Для шифрування данних використовується алгоритм AES-GCM-256. Був вибраний GCM режим так як, крім власне шифрування даних, він забезпечує цілісність даних. Рекомендовано використовувати AES для симетричного шифрування, так як він є більш ефективним та дозволяє використовувати ключі різних довжин (128, 192, 256 bit). Використовувалась імплементація AesGcm з System.Security.Cryptography.

Для збільшення безпеки також можна додати шифрування даних на рівні бази (TDE) та шифрування жорсткого диску на рівні файлової системи.

Поле з зашифрованими даними має такий склад:

4 байта: довжина nonce

12 байт: довжина nonce

16 байт: довжина тега – використовується для перевірки цілісності

Далі: зашифрований текст

Для зберігання ключа використовується Azure Vault.

Збережена інформація може бути втрачена якщо зловмисником буде отриманий доступ до бази та Azure Vault. Одним із способів ускладнити це є використання envelope encryption, тобто зашифрувати ключі додатковим ключем і зберігати його в іншому місці, також можна додати ротацію ключа (наприклад робити це через деякий час, через деяку кількість зашифрованих цим ключем даних, якщо ключ був скомпрометований).