Term	Definition	Explanation
DNSSEC	Domain Name System Security Extensions	A suite of extensions to DNS that adds a layer of security to prevent attacks like cache poisoning and spoofing.
DNSKEY Record	A record that holds the public keys used to verify DNSSEC signatures.	DNSKEY records contain the public key needed to validate signatures for the zone.
Zone Signing Key (ZSK)	A key used to sign all DNS records within a DNS zone.	The ZSK is responsible for signing zone data. It is shorter and changed more frequently than the KSK.
Key Signing Key (KSK)	A key used to sign the DNSKEY records in the zone.	The KSK signs the DNSKEY records and its public key is submitted to the parent zone as part of the DNSSEC chain of trust.
RRSIG Record	Resource Record Signature - contains the digital signature for DNS records.	RRSIG records hold the cryptographic signatures for each DNS record, proving their authenticity.
NSEC Record	Next Secure Record - shows the next valid DNS name and proves non-existence of records.	NSEC records prevent spoofing by showing what records do and do not exist in a zone.
NSEC3 Record	A hashed version of NSEC, used to prevent zone enumeration.	NSEC3 is more secure than NSEC because it prevents attackers from easily enumerating all DNS records in a zone.
DS Record	Delegation Signer Record - a pointer from a parent zone to a child's DNSKEY.	DS records are placed in the parent zone to establish a chain of trust between the parent and child zones.
CDNSKEY Record	Child DNSKEY Record - a child zone's DNSKEY record meant for automatic DS record creation.	A DNSKEY that is published in the child zone and used by the parent zone to generate a DS record.
DO Flag	DNSSEC OK Flag - indicates that the client supports DNSSEC and requests DNSSEC records.	When set, it tells the DNS server to provide DNSSEC records (e.g., RRSIG) in the response.
AD Flag	Authenticated Data Flag - indicates that DNSSEC validation was successful.	Set in the response by a resolver to indicate that the DNSSEC data was validated correctly.
AA Flag	Authoritative Answer Flag - indicates that the response comes from an authoritative DNS server.	Used to show that the DNS server answering the query is authoritative for the domain.
EDNS (Extension Mechanisms for DNS)	An extension to DNS that allows larger packet sizes and supports new features like DNSSEC.	EDNS adds capabilities like larger UDP message sizes (over 512 bytes) and optional extensions for future features.
DNSSEC Validation	The process of checking DNSSEC signatures to ensure that DNS records are authentic and untampered.	Validation is done by DNS resolvers to verify the integrity of the DNS records using DNSKEY, RRSIG, and DS records.
KSK Rollover	The process of replacing the Key Signing Key with a new key while maintaining DNSSEC functionality.	KSK rollovers happen less frequently than ZSK rollovers but are critical for long-term DNSSEC management.
ZSK Rollover	The process of replacing the Zone Signing Key with a new key.	ZSK rollovers happen more frequently to reduce the risk of key compromise.
Trust Anchor	A DNSKEY record that is configured in a DNS resolver to establish a trust chain for DNSSEC.	The Trust Anchor is the root or top-level key that DNSSEC resolvers use to begin validating a DNSSEC chain of trust.
Chain of Trust	The hierarchical relationship in DNSSEC between DNS zones and their parent zones, verified by DS records.	DNSSEC works by creating a chain of trust from the root zone down to individual domain zones using DS and DNSKEY records.
Unsigned Zone	A DNS zone that does not use DNSSEC for authentication.	Zones without DNSSEC do not have cryptographic signatures and are vulnerable to spoofing and other attacks.
Signed Zone	A DNS zone that has been signed with DNSSEC keys.	A zone that uses DNSSEC to provide cryptographic authentication of its DNS records.
Rollover	The process of replacing cryptographic keys in DNSSEC without interrupting the DNS service.	Key rollovers are done periodically to ensure the security of the zone's DNSSEC keys.
Bad Signature	Indicates that the DNSSEC signature on a record could not be verified or is invalid.	If a DNSSEC signature fails, the client may reject the DNS response to prevent tampered data from being used.

Term	Definition	Explanation
DNS Cookie	A lightweight security mechanism in EDNS to prevent DNS spoofing and other attacks.	DNS Cookies are part of the EDNS extensions and are used to secure DNS transactions between clients and servers.
Fallback to TCP	DNS resolvers switching from UDP to TCP when DNSSEC response size exceeds the UDP limit.	DNSSEC responses can be large, and if they exceed the UDP packet size, the client retries using TCP for the full response.