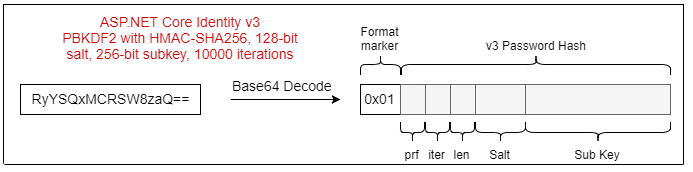
Як стандартний identity manager framework використовувався ASP NET Core Identity V3.

В ньому стандартним форматом хешування є:

PBKDF2 with HMAC-SHA256, 128-bit salt, 256-bit subkey, 10000 iterations



Iter – к-сть ітерацій

Prf – псевдо рандомна функція, яка використовується для ключа

Len – довжина солі

Salt – сіль

Sub Key – хеш

PBKDF2 – включений в один з трьох рекомендованих алгоритмів в OWASP, використовуються, якщо є спеціальні рекомендації для відповідності NIST і FIPS-140.

Серед інших алгоритмів, вказаних в OWASP: Argon2id та Bcrypt. Враховуючи рекомендації, було вирішено змінити алгоритм на Bcrypt, так як Argon2id вимагає додаткових знань для налаштування.

Як і описано в рекомендаціях, значення для хешування має бути лімітованим в довжині: від 64 до 128 символів (64 для Bcrypt через обмеження алгоритму) через обчислювальну складність алгоритмів і можливу через це DoS атаку. Тому в класі BcryptPasswordHasher.cs пароль перед цим хешується SHA256, що на виході дає рядок довжиною 64 символа.

Джерела:

<https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html#pbkdf2>

<https://andrewlock.net/migrating-passwords-in-asp-net-core-identity-with-a-custom-passwordhasher/>