Safely providing authenticity of authenticated data, content of the plaintext and information leakage [0] protection for the plaintext, for AES-GCM, up to 2^48 128-bit blocks (2^64 bytes) as the total data amount of all of the (padded) records in a session can be encrypted with a single key while having a negligible risk of a collision among the 128-bit blocks of the ciphertext below 2^(-32), assuming that the (padded) record size is either 128 bits, a multiple of 128 bits or close to that. If the record size is 2^x bytes, then the data limit with GCM for each key is 2^(64-x) records.

When the padded record size is less than 128 bits (16 bytes), if *l* is the length of the padded record in bits, then the data limit with GCM for each key is reduced to around 2^64 x *l* /128 bytes or 2^(64-x) x l/128 records.

[[AEAD-LIMITS](https://tools.ietf.org/html/draft-ietf-tls-tls13-18#ref-AEAD-LIMITS)] provides the analysis for the data limit recommendation for GCM above.

For ChaCha20/Poly1305, the record sequence number would wrap before the safety limit is reached.

Since the block size of AES is 128 bits, there will be collisions among different sets of ciphertext from multiple sessions using GCM (or any other modes of AES) when the total amount of the ciphertext of all considered sessions is more than 2^64 128-bit blocks. This fact does not seem to create a practical security weakness of using AES GCM.

[0]: Information leakage in the context of TLS is a chosen-plaintext distinguishing attack where the attacker provides 2 128-bit plaintext blocks to a GCM encryption engine, after seeing one encrypted block for one of the 2 plaintext blocks, the attacker knows which plaintext block was encrypted. Or, it means that there is a collision among 128-bit blocks of the ciphertext.