The TSIG routines are used to implement transaction/request security of DNS messages. and are the basic routines. and are used to sign/verify TCP messages that may be split into multiple packets, such as zone transfers, and initialize the state structure necessary for TCP operations. locates the TSIG record in a message, if one is present. the incoming DNS message, which will be modified the length of the DNS message, on input and output the size of the buffer containing the DNS message on input the value to be placed in the TSIG error field the (DST_KEY *) to sign the data for a response, the signature contained in the query the length of the query signature a buffer to be filled with the generated signature the length of the signature buffer on input, the signature length on output the incoming DNS message, which will be modified the length of the DNS message, on input and output the size of the buffer containing the DNS message on input the value to be placed in the TSIG error field the state of the operation non-zero value signifies that this is the last packet the (DST_KEY *) to sign the data for a response, the signature contained in the query the length of the query signature the state of the operation, which this initializes the incoming DNS message, which will be modified the length of the DNS message, on input and output the (DST_KEY *) to sign the data for a response, the signature contained in the query the length of the query signature a buffer to be filled with the signature contained the length of the signature buffer on input, the signature length on output non-zero value means that the TSIG is left intact the incoming DNS message, which will be modified the length of the DNS message, on input and output the state of the operation non-zero value signifies that a TSIG record must be present at this step the (DST_KEY *) to verify the data for a response, the signature contained in the query the length of the query signature the state of the operation, which this initializes the incoming DNS message the length of the DNS message returns a pointer to the TSIG record if one is found, and NULL otherwise. All other routines return 0 on success, modifying arguments when necessary. and return the following errors: bad input data The key was invalid, or the signing failed the message buffer is too small. and return the following errors: bad input data The message is malformed The message does not contain a TSIG record The TSIG original ID field does not match the message ID Verification failed due to an invalid key Verification failed due to an invalid signature Verification failed due to an invalid timestamp Verification succeeded but the message had an error of BADKEY Verification succeeded but the message had an error of BADSIG Verification succeeded but the message had an error of BADTIME Brian Wellington, TISLabs at Network Associates