 

Digitalization of Admissibility

Security Architecture

OneID

Document Author: Ashish Sharma

Date Created: 16 Mar 2024

**1. Project Overview**

* **Description of the Project:** Overview of the Digitalization of Admissibility project, focusing on the integration of OneID.
* **Scope of the Assessment:** Boundaries of the security assessment, including systems, data, and processes evaluated.

**2. Security Architecture Review**

* **System Architecture:** Detailed description of the project's architecture, including all components and their interactions.
* **Data Flow Diagrams:** Visual representations of how data moves through the system, identifying trust boundaries and data processing points.

**3. Threat and Risk Assessment**

* **Threat Modeling:** Identification of potential threats using models like STRIDE or PASTA, considering various actors, methods, and targets.
* **Risk Analysis:** Evaluation of identified threats to determine potential impact and likelihood, resulting in a risk level for each threat.

**4. Vulnerability Assessment**

* **Methodology:** Description of the methods used to identify vulnerabilities, such as automated scanning, manual testing, and code review.
* **Findings and Vulnerabilities:** Detailed list of identified vulnerabilities, including their severity, impact, and exploitability.

**5. Security Controls Review**

* **Current Security Measures:** Overview of the existing security controls in place, such as encryption, authentication, and access controls.
* **Effectiveness of Controls:** Evaluation of how effectively current security measures protect against identified risks and threats.

**6. Compliance and Standards**

* **Regulatory Compliance:** Analysis of the project's adherence to applicable legal and regulatory requirements, such as GDPR, CCPA, or aviation-specific standards.
* **Security Standards:** Assessment of compliance with industry standards and best practices, like ISO 27001, NIST, or IATA guidelines.

**7. Recommendations**

* **Remediation Actions:** Specific recommendations to address identified vulnerabilities and enhance the security posture.
* **Strategic Improvements:** Long-term suggestions for improving the security framework and processes of the project.

**8. Conclusion**

* Summary of the security assessment, emphasizing critical findings and prioritizing recommended actions.

**9. Appendices**

* **Appendix A:** Detailed Findings and Technical Details
* **Appendix B:** Risk Assessment Matrix
* **Appendix C:** Glossary of Terms

**Glossary:**

* **OneID:** A globally recognized identity management standard in the airline industry.
* **STRIDE:** A threat model acronym for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege.
* ...

This Security Assessment Report serves as a crucial document, highlighting the security status of the Digitalization of Admissibility project and providing a roadmap for mitigating potential security risks. The report should be comprehensive, clear, and actionable, guiding stakeholders through the necessary steps to secure the project effectively.

**Appendix 1 – Risk Rating Criteria**

|  |  |  |
| --- | --- | --- |
|  | Very high | * It will have major effect on security posture and brand value of the organization * Affects majority of all critical services or entire operations of EAG * All or most of sensitive information stored or processed can be compromised * Exploitation significantly increases the probability of additional vulnerabilities being exploited * Major non-compliance with mandatory requirements of organization’s policies and legal, regulatory & statutory regulations and standards. |
|  | High | * It will have substantial effect on security posture and brand value of the organization * Affects considerable amount of critical services and operations of EAG * Considerable % of sensitive information stored or processed is compromised * Exploitation increases the probability of additional vulnerabilities being exploited * Considerable non-compliance with some of the mandatory requirements of organization’s policies and legal, regulatory & statutory regulations and standards. |
|  | Medium | * It will have limited effect on security posture and brand value of the organization * Affects limited amount of services and operations of EAG * Limited % of sensitive information stored or processed is compromised * Exploitation could increase the probability of additional vulnerabilities being exploited * Partial non-compliance with some of the mandatory requirements of organization’s policies and legal, regulatory & statutory regulations and standards. |
|  | Low | * It will have a minor effect on security posture and/or brand value of the organization * Affects insignificant amount of critical services and operations of EAG * Insignificant % of sensitive information stored or processed is compromised * Effect of vulnerability is tightly contained, does not increase the probability of additional vulnerabilities being exploited. * Minor non-compliance with respect to some of the recommended controls defined in the organization’s policies and other legal, regulatory and statutory regulations and standards. |
|  | Very Low | * It will have negligible or no effect on security posture and brand value of the organization * Has negligible or no effect on critical services and operations of EAG / * Negligible amount of sensitive information stored or processed is compromised |

**Note:** Highlight the areas that correspond to the risk ratings assigned to the observed security issues or findings.