ADR

**Title:**

Password Based Authentication.

**Context + Problem Statement:**

We need a reliable authentication system for our application registration that follows GDPR guidelines. The password should restrict unauthorized individuals from accessing certain resources and functionality (Enzoic, 2019).

**Decision Driver:**

* To ensure users can securely register and sign into the application.
* Ensure it aligns with data protection regulations (GDPR).

**Option:**

OAuth 2.0 open id connect. Magic links. Multi-factor authentication. Email verification authentication.

**Considered Options:**

* OAuth 2.0 open id connect: uses third party sites to register rather than creating new ones/repeating (Microsoft, n.d.).
* Email verification authentication: this is a security measure that verifies the person and if they are genuine (Beyond Encryption, n.d.).
* Multi-factor authentication: is a login process that requires the user to enter more information than just a password (AWS, 2023).

**Decision Outcomes:**

Chosen option: email verification authentication.

This is because it verifies the email address which prevents fake or incorrect email submissions, it can reduce frauds and has a limited time before expiring, which would reduce the risk of misuse. Verifying emails also aligns with data protection regulations by ensuring consent comes from a real user (Intersoft Consulting, 2018).

There is a possibility of joining different options, such as the email verification with OAuth 2.0, which would make it even more secure and safe, however due to the time constraints and limited knowledge focusing on the email verification is most realistic.

**Consequences:**

Good, because it is reliable and follows GDPR guidelines.

Good, because it ensures the email is valid.

Good, because it’s a popular way of authentication for registration and a familiar tool for many users.

Good, because it’s a service in Firebase which will be used and will be quicker.

Bad, because there is a dependency on email access, which can cause issues if the user loses access to the email account.

Bad, because delayed emails can occur which holds the user from being able to access functionalities as a member.

Bad, because verification requires an active internet connection.

Bad, because there are more secure methods, such as multi-factor authentication.

**Confirmation:**

Before implementing the application, which has been approved.

**Pros and Cons:**

Pros:

* Follows GDPR guidelines.
* Ensures email is valid.
* Familiar with users.
* Compatible with stack.

Cons:

* Dependency on email access and internet connection.
* Other options are more secure.

# Resources

Enzoic. (2019, September 3). *GDPR Password Policy: Critical Components | Enzoic*.

Enzoic. <https://www.enzoic.com/blog/gdpr-password-policy-critical-components/>

Beyond Encryption. (n.d.). *What Is Email Authentication?* Www.beyondencryption.com.

<https://www.beyondencryption.com/blog/what-is-email-authentication>

Microsoft. (n.d.). *What Is OpenID Connect (OIDC)? | Microsoft Security*.

Www.microsoft.com.

<https://www.microsoft.com/en-us/security/business/security-101/what-is-openid-connect-oidc>

AWS. (2023). *What is Multi-Factor Authentication (MFA)? - Cloud Security Beginner’s*

*Guide - AWS*. Amazon Web Services, Inc. <https://aws.amazon.com/what-is/mfa/>

Intersoft Consulting. (2018). *General Data Protection Regulation (GDPR)*. General Data

Protection Regulation (GDPR). <https://gdpr-info.eu/issues/consent/>