The co-operative bank
good with money

Authorised User bsecure Service Identity Certificate Policy

Version 1.0

IMPORTANT NOTE ABOUT THIS DOCUMENT

Contact

Computer Banking Services
The Co-operative Bank plc
Kings Valley
Yew Street
Stockport
SK4 2JU

Table of Contents

1 POLICY OUTLINE

This Certificate Policy (CP) is applicable to The Co-operative Bank plc bsecure Service. Certificate issuance and usage is restricted to Customers of The Co-operative Bank plc who have signed and agreed to the Terms & Conditions for the bsecure Service and, where appropriate, this CP.
Certificate users have been accepted by The Co-operative Bank plc using a robust registration process thus ensuring a high level of confidence for the binding between an individual identity and a Public Key. Thus a Certificate issued under this CP provides the highest level of assurance for correct authentication of the Subscriber.
The Co-operative Bank plc has a common set of definitions that are used in this Certificate Policy and the Terms & Conditions for the bsecure Service and associated documents. A definition for all words appearing in capitals in these documents can be found in Schedule A of the Terms & Conditions for the bsecure Service.
Only contracted parties within the Identrus Scheme may use and rely upon an Authorised User bsecure Service Identity Certificate.

1.1. Community & Applicability

Authorised User bsecure Service Identity Certificates are only to be used by parties contracted with The Co-operative Bank plc. Use of such Certificates outside this community is not permitted or supported.

Authorised User bsecure Service Identity Certificates are only to be used for the purpose of providing the following Identity Validation services:

- User authenticity;
- Digital signing;
- Data integrity;
- Non-repudiation.

Neither The Co-operative Bank plc nor Identrus provide warranty services for Certificates under this CP, except as expressly defined within the Terms & Conditions for the bsecure Service.

Authorised User bsecure Service Identity Certificates are restricted to those services described above by defined Key Usage fields within the Certificate

1.2. Contact Details

Computer Banking Services
The Co-operative Bank plc
Kings Valley
Yew Street
Stockport
SK4 2JU

Tel No: 08457 616 616
Fax No: 0161 480 2501
08:00 – 18:00 Monday to Friday (excluding English Public Holidays)

2 CP PROVISIONS

2.1. Obligations

The Co-operative Bank 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 Identrus;

- 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;

- Revoking/Suspending Certificates and updating the Validation Authority in a timely manner, consistent with Identrus requirements.

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 Terms & Conditions for the bsecure Service and this CP;

- Is personally and solely responsible for the confidentiality and integrity of its Private Key(s);

- Must ensure its Authorised Users 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 Co-operative Bank plc of compromise or suspected compromise of its Private Key(s);

- Is to immediately inform The Co-operative Bank 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 a directory which may be made available to other Customers within the Identrus 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:

- Will exercise due diligence and reasonable judgement before deciding to rely on a Certificate based service, including obtaining Certificate status through The Co-operative Bank plc and trusting and relying only on a Certificate that has not expired, or been revoked or been suspended;

- 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 Terms & Conditions for the bsecure Service.

2.3. Interpretation & Enforcement

Governing Law

This is covered under the Terms & Conditions for the bsecure Service.

Contractual Infrastructure

This CP is a part of and subject to the Terms & Conditions for the bsecure Service.

Priority of Documents

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

1. Terms & Conditions for the bsecure Service
2. Authorised User bsecure Service Identity Certificate Policy.

2.4. Publication & Repository

Electronic versions of this CP are available from The Co-operative Bank plc (reference section 1.2).

2.5. Confidentiality

2.5.1. Types of Information to be Kept Confidential

Detailed provisions regarding confidentiality are defined in the Terms & Conditions for the bsecure 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 Co-operative Bank 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 Co-operative Bank 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 Co-operative Bank plc's Validation Authority reports to Relying Customers that suspended Certificates are, in fact, revoked.

Disclosure of Certificate Status Information

Customers' Certificate Status information is provided via The Validation Authority 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 User common name (cn) component of the Certificate's Distinguished Name (Dname) is unique.

It is made up as follows:

- Authorised User's forename
- Authorised User's surname

3.1.2. Routine Rekey

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

3.1.3. 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 User.

4 Operational Requirements

4.1 Certificate Application, Issuance & Acceptance

Once a Business has expressed an interest in using Certificates provided by the bsecure Service, the Customer must complete and sign an application form to apply for membership of the bsecure Service.

4.1.1 Pre-requisites

Before a Business Customer is enrolled The Co-operative Bank plc ensure that:

- The applicant is an approved Business Customer of The Co-operative Bank;
- An Authorised Signatory(s) is established and that signatures are verifiable.

4.1.2 Initial Application Comprises the Following Steps

- The Co-operative Bank plc requires the Authorised Signatory(s) to complete a bsecure Application Form;
- That Contact details are established with the Customer and their details are entered on the bsecure Application Form;
- The Customer nominates a number of Authorised Users using the bsecure Application Form;
- The bsecure Application Form must then be approved and signed by the Authorised Signatory(s);
- The bsecure Application Form is returned to The Co-operative Bank plc for approval and processing;
- Upon application approval, the Contact is issued with hardware tokens holding the bsecure Service Identity and Utility Key Pairs and Certificates for each nominated Authorised User;
- Each Authorised User receives a PIN mailer supplying them a temporary PIN. Users are then required to change the PIN upon first use of their hardware token.

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

4.2 Certificate Suspension & Revocation

Certificate suspension results in a temporary inability to use the Certificate. Although the Authorised User retains possession of the Certificate, if they use the Certificate within the Identrus 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 Identity Certificate.

All requests for Certificate suspension and revocation will be performed in accordance with the Terms & Conditions for the bsecure Service.

4.2.1 Circumstances for Certificate Revocation/Suspension

The following events will result in the revocation or suspension of a bsecure Service Identity Certificate:

The Co-operative Bank plc initiates suspension or revocation:

- To protect their, their Customer's or Identrus' interests;
- Upon expiry of the Suspension Grace Period;
- Upon receipt of multiple suspension requests;
- Upon termination of the Terms & Conditions for the bsecure Service.

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

- Person/Token Removal - the Authorised User of the hardware token has left the position needing the Certificate or if a token used to exercise the Certificate is no longer needed;
- Person Dismissal - the Authorised User has been dismissed or resigned from their Business;
- Extended Leave - where the Authorised User 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 Users Certificates, reflects the new Business company name;
- Affiliation Change - the Authorised User has changed functional department / responsibilities where a different or new Certificate must be issued to the Customer for that individual;
- Hardware Token Failure - due to token malfunction the Authorised User is unable to use either the keys or Certificate or both;
- Hardware Token Lost/Stolen - the token has been lost or stolen;
- Hardware Token Blocked - the pass phrase for the token has been locked due to excessive unsuccessful attempts;
- Termination of the Terms & Conditions for the bsecure Service.

4.2.2 Procedure for Suspension or Revocation Request

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

Valid requests for revocations and suspensions will be processed within 2 hours of The Co-operative Bank plc acknowledging receipt of a correctly completed request.

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

The Co-operative Bank plc will provide notice to Customers of any revocation or suspension activity as detailed in the Terms & Conditions for the bsecure Service.

4.2.3 Certificate Re-activation

Business Customer Authorised User 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 Co-operative Bank plc. Requests for re-activation will be assessed on a case by case basis.

4.2.4 Suspension Period Limitations

Suspension of Authorised User bsecure Service Identity Certificates may not exceed 30 days for any one period. If the suspension of an Authorised User's bsecure Service Identity Certificate is requested more than twice by the Customer or The Co-operative Bank plc, the Certificate will be fully revoked immediately upon receipt of the third request.

4.2.5 On-line Revocation Checking Requirements

The Co-operative Bank plc, in line with Identrus requirements provides an online revocation checking facility for its bsecure Service Identity Certificates. Relying Participants must use this facility to obtain Certificate status for Relying Customers.

Relying Customers may also obtain the Certificate status of their Relying Participants by using Identrus' root Validation Authority by way of their Relying Participant.

5 Technical Security Controls

5.1 Key Pair Generation and Installation

All Key Pairs used in relation with the Authorised User bsecure Service Identity Certificates are generated in hardware meeting FIPS 140-1 Level 3. Keys are securely distributed in Hardware Security Modules, Personalised Smart Cards or other hardware tokens. Keys are centrally generated and installed meeting The Co-operative Bank plc key management policies.

5.2 Private Key Protection

Identity Private Keys are protected in hardware meeting FIPS 140-1 Level 2. Access to the Identity Private Key requires that the Authorised User provides a secret pass phrase or PIN to the hardware token. This is required before every use of the key where appropriate to the token type, in accordance with The Co-operative Bank plc key management policies.

5.2.1 Private Key Escrow, Backup and Archiving

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

5.2.2 Activation Data

Activation data is kept secure and distributed separately from the hardware token holding the Authorised User's Private Key(s).

5.3 Certificate Profiles

Authorised User bsecure Service Identity Certificate Profile

Field	Content
1 X.509v1 Field	
1.1 Version	V3
1.2 Serial Number	Allocated automatically by the Issuing CA
1.3 Signature Algorithm	SHA-1 with RSA Signature
1.4 Issuer Distinguished Name	
1.4.1 Country (C)	GB
1.4.2 Organisation (O)	The Royal Bank of Scotland plc
1.4.3 Organisational Unit (OU)	The Royal Bank of Scotland plc Identrus Infrastructure
1.4.4 Common Name (CN)	The Royal Bank of Scotland plc Identrus CA
1.5 Validity	

Field			Content
	1.5.1	Not Before	e.g. “00:00:01" Wednesday 13 December 2000
	1.5.2	Not After	e.g. “23:59:59" Friday 12 December 2003
1.6	Subject		
	1.6.1	Country (C)	GB
	1.6.2	Organisation (O)	The Co-operative Bank p.l.c.
	1.6.3	Organisational Unit (OU)	.Customer Business name
	1.6.4	Common Name (CN)	e.g. John Doe
1.7	Subject Public Key Info		RSA (1024 bits) Public key encoded in accordance with RFC2459 & PKCS#1
2	X.509v3 Extensions		
2.1	Authority Key Identifier		
	2.1.1	Key Identifier	e.g. KeyID=BF8A 85EE E811 BF2C 8CD4 33C0 D8C0 BA7D 8F00 6389
	2.1.2	AuthorityCertIssuer	Not present
	2.1.3	AuthorityCertSerialNumber	Not present
2.2	Subject Key Identifier		The key Identifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subject Public Key (excluding the tag, length, and number of unused bits); e.g. 3DAD 64B8 9232 2B02 B814 3356 DD3F A309 E9C0 F376
2.3	Key Usage		
	2.3.1	Digital Signature	Selected
	2.3.2	Non Repudiation	Selected
	2.3.3	Key Encipherment	Not selected
	2.3.4	Data Encipherment	Not selected
	2.3.5	Key Agreement	Not selected
	2.3.6	Key Certificate Signature	Not selected
	2.3.7	CRL Signature	Not selected
2.4	Certificate Policies		
	2.4.1	Policy Identifier	1.2.840.114021.1.4.1
	2.4.2	Policy Qualifier ID	e.g. 1.3.6.1.5.5.7.2.2
	2.4.3	Policy Qualifier	”This certificate is for the sole use of Identrus, its Participants and their customers. Identrus accepts no liability for any claim except as expressly provided in its Operating Rules IL-OPRUL”.

Field	Content
2.5.4. Policy Identifier	1.2.826.0.2.90312.10.1.2.1.1.3.6
2.5.5. Policy Qualifier ID	1.3.6.1.5.5.7.2.2
2.5.6. User Notice	This Identity Certificate is for the sole use of Identrus, its Participants and their customers. Only contracted parties within the Identrus Scheme may use and rely upon this certificate.
2.5 Subject Alternate Names	Optional
2.5.1 rfc822Name	e.g. john.smith@XYZCorp.com
2.6 Basic Constraints	
2.6.1 Subject Type	Not present
2.6.2 Path Length Constraint	Not present
2.7 Authority Information Access	
2.7.1 Access Description	
2.7.1.1 Access Method	On-line Certificate Status Protocol e.g. 1.3.6.1.5.5.7.48.1
2.7.1.2 Alternative Name	e.g. URL=https://vi.OCSP. rbs.co.uk
2.7.2 Access Description	
2.7.2.1 Access Method	Identrus Certificate Status Check Protocol(1.2.840.114021.4.1)
2.7.2.2 Alternative Name	URL=https://vi.TC.rbs.co.uk

6 Policy Specification and Administration

6.1 Policy Specification and Change Approval Procedures

The Co-operative Bank 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 Terms & Conditions for the bsecure 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 bsecure Service. Such CAs shall post notice of such proposed changes and shall advise their registered Subscribers of the proposed changes as detailed in the Terms & Conditions for the bsecure Service.

6.5 Items Whose Change Requires a New Policy

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