DNS SEC

Il DNSSEC definisce nuovi tipi di **record** e nuove modalità di interazione client/server; questo sistema si ottiene tramite l'uso di segnature digitali prodotte con algoritmi crittografici asimmetrici; le segnature digitali sono prodotte utilizzando la **chiave privata** dell'origine.

Una singola chiave privata viene utilizzata per segnare tutte le informazioni relative ad una zona (record: A, MX, NS, PTR….); lo schema DNSSEC prevede anche la possibilità di autenticare i messaggi scambiati per ogni singola risoluzione.

Per la verifica delle informazione il client DNS deve disporre della **chiave pubblica** corrispondente alla chiave privata utilizzata per il processo di segnatura; la chiave pubblica può essere veicolata all'interno del protocollo DNSSEC e può essere oggetto di certificazione.

Record	Descrizione
KEY	Definisce l'associazione tra un FQDN ed la sua chiave pubblica
CERT	Definisce l'associazione tra un FQDN ed il certificato della chiave pubblica
SIG	Mantenimento segnatura di qualsiasi record
NXT	Permette di stabilire la **non** esistenza di una informazione

Messaggi DNSSEC: