



# Bacstel-IP

## Authorised Security Contact Trust Assured Service Identity Certificate Policy

### Table of Contents

---

- 1 Policy Outline**..... 3
  - 1.1. Community and Applicability..... 3
  - 1.2 Contact Details..... 3
- 2 CP Provisions**..... 4
  - 2.1. Obligations..... 4
  - 2.2. Liability..... 4
  - 2.3. Interpretation and Enforcement..... 4
  - 2.4. Publication and 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 and 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**..... 7
  - 4.1 Certificate Application, Issuance and Acceptance..... 7
    - 4.1.1 Pre-requisites..... 7
    - 4.1.2 Initial Application Comprises the Following Steps..... 7
  - 4.2 Certificate Suspension and Revocation..... 7
    - 4.2.1 Circumstances for Certificate Revocation/Suspension..... 7
    - 4.2.2 Procedure for Suspension or Revocation Request..... 8
    - 4.2.3 Certificate Re-activation..... 8
    - 4.2.4 Suspension Period Limitations..... 8
    - 4.2.5 On-line Revocation Checking Requirements..... 8
- 5 Technical Security Controls**..... 9
  - 5.1 Key Pair Generation and Installation..... 9
  - 5.2 Private Key Protection..... 9
    - 5.2.1 Private Key Escrow, Backup and Archiving..... 9
    - 5.2.2 Activation Codes..... 9
  - 5.3 Certificate Profiles..... 9
- 6 Policy Specification and Administration**.....11
  - 6.1 Policy Specification and Change Approval Procedures..... 11
  - 6.2 Items that can Change without Notification..... 11
  - 6.3 Changes with Notification..... 11
  - 6.4 Publication and Notification of Procedures..... 11

## 1. Policy Outline

---

This Certificate Policy (CP) is applicable to TrustAssured Service as made available by The Royal Bank of Scotland p.l.c. to users of the Bacstel-IP service sponsored and introduced by AIB Group (UK) p.l.c.

Certificate issuance and usage is restricted to Customers of AIB Group (UK) p.l.c. who have signed and agreed to the Business Customer Agreement for the TrustAssured Service and, where appropriate, this CP.

Certificate users have been accepted by AIB Group (UK) p.l.c. 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.

AIB Group (UK) p.l.c. 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 Security Contact TrustAssured Service Identity Certificate.**

### 1.1. Community and Applicability

Authorised Security Contact TrustAssured Service Identity Certificates are only to be used by parties contracted with AIB Group (UK) p.l.c. and / or the Royal Bank of Scotland p.l.c. Use of such Certificates outside this community is not permitted or supported.

Authorised Security Contact TrustAssured 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 AIB Group (UK) p.l.c., The Royal Bank of Scotland p.l.c. nor Identrust provide warranty services for Certificates under this CP, except as expressly defined within the Business Customer Agreement for the TrustAssured Service.

Authorised Security Contact TrustAssured Service Identity Certificates are restricted to those services described above by defined Key Usage fields within the Certificate Contact Details

### 1.2 Contact Details

AIB  
BACS Customer Service  
92 Ann Street  
Belfast  
BT1 3HH

Telephone: (01604) 235515  
Email: bacssupport@aib.ie

### 2.1. Obligations

#### **AIB Group (UK) p.l.c. is responsible for:**

- Validation and verification of all communications and information received from its Subscribing Customers;
- Making reasonable efforts to ensure it conducts the administration of its Subscribing Customer PKI requirements in an efficient and trustworthy manner;

#### **The Royal Bank of Scotland p.l.c. 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 AIB Group (UK) p.l.c. at the time of issue, and are free from data entry errors;
- Revoking/Suspending Certificates and updating its Validation Authority in a timely manner, consistent with Identrust 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 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 Security Contacts 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 AIB Group (UK) p.l.c. of compromise or suspected compromise of its Private Key(s);
- Is to immediately inform AIB Group (UK) p.l.c. 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 p.l.c. owned directory service 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 of 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 Royal Bank of Scotland p.l.c. 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 Business Customer Agreement for the TrustAssured Service.

### 2.3. Interpretation and 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 AIB Group (UK) p.l.c., the order of controlling priority, in descending order, shall be as follows:

1. Business Customer Agreement for the TrustAssured Service
2. Authorised Security Contact TrustAssured Service Identity Certificate Policy.

## 2.4. Publication and Repository

Paper copies and electronic versions of this CP are available from AIB Group (UK) p.l.c. Bacs Customer Service  
aibni.co.uk/bacstel  
aibgb.co.uk/bacstel

## 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 AIB Group (UK) p.l.c. 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 AIB Group (UK) p.l.c. and The Royal Bank of Scotland p.l.c. 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

#### 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 p.l.c. 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 Royal Bank of Scotland p.l.c. Validation Authority where the following status response is provided:

- Good
- Revoked
- Unknown

A revocation reason is not provided with the response.

### 3.1 Initial Registration

#### 3.1.1. Uniqueness of Names:

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

- Authorised Security Contact's forename
- Authorised Security Contact's surname

#### 3.1.2. Authentication of Business Customer Identity

In order to comply with AIB Group (UK) p.l.c.'s application requirements, the Customer must provide documents to identify their Business and allow AIB Group (UK) p.l.c. to verify this identity.

Documents may include, but are not limited to:

- A government filing to register their Business;
- A list of officers within the Business;
- A list of Authorised Security Contacts of the Business who will be using the TrustAssured Service.

AIB Group (UK) p.l.c. personnel will validate the identity of the Customer with the corresponding government institution to assure the identity of the Customer. If AIB Group (UK) p.l.c. is unable to verify a Customer's identity, it will refuse to provide the service. Customers will be notified within a reasonable amount of time from application, of their acceptance or denial of service.

AIB Group (UK) p.l.c. requires the Customer to ensure accurate authentication of their Authorised Security Contact

#### 3.1.3. Routine Rekey

Certificates and hardware tokens holding Private Keys expire at the same time. In coordination with AIB Group (UK) p.l.c., The Royal Bank of Scotland p.l.c. will automatically provide customers with instructions in order to obtain the rekeyed Certificate and 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 Security Contact.

## 4 Operational Requirements

---

### 4.1 Certificate Application, Issuance and Acceptance

Once a Business has expressed an 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

#### 4.1.1 Pre-requisites

Before a Business Customer is enrolled AIB Group (UK) p.l.c. will ensure that:

- The applicant is an approved Business Customer of the AIB Group (UK) p.l.c. Group of Companies;
- An Authorised Signatory(ies) is/are established and that signature(s) is/are verifiable.

#### 4.1.2 Initial Application Comprises the Following Steps

- AIB Group (UK) p.l.c. requires the Authorised Signatory(ies) to complete a Business Customer Application Form (BCA);
- That Authorised Security Contacts are established by the Customer and their details are entered on the Authorised Security Contact Application Form;
- The Customer nominates a number of Authorised Security Contacts using the Business Customer Authorised Security Contact Application (ASCA) Form(s);
- The ASCA forms must then be approved and signed by the Authorised Signatory(ies);
- The ASCA forms are returned to AIB Group (UK) p.l.c. for approval and processing;
- Upon application approval, the Authorised Security Contact is issued with a hardware token and instructions of how to generate their Identity and Utility keys and obtain their Identity and Utility Certificates. Users are required to change the PIN upon first use of their hardware token;
- Each Authorised Security Contact also receives an e-mail with a link to a web page where they will be able to activate the Certificate. Activation of the card and Certificate using the PIN shall constitute acceptance of the Certificate and Card.

### 4.2 Certificate Suspension and Revocation

Certificate suspension results in a temporary inability to use the Certificate. Although the Authorised Security Contact 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 Identity 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 TrustAssured Service Identity Certificate:

##### **AIB Group (UK) p.l.c. or The Royal Bank of Scotland p.l.c. initiates suspension or revocation:**

- To protect their, their Customers' 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 Security Contact associated with 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 Security Contact has been dismissed or resigned from the Business;
- Extended Leave - where the Authorised Security Contact 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 Security Contact Certificates, reflects the new Business company name;
- Affiliation Change - the Authorised Security Contact 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 Security Contact 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 blocked 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 Security Contact Certificate Management Forms (SCCM) are used to indicate the reason for the revocation or suspension. These must be approved by the Authorised Signatory(ies) and faxed to AIB Group (UK) p.l.c. The signed original copy(ies) of the request must be furnished to AIB Group (UK) p.l.c. as soon as possible.

Valid requests for revocations and suspensions will be processed within 1 hour of AIB Group (UK) p.l.c. acknowledging receipt of the request.

Where revocation is requested, AIB Group (UK) p.l.c. will initially request The Royal Bank of Scotland p.l.c. to suspend the Certificate until receipt of the signed original request, upon which time the Certificate will be fully revoked. AIB Group (UK) p.l.c. 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 Security Contact Certificate Management Forms (SCCM) are used to indicate the reason for reactivation of a suspended Certificate. These must be signed by the Authorised Signatory(ies) and the signed original copy(ies) of the SCCM form must be furnished to AIB Group (UK) p.l.c. Requests for re-activation will be assessed on a case by case basis.

#### **4.2.4 Suspension Period Limitations**

Suspension of Authorised Security Contact TrustAssured Service Identity Certificates may not exceed 30 days for any one period. If the suspension of an Authorised Security Contact's TrustAssured Service Identity Certificate is requested more than twice by the Customer or AIB Group (UK) p.l.c., 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 p.l.c., in line with Identrust requirements provides an online revocation checking facility for its TrustAssured 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 Identrust' 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 Security Contact Trust Assured 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. Where keys are centrally generated they are installed in compliance with The Royal Bank of Scotland p.l.c. 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 Security Contact 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 Royal Bank of Scotland p.l.c. 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 Codes

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

### 5.3 Certificate Profiles

Authorised Security Contact Trust Assured Service Qualified Identity Certificate Profile

Field	Content	Mandatory	Critical*
1. X.509v1 Field			
1.1. Version	v3	y	
1.2. Serial Number	Allocated automatically by the Issuing CA	y	
1.3. Signature Algorithm	SHA-1 with RSA Signature	y	
1.4. Issuer Distinguished Name		y	
1.4.1. Country (C)	GB	n	
1.4.2. Organization (O)	The Royal Bank of Scotland p.l.c.	y	
1.4.3. Organizational Unit (OU)	The Royal Bank of Scotland p.l.c. Identrust Infrastructure	y	
1.4.4. Common Name (CN)	The Royal Bank of Scotland p.l.c. Identrust CA	y	
1.5. Validity		y	
1.5.1. Not Before	e.g. "00:00:01 13 December 2000"	y	
1.5.2. Not After	e.g. "23:59:59 12 December 2003"	y	
1.6. Subject		y	
1.6.1. Country (C)	e.g., "GB" (entered by the RA)	n	
1.6.2. Organization (O)	e.g., "The XYZ Company" (entered by the RA)	y	
1.6.3. Organizational Unit (OU)	e.g., "International Financial Services" (entered by the RA)	y	
1.6.4. Common Name (CN)	e.g., "John Doe" (entered by the RA)	y	



Field	Content	Mandatory	Critical*
1.7. Subject Public Key Info	1024-Bit Public key encoded in accordance with IETF RFC3280 & PKCS#1	y	
2. X.509v3 Extensions			
2.1. Authority Key Identifier		y	n
2.1.1. Key Identifier	the Subject Key Identifier of the Issuer of this Certificate	y	
2.1.2. Authority Cert Issuer	Not present	n	
2.1.3. Authority Cert Serial Number	Not present	n	
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).	y	n
2.3. Key Usage		n	y
2.3.1. Digital Signature	Selected "1"	y	
2.3.2. Non Repudiation	Selected "1"	y	
2.3.3. Key Encipherment	Not selected "0"	y	
2.3.4. Data Encipherment	Not selected "0"	y	
2.3.5. Key Agreement	Not selected "0"	y	
2.3.6. Key Certificate Signature	Not selected "0"	y	
2.3.7. CRL Signature	Not selected "0"	y	
2.4. Certificate Policies		n	n
2.4.1. Policy Identifier	1.2.840.114021.1.30.2	y	
2.4.2. Policy Qualifier ID	1.3.6.1.5.5.7.2.2	y	
2.4.2.1. 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	y	
2.4.2.2. Policy Identifier	1.2.826.0.2.90312.10.1.2.1.1.4.0	n	
2.4.2.3. Policy Qualifier ID	1.3.6.1.5.5.7.2.2	n	
2.4.2.4. 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."	n	
2.5. Subject Alternate Names	Optional	n	n
2.5.1. rfc822 Name	e.g., "john.doe@XYZCorp.com"	y	
2.5.2. registered ID	Optional, "OID as per IP-NAMOID"	n	
2.6. Basic Constraints	Not present	n	
2.6.1. Subject Type	Not present	n	
2.6.2. Path Length Constraint	Not present	n	
2.7. Authority Information Access		y	n
2.7.1. Access Description		y	

Field	Content	Mandatory	Critical*
2.7.1.1. Access Method	On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	y	
2.7.1.2. Alternative Name	URL=https://vi.OCSP.rbs.co.uk	y	
2.7.2. Access Description			
2.7.2.1. Access Method	Identrust Certificate Status Check Protocol (1.2.840.114021.4.1)	y	
2.7.2.2. Alternative Name	URL=https://vi.TC.rbs.co.uk	y	
2.8. CRL Distribution Point		No	
2.9. 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

AIB Group (UK) p.l.c. Bacs Customer Service 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.

If you need this brochure in Braille, in large print or on audio, ring 0345 600 5925<sup>†</sup> or ask your relationship manager. Customers with hearing difficulties can use our Text Relay Service by dialling 18001 0345 6005 925<sup>†</sup>.

**Call into any branch | [aibni.co.uk](http://aibni.co.uk)**

<sup>†</sup>Calls may be recorded. Call charges may vary please refer to your service provider.



Information correct as at August 2020

The AIB logo and AIB (NI) are trade marks used under licence by AIB Group (UK) p.l.c. incorporated in Northern Ireland. Registered Office 92 Ann Street, Belfast BT1 3HH. Registered Number NI018800. Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.