(DNS Key Generator) is a tool to generate and maintain keys for DNS Security within the DNS (Domain Name System). can generate public and private keys to authenticate zone data, and shared secret keys to be used for Request/Transaction signatures. Dnskeygen will generate a key. must be one of [512, 576, 640, 704, 768, 832, 896, 960, 1024]. Dnskeygen will generate an key. must be between 128 and 504. Dnskeygen will generate an key. must be between 512 and 4096. Use a large exponent for key generation. These flags define the type of key being generated: Zone (DNS validation) key, Host (host or service) key or User (e.g. email) key, respectively. Each key is only allowed to be one of these. Indicates that the key be used for authentication. Indicates that the key be used for encryption. Sets the key's protocol field to ; the default is (DNSSEC) if or is specified and (EMAIL) otherwise. Other accepted values are (TLS), (IPSEC), and (ANY). Sets the key's strength field to the default is Sets the key's name to stores each key in two files: and The file contains the private key in a portable format. The file contains the public key in the DNS zone file format: No environmental variables are used. on secure DNS and the Internet Draft. Olafur Gudmundsson (ogud@tis.com). The underlying cryptographic math is done by the DNSSAFE and/or Foundation Toolkit libraries. None are known at this time