

EBIZID

EBIZID CPS

Certification Practice Statement

Version 1.02

Contents

1 General 7

1.1 EBIZID 7

1.2 Digital Certificates 7

1.3 User Interaction for Selecting a Certification Service 7

1.4 EBIZID Registration Authorities 7

1.5 Subscribers 8

1.6 Relying Parties 8

1.7 EBIZID CPS 8

2 Technology 9

2.1 Digital Certificate Management 9

2.2 EBIZID Directories, Repository and Certificate Revocation List 9

2.3 Trustworthy Systems 9

2.4 Types of EBIZID Certificates 9

2.4.1 EBIZID Secure Server Certificates 9

2.5 Approval of Software and Hardware Devices 10

2.6 Extensions and Naming 11

2.6.1 Digital Certificate Extensions 11

2.6.2 Incorporation by Reference for Extensions and Enhanced Naming 11

2.7 Private Key Generation Process 11

2.7.1 EBIZID Key Generation 11

2.7.2 Secret Sharing 11

2.8 EBIZID Certificates Profile 11

2.8.1 Key Usage extension field 11

2.8.2 Extension Criticality Field 12

2.8.3 Basic Constraints Extension 12

2.8.4 Certificate policy 12

2.9 EBIZID Certificate Revocation List Profile 15

3 Organisation 16

- 3.1 EBIZID Infrastructure 16
- 3.2 Conformance to this CPS 16
- 3.3 Termination of CA Operations 16
- 3.4 Form of Records 16
- 3.5 Records Retention Period 16
- 3.6 Logs for Core Functions 16
- 3.7 Audit for Core Functions 16
- 3.8 Contingency Plans and Disaster Recovery 17
- 3.9 Availability of EBIZID Certificates 17
- 3.10 Publication of Information on Issued Certificates 17
- 3.11 Confidentiality Information 17

Page 2 of 34

- 3.12 Secure Facilities 17
- 3.13 Personnel Management and Practices 17
 - 3.13.1 Confidential Information 17
- 3.14 Publication of information 17

4 Practices and Procedures 19

- 4.1 Certificate Application Requirements 19
 - 4.1.1 Delegation 19
 - 4.1.2 Key Pair Generation 19
 - 4.1.3 Key Pair Protection 19
 - 4.1.4 Use of Secure Devices and Products 19
 - 4.1.5 Delegating Responsibilities for Private Keys 19
- 4.2 Subscriber Identification 19
- 4.3 Validation Information for Certificate Applications 19
 - 4.3.1 Application Information for Organizations 19
- 4.4 Validation Requirements for Certificate Applications 20
 - 4.4.1 Personal Presence 20
 - 4.4.2 Third-Party Confirmation of Business Entity Information 20
 - 4.4.3 Domain Name Confirmation and Serial Number Assignment 20
- 4.5 Time to Confirm Submitted Data 21
- 4.6 Approval and Rejection of Certificate Applications 21
- 4.7 Certificate Issuance and Subscriber Consent 21
- 4.8 Certificate Validity 21
- 4.9 Certificate Acceptance by Subscribers 21
- 4.10 Publication of Issued Certificates 21
- 4.11 Verification of Digital Signatures 21
- 4.12 Reliance on Digital Signatures 22
- 4.13 Certificate Suspension and Revocation 22
 - 4.13.1 Request for Suspension or Revocation 22

4.13.2 Effect of Suspension or Revocation 22

4.14 Renewal 22

4.15 Notice Prior to Expiration 22

5 Legal Conditions of Issuance 23

5.1 EBIZID Representations 23

5.2 Information Incorporated by Reference into a Digital Certificate 23

5.3 Pointers to Incorporate by Reference 23

5.4 Displaying Liability Limitations, and Warranty Disclaimers 23

5.5 Publication of Certificate Data 23

5.6 Duty to Monitor the Accuracy of Submitted Information 23

5.7 Publication of Information 23

5.8 Interference with EBIZID Implementation 24

5.9 Standards 24

5.10 EBIZID Partnerships Limitations 24

5.11 EBIZID Limitation of Liability for a EBIZID Partner 24

Page 3 of 34

5.12 Secret Shares 24

5.13 Choice of Cryptographic Methods 24

5.14 Reliance on Unverified Digital Signatures 24

5.15 Issued but not Accepted Certificates 24

5.16 Refusal to Issue a Certificate 24

5.17 Subscriber Obligations 25

5.18 Representations by Subscriber upon Acceptance 25

5.19 Indemnity by Subscriber 26

5.20 Obligations of EBIZID Registration Authorities and Local Registration Authorities 26

5.21 Obligations of a Relying Party 26

5.22 Legality of Information 26

5.23 Subscriber Liability to Relying Parties 26

5.24 Duty to Monitor Agents 27

5.25 Use of Agents 27

5.26 Conditions of usage of the EBIZID Repository and Web site 27

5.27 Reliance at Own Risk 27

5.28 Accuracy of Information 27

5.29 Failure to Comply 27

5.30 Obligations of EBIZID 27

5.31 Fitness for a Particular Purpose 28

[5.32 Other Warranties](#) *28*

[5.33 Non Verified Subscriber Information](#) *28*

[5.34 Exclusion of Certain Elements of Damages](#) *28*

[5.35 Damage and Loss Limitations](#) *29*

[5.36 Conflict of Rules](#) *29*

[5.37 Intellectual Property Rights](#) *29*

[5.38 Infringement and Other Damaging Material](#) *29*

[5.39 Ownership](#) *29*

[5.40 Governing Law](#) *29*

[5.41 Jurisdiction](#) *30*

[5.42 Dispute Resolution](#) *30*

[5.43 Successors and Assigns](#) *30*

[5.44 Severability](#) *30*

[5.45 Interpretation](#) *30*

[5.46 No Waiver](#) *30*

[5.47 Notice](#) *31*

[5.48 Fees](#) *31*

[5.49 Survival](#) *31*

[6 General Issuance Procedure](#) *32*

Page 4 of 34

[6.1 General](#) *32*

[6.2 Certificates issued to Individuals and Organizations](#) *32*

[6.3 Content](#) *32*

[6.4 Submitted Documents to Identify the Applicant](#) *32*

[6.5 Time to Confirm Submitted Data](#) *33*

[6.6 Issuing Procedure](#) *33*

[6.7 Insurance](#) *33*

Page 5 of 34

You may email your comments to this CPS to info@ebizid.com or send them by post to:

EBIZID
USA Offices 24613 Powers Dearborn Heights, Michigan 48125
Attention: Legal Practices
Email: info@ebizid.com

Page 6 of 34

1 General

This section gives an overview of the EBIZID public certification services.

1.1 EBIZID

EBIZID is a Certification Authority (CA) that issues high quality and highly trusted digital certificates to entities including private, public and individuals. A Certification authority is an organisation, such as EBIZID, that performs functions associated with public key operations that include issuing, suspending, or revoking a digital certificate. In delivering its PKI services EBIZID commits itself to high-level international standards

including those on Qualified Certificates pursuant to the European Directive 99/93. EBIZID acknowledges the UK law on electronic signatures, within the limits of which it operates.

1.2 Digital Certificates

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

While a digital certificate does not necessarily imply any authority it can be used for functions that include identification, electronic signing, authentication and encryption.

1.3 User Interaction for Selecting a Certification Service

Although EBIZID currently offers a wide range of certificates, it disclaims that the model used is fully tamperproof for all applications and transaction contexts. Subscribers are urged to appropriately study their requirements for their specific application for secure communications before applying for a EBIZID certificate.

1.4 EBIZID Registration Authorities

EBIZID makes digital certificates available only following verification of the identity of the applicant.

Hence, through a network of Registration Authorities (RA) and Local Registration Authorities (LRA) EBIZID makes its services available to its subscribers. EBIZID RAs and LRAs:

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

- register subscribers to EBIZID certification services.

- attend all stages of the identification of subscribers as assigned by EBIZID according to the type of certificate they issue.

- use official, notarized or otherwise indicated document to evaluate a subscriber application.

- following approval of an application notifies EBIZID to issue a certificate.

- initiate the process to revoke a certificate and request a certificate revocation from EBIZID.

EBIZID RA/LRAs act locally within their own context of geographical or business partnerships on approval and authorization by EBIZID in accordance with EBIZID practices and procedures. A EBIZID LRA performs registration tasks on behalf of a EBIZID RA. A EBIZID RA supervises a EBIZID LRA.

EBIZID extends the use of Registration Authorities for its Web Host Reseller, Enterprise Public Key Infrastructure (EPKI) Manager and Powered SSL programs. Upon successful approval to join the respective programs the Web Host Reseller Subscriber, EPKI Manager Subscriber or Powered SSL Subscriber are permitted to act as an RA on behalf of EBIZID. RAs are restricted to operating within the set validation guidelines published by EBIZID upon joining the programs. Certificates issued through an RA contains an amended Certificate Profile (section 2.8.4 of this CPS) to represent the involvement of the RA in the issuance process to the Relying Party.

Page 7 of 34

1.5 Subscribers

Subscribers of EBIZID services are natural or legal persons that use PKI in relation with EBIZID 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 EBIZID.

1.6 Relying Parties

Relying parties are natural or legal persons that use PKI services in relation with EBIZID 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 at all times refer to a EBIZID Directory that includes a Certificate Revocation List (CRL) prior to relying on information featured in a certificate.

1.7 EBIZID CPS

The EBIZID CPS is a public statement of the practices of EBIZID and the conditions of issuance, suspension, revocation etc. of a certificate issued under EBIZID's own hierarchy. Pursuant to the division of the tasks of a CA, this CPS is largely divided in the following sections: Technical, Organizational, Practices and Legal.

This CPS is available from www.ebizid.com email from info@ebizid.com by mail from:

EBIZID Ltd.

Attention: Legal Practices, EBIZID 24613 Powers Dearborn Heights, Michigan 48125

Voice: +1-313-299-0593

Fax: +1-443-337-0305

Email: info@ebizid.com

Page 8 of 34

2 Technology

This section addresses certain technology aspects of the EBIZID infrastructure and PKI services.

2.1 Digital Certificate Management

EBIZID certificate management at large refers to functions that include the following:

- Verification of the identity of an applicant of a certificate.
- Authorizing 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.

Within the EBIZID Trust hierarchy EBIZID does the overall certification management, directly or through an agent. EBIZID is not involved in functions associated with the generation, issuance, decommissioning or destruction of a key pair that remain exclusively within the domain of control of a subscriber.

2.2 EBIZID Directories, Repository and Certificate Revocation List

Directly or through third party services, EBIZID makes publicly available and manages directories of issued, suspended and revoked certificates to enhance the level of Trust in its services. A Certificate Revocation List is such a Directory. 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. EBIZID updates frequently its directory of revoked certificates.

EBIZID also publishes repositories of legal notices regarding its PKI services, including this CPS as well as any other information it considers essential to its services.

2.3 Trustworthy Systems

EBIZID makes use of trustworthy systems with relation to its 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.

2.4 Types of EBIZID Certificates

EBIZID currently offers an array 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.

EBIZID 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 EBIZID products creates no claims by any third party. Upon the inclusion of a new certificate product in the EBIZID hierarchy, an amended version of this CPS will be made public on the official EBIZID websites.

Issued, suspended or revoked certificates are appropriately published on EBIZID directories.

2.4.1 EBIZID Secure Server Certificates

EBIZID 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. EBIZID Secure

Page 9 of 34

Server Certificates are offered in two variants; Trust SSL and Select SSL certificates. Pricing for the certificates are made available on the relevant official EBIZID websites. From time to time EBIZID reserve the right to make available promotional offers that may affect the standard price card.

EBIZID: SSL Certificates are the entry level Secure Server Certificate from EBIZID. Their intended usage is for the use of SSL for websites conducting ecommerce or transferring data of low value and also for within internal networks.

EBIZID SSL Certificates utilize IdAuthority to assist with certificate application validation in order to provide an increased speed in the issuance of the certificate. The IdAuthority contains records of over 5 million unique legal entities sourced from a combination of publicly available resources. Where possible, the directory will be used to confirm the identity of a certificate applicant. If the directory cannot be used to sufficiently validate a certificate applicant, further validation processes will be used. These may include an out of bands validation of the applicant's submitted information.

Due to the increased validation speed and the nature of how EBIZID intend SSL certificates to be used, the certificates carry a reduced warranty. The maximum warranty associated with an SSL certificate is \$50.

EBIZID: Select Certificates are the professional level Secure Server Certificates from EBIZID. Their intended usage is for the use of SSL for websites conducting ecommerce and transferring data and also within internal networks.

Select Certificates may also utilize the IdAuthority to assist as part of the certificate application. All Select Certificate applications include an out of bands validation of the applicant's submitted information.

The maximum warranty associated with an Select certificate is \$2500.

Super: SSL Certificates are the professional level Secure Server Certificates from EBIZID. Their intended usage is for the use of SSL for websites conducting high value ecommerce and transferring data and also within internal networks.

Super Certificates may also utilize the IdAuthority to assist as part of the certificate application. All Super Certificate applications include an out of bands validation of the applicant's submitted information.

The maximum warranty associated with a Super certificate is \$10,000.

IntraCert: Intranet SSL Certificates are Secure Server Certificates designed to be used exclusively on internal networks. Their usage is restricted to private IP addresses or full server names only.

As Intranet SSL Certificates are not used commercially the relying party does not require EBIZID, the trusted third party, to provide a warranty against misissuance. As the Intranet SSL Certificate is for use only within a closed network, EBIZID does not exercise validation in the issuance of an Intranet SSL Certificate. There is no warranty attached to an Intranet SSL Certificate.

Trial SSL: Trial SSL 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.

Trial SSL Certificates may be used in an external environment and ultimately may contain information relied upon by the relying party. Therefore all Trial SSL Certificates are validated prior to issuance.

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

2.5 Approval of Software and Hardware Devices

EBIZID approves directly or through an authorized EBIZID consultant all hardware and software that it uses to provide its public PKI services.

Page 10 of 34

2.6 Extensions and Naming

2.6.1 Digital Certificate Extensions

EBIZID uses the standard X.509, version 3 to construct digital certificates, for its PKI products and services. According to the X.509v3 a CA can add certain certificate extensions to the basic certificate structure. EBIZID's public services use a number of controls 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.

2.6.2 Incorporation by Reference for Extensions and Enhanced Naming

Enhanced naming is the usage of an extended organization field in an X.509v3 certificate. Extensions and enhanced naming are usually expressed in a subscriber certificate. They can also be partially defined in a subscriber certificate while the remainder can be a shelved document that is incorporated by reference in the subscriber certificate. Information included in such a shelved document can be made available to requesting parties.

Information contained in the organizational unit field is also included in the Certificate Policy extension that EBIZID may use.

2.7 Private Key Generation Process

EBIZID uses a trustworthy key generation process for the generation of its root private key(s). EBIZID distributes the secret shares of its private key(s). EBIZID is the lawfully owner or holder of the private key(s) that it uses through to secret sharing. EBIZID has the authority to transfer such secret shares to secret-shareholders that have appropriately been authorized.

2.7.1 EBIZID Key Generation

EBIZID securely generates and protects its own private key(s), using a trustworthy system (IBM 4758 accredited to FIPS PUB 140-1 level 4), and take necessary precautions to prevent the compromise or unauthorized usage of it. EBIZID implements and documents key generation procedures, in line with this CPS. EBIZID acknowledges public international and European standards on trustworthy systems and it uses its best endeavors to appropriately follow them to the extent permitted by an application.

2.7.2 Secret Sharing

EBIZID uses secret sharing and multiple authorized holders of secret shares, to safeguard and improve the trustworthiness of its private key(s) and provide for key recovery.

2.8 EBIZID Certificates Profile

A Certificate profile contains fields as specified below:

2.8.1 Key Usage extension field

The Key Usage extension field specifies the purpose of the key contained in the certificate. The usage restriction might be employed when a key that could be used for more than one operation must be restricted. 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

Page 11 of 34

- 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

2.8.2 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.

2.8.3 Basic Constraints Extension

The Basic Constraints extension specifies whether the subject of the certificate may act as a CA or only as an end-user. If the subject may act as a CA, then the certificate is a cross-certificate, and it may also specify the maximum acceptable length of a certificate beyond the cross-certificate. This extension should always be marked as critical, otherwise some implementations will ignore it and allow a non-CA certificate to be used as a CA certificate.

2.8.4 Certificate policy

Certificate policy 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.

Specific EBIZID certificate profiles are as per the tables below:

EBIZID Secure Server Certificate (Trust / Select / Super):

Fields marked in *Italics* are optional OU entries only applicable if the Certificate has been issued through a EBIZID RA (listed in section 1.4 of the CPS):

EBIZID Secure Server Certificate – Trust / Select / Super		
Signature Algorithm		Sha1
Issuer	CN	EBIZID Class 3 Security Services CA
OU	(c)2002 EBIZID Limited	
OU	Terms and Conditions of use: http://www.ebizid.com/repository	
OU	EBIZID Trust Network	
O	EBIZID Limited	
C	GB	
Validity		1 Year / 2 Year / 3 Year
Subject	CN	Common Name
OU	Trust / Select / Super / <i>Product Name*</i>	
<i>OU</i>	<i>Hosted by [Web Host Reseller Subscriber Name] Issued through [EPKI Manager Subscriber Name] Provided by [Powered SSL Subscriber Name]</i>	
O	Organization	
OU	Organization Unit	
L	Locality	
S	Street	
C	Country	
Authority Key Identifier		KeyID=7E7E 8DC4 5055 B52E D34F 59D9 6559 A1F1 5A0C EAB1
Key Usage (NonCritical)		Digital Signature , Key Encipherment(A0)

Netscape Certificate Type	SSL Server Authentication(40)
Basic Constraint	Subject Type=End Entity Path Length Constraint=None

Page 12 of 34

Certificate Policies	[1]Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.6449.1.2.1.3.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.ebizid.com/cps_ebizid.pdf
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.ebizid.comClass3SecurityServices.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.ebizid.com/Class3SecurityServices.crl [3]CRL Distribution Point Distribution Point Name: Full Name: RFC822 Name=Class3SecurityServices@ebizid.com
Subject Alternate Name	DNS Name
NetscapeSSLServerName	
Thumbprint Algorithm	SHA1
Thumbprint	

* Subscribers to the Powered SSL service have the opportunity to rebrand either a EBIZID SSL Certificate, EBIZID SSL Select, Super Certificate, Intranet SSL Certificate or Trial SSL Certificate with their own product naming.

EBIZID Secure Server Certificate (Intranet SSL):

EBIZID Secure Server Certificate – Intranet SSL		
Signature Algorithm	Sha1	
Issuer	CN	EBIZID Class 3 Security Services CA
OU	(c)2002 EBIZID Limited	
OU	Terms and Conditions of use: http://www.ebizid.com/repository	
OU	EBIZID Trust Network	
O	EBIZID Limited	
C	GB	
Validity	1 Year / 2 Year / 3 Year	
Subject	CN	Common Name
OU	Intranet SSL*	

OU	INTRANET USE ONLY - NO WARRANTY ATTACHED - COMPANY NOT VALIDATED
OU	<i>Hosted by [Web Host Reseller Subscriber Name] Issued through [EPKI Manager Subscriber Name] Provided by [Powered SSL Subscriber Name]</i>
O	Organization
OU	Organization Unit
L	Locality
S	Street
C	Country
Authority Key Identifier	KeyID=7E7E 8DC4 5055 B52E D34F 59D9 6559 A1F1 5A0C EAB1
Key Usage (NonCritical)	Digital Signature , Key Encipherment(A0)

Page 13 of 34

Netscape Certificate Type	SSL Server Authentication(40)
Basic Constraint	Subject Type=End Entity Path Length Constraint=None
Certificate Policies	[1]Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.6449.1.2.1.3.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://secure.ebizid.com/CPS
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.ebizid.com/Class3SecurityServices.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.ebizid.com/Class3SecurityServices.crl [3]CRL Distribution Point Distribution Point Name: Full Name: RFC822 Name=Class3SecurityServices@ebizid.com
Subject Alternate Name	DNS Name
NetscapeSSLServerName	
Thumbprint Algorithm	SHA1
Thumbprint	

* Subscribers to the Powered SSL service have the opportunity to rebrand either a EBIZID Trust SSL Certificate, Select SSL Super SSL Certificate, Trial SSL Certificate with their own product naming.

EBIZID Secure Server Certificate (Trial SSL):

EBIZID Secure Server Certificate – Trial SSL		
Signature Algorithm		Sha1
Issuer	CN	EBIZID Class 3 Security Services CA
OU	(c)2002 EBIZID Limited	
OU	Terms and Conditions of use: http://www.ebizid.com/repository	
OU	EBIZID Trust Network	
O	EBIZID Limited	
C	GB	
Validity		1 Year / 2 Year / 3 Year
Subject	CN	Common Name
OU	Trial SSL*	
OU	TEST USE ONLY - NO WARRANTY ATTACHED	
OU	<i>Hosted by [Web Host Reseller Subscriber Name] Issued through [EPKI Manager Subscriber Name] Provided by [Powered SSL Subscriber Name]</i>	
O	Organization	
OU	Organization Unit	
L	Locality	
S	Street	
C	Country	

Page 14 of 34

Authority Key Identifier	KeyID=7E7E 8DC4 5055 B52E D34F 59D9 6559 A1F1 5A0C EAB1
Key Usage (NonCritical)	Digital Signature , Key Encipherment(A0)
Netscape Certificate Type	SSL Server Authentication(40)
Basic Constraint	Subject Type=End Entity Path Length Constraint=None
Certificate Policies	[1]Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.6449.1.2.1.3.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://secure.ebizid.com/CPS

CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.ebizid.com/Class3SecurityServices.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.ebizid.com/Class3SecurityServices.crl [3]CRL Distribution Point Distribution Point Name: Full Name: RFC822 Name=Class3SecurityServices@ebizid.com
Subject Alternate Name	DNS Name
NetscapeSSLServerName	
Thumbprint Algorithm	SHA1
Thumbprint	

* Subscribers to the Powered SSL service have the opportunity to rebrand either a EBIZID Trust SSL Certificate, Select SSL Super SSL Certificate, Trial SSL Certificate with their own product naming.

2.9 EBIZID Certificate Revocation List Profile

The profile of the EBIZID Certificate Revocation List is as per the table below:

Version	[Version 1]
Issuer Name	countryName=[Root Certificate Country Name], organizationName=[Root Certificate Organisation], commonName=[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]

Page 15 of 34

3 Organisation

This part describes the Organisation and the Trust conditions of EBIZID

3.1 EBIZID Infrastructure

EBIZID strives to maintain its sound organisation, technology standing and framework of published practices and procedures.

3.2 Conformance to this CPS

EBIZID conforms to this CPS and other obligations it undertakes through adjacent contracts when it provides its services.

3.3 Termination of CA Operations

In case of termination of CA operations for any reason whatsoever, EBIZID provides timely notice and transfer of responsibilities to succeeding entities, maintenance of records, and remedies. Before terminating its own CA activities, EBIZID 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 EBIZID's.

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

3.4 Form of Records

EBIZID retains records in electronic or in paper-based format. EBIZID may require its registration authorities, local registration authorities, subscribers, or their agents to submit documents appropriately in support of this requirement.

3.5 Records Retention Period

EBIZID retains in a trustworthy manner the records of EBIZID digital certificates and the associated documentation for a term of no less than 10 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 EBIZID may see fit.

3.6 Logs for Core Functions

EBIZID maintains in a trustworthy manner logs of the following events:

Key generation.

Key management.

Perimeter controls.

3.7 Audit for Core Functions

EBIZID makes its infrastructure available to inspection as it sees fit. EBIZID is not obliged to endorse or approve any of the content, findings, and recommendations of such auditing reports and it may review such auditing reports with a view to protect EBIZID services. EBIZID is not to be held responsible for any damages to anyone resulting from EBIZID's reliance on such auditing reports or from non-applying the findings of such reports.

Page 16 of 34

3.8 Contingency Plans and Disaster Recovery

To maintain the integrity of its services EBIZID implements, documents, and periodically tests appropriate contingency and disaster recovery plans and procedures. Such plan is revised and updated as may be required at least once a year.

3.9 Availability of EBIZID Certificates

EBIZID may make available to parties copies of certificates in which EBIZID is the subject as well as any related revocation data to verify a signature that is verifiable with reference to a digital certificate.

3.10 Publication of Information on Issued Certificates

EBIZID publishes all issued public digital certificates, any revocation data or expiration data on these digital certificates, and this CPS.

3.11 Confidentiality Information

EBIZID observes applicable rules on the protection of personal data. EBIZID also treats as confidential and as prescribed by law information that includes the following:

Subscriber agreements.

Certificate application records.

Transaction records.

External or internal audit trail records and reports.

Contingency plans and disaster recovery plans.

Internal tracks and records on the operations of EBIZID infrastructure, certificate management and enrolment services and data.

EBIZID does not release nor is it required to release any confidential information without an authenticated, reasonably specific request by an authorized party specifying:

The party to whom EBIZID owes a duty to keep information confidential.

The party requesting such information.

A court order, if any.

EBIZID may charge an administrative fee to process such disclosures.

3.12 Secure Facilities

Physical access to the secure part of EBIZID facilities is limited to appropriately authorised individuals. Certificate issuance facilities are protected from environmental hazards. Loss, damage or compromise of assets and interruption to business activities are detected, and reasonably prevented. Compromise or theft of information and information processing facilities are detected and reasonably prevented.

3.13 Personnel Management and Practices

Consistent with this CPS EBIZID 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.

3.13.1 Confidential Information

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

3.14 Publication of information

The EBIZID certificate services and the EBIZID repository are accessible through several means of communication:

On the web: www.Ebizid.com

by email from legal@Ebizid.com

and by mail from:

Page 17 of 34

EBIZID Ltd.

Attention: Legal Practices, 24613 Powers, Dearborn Heights Michigan, 48125

Voice: + 1-313-299-0593

Fax: + 1-313-443-0305

Email: legal@EBIZID.com

Page 18 of 34

4 Practices and Procedures

This part presents the practices and procedures of the EBIZID PKI services.

4.1 Certificate Application Requirements

Prior, upon or during application for a digital certificate, applicants of certificates (collectively called subscribers) take the following steps prior to requesting a EBIZID certificate:

Generate a key pair and demonstrate to EBIZID that it is such a key pair that the private key corresponds to the public key.

Protect the integrity of the private key of the generated key pair.

Submit a certificate application and agree with the terms of a subscriber agreement and this CPS.

Submit the public key of the generated key pair to EBIZID.

Provide proof of their identity according to EBIZID or other standard defined procedures as EBIZID may have acknowledged them.

4.1.1 Delegation

Depending on the type of a certificate, an application for a EBIZID digital certificate can be made in person or through an agent.

4.1.2 Key Pair Generation

Subscribers are exclusively responsible to generate securely their own private key pair, using a trustworthy system as required by the product or application.

4.1.3 Key Pair Protection

Subscribers are exclusively responsible to take all necessary measures to prevent the compromise, loss, disclosure, modification, or otherwise unauthorized use of their private key.

4.1.4 Use of Secure Devices and Products

Unless otherwise stated in this CPS, subscribers use secure devices and products that provide for the protection of their keys.

4.1.5 Delegating Responsibilities for Private Keys

Subscribers shall be exclusively responsible for the acts and omissions of partners and agents they use to generate, retain, escrow, or destroy their private keys.

4.2 Subscriber Identification

Prior to issuing a certificate EBIZID mandates controls to establish the identity of a subscriber. Such controls are the role of a EBIZID RA/LRA. A EBIZID RA/LRA also supervises the application of such procedures on the basis of EBIZID issued guidelines that are to be used on-line and/or off-line.

4.3 Validation Information for Certificate Applications

Applications for EBIZID certificates are supported by appropriate documentation to establish the identity of an applicant as described in the product information below.

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

Such documentation shall include identification elements such as the following.

4.3.1 Application Information for Organizations

Critical information elements for a EBIZID certificate issued to a legal person may include the following elements.

Name of the applicant

Name of the legal representative and authorization letter

Page 19 of 34

Domain name
IP address
Legal Name of the Organization
Organizational unit
Street, city, postal/zip code, country
Technical and billing contact persons and legal representative
VAT-number
Trade Register number
Server Software Identification
Payment Information
Proof of right to use name
Proof of existence of the Organization
Proof of organizational status such as articles of incorporation of a company, letter from office of Dean or Principal (for Educational Institutions), official letter from an authorized representative of a government organization.
Registration form signed and properly filled in
Subscriber agreement, signed

4.4 Validation Requirements for Certificate Applications

Upon receipt of an application for a digital certificate and based on the submitted information, EBIZID 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.

EBIZID controls the accuracy of the information published as submitted by the applicant at the moment the certificate is issued.

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

4.4.1 Personal Presence

To establish the link between an applicant and an applicant's public key EBIZID may require the personal presence of an applicant before a RA/LRA for certain types or classes of digital certificates while it reserves its right to modify such registration requirements as it sees appropriate or it may be prescribed by law.

4.4.2 Third-Party Confirmation of Business Entity Information

EBIZID may require a third party to confirm information on a business entity that applies for a EBIZID digital certificate. EBIZID accepts confirmation from third party organizations, other third party databases and government entities while it may examine other third party references as it may be provided within a business context.

Certain entities such as banks and financial institutions may be required to provide proof of their activity prior to having digital certificates issued to them with a purpose to perform banking or otherwise licensed or controlled functions.

EBIZID 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.

EBIZID may use any means of communication at its disposal to ascertain the identity of a legal entity.

4.4.3 Domain Name Confirmation and Serial Number Assignment

Only EBIZID has discretion to assign Relative Distinguished Names (RDNs) and certificate serial numbers that appear in a EBIZID certificates. EBIZID may use the Domain Name Service for resolving RDN assignment if necessary.

Page 20 of 34

4.5 Time to Confirm Submitted Data

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

4.6 Approval and Rejection of Certificate Applications

Following successful completion of all required validations of a certificate application EBIZID approves an application for a digital certificate.

If the validation of a certificate application fails, EBIZID rejects the certificate application. Upon such rejection EBIZID 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.

EBIZID 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 EBIZID 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

EBIZID 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 EBIZID accepts a certificate application.

EBIZID issues a certificate pursuant to an applicant's consent. Consent to issue a certificate is demonstrated by submitting an application notwithstanding the fact that acceptance of a certificate has not yet occurred.

4.8 Certificate Validity

Certificates are valid upon issuance by EBIZID and acceptance by the subscriber.

4.9 Certificate Acceptance by Subscribers

A subscriber is deemed to have accepted a certificate when:

- Subscriber's approval of the certificate is manifested to EBIZID by means of an on-line or email notice sent to EBIZID by the subscriber.
- Using the certificate.
- 15 days pass from the date of the issuance of a certificate.

4.10 Publication of Issued Certificates

Upon subscriber's acceptance of the certificate, and checking by EBIZID, EBIZID publishes a copy of the certificate in a EBIZID repository. While EBIZID may publish a certificate on other repositories, as it might see fit it assumes no responsibility for the validity, completeness or availability of directories issued by such third parties. Subscribers on their turn may also publish their EBIZID certificates in other repositories.

4.11 Verification of Digital Signatures

Verification of a digital signature aims at determining that:

the digital signature was created by the private key corresponding to the public key listed in the signer's certificate.

the associated message has not been altered since the digital signature was created.

Page 21 of 34

4.12 Reliance on Digital Signatures

The final decision concerning whether or not to rely on a verified digital signature is exclusively that of the verifier. A digital signature can be trusted to rely upon if:

The digital signature was created during the operational period of a valid certificate and it can be verified by referencing a validated certificate.

Reliance is reasonable under the circumstances.

4.13 Certificate Suspension and Revocation

Suspension of a certificate is to make it temporarily inoperable. Revocation of a certificate is to permanently end the operational period of such certificate as of a specified time forward. EBIZID suspends or revokes a digital 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 subject (whether EBIZID or a 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.

4.13.1 Request for Suspension or Revocation

The subscriber or other appropriately authorized parties can request suspension or revocation of a certificate. Suspension or revocation can be done through the EBIZID web site, by email or phone. The identity of the requesting party shall be verified as appropriate.

4.13.2 Effect of Suspension or Revocation

During suspension, or upon revocation of a certificate, the operational period of that certificate is immediately considered terminated.

4.14 Renewal

The validity period of EBIZID certificates is indicated on the appropriate certificate field and is one year (365 days) from the date of issuance. While requirements may vary from those originally required to subscribe to the service, EBIZID makes available a conditional renewal of digital certificates it has issued. Renewal is allowed only if all data on a certificate remains correct as per the initial application.

The subscriber must at all times control the correctness and accuracy of the information published in a renewed certificate. Requests for renewal must be addressed to EBIZID at least 10 days prior to expiration date.

4.15 Notice Prior to Expiration

To keep intact the capacity of users of digital certificates to digitally sign, approximately thirty (30) days prior to the expiration of a digital certificate, EBIZID shall make reasonable efforts to notify subscribers via e-mail, of the imminent expiration of a digital certificate.

Page 22 of 34

5 Legal Conditions of Issuance

This part describes the legal representations, warranties and limitations associated with EBIZID digital certificates.

5.1 EBIZID Representations

EBIZID makes to all subscribers and relying parties certain representations regarding its public service, as described below. EBIZID 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

EBIZID incorporates by reference the following information in every digital certificate it issues:

- terms and conditions in this CPS.
- any other applicable certificate policy as may be stated on an issued EBIZID certificate.
- the mandatory elements of the standard X.509v3.
- any non-mandatory but customized 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 Pointers to Incorporate by Reference

To incorporate information by reference EBIZID uses computer-based and text-based pointers. EBIZID may use URLs (Universal Resource Locators), OIDs (Object Identifiers) or any other means to incorporate information by reference, as they may become available.

5.4 Displaying Liability Limitations, and Warranty Disclaimers

EBIZID 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 EBIZID may use:

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

5.5 Publication of Certificate Data

EBIZID reserves its right and the subscriber agrees to publish a certificate and certificate related data in any accessible repository including two LDAP (Light Directory Application Protocol) directories as well as by means of a CRL (Certificate Revocation List), OCSP (Online Certificate Status Protocol) or other available technology as it may be indicated.

As EBIZID manages directories of featured certificates to enhance the level of Trust in its services users and relying parties are strongly advised to consult the directories of issued and revoked certificates at all times prior to relying on information featured on a certificate.

5.6 Duty to Monitor the Accuracy of Submitted Information

In all cases and for all types of EBIZID certificates the subscriber (and not EBIZID) has a continuous obligation to monitor the accuracy of the submitted information and notify EBIZID of any such changes.

5.7 Publication of Information

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

Page 23 of 34

5.8 Interference with EBIZID Implementation

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

5.9 Standards

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

5.10 EBIZID Partnerships Limitations

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

5.11 EBIZID Limitation of Liability for a EBIZID Partner

As the EBIZID network may include RAs and LRAs that operate under EBIZID practices and procedures EBIZID warrants the integrity of any certificate issued under its own root within the limits of the EBIZID insurance policy.

5.12 Secret Shares

EBIZID uses secret shares to protect its private key.

5.13 Choice of Cryptographic Methods

Parties acknowledge that they are solely responsible for and have exercised independent judgement 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.

5.14 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 a CRL or any other available directory published by EBIZID. Relying parties are alerted that an unverified digital signature cannot be assigned as the signature of the subscriber.

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

By means of this CPS EBIZID has adequately informed relying parties on the usage and validation of digital signatures through this CPS and other documentation published in its public repository.

5.15 Issued but not Accepted Certificates

An applicant for a certificate that submits an application to EBIZID for a certificate that EBIZID does not accept as a valid one for any reason whatsoever, may never create digital signatures using a private key corresponding to the public key included in a certificate if the effect is to create the conditions of relying upon such certificate.

5.16 Refusal to Issue a Certificate

EBIZID 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.

Page 24 of 34

5.17 Subscriber Obligations

Unless otherwise stated in this CPS, EBIZID subscribers and not EBIZID shall exclusively be responsible:

- Have knowledge and if necessary request training on using digital certificates and PKI.
- To generate securely their own private key pair, using a trustworthy system.
- Ensure that the public key submitted to EBIZID corresponds with the private key used.
- Ensure that the public key submitted to EBIZID is the correct one.
- Provide correct and accurate information in its communications with EBIZID.
- Re-apply for a certificate if at the stage of certificate renewal any information originally submitted has changed since it had been originally submitted to EBIZID.
- Generate a new, secure key pair to be used in association with a certificate that it requests from EBIZID.
- Read, understand and agree with all terms and conditions in this EBIZID CPS and associated policies published in the EBIZID Repository.
- Refrain from tampering with a EBIZID certificate.
- Use EBIZID certificates for legal and authorized purposes in accordance with this EBIZID CPS.
- Notify EBIZID or a EBIZID RA of any changes in the information submitted.
- Cease using a EBIZID certificate if any information in it becomes misleading obsolete or invalid.
- Cease using a EBIZID 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 EBIZID issued certificate under its own name to have other certificates issued.
- Use a EBIZID certificate, as it may be reasonable under the circumstances.
- Prevent the compromise, loss, disclosure, modification, or otherwise unauthorized use of the private key corresponding to the public key published on a EBIZID certificate.
- To use secure devices and products that provide appropriate protection to their keys.
- Request the suspension or revocation of a certificate in case of an occurrence that materially affects the integrity of a EBIZID certificate.
- For acts and omissions of partners and agents they use to generate, retain, escrow, or destroy their private keys.
- To refrain from submitting to EBIZID or any EBIZID directory any material that contains statements that are libellous, defamatory, obscene, pornographic, abusive, bigoted, hateful, or racially offensive, advocate illegal activity or discuss illegal activities with the intent to commit them or may otherwise violate any law.

5.18 Representations by Subscriber upon Acceptance

Upon accepting a certificate the subscriber represents to EBIZID 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 unauthorized person has ever had access to the subscriber's private key.

All representations made by the subscriber to EBIZID 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 EBIZID of any material inaccuracies in such information.

The certificate is used exclusively for authorized and legal purposes, consistent with this CPS.

Use a EBIZID certificate only in conjunction with the entity named in the organization 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 unauthorized use.

The subscriber is an end-user subscriber and not a 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 a CA or otherwise, unless expressly agreed in writing between subscriber and EBIZID.

The subscriber agrees with the terms and conditions of this CPS and other agreements and policy statements of EBIZID.

Page 25 of 34

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 use goods as may be applicable.

5.19 Indemnity by Subscriber

By accepting a certificate, the subscriber agrees to indemnify and hold EBIZID, 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 EBIZID, 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 her 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, EBIZID, or any person receiving or relying on the certificate.

Failure to protect the subscriber's private key, to use a trustworthy system as required, or to take precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorised use of the subscriber's private key.

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

5.20 Obligations of EBIZID Registration Authorities and Local Registration Authorities

A EBIZID RA/LRA operating under the EBIZID network promises to:

Receive applications for EBIZID certificates in accordance with this EBIZID CPS.

Perform all verification actions prescribed by the EBIZID procedures and this CPS.

Receive, verify and relay to EBIZID all requests for revocation of a EBIZID certificate in accordance with the EBIZID procedures and the EBIZID CPS.

Act according to the Law and regulations.

5.21 Obligations of a Relying Party

A party relying on a EBIZID certificate promises to:

Have knowledge and if necessary request training on using digital certificates and PKI.

Study the limitations to the usage of digital certificates and the value of the transactions permitted.

Read and agree with the terms of the EBIZID CPS and relying party agreement or disclosure statement.

Verify a EBIZID certificate by using among others a CRL (including the EBIZID CRL) in accordance with the certificate path validation procedure.

Trust a EBIZID certificate only if all information featured on that can be verified it is correct and updated.

Rely on a EBIZID certificate, only as it may be reasonable under the circumstances.

5.22 Legality of Information

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

5.23 Subscriber Liability to Relying Parties

Without limiting other subscriber obligations stated in this 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.

5.24 Duty to Monitor Agents

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

5.25 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 EBIZID, and its agents and contractors.

5.26 Conditions of usage of the EBIZID Repository and Web site

Parties (including subscribers and relying parties) accessing the EBIZID Repository and web site agree with the provisions of this CPS and any other conditions of usage that EBIZID may make available except for information provided in or used for demo, free of price and test certificates. 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 information or services provided. Conditions of usage of the EBIZID Repositories include:

- Information provided as a result of the search for a digital certificate.
- Verification of the status of digital signatures created with a private key corresponding to a public key included in a certificate.
- Information published on the web site of EBIZID.
- Any other services that EBIZID might advertise or provide through its web site.

5.27 Reliance at Own Risk

It is the sole responsibility of the parties that access information featured in the EBIZID 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.

EBIZID shall take all steps necessary to update its records and directories on the status of the certificates.

5.28 Accuracy of Information

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

5.29 Failure to Comply

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

5.30 Obligations of EBIZID

To the extent specified in the relevant sections of the CPS, EBIZID promises to:

- Comply with this 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 EBIZID 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 CPS and fulfill its obligations presented herein.
- Upon receipt of a request from an RA operating within the EBIZID network act promptly to issue a EBIZID certificate in accordance with this EBIZID CPS.

Upon receipt of a request for revocation from an RA operating within the EBIZID network act promptly to revoke a EBIZID certificate in accordance with this EBIZID CPS.

- Publish accepted certificates in accordance with this CPS.
 - Provide support to subscribers and relying parties as described in this CPS.
 - Revoke certificates according to this CPS.
 - Provide for the expiration and renewal of certificates according to this CPS.
 - Comply with various provisions explained contained in this CPS.
 - Make available a copy of this 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 99/93.
 - 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 99/93.
- EBIZID acknowledges that it has no further obligations under this CPS.

5.31 Fitness for a Particular Purpose

EBIZID 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.

5.32 Other Warranties

Except as it may have otherwise been stated in relation to Qualified Certificates issued pursuant to the requirements of the European Directive 99/93 EBIZID 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 EBIZID except as it may be stated in the relevant product description below in this CPS and in the EBIZID insurance policy.

The accuracy, authenticity, completeness or fitness of any information contained in EBIZID 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 CPS.

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

Although EBIZID 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 EBIZID.

5.33 Non Verified Subscriber Information

Notwithstanding limitation warranties under the product section of this CPS, EBIZID shall not be responsible for non-verified subscriber information submitted to EBIZID, or the EBIZID 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 99/93.

5.34 Exclusion of Certain Elements of Damages

In no event (except for fraud or willful misconduct) shall EBIZID 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 CPS.

Any other damages except for those due to reliance, on the information featured on a certificate, on the verified information in a certificate, except for information featured on EBIZID Personal Sign 1, free, test or demo certificates.

Any liability incurred in this case or any other case if the fault in this verified information is due to fraud or willful 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 CPS.

Page 28 of 34

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 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.

5.35 Damage and Loss Limitations

In no event (except for fraud or willful misconduct) will the aggregate liability of EBIZID 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 EBIZID insurance plan below in this CPS.

5.36 Conflict of Rules

When this CPS conflicts with other rules, guidelines, or contracts, this 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 CPS.

Expressly superseding this CPS for which such contract shall govern as to the parties thereto, and to the extent permitted by law.

5.37 Intellectual Property Rights

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

5.38 Infringement and Other Damaging Material

EBIZID subscribers represent and warrant that when submitting to EBIZID 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, tortious 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 EBIZID harmless for any loss or damage resulting from any such interference or infringement.

5.39 Ownership

Certificates are property of EBIZID. EBIZID gives permission to reproduce and distribute certificates on a nonexclusive, royalty-free basis, provided that they are reproduced and distributed in full, except that certificates shall not be published in any publicly accessible repository or directory without the express written permission of EBIZID.

The scope of this restriction is also intended to protect subscribers against the unauthorised republication of their personal data featured on a certificate.

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

Secret shares of the EBIZID private key remain property of EBIZID.

5.40 Governing Law

This CPS is governed by, and construed in accordance with the laws of the United Kingdom. This choice of law is made to ensure uniform interpretation of this CPS, regardless of the place of residence or place of use of EBIZID digital certificates or other products and services. The law of

Page 29 of 34

UK applies in all EBIZID commercial or contractual relationships in which this CPS may apply or quoted implicitly or explicitly in relation to EBIZID products and services where EBIZID acts as a provider, supplier, beneficiary receiver or otherwise.

5.41 Jurisdiction

Each party, including EBIZID partners, subscribers and relying parties, irrevocably agrees that the District Court of Bradford, UK 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 CPS or the provision of EBIZID PKI services.

5.42 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 EBIZID of the dispute with a view to seek dispute resolution.

5.43 Successors and Assigns

This 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 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 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.

5.44 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 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 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.

5.45 Interpretation

This 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 CPS parties shall also take into account the international scope and application of the services and products of EBIZID and its international network of Registration and Local Registration Authorities as well as the principle of good faith as it is applied in commercial transactions.

The headings, subheadings, and other captions in this CPS are intended for convenience and reference only and shall not be used in interpreting, construing, or enforcing any of the provisions of this CPS.

Appendices and definitions to this CPS, are for all purposes an integral and binding part of the CPS.

5.46 No Waiver

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

Page 30 of 34

5.47 Notice

EBIZID 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 EBIZID 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:

EBIZID

EBIZID Ltd.

Attention: Legal Practices

Bradford, UK

Voice: + 44

Fax: + 44

Email: legal@EBIZID.com

5.48 Fees

EBIZID may charge subscriber fees for the use of EBIZID products and services as published on its web site. EBIZID retains its right to effect changes to such fees. Certificate fees are displayed on the official EBIZID websites.

5.49 Survival

The obligations and restrictions contained under sections entitled: *Audit, Confidential Information, Obligations of EBIZID, and Limitations upon Such Obligations, Indemnity by the Subscriber and Miscellaneous Provisions* survive the termination of this CPS.

Page 31 of 34

6 General Issuance Procedure

6.1 General

EBIZID certificates offer identity assurance also requiring personal presence before a registration authority for certain types of certificates issued to natural persons. For organizational certificates EBIZID requires corporate documentation to verify the identity of the applying organization.

EBIZID certificates are issued to natural persons (individuals) or legal persons.

The validity period of EBIZID certificates varies dependent on the certificate type, but typically a certificate will be valid for either 1 year, 2 years or 3 years.

6.2 Certificates issued to Individuals and Organizations

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 EBIZID. Additional documentation in support of the application may be required so that EBIZID verifies the identity of the applicant. The applicant submits to EBIZID such additional documentation. Upon verification of identity, EBIZID issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate to its device. The applicant must notify EBIZID 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.

6.3 Content

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

Applicant's e-mail address.

Applicant's name.

Applicant's public key.

Code of applicant's country.

Affiliate organization or liberal profession.

Issuing certification authority (EBIZID).

EBIZID digital signature.

Type of algorithm.

Validity period of the digital certificate.

Serial number of the digital certificate.

6.4 Submitted Documents to Identify the Applicant

In all cases, the applicant must submit to a EBIZID Registration Authority or Local Registration Authority a signed registration form, a signed subscriber agreement. Depending on the class of certificate the applicant must additionally submit proof of professional context and a copy of identity proof as indicated in the registration procedure.

For an employee it is required to submit an extract of the register of commerce or other similar third party confirmation of the status of its affiliated organization and confirmation by a legal representative of such organization.

For a self-employed person that works independently of an association or professional group an extract of the register of commerce or other similar third party confirmation is required in addition to the above-mentioned documents.

For self-employed persons belonging to an association or professional group an official document from the professional group and a member card is required in addition to the above-mentioned documents.

Page 32 of 34

EBIZID may prescribe additional identification proof in support of the verification of the identity of the applicant.

For organizational certificates the applicant must submit to a EBIZID Registration Authority a signed registration form, a signed subscriber agreement and any other documents as indicated on the on line registration form.

6.5 Time to Confirm Submitted Data

EBIZID makes reasonable efforts to confirm certificate application information and issue a digital certificate within reasonable time frames that may vary from one (1) to five (5) working days.

6.6 Issuing Procedure

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

- 1 The applicant fills out the online request on EBIZID's web site.
- 2 The applicant submits the required information.
- 3 The applicant submits the required information: Certificate Signing Request (CSR), e-mail address, common name, organizational information, country code, verification method, billing information.
- 4 The applicant accepts the on line subscriber agreement.
- 5 The applicant pays the certificate fees.
- 5 The online request are sent to EBIZID automatically.
- 6 EBIZID verifies the submitted information using third party databases and Government records
- 8 EBIZID may issue the certificate to the applicant.
- 9 EBIZID publishes the issued certificate in on line database.
- 10 Renewal: allowed.
- 11 Revocation: allowed.

6.7 Insurance

Except to the extent of willful misconduct, the cumulative maximum liability accepted by EBIZID 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.

EBIZID SSL Certificates: The cumulative liability of EBIZID to applicants, subscribers and relying parties shall not exceed \$50.00 (fifty US dollars).

EBIZID Select Certificates: The cumulative liability of EBIZID to applicants, subscribers and relying parties shall not exceed \$2500.00 (two thousand five hundred US dollars).

Super SSL Certificates: The cumulative liability of EBIZID to applicants, subscribers and relying parties shall not exceed \$10,000.00 (ten thousand US dollars).

Intranet SSL Certificate: There is no liability of EBIZID to applicants, subscribers and relying parties.

Trial SSL Certificate: There is no liability of EBIZID to applicants, subscribers and relying parties.

Page 33 of 34 Page 34 of 34

A Document Control and References

EBIZID	24613 Powers Dearborn Heights Michigan, 48125
URL: http://www.EBIZID.com E-mail: legal@EBIZID.com	Phone: +1-313-299-0593 Facsimile: +1-443-337-0305

Copyright Notice

Copyright . EBIZID 2002. All rights reserved.

No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photocopying, recording or otherwise) without prior written permission of EBIZID.

Requests for any other permission to reproduce this EBIZID document (as well as requests for copies from EBIZID) must be addressed to:

EBIZID

24613 Powers Dearborn Heights Michigan, 48125

E-mail: legal@EBIZID.com

The trademarks "EBIZID" are registered trademarks of EBIZID Limited.

Changes forecast

No changes foreseen.