# Exchange Migrations over Encrypted Networks

Priasoft

## Encrypted Networks?

Migration over an Encrypted Network?

From time to time, a migration project will occur where the data to be migrated must travel across a network path that is encrypted. This is most commonly due to a VPN solution being employed to provide connectivity between 2 physical sites. However, a VPN is not the only reason for data to be encrypted and it does happen even on private lines of communication.

The question should always be asked, whether data will be encrypted at the network layer (typically Layer 3). Network encryption can happen in both LAN and WAN scenarios, and the question should not be discarded just because data is traveling across LAN segments. However, it is much more common to find network encryption on WAN segments.

Most Layer 3 encryption (and above) employ some type of IPSEC involving encryption key generation and public/private keys. The typical configuration for such is to have the encryption keys expire after some amount of time to reduce the chance of an outside attacker having enough time to brute force the key discovery and potentially decrypt the data in transit. Such is the reason, but not necessarily a requirement all the time.

## The Issue

When migration Exchange data over an encrypted network segment, whether it be one small segment on a LAN, or WAN, or multiple distinct segments each with its own encryption, the issue remains about **key lifetime**. Based on many years of prior experience, MAPI (the underlying protocol used to access Microsoft Exchange Data) has been shown to be very sensitive to network interruptions and latency. This sensitivity manifests in different ways and with different symptoms. Sometimes the issue is easily recoverable and other times can cause the entire MAPI session to unwind and become unusable. If you have ever seen the “Please wait while Outlook attempt to reconnect to the server” message, such is a symptom that can occur due to a network drop or very high latency. During a migration effort, the symptoms can be failed messages, failing mailboxes, or slow throughput for a short time until the network stabilizes.

Specific to encryption, when data is encrypted, it does so with dynamically generated keys. These keys are negotiated between the endpoints and are used secure the data across that network segment. When the **key lifetime** (a configured duration after which the keys are expired) is reached, or exceeded, any encrypted packets are un-readable and have to be returned to the sender for resubmission with the new keys. This re-submit plus the time to negotiate the new keys can be enough time to cause MAPI to have an issue. This issue is difficult to track since duration, packet size, and session details have much to do with whether the issue is

exposed. The larger the mailbox, the more likely that the session will cross over the key lifetime. Smaller mailboxes that complete in minutes often do not see the issue, UNLESS it just so happens that the start of the mailbox is near the end of the key lifetime.

An argument could likely be made to try not to start a mailbox too late in the key lifetime cycle, however access to such information is typically not tracked, and the encrypted segment may not be local to the network adapter and as such no inspection of encryption details could be made.

# Best Practice

Priasoft's recommendation is to implement a longer key lifetime for any encrypted network segments across which migration must occur, unless encryption can be bypassed or removed/eliminated. This extended key lifetime only needs to exist for the entire migration window, which might only be a few hours to a couple of days. Many encryption technologies limit the lifetime to a maximum of 24 hours, which is sufficient. The goal is to create a long enough lifetime such that a very large mailbox, by item count, is able to complete before the likelihood of the encryption keys being changed.

If, using dry-run features, it can be determined that some large mailboxes take 15 hours to complete, a 24 hour key life time is sufficient, provided that those large mailboxes start early. The argument quickly made here is that it may be impossible to determine when the encryption keys last changed and such might occur 1 hour into the 15 hour duration of the mailbox. While true, such is not so critical to track. Priasoft's migration technology will automatically restart any failed mailbox 2 times before actually reporting it as a failure and taking it out of the dispatch routine. In this fashion, even a severe failure due to encryption key changes (or any other network issue, or even a power outage somewhere) are, in most cases, automatically recovered by the restart. The migrator will quickly move past previously copied items so that it can pick up where it last left off. This technology is available both in a dry-run and a production run scenario.

The question may be asked then "why adjust the encryption keys at all?" The answer is really about controlling variables and providing a smooth finish. Just because the process has built-in restarts, does not mean that the issue is eliminated. When a mailbox is failed the first or second time, it is dropped to the bottom of the work queue. Such mailboxes may not restart for many minutes or hours (depending up the size of the batch) and when they finally do start, they could again be near the end of the key lifetime.

(Graphic exists on next page)

The following provides a visual representation of the issue: