**{Authentication}**

**Context and Problem Statement**

{The system needs to authenticate users who log in to allow them to borrow items securely. Authentication is essential to ensure accountability, protect user data, and prevent unauthorised access (Jones, Bradley, & Sakimura, 2015).}

**Decision Drivers**

* {Security will prevent unauthorised access and ensure user data is protected (Ethelbert et al., 2017).}
* {Compliance will meet the industry security standards and regulations(e.g., GDPR) (Singh et al., 2023).}
* {Easier to manage user roles and permissions (Nardone & Scarioni, 2023).}

**Considered Options**

* {Authentication: Username and password-based authentication}
* {No Authentication: Open access, allowing borrowing without verification}
* {JSON Web Tokens: Uses a token with claims to authenticate the user (Jones, Bradley, & Sakimura, 2015).}

**Decision Outcome**

Chosen option: "{JSON Web Tokens}", because this ensures security, accountability, and a seamless borrowing process while meeting regulatory requirements (Ethelbert et al., 2017). Open access is not viable for a secure system.

**Consequences**

* Good, because {Provides accountability and prevents unauthorised use (Ethelbert et al., 2017).}
* Good, because {Ensures user data is protected (Singh et al., 2023.}
* Good, because {Allows rate limiting (Shingala, 2019).}
* Neutral, because {Authentication can add complexity.}
* Bad, because {Requires users to create and remember credentials (Nardone & Scarioni, 2023).}

**Confirmation**

The implementation will be validated through:

1. Design Review: Ensuring the authentication process meets system requirements.
2. Code Testing: Using unit tests to verify functionality.
3. Security Testing: Conduct tests to ensure the system can handle attacks (Shingala, 2019).

**Pros and Cons of the Options**

**{Authentication}**

* Good, because {Provides reliability and security (Singh et al., 2023).}
* Good, because {Supports future enhancements (e.g., 2FA) (Nardone & Scarioni, 2023).}
* Neutral, because {Can add minor complexity for end-users.}
* Bad, because {May require additional development time and cost.}

**{No Authentication}**

* Good, because {Simpler to implement, reducing initial development time.}
* Bad, because {No accountability for borrowed items (Ethelbert et al., 2017).}
* Bad, because {Expose the system to unauthorised access (Jones, Bradley, & Sakimura, 2015).}

**{JSON Web Token}**

* Good, because {More secure than the other two options (Jones, Bradley, & Sakimura, 2015).}]
* Good, because {You can rate limit the access (Shingala, 2019).}
* Neutral, because {It is more difficult to implement than the other two options.}
* Bad, because {Without refresh tokens, it’s hard to revoke access (Singh et al., 2023).}

**More Information**

**References**

* Ethelbert, O., Moghaddam, F. F., Wieder, P., & Yahyapour, R. (2017). A JSON token-based authentication and access management schema for cloud SaaS applications. *arXiv preprint arXiv:1710.08281*.<https://arxiv.org/abs/1710.08281>
* Jones, M. B., Bradley, J., & Sakimura, N. (2015). *JSON Web Token (JWT)* (RFC 7519). Internet Engineering Task Force. <https://doi.org/10.17487/RFC7519>
* Nardone, M., & Scarioni, C. (2023). JSON Web Token (JWT) Authentication. In *Pro Spring Security* (pp. 239–279). Springer. <https://doi.org/10.1007/979-8-8688-0035-1_9>
* Shingala, K. (2019). JSON Web Token (JWT) based client authentication in Message Queuing Telemetry Transport (MQTT). *arXiv preprint arXiv:1903.02895*.<https://arxiv.org/abs/1903.02895>
* Singh, P., Choudhary, G., Shandilya, S. K., & Sihag, V. (2023). Enhancing the security of JSON Web Token using Signal Protocol and Ratchet System. In *Proceedings of Emerging Trends and Technologies on Intelligent Systems* (pp. 387–400). Springer Nature. <https://doi.org/10.1007/978-981-19-4182-5_31>