SGSITES®
TECHNOLOGIES

SGSITES® Trust Center

Certification Practice Statement

SGSITES Trust Center

Certification Practice Statement

Version: 1.1
Effective date: 01.08.2015

Table of Contents

1. Introduction

This Certification Practice Statement (CPS) of the SGSITES Technologies Certification Authority (hereinafter SGSITES Trust Center) applies to the services of the SGSITES Trust Center that are associated with the issuance of and management of digital certificates. This CPS can be found on the SGSITES Trust Center repository at: http://pki.sgsites.net/repository/. This CPS may be updated from time to time.

This CPS addresses the technical, procedural personnel policies and practices of the CA in all services and during the complete life cycle of certificates as issued by the SGSITES Trust Center. The SGSITES Trust Center is operated and owned by Stefan Genchev. The services of the SGSITES Trust Center are provided free of charge to the general public. The identity verification process may include administrative fees.

Inquiries on this SGSITES Trust Center CPS can be addressed to:

Stefan Genchev
Attn: SGSITES Trust Center
13 Ivac voivoda str.
1124 Sofia
Bulgaria

pki@sgsites.net
pki.sgsites.net

This CPS is final and binding between Stefan Genchev (operating and owning the SGSITES Trust Center) and the subscriber and/or relying parties, who use rely or attempt to rely upon certification services made available by the SGSITES Trust Center.

For subscribers this CPS becomes effective and binding by accepting a subscriber agreement. For relying parties this CPS becomes binding by merely addressing a certificate related request on a SGSITES Technologies certificate to a SGSITES Technologies directory. The subscriber agreement

forfeits the consent of the relying party with regard to accepting the conditions laid out in this CPS.

SGSITES, the SGSITES logo, SGSITES Trust Center, My ePass, and other trademarks, service marks, and designs are registered or unregistered trademarks in Bulgaria or in other countries.

1.1 Overview

This CPS applies to the specific domain of the SGSITES Trust Center. The purpose of this CPS is to present the SGSITES Technologies practices and procedures in managing certificates and to demonstrate compliance with requirements pertaining to the issuance of digital certificates according to SGSITES Technologies's own and industry requirements pursuant to the standards set out above. The certificate type addressed in this CPS is the following:

- Server certificate
- Client certificate

These certificates:

- Can be used for electronic signatures in order to replace handwritten signatures where transacting parties choose for them

- Can be used to authenticate web resources, such as servers and other devices.

This CPS identifies the roles, responsibilities and practices of all entities involved in the life cycle, use, reliance upon and management of SGSITES Technologies certificates. The provisions of this CPS with regard to practices, level of services, responsibilities and liability bind all parties involved including the SGSITES Trust Center, SGSITES Technologies RA, subscribers and relying parties. Certain provisions might also apply to other entities such as the certification service provider, application providers etc.

A subscriber or relying party of a SGSITES Trust Center certificate must refer to the SGSITES Technologies CPS in order to establish Trust. It is also essential to establish the trustworthiness of the entire certificate chain of the SGSITES Technologies certificate hierarchy, including the Brand Root.

This CPS is made available on-line under: http://pki.sgsites.net/csp/.

The SGSITES Trust Center accepts comments regarding this CPS addressed to the address mentioned above in the Introduction of this document

1.2 Document History

1.1	Version 1 of the SGSITES Trust Center Certification Practice Statement

1.3 Acknowledgments

This SGSITES Trust Center CPS endorses in whole or in part the following industry standards:

- RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policies and Certification Practices Framework (obsoletes RFC 2527)
- RFC 2459: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile.
- RFC 3279: Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRI Profile
- The ISO 1-7799 standard on security and infrastructure

1.4 Terms and Acronyms Used in the CPS

1.4.1 Acronyms

Acronym	Description
CA	Certificate Authority
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CVC	Content Verification Certificate
EPKI	Enterprise Public Key Infrastructure Manager
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
MDC	Multiple Domain Certificate
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (based on X.509 Digital Certificates)
PKCS	Public Key Cryptography Standard
RA	Registration Authority
SGC	Server Gated Cryptography
SSL	Secure Sockets Layer
SSCD	Secure Signature Creation Device
TLS	Transaction Layer Security
URL	Uniform Resource Locator
X.509	The ITU-T standard for Certificates and their corresponding authentication framework

1.4.2 Terms

Term	Description
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 that 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 pki.sgsites.net/legal.
Relying Party Agreement	The Relying Party Agreement is an agreement that must be read and accepted by a Relying Party prior to validating, relying on or using a Certificate and is available for reference at pki.sgsites.net/legal.
Certificate Policy	The Certificate Policy is a statement of the issuer that corresponds to the prescribed usage of a digital certificate within an issuance context.

1.5 Types of Certificates

1.5.1 Server Certificates

SGSITES Technologies Server certificates can be used for web based transactions. It is meant for entities that wish to participate in secure communication and transactions at the web-server level. By using Secure Socket Layer (SSL) technology these certificates are essential to web-based businesses engaging in secured transactions. The identity of the certificate-holder is fully authenticated by SGSITES Trust Center.

1.5.2 Client Certificates

SGSITES Technologies Client certificates may be used to provide authentication services, secure e-mail capabilities, inter-organizational communications, access to personal financial information and to authenticate the subscriber in online Internet transactions. They require professional context affiliation to be incorporated into the certificate.

1.6 Acceptable Subscriber Name

For publication in its certificates SGSITES Trust Center accepts subscriber names that are meaningful and can be authenticated as required.

1.7 Pseudonyms

SGSITES Trust Center may allow the use of pseudonyms, reserving its right to disclose the identity of the subscriber as may be required by law or a following a reasoned and legitimate request.

1.8 Registration Procedures

SGSITES Trust Center reserves the right to update registration procedures and subscriber submitted data to improve the identification and registration process.

2. Server Certificates

2.1 General

SGSITES Technologies certificates are meant for secure communication with, for example, a web-site through an SSL or TLS link.

The applicant is an individual or organization that has an Internet Server such as a website. SGSITES Technologies certificates are used to assure a confidential communication with the Internet Server.

SGSITES Technologies certificates validity period is between one and three years.

SGSITES Technologies certificates are issued to entities and individuals who own a domain name, or have the right to request a SGSITES Technologies certificate for a specific domain.

2.2 Certificate Request

A certificate request can be made in the following way:

The certificate applicant submits an application following a procedure provided by SGSITES Trust Center. Additional documentation in support of the application may be required so that SGSITES Trust Center verifies that the domain name belongs to the applicant, or that the applicant is authorized to request a certificate for that domain name. The applicant submits to SGSITES Trust Center the additional documentation. Upon verification of ownership or right to use of the domain name, SGSITES Trust Center issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate on the server. The applicant must notify SGSITES Trust Center of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of changes to the information to be included in the certificate.

2.3 Certificate Content

Typical information published on a SGSITES Technologies certificate includes the following elements

- Applicant's domain name
- Applicant's public key
- Issuing certification authority (SGSITES Trust Center)
- SGSITES Technologies electronic signature
- Type of algorithm
- Validity period of the digital certificate
- Serial number of the digital certificate

2.4 Information Submitted to verify Ownership or Right of Use

The applicant must provide contact details to SGSITES Trust Center. SGSITES Trust Center has the right to request a signed registration form or a signed subscriber agreement. SGSITES Trust Center has the right to request proof of the ownership of the domain name or can ask the owner of the domain name to validate the request of the applicant.

2.5 Issuance Procedure

The issuing procedure for a SGSITES Technologies Server certificate is as follows:

1: The applicant creates Certificate Signing Request (CSR) and a key pair using appropriate server software.

2: The applicant follows the registration procedure.

3: The applicant submits the required information including technical contact and server information.

4: The applicant accepts the subscriber agreement.

6: SGSITES Trust Center verifies the submitted information by checking domain ownership or domain right to use and any other information as it sees fit.

7: SGSITES Trust Center may positively verify the applicant.

8: SGSITES Trust Center may issue the certificate to the applicant.

9: SGSITES Trust Center may publish the issued certificate in an online database

10: Renewal: allowed

11: Revocation: allowed

SGSITES Technologies might apply variations of this procedure in order to meet service, standards or legal requirements.

2.6 Limited Warranty

SGSITES Technologies accepts no liability per loss due to a false domain name (lack of ownership or lack of right to use domain) in a certificate issued according to the CPS.

3. Client Certificates

3.1 General

SGSITES Technologies Client certificates are intended for certain communications and transactions that require a minimum verification of the identity. They can be distributed for communications and transactions with a need to authenticate the communicating parties and encrypt the exchanged communications. The validity period is between one and three years. SGSITES Technologies Client certificates are issued to natural persons (individuals) within their professional context.

3.2 Certificate Request

A certificate request can be made by the following means:

The certificate applicant submits an application according to a procedure provided by SGSITES Technologies. Additional documentation in support of the application may be required so that

SGSITES Trust Center can verify the identity of the applicant. The applicant submits to SGSITES Technologies such additional documentation. Upon verification of identity, SGSITES Trust Center issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate to the applicant's device. The applicant must notify SGSITES Trust Center of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of changes to the information to be included in the certificate.

3.3 Certificate Content

Typical content of information published on a SGSITES Technologies Client certificate includes the following elements:

- Subscriber's e-mail address
- Subscriber's name
- Applicant's professional organization
- Applicant's public key
- Code of applicant's country
- Issuing certification authority (SGSITES Trust Center)
- SGSITES Technologies electronic signature
- Type of algorithm
- Validity period of the digital certificate
- Serial number of the digital certificate

3.4 Documents submitted to verify the Identity of the Applicant

In all cases, the applicant must submit to SGSITES Trust Center a signed subscriber agreement. SGSITES Trust Center must have access to a copy of identity proof.

SGSITES Trust Center may require additional proof of identity in support of the verification of the applicant.

3.5 Issuance Procedure

The issuing procedure for a SGSITES Technologies Client certificate is as follows:

1: The applicant submits the required information: e-mail address, common name, organizational information and country code.

2: The applicant accepts the subscriber agreement.

3: A key pair is generated on an applicant's device (e.g. computer, smart card device etc.).

4: Applicant must provide to SGSITES Trust Center proof of identity, if required.

5: SGSITES Trust Center may positively verify the applicant.

6: SGSITES Trust Center may issue the certificate to the applicant.

7: Renewal: allowed.

8: Revocation: allowed.

SGSITES Trust Center might apply variations of this procedure in order to meet service, standards or legal requirements.

3.6 Limited Warranty

SGSITES Technologies accepts no liability per loss due to a false identity in a certificate issued following the CPS.

4. PKI Participants

The SGSITES Trust Center makes its services available to SGSITES Technologies certificate subscribers. These subscribers include without limitation entities that uses the SGSITES Technologies certificates for the purposes of:

Authentication (digital signature)

Encryption

4.1 SGSITES Trust Center

A Certification Authority, such as SGSITES Trust Center, is an organization that issues digital certificates to be used in public or private domains, within a business framework, a transaction context etc. A certification authority is also referred to as the Issuing Authority to denote the purpose of issuing certificates.

The SGSITES Trust Center drafts and implements the policy prevailing in issuing a certain type or class of digital certificates.

The SGSITES Trust Center ensures the availability of all services pertaining to the management of SGSITES Technologies certificates, including without limitation the issuing, revocation, status verification of a certificate, as they may become available or required in specific applications.

Appropriate publication is necessary to ensure that relying parties obtain notice or knowledge of functions associated with the revoked and/or suspended certificates. Publication is manifested by including a revoked or suspended certificate in a certificate revocation list that is published in an online directory.

The domain of responsibility of the SGSITES Trust Center's comprises the overall management of the certificate lifecycle including the following actions:

- Issuance
- Revocation
- Renewal
- Status validation

4.2 Subscribers

Subscribers of SGSITES Technologies services are natural persons that successfully apply for a certificate. Subscribers are parties that have ultimate authority over the private key corresponding to the public key that is listed in a subject certificate.

Natural persons that are subscribers typically hold a valid identification document, which might be used as credential in order to issue SGSITES Technologies certificates.

Additional credentials are required as explained in the process for the application for a certificate.

4.3 Relying Parties

Relying parties are natural or legal persons that rely on a certificate and/or a digital signature verifiable with reference to a public key listed in a subscriber's certificate.

To verify the validity of a digital certificate, relying parties must always refer to SGSITES Trust Center revocation information such as a Certificate Revocation List (CRL). Certificate validation takes place prior to relying on information featured in a certificate. Relying parties meet specific obligations as described in this CPS.

5. Certificate Use

5.1 Appropriate Certificate Usage

Certain limitations apply to the use of SGSITES Technologies certificates. A SGSITES Technologies certificate can only be used for purposes explicitly permitted as they are listed below:

Electronic signature: Electronic signature can only be used for specific electronic transactions that support electronic signing of electronic forms, electronic documents, electronic mail etc. The signature certificate is only warranted to produce electronic signatures in the context of applications that support digital certificates. To describe the function of an electronic signature, the term non-repudiation is often used. SGSITES Technologies Client certificates are appropriate for electronic signatures.

Authentication (Users): User authentication certificates can be used for specific electronic authentication transactions that support accessing web sites and other online content, electronic mail etc. The Authentication function of a digital certificate can be ascertained in any transaction context with the purpose of authenticating the end user subscriber to a digital certificate. To describe the function of authentication, the term digital signature is often used. SGSITES Technologies Client certificates are appropriate for user authentication.

Authentication (Devices): Device authentication certificates can be used for specific electronic authentication transactions that support the identifying of web sites and other on line resources. The Authentication function of a digital certificate can be ascertained in any transaction context with the purpose of authenticating a device that the subscriber seeks to secure through a digital certificate. To describe the function of authentication, the term digital signature is often used. SGSITES Technologies Server certificates are appropriate for user authentication.

Confidentiality: All certificate types can be used to ensure the confidentiality of communications effected by means of digital certificates. Confidentiality is required to assure the confidentiality of

business and personal communications as well as for purposes of personal data protection and privacy. All SGSITES Technologies certificates are appropriate for confidentiality.

Any other use of a digital certificate is not supported by this CPS. When using a digital certificate the functions of electronic signature (non-repudiation) and authentication (digital signature) are permitted together with the same certificate.

5.2 Prohibited Certificate Usage

No information available in this version of the CPS.

5.3 Certificate Extensions

No information available in this version of the CPS.

5.4 Critical Extensions

No information available in this version of the CPS.

6. Policy Administration

The Policy Managing Authority of the SGSITES Trust Center manages this SGSITES Technologies CPS. The SGSITES Trust Center registers, observes the maintenance, and interprets this CPS. The SGSITES Trust Center makes available the operational conditions prevailing in the life-cycle management of SGSITES Technologies certificates.

6.1 Scope

SGSITES Technologies may make revisions and updates to its policies as it sees fit or required by the circumstances. Such updates become binding for all certificates that have been issued or are to be issued 30 days after the date of the publication of the updated version of the CPS.

6.2 SGSITES Trust Center Policy Management Authority

New versions and publicized updates of SGSITES Technologies policies are approved by the SGSITES Technologies Policy Management Authority. The SGSITES Technologies Policy Management Authority in its present organizational structure comprises of members as indicated below:

• At least one member of the management of SGSITES Trust Center.

• At least one authorized agents directly involved in the drafting and development of SGSITES Technologies practices and policies.

6.3 Acceptance of Updated Versions of the CPS

Upon approval of a CPS update by the SGSITES Technologies Policy Management Authority, that CPS is published in the SGSITES Technologies online Repository at http://pki.sgsites.net/csp/.

The updated version is binding against all existing and future subscribers unless notice is received within 30 days after communication of the notice. After such period the updated version of the CPS is binding against all parties including the subscribers and parties relying on certificates that have been issued under a previous version of the SGSITES Technologies CPS.

SGSITES Trust Center publishes on its web site at least the two latest versions of its CPS.

6.4 Version Management and Denoting Changes

Changes are denoted through new version numbers for the CPS. New versions are indicated with an integer number followed by one decimal that is zero. Minor changes are indicated through one decimal number that is larger than zero. Minor changes include:

• Minor editorial corrections

• Changes to contact details

7. Identification and Authentication

SGSITES Technologies CA maintains appropriate procedures to address naming practices, including the recognition of trademark rights in certain names.

SGSITES Technologies CA authenticates the requests of parties wishing to revoke certificates under this policy.

7.1 Initial Identity Verification

The identification of the applicant for a certificate is carried out according to a documented procedure.

For the identification and authentication procedures of the initial subscriber registration, SGSITES Trust Center might rely on such resources as third party databases.

7.2 Subscriber Registration Process

SGSITES Trust Center ensures that:

• Subscribers of certificates are properly identified and authenticated

• Subscriber certificate requests are complete, accurate and duly authorized.

7.2.1 Documents Used for Subscriber Identification

SGSITES Technologies CA typically verifies certificate request by appropriate means and on the basis of a documented procedure: the applicant must submit to SGSITES Trust Center a Subscriber Agreement, both accepted and agreed to.

SGSITES Trust Center may prescribe additional identification proof in support of the verification of the applicant ownership or right to use of the domain.

7.2.2 Records for Subscriber Registration

SGSITES Trust Center maintains records of the executed subscriber agreement and any material or documents that support the application which also include but are not limited to:

• SGSITES Trust Center subscriber agreement as approved of, and executed by, the applicant.

• Consent to the keeping of a record by SGSITES Technologies of information used in registration and any subsequent certificate status change and passing of this information to third parties under the same conditions as required by this CPS in the case of the CA terminating its services.

• That information held in the certificate is correct and accurate.

• A specifically designed attribute that uniquely identifies the applicant within the context of the SGSITES Trust Center.

The records identified above shall be kept for a period of no less than 2 years following the expiration of a certificate.

7.2.3 Identification and Authentication for Revocation

For the identification and authentication procedures of revocation requests, SGSITES Trust Center requires using an online authentication mechanism and/or a request addressed to the SGSITES Trust Center.

8. Certificate Life-Cycle Operational Requirements

The following operational requirements apply to Certificate Life-Cycle.

All entities within the SGSITES Technologies domain including subscribers or other participants have a continuous duty to inform the SGSITES Trust Center of all changes in the information featured in a certificate during the operational period of such certificate and until it expires or revoked.

To carry out its tasks SGSITES Technologies may use third party agents for which SGSITES Trust Center assumes responsibility.

Subscribers undergo an enrollment process that requires:

a. Generating a key pair.

b. Delivering the generated public key corresponding to a private key to SGSITES Trust Center.

c. Accepting the subscriber agreement.

The subscriber is required to accept the issuance terms by a subscriber agreement that will be executed with the SGSITES Trust Center. The subscriber agreement incorporates by reference this CPS.

8.1 Certificate Application Processing and Issuance

SGSITES Trust Center acts upon a SGSITES Technologies certificate application to validate the submitted information. Subsequently, the application is either approved or rejected. Such approval or rejection does not necessarily have to be justified to the applicant or any other party.

For rejected applications of certificate requests, SGSITES Trust Center notes the reason for rejecting the application.

Following issuance of the approved certificate, the SGSITES Trust Center delivers the issued certificate to the subscriber.

8.2 Certificate Generation

With reference to the issuance and renewal of certificates, SGSITES Trust Center represents towards all parties that certificates are issued securely according to the conditions set below:

• The procedure to issue a certificate is securely linked to the associated registration, including the provision of any subscriber generated public key.

• The confidentiality and integrity of registration data is ensured at all times through appropriate SSL (Secure Socket layer) links.

• Certificate requests and generation are also supported by robust and tested procedures that have been scrutinized for compliance with the prevailing standards.

8.3 Certificate Acceptance

An issued SGSITES Technologies certificate is deemed accepted by the subscriber when no objection is received by SGSITES Technologies from the subscriber within three (3) working days after it being received. Any objection to accepting an issued certificate must explicitly be notified to the SGSITES Trust Center. The reasoning for rejection including any fields in the certificate that contain erroneous information must also be submitted.

The SGSITES Trust Center might post the issued certificate on a repository. The SGSITES Trust Center also reserves its right to notify the certificate issuance by the SGSITES Trust Center to other entities.

8.4 Key Pair and Certificate Usage

The responsibilities relating to the use of keys and certificates include the ones addressed below:

8.4.1 Subscriber

The obligations of the subscriber include the following ones:

8.4.1.1 Subscriber Duties

Unless otherwise stated in this CPS, the duties of subscribers include the following:

1. Accepting all applicable terms and conditions in the CPS of SGSITES Trust Center published in the SGSITES Technologies repository.
2. Notifying the SGSITES Trust Center of any changes in the information submitted that might materially affect the trustworthiness of that certificate.
3. Ceasing to use a SGSITES Technologies certificate when it becomes invalid.
4. Using a SGSITES Technologies certificate, as it may be reasonable under the circumstance.
5. Preventing the compromise, loss, disclosure, modification, or otherwise unauthorized use of their private key.
6. Using secure devices and products that provide appropriate protection to their keys.

7. Refraining from submitting to SGSITES Trust Center or any SGSITES Technologies directory any material that contains statements that violate any law or the rights of any party.
8. Requesting the revocation of a certificate in case of an occurrence that materially affects the integrity of a SGSITES Technologies certificate.
9. Refraining from tampering with a certificate.
10. Only using certificates for legal and authorized purposes in accordance with the CPS.
11. Refrain from using a certificate outside possible license restrictions imposed by SGSITES Trust Center.

The Subscriber has all above stated duties towards the CA at all times.

8.4.1.2 Subscriber Duties Towards Relying Parties

Without limiting other subscriber obligations stated elsewhere in this CPS, subscribers have a duty to refrain from any misrepresentations they make in certificates to third parties that reasonably rely on the representations contained therein.

10.4.1.3. Reliance at own Risk

It is the sole responsibility of the parties accessing information featured in the SGSITES Trust Center repositories and web site to assess and rely on information featured therein. Parties acknowledge that they have received adequate information to decide whether to rely upon any information provided in a certificate. The SGSITES Trust Center takes steps necessary to update its records and directories concerning the status of the certificates. Failure to comply with the conditions of usage of the SGSITES Trust Center repositories and web site may result in terminating the relationship between the SGSITES Trust Center and the party.

8.4.2 Relying Party

The duties of a relying party are as follows:

8.4.2.1 Relying Party Duties

A party relying on a SGSITES Technologies certificate will:

• Validate a SGSITES Technologies certificate by using certificate status information (e.g. CRL) published by SGSITES Trust Center.

• Trust a SGSITES Trust Center certificate only if all information featured on such a certificate can be verified via such a validation procedure as being correct and up to date.

• Rely on a SGSITES Technologies certificate, only as it may be reasonable under the circumstances.

• Trust a certificate only if it has not been revoked.

8.4.2.2 SGSITES Trust Center Repository

Parties, including subscribers and relying parties, accessing the SGSITES Trust Center Repository and web site agree with the provisions of this CPS and any other conditions of use that the SGSITES Trust Center may make available. Parties demonstrate acceptance of the conditions of

usage of the CPS by submitting a query with regard to the status of a digital certificate or by using or relying upon any such information or services provided:

• Obtaining information as a result of the search for a digital certificate.

• Validating the status of a digital certificate before encrypting data using the public key included in a certificate

• Obtaining information published on the SGSITES Trust Center web site.

8.5 Certificate Renewal

Subscribers may request the renewal of SGSITES Technologies certificates. To request the renewal of a SGSITES Technologies certificate, an end user lodges a request.

Requirements for renewal of certificates, where available, may vary from those originally required for subscribing to the service.

8.6 Certificate Revocation

SGSITES Trust Center shall use reasonable efforts to publish clear guidelines for revoking certificates, and maintain a 24/7 ability to accept and respond to revocation requests.

The identification of the subscriber who applies for a revocation or suspension of a certificate is carried out according to an internal documented procedure.

The SGSITES Trust Center revokes a SGSITES Technologies certificate if:

- There has been loss, theft, modification, unauthorized disclosure, or other compromise of the private key of the certificate's subject.
- The certificate's subscriber has breached a material obligation under this CPS.
- The performance of a person's obligations under this 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 contained in the certificate of the certificate's subject.

8.7 Certificate Status Services

The SGSITES Trust Center makes available certificate status checking services including CRLs, and appropriate Web interfaces.

12.7.1. CRL

A CRL lists all revoked and suspended certificates during the application period. CRLs for the different products are pointed to from within the certificate through the CDP extension.

8.8 End of Subscription

Subscriber subscription ends when a certificate is revoked, expired or the service is terminated.

8.9 Certificates Problem Reporting and Response Capability

In addition to certificate revocation, SGSITES Trust Center provides subscribers, relying parties, and other third parties with clear instructions for reporting complaints or suspected Private Key compromise, certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to certificates. SGSITES Trust Center shall use reasonable efforts to provide a timely capability to accept and acknowledge and respond to such reports.

9. Management, Operational and Physical Controls

This section describes non-technical security controls used by SGSITES Trust Center to perform the functions of key generation, subject authentication, certificate issuance, certificate revocation, audit, and archival.

9.1 Physical Security Controls

The SGSITES Trust Center implements physical controls on its own, leased or rented premises.

The SGSITES Trust Center infrastructure is logically separated from any other certificate management infrastructure, used for other purposes.

The SGSITES Trust Center secure premises are located in an area appropriate for high-security operations.

Physical access is restricted by implementing mechanisms to control access from one area of the facility to another or access into high-security zones.

The SGSITES Trust Center implements prevention and protection as well as measures against fire exposures.

Media are stored securely. Backup media are also stored in a separate location that is physically secure and protected from fire and water damages.

The sites of the SGSITES Trust Center host the infrastructure to provide the SGSITES Trust Center. The SGSITES Trust Center sites implement proper security controls, including access control, intrusion detection and monitoring. Access to the sites is limited to authorized personnel listed on an access list.

9.2 Procedural Controls

The SGSITES Trust Center follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of the members of the staff and of the satisfactory performance of their duties in the fields of the electronic signature-related technologies.

The SGSITES Trust Center obtains a signed statement from each member of the staff on not having conflicting interests, maintaining confidentiality and protecting personal data.

All members of the staff operating the key management operations administrators, security officers, and system auditors or any other operations that materially affect such operations are considered as serving in a trusted position.

The SGSITES Trust Center conducts an initial investigation of all members of staff who are candidates to serve in trusted roles to make a reasonable attempt to determine their trustworthiness and competence.

Where dual control is required at least two trusted members of the SGSITES Trust Center staff need to bring their respective and split knowledge in order to be able to proceed with an ongoing operation.

The SGSITES Trust Center ensures that all actions with respect to the SGSITES Trust Center can be attributed to the system and the person of the CA that has performed the action.

The SGSITES Trust Center implements dual control for critical CA functions.

9.3 Personnel Security Controls

9.3.1 Qualifications, Experience, Clearances

The SGSITES Trust Center perform checks to establish the background, qualifications, and experience needed to perform within the competence context of the specific job.

9.3.2 Training Requirements and Procedures

The SGSITES Trust Center makes available training for their personnel to carry out their functions.

11.3.4 Retraining Periods and Retraining Procedures

Periodic training updates might also be performed to establish continuity and updates in the knowledge of the personnel and procedures.

11.3.5 Sanctions against Personnel

SGSITES Trust Center sanctions personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of systems for the purpose of imposing accountability on a participant's personnel, as it might be appropriate under the circumstances.

11.3.6 Controls of Independent Contractors

Independent contractors and their personnel are subject to the same privacy protection and confidentiality conditions as SGSITES Trust Center personnel.

11.3.7 Documentation for Initial Training and Retraining

The SGSITES Trust Center make available documentation to personnel, during initial training, retraining, or otherwise.

11.4 Audit Logging Procedures

Audit logging procedures include event logging and audit systems, implemented for the purpose of maintaining a secure environment.

SGSITES Trust Center implements the following controls:

SGSITES Trust Center audit records events that include but are not limited to

- Issuance of a certificate
- Revocation of a certificate
- Publishing of a CRL
- Audit trail records contain:
- The identification of the operation
- The data and time of the operation
- The identification of the certificate, involved in the operation
- The identification of the person that performed the operation
- A reference to the request of the operation.

Documents available include:

- Infrastructure plans and descriptions.
- Physical site plans and descriptions.
- Configuration of hardware and software.
- Personnel access lists.

SGSITES Trust Center ensures that designated personnel review log files at regular intervals and detect and report anomalous events.

Log files and audit trails are archived for inspection by the authorized personnel of SGSITES Trust Center. The log files should be properly protected by an access control mechanism. Log files and audit trails are backed up and must be available to independent auditors upon request.

11.5 Records Archival

SGSITES Trust Center keeps archives in a retrievable format.

SGSITES Trust Center ensures the integrity of the physical storage media and implements proper copying mechanisms to prevent data loss.

Archives are accessible to authorized personnel of SGSITES Trust Center as appropriate.

The SGSITES Trust Center keeps internal records of the following items:

• All certificates for a period of a minimum of 2 years after the expiration of the certificate.

• Audit trails on the issuance of certificates for a period of a minimum of 2 years after issuance of a certificate.

• Audit trail of the revocation of a certificate for a period of a minimum of 2 years following the revocation of a certificate.

• CRLs for a minimum of 1 year after expiration or revocation of a certificate.

• Support documents on the issuance of certificates for a period of 2 years after expiration of a certificate. Support documents can be electronically stored.

11.5.1 Types of Records

SGSITES Trust Center retains in a trustworthy manner records of SGSITES Trust Center digital certificates, audit data, certificate application information, log files and documentation supporting certificate applications.

11.5.2 Retention Period

SGSITES Trust Center retains in a trustworthy manner records of certificates for at least 2 years.

11.5.3 Protection of Archive

Conditions for the protection of archives include:

Only the records administrator (member of staff assigned with the records retention duty) may view the archive:

• Protection against modification of archive, such as storing the data on a write once medium.

• Protection against deletion of archive.

• Protection against deterioration of the media on which the archive is stored, such as a requirement for data to be migrated periodically to fresh media.

11.5.4 Archive Collection

The SGSITES Trust Center archive collection system is internal.

11.5.5 Procedures to Obtain and Verify Archive Information

To obtain and verify archive information SGSITES Trust Center maintains records under clear hierarchical control.

The SGSITES Trust Center retains records in electronic or in paper-based format. The SGSITES Trust Center may require subscribers, or their agents to submit documents appropriately in support of this requirement.

Filing terms begin on the date of expiration or revocation. Such records may be retained in electronic or in paper-based format or any other format that the SGSITES Trust Center may see fit.

11.6 Compromise and Disaster Recovery

In a separate internal document, the SGSITES Trust Center documents applicable incident, compromise reporting and handling procedures. The SGSITES Trust Center documents the recovery procedures used in computing resources, software, and/or data are corrupted or suspected of being corrupted.

The SGSITES Trust Center establishes the necessary measures to ensure full recovery of the service, in an appropriate time frame depending on the type of disruption, in case of a disaster, corrupted servers, software or data.

12 Certificate and CRL Policies

This section specifies the certificate format and CRL formats.

12.1 Certificate Profile

SGSITES Technologies certificate profiles are available upon request.

12.2 CRL Profile

The SGSITES Trust Center maintains a record of the CRL profile it uses in an independent technical document. This will be made available at the discretion of the SGSITES Trust Center, on request from parties explaining their interest.

13 Compliance Audit and Other Assessments

SGSITES Trust Center accepts under condition the auditing of practices and procedures it does not publicly disclose. SGSITES Technologies CA gives further consideration and evaluates the results of such audits before possibly implementing them.

Following its own approval with regard to the scope and content, SGSITES Trust Center accepts compliance audits to ensure it meets requirements, standards, procedures and service levels according to this CPS and accreditation schemes it publicly claims compliance with.

14 Other Business and Legal Matters

Certain legal conditions apply to the issuance of the SGSITES Technologies certificates under this CPS as described in this section.

14.1 Financial Responsibility

SGSITES Trust Center maintains sufficient resources to meet its perceived obligations under this CPS. The SGSITES Trust Center makes this service available on an “as is” basis.

14.2 Confidentiality of Business Information

SGSITES Trust Center observes personal data privacy rules and confidentiality rules as described in the SGSITES Technologies CPS. Confidential information includes:

- Any personal identifiable information on subscribers, other than that contained in a certificate.
- Reason for the revocation of a certificate, other than that contained in published certificate status information.
- Audit trails.
- Correspondence regarding CA services.
- CA Private key(s).

The following items are not confidential information:

- Certificate and their content.
- Status of a certificate.

SGSITES Trust Center does not release nor is it required to release any confidential information without an authenticated and justified request specifying either:

- The party to whom the SGSITES Trust Center owes a duty to keep information confidential is the party requesting such information.
- A court order.

Parties requesting and receiving confidential information are granted permission on the assumption that they use it for the requested purposes, secure it from compromise, and refrain from using it or disclosing it to third parties.

14.2.1 Disclosure Conditions

Non-confidential information can be disclosed to any subscriber and relying party under the conditions below:

- Only a single certificate is delivered per inquiry by subscriber or relying party.
- The status of a single certificate is provided per inquiry by a subscriber or relying party.
- Subscribers can consult the information the CA holds about them.

Confidential information may not be disclosed to subscribers nor to relying parties. SGSITES Trust Center properly manages the disclosure of information to the CA personnel.

To incorporate information by reference, SGSITES Trust Center might use computer-based and text-based pointers that include URLs, etc.

14.3 Privacy of Personal Information

SGSITES Trust Center has an internal policy for the protection of personal data of the applicant applying for an SGSITES Technologies certificate.

14.4 Intellectual Property Rights

SGSITES Trust Center owns and reserves all intellectual property rights associated with its databases, web sites, SGSITES Technologies certificates and any other publication whatsoever originating from SGSITES Trust Center including this CPS.

The distinguished names in use across SGSITES Trust Center, remain the sole property of SGSITES Trust Center, which enforces these rights.

Certificates are and remain property of SGSITES Trust Center. SGSITES Trust Center permits the reproduction and distribution of certificates on a non-exclusive, royalty-free basis, provided that they are reproduced and distributed in full, except that certificates are not published in any publicly accessible repository or directory without the express written permission of SGSITES

Trust Center. The scope of this restriction is also intended to protect subscribers against the unauthorized re-publication of their personal data featured on a certificate.

SGSITES Trust Center owns and reserves all intellectual property rights associated with its own products and services that it has not explicitly transferred or released to another party.

14.5 Representations and Warranties

SGSITES Trust Center uses this CPS and a subscriber agreement to convey legal conditions of usage of SGSITES Technologies certificates to subscribers and relying parties.

Participants that may make representations and warranties include SGSITES Trust Center, subscribers, relying parties, and any other participants as it might become necessary.

All parties of the SGSITES Technologies domain, including the SGSITES Trust Center and subscribers warrant the integrity of their respective private key(s). If any such party suspects that a private key has been compromised they will immediately notify SGSITES Trust Center.

14.5.1 SGSITES Trust Center Repository

Parties (including subscribers and relying parties) accessing the SGSITES Trust Center repository and web site agree with the provisions of this CPS and any other conditions of usage that SGSITES Technologies may make available. Parties demonstrate acceptance of the conditions of usage of the CPS by submitting a query with regard to the status of a digital certificate or by anyway using or relying upon any such information or services provided. The SGSITES Trust Center repositories include or contain:

- Information provided as a result of the search for a digital certificate.
- Information to verify the status of an SGSITES Technologies certificate.
- Information published on the SGSITES Trust Center web site.
- Any other services that SGSITES Trust Center might advertise or provide through its web site.
- If a repository becomes aware of or suspects the compromise of a private key, it will immediately notify SGSITES Trust Center.

The SGSITES Trust Center maintains a certificate repository during the application period and for a minimum of two years after the expiration or revocation of a certificate.

14.5.2 Reliance at Own Risk

It is the sole responsibility of the parties accessing information published on the SGSITES Trust Center repositories and web site to assess and rely on information featured therein. Parties acknowledge that they have received adequate information to decide whether to rely upon any information provided in a certificate. SGSITES Trust Center takes steps necessary to update its records and directories concerning the status of the certificates and issue warnings about. Failure to comply with the conditions of usage of the SGSITES Technologies repositories and web site may result in terminating the relationship between the SGSITES Trust Center and the party.

14.5.3 Accuracy of Information

SGSITES Trust Center makes every effort to ensure that parties accessing its repositories receive accurate, updated and correct information. SGSITES Trust Center, however, cannot accept any liability beyond the limits set in this CPS and the SGSITES Trust Center insurance policy.

14.5.4 Information Incorporated by Reference into a Digital Certificate

SGSITES Trust Center incorporates by reference the following information in every digital certificate it issues:

- Terms and conditions of the SGSITES Trust Center CPS.
- Any other applicable certificate policy as may be stated on an issued SGSITES Technologies certificate.
- The mandatory elements of the standard X.509.
- Any non-mandatory but customized elements of the standard X.509.
- 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.

14.5.5 Pointers to Incorporate by Reference

To incorporate information by reference SGSITES Technologies uses computer-based and text-based pointers. SGSITES Technologies may use URLs, OIDs etc.

14.6 Disclaimers of Warranties

This section includes disclaimers of express warranties.

14.6.1 Limitation for Other Warranties

SGSITES Trust Center does not warrant:

- The accuracy of any unverifiable piece of information contained in certificates.
- The accuracy, authenticity, completeness or fitness of any information contained in, free, test or demo certificates.

14.6.2 Exclusion of Certain Elements of Damages

In no event is SGSITES Trust Center liable for:

- Any loss of profits.
- Any loss of data.
- Any indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, and performance or non-performance of certificates or digital signatures.
- Any transactions or services offered or within the framework of this CPS.

- Any other damages except for those due to reliance on the verified information in a certificate, except for information featured on, free, test or demo certificates.
- Any liability incurred in any case if the error in such verified information is the result of fraud or willful misconduct of the applicant.

14.7 Term and Termination

This CPS remains in force until notice of the opposite is communicated by SGSITES Trust Center on its web site or repository.

Notified changes are appropriately marked by an indicated version. Following publications, changes become applicable 30 days thereafter.

14.8 Individual Notices and Communications with Participants

SGSITES Trust Center accepts notices related to this CPS by means of digitally signed messages or in paper form. Upon receipt of a valid, digitally signed acknowledgment of receipt from SGSITES Trust Center the sender of the notice deems its communication effective. The sender must receive such acknowledgment within twenty (20) business 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. Individuals communications made to SGSITES Trust Center must be addressed to pki@sgsites.net or by post to SGSITES Technologies in the address mentioned in the introduction of this document.

14.9 Amendments

Changes to this CPS are indicated by appropriate numbering.

14.10 Dispute Resolution Procedures

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 SGSITES Trust Center of the dispute with a view to seek dispute resolution.

Upon receipt of a Dispute Notice, SGSITES Trust Center convenes a Dispute Committee that advises SGSITES Technologies management on how to proceed with the dispute. The Dispute Committee convenes within twenty (20) business days from receipt of a Dispute Notice. The Dispute Committee is composed by a counsel, a member of SGSITES Trust Center operational management and a security officer. The counsel or data protection officer chair the meeting. In its resolutions the Dispute Committee proposes a settlement to SGSITES Trust Center executive management. SGSITES Trust Center executive management may subsequently communicate the proposed settlement to the resting party.

14.11 Governing Law

This CPS is governed, construed and interpreted in accordance with the laws of Bulgaria. This choice of law is made to ensure uniform interpretation of this CPS, regardless of the place of residence or place of use of SGSITES Technologies certificates or other products and services. The law of Bulgaria apply to all SGSITES Trust Center commercial or contractual relationships in which this CPS may apply or quoted implicitly or explicitly in relation to SGSITES Trust Center products and services where SGSITES Trust Center acts as a provider, supplier, beneficiary receiver or otherwise.

14.12 Compliance with Applicable Law

SGSITES Trust Center complies with applicable laws of Bulgaria.

14.13 Miscellaneous Provisions

14.13.1 Survival

The obligations and restrictions contained under section 8 Other Business and Legal Matters survive the termination of this CPS.

14.13.2 Severability

If any provision of this CPS, including limitation of liability clauses, is found to be invalid or unenforceable, the remainder of this CPS should be interpreted in such manner as to affect the original intention of the parties.