CERTIFICATION PRACTICE STATEMENT

In Relation To The Unipass Digital Certificate Service

Version 5.5
Publication Date: April 2021

ISBN 0-9653555-4-3

Contents

Page

1 INTRODUCTION

1.1 Overview

1.1.1 Unipass Service and Certificates

This Certification Practice Statement ("CPS") describes the Unipass Service provided by Origo Secure Internet Services Limited ("OSIS") to members of the Unipass Community. Capitalised words have the meaning defined in Appendix 1 to this CPS. Abbreviations and acronyms have the meaning defined in Appendix 2 to this CPS. The CPS constitutes a "Certificate Policy" as defined by the X.509 Standard (ISO/IEC 9594-8). The CPS is subject to change in accordance with Section 11.

The main element of the Unipass Service is the OSIS Public Key Infrastructure ("Unipass PKI") consisting principally of:

- Unipass Certificates;
- The Certificate Revocation Status Service ("CRSS"), which must be used by Organisations who automate reliance on Certificates presented to them; and
- The Repository, which is a database for storing and retrieving Certificates and other information related to Certificates.

OSIS currently offers three different types of Certificate:

- Individual Certificates – which identify an Individual;
- Organisation Certificates – which identify an Organisation (or Associated Company if applicable); and
- Trial Certificates – which an Organisation (or Associated Company or Network Member if applicable) can use only for testing purposes.

In relation to the use of Certificates, it should be noted that:

- All Individuals who receive an Individual Certificate must first accept the "Individual Certificate Rules of Use". In addition, their Organisation must also first accept an appropriate "Organisation Contract" (depending on the type of Organisation);
- All Organisations that receive an Organisation Certificate must first accept an appropriate "Organisation Contract" (depending on the type of Organisation and intended use of the Unipass Service);
- All Individuals that wish to receive a Trial Certificate must agree to use the Trial Certificate in accordance with "Unipass Trial Certificate Terms and Conditions" (which normally take the form of online terms and conditions which must be accepted before a Trial Certificate can be collected or used). In some instances where the Trial Certificates will not denote that they are for trial use or where access to the CRSS is required, then the relevant Organisation must also enter into a contract with OSIS;
- A Certificate is not evidence of authority and shall not be accepted as such;
- Only members of the Unipass Community shall be entitled to use or rely on any Certificate issued as part of the Unipass Service; and
- Certificates are issued as part of the Unipass Service only for use by members of the Unipass Community in order to conduct business with other members of the Unipass Community.

1.1.2 Organisations

There are currently two broad groups of Organisation that can receive the Unipass Service as follows:

- Relying Party Organisations, who rely on Unipass to authenticate users of their electronic services; and
- End User Organisations, who use Unipass Certificates as credentials when challenged for authentication while using electronic services.

1.1.2.1 Relying Party Organisations

All Relying Party Organisations are required to sign an appropriate Relying Party Organisation Contract (which incorporates this CPS) before the Unipass Service is made available to them. As is stated in the definition of "Relying Party Organisation" there are a variety of different types of relying party and, depending on what type of organisation is involved, a different form of Relying Party Organisation Contract shall be supplied by OSIS as part of membership of the Unipass Community for use of the Unipass Service.

In certain circumstances where the Relying Party Organisation Contract permits, Certificates may be issued to certain third parties (including without limitation Associated Companies and their Individuals and Nominated Persons). In such circumstances, the rights and obligations of such third parties are set out in the Relying Party Organisation Contract. The Relying Party Organisation shall ensure that any such third parties shall abide by the rules governing the use of the Unipass Service as laid down in the Relying Party Organisation Contract and this CPS.

All Individuals of Associated Companies or Network Members must also accept the Individual Certificate Rules of Use.

1.1.2.2 End User Organisations

All End User Organisations are required to sign an appropriate End User Organisation Contract before the Unipass Service is made available to them.

1.2 Provision of the Unipass Service

1.2.1 Elements of the Unipass Service

The elements of the Unipass Service which could potentially be made available to members of the Unipass Community are:

- The Certificate Revocation Status Service ("CRSS") to facilitate reliance on certificates presented as authentication credentials;
- Individual Certificates for use by the Individuals of the relevant Organisation, if required;
- Trial Certificates to facilitate testing of the Unipass Service; and
- Organisation Certificate(s) for use by the Organisation and each Associated Company (if applicable), if required.

1.2.2 OSIS' Suppliers

OSIS may provide the Unipass Service to members of the Unipass Community using a number of Suppliers. This includes without limitation the use of Suppliers to provide OSIS' Certification Authority ("CA") service.

1.2.3 OSIS' Right to Refuse

OSIS may refuse to issue a Certificate to any person, at their sole discretion, without OSIS or its Suppliers incurring any liability or responsibility for any loss or expenses arising out of such refusal.

1.2.4 Role of Unipass Controllers and Nominated Persons

To make it easier for Organisations to manage applications from Individuals within their Organisation to use Individual Certificates, an Organisation can appoint an officer, partner, principal, director or employee of the Organisation to act as a Unipass Controller. The Organisation must take care to make sure that the person they appoint as a Unipass Controller meets the Trusted Role Requirements. Once appointed, the Unipass Controller must fulfil his role in accordance with the Unipass Controller Guidelines and the other provisions of the Individual Certificate Rules of Use.

The first Individual from an Organisation that applies for a Unipass Certificate is automatically by default appointed by that Organisation as a Unipass Controller. On receiving their Unipass Certificate that Individual may appoint another Individual as a Unipass Controller and/or remove their own status as a Unipass Controller.

Where an Organisation Certificate is to be issued, the Organisation must appoint a Nominated Person to apply for the Organisation Certificate on its behalf. The Nominated Person can be an officer, partner, principal, director employee and/or sub-contractor of the Organisation. The Organisation must take care to make sure that the person they appoint as a Nominated Person meets the Nominated Person Requirements. Once appointed, the Nominated Person must fulfil his role in accordance with the Nominated Person Guidelines and the relevant Organisation Contract.

1.3 Structure of the CPS

The CPS takes a life cycle approach to describing the issue and management of Unipass Certificates. The stages and steps of the process from application through to accepting, installing and managing an Individual Certificate in the Individual's browser or an Organisation Certificate on the Organisation's (or, where appropriate, its Associated Companies') server(s) are as described below.

1) Application (in accordance with Section 4)
2) Validation of application and notification of results (in accordance with Section 5)
3) Certificate collection (in accordance with Section 6)
   a) Authentication and acceptance of terms
   b) Certificate Signing Request generation and Certificate issuance
   c) Certificate installation
4) Expiry and renewal (in accordance with Section 8)
   a) Renewal by authentication and confirmation of details before Certificate expiry
   b) Obtaining a new Certificate after Certificate expiry
5) Revocation and contract cancellation and (in accordance with Section 8) 6) Change of details (in accordance with Section 9).

The life cycle is defined in more detail in Sections 4 to 9.

1.4 Accessing this CPS

This CPS is published in electronic form and may be downloaded from the Unipass Website at **www.unipass.co.uk.**

1.5 Education and Training

Before engaging in the Unipass Service, Individuals and Organisations should ensure they have received adequate training. This CPS assumes that the reader has some understanding of PKI and the use of Certificates.

1.6 Contact Details

All enquiries on this CPS should be directed to: customerservices@origo.com.

2 THE UNIPASS SERVICE

2.1 Purpose

The role of the Unipass Service is to facilitate electronic commerce by providing Certificates and associated components of the Unipass PKI to satisfy Individuals' and Organisations' technical and business needs for certain Security Mechanisms. Certificates only provide evidence of identity (and not authority) as set out in Sections 2.3.1, 2.3.2 and 7.2.

2.1.1 Role of the Unipass PKI

The Unipass PKI serves to facilitate the confirmation of the relationship between Public Keys and members of the Unipass Community. Such confirmation is represented by Certificates issued by OSIS. The process of Certificate management includes the activities of registration (naming, appropriate applicant authentication, issuance and acceptance), management and audit-trail generation.

2.2 Exclusions

The Unipass PKI supports a variety of Security Mechanisms to protect communications and information assets, which may be used by Individuals and Organisations. Certificates alone, however, do not constitute such a mechanism. Organisations acknowledge that they and not OSIS are responsible for the selection and use of appropriate Security Mechanisms and items (software, hardware and Encryption devices) for their own individual purposes and where appropriate for their Individuals', Associated Companies' and Network Members' purposes. OSIS is not responsible for the provision of these Security Mechanisms and items and does not accept liability for them.

2.3 Certificates and suitability for purpose

All Individual Certificates and Organisation Certificates are issued to provide for a general purpose level of trust. Individuals and Organisations must ascertain whether the set of service qualities associated with Individual Certificates and Organisation Certificates (as appropriate) adequately meets their needs.

OSIS makes its CPS publicly available so that users have sufficient information to make their own evaluation before applying for, using, or relying on any Certificate issued as part of the Unipass Service.

OSIS does not provide any recommendation or endorsement of Individual Certificates or Organisation Certificates for any particular application or purpose. Each Individual and Organisation (or Associated Company or Network Member where applicable) is responsible for assessing whether Individual Certificates and/or Organisation Certificates are appropriate for any particular application or intended purpose, and OSIS shall have no liability or responsibility in this regard.

2.3.1 Individual Certificates

Description: Individual Certificates confirm that the information provided by the Individual has been validated by the Help Desk and/or Unipass Controller (as appropriate) as confirming that the Individual is a member of an eligible Organisation (or Associated Company or Network Member where applicable).

Following the submission of an application, the enrolment information submitted by the Individual Certificate applicant will be confirmed in accordance with the specific procedures set out in Sections 4 and 5. Based upon such confirmation, OSIS will either approve or reject the application in accordance with Section 5.

Assurance level: In order to obtain Individual Certificates, various procedures are utilised (as set out in Sections 4 and 5) to validate Organisations and obtain evidence of the identity of Individual Certificate applicants. The validation procedures provide assurances of an Individual's identity, and the requirements for "off-line" communication with the Individual and confirmation of information about the Organisation via third parties provide further assurance of trustworthiness.

2.3.2 Organisation Certificates

Description: Organisation Certificates confirm that the information provided by the Organisation has been validated by OSIS as confirming the existence and eligibility of the Organisation. Following the submission of an application to OSIS from the Organisation, the enrolment information submitted will be confirmed in accordance with the specific procedures set out in Sections 4 and 5. Based upon such confirmation, OSIS will either approve or reject the application in accordance with Section 5.

Assurance Level: In order to obtain Organisation Certificates, various procedures are utilised (as set out in Sections 4 and 5) to validate Organisations. The validation procedures provide assurances of an Organisation's identity and confirmation of information about the Organisation via third parties provide further assurance of trustworthiness.

2.3.3 Trial Certificates

Description: Trial Certificates are for in-house testing and assessment purposes only and must not be used for any transaction which has economic value or which affects the rights and liabilities of the communicating parties or any other party. The information contained within a Trial Certificate is non-verified information. All Organisations shall ensure that only members of their staff (and/or certain subcontractors approved in advance by OSIS) can be issued with or otherwise use Trial Certificates and that such persons abide by the "Unipass Trial Certificate Terms and Conditions". Please note that these terms and conditions (a copy of which is available upon request) are displayed or sent by OSIS (depending on the precise circumstances of use of a Trial Certificate) to all persons who receive a Trial Certificate at the time of collection.

Assurance Level: None. OSIS shall have no liability for any costs, claims, expenses, loss and/or damage arising under or in connection with Trial Certificates, whether arising in contract, tort (including negligence) or otherwise and including any liability arising by virtue of OSIS' employees, agents or contractors and Suppliers in connection with Trial Certificates.

All warranties and conditions, whether express or implied by statute, common law or otherwise (including, but not limited to, as to fitness for purpose or satisfactory quality) in relation to Trial Certificates are hereby excluded to the extent permitted by law.

2.4 Protection of the Private Keys of OSIS' signing Certificates

The Private Keys of all CA Certificates are secured against compromise including by using trustworthy hardware products meeting at least FIPS 140 – 1 level 3.

2.5 Third Party Software

OSIS publishes details of any specified third party software that is required to use the Unipass Service on the Unipass Website. Individuals and Organisations are responsible for obtaining such third party software and OSIS shall have no liability in such regard. OSIS shall also have no liability in relation to the operation or use of such software or, in the event that such third party software is changed, for its continued compatibility with the Unipass Service.

2.6 Private Key Protection

OSIS strongly recommends that the secrecy and integrity of Private Keys should be protected through the use of software and passwords or PINs.

Any loss, disclosure, modification, unauthorised use or other compromise of any Private Key is not the responsibility of OSIS and OSIS shall have no liability in this regard.

2.6.1 Individual Certificates

Individuals are obliged to keep secure the Private Keys of their Individual Certificates in accordance with the Individual Certificate Rules of Use.

Organisations are obliged in their Organisation Contract to procure that their Individuals, and also Individuals of their Associated Companies or Network Members (where applicable), comply with the Individual Certificate Rules of Use.

2.6.2 Organisation Certificates

Organisations are obliged to keep secure the Private Keys of their Organisation Certificates in accordance with their Organisation Contract.

Where Associated Companies have an Organisation Certificate, their Organisations are also obliged in accordance with their Organisation Contract to procure that these Associated Companies keep their own Private Keys secure.

Each Organisation must take all necessary precautions to prevent the loss, disclosure, modification, unauthorised use or other compromise of its Private Key or Private Keys and where appropriate, each Organisation must also ensure that each Associated Company takes all necessary precautions to prevent the loss, disclosure, modification, unauthorised use or other compromise of its Private Key or Private Keys, including use of appropriate physical, logical and network access controls and associated monitoring mechanisms.

2.7 PKI Hierarchies

2.7.1 Certificate Chains and Types of CAs

A PKI provides and uses chains of Certificates. Certificates are linked together in chains by means of the identifiers (the mandatory issuerName and SubjectName Fields) and Digital Signatures they contain. Chains enable users to validate and rely upon Certificates other than their own.

In any PKI, a chain is composed of a Certificate from the lowest level of the hierarchy (the one being used or relied upon) and at least one CA Certificate (i.e. at least the Certificate for the CA that issued the lowest level Certificate in question). The number of CA Certificates present in a chain depends on the configuration of the hierarchy. Each CA Certificate in a chain may identify a CA of one of the following types:

- the Root CA;
- CA for another CA; and
- CA for customers.

The Root CA Certificate is issued to and by the Root CA itself and is therefore 'self-signed' by its own Private Key. The signature may be verified by means of the Root CA's Public Key (contained in the same Certificate). As a self-signed Certificate provides no intrinsic protection against forgery, it is normal to provide users with other means to verify that the Root CA Certificate is valid. Such self-signed certificates are commonly trusted by verifying their thumbprints directly with the certificate subject.

A CA other than a Root CA must be *subordinate to* another CA, therefore its Certificate is signed by the superior CA's

Private Key, and the signature may be verified by means of the superior CA's Public Key contained in that CA's Certificate. Subordination is denoted by the issuerName field in the Subordinate CA Certificate identifying the superior CA.

2.7.2 Unipass PKI Hierarchy

The Unipass PKI is established as a private, rather than public, hierarchy.

The G3 Unipass Certificate hierarchy has been in operation since 5th July 2015. G3 is composed solely of a root CA (Origo Root CA – G3). The thumbprint of this certificate is: **3CA4 8782 C087 6732 A309 C48A BFE0 3858 BC85 3B63** . The Origo Root CA key size remains 4096 bits. A trustworthy hardware device (FIPS 140-1 Level 3 certifiable) will be used to create, protect, and destroy its Private Key. The Origo Root CA – G3 currently signs directly all Individual Certificates, Organisation Certificates and Trial Certificates issued as part of the Unipass Service.

2.8 Certificate Structure

The Unipass PKI supports the use of X.509 v3 Certificates. X.509 v3 Certificates include the ability to add Certificate Extensions.

2.8.1 Certificate Extensions

Certificate Extensions are optional fields of a Certificate that provide various management and administrative controls useful for authenticating large-scale Certificate user populations for multiple purposes. Information contained in certain extensions may be duplicated elsewhere in the Certificate. The extensions defined for the Unipass PKI provide the following controls:

- whether a Certificate can be used by a CA to issue other Certificates and therefore can be relied upon as part of a Certificate chain;
- the security services with which the Certificate is intended to be used (some of these security services are required by the Unipass PKI itself);
- appropriate reference to this CPS;
- the location from which revocation information may be obtained; and
- the Certificate type as recognised by Netscape browsers and other software.

Neither Individuals nor Organisations nor Associated Companies nor Network Members are able to define additional "private" extensions for purposes or modes of use other than those defined in this CPS, e.g. specific to a particular application environment.

Tables 1(a) and 1(b) summarise the typical contents of Certificate Extensions for each type of Certificate implemented for the Unipass PKI.

Name	Described in	Value
Basic Constraints	Section 2.8.3.1	Critical Subject Type=CA Path Length Constraint=0
Key Usage	Section 2.8.3.2	Critical Certificate Signing, Off-line CRL Signing, CRL Signing (06)

Table 1a – OSIS Certificate extensions (for root CA)

Name	Described in	Value
Basic Constraints	Section 2.8.3.1	Non Critical Subject Type=End Entity Path Length Constraint=None
Key Usage	Section 2.8.3.2	Non Critical Digital Signature, Key Encipherment (a0)
Certificate Policies	Section 2.8.3.3	Non Critical [1]Certificate Policy: PolicyIdentifier=1.2.826.0.2.201466.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.unipass.co.uk/cps [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= *Warning: Do not use this certificate unless you* are a member *of the Unipass Community. OSIS accepts no liability for unauthorised use. You MUST read www.unipass.co.uk/tou for more details.*

CRL Distribution Points	Section 2.8.3.4	Non Critical [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://onsitecrl.trustwise.com/OrigoSecureInternetServicesLtdOrigoRootCAG3/LatestCRL.crl Note: the above URL is the X.509 version. The PKCS#7 version is at: http://onsitecrl.trustwise.com/OrigoSecureInternetServicesLtdOrigoRootCAG3/LatestCRL and the LDIF version is at http://onsitecrl.trustwise.com/OrigoSecureInternetServicesLtdOrigoRootCAG3/LatestCRL.ldif
Authority Information Access	Section 2.8.3.5	Non Critical [1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://unipass-ocsp.trustwise.com

Table 1b – OSIS Certificate extensions (Individual & Organisation certificates)

The extensions and the meaning of the entries in Tables 1(a) and 1(b) are described further in the remainder of Section 2.8.

2.8.2 Function and Criticality of Extensions

The function of each extension is indicated by a standard Object Identifier value corresponding to the name given in Tables 1(a) and 1b). Usually this identifier is not human readable, but some software may be able to display it. Additionally, each extension in a Certificate is assigned a "criticality" true/false value. The presence of each criticality value upon a specific extension is as follows:

- true (i.e. "a critical extension") requires any person validating the Certificate (and in particular, hardware or software which has been activated or operated by or on behalf of the person to do so, referred to as "Certificate Validating Software"), who (or that) cannot recognise and process the content of the extension in accordance with the applicable definition, to consider the Certificate to be invalid; if it can recognise and process the content of the extension and obtains a negative result, depending on the applicable definition, it will also consider the Certificate to be invalid. • false (i.e. "a non-critical extension") requires Certificate Validating Software (as defined above) to either process the content of the extension in accordance with the applicable definition, or ignore the extension entirely; so, if the extension is processed but a negative result arises – depending on the applicable definition - the entire Certificate will be considered to be invalid, as above, but if the extension is not processed, Certificate validity does not depend on the extension value at all.

Certificate Validating Software that processes extensions (depending on the applicable definition and the criticality of the extension) with a negative result will consider the whole Certificate to be invalid, irrespective of whether it would be valid for other reasons defined in this CPS (e.g. not expired, not revoked etc.).

2.8.3 Defined Extensions

Certificates issued from the Unipass PKI contain the following extensions whose meaning is defined by the organisations indicated (ISO, IETF or Netscape).

2.8.3.1 ISO-Defined Basic Constraints Extension

The Basic Constraints extension serves to delimit the role and position that a CA Certificate, Individual Certificate or Organisation Certificate plays in a chain of Certificates, and therefore identify whether the Certificate is a CA Certificate, or either of an Individual Certificate or Organisation Certificate as follows:

- if a Certificate contains a Basic Constraints extension that permits it to be used as a CA Certificate it identifies a CA (as defined above);
- if a Certificate contains a Basic Constraints extension that prevents it from being used as a CA Certificate it identifies an Individual in relation to an Individual Certificate, or an Organisation, in relation to an Organisation Certificate.

The Basic Constraints extension in CA Certificates also define by means of a specified path length how many CAs may appear subordinate to it in any Certificate chain.

2.8.3.2 ISO-Defined Key Usage Extension

The Key Usage extension serves to limit the technical purposes for which a Certificate may be used as follows:

- CA Certificates contain a Key Usage extension that limits the corresponding Private Key to be used for signing Certificates and Certificate Revocation Lists;
- Individual Certificates and Organisation Certificates contain a Key Usage extension that limits the corresponding Private Key to be used to generate Digital Signatures and to encipher other keys; and

- Individual Certificates are suitable for SSL clients and S/MIME e-mail and Organisation Certificates are suitable for SSL clients and in particular digitally signing XML messages transmitted between Organisations.

Therefore no Certificate in the Unipass PKI is indicated as being suitable for object signing or data Encryption (i.e. Encryption of persistent files rather than e-mail messages).

2.8.3.3 ISO-Defined Certificate Policy Extension

The Certificate Policy extension limits a Certificate to the practices required by (or indicated to) Individuals, Organisations, Associated Companies or Network Members who are relying on Certificates as follows:

- It denotes this CPS by means of its Object Identifier (as assigned by OSIS) as the applicable definition of the practices required by (and indicated to) Individuals, Organisations, Associated Companies or Network Members who are relying on those Certificates;
- It contains a notice warning Individuals, Organisations, Associated Companies or Network Members (or any other party that may attempt to rely upon the Certificate) of the applicable terms and conditions associated with the use of, and reliance on, the Certificate.

A warning notice is provided in the Certificate as follows:
"*Warning: Do not use this certificate unless you* are a member *of the Unipass Community. OSIS accepts no liability for unauthorised use. You MUST read* ***www.unipass.co.uk/tou*** *for more details.*"

If Certificate Validating Software can process this extension, it may allow Individuals, Organisations, Associated Companies or Network Members to display both the reference to the CPS (and other applicable documents held on the Unipass Website), and the warning notice.

If it cannot process this extension, OU Attributes in the SubjectName Field (see Section 2.8.5) are provided for the same purpose. In addition, a further reference to a summary of the terms of use for Certificates is provided in one of the OU fields that is not duplicated in the extension.

A warning notice and a summary of the terms of use of the Certificate is provided. The warning notice and the summary of the terms of use of a Certificate are indicated in the Certificate by a further pointer (composed of text and a URL – "*Warning/Terms of Use: www.unipass.co.uk/tou")*, in an OU field (which is limited to 64 characters).

The warning notice and summary of terms document posted at the URL above contains the following text:
*"**Warning:** Do* NOT *use this certificate unless you* are a member *of the Unipass Community. OSIS accepts no liability for unauthorised use. You MUST read* ***www.unipass.co.uk/tou*** *for more details."*

"Terms of Use for Certificates
This Certificate has been issued in accordance with the procedures summarised in the Certification Practice Statement (CPS) of Origo Secure Internet Services Limited ("OSIS"). The CPS (as updated from time to time) is available on the Unipass Website at ***www.unipass.co.uk****. The CPS contains guidelines concerning the use of and reliance upon this Certificate, and persons who wish to use or rely upon this Certificate should read the CPS before doing so.*

You must not use or rely on this Certificate unless you have first entered into a contract with OSIS to become a member of the Unipass Community or have accepted the Individual Certificate Rules of Use (which give you automatic membership of the Unipass Community). If you fail to do so, then neither OSIS nor its Suppliers shall be liable to you or to any other third party in respect of your use of, or reliance on, this Certificate (which for the avoidance of doubt is unauthorised). Do NOT use or rely on this Certificate if this Certificate has expired or has been revoked pursuant to the Unipass Service (please refer to the CPS for details about Certificate revocation).

The rights of members of the Unipass Community against OSIS are expressly limited to those set out in the relevant contract with OSIS.

This Certificate is copyrighted: Copyright © Origo Secure Internet Services Ltd. All rights reserved.

Other than as expressly authorised in the relevant contract with OSIS, copying, extraction and/or re-utilisation of all or a substantial part of: (i) this Certificate, (ii) the contents of or data in this Certificate and/or (iii) any database within which this Certificate is held or otherwise stored or any other database of OSIS*, is not permitted unless OSIS, and where applicable its Suppliers, have granted an express licence to do so. OSIS and its Suppliers reserve the right to pursue such unauthorised use, or infringement of their intellectual property rights."*

2.8.3.4 IETF-Defined CRL Distribution Point Extension

The CRL Distribution Points extension identifies where CRL information is obtained. The Unipass PKI provides a single distribution point per hierarchy, specified as a URL from which it is possible to obtain the latest CRL.

2.8.3.5 IETF-Defined Authority Information Access Extension

The Authority Information Access extension identifies where the OCSP responder can be found, and the protocol to be used for OCSP queries. The Unipass PKI provides a single OCSP responder location, specified as a URL from which it is possible to obtain the latest real time revocation information.

2.8.4 Issuer and Subject Distinguished Names

All Certificates contain issuerName and SubjectName Fields implemented as Distinguished Names (DNs). The DNs in Individual Certificates and Organisation Certificates comprise the following X.520 Attributes, including additional "organisational unit" (OU) Attributes to convey duplicate information contained in certain Certificate Extensions, and to convey other information. The set of Attributes uniquely identify each Individual (in relation to Individual Certificates) or each Organisation (in relation to Organisation Certificates) and have meaningful values as specified in Table 2.

Table 2 – OSIS Certificate attributes and contents

Field	Attribute	Content
IssuerName	CN	Always set to the value value 'Origo Root CA - G3'. Please note that the format of the ' - G3' suffix is <space><hyphen><space>G3.
	O	Always set to the value 'Origo Secure Internet Services Ltd'.
SubjectName	E	Internet e-mail address in the form *x@y.z* where 'x' is the unique identifier for an e-mail account (and may be in more than 1 part) and 'y.z' is a domain name (and may be in more than 2 parts). For example, *Joe.Bloggs@osis.uk.net* and *enquiries@origoservices.com* are both valid e-mail addresses.
	CN	In relation to Individual Certificates, forename(s) and last name(s) (free text) as specified by applicant (note: this data is present only to facilitate Certificate retrieval from the Repository and Certificate management, and should not be relied upon to uniquely identify the Individual). In relation to Organisation Certificates, organisation name (free text) as specified by applicant and verified by OSIS but not including special characters reserved by the CA software such as '&', which will instead be removed by OSIS and replaced with 'and'. (Note: this data is present only to facilitate Certificate retrieval from the Repository and Certificate management, and should not be relied upon to uniquely identify the organisation)
	OU_1	Branch or Outlet postcode associated with the Certificate holder or with the specific location of an
Field	**Attribute**	**Content**
		Organisation Certificate. The text 'BP' followed by: the 2, 3 or 4 characters of the outer postcode; a single space; and lastly, the 3 characters of the inner postcode as follows (where + is a metacharacter indicating string concatenation in sequence with no spaces) • 'BP'+outerPostcode+' '+innerPostcode (note the space between outer and inner codes) For example, in the case of a London-based employee of an intermediary firm with an office in London which is the registered 'head office', the postal code in the OrganisationID will be the London postal code known to the FCA and associated with their FCA reference number, and the postal code in this field will be the same. If however, an employee in a branch in Edinburgh obtains a Certificate, the postal code in the Organisation ID will remain as London, but the postal code here will be that for the Edinburgh branch.
	OU_2	Name of Organisation or Associated Company of the Organisation.
	OU_3	In relation to Individual Certificates this is the Employee ID component. The text 'EmployeeID' followed by a set of subcomponents as follows: (where + is a meta-character indicating string concatenation, and the first character identifies uniquely the combination of subcomponents following): • '0' + trialCert + indType + indRef or • '1' + trialCert + indType + indRef + fcaIRN Allocated based on data provided by applicant. In relation to Organisation Certificates this contains data to identify the Certificate as an Organisation Certificate plus a copy of the Organisation Reference as held in the Organisation ID component in the O attribute of the Subject Name. The text 'CompanyOID' followed by a set of subcomponents as follows: (where + is a meta-character indicating string concatenation, and the first character identifies uniquely the fact that this is an Organisation Certificate): • '2' + trialCert + 'x' + variable content of the Organisation ID component (i.e. excluding the text "FirmID")
	OU_4	OSIS Warning URL.
	OU_5	CPS URL

	O	(Organisation ID component) The text 'FirmID' followed by a set of subcomponents as follows (where + is a meta-character indicating string concatenation in sequence with no spaces, and the first character identifies uniquely the combination of subcomponents following): '0'+ orgType + orgRef (if no FCA reference number or postal code is specified by the applicant) '1' + orgType+ orgRef + fcaNumber (if an FCA reference number but no postal code was specified) '2' + orgType + orgRef + fcaNumber + postCode (if an FCA reference number and postal code were specified) '3' + orgType + orgRef + postCode (if a postal code but no FCA reference number was specified) Allocated based on data provided by applicant.
	C	Where the associated Head office postcode of the Organisation is within the UK the value is set to 'GB. If within the Isle of Man the value is set to 'IM', if within Jersey the value is set to JE and if within Guernsey the value is set to GG.

Table 2 – OSIS Certificate attributes and contents

The Organisation ID and Employee ID subcomponents are further specified in Table 3 as follows:

Table 3 – OSIS Certificate attribute subcomponents

Subcomponent	subjectName Attribute	Content
Trial Certificate or trialCert	OU_3	Defines whether the Certificate has been issued for test purposes. '1' This IS a Trial Certificate. All other values indicate that this IS NOT a Trial Certificate. In practice '0' and 'x' have been used in Individual and Organisation Certificates respectively.
Individual Type or indType	OU_3 (Employee ID)	The category of Individual as follows: '1' Approved Person *(Organisation Type 1 only)* '2' Business support *(any Organisation Type)* '3' Reserved for future use '4' IT specialist *(any Organisation Type)* '5' Reserved for future use '6' Financial Institution specified other Individual *(only if Organisation Type is 5)* '7' Reserved for future use '8' Reserved for future use
Individual Reference or indRef	OU_3 (Employee ID)	A unique identifier for the Individual composed of the following values concatenated in sequence with no spaces: • RA number (4 digits, allocated by OSIS, currently fixed value of '0001') • Sequential count (6 digits, left padded with zeros, example value '000022') • Check digit (1 digit, calculated over the preceding IndividualID digits using the same method as for the FirmID check digit).
FCA Individual reference number or fcaIRN	OU_3 (Employee ID)	FCA Individual reference number (formerly PIA number) of the Individual, *(if specified, three alphabetic characters (A...Z) followed by five digits (0...9) as held by the FCA, example value* 'ABC01234'*).*
Organisation Type or orgType	O (Organisation ID)	The Organisation Type as defined below: '1' Intermediaries authorised by the FCA (either directly authorised or appointed representative firms) '2' Reserved for future use '3' OSIS and its subcontractors '4' Third party services provider '5' Financial Institution '6' Organisations of Financial Intermediaries not regulated by the FCA

Organisation Reference or orgRef	O (Organisation ID)	A unique identifier for the Organisation composed of the following values concatenated in sequence with no spaces: • RA number (4 digits, allocated by OSIS, currently fixed value of '0001') • Sequential count (6 digits, left padded with zeros, example value '000922') • Check digit (1 digit, calculated as the digit sum of the preceding FirmID digits itself digit summed repeatedly until a single digit remains, example value '5', calculated as follows: 0+0+0+1+0+0+0+9+2 +2 =14, 1+4 = 5).
FCA Number or fcaNumber	O (Organisation ID)	FCA reference number (formerly SIB number) of the Organisation or an Associated Company of the Organisation, *(if specified, six digits (0...9) as held by the FCA, example value* '000209'*)*. Where an FCA reference number is present in a Certificate, the Organisation name in OU_2 (see Table 2 above) will correspond to the name of the organisation as held by the FCA for that number, or a group company of that organisation if applicable.
Postal Code or postCode	O (Organisation ID)	The postcode associated with the head office or normal place of business of the firm *(up to 7 character alphanumeric with no embedded spaces, example value* 'HP84AR'*)*.

Table 3 – OSIS Certificate attribute subcomponents

2.9 OSIS Naming Authority

OSIS in its capacity as the Naming Authority for the Unipass PKI controls the issuance of distinguished names (DNs) contained in the Repository and in SubjectName Fields of each Individual Certificate and Organisation Certificate (as defined in Tables 2 and 3). The principal means by which it does this is by controlling the definition of Certificate contents as specified in this CPS. This Section defines any further rules for the allocation of DNs.

2.9.1 RA Numbering

OSIS allocates RA numbers to permit unambiguous generation of unique Individual IDs to allow for other RAs to be set up in future. This capability is not currently utilised and the value for the RA will always be '0001'.

2.9.2 Future naming conventions

OSIS may also specify naming conventions for other elements of subject names that may be added in the future, and naming conventions for subject names in the Repository for other Certificate types that may also be defined in the future. These naming conventions may also vary between issuance and re-issuance/re-enrolment.

2.10 Repository

The Repository is a database for storing and retrieving Certificates and other information related to Certificates, including CRSS information. It may contain personal data which must be protected by law.

Any person or entity who accesses the Repository and/or the CRSS whether to rely on a Certificate or for any other purpose agrees and acknowledges that they shall not copy, use, distribute, or otherwise make available to any third party any of the information contained in the Repository and/or the CRSS (except as permitted by the terms of this CPS or the Organisation Contract (if applicable)).

2.10.1 Publication

The CA promptly publishes Certificates, notices of Certificate revocation, and other information in the Repository, in accordance with the requirements of this CPS.

2.11 Unipass Controllers and Nominated Persons

The Organisation shall procure that each Unipass Controller which it appoints complies with the Unipass Controller Guidelines and the Individual Certificate Rules of Use (Rule 3 of Section B).

The Organisation shall procure that each Nominated Person which it appoints complies with the Nominated Person Guidelines.

Without prejudice to any other rights or remedies OSIS may have under the Organisation Contract or otherwise, where OSIS reasonably believes that the appointed Unipass Controller does not meet the Trusted Role Requirements or where the Unipass Controller is in breach of the Unipass Controller Guidelines, the Organisation shall on request by OSIS replace the Unipass Controller with a person who meets the Trusted Role Requirements. OSIS shall not be liable for any claims, demands, actions, costs, expenses (including, but not limited to legal costs and disbursements on a solicitor and own client basis), losses or damages caused by or arising out of such replacement.

Without prejudice to any other rights or remedies OSIS may have under the Organisation Contract or otherwise, where OSIS reasonably believes that the appointed Nominated Person does not meet the Nominated Person Requirements or where the Nominated Person is in breach of the Nominated Person Guidelines, the Organisation shall on request by OSIS replace the Nominated Person with a person who meets the Nominated Person Requirements. OSIS shall not be liable for any claims, demands, actions, costs, expenses (including, but not limited to legal costs and disbursements on a solicitor and own client basis), losses or damages caused by or arising out of such replacement.

The Help Desk may re-confirm the identities of Unipass Controllers. If a Unipass Controller does not respond to such reconfirmation within a reasonable time, OSIS may, in its sole discretion and after reasonable investigations have been

made, revoke existing Certificates and require the Organisation to apply for new Individual Certificates for all of its Individuals, or where appropriate the Individuals of its Associated Companies or Network Members.

The Help Desk may re-confirm the identities of Nominated Persons. If a Nominated Person does not respond to such reconfirmation within a reasonable time, OSIS may, in its sole discretion and after reasonable investigations have been made, revoke existing Organisation Certificates and require the Organisation to apply for new Organisation Certificates, and where appropriate to apply for new Organisation Certificates for its Associated Companies.

2.12 Service Levels

Applications for Individual Certificates and Organisation Certificates shall be processed in accordance with the procedures set out in Section 4. If successful, Collection E-mails, which enable Certificates to be obtained, will be issued.

The ability to issue Collection E-mails in a timely manner depends upon timely submission of complete and accurate information, and prompt response to any administrative requests. These administrative requests may include the provision of satisfactory references from Financial Institutions where appropriate.

3 SERVICE STANDARDS AT OSIS AND ITS SUPPLIERS

3.1 OSIS' Suppliers and service standards

OSIS and its Suppliers ensure that quality of service is maintained, regardless of functional and physical distribution of service provision, by agreeing contracts with adequate service standards.

3.2 Equipment

OSIS and its Suppliers utilise only Secure Systems in performing their respective obligations as set out in this CPS.

3.3 Compliance, Records and Audit

Each of OSIS' Suppliers maintains and makes available to OSIS, upon request, complete and accurate records relating to the performance of their obligations under this CPS, including:

- documentation of its own compliance with the CPS; and
- such documentation and, as appropriate, computer audit trails of actions and information which shows that it has carried out in accordance with the procedures specified in this CPS each Certificate application and each Material Event of each Certificate it issues or in relation to each Individual which it has authenticated.

Without prejudice to the foregoing, these records include all relevant information in the Supplier's possession regarding:

- the identity of each Certificate holder;
- the identity of persons requesting Certificate revocation;
- the compliance of each Certificate applicant with their obligations, including but not limited to their explicit consent to OSIS' data protection policy;
- other facts represented in the Certificate; and • Time Stamps.

3.4 Time Stamping

Certain transactions in the verification process are Time Stamped to ensure the integrity of the Unipass PKI and to enhance the trustworthiness of Certificates and to prevent the repudiation of digitally signed messages. Time Stamps reflect Greenwich Mean Time (GMT) and adopt the Universal Time Conventions (UTC). For purposes of this CPS, any two-digit year in the range 00-99 means 2000-2099.

The following data is Time Stamped, either directly on the data or on a correspondingly trustworthy audit trail, by the applicable Supplier at the time of creation of the data:

- Certificates;
- CRLs and other revocation information;
- each version of the CPS; and
- other information, as prescribed by this CPS.

3.5 Retention Period

Each of OSIS' Suppliers retains records associated with Certificates (as stipulated in Section 3.3 above) for at least seven (7) years after the date a Certificate is revoked or expires.

Where records are held by a Supplier and where the appointment of the Supplier is terminated or expires prior to the expiry of the seven (7) year period referred to in this Section 3.5, the Supplier must provide OSIS with such records prior to them ceasing to act and OSIS will retain the records for the remaining portion of the seven (7) year retention period.

3.6 Inspections and Audits

OSIS may require the following inspections and audits to be carried out.

3.6.1 Independent Audits

An independent professional firm with demonstrated expertise in computer security or a recognised computer security accreditation may audit the operations of the Suppliers, including such functions of the Suppliers as OSIS may in its sole

discretion determine, not more than once in any one year. This audit will evaluate the compliance of such Suppliers with this CPS and other applicable agreements, guidelines, procedures, and standards.

3.6.2 Supplier Audits

A Supplier may conduct inspections and audits of its sites and operations periodically to validate that they are functioning in accordance with the security and other practices and procedures set out in this CPS.

3.7 Continuity and Availability

Suppliers produce detailed business continuity plans in order to minimise disruption to the Services in the event of a Discontinuity. OSIS has in place adequate procedures to be followed in the event of a Discontinuity and/or compromise of any CA Private Key.

During recovery from a Discontinuity certain technical services may be temporarily suspended (e.g. because the Repository needs to be restored from backup) but OSIS and its Suppliers shall make reasonable efforts to continue to accept revocation requests and to provide services to support the operation of the Unipass Service.

OSIS has taken steps to ensure that by use of a key splitting/sharing scheme, the Root CA Key Pair can be recreated should the need arise.

3.8 Personnel Security Controls

OSIS and its Suppliers take all reasonable steps to ensure the trustworthiness and competence of their Personnel and of the satisfactory performance of their duties. Such practices are consistent with the guidelines below.

3.8.1 Key Roles

Those Personnel of OSIS and its Suppliers that have access to or control over operations that may materially affect the issuance, use or revocation of Certificates, including access to restricted operations of the Repository, are, for the purposes of this CPS, deemed to be serving in a Key Role.

3.8.2 Vetting

Each of OSIS and its Suppliers vet their respective Personnel who are candidates to serve in Key Roles as referred to in Section 3.8.1 above to determine their trustworthiness and competence. OSIS and its Suppliers may conduct reasonable periodic investigations of their respective Personnel who serve in Key Roles to verify their continued trustworthiness and competence in accordance with relevant and established Personnel procedures or practices.

It is at the sole discretion of OSIS and its Suppliers (as appropriate) whether to remove any person employed by them serving in a Key Role who fails any periodic investigation carried out pursuant to the above.

3.8.3 Personnel Procedures Guidelines

Appropriate controls should be implemented in relation to Personnel deployed in Key Roles, together with any division of responsibilities into roles, intended to facilitate the operation of procedural controls.

Personnel should be employed or retained in accordance with suitable background, qualifications, experience and clearance requirements. All prospective Personnel are required to prove identity by means of appropriate documentation.

Investigations should be conducted, as appropriate and to the extent permitted by law, of the existence of undeclared criminal convictions and undischarged bankruptcies, etc. so as to reasonably ensure that Personnel are not subject to criminal or financial pressure that might affect the performance of their duties, if those duties are not supervised or monitored.

All Personnel should be appropriately trained. All Personnel should be supplied with manuals, work instructions and/or technical specifications as appropriate.

Personnel involved in the handling of Certificate applications and the issuance of Certificates must meet the requirements specified in Table 4 below.

Requirements	
Education	No less than requirements for the company's human resources personnel handling company confidential employee records
Accreditations	Must be an employee in good standing with his/her employer

Table 4 – Personnel requirements

3.9 Miscellaneous Security Controls

3.9.1 Communication Security Controls

All electronic communications between OSIS and its Suppliers containing Individuals' personal data are appropriately secured.

3.9.2 Environmental Security Controls

Suppliers operate from physically and procedurally secure environments, at a minimum within the meaning defined below and in accordance with their own security policies and procedures.

Any party or exterior walls, and any ceilings and roofs as appropriate, that could otherwise afford unauthorised access should be of adequate construction to maintain the overall integrity of the physical security. Any party walls should connect at both top and bottom with floors and ceilings/roofs as appropriate (i.e. they should penetrate suspended ceilings or floors that could afford access via void spaces). Physical access should be restricted by means of locks, entry control systems, and intruder detection as appropriate. Sufficient power supply protection should be employed to mitigate the risk that Critical Processing equipment can malfunction due to mains power interruption, spikes, or surges.

Sufficient air conditioning should be employed to mitigate the risk that Critical Processing equipment could malfunction due to overheating. Protection should be employed from exposure to flood (including both external incursion and leakage of water coolant and/or heating systems) that could affect Critical Processing operations. Protection should be employed from fire that could affect computers, media, equipment, and paper records. Any paper records or media bearing confidential information should be disposed of securely.

Secure off site backup facilities as appropriate should be maintained for computer media. A separate archive store should be maintained for computer media and paper records. Tests should be conducted at least every six (6) months, that backup media can be accessed and read.

3.10 Transfer of Supplier Operations on Termination

The following obligations are intended to facilitate the transfer from one Supplier to another if required.

OSIS uses all reasonable endeavours to ensure continuity of the Unipass Service to Individuals and Organisations in the event of any cessation of activity by any Supplier and the following transition of that service to any replacement Supplier.

Before ceasing to act as a Supplier, a Supplier must:

- notify OSIS of its intention to cease acting as a Supplier at least four (4) months before doing so;
- where OSIS so directs, provide to the Individual of each Individual Certificate it has issued and to the Organisation (and its Associated Companies if applicable) of each Organisation Certificate it has issued and which is still valid four (4) months notice of its intention to cease acting as a Supplier and the alternative arrangements that will apply thereafter;
- where OSIS so directs, revoke all Certificates that remain un-revoked or unexpired at the end of the four (4) months notice period, whether or not the Individuals (in relation to Individual Certificates) and Organisations and/or Associated Companies or Network Members (in relation to Organisation Certificates) have requested revocation;
- give notice of revocation to each affected Individual, Organisation, Associated Company and Network Member, in accordance with Section 8;
- use all reasonable efforts to ensure that discontinuing its services causes minimal disruption to Individuals, Organisations and to persons duly needing to verify Digital Signatures by reference to the Public Keys contained in outstanding Certificates;
- provide reasonable assistance and co-operation to OSIS to ensure the smooth transition of the services to OSIS or any replacement third party Supplier; and
- return all documentation to OSIS in accordance with Section 3.5.

3.11 Suspension of the Unipass Service

OSIS may suspend the Unipass Service (including the availability of the Unipass Help Desk and Unipass Website) at any time where it is necessary to do so for repairs, improvement or maintenance. Although OSIS will endeavour to give advance notice of such suspensions where it is reasonably practicable to do so, on occasion it may not be possible to give such notice. Any disruption to the Unipass Service will be kept to a minimum.

4 HOW TO APPLY

4.1 Introduction

As described in Section 1, OSIS currently offers three types of Certificate: Individual; Organisation; and Trial. The latter two types of Certificate currently represent only a small minority of those issued by OSIS, with by far the main element of the Unipass Service being the provision of Individual Certificates.

4.2 Individual Certificates

The process from applying through to collection of an Individual Certificate is summarised below:

- Applications are made on the Unipass website at **www.unipass.co.uk** and instructions and help are provided throughout;
- During the first application from any organisation, details of the organisation must be entered, but these need not be entered again for subsequent applicants from that organisation;
- The organisational details may include references (to be taken up with Financial Institutions);
- The first applicant from Intermediary firms and Third Party Services Providers must be authorised to enter into contracts on behalf of the organisation; for other firm types, this may not be necessary as paper contracts will be executed with wet signatures;
- The first applicant will by default become a Unipass Controller for the organisation (this can subsequently be changed if required by replacing the default Unipass Controller or by adding additional Unipass Controllers to the account);
- The Principal of the firm (where applicable, otherwise Managing Director or equivalent) will also receive a letter notifying them that the applicant has entered their firm into the contract for use of the Unipass Service;
- Organisations must provide approval of each applicant, normally via a Unipass Controller;
- Once an Organisation has established one or more Unipass Controllers with their own Unipass Certificates, a Unipass Controller can then approve or deny applications made by Individuals within their Organisation, either via the Unipass Controller pages on the Unipass website, or by e-mail to **helpdesk@unipass.co.uk**;
- Where no Unipass Controller exists, the Contract Owner or other authorised representative of the Organisation must approve or deny applications;
- Validation rules apply for both organisations and individuals (see Section 5 for details);
- OSIS may allow some rework where application data or documentation is ambiguous; and
- On successful completion, the applicant will receive an e-mail with instructions on how to collect their Certificate.

4.3 Approval of applications by Unipass Controllers and/or Contract Owners

No applicant can obtain a Unipass Certificate without the approval of his or her organisation. OSIS will seek approval of an application from either:

- the applicant's Contract Owner or other suitably authorised representative (by e-mail); or
- a Unipass Controller for the organisation (via the Unipass Controller web pages, or alternatively by e-mail).

To make it easier for Organisations to manage applications from Individuals within their Organisation to use Individual Certificates, an Organisation can appoint one or more officers, partners, principals, directors or employees of the Organisation to act as Unipass Controllers. The Organisation must take care to make sure that any person they appoint as a Unipass Controller meets the Trusted Role Requirements. Once appointed, a Unipass Controller must fulfil his role in accordance with the Unipass Controller Guidelines and the provisions of the Individual Certificate Rules of Use (Rule 3 of Section B).

4.4 Security of web application forms

To assure the security of the input data (and where appropriate, also to assure the identity of the user), the web forms are protected using a Secure Sockets Layer ("SSL") connection. Only the in force credentials of currently valid Unipass Controllers can be used to access and submit data using the Unipass Controller web forms.

The web forms perform primary data input validation as appropriate and practical to reduce the validation effort at the next stage (e.g. the name fields must not be blank). In addition, some specific validation rules are specified in Section 5, such as those relating to postcode validation.

4.5 Organisation Certificates and Trial Certificates

Applications for both Organisation Certificates and Trial Certificates are made direct to OSIS, either by telephone on 0131 385 8888, or by e-mail to **helpdesk@unipass.co.uk**.

5 VALIDATION OF CERTIFICATE APPLICATIONS

5.1 Introduction

Applications for Certificates received by OSIS are validated in accordance with this Section 5.

5.2 Validation of applications and formation of contract

The rules to be followed are specified in Table 5 below. Business entity confirmation by taking up references is performed only once per Organisation during the first application, after which only Certificate applicant details will be required.

Table 5 –Validation Rules

Validation	Rules	By
Application data confirmation	Assess the data supplied to verify its basic accuracy as follows: • Confirm no obvious signs of erroneous or fraudulent application details. • Telephone check may be used to help resolve inconsistencies.	OSIS
Business Entity confirmation (including references from Financial Institutions where applicable)	For Individual Certificates in Intermediary firms: • At least one of the Financial Institution references supplied must confirm that the Organisation has current agency agreement(s) with them For Organisation Certificates in Intermediary firms: • Financial Institution references supplied must confirm that the applicant's Organisation has current agency agreement(s) with them. Compare the information supplied with external data sources as appropriate: • Company name and address details consistent with Companies House record or other applicable business directory record. • For regulated firms, ensure that the name and address details supplied match those held by the FCA, or in exceptional cases, addresses known to OSIS to be valid. • Postcode is valid and postal code record is consistent with street address or PO Box number supplied on-line for head office.	OSIS
	Check that Branch Postcode supplied is valid for applicant in the Organisation.	Unipass Controller (where available)
Applicant confirmation	For applicants purporting to be Approved Persons, match personal details with those supplied on-line by the FCA.	OSIS
	Check that if the applicant is an Approved Person, they are registered with the FCA. Check that appropriate organisational procedures have been followed to ascertain that the applicant is a legitimate member of the Organisation (such as the personnel/HR department taking up references for employment, or seeking appropriate indemnities for contractors). Check that applicant has a legitimate requirement to hold a Certificate on behalf of that Organisation. Check that applicant fulfils the role specified in the application.	Unipass Controller

Table 5 –Validation Rules

5.3 Inconsistencies in information provided to OSIS

If there are inconsistencies in the information submitted for validation, the applicant may be contacted by telephone or email to seek further evidence and/or an explanation to resolve the inconsistencies or inaccuracies.

5.4 External data sources

OSIS may employ certain external data sources for validation purposes. OSIS and its Suppliers shall not be held liable for any inaccuracy in external data sources that is beyond their reasonable control.

5.5 Procedure for successful applications

If all required validations are successful OSIS will:

- create a new, or assign an existing, Organisation Reference (OrganisationID) to be included in the Certificate;
- if applicable, create a new Individual Reference (IndividualID) to be included in the Individual Certificate; and
- issue a Collection E-mail to the Individual Certificate applicant or Nominated Person (as appropriate) to enable the Certificate applicant to collect their Certificate.

5.6 Procedure for unsuccessful applications

If a validation fails, OSIS will reject the application. Unsuccessful validation on one attempt is not in itself a reason to refuse a subsequent application, but OSIS reserves the right to require re-submission of any or all relevant information. In the event of a failure or refusal to issue a Certificate, OSIS will notify the Certificate applicant giving the reason for the failure or refusal.

6 COLLECTION OF CERTIFICATES

6.1 Introduction

Once an application has been processed successfully in accordance with Sections 4 and 5, the Certificate applicant will be sent a Collection E-mail outlining the steps to follow to collect their Certificate.

6.2 Collection Procedure

Successful Certificate applicants have 24 days from the date of the Collection E-mail to collect their Certificate. Once this period has expired, applicants must contact the Help Desk to determine whether their application can be re-initiated.

Having reviewed the Collection E-mail and made the decision to proceed, the Certificate applicant or Nominated Person can direct their browser to the collection page on the Unipass Website using the link provided in the Collection E-mail. In relation to Individual Certificates the Unipass Website will display the collection page where users must enter the necessary credentials to authenticate themselves. In addition, before being allowed to proceed, they are required to signify by clicking on a tick box their acceptance of the Unipass Data Protection Policy and the Individual Certificate Rules of Use. The user may optionally view each of these documents in full by clicking on the appropriate hyperlink on the page. Only after having confirmed their acceptance of the necessary terms and conditions can the user proceed to collect their certificate.

In relation to Organisation Certificates the Unipass Website will display the following details:

- a copy of the Nominated Person Guidelines and a warning that by agreeing to proceed the Nominated Person accepts the terms and conditions of those Nominated Person Guidelines;
- a copy of the Data Protection Policy and a warning that by agreeing to proceed the Nominated Person accepts the terms and conditions of that Policy; and
- the enrolment page where Nominated Persons must enter the necessary credentials to authenticate themselves and request the creation of a Unipass Organisation Certificate.

6.3 Creation of the Certificate

If the applicant successfully authenticates on the enrolment page:

- the CA software transmits a code to the client browser, or otherwise causes the client browser to create the Public/Private Key Pair for the Certificate and forward the Public Key;
- the CA software then submits to the CA the Public Key together with the intended Certificate content as held in OSIS' records;
- on receipt of this submission the CA creates the Certificate and supplies a copy of it to the Repository; and
- the CA software transmits a code to the client browser, or otherwise causes the client browser to download the copy of the Certificate.

If the Certificate applicant or Nominated Person does not agree to proceed, Certificate collection will be deemed to have failed. The Help Desk can be contacted on 0871 22 12345 to attempt to resolve the failure. If the Certificate applicant or Nominated Person fails to do this no further action will be taken, but it will still be possible for the Certificate applicant or Nominated Person to return within the original time limit as specified in Section 6.2 to collect their Certificate.

If the Certificate applicant or Nominated Person contacts the Help Desk (e.g. because he does not understand what he is being asked to do, or does not accept displayed warnings) the Help Desk will determine the nature of the caller's refusal to accept, attempt to resolve any misunderstanding and agree with the caller either that the application should be withdrawn or that the Certificate applicant or Nominated person will now proceed with collection (on the basis that the Certificate applicant or Nominated Person now understands and has to accept any displayed warnings).

The Individual (in relation to Individual Certificates) or the Organisation (in relation to Organisation Certificates) is responsible for checking at the time of collection of the Certificate that it is not damaged or corrupted, that the contents are correct and that the Certificate is suitable for their intended purpose. The Individual, Organisation, Associated Company or Network Member must notify the Help Desk in the event that the Certificate is damaged or corrupted, or its contents are inaccurate, promptly after collection of the Certificate, or upon earlier discovery of incorrect informational content included, or to be included, in the Certificate.

A test page is available on the Unipass Website where Certificate contents can be displayed and verified.

6.4 Publication

Upon collection of a Certificate, the CA publishes a copy of the Certificate in the Repository.

6.5 Trial Certificates

The procedure used to issue Trial Certificates is different from that used for Individual Certificates and Organisation Certificates. Key generation is performed during the Trial Certificate application, and Trial Certificates must therefore be collected on the PC on which the application was made.

In relation to Trial Certificates the Unipass Website will display the following details:

- a copy of the "Unipass Trial Certificate Terms and Conditions" and a warning that by agreeing to proceed the collector accepts the terms and conditions of such "Unipass Trial Certificate Terms and Conditions";
- a copy of the Data Protection Policy and a warning that by agreeing to proceed the collector accepts the terms and conditions of that Policy; and
- the enrolment page where collectors must enter the necessary credentials to authenticate themselves and request the creation of a Unipass Trial Certificate.

7 USE OF CERTIFICATES

7.1 Reliance on Certificates

Certificates and their associated Private Keys may be used to support various Security Mechanisms (see Section 2.2). All such Security Mechanisms involve the generation of Digital Signatures using Private Keys and reliance upon those Digital Signatures using the corresponding Certificates.

In relation to Individual Certificates, a Digital Signature shall be binding between the Individual referred to in the Individual Certificate and the Individual or Organisation (or an Associated Company or Network Member of an Organisation) that is relying on the Individual Certificate, provided that the parties in each case have complied with their respective obligations set out in the Individual Certificate Rules of Use or relevant Organisation Contract (as appropriate).

In relation to Organisation Certificates, a Digital Signature shall be binding between the Organisation who has provided the Organisation Certificate and the Organisation (or an Associated Company or Network Member of an Organisation) who is relying on the Organisation Certificate, provided that the Organisation (and/or the Associated Company or Network Member of an Organisation) has in each case complied with the requirements of the relevant Organisation Contract and, if applicable, this CPS.

Verification of a Digital Signature must be undertaken to determine that:

- the Digital Signature was created by the Private Key corresponding to the Public Key listed in the signer's Certificate; and
- the associated message has not been altered since the Digital Signature was created.

An Individual, Organisation (or, where appropriate, Associated Company or Network Member) who receives a message signed by a Digital Signature must ascertain that:

- the Digital Signature was created during the operational period of a valid Certificate; and
- it can be verified by referencing the Certificate chain of the Unipass PKI hierarchy in accordance with Section 2.7.2 and the CRSS in accordance with Section 8.

An Individual, Organisation (or, where appropriate, Associated Company or Network Member) who receives a digitally signed message is only entitled to rely upon the Digital Signature and the corresponding Certificate if:

- such reliance is reasonable under the circumstances (including as to whether the Certificate is suitable for the purpose or application for which it is being used). If the circumstances indicate a need for additional assurances, the Individual, Organisation, Associated Company or Network Member (as appropriate) must obtain such assurances for such reliance to be reasonable;
- he has no knowledge or notice of a breach of the requirements of this CPS by the signer;
- in relation to an Individual, he has complied with all the requirements set out in the Individual Certificate Rules of Use; and
- in relation to an Organisation (or Associated Company or Network Member), it has complied with all the requirements set out in the Organisation Contract.

A Certificate that fails any of the above tests shall be deemed as unverified and a person relying on it assumes all risks with regard to it.

7.2 A Certificate is not Evidence of Authority

The use of Certificates and their corresponding Private Keys does not convey evidence of authority on the part of any Individual to act on behalf of any person or to undertake any particular act or of any Organisation or its Associated Companies or Network Members to undertake any particular act. Certificates shall only establish that reasonable steps have been taken to validate the identity of the Individual (in relation to Individual Certificates) and of the Organisation and/or Associated Company or Network Member (in relation to Organisation Certificates). Verifiers of digitally signed messages shall therefore be solely responsible for exercising due diligence and reasonable judgement before relying on Certificates to ensure that the Individual, Organisation or any of its Associated Companies or Network Members (as appropriate) has the appropriate authority to enter into any transaction.

7.3 Legal Requirements as to Form

It shall be the sole responsibility of the Individual, Organisation, Associated Company or Network Member (as the case may be) when relying on a Certificate to (i) decide what weight and reliance should be given to a message bearing a Digital Signature verified by the Public Key included in a valid Certificate and (ii) to decide whether it considers such message (bearing a Digital Signature verified by the Public Key included in a valid Certificate) to have the same legal validity, effectiveness, and enforceability as if such message had been written and signed on paper. OSIS expressly does not guarantee, represent, warrant or undertake that any such message (bearing a Digital Signature verified by the Public Key included in a valid Certificate) will have the same legal validity, effectiveness, and enforceability as if such message had been written and signed on paper and further recommends that the Individual, Organisation, Associated Company or

Network Member (as the case may be) seeks advice from its lawyer so as to make an informed decision in respect of the same.

7.4 Confidentiality of Messages

Where a Digital Certificate is used to sign an associated message the Individual sending the message shall be responsible for ensuring the confidentiality of the message by other appropriate means, such as through the use of Encryption.

The recipient's Certificate provides one means to support Encryption. Message originators relying on recipients' Certificates for this purpose shall be solely responsible before Encrypting a message for ascertaining that the Certificate is valid and can be validated by referencing a validated Certificate chain.

It should be noted that OSIS strongly recommends that a Certificate should not be used to Encrypt stored files, i.e. where no means other than Decryption (using the corresponding Private Key) could be used to recover the original plain text, because either loss of the Private Key would render the files inaccessible, or the copying of the Private Key to systems administrators or other personnel in the Organisation or any of its Associated Companies or Network Members (e.g. for the purpose of file retrieval in an emergency) would incur the risk that Digital Signatures generated by that Private Key are no longer uniquely linked to the Individual identified by that Certificate.

7.5 Individual Obligations

The obligations of Individuals in relation to their applying for, accepting, using and relying on Individual Certificates are set out in the Individual Certificate Rules of Use (or earlier Individual Contract or Customer Contract).

For the avoidance of doubt, failure by an Individual to comply with any of these obligations may result in:

- the revocation of the Individual Certificate by the Unipass Controller or OSIS;
- the termination of the Individual Contract or Customer Contract (if applicable);
- the termination of the Individual's membership of the Unipass Community;
- the Organisation of the Individual being liable to OSIS for any loss or damage which OSIS suffers as a result.

7.6 Organisation Obligations

Organisations are required in terms of their Organisation Contract to procure that their Individuals comply with the Individual Certificate Rules of Use (or earlier Individual Contract or Customer Contract) in all respects. Organisations are also required to procure that their Associated Companies or Network Members in turn procure that Individuals of these Associated Companies or Network Members comply with the Individual Certificate Rules of Use (or earlier Individual Contract or Customer Contract) in all respects.

7.6.1 End User Organisations

The obligations of End User Organisations are contained in the relevant End User Organisation Contract.

7.6.2 Relying Party Organisations

It is acknowledged and agreed between OSIS and the Relying Party Organisations that in relying on a Certificate that Organisation does so in accordance with the terms of its Organisation Contract and this CPS. The Relying Party Organisation shall ensure that where any of its Associated Companies are permitted to rely on Certificates that such Associated Companies do so in accordance with the terms of the Relying Party Organisation Contract and this CPS. The Relying Party Organisation (and its Associated Companies where permitted) shall only rely upon a Certificate for the purpose for which it was issued.

Failure to comply with any of the obligations stated above in this Section 7.6.2:

- shall result in the forfeiture of any claims made by the relevant Organisation against OSIS regarding a Certificate in the event of a dispute arising from the failure of that Organisation to meet those obligations;
- may result in the relevant Organisation being liable to OSIS for any loss or damage which OSIS suffers as a result; and
- may result in the termination of the relevant Organisation Contract which has been entered into between OSIS and that Organisation.

7.7 Additional Obligations in respect of Organisation Certificates

7.7.1 End User Organisations

The obligations of End User Organisations in relation to their applying for, accepting, using and relying on Organisation Certificates are now set out in the End User Organisation Contract for use of an Organisation Certificate.

7.7.2 Relying Party Organisations

The obligations of Relying Party Organisations in relation to their applying for, accepting, using and relying on Organisation Certificates are now set out in the appropriate Relying Party Organisation Contract and the following provisions of this Section 7.7.

In applying for, accepting and in using an Organisation Certificate issued under this CPS, each Relying Party Organisation shall (and, where appropriate, shall ensure that its Associated Companies shall):

- use reasonable endeavours to prevent any loss, disclosure, or unauthorised use of the Private Key;
- ensure that any information provided to OSIS is true, complete and accurate;

- use the Organisation Certificate only in accordance with the relevant Organisation Contract and this CPS;
- use the Organisation Certificate only during the period for which it is stated as being valid;
- comply with the terms of the relevant Organisation Contract and any other agreement to which they are subject regarding their acceptance and use of Organisation Certificates;
- use the Organisation Certificate only in order to conduct business within the UK financial services industry;
- revoke the Organisation Certificate promptly upon any actual or suspected loss, disclosure, or other compromise of their Private Key in accordance with the requirements in Section 8;
- only install and use the Organisation Certificate on equipment over which it has control at all times and ensure that any such equipment shall meet the requirements of Secure Systems;
- install the Organisation Certificate on one server only, unless it receives prior written consent from OSIS to install the Organisation Certificate on more than one server; and
- for the avoidance of doubt each Relying Party Organisation shall not (and, where appropriate, shall ensure that its Associated Companies shall not) copy the Organisation Certificate or its associated Private Key, nor provide the Organisation Certificate or its associated Private Key to any third parties.

In accepting and in using an Organisation Certificate issued under the relevant Organisation Contract and this CPS, each Relying Party Organisation (and, where appropriate, its Associated Companies) shall not:

- misrepresent themselves in any communications with OSIS or its Suppliers; or
- use the Organisation Certificate after it has been revoked or after any instruction to revoke the Certificate has been sent to OSIS; or
- use the Organisation Certificate for any unlawful purposes; or
- use the Organisation Certificate in connection with messages which send, upload, download, use or re-use any information or material which is offensive, abusive, indecent, defamatory, obscene or menacing, or in breach of confidence, copyright, privacy or any other rights or which comprise unsolicited advertising or promotional material, or knowingly to receive responses to any unsolicited advertising or promotional material sent or provided using Organisation Certificates by any third party.

Failure to comply with any of the obligations stated above in this Section 7.7.2 may result in:

- the revocation of the Organisation Certificate by OSIS;
- the termination of the relevant Organisation Contract;
- the forfeiture of all claims made by the Organisation against OSIS regarding that Organisation Certificate in the event of a dispute arising from the failure of the Organisation (or its Associated Companies) to meet these obligations; and
- the Organisation being liable for any loss or damage which OSIS suffers as a result.

8 CERTIFICATE VALIDITY, REVOCATION, EXPIRATION AND RENEWAL

8.1 Certificate validity period

Individual Certificates are valid for a period of one year and Organisation Certificates are valid for a period of three years from issue unless they are revoked. Certificates contain the appropriate valid from and valid to (or issue and expiration) dates and it is only within these dates that the Certificate is valid.

8.2 Certificate Revocation

Revocation is the process that renders a Certificate invalid. This is achieved by a revocation request being made for a particular Certificate, resulting in the updating of the Certificate data published in the Repository. Certificate status information in the Repository is updated immediately when a revocation is performed.

The Repository is only updated following successfully authenticated revocation requests submitted via OSIS, the Help Desk or the Unipass Website in accordance with this CPS. Revocation becomes effective from the moment the updated Certificate data is published in the Repository. Revocation status details of a revoked Certificate shall only be guaranteed to remain in the Repository until the Certificate expires, although in practice such information may be available for longer. There are no valid forms of revocation other than publication in the Repository.

There are no grace periods for Certificate revocation and any revocation of a Certificate is final.

8.2.1 Individual Duty to Prevent Private Key Disclosure

In the event of any actual or suspected loss, disclosure or other compromise of the Individual's Private Key the Individual is required under the Individual Certificate Rules of Use (or if earlier, the Individual Contract) to request immediately that the Individual Certificate be revoked.

In the event of any actual or suspected loss, disclosure or other compromise of the Private Key of either the Organisation and/or its Associated Company or Network Member, the Organisation must immediately request revocation of the Organisation Certificate. Any revocation will be performed in accordance with this Section 8.

8.2.2 How to revoke Certificates

Individuals, including Unipass Controllers, Organisations, Associated Companies and Network Members can request revocation of their own Certificates by:

- using the revocation function on the Unipass Website (by logging in to the "My Toolbox" section);
- contacting a Unipass Controller for their Organisation who can then perform the revocation by logging in to the Unipass Controller pages (in relation to Individual Certificates);
- contacting the Nominated Person for the Organisation, Associated Company or Network Member (in relation to Organisation Certificates);
- contacting the Help Desk during its normal working hours (see Section 10).

The primary means of revoking Certificates is to do so using the revocation function on the Unipass Website described above. Successful use of the revocation function of the system is reflected in real time in the Repository.

In addition to revocation via our website, Unipass Controllers and Contract Signatories can initiate the revocation process for Certificates held in the name of their own Organisation (e.g. when an employee leaves) by contacting the Help Desk. Similarly, Nominated Persons and Contract Signatories can instruct revocation of Organisation Certificates.

8.2.3 Checking whether a Certificate has been revoked

An Individual or Organisation (and any of its Associated Companies or Network Members if appropriate) when relying on a Certificate must check the current status of a Certificate before relying on it. To check whether a Certificate has been revoked, Organisations must subscribe to the Certificate Revocation Status Service (CRSS) and perform a lookup using either Online Certificate Status Protocol (OCSP) to interrogate the Repository in real time; or the current Certificate Revocation List (CRL) to interrogate a snapshot of the Repository.
:
The CRSS is a secured service and Organisations must explicitly subscribe to it in order to access the service. On completion of the appropriate agreement, OSIS will enable CRSS access for an Organisation.

8.2.3.1 Using Online Certificate Status Protocol (OCSP)

OCSP is a protocol which facilitates checking of revocation information in the Repository in real time. Information on a Certificate is only available from the Repository until the Certificate expires.

An Individual or Organisation (or any of its Associated Companies where appropriate) accessing the revocation data in the Repository using OCSP must verify the authenticity of the message returned by the OCSP responder by checking the Digital Signature of the returned message.

8.2.3.2 Using the CRL

The CRL is a snapshot of the revocation information in the Repository. It is a small file containing the serial numbers and revocation timestamps of all revoked Certificates whose expiry date has not yet been reached. Revoked Certificates continue to be published on the CRL until the next issue of the CRL after the expiry date of the Certificate. The CRL is republished at hourly intervals. The CRL itself denotes its "Effective Date" and also the "Next Update" time. The standard refresh cycle is every 24 hours. Due to software constraints the "Next Update" field denoted on the CRL will always reflect the 24-hourly cycle of the standard service. However, the Unipass Service provides a premium hourly revocation service, and the information in this field should therefore be ignored.

An Individual or Organisation (or any of its Associated Companies where appropriate) accessing a CRL must verify the CRL by checking its Digital Signature with the associated CA Certificate (and Certificate chain as appropriate), and whether it has expired.

The CRL is normally updated within one (1) hour of a revocation request being made to the Help Desk or the Unipass Website, though this may not always be possible. Each Supplier will use reasonable efforts to minimise delays in updating the CRL caused by technical or operational problems.

The point at which revocation of a Certificate occurs is the moment that the updated Certificate data is published in the Repository. However, since the CRL is re-published on an hourly basis it will not give notice of revocations which have occurred subsequent to the time the CRL was created.

Individuals and Organisations (and their Associated Companies where appropriate) using the CRL accept the risk of relying on a Certificate whose status has not been checked by searching the Repository. To minimise the risk, Individuals and Organisations (and their Associated Companies where appropriate) are advised to regularly update any local copy of the CRL and to establish their own procedures for deciding whether to rely on a Certificate which may have been revoked since the date and time of the most recent copy of the CRL available to that Individual or Organisation (or Associated Company).

OSIS also recommends that Individuals and Organisations take additional steps to prevent the checking of superseded CRLs. For example, some revocation checking software will by default use the "Next Update" field referred to above to determine the refresh frequency for the CRL, and as explained above, this is not a valid approach for this service. OSIS can provide advice on the configuration of CRL checking software if required.

8.2.4 Obligatory revocation of Certificates

Table 6 –Obligatory revocation

Revocation by	Obligations
Individuals and Unipass Controllers	Individuals and Unipass Controllers (where appointed) must request revocation of an Individual Certificate in accordance with the Individual Certificate Rules of Use (or earlier Individual Contract).
Nominated Persons	Nominated Persons must request revocation of an Organisation Certificate in accordance with the Nominated Person Guidelines.
End User Organisations	End User Organisations shall request revocation of the Individual Certificates of their Individuals in accordance with the relevant End User Organisation Contract. End User Organisations shall request revocation of their Organisation Certificates in accordance with the relevant End User Organisation Contract.
Relying Party Organisations and their Associated Companies	These Organisations, Associated Companies and Network Members (where applicable) shall request revocation of their Certificates or those of their Individuals (as applicable) when: • any of the information that the Certificates contain is known or suspected to be inaccurate or could reasonably be believed to have been compromised; • there has been a loss, theft, modification, disclosure or other compromise of the Private Key of a Certificate; • any activation data, such as a password or PIN, used to protect the Private Key of a Certificate is compromised or suspected to have been compromised; • there is a change in the identity of that Organisation, Associated Company or Network Member, e.g. through merger or acquisition, or cessation of membership; or • the integrity/security of a Certificate or the Private Key is potentially compromised by an event of Force Majeure or computer or communications failure.

Table 6 –Obligatory revocation

8.2.5 Discretionary revocation

OSIS will revoke a Certificate or Certificates where it reasonably determines it is necessary to do so.

Individuals, Unipass Controllers or OSIS may request revocation of an Individual Certificate and Nominated Persons, Associated Companies, Organisations or OSIS may request revocation of an Organisation Certificate when:

- a change of details requires a Certificate to be issued with content different than the original;

- in relation to an Individual Certificate, the performance of an Individual's or OSIS' obligations under the Individual Certificate Rules of Use (or earlier Individual Contract or other applicable agreement) is delayed or prevented by an event beyond either party's reasonable control;
- in relation to an Organisation Certificate, the performance of a Nominated Person's, an Organisation's, an Associated Company's, or OSIS' obligations under the Organisation Contract or other applicable agreement is delayed or prevented by an event beyond either party's reasonable control;
- in relation to Individual Certificates, the Individual is in breach of the Individual Certificate Rules of Use (or earlier Individual Contract);
- in relation to Organisation Certificates, the Organisation or its Associated Companies are in material breach of the Organisation Contract;
- in relation to Organisation Certificates, the Nominated Person is in material breach of the Nominated Person Guidelines; or
- it is discovered that the Individual Certificate or Organisation Certificate was not issued in accordance with the requirements of this CPS.

8.2.6 Authority for Revocation

Revocation requests are permitted from a number of sources, but authority to revoke varies as defined in Table 8 below.

Table 7 – revocation request sources and authority levels

Source of revocation request	Authority to request revocation for
OSIS	Any, or all, Individual Certificates or Organisation Certificates.
Contract Owner, or another appropriately authorised representative	Own Individual Certificate, or Individual Certificates for Individuals within the Organisation (or Associated Company or Network Member if appropriate) of the Contract Owner/authorised representative.
Unipass Controller	Own Individual Certificate, or Individual Certificates for Individuals within the Organisation of the Unipass Controller.
Individual	Own Individual Certificate.
Organisation and any Associated Companies where permitted	Own Organisation Certificate (via Nominated Person or Contract Owner or authorised representative).

Table 7 – revocation request sources and authority levels

8.2.7 Effect of revocation on Certificates and underlying obligations

Upon revocation of a Certificate, that Certificate's operational period is immediately terminated. Such revoked Certificates should not be used or relied upon. Revocation of a Certificate does not affect any underlying contractual obligations created under the relevant Contract.

8.2.8 Appeals against revocation

Individuals and Organisations shall have the right of appeal to OSIS in respect of the revocation of their Individual Certificate or Organisation Certificate (or their Associated Company's Organisation Certificate) if this has occurred at the request of any third party.

If an Individual's or Organisation's appeal is successful and OSIS determines that the Certificate should not have been revoked, a new Certificate may be issued in accordance with the normal procedure.

Re-issuance using the same Distinguished Name may not be permitted following revocation by parties other than the Individual. For example, if an Individual leaves Organisation 'A' and joins another Organisation 'B', the Individual shall not be permitted to obtain a Certificate containing an identity that refers to the Individual as belonging to Organisation 'A'.

8.2.9 Cancellation of contracts and revocation

Cancellation is the process by which an Individual or Organisation terminates their Contract with OSIS under whose terms they have participated in the Unipass Service. Any Certificates issued under the terms of the Contract in question shall be revoked on the date of termination of the Contract, or earlier if requested by the Individual or Organisation.

8.3 Renewal of Certificates

8.3.1 Renewal notification

Within the last thirty days of the validity period of an Individual Certificate or within the last sixty days of the validity period in case of an Organisation Certificate, an e-mail renewal notice is sent to the Individual or Nominated Person to inform them that the Certificate is about to expire. The e-mail provides a hyperlink to a renewal page on the Unipass Website. On following this link, an Individual Certificate user must renew their acceptance of the Unipass Data Protection Policy and the Unipass Certificate Rules Of Use. A similar process is employed for Organisation Certificate users. As with Collections, the user may optionally view each of these documents in full by clicking on the appropriate hyperlink on this page. A similar renewal process may be employed for Trial Certificates, at the discretion of OSIS.

8.3.2 Renewal process – authentication requirements

The electronic request for Certificate renewal requires successful authentication through presentation of the appropriate in force credentials.

8.3.3 Certificate contents on renewal

During the renewal process, a new Key Pair is generated by the client browser, and the new Certificate is created and installed in the browser. The new Individual Certificate or the new Organisation Certificate retains the contents of the Certificate it replaces except for the validity dates, Public Key, and Certificate serial number, and there will, of course, also be a new Private Key, although this latter is not contained in the Certificate.

8.3.4 Effect of failure to renew before Expiry

Certificate renewal must take place prior to the expiration date of the current Certificate. Failure to renew prior to expiration will result in the Individual or Organisation or Associated Company or Network Member having to contact the Help Desk if a new Certificate is required.

8.3.5 Effect of Revocation on Renewal

If revocation has taken place prior to Certificate expiry, then Certificate renewal will not be offered. This will result in the Individual or Organisation or Associated Company or Network Member having to contact the Help Desk if a new Certificate is required.

8.4 Effect of Expiry and Revocation on contractual obligations

The expiry or revocation of a Certificate does not affect the validity of any underlying obligations arising under the relevant Individual Certificate Rules of Use (or earlier Individual Contract) or Organisation Contract (as appropriate).

9 CHANGE OF DETAILS

9.1 Introduction

A change of details may occur when an Individual's, Organisation's, Associated Company's, Network Member's or Nominated Person's circumstances change. OSIS must be promptly notified of such change of details. In relation to Individual Certificates it is the responsibility of the Individual and/or Unipass Controller, where one is established, to notify OSIS. In relation to Organisation Certificates, the Organisation or Associated Company must notify OSIS. There may be a resultant change of the Distinguished Name in one or more Certificates or any of the Distinguished Name's component Attributes, requiring a new Certificate or Certificates to be issued. This may also occur if there is a change in the role of the Individual that affects the identity in the Certificate (for example, where the Individual changes their department or job within the Organisation).

9.2 Change of details

At any time in the Certificate lifecycle, including during renewal, the Individual or Unipass Controller (as appropriate) in relation to Individual Certificates, and the Nominated Person in relation to Organisation Certificates, may request the amendment of details contained in OSIS' records. In some cases this will require revocation of the current Certificate and creation of a new Certificate reflecting the amended details. In others, only amendment of OSIS' records will be required.

The Help Desk will initiate re-issue of Individual Certificates following changes of details that trigger revocation where required, including re-issuing Individual Certificates to all Individuals of an Organisation as necessary.

9.2.1 Validation requirements

Change of detail requests for Individual Certificates are captured via a web form on the Unipass Website. The change of details web form requires authentication. The Individual or Unipass Controller requesting the change must provide reasons for changes (e.g. surname changed because Individual has married) together with supporting documentation where requested / if appropriate.

Changes of details of Organisation Certificates are captured via telephone to the Help Desk. The Nominated Person must provide reasons for changes together with supporting documentation where requested / if appropriate.

9.2.2 Determining whether change of details requires revocation

For Individual Certificates, revocation is necessary when changes are required to any part of the SubjectName field including: Forename, Surname, e-mail address, Individual type, or additional OU attributes.

Where Organisation details change, revocation of all Certificates issued to the Organisation, Associated Company or Network Member is necessary when changes are required to: Organisation type, Organisation name, Organisation postal code, or FCA Reference number.

10 THE HELP DESK AND UNIPASS WEBSITE

10.1 Help Desk

10.1.1 Functions of the Help Desk

The Help Desk performs a number of elements of the Unipass Service including the provision of:

- help and advice;
- processing and validation of applications;
- processing and validation of revocations and changes of detail;
- Certificate application status updates; and
- processing and validation of contract cancellation requests,.

10.1.2 Hours of operation

The Help Desk (including in relation to the processing and validation of Certificate applications and the revocation of Certificates) is usually available from Monday to Friday between the hours of 9am – 5pm (excluding bank holidays in England or Scotland).

10.1.3 Contact details

The telephone number for the Help Desk is 0131 385 8888. The Help Desk can also be contacted by e-mail using **helpdesk@unipass.co.uk** or by using the Contact Us page on the Unipass Website.

10.1.4 Validation of telephone requests to the Help Desk

On receipt of an inbound telephone request where authentication of the caller is required (e.g. revocation, change of pass phrase), the Help Desk will attempt to identify the caller using their name, registered telephone number, Organisation, Associated Company or Network Member name (as appropriate), and any other available data that helps uniquely identify the caller.

If the caller is satisfactorily identified, the Help Desk will authenticate the caller using the answer to their secret questions.

10.2 Unipass Website

The primary URL for the Unipass Website is **www.unipass.co.uk**.

Other than for planned maintenance, it is usually available 24 x 7 x 365.

10.2.1 Functions of the Unipass Website

The Unipass Website provides an overview of the service and lots of relevant information and functionality including:

- the Certificate application pages;
- the Unipass Controller pages;
- the latest information on where Unipass can be used;
- a Contact Us page;
- Frequently Asked Questions (FAQs);
- a test page to allow easy testing of whether a Certificate is operational and valid;
- revocation facilities to allow Certificates to be rendered inoperative for security or other reasons; • change of details pages;
- contractual and legal terms; and
- copies of this CPS, both current and one prior version.

11 MISCELLANEOUS PROVISIONS

11.1 Fiduciary Relationships

OSIS, and its CA are not the agents, fiduciaries, trustees, broker, partner or other representatives of Individuals, Organisations, Associated Companies or Network Members. The relationship which OSIS has with Individuals, Organisations, Associated Companies and Network Members is not that of agent and principal and this CPS shall not create a partnership or relationship of principal and agent between OSIS and any Individual, Organisation, Associated Company or Network Member or between any Supplier and any Individual, Organisation, Associated Company or Network Member. Neither Organisations, Associated Companies nor Individuals have any authority to bind OSIS, by contract or otherwise, to any obligation. OSIS shall make no representations to the contrary, either expressly, implicitly, by appearance, or otherwise.

11.2 Amending this CPS

OSIS may amend this CPS from time to time and at its sole discretion. Any such change shall only be made prospectively; no retrospective amendments shall be made. Such amendments shall supersede any conflicting and designated provision(s) of the referenced version of the CPS.
Subject to Section 11.5.1, the most recent effective copy of the CPS supersedes all previous versions and is binding on Individuals in respect of their use of, or reliance upon, Certificates after the date the change becomes effective. The CPS shall be available on the Unipass Website.

11.2.1 Routine Amendments

Subject to Section 11.2, amendments to the CPS shall become effective fifteen (15) days after OSIS publishes an updated version of the CPS on the Unipass Website, unless OSIS publishes a notice of withdrawal of the amendment prior to the end of such fifteen (15) day period. OSIS shall normally discuss amendments to the CPS with appropriate members of the Unipass Community, including The Unipass User Group, in advance of publication of an amended version of the CPS, but may at the sole discretion of OSIS publish an amended version of the CPS without such prior discussion.

11.2.2 Emergency Amendments

If, notwithstanding Section 11.2.1, OSIS needs to make amendments to this CPS where OSIS, acting reasonably and in good faith, is unable to give prior notice of the changes to be made, the change shall become effective immediately upon publication on the Unipass Website.

11.3 Intellectual Property Rights

OSIS shall own the Intellectual Property Rights and all other rights in relation to this CPS and any other documents, specifications or guidelines created or issued by OSIS.

OSIS or its Suppliers (as the case may be) shall own the Intellectual Property Rights and other rights in: (i) any data or information to the extent that it has been processed or generated by OSIS or its Suppliers in relation to the provision of the Unipass PKI and (ii) relation to Individual Certificates, Organisation Certificates, and Trial Certificates and CRLs issued by OSIS or its Suppliers.

In relation to Individual Certificates, the Individual's Public Keys and the Individual's Private Keys are the property of the Individual. In relation to Organisation Certificates, the Organisation's Public Keys and the Organisation's Private Keys are the property of the Organisation. OSIS' Public Keys and OSIS' Private Keys, including any that are assigned to or used by its Suppliers, are the property of OSIS.

For the avoidance of doubt and other than as expressly authorised in the other provisions of this CPS, copying, extraction and/or re-utilisation of all or a substantial part of: (i) Certificates, (ii) the contents of or data in any Certificate and/or (iii) any database containing Certificates (including without limitation the Repository) or other database of OSIS, is not permitted unless OSIS, and where applicable its Suppliers, have granted an express licence to do so. OSIS and its Suppliers reserve the right to pursue such unauthorised use, or infringement of its Intellectual Property Rights.

Each Certificate is copyrighted: Copyright © Origo Secure Internet Services Limited (OSIS). All rights reserved.

11.4 Successors and assignees

This CPS is binding upon OSIS and its successors and assignees.

11.5 Liability

11.5.1 Old Customer Contracts

Notwithstanding any other provision of this CPS, the liability of OSIS and Customers in terms of those Customer Contracts which are still in force and which were entered into with OSIS prior to April 24th 2003 shall be governed by section 11.5 of the appropriate earlier version of the Certification Practice Statement of OSIS which was effective at the date when the Customer Contracts were entered into.

11.5.2 Trial Certificates

OSIS shall have no liability for any costs, claims, expenses, loss and/or damage arising under or in connection with Trial Certificates.

11.5.3 Members of Unipass Community

Subject to Sections 11.5.1 and 11.5.2 above, the liability of OSIS to members of the Unipass Community is set out in the appropriate Contract and Individual Certificate Rules of Use.

11.5.4 Non-Members of Unipass Community

OSIS shall not be liable to third parties who use or rely on a Certificate where they are not a member of the Unipass Community. For the avoidance of doubt, Certificates are only issued to members of the Unipass Community for use by those members and by other members of the Unipass Community and NOT for the use of any third party.

11.6 Severability

If any provision of this CPS is found to be invalid, illegal or unenforceable for any reason by any court or regulatory body of competent jurisdiction, that provision shall be severed and the remainder of the provisions of this CPS shall continue in full force and effect as if this CPS had been executed with the invalid, illegal or unenforceable provision eliminated. The invalid, illegal or unenforceable term shall be replaced by a valid and enforceable term that is as close as possible to the economic effect of the original term. Each obligation of the CPS shall be construed as a separate obligation in each country and if one or more of the obligations or part of an obligation in the CPS is held by a court or regulatory body of competent jurisdiction to be invalid, illegal or unenforceable in any respect, then the validity, legality and enforceability of that obligation or part thereof shall not be affected or impaired in any way in any other jurisdiction.

11.7 Survival

Sections of this CPS shall, in respect of any actions based upon a Certificate issued subject to this CPS, survive the termination or withdrawal from use of this CPS, irrespective of whenever and however that termination or withdrawal from use occurs. Any such termination or withdrawal from use of this CPS shall not prejudice or affect any right of action or remedy that may have accrued to any person up to and including the date of such termination or withdrawal.

11.8 Complaints

In submitting a complaint to OSIS in relation to the Unipass Service, the applicant or Individual shall accept OSIS' absolute authority in this matter. OSIS shall acknowledge receipt of the complaint upon receipt, indicating the anticipated period for the complaint to be investigated.

11.9 Definitions and interpretation

In this CPS, unless otherwise specified or the context otherwise requires:

- the terms and expressions which are set out in Appendix 1 of this CPS shall have the meanings set out therein; • the masculine includes the feminine and the neuter; and
- the singular includes the plural and vice versa.

Headings are used in this CPS for ease of reference only and shall not affect the interpretation or construction of this CPS.

References to Sections are to the sections of this CPS. References to persons are to individuals, bodies corporate, firms, other unincorporated associations and governmental or supra-national authorities.

A reference to any statute, enactment, ordinance, order, regulation or other similar instrument shall be construed as a reference to the statute, enactment, ordinance, order, regulation or instrument as amended by any subsequent statute, enactment, ordinance, order, regulation or instrument or as contained in any subsequent re-enactment thereof.
In the event and to the extent only of any conflict or inconsistency between:

- the terms of this CPS and the Individual Certificate Rules of Use, the terms of the Individual Certificate Rules of Use take precedence over this CPS; or
- the terms of this CPS and any Guidelines, the terms of those Guidelines shall take precedence over this CPS; or
- the terms of this CPS and any Organisation Contract, those Organisation Contracts shall, subject to the further provisions of this Section as noted below, take precedence over this CPS.

So as to give effect and proper meaning to all Customer Contracts which are still valid and in force:

- References in this CPS to “Individuals” shall be construed as meaning “Customers” when read in conjunction with a Customer Contract;
- References in this CPS to “Individual Certificate Rules of Use” shall unless the context otherwise requires, be construed as meaning “Customer Contract” when read in connection with the obligations of a Customer pursuant to a Customer Contract;
- References in this CPS to “Unipass Controllers” shall be construed as meaning “Certificate Administrators” when read in conjunction with a Customer Contract; • References in this CPS to “Unipass Community” shall be construed as meaning “Customer Community” when read in conjunction with a Customer Contract; and
- References in Clauses 3 and 4 of the Customer Contract to the Customer’s “obligations set out in the CPS” shall be construed as meaning “obligations set out in the Individual Certificate Rules of Use”.

References in this CPS to “Individual Certificate Rules of Use” shall unless the context otherwise requires, be construed as meaning “Individual Contract” when read in connection with the obligations of an Individual pursuant to an Individual Contract.

Please note that some Organisation Contracts which are still valid and in force may refer to “Administrator” and “Administrator Guidelines”. For the avoidance of any doubt these are the old terms for describing “Unipass Controllers” and “Unipass Controller Guidelines” respectively and references in any Organisation Contract to any such terms should be construed as meaning “Unipass Controllers” and “Unipass Controller Guidelines” as appropriate.

Please note that some Organisation Contracts which are still valid and in force may refer to “Product Provider Organisations”, “Portal Organisations” or “Network Organisations”. For the avoidance of any doubt these are old terms for describing types of Organisation which are now collectively known as “Relying Party Organisations” and references in any Organisation Contract to any such term should be construed as meaning a “Relying Party Organisation”.

11.10 Waiver

The failure of OSIS to insist upon strict performance of any provision of this CPS, or the failure of OSIS to exercise any right or remedy to which it is entitled under this CPS, shall not constitute a waiver thereof and shall not cause a diminution of the obligations established by this CPS. A waiver of any breach of this CPS shall not constitute a waiver of any subsequent breach of this CPS. No waiver of any of the provisions of this CPS shall be effective unless it is expressly stated to be a waiver and communicated to the other relevant parties in writing.

11.11 Third party rights

Nothing in this CPS shall give, directly or indirectly, any third party (including without limitation any Associated Company, Network Member, Nominated Person or Individual) any benefit or any right of action against OSIS and such third parties shall not be entitled to enforce any term of this CPS against OSIS.

APPENDIX 1

DEFINITIONS

"Administrator"	:	shall have the same meaning as “Unipass Controller”;
"Administrator Guidelines”	:	shall have the same meaning as “Unipass Controller Guidelines”;
"Approved Person"	:	means a person who is authorised under the Financial Services and Markets Act 2000, and whose activities are regulated by the FCA (formerly known as a Registered
"Associated Company"	:	Individual);
		means any holding company from time to time of a Relying Party Organisation or any subsidiary from time to time of a Relying Party Organisation or of any such holding company (as defined by section 1261 of the Companies Act 2006 as amended, modified or reenacted from time to time) and Associated Companies shall be construed accordingly;;
"Attribute"	:	
"Basic Constraints"		means a subcomponent of a Distinguished Name as defined by the X.520 standard or other related standard;
	:	means a Certificate Extension identifying whether the Certificate denotes a CA, Organisation or Individual, and for a CA any restrictions upon that CA for the Certificates it may issue;
“CA Certificate”	:	
		means a Certificate issued to a CA subject to the requirements set out in Section 2.7;
"Certificate"	:	
		means a data file conforming to the X.509 standard that identifies the, Individual, Organisation, the Subordinate CA or Root CA (as appropriate), contains the Individual's, the Organisation's, the Subordinate CA's or Root CA's (as appropriate) Public Key, identifies the Certificate's operational period, contains a Certificate serial no and identifies OSIS as the
"Certificate Extension"		issuer of the Certificate;
	:	means a non-mandatory (relative to compliance with the X.509 standard) field of a Certificate bearing additional information about the usage or subject of the Certificate;
"Certificate Revocation List" or "CRL"	:	means a list of unique serial numbers and associated revocation timestamps identifying those Certificates that have been revoked in accordance with this CPS and as published by
"Certificate Revocation Status Service" or "CRSS"	:	OSIS or its Suppliers;
		means online access to the revocation information in the Repository, via either of the CRL or OCSP, being the two methods of access currently made available by OSIS, to enable certain Organisations (and their Associated Companies where applicable) to identify those Certificates that have been revoked;
"Certificate Validating Software"	:	means hardware or software that is or has been activated for the purpose of validating a Certificate;
"Certification Authority" or "CA"	:	means an entity that is widely trusted to create, assign and manage Certificates;
"Certification Practice Statement" or “CPS”	:	means a statement of the practices that are employed in issuing, revoking and managing Certificates;
"Collection E-mail"	:	means the information to enable collection of a Certificate sent in an e-mail from OSIS to an applicant in response to a valid application for a Certificate;
“Contract”	:	means an Organisation Contract (or an Individual Contract if still applicable);
“Contract Owner”	:	means any person who is either an employee, contractor, partner, principal, director or officer of an Organisation who (i) is designated by OSIS as the relevant “contract owner” for that Organisation in connection with the provision of the Unipass Service by OSIS to that Organisation and its Individuals pursuant to the relevant Organisation Contract and (ii) has authority from his Organisation to be the initial signatory to the Organisation Contract and/or the authorised person who is responsible for the performance of aspects of the Organisation

Contract and use of the Unipass Service by other Individuals of that Organisation);

"Critical Processing" : means any series of data processing tasks or steps forming a discrete and indivisible whole that must be completed within a finite period of time to meet contractual requirements;

"CRL Distribution Points"		means a Certificate Extension identifying from where the CRL relevant to the Certificate may be obtained;
“Customer”	:	means any person who was issued with, or who uses or relies on a Certificate and who has entered into a Customer Contract with OSIS;
“Customer Contract”	:	means the online contract between Customers and OSIS with the heading “Customer Contract” which was used up to April 24th 2003 and then replaced by OSIS with the Individual Contract on April 24th 2003;
"Decryption"	:	see the definition for Encryption and the word “Decrypted” shall be construed accordingly;
"Digital Signature"	:	means a datum that is uniquely associated with a message, file or other data from which it has been generated, and is of a form by which it can be unambiguously associated with or linked to a person or entity, generally by means of a suitable cryptographic key;
"Discontinuity"	:	means the occurrence of a significant incident or disaster;
"Distinguished Name"	:	means a data structure comprising one or more Attributes each of which has an associated value, the combination of Attributes being unique relative to the naming hierarchy within which it is defined;
“Encryption”	:	means the process of disguising data by means of a cryptographic key and an appropriate algorithm so that the meaning of the data is only clear to an intended recipient (one that can undertake the reverse process, that of Decryption, in order to reveal that meaning) and the words “Encrypt”, “Encrypted” and “Encrypted” shall be construed accordingly;
"End User Organisation"	:	means firms within, or transacting with, the UK financial services industry, including financial intermediaries, advisers, brokers and any other related or similar classes of firm who form part of the UK financial services industry, who wish to use Organisation Certificates and/or Individual Certificates (as applicable) to identify themselves in electronic trading;
"End User Organisation Contract"	:	means the contract between OSIS and an End User Organisation setting out the obligations of the End User Organisation either in relation to (i) the acceptance, use and reliance on Organisation Certificates by it and its Nominated Persons, and/or (ii) the acceptance, use and reliance on Individual Certificates by its Individuals; means a firm or other business entity which may be authorised by the Financial Services Authority, which firm or business entity forms part of the Unipass Community referred to in Section 1, and which may utilise financial intermediaries as a channel to market for its products, including Product Providers, mortgage lenders, fund managers, healthcare
"Financial Institution"	:	providers and insurance providers;
"Force Majeure"	:	means any cause affecting the performance by any person of its obligations under this CPS arising from acts, events, omissions, happenings or non-happenings beyond its reasonable control including, without prejudice to the generality of the foregoing, acts of God, governmental regulations, fire, flood, war or civil disturbance or any disaster or any industrial dispute or action affecting a third party for which a substitute third party is not reasonably available;
“Guidelines”		means the Unipass Controller Guidelines, Trusted Role Requirements, Nominated Person Guidelines, Nominated Person Requirements, Secure System Guidelines and any other guidelines which are available on the Unipass Website at **https://www.unipass.co.uk/Content/Documents/pdf/guidelines.pdf** and all of which may be updated or amended by OSIS from time to time;
“Help Desk”	:	means the support facility provided by OSIS to answer Certificate related queries, as described in Section 10;
"Individual"	:	means any person who is either an employee, affiliate, contractor, franchisee, partner, principal, director or officer of an Organisation who is issued with, uses or relies on an Individual Certificate or acts as a Unipass Controller and who has accepted the Individual

: Certificate Rules of Use (or if earlier, has entered into an Individual Contract with OSIS);

"Individual Certificate" : means a Certificate issued to an Individual to enable the Individual to identify himself;

"Individual Certificate Rules of Use"	:	means the rules that Individuals (including but not limited to Unipass Controllers) are required to accept and adhere to regarding (i) accepting, using or relying on an Individual Certificate and/or (ii) agreeing to act as a Unipass Controller, and which are available from the "Contracts & Legals" section of the Unipass Website;
"Individual Contract"	:	means the online contract between Individuals and OSIS with the heading "Contract for use of an Individual Certificate" which was used from 24th April 2003 and then replaced by OSIS with the Individual Certificate Rules of Use on 7th July 2006;
"Individual Identifier"	:	means a subcomponent of the SubjectName Field of a Certificate denoting the Individual who is the subject of the Certificate;
"Individual Type"	:	means the indication within an Individual Identifier that denotes the business role of the Individual within the meanings defined by this CPS;
"Intellectual Property Rights"	:	means patents, petty patents and utility models, trade marks, service marks, design rights (whether registrable or otherwise), semiconductor topography rights, applications for any of the foregoing, copyright, know-how, trade or business names, domain names and other similar rights or obligations whether registrable or not in any country;
"International Standards Organisation"	:	means the United Nations body that defines and agrees technical standards that are generally accepted by member countries;
"Key Pair"	:	means a Public Key and Private Key related in such a way that data encrypted using one half of the Key Pair can be decrypted using the other half. As a minimum, data Encrypted using a Public Key can be Decrypted using the associated Private Key, and a Digital Signature generated using a Private Key can be verified using the associated Public Key;
"Key Role"	:	means those employees, consultants or contractors of OSIS or Suppliers who are engaged in activities that result in access to or control over operations that may materially affect the issuance, use or revocation of Certificates;
"Key Usage"	:	means a Certificate Extension identifying the uses to which the Certificate and/or corresponding Private Key may be put;
"Material Event"	:	means an action of issuing, revoking, or managing a Certificate;
"Naming Authority"	:	means a body responsible for allocating digital identities or determining the procedures by which such allocation may occur in an orderly and unambiguous manner;
"Network Member"	:	means any organisation that is an official member of the Network Organisation;
"Network Organisation"	:	means an organisation that has official members conducting business within the UK financial services industry and which takes responsibility for the actions and omissions of its members (e.g. a directly authorised financial services intermediary which has appointed representatives);
"Nominated Person"	:	means an officer, partner, principal, director, employee and/or sub-contractor of an Organisation or Associated Company, who is responsible for performing certain activities in relation to Organisation Certificates as set out in the relevant Organisation Contract (and this CPS where applicable) on behalf of that Organisation or Associated Company (as applicable);
"Nominated Person Guidelines"	:	means the guidelines for Nominated Persons which are available on the Unipass Website at **https://www.unipass.co.uk/Content/Documents/pdf/guidelines.pdf** and which may be updated or amended by OSIS from time to time;
"Nominated Person Requirements"	:	means the criteria that all successful applicants for the position of Nominated Person are required to satisfy and which are available on the Unipass Website at **https://www.unipass.co.uk/Content/Documents/pdf/guidelines.pdf;**
"Object Identifier"	:	means a datum meeting the rules set forth by the relevant Naming Authority that uniquely

	:	identifies an object, typically a Certificate Policy, data type definition, or message definition;
"Online Certificate Status Protocol" or "OCSP"	:	means the mechanism allowing certain Organisations (and their Associated Companies where applicable) to determine in real time whether a Certificate has been revoked by interrogating the revocation information in the Repository;
"Organisation"	:	means a Relying Party Organisation or End User Organisation (as appropriate) which has entered into an Organisation Contract with OSIS;

"Organisation Certificate"	:	means a Certificate issued to an Organisation (or an Associated Company where applicable) for use by the Organisation (or Associated Company where applicable) to enable it to identify itself;
"Organisation Contract"	:	means a Relying Party Organisation Contract or End User Organisation Contract (as appropriate);
"Organisation Identifier"	:	means a subcomponent of the SubjectName Field of a Certificate denoting the Organisation to which the Individual who is the subject of the Certificate belongs;
"Organisation Type"	:	means an indicator within an Organisation Identifier denoting the type of Organisation within the meanings defined by this CPS;
"Personnel"	:	means the employees, consultants or contractors of OSIS and/or its Suppliers (as applicable) who are involved in the handling of Certificate applications and the issuance of Certificates;
"Private Key"	:	means a cryptographic key that may be used to generate Digital Signatures and for Decryption;
"Portal"	:	means software product vendors and providers of financial "portal" services including without limitation third party information services, aggregation services and comparative quotation services;
"Product Provider"	:	means a firm or other business entity authorised by the Financial Services Authority to carry out investment business, specifically to provide financial products covered by the regulations contained in the Financial Services Act 1986 or, from 30 November 2001, the Financial Services and Markets Act 2000, which firm or business entity forms part of the community referred to in Section 1;
"Public Key"	:	means a cryptographic key that may be used to verify Digital Signatures and for Encryption;
"Public Key Infrastructure" or "PKI"	:	means the set of hardware, software, people, policies and procedures needed to create, manage, store, distribute, and revoke Certificates based on public-key cryptography;
"Registered Individual"	:	see Approved Person;
"Registration Authority" or "RA"	:	means an entity by which certain management functions are carried out under this CPS, including the validation of requests to issue and revoke Certificates;
"Relying Party Organisation"	:	means firms or other organisations within the UK financial services industry, including without limitation Financial Institutions, Portals, Network Organisations and/or hub services, and any other related or similar classes of firm or organisation who form part of the UK financial services industry, who wish to use Organisation Certificates and/or Individual Certificates (as applicable) to identify their trading partners in electronic trading;

:

"Relying Party Organisation Contract"	:	means the contract between OSIS and a Relying Party Organisation setting out the obligations of the Relying Party Organisation in relation to (i) its acceptance and use of or reliance on Certificates and (ii) the acceptance and use of or reliance on Certificates by its Individuals, Nominated Persons, Associated Companies (and their Individuals and/or Nominated Persons), Network Members (and their Individuals and/or Nominated Persons), all as appropriate;
"Repository"	:	means a generally accessible database containing Certificates and certain other information relating to Certificates;
“Root CA”	:	means the CA in the Unipass PKI whose Public Key has been self-signed (see Section 2.6.1) and which meets the requirements in Section 2.7.1, and which is at the top of the OSIS private hierarchy, and under which subordinate CAs and/or Customer CA’s are located;
“Root CA Certificate”	:	means the CA Certificate issued to the Root CA by itself;
"Secure System"	:	means computer hardware and software, which are reasonably secure from intrusion and misuse, are adequately available, reliable and suitable for use in relation to the Unipass Service, and practices and procedures in respect of the same which incorporate provisions aimed at achieving the objectives set out in the Secure System Guidelines and which are enforced;

	:	
"Secure System Guidelines"		means the guidelines for the deployment and operation of a Secure System and which are available on the Unipass Website at **https://www.unipass.co.uk/Content/Documents/pdf/guidelines.pdf**;
"Security Mechanism"	:	means an algorithm or procedure embodied in hardware or software to provide one or more functions that fulfil generally accepted security requirements;
"SubjectName Field"	:	means the field of a Certificate giving the Distinguished Name of the Individual to whom the Individual Certificate is or has been issued or of the Organisation to whom the Organisation Certificate is or has been issued;
"Subordinate CA"	:	means a CA whose Public Key has been certified by another CA;
"Supplier"	:	means any entity contracted by OSIS to provide certain services to support the operation of
"Time Stamp"	:	the Unipass Service;
		means a datum included within or associated with an audit or other record denoting the date and time at which a particular event occurred and the words “Time Stamped” and “Time Stamping” shall be construed accordingly;
"Trial Certificate"	:	means a Certificate, with data content that either (i) signifies that it is for trial use or (ii) is non-verified fictitious information, that is issued to an Organisation (or Associated Company where applicable) and/or their staff for the limited purpose of assessing and testing the technology of the Unipass Service on a trial use basis (in accordance with (a) this CPS and any relevant additional contract in the case of Organisations and (b) the “Unipass Trial Certificate Terms and Conditions” in the case of their staff);
"Trusted Role Requirements"	:	means the criteria that all successful applicants for the position of Unipass Controller are required to satisfy and which are available on the Unipass Website at **https://www.unipass.co.uk/Content/Documents/pdf/guidelines.pdf**;
"Unipass Community"	:	means the assembled collection of individuals, firms and other entities which either (i) have entered into contracts with OSIS or (ii) are subject to contracts, in each case regarding the issue and use of Certificates participating in the Unipass Service for mutual benefit (including without limitation Individuals, Organisations, Associated Companies and Network Members);
"Unipass Controller" (formerly called “Administrator”)	:	means an officer, partner, principal, director or employee of an Organisation or of any Associated Company or Network Member who is responsible for performing certain registration and other activities in relation to Individual Certificates as set out in the relevant Individual Certificate Rules of Use and/or Contract (and this CPS where applicable) on behalf of that Organisation and other Individuals of that Organisation, Associated Company or Network Member as appropriate;
"Unipass Controller Guidelines" (formerly called “Administrator Guidelines”)	:	means the guidelines for Unipass Controllers which are available on the Unipass Website at **https://www.unipass.co.uk/Content/Documents/pdf/guidelines.pdf** and which may be updated or amended by OSIS from time to time;
"Unipass PKI"	:	means the Public Key Infrastructure operated by OSIS as part of the Unipass Service which, for the avoidance of doubt, includes without limitation the Repository and the CRSS;
"Unipass Service"	:	means the creation, validation, management, distribution, and revocation by OSIS and/or its Suppliers from time to time of Certificates based on public-key cryptography for business dealings between members of the Unipass Community within the financial services industry which service, for the avoidance of doubt, includes without limitation the Unipass PKI and the

"Unipass Website"	:	Help Desk;
"Universal Time Convention"	:	means the website(s) of OSIS, currently using a primary URL of **www.unipass.co.uk**, which may change from time to time at the sole discretion of OSIS; and means a date (year, month, day) and time value expressed in digits in the format YYMMDDHHMMSSZ, where the YY value if greater than or equal to 50 denotes the year 19YY and if less than 50 indicates the year 20YY, where the MM value is in the range 01 to 12 inclusive, where the DD value is in the range 01 to the number of days in the corresponding month of the corresponding year, where the HH value is in the range 00 to 23, where the MM value is in the range 00 to 59, where the SS value is in the range 00 to 59 and must always be included (even if zero), and where the letter Z must be included to denote Zulu (GMT).

APPENDIX 2

TABLE OF ACRONYMS AND ABBREVIATIONS

"FCA"	:	UK Financial Conduct Authority
"FIPS"	:	Federal Information Processing Standard
"GMT"	:	Greenwich Mean Time
"HTTP"	:	Hypertext Transfer Protocol
"HTTPS"	:	Hypertext Transfer Protocol with SSL
"IEC"	:	International Electrotechnical Commission, an industry standards body
"IETF"	:	Internet Engineering Task Force
"ISO"	:	International Standards Organisation
"ITU-T"	:	Technical committee of the International Telecommunications Union, an industry standards body
"OSIS"	:	Origo Secure Internet Services Limited
"PIA"	:	Personal Investments Authority, a former regulatory body that is now part of the FCA
"PIN"	:	Personal Identification Number
"SIB"	:	Securities and Investments Board, a former regulatory body that is now part of the FCA
"S/MIME"	:	Secure Multipurpose Internet Mail Extensions
"SSL"	:	Secure Sockets Layer
"URL"	:	Uniform Resource Locator, address of a web page or other object accessible via the WWW
"URN"	:	Unique Reference Number
"WWW or Web"	:	World Wide Web

:

"X.509"	:	The ISO and IEC/ITU-T standard for Certificates and their corresponding authentication framework
"X.520"	:	The ISO and IEC/ITU-T standard for Attributes of Distinguished Names