DIGI-SIGN

Certificate Practice Statement v3.6

Certificate Practice Statement
from Digi-Sign Limited.

Digi-CPS™

Version 3.6.
Produced by the Legal & Technical Departments

For further information, please contact:

CONTACT: Przemek Michalski

E-MAIL: cps@digi-sign.com
WEB: www.Digi-Sign.com

Digi-Sign Certificate Practice Statement – Digi-CPS™

Document Revision Date: 24 November, 2005.

Terms and Acronyms Used in this Digi-CPS™

Acronyms:

CA	Certificate Authority
CPS	Certification Practice Statement
Digi-CPS™	Digi-Sign CPS
CSR	Certificate Signing Request
HTTP	Hypertext Transfer Protocol
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardisation Sector
FTP	File Transfer Protocol
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (based on X.509 Digital Certificates)
PKCS	Public Key Cryptography Standard
URL	Uniform Resource Locator
CRL	Certificate Revocation List
SSL	Secure Sockets Layer
Digi-SSL™	Digi-Sign SSL
TLS	Transaction Layer Security
X.509	The ITU-T standard for Certificates and their corresponding authentication framework

Terms:

Applicant:	The Applicant is an entity applying for a Certificate.
Subscriber:	The Subscriber is an entity that has been issued a Certificate
Relying Party:	The Relying Party is an entity that relies upon the information contained within the Certificate.
Subscriber Agreement:	The Subscriber Agreement is an agreement, which must be read and accepted by an Applicant before applying for a Certificate. The Subscriber Agreement is specific to the Digital Certificate product type as presented during the product online order process and is available for reference at www.digi-sign.com.
Relying Party Agreement:	The Relying Party Agreement is an agreement which must be read and accepted by a Relying Party prior to validating, relying on or using a Certificate or accessing or using Digi-Sign's Repository and is available for reference at www.digi-sign.com.

DIGI-SIGN

INDEX

1 General

This document is the Digi-Sign Certification Practice Statement [Digi-CPS™] and outlines the legal, commercial and technical principles and practices that Digi-Sign employ in approving, issuing, using and managing of Digital Certificates and in maintaining a x.509 Certificate-based public key infrastructure (PKIX) in accordance with the Certificate Policies [Digi-CP™] determined by Digi-Sign. It also defines the underlying certification processes for Subscribers and describes Digi-Sign's repository operations. The CPS is also a means of notification of roles and responsibilities for parties involved in Certificate based practices within the Digi-Sign PKI.

1.1 Digi-Sign

Digi-Sign is a Certification Authority [CA] that issues high quality and highly trusted digital certificates to entities including private and public companies and individuals in accordance with this Digi-CPS™. In its role as a CA Digi-Sign performs functions associated with public key operations that include receiving requests, issuing, revoking and renewing a digital certificate and the maintenance, issuance and publication of Certificate Revocation Lists [CRLs] for users within the Digi-Sign PKI. In delivering its PKI services Digi-Sign commits itself to high-level international standards including those on Qualified Certificates pursuant to the European Directive 1999/93/EC. Digi-Sign acknowledges the relevant law on electronic signatures within the limits of which it operates.

Digi-Sign extends, under agreement, membership of its PKI to approved third parties known as Registration Authorities. The international network of Digi-Sign RAs share Digi-Sign's policies and practices and CA infrastructure to issue Digi-Sign digital certificates, or if appropriate, private labelled digital certificates.

1.2 Digi-Sign CPS

The Digi-CPS™ is a public statement of the practices of Digi-Sign and the conditions of issuance, revocation and renewal of a certificate issued under Digi-Sign's own hierarchy. Pursuant to the division of the tasks of a CA, this Digi-CPS™ is largely divided in the following sections: Technical, Organisational, Practices and Legal.

This Digi-CPS™, related agreements and Digi-CP™ referenced within this document are maintained by the Digi-Sign Certificate Policy Authority. The Certificate Policy Authority may be contacted at the below address:

Digi-Sign Limited
Enterprise Centre
Taylor's Lane
Dublin 8
Ireland
www.Digi-Sign.com

Attention: Legal Practices

Email: legal@digi-sign.com

This Digi-CPS™, related agreements and Certificate policies referenced within this document are available online at www.digi-sign.com/repository/

1.2.1 Digi-Sign CPS Suitability, Amendments and Publication

The Digi-Sign Certificate Policy Authority is responsible for determining the suitability of certificate policies illustrated within the Digi-CPS™. The Authority is also responsible for determining the suitability of proposed changes to the Digi-CPS™ prior to the publication of an amended edition. Upon the Certificate Policy Authority accepting such changes an updated edition of the Digi-CPS™ will be published at the Digi-Sign repository (available at www.digi-sign.com/repository/) and suitable incremental version numbering will be used to identify new editions.

Controls are in place to reasonably ensure that the Digi-CPS™ is not amended and published without the prior authorisation of the Certificate Policy Authority.

1.3 Other Practice Statements & Agreements

This Digi-CPS™ will from time to time mention external documents. The document name, location of and status, whether public or private, are detailed below:

Document	Status	Location
Digi-Sign Certification Practice Statement	Public	Digi-Sign Repository: www.digi-sign.com/repository/
Relying Party Agreement	Public	Digi-Sign Repository: www.digi-sign.com/repository/
Digi-SSL™ Lite Certificate Subscriber Agreement	Public	Digi-Sign Repository: www.digi-sign.com/repository/
Digi-SSL™ Premium Certificate Subscriber Agreement	Public	Digi-Sign Repository: www.digi-sign.com/repository/
Digi-SSL™ Trial Certificate Subscriber Agreement	Public	Digi-Sign Repository: www.digi-sign.com/repository/
Digi-ID™ Secure Email Certificate Subscriber Agreement	Public	Digi-Sign Repository: www.digi-sign.com/repository/
Digi-ID™ Enterprise Public Key Infrastructure Manager Agreement	Confidential	Presented to partners accordingly
Reseller Agreement	Confidential	Presented to partners accordingly
Reseller Agreement	Confidential	Presented to partners accordingly
Enterprise Public Key Infrastructure Manager Guide	Confidential	Presented to partners accordingly
Reseller Guide	Confidential	Presented to partners accordingly
Reseller Guide	Confidential	Presented to partners accordingly
Reseller Validation Guidelines	Confidential	Presented to partners accordingly

1.4 Governing Law

This agreement shall be governed by and construed in accordance with Irish law and the parties hereto agree to submit to the non-exclusive jurisdiction of the Irish courts.

1.5 Liability of Digi-Sign

For legal liability of Digi-Sign under the provisions made in this Digi-CPS™, please refer to section 5; legal conditions of issuance.

1.6 Compliance with applicable standards

The practices specified in this Digi-CPS™ have been designed to meet or exceed the requirements of generally accepted and developing industry standards including the AICPA/CICA WebTrust Program for Certification Authorities, ANS X9.79: 2001 PKI Practices and Policy Framework; BS 7799-2 for information Security Management Systems; Directive 1999/93/EC the Community Directive for the issuance of Qualified Electronic Signatures; and other industry standards related to the operation of CAs.

An audit is performed to assess Digi-Sign's compliancy with the aforementioned standards for Certification Authorities. Topics covered by the annual audit include the following:

- CA business practices disclosure
- Service integrity
- CA environmental controls

1.7 Digital Certificate Policy Overview

A digital certificate is formatted data that cryptographically binds an identified subscriber with a public key. A digital certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction. Digital certificates are used in commercial environments as a digital equivalent of an identification card.

As detailed in this Digi-CPS™, Digi-Sign offers a range of distinct certificate types. The different certificate types have differing intended usages and differing policies.

Applicant	Certificate Type	Channels Available	Validation Levels	Suggested Usage
Individual or Company	Secure Server Certificate: Digi-SSL™ Xs	• Digi-Sign Website • Reseller Network • Web Host Network	Confirmation of right to use the business name used in the application through the use of third party databases and / or business documentation plus right to use the domain name used in the application.	Establishes SSL / TLS session between the server housing the Secure Server Certificate and a client / customer / website visitor. The protocol is designed to authenticate a server to a client and provide confidentiality of data passed through the SSL / TLS session.
Individual or Company	Secure Server Certificate: Digi-SSL™ Xp	• Digi-Sign Website • Reseller Network • Web Host Network	Confirmation of right to use the business name used in the application through the use of third party databases and / or business documentation plus right to use the domain name used in the application.	Establishes SSL / TLS session between the server housing the Secure Server Certificate and a client / customer / website visitor. The protocol is designed to authenticate a server to a client and provide confidentiality of data passed through the SSL / TLS session.
Individual or Company	Secure Server Certificate: Digi-SSL™ Trial	• Digi-Sign Website • Reseller Network • Web Host Network	Confirmation of right to use the business name used in the application through the use of third party databases and / or business documentation	Establishes SSL / TLS session between the server housing the Secure Server Certificate and a client / customer / website visitor. The protocol is

			plus right to use the Domain name used in the Application.	designed to authenticate a server to a client and provide confidentiality of data passed through the SSL / TLS session.
Individual – non commercial use	Secure Email Certificate: Free Version	• Digi-Sign Website • Reseller Network	Email address search to ensure it is distinguished within the Digi-Sign PKI. Email ownership automated challenge is conducted as part of the collection process.	Allows certificate owner to digitally sign email, and for relying parties to verify a digitally signed email and to encrypt email for the certificate owner. May also be used for web based access control where prior validation of the certificate owner is deemed unnecessary.
Individual – corporate representative	Secure Email Certificate: Corporate Version	• On-Site	When opening an On-Site Control Centre Account, applicant must provide confirmation of right to use the business name used in the application through the use of third party databases and / or business documentation. Email address search to ensure it is distinguished within the On-Site Manager account. Company	Allows certificate owner to digitally sign email to prove corporate authorship, and for relying parties to verify a digitally signed email and to encrypt email for the certificate owner. May also be used for web based access control where prior validation of the certificate owner is deemed necessary.

			administering the On-Site Control Centre account must submit domain names for right to use validation prior to issuance of a Corporate Secure Email Certificate.	

Note: Validation levels: Validation is conducted by Digi-Sign or a Digi-Sign Registration Authority (if the application is made through a Reseller or Partner); a Global Validations Officer; or a Nominated Validations Officer under strict guidelines provided to the Registration Authority. Section 1.9 of this Digi-CPS™ identifies the Registration Authorities and outlines the roles and responsibilities of such entities.

As the suggested usage for a digital certificate differs on a per application basis, Subscribers are urged to appropriately study their requirements for their specific application before applying for a specific Digi-Sign certificate.

1.8 Digi-Sign PKI Hierarchy

Digi-Sign partner with USERTrust, Inc and GTE CyberTrust Solutions, Inc. (both are AICPA/CICA WebTrust Program for Certification Authorities approved security provider) for their Root CA Certificates. The partnership allows Digi-Sign to issue highly trusted digital certificates by inheriting the trust level associated with USERTrust, Inc and GTE CyberTrust Solutions, Inc. root certificates. The following high-level example of the Digi-Sign PKI is used to illustrate the hierarchy utilised.

UTN-USERFIRST-Hardware Root Expiry 9 July, 2019, 19:19:22
(serial number = 44 be 0c 8b 50 00 24 b4 11 d3 36 2a fe 65 0a fd)

Digi-Sign CA Digi-SSL Xp Expiry 9 July, 2019, 18:19:22
(serial number = 0b 41 f1 c4 71 62 6d d1 d3 55 42 af c5 62 bb cb)

End Entity SSL / End Entity Secure Email (serial number = x, expiry = 1/2/3 year from issuance)

1.9 Digi-Sign Certification Authority

In its role as a Certification Authority [CA] Digi-Sign provides certificate services within the Digi-Sign PKI. The Digi-Sign CA:

- Conform its operations to the CPS (or other CA business practices disclosure), as the same may from time to time be modified by amendments published in the Digi-Sign repository (http://www.digi-sign.com/repository/).

- Issue and publish certificates in a timely manner in accordance with the issuance times set out in this Digi-CPS™.

- Upon receipt of a valid request to revoke the certificate from a person authorised to request revocation using the revocation methods detailed in this Digi-CPS™, revoke a certificate issued for use within the Digi-Sign PKI.

- Publish CRLs on a regular basis, in accordance with the applicable Certificate Policy and with provisions described in this Digi-CPS™.

- Distribute issued certificates in accordance with the methods detailed in this Digi-CPS™.

- Notify applicants if a certificate application is rejected for reasons stated within this Digi-CPS™.

- Notify subscribers that a certificate has been revoked and update CRLs in a timely manner as detailed in this Digi-CPS™.

- Notify subscribers via email of the imminent expiry of their Digi-Sign issued certificate (for a period disclosed in this Digi-CPS™).

1.10 Digi-Sign Registration Authorities

Digi-Sign has established that the necessary secure infrastructure to fully manage the lifecycle of digital certificates within its PKI providers. Through a network of Registration Authorities [Digi-RA™], Digi-Sign also makes its certification authority services available to its subscribers. Digi-Sign RAs:

- Accept, evaluate, approve or reject the registration of certificate applications.

- Verify the accuracy and authenticity of the information provided by the subscriber at the time of application as specified in the Digi-Sign validation guidelines documentation.

- Use official notarised or otherwise indicated document to evaluate a subscriber application.

- Verify the accuracy and authenticity of the information provided by the subscriber at the time of reissue or renewal as specified in the Digi-Sign validation guidelines documentation.

A Digi-Sign Digi-RA™ acts locally within their own context of geographical or business partnerships on approval and authorisation by Digi-Sign in accordance with Digi-Sign practices and procedures.

Digi-Sign extends the use of Registration Authorities for its Reseller, On-Site™ Control Centre and Partner programs. Upon successful approval to join the respective programs the Reseller Subscriber, On-Site™ Subscriber or Partner Subscriber are permitted to act as a Digi-RA™ on behalf of Digi-Sign. Digi-RA™s are restricted to operating within the set validation guidelines published by Digi-Sign to the Digi-RA™ upon joining the programs. Certificates issued through A Digi-RA™ contains an amended Certificate Profile within an issued certificate to represent the involvement of the Digi-RA™ in the issuance process to the Relying Party.

1.10.1 Digi-Partner™: Referring

Digi-Sign operates a Reseller Partner Network [Digi-Partner™] that allows authorised Digi-Partners™ to integrate Digi-Sign digital certificates into their own product portfolios. Digi-Partners™ are responsible for referring digital certificate customers to Digi-Sign, who maintain full control over the certificate lifecycle process, including application, issuance, renewal and revocation. Due to the nature of the Digi-Partner™ program, the Digi-Partner™ must authorise a pending customer order made through its Digi-Partner™ account prior to Digi-Sign instigating the validation of such Certificate orders.

All Digi-Partner™ Partners are required to provide proof of organisational status and must enter into a Digi-Sign Digi-Partner™ agreement prior to being provided with Digi-Partner™ facilities.

1.10.2 Digi-Partner™: Provisioning

The Digi-Partner™ program also allows certain organisations providing hosting facilities to manage the certificate lifecycle on behalf of their hosting customers. Such Digi-Partners™ are permitted to apply for Digi-SSLs™ and Digi-IDs™ on behalf of their hosting customers.

Through a “front-end” referred to as the Control Centre™, the Digi-Partner™ has access to the Digi-RA™ functionality including the issuance of Digi-SSLs™ and Digi-IDs™. The Digi-Partner™ adheres to the validation processes detailed in the validation guidelines documentation presented by Digi-Sign as part of the agreement. The Digi-Partner™ is obliged to conduct validation in accordance with the validation guidelines and agrees via an online process that sufficient validation has taken place prior to issuing a certificate.

All Digi-Partners™ are required to provide proof of organisational status and must enter into a Digi-Sign Digi-Partner™ agreement prior to being provided with Digi-Partner™ facilities.

1.10.3 Control Centre™ Account Holders

Digi-Sign Control Centre™ Account Holders is a fully outsourced enterprise public key infrastructure service that allows authorised Digi-Partners™ account holders to control the entire certificate lifecycle process, including application, issuance, renewal and revocation, for certificates designated to company servers, intranets, extranets, partners, employees and hardware devices.

T hrough a “front-end” referred to as the Control Centre™, the Digi-Partner™ has access to the Digi-RA™ functionality including the issuance of Digi-SSLs™, Digi-Access™, Digi-Mail™ and Digi-IDs™.

The Account Holder is obliged to issue certificates only to legitimate company resources, including domain names (servers), intranets, extranets, partners, employees and hardware devices.

1.11 Subscribers

Subscribers of Digi-Sign services are individuals or companies that use PKI in relation with Digi-Sign supported transactions and communications. Subscribers are parties that are identified in a certificate and hold the private key corresponding to the public key that is listed in a subscriber certificate. Prior to verification of identity and issuance of a certificate a subscriber is an applicant for the services of Digi-Sign.

1.12 Relying Parties

Relying parties use PKI services in relation with Digi-Sign certificates that reasonably rely on such certificates and/or digital signatures verifiable with reference to a public key listed in a subscriber certificate. To verify the validity of a digital certificate they receive, relying parties must refer to the Certificate Revocation List [CRL] prior to relying on information featured in a certificate to ensure that Digi-Sign has not revoked the certificate. The CRL location is detailed within the certificate and is available from the Digi-Sign repository at: www.digi-sign.com.

2 Technology

This section addresses certain technology aspects of the Digi-Sign infrastructure and PKI services.

2.1 CA Infrastructure

The Digi-Sign CA Infrastructure uses trustworthy systems to provide certificate services. A trustworthy system is computer hardware, software, and procedures that provide an acceptable level against security risks, provide a reasonable level of availability, reliability, and correct operation and enforce a security policy.

2.1.1 Root CA Signing Key Protection & Recovery

The protection of the CA Root signing key pairs is ensured by the use of IBM 4578 crypto processor devices, which are certified to FIPS 140-1 Level 4, for key generation, storage and use. The CA Root signing key pairs are 2048 bit and was generated within the IBM 4578 device using the RSA algorithm.

For CA Root key recovery purposes, the Root CA signing keys are encrypted and stored within a secure environment. The decryption key is split across m removable media and require n of m to reconstruct the decryption key. Custodians in the form of 2 or more authorised officers are required to physically retrieve the removable media from the distributed physically secure locations.

Where CA Root signing keys are backed up to another cryptographic hardware security module, such keys are transferred between devices in encrypted format only.

USERTrust, Inc and GTE CyberTrust Solutions, Inc. ensure the protection of their respective CA Root signing key pairs in accordance with its AICPA/CICA WebTrust program compliant infrastructure and CPS. Details of USERTrust, Inc and GTE CyberTrust Solutions, Inc. WebTrust compliancy are available at their official websites.

2.1.2 CA Root Signing Key Generation Process

The private key(s) are securely generated and protected using a trustworthy system (IBM 4758 accredited to FIPS PUB 140-1 level 4), that takes necessary precautions to prevent the compromise or unauthorised usage of it.

The CA Root key was generated in accordance with the guidelines detailed in the Root Key Generation Ceremony Reference. The activities undergone and the personnel involved in the Root Key Generation Ceremony are recorded for audit purposes. Subsequent Root Key Generation Ceremonies are to follow the documented reference guide also.

2.1.3 CA Root Signing Key Archival

When the CA Root Signing Key pair expires, they will be archived for at least 7 years. The keys will be archived in a secure cryptographic hardware module as per their secure storage prior to expiration as detailed in section 2.1.1 of this Digi-CPS™.

2.1.4 Procedures employed for CA Root Signing Key Changeover

The Digi-Sign CA root signing private key is valid until 18:19:22pm 9 July, 2019. Upon the end of the private key's lifetime, a new CA signing key pair is generated and all subsequently issued certificates and CRLs are signed with the new private signing key. The corresponding new CA public key certificate is provided to subscribers and relying parties through the delivery methods detailed in section 2.1.5 of this Digi-CPS™.

2.1.5 CA Root Public Key Delivery to Subscribers

All CA Root Certificates are available from the online repository located at the following URL: (www.digi-sign.com.com/repository/). The UTN and GTE Root certificates are present in Internet Explorer 5.x and above, Netscape 4.x and above and Opera 5.x and above and is made available to relying parties through these browsers.

Digi-Sign provides the full certificate chain (see section 1.8 of this Digi-CPS™) to the Subscriber upon issuance and delivery of the Subscriber certificate.

2.1.6 Physical CA Operations

Access to the secure part of Digi-Sign's nominated facilities is limited through the use of physical access control and is only accessible to appropriately authorised individuals (referred to hereon as Trusted Personnel). Card access systems are in place to control, monitor and log access to all areas of the facility. Access to the Digi-Sign CA physical machinery within the secure facility is protected with locked cabinets and logical access control.

Digi-Sign has made reasonable efforts to ensure its secure facilities are protected from:

- Fire and smoke damage (fire protection is in accordance with fire regulations)
- Flood and water damage

Digi-Sign's nominated secure facilities have a primary and secondary power supply and ensure continuous, uninterrupted access to electric power. Heating / air ventilation systems are used to prevent overheating and to maintain a suitable humidity level.

Digi-Sign assert that it makes every reasonable effort to detect and prevent material breaches, loss, damage or compromise of assets and interruption to business activities.

2.2 Digital Certificate Management

Digi-Sign certificate management refers to functions that include the following:

- Verification of the identity of an applicant of a certificate.
- Authorising the issuance of certificates.
- Issuance of certificates.
- Revocation of certificates.
- De-commissioning of the corresponding private keys through a process involving the revocation of certificates.
- Listing of certificates.
- Distributing certificates.
- Publishing certificates.
- Storing certificates.
- Retrieving certificates in accordance with their particular intended use.

Digi-Sign conducts the overall certification management within the Digi-Sign PKI, either directly or through a Digi-Sign approved Digi-RA™. Digi-Sign is not involved in functions associated with the generation, issuance, decommissioning or destruction of a Subscriber key pair.

2.3 Digi-Sign Directories, Repository and Certificate Revocation List

Digi-Sign makes publicly available directories of revoked certificates through the use of CRLs. Users and relying parties are strongly urged to consult the directories of issued and revoked certificates at all times prior to relying on information featured on a certificate. Digi-Sign updates and publishes a new CRL daily or more frequently under special circumstances.

Digi-Sign also publishes a repository of legal notices regarding its PKI services, including this CPS, agreements and notices references within this CPS as well as any other information it considers essential to its services. The Digi-Sign legal repository may be accessed at www.digi-sign.com.com/repository/.

2.4 Types of Digi-Sign Certificates

Digi-Sign currently offers a portfolio of digital certificates and related products that can be used in a way that addresses the needs of users for secure personal and business communications, including but not exclusively secure email, protection of online transactions and identification of persons, whether legal or physical, or devices on a network or within a community.

Digi-Sign may update or extend its list of products, including the types of certificates it issues, as it sees fit. The publication or updating of the list of Digi-Sign products creates no claims by any third party. Upon the inclusion of a new certificate product in the Digi-Sign hierarchy, an amended version of this Digi-CPS™ will be made public on the official Digi-Sign websites.

Issued certificates are published in Digi-Sign directories. Suspended or revoked certificates are appropriately referenced in CRLs and published in Digi-Sign directories. Digi-Sign does not perform escrow of subscriber private keys.

2.4.1 Digi-SSL™ Secure Server Certificates

Digi-Sign makes available Secure Server Certificates that in combination with a Secure Socket Layer [SSL] web server attest the public server's identity providing full authentication and enable secure communication with corporate customers and corporate business partners.

Digi-Sign Secure Server Certificates are offered in two variants; Digi-SSL™ Xs and Digi-SSL™ Xp certificates. Pricing for the certificates are made available on the relevant official Digi-Sign websites. From time to time Digi-Sign reserve the right to make available promotional offers that may affect the standard price card.

a. Digi-SSL™ Xs

Digi-SSL™ Xs Certificates are the entry level Secure Server Certificate. Their intended usage is for the use of SSL for website authentication for the conduct of ecommerce or transferring data of low value and also for within internal networks.

The maximum warranty associated with a Digi-SSL™ Xs certificate is €1.00. Subscriber fees for a Digi-SSL™ Premium Certificate are available from the official Digi-Sign website.

b. Digi-SSL™ Xp

Digi-SSL™ Xp Certificates are the professional level Secure Server Certificatesn. Their intended usage is for the use of SSL for website authentication for the conduct of high value ecommerce and transferring data and also within internal networks.

All Digi-SSL™ Xp Certificate applications include an out of bands validation of the applicant's submitted information.

The maximum warranty associated with a Digi-SSL™ Xp certificate is €10,000. Subscriber fees for a Digi-SSL™ Premium Certificate are available from the official Digi-Sign website.

d. Digi-SSL™ Trial

Digi-SSL™ Trial Certificates are Secure Server Certificates designed to help customers use SSL in a test environment prior to the roll out of a full SSL solution.

Digi-SSL™ Trial Certificates may not be used in an external environment and ultimately should not contain information relied upon by the relying party. Digi-SSL™ Trial Certificates are not validated prior to issuance in accordance.

Digi-SSL™ Trial Certificates are for test use only and do not carry a warranty.

There is no charge for a Digi-SSL™ Trial Certificate.

2.4.2 Digi-Access™ Two Factor Authentication Certificates

Digi-Sign makes available Digi-ID™ Two Factor Authentication Certificates [Digi-Access™] that allow subscribers to authenticate to servers and devices for relying parties or relying parties to authenticate the subscriber. Pricing for the Digi-Access™ Certificates are made available on the relevant official Digi-Sign websites. From time to time Digi-Sign reserve the right to make available promotional offers that may affect the standard price card.

a. Free Digi-Access™ Certificate

Free Digi-Access™ Certificates are issued to natural persons only and may not be used by an individual as a means of representation for a specific company.

In accordance with section 4.2.4 (Validation Practices) of this Digi-CPS™, and through the use of an email ownership validation check, Digi-Sign asserts that the subscriber owns, or has direct access to, the email address stated within the Digi-Access™ Certificate. However, as verification of the subscriber does not take place the identity of the subscriber cannot be warranted.

There is no charge for a Free Digi-Access™ Certificate.

b. Digi-Access™ Corporate Certificates

Corporate Digi-Access™ Certificates are issued to natural persons only and may be used by an individual as a means of representation for a company named within the certificate.

Corporate Digi-Access™ Certificates are available to holders of an On-Site™ or Digi-CA™ account. The account may be used to apply for Digi-Sign certificates (SSL, Secure Email and Two Factor Authentication) and will contain the corporate details (name, address, country) of the account holding company.

On-Site™ and Digi-CA™ authorised administrators may log into the Control Centre™ account and apply for Corporate Digi-Access™ Certificates for employees or authorised representatives of the company only.

In accordance with section 4.2.5 (Validation Practices) of this Digi-CPS™, Digi-Sign validates the right of the company to use the domain name specified within the Corporate Digi-Access™ Certificate. The company must attest to the legitimacy of the individual named within the application prior to the issuance of the Corporate Digi-Access™ Certificate.

The maximum warranty associated with a Corporate Digi-Access™ Certificate is €10,000.

Subscriber fees for a Corporate Digi-Access™ Certificate are available from the official Digi-Sign website.

2.4.3 Digi-Mail™ Secure Email Certificates

Digi-Sign makes available Digi-ID™ Secure Email Certificates [Digi-Mail™] that in combination with a S/MIME compliant email application allow subscribers to digitally sign email for relying parties or relying parties to encrypt email for the subscriber. Pricing for the Digi-Mail™ Certificates are made available on the relevant official Digi-Sign websites. From time to time Digi-Sign reserve the right to make available promotional offers that may affect the standard price card.

b. Free Digi-Mail™ Certificate

Free Digi-Mail™ Certificates are issued to natural persons only and may not be used by an individual as a means of representation for a specific company.

In accordance with section 4.2.4 (Validation Practices) of this Digi-CPS™, and through the use of an email ownership validation check, Digi-Sign asserts that the subscriber owns, or has direct access to, the email address stated within the Digi-Mail™ Certificate. However, as verification of the subscriber does not take place the identity of the subscriber cannot be warranted.

There is no charge for a Free Digi-Mail™ Certificate.

b. Digi-Mail™ Corporate Certificates

Corporate Digi-Mail™ Certificates are issued to natural persons only and may be used by an individual as a means of representation for a company named within the certificate.

Corporate Digi-Mail™ Certificates are available to holders of an On-Site™ or Digi-CA™ account. The account may be used to apply for Digi-Sign certificates (SSL, Secure Email and Two Factor Authentication) and will contain the corporate details (name, address, country) of the account holding company.

On-Site™ and Digi-CA™ authorised administrators may log into the Control Centre™ account and apply for Corporate Digi-Mail™ Certificates for employees or authorised representatives of the company only.

In accordance with section 4.2.5 (Validation Practices) of this Digi-CPS™, Digi-Sign validates the right of the company to use the domain name specified within the Corporate Digi-Mail™ Certificate. The company must attest to the legitimacy of the individual named within the application prior to the issuance of the Corporate Digi-Mail™ Certificate.

The maximum warranty associated with a Corporate Digi-Mail™ Certificate is €10,000.

Subscriber fees for a Corporate Digi-Mail™ Certificate are available from the official Digi-Sign website.

2.4.4 Digi-ID™ Multi-Use Certificates

Digi-Sign makes available Digi-ID™ Certificates for Digi-Access™, Digi-Mail™ and other uses for Digi-IDs™ such as device-to-device authentication, IPSec Certificates [Digi-IPSec™], transaction signing, electronic signature and digital identity that allow subscribers to use the multiple functions of the Digi-ID™. Pricing for the Digi-ID™ Certificates are made available on the relevant official Digi-Sign websites. From time to time Digi-Sign reserve the right to make available promotional offers that may affect the standard price card.

c. Free Digi-ID™ Certificate

Free Digi-ID™ Certificates are issued to natural persons only and may not be used by an individual as a means of representation for a specific company.

In accordance with section 4.2.4 (Validation Practices) of this Digi-CPS™, and through the use of an email ownership validation check, Digi-Sign asserts that the subscriber owns, or has direct access to, the email address stated within the Digi-Mail™ Certificate. However, as verification of the subscriber does not take place the identity of the subscriber cannot be warranted.

There is no charge for a Free Digi-ID™ Certificate.

b. Digi-ID™ Corporate Certificates

Corporate Digi-ID™ Certificates are issued to natural persons only and may be used by an individual as a means of representation for a company named within the certificate.

Corporate Digi-ID™ Certificates are available to holders of an On-Site™ or Digi-CA™ account. The account may be used to apply for Digi-Sign certificates (SSL, Secure Email and Two Factor Authentication) and will contain the corporate details (name, address, country) of the account holding company.

On-Site™ and Digi-CA™ authorised administrators may log into the Control Centre™ account and apply for Corporate Digi-ID™ Certificates for employees or authorised representatives of the company only.

In accordance with section 4.2.5 (Validation Practices) of this Digi-CPS™, Digi-Sign validates the right of the company to use the domain name specified within the Corporate Digi-ID™ Certificate. The company must attest to the legitimacy of the individual named within the application prior to the issuance of the Corporate Digi-Mail™ Certificate.

The maximum warranty associated with a Corporate Digi-ID™ Certificate is €10,000.

Subscriber fees for a Corporate Digi-Mail™ Certificate are available from the official Digi-Sign website.

2.5 Extensions and Naming

2.5.1 Digital Certificate Extensions

Digi-Sign uses the standard X.509, version 3 to construct digital certificates for use within the Digi-Sign PKI. X.509v3 allows a CA to add certain certificate extensions to the basic certificate structure. Digi-Sign use a number of certificate extensions for the purposes intended by X.509v3 as per Amendment 1 to ISO/IEC 9594-8, 1995. X.509v3 is the standard of the International Telecommunications Union for digital certificates.

2.5.2 Reference for Extensions & Enhanced Naming

Enhanced naming is the usage of an extended organisation field in an X.509v3 certificate. Information contained in the organisational unit field is also included in the Certificate Policy extension that Digi-Sign may use.

2.6 Subscriber Private Key Generation Process

The Subscriber is solely responsible for the generation of the private key used in the certificate request. Digi-Sign does not provide key generation, escrow, recovery or backup facilities.

Upon making a certificate application the Subscriber is solely responsible for the generation of an RSA key pair appropriate to the certificate type being applied for. During application the Subscriber will be required to submit a public key and other personal / corporate details in the form of a Certificate Signing Request [CSR].

Typically, Digi-SSL™ requests are generated using the key generation facilities available in the Subscriber's webserver software. Typically, Digi-Mail™ requests are generated using the FIPS 140-1 Level 1 cryptographic service provider module software present in popular browsers.

2.7 Subscriber Private Key Protection and Backup

The Subscriber is solely responsible for protection of their private keys. Digi-Sign maintains no involvement in the generation, protection or distribution of such keys.

Digi-Sign strongly urge Subscribers to use a password or equivalent authentication method to prevent unauthorised access and usage of the Subscriber private key.

2.8 Subscriber Public Key Delivery to Digi-Sign

Digi-SSL™ requests are generated using the Subscriber's webserver software and the request is submitted to Digi-Sign in the form of a PKCS #10 CSR. Submission is made electronically via the Digi-Sign website or through a Digi-Sign approved Digi-RA™.

Digi-Mail™ Certificate requests are generated using the Subscriber's cryptographic service provider software present in the Subscriber's browser and is submitted to

Digi-Sign in the form of a PKCS#10 Certificate Signing Request [CSR]. Submission is generally made automatically by the Subscriber's browser.

2.9 Delivery of Issued Subscriber Certificate to Subscriber

Delivery of Subscriber certificates to the associated Subscriber is dependent on the certificate product type:

2.9.1 Secure Server Certificate: Digi-SSL™ product type

If the Digi-Sign operated database holds sufficient validation information, an automatic validation of the Digi-SSL™ certificate application may take place. In the event of such an automated validation the Digi-SSL™ certificate is delivered to commonly used generic email addresses ordinarily belonging to authorised personnel at the domain name used in the application, such as webmaster@... admin@... postmaster@... Confirmation of the certificate delivery location is provided to the administrator contact provided during the application process.

2.9.2 Digi-SSL™

Digi-SSL™ Xs and Digi-SSL™ Xp certificates are delivered via email to the Subscriber through the use of the administrator contact email address provided during the application process; or they are delivered through the On-Site™ or Digi-CA™ Control Centre™.

2.9.3 Digi-Access™

Upon issuance of the Digi-Access™ Certificate the Subscriber is emailed a collection link using the email provided during the application. The Subscriber must visit the collection link using the same computer from which the original Digi-Access™ request was made. The Subscriber's cryptographic service provider software is initiated to ensure the Subscriber holds the private key corresponding to the public key submitted during application. Pending a successful challenge, the issued Digi-Access™ is installed automatically onto the Subscriber's computer; or they are delivered through the On-Site™ or Digi-CA™ Control Centre™ for the Administrator to distribute on hardware such as a USB Key Token [Digi-Token™] or smart card [Digi-Card™] or as a software delivery in PKCS#12 format that is protected by a password.

2.9.4 Digi-Mail™

Upon issuance of the Digi-Mail™ Certificate the Subscriber is emailed a collection link using the email provided during the application. The Subscriber must visit the collection link using the same computer from which the original Digi-Mail™ request was made. The Subscriber's cryptographic service provider software is initiated to ensure the Subscriber holds the private key corresponding to the public key submitted during application. Pending a successful challenge, the issued Digi-Mail™ is installed automatically onto the Subscriber's computer; or they are delivered through the On-Site™ or Digi-CA™ Control Centre™ for the Administrator to distribute on hardware such as a USB Key Token [Digi-Token™] or smart card

[Digi-Card™] or as a software delivery in PKCS#12 format that is protected by a password.

2.9.5 Digi-ID™

Upon issuance of the Digi-ID™ Certificate the Subscriber is emailed a collection link using the email provided during the application. The Subscriber must visit the collection link using the same computer from which the original Digi-ID™ request was made. The Subscriber's cryptographic service provider software is initiated to ensure the Subscriber holds the private key corresponding to the public key submitted during application. Pending a successful challenge, the issued Digi-ID™ is installed automatically onto the Subscriber's computer; or they are delivered through the On-Site™ or Digi-CA™ Control Centre™ for the Administrator to distribute on hardware such as a USB Key Token [Digi-Token™] or smart card [Digi-Card™] or as a software delivery in PKCS#12 format that is protected by a password.

2.10 Delivery of Issued Digi-SSL™ to Digi-Partner™

Issued Digi-SSL™ Certificates applied for through a Digi-Partner™ on behalf of the Subscriber are emailed to the administrator contact of the Digi-Partner™ account; or they can collect the issued Digi-SSL™ from a Digi-Partner™ account specific URL; or they are delivered for collection through the On-Site™ or Digi-CA™ Control Centre™.

2.11 Delivery of Issued Digi-ID™ to Digi-Partner™

Issued Digi-IDs™, Digi-Access™ and Digi-Mail™ applied for by the Digi-Partner™ through the On-Site™ or Digi-CA™ are delivered as per sub-sections 2.9.3, 2.9.4, 2.9.5, of this Digi-CPS™.

2.12 Digi-Sign Certificates Profile

A Certificate profile contains fields as specified below:

2.12.1 Key Usage extension field

Digi-Sign certificates are general purpose and may be used without restriction on geographical area or industry. In order to use and rely on a Digi-Sign certificate the relying party must use X.509v3 compliant software. Digi-Sign certificates include key usage extension fields to specify the purposes for which the certificate may be used and also to technically limit the functionality of the certificate when used with X.509v3 compliant software. Reliance on key usage extension fields is dependent on correct software implementations of the X.509v3 standard and is outside of the control of Digi-Sign.

The possible key purposes identified by the X.509v3 standard are the following:

a) Digital signature, for verifying digital signatures that have purposes other than those identified in b), f) or g), that is, for entity authentication and data origin authentication with integrity.

b) Non-repudiation, for verifying digital signatures used in providing a non-repudiation service which protects against the signing entity falsely denying some action (excluding certificate or CRL signing, as in f) or g) below).

c) Key encipherment, for enciphering keys or other security information, e.g. for key transport.

d) Data encipherment, for enciphering user data, but not keys or other security information as in c) above.

e) Key agreement, for use as a public key agreement key

f) Key certificate signing, for verifying a CA's signature on certificates, used in CA-certificates only.

g) CRL signing, for verifying a CA's signature on CRLs.

h) Encipher only, public key agreement key for use only in enciphering data when used with key agreement.

i) Decipher only, public key agreement key for use only in deciphering data when used with key agreement.

2.12.2 Extension Criticality Field

The Extension Criticality field denotes two separate uses for the Key Usage field. If the extension is noted as critical, then the key in the certificate is only to be applied to the stated uses. To use the key for another purpose in this case would break the issuer's policy. If the extension is not noted as critical, the Key Usage field is simply there as an aid to help applications find the proper key for a particular use.

2.12.3 Basic Constraints Extension

The Basic Constraints extension specifies whether the subject of the certificate may act as a CA or only as an end-entity certificate. Reliance on basic constraints extension field is dependent on correct software implementations of the X.509v3 standard and is outside of the control of Digi-Sign.

2.12.4 Certificate Policy [Digi-CP™]

Certificate Policy [Digi-CP™] is a statement of the issuer that corresponds to the prescribed usage of a digital certificate within an issuance context. A policy identifier is a number unique within a specific domain that allows for the unambiguous identification of a policy, including a certificate policy.

Example Digi-Sign certificate profiles are as per the tables on the proceeding pages:

Digi-SSL™ Xp	
Signature Algorithm	SHA1
Issuer	CN: Digi-Sign CA Digi-SSL Xp OU: Terms and Conditions of use: http://www.digi-sign.com/repository OU: Digi-Sign Trust Network O: Digi-Sign Limited L: Dublin S: Dublin C: IE
Validity	1 Year / 2 Year / 3 Year
Subject	CN: [Common Name - Host name] OU: Digi-SSL Xp OU: Provided by Digi-Sign Limited O: [Organisation] OU: [Organisation Unit] L: [Locality] S: [State] C: [Country]
Authority Key Identifier	KeyID=33 5a 0b 4e 35 da b8 8e 87 05 64 5f d8 ec 7d 25 98 da ba 3f
Key Usage (Critical)	Digital Signature, Key Encipherment (A0)
Netscape Certificate Type	SSL Client Authentication, SSL Server Authentication (c0)
Basic Constraint	Subject Type=End Entity Path Length Constraint=None
Certificate Policies	[1]Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.6449.1.2.2.9 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.digi-sign.com/repository
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.digi-sign.com/DigiSignCADigiSSLXp.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl2.digi-sign.com/DigiSignCADigiSSLXp.crl
Thumbprint Algorithm	SHA1

Digi-SSL™ Xs	
Signature Algorithm	SHA1
Issuer	CN: Digi-Sign CA Digi-SSL Xs OU: Terms and Conditions of use: http://www.digi-sign.com/repository OU: Digi-Sign Trust Network O: Digi-Sign Limited L: Dublin S: Dublin C: IE

Validity	1 Year / 2 Year / 3 Year
Subject	CN: [Common Name - Host name] OU: Digi-SSL Xs OU: Provided by Digi-Sign Limited O: [Organisation] OU: [Organisation Unit] L: [Locality] S: [State] C: [Country]
Authority Key Identifier	KeyID=a1 72 5f 26 1b 28 98 43 95 5d 07 37 d5 85 96 9d 4b d2 c3 45
Key Usage (Critical)	Digital Signature, Key Encipherment (A0)
Netscape Certificate Type	SSL Client Authentication, SSL Server Authentication (c0)
Basic Constraint	Subject Type=End Entity Path Length Constraint=None
Certificate Policies	[1]Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.6449.1.2.2.9 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.digi-sign.com/repository
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.digi-sign.com/DigiSignCADigiSSLXs.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl2.digi-sign.com/DigiSignCADigiSSLXs.crl
Thumbprint Algorithm	SHA1

Digi-SSL™ Xg	
Signature Algorithm	SHA1
Issuer	CN: Digi-Sign CA Digi-SSL Xs OU: Terms and Conditions of use: http://www.digi-sign.com/repository OU: Digi-Sign Trust Network O: Digi-Sign Limited L: Dublin S: Dublin C: IE
Validity	1 Year / 2 Year / 3 Year
Subject	CN: [Common Name - Host name] OU: Digi-SSL Xs OU: Provided by Digi-Sign Limited O: [Organisation] OU: [Organisation Unit] L: [Locality] S: [State] C: [Country]

Authority Key Identifier	KeyID=a1 72 5f 26 1b 28 98 43 95 5d 07 37 d5 85 96 9d 4b d2 c3 45
Key Usage (Critical)	Digital Signature, Key Encipherment (A0)
Netscape Certificate Type	SSL Client Authentication, SSL Server Authentication (c0)
Basic Constraint	Subject Type=End Entity Path Length Constraint=None
Certificate Policies	[1]Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.6449.1.2.2.9 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.digi-sign.com/repository
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.digi-sign.com/DigiSignCADigiSSLXs.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl2.digi-sign.com/DigiSignCADigiSSLXs.crl
Thumbprint Algorithm	SHA1

Digi-SSL™ Trial		
Signature Algorithm	SHA1	
Issuer	CN	Digi-Sign CA Digi-SSL Xs
	OU	Terms and Conditions of use: http://www.digi-sign.com/repository
	OU	Digi-Sign Trust Network
	O	Digi-Sign Limited
	L	Dublin
	S	Dublin
	C	IE
Validity	1 Year / 2 Year / 3 Year	
Subject	CN	[Common Name - Host name]
	OU	Provided by Digi-Sign Limited
	O	[Organisation]
	OU	[Organisation Unit]
	L	[Locality]
	S	[State]
	C	[Country]
Authority Key Identifier	KeyID=a1 72 5f 26 1b 28 98 43 95 5d 07 37 d5 85 96 9d 4b d2 c3 45	
Key Usage (Critical)	Digital Signature, Key Encipherment (A0)	
Netscape Certificate Type	SSL Client Authentication, SSL Server Authentication (c0)	
Basic Constraint	Subject Type=End Entity Path Length Constraint=None	
Certificate Policies	[1]Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.6449.1.2.2.9 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.digi-sign.com/repository	

CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.digi-sign.com/DigiSignCADigiSSLXs.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl2.digi-sign.com/DigiSignCADigiSSLXs.crl
Thumbprint Algorithm	SHA1

Digi-Access™ (Free Trial Version)		
Signature Algorithm	SHA1	
Issuer	CN	Digi-Sign CA Digi-Access
	OU	Terms and Conditions of use: http://www.digi-sign.com/repository
	O	Digi-Sign Limited
	L	Dublin
	S	Dublin
	C	IE
Validity	14 Days / 30 Days	
Subject	E	[Email address]
	CN	[Common Name - Name of subscriber]
	OU	DEMO ONLY, NOT VALIDATED, NO WARRANTY ATTACHED
	OU	issued by Digi-Sign Limited
	O	[Organisation]
	OU	[Organisation Unit]
	L	[Locality]
	C	[Country]
	Ph	[Phone]
Authority Key Identifier	KeyID=08 0d 00 61 c3 a6 ce d4 ac 6e df 57 9e 60 ed 44 10 5b 81 4e	
Key Usage (Critical)	Digital Signature, Key Encipherment (A0)	
Extended Key Usage (NonCritical)	Client Authentication (1.3.6.1.5.5.7.3.2)	
Netscape Certificate Type	SSL Client Authentication	
Basic Constraint	Subject Type=End Entity Path Length Constraint=None	
Certificate Policies	[1] Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.6449.1.2.2.9 [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.digi-sign.com/repository	
CRL Distribution Points	[1] CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.digi-sign.com/DigiSignCADigiAccess.crl [2] CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl2.digi-sign.com/DigiSignCADigiAccess.crl	
Thumbprint Algorithm	SHA1	

Digi-Access™ (Corporate Version)		
Signature Algorithm	SHA1	
Issuer	CN	Digi-Sign CA Digi-Access
	OU	Terms and Conditions of use: http://www.digi-sign.com/repository
	O	Digi-Sign Limited
	L	Dublin
	S	Dublin
	C	IE
Validity	1 Year / 2 Years / 3 Years	
Subject	E	[Email address]
	CN	[Common Name - Name of subscriber]
	OU	validated by [Corporate Name]
	OU	issued by Digi-Sign Limited
	O	[Organisation]
	OU	[Organisation Unit]
	L	[Locality]
	C	[Country]
	Ph	[Phone]
Authority Key Identifier	KeyID=08 0d 00 61 c3 a6 ce d4 ac 6e df 57 9e 60 ed 44 10 5b 81 4e	
Key Usage (Critical)	Digital Signature, Key Encipherment (A0)	
Extended Key Usage (NonCritical)	Client Authentication (1.3.6.1.5.5.7.3.2)	
Netscape Certificate Type	SSL Client Authentication	
Basic Constraint	Subject Type=End Entity Path Length Constraint=None	
Certificate Policies	[1] Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.6449.1.2.2.9 [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.digi-sign.com/repository	
CRL Distribution Points	[1] CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.digi-sign.com/DigiSignCADigiAccess.crl [2] CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl2.digi-sign.com/DigiSignCADigiAccess.crl	
Thumbprint Algorithm	SHA1	

Digi-Mail™ (Free Trial Version)		
Signature Algorithm	SHA1	
Issuer	CN	Digi-Sign CA Digi-ID Xp
	OU	Terms and Conditions of use: http://www.digi-sign.com/repository
	O	Digi-Sign Limited
	L	Dublin
	S	Dublin
	C	IE

Validity	14 Days / 30 Days	
Subject	E	[Email address]
	CN	[Common Name - Name of subscriber]
	OU	DEMO ONLY, NOT VALIDATED, NO WARRANTY ATTACHED
	OU	issued by Digi-Sign Limited
	O	[Organisation]
	OU	[Organisation Unit]
	L	[Locality]
	C	[Country]
	Ph	[Phone]
Authority Key Identifier	KeyID=91 b3 8a e8 7e 16 6f f9 12 1c 3f 29 a4 50 10 44 0b d9 77 76	
Key Usage (Critical)	Digital Signature, Key Encipherment (A0)	
Extended Key Usage (NonCritical)	Secure Email (1.3.6.1.5.5.7.3.4) Client Authentication (1.3.6.1.5.5.7.3.2) [not in use]	
Netscape Certificate Type	SSL Client Authentication [not in use], SMIME (A0)	
Basic Constraint	Subject Type=End Entity Path Length Constraint=None	
Certificate Policies	[1] Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.6449.1.2.2.9 [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.digi-sign.com/repository	
CRL Distribution Points	[1] CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.digi-sign.com/DigiSignCADigiIDXp.crl [2] CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl2.digi-sign.com/DigiSignCADigiIDXp.crl	
Thumbprint Algorithm	SHA1	

Digi-Mail™ (Xp™ Corporate Version)		
Signature Algorithm	SHA1	
Issuer	CN	Digi-Sign CA Digi-ID Xp
	OU	Terms and Conditions of use: http://www.digi-sign.com/repository
	O	Digi-Sign Limited
	L	Dublin
	S	Dublin
	C	IE
Validity	1 Year / 2 Years / 3 Years	
Subject	E	[Email address]
	CN	[Common Name - Name of subscriber]
	OU	validated by [Corporate Name]
	OU	issued by Digi-Sign Limited
	O	[Organisation]
	OU	[Organisation Unit]
	L	[Locality]
	C	[Country]
	Ph	[Phone]

Authority Key Identifier	KeyID=91 b3 8a e8 7e 16 6f f9 12 1c 3f 29 a4 50 10 44 0b d9 77 76
Key Usage (Critical)	Digital Signature, Key Encipherment (A0)
Extended Key Usage (NonCritical)	Secure Email (1.3.6.1.5.5.7.3.4) Client Authentication (1.3.6.1.5.5.7.3.2) [not in use]
Netscape Certificate Type	SSL Client Authentication [not in use], SMIME (A0)
Basic Constraint	Subject Type=End Entity Path Length Constraint=None
Certificate Policies	[1] Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.6449.1.2.2.9 [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.digi-sign.com/repository
CRL Distribution Points	[1] CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.digi-sign.com/DigiSignCADigiIDXp.crl [2] CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl2.digi-sign.com/DigiSignCADigiIDXp.crl
Thumbprint Algorithm	SHA1

Digi-ID™ (Free Trial Version)		
Signature Algorithm	SHA1	
Issuer	CN	Comodo Class 3 Security Services CA
	OU	(c)2002 Comodo Limited
	OU	Terms and Conditions of use: http://www.comodo.net/repository
	OU	Comodo Trust Network
	O	Comodo Limited
	C	GB
Validity	14 Days / 30 Days	
Subject	E	[Email address]
	CN	[Common Name - Name of subscriber]
	OU	DEMO ONLY, NOT VALIDATED, NO WARRANTY ATTACHED
	OU	issued by Digi-Sign Limited
	O	[Organisation]
	OU	[Organisation Unit]
	L	[Locality]
	C	[Country]
	Ph	[Phone]
Authority Key Identifier	KeyID=36 e0 e8 7c 6d 9d 45 91 ee 99 e5 42 76 4d 70 b3 50 30 ac 5e	
Key Usage (Critical)	Digital Signature, Key Encipherment (A0)	
Extended Key Usage (NonCritical)	Secure Email (1.3.6.1.5.5.7.3.4) Client Authentication (1.3.6.1.5.5.7.3.2)	
Netscape Certificate Type	SSL Client Authentication, SMIME (A0)	
Basic Constraint	Subject Type=End Entity Path Length Constraint=None	
Certificate Policies	[1] Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.6449.1.2.1.3.5	

	[1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://secure.comodo.net/CPS
CRL Distribution Points	[1] CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.comodo.net/Class3SecurityServices_3.crl [2] CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.comodoca.com/Class3SecurityServices_3.crl [3]CRL Distribution Point Distribution Point Name: Full Name: RFC822 Name= Class3SecurityServices_3@crl.comodo.net
Thumbprint Algorithm	SHA1

Digi-ID™ (Corporate Version)		
Signature Algorithm	SHA1	
Issuer	CN	Comodo Class 3 Security Services CA
	OU	(c)2002 Comodo Limited
	OU	Terms and Conditions of use: http://www.comodo.net/repository
	OU	Comodo Trust Network
	O	Comodo Limited
	C	GB
Validity	1 Year / 2 Years / 3 Years	
Subject	E	[Email address]
	CN	[Common Name - Name of subscriber]
	OU	validated by [Corporate Name]
	OU	issued by Digi-Sign Limited
	O	[Organisation]
	OU	[Organisation Unit]
	L	[Locality]
	C	[Country]
	Ph	[Phone]
Authority Key Identifier	KeyID=36 e0 e8 7c 6d 9d 45 91 ee 99 e5 42 76 4d 70 b3 50 30 ac 5e	
Key Usage (Critical)	Digital Signature, Key Encipherment (A0)	
Extended Key Usage (NonCritical)	Secure Email (1.3.6.1.5.5.7.3.4) Client Authentication (1.3.6.1.5.5.7.3.2)	
Netscape Certificate Type	SSL Client Authentication, SMIME (A0)	
Basic Constraint	Subject Type=End Entity Path Length Constraint=None	
Certificate Policies	[1] Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.6449.1.2.1.3.5 [1,1] Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://secure.comodo.net/CPS	
CRL Distribution Points	[1] CRL Distribution Point	

	Distribution Point Name: Full Name: URL= http://crl.comodo.net/Class3SecurityServices_3.crl [2] CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.comodoca.com/Class3SecurityServices_3.crl [3]CRL Distribution Point Distribution Point Name: Full Name: RFC822 Name= Class3SecurityServices_3@crl.comodo.net
Thumbprint Algorithm	SHA1

2.13 Digi-Sign Certificate Revocation List Profile

The profile of the Digi-Sign Certificate Revocation List is as per the table below:

Version	**[Version 1]**	
Issuer Name	Country Name=[Root Certificate Country Name], Organisation Name=[Root Certificate Organisation], Common Name=[Root Certificate Common Name] [UTF8String encoding]	
This Update	[Date of Issuance]	
Next Update	[Date of Issuance + 2 hours]	
Revoked Certificates	CRL Entries	
	Certificate Serial Number	[Certificate Serial Number]
	Date and Time of Revocation	[Date and Time of Revocation]

3 Organisation

Digi-Sign operates within the United States of America, Ireland, the United Kingdom Poland, Turkey and India, with separate operations, research & development and server operation sites. All sites operate under a security policy designed to, within reason, detect, deter and prevent unauthorised logical or physical access to CA related facilities. This section of the Digi-CPS™ outlines the security policy, physical and logical access control mechanisms, service levels and personnel policy in use to provide trustworthy and reliable CA operations.

3.1 Conformance to this Digi-CPS™

Digi-Sign conforms to this Digi-CPS™ and other obligations it undertakes through adjacent contracts when it provides its services.

3.2 Termination of CA Operations

In case of termination of CA operations for any reason whatsoever, Digi-Sign provides timely notice and transfer of responsibilities to succeeding entities, maintenance of records, and remedies. Before terminating its own CA activities, Digi-Sign takes the following steps:

- Providing subscribers of valid certificates with ninety (90) days notice of its intention to cease acting as a CA.
- Revoking all certificates that are still unrevoked or unexpired at the end of the ninety (90) day notice period without seeking subscriber's consent.
- Giving timely notice of revocation to each affected subscriber.
- Making reasonable arrangements to preserve its records according to this CPS.
- Reserving its right to provide succession arrangements for the re-issuance of certificates by a successor CA that has all relevant permissions to do so and complies with all necessary rules, while its operation is at least as secure as Digi-Sign's.

The requirements of this article may be varied by contract, to the extent that such modifications affect only the contracting parties.

3.3 Form of Records

Digi-Sign retains records in electronic or in paper-based format for a period detailed in section 3.4 of this Digi-CPS™. Digi-Sign may require subscribers to submit appropriate documentation in support of a certificate application.

Digi-RAs™ are required to submit appropriate documentation as detailed in the Digi-Partner™ agreements, On-Site™ and Digi-CA™ agreements, prior to being validated and successfully accepted as an approved Digi-RA™.

In its role as a Digi-RA™, Digi-RA™ may require documentation from subscribers to support certificate applications. In such circumstances, Digi-RAs™ are obliged to retain such records in line with the practices of record retention and protection as used by Digi-Sign and as stated in this Digi-CPS™.

3.4 Records Retention Period

Digi-Sign retains the records of Digi-Sign digital certificates and the associated documentation for a term of no less than 7 years. The retention term begins on the date of expiration or revocation. Such records may be retained in electronic, in paper-based format or any other format that Digi-Sign may see fit.

Such records are archived at a secure off-site location and are maintained in a form that prevents unauthorised modification, substitution or destruction.

3.5 Logs for Core Functions

The following events for core functions for audit purposes are maintained by electronic or manual logs. All logs are archived at a secure off-site location and both current and archived logs are maintained in a form that prevents unauthorised modification, substitution or destruction.

All logs include the following elements:

- Date and time of entry
- Serial or sequence number of entry
- Kind of entry
- Source of entry
- Identity of entity making log entry

3.5.1 CA & Certificate Lifecycle Management

- CA Root signing key functions, including key generation, backup, recovery and destruction
- Subscriber certificate life cycle management, including successful and unsuccessful certificate applications, certificate issuances, certificate re-issuances, certificate renewals
- Subscriber certificate revocation requests, including revocation reason
- Subscriber changes of affiliation that would invalidate the validity of an existing certificate
- Certificate Revocation List updates, generations and issuances

- Custody of keys and of devices and media holding keys
- Compromise of a private key

3.5.2 Security Related Events

- System downtime, software crashes and hardware failures
- CA system actions performed by Digi-Sign personnel, including software updates, hardware replacements and upgrades
- Cryptographic hardware security module events, such as usage, deinstallation, service or repair and retirement
- Successful and unsuccessful Digi-Sign PKI access attempts
- Secure CA facility visitor entry and exit

3.5.3 Certificate Application Information

- The documentation and other related information presented by the applicant as part of the application validation process
- Storage locations, whether physical or electronic of presented documents.

3.5.4 Log Retention Period

Logs are maintained for a period of 7 years, or longer if necessary to comply with applicable laws.

3.6 Business Continuity Plans and Disaster Recovery

To maintain the integrity of service, periodical tests, appropriate contingency and disaster recovery plans and procedures are implemented and documented. Such plans are revised and updated as may be required at least once a year.

- The CA system operated is fully redundant. The backup CA is readily available in the event that the primary CA should cease operation.
- Operations are distributed across two sites, with Bradford West Yorkshire, UK being the primary operations site and Tonbridge, Kent, UK being the secondary site. Both sites offer facilities to manage the lifecycle of a certificate, including the application, issuance, revocation and renewal of such certificates.
- Backup of critical CA software is performed weekly and is stored offsite.

- Backup of critical business information is performed daily and is stored offsite.

As well as a fully redundant CA system, provisions for the activation of a backup CA and a secondary site is maintained should the primary site suffer a total loss of systems. This disaster recovery plan states that an interruption in CA operations will not exceed 72 hours.

3.7 Availability of Revocation Data

Digi-Sign publishes CRLs to allow relying parties to verify a digital signature made using a Digi-Sign issued digital certificate. Each CRL is valid for 24 hours, and Digi-Sign issue a new CRL prior to the expiry of the current CRL. Under special circumstances Digi-Sign may publish new CRLs prior to the expiry of the current CRL. All expired CRLs are archived for a period of 7 years, or longer if applicable. Digi-Sign CRLs are available at the Digi-Sign repository at www.digi-sign.com/repository/.

3.8 Publication of Critical Information

Digi-Sign publishes any revocation data on issued digital certificates, this Digi-CPS™, certificate terms and conditions, the relying party agreement and copies of all subscriber agreements the official Digi-Sign repository at www.digi-sign.com/repository/. The Digi-Sign repository is maintained by the Digi-Sign Certificate Policy Authority and all updates, amendments and legal promotions are logged in accordance with the logging procedures referenced in this Digi-CPS™.

3.9 Confidential Information

Digi-Sign observes applicable rules on the protection of personal data deemed by law or the Digi-Sign privacy policy (see section 3.11 of this Digi-CPS™) to be confidential.

3.9.1 Types of Information deemed as Confidential

Digi-Sign keeps the following types of information confidential and maintains reasonable controls to prevent the exposure of such records to non-trusted personnel.

- Subscriber agreements
- Certificate application records and documentation submitted in support of certificate applications whether successful or rejected
- Transaction records and financial audit records
- External or internal audit trail records and reports, except for WebTrust audit reports which may be published at the discretion of Digi-Sign

- Contingency plans and disaster recovery plans
- Internal tracks and records on the operations of Digi-Sign infrastructure, certificate management and enrolment services and data

3.9.2 Types of Information not deemed as Confidential

Subscribers acknowledge that revocation data of all certificates issued by the Digi-Sign CA is public information is periodically published every 24 hours at the Digi-Sign repository.

Subscriber application data marked as "Public" in the relevant subscriber agreement and submitted as part of a certificate application is published within an issued digital certificate in accordance with section 2.12.4 of this Digi-CPS™.

3.9.3 Access to Confidential Information

All personnel in trusted positions handle all information in strict confidence. Especially personnel of RA/LRAs comply with the requirements of the Irish law on the protection of personal data.

3.9.4 Release of Confidential Information

Digi-Sign is not required to release any confidential information without an authenticated, reasonably specific request by an authorised party specifying:

- The party to whom Digi-Sign owes a duty to keep information confidential.
- The party requesting such information.
- A court order, if any.

3.10 Personnel Management and Practices

Consistent with this Digi-CPS™ Digi-Sign follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties.

3.11 Privacy Policy

Digi-Sign has implemented a privacy policy, which is in compliance with this Digi-CPS™. The Digi-Sign privacy policy is published at the Digi-Sign repository at www.digi-sign.com/repository/.

3.12 Publication of information

The Digi-Sign certificate services and the Digi-Sign repository are accessible through several means of communication:

- On the web: www.Digi-Sign.com
- By email from legal@Digi-Sign.com
- and by mail from:

Digi-Sign Limited
Enterprise Centre
Taylor's Lane
Dublin 8
Ireland

Tel: +353 (1) 662-1249
Fax: +353 (1) 662-1652
Web: www.digi-sign.com
Email: legal@digi-sign.com

4 Practices and Procedures

This section describes the certificate application process, including the information required to make and support a successful application.

4.1 Certificate Application Requirements

All Certificate applicants must complete the enrolment process which includes:

- Generate a RSA key pair and demonstrate to Digi-Sign ownership of the private key half of the key pair through the submission of a valid PKCS#10 Certificate Signing Request (CSR)
- Make reasonable efforts to protect the integrity the private key half of the key pair
- Submit to Digi-Sign a certificate application, including application information as detailed in this CPS, a public key half of a key pair, and agree to the terms of the relevant subscriber agreement
- Provide proof of identity through the submission of official documentation as requested by Digi-Sign during the enrolment process

Certificate applications are submitted to either Digi-Sign or a Digi-Sign approved Digi-RA™. The following table details the entity(s) involved in the processing of certificate applications. Digi-Sign issue all certificates regardless of the processing entity.

Certificate Type	Enrolment Entity	Processing Entity	Issuing Authority
Digi-SSL™ – all types as per section 2.4.1 of this Digi-CPS™	End Entity Subscriber	Digi-Sign	Digi-Sign
Digi-SSL™ – all types as per section 2.4.1 of this Digi-CPS™	Digi-Partner™ on behalf of End Entity Subscriber	Digi-Partner™	Digi-Sign
Digi-Access™ – all types as per section 2.4.2 of this Digi-CPS™	End Entity Subscriber	On-Site™ or Digi-CA™ Account	Digi-Sign
Digi-Access™ – all types as per section 2.4.2 of this Digi-CPS™	Digi-Partner™ on behalf of End Entity Subscriber	Digi-Partner™	Digi-Sign
Digi-Mail™ – all types as per section 2.4.3 of this Digi-CPS™	End Entity Subscriber	On-Site™ or Digi-CA™ Account	Digi-Sign
Digi-Access™ – all types as per section 2.4.3 of this Digi-CPS™	Digi-Partner™ on behalf of End Entity Subscriber	Digi-Partner™	Digi-Sign

Digi-ID™ – all types as per section 2.4.4 of this Digi-CPS™	End Entity Subscriber	On-Site™ or Digi-CA™ Account Holder	Digi-Sign
Digi-Access™ – all types as per section 2.4.4 of this Digi-CPS™	Digi-Partner™ on behalf of End Entity Subscriber	Digi-Partner™	Digi-Sign

4.1.1 Reseller Partner Certificate Applications

Reseller Partners may act as RAs under the practices and policies stated within this Digi-CPS™. The Digi-RA™ may make the application on behalf of the applicant pursuant to the Digi-Partner™ program.

Under such circumstances the Digi-RA™ is responsible for all the functions on behalf of the applicant detailed in section 4.1 of this Digi-CPS™. Such responsibilities are detailed and maintained within the Reseller agreement and guidelines.

4.1.2 Account Holder Certificate Applications

Control Centre™ Account Holders act as Digi-RAs™ under the practices and policies stated within this Digi-CPS™. The Digi-RA™ makes the application for a Digi-SSL™ certificate to be used by a named server, or a Digi-Access™ certificate to be used by a named employee, partner or extranet user, or a Digi-Mail™ certificate to be used by a named employee, partner or extranet user under a domain name that Digi-Sign has validated either belongs to, or may legally be used by the Control Centre™ Account holding organisation.

4.1.3 Methods of application

Generally, applicants will complete the online forms made available by Digi-Sign or by approved Digi-RAs™ at the respective official websites. Under special circumstances the applicant may submit an application via email, however this process is available at the discretion of Digi-Sign or its Digi-RAs™.

Control Centre™ Account Holder applications are made through the Control Centre™ Adminster console – a web based console hosted and supported by Digi-Sign.

4.2 Application Validation

Prior to issuing a certificate Digi-Sign employs controls to validate the identity of the subscriber information featured in the certificate application. Such controls are indicative of the product type:

4.2.1 Digi-SSL™ Application Two Step Validation Process

Digi-Sign utilises a two step validation process prior to the issuance of a secure server certificate.

This process involves Digi-Sign, automatically or manually, reviewing the application information provided by the applicant (as per section 4.3 of this CPS) in order to assert that:

1. The applicant has the right to use the domain name used in the application

- Validated by reviewing domain name ownership records available publicly through Internic or approved global domain name registrars
- Validation may be supplemented through the use of the administrator contact associated with the domain name register record for communication with Digi-Sign validation staff or for automated email challenges
- Validation may be supplemented through the use of generic emails which ordinarily are only available to the person(s) controlling the domain name administration, for example webmaster@..., postmaster@..., admin@...

2. The applicant is an accountable legal entity, whether an organisation or an individual.

- Validated by requesting official company documentation, such as:

  Business License, Articles of Incorporate, Sales License or other relevant documents. For non-corporate applications, documentation such as bank statement, copy of passport, copy of driving license or other relevant documents.

The above assertions are reviewed through automated processes, manual review of supporting documentation and reference to third party official databases.

4.2.2 Digi-SSL™ Trial, Digi-SSL™ Xs & Digi-SSL™ Xp Type

Digi-SSL**™** Xp, Digi-SSL**™** Xs and Digi-SSL**™** Trial Certificates are processed manually by a Digi-Sign validation officer in accordance with the two-step process outlined in section 4.2.1 of this Digi-CPS**™**.

4.2.3 Digi-Access™, Digi-Mail™ & Digi-ID™: Free version

The free versions of Digi-Access™, Digi-Mail™ or Digi-ID™ is *persona non validate*d. Only the right for the applicant to use the submitted email address is validated by Digi-Sign. This is achieved through the delivery via email of unique login details to online certificate collection facilities hosted by Digi-Sign. The login details are sent via email to the address submitted during the free versions of Digi-Access™, Digi-Mail™ or Digi-ID™Certificate applications

Once logged into the online certificate collection facilities and prior to the installation of the free versions of Digi-Access™, Digi-Mail™ or Digi-ID™, Digi-Sign validate through the use of an automated cryptographic challenge that the applicant holds the private key associated with the public key submitted during the application

process. If the automated challenge is successful, Digi-Sign will release the digital certificate to the subscriber.

4.2.4 Digi-Access™, Digi-Mail™ & Digi-ID™: Corporate version

Corporate versions of Digi-Access™, Digi-Mail™ or Digi-ID™ Certificates are only available through the Control Centre™ issued to email addresses within approved domain names. The Control Centre™ Account Holder must first submit a domain name to Digi-Sign and appropriate domain name ownership, or right to use a domain name, validation takes place in accordance with 4.2.1 of this Digi-CPS™. Upon successful validation of a submitted domain name Digi-Sign allows the Control Centre™ Account Holder to utilise email addresses within the domain name.

Corporate versions of Digi-Access™, Digi-Mail™ or Digi-ID™ Certificates are applied for by the Control Centre™ nominated administrator. The administrator will submit the Digi-Access™, Digi-Mail™ & Digi-ID™ certificate end-entity information on behalf of the end-entity. An email is then delivered to the end-entity containing unique login details to online certificate generation and collection facilities managed by Digi-Sign.

Once logged into the online certificate generation and collection facilities, the end-entity's browser creates a public and private key pair. The public key is submitted to Digi-Sign who will issue a Corporate version of Digi-Access™, Digi-Mail™ or Digi-ID™ Certificate containing the public key. Validation occurs through the use of a automated cryptographic challenge that the applicant holds the private key associated with the public key submitted during this automated application process. If the automated challenge is successful, Digi-Sign will release the digital certificate to the end-entity subscriber.

4.3 Validation Information for Certificate Applications

Applications for Digi-Sign certificates are supported by appropriate documentation to establish the identity of an applicant.

From time to time, Digi-Sign may modify the requirements related to application information for individuals to respond to own Digi-Sign requirements, the business context of the usage of a digital certificate, or as it may be prescribed by law.

4.3.1 Supporting Documentation for Organisational Applicants

Documentation requirements for Organisational applicants shall include identification elements such as:

- Articles of Association
- Business License
- Articles of Association
- Certificate of Compliance
- Certificate of Incorporation
- Certificate of Authority to Transact Business
- Sales Tax Certificate
- Corporate Charter
- Official letter from office of Dean or Principal (for Educational Institutions)

- Official letter from an authorised representative of a government organisation

Digi-Sign may accept at its discretion other official organisational documentation supporting an application.

4.3.2 Application Information for Organisational Applicants

Critical information elements for a Digi-Sign certificate issued to an Organisation may include the following elements. Those elements marked with PUBLIC are present within an issued certificate and are therefore within the public domain. Those elements not marked with PUBLIC remain confidential in line with the privacy and protection of data provisions outlined in this Digi-CPS™.

- Legal Name of the Organisation (PUBLIC)
- Organisational unit (PUBLIC)
- Street, city, postal/zip code, country (PUBLIC)
- VAT-number (if applicable)
- Company / DUNS number (if available)
- Server Software Identification
- Payment Information
- Administrator contact full name, email address and telephone
- Billing contact persons and organisational representative
- Fully Qualified Domain Name / Network Server Name / Public or Private IP (PUBLIC)
- Public Key (PUBLIC)
- Proof of right to use name
- Proof of existence and organisational status of the Organisation as per section 4.3.1 of this Digi-CPS™
- Subscriber agreement, signed (if applying out of bands)

4.3.3 Supporting Documentation for Individual Applicants

Documentation requirements for Individual applicants shall include identification elements such as:

- Passport
- Driving License
- Bank statement
- Home Utility Invoice

Digi-Sign may accept at its discretion other official documentation supporting an application.

4.3.4 Application Information for Individual Applicants

Critical information elements for a Digi-Sign certificate issued to a legal person may include the following elements.

- Legal Name of the Individual (PUBLIC)
- Organisational unit (PUBLIC)

- Street, city, postal/zip code, country (PUBLIC)
- VAT-number (if applicable)
- Server Software Identification
- Payment Information
- Administrator contact full name, email address and telephone
- Billing contact persons and organisational representative
- Fully Qualified Domain Name / Network Server Name / Public or Private IP (PUBLIC)
- Public Key (PUBLIC)
- Proof of right to use name
- Proof of existence and organisational status of the Organisation as per section 4.3.1 of this Digi-CPS™
- Subscriber agreement, signed (if applying out of bands)

4.4 Validation Requirements for Certificate Applications

Upon receipt of an application for a digital certificate and based on the submitted information,
Digi-Sign confirms the following information:

- The certificate applicant is the same person as the person identified in the certificate request.
- The certificate applicant holds the private key corresponding to the public key to be included in the certificate.
- The information to be published in the certificate is accurate, except for non-verified subscriber information.
- Any agents who apply for a certificate listing the certificate applicant's public key are duly authorised to do so.

In all types of Digi-Sign certificates the subscriber has a continuous obligation to monitor the accuracy of the submitted information and notify Digi-Sign of any changes that would affect the validity of the certificate.

4.4.1 Third-Party Confirmation of Business Entity Information

Digi-Sign may use the services of a third party to confirm information on a business entity that applies for a digital certificate. Digi-Sign accepts confirmation from third party organisations, other third party databases and government entities.

Digi-Sign controls include Trade Registry transcripts that confirm the registration of the applicant company and state the members of the board, the management and Directors representing the company.

Digi-Sign may use any means of communication at its disposal to ascertain the identity of an organisational or individual applicant.

4.4.2 Serial Number Assignment

Digi-Sign assigns certificate serial numbers that appear in a Digi-Sign certificates. Assigned serial numbers are unique.

4.5 Time to Confirm Submitted Data

Digi-Sign makes reasonable efforts to confirm certificate application information and issue a digital certificate within reasonable time frames.

Digi-Sign assures that all certificates will be issued within 2 working days after the receipt of all required validation information as per this Digi-CPS™.

4.6 Approval and Rejection of Certificate Applications

Following successful completion of all required validations of a certificate application Digi-Sign approves an application for a digital certificate.

If the validation of a certificate application fails, Digi-Sign rejects the certificate application. Upon such rejection Digi-Sign promptly notifies the applicant by any means of communication it sees appropriate and provides a reason for such failure to the extent permitted by law.

Digi-Sign reserves its right to reject applications to issue a certificate to applicants if on its own assessment, by issuing a certificate to such parties the good and trusted name of Digi-Sign might get tarnished, diminished or have its value reduced and under such circumstances may do so without incurring any liability or responsibility for any loss or expenses arising as a result of such refusal.

Applicants whose applications have been rejected may subsequently re-apply.

4.7 Certificate Issuance and Subscriber Consent

Digi-Sign issues a certificate upon approval of a certificate application. A digital certificate is deemed to be valid at the moment a subscriber accepts it. Issuing a digital certificate means that Digi-Sign accepts a certificate application.

4.8 Certificate Validity

Certificates are valid upon issuance by Digi-Sign and acceptance by the subscriber. Generally the certificate validity period with be 1, 2 or 3 years, however Digi-Sign reserves the right to offer validity periods outside of this standard validity period.

4.9 Certificate Acceptance by Subscribers

An issued certificate is either delivered via email or installed on a subscriber's computer / hardware security module through an online collection method. A subscriber is deemed to have accepted a certificate when:

- The subscriber uses the certificate
- 30 days pass from the date of the issuance of a certificate

4.10 Verification of Digital Signatures

Verification of a digital signature is used to determine that:

- The digital signature was created by the private key corresponding to the public key listed in the signer's certificate.
- The signed data associated with this digital signature has not been altered since the digital signature was created.

4.11 Reliance on Digital Signatures

The final decision concerning whether or not to rely on a verified digital signature is exclusively that of the relying party. Reliance on a digital signature should only occur if:

- The digital signature was created during the operational period of a valid certificate and it can be verified by referencing a validated certificate
- The relying party has checked the revocation status of the certificate by referring to the relevant Certificate Revocation Lists
- The relying party understands that a digital certificate is issued to an subscriber for a specific purpose and that the private key associated with the digital certificate may only be used in accordance with the usages suggested in the CPS and named as Object Identifiers in the certificate profile

Reliance is accepted as reasonable under the provisions made for the relying party under this Digi-CPS™ and within the relying party agreement. If the circumstances of reliance exceed the assurances delivered by Digi-Sign under the provisions made in this Digi-CPS™, the relying party must obtain additional assurances.

4.12 Certificate Suspension

Digi-Sign does not utilise certificate suspension.

4.13 Certificate Revocation

Revocation of a certificate is to permanently end the operational period of the certificate prior to reaching the end of its stated validity period. Digi-Sign will revoke a digital certificate if:

- There has been loss, theft, modification, unauthorised disclosure, or other compromise of the private key associated with the certificate
- The Subscriber or Digi-Sign has breached a material obligation under this Digi-CPS™
- Either the Subscriber's or Digi-Sign's obligations under this Digi-CPS™ is delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result another person's information is materially threatened or compromised

- There has been a modification of the information pertaining to the Subscriber that is contained within the certificate

4.13.1 Request for Revocation

The subscriber or other appropriately authorised parties can request suspension or revocation of a certificate. Prior to the revocation of a certificate Digi-Sign will verify that the revocation request has been:

- Made by the organisation or individual entity that has made the certificate application.

- Made by the RA on behalf of the organisation or individual entity that used the RA to make the certificate application Digi-Sign employ the following procedure for authenticating a revocation request:

    - The revocation request must be received by the Administrator contact associated with the certificate application. Digi-Sign may if necessary also request that the revocation request be made by either / or the organisational contact and billing contact.
    - Upon receipt of the revocation request Digi-Sign will request confirmation from the known administrator out of bands contact details, either by telephone or fax.
    - Digi-Sign validation personnel will then command the revocation of the certificate and logging of the identity of validation personnel and reason for revocation will be maintained in accordance with the logging procedures covered in this Digi-CPS™.

4.13.2 Effect of Revocation

Upon revocation of a certificate, the operational period of that certificate is immediately considered terminated. The serial number of the revoked certificate will be placed within the CRL. An updated CRL is published on the Digi-Sign website every 24 hours, however under special circumstances the CRL may be published more frequently.

4.14 Renewal

Depending on the option selected during application, the validity period of Digi-Sign certificates is one year (365 days), two years (730 days) or three years (1095 days) from the date of issuance and is detailed in the relevant field within the certificate.

Renewal fees are detailed on the official Digi-Sign websites and within communications sent to subscriber's approaching the certificate expiration date.

Renewal application requirements and procedures are the same as those employed for the application validation and issuance requirements detailed for new customers.

4.15 Notice Prior to Expiration

Digi-Sign shall make reasonable efforts to notify subscribers via e-mail, of the imminent expiration of a digital certificate. Notice shall ordinarily be provided within a 60 day period prior to the expiry of the certificate.

5 Legal Conditions of Issuance

This part describes the legal representations, warranties and limitations associated with Digi-Sign digital certificates.

5.1 Digi-Sign Representations

Digi-Sign makes to all subscribers and relying parties certain representations regarding its public service, as described below. Digi-Sign reserves its right to modify such representations as it sees fit or required by law.

5.2 Information Incorporated by Reference into a Digital Certificate

Digi-Sign incorporates by reference the following information in every digital certificate it issues:

- Terms and conditions of the digital certificate.
- Any other applicable certificate policy as may be stated on an issued Digi-Sign certificate, including the location of this Digi-CPS™.
- The mandatory elements of the standard X.509v3.
- Any non-mandatory but customised elements of the standard X.509v3.
- Content of extensions and enhanced naming that are not fully expressed within a certificate.
- Any other information that is indicated to be so in a field of a certificate.

5.3 Displaying Liability Limitations, and Warranty Disclaimers

Digi-Sign certificates may include a brief statement describing limitations of liability, limitations in the value of transactions to be accomplished, validation period, intended purpose of the certificate and disclaimers of warranty that may apply. Such information may alternatively be displayed through a hypertext link. To communicate information Digi-Sign may use:

- An organisational unit attribute.
- A Digi-Sign standard resource qualifier to a certificate policy.
- Proprietary or other vendors' registered extensions.

5.4 Publication of Certificate Revocation Data

Digi-Sign reserves its right and the subscriber agrees to publish a CRL (Certificate Revocation List) as it may be indicated.

5.5 Duty to Monitor the Accuracy of Submitted Information

In all cases and for all types of Digi-Sign certificates the subscriber has a continuous obligation to monitor the accuracy of the submitted information and notify Digi-Sign of any such changes.

5.6 Publication of Information

Published critical information may be updated from time to time as prescribed in this Digi-CPS™. Such updates shall be indicated through appropriate version numbering and publication date on any new version.

5.7 Interference with Digi-Sign Implementation

Subscribers, relying parties and any other parties shall refrain from interfering with, or reverse engineering the technical implementation of Digi-Sign PKI services including the key generation process, the public web site and the Digi-Sign repositories except as explicitly permitted by this Digi-CPS™ or upon prior written approval of Digi-Sign.

5.8 Standards

Digi-Sign assumes that user software that is claimed to be compliant with X.509v3 and other applicable standard enforces the requirements set out in this Digi-CPS™. Digi-Sign cannot warrant that such user software will support and enforce controls required by Digi-Sign while the user should seek appropriate advice.

5.9 Digi-Sign Partnerships Limitations

Partners of the Digi-Sign network shall refrain from undertaking any actions that might imperil, put in doubt or reduce the trust associated with the Digi-Sign products and services. Digi-Sign partners shall specifically refrain from seeking partnerships with other root authorities or apply procedures originating from such authorities.

5.10 Digi-Sign Limitation of Liability for a Digi-Sign Partner

As the Digi-Sign network includes Digi-RAs™ that operate under Digi-Sign practices and procedures Digi-Sign warrants the integrity of any certificate issued under its own root within the limits of the Digi-Sign insurance policy.

5.11 Choice of Cryptographic Methods

Parties acknowledge that they are solely responsible for and have exercised independent judgment and employed adequate training in choosing security software, hardware, and encryption/digital signature algorithms, including their respective parameters, procedures, and techniques as well as PKI as a solution to their security requirements.

5.12 Reliance on Unverified Digital Signatures

Parties relying on a digital certificate must verify a digital signature at all times by checking the validity of a digital certificate against the relevant CRL published by Digi-Sign. Relying parties are alerted that an unverified digital signature cannot be assigned as a valid signature of the subscriber.

Relying on an unverifiable digital signature may result to risks that the relying party and not Digi-Sign assume in whole.

By means of this CPS Digi-Sign has adequately informed relying parties on the usage and validation of digital signatures through this CPS and other documentation published in its public repository available at:

www.digi-sign.com/repository/

Or by contacting via out of bands means the contact address as specified in this Digi-CPS™.

5.13 Rejected Certificate Applications

The private key associated with a public key, which has been submitted as part of a rejected certificate applications may not under any circumstances be used to create a digital signature if the effect of the signature is to create conditions of reliance upon the rejected certificate.

5.14 Refusal to Issue a Certificate

Digi-Sign reserves its right to refuse to issue a certificate to any party as it sees fit, without incurring any liability or responsibility for any loss or expenses arising out of such refusal.

5.15 Subscriber Obligations

Unless otherwise stated in this Digi-CPS™, subscribers shall exclusively be responsible:

- To minimise internal risk of private key compromise by ensuring adequate knowledge and training on PKI is provided internally.
- To generate their own private / public key pair to be used in association with the certificate request submitted to Digi-Sign or a Digi-Sign RA.
- Ensure that the public key submitted to Digi-Sign or a Digi-RA™ corresponds with the private key used.
- Ensure that the public key submitted to Digi-Sign or a Digi-RA™ is the correct one.
- Provide correct and accurate information in its communications with Digi-Sign or a Digi-RA™.
- Alert Digi-Sign or a Digi-RA™ if at any stage whilst the certificate is valid, any information originally submitted has changed since it had been submitted to Digi-Sign.
- Generate a new, secure key pair to be used in association with a certificate that it requests from Digi-Sign or a Digi-RA™.
- Read, understand and agree with all terms and conditions in this Digi-CPS™ and associated policies published in the Digi-Sign Repository at www.digi-sign.com/repository/index.php.
- Refrain from tampering with a Digi-Sign certificate.

- Use Digi-Sign certificates for legal and authorised purposes in accordance with this suggested usages and practices Digi-CPS™.
- Cease using a Digi-Sign certificate if any information in it becomes misleading obsolete or invalid.
- Cease using a Digi-Sign certificate if such certificate is expired and remove it from any applications and/or devices it has been installed on.
- Refrain from using the subscriber's private key corresponding to the public key in a Digi-Sign issued certificate to issue end-entity digital certificate or subordinate CAs.
- Make reasonable efforts to prevent the compromise, loss, disclosure, modification, or otherwise unauthorised use of the private key corresponding to the public key published in a Digi-Sign certificate.
- Request the revocation of a certificate in case of an occurrence that materially affects the integrity of a Digi-Sign certificate.
- For acts and omissions of partners and agents they use to generate, retain, escrow, or destroy their private keys.

5.16 Representations by Subscriber upon Acceptance

Upon accepting a certificate the subscriber represents to Digi-Sign and to relying parties that at the time of acceptance and until further notice:

- Digital signatures created using the private key corresponding to the public key included in the certificate is the digital signature of the subscriber and the certificate has been accepted and is properly operational at the time the digital signature is created.

- No unauthorised person has ever had access to the subscriber's private key.

- All representations made by the subscriber to Digi-Sign regarding the information contained in the certificate are accurate and true.

- All information contained in the certificate is accurate and true to the best of the subscriber's knowledge or to the extent that the subscriber had notice of such information while the subscriber shall act promptly to notify Digi-Sign of any material inaccuracies in such information.

- The certificate is used exclusively for authorised and legal purposes, consistent with this Digi-CPS™.

- Use a Digi-Sign certificate only in conjunction with the entity named in the organisation field of a digital certificate (if applicable).

- The subscriber retains control of her private key, use a trustworthy system, and take reasonable precautions to prevent its loss, disclosure, modification, or unauthorised use.

- The subscriber is an end-user subscriber and not an CA, and will not use the private key corresponding to any public key listed in the certificate for purposes of signing any certificate (or any other format of certified public key) or CRL, as an CA or otherwise, unless expressly agreed in writing between subscriber and Digi-Sign.

- The subscriber agrees with the terms and conditions of this Digi-CPS™ and other agreements and policy statements of Digi-Sign.

- The subscriber abides by the laws applicable in his/her country or territory including those related to intellectual property protection, viruses, accessing computer systems etc.

- The subscriber complies with all export laws and regulations for dual usage goods as may be applicable.

5.17 Indemnity by Subscriber

By accepting a certificate, the subscriber agrees to indemnify and hold Digi-Sign, as well as its agent(s) and contractors harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind, including reasonable attorneys' fees, that Digi-Sign, and the above mentioned parties may incur, that are caused by the use or publication of a certificate, and that arises from:

- Any false or misrepresented data supplied by the subscriber or agent(s).

- Any failure of the subscriber to disclose a material fact, if the misrepresentation or omission was made negligently or with intent to deceive the CA, Digi-Sign, or any person receiving or relying on the certificate.

- Failure to protect the subscriber's private key, or failure to take reasonable precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorised use of the subscriber's private key.

- Breaking any laws applicable in their country or territory including those related to intellectual property protection, viruses, accessing computer systems etc.

5.18 Obligations of Digi-Sign Registration Authorities

A Digi-RA™ operates under the policies and practices detailed in this Digi-CPS™ and also the associated Digi-Partner™ agreement and/or Control Centre™ Account agreement. The Digi-RA™ is bound under contract to:

- Receive applications for Digi-Sign certificates in accordance with this Digi-CPS™.

- Perform all verification actions prescribed by the Digi-Sign validation procedures and this Digi-CPS™.
- Receive, verify and relay to Digi-Sign all requests for revocation of a Digi-Sign certificate in accordance with the Digi-Sign revocation procedures and this Digi-CPS™.
- Act according to the Law and regulations.

5.19 Obligations of a Relying Party

A party relying on a Digi-Sign certificate accepts that in order to reasonable rely on a Digi-Sign certificate they must:

- To minimise the risk of relying on an digital signature created by an invalid, revoked, expired or rejected certificate, the relying party must have reasonably made the effort to acquire sufficient knowledge on using digital certificates and PKI.
- Study the limitations to the usage of digital certificates and be aware through the Relying Party agreement the maximum value of the transactions that can be made using a Digi-Sign digital certificate.
- Read and agree with the terms of the Digi-CPS™ and relying party agreement.
- Verify a Digi-Sign certificate by referring to the relevant CRL and also the CRLs of intermediate CA and root CA as available in the Digi-Sign repository.
- Trust a Digi-Sign certificate only if it is valid and has not been revoked or has expired.
- Rely on a Digi-Sign certificate, only as it may be reasonable under the circumstances listed in this section and other relevant sections of this Digi-CPS™.

5.20 Legality of Information

Subscribers shall solely be responsible for the legality of the information they present for use in certificates issued under this Digi-CPS™, in any jurisdiction in which such content may be used or viewed.

5.21 Subscriber Liability to Relying Parties

Without limiting other subscriber obligations stated in this Digi-CPS™, subscribers are liable for any misrepresentations they make in certificates to third parties that reasonably rely on the representations contained therein and have verified one or more digital signatures with the certificate.

5.22 Duty to Monitor Agents

The subscriber shall control the data that an agent supplies to Digi-Sign. The subscriber must promptly notify the issuer of any misrepresentations and omissions made by an agent. The duty of this article is continuous.

5.23 Use of Agents

For certificates issued at the request of a subscriber's agent, both the agent and the subscriber shall jointly and severally indemnify Digi-Sign, and its agents and contractors.

5.24 Conditions of usage of the Digi-Sign Repository and Web site

Parties (including subscribers and relying parties) accessing the Digi-Sign Repository (www.digi-sign.com/repository/) and official web site(s) agree with the provisions of this CPS and any other conditions of usage that Digi-Sign may make available.

Parties demonstrate acceptance of the conditions of usage of the Digi-CPS™ by using a Digi-Sign issued certificate.

5.25 Accuracy of Information

Digi-Sign recognising its trusted position makes every effort to ensure that parties accessing its Repositories receive accurate, updated and correct information. Digi-Sign, however, cannot accept any liability beyond the limits set in this Digi-CPS™and the Digi-Sign insurance policy.

5.26 Failure to Comply

Failure to comply with the conditions of usage of the Digi-Sign Repositories and web site may result in terminating the relationship between Digi-Sign and the party.

5.27 Obligations of Digi-Sign

To the extent specified in the relevant sections of the Digi-CPS™, Digi-Sign promises to:

- Comply with this Digi-CPS™ and its internal or published policies and procedures.
- Comply with applicable laws and regulations.
- Provide infrastructure and certification services, including the establishment and operation of the Digi-Sign Repository and web site for the operation of PKI services.
- Provide Trust mechanisms, including a key generation mechanism, key protection, and secret sharing procedures regarding its own infrastructure.

- Provide prompt notice in case of compromise of its private key(s).
- Provide and validate application procedures for the various types of certificates that it may make publicly available.
- Issue digital certificates in accordance with this Digi-CPS™ and fulfills its obligations presented herein.
- Upon receipt of a request from an RA operating within the Digi-Sign network act promptly to issue a Digi-Sign certificate in accordance with this Digi-CPS™.
- Upon receipt of a request for revocation from an RA operating within the Digi-Sign network act promptly to revoke a Digi-Sign certificate in accordance with this Digi-CPS™.
- Publish accepted certificates in accordance with this Digi-CPS™.
- Provide support to subscribers and relying parties as described in this Digi-CPS™.
- Revoke certificates according to this Digi-CPS™.
- Provide for the expiration and renewal of certificates according to this Digi-CPS™.
- Make available a copy of this Digi-CPS™ and applicable policies to requesting parties.
- Warrant the accuracy of information published on a Qualified Certificate issued pursuant to the requirements of the European Directive 1999/93/EC.
- Warrant that the signatory held the private key at the time of issuance of a certificate issued pursuant to the requirements for Qualified Certificates as in the European Directive 1999/93/EC.

Digi-Sign acknowledges that it has no further obligations under this Digi-CPS™.

5.28 Fitness for a Particular Purpose

Digi-Sign disclaims all warranties and obligations of any type, including any warranty of fitness for a particular purpose, and any warranty of the accuracy of unverified information provided.

5.29 Other Warranties

Except as it may have otherwise been stated in relation to Qualified Certificates issued pursuant to the requirements of the European Directive 1999/93/EC Digi-Sign does not warrant:

- The accuracy, authenticity, completeness or fitness of any unverified information contained in certificates or otherwise compiled, published, or disseminated by or on behalf of Digi-Sign except as it may be stated in the relevant product description below in this Digi-CPS™ and in the Digi-Sign insurance policy.

- The accuracy, authenticity, completeness or fitness of any information contained in Digi-Sign Personal certificates class 1, free, test or demo certificates.

- And shall not incur liability for representations of information contained in a certificate except as it may be stated in the relevant product description below in this Digi-CPS™.

- Does not warrant the quality, functions or performance of any software or hardware device.

- Although Digi-Sign is responsible for the revocation of a certificate it cannot be held liable if it cannot execute it for reasons outside its own control.

- The validity, completeness or availability of directories of certificates issued by a third party (including an agent) unless that is specifically stated by Digi-Sign.

5.30 Non Verified Subscriber Information

Notwithstanding limitation warranties under the product section of this Digi-CPS™, Digi-Sign shall not be responsible for non-verified subscriber information submitted to Digi-Sign, or the Digi-Sign directory or otherwise submitted with the intention to be included in a certificate, except as it may have otherwise been stated in relation to Qualified Certificates issued pursuant to the requirements of the European Directive 1999/93/EC.

5.31 Exclusion of Certain Elements of Damages

In no event (except for fraud or wilful misconduct) shall Digi-Sign be liable for:

- Any indirect, incidental or consequential damages.
- Any loss of profits.
- Any loss of data.
- Any other indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, performance or non performance of certificates or digital signatures.
- Any other transactions or services offered within the framework of this Digi-CPS™.
- Any other damages except for those due to reliance, on the information featured on a certificate, on the verified information in a certificate.

- Any liability incurred in this case or any other case if the fault in this verified information is due to fraud or wilful misconduct of the applicant. Any liability that arises from the usage of a certificate that has not been issued or used in conformance with this Digi-CPS™.
- Any liability that arises from the usage of a certificate that is not valid.
- Any liability that arises from usage of a certificate that exceeds the limitations in usage and value and transactions stated upon it or on the Digi-CPS™.
- Any liability that arises from security, usability, integrity of products, including hardware and software a subscriber uses.
- Any liability that arises from compromise of a subscriber's private key.

5.32 Certificate Insurance Plan

Except to the extent of wilful misconduct, the cumulative maximum liability accepted by Digi-Sign for the issuance of a certificate containing invalid information pertaining to the certificate subscriber that has been validated using the methods appropriate for the certificate class and/or type is laid out below.

5.32.1 Digi-SSL™ Xs Certificates

The cumulative liability of Digi-Sign to applicants, subscribers and relying parties shall not exceed €1.00 (two thousand five hundred Euro).

5.32.2 Digi-SSL™ Premium Certificates

The cumulative liability of Digi-Sign to applicants, subscribers and relying parties shall not exceed €10,000.00 (ten thousand Euro).

5.32.3 Digi-SSL™ Trial Certificate

There is no liability of Digi-Sign to applicants, subscribers and relying parties.

5.33 Financial Limitations on Certificate Usage

Digi-Sign certificates may only be used in connection with transactions having a Euro (€) value no greater than the level of warranty associated with the certificate and detailed in section 5.32 of this Digi-CPS™.

5.34 Damage and Loss Limitations

In no event (except for fraud or wilful misconduct) will the aggregate liability of Digi-Sign to all parties including without any limitation a subscriber, an applicant, a recipient, or a relying party for all digital signatures and transactions related to such certificate exceeds the applicable liability cap for such certificate as stated in the Digi-Sign insurance plan detailed section 5.32 of this Digi-CPS™.

5.35 Conflict of Rules

When this Digi-CPS™conflicts with other rules, guidelines, or contracts, this Digi-CPS™ shall prevail and bind the subscriber and other parties except as to other contracts either:

- Predating the first public release of the present version of this Digi-CPS™.
- Expressly superseding this Digi-CPS™ for which such contract shall govern as to the parties thereto, and to the extent permitted by law.

5.36 Intellectual Property Rights

Digi-Sign or its partners or associates own all intellectual property rights associated with its databases, web sites, Digi-Sign digital certificates and any other publication originating from Digi-Sign including this Digi-CPS™.

5.37 Infringement and Other Damaging Material

Digi-Sign subscribers represent and warrant that when submitting to Digi-Sign and use a domain and distinguished name (and all other certificate application information) they do not interfere with or infringe any rights of any third parties in any jurisdiction with respect to their trademarks, service marks, trade names, company names, or any other intellectual property right, and that they are not seeking to use the domain and distinguished names for any unlawful purpose, including, without limitation, tortuous interference with contract or prospective business advantage, unfair competition, injuring the reputation of another, and confusing or misleading a person, whether natural or incorporated. Certificate subscribers shall defend, indemnify, and hold Digi-Sign harmless for any loss or damage resulting from any such interference or infringement.

5.38 Ownership

Certificates are property of Digi-Sign. Digi-Sign gives permission to reproduce and distribute certificates on a nonexclusive, royalty-free basis, provided that they are reproduced and distributed in full.

Private and public keys are property of the subscribers who rightfully issue and hold them.

Secret shares of the Digi-Sign private key remain property of Digi-Sign.

5.39 Governing Law

This Digi-CPS™ is governed by, and construed in accordance with Irish law. This choice of law is made to ensure uniform interpretation of this Digi-CPS™, regardless of the place of residence or place of use of Digi-Sign digital certificates or other products and services. Irish law applies in all Digi-Sign commercial or contractual relationships in which this Digi-CPS™ may apply or quoted implicitly or explicitly in relation to Digi-Sign products and services where Digi-Sign acts as a provider, supplier, beneficiary receiver or otherwise.

5.40 Jurisdiction

Each party, including Digi-Sign partners, subscribers and relying parties, irrevocably agrees that the District Court of Dublin, Ireland has exclusive jurisdiction to hear and decide any suit, action or proceedings, and to settle any disputes, which may arise out of or in connection with this Digi-CPS™ or the provision of Digi-Sign PKI services.

5.41 Dispute Resolution

Before resorting to any dispute resolution mechanism including adjudication or any type of Alternative Dispute Resolution (including without exception mini-trial, arbitration, binding expert's advice, co-operation monitoring and normal expert's advice) parties agree to notify Digi-Sign of the dispute with a view to seek dispute resolution.

5.42 Successors and Assigns

This Digi-CPS™ shall be binding upon the successors, executors, heirs, representatives, administrators, and assigns, whether express, implied, or apparent, of the parties. The rights and obligations detailed in this Digi-CPS™ are assignable by the parties, by operation of law (including as a result of merger or a transfer of a controlling interest in voting securities) or otherwise, provided such assignment is undertaken consistent with this Digi-CPS™ articles on termination or cessation of operations, and provided that such assignment does not effect a novation of any other debts or obligations the assigning party owes to other parties at the time of such assignment.

5.43 Severability

If any provision of this CPS, or the application thereof, is for any reason and to any extent found to be invalid or unenforceable, the remainder of this Digi-CPS™ (and the application of the invalid or unenforceable provision to other persons or circumstances) shall be interpreted in such manner as to effect the original intention of the parties.

Each and every provision of this Digi-CPS™ that provides for a limitation of liability, disclaimer of or limitation upon any warranties or other obligations, or exclusion of damages is intended to be severable and independent of any other provision and is to be enforced as such.

5.44 Interpretation

This Digi-CPS™ shall be interpreted consistently within the boundaries of business customs, commercial reasonableness under the circumstances and intended usage of a product or service. In interpreting this Digi-CPS™ parties shall also take into account the international scope and application of the services and products of Digi-Sign and its international network of Registration as well as the principle of good faith as it is applied in commercial transactions. The headings, subheadings, and other captions in this Digi-CPS™ are intended for convenience and reference only

and shall not be used in interpreting, construing, or enforcing any of the provisions of this Digi-CPS™. Appendices and definitions to this Digi-CPS™, are for all purposes an integral and binding part of the Digi-CPS™.

5.45 No Waiver

This Digi-CPS™ shall be enforced, as a whole while failure by any person to enforce any provision of this Digi-CPS™ shall not be deemed a waiver of future enforcement of that or any other provision.

5.46 Notice

Digi-Sign accepts notices related to this Digi-CPS™ by means of digitally signed messages or in paper form. Upon receipt of a valid, digitally signed acknowledgment of receipt from Digi-Sign the sender of the notice shall deem her communication effective. The sender must receive such acknowledgment within five (5) days, or else written notice must then be sent in paper form through a courier service that confirms delivery or via certified or registered mail, postage prepaid, return receipt requested, addressed as follows:

Digi-Sign Limited
Enterprise Centre
Taylor's Lane
Dublin 8
Ireland

Attention: Legal Practices
Email: legal@digi-sign.com

This Digi-CPS™, related agreements and Certificate policies referenced within this document are available online at www.digi-sign.com/repository/.

5.47 Fees

Digi-Sign charges Subscriber fees for some of the certificate services it offers, including issuance, renewal and reissues (in accordance with the Digi-Sign Reissue Policy stated in 5.48 of this Digi-CPS™). Such fees are detailed on the official Digi-Sign websites (www.Digi-Sign.com).

Digi-Sign does not charge fees for the revocation of a certificate or for a Relying Party to check the validity status of a Digi-Sign issued certificate through the use of Certificate Revocation Lists.

Digi-Sign retains its right to affect changes to such fees. Digi-Sign partners, including Digi-Partners™ and Control Centre™ Account Holders, will be suitably advised to price amendments as detailed in the relevant partner agreements.

5.48 Reissue Policy

Digi-Sign does not offers a 7-day reissue policy. During a 7-day period (beginning when a certificate is first issued) the Subscriber may request a reissue of their certificate and incur no further fees for the reissue. If details other than just the public key require amendment, Digi-Sign reserves the right to revalidate the application in accordance with the validation processes detailed within this Digi-CPS™. If the reissue request does pass the validation process, Digi-Sign reserves the right to refuse the reissue application. Under such circumstances, the original certificate may be revoked and a refund provided to the applicant.

Digi-Sign is not obliged to reissue a certificate after the 7-day reissue policy period has expired.

5.49 Refund Policy

Digi-Sign offers a 7-day refund policy. During a 7-day period (beginning when a certificate is first issued) the Subscriber may request a full refund for their certificate. Under such circumstances, the original certificate may be revoked and a refund provided to the applicant. Digi-Sign is not obliged to refund a certificate after the 7-day reissue policy period has expired.

5.50 Survival

The obligations and restrictions contained under sections entitled: Audit, Confidential Information, Obligations of Digi-Sign, and Limitations upon such Obligations, Indemnity by the Subscriber and Miscellaneous Provisions survive the termination of this Digi-CPS™.

6 General Issuance Procedure

6.1 General

Digi-Sign offers different certificate types to make use of SSL, Two Factor Authentication and S/MIME technology for secure online transactions, secure authentication and secure email respectively. Prior to the issuance of a certificate Digi-Sign will validate an application in accordance with this Digi-CPS™, which may involve the request by Digi-Sign to the applicant for relevant official documentation supporting the application.

Digi-Sign certificates are issued to organisations or individuals.

The validity period of Digi-Sign certificates varies dependent on the certificate type, but typically a certificate will be valid for either 1 year, 2 years or 3 years. Digi-Sign reserves the right to, at its discretion, issues certificates that may fall outside of these set periods.

6.2 Certificates issued to Individuals and Organisations

A certificate request can be done according to the following means:

On-line: Via the Web (https). The certificate applicant submits an application via a secure on-line link according to a procedure provided by Digi-Sign. Additional documentation in support of the application may be required so that Digi-Sign verifies the identity of the applicant. The applicant submits to Digi-Sign such additional documentation. Upon verification of identity, Digi-Sign issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate to its device. The applicant must notify Digi-Sign of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of informational content to be included in the certificate.

Digi-Sign may at its discretion accept applications via email.

6.3 Content

Typical content of information published on a Digi-Sign certificate may include but is not limited to the following elements of information:

6.3.1 Digi-SSL™ Secure Server Certificates

- Applicant's fully qualified domain name.
- Applicant's organisational name.
- Code of applicant's country.
- Organisational unit name, street address, city, state.
- Issuing certification authority (Digi-Sign).
- Applicant's public key.
- Digi-Sign digital signature.
- Type of algorithm.
- Validity period of the digital certificate.

- Serial number of the digital certificate.

6.3.2 Digi-Access™, Digi-Mail™ & Digi-ID™ Certificates

- Applicant's e-mail address.
- Applicant's name.
- Code of applicant's country.
- Organisation name, organisational unit name, street address, city, state.
- Applicant's public key.
- Issuing certification authority (Digi-Sign).
- Digi-Sign digital signature.
- Type of algorithm.
- Validity period of the digital certificate.
- Serial number of the digital certificate.

6.4 Time to Confirm Submitted Data

Digi-Sign makes reasonable efforts to confirm certificate application information and issue a digital certificate within reasonable time frame. The time frame is greatly dependent on the Subscriber providing the necessary details and / or documentation in a timely manner. Upon the receipt of the necessary details and / or documentation, Digi-Sign aim to confirm submitted application data and to complete the validation process and issue / reject a certificate application within 2 working days.

From time to time, events outside of the control of Digi-Sign may delay the issuance process however Digi-Sign will make every reasonable effort to meet issuance times and to make applicants aware of any factors that may affect issuance times in a timely manner.

6.5 Issuing Procedure

The following steps describe the milestones to issue a Secure Server Certificate:

a) The applicant fills out the online request on Digi-Sign's web site and the applicant submits the required information: Certificate Signing Request [CSR], e-mail address, common name, organisational information, country code, verification method and billing information.
b) The applicant accepts the on line subscriber agreement.
c) The applicant submits the required information to Digi-Sign.
d) The applicant pays the certificate fees.
e) Digi-Sign verifies the submitted information using third party databases and Government records
f) Upon successful validation of the application information, Digi-Sign may issue the certificate to the applicant or should the application be rejected, Digi-Sign will alert the applicant that the application has been unsuccessful.
g) Renewal is conducted as per the procedures outlined in this Digi-CPS™ and the official Digi-Sign websites.
h) Revocation is conducted as per the procedures outlined in this Digi-CPS™.

7 Document Control and References

This document

Digi-Sign Limited
Enterprise Centre
Taylor's Lane
Dublin 8
Ireland

Tel: +353 (1) 662-1249
Fax: +353 (1) 662-1652
Web: www.Digi-Sign.com