Document Name	**tScheme for Police Assessment Procedures**
File Name	tScheme for Police Assessment Procedures-v1_0.doc
Version	1.0
Date	7 June 2010
Author	Chris Harrison (mailto:chris.harrison@npia.pnn.police.uk)

Authorisation	P3MA & tScheme Board
Signed version held by	P3MA Secretariat

© NPIA (National Policing Improvement Agency) 2010

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 the National Policing Improvement Agency or its representative.

Table of Contents

REFERENCE DOCUMENTS **4**

1 INTRODUCTION **5**

1.1 PURPOSE 5

1.2 SCOPE 5

1.3 AUDIENCE 5

1.4 STATUS 6

1.5 DOCUMENT ADMINISTRATION 6

2 OVERVIEW **7**

2.1 POLICE SERVICE PKI 7

2.2 CERTIFICATE POLICY COMPLIANCE 7

2.3 TSCHEME FOR POLICE 7

3 POLICE SERVICE PKI SERVICE DEFINITIONS **9**

3.1 OVERVIEW 9

3.2 CERTIFICATION AUTHORITY (CA) SERVICE DEFINITION 9

3.3 REGISTRATION AUTHORITY (RA) SERVICE DEFINITION 9

3.4 APPROVAL PROFILE APPLICABILITY 10

3.5 APPROVAL PROFILES AND THE POLICE SERVICE PKI CERTIFICATE POLICIES 10

4 REGISTERING FOR AN ASSESSMENT **11**

4.1 OVERVIEW 11

4.2 REGISTRATION PROCEDURE 11

4.3 ADDITIONAL READING REQUIRED 11

4.4 RESOURCES 12

5 CONTRACTING FOR AN ASSESSMENT **13**

5.1 OVERVIEW 13

5.2 ADDITIONAL READING REQUIRED 13

5.3 RESOURCES 13

6 PERFORMANCE OF ASSESSMENTS **14**

6.1 OVERVIEW 14

6.2 ASSESSMENT SCHEDULE 14

6.3 STAGE I ASSESSMENT 14

6.4 WITNESSING OF KEY-SIGNING CEREMONY 15

6.5 STAGE II ASSESSMENT 15

6.6 ADDITIONAL READING REQUIRED 16

6.7 RESOURCES 16

7 APPLYING FOR APPROVAL 17

7.1 OVERVIEW 17

7.2 APPROVAL PROCEDURE 17

7.3 ADDITIONAL READING REQUIRED 17

7.4 RESOURCES 18

8 ONGOING GOOD CONDUCT 19

8.1 OVERVIEW 19

8.2 ONGOING ASSESSMENT PROCEDURE 19

8.3 ADDITIONAL READING REQUIRED 20

9 CONTROL PAGE 21

A TSCHEME FOR POLICE ASSESSMENT PROCESS 22

B SCHEDULE OF FEES 23

B.1 FEES FOR *TSCHEME FOR POLICE* ASSESSMENTS 23

Reference Documents

Ref	Description	Document reference	Revision
A.	Police Service PKI Certificate Policies	n/a	Latest version
B.	tScheme Required Reference Procedures	tSd 0244	Issue 1.01 (2004-08-26)
C.	Police Service PKI Compliance Policy	n/a	Latest version
D.	Business Process for Obtaining Certification from the Police Service PKI Root Issuing Authority	Business Process for Obtaining Certification from Police Root-v0_2.doc	Latest version
E.	tScheme for Police Applicant Letter	tSi0282_0-01	-
F.	tScheme for Police Submission Letter	tSi0283_0-01	-
G.	Model tScheme for Police Assessment Report	tSd0287_0-01	-
H.	Model tScheme for Police S3A	n/a	Latest version

1 Introduction

1.1 Purpose

1.1.1 This document describes the procedures for tScheme assessment of UK Police bodies participating in the Police Service PKI, in compliance with the Police Service PKI Certificate Policies (CP) [REF A].

1.1.2 The purpose of the document is to act as a supplement to existing tScheme procedures, describing the specifics of the *tScheme for Police* assessment model.

1.2 Scope

1.2.1 The scope of the document is to define the tScheme assessment procedures for Police bodies participating in the Police Service PKI. These procedures are based on the existing tScheme Required Assessment Procedures [REF B].

1.2.2 This document summarises the applicable sections of the Required Assessment Procedures [REF B] and details the variations specific to the Police Service PKI.

1.2.3 Note that this document does not replace the existing tScheme documentation, which it must be read in conjunction with.

1.3 Audience

1.3.1 This document is required reading for all those involved in *tScheme for Police* assessments. These are:

- tScheme-recognised Assessors (who perform *tScheme for Police* assessments);
- Police Bodies entitled to operate Certification Authorities and Registration Authorities as defined in the Police Service PKI Certificate Policies [REF A]);
- tScheme representatives (who are responsible for the operation of the scheme and the continued application and maintenance of these, and other, procedures);
- The Police PKI Policy Management Authority (who are responsible for the operation of the Police Service PKI and the compliance of participating Trust Service Providers with its Certificate Policies).

1.3.2 Note that the *tScheme for Police* assessment procedure is only applicable to UK Police bodies. *tScheme for Police* eligibility criteria are further defined in section 3.

1.4 Status

1.4.1 This is the fourth draft of *tScheme for Police Assessment Procedures* for review by Richard Trevorah (tScheme Technical Director), Phil Willoughby (LRQA) and Simon Langley (KPMG).

1.5 Document Administration

1.5.1 Ownership

1.3.1.1 This document is jointly owned and authorised by tScheme and the Police PKI Policy Management Authority (P3MA).

1.5.2 Monitoring and Review

1.3.1.2 This document will be reviewed on an annual basis, as a minimum.

1.5.3 Contact Information

1.3.1.3 Comments and questions regarding this document should be directed to the P3MA single point of contact (SPoC).

1.3.1.4 P3MA SPoC Email: p3ma@npia.pnn.police.uk

2 Overview

2.1 Police Service PKI

2.1.1 The Police Service Public Key Infrastructure (PKI) has been implemented primarily to support the National Policing Improvement Agency (NPIA) Identity and Access Management (IAM) programme by enabling the issuance of high-assurance digital credentials for users, devices, applications and services.

2.1.2 The Police Service PKI is governed by the Police PKI Policy Management Authority (P3MA), which sets the standard for the Police Service PKI by defining, managing and enforcing policy. This is achieved by implementing the Police Service PKI Certificate Policies [REF A].

2.1.3 The Police Service PKI Certificate Policies accommodate participating organisations operating either as a Certification Authority (CA) or a Registration Authority (RA). The service types and their eligibility for tScheme for Police are defined in section 3 of this document.

2.2 Certificate Policy Compliance

2.2.1 It is the P3MA's responsibility is to ensure that there is a consistent and appropriate level of trust in the Police Service PKI and all certificates issued by participating organisations, ensuring that only authorised individuals have access to sensitive data. The P3MA define and publish compliance and audit requirements for participating organisations in the Police Service PKI Compliance Policy [REF C].

2.2.2 The P3MA require that Police Service PKI Certification Authorities (CAs) and Registration Authorities (RAs) undergo independent tScheme assessment to assure the robustness of the organisations' security services and the integrity and rigour of their management and operation. The assessment provides a basis for trust of digital identities across the police service.

2.2.3 Organisations operating as self-contained CAs or independent RAs are eligible for tScheme assessments with a limited scope. This assessment model is termed *tScheme for Police*.

2.3 tScheme for Police

2.3.1 The scope of *tScheme for Police* assessments is an organisation's compliance with the Police Service PKI Certificate Policies [REF A]. This is achieved by leveraging the standard tScheme procedures and Approval Profiles as the assessment mechanism.

2.3.2 The compliance assessment will not cover wider security issues such as full compliance with the ISO 27001:2005 international standard for security, therefore the tScheme Base Approval Profile will be excluded from *tScheme for Police* assessments.

2.3.3 Police Forces of England, Wales, Northern Ireland and Scotland are mandated by the Association of Chief Police Officers (ACPO) and the Association of Chief Police Officers in Scotland (ACPOS) to attain compliance with the ACPO Community Security Policy (CSP), as determined by the ACPO Police Information Assurance Board (PIAB), by establishing an information security management framework based on ISO/IEC 27002 Code of Practice for Information Security, the HMG Security Policy Framework, the Government Protective Marking Scheme and CESG Information Security Standards and Guidance.

2.3.4 The combination of the ACPO CSP initiative and the requirement for external tScheme assessment of Police Service PKI services shall provide sufficient evidence to the P3MA and Police bodies that PKI digital identities may be trusted within the Police community.

2.3.5 tScheme is an internationally recognised assessment standard which will provide an independent assessment of Police Service PKI participants. This will allow relying parties and trust service providers, both internal and external to the Police community, to make informed decisions as to the level of identity assurance provided by Police Service PKI identities.

2.3.6 To clarify to Trust Service Providers and relying parties outside of the Police Service PKI that participating services have not undergone a full tScheme assessment, the term *tScheme for Police* shall be adopted.

2.3.7 *tScheme for Police* represents an assessment in accordance with rigorous tScheme standards, but with a limited scope and as such is considered a lower level of assurance.

3 Police Service PKI Service Definitions

3.1 Overview

3.1.1 The Police Service PKI consists of a number of Certification Authorities (CAs) and Registration Authorities (RAs), amongst other components. These components work in collaboration with each other to deliver a viable and trustworthy environment for managing digital certificates.

3.1.2 This Section 3 defines the CA and RA service types in the context of tScheme for Police, the eligibility criteria for assessment and the applicable tScheme Approval Profiles for each service type.

3.2 Certification Authority (CA) Service Definition

3.2.1 Organisations eligible to operate as Certification Authorities are defined in the Police Service PKI Certificate Policies [REF A].

3.2.2 An organisation operating a CA is also assumed to be providing RA and certificate status validation services and shall be assessed accordingly.

3.2.3 A CA service provider is considered eligible for *tScheme for Police* assessment as a CA if all CA and RA services are performed by the CA organisation. This does not preclude the CA providing services to external organisations if all RA functions and responsibilities are performed by the CA organisation.

3.2.4 In cases where a CA is providing services to one or more external organisations acting as RAs, the CA service provider is not eligible for *tScheme for Police* and must undergo a standard tScheme assessment in accordance with [REF B].

3.2.5 In cases where CA organisations are operating additional trust services outside of the jurisdiction of the P3MA and the Police Service PKI Certificate Policies (e.g. issuing certificates under local policies), these additional services may not necessarily be subject to inclusion within the scope of the *tScheme for Police* assessment. It shall be at the discretion of the independent tScheme assessor to determine whether any additional trust services operated by the CA affect the integrity of services operated as part of the Police Service PKI. Local CA services are not precluded from *tScheme for Police* assessment, should an organisation wish to extend the scope of their own assessment.

3.3 Registration Authority (RA) Service Definition

3.3.1 Organisations eligible to operate as Registration Authorities are defined in the Police Service PKI Certificate Policies [REF A].

3.3.2 Organisations operating as Registration Authorities shall be subject to assessment against the Approval Profiles identified below.

3.3.3 Organisations operating independent RAs subscribing to a governing CA must complete the full *tScheme for Police* assessment procedure as defined in sections 4 - 8.

3.4 Approval Profile Applicability

3.4.1 *tScheme for Police* applicants shall be assessed against the following tScheme Approval Profiles:

Approval Profile	**CA**	**RA**
Approval Profile for Registration	✓	✓
Approval Profile for a Certification Authority	✓	
Approval Profile for Certificate Generation	✓	
Approval Profile for Certificate Dissemination	✓	
Approval Profile for Certificate Status Management	✓	
Approval Profile for Certificate Status Validation	✓	

3.5 Approval Profiles and the Police Service PKI Certificate Policies

3.5.1 The clauses contained within the tScheme Approval Profiles are designed to cover a broad range of trust services and as such do not correlate in entirety to the requirements of the Police Service PKI Certificate Policies (CP) [REF A]; however, the tScheme Approval Profiles do represent a recognised methodology for assessing trust services to high quality standards and to a high degree of rigour.

3.5.2 In addition to the specific clauses set out in the tScheme Approval Profiles, organisations are required to comply with all sections of the Police Service PKI Certificate Policies relevant to the service they are operating, and should be prepared to be assessed accordingly. Compliance with the Police Service PKI CP shall be a mandatory declaration included in all *tScheme for Police* applicants' Statement of Services Subject to Assessment (S3A).

3.5.3 tScheme Approval Profile clauses specific to Qualified Certificates are not applicable to *tScheme for Police* Assessments.

4 Registering for an Assessment

4.1 Overview

4.1.1 Registration for a tScheme for Police assessment is has been tailored to meet the specific requirements of tScheme, the P3MA and participating Police bodies.

4.1.2 The standard tScheme procedure of an organisation requesting Registered Applicant status and agreeing the associated terms and conditions is substituted in the case of *tScheme for Police* with a single letter of application from the applicant organisation to tScheme.

4.1.3 All eligible CAs and RAs are required to follow the registration procedure below.

4.2 Registration Procedure

4.2.1 Organisations must first select a tScheme-recognised assessor prior to registering with tScheme. The list of recognised assessors is maintained at www.tscheme.org.

4.2.2 Prior to registering with tScheme, organisations shall complete an Outline Statement of Services Subject to Assessment (S3A) document, in accordance with the Model tScheme for Police Outline S3A [REF H].

4.2.3 Organisations shall submit to tScheme Limited their completed Outline S3A together with a completed tScheme for Police Applicant Letter [REF E].

4.2.4 tScheme will communicate receipt of tScheme for Police applications to the P3MA, as appropriate.

4.2.5 Registrations of individual organisations for *tScheme for Police* will not be published via the tScheme website.

4.2.6 The Business Process for Obtaining Certification from the Police Service PKI Root Issuing Authority [REF D] document provides further information as to when tScheme registration should be submitted in relation to the overall process of joining the Police Service PKI.

4.3 Additional Reading Required

4.3.1 The following additional documents should be read in conjunction with this document when registering for a tScheme for Police assessment:

- Police Service PKI Compliance Policy [REF C]

- Business Process for Obtaining Certification from the Police Service PKI Root Issuing Authority [REF D]
- tScheme Required Assessment Procedures [REF B]

4.4 Resources

4.4.1 *tScheme for Police* applicants are required to use the following resources when preparing for registration:

- tScheme for Police Applicant Letter [REF E]
- Model tScheme for Police Outline S3A [REF H]

5 Contracting for an Assessment

5.1 Overview

5.1.1 *tScheme for Police* applicants shall form a contractual agreement with a tScheme-recognised assessor for the independent assessment of their defined trust services.

5.1.2 Contracts for assessment are solely between the applicant organisation and their selected tScheme assessor and are independent of tScheme Limited and the P3MA.

5.1.3 All eligible CAs and RAs are required to contract directly with a tScheme-recognised assessor for the performance of a *tScheme for Police* assessment as described in section 6.

5.2 Additional Reading Required

5.2.1 The following additional documents should be read in conjunction with this document when registering for a tScheme for Police assessment:

- tScheme Required Assessment Procedures [REF B]

5.3 Resources

5.3.1 The list of tScheme-recognised assessors can be found at the following location:

http://www.tscheme.org/directory/assessors.html

6 Performance of Assessments

6.1 Overview

6.1.1 The performance of *tScheme for Police* assessment shall be carried out in accordance with standard tScheme procedures.

6.1.2 The scope and criteria for assessments are determined by the service description and approval profiles included as part of the S3A, the details of which are agreed between the applicant organisation and their chosen assessor.

6.2 Assessment Schedule

6.2.1 Based on assessment against a common Certificate Policy applicable to all *tScheme for Police* applicants, and the exclusion of the tScheme Base Approval Profile, the *tScheme for Police* assessment schedule shall be consolidated into two main stages:

- Stage I – Documentation Assessment
- Stage II – Objective Evidence Assessment

6.2.2 The Business Process for Obtaining Certification from the Police Service PKI Root Issuing Authority [REF D] document provides further information as to when stages of *tScheme for Police* assessment should be undertaken in relation to the overall process of joining the Police Service PKI.

6.3 Stage I Assessment

6.3.1 Applicant organisations shall undergo a tScheme for Police Stage I assessment prior to certification from the Police Service PKI Root CA, in order to provide the P3MA with an independent readiness assessment of the organisation's procedures and practices' compliance with the Police Service PKI Certificate Policies [REF A].

6.3.2 Stage I assessments shall cover the following documents:

- Statement of Services Subject to Assessment (S3A);
- Approval Profiles;
- Certification Practice Statement (CPS);
- RMADS;
- [Supporting Procedures and Practices];

- [Evidence of Authority].

6.3.3 Applicant organisations shall provide all of the above documentation in completed form to the assessor.

6.3.4 The assessor shall review the provided documentation and produce a Stage I assessment report. The time required to perform a Stage I *tScheme for Police* assessment shall be determined by the independent tScheme assessor. The duration of an assessment is dependent on the organisation under assessment's state of readiness and provision of the required document set and evidential records.

6.3.5 Where the assessment report identifies non-conformities, the applicant organisation and assessor shall determine an appropriate course of action to address any deficiencies.

6.3.6 On completion of a successful Stage I assessment, the applicant organisation shall send the assessment report to the P3MA as evidence or readiness for certificate signing. On approval of the P3MA the applicant organisation may progress with certificate signing as described in the Business Process for Obtaining Certification from the Police Service PKI Root Issuing Authority [REF D].

6.4 Witnessing of Key-Signing Ceremony

6.4.1 As part of the preparation for the CA certificate signing process, applicant organisations must arrange for a tScheme assessor, or an independent, demonstrably competent representative (e.g. a representative of the P3MA), to be present to witness the CA's key-signing ceremony in order to ensure suitably controlled conditions are in place and the defined procedures are followed.

6.4.2 A record of the key-signing ceremony, identifying the people involved, their roles and the outcome of the ceremony shall be maintained by the applicant organisation for the lifetime of the key.

6.5 Stage II Assessment

6.5.1 Following certification of the applicant organisation by the Police Service PKI Root CA, the organisation is required to undergo a tScheme objective evidence assessment.

6.5.2 The assessor shall review the objective evidence as required and produce a Stage II assessment report. The time required to perform a Stage II *tScheme for Police* assessment shall be determined by the independent tScheme assessor. The duration of an assessment is dependent on the organisation under assessment's state of readiness and provision of the required document set and evidential records.

6.5.3 Where the assessment report identifies non-conformities, the applicant organisation and assessor shall determine an appropriate course of action to address any deficiencies.

6.5.4 On completion of a successful Stage II assessment, the applicant organisation shall apply to tScheme for a grant of approval as described in Section 7.

6.6 Additional Reading Required

6.6.1 The following additional documents should be read in conjunction with this document when preparing for a tScheme for Police assessment:

- tScheme Required Assessment Procedures [REF B]
- Business Process for Obtaining Certification from the Police Service PKI Root Issuing Authority [REF D]

6.7 Resources

6.7.1 *tScheme for Police* applicants are required to use the following resources when preparing for an assessment:

- Model tScheme for Police S3A [REF H]

7 Applying for Approval

7.1 Overview

7.1.1 Application for *tScheme for Police* approval has been tailored to meet the specific requirements of tScheme, the P3MA and participating Police bodies.

7.1.2 The standard tScheme procedure of an organisation requesting tScheme Approved status and agreeing the associated terms and conditions is substituted in the case of *tScheme for Police* with a single letter of submission from the applicant organisation to tScheme, accompanied by the tScheme assessors final report and a purchase order for the registration fee.

7.2 Approval Procedure

7.2.1 Applications for *tScheme for Police* approval are only to be submitted to the tScheme board following the successful outcome of the Stage II assessment and receipt of the assessor's final report.

7.2.2 Organisations shall submit to tScheme Limited their assessor's final report together with a completed tScheme for Police Submission Letter [REF F] and a purchase order for the appropriate registration fee as per Appendix **Error! Reference source not found.**.

7.2.3 tScheme will communicate the status of tScheme for Police applications to the P3MA, as appropriate.

7.2.4 Approvals of individual organisations for *tScheme for Police* will not be published via the tScheme website.

7.2.5 The Business Process for Obtaining Certification from the Police Service PKI Root Issuing Authority [REF D] document provides further information as to when tScheme approval should be completed in relation to the overall process of joining the Police Service PKI.

7.3 Additional Reading Required

7.3.1 The following additional documents should be read in conjunction with this document when applying for a tScheme for Police grant:

- tScheme Required Assessment Procedures [REF B]
- Business Process for Obtaining Certification from the Police Service PKI Root Issuing Authority [REF D]

7.4 Resources

7.4.1 *tScheme for Police* applicants are required to use the following resources when applying for a tScheme for Police grant:

- tScheme for Police Submission Letter [REF F]

8 Ongoing Good Conduct

8.1 Overview

8.1.1 Following initial tScheme for Police approval, Police Service PKI CAs and RAs shall be subject to a full re-assessment every three years.

8.1.2 Between full tScheme for Police assessments, approved organisations shall be subject to an annual maintenance assessment.

8.2 Ongoing Assessment Procedure

8.2.1 Organisation shall contract with a tScheme-recognised assessor to conduct an interim assessment that shall take place no more than twelve months after the previous assessment.

8.2.2 The scope of the annual assessment will cover all controls from the applicable tScheme Profiles as determined by the tScheme Assessor.

8.2.3 The assessor shall review the evidence as required and produce an interim assessment report. The time required to perform an interim *tScheme for Police* assessment shall be determined by the independent tScheme assessor. The duration of an assessment is dependent on the organisation under assessment's state of readiness and provision of the required document set and evidential records..

8.2.4 Where the assessment report identifies non-conformities, the applicant organisation and assessor shall determine an appropriate course of action to address any deficiencies.

8.2.5 Organisations shall submit to tScheme Limited their assessor's interim assessment report together with a purchase order for the appropriate annual license fee[1] as per Appendix **Error! Reference source not found.**.

8.2.6 tScheme will communicate the status of tScheme for Police organisations to the P3MA, as appropriate.

8.2.7 Organisations shall undergo a full re-assessment, in accordance with the procedures described in this document, no more than three years after the previous full assessment.

[1] Note that following payment of the tScheme for Police fee on initial approval, organisations are only required to pay the annual license fee in subsequent years.

8.3 Additional Reading Required

8.3.1 The following additional documents should be read in conjunction with this document when registering for a tScheme for Police assessment:

- tScheme Required Assessment Procedures [REF B]

9 Control Page

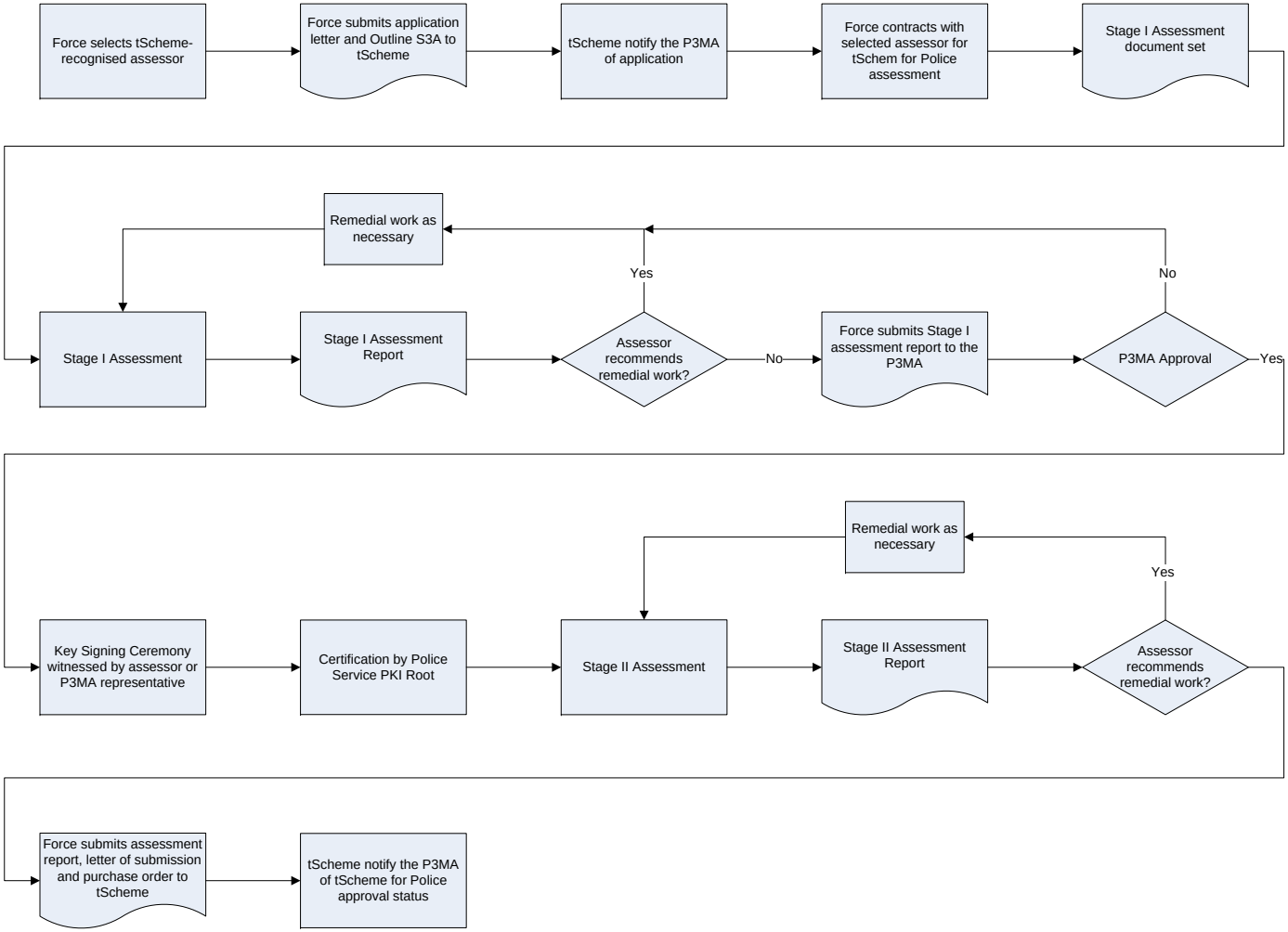
Distribution list

Recipient	Title	Location
Richard Trevorah	tScheme Technical Director	-
Simon Langley	KPMG Audit Plc tScheme Representative	-
Phil Willoughby	LRQA tScheme Representative	-
Graham Dunn	FNI Programme Manager	NKBH
Fraser Ross	Police PKI Assurance Group Chair	NKBH

Change control

Version	Date	Author	Authorisation	Record of change
0.1	21 Jan 10	Chris Harrison	n/a	Draft version prepared for discussion with PAG Chair and tScheme Technical Director.
0.2	02 Feb 10	Chris Harrison	n/a	Updated following meeting with tScheme Technical Director.
0.3	27 Apr 10	Chris Harrison	n/a	Updated following comments from tScheme assessors and IAM programme team.
0.4	7 June 10	Chris Harrison	n/a	Updated following further discussion with tScheme Technical Director and tScheme assessors.
1.0	01 July 10	Chris Harrison	Graham Dunn	Final baseline version for presentation to P3MA

A tScheme for Police Assessment Process



B Schedule of Fees

B.1 Fees for *tScheme for Police* Assessments

B.1.1 The following fees are set by an agreement between the National Policing Improvement Agency (NPIA), on behalf of the Police PKI Policy Management Authority (P3MA), and tScheme Limited solely for the purpose of the supporting the *tScheme for Police* process.

B.1.2 The fees relate only to Police Bodies and other organisations entitled to operate Certification Authorities and Registration Authorities as defined in the Police Service PKI Certificate Policies [REF A].

B.1.3 The fees stated represent reduction to the registration fees for full tScheme approvals on the basis that they do not include the Base Profile.

B.1.4 Note that these fees DO NOT include the cost of assessment, which must be agreed between the applicant organisation and their selected tScheme-recognised assessor.

Operating Model	**Initial License Fee**	**Annual License Fee**
Police Service PKI Certification Authority	£4,000	£2,000
Police Service PKI Registration Authority	£2,000	£1,000