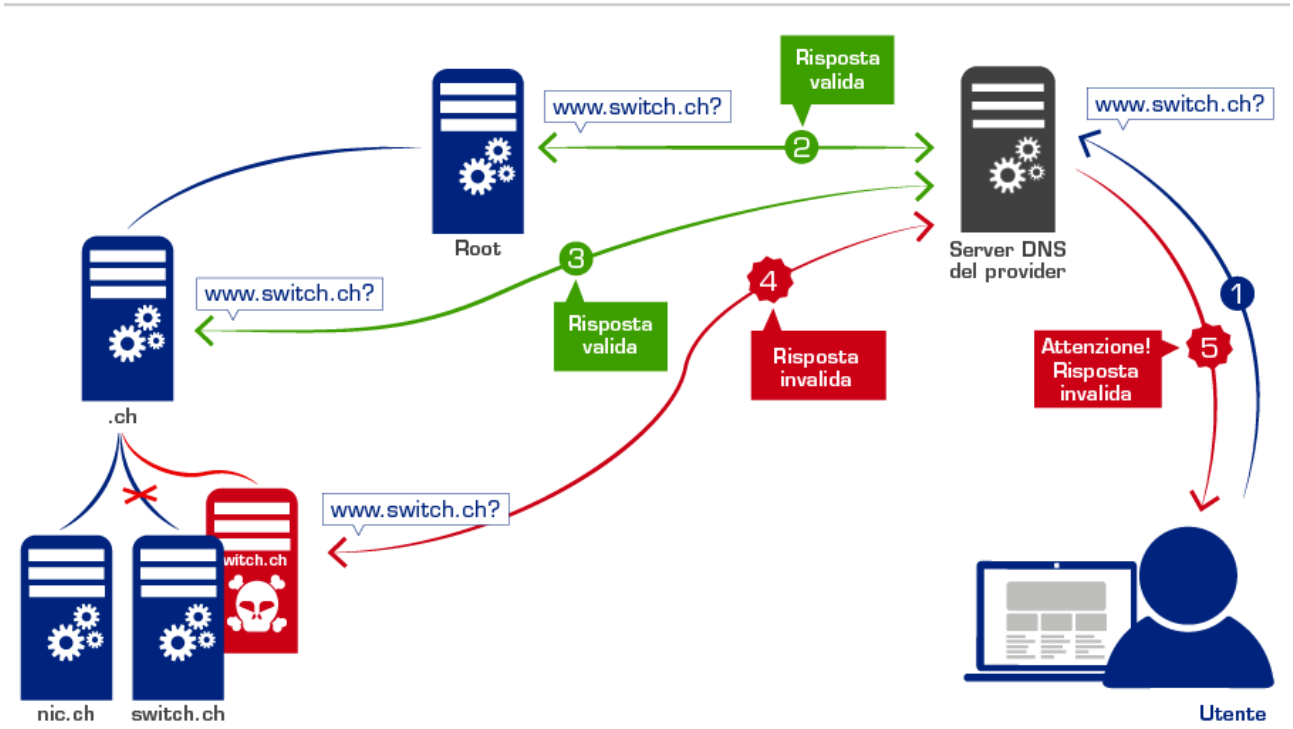
Se un resolver si fida della chiave pubblica della zona radice, può fidarsi delle chiavi pubbliche delle zone di primo livello firmate dalla chiave privata della radice, come ad esempio la chiave pubblica della zona *tld (es. org)*. E poiché il resolver può fidarsi della chiave pubblica della zona *org*, può fidarsi delle chiavi pubbliche firmate dalla rispettiva chiave privata, come la chiave pubblica di *xxx.org*.

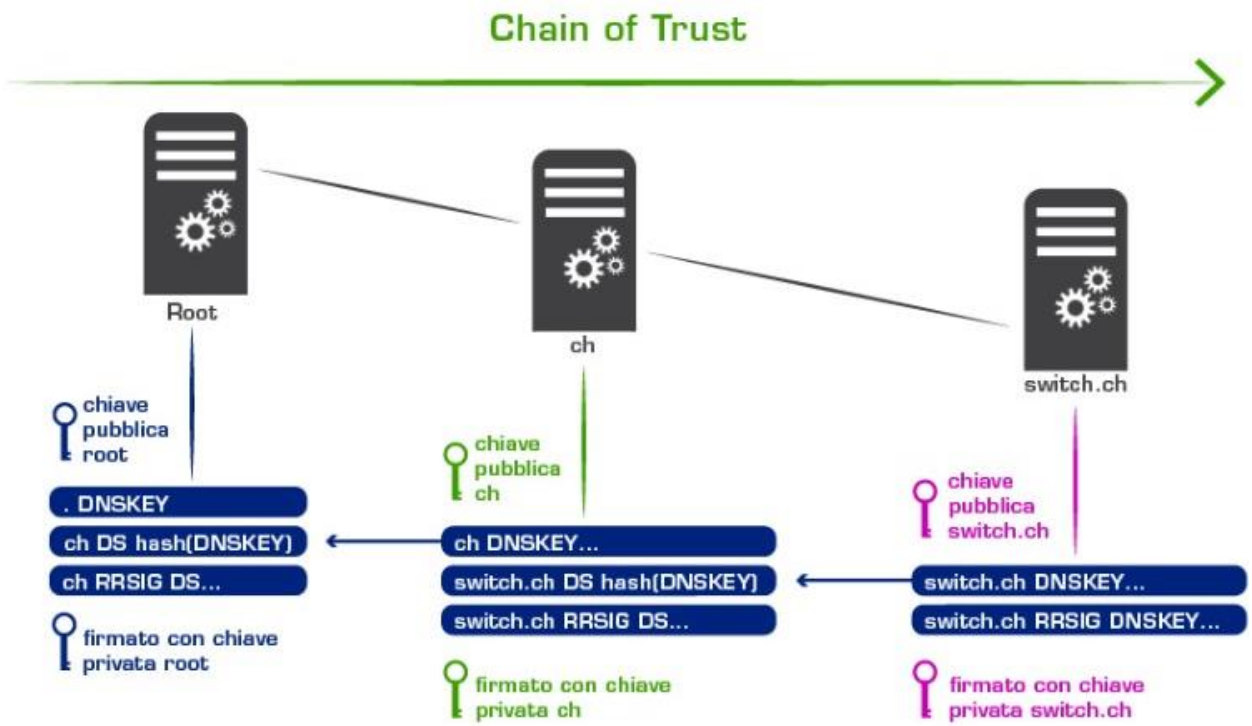
La firma generazione della chiave della root DNSSEC segue un articolato processo **Tecnico/Organizzativo** detto **"cerimonia di firma della root DNSSEC"** atto a garantire elevatissimi livelli di sicurezza tecnica ed organizzativa per l’affidabilità della chiave pubblica pubblicata dl root server.

Tecnicamente la zona genitore non firma direttamente la chiave della zona figlio ma l’algoritmo è più complesso, tuttavia, il risultato è lo stesso che si avrebbe se la zona "genitore" firmasse la chiave della zona "figlio".

La sequenza di chiavi crittografiche che firmano altre chiavi crittografiche è chiamata **"chain of trust"** (catena di fiducia). La chiave pubblica all'inizio di una catena di fiducia è chiamata "**ancora di fiducia**". Un resolver ha un elenco di ancore di fiducia, che sono chiavi pubbliche per diverse zone di cui il resolver si fida implicitamente.

La catena si basa quindi sull’interattività della deroga verso il livello superiore che è autorevole per garantire l’autenticità per lo specifico livello di dominio.





Scenari di attacco verso i quali il DNSSEC è efficace

DNS Spoofing

In questa tipologia di attacco il sistema vittima effettua una query DNS che viene catturata dall'attaccante che **si spaccia per il DNS destinatario** inviando alla vittima una risposta contenente informazioni false per **ridirezionare** la connessione della vittima **verso un dominio diverso**, solitamente predisposto **per effettuare attività fraudolente** o veicolare altri tipi di attacchi sulla vittima.

In assenza di DNSSEC che verifica l'autenticità delle risposte all'attaccante, può essere sufficiente **intercettare l'ID della query DNS** inviata e rispondere al mittente inserendo l'ID atteso prima del DNS destinatario per **spacciare la risposta per quella del reale DNS server**

DNS Cache Poisoning

Questo tipo di attacco sfrutta la necessità dei DNS di utilizzare cache con un determinato periodo di vita (TTL) in cui sono presenti porzioni del record di corrispondenze IP/URL per rispondere più velocemente alle richieste.

L'attacco va ad inserire nella cache dei name server dei **record fake** creati ad hoc **per reindirizzare la connessione della vittima** con un TTL molto grande in modo che restino per molto tempo nella cache del name server prima di essere sostituiti con quelli presenti nel database.

Anche in questo caso, **in assenza del DNSSEC** per autenticare le risposte, se l'attacco riesce e la cache viene avvelenata (poisoned) **la vittima riceverà in risposta l'indirizzo malevolo** spacciato invece di quello presente nel record DNS autentico.

L'impatto del DNNSSEC sullo score reputazionale del dominio

Analogamente allo scoring di sicurezza del siti web, sono state sviluppate varie soluzioni che permettono di effettuare rapidamente, online, una **valutazione dei parametri significativi per l'affidabilità della configurazione dei DNS** su determinati domini.

Questi strumenti valutano principalmente:

- Se il nome a dominio è raggiungibile attraverso i protocolli IPv4 e IPv6
- Se tutti i nameserver associati al nome a dominio sono operativi
- Se sul nome a dominio è **abilitata la funzionalità DNSSEC** (Domain Name Security Extensions)

In base a questi valori viene emesso un punteggio che risente in modo importante dell'eventuale assenza di DNSSEC.

Esempi di configurazione di record DNSSEC sulle zone del dominio.

Di seguito vengono riportate le tipologie di record aggiunte al DNS con la configurazione del DNSSEC e la descrizione della loro funzione:

- **DNSKEY**
  Chiave pubblica che il resolver DNS utilizza per verificare le firme DNSSEC nei record DNS firmati (RRSIG)

- **RRSIG (resource record signature**)
  Contiene la firma DNSSEC per un record set. I resolver DNS verificano la firma con una chiave pubblica, memorizzata nel record DNSKEY.

- **DS (delegation signer)**
  Record che fa riferimento alla DNSKEY di una zona delegata. Il record DS si trova nella zona del nome a dominio e fa riferimento ai dati DNSSEC del sottodominio su name server esterno, in modo da poter verificare la correttezza dei dati DNSSEC del sottodominio. Il record DS viene inserito nella zona padre insieme ai record NS delegati. Questo record mappa la "Chain of Trust".

- Record per il **denial-of-existence esplicito di un record DNS**
  - **NSEC (next secure record)**
    Contiene un collegamento al nome del record successivo nella zona ed elenca i tipi di record esistenti per il nome del record. I resolver DNS utilizzano i record NSEC per verificare l'inesistenza di un nome e di un tipo di record come parte della convalida DNSSEC.

  - **NSEC3 (next secure record version 3)**
    Contiene collegamenti al nome del record successivo nella zona (in ordine di ordinamento dei nomi con hash) ed elenca i tipi di record esistenti per il nome coperto dal valore hash nella prima etichetta del nome proprio del record NSEC3. Questi record possono essere utilizzati dai resolver per verificare l'inesistenza di un nome e di un tipo di record nell'ambito della convalida DNSSEC. I record NSEC3 sono simili ai record NSEC, ma NSEC3 utilizza nomi di record con hash crittografico per evitare l'enumerazione dei nomi di record in una zona.

  - **NSEC3PARAM (next secure record version 3 parameters)**
    I server DNS autoritativi utilizzano questo record per calcolare e determinare quali record NSEC3 includere nelle risposte alle richieste DNSSEC per nomi/tipi non esistenti.

Implicazioni tecniche nell'utilizzo del DNSSEC

Di seguito sono riportati le principali implicazioni tecniche e punti di attenzione da considerare con l'adozione del protocollo DNSSEC, ampiamente compensati dai vantaggi di sicurezza che il protocollo introduce:

- Le risposte alle query DNS possono essere molto lunghe e contenere più record **DNSKEY** e **RRSIG** e in casi di attacchi DDoD ai DNS amplificarne l'effetto di saturazione delle risorse.

- Potenziali **errori nell'inserimento delle DNSKEY,** ove non generate e inserite con strumenti automatici, possono rendere le zone non visibili.

- Maggiori requisiti computazionali e cache dei resolver ricorsivi DNSSEC è molto più grande in data la necessità di gestire firme e chiavi.

- Se i client utilizzano resolver che non supportano il DNSSEC le zone con DNSSEC configurato non saranno visibili.

Esempio di attivazione di DNSSEC da Pannello di Controllo

L'attivazione del protocollo DNSSEC tramite ***Register.it*** è disponibile gratuitamente sui TLD più comuni e su molte altre estensioni.
Nella maggior parte dei casi il DNSSEC è automaticamente attivo nel momento della registrazione di un nuovo dominio o del trasferimento di un dominio su ***Register.it***.

Per alcune estensioni, come i domini **.it,** il protocollo DNSSEC è disponibile all'interno dell'Area Clienti e si Sriporta di seguito il link ad un pratico tutorial step by step per la sua attivazione.

https://www.register.it/help/come-abilitare-il-protocollo-dnssec-sul-dominio/