

Authorised Operator TrustAssured Service Utility Certificate Policy

Version 4.0

IMPORTANT NOTE ABOUT THIS DOCUMENT

The information contained herein is the property of The Royal Bank of Scotland plc and may not be copied, used or disclosed in whole or in part except with the prior written permission of The Royal Bank of Scotland plc.

This document is controlled and managed under the authority of The Royal Bank of Scotland Policy Approval Authority (PAA).

© The Royal Bank of Scotland plc 2000 – 2006

All Rights Reserved

Contact

The Royal Bank of Scotland plc
TrustAssured
5th Floor
2 Waterhouse Square
138-142 Holborn
London EC1N 2TH
United Kingdom
Tel no: +44 (0) 207 427 9355
Fax no: +44 (0) 207 427 8342
09:00 – 17:00 Monday to Friday (excluding English Public Holidays)

Related Documentation

Reference No.	Title:	Author:	Version & Date
	Business Customer Agreement for the TrustAssured Service	Simon Hobby	3.5 or later

Table of Contents

1. POLICY OUTLINE	3
1.1. Community & Applicability	3
1.2. Contact Details.....	3
2. CP PROVISIONS	4
2.1. Obligations.....	4
2.2. Liability	4
2.3. Interpretation & Enforcement	4
2.4. Publication & Repository.....	5
2.5. Confidentiality	5
2.5.1. Types of Information to be Kept Confidential	5
2.5.2. Types of Information Not Considered Confidential	5
3. IDENTIFICATION & AUTHENTICATION	6
3.1. Initial Registration	6
3.1.1. Uniqueness of Names	6
3.1.2. Authentication of Business Customer Identity	6
3.1.3. Routine Rekey.....	6
3.1.4. Rekey after Revocation.....	6
4. OPERATIONAL REQUIREMENTS	6
4.1. Certificate Application, Issuance & Acceptance	6
4.2. Certificate Suspension & Revocation.....	6
4.2.1. Circumstances for Certificate Revocation/Suspension	6
4.2.2. Procedure for Suspension or Revocation Request.....	7
4.2.3. Certificate Re-activation	7
4.2.4. Suspension Period Limitations.....	7
4.2.5. On-line Revocation Checking Requirements	7
5. TECHNICAL SECURITY CONTROLS	8
5.1. Key Pair Generation and Installation	8
5.2. Private Key Protection	8
5.2.1. Private Key Escrow, Backup and Archiving	8
5.2.2. Activation Codes.....	8
5.3. Certificate Profiles	8
6. POLICY SPECIFICATION AND ADMINISTRATION	10
6.1. Policy Specification and Change Approval Procedures.....	10
6.2. Items that can change without Notification	10
6.3. Changes with Notification.....	10
6.4. Publication and Notification of Procedures	10
6.5. Items Whose Change Requires a New Policy	10

POLICY IDENTIFICATION

Policy Name	Authorised Operator TrustAssured Service Utility Certificate Policy.
Policy Qualifier	This Utility Certificate may only be relied upon only by either (1) a Relying Customer of an Identrust Participant, or (2) a party bound to the alternative policy regime specified elsewhere in this Certificate.
Policy Version	4.0
Policy Status	Changes required for on board key generation
Policy Ref/OID	1.2.826.0.2.90312.10.1.2.1.2.4.0
Date of Issue	1st April 2006
Date of Expiry	

1. POLICY OUTLINE

This Certificate Policy (CP) is applicable to The Royal Bank of Scotland plc TrustAssured Service. Certificate issuance and usage is restricted to Customers of The Royal Bank of Scotland plc who have signed and agreed to the Business Customer Agreement for the TrustAssured Service and, where appropriate, this CP.

Authorised Operator TrustAssured Service Utility Certificates are only issued to Customers in conjunction with an Identity Certificate, unless otherwise stated.

The Royal Bank of Scotland plc has a common set of definitions that are used in this Certificate Policy and the Business Customer Agreement for the TrustAssured Service and associated documents. A definition for all words appearing in capitals in these documents can be found in Schedule A of the Business Customer Agreement for the TrustAssured Service.

Only contracted parties within the Identrust Scheme may use and rely upon an Authorised Operator TrustAssured Service Utility Certificate.

1.1. Community & Applicability

Authorised Operator TrustAssured Service Utility Certificates are only to be used by parties contracted with The Royal Bank of Scotland plc. Use of such Certificates outside this community is not permitted or supported.

Authorised Operator TrustAssured Service Utility Certificates are only to be used for the purpose of providing the following Identity Validation services:

- Data confidentiality and integrity;
- Secure key distribution;
- Key agreement;
- Non-Identrust identity related digital signatures.

Authorised Operator TrustAssured Service Utility Certificates are restricted to those services described above by defined Key Usage fields within the Certificate.

1.2. Contact Details

The Royal Bank of Scotland plc
TrustAssured
5th Floor
2 Waterhouse Square
138-142 Holborn
London EC1N 2TH
United Kingdom
Tel No: +44 (0)207 427 9355
Fax No: +44 (0)207 427 8342
09:00 – 17:00 Monday to Friday (excluding English Public Holidays)

2. CP PROVISIONS

2.1. Obligations

The Royal Bank of Scotland plc is responsible for:

- Making reasonable efforts to ensure it conducts an efficient and trustworthy operation in line with the operating rules and guidelines of Identrust;
- Issuing Certificates that are factually correct from the information presented to them by the Customer at the time of issue, and that they are free from data entry errors;
- Where appropriate, the revocation/suspension of Certificates and updating its Validation Authority or other directory services as appropriate, in a timely manner, consistent with the requirements of The Royal Bank of Scotland plc.

A Subscribing Customer:

- Is obliged to protect Private Key(s) at all times, against loss, disclosure to any other party, modification and unauthorised use, in accordance with the Business Customer Agreement for the TrustAssured Service and this CP;
- Is personally and solely responsible for the confidentiality and integrity of its Private Key(s);
- Must ensure its Authorised Operators never store their PIN(s) (Personal Identity Number) or pass phrase(s), used to protect unauthorised use of the Private Key(s), in the same location as the Private Key(s) or next to the storage media, or otherwise in an unprotected manner without sufficient protection;
- Is responsible for the accuracy of the data it transmits as part of a Certificate request;
- Is required to immediately inform The Royal Bank of Scotland plc of compromise or suspected compromise of its Private Key(s);
- Is to immediately inform The Royal Bank of Scotland plc if there is any change in its information included in its Certificate(s) or provided during the application process;
- Accepts that its Certificate(s) may be published in The Royal Bank of Scotland plc owned directory services which may be made available to other Customers within the Identrust Scheme; and
- Is responsible for checking the correctness of the content of its published Certificate(s) within seven (7) days from their issuance.

A Relying Customer:

- Is to exercise due diligence and reasonable judgement before deciding to rely on an Authorised Operator TrustAssured Service Utility Certificate;
- Is to acknowledge that the assurance provided by an Authorised Operator TrustAssured Service Utility Certificate is not guaranteed in any form by The Royal Bank of Scotland plc or Identrust;
- Will ensure that it complies with any local laws and regulations, which may impact their right to use certain cryptographic instruments.

2.2. Liability

This is covered under the Business Customer Agreement for the TrustAssured Service.

2.3. Interpretation & Enforcement

Governing Law

This is covered under the Business Customer Agreement for the TrustAssured Service.

Contractual Infrastructure

This CP is a part of and subject to the Business Customer Agreement for the TrustAssured Service.

Priority of Documents

In the event that there is a conflict between the documents provided by The Royal Bank of Scotland plc, the order of controlling priority, in descending order, shall be as follows:

1. Business Customer Agreement for the TrustAssured Service.
2. Authorised Operator TrustAssured Service Utility Certificate Policy.

2.4. Publication & Repository

Paper copies and electronic versions of this CP are available from The Royal Bank of Scotland plc.

2.5. Confidentiality

2.5.1. Types of Information to be Kept Confidential

Detailed provisions regarding confidentiality are defined in the Business Customer Agreement for the TrustAssured Service.

A Customer shall treat all confidential information as confidential and proprietary to its owner. A Customer shall use at least the same degree of care to protect the confidentiality of another party's confidential information as the Customer uses to protect its own similar confidential information, which degree of care shall be no less than reasonable care.

Information supplied to The Royal Bank of Scotland plc as a result of the practices described in this CP may be subject to national government or other privacy legislation or guidelines.

Access to confidential information by The Royal Bank of Scotland plc operational staff is on a need-to-know basis. Paper-based records, electronic records, and other documentation containing confidential information are to be kept in secure and locked containers or filing systems, separate from all other records.

Application Records

All application records are considered confidential information, including:

- Certificate applications, whether approved or rejected;
- Proof of identification documentation and details as applicable;
- Certificate information collected as part of the application records, but this does not prevent publication of Certificate information in the Certificate repository.

Certificate Information

The reason for a Certificate being suspended or revoked is considered confidential information.

2.5.2. Types of Information Not Considered Confidential

Certificate Information

The information contained in Certificates issued to contracted Customers is not considered confidential.

Disclosure of Certificate Suspension Information

Status request information on Certificate suspension is not disclosed to the Relying Customer. A suspended Certificate is not considered reliable and The Royal Bank of Scotland plc' Validation Authority reports to Relying Customers that suspended Certificates are, in fact, revoked.

Disclosure of Certificate Status Information

Where appropriate, Customers' Certificate Status information is provided via The Royal Bank of Scotland plc's Validation Authority or other directory services where the following status response is provided:

- Good
- Revoked
- Unknown

A revocation reason is not provided with the response.

3. IDENTIFICATION & AUTHENTICATION

3.1. Initial Registration

3.1.1. Uniqueness of Names

The Authorised Operator common name (cn) component of the Certificate's Distinguished Name (Dname) is unique. The format is as follows:

- Authorised Operator's forename
- Authorised Operator's surname
- Utility Certificate identifier [Utility];

3.1.2. Authentication of Business Customer Identity

An Authorised Operator TrustAssured Service Utility Certificate is issued together with an Authorised Operator TrustAssured Service Identity Certificate. On successful application for an Identity Certificate, a Utility Certificate will be provided on the hardware token provided to the Authorised Operator.

3.1.3. Routine Rekey

Certificates and hardware tokens holding Private Keys expire at the same time. The Royal Bank of Scotland plc will automatically provide the rekeyed Certificate and hardware token (if necessary) 30 days prior to its expiration.

3.1.4. Rekey after Revocation

Rekeying after Certificate revocation is not permitted. Customers must apply for a new Certificate and complete the initial application process as though they were a new Authorised Operator.

4. OPERATIONAL REQUIREMENTS

4.1. Certificate Application, Issuance & Acceptance

Once a Customer has expressed interest in using Certificates provided by the TrustAssured Service, the Customer must complete and sign an application form to apply for membership of the TrustAssured Service (refer to related documentation).

After initial application and Certification of the Identity Public Key, Customers will obtain their Key Pairs and a Utility Certificate on the provided Identrust compatible hardware token using the same process detailed for the Identity Certificate.

After review of the Utility Certificate, an Authorised Operator's use of their Key Pairs/Utility Certificate shall constitute acceptance of the Key Pairs and Certificate.

4.2. Certificate Suspension & Revocation

Certificate suspension results in a temporary inability to use the Certificate. Where appropriate, The Royal Bank of Scotland plc may provide directory services in order to facilitate the validation of a Utility Certificate outside of the TrustAssured Service. In such cases as The Royal Bank of Scotland plc implements validation for Utility Certificates the following will apply.

Although the Authorised Operator retains possession of the Certificate; if they use the Certificate within the Identrust Scheme, the validity of the Certificate will be returned as revoked and should not be trusted. Certificate revocation results in the permanent inability to use the Certificate.

All requests for Certificate suspension and revocation will be performed in accordance with the Business Customer Agreement for the TrustAssured Service.

4.2.1. Circumstances for Certificate Revocation/Suspension

The following events will result in the revocation or suspension of a Utility Certificate:

The Royal Bank of Scotland plc initiates suspension or revocation:

- To protect their, their Customer's or Identrust's interests;
- Upon expiry of the Suspension Grace Period;
- Upon receipt of multiple suspension requests;
- Upon termination of the Business Customer Agreement for the TrustAssured Service.

The Customer initiates suspension or revocation due to but not limited to the following:

- Person/Token Removal – the Authorised Operator has left the position needing the Certificate or if a hardware token used to exercise the Certificate is no longer needed;
- Person Dismissal – the Authorised Operator has been dismissed or resigned from their Business;
- Extended Leave – where the Authorised Operator is absent from the Business for an extended period of time.
- Key Compromise – the keys associated with the Certificate have been or are believed to be compromised, for example PIN disclosure.
- Change of Business Company Name – the Business changes its company name which will require that the Organisation Name, as detailed on each of the Authorised Operators Certificates, reflects the new Business company name;
- Affiliation Change – the Authorised Operator has changed functional department/responsibilities where a different or new Certificate must be issued to the Business for that individual;
- Hardware Token Failure – due to token malfunction the Authorised Operator is unable to use either the Key Pairs or Certificate or both;
- Hardware Token Lost/Stolen – the token has been lost or stolen; or
- Hardware Token Blocked – the pass phrase for the token has been locked due to excessive unsuccessful attempts;
- Termination of the Business Customer Agreement for the TrustAssured Service.

4.2.2. Procedure for Suspension or Revocation Request

Business Customer Authorised Operator Certificate Management Forms (OCM) are used to indicate the reason for the revocation or suspension. These must be signed by the Authorised Signatory(s) and faxed to The Royal Bank of Scotland plc. The signed original copy(s) of the request must be furnished to The Royal Bank of Scotland plc as soon as possible.

Valid requests for revocations and suspensions will be processed within 1 hour of The Royal Bank of Scotland plc acknowledging receipt of the request.

Where revocation is requested, The Royal Bank of Scotland plc will initially suspend the Certificate until receipt of the signed original request, upon which the Certificate will be fully revoked.

The Royal Bank of Scotland plc will provide notice to Customers of any revocation or suspension activity as detailed in the Business Customer Agreement for the TrustAssured Service.

4.2.3. Certificate Re-activation

Business Customer Authorised Operator Certificate Management Forms (OCM) are used to indicate the reason for reactivation of a suspended Certificate. These must be signed by the Authorised Signatory(s) and the signed original copy(s) of the OCM form must be furnished to The Royal Bank of Scotland plc. Requests for re-activation will be assessed on a case by case basis.

4.2.4. Suspension Period Limitations

Suspension of Authorised Operator TrustAssured Service Utility Certificates may not exceed 30 days for any one period. If the suspension of an Authorised Operator's TrustAssured Service Utility Certificate is requested more than twice by the Customer or The Royal Bank of Scotland plc, the Certificate will be fully revoked following receipt of the third request.

4.2.5. On-line Revocation Checking Requirements

The Royal Bank of Scotland plc, at its discretion may provide Utility Status checking facilities for those entities as required.

5. TECHNICAL SECURITY CONTROLS

5.1. Key Pair Generation and Installation

All Key Pairs used in relation with the Authorised Operator TrustAssured Service Utility Certificates are generated in hardware meeting FIPS140-1 Level 3. Keys are securely distributed in Hardware Security Modules, Personalised smartcards or other hardware tokens. Where keys are centrally generated they are installed in compliance with The Royal Bank of Scotland plc' key management policies.

5.2. Private Key Protection

Private Keys are protected in hardware meeting FIPS 140-1 Level 2.

5.2.1. Private Key Escrow, Backup and Archiving

Utility Private Keys are not escrowed, backed up or archived.

5.2.2. Activation Codes

Activation codes are kept secure and distributed by the provision of two separate activation codes. A security code is provided by way of a personalised email direct to the Authorised Operator, details of the authorisation code are included with the hardware token pack that is posted to the Authorised Operator.

5.3. Certificate Profiles

Authorised Operator TrustAssured Service Qualified Utility Certificate Profile

Field	Content	Mandatory	Critical*
1. X.509v1 Field			
1.1. Version	v3	Yes	
1.2. Serial Number	Allocated automatically by the Issuing CA	Yes	
1.3. Signature Algorithm	SHA-1 with RSA Signature	Yes	
1.4. Issuer Distinguished Name		Yes	
1.4.1. Country (C)	GB	No	
1.4.2. Organization (O)	The Royal Bank of Scotland plc	Yes	
1.4.3. Organizational Unit (OU)	The Royal Bank of Scotland plc Identrust Infrastructure	Yes	
1.4.4. Common Name (CN)	The Royal Bank of Scotland plc Identrust CA	Yes	
1.5. Validity		Yes	
1.5.1. Not Before	e.g. "00:0:01 13 December 2000"	Yes	
1.5.2. Not After	e.g. "23:59:59 12 December 2003"	Yes	
1.6. Subject		Yes	
1.6.1. Country (C)	e.g., "GB" (entered by the RA)	No	
1.6.2. Organization (O)	e.g., "The XYZ Company" (entered by the RA)	Yes	
1.6.3. Organizational Unit (OU)	e.g., "International Financial Services" (entered by the RA)	Yes	
1.6.4. Common Name (CN)	e.g., "John Doe" (entered by the RA)	Yes	
1.7. Subject Public Key Info	1024-Bit Public key encoded in accordance with IETF RFC3280 & PKCS#1	Yes	
2. X.509v3 Extensions			
2.1. Authority Key Identifier		Yes	No
2.1.1. Key Identifier	the Subject Key Identifier of the Issuer of this Certificate	Yes	
2.1.2. AuthorityCertIssuer	Not present	No	
2.1.3. AuthorityCertSerialNumber	Not present	No	
2.2. Subject Key Identifier	The Key Identifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).	Yes	No
2.3. Key Usage		Yes	Yes
2.3.1. Digital Signature	Selected "1"	Yes	
2.3.2. Non Repudiation	Not selected "0"	Yes	
2.3.3. Key Encipherment	Selected "1"	Yes	
2.3.4. Data Encipherment	Selected "1"	Yes	
2.3.5. Key Agreement	Selected "1"	Yes	
2.3.6. Key Certificate Signature	Not selected "0"	Yes	
2.3.7. CRL Signature	Not selected "0"	Yes	

Field	Content	Mandatory	Critical*
2.4. Extended Key Usage (can define other OIDs for other uses)		No	No
2.4.1. Server Authentication	Not selected		
2.4.2. Client Authentication	Selected		
2.4.3. Code Signing	Not selected		
2.4.4. E-mail Protection	Selected		
2.4.5. IPSEC End System	Not selected		
2.4.6. IPSEC Tunnel	Not selected		
2.4.7. IPSEC User	Optional		
2.4.8. Time Stamping	Not selected		
2.4.9. OCSP Server	Not selected		
2.4.10. Cert Trust List Signing	Not selected		
2.4.11. MS Server Gated Crypto	Not selected		
2.4.12. NS Server Gated Crypto	Not selected		
2.5. Certificate Policies		Yes	No
2.5.1. Policy Identifier	1.2.840.114021.1.31.2		
2.5.2. Policy Qualifier ID	1.3.6.1.5.5.7.2.2	Yes	
2.5.2.1. User Notice	This Certificate may be relied upon only by either: (1) a Relying Customer of an Identrust Participant, or (2) a party bound to the alternative policy regime specified elsewhere in this Certificate.	Yes	
2.5.2.2. Policy Identifier	1.2.826.0.2.90312.10.1.2.1.2.4.0	No	
2.5.2.3. Policy Qualifier ID	1.3.6.1.5.5.7.2.2	No	
2.5.2.4. User Notice	"This Certificate is for the sole use of RBS, their customers, and other contracted parties of associated supported Schemes. RBS accepts no liability for any claim except as expressly provided in its Business Customer Agreement Terms & Conditions."	No	
2.6. Subject Alternate Names		Yes	No
2.6.1. rfc822Name	e.g., "john.doe@XYZCorp.com"	Yes	
2.6.2. registeredID	Optional, OID TBD	No	
2.7. Basic Constraints	Not present		
2.7.1. Subject Type	Not present		
2.7.2. Path Length Constraint	Not present		
2.8. Authority Information Access		Yes	No
2.8.1. Access Description		Yes	
2.8.1.1. Access Method	On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	Yes	
2.8.1.2. Alternative Name	e.g., "URL=https://IV.OCSPBank-XYZ.com"	Yes	
2.8.2. Access Description		Yes	
2.8.2.1. Access Method	On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	Yes	
2.8.2.2. Alternative Name	https://rbstnca.identrust.com	Yes	
2.9. CRLDistributionPoint		No	
2.10. QC Statements	This certificate is issued as a Qualified Certificate according to Annex I and II of the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, as implemented in the law of the United Kingdom.	No	

*not used for attributes, only extensions

6. POLICY SPECIFICATION AND ADMINISTRATION

6.1. Policy Specification and Change Approval Procedures

The Royal Bank of Scotland Policy Approval Authority (PAA) is responsible for the specification, approval and issue of all changes to this Certificate Policy.

6.2. Items that can change without Notification

Typographical and editorial corrections or changes to the contact details may be made to this specification without notification.

6.3. Changes with Notification

Any item in this Certificate Policy may be changed with 30 days' notice as detailed within the Business Customer Agreement for the TrustAssured Service.

6.4. Publication and Notification of Procedures

All proposed changes that may materially impact users of this Certificate Policy will be notified in writing to Certification Authorities (CAs) registered with the TrustAssured Service. Such CAs shall post notice of such proposed changes and shall advise their registered Subscribers of the proposed changes as detailed in the Business Customer Agreement for the TrustAssured Service.

6.5. Items Whose Change Requires a New Policy

If a change to this Certificate Policy is determined by the PAA to have a material impact on users of the policy, the PAA may, at its sole discretion, assign a new Object Identifier to the modified policy.