



**MINISTRY OF BUSINESS,
INNOVATION & EMPLOYMENT**
HĪKINA WHAKATUTUKI



Immigration New Zealand

3644 Biometric Capability Update (BCU) Solution Design Part A

Version: 1.5

Date: 05/08/2021



1. Document control

Version history

Date	Version	Author	Description of change
30 th October 2019	0.1	s9(2)(a)	Initial Draft
21 st January 2020	0.2		Addition of NEC logical design.
11 th March 2020	0.3		Revisions
2 nd April 2020	0.4		Revisions following team review
8 th April 2020	0.5		Revisions
17 th April 2020	0.6		Revisions following ARG
28 th April 2020	1.0		Final and approved by Architecture Review Board (ARB)
25/06/2021	1.1		- Updated the Document Reference section - Updated Identity Management Component diagram - Updated High Level Architectural View - Updated Logical View - Updated Component View with the component descriptions - Added Security Architecture Goals - Added Security Architecture Constraints - Modified Authentication section - Modified Authorisation section - Added Security Logging - Modified the Security Controls - Updated the Data Replication section - Updated Data storage section - Updated Data Migration section with migration approach - Added Deployment views - Added Decommission section and described which components are decommissioned - Added Appendix section to record Design Decisions and NEC Workflows
29/07/2021	1.2		- Updated Part A submitted for ARG review
30/07/2021	1.3		- Updated the Core ISIDM Topology diagram - Updated the Capacity & Continuity in Operational Considerations section. - Updated the Business Requirements section under Requirements Realisation section - Updated Continuity with high level DR process



03/08/2021	1.4	s9(2)(a)	- Incorporated feedback - Updated Operational considerations - Updated Security user roles table - Updated Architectural risk and assumptions table - Updated Data Migration sub sections - Added new Appendix for Code Tables - Added APIM load balancing design consideration
05/08/2021	1.5		- Updated document with ARG feedback - Updated Architectural Risks and highlighted key NFRs that the solution is to meet.

Template information

This document was produced using the Capital Portfolio Office's Project Delivery Model 'solution design part A' template, version 2.2

Approved by

The following people have approved this document.

Name	Role	Date	Signature*
ARG	Endorsement	7 th April 2020	
ARB	Approval	28 th April 2020	 FW 280420 ARB Meeting Minutes dc
ARG	Updated Endorsement	04 th August 2021	
ARB	Updated Approval	10 th August 2021	 BCU Part A - ARB Endorsement - 2021

Reviewed by

The following people have a formal quality assurance role with respect to this document.

Name	Role	Supported?	Date	Signature
s9(2)(a)	Business Architect	Yes	30 th March 2020 v0.4	
	ICT Systems Manager	Yes	30 th March 2020 v0.4	
	Solution Architect	Yes	30 th March 2020 v0.4	
	Project Manager	Yes	30 th March 2020 v0.4	
	Manager Customer Delivery	Yes	30 th March 2020 v0.4	
	Senior Business Analyst	Yes	30 th March 2020 v0.4	



Name	Role	Supported?	Date	Signature
s9(2)(a)		Yes	30 th March 2020 v0.4	
		Yes	30 th March 2020 v0.4	
			5 th June 2020 v1.0	
		Yes		
		Yes		
		Yes		
		Yes		
		Yes		

Consulted

The following people have been consulted in the production of this document (list excludes approvers and reviewers).

Name	Role	Date
s9(2)(a)		

Distributed to

The following people / groups have been sent a copy of this document (list excludes approvers, reviewers, and consulted).

Name	Role	Date
s9(2)(a)		



Contents

1. Document control	i
Version history	i
Template information	ii
Approved by	ii
Reviewed by	ii
Consulted	iii
Distributed to	iii
2. Introduction	5
Purpose	5
Project Context	5
Project Information	5
Document references	5
3. Terms and definitions	7
4. Business Problem Definition	9
Background	9
5. Solution description	11
Solution background	11
Solution Options	11
Identity Management Components	14
Solution stakeholders	16
Users of the solution	17
Act(s) and/or Regulation(s)	17
6. High level architectural view	19
Overview	19
Architectural Principles	20
Architectural goals	20
Architectural constraints	21
Assumptions	21
Design considerations	22
Architectural risks	23
7. Business view	25
Overview	25
Conceptual overview	25
Processes	26
Matching and filing identity data captured by INZ	26



Capture.....	27
Matching	28
Processing	29
Analysis/Resolution.....	30
Final Processing.....	31
s6(c)	31
Adhoc matching activities	31
Quality Control (QC) Edit	32
Legislative reporting activities.....	32
8. Requirements realisation	33
Business Requirements	33
Functional Requirements	33
Non-functional requirements	34
9. Logical Design View.....	38
Overview	38
Logical view	39
High Level Solution Capabilities.....	39
User interaction and System Integration:	44
External Concurrency	48
Overview.....	48
Pre-requisites.....	48
Description	49
Component View.....	51
Existing components.....	51
New components	55
Opportunities for reuse.....	57
Platform Decommissioning	57
10. Security architecture.....	60
Overview	60
Security architecture goals.....	60
Security architecture constraints	60
Assumptions.....	61
Identity and Access Management.....	61
Security User Roles	61
Authentication.....	62
NEC User Interfaces Applications.....	62
API Integrations within BCU.....	62
MSMQ Integration between AMS & NEC IDme	63



Authorisation	63
Logging and Auditing	63
Security Events Logging	64
Security Controls	65
11. Data view	70
Overview	70
Conceptual data model	70
Logical data model	71
Logical Data Model – NEC.....	71
Logical Data Model - AMS	72
Data Classification	73
Data replication (master-slave relationships)	73
Data storage, archiving and retention	73
Data migration.....	75
Overview.....	75
Biographic Data	75
Biometric Data.....	75
Migration Approach	78
Introduction	78
Migration Approach diagram.....	79
Migration Approach Data Diagram.....	80
Records management	80
12. Operating considerations	81
Availability and reliability	81
Capacity	81
Continuity.....	82
Deployment / implementation	83
Performance.....	84
Scalability.....	84
System management, monitoring, and administration	84
13. Deployment view.....	86
Core ISIDM Topology.....	86
High Level Deployment View	87
14. Appendix.....	88
Appendix 1: NEC Workflows.....	88
Automated Parallel/Verify Workflow	88
AMS Maintenance Workflow	88
s6(c)	88



Appendix 2: Code Tables	89
Image Type Code Table	89
Reason for Fingerprint Code Table	89
Fingerprint Case Type Code Table	90
Fingerprint Usage Qualifier Code Table	90

Figures and tables

Figure 1: Identity Management Components	14
Figure 2: High Level Architecture View	19
Figure 3: Basic business goal of the Matching and filing identity data captured by INZ	26
Figure 4: High-level Matching and filing process	27
Figure 5: Sequence of Identity Flow after NEC IDme based capture	27
Figure 6: Sequence of Identity Biometric/Biographic Matching in NEC IDme and IQ Office	28
Figure 7: Sequence of Identity processing in NEC IDme and AMS	29
Figure 8: Sequence of Identity Analysis/Resolution in NEC IDme	30
Figure 9: Sequence of Identity final processing in NEC IDme	31
Figure 10: BCU Solution Overview	38
Figure 11: Identity Management Logical View	39
Figure 12: External Concurrency Solution	48
Figure 13: Biometric Capability Upgrade Component View	51
Figure 14: Biometric Capability Upgrade Component View	63
Figure 15: Conceptual BCU Data View	70
Figure 16: NEC Identity Data Model	71
Figure 17: AMS Identity Data Model	72
Figure 18: Future State Data Flow	74
Figure 19: Migration Approach Diagram	79
Figure 20: Migration Approach Data Diagram	80
Figure 21: Core ISIDM Topology	87
Figure 22: High Level Deployment View	87

pages 9-85 and 96-448 of this Appendix are withheld in full under section 6(c) of the Official Information Act 1982



3644 Biometrics Capability Update Infrastructure Solution Design Part B

Version: 2.0

Version Date: 12th November 2025

Issue Date: 12th November 2025



1. Document control

This section is for recording the document versions, the review cycles and approvals sought and sign-off gained from a minimum of the Business (Project sponsor and / executive, Business Owner), Subject matter expert, and Primary architect. Ensure that the version number of this document is updated for set of changes. Follow the document version control guidelines.

1.1 Version history

Date	Version	Author	Description of change
6th April 2023	0.1	s 9(2)(a)	Initial draft released for BCU Solution Architecture review.
13th April 2023	0.2		Updates to draft version following internal project review.
19th April 2023	0.2.1		Updates to the UAT environment Section • s 6(c) allocation • Moved s 6(c) to Shared Pool • Moved s 6(c) to Private Cloud • Design decision to use s 6(c)
21st April 2023	0.2.2		Minor changes to diagram and spelling.
1st May 2023	0.2.3		Added decision for on-prem connectivity firewall rules s 6(c)
4th May 2023	0.2.4		Added s 6(c) firewall rule. Added target VDC Pools for UAT servers.
16th May 2023	0.2.5		Added Pre-production sections.
23rd May 2023	0.3.0		Updated UAT and PREPROD sections to reflect SIT 4.18 details Restructured UAT section to match PreProd Added PROD section initial draft. s 6(c)
14th June 2023	0.3.1		



			s 6(c)
5 th July 2023	1.0	s 9(2)(a)	Accepted all changes prior to DRB Review.
10 th July 2023	1.1		s 6(c)
31 st July 2023	1.2		



			s 6(c)
11 th January 2024	1.3		s 9(2)(a)



			s 6(c)
17/04/2024	1.4	s 9(2)(a)	



-s 6(c)



			s 6(c)
13/08/2024	1.6	s 9(2)(a)	Accepted all changes and released for DRB.
13/08/2024	1.7		s 6(c)



S 6(c)



			s 6(c)
13/01/2025	1.7		s 9(2)(a)
17/02/2025	1.7		
20/02/2025	1.7		



		s 6(c)
21/02/2025	1.7	s 9(2)(a)
06/03/2025	1.7	
11/03/2025	1.7	
18/03/2025	1.7	
20/03/2025	1.7	
21/03/2025	1.7	
24/03/2025	1.7	
25/03/2025	1.7	
31/03/2025	1.7	
01/04/2025	1.8	
07/04/2025	1.8	
09/04/2025	1.8	
14/04/2025	1.8	



15/04/2025	1.8	s 9(2)(a)	s 6(c)
17/06/2025	1.8		
29/04/2025	1.8		
02/05/2025	1.8		
05/05/2025	1.9		
12/05/2025	1.9		
20/05/2025	1.9		
12/06/2025	1.9		
16/06/2025	1.9		
19/06/2025	1.9		



		s 6(c)
2/7/2025	1.9	s 9(2)(a)
16/07/2025	1.9	
22/07/2025	1.9	
11/08/2025	1.9	
13/08/2025	1.9	
19/08/2025	2.0	
25/08/2025	2.0	
28/08/2025	2.0	
01/09/2025	2.0	
03/09/2025	2.0	
08/09/2025	2.0	



10/09/2025	2.0	s 9(2)(a)	s 6(c)
25/09/2025	2.0		
21/10/2025	2.0		
28/10/2025	2.0		
12/11/2025	2.0		

1.2 Template information

This document was produced using the Capital Portfolio Office's Project Delivery Model 'CPO Solution Design part B' template, version 2.1

1.3 Approved by

The following people have approved this document.

Name	Role	Date	Signature*
	Architecture Review Board		

1.4 Reviewed by

The following people have a formal quality assurance role with respect to this document.

Name	Role	Supported?	Date	Signature
s 9(2)(a)		Yes	28/07/2023	 s 9(2)(a) 3CU Part B Artefact IN-
		Yes	28/07/2023	 s 9(2)(a) 3CU Part B Artefact IN-
		Yes	31/07/2023	 s 9(2)(a) 3CU Part B Artefact IN-



s 9(2)(a)	Yes	31/07/2023	 s 9(2) BCU Part B ort Artefact IN-
	Yes	28/07/2023	 s 9(2) BCU Part B (a) t Artefact IN-
	Yes	28/07/2023	 s 9(2) CU Part B (a) artefact IN-

1.5 Consulted

The following people have been consulted in the production of this document (list excludes approvers and reviewers).

Name	Role	Date
s 9(2)(a)		25/07/2023
		25/07/2023
		25/07/2023
		25/07/2023
		25/07/2023
		25/07/2023
		25/07/2023
		25/07/2023

1.6 Distributed to

The following people / groups have been sent a copy of this document (list excludes approvers, reviewers, and consulted).

Name	Role	Date
s 9(2)(a)		05/07/2023
		05/07/2023
		05/07/2023
		05/07/2023



Contents

1. Document control	i
1.1 Version history	i
1.2 Template information	xii
1.3 Approved by	xii
1.4 Reviewed by	xii
1.5 Consulted	xiii
1.6 Distributed to	xiii
2. Overview	viii
3. Purpose	ix
3.1 Figures and tables	ix
3.2 Context	10
3.3 Project information	10
3.4 Document references	10
4. Terms and definitions	12
5. Solution overview	13
5.1 Overview	13
5.2 Software components	19
5.3 Hardware components	20
5.4 Naming Convention	22
5.5 Server Function Naming Allocation	23
5.6 Certificate Standard for S 6(c)	25
5.6.1 Approved Cipher Standards	27
6. Production Environment	28
6.1 Network	28
6.1.1 Network Topology Diagram	28
6.1.2 VLAN	30
6.1.2.1 S 6(c)	31
6.1.3 IP Addressing	32
6.1.3.1 Servers	32
6.1.3.2 S 6(c)	34
6.1.4 DNS Records	35
6.1.4.1 Server Records	35
6.1.4.2 S 6(c)	37
6.1.4.3 Azure Application Gateway Traffic Manager	38



6.1.4.4	Azure DNS Records	39
6.1.5	Routing	40
6.1.6	s 6(c)	40
6.1.6.1	s 6(c)	40
6.1.6.2	s 6(c)	41
6.1.6.3	s 6(c)	43
6.1.7	Firewall Details.....	45
6.1.7.1	Firewall Objects	45
6.1.7.2	System Firewall Rules	48
6.1.7.3	Database Connectivity Firewall Rules.....	56
6.1.7.4	s 6(c)	58
6.1.7.5	s 6(c)	62
6.1.7.6	Temporary Firewall Rules	63
6.1.7.7	Common Management and Logging Firewall Rules	64
6.1.7.8	Firewall Rule Exemptions.....	67
6.1.8	Zscaler Internet Access requirements.....	67
6.1.9	Zscaler Private Access requirements	70
6.1.10	Switching requirements	71
6.1.11	Additional requirements	71
6.2	Servers	72
6.2.1	Detailed deployment view	72
6.2.2	Existing Servers	73
6.2.3	New server overview	73
6.2.4	Server Virtualisation Resources	74
6.2.4.1	Virtualisation Anti-Affinity Rules	76
6.2.5	New server provisioning details.....	77
6.2.5.1	Disaster Recovery for Virtual Machine Replication	78
6.2.6	SAN Storage	83
6.2.7	NAS Storage	87
6.2.8	Capacity.....	89
6.2.9	Application Whitelisting.....	89
6.2.10	Additional requirements	91
6.2.11	Directory Schedules	93
6.2.11.1	Entra ID	93
6.2.11.2	Active Directory	93
6.2.11.3	Active Directory Security Groups.....	93
6.2.11.4	Security Group Access	95



6.2.11.5	Service Accounts	99
6.2.11.6	Service Account Additional Info.....	103
6.2.11.7	Certificates Schedules.....	103
6.2.12	Database	108
6.2.12.1	Database requirements	108
6.2.12.2	S 6(c)	111
6.2.13	Multi-Subnet Configuration	112
7.	Pre-Production Environment	119
7.1	Network	119
7.1.1	Network Topology Diagram	119
7.1.2	VLAN.....	122
7.1.2.1	S 6(c)	122
7.1.3	IP Addressing.....	122
7.1.3.1	Servers	122
7.1.3.2	S 6(c)	125
7.1.4	DNS Records.....	125
7.1.4.1	Server Records.....	125
7.1.4.2	S 6(c)	127
7.1.4.3	Azure App Gateway Traffic manager	128
7.1.4.4	Azure DNS Records	129
7.1.5	Routing.....	130
7.1.6	S 6(c)	130
7.1.6.1	S 6(c)	130
7.1.6.2	S 6(c)	131
7.1.6.3	S 6(c)	133
7.1.7	Firewall Details.....	135
7.1.7.1	Firewall Objects	135
7.1.7.2	System Firewall Rules	138
7.1.7.3	Database Connectivity Firewall Rules.....	143
7.1.7.4	S 6(c)	144
7.1.7.5	S 6(c)	147
7.1.7.6	Temporary Firewall Rules	147
7.1.7.7	Common Management and Logging Firewall Rules	148
7.1.7.8	Firewall Rule Exemptions.....	152
7.1.8	Zscaler Internet Access requirements.....	152



7.1.9	Zscaler Private Access requirements	154
7.1.10	Switching requirements	156
7.1.11	Additional requirements	156
7.2	Servers	157
7.2.1	Detailed deployment view	157
7.2.2	Existing Servers	158
7.2.3	New server overview	158
7.2.4	Server Virtualisation Resources	159
7.2.4.1	Virtualisation Anti-Affinity Rules	160
7.2.5	New server provisioning details.....	160
7.2.6	SAN Storage	161
7.2.7	NAS Storage	164
7.2.8	Capacity.....	165
7.2.9	Application Whitelisting.....	165
7.2.10	Additional requirements	168
7.2.11	Directory Schedules	169
7.2.11.1	Entra ID	169
7.2.11.2	Active Directory	169
7.2.11.3	Active Directory Security Groups.....	169
7.2.11.4	Security Group Access	171
7.2.11.5	Service Accounts.....	174
7.2.11.6	Service Account Additional Info.....	178
7.2.11.7	Certificates Schedules.....	178
7.2.12	Database	184
7.2.12.1	Database requirements	184
7.2.12.2	S 6(c)	187
8.	User Acceptance Testing Environment.....	197
8.1	Network	197
8.1.1	Network Topology Diagram	197
8.1.2	VLAN.....	199
8.1.2.1	S 6(c)	199
8.1.3	IP Addressing.....	199
8.1.3.1	Servers	199
8.1.3.2	S 6(c)	201
8.1.4	DNS Records.....	202
8.1.4.1	Server Records.....	202
8.1.4.2	S 6(c)	204



8.1.4.3	Azure App Gateway Traffic Manager.....	206
8.1.4.4	Azure DNS Records	206
8.1.5	Routing.....	207
8.1.6	s 6(c)	207
8.1.6.1	s 6(c)	207
8.1.6.2	s 6(c)	208
8.1.6.3	s 6(c)	210
8.1.7	Firewall Details.....	213
8.1.7.1	Firewall Objects	213
8.1.7.2	System Firewall Rules	217
8.1.7.3	Database Connectivity Firewall Rules.....	224
8.1.7.4	s 6(c)	225
8.1.7.5	s 6(c)	230
8.1.7.6	Temporary Firewall Rules	231
8.1.7.7	Common Management and Logging	231
8.1.7.8	Firewall rule exemptions	234
8.1.8	Proxy requirements s 6(c)	234
8.1.9	Zscaler Internet Access requirements.....	235
8.1.10	Zscaler Private Access requirements	236
8.1.11	Switching requirements	238
8.1.12	Additional requirements	238
8.2	Servers	239
8.2.1	Detailed deployment view	239
8.2.2	Existing Servers	240
8.2.3	New server overview	240
8.2.4	Server Virtualisation Resources	241
8.2.4.1	s 6(c)	242
8.2.5	New server provisioning details.....	243
8.2.6	SAN Storage	245
8.2.7	NAS Storage	249
8.2.8	Capacity.....	249
8.2.9	Application Whitelisting.....	250
8.2.10	Additional requirements	252
8.2.11	Directory Schedules	254
8.2.11.1	Entra ID	254
8.2.11.2	Active Directory	254



8.2.11.3	Active Directory Security Groups.....	254
8.2.11.4	Security Group Access	256
8.2.11.5	Service Accounts	260
8.2.11.6	Service Account Additional Info.....	263
8.2.11.7	Certificates Schedules.....	263
8.2.12	Database	270
8.2.12.1	Database requirements	270
8.2.12.2	S 6(c)	272
9.	Development (SIT) environment.....	282
9.1	Network	282
9.1.1	Network Topology Diagram	282
9.1.2	IP Addressing.....	283
9.1.3	DNS Records.....	284
9.1.4	Routing	284
9.1.5	Firewall Objects.....	284
9.1.6	Firewall Rules	284
9.1.7	Firewall rule exemptions.....	285
9.1.8	Proxy requirements.....	285
9.1.9	Switching requirements	285
9.1.10	Additional requirements	286
9.2	Servers	286
9.2.1	Detailed deployment view	286
9.2.2	Existing Servers	287
9.2.3	New server overview	288
9.2.4	New server provisioning details.....	288
9.2.5	Additional requirements	288
9.2.6	Database	289
9.2.7	Database requirements	289
10.	Security	290
10.1	Security Controls.....	290
10.2	Identity and Access Management	291
10.2.1	Security user roles.....	291
10.2.2	Authentication	291
10.2.3	Access rules	292
10.2.4	Security groups.....	292
10.3	Other effected systems.....	292
11.	Realisation.....	294
11.1	Non-functional Requirements	294



11.2	Security goals and constraints	309
12.	Service Management	310
12.1	Management and Monitoring	310
12.2	Network Topology	311
12.3	S 6(c)	311
12.4	Incident Management	312
13.	Appendix: Additional Information	314
13.1	Design Decisions	314
13.2	Prerequisite Software Packages	330
13.2.1	Linux Packages	330
13.2.1.1	Opensearch Install Notes.....	331
13.2.1.2	Opensearch Dashboard Installation	331
13.2.1.3	Agents: FluentD	331
13.2.2	Windows Packages.....	331
13.2.3	Linux Support Tools.....	333
13.3	Operating System Playbooks	335
13.3.1	Linux	335
13.3.1.1	Search Broker Servers S 6(c)	335
13.3.1.2	Search Node Servers S 6(c)	336
13.4	Backup Policies.....	337
13.4.1	Production.....	337
13.4.2	Non-Production.....	338



2. Overview

Page left intentionally blank