

THESIS

**Designing Reference Architecture for KYC Data Protection to Minimize Data
Breach Risk in Organization XYZ**

By

Vincent Zavellino

22351023

MASTER'S DEGREE

in

MASTER OF INFORMATION TECHNOLOGY

FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY



SWISS GERMAN UNIVERSITY

The Prominence Tower

Jalan Jalur Sutera Barat No. 15, Alam Sutera

Tangerang, Banten 15143 - Indonesia

Revision After Thesis Defense on 5 February 2025

STATEMENT BY THE AUTHOR

I hereby declare that this submission is my own work and to the best of my knowledge, it contains no material previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any other degree or diploma at any educational institution, except where due acknowledgement is made in the thesis.

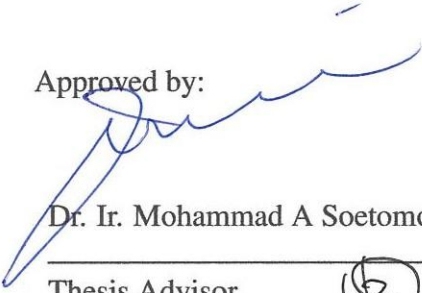

Vincent Zavellino

Student

18 Feb 2025

Date

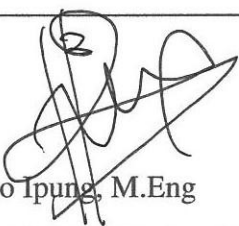
Approved by:


Dr. Ir. Mohammad A Soetomo, DSc

Thesis Advisor

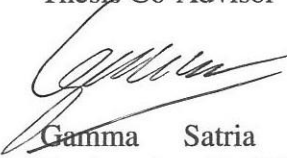
17 Feb 25

Date


Dr. Ir. Heru Purnomo Ipung, M.Eng

Thesis Co-Advisor

Date


Gamma Satria Kurniawan (VP of
Engineering, PT. XYZ)

Thesis Co-Advisor

18 Feb 2025

Date

Dr. Maulahikmah Galinium, S.Kom, M.Sc

Dean of Faculty of Engineering and
Information Technology

Date

ABSTRACT

Designing Reference Architecture for KYC Data Protection to Minimize Data Breach Risk in Organization XYZ

By

Vincent Zavellino

Dr. Ir. Mohammad A Soetomo, DSc, Advisor

Dr. Ir. Heru Purnomo Ipung, M.Eng, Co-Advisor

Gamma Satria Kurniawan (VP of Engineering, PT. XYZ), Co-Advisor

SWISS GERMAN UNIVERSITY

This thesis aims to design a reference architecture for data protection to reduce data breach risk in organization XYZ, a software development company, with a specialization in KYC (Know Your Customer) data with an expected result of a risk management reference architecture. The reference architecture takes translated controls from PCI DSS, POJK and UU PDP that is specifically chosen for organization XYZ's needs, this aligns the business goals and risk appetite in order to comply with Undang-Undang No. 27 Tahun 2022 Tentang Perlindungan Data Pribadi. With this reference architecture, it is expected that XYZ's maturity level would grow as currently there are no existing measures that are specially made to cover data protection in XYZ.

Keywords: KYC, Data Protection, Data Breach, Risk Management, Reference Architecture.



DEDICATION

I dedicate this thesis to improving society and the future.



ACKNOWLEDGEMENT

I would like to express my gratitude to my advisor and co-advisor Pak Amin and Pak Ipung for their patience and guidance during the course of this thesis. To Mas Gamma for allowing and supporting me pursue a higher degree of education. To my family, friends and colleagues who have always supported me both in my career and studies.



Table of Contents

	Page
STATEMENT BY THE AUTHOR	1
ABSTRACT	2
DEDICATION	4
ACKNOWLEDGEMENT	5
TABLE OF CONTENTS	8
LIST OF FIGURES	10
LIST OF TABLES	11
1. INTRODUCTION	12
1.1 Background	12
1.2 Problem Statement	16
1.3 Research Objective	18
1.4 Research Question	19
1.5 Hypothesis	19
1.6 Research Scope and Limitation	19
1.7 Significance of Study	20
1.8 Thesis Structure	20
2. LITERATURE REVIEW	21
2.1 Organization XYZ	21
2.2 Customer Loyalty Program and Data Protection	21
2.3 KYC Data and Process in XYZ	23

2.4	KYC and Data Protection Regulations in Indonesia	25
2.5	Reference Architecture	27
2.6	NIST Privacy Framework	29
2.6.1	Comparative Analysis of NIST SP 800-53 Against Similar Frameworks	30
2.7	NIST Security Guidelines for Storage Infrastructure	30
2.8	PCIDSS	31
2.8.1	Mapping PCI DSS to POJK and UU PDP	32
2.9	Disaster Recovery	33
2.10	Cybersecurity Metrics	33
2.11	Methods of Data Protection	35
2.11.1	Reference Architecture	36
2.11.2	Virtual Machine Hardening	37
2.11.3	Blockchain as a Means of Data Protection	37
2.11.4	Data Encryption Methods	39
2.11.4.1	DES	39
2.11.4.2	AES	41
2.11.4.3	RSA	42
2.11.4.4	Data Masking and Envelope Encryption	43
2.11.5	Intrusion Detection Systems	44
2.11.6	IAM and RBAC	45
2.12	Previous Studies	47
3.	RESEARCH METHODOLOGY	56
3.1	Research Framework	56
3.2	Literature Review	59
3.3	Gap Analysis	59
3.4	Compliance and Technology Based Approach	62
3.5	Evaluation and Validation	62
4.	Results and Discussions	68
4.1	Data Collection: IDS	68
4.2	Data Collection: Monitoring and Anomaly Detection	70

4.2.1 Prometheus	70
4.2.2 Grafana	72
4.2.3 Elasticsearch, Logstash and Kibana (ELK)	73
4.2.4 Datadog	74
4.2.5 Monitoring and Anomaly Detection Conclusion	75
4.3 Data Collection: Hardening	76
4.3.1 CIS	77
4.3.2 STIG	78
4.3.3 Hardening Conclusion	79
4.4 Data Collection: Encryption	80
4.5 Data Collection: IAM	81
4.5.1 IAM Conclusion	83
4.6 Reference Architecture Formulation	84
4.7 Implementation Timeline	84
4.8 Evaluation and Validation	85
4.9 Recommendations	88
5. CONCLUSION	92
REFERENCES	138

List of Figures

1.1	Fishbone Diagram on Data Protection Challenges	18
2.1	HIDS VS NIDS by Wonhyung Park ([016])	46
2.2	Conventional RBAC by Min-Yu Chen ([013])	47
2.3	Access Control Methods and Attributes by Sigit Wibawa ([024])	48
2.4	Comparison of Related Works	55
3.1	Security Framework by Maikel Mardjan ([021])	57
3.2	Privacy Framework by Maikel Mardjan ([021])	58
3.3	Research Framework	58
4.1	Architecture of Prometheus Cited from Turnbull ([018])	71
4.2	Architecture of ELK Cited from Gupta ([015])	74
4.3	Resulting Data Protection Reference Architecture	90
4.4	Reference Architecture Implementation Timeline	91
1	e-KYC Process in XYZ Part 1	94
2	e-KYC Process in XYZ Part 2	95
3	e-KYC Process in XYZ Part 3	96
4	e-KYC Process in XYZ Part 4	97
5	Mitre Att&ck Framework	101
6	DES Architecture as Cited from Mahajan and Sachdeva ([013])	103
7	DES Architecture as Cited from Singh ([013])	104
8	AES Architecture as Cited from Singh ([013])	105
9	AES Architecture as Cited from Mahajan and Sachdeva ([013])	106
10	RSA Architecture as Cited from Singh ([013])	107
11	RSA Architecture as Cited from Mahajan and Sachdeva ([013])	108
12	IAM Architecture as Cited from Singh et al. ([023])	109

13	IAM Components as Cited from Devlekar and Ramteke (022)	109
14	Access Management Components as Cited from Devlekar and Ramteke	
	(022)	110
15	Thesis Evaluation with Bagus Mukmin	111
16	Thesis Evaluation with Warieh Priyono	112
17	CV Vincent Zavellino	114
18	CV Warieh Priyono	116
19	CV Bagus Part 1	118
20	CV Bagus Part 2	119
21	CV Bagus Part 3	120
22	CV Suwaji Harsono Part 1	122
23	CV Suwaji Harsono Part 2	123
24	CV Suwaji Harsono Part 3	124
25	CV Suwaji Harsono Part 4	125



List of Tables

1.1 Data Breach Incidents in Indonesia	17
2.1 Security And Privacy Control Families NIST (0206)	51
2.2 Mapping PCI DSS Requirements into POJK and UU PDP Controls . . .	52
2.3 Comparison of Reference Architectures	53
2.4 Comparison of Reference Architectures	54
3.1 Security Control Selection	65
3.2 Protection Controls and Gap Analysis	66
3.3 Mapping FGD Questions to Success Indicators	67
4.1 Comparison of Snort and Suricata	69
4.2 Comparative Analysis between Monitoring Systems	75
4.3 Comparative Analysis between CIS and STIG	79
4.4 Comparative Analysis on Encryption Methods	81
4.5 Comparative Analysis on IAM Methods	83
4.6 Evaluation of FGD Questions and Indicators to Results	86
1 POJK Article 19:1, 3-4	98
2 POJK Article 20:1-2	99
3 POJK Article 22:1-2	99
4 POJK Article 24:1-5	100