Personalizzazione domini certificati

InfoCert permette di definire ed attivare in autonomia domini certificati personalizzati, usualmente di terzo livello, diversi dallo standard **legalmail.it**.

In generale sono disponibili due tipologie di domini:

A. Sottodominio interno al dominio legalmail.it

Il sottodominio interno ad InfoCert sarà configurato come un dominio di terzo livello del tipo nomedominio.legalmail.it, al cui interno verranno definite caselle di posta del tipo nome.cognome@nomedominio.legalmail.it.
Il nome del dominio di terzo livello, nomedominio.legalmail.it, verrà proposto dal cliente, ma dovrà essere confermato da InfoCert sulla base di verifiche di congruità (domini o Nominativi già registrati, ecc.).
La scelta di questa tipologia di sottodominio non comporta nessun coinvolgimento operativo da parte del provider/maintainer del dominio del cliente.

B. Sottodominio personalizzato esterno diverso dal dominio legalmail.it

La certificazione PEC di un sottodominio di un dominio già esistente permette di attivare caselle di posta certificata del tipo nome.cognome@pec.propriodominio.it (dove "pec" può essere sostituito da qualsiasi dicitura).
Il cliente dovrà verificare che siano configurati opportunamente i server DNS del propriodominio.it in modo che i messaggi inviati o ricevuti dalle caselle PEC definite nel sottodominio certificato vengano correttamente indirizzati verso i server di Posta Certificata di InfoCert.

I casi possibili sono due:

(1) il dominio di terzo livello pec.propriodominio.it non esiste;
(2) il dominio di terzo livello pec.propriodominio.it esiste;

Nel caso (1) il provider/maintainer deve inserire nel dominio propriodominio.it i 2 record:
pec IN MX 10 mx.cert.legalmail.it
pec IN TXT "v=spf1 include:_spf-legalmail.infocert.it -all"

Nel caso (2) il provider/maintainer deve inserire nel dominio pec.propriodominio.it il record:
@ IN MX 10 mx.cert.legalmail.it
@ IN MX TXT "v=spf1 include:_spf-legalmail.infocert.it -all"

Attenzione ad utilizzare le giuste virgolette "" per record di tipo TXT, esempio:
Virgoletta doppia sinistra: Alt + 2 (") e doppia destra: Alt + Shift + 2 (")

In entrambi i casi è necessario verificare che, una volta inserito i record MX e TXT sul DNS server Master, questo venga propagato anche a tutti i DNS server "slave" che hanno in gestione la "zona".

Per verificare che il DNS del dominio di posta certificata personalizzato sia correttamente configurato, è possibile accedere all'interfaccia command line della propria stazione di lavoro e digitare il comando:

Per il record MX:

nslookup -type=mx pec.propriodominio.it

La risposta deve riportare il seguente contenuto:
pec.propriodominio.it MX preference = 10, mail exchanger =mx.cert.legalmail.it

Per il record TXT:

nslookup -type=txt pec.propriodominio.it

La risposta deve riportare il seguente contenuto:
pec.propriodominio.it TXT value "v=spf1 include:_spf-legalmail.infocert.it -all"

La verifica può essere fatta, in alternativa, con qualsiasi altro strumento, grafico o no, che consenta di interrogare direttamente un DNS pubblico e di ottenere le informazioni sui record di posta di un dominio (record MX) e sul record informativo del dominio (record TXT).

Ad avvenuto completamento di tali attività da parte del provider/mantainer, sarà possibile **inserire e richiedere il sottodominio certificato dalla consolle di Autogestione Legalmail**.
InfoCert provvederà a configurare il dominio nei sistemi InfoCert e pubblicare il dominio nell'Indice del AGID (come previsto dalla Normativa).

Usualmente entro 5 giorni dalla data di richiesta, il sottodominio certificato è attivo e funzionante.

Nel caso di errata configurazione del dominio:
- le caselle continueranno ad inviare e ricevere correttamente i messaggi da caselle PEC gestite da InfoCert
- verranno considerate non certificate dagli altri gestori PEC
- non potranno comunque ricevere o inviare da caselle di altri gestori PEC e di gestori di posta ordinaria.

NOTE TECNICHE:

Sender Policy Framework (SPF) è un semplice sistema di validazione delle email progettato per individuare tentativi di email spoofing, fornendo un meccanismo tale da consentire a coloro che ricevono una mail di verificare che la mail in arrivo da un determinato dominio provenga da un host autorizzato dagli amministratori di dominio.[1] La lista degli host autorizzati ad inviare email per un determinato dominio è pubblicata nei record del Domain Name System (DNS) per quel dominio, sotto forma di record TXT appositamente formattato.

Se un dominio pubblica un record SPF, è meno probabile che spammers e phishers riescano a falsificare le email fingendo che provengano da quel dominio, questo perché le email falsificate sono catturare dai filtri anti spam con più probabilità. Perciò un dominio protetto da SPF è meno attrattivo per spammers e phishers. Dato che un dominio protetto da SPF è meno attrattivo come “spoofed address” (falso indirizzo), è meno probabile che venga inserito in una blacklist dai filtri anti spam e perciò, in ultima analisi, la email legittime provenienti dal dominio in questione hanno anche una trust maggiore.

ATTENZIONE: Infocert non si assume la responsabilità di garantire la correttezza dei dati inseriti, pertanto tutto ciò che riguarda la gestione dei Record TXT, dei dati SPF e la loro abilitazione/certificazione è interamente a carico del cliente e non verrà data assistenza a riguardo.