



New Zealand Government

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.

Version history

Date	Version	Author	Description of change
16/10/2020	0.1	s9(2)(a)	Split off this IPE design from the BCU part B due to IPE commercial delay
28/10/2020	0.2	s9(2)(a)	Updated DCS and software installation / patching

Table 1: Version History

Template information

This document was produced using the Capital Portfolio Office's ICT Workpackage SDLC template:

- Delivery Model 'Solution Design Part B', [version 2.1](#)

Confluence schedules

For ease of collaboration and maintenance of information between the various solution vendors, detailed design information has been moved from this template into MBIE Confluence pages, collectively referred to as the *ISIDM Detailed Design Schedules* (confluence [link¹](#)).

Approved by

The following people have approved this document.

Name	Role	Date	Signature
ARG	Architecture Review Governance		
ARB	Architecture Review Board		

Reviewed by

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

Name	Role	Supported?	Drop 1 Date	Signature

Consulted

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

Name	Role	Date

Distributed to

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

Name	Role	Date

s 6(c)

Contents

1	Document control	2
	Version history	2
	Template information	3
	Approved by	3
	Reviewed by	3
	Consulted	3
	Distributed to	3
2	Overview	9
	Purpose	9
	Context	9
	Project information	9
	Document references	10
3	Terms and definitions	11
4	Solution Overview	12
	Solution Overview	12
	Software Components	13
	Hardware Components	13
5	Things in the wrong place	15
	Backup and Restore Services	15
	s 6(c)	15
	s 6(c)	15
	Backup and retention policies	15
6	Production Environment	16
	Network	16
	Network Topology Diagram	16
	IP Addressing	16
	DNS Records	17
	Routing	17
	Firewall Objects	17
	Firewall Rules	17
	Firewall rule exemptions	18
	Proxy requirements	18
	Switching requirements	19
	Additional requirements	19
	s 6(c)	19
	Servers	19

Detailed deployment view	20
Existing Servers	20
New server overview	20
New server provisioning details.....	21
Additional requirements	21
Storage	21
s 6(c)	21
Database	22
Database Cluster Details	22
Database RDM Storage Requirements – Production – s 6(c)	23
Database RDM Storage Requirements – DR – s 6(c)	23
Database RDM Storage Requirements – Production – s 6(c)	23
Database RDM Storage Requirements – DR – s 6(c)	24
7 Pre-production environment	25
Network	25
Network Topology Diagram	25
IP Addressing.....	25
DNS Records.....	25
Routing.....	25
Firewall Objects.....	25
Firewall Rules	25
Firewall rule exemptions.....	25
Proxy requirements.....	25
Switching requirements	25
Additional requirements	25
Servers	25
Detailed deployment view	26
Existing Servers	26
New server overview	26
New server provisioning details.....	26
Additional requirements	27
Database	27
Database requirements.....	27
8 User Acceptance testing environment	28
Network	28
Network Topology Diagram	28
IP Addressing.....	28
DNS Records.....	28
Routing.....	28
Firewall Objects.....	28
Firewall Rules	29

Firewall rule exemptions.....	29
Proxy requirements.....	29
Switching requirements	29
Additional requirements	29
Servers	29
Detailed deployment view	29
Existing Servers	30
New server overview	30
New server provisioning details.....	30
Additional requirements	31
Database	31
Database requirements.....	31
9 System Integration Test (SIT) Environment	32
Non-production environment design details	32
Network	32
Network Topology Diagram	32
IP Addressing.....	34
DNS Records.....	34
Routing.....	34
Firewall Objects.....	34
Firewall Rules	34
Firewall rule exemptions.....	34
Proxy requirements.....	34
Switching requirements	34
Additional requirements	34
Servers	34
Detailed deployment view	34
Existing Servers	35
New server overview	35
New server provisioning details.....	35
Additional requirements	36
Database	36
Database requirements.....	36
10 Security	38
Security Controls.....	38
Identity and access management	41
Database named Service Accounts	41
Security groups.....	41
Security user roles.....	41
11 Realisation.....	42
Non-functional requirements	42

Auditing and Logging.....	42
Availability.....	42
Deployment.....	43
Flexibility	43
Interoperability	43
Maintainability	43
Monitoring and Alerts	44
Performance.....	44
Recoverability.....	45
Reliability.....	45
Scalability	46
Security.....	47
Usability.....	51
Appendix One: Disaster Recovery	54
Overview	54
Scope.....	54
DR scenarios.....	55
s 6(c)	55
Appendix Two: All environments	56
Database	56
s 6(c)	56
Logging & Monitoring	57
s 6(c)	58
s 6(c)	58
Server healthcheck.....	58
NEC App servers	58
Database servers.....	58
s 6(c)	58
s 6(c)	58
NEC Logging.....	59
Appendix 2: Candidate Transactions	60
Appendix 3: Data Model.....	61

Figures and tables

Figure 1: IPE Solution – Overview.....	12
Figure 14: Production Network Topology	16
Figure 3: Detailed deployment diagram goes here	20
Figure 5: Detailed deployment diagram goes here	26
Figure 6: Network topology diagram goes here	28
Figure 5: Detailed deployment diagram goes here	30
Figure 15: SIT Network Topology	33
Figure 5: Detailed deployment diagram goes here	35
Figure 13: MySQL high availability overview	57
Table 1: Version History	2
Table 15: Backup and retention schedules s 6(c)	15
Table 16: Retention Policies s 6(c)	15
Table 25: s 6(c)	19
Table 24: s 6(c)	22
Table 19: BCU New Servers	23
Table 20: BCU Database Storage Requirements s 6(c)	23
Table 21: BCU Database Storage Requirements s 6(c)	23
Table 22: BCU Database Storage Requirements s 6(c)	24
Table 23: BCU Database Storage Requirements s 6(c)	24
Table 27: Candidate Transactions	60

pages 9-61, 68-134, 144-751, 757-809, and 825-870 of this Appendix are withheld in full under section 6(c) of the Official Information Act 1982



3644 BCU PA/OIA Report solution

Combined Part A/B

Version: 1.3
Date: 02/05/2025



1. Document control

1.1 Version history

Date	Version	Author	Description of change
13/08/2024	0.1	s 9(2)(a)	Initial draft
13/11/2024	0.2		Updates following consultations with Datacom
22/11/2024	1.0		Initial version for peer reviewing
2/12/2024	1.1		Updates following feedback
18/3/2025	1.2		Added Zscaler configuration (section 11.2)
02/05/2025	1.3		Modified to add another IDme API operation to be utilised by the solution. Updated section 11.4 with the DB roles for s 9(2)(a)

1.2 Template information

This document was produced using the Capital Portfolio Office's Project Delivery Model 'CPO Solution Design Part A' template, version 2.2

1.3 Approved by

The following people have approved this document.

Name	Role	Date	Signature*
Design Review Board	Design Review Board	10/12/2024	Endorsed

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	2/12/2024	 RE_ BCU project - PA_OIA Report solut
		Yes	29/11/2024	 RE_ BCU project - PA_OIA Report solut
		Yes	25/11/2024	 RE_ BCU project - PA_OIA Report solut



Name	Role	Supported?	Date	Signature
s 9(2)(a)		Yes	28/11/20204	 RE_BCU project - PA_OIA Report solut
		Yes	26/11/2024	 BCU PA-OIA Report solutionPart A-B_do
		Yes	26/11/2024	 s 9(2) Ei
		Yes	25/11/2024	 RE_BCU project - PA_OIA Report solut

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)		Various
		Various
		Various
		Various

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)		22/11/2024
		22/11/2024
		22/11/2024
		22/11/2024



1.7 Contents

1. Document control.....	ii
1.1 Version history	ii
1.2 Template information	ii
1.3 Approved by.....	ii
1.4 Reviewed by	ii
1.5 Consulted	iii
1.6 Distributed to	iii
1.7 Contents.....	4
2. Overview	7
2.1 Purpose	7
2.1.1 Project information.....	7
2.1.2 Document references	7
2.1.3 Standards and Patterns.....	9
3. Terms and definitions	10
4. Solution description.....	12
4.1 Solution background	12
4.1.1 Current IGMS Reporting solution.....	13
4.2 Solution stakeholders	14
4.2.1 Internal stakeholders	14
4.2.2 External stakeholders.....	15
4.3 Users of the solution.....	16
4.4 Act(s) and/or Regulation(s).....	16
5. High level architectural view	17
5.1 Architectural goals	17
5.2 Architectural constraints.....	17
5.3 Assumptions.....	17
5.4 Business risks	18
5.5 Architectural risks	18
5.6 Architectural issues.....	18
6. Solution Overview	20
6.1 Overview	20
6.2 Solution Overview.....	20
6.3 Existing components	21
6.4 New components	22
6.5 Opportunities for reuse	22



7. Requirements realisation	24
7.1 Use Cases	24
7.2 Business Requirements	25
7.3 Non-Functional Requirements	26
7.3.1 Availability	27
7.3.2 Capacity, performance and Scalability	27
7.3.3 Information Management	27
7.3.4 Security	28
7.3.5 Applicable Standards and Legislation	28
7.3.6 Maintainability	28
8. Security architecture	29
8.1 Overview	29
8.2 Security architecture goals	29
8.3 Security architecture constraints	29
8.4 Assumptions	30
8.5 Regulations and standards	30
8.6 Privacy and confidentiality concerns	31
8.7 Security controls	31
8.8 Identity and access management	53
8.8.1 Security user roles	53
8.8.2 Authentication	53
8.8.2.1 User authentication	53
8.8.2.2 System-to-system authentication	54
9. Data view	55
s 6(c)	55
9.1.1 Conceptual data model	55
9.1.1.1 s 6(c)	55
9.1.1.2 s 6(c)	55
9.1.2 Logical data model	55
9.1.3 Data management	56
10. Operating considerations	57
10.1 Availability and reliability	57
10.2 Capacity	57
10.3 Continuity	57
10.4 Deployment / implementation	57
10.5 Performance	58
10.6 Scalability	58
10.7 System management, monitoring, and administration	58



11. Deployment view.....	60
11.1 IGMS Vans	62
11.2 Zscaler configuration.....	63
11.2.1 Production.....	63
11.2.1.1 Zscaler firewall rules	63
11.2.1.2 Zscaler Internet Access requirements.....	63
11.2.2 Pre-Production	64
11.2.2.1 Zscaler firewall rules	64
11.2.2.2 Zscaler Internet Access requirements.....	64
11.2.3 UAT.....	65
11.2.3.1 Zscaler firewall rules	65
11.2.3.2 Zscaler Internet Access requirements.....	65
11.2.4 SIT.....	66
11.2.4.1 Zscaler firewall rules	66
11.2.4.2 Zscaler Internet Access requirements.....	66
11.3 Firewall rules.....	67
11.3.1 Production.....	67
11.3.2 Pre-Production	67
11.3.3 UAT.....	67
11.3.4 SIT.....	68
11.4 Service accounts.....	68
11.4.1 Production.....	68
11.4.2 Pre-Production	68
11.4.3 UAT.....	69
11.4.4 SIT.....	69
11.5 Application registration	70
11.5.1 Production.....	70
11.5.2 Pre-Production	71
11.5.3 UAT.....	72
11.5.4 SIT.....	72



3644 BCU Compensating Controls Security Mitigation

Combined Part A/B

Version: 1.0

Date: 20th November 2025

Issue Date: 20th November 2025



1. Document control

1.1 Version history

Date	Version	Author	Description of change
10/04/2024	0.1	9(2)(a)	Initial draft
20/05/2025	0.2		Added Architectural Risk around legacy DRN usage post meeting with s 9(2)(a) s 9(2)(a)
12/06/2025	0.3		Updated SQL CheckPoint section with details for the VIP, CheckPoint Firewall rules and ZPA for SIT+ environments.
18/06/2025	0.4		Updated APIM to F5 mTLS section with certificate and F5 VIP changes required. Also includes backend service changes on Nginx service.
27/06/2025	0.5		Updated host-based firewall rules 6(c)
21/07/2025	0.5		Updated PROD Datawarehouse AL Name to reflect the changes in the EDW design due to length of name limited to 15 characters. 6(c)
23/07/2025	0.5		Added F5 Capacity upgrade requirements to the design in section 11.1.1 F5 Capacity Upgrade
28/07/2025	0.5		Updated DNS record for SQL Choke Point in PROD section 11.8.1.3 6(c) 6(c) and UAT section 11.8.3.3 6(c) 6(c) to reflect detail in EDW design
04/08/2025	0.6		Added SQL ChokePoint VIP monitoring for MariaDB and required firewall rules to be removed post cutover to the VIP for services.
19/08/2025	0.6		Added ICAP Firewall rules detail for Binary Scanning section.
26/08/2025	0.6		Added VIP details and Websites to Insecure API Endpoints section.

Added Enterprise Firewall deny list.



03/09/2025	0.6	9(2)(a)	Removed references to EDW for PROD and UAT as the BCU EDW solution is decommissioned.
			Added additional BCU PROD SQL Servers and UAT SQL Servers
17/09/2025	0.6		Updated SQL ChokePoint with port mapping to support simplified routing.
01/10/2025	0.6		Updates details for LMS-02 around design for IPE Devices auth to not use mTLS and use APM and WAF on the F5 VIP.
06/10/2025	0.6		Updated details for F5 VIP ChokePoint to remove iRules as HTTP requests not being sent. Added new certificate details for MariaDB to support SSL verification.
31/10/2025	0.6		Added Windows Defender Firewall GPO and AD Group details. Removed firewall table details from initial draft.
			Issued to MBIE.
12/11/2025	0.7		Updated APIM to MBIE-REST section for F5 Health Monitoring certificate use and remove MBIS certificate as not required due to the use of the Host certificates
			Accepted all changes and issued to MBIE.
20/11/2025	1.0		Added GPO details to appendix for Windows Defender Firewall
			Issued to MBIE as version 1.0 for project pause.

1.2 Template information

This document was produced using the Capital Portfolio Office's Project Delivery Model 'Exemption form for MIQ) - Combined Part A/B' template, version 2.2

1.3 Approved by

The following people have approved this document.

Name	Role	Date	Signature*
Design Review Board	Design 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
9(2)(a)				

1.5 Consulted

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

Name	Role	Date
9(2)(a)		

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
9(2)(a)		



1.7 Contents

1. Document control.....	ii
1.1 Version history	ii
1.2 Template information	iii
1.3 Approved by	iii
1.4 Reviewed by	iv
1.5 Consulted	iv
1.6 Distributed to	iv
1.7 Contents	5
2. Overview	10
2.1 Purpose	10
2.1.1 Project information	10
2.1.2 Document references	10
2.1.3 Standards and Patterns.....	11
2.2 Benefits	11
2.3 Delivery Approach.....	12
3. Terms and definitions	14
4. Solution description.....	15
4.1 Solution background	15
4.2 Solution stakeholders	17
4.2.1 Internal stakeholders	17
4.2.2 External stakeholders.....	18
4.3 Users of the solution	18
4.4 Act(s) and/or Regulation(s).....	19
5. High level architectural view	21
5.1 Architectural goals	21
5.2 Architectural constraints.....	21
5.3 Assumptions.....	21
5.4 Business risks	21
5.5 Architectural risks	22
5.6 Architectural issues	22
6. Solution Overview	23
6.1 Overview	23
6.2 Solution Overview	23
6.3 Existing components	26
6.4 New components	27



7. Requirements realisation	28
7.1 Non-Functional Requirements	28
7.1.1 Capacity, performance and Scalability	28
7.1.2 Maintainability	28
8. Security architecture	30
8.1 Security architecture goals	30
8.2 Security architecture constraints	30
8.3 Regulations and standards	30
8.4 Security controls	31
8.5 Identity and access management	32
8.5.1 Authentication	32
8.5.1.1 s 6(c)	32
9. Data view	33
9.1.1 Conceptual data model	33
9.1.2 Logical data model	33
10. Operating considerations	34
10.1 Availability and reliability	34
10.2 Capacity	34
10.3 Continuity	34
10.4 Deployment / implementation	34
10.5 Performance	35
10.6 Scalability	35
10.7 System management, monitoring, and administration	35
11. Deployment view	37
11.1 Threat Scanning	38
11.1.1 F5 Capacity Upgrade	38
11.1.2 ASM Policy	38
11.1.3 APIM to MBIE-REST Configuration Changes	44
11.1.3.1 PROD	45
11.1.3.2 PREPROD	46
11.1.3.3 UAT	48
11.1.3.4 SIT	49
11.1.4 F5 ASM Policy Scope	50
11.2 RBAC User and Client Connectivity	53
11.2.1 Zscaler Application Segment Updates	53
11.2.1.1 PROD Insights	53
11.2.1.2 PROD MBIS	54
11.2.1.3 PROD MBISREST	54



11.2.1.4	PROD Reveal.....	54
11.2.1.5	PROD IDME Auth.....	54
11.2.1.6	PROD LMS	55
11.2.1.7	PRE Insights	55
11.2.1.8	PRE MBIS	55
11.2.1.9	PRE MBISREST	56
11.2.1.10	PRE Reveal	56
11.2.1.11	PRE IDME Auth	56
11.2.1.12	PRE LMS	56
11.2.1.13	UAT Insights.....	57
11.2.1.14	UAT MBIS.....	57
11.2.1.15	UAT MBISREST	57
11.2.1.16	UAT Reveal	58
11.2.1.17	UAT IDME Auth.....	58
11.2.1.18	UAT LMS	58
11.2.1.19	SIT Insights.....	59
11.2.1.20	SIT MBIS.....	59
11.2.1.21	SIT MBISREST	59
11.2.1.22	SIT Reveal.....	59
11.2.1.23	SIT IDME Auth.....	60
11.2.1.24	SIT LMS	60
11.2.1.25	CheckPoint Firewall Rules updates.....	60
11.3	Clear text protocols.....	69
11.4	Host-based firewall rules	70
11.4.1	Red Hat Enterprise Linux firewalld.....	70
11.4.2	Windows Defender Firewall.....	70
11.5	Enterprise Firewall Rules.....	73
11.6	Binary Scanning.....	76
11.7	Insecure s 6(c)	79
11.8	Inbound s 6(c)	82
11.8.1	PROD	83
11.8.1.1	F5 VIP Configuration	85
11.8.1.2	Firewall Rules	86
11.8.1.3	DNS Records.....	88
11.8.1.4	Certificates	88
11.8.2	PREPROD	90
11.8.2.1	F5 VIP Configuration	91
11.8.2.2	Firewall Rules	92



11.8.2.3	DNS Records.....	93
11.8.2.4	Certificates	93
11.8.3	UAT.....	95
11.8.3.1	F5 VIP Configuration	96
11.8.3.2	Firewall Rules	97
11.8.3.3	DNS Records.....	98
11.8.3.4	Certificates	98
11.8.4	SIT.....	99
11.8.4.1	F5 VIP Configuration	100
11.8.4.2	Firewall Rules	101
11.8.4.3	DNS Records.....	102
11.8.4.4	Certificates	102
11.9	Execute Batch Jobs.....	104
12.	F5 VIP Configurations.....	105
12.1	PROD s 6(c)	105
12.2	PREPROD s 6(c)	107
12.3	UAT s 6(c)	108
12.4	SIT s 6(c)	110
13.	Appendix.....	112
13.1	Windows Defender Firewall Policies GPO Details.....	112
13.1.1	PROD	112
13.1.1.1	BCU_FW_IPC_EAG	112
13.1.1.2	BCU_FW_LMS_Enrolment_Server	131
13.1.1.3	BCU_FW_IQ_Office_Server.....	148
13.1.1.4	BCU_FW_Management_Server	165
13.1.1.5	BCU_FW_SQL_Server.....	177
13.1.2	PREPROD	201
13.1.2.1	BCU_FW_IPC_EAG_PRE	201
13.1.2.2	BCU_FW_LMS_Enrolment_Server_PRE.....	216
13.1.2.3	BCU_FW_IQ_Office_Server_PRE.....	233
13.1.2.4	BCU_FW_Management_Server_PRE	247
13.1.2.5	BCU_FW_SQL_Server_PRE.....	259
13.1.3	UAT.....	278
13.1.3.1	BCU_FW_IPC_EAG_UAT.....	278
13.1.3.2	BCU_FW_LMS_Enrolment_Server_UAT	296
13.1.3.3	BCU_FW_IQ_Office_Server_UAT	315
13.1.3.4	BCU_FW_Management_Server_UAT	332



13.1.3.5	BCU_FW_SQL_Server_UAT	346
13.1.4	SIT	370
13.1.4.1	BCU_FW_IPC_EAG_SIT	370
13.1.4.2	BCU_FW_LMS_Enrolment_Server_SIT	428
13.1.4.3	BCU_FW_IQ_Office_Server_SIT	472
13.1.4.4	BCU_FW_Management_Server_SIT	512
13.1.4.5	BCU_FW_SQL_Server_SIT	552

DRAFT

Immigration New Zealand

IDme Rescaling

3586 In-Person Enrolment (IPE) Solution Design Part A

Version 1.3

Document Control

Version History

Date	Version	Name	Comments
3 rd October 2019	0.1	9(2)(a)	Initial Draft
20 th March 2020	0.2	9(2)(a)	Updated per recent BCU and NEC discussions
27 th March 2020	0.5	9(2)(a)	Initial draft for NEC
31 st March 2020	0.6	9(2)(a)	Updated section 10 data architecture
2 nd April 2020	0.7	9(2)(a)	Clarified support for <i>Identity Search</i> . Completed Operating Considerations. Added indicative security controls
3 rd April 2020	0.8	9(2)(a)	Draft for NEC and stakeholder review.
9 th April 2020	1.0	9(2)(a)	NEC comment incorporated; Version for MBIE Architecture Reference Group review
16 th April 2020	1.1	9(2)(a)	Incorporating comments/changes from Architecture Reference Group review
17 th April 2020	1.2	9(2)(a)	Handful of corrections by the business/systems owner.
23 rd April 2020	1.3	9(2)(a)	ARG/ARB updates including add Deployment View, overview of workstation maintenance. Added Enrolment Manager to overview plus miscellaneous minor updates.

Template Capital Portfolio Office's (CPO) Project delivery model template, version 3.0.

Approval

Name	Role	Date	Signature
ARG	Architecture Reference Group	14/4/2020	9(2)(a)
ARB	Architecture Review Board	21/4/2020	Endorsed April 21 2020

Reviewed By

Name	Role	Date
9(2)(a)		07/04/2020, 09/04/2020
		07/04/2020

Table of Contents

1.	Introduction	6
1.1	Purpose	6
1.2	Project Context	6
1.3	Document References	7
2.	Terms and definitions	8
2.1	Enrolment versus Registration.....	8
2.2	Other terms in this solution.....	8
3.	Business View	9
3.1	Enrolment business process	9
3.2	Users of the solution.....	9
3.3	Current problems.....	10
3.4	Solution objectives.....	10
3.5	Strategic alignment.....	11
3.5.1	Future state architecture	11
3.5.2	Identity strategy.....	11
3.7	Solution stakeholders	12
4.	Architectural overview	13
4.1	Capture equipment.....	15
4.1.1	IPE Workstations (type F).....	15
4.1.2	IPE Mobile Workstations (type M).....	15
4.1.3	Hardware spec	15
4.2	Application software.....	16
4.2.1	SmartScan	16
4.2.2	Other relevant user interfaces.....	16
4.2.3	Access customised by role and need	16
4.3	Capture workstation maintenance	17
4.4	Surfacing IDme processing state at point of capture	17
4.5	Architectural principles.....	19
4.6	Architectural goals	21
4.7	Architectural constraints	22
4.8	Assumptions.....	22
4.9	Architectural risks	22
5.	Business Requirement realisation	23
5.1	Functional requirements	23
5.2	Non-functional requirements	27
6.	Logical design view	30
6.1	Proposed product & technology selections.....	31
6.2	SmartScan capture workstation software	32
6.3	Enrolment Manager instancing	33
6.4	Interfaces	34
6.4.1	SmartScan	34
6.4.2	Enrolment / Search Transaction Submission	35

6.4.3	IDme / AMS synchronisation for IPE-registered identities	36
6.5	User Interaction and System Integration.....	37
6.5.1	User Level Interaction	37
6.5.2	System Level Interaction.....	37
7.	Security architecture	38
7.1	Identity and access management	38
7.1.1	Security user roles.....	38
7.1.2	User Authentication	38
7.1.3	Authorisation	39
7.1.4	User authentication context flow	40
7.2	Logging and Monitoring.....	41
7.3	Security Controls (indicative).....	42
8.	Data view.....	47
8.1	Conceptual data model.....	47
8.2	Logical data model	48
8.2.1	NIST Enrolment Mapping Specification	48
8.2.2	Aligning MRP data with AMS	48
8.3	Data classification	50
8.4	Data replication (master-slave relationships).....	50
8.5	Data storage, archiving and retention	50
8.6	Data migration	51
8.7	Records management.....	51
9.	Operating considerations.....	52
9.1	Availability and reliability.....	52
9.2	Performance and Scalability	53
9.3	Continuity.....	55
9.4	Maintainability.....	57
9.5	Deployment/implementation.....	57
9.6	System management, monitoring and administration.....	57
10.	Deployment view	58

Table of figures

Figure 1 Identity enrolment journey showing capture and registration	8
Figure 2 Overview of upgraded interfaces for identity capture and registration.....	13
Figure 3 IPE Logical components and data flows.....	30
Figure 4 Workstation to enrolment manager interfacing.....	34
Figure 5 Enrolment manager to IDme interfacing	35
Figure 6 In person enrolment: IDme/AMS sync'ing.....	37
Figure 7 Authentication context flow and switching.....	40
Figure 8 Conceptual information model.....	47
Figure 9 Indicative deployment view	58



3644 Biometric Capability Update (BCU) - Application Solution Design part B

Version: 2.13

Date: 31/10/2025



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
01/08/2022	0.1	9(2)(a)	Initial draft (IPE part)
31/03/2023	0.2		Updates to draft (IDMe part)
28/04/2023	0.3		Updates to draft (rearranging sections; removing unnecessary details)
05/07/2023	0.4		Multiple updates: preparing for pre-DRB review by domain architects
12/07/2023	0.5		Updated following feedback from Ed Tissink
21/07/2023	1.0		Updated following feedback from Jane Peng, Jeff Dahlberg, Michael Chen
03/08/23	1.1		Added reference to retention policy in Section 14 EDW reports, from DRB review by Information Management
6/10/23	1.2		Updated section 5.2.1.4.4 with reference to the IBW registry keys and security ciphers required
13/12/2023	2		Updated section 5.2.3.1 with a sequence diagram for IBW client authentication and authorisation
08/08/2024	2.11		Added Appendix M to provide information on security amendments recommended and/or mandated by Cyber Security. Amended Appendix B (Active Directory groups) to reflect the changes and adding groups for Blind Assessment Rates. Amended sections on Alerting and Monitoring, and SIEM.
12/08/2024	2.12		Updates to section 16.1 following additional details from NEC.
31/10/2025	2.13		Updates with information obtained and additional changes post the conditional endorsement by the DRB .



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*
	Design 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
9(2)(a)		Yes	28/07/2023	9(2)(a)
		Yes	28/07/2023	
		Yes	31/07/2023	
		Yes	28/07/2023	
		Yes	27/07/2023	
		Yes	28/07/2023	
		Yes	25/07/2023	
		Yes	9/08/2024	
		Yes	13/08/2024	



Name	Role	Supported?	Date	Signature
9(2)(a)		Yes	13/08/2024	9(2)(a)
TODO prior to submission to the DRB obtain OKs via email from EA, Cyber, Arch Capability Lead as above				

1.5 Consulted

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

Name	Role	Date
9(2)(a)		Multiple; last 12/08/23
		Multiple; last 12/08/23
		Multiple; last 24/07/23
		Multiple; last 24/07/23
		Multiple; last 08/06/23
		Multiple; last 30/06/23
		Multiple; last 07/06/23
		Multiple; last 08/06/23
		Multiple; last 18/07/23
		Multiple; last 16/07/23
		Multiple; last 16/07/23

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
9(2)(a)		05/07/23 and again 09/08/24
		05/07/23 and again 09/08/24



Name	Role	Date
		 RE, BCU Application Part B - i
9(2)(a)		05/07/23 and again 09/08/24



Contents

1	Document control	i
1.1	Version history	i
1.2	Template information	ii
1.3	Approved by	ii
1.4	Reviewed by	ii
1.5	Consulted	iii
1.6	Distributed to	iii
1.7	Figures	viii
1.8	Tables	ix
2	Overview	1120
2.1	Purpose	1120
2.2	Context	1120
2.2.1	Project information	1120
2.2.2	Document references	1221
3	Terms and definitions	1423
4	Solution overview	1726
4.1	Overview	1726
4.2	Software components	2029
4.2.1	User Applications	2029
4.2.2	Backend applications and datastores	2130
4.2.2.1	Key NEC components	2130
4.2.2.2	Existing MBIE systems	2433
4.3	Human Actors	2434
4.4	Hardware components	2534
5	IDme Solution Details	2635
5.1	Design Decisions	2635
5.2	User Interface	3039
5.2.1	Operator Analysis and Investigation	3039
5.2.1.1	NeoFace Reveal Web Application	3140
5.2.1.2	Reveal Dashboard	3140
5.2.1.3	Reveal Client Requirements	3241
5.2.1.4	Integrated Biometric Workstation (IBW) overview	3241
5.2.2	Operational Management	3746
5.2.3	User Authentication and Authorisation	3948



5.2.3.1	NEC User Interfaces – Role Based Access Control	3948
5.2.4	Reporting and Auditing	4655
5.2.4.1	NEC reporting	4655
5.2.4.2	Auditing	4756
5.2.5	In-Person Enrolment	4756
5.3	Application Layer	4756
5.4	Data	4958
5.4.1	Data classification	4958
5.4.2	System of record	5059
5.4.3	Data storage location	5059
5.4.4	Data security	5059
5.4.5	Data replication	5059
5.4.6	Data backup	5059
5.4.6.1	MS-SQL backup schedule	5059
5.5	Integration	5160
5.5.1	Authentication and integration	5261
5.5.1.1	API Integrations within BCU	5261
5.5.1.2	MSMQ Integration between AMS & NEC IDme	5261
5.5.1.3	JWT authentication for access to MBIS RESTful APIs (NEC-internal integration)	5362
5.5.2	API Integrations	5463
5.5.2.1	API standards and guidelines	5766
5.5.2.2	Audit logging	5766
5.5.2.3	API patterns used by the solution	5867
5.5.3	Changes to the existing systems	6069
5.5.3.1	IGMS	6069
5.5.3.2	IQ Office Updates	6574
5.5.3.3	AMS	6675

6(c) of the OIA

5.6	Logging	7281
6	IPE Solution Details	7483
6.1	Overview	7483
6.2	SmartScan: off-line backup and restore	7685
6.3	SmartScan and Central LMS	7685
6.3.1	SmartScan Summary	7685
6.3.2	Operating System	7685
6.3.3	Hardware Drivers	7786



6.3.4	Windows 10+	7786
6.3.5	SmartScan Software	7786
6.3.5.1	Overview	7887
6.3.5.2	SmartScan Transaction Volumes.....	8089
6.3.5.3	IPE Hardware.....	8190
6.3.6	Central LMS	8190
6.3.6.1	Support and configuration	8291
6.3.6.2	Systems Components.....	8291
6.3.7	Authentication and Authorisation	8392
6.3.7.1	SmartScan Authentication	8392
6.3.7.2	SmartScan Authorisation	8493
6.3.7.3	Central LMS Authentication & Authorisation	8594
6.3.8	Data	8695
6.3.8.1	Data Classification	8695
6.3.8.2	Type of Data Captured	8695
6.3.8.3	System of Record	8695
6.3.8.4	Data Capture Lifecycle	8695
6.3.8.5	Data Exchange.....	8897
6.3.8.6	Data encryption.....	8998
6.3.8.7	Data Replication	91100
6.3.8.8	Temporary Data Retention Periods	92101
6.3.8.9	NIST Record Structure	92101
6.3.9	Monitoring, Auditing and Reporting	92101
6.3.9.1	System monitoring	92101
6.3.9.2	Application auditing and monitoring	92101
6.3.9.3	Reporting.....	93102
7	Production Environment	94103
8	Pre-production environment.....	95104
9	User Acceptance testing environment	96105
10	Development environment	97106
11	Security	98107
11.1	Security Controls	98107
11.2	Identity and access management	98107
11.2.1	User teams	98107



11.2.2	Authentication	99108
11.2.3	Authorisation	99108
11.3	Network	99108
11.4	Security updates and patching.....	101112
11.4.1	Azure solution components: vulnerability, configuration, patch management.....	101112
11.4.1.1	How vulnerability OR configuration defect detection is done.....	101112
11.4.1.2	How vulnerability OR configuration defect severity is determined.....	101112
11.4.1.3	How applicability to MBIE and INZ is assessed	101112
11.4.1.4	Vulnerability tools and/or configuration analysis used for scanning, detection, and triage	102113
11.4.1.5	Patching and defect remediation.....	102113
11.4.1.6	Patching schedule or remediation schedule based on severities are across the production and non-production environments for MBIE and INZ Azure environment ...	102113
11.4.2	Software integrity	102113
12	Monitoring and alerting	103114
12.1	Operating System monitoring.....	104115
12.2	Database monitoring	104115
12.3	Application monitoring	105116
12.3.1	Monitoring thresholds.....	105116
12.3.2	Monitored applications.....	105116
12.3.3	Service Health checks.....	106117
12.4	Application Log Monitoring	106117
12.4.1	Monitoring Thresholds.....	106117
12.5	Transaction and licences monitoring.....	107118
12.5.1	Licences	107118
12.5.1.1	IQ Office	107118
12.5.1.2	AimXM.....	107118
12.5.1.3	Transactions status	108119
13	SIEM.....	109120
14	Reports and analytics.....	110122
14.1	Snowflake data warehouse (Cloud Data Platform – CDP)	110122
	Solution overview	Error! Bookmark not defined.Error! Bookmark not defined.
14.1.1		111123
14.1.2	Data	111123
14.1.2.1	Data classification	112124
14.1.2.2	Full replication.....	112124
14.1.2.3	Change Data Capture	112124



14.1.2.4	Volumes and performance.....	113125
14.1.2.5	Additional data sources	113125
14.1.3	Security.....	114126
14.1.3.1	Data encryption.....	114126
14.1.3.2	Access control	114126
14.1.4	HA and DR	115127
14.1.4.1	Potential data loss scenarios.....	120132
14.2	PA/OIA report	122135
15	Data Consistency Report	123136
16	High Availability and Disaster Recovery	125138
16.1	High Availability.....	125138
16.2	Disaster Recovery.....	127140
17	Realisation.....	130143
17.1	Non-functional requirements	130143
17.1.1	Applicable standards.....	131144
17.1.2	Auditing and logging	131144
17.1.3	Availability.....	134147
17.1.4	Deployment.....	138151
17.1.5	Extensibility	140153
17.1.6	Flexibility	140153
17.1.7	Interoperability	141154
17.1.8	Maintainability	143156
	System/file updates.....	144157
	Description	144157
17.1.9	Monitoring and alerting	147160
17.1.10	Performance.....	149162
17.1.11	Recoverability.....	150163
17.1.12	Reliability.....	153166
17.1.13	Reusability.....	155168
17.1.14	Scalability	156169
17.1.15	Security.....	158171
17.1.16	Usability.....	159172
17.2	Additional security NFRs and controls	163176
17.2.1	Security NFRs identified by MBIE Cyber Security.....	163176
17.2.2	Additional Security Controls	186199
17.2.3	IPE-specific Security Risks and Controls	200213
	Appendix A: Security controls at a glance	209222



Appendix B: The Active Directory groups mapping for authorisation and Blind Assessment Rates ... 210223

17.3	Keycloak Application AD Security Groups:.....	211224
17.4	MBIS Core Application AD Security Groups:	211224
17.5	SmartScan AD Security Groups:	212225
17.6	Blind Assessment Rate AD Groups.....	213227

18 Appendix C - IPE Hardware Kits 215228

19 Appendix D: NIST record structures 216229

19.1	Type 1 Records.....	216229
------	---------------------	--------

20 Appendix F: IDme Audit list 218231

21 Appendix G: Open source libraries..... 221234

22 Appendix H: Human actors..... 226239

23 Appendix I: IDme web applications configuration 228241

23.1	Reveal web application	228241
23.2	Insights web application	228241
23.3	MBIS web application	229242
23.4	Keycloak	230243

24 Appendix J: Data migration 231244

24.1.1.1	Biographic Data.....	231244
24.1.1.2	Biometric Data	231244
24.1.1.3	Types of migration	231244
24.1.1.4	Migration process	233246

25 Appendix K: SmartScan and LMS deployment configuration..... 234248

25.1	Central LMS URL.....	234248
25.2	SmartScan Workstation Configuration	235249
25.3	Central LMS connection to MBIS	237251

26 Appendix L: Application monitoring and service Health checks..... 238252

26.1	Application monitoring	238252
26.1.1	MBIS	238252
26.1.2	Reveal.....	238252
26.1.3	Keycloak	238252
26.1.4	IBW (server-side).....	238252
26.1.5	LSMS.....	238252
26.1.6	Search Broker.....	238252
26.1.7	Search Nodes.....	238252
26.1.8	EAI Interface.....	239253



26.1.9	LSMS Service	239253
26.1.10	Central LMS	239253
26.1.11	IQ Office	240254
26.1.12	Log Server	240254
26.1.13	Reporting	240254
26.1.14	SOLR	240254
26.2	Service Health checks.....	240254
26.2.1	Reveal Wildfly Service	240254
26.2.2	Reveal User Interface	241255
26.2.3	Insights Wildfly Service	241255
26.2.4	Insights User Interface	241255
26.2.5	MBIS Wildfly Service	241255
26.2.6	MBIS User Interface	241255
26.2.7	IBW Wildfly Service	241255
26.2.8	IBW via F5.....	242256
26.2.9	Keycloak	242256
26.2.10	Keycloak via F5	242256
26.2.11	SBSC.....	242256
26.2.12	Search Node	242256
26.2.13	EAI Interface.....	243257
26.2.14	LSMS Service	243257
26.3	Logfiles	244258
27	Appendix M: Other security controls considerations	245259
27.1	SQL column level encryption	245259
27.1.1	Column Level Encryption	245259
27.1.2	The reason for investigation of this control.....	245259
27.1.3	Types of column level encryption	245259
27.1.4	How it works	245259
27.1.5	Limitations.....	246260
27.1.6	Always Encrypted with secure enclaves	246260
27.1.7	Options overview	246260
27.1.8	Recommendation.....	247261
27.1.8.1	Recommendation rationale:	247261
27.1.8.2	For noting	248262
27.2	Application traffic inspection	249263
27.2.1	Traffic Inspection of inbound traffic to IDme	249263
27.2.2	Zscaler Zero Trust Exchange Platform.....	250264
27.2.3	Recommendation.....	252266
27.3	Key management	253267
27.3.1	Background	253267



27.3.2	Expected benefits.....	253267
27.3.3	TDE keys	253267
27.3.3.1	SQL DB.....	253267
27.3.3.2	Maria DB.....	254268
27.3.4	Azure APIM API subscription keys	254268
27.3.4.1	Recommendation.....	255269
27.3.5	IDMe system storage encryption keys.....	255269
27.3.5.1	Datacom provided the following info – see the embedded email (via PDM; not quite clear if the keys are rotated though – awaiting clarification):	255269
27.3.5.2	Recommendation.....	256270
27.3.6	SSH keys	256270
27.3.6.1	Investigation.....	256270
27.3.6.2	Recommendation.....	256270
27.3.7	Column encryption keys.....	256270
27.3.7.1	Recommendation.....	256270
27.4	Additional enterprise-wise pre-existing security concerns.....	256270
27.4.1	Summary	256270
27.4.2	Validation of a revocation status of PKI certificates utilised at API endpoints.....	256270
27.4.2.1	Investigation.....	257271
27.4.2.2	Other considerations	257271
27.4.2.3	Recommendation.....	257271
27.4.3	F5s in bridging mode not validating certificates of the backend servers	258272
27.4.3.1	Investigation.....	258272
27.4.3.2	Other considerations	258272
27.4.3.3	Recommendation.....	258272
28	Appendix N: API definitions.....	260274
29	Appendix O: Data to be replicated to a DW.....	261275

1.7 Figures

Figure 1. A logical view of the NEC MBIS platform, including integrations with existing MBIE systems. ...	1827
Figure 2 IDme solution capabilities.....	1928
Figure 3. Solution components mapping to logical functions.	2635
Figure 4 Service Decomposition.....	3039
Figure 5 Service to Application mapping	3039
Figure 6. Reveal identity resolution workflow	3140
Figure 7 Reveal dashboard component model.....	3241
Figure 8 Police use of IBW – application workflow.....	3443



Figure 9. IBW resolution workflow	3443
Figure 10. MBIS Web Application workflow	3948
Figure 11. Insights Web Application workflow (note: F5 will use round robin load balancing)	3948
Figure 12. Keycloak-AD sequence	4352
Figure 13. IBW logon flow	4453
Figure 14. Reporting services process	4756
Figure 15. Service decomposition (Figure 4 copied here for ease of reference)	4756
Figure 16: API invocation sequence – high level	5261
Figure 17 BCU Application integration (link	5564
Figure 18. On-premises to Azure Cloud API invocation	5968
Figure 19. Azure Cloud to on-premises API invocation.	5968
Figure 20. On-premises to on-premises API invocation.	6069
Figure 21. Changed DMS components and flows	6170
Figure 22. IGMS IMB integration with AMS	6271
Figure 23. AMS integration to IGMS	6372
Figure 24. IGMS Online application submission	6372
Figure 25. NEC IDme integration to IGMS	6473
Figure 26. Ineligible check	6574
Figure 27. MBIS-IQOffice integration	6675
Figure 28. MBIS-AMS integration	6776
Figure 29. 6(c) of the OIA	7079
Figure 30. Centralised application logging	7382
Figure 31 IPE High level solution overview diagram	7584
Figure 32 SmartScan Workstation OU	7786
Figure 33. SmartScan Overview	7988
Figure 34. Central LMS overview	8291
Figure 35. SmartScan login sequence	8493
Figure 36. Central LMS authentication sequence	8594
Figure 37 Data Lifecycle	8796
Figure 38 Data Exchange	8998
Figure 39 Data Replication	91100
Figure 40. High level view of solution network segmentation (#6 has been intentionally removed as not reflecting the correct NEC IDme->EAG pathway). Refer to section 5.3 Application Layer (Table 12; Transaction Controller entry) for description of Hazelcast being used for co-ordination of work between MBIS components (#5 in the diagram above).	100111
Figure 41. Nagios monitoring	103114
Figure 42 Qlik-to-Snowflake data replication	111123
Figure 43. PA/OIA report solution – high-level design (this option obtained “Proceed” from the DRB) ..	122135
Figure 44. Data consistency report – component model	123136
Figure 45. Security controls at a glance	209222

1.8 Tables

Table 1. Mapping between capability and solution components	2029
Table 2. Solution User applications	2130
Table 3. Solution backend applications and datastores	2333
Table 4. MBIE's existing components/systems utilised by the solution	2434
Table 5. Design decisions	2938
Table 6. Investigation and analysis applications	3140



Table 7. Reveal Client Requirements	3241
Table 8. IBW suite of applications.....	3342
Table 9. SCCM packages for IBW deployment.....	3544
Table 10. IBW client requirements	3544
Table 11. NEC applications summary.....	3847
Table 12. NEC components - Application layer.....	4958
Table 13. MBIS databases	4958
Table 14. System of Record for IDme-collected data	5059
Table 15. MS SQL backup schedule	5059
Table 16. Integration pathways	5261
Table 17. API integrations.....	5766
Table 18. SmartScan components	7887
Table 19 SmartScan Workflow.....	8089
Table 20. SmartScan expected transaction volumes	8190
Table 21 Central LMS system components.....	8392
Table 22 System of Record for IPE-collected data.....	8695
Table 23 Data Capture Lifecycle.....	8796
Table 24 Data Storage Location	8897
Table 25 Polling Intervals	8998
Table 26 Data encryption.....	9099
Table 27 Data Replication	92101
Table 28 Temp Data Retention Periods	92101
Table 29. Standard LMS reports.....	93102
Table 30. User roles	98107
Table 31 Operating System Monitoring.....	104115
Table 32 Database Monitoring	105116
Table 33. Application monitoring thresholds	105116
Table 34. Log files monitoring.....	107118
Table 35. Solution's HA mechanisms	127140
Table 36. Disaster Recovery - affected functionality and recovery approach.....	129142
Table 37 NIST Type 1 records.....	217230
Table 38 Central LMS URL.....	234248
Table 39 Central LMS Servers per environment	234248