



<i>Document Name</i>	<b>IAM Code of Connection</b>
<i>File Name</i>	CIC204-0000-IAM Coco-v1_0-IAM.doc
<i>Authors</i>	██████████ ██████████
<i>Version</i>	1.0
<i>Issue Date</i>	11 <sup>th</sup> November 2009

THIS DOCUMENT HAS BEEN APPROVED BY THE FOLLOWING FOR RELEASE, BUT IS SUBJECT TO APPROVAL BY PIAB

<i>Authorisation</i>	Police National Accreditor
<i>Signature</i>	██████████

<i>Authorisation</i>	Police PKI Policy Management Authority (P3MA)
<i>Signature</i>	██████████

© - NPIA (National Policing Improvement Agency) 2009

All rights reserved. No part of this publication may be reproduced, modified, amended, stored in any retrieval system or transmitted, in any form or by any means, without the prior written permission of NPIA (National Policing Improvement Agency) or its representative.

For additional copies, or to enquire about the content of this document please contact IAM on 0208 200 3268.

For copyright specific enquiries, please telephone the National Police Library on 01256 602650.

# Table of Contents

<b>1</b>	<b>Reference Documents</b>	<b>ii</b>
<b>2</b>	<b>Definitions</b>	<b>i</b>
<b>3</b>	<b>Introduction</b>	<b>1</b>
3.1	Background	1
3.2	Purpose	1
3.3	Scope	1
3.4	Assumptions and Dependencies	2
3.5	Future Development	2
<b>4</b>	<b>Compliance Governance</b>	<b>3</b>
4.1	Governance	3
4.2	Statement of Applicability	3
4.3	Accreditation Regime	3
4.4	Compliance Certificate	3
4.5	Annual Code of Connection Submission	4
4.6	Non-Compliance	4
<b>5</b>	<b>Code of Connection</b>	<b>5</b>
5.1	Overview	5
5.2	ACPO/ACPOS Compliance	5
5.3	Identity Verification and Personnel Vetting	5
5.4	Local Governance and Accreditation	6
5.5	Local Implementation	7
5.6	CJX and xCJX Connectivity	8
5.7	Confidentiality Impact Level 3 (RESTRICTED)	9
5.8	Confidentiality Impact Level 4 (CONFIDENTIAL)	9
5.9	Multi Factor Authentication: PKI/Smart Card	10
5.10	Single Factor Authentication: Username and Password	11
	<b>Appendix A – Application for IAM Compliance Certificate</b>	<b>12</b>
	<b>Appendix B - Compliance Checklist</b>	<b>13</b>
	<b>Appendix C – Glossary of Terms</b>	<b>14</b>
	<b>Control Page</b>	<b>15</b>

# 1 Reference Documents

The following documents are referenced in this document.

Ref	Description	Document reference	Revision
[A]	CJX Code of Connection	<a href="http://www.npiaextranet.pnn.police.uk/microsite/polwarp/index.htm">http://www.npiaextranet.pnn.police.uk/microsite/polwarp/index.htm</a> (Registration Required)	5.2
[B]	PND Code of Connection	<a href="http://www.npiaextranet.pnn.police.uk/microsite/polwarp/index.htm">http://www.npiaextranet.pnn.police.uk/microsite/polwarp/index.htm</a> (Registration Required)	1.1
[C]	IAM Entity Attributes	<a href="http://www.npiaextranet.pnn.police.uk/microsite/fni/prog_info/iam">http://www.npiaextranet.pnn.police.uk/microsite/fni/prog_info/iam</a>	1.0
[D]	IAM Force Action Plan (FAP)	<a href="http://www.npiaextranet.pnn.police.uk/microsite/fni/prog_info/iam">http://www.npiaextranet.pnn.police.uk/microsite/fni/prog_info/iam</a>	1.1
[E]	ACPO/ACPOS National Vetting Policy	<a href="http://www.npiaextranet.pnn.police.uk/microsite/polwarp/index.htm">http://www.npiaextranet.pnn.police.uk/microsite/polwarp/index.htm</a> (Registration Required)	3.0
[F]	ACPO/ACPOS Information Systems Community Security Policy	<a href="http://www.npiaextranet.pnn.police.uk/microsite/polwarp/index.htm">http://www.npiaextranet.pnn.police.uk/microsite/polwarp/index.htm</a> (Registration Required)	3.3
[G]	HMG's Minimum Requirements for the Verification of the Identity of Individuals	<a href="http://www.cabinetoffice.gov.uk/media/cabinetoffice/csia/assets/hmg_reqmnt_v_eri_id_individual.pdf">http://www.cabinetoffice.gov.uk/media/cabinetoffice/csia/assets/hmg_reqmnt_v_eri_id_individual.pdf</a>	2.0
[H]	CESG Good Practice Guide 13 ("Protective Monitoring for HMG ICT Systems")	<a href="http://cesg.gsi.gov.uk/">http://cesg.gsi.gov.uk/</a>	1.0
[I]	tScheme Model Specification of Service Subject to Assessment	<a href="http://www.tscheme.org/library/">http://www.tscheme.org/library/</a>	4.01
[J]	Common Criteria	<a href="http://www.commoncriteriaportal.org/">http://www.commoncriteriaportal.org/</a>	N/A
[K]	Police Service PKI Compliance Policy	<a href="http://www.npiaextranet.pnn.police.uk/microsite/fni/prog_info/iam">http://www.npiaextranet.pnn.police.uk/microsite/fni/prog_info/iam</a>	0.4
[L]	Police Service PKI Certificate Policies	<a href="http://www.npiaextranet.pnn.police.uk/microsite/fni/prog_info/iam">http://www.npiaextranet.pnn.police.uk/microsite/fni/prog_info/iam</a>	3.0
[M]	Police Service PKI Certificate Profiles	<a href="http://www.npiaextranet.pnn.police.uk/microsite/fni/prog_info/iam">http://www.npiaextranet.pnn.police.uk/microsite/fni/prog_info/iam</a>	0.8
[N]	Police Service PKI Naming Policy	<a href="http://www.npiaextranet.pnn.police.uk/microsite/fni/prog_info/iam">http://www.npiaextranet.pnn.police.uk/microsite/fni/prog_info/iam</a>	0.7
[O]	Police Service PKI Cryptographic Algorithms Policy	<a href="http://www.npiaextranet.pnn.police.uk/microsite/fni/prog_info/iam">http://www.npiaextranet.pnn.police.uk/microsite/fni/prog_info/iam</a>	0.7
[P]	IAM Compliant Card-Edge Specification	<a href="http://www.npiaextranet.pnn.police.uk/microsite/fni/prog_info/iam">http://www.npiaextranet.pnn.police.uk/microsite/fni/prog_info/iam</a>	1.2
[Q]	IAM Smart Card Standard	<a href="http://www.npiaextranet.pnn.police.uk/microsite/fni/prog_info/iam">http://www.npiaextranet.pnn.police.uk/microsite/fni/prog_info/iam</a>	1.1
[R]	Unique Identifier Standard (UNI) Standard	<a href="http://www.npiaextranet.pnn.police.uk/microsite/fni/prog_info/iam">http://www.npiaextranet.pnn.police.uk/microsite/fni/prog_info/iam</a>	1.0
[S]	NPIA Protective Monitoring Guidance	<a href="http://www.npiaextranet.pnn.police.uk/microsite/polwarp/index.htm">http://www.npiaextranet.pnn.police.uk/microsite/polwarp/index.htm</a> (Registration Required)	1.1

## 2 Definitions

The following table defines the terms used in this document.

Term	Definition
IAM Organisation	Any Police Force or Partner Organisation which uses IAM Central Services.
National Applications	Any "National" level applications which utilise one or more elements of IAM.
Code of Connection	<p>The IAM Code of Connection (CoCo) is a statement of the security standards that IAM Organisations must meet in order to connect to, and remain connected to the IAM Central Services.</p> <p>The primary purpose of the CoCo is to safeguard the operations on the Police Infrastructure and the organisations that are connected to it.</p> <p>Organisations wishing to connect to the IAM Central Services must prove that they have taken adequate steps to protect the Police Infrastructure and the information carried over it.</p>
Police Root CA	Police Service PKI Root Certificate Authority
xCJX	Criminal Justice eXtranet with Impact Level 4 capability.

## 3 Introduction

### 3.1 Background

- 3.1.1 The NPIA Identity and Access Management (IAM) programme applies a common, UK-wide, standards-based approach to identification, authentication, authorisation and access control services concerning Information Communications Technology (ICT) systems based in Police Forces and other authorised criminal justice partners.
- 3.1.2 The IAM Programme will deliver the central infrastructure and services to support the implementation of IAM for UK Police Service National Applications. It will also provide interfaces to enable the IAM Organisations to achieve a higher level of security when sharing data and gaining access to applications. The IAM programme addresses a growing need to provide strong assurance of digital identities and appropriate authority across the IAM Organisations, which will lead to enhanced information and intelligence sharing between such organisations.

### 3.2 Purpose

- 3.2.1 The purpose of this document is to describe the Code of Connection for the IAM Organisations which will connect to and utilise IAM Central Services.
- 3.2.2 The IAM Code of Connection defines the minimal standards to be adopted and maintained by all organisations that wish to connect to IAM Central Services. It is based on standards and guidelines that are primarily concerned with the technical and security aspects of IAM integration at a local organisation level.

### 3.3 Scope

- 3.3.1 The IAM Code of Connection covers all IAM Organisations that use the IAM Central Services. It is relevant to all aspects of IAM at the local level including, for example, provision of authoritative data, security, personnel vetting and technical requirements.
- 3.3.2 The IAM Code of Connection does not cover any individual National Applications; compliance with additional Codes of Connection may be required for each National Application to which an IAM Organisation connects. Additional Codes of Connection will apply irrespective of how an IAM Organisation accesses them, such as via one or more IAM interfaces<sup>1</sup>. The Code of Connection for a National Application may specify additional requirements which exceed those described within this IAM Code of Connection.

---

<sup>1</sup>



3.3.3 For the purpose of explicit clarity, compliance with the IAM Code of Connection must not be construed as compliance with any other Code of Connection or taken as implied permission to connect to any National Application, Network or other systems.

3.3.4 [Redacted]

**3.4 Assumptions and Dependencies**

3.4.1 [Redacted]

3.4.2 IAM Organisations must follow all appropriate HMG Information Assurance standards and undergo usual Information Assurance accreditation by their Local Accreditor. An implementation of IAM may require re-accreditation by the Local Accreditor of local infrastructure where an enterprise deployment has an impact on local authentication, authorisation, privilege management and access to applications.

3.4.3 This Code of Connection does not assume any particular type of network media or transport. It applies equally to all connectivity between IAM Organisations' local systems and the IAM Central Services, whether such connectivity is achieved through wired, wireless or by any other method yet to be invented.

3.4.4 This Code of Connection assumes that the IAM Organisation will comply with any relevant national policing policies, national/EU/international legislation, ACPO mandates, changes to underlying Codes of Connection or other requirements as may be published.

3.4.5 [Redacted]

3.4.6 An assumption has been made that all IAM Organisations will have a Local Accreditor, Information Security Officer and Senior Information Risk Owner (or equivalent roles).

**3.5 Future Development**

3.5.1 [Redacted]

## 4 Compliance Governance

### 4.1 Governance

4.1.1 The primary accreditation authority is the Police National Accrerator, who under the authority of the Police Information Assurance Board (PIAB) and ACPO IMBA will be responsible for approval of audit compliance aspects of the IAM Code of Connection.

4.1.2



### 4.2 Statement of Applicability

4.2.1 This Code of Connection will be applicable to any IAM Organisation as defined in the Definitions section.

4.2.2 This Code of Connection will apply to all separate IAM Organisations engaging with IAM, whether directly or indirectly (including but not limited to, mediated via a third party or regional grouping). An example of this is any IAM Organisation which has its connection to IAM brokered via a third party supplier (e.g. via the IAM Framework Managed Service) or via a single Regional Police Force. Each IAM Organisation, irrespective of brokerage or connection mediation, must sign up to this IAM Code of Connection on an individual basis as there will be a local requirement to achieve Information Assurance and Multi-Factor Authentication Mechanism accreditation.

### 4.3 Accreditation Regime

4.3.1



### 4.4 Compliance Certificate

4.4.1 The "Application for IAM Compliance Certificate" (Appendix A) is to be completed and submitted along with all other materials as part of an IAM Organisation's IAM Code of Connection submission. This application is to be completed in full and **must** be signed by the Senior Information Risk Officer (SIRO) within the IAM Organisation. In addition, the "Application for IAM Compliance Certificate" **must** be counter-signed by the IAM Organisation's

local Information Security Officer (ISO), who will attest to the security compliance aspects. Following successful application, an IAM Compliance Certificate will be issued and will have a validity period of one calendar year.

#### **4.5 Annual Code of Connection Submission**

4.5.1 Application and evidential material shall be submitted to the Police National Accrerator at [REDACTED]. The Police National Accrerator will respond within 30 days. Each IAM Organisation must submit its application no earlier than 90 days, and at least 30 days, before the expiry date of the (previous) IAM Code of Connection Certificate.

4.5.2 All queries relating to the IAM Code of Connection should be directed to the Identity and Access Management ("IAM") single point of contact (SPoC) in the first instance at [REDACTED].

#### **4.6 Non-Compliance**

4.6.1 IAM Organisations **must** meet the requirements stipulated in this Code of Connection at both initial connection and thereafter in order to maintain ongoing connectivity to the National IAM. Should an IAM Organisation make any change which might have an impact on its compliance with these requirements, then that IAM Organisation will be subject to immediate re-certification to validate that the requirements continue to be met. Changes must also be reflected in appropriately updated RMADS documentation.

4.6.2 Should the Police National Accrerator deem that an IAM Organisation is no longer meeting the requirements of this Code of Connection, the issue shall be escalated through the appropriate channels and require that immediate action be taken to bring the IAM Organisation back into compliance. Failure to comply will result in sanctions, potentially including disconnection from IAM Central Services and consequently from those applications or services which rely upon them.

---

## 5 Code of Connection

### 5.1 Overview

The following section describes the requirements to be met by an IAM Organisation before connection to IAM. Requirements are grouped by subject area or IAM component.

### 5.2 ACPO/ACPOS Compliance

#### 5.2.1 Background

Each IAM Organisation is required to achieve compliance with all relevant ACPO/ACPOS policies. At the time of writing, there are two ACPO/ACPOS policies which must be complied with, namely the National Vetting Policy [Ref E] and Community Security Policy [Ref F]. These policies should be available from the local Accreditor, for Non-ACPO/ACPOS governed IAM Organisations these policies could be supplied on application to the Police National Accreditor.

#### 5.2.2 Note for Non-ACPO/ACPOS Governed IAM Organisations

For IAM Organisations outside of ACPO/ACPOS authority (for example, non-Police organisations participating in IAM), those IAM Organisations are required to demonstrate (with documented evidence) that equivalent controls **meet or exceed** the requirements stipulated by ACPO/ACPOS. The final decision on the suitability and admissibility of equivalent controls is to be made by the Police National Accreditor.

#### 5.2.3 ACPO National Vetting Policy

All IAM Organisations are required to have achieved compliance with the ACPO National Vetting Policy. As part of the IAM Code of Connection submission, the IAM Organisation **must** provide documentation proving compliance with the ACPO National Vetting Policy (for example, a check on the ACPO/ACPOS CSP compliance matrix at the corresponding criteria).

#### 5.2.4 ACPO/ACPOS Community Security Policy

All IAM Organisations are required to have achieved compliance with both mandatory controls and non-mandatory controls at the level as specified in the ACPO/ACPOS Community Security Policy. As part of the IAM Code of Connection submission, the IAM Organisation **must** provide documentation proving compliance with the ACPO/ACPOS Community Security Policy.

### 5.3 Identity Verification and Personnel Vetting

#### 5.3.1 Background



[REDACTED]

5.3.2 Universal IAM Identity and Vetting Requirement

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

**5.4 Local Governance and Accreditation**

5.4.1 Background

Each IAM Organisation is required to implement suitable local governance structures and undertake its usual information assurance accreditation.

5.4.2 Local IAM Management Authority

[REDACTED]

5.4.3 Risk Management Accreditation Document Set (RMADS)

As with any system handling protectively marked information, there is a requirement to produce and approve a Risk Management Accreditation Document Set (RMADS) prior to live operation. The RMADS must conform to HMG Security Policy in accordance with HMG Information Assurance Standard Number 2, and must include a full risk assessment in accordance with HMG Information Assurance Standard 1. This documentation must include the local IAM Design, Network, Physical and Logical connection to

the IAM Central Services. The IAM RMADS **must** be submitted as part of the IAM Code of Connection submission. It is acceptable that this requirement is met by the provision of an RMADS which has a wider scope than just IAM, as long as the RMADS includes the requirements listed above.

5.4.4 Multi-Factor Authentication Mechanism Accreditation

In addition to Information Assurance accreditation, each IAM Organisation will be required to demonstrate (with evidence) that it has a sufficient level of assurance surrounding the complete lifecycle of digital identities, from initial registration through to revocation/termination. Specific requirements are stipulated based on the Multi-Factor Authentication Mechanism in question, and these are detailed in the relevant section of this document.

**5.5 Local Implementation**

5.5.1 Multi-Factor Authentication Mechanism

[Redacted]

5.5.2 Authoritative Data Source

Each IAM Organisation is required to establish and maintain an Authoritative Data Source (ADS) which delivers "a single source of truth" for user identities on which its IAM implementation can rely.

[Redacted]

[Redacted]

[Redacted]

5.5.3 General IAM Standards/Policies/Procedures/Guidelines

[Redacted]

[Redacted]

[Redacted]

5.5.4 Frequency of Data Feed to IAM Central Services

Each IAM Organisation is expected to feed its relevant IAM data (including, but not limited to, identity and privilege data) into IAM Central Services with a frequency to reflect their local business needs and also that of appropriate Service Level Agreements (SLAs).

5.5.5 Security Auditing / Protective Monitoring

Each IAM Organisation is required to update its protective monitoring capabilities to accommodate and reflect the auditing needs of handling material [REDACTED]

[REDACTED] Each IAM Organisation must ensure that its local retention and security of audit data is compliant with relevant legislation and ACPO policies. Details about an IAM Organisation's Protective Monitoring capabilities **must** appear in the appropriate RMADS.

5.5.6 Disaster Recovery and Business Continuity

Each IAM Organisation is required to implement an appropriate combination of technical, environmental, personnel and procedural controls to ensure that their local IAM implementation will deliver a suitably robust and reliable IAM service. For IAM Organisations integrating IAM into their wider enterprise architecture, this will be of particular importance. IAM Organisations should ensure that they include their IAM capabilities within standard continuity preparations and those plans are tested and documented, updating any Service Level Agreement (SLA) as necessary. IAM Organisations should include information on how resilience and continuity is to be achieved for their local IAM implementation as part of their IAM Code of Connection submission.

5.5.7 Physical Security

Each IAM Organisation is required to deploy appropriate physical security controls to secure systems and environments to the necessary levels.

[REDACTED]

[REDACTED] **d xCJX Connectivity**

5.6.1 Each IAM Organisation must have membership of, and accredited connection to, both CJX and xCJX. The IAM Organisation **must** submit its accreditation certificate for CJX and xCJX connectivity as part of the IAM Code of Connection submission. [REDACTED]

**5.7 Confidentiality Impact Level 3 (RESTRICTED)**

5.7.1

[Redacted]

**5.8 Confidentiality Impact Level 4 (CONFIDENTIAL)**

5.8.1

[Redacted]

5.8.2

[Redacted]

5.8.3

[Redacted]

5.8.4

[Redacted]



**5.9 Multi Factor Authentication: PKI/Smart Card**

5.9.1 Background

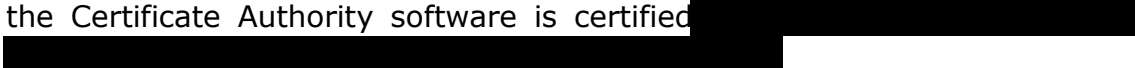
It is envisaged that most IAM Organisations will utilise a Public Key Infrastructure (PKI) that is integrated with a smart card solution to provide a high assurance authentication credential to their user populations.

5.9.2 PKI Participants Register



5.9.3 Certificate Authority (CA)

IAM Organisations deploying their own Certificate Authority (CA), whether locally in their enterprise or through a managed service, must ensure that the Certificate Authority software is certified

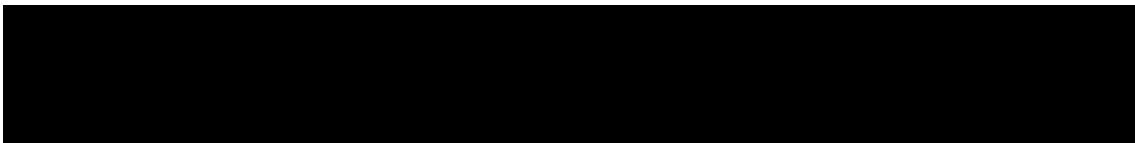


5.9.4



- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

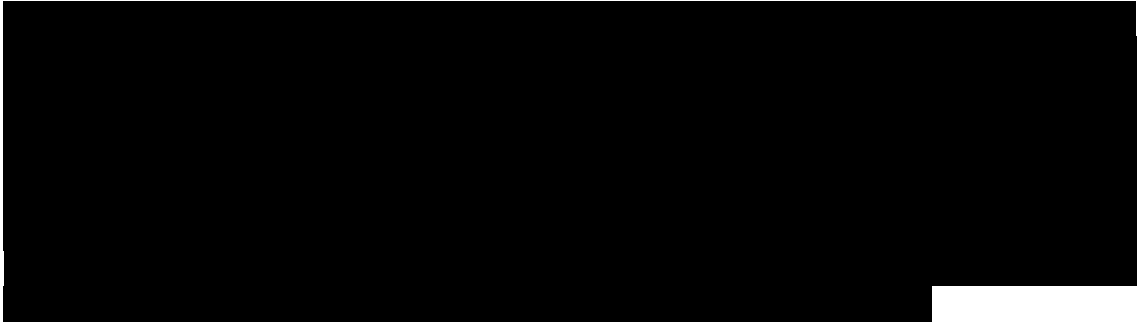
5.9.5





**5.10 Single Factor Authentication: Username and Password**

5.10.1 Requirements for Username and Password Authentication



# Appendix A – Application for IAM Compliance Certificate

Name of IAM Organisation: \_\_\_\_\_

Application Date: \_\_\_\_\_

***This application covers one calendar year only, from the date shown above.***

1. I, on behalf of the IAM Organisation named above (“my organisation”) that I represent, accept and understand both the requirements and statements as defined within this IAM Code of Connection. My organisation will adhere to these standards at all times, and maintain appropriate documented evidence of compliance which will be made available to the Police National Accrerator on request.
2. I accept responsibility for the security of all aspects of all elements which comprise my organisation’s local implementation of IAM. I certify that appropriate, accredited capabilities exist to support IAM usage up to and including Impact Level 4 for Confidentiality (CONFIDENTIAL).
3. It is fully understood and accepted that my organisation’s connection to the IAM Central Services may be subject to sanctions (up to and including suspension) if the Managing Authority is not satisfied that my organisation is adhering to the Code of Connection (and does not have an agreed waiver granted by the Authority to cover any such gaps as may be identified from time-to-time).

Signed on behalf of the connecting IAM Organisation: \_\_\_\_\_

*Senior Information Risk Owner (SIRO)*

Print Name: \_\_\_\_\_

Role / Position: \_\_\_\_\_

Date: \_\_\_\_\_

Countersigned by IAM Organisation Local Accrerator: \_\_\_\_\_

Print Name: \_\_\_\_\_

Date: \_\_\_\_\_

## Appendix B - Compliance Checklist

The following summarises the evidence required on submission of the IAM Code of Connection application. Please refer to the policy text for full details.

	Subject Area	Policy / Compliance	Evidence	IAM CoCo Ref	Note(s)
1	ACPO/ACPOS Compliance	ACPO National Vetting Policy	Documentation proving compliance	5.2	Non-ACPO(S) Governed IAM Organisations refer to section 5.2.2
2	ACPO/ACPOS Compliance	ACPO/ACPOS Community Security Policy	Documentation proving compliance	5.2	See above
3	Local Governance and Accreditation	Local IAM Management Authority	Documentation of formation and duties of the Local IAM Management Authority	5.4	
4	Local Governance and Accreditation	Risk Management Accreditation Document Set (RMADS)	The IAM RMADS	5.4	Specific areas to be included in the RMADS are detailed in section 5.5
5	CJX and xCJX Connectivity	CJX and xCJX Connectivity	Accreditation certificates for CJX and xCJX	5.6	No xCJX Certificate required for IAM Organisations only using IL3
6	Confidentiality Impact Level 3 (IL3) (RESTRICTED)	Confidentiality Impact Level 3	Accreditation certificate for the local IL3 environment	5.7	
7	Confidentiality Impact Level 4 (IL4) (CONFIDENTIAL)	Confidentiality Impact Level 4	Documentation on evidence of compliance with the policy defined within the PND CoCo	5.8	May be formal accreditation certificate for IL4 environment
8	Multi Factor Authentication: PKI/Smart Card	"tScheme for Police"	PKI accreditation as described in the Police Service PKI Compliance Policy	5.9	Required for all IAM Organisations participating in the Police Service PKI

## Appendix C – Glossary of Terms

The following defined terms are referred to in this document:

Term	Definition
ACPO/ACPOS	Association of Chief Police Officers / Association of Chief Police Officers in Scotland
Certificate	A data record produced by a CA that, at a minimum: identifies the CA issuing it, names or otherwise identifies its subscriber and subject, contains a public key that corresponds to a private key under the control of the subscriber, identifies its validity period, contains a serial number and is digitally signed by the CA.
Certification Authority (CA)	An organisation trusted and authorised by the P3MA (indicated by the issue of a CA certificate to the authority concerned by the Police Service PKI Root Authority) to issue and manage X.509 Public Key Certificates and ARLs or CRLs within the Police Service PKI.
CESG	Communications-Electronics Security Group, is the UK Government's National Technical Authority for Information Assurance, responsible for enabling secure and trusted knowledge sharing.
CONFIDENTIAL	A Government Protective Marking Scheme classification, as defined in HMG Security Policy.
Digital Signature	The result of the transformation of a message by means of a cryptographic system using private/public key pairs and certificates such that the recipient of the message and signature can determine: (1) whether the transformation was created using the private key which complements the public key in the certificate; and (2) whether the message has been altered since the transformation was made.
Entity	An autonomous element within the PKI. This may be a CA, RA, Subscriber, Subject, Relying Party, Representative, Device or other system component.
P3MA	Police PKI Policy Management Authority
PIAB	Police Information Assurance Board
Private Key	The secret key which complements the key identified in the certificate (the public key).
Public Key	The revealed part of an asymmetric key pair, as used to verify a digital signature or encrypt a message. The public key is made freely available to anyone who will receive digitally signed messages from the holder of the key pair. Certificates issued in the Police Service PKI contain the subject's public key.
Public Key Infrastructure (PKI)	One or more Certification and Registration Authorities and associated systems, accompanied by a set of controls and standards governing their management, to ensure recognition and interoperability of digital certificates.
RESTRICTED	A Government Protective Marking Scheme classification, as defined in HMG Security Policy.
RMADS	Risk Management Accreditation Document Set
X.509	A public key certificate specification developed as part of the X.500 directory specification, often used in public key systems.

## Control Page

### Distribution list

Recipient	Title	Location
IAM team		NKBH

### Change control

Version	Date	Authority	Evidence of approval	Record of change
0.1	3 Mar 2009			First draft for IAM team review.
0.2	13 Mar 2009			Updated following comments from IAM team.
0.3	17 Mar 2009			Further development on the Compliance Matrix.
0.4, 0.5	26 Mar 2009			Updated following comments from IAM team.
0.6	30 Mar 2009			■ - Changes to include comments from the National Accreditor
0.9	01 June 2009			■ - Rework document structure for clarity
0.9d	15 June 2009			■ - Draft for NPIA internal review
0.9e	28 July 2009			Updated following comments from quality review of 9d and workshop part I.
0.9g	17 Sep 2009			Updated following comments from IAM Workshop Part II.
0.9h	28 Oct 2009			■ - Some resolved issues & "low" updates from previous QRF round
0.9i	05 Nov 2009			■ - Changes to reflect resolved issues
0.9j	09 Nov 2009			■ - Final set of changes from CQRF round before v1.0 approval
1.0	11 Nov 2009	■■■■■■■■	E-Mail Trail & Signatures	■ - Move document to 1.0