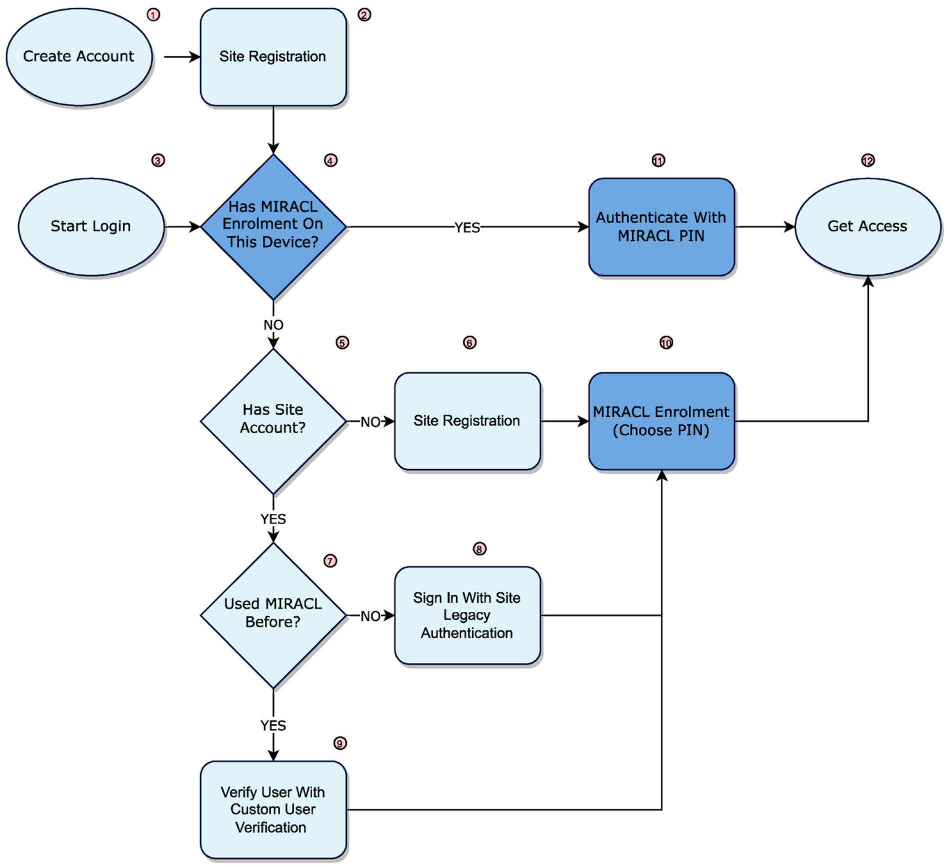
# MIRACL Retrofitted Using Custom User Verification



1
Create Account
2
Site Registration
3
Start Login
4
Has MIRACL Enrolment On This Device?
YES
11
Authenticate With MIRACL PIN
12
Get Access
NO
5
Has Site Account?
NO
6
Site Registration
10
MIRACL Enrolment (Choose PIN)
YES
7
Used MIRACL Before?
NO
8
Sign In With Site Legacy Authentication
YES
9
Verify User With Custom User Verification

**Steps are either;**

1. The User creates an account on the site, or an account is created for them
2. The process of creating an account on the site is completed

**OR**

3. The User selects the client site Login link or button
4. Does this particular user have an identity registered (enrolled) on this particular device, where device could mean a specific browser on that device. A user can also choose to reset their PIN
5. Does the user have site access, i.e. access to that service that is sitting behind the MIRACL authentication service
6. Request that the user registers for site access, this is the same process as number 2
7. Determine whether the user has previously enrolled with MIRACL, i.e. they have a stored identity
8. If the user has not previously enrolled with MIRACL, allow them to authenticate using legacy credentials
9. MIRACL's client defines the processes and flows suitable to verify the user's identity, after which control is passed to number 10
10. Enrolment means using the mPINPAD to ask the user to type their PIN, and then ask them to type it again to confirm their choice
11. Authentication requires that the user is asked to type their PIN on the mPINPAD
12. Process End, user has access to the site/resource