

# Certificate Practice Statement

## I. INTRODUCTION

### A. Overview

This Equifax SecureMark Certificate Practice Statement (the “CPS”) presents the principles and procedures that Equifax plc. (“Equifax”) and GeoTrust, Inc. (“GeoTrust”) employ in the issuance and life cycle management of Equifax SecureMark Certificates (SecureMark is the registered trade mark of Equifax, Inc.) (the “Services”). This CPS and any and all amendments thereto are incorporated by reference into all Equifax SecureMark Certificates.

### B. Definitions

For the purposes of this CPS, all capitalised terms used herein shall have the meaning given to them in Section VIII, Definitions, or elsewhere in this CPS.

### C. Description and Use of Certificates

#### 1. Equifax Secure SecureMark Certificates

Equifax SecureMark Certificates are X.509 Certificates that chain to a Root CA, which the CA has S/MIME enabled to permit a consistent way to send and receive S/MIME data and provide limited authentication of a Subscriber’s browser. Acceptance of applications for SecureMark certificates will be based on the following guidelines: HM Government’s minimum requirements for validation and verification of the identity of individuals and organisations for Level 2 transactions as published on 12 February 2002 ([www.e-envoy.gov.uk](http://www.e-envoy.gov.uk)).

Equifax SecureMark Certificates have an Operational Period of three hundred and seventy-nine (379) days from the date of issuance, unless another time period or expiration date is specified on such Equifax SecureMark Certificate, or unless the Equifax SecureMark Certificate is revoked prior to the expiration of its Operational Period.

#### 2. Technical Requirements of Equifax SecureMark Certificates

In order to use an Equifax SecureMark Certificate, a Subscriber must use Lotus Notes Web Navigator 5.x (or later version), Netscape Navigator 4.X (or later version) or Microsoft Internet Explorer 4.X (or later version) (provided that any such browsers can accommodate 128 bit encryption).

---

## II. GENERAL PROVISIONS

### A. Obligations

#### 1. Equifax and GeoTrust Obligations

Equifax will perform limited authentication of Subscribers as detailed in this CPS and GeoTrust will issue Equifax SecureMark Certificates to the Subscribers after their successful authentication by Equifax in accordance with this CPS. Upon the revocation of an Equifax SecureMark Certificate, Equifax will notify GeoTrust, who will update the Certificate Revocation List accordingly, Equifax and GeoTrust will perform other functions which are described in more detail in this CPS.

## Certificate Practice Statement

### 2. Subscriber Obligations

Subscribers will submit truthful information about him/her, their business entity, and contacts, as applicable. Subscribers will at all times abide by this CPS and a Subscriber will immediately request revocation of an Equifax SecureMark Certificate if the related Private Key is Compromised. The Subscriber will only use the Equifax SecureMark Certificate for authenticating the Subscriber and/or utilising S/MIME applications. The Subscriber is solely responsible for the protection of his/her Private Key and shall notify Equifax immediately in the event that his/her Private Key has been Compromised.

### 3. Relying Party Obligations

Relying Parties must verify that the Equifax SecureMark Certificate is valid by examining the Certificate Revocation List before initiating a transaction involving such Equifax SecureMark Certificate.

Equifax and GeoTrust do not accept any responsibility whatsoever for reliance on an Equifax SecureMark Certificate that is on the Certificate Revocation List.

## **B. Limited Warranty/Disclaimer**

1. Equifax provides the following promise at the time the Equifax SecureMark Certificate is issued; (i) the information contained within the Equifax SecureMark Certificate accurately reflects the information provided to Equifax by the Applicant in all material respects; and (ii) Equifax has taken reasonable steps to verify that the information within the Equifax SecureMark Certificate is accurate. The nature of the steps Equifax takes to verify the information contained in an Equifax SecureMark Certificate is described in Section III of this CPS.

2. EXCEPT FOR THE PROMISE DESCRIBED ABOVE:

(I) (AND FOR ANY RIGHTS TO WHICH SUBSCRIBER, RELYING PARTY OR APPLICANT AS RELEVANT) IS ENTITLED AT LAW (INCLUDING THEIR RIGHT TO RECEIVE GOODS OF SATISFACTORY QUALITY AND FIT FOR PURPOSE AND A REASONABLE STANDARD OF SERVICE (MORE DETAILS REGARDING STATUTORY RIGHTS CAN BE OBTAINED BY CONTACTING YOUR LOCAL TRADING STANDARDS OR CITIZENS ADVICE BUREAU)), EQUIFAX DISCLAIMS ANY WARRANTIES (PROMISES) WITH RESPECT TO THE CERTIFICATE AND RELATED SERVICES PROVIDED BY EQUIFAX UNDER THIS AGREEMENT.

(II) EQUIFAX ONLY MAKES AVAILABLE THE CERTIFICATE AND THEREFORE CAN NOT WARRANT (PROMISE), AND CANNOT BE HELD RESPONSIBLE FOR, THE SECURITY OF ANY COMMUNICATIONS OR THE ACCURACY OF THE RESULTS OF ANY ENCRYPTION METHODS USED BY THE SUBSCRIBER, RELYING PARTY OR APPLICANT OR ANY OTHER PERSON WHICH ARE OUTSIDE OF EQUIFAX'S CONTROL.

## Certificate Practice Statement

- (III) THE SUBSCRIBER, RELYING PARTY OR APPLICANT (AS RELEVANT) ACKNOWLEDGES THAT THE ENCRYPTION INCLUDED IN THE CERTIFICATE PROVIDES SECURE ENCRYPTION BASED ON BEST INDUSTRY PRACTICE AND KNOWLEDGE AT THE TIME BUT THAT NO ENCRYPTION IS COMPLETELY SAFE AND THEREFORE THE SUBSCRIBER, RELYING PARTY OR APPLICANT (AS RELEVANT) IS URGED TO CONSIDER SUCH RISKS CAREFULLY BEFORE SENDING HIGHLY CONFIDENTIAL OR SENSITIVE INFORMATION VIA ELECTRONIC MEANS; AND
- (IV) GEOTRUST EXPRESSLY DISCLAIM AND MAKE NO OTHER REPRESENTATIONS, WARRANTIES OR COVENANTS OF ANY KIND, WHETHER EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, WITH RESPECT TO THIS CPS OR ANY EQUIFAX SECUREMARK CERTIFICATE ISSUED HEREUNDER, INCLUDING WITHOUT LIMITATION, ALL WARRANTIES OF SATISFACTORY QUALITY AND FITNESS FOR A PARTICULAR PURPOSE OR USE OF AN EQUIFAX SECUREMARK CERTIFICATE OR ANY SERVICE PROVIDED BY GEOTRUST AS DESCRIBED HEREIN, AND ALL WARRANTIES, REPRESENTATIONS, CONDITIONS, UNDERTAKINGS, TERMS AND OBLIGATIONS IMPLIED BY STATUTE OR COMMON LAW, TRADE USAGE, COURSE OF DEALING OR OTHERWISE ARE HEREBY EXCLUDED TO THE FULLEST EXTENT PERMITTED BY LAW. EXCEPT FOR THE LIMITED WARRANTY DESCRIBED ABOVE, GEOTRUST FURTHER DISCLAIMS AND MAKES NO REPRESENTATION, WARRANTY OR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, TO ANY APPLICANT, SUBSCRIBER OR ANY RELYING PARTY THAT THE RESULTS OF ANY CRYPTOGRAPHIC METHOD IMPLEMENTED IN CONNECTION WITH THE EQUIFAX SECUREMARK CERTIFICATE IS ACCURATE, AUTHENTIC, COMPLETE OR RELIABLE.
3. It is agreed and acknowledged that Applicants are liable for any misrepresentations made to Equifax and/or GeoTrust. Equifax and GeoTrust simply provide the Certificate and neither Equifax nor GeoTrust are responsible for the contents or intent behind the sending of any communications using the Certificate and therefore are not able to promise or guarantee under any circumstances that Subscribers and/or Relying Parties will honour any transaction entered into by the Subscriber and/or Relying Party involving the use of or reliance on an Equifax SecureMark certificate.
4. It is understood and agreed upon by Subscribers and Relying Parties that in using and/or relying on an Equifax SecureMark certificate they are (save for Equifax's promises as set out in paragraph B1 above) solely responsible for their reliance on that Equifax SecureMark certificate and that such parties must consider the facts, circumstances and context surrounding the transaction in which the certificate is used in determining such reliance.

## Certificate Practice Statement

5. The Subscribers and Relying Parties agree and acknowledge that each Equifax SecureMark certificate has a limited operational period and may be revoked at any time. Subscribers and Relying Parties are responsible for verifying whether an Equifax SecureMark certificate is expired or has been revoked. Equifax will not be responsible where Subscribers and Relying parties do not follow such procedures and where Equifax itself is not negligent or in breach of its obligations under this CPS. More information about the situations in which an Equifax SecureMark Certificate may be revoked can be found in section III I of this CPS.
6. Equifax and GeoTrust do not have any control over and therefore cannot provide any promises with respect to another party's software, hardware or telecommunications or networking equipment utilised in connection with the issuance, revocation or management of Equifax SecureMark Certificates or providing other services with respect to this CPS. Applicants, Subscribers and Relying Parties agree and acknowledge that neither Equifax is responsible or liable for any misrepresentations or incomplete representations of Equifax SecureMark Certificates or any information contained therein caused by another party's application software or graphical user interfaces. The cryptographic key-generation technology used by Applicants, Subscribers and Relying Parties in conjunction with the Equifax SecureMark Certificates may or may not be subject to the intellectual property rights of third parties. It is the responsibility of Applicants, Subscribers and Relying Parties to ensure that they are using technology which is properly licensed or to otherwise obtain the right to use such technology.

### C. Limitation on Liability

1. Applicants, Subscribers and Relying Parties agree that Equifax and its suppliers shall not in any circumstances be liable for any loss or damage at all arising from any inaccuracies, faults or omissions in, or in the provision of, the Service unless caused by its negligence or breach by Equifax of its obligations and promises under this CPS.
2. SUBJECT TO PARAGRAPH C7 BELOW, IN NO EVENT SHALL THE AGGREGATE LIABILITY OF EITHER EQUIFAX OR GEOTRUST FOR ALL CLAIMS RELATED TO THE USE OF OR RELIANCE ON AN EQUIFAX SECUREMARK CERTIFICATE OR FOR THE SERVICES PROVIDED HEREUNDER INCLUDING WITHOUT LIMITATION ANY CAUSE OF ACTION ARISING IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, FOR BREACH OF A STATUTORY DUTY OR IN ANY OTHER WAY EXCEED ONE THOUSAND POUNDS STERLING (£1,000.00)
3. Applicants, Subscribers and Relying Parties acknowledge that Equifax provides the Services at a price that does not reflect any benefit Applicants, Subscribers and Relying Parties may obtain from them, including any profit that they may make or the amount of any credit that they may give. Applicants, Subscribers and Relying Parties agree that, subject to paragraph C7 below, Equifax and its suppliers shall not in any circumstances be liable for:
  - (i) any damages or losses not caused by a breach of this CPS or failure or negligence on the part of Equifax;
  - (ii) any economic losses (including without limitation loss of revenues, profits, contracts, business or anticipated savings) which may arise where the

## Certificate Practice Statement

Subscriber, Relying Party or Applicant as applicable uses the Certificate in the course of a business);

- (iii) any loss of goodwill or reputation (which may arise where the Subscriber, Relying Party or Applicant as applicable uses the Certificate in the course of a business); or
  - (iv) any loss or damage that could not reasonably be foreseen by the Subscriber, Relying Party or Applicant as applicable and Equifax as likely to arise at the time that the subscriber Agreement was entered into.
4. The foregoing limitations of liability shall apply on a certificate-by-certificate basis, regardless of the number of transactions or claims related to each Equifax SecureMark certificate, and shall be apportioned first to the earlier claims to achieve final resolution.
  5. In no event will Equifax or its suppliers be liable for any damages to Applicants, Subscribers, Relying Parties or any other party arising out of or related to the use or misuse of, or reliance on any Equifax SecureMark Certificate issued under this CPS that: (i) has expired or been revoked; (ii) has been used for any purpose other than as set forth in the CPS (See Section I (C) and II (A) (2) for more detail); (iii) has been tampered with; (iv) with respect to which the Key Pair underlying such Equifax SecureMark Certificate or the cryptography algorithm used to generate such Equifax SecureMark Certificate's Key Pair, has been Compromised by the action of any party other than Equifax or GeoTrust (including without limitation the Subscriber or Relying Party); or (v) is the subject of misrepresentations or other misleading acts or omissions of any other party, including but not limited to Applicants, Subscribers and Relying Parties.
  6. In no event shall Equifax or its suppliers be liable to the Applicant, Subscriber, Relying Party or other party for damages arising out of any claim that an Equifax SecureMark Certificate infringes any patent, trademark, copyright, trade secret or other intellectual property right of any party.
  7. Nothing in this CPS shall exclude or limit the liability of Equifax for death or personal injury resulting from Equifax's negligence, or for fraud.

### **D. Force Majeure**

Equifax and its suppliers shall not be liable for any delay in, or failure of, performance of its obligations under this CPS arising from any cause beyond its reasonable control including any of the following: act of God, governmental act, war, terrorism, fire, flood, explosion or civil commotion, failure in information technology or telecommunications services, failure of a third party (including failure to supply data) and industrial action.

### **E. Financial Responsibility**

#### 1. Fiduciary Relationships

Neither Equifax nor GeoTrust is an agent, fiduciary, trustee, or other representative of the Applicant, Relying Party or Subscriber and the relationship between Equifax and GeoTrust and the Applicant and the Relying Party and the Subscriber is not that of an agent or a principal. Neither Equifax nor GeoTrust make any representations to the contrary, either explicitly, implicitly, by appearance or otherwise. Neither the

## Certificate Practice Statement

Applicant nor the Relying Party nor the Subscriber has any authority to bind Equifax or GeoTrust by contract or otherwise, to any obligation.

### 2. Indemnification by Applicant and Subscriber

Unless otherwise set forth in this CPS and/or Subscriber Agreement, Applicant and Subscriber, as applicable, hereby agree to indemnify and hold Equifax (including, but not limited to, each of its officers, directors, employees, agents, successors and assigns) harmless from any claims, actions, or demands that are caused by the use or publication of an Equifax SecureMark Certificate and that arise from (a) any false or misleading statement of fact by the Applicant (or any person acting on the behalf of the Applicant) (b) any failure by the Applicant or the Subscriber to disclose a material fact, if such omission was made negligibly or with the intent to deceive; (c) any failure on the part of the Subscriber to protect its Private Key or Equifax SecureMark Certificate or to take the precautions necessary to prevent the Compromise, disclosure, loss, modification or unauthorised use of the Private Key or Equifax SecureMark Certificate; or (d) any failure on the part of the Subscriber to promptly notify Equifax and GeoTrust, as the case may be, of the Compromise, disclosure, loss, modification or unauthorised use of the Private Key or Equifax SecureMark Certificate once the Subscriber has constructive or actual notice of such event

## F. Interpretation & Enforcement

### 1. Governing Law

This CPS shall be governed by and construed in accordance with the laws of England and Wales and shall be subject to the -exclusive jurisdiction of the courts of England and Wales.

### 2. Severability

If any provision of this CPS shall be held to be invalid, illegal, or unenforceable, the validity, legality, or enforceability of the remainder of this CPS shall not in any way be affected or impaired hereby.

### 3. Dispute Resolution Procedures

If any dispute, controversy or claim ("**Dispute**") arises under, in connection with or relating to this CPS or any Certificate issued by Equifax, then the parties shall first attempt to settle such Dispute in good faith. If the parties fail to settle the Dispute within 14 days of the Dispute arising, then either party may serve upon the other notice to commence a mediation to settle the Dispute. On receipt of such notice either party may within seven days notify *The Centre for Effective Dispute Resolution* ("**CEDR**") and request that a mediator be appointed. The mediation shall be deemed to have commenced upon the notification to both parties in writing of the appointment of a mediator by *CEDR* and upon written confirmation having been received by the parties of the mediator's acceptance of the appointment. There shall be one arbitrator appointed by *CEDR* who shall exhibit a reasonable familiarity with the issues involved or presented in such dispute, controversy or claim. The award of the arbitrator shall be binding and final upon all parties, and judgment on the award may be entered by any court having proper jurisdiction thereof. This CPS and the rights and obligations of the parties hereunder and under any Certificate issued by Equifax shall remain in full force and effect pending the outcome and award in any arbitration proceeding hereunder. In any arbitration arising hereunder, each party to the preceding shall be responsible for its own costs incurred in connection with the

## Certificate Practice Statement

arbitration proceedings, unless the arbitrator determines that the prevailing party is entitled to an award of all or a portion of such costs, including reasonable attorneys fees actually incurred.

### G. Repository

With regard to Equifax SecureMark Certificates, GeoTrust shall operate a Certificate Revocation List that will be available to both Subscribers and Relying Parties.

The repository is the official store for CRLS, directories and other status information (the "Repository"). Relying Parties wishing to validate certificate status should refer to the CDP field within the SecureMark certificates for the location of the Repository.

GeoTrust shall post the Certificate Revocation List every twenty-four (24) hours in a DER format

### H. Confidentiality Policy

#### 1. Individual Subscriber Information

Except as provided herein, certain information regarding Subscribers that is submitted on enrolment forms for Certificates will be kept confidential by Equifax (such as contact information for individuals and credit card information) and Equifax shall not release such information without the prior consent of the Subscriber. Notwithstanding the foregoing, Equifax may make such information available (a) to courts, law enforcement agencies or other third parties (including release in response to civil discovery) upon receipt of a court order or subpoena or upon the advice of Equifax's legal counsel, (b) to law enforcement officials and others for the purpose of investigating suspected fraud, misrepresentation, unauthorized access, or potential illegal activity by the Subscriber in the opinion of Equifax, (c) to an acquirer of Equifax or substantially all of the assets related to any portion of its business, to the extent that such information pertains to the acquired assets or line(s) of business, and (d) to third party service providers and vendors performing functions related to the Equifax products and services or as otherwise necessary for Equifax to perform its responsibilities under this Agreement, subject to such third parties' agreement to maintain the confidentiality of personally-identifiable Subscriber information. The foregoing confidentiality obligation shall not apply, however, to information appearing on Certificates, information relating to Certificate revocation, or to information regarding Subscribers that is already in the possession of or separately acquired by Equifax.

Subscriber acknowledges that Subscriber information will be controlled and processed in the United States, and to the extent that Subscriber is located outside the United States, Subscriber expressly consents to the transfer of such information to the United States for such control and processing.

#### 2. Aggregate Subscriber Information

Notwithstanding the previous Section, Equifax may disclose Subscriber information on an aggregate basis, and the Subscriber hereby grants to Equifax a license to do so, including the right to modify the aggregated Subscriber information and to permit third parties to perform such functions on its behalf.

## Certificate Practice Statement

### III. OPERATIONAL REQUIREMENTS

#### A. Application Requirements for an Equifax SecureMark Certificate

An Applicant for an Equifax SecureMark Certificate shall complete an Equifax SecureMark Certificate application in a form prescribed by Equifax. All applications are subject to review, approval and acceptance by Equifax. All Applicants are required to include a personal name and email address within an Equifax SecureMark Certificate application which will also appear on an Equifax SecureMark Certificate. An Equifax SecureMark Certificate may contain additional information as well.

#### B. Equifax SecureMark Certificate Information

##### 2. Organisational Name

If an Equifax SecureMark Certificate contains an Organisational Name, Equifax will make a reasonable attempt to establish that a request made on behalf of that organisation is legitimate and properly authorised. Equifax will not include an Organisational Name in an Equifax SecureMark Certificate without first ensuring the following: (a) the Organisational Name appears in conjunction with a country and possibly a state, region or province of other locality to sufficiently identify its place of registration or a place where it is currently doing business; and (b) in the case of an organisation that could reasonably be expected to be registered with a local, state or national authority, in certain circumstances Equifax will obtain, view and verify copies of the registration documents. For instance, Equifax may (i) verify the validity of the registration through the authority that issued it, or (ii) verify the validity of the registration through a reputable third party database or other resource, or (iii) verify the validity of the organisation through a trusted third party, or (iv) confirm that the organisation exists if such organisation is not the type that is typically registered or is capable of being verified under sub-clause (iii) above.

In addition, to prove that an Equifax SecureMark Certificate is duly authorised by the organisation, Equifax will typically request the name of a contact person who is employed by or is an officer of the organisation. Equifax will also typically require a form of authorisation from the organisation confirming its intent to obtain an Equifax SecureMark Certificate and will usually document the organisation's contact person. Equifax normally confirms the contents of this authorisation with the listed contact person.

##### 3. Personal Name

In the case of a personal name (i.e., the name of the Subscriber), Equifax will require proof of identity. Equifax will use all reasonable endeavours to obtain corroboration and confirmation of the personal name. For instance, Equifax may verify that the personal name is the name of the Subscriber by (a) the use of a Shared Secret or other similar form of identification, or (b) utilising existing credit or other databases, or (c) corroboration of the identity by having a number of existing identified Equifax SecureMark Certificate users attest to the identity.

##### 4. Email Address

In the case of an email address, Equifax will use reasonable endeavours to ascertain that the email address belongs to the Subscriber. At a minimum, Equifax will determine that the Subscriber has the ability to read email sent to that email address. In addition, Equifax may validate that the email address belongs to the Subscriber by

## **Certificate Practice Statement**

(a) the use of an Email Ping, or (b) obtaining proof that the Subscriber has the necessary mail server credentials to retrieve email sent to that email address, or (c) confirming from the email administrator or organisation owning the email domain name that they regard the Subscriber as a legitimate holder of a Certificate containing that email address.

### **C. Procedure for Processing Certificate Applications**

Equifax will process the Equifax SecureMark Certificate applications to confirm the information on the Equifax SecureMark Certificates as set out in paragraph B above. However, Equifax reserves the right to waive such procedures and issue an Equifax SecureMark Certificate utilising different authentication procedures in certain circumstances; provided that the general principles for verifying the application information are maintained. In addition, Equifax or GeoTrust may use subcontractors or other third parties to assist in the performance of its operational requirements or any other obligation under this CPS.

### **D. Application Issues**

At certain times during the application process in which Equifax is not able to verify information in an Equifax SecureMark Certificate application, a customer service representative may be assigned to the Applicant to facilitate the completion of the application process. Otherwise, the Applicant may be required to correct its associated information with third parties and re-submit its application for an Equifax SecureMark Certificate

### **E. Certificate Delivery**

If Equifax finds that the Applicant's Equifax SecureMark Certificate application was sufficiently verified, then Equifax will notify GeoTrust and GeoTrust will sign the Applicant's Equifax SecureMark Certificate. Upon signing the Applicant's Equifax SecureMark Certificate, GeoTrust will return the signed Equifax SecureMark Certificate to Equifax. Equifax will notify the Applicant via email and send such email to the appropriate contact. The email will include the date the Equifax SecureMark Certificate was issued, the date the Equifax SecureMark Certificate will expire and the relevant URL for the Applicant's use in retrieving the Equifax SecureMark Certificate. In certain circumstances the email may include an Equifax customer service representative telephone number and email address for any technical or customer service problems.

### **F. Certificate Acceptance**

The Applicant expressly indicates acceptance of an Equifax SecureMark Certificate by using such Equifax SecureMark Certificate.

### **G. Certificate Renewal**

The Subscriber is required to generate a new Public Key and complete a new Equifax SecureMark Certificate request before the Subscriber will be able to obtain a renewal Equifax SecureMark Certificate.

### **H. Certificate Expiration**

Equifax will attempt to notify all Subscribers of the expiration date of their Equifax SecureMark Certificate.

## Certificate Practice Statement

### I. Certificate Revocation

#### 1. Circumstances For Revocation

Equifax SecureMark Certificate revocation is the process by which the Operational Period of an Equifax SecureMark Certificate is prematurely ended.

##### a. Permissive Revocation

A Subscriber may request revocation of its Equifax SecureMark Certificate at any time for any reason.

##### b. Required Revocation

A Subscriber shall inform Equifax and promptly request revocation of an Equifax SecureMark Certificate:

- whenever any of the information on an Equifax SecureMark Certificate changes or becomes obsolete; or
- whenever the Private Key, or the media holding the Private Key, associated with the Equifax SecureMark Certificate is Compromised; or

Equifax shall revoke a Certificate:

- upon request of a Subscriber;
- If the Private Key used to sign an Equifax SecureMark Certificate has been compromised;
- upon the Subscriber's breach of either this CPS or Subscriber Agreement;
- if Equifax determines that the Equifax SecureMark Certificate was not properly issued or the Subscriber's Private Key has been compromised.

In the event that Equifax ceases operations, all Equifax SecureMark Certificates issued by Equifax shall be revoked prior to the date that Equifax ceases operations.

#### 2. Who Can Request Revocation

The only persons permitted to request revocation of or revoke an Equifax SecureMark Certificate issued by Equifax are the Subscribers and Equifax.

#### 3. Procedure For Revocation Request

The Subscriber must contact Equifax, either by a national/regional postal service, facsimile or overnight courier, and request revocation of an Equifax SecureMark Certificate. Equifax may also accept email requests to request revocation from Subscribers but is not required to do so without supporting verification. Equifax shall revoke such Equifax SecureMark Certificate within the next business day by notifying GeoTrust, who will then update the Certificate Revocation List.

## Certificate Practice Statement

### **J. Records Archival**

Equifax shall maintain and archive records relating to the issuance of the Equifax SecureMark Certificates for seven (7) years following the issuance of the applicable Equifax SecureMark Certificate.

---

## **IV. SECURITY CONTROLS**

### **A. Equifax Secure Physical Security Controls**

Equifax and GeoTrust currently utilise one of the largest secure data centres in the world, in order to accommodate the special needs of operating a public key infrastructure.

### **B. Features of Equifax Electronic Commerce Solutions Operations Centre**

- Slab to slab barriers
- Electronic control access systems
- Alarmed doors and video monitoring
- Security logging and audits
- Card key access for specially approved employees with defined levels of management approval required
- Quarterly reviews for continued need of access
- Annual re-certification of access privileges
- Annual formal audit of all management processes and control processes
- Conditions of employment guidelines for all employees

---

## **V. TECHNICAL SECURITY CONTROLS**

### **A. Root Key Generation**

Key Pair generation is performed on a highly secure hardware device (either nCipher or IBM 4758 cryptographic processor).

### **B. Root Key Management**

The Root Keys are maintained in a trusted and highly secured environment with backup and key recovery procedures. In the event of the Compromise of the Root Key(s), Equifax shall promptly notify the Subscribers and revoke all Equifax SecureMark Certificates issued with such Root Key(s).

## **VI. CPS ADMINISTRATION**

### **A. CPS Change Procedures**

From time to time it may be necessary to make changes to the CPS. Certificates are subject to the CPS in effect at the time the Certificate was issued. All active CPS will be published on the Equifax web site under the applicable, related dates. In the event, a change in the CPS would be retroactively applicable, a notice will be sent to the affected Subscribers and a notice published to Relying Parties at the Equifax web site.

## Certificate Practice Statement

---

### VII. GENERAL PROVISIONS

#### A. Conflict of Provisions

This CPS represents the entire agreement between any Subscriber (including the Subscriber Agreement, if any) or Relying Party and Equifax and supersedes any and all prior understandings and representations pertaining to its subject matter. In the event, however, of a conflict between this CPS and any other express agreement a Subscriber has with Equifax with respect to an Equifax SecureMark Certificate, including but not limited to a Subscriber Agreement, such other agreement shall take precedence.

#### B. Waiver

A failure or delay in exercising any right or remedy hereunder shall not operate as a waiver of that right or remedy, nor shall any single or partial exercise of any right or remedy preclude any other or further exercise thereof or the exercise of any other right or remedy.

#### C. Severance

If any provision of this CPS is or becomes invalid or unenforceable it will be severed from the rest of this CPS so that it is ineffective to the extent that it is invalid or unenforceable and no other provision of this CPS shall be rendered invalid, unenforceable or be otherwise affected.

#### D. Export

Subscribers and Relying Parties acknowledge and agree to use the Equifax SecureMark Certificates in compliance with all applicable laws and regulations. Equifax may refuse to issue or may revoke an Equifax SecureMark Certificate if in its reasonable opinion such issuance or the continued use of such Equifax SecureMark Certificate would contravene applicable laws and regulations.

---

### VIII. DEFINITIONS

**Applicant.** A person or authorised agent that requests the issuance of an Equifax SecureMark Certificate.

**Certificate.** A record that, as a minimum: (a) identifies the CA issuing it; (b) names or otherwise identifies its Subscriber; (c) contains a Public Key that corresponds to a Private Key under the control of the Subscriber; (d) identifies its Operational Period; and (e) contains a Certificate serial number and is digitally signed by the CA.

**Certificate Revocation List.** A time-stamped list of revoked Certificates that has been digitally signed by the CA.

**CA/Certification Authority.** An entity which issues Certificates and performs all of the functions associated with issuing such Certificates.

**Certificate Distribution Point (CDP).** Also known as CRL Distribution Point or Certificate Revocation List Distribution Point. This field is within the certificate and contains a URL that provides access to the current published Certificate Revocation List.

## Certificate Practice Statement

**Compromise.** Suspected or actual unauthorised disclosure, loss, loss of control over, or use of a Private Key associated with Certificate.

**CRL.** See Certificate Revocation List.

**DER (Distinguished Encoding Rules).** A standard used to format information within the Repository for access by Relying Parties and Subscribers.

**Email Ping.** A correspondence sent to the email address to which the recipient of the email must reply as proof of receipt

**Extension.** A means to place additional information about a Certificate within a Certificate. The X.509 standard defines a set of Extensions that may be used in Certificates.

**Key Pair.** Two mathematically related keys, having the following properties: (i) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally impractical to discover the other key.

**Operational Period.** A Certificate's period of validity. It would typically begin on the date the Certificate is issued (or such later date as specified in the Certificate), and ends on the date and time it expires as noted in the Certificate or is earlier revoked unless it is suspended.

**Private Key.** The key of a Key Pair used to create a digital signature. This key must be kept a secret.

**Public Key.** The key of a Key Pair used to verify a digital signature. The Public Key is made freely available to anyone who will receive digitally signed messages from the holder of the Key Pair. The Public Key is usually provided via a Certificate issued by the CA. A Public Key is used to verify the digital signature of a message purportedly sent by the holder of the corresponding Private Key.

**Relying Party.** A recipient of a digitally signed message who relies on a Certificate to verify the digital signature on the message. Also, a recipient of a Certificate who relies on the information contained in the Certificate.

**Repository.** The database where certificates and revocation status information such as CRL's are stored. The official designation of a database as a repository is intended to signal that the operation of the facility is reliable and trustworthy.

**Root CA (Root Certificate Authority).** The authority that the certificate-using application trusts and has securely imported and stored its public key. These roots are often pre-loaded in browsers and shipped or downloaded to the user as part of installing the browser.

**Root Key(s).** The Private Key used by GeoTrust to sign the Equifax SecureMark Certificates.

**S/MIME (Secure Multipurpose Internet Mail Exchange).** A set of specifications that provides a way to securely enable multimedia email among many different computer systems that use Internet mail standards.

**Shared Secret.** Information not in the public domain and known only by the Applicant or Subscriber

**Subscriber.** A person or entity who (1) is the subject named or identified in a Certificate issued to such person or entity, (2) holds a Private Key that corresponds to a Public Key listed

## Certificate Practice Statement

in that Certificate, and (3) the person or entity to whom digitally signed messages verified by reference to such Certificate are to be attributed. For the purpose of this CPS, a person or entity who applies for a Certificate by the submission of an application is also referred to as a Subscriber.

**X.509.** An International Telecommunication Union / Telecommunication Standardisation Secure and ISO/International Electro-technical Commission (IEC) certificate format standard with versions published in 1988 (v1), 1993 (v2), and 1996(v3) to allow additional extension fields. An X.509v3 certificate encompasses