certipost
a bpost company

Definitions and Acronyms

Version	1.0
Document name	DaA_CTP_TSP_V1_0.docx
© Certipost NV ALL RIGHTS RESERVED.	

1. Document control

Review history

Reviewer	**Date**	**Action**	**Version**	**Status**
CEPRAC members	31/01/2012	Generation, review and approval	1.0	Approved

2. Index

3. Scope

The scope of these Definitions and Acronyms is limited to Certipost Trust Services. A trust service is an electronic service which enhances trust and confidence in electronic transactions. Certipost acts as a Trust Service Provider (TSP) – an entity which provides one or more electronic Trust Services – in multiple domains.

4. List of Definitions and Acronyms

Definitions and acronyms have a dynamic nature as they tend to be expanded regularly. A generic document with the definitions and acronyms is available on-line on http://pki.certipost.com

Term or acronym	Definition
Activation Data	Data values, other than keys, that are required to use smart cards and that need to be protected (e.g. PIN and password).
Advanced Electronic Signature	Electronic data, attached or logically linked to other electronic data, enabling authentication method and satisfying the following conditions: • Be uniquely linked to the signatory • Allow identification of the signatory • Be created by means that the signatory is the only person to control • Be linked to the correspondent electronic data so that any later modification of the data can be detected.
AES	Advanced Electronic Signature
Affiliate of a CA	A corporation, partnership, joint venture or other entity controlling, controlled by or under common control with a CA. As used in this definition, “control” (and its correlative meanings, “controlled by” and “under common control with”) means possession, directly or indirectly, of more than fifty percent of the voting shares of such entity or the power to direct the management and affairs of such entity
ARL	Authority Revocation List
ASN.1	Abstract Syntax Notation 1
attribute	information bounded to an entity that specifies a characteristic of an entity, such as group membership or a role, or other authorization information associated with the Attribute Certificate holder NOTE: An attribute may be further defined as an inherent characteristic or set of qualities closely associated with (bounded to) an object (person or entity).
BIPM	Bureau International des Poids et Mesures
CA	Certification Authority
CAA	Certification Authority Auditor
CAdES	CMS Advanced Electronic Signature
CAO	Certification Authority Officer
CC	Common Criteria
ccTLD	Country Code Top-Level Domain
CEO	Chief Executive Officer
CEPRAC	Certipost CErtification PRactices Council
Certificate	An electronic statement that maps the signature verification data to a physical, a moral person or an entity and confirms the identity of this person or entity (subject).

Certificate Holder	A physical or moral person (subject) to which a Certification Service Provider has delivered a Certificate.
Certificate Policy	A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.
Certificate Public Registry	The repository that hold the publicly available certificates, CRL's and ARL's, issued by the CA's.
Certificate revocation list (CRL)	A published list of the serial numbers of revoked / suspended certificates issued and signed by a CA
Certification Authority (CA)	The organization and authority that issues and manages certificates. The CA signs the certificates with a Private Key that belongs to CA and according to the CPS.
Certification Authority Auditor (CAA)	The Certipost Internal CA Auditor that audits the operations of the CA related Entities.
Certification Practice Statement (CPS)	A statement of the practices, providing the framework to support Certificate Policies, which a Certification Service Provider applies for the creation, issuance and management of certificates.
Certification Service Provider	Any physical or legal person who delivers and manages certificates or provides other services related to electronic signatures.
certification signature	signature that is used in conjunction with modification detection permissions (MDP) as defined by ISO 32000-1, clause 12.8.2.2
Certipost Certificate Enterprise Program	This program consists in providing corporate customers with a dedicated Certipost e-Certificates sub-Infrastructure. This will imply usually the set up of an Enterprise CA and subordinate RA(s).
Certipost Certificate Infrastructure	The Certipost Public Key Infrastructure that is deployed by Certipost to provide the Certipost Certification Services.
Certipost Certificate Public Registry	The electronic registry used by Certipost e-Certificates Services to publish the issued Certificates and Certificate Revocation Lists.
Certipost CErtification PRactices Council	The Policy Approval Authority within Certipost e-Certificates is called the Certipost CErtification PRactices Council(CEPRAC). It is the high level management body with final authority and responsibility for : -Specifying and approving the Certipost e-Certificates infrastructure and practices. - Approving the Certipost e-Certificates Certification Practice Statement(s), Certipost e-Certificates Certificate Policies, General Terms & Conditions and Definitions and Acronyms. - Defining the risk management and compliance process for certification practices and Certificate Policies including responsibilities for maintaining the Certipost e-Certificates Certification Practice Statement(s), Certipost e-Certificates Certificate Policies, General Terms & Conditions and Definitions and Acronyms. -Defining the compliance process that ensures that the certificate practices are properly implemented by the CAs. -Defining the compliance process that ensures that the Certificate Policies are supported by the CAs Certification Practice Statement(s). -Publication to the Subscribers and relying parties of the Certipost e-Certificates Certification Practice Statement(s), Certipost e-Certificates Certificate Policies, General Terms & Conditions and Definitions and Acronyms. -Specifying other procedures
Certipost e-Certificates RA Procedures and Guidelines	Procedures and Guidelines that must be strictly followed by Registration Authorities (Central or Local) in the context of the Certipost Certification Services.
Certipost e-Certificates Services	The Certipost Certification services.
Certipost e-Signing Automated (CEA)	This service is integrated with the Exbo invoice scanning application. CEA makes use of the Certipost Signing Service (CSS).
Certipost or Certipost e-Certificates Services	Certipost n.v./s.a., with registered offices in Muntcentrum ,B-1000 Brussels, Belgium
Certipost Signing Service (CSS)	Certipost Signing Service is the service that helps sign the documents created by the document creator and signed by the document signer.
CFO	Chief Financial Officer
CGA	Certification Generation Application

CICA	Chartered Accountants of Canada
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMS	Cryptographic Message Syntax
Confirmation Request	An appropriate out-of-band communication requesting verification or confirmation of the particular fact at issue.
Conforming signature handler	software application, or part of a software application, that knows how to perform digital signature operations (e.g. signing and/or verifying) in conformance with ISO 32000-1 and the requirements of the appropriate profile
Contractual signature policy	set of rules for the creation and validation of multiple signatures under which signatures on a contract can be determined to be valid
COO	Chief Operating Officer
Coordinated Universal Time (UTC)	time scale based on the second as defined in ITU-R Recommendation TF.460-5 NOTE: For most practical purposes UTC is equivalent to mean solar time at the prime meridian (0°). More specifically, UTC is a compromise between the highly stable atomic time (Temps Atomique International - TAI) and solar time derived from the irregular Earth rotation (related to the Greenwich mean sidereal time (GMST) by a conventional relationship). (See annex C for more details).
CP	Certificate Policy (plural CPs)
CPA	Chartered Professional Accountant
CPS	Certification Practice Statement
CRA	Central Registration Authority
CRAO	Central Registration Authority Officer
CRL	Certificate Revocation List
CSO	Chief Security Officer
CSP	Certification Service Provider
DAP	Directory Access Protocol
Digital signature	data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g. by the recipient (ISO 7498-2)
DSA	Digital Signature Algorithm. A signature algorithm used in conjunction with SHA-1
DTBS	Data to be Signed
EAL	Evaluation Assurance Level
Electronic Signature	Electronic data, attached or logically linked to other electronic data that enables authentication. A further meaning can be an electronic equivalent of a traditional signature.
Enterprise EV Certificate	An EV Certificate that an Enterprise RA authorizes the CA to issue at third and higher domain levels that are contained within the domain that was included in an original Valid EV certificate issued to the Enterprise RA.
European Directive(The)	The European Directive 1999/93/EC of the European Parliament and the Council of 13 December 1999 “on a community framework for electronic signature”.
EV	Extended Validation
EV Authority	A source other than the Certificate Approver, through which verification occurs that the Certificate Approver is expressly authorized by the Applicant, as of the date of the EV certificate Request, to take the Request actions described in these Guidelines.
EV Certificate	A certificate that contains information specified in these Guidelines and that has been validated in accordance with these Guidelines.
Extended Validation Certificate	See EV Certificate.

FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
GMT	Greenwich Mean Time
GSM	Global System for Mobile communication
gTLD	Generic Top-Level Domain
Hash function	A function that maps string of bits to fixed-length strings of bits, satisfying the following two properties: - It is computationally unfeasible to find for a given output an input that map to this output - It is computationally unfeasible to find for a given input a second input which maps to the same output
HI	Human Interface
High Risk Applicants	Applicants likely to be at a high risk of being targeted for fraudulent attacks.
HSM	Hardware Security Module
HTTP	HyperText Transfer Protocol
HW	Hardware
I/O	Input / Output
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IERS	International Earth Rotation Service
IETF	Internet Engineering Task Force
IFAC	International Federation of Accountants
IM	Instant Messaging
Individual	A natural or physical person.
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
ITU	International Telecommunications Union
Jurisdiction of Incorporation	In the case of a Private Organization, the country and (where applicable) the state or province or locality where the organization's legal existence was established by a filing with (or an act of) an appropriate government agency or entity (e.g., where it was incorporated). In the case of a Government Entity, the country and (where applicable) the state or province where the Entity's legal existence was created by law.
Jurisdiction of Registration	In the case of a Business Entity, the state, province, or locality where the organization has registered its business presence by means of filings by a Principal Individual involved in the business.
KRO	Key Recovery Officer
LCP	Lightweight Certificate Policy
LDAP	Lightweight Directory Access Protocol
Legal Existence	A Private Organization, Government Entity, or Business Entity has Legal Existence if it has been validly formed and not otherwise terminated, dissolved, or abandoned.
Legal Practitioner	A person who is either a lawyer or notary competent to render an opinion on factual claims of the Applicant.

Lightweight Certificate	A Certificate that is issued according to the requirements of the ETSI technical standard TS 102 042 Lightweight Certificate Policy (LCP), incorporating less demanding policy requirements than the Normalised Certificate and used to support any usage but Qualified Electronic Signatures of a cryptographic key pair whose corresponding public key pair is certified. The certified key usage's can be any or any mix of the following usage's: encryption, authentication, non-Qualified signatures, etc.
LLC	Limited Liability Company
LRA	Local Registration Authority
LRAO	Local Registration Authority Officer
LTV	Long Term Validation
Maximum Validity Period	The maximum time period for which the issued certificate is valid.
may	means that a course of action is permissible within a profile
MD5	Message Digest 5
MDP	Modification Detection Permissions
Message Digest 5 (MD5)	one way hash function that provides an 128 bits output
NCP	Normalised Certificate Policy
NGO	Non-Governmental Organization
NIST	(US Government) National Institute of Standards and Technology
Normalized Certificate	A Certificate that is issued according to the requirements of the ETSI technical standard TS 102 042 or equivalent Normalised Certificate Policy (either NCP or NCP+), and used to support any usage but Qualified Electronic Signatures of a cryptographic key pair whose corresponding public key pair is certified. Normalized gives the highest level of assurance provided by a Qualified Trusted Service Provider (supervised/accredited by the referenced Member State for compliance with the relevant provisions laid down in Directive 1999/93/EC), supporting the same level of quality as certification authorities issuing qualified certificates (as required by article 5.1 of the Directive) but "normalized" for wider applicability. Evidence of the identity is checked against a physical person either directly or indirectly using means which provides equivalent assurance to physical presence.
Object Identifier	A unique alphanumeric/numeric identifier registered under the International Standards Organization's applicable standard for a specific object or object class.
OCC	(US Government) Office of the Comptroller of the Currency
OCSP	see Online Certificate Status Protocol
OCSP Responder	An online software application operated under the authority of the CA and connected to its Repository for processing EV Certificate status requests. See also, Online Certificate Status Protocol.
OED	Oxford English Dictionary
OID	Object Identifier
Online Certificate Status Protocol	An online Certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate. See also OCSP Responder
OS	Operating System
PAdES	PDF Advanced Electronic Signature
PAdES-BES	PAdES Basic Electronic Signature
PAdES-EPES	PAdES Explicit Policy Electronic Signature
Parent Company	A company that owns a majority of a Subsidiary Company and this can be verified by reference to a QIIS or from financial statements supplied by a registered Chartered Professional Accountant (CPA) or equivalent outside of the USA.
PDA	Personal Digital Assistant
PDF	Portable Document Format

PDF Conforming signature handler	software application, or part of a software application, that knows how to perform digital signature operations (e.g. signing and/or verifying) in conformance with ISO 32000-1 and the requirements of the appropriate profile
PDF document creator	entity that creates a PDF document
PDF serial signature	specific signature workflow where the second (and subsequent) signers of a PDF not only sign the document but also the signature of the previous signer and any modification that may also have taken place (e.g. form fill-in)
PDF signature	binary data object based on the CMS (RFC 3852) or related syntax containing a digital signature placed within a PDF document structure as specified in ISO 32000-1, clause 12.8 with other information about the signature applied when it was first created
Physical Person	A natural person.
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (X.509) (IETF Working Group)
Place of Business	The location of any facility (such as a factory, retail store, warehouse, etc) where the Applicant's business is conducted.
PP	Protection Profile
Principal Individual	An individual of a Private Organization, Government Entity, or Business Entity that is either an owner, partner, managing member, director, or officer, as identified by their title of employment, or an employee, contractor or agent authorized by such entity or organization to conduct business related to the request, issuance, and use of certificates.
Private Key	The private part of an asymmetric key pair, kept secret by the holder, and used for Public Key encryption techniques. The Private Key is typically used for creating digital signatures or decrypting messages.
Private Organization	A non-governmental legal entity (whether ownership interests are privately held or publicly traded) whose existence was created by a filing with (or an act of) the Incorporating Agency in its Jurisdiction of Incorporation.
Private Signing Key	Private Key that is exclusively used for signing data.
PSE	Personal Security Environment
Public Key	The public part of an asymmetric key pair used for Public Key encryption techniques. The Public Key is typically used for verifying digital signatures or to encrypt messages to the owner of the Private Key. The public key may be publicly disclosed by the holder of the corresponding Private Key.
public key certificate	public keys of a user, together with some other information, rendered unforgeable by encipherment with the private key of the certification authority which issued it (ITU-T Recommendation X.509)
Public Key Infrastructure	A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.
QCP	Qualified Certificate Policy
QGIS	Qualified Government Information Source
QIIS	Qualified Independent Information Source
QTIS	Qualified Government Tax Information Source

Qualified Certificate	A Certificate that is used exclusively to support electronic signatures and that complies to the requirements of Annex I of the 09 July 2001 Law Annex I and is delivered by a Certification Service Provider that satisfies to the Annex II of the 09 July 2001 Law, and by referencing the technical standard ETS TS 101 456 or equivalent, the technical standard ETSI TS 101 862 "Qualified Certificate profile" and the RFC 3739 "Internet X.509 Public Key Infrastructure Qualified Certificate Profile". Qualified provides the highest level of assurance provided by a Qualified Trusted Service Provider (supervised/accredited by the referenced Member State for compliance with the relevant provisions laid down in Directive 1999/93/EC). Evidence of the identity is checked against a physical person either directly or indirectly using means which provides equivalent assurance to physical presence.
Qualified electronic signature	Electronic Signature that satisfies the Article 5.1 of The European Directive and Article 2, 2° of the 09 July 2001 Law. It is an advanced electronic signature which is based on a qualified certificate and which is created by a secure-signature-creation device.
Qualified Government Information Source	A regularly-updated and current, publicly available, database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information, provided that its contents are maintained by a Government Entity, the reporting of data is required by law, and false or misleading reporting is punishable with criminal or civil penalties.
Qualified Government Tax Information Source	Qualified Governmental Information Source that specifically contains tax information relating to Private Organizations, Business Entities, or Individuals.
Qualified Independent Information Source	A regularly-updated and current, publicly available, database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information.
RA	Registration Authority
Race Integrity Primitives Evaluation Message Digest 160 (RIPEMD-160)	way hash function that provides a 160 bits output
RAO	Registration Authority Officer
Registered Office	The official address of a company, as recorded with the Incorporating Agency, to which official documents are sent and at which legal notices are received.
Registration Authority (RA)	An entity, constituted of as an example, but not limited to a Central Registration Authority (CRA) or Local Registration Authority (LRA), that undertakes to identify and authenticate Subscribers on behalf of a CA.
Relying Party	A person, an organization or a computer system that relies on a valid certificate. Also a recipient of a time-stamp token who relies on that time-stamp-token based on a valid certificate is a Relying Party.
Repository	An online database of EV Certificate status information, either in the form of a CRL or an OCSP response.
RFC	Request For Comments
RIPEMD-160	Race Integrity Primitives Evaluation Message Digest 160
Risk Assessments	Activities that: (i) identify reasonably foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any EV Data or EV Processes; (ii) assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the EV Data and EV Processes; and (iii) assess the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to control such risks.
Rivest Shamir Adleman (RSA)	algorithm usable either for signature or encryption
role	part played in a transaction or protocol; one's function, what one is appointed or expected or has undertaken to do
Root CA	The top level Certification Authority that issues the self-signed Root Certificate under which the CA issues Certificates.
Root CA Key Pair	The Private Key and its associated Public Key held by the Root CA.
Root Certificate	The self-signed certificate issued by the Root CA to identify itself and to facilitate signing of certificates identifying its Subordinate CAs.
Root Key Generation Script	A documented plan of procedures to be performed for the generation of the Root CA key pair.

RSA	A specific Public Key algorithm published by Rivest, Shamir, and Adleman
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SCA	Signature-Creation Application
SDO	Signed Data Object
SEC	(US Government) Securities and Exchange Commission
Secret key	A key used in symmetric encryption where the sender and receiver of encrypted messages use the same secret key.
Secure Hash Function 1(SHA-1)	one way hash function that provides a 160 bits output
Secure Signature Creation Device	A software or hardware device that is configured to apply the Signature Creation Data and that satisfies the requirements of the Annex III of the European Directive and of the 09 July 2001 Law.
Secure User Device	Device which holds the user's private key, protects this key against compromise and performs signing or decryption functions on behalf of the user.
Seed value dictionary	PDF data structure, of type dictionary, as described in ISO 32000-1, clause 12.7.4.5, table 234, that contains information that constrains the properties of a signature that is applied to a specific signature field
Service Entity	A limited range of possible certificates which can be independently managed by an organization including their issuance based on pre-filled and unchangeable values. For example, for SSL certificates, only the hostname may be freely filled in to form a new FQDN if it is proven that the Subscriber is the owner of the domain name from the TLD down to the level above the hostname.
SF	Security Function
SFP	Security Function Policy
SHA-1	Secure Hash Function 1
shall	means that the definition is an absolute requirement of a profile NOTE: It has to strictly be followed in order to conform to the present document
should	Means that among several possibilities one is recommended, in a profile, as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required NOTE: Implementers may know valid reasons in particular circumstances to ignore this recommendation, but the full implications have to be understood and carefully weighed before choosing a different course.
Signature attributes	Additional information that is signed together with the Signer's Document.
Signature Creation Data	Unique data, such as codes or cryptographic Private Keys, used by the signatory to create an (advanced / qualified) electronic signature.
Signature Creation Device (SCD)	Configured software and hardware used to create a digital signature.
signature dictionary	PDF data structure, of type dictionary, as described in ISO 32000-1, clause 12.8.1, table 252 that contains all the information about the Digital Signature
Signature Policy (SP)	a set of technical and procedural requirements for the creation and verification of an electronic signature, under which the signature can be determined to be valid.
Signature policy identifier	Object Identifier that unambiguously identifies a Signature Policy.
signature policy issuer	Entity or organization that that creates, maintains and publishes a signature policy, which defines the technical and procedural requirements for electronic signature creation and validation, in order to meet a particular business need.
Signature policy issuer name	A name of a Signature Policy Issuer.
Signature Time-stamp	A time-stamp in a container for a time-stamp token over the Signature Value to protect against repudiation in case of a key compromise. This time-stamp is evidence that the signature existed before the asserted time and can be used to prove the signature's validity after the expiration, revocation or compromise of the signing certificate. The process for time-stamping a digital signature is described in RFC 3161.
signature validation policy	part of the signature policy which specifies the requirements on the signer in creating a signature and verifier when validating a signature

Signature verification	a process performed by a Verifier either soon after the creation of an electronic signature or later to determine if an electronic signature is valid against a signature policy implicitly or explicitly referenced.
Signature Verification Data	Data, such as codes or cryptographic Public Keys, that are used to verify an (Advanced / Qualified) Electronic Signature.
Signature Verification Device	A software or hardware device that is configured to apply the Signature Creation Data
signer	person or entity that creates an (electronic) signature
Signing Authority	One or more Certificate Approvers designated to act on behalf of the Applicant.
Signing role	role specified in a signature policy, allocated to or adopted by a signer, which defines the relationship between its signature and any other signatures as required by the signature policy
SIM	Subscriber Identity Mode
SMK	Storage Master Key
SOF	Strength of Function
Sovereign State	A state, or country, that administers its own government, and is not dependent upon, or subject to, another power.
SRA	Suspension and Revocation Authority
SRAO	Suspension and Revocation Authority Officer
SSCD	Secure Signature-Creation Device
SSL	Secure Sockets Layer
ST	Security Target
Subject	An entity identified in a certificate, in the Subject field, as the holder of the Private Key associated with the Public Key given in the Certificate. Depending on the CP the identity of the Subject is unambiguously bound to the Public Key specified in the certificate. An Applicant becomes a Subject when the certificate it requested is issued.
Subordinate CA	A Certification Authority whose certificates are signed by the Root CA, or another Subordinate CA. Certificates issued by a Subordinate CA will be valid if the appropriate OID(s) or the special any Policy OID are specified in the certificate Policies extension of the certificates issued to it.
Subscriber	An entity (person or organization) that requests certificates and subscribes with a CA by means of a Subscriber Agreement on behalf of the Subject. The Subscriber may or may not be the Subject. A Subscriber may also subscribe to other services of a Trust Service Provider.
Subscriber Agreement	An agreement between the CA and the Subscriber.
Subsidiary Company	A subsidiary company is defined as a company that is majority owned by the Applicant as verified by reference to a QIIS, or from financial statements supplied by a registered Chartered Professional Accountant (CPA) or equivalent outside of the USA.
SUD	Secure User Device
Suspect code	Code that contains malicious functionality or serious vulnerabilities, including spyware, malware and other code that installs without the user's consent and/or resists its own removal, and code that can be exploited in ways not intended by its designers to compromise the trustworthiness of the platforms on which it executes.
Suspension and Revocation Authority (SRA)	An Authority that suspends, unsuspends and/or revokes Certificates on behalf of the CA.
SVD	Signature-Verification Data
TAI	International Atomic Time
The 09 July 2001 Law	Belgian electronic signature law implementing the European Directive, published on 29 September 2001.
Time stamp service	A service that provides a trusted association between a date and a particular point in time, in order to establish reliable evidence indicating the time at which the datum existed.

Time-Mark	A proof-of-existence for a datum at a particular point in time, in the form of a record in a secure audit trail, which includes at least a trustworthy time value and a hash representation of the datum.
Time-stamp	A proof-of-existence for a date at a particular point in time, in the form of a data structure signed by a Time Stamping Authority, which includes at least a trustworthy time value, a unique identifier for each newly generated time stamp, an identifier to uniquely indicate the time-stamp policy under which the time stamp was created, a hash representation of the datum, i.e. a data imprint associated with a one-way collision resistant uniquely identified hash-function.
time-stamp policy	named set of rules that indicates the applicability of a time-stamp token to a particular community and/or class of application with common security requirements
time-stamp token	data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time
Time-Stamping Authority (TSA)	Trust Service Provider which act as an authority to issue time-stamp tokens
Time-stamping unit	set of hardware and software which is managed as a unit and has a single time-stamp token signing key active at a time
TLD	Top-Level Domain
TLS	Transport Layer Security
TOE	Target of Evaluation
Transactional signature policy	set of rules for the creation and validation of multiple signatures, under which signatures giving effect to a transaction can be determined to be valid
Translator	An individual or Business Entity that the CA has reason to believe possesses the requisite knowledge and expertise to accurately translate the words of a document written in one language to the native language of the CA.
Trustworthy System	Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.
TSA	Time-Stamping Authority
TSA Disclosure statement	set of statements about the policies and practices of a TSA that particularly require emphasis or disclosure to subscribers and relying parties, for example to meet regulatory requirements
TSA practice statement	statement of the practices that a TSA employs in issuing time-stamp tokens
TSA system	composition of IT products and components organized to support the provision of time-stamping services
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	Trusted Service Provider
TST	Time-Stamp token
TSU	Time-Stamping Unit
UBL	Universal Business Language
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
Valid	An certificate that has not expired and has not been revoked.
Valid electronic signature	electronic signature which passes validation according to a signature validation policy
Validation data	data that may be used by a verifier of electronic signatures to determine that the signature is valid (e.g. certificates, CRLs, OCSP responses, time-stamps)
Validation Specialists	Personnel performing validation duties.

Verifier	entity that validates an electronic signature
VOIP	Voice Over Internet Protocol
WebTrust EV Program	The additional audit procedures specified for CAs that issue EV Certificates by the AICPA/CICA to be used in conjunction with its WebTrust Program for Certification Authorities.
WebTrust Program for CAs	The then-current version of the AICPA/CICA WebTrust Program for Certification Authorities, available at http://www.webtrust.org/certauth fin.htm.
WebTrust Seal of Assurance	An affirmation of compliance resulting from the WebTrust Program for CAs.
XAdES	XML Advanced Electronic Signatures
XFA	XML Forms Architecture
XML	eXtensible Markup Language