Micros

Certification Practices Statement

Version 2.1.1

Effective Date: July 14, 2010

Micros

Certification Practices Statement

Published date: July 14, 2010

Trademark Notices

MICROS Systems, Inc.
Attn: Jim Walsh, CISO
7031 Columbia Gateway Dr.
Columbia, MD 21046
443-285-6087
jwalsh@Micros.com

Table of Contents

Revision History

Changes	Approving Manager(s)	Date
Ver. 2.1.0 - Initial Publication	Director of Infrastructure Manager Network Services	Mar 30, 2010
Ver. 2.1.1	Micros Counsel	July 14, 2010

1. INTRODUCTION

This document is Micros (hereinafter "Micros") Certification Practices Statement ("CPS") which details the following information:

- the practices, procedures, and infrastructure employed by Micros Certification Authority ("CA") for its operations and business continuity,
- the practices and procedures employed in the creation, management, and termination of our Root CA Keys,
- the practices and procedures that apply generally to all End-Entity Certificates issued by our CA,
- the physical, environmental, and logical security controls employed by Micros to protect our Root CA Certificates, and
- the legal structure of the relationship between Micros, Subscribers (End-Entities), and Relying Parties.

Micros provides certification services for a number of different types of End-Entity Certificates, each of which may have differing uses and purposes which necessitate different processes and procedures employed during the vetting process and the overall Certificate lifecycle. The digital Certificate lifecycle includes public and private key generation, the vetting of the information contained within the Certificate by the CA, the CA signing of the Certificate, the implementation and use of the digital Certificate, and finally, the termination of use of the digital Certificate. The processes and procedures used for the different Certificate types are also detailed in the relevant sections within this document.

In summary, this CPS focuses on the overall CA operations and Root CA Key policies and procedures while also focusing on the policies and procedures surrounding End-Entity Certificates. This CPS, together with documents incorporated by reference, constitutes the entirety of the obligations, representations, warranties, policies, and procedures that apply to a digital Certificate issued by Micros. In the event that there is a discrepancy between the following procedures and the CA/Browser Forum Guidelines, the CA/Browser Forum Guidelines will supersede the procedures detailed below.

1.1 Overview

Micros operates and maintains one globally trusted Root CA key pair identified by the following names:

- **Micros Certification Authority** ("CCA") The CCA is signed by Trustwave Holdings, Inc.

This CPS governs the operation and maintenance of and is applicable to the above-listed Root CA Keys. In addition, Micros maintains one subordinate certification authority immediately subordinate to this Root CA:

- **Micros Internal SSL Certification Authority** ("MISCA"). This CA only issues Certificates for Micros employees' and customers' internal SSL communications.

Micros certification authorities enumerated above are collectively known as the "Micros Public Key Infrastructure Hierarchy" ("MPH"). All activities of the MPH listed above, and the Certificate policies associated with the Certificates that these CA's issue, are defined and governed by this document.

In addition, the entirety of the MPH as explained above, the practices associated with this certification authority, and of Certificates issued by the certification authorities within the MPH are delimited within this document. However, since the root certification authority within the MPH is signed by Trustwave Holdings, Inc., additional governance and requirements for all certification authorities underneath and including CCA are defined and contained within the current Certification Practices Statement of Trustwave Holdings, Inc ("Trustwave"). Consequently, the use, issuance, governance, maintenance, and revocation of Certificates issued from the CCA and its subordinate certification authorities shall comply with the Trustwave CPS.

Micros issues the following Certificate types, which can be identified by the Certificate Policy Object Identifier ("OID" or "CP OID") contained within the End-Entity Certificate:

- End-Entity Internal SSL Certificates
  CP OID: 1.3.6.1.4.1.35539.3.3.3.3.4.3.3

All Certificates issued by Micros will contain a CP OID so that End-Entities and Relying Parties can identify the type of Certificate and the policies and procedures that were followed in the Certificate lifecycle including the vetting processes used prior to the issuance and the intended purposes of the Certificate.

All of the CPs are contained within this CPS. This shall be published at https://ssl.trustwave.com/CA/Micros

1.2 Document Name and Identification

This document is Micros Certification Practices Statement. All Micros Certificates contain a CP OID corresponding to the applicable Certificate type (See Section 1.1). Because this CPS is incorporated within all CP's, this CPS does not have a unique OID associated with it. This CPS contains the relevant CP's.

1.3 PKI Participants

1.3.1 Certification Authorities

The only Certification Authority specifically governed by this document is Micros.

1.3.2 Registration Authorities

A Registration Authority ("RA") is an entity that performs identification and authentication of Certificate applicants for End-Entity Certificates. An RA may vet subscribers, initiate or pass along Certificate requests, and approve or pass along other Certificate lifecycle actions including renewals, re-keys, and revocations. Micros may act as an RA for Certificates it issues.

Micros shall not, without written consent from Trustwave, enter into agreements with third parties to operate as an RA under this CPS.

1.3.3 Subscribers

Subscribers are the end entities that hold Certificates issued by Micros. Subscribers are sometimes also referred to as Applicants prior to the issuance of a Certificate. The context in which either term is used will invoke the correct understanding.

All subscribers within the MPH shall be:

- Employees, vendors, customers or contractors of Micros
- Computing devices wholly owned, controlled, and managed by Micros or Micros Customers

1.3.4 Relying Parties

A Relying Party is any individual or entity that relies on the information contained within a Certificate issued by Micros to perform an act. An example of such an act would be an individual who relies upon the information contained within a Certificate when making a connection to a secure web site to confirm that the web site owner is, in fact, who he, she, or it claims to be. A Relying Party may also be a Subscriber.

1.3.5 Other Participants

The three main participants in a PKI are the CA, Subscribers, and Relying Parties. However, a device can also have a Certificate associated with it that is not connected to a specific entity or individual. In cases where a device, such as a firewall, a router, or a server has a Certificate, the Relying Party should refer to the appropriate Certificate Policy embedded in that specific Certificate to determine the purpose, usefulness, and policies that apply.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Please refer to the CP identified by the CP OID embedded within the Certificate to determine the appropriate uses of the particular Certificate in question.

1.4.2 Prohibited Certificate Uses

Certificates issued by Micros shall be used only to the extent that the use is consistent with this Micros CPS, applicable law, including without limitation, applicable export or import laws.

Micros Certificates are not designed, intended, or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, or weapon control systems, where failure could lead directly to death, personal injury, or severe environmental damage.

Please refer to the CP identified by the CP OID embedded within the Certificate for further information regarding uses of Certificates prohibited by that particular Certificate type. Certificates may only be used for the purpose specifically stated in the applicable CP.

Micros occasionally re-keys subordinate CAs, and Subscribers may re-key their Certificates upon their request. Third party applications or platforms may not operate as designed or intended after a re-key. It is the sole obligation of the Subscriber to make any modifications necessary and/or perform any required testing to assure a Certificate will continue to work as intended upon a re-key. Micros does not warrant any use of subordinate CAs as root Certificates. If Micros determines that it is necessary or appropriate to re-key a subordinate CA, notice to do so will be provided to Subscribers at least 30 days in advance of a re-key occurring. Upon a re-key event, Subscribers must cease reliance upon the old keys. Micros shall not warrant any actions or activities by Subscribers based upon the previous keys following a re-key event of a CA.

1.5 Policy Administration

1.5.1 Organization Administering the Document

MICROS Systems, Inc.
7031 Columbia Gateway Dr.
Columbia, MD 21046

1.5.2 Contact Persons

Jim Walsh, CISO

1.5.3 Persons Determining CPS and CP Suitability for the Policy

Jim Walsh, CISO
443-285-6087
jwalsh@Micros.com

1.5.4 CPS and CP Approval Procedures

All changes and revisions to this CPS and the related CPs shall be approved by those person identified in section 1.5.3, as well as Trustwave's Certification Practice Board. All amendments and updates shall be posted in Micros' repository located https://ssl.trustwave.com/CA/micros.

1.6 Definitions and Acronyms

Activation Data: Data (other than keys) required for operating hardware or software cryptographic modules. Examples include personal identification numbers (PINs), passwords, and pass phrases.

Authentication: The process of establishing identity based on the possession of a trusted credential.

Certificate: A public key certificate.

Certificate Approver: A Certificate Approver is a natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant to (i) act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester, and (ii) to approve Certificate Requests submitted by other Certificate Requesters.

Certification Authority: An entity which issues, manages, revokes, and renews Certificates.

Certificate Policy (CP): 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" [X509].

Certification Practices Statement (CPS): A statement of the practices which a Certification Authority employs in issuing and managing Certificates. The Trustwave CPS, which governs the Trustwave's Public Key Hierarchy, may be found at https://ssl.trustwave.com/CA

Certificate Revocation List (CRL): A list of Certificates previously issued by the subject CA that have been subsequently compromised or otherwise invalidated.

Compromise: Suspected or actual unauthorized disclosure, loss, loss of control or use of a Private Key associated with Certificate.

Contract Signer: A Contract Signer is a natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to sign Subscriber Agreements and other related agreements.

Cross-Certificate: A Certificate issued by the subject CA certifying the public key of another CA.

Data Integrity: Cryptographically secure assurance that no change has occurred in a document, message, data file, or data transmission.

Decryption Private Key: A private key used to decrypt data or session keys encrypted by the corresponding public key. In the context of this document, the public key is presumed to be contained and conveyed by an encryption Certificate.

Distinguished Name: A distinguished name is the concatenation of selected attributes from each entry, called the *relative distinguished name* (RDN), in the X.500 directory tree along a path leading from the root of the X.500 namespace down to the named entry.

FMS Community: The US Department of Treasury, Financial Management Service (FMS), or any person or organization operating under the authority and direction of the FMS, either directly or through a contractual relationship.

Domain (of a CA): The scope of authority of a CA, generally limited to RAs and End-Entities registered with or certified by the CA.

Encryption Certificate: A Certificate containing and conveying a public key used to encrypt electronic messages, files, documents, data transmissions, etc., or to establish a session key for those purposes.

End-Entity (EE): A person, computer system, or a communications device that is a subject or user of a Certificate, but is not a CA or RA. An End-Entity is a Subscriber, a Relying Party, or both.

Entity: A CA, RA, or End-Entity.

Identity Certificate: A Certificate issued for the purpose of binding the identity of the subject (as stated in the Certificate) to a public key issued to that subject. In X.509 Certificates, the identity of the subject is equivalent to the Distinguished Name of the subject.

Intersite Trust Agreement: An agreement between sites for allowing cross-site use of Certificates.

Key: A value supplied to a cryptographic algorithm to encrypt or decrypt data.

Key Materials: A tangible representation of a key. Examples include a key stored in computer memory, computer disk, smart card, or other key carrier.

PKI: See Public Key Infrastructure.

Place of Business: An entity's principal place of business, a satellite office, or a regional office.

Private Key: The portion of a public-private key pair known only to the holder.

Public Key: The portion of a public-private key pair that may be publicly known or distributed without reducing the security of the cryptography system. In the context of this Policy, Public Keys (after initial issuance) are always distributed through the use of Public Key Certificates.

Public Key Algorithm: A cryptographic algorithm in which the encryption and decryption functions are divided between a pair of mathematically related keys. In some common Public Key Algorithms (e.g., RSA), the encryption/decryption functions are reciprocal, i.e., either key of the pair can be used to encrypt or decrypt, with the other key able to decrypt or encrypt respectively.

Public Key Certificate: The public key portion of a public-private key pair that has been digitally signed by a CA, thereby certifying the validity and data integrity of the Public Key contained in the Certificate, in accordance with the applicable Certificate Policy.

Public Key Infrastructure (PKI): A system for using public key cryptography and providing a trusted mechanism for distributing and managing public keys through the appropriate use of Certificates.

Qualified Government Agency Source: A regularly-updated and current online 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 they are maintained by a government entity.

Qualified Government Information Source ("QGIS"): A regularly updated and current publicly available source which is 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 they are maintained by a government entity.

Qualified Government Tax Information Source ("QGTIS"): A QGIS that specifically contains tax information, e.g., the I.R.S. in the United States.

Qualified Independent Information Source ("QIIS"): 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. A commercial database is a QIIS if the following are true: (i) data it contains that will be relied upon has been independently verified by other independent information sources; (ii) the database distinguishes between self-reported data and data reported by independent information sources; (iii) the database provider identifies how frequently they update the information in their database; (iv) changes in the data that will be relied upon will be reflected in the database in no more than twelve (12) months; and (v) the database provider uses authoritative sources independent of the subject, or multiple corroborated sources, to which the data pertains.

Registration Authority (RA): A person or other entity operating under the authority of a CA that is responsible for identification and authentication of Certificate subjects and other duties as assigned in the site CPS.

Registration Number. The unique number or code assigned to an entity after its application for registration to do business in a particular jurisdiction is approved.

Registered Office. An entity's physical address identified in its application for registration to do business in a particular jurisdiction or its principal place of business.

Relying Party: Any user or recipient of a Certificate that acts in reliance on that Certificate. In this document, the terms "Certificate user" and "Relying Party" are used interchangeably.

Session Key: A key, typically for a symmetric algorithm, established between communicating parties for subsequent encryption/decryption of electronic messages, files, documents, data transmissions, etc. Its use is generally limited to that purpose and a single transaction or session.

Signing Private Key: A private key used to create digital signatures.

Sponsor: A person or organization with which the Subscriber is affiliated (e.g., as an employee, user of service, or customer).

Subject End-Entity: An End-Entity that is the subject of a Certificate.

Subscriber: A person or entity who is the subject named or identified in a Certificate issued to such person or entity, holds a Private Key that corresponds to a Public Key listed in that Certificate, and the person or entity to whom digitally signed messages verified by reference to such Certificate are to be attributed.

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.

Symmetric Algorithm: A cryptographic algorithm in which data is encrypted and decrypted using the same key.

Validity Period. A Certificate's period of validity. It typically begins on the date the Certificate is issued (or such later date as specified in the Certificate), and ends on the date and time it expires as noted in the Certificate unless the Certificate is revoked before its expiration.

Verified Accountant Letter: A letter signed by a duly licensed accountant, with active status, whereby the accountant attests to the existence, validity and accuracy of the entity's legal existence, name and/or assumed names under which Applicant conducts business and that such is current and duly registered in the appropriate jurisdiction.

Verified Legal Opinion: A letter signed by an attorney, with active status, licensed to practice law in the country of Applicant's jurisdiction of incorporation or registration or any jurisdiction where Applicant maintains an office or physical facility whereby the attorney attests to the existence, validity and accuracy of the entity's legal existence, name and/or assumed names under which Applicant conducts business and that such is current and duly registered in the appropriate jurisdiction.

ABBREVIATIONS

MPH	Micros Public-Key Hierarchy
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practices Statement
CRL	Certificate Revocation List
FQDN	Fully Qualified Domain Name
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
IEC	International Electro-technical Commission
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International Organization for Standardization
ITU	International Telecommunications Union
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure - X.509 (IETF Working Group)
RA	Registration Authority
RFC	Request for Comments
RSA	Rivest-Shamir-Adelman Encryption Algorithm
TPH	Trustwave Public Key Hierarchy
TW	Trustwave Holdings, Inc.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

Trustwave, on behalf of Micros, maintains three separate Repositories:

1. **Certificate Repository.** Digital Certificates that are issued to End-Entities are stored on non-public file systems and in internal directories at Trustwave.

2. **Document Repository.** Legal documents, including this CPS, associated CP's, Subscriber Agreements, Relying Party Agreements, and other documents related to Micros Certificate services are publicly available at the following URL: https://ssl.trustwave.com/CA/Micros.
3. **Certificate Status Information Repository.** Certificate status information is available through a publicly published Certificate Revocation List ("CRL") and/or other online Certificate status protocols. Every Certificate issued from any of the CA Certificates governed by this CPS will contain information within the Certificate that will identify the location where Certificate status information can be found.

2.2 Publication of Certificate Information

Trustwave, on behalf of Micros, will maintain and publish a current version of this CPS, including its associated CP's, Subscriber Agreements, Relying Party Agreements, and all other relevant legal documents at the following URL: https://ssl.trustwave.com/CA/Micros/. The repositories allow Relying Parties and others to view Certificate status information, including without limitation, a Certificate's revocation status. Micros shall ensure and deliver to Trustwave a current copy of all documentation and agreements related to the MPH.

Certificate status information is provided in accordance with the CP identified in each End-Entity Certificate.

2.3 Time or Frequency of Publication

Updates to this CPS and the associated CPs are approved and published as set forth in Section 9.12 herein. Subscriber Agreements and Relying Party Agreements are published as necessary. Certificates are published when issued. Certificate status information is published in accordance with the CP identified in each End-Entity Certificate. CRL information shall be generated and published on a daily basis.

2.4 Access Controls on Repositories

Information published in the Document Repository and Certificate Status Information Repository is available on a read-only basis. Information contained in the Certificate Repository is available to the End-Entity who owns the Certificate as well as Micros and Trustwave staff. Micros and Trustwave have physical and logical security controls in place to prevent unauthorized persons from adding, deleting, or modifying the information contained within its repositories.

3. IDENTIFICATION AND AUTHENTICATION

In the event that there is a discrepancy between the following procedures and the CA/Browser Forum Guidelines, the CA/Browser Forum Guidelines will supersede the procedures detailed below.

3.1 Naming

3.1.1 Types of Names

All Certificates issued by Micros certification authorities shall be in the form of and will comply with the ISO/ITU X.500 naming convention. All Certificates will have the subject field (subject alternative name) of the Distinguished Name set as per the following:

MISCA Internal SSL Certificates	The subject in the Internal SSL shall include the following: 1) The commonName (CN) component shall include the subject's full Micros internal network domain name or address. 2) The organization component shall contain 'Micros Corp.'. 3) The city, state and Locality fields shall include the address identifiers for Micros Corp.

3.1.2 Need for Names to be Meaningful

The subject field within the Certificates of each of the MPH participants defined in section 1.1 shall uniquely identify each of Micros capabilities in a human readable format. Additionally:

MISCA Internal SSL Certificates	Micros ensures via the practices and procedures as defined within this document, and in 3.2.2, that the subject name uniquely identifies the common name of the Subscriber as described by a Micros internal network address or domain name.

3.1.3 Anonymity or Pseudonymity of Subscribers

Anonymous or pseudonymous Certificates shall not be issued by Micros Certification Authorities.

3.1.4 Rules for Interpreting Various Name Forms

Name forms within Micros Certification Authority Certificates and Micros issued End- Entity Certificates shall adhere to the ISO/ITU X.500 series naming standards.

3.1.5 Uniqueness of Names

The uniqueness of names within Micros-issued Certificates shall be determined as per the following:

MISCA Internal SSL Certificates	The subject of all Internal SSL Certificates issued by Micros shall be unique.

3.1.6 Recognition, Authentication, and Role of Trademarks

Micros and Trustwave do not determine the validity or rights of a Subscriber or Applicant to use any name, trademarks, trade names, domain names, service marks, or other marks ("marks"). Applicants and Subscribers shall not use other parties' marks in their Certificate applications, Subscriber Agreement or other related documentation. Micros and Trustwave may each, within their sole discretion, reject or suspend a Certificate application due to potential trademark infringement.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

All End-Entity Applicants within the MPH shall submit a digitally signed PKCS#10 CSR to establish that it holds the private key corresponding to the public key to be included in a Certificate. Trustwave, on behalf of Micros, shall verify that the CSR's signature was created by the private key associated with the public key in the CSR.

3.2.2 Authentication of Organization Identity

MISCA Internal SSL Certificates	Micros will determine that an Applicant is an employee, customer or contractor of the organization through correlation with Human Resources and/or contractor records and/or Micros Internal Customer Identifying Systems, prior to enrollment in the program. Furthermore, Micros shall ensure that all employees customers, contractors, vendors and any other entity issued a certificate shall execute a confidentiality agreement wherein, he or she agrees to maintain all Micros and Trustwave proprietary data, including without limitation all non-public information regarding the TPH and the MPH.

3.2.3 Authentication of Individual Identity

MISCA Internal SSL Certificates	Micros shall take all steps reasonably necessary to determine and confirm the validity of the employee, customers, contractor, or other Applicant's internal domain name or address. Micros shall verify the Applicant's identity and domain name or address through correlation and documented confirmation from Micros's Human Resources Department records and/or Micros Internal Customer Identifying Systems and/or contractor records prior to the issuance of such Applicant's Certificate.

3.2.4 Non-Verified Subscriber Information

All information contained within Certificates issued by Micros will be verified, except as it may have otherwise been stated in section 3.2.3 for MISCA Internal SSL Certificates or in relation to Qualified Certificates issued pursuant to the requirements of the European Directive 99/93.

3.2.5 Validation of Authority

No stipulation.

3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

Prior to the expiration of an existing Subscriber's Certificate, it may be necessary for the Subscriber to obtain a new Certificate to maintain continuity of Certificate usage. This process is defined as Certificate Re-key. Subscribers shall generate a new Key Pair to replace the expiring Key Pair. For purposes of this CPS, and for all Certificates issued within the MPH, Renewal Certificate Applications are subject to the same authentication steps outlined in this CPS as they apply to initial issuance of a Certificate. Expiring Certificates are not revoked by Micros upon issuance of the renewal Certificate. The Subscriber shall pay any fees and comply with the other terms and conditions for renewal as presented on Micros's web site.

3.3.2 Identification and Authentication for Re-key after Revocation

There is no Re-key after revocation. After revocation, a Subscriber shall submit a new Application.

3.4 Identification and Authentication for Revocation Request

3.4.1 Circumstances For Revocation

Certificate revocation is the process by which Micros or Trustwave prematurely ends the Validity Period of any Certificate by posting the serial number of the Certificate to a Certificate Revocation List. Micros will revoke a Certificate when any of the following events set forth in section 4.9.1 occur.

3.4.2 Who Can Request Revocation

The only persons permitted to request revocation of a Certificate issued by Micros is the Subscriber, which includes its designated representatives, and those persons designated by Micros in section 1.5.3:

Trustwave is granted by Micros the right to unilaterally revoke any certificate issued within the MPH; and Trustwave reserves the right to unilaterally revoke any certificate issued within the MPH.

3.4.3 Procedure For Revocation Request

See section 4.9.3.

4. CERTIFICATE LIFECYCLE OPERATIONAL REQUIREMENTS

This CPS includes operational aspects of Micros Certification Authority that pertain to all types of Certificates issued from the Root CA Certificates governed by this CPS.

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Applications can be submitted by the individuals set forth below who comply with the provisions specified in the registration form, CP/CPS and relevant End-User Agreements.

MISCA Internal SSL Certificates	Applications for Internal SSL shall only be requested by an employee, a full-time contractor, a customer or a vendor of Micros.

4.1.2 Enrollment Process and Responsibilities

MISCA Internal SSL	The primary steps for a Certificate registration are: 1. Valid identification documentation is provided as set forth in section 3.2.3 and complete registration forms have been accepted by the Applicant 2. The CP's/CPS and End-User Agreement have been accepted by the Applicant; and 3. All documents and information provided by Applicant are approved by Micros.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

MISCA Internal SSL	Before issuing a Certificate, Micros shall ensure that all Subject organization information in the Certificate conforms to the requirements of, and has been verified in accordance with, the provisions as set forth in Micros CPS and matches the information confirmed and documented by Micros pursuant to the verification processes. The verification process shall accomplish: Verification and authentication of Applicant's existence and legal identity. **Maximum Validity Period for Validated Data** The age of validated data used to support issuance of a Certificate (before revalidation is required) shall not exceed the following limits: (1) Legal existence and identity – 13 months;

	(2) Assumed name – 13 months; **Note on Reuse and Updating Information and Documentation** (a) Use of Documentation to Support Multiple Certificates Micros may issue multiple Certificates listing the same Subject and based on a single Certificate Request, subject to the aging and updating requirement in (b) below. (b) Use of Pre-Existing Information or Documentation (1) Each Certificate issued by Micros must be supported by a valid current Certificate Request and a Subscriber Agreement signed by the appropriate Applicant Representative on behalf of Applicant. (2) The age of information used by Micros to verify such an Certificate Request shall not exceed the Maximum Validity Period, as defined above, for such, based on the earlier of the date the information was obtained or the date the information was last updated by the source (e.g., if an online database was accessed by Micros on July 1, but contained data last updated by the vendor on February 1, then the date of information would be considered to be February 1). (3) In the case of outdated information, Micros shall repeat the verification processes required in this CPS.

4.2.2 Approval or Rejection of Certificate Applications

The approval or rejection of a Certificate request is made following completion of all requirements in 4.2.1. An approval requires that Micros be in good payment standing.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

Following successful completion of all relevant sections within 3.1 and 4.2, Micros will approve the Certificate application and issue the Subscriber's Certificate.

4.3.2 CA Actions for Non-Latin Organization Name Encoding

No Stipulation.

4.3.3 Notification to Subscriber by the CA of Issuance of Certificate

Micros shall notify the Applicant that the Certificate has been issued via e-mail, telephone, or face-to-face contact. Once the Applicant has been notified, the Subscriber will either download the Certificate over HTTPS, or receive the Certificate via e-mail.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The Subscriber expressly indicates acceptance of a Certificate by using such Certificate or downloading and installing the Certificate.

4.4.2 Publication of the Certificate by the CA

Due to privacy concerns, Micros does not publish End-Entity Certificates in any form of a global directory.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers, for all forms of Micros issued digital Certificates, shall

- possess at least a rudimentary knowledge of public key cryptography and digital Certificates;
- have completed all necessary enrollment forms;
- read and agree to this CPS, any and all relevant CPs, and any and all Subscriber Agreements;
- protect their private key from unauthorized access and Compromise;
- not share their private key and or passwords protecting their private key;
- notify Micros of any change to the information contained within the Certificate;
- comply with all laws and regulations applicable to the export, import, and use of cryptography with Certificates issued by Micros.

4.5.2 Relying Party Public Key and Certificate Usage

Relying Parties shall:

- possess at least a rudimentary knowledge of public key cryptography and digital Certificates and their associated risks;
- read and agree to this CPS, any and all relevant CPs, and any and all Relying Party Agreements;
- verify, prior to using and relying on a Certificate, its validity by using CRLs (or OCSP) with correct certification path validation procedures and all critical extensions;
- comply with all laws and regulations applicable to the export, import, use and reliance on a Certificate issued by Micros.

4.6 Certificate Renewal

Certificate renewal involves a process whereby the Subscriber retains the key pair used within a previously issued Certificate, but submits updated or current identity and/or validity information. Neither Micros root CAs, nor any member CA of the MPH, shall support Certificate renewal. Micros shall support only certificate re-key as defined in 4.7

4.6.1 Circumstance for Certificate Renewal

No stipulation.

4.6.2 Who May Request Renewal

No stipulation.

4.6.3 Processing Certificate Renewal Requests

No stipulation.

4.6.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

No stipulation.

4.6.6 Publication of the Renewal Certificate by the CA

No stipulation.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.7 Certificate Re-key

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to obtain a new Certificate to maintain continuity of Certificate usage. This process is defined as Certificate Re-key. Subscribers shall always generate a new key pair to replace the expiring key pair. For purposes of this CPS, Re-key Certificate Applications are subject to the same authentication steps outlined in this CPS as apply to initial issuance of a Certificate. Expiring Certificates are not revoked by Micros upon issuance of the new Certificate. The Subscriber shall comply with the other terms and conditions for renewal as presented by Micros, including those defined within this, Micros CPS.

4.7.1 Circumstance for Certificate Re-key

No stipulation.

4.7.2 Who May Request Certification (Signing) of a New Public Key

No stipulation.

4.7.3 Processing Certificate Re-keying Requests

No stipulation.

4.7.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

No stipulation.

4.7.6 Publication of the Re-keyed Certificate by the CA

No stipulation.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.8 Certificate Modification

Certificate modification is the process through which a Subscriber requests a Certificate with modified subject information. Micros shall deem such request as an initial registration request. The Subscriber is therefore required to start a new Certificate request.

4.8.1 Circumstance for Certificate Modification

No stipulation.

4.8.2 Who May Request Certificate Modification

No stipulation.

4.8.3 Processing Certificate Modification Requests

No stipulation.

4.8.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

No stipulation.

4.8.6 Publication of the Modified Certificate by the CA

No stipulation.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

Certificate revocation is the process by which Micros prematurely terminates the Validity Period of a Certificate by posting the serial number of the Certificate to a Certificate Revocation List. Micros and/or Trustwave will revoke the Certificate when any of the following events occurs:

(1) The Subscriber requests revocation of its Certificate;
(2) The Subscriber indicates that the original Certificate Request was not authorized and does not retroactively grant authorization;
(3) Micros or Trustwave obtains reasonable evidence that the Subscriber's Private Key (corresponding to the Public Key in the Certificate) has been Compromised, or that the Certificate has otherwise been misused;
(4) Micros or Trustwave receives notice or otherwise becomes aware that a Subscriber violates any of its material obligations under the Subscriber Agreement;
(5) Micros receives notice or otherwise becomes aware that a court or arbitrator has revoked a Subscriber's right to use the domain name listed in the Certificate, or that the Subscriber has failed to renew the domain name;
(6) Micros or Trustwave receives notice or otherwise becomes aware of a material change in the information contained in the Certificate;
(7) A determination, in Micros's or Trustwave's discretion, that the Certificate was not issued in accordance with the terms and conditions of this CPS or the applicable CP;

(8) Micros or Trustwave determines that any of the information appearing in the Certificate is not accurate;
(9) Micros ceases operations for any reason and has not arranged for another CA to provide revocation support for the Certificate;
(10) The Private Key for that Certificate has been compromised;
(12) Micros or Trustwave receives notice or otherwise becomes aware that a Subscriber has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination under the laws of Micros's jurisdiction of operation.
(13) The Subscriber's employment and/or contractual relationship with Micros is terminated or expires. In the case of a Subscriber that is a device, the Certificate shall be revoked if Micros ceases management, ownership, and/or control of such device.

4.9.2 Who Can Request Revocation

The only persons permitted to request revocation of a Certificate issued by Micros is the Subscriber (including designated representatives; Certificate Approver, Contract Signer).

In addition, Micros reserves the right to unilaterally revoke any certificate without cause.

4.9.3 Procedure for Revocation Request

To request revocation, a Subscriber shall contact Micros or Trustwave, either by e-mail message, a national/regional postal service, facsimile, or overnight courier, and specifically request "revocation" (using that term) of a particular Certificate identified by the Subscriber. Upon receipt of a revocation request, Micros will seek confirmation of the request by e-mail message to the person requesting revocation (as defined in 4.9.2 above). The message will state that, upon confirmation of the revocation request, Micros shall revoke the Certificate and that posting the revocation to the appropriate CRL shall constitute notice to the Subscriber that the Certificate has been revoked. Micros shall require a confirming e-mail message back from either the administrative or technical contact authorizing revocation (or by other means of confirmation acceptable to Micros). Upon receipt of the confirming e-mail message, Micros shall revoke the Certificate and the revocation shall be posted to the appropriate CRL. Notification shall be sent to the subject of the Certificate and the subject's designated contacts. There is no grace period available to the Subscriber prior to revocation, and Micros shall respond to the revocation request within the next business day and post the revocation to the next published CRL. In the event of Compromise of Micros's Private Key used to sign a Certificate, Micros shall send an e-mail message as soon as practicable to all Subscribers with Certificates issued off the Private Key stating that the Certificates shall be revoked by the next business day and that posting the revocation to the appropriate CRL shall constitute notice to the Subscriber that the Certificate has been revoked.

4.9.4 Revocation Request Grace Period

See 4.9.3

4.9.5 Time within Which CA Must Process the Revocation Request

See 4.9.3

4.9.6 Revocation Checking Requirement for Relying Parties

No stipulation.

4.9.7 CRL Issuance Frequency

CRL's shall be issued by all certification authorities within the MPH on a daily basis.

4.9.8 Maximum Latency for CRLs

As per 4.9.7, all CRLs issued by certification authorities within the MPH shall be issued on a daily basis and without delay. The maximum latency for any CRL within the MPH shall be one day.

4.9.9 On-line Revocation/Status Checking Availability

No stipulation.

4.9.10 On-line Revocation Checking Requirements

No stipulation.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements Regarding Key Compromise

No stipulation.

4.9.13 Circumstances for Suspension

No certification authority within the MPH shall suspend Certificates.

4.9.14 Who Can Request Suspension

No stipulation. See 4.9.13

4.9.15 Procedure for Suspension Request

No stipulation. See 4.9.13

4.9.16 Limits on Suspension Period

No stipulation. See 4.9.13

4.10 Certificate Status Services

No stipulation. Currently, Micros does not provide OCSP services.

4.10.1 Operational Characteristics

No stipulation.

4.10.2 Service Availability

No stipulation.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

Micros shall attempt to notify all Subscribers of the expiration date of their Certificate. Notifications will generally be by e-mail message to the administrative / Certificate Requester

contacts listed during enrollment submitted by the Certificate Requester, and will likely occur periodically during the 90 day period prior to the expiration date and the 14 day period following the expiration date. If the Subscriber's enrollment form was submitted by another party on the Subscriber's behalf, Micros may not send expiration notices to that party. Micros is not responsible for ensuring that the customer is notifed prior to the expiration of their Certificate.

4.12 Key Escrow and Recovery

Micros does not provide nor perform any form of key escrow or recovery services.
No certification authority within the MPH shall escrow their private keys.

4.12.1 Key Escrow and Recovery Policy and Practices

No stipulation.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

All computing devices and corresponding processes associated with the management, operation, and physical housing of Micros's public key infrastructure are within the confines of Trustwave Holdings, Inc.

5.1 Physical Controls

5.1.1 Site Location and Construction

Trustwave CA operations are conducted within a physically secure environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems whether covert or overt.

Trustwave maintains "cold" disaster recovery systems at a geographically separate facility for its CA operations. The systems do not contain key material and are kept off-line and are stored in a physically secure manner. The disaster recovery procedures are detailed further in Section 5.7.

5.1.2 Physical Access

Physical Access is restricted to the secure server room. The room can only be accessed through dual-access controls which require that two persons be present and utilize two distinct methods of access consisting of a combination of PIN numbers, proximity cards, and Keys. The system has been designed so that entry by a single individual is not possible.

5.1.3 Power and Air Conditioning

Trustwave's facility is equipped with primary and backup:

- power systems to ensure the operation of its servers and its network connections; and
- HVAC systems to control temperature and relative humidity.

5.1.4 Water Exposures

Trustwave has taken reasonable precautions to minimize the impact of water exposure to its systems.

5.1.5 Fire Prevention and Protection

Trustwave has taken reasonable precautions to prevent fires and has fire suppression equipment available on-site.

5.1.6 Media Storage

All media containing production software and data, audit, archive, or backup information is stored within Trustwave facilities or in a secure off-site storage facility with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage (e.g., water, fire, and electromagnetic).

5.1.7 Waste Disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or zeroed in accordance with the manufacturer's guidance prior to

disposal. Other waste is disposed of in accordance with Micros's normal waste disposal requirements.

5.1.8 Off-site Backup

Trustwave performs routine backups of critical system data, audit log data, and other sensitive information. This information is stored in a physically secure location geographically separate from the main CA facility.

5.2 Procedural Controls

5.2.1 Trusted Roles

Trusted Persons include all employees, contractors, and consultants that have access to or control authentication or cryptographic operations that may materially affect:

- the validation of information in Certificate Applications;
- the acceptance, rejection, or other processing of Certificate Applications, revocation requests, renewal requests, or enrollment information;
- the issuance, or revocation of Certificates, including personnel having access to restricted portions of its repository; and
- the handling of Subscriber information or requests.

Trusted Persons include, but are not limited to:

- Micros personnel as designated and authorized by Micros;
- customer service personnel;
- cryptographic business operations personnel;
- security personnel;
- system administration personnel;
- designated engineering personnel; and
- Trustwave executives that are designated to manage infrastructural trustworthiness.

Trustwave considers the categories of personnel identified in this section as Trusted Persons having a Trusted Position. Persons seeking to become Trusted Persons by obtaining a Trusted Position shall successfully complete the screening requirements set out in this CPS.

5.2.2 Number of Persons Required per Task

Trustwave has established, maintains, and enforces rigorous control procedures to ensure the segregation of duties based on job responsibility and to ensure that multiple Trusted Persons are required to perform sensitive tasks.

Policy and control procedures are in place to ensure segregation of duties based on job responsibilities. The most sensitive tasks, such as access to and management of CA cryptographic hardware (Hardware Security Module or HSM) and associated key material require multiple Trusted Persons.

These internal control procedures are designed to ensure that at a minimum, two Trusted Persons are required to have either physical or logical access to the device. Access to CA cryptographic hardware is strictly enforced by multiple Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a module

is activated with operational keys, further access controls are invoked to maintain split control over both physical and logical access to the device.

5.2.3 Identification and Authentication for Each Role

For all personnel seeking to become Trusted Persons, verification of identity is performed through the personal (physical) presence of such personnel before Trusted Persons performing Micros or Trustwave HR or security functions, respectively, and a check of well-recognized forms of identification (e.g., passports and driver's licenses). Identity is further confirmed through the background checking procedures in Section 5.3.1.

Micros ensures that personnel have achieved Trusted Status and departmental approval has been given before such personnel are:

- issued access devices and granted access to the required facilities;
- issued electronic credentials to access and perform specific functions on Micros CA, RA, or other IT systems.

5.2.4 Roles Requiring Separation of Duties

Roles requiring Separation of duties include (but are not limited to):

- the generation, issuing, backups, or destruction of a Root CA key pair;
- the loading of Root CA Keys on an HSM;
- the storage of or access to Root CA Key Material; and
- access to all CA private keys for the purposes of Certificate issuance.

5.3 Personnel Controls

The entirety of section 5.3 applies to all Trustwave and Micros personnel who have, or may potentially have access, to any certification authority private key within the MPH.

5.3.1 Qualifications, Experience, and Clearance Requirements

Consistent with this CPS, Micros and Trustwave maintain personnel and management practices that provide reasonable assurance of the trustworthiness and competence of its employees and of the satisfactory performance of their duties. Additionally, Micros shall maintain the following practices.

1. Micros and Trustwave shall provide all employees and contractors interacting with the MPH in a role supporting certificate issuance with skills training that covers basic public key infrastructure knowledge, authentication and verification policies and procedures, and overview of common threats to the validation process, and this certification practice statement itself.
2. Micros and Trustwave shall maintain all records associated with training of the employees and contractors within the MPH for seven years.
3. Individuals responsible for the progression of initially gathering, then validating, subsequently approving, and finally auditing information, associated with any Certificate issuance process, shall qualify for each skill level prior to advancing to the next. This qualification will consist of an internally administered examination.

5.3.2 Background Check Procedures

Micros and Trustwave requires its employee to undergo a successful completion of background investigation which includes the following:

- Social Security Number Verification;
- Criminal Records Search;
- Credit History Review;
- Education Verification;
- Employment History Verification; and
- Foreign Records Search.

5.3.3 Training Requirements

Micros and Trustwave provide all personnel performing validation duties ("Validation Specialists") with skills training that covers basic Public Key Infrastructure (PKI) knowledge, authentication and verification policies and procedures, common threats to the validation process, including phishing and other social engineering tactics, this CPS, and all CA/Browser Forum Guidelines.

5.3.4 Retraining Frequency and Requirements

All Micros and Trustwave employees and contractors interacting with the MPH in a role supporting extended validation shall undergo an annual retraining exercise.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

Failure of any Micros or Trustwave employee or agent to comply with the provisions of this CPS, whether through negligence or malicious intent, will subject such individual to appropriate administrative and disciplinary actions, which may include termination as an employee or agent and possible civil and criminal sanctions.

5.3.7 Independent Contractor Requirements

Independent contractors who are assigned to perform Trusted Roles interacting with any component of the MPH are subject to the duties and requirements specified for such roles in this Section 5.3 and are subject to sanctions stated above in Section 5.3.6.

5.3.8 Documentation Supplied to Personnel

Employees and contractors in a role supporting extended validation are provided with the documentation necessary to perform the role to which they are assigned, including a copy of this CPS and all technical and operational documentation needed to maintain the integrity of the MPH CA operations.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

In addition to standard best practice system auditing procedures, Micros and Trustwave shall maintain records that include documenting:

- Compliance with this CPS and other obligations under Micros's agreements with subscribers;
- All actions, information, and events material to the enrollment, creation, issuance, use, expiration, and revocation of all Certificates issued within the MPH.

Specifically, Trustwave, on behalf of Micros, shall record the following events:

- CA key lifecycle management events, including:
  - Key generation, backup, storage, recovery, archival, and destruction; and
  - Cryptographic device lifecycle management events.
- CA and Subscriber Certificate lifecycle management events, including:
  - EV Certificate Requests, renewal requests, re-key requests, and revocation;
  - Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
  - Acceptance and rejection of Certificate Requests;
  - Issuance of Certificates; and
  - Generation of Certificate Revocation Lists (CRLs) and OCSP entries.
- Security events, including:
  - Successful and unsuccessful PKI system access attempts;
  - PKI and security system actions performed;
  - Security profile changes;
  - System crashes, hardware failures, and other anomalies;
  - Firewall and router activities; and
  - Entries to and exits from the CA facility.

5.4.2 Frequency of Processing Log

Trustwave, on behalf of Micros, shall review the content of all logs at least on a weekly basis. Follow-ups to all exceptions are required.

5.4.3 Retention Period for Audit Log

Trustwave, on behalf of Micros, shall maintain the written reviews of all audit log analysis for at least seven years.

5.4.4 Protection of Audit Log

Trustwave, on behalf of Micros, shall perform best effort mechanisms to protect all audit logs, including but not limited to:

- Network segregation;
- Network intrusion detection systems;
- Network firewalls; and
- Antivirus systems (where applicable).

In addition, Trustwave, on behalf of Micros, shall deploy system-level access control such that only individuals with a “need to know” shall be able to view audit logs.

5.4.5 Audit Log Backup Procedures

Trustwave, on behalf of Micros, and all certification authority members of the MPH, shall perform daily backup operations for all systems, including systems responsible for log collection.

5.4.6 Audit Collection System (Internal vs. External)

No stipulation.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

Trustwave, on behalf of Micros, performs monthly vulnerability scanning across Micros managed certification authority infrastructure.

5.5 Records Archival

5.5.1 Types of Records Archived

In addition to the audit logs specified above, Trustwave, on behalf of Micros, shall maintain records that include documenting the following.

- All Certificate issuance records are retained as records in electronic and/or in paper-based archives for the period detailed below in Section 5.5.2. Copies of Certificates are held, regardless of their status as expired or revoked;
- All appropriate documentation submitted by Applicants in support of a Certificate application;
- All records associated with Certificate issuance as part of its Certificate;
  - Approval checklist process;
  - the Subscriber's PKCS#10 CSR;
  - documentation of individual identity for individual Applicants;
  - screen shot of WHOIS record for domain name to be listed in the Certificate;
  - mailing address validation (if different than those identified through the resources listed above);
  - submission of the Certificate application, including acceptance of the Subscriber Agreement;
  - name, e-mail, and IP address of person acknowledging authority of the Contract Signer and Approver;
  - other relevant contact information for the Applicant/Subscriber; and
  - copies of Digital Certificates issued.

5.5.2 Certificate Revocation

Requests for Certificate revocation are recorded and archived, including the name of the person requesting revocation, the reason for the request and Micros and Trustwave personnel involved in authorizing revocation. This information and all resulting CRLs are retained as records in electronic archives for the period detailed in Section 5.5.3 below.

5.5.3 Retention Period for Archive

Trustwave, on behalf of Micros, retains the records of all certification authority activities and the associated documentation for a term of no less than 7 years.

5.5.4 Protection of Archive

Archive records are stored at a secure off-site location and are maintained in a manner that prevents unauthorized modification, substitution or destruction.

5.5.5 Archive Backup Procedures

No stipulation.

5.5.6 Requirements for Time-stamping of Records

All system time settings for all components within the MPH utilize the Network Time Protocol (NTP) with synchronization on at least a daily basis. All archives and log entries shall utilize the local network time provider which has been synchronized via NTP.

5.5.7 Procedures to Obtain and Verify Archive Information

No stipulation.

5.6 Key Changeover

Trustwave, on behalf of Micros, shall cease using any certification authority key one year prior to its expiration. After such time, the sole use for this key shall be to sign CRLs. A new CA signing key pair shall be commissioned, and all subsequently issued Certificates and CRLs are signed with the new private signing key. Both the old and the new Key Pairs may be concurrently active.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

If any CA within the MPH has its private key (or suspected to be) compromised, Micros and Trustwave shall:

- Inform all subscribers and relying parties of which the CA is aware;
- Terminate the certificates and CRL distribution services for certificates and CRLs issued using the compromised key.

5.7.2 Entity Private Key Compromise Procedures

If any CA within the MPH has its private key (or suspected to be) compromised, Micros and Trustwave shall:

- notify all subordinate CAs;
- make a reasonable effort to notify subscribers;
- terminate issuing and distribution of Certificates and CRLs;
- request revocation of the compromised Certificate; and
- generate a new CA key pair and Certificate and publish the Certificate in the Repository.

5.7.3 Business Continuity Capabilities After a Disaster

Trustwave maintains several documented disaster recovery and business continuity plans for use in the case of a declared disaster. All certification authorities managed by Trustwave within the MPH shall adhere to and follow these plans in the case of a declared disaster associated with any certification authority. These plans are as follows:

- Trustwave IT Disaster Recovery Plan (current: version 3.0, October 2007);
- Trustwave Business Continuity Plan (current: version 1.0, October 2007);
- MING System Disaster Recovery Plan (current: version 1.0, October 2007).

5.8 CA or RA Termination

In the event that Micros or its CAs cease operating, Micros shall make a commercially reasonable effort to notify Subscribers, Relying Parties, and other affected entities of such termination in advance. If practicable, Micros will develop a termination plan to minimize disruption to Subscribers and Relying Parties. Such termination plans may address the following, as applicable:

- Provision of notice to parties affected by the termination, such as Subscribers and Relying Parties;
- Informing such parties of the status of the CA;
- Handling the cost of such notice;

- The preservation of the CA's archives and records for the time periods required in this CPS;
- The continuation of Subscriber and customer support services;
- The continuation of revocation services, such as the issuance of CRL's;
- The revocation of unexpired, unrevoked Certificates of Subscribers and subordinate CAs, if necessary;
- The payment of compensation (if necessary) to Subscribers whose unexpired, unrevoked Certificates are revoked under the termination plan or provision, or alternatively, the issuance of replacement Certificates by a successor CA;
- Disposition of the CA's Private Key and the hardware tokens containing such Private Key;
- Provisions needed for the transition of the CA's services to a successor CA; and
- The identity of the custodian of Micros' CA and RA archival records.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

CA Key Pair generation is performed by multiple trained and trusted individuals using secure systems and processes that provide for the security and required cryptographic strength for the keys that are generated. All CA Key Pairs are generated in pre-planned key generation ceremonies in accordance with the requirements of Micros security and audit requirements guidelines and the CA/Browser Forum Guidelines. The activities performed in each key generation ceremony are recorded, dated, and signed by all individuals involved. These records are kept for audit and tracking purposes for a length of time deemed appropriate by Micros management.

Micros CA Key Pairs are maintained in a trusted and highly secured environment with backup and key recovery procedures. In the event of the Compromise of one or more of Micros Key(s), Micros and Trustwave shall promptly notify all Subscribers via e-mail and notify Relying Parties and others via the CRL and additional notice posted at http://www.Micros.com/CA. Trustwave shall also revoke all Certificates issued with such Micros CA Key(s).

When Micros CA Key Pairs reach the end of their Validity Period, such CA Key Pairs will be archived for a period of at least 7 years. Archived CA Key Pairs will be securely stored using off-line media. Procedural controls will prevent archived CA Key Pairs from being returned to production use. Upon the end of the archive period, archived CA Private Keys will be securely destroyed. Micros CA Key Pairs are retired from service at the end of their respective maximum lifetimes as defined above. This helps to ensure there is no key changeover. Certificates may be renewed as long as the cumulative certified lifetime of the Certificate Key Pair does not exceed the maximum CA Key Pair lifetime. New CA Key Pairs will be generated as necessary, for example to replace CA Key Pairs that are being retired, to supplement existing, active Key Pairs and to support new services in accordance with this CPS.

6.1.1 Key Pair Generation

6.1.1.1 Micros Certification Authority Key Pair Generation

All Micros certification authority key pairs shall be:

1. Generated in hardware security modules as defined in section 6.2;
2. RSA key pairs generated before December 31, 2009 shall be of at least 2048 bit size. RSA key pairs generated after January 1, 2010 shall be of at least 4096 bit size;
3. Performed in accordance with a documented key generation ceremony that is videotaped. Following completion of the ceremony, all Trustwave employees present shall attest in signatory form to the adherence of the procedure. These records shall be kept for seven years; and
4. Performed by multiple trusted and qualified Trustwave employees.

6.1.1.2 Subscriber key pair generation

Neither Micros nor Trustwave shall perform Subscriber key pair generation. All end entity keys shall be performed within the Subscriber's infrastructure. Neither Micros nor Trustwave mandates storage of private keys within hardware security modules for Subscribers.

6.1.2 Private Key Delivery to Subscriber

Neither Micros nor Trustwave shall perform private key generation or delivery to Subscribers.

6.1.3 Public Key Delivery to Subscriber

If Micros and/or Trustwave find all of the information and material supplied by the Applicant to be sufficiently verified, a Certificate will be issued to the Applicant by Micros. Upon issuance of the Applicant's Certificate, Micros will attach such Certificate to an e-mail and send such e-mail to the appropriate contacts. The e-mail will typically be sent only to the verified Certificate requester. In certain circumstances, the e-mail may include a Micros customer service representative telephone number and e-mail address for any technical or customer service problems. Micros, in its sole discretion, may provide such technical or customer support to the Applicants/Subscribers.

Micros may also deliver the Subscriber's signed Certificate via an online account download or through an Application Programming Interface (API).

6.1.4 CA Public Key Delivery to Relying Parties

Relying Parties can find Trustwave root certification authority Certificates within commonly used operating systems and browsers. Relying Parties may also obtain Trustwave and Micros certification authority root Certificates from https://ssl.trustwave.com/CA.

6.1.5 Key Sizes

All certification authorities within the MPH shall use at least 2048 bit RSA keys. Micros recommends that CSRs of Applicants use at least 1024 bit RSA keys. Trustwave may, at its discretion, not approve CSRs utilizing 512 bit or lower key size. Following December 31, 2009, Micros shall not accept CSRs for certificates of less than 2048 bit RSA keys.

6.1.6 Public Key Parameters Generation and Quality Checking

The public exponent of all root keys within the MPH shall use a public exponent of 3, 5, 17, or 65,537 for the generation of their RSA key pair. All hardware security modules used for storage of Micros-managed certification authority keys shall be FIPS 186-3 compliant and shall provide hardware-based pseudo-random number generation.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

All Certificates within the MPH shall contain the X.509 v3 key usage field so that the usage of the private key can be delimited and determined by X.509 compliant software. In addition, the Subscriber and End-Entity Certificates may have extended key usage extensions set.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

All private keys within the MPH shall be protected via Federal Information Processing Standard (FIPS) 140-2 Level 3 hardware security modules.

6.2.2 Private Key (n out of m) Multi-Person Control

Access, both electronic and physical, to all private keys associated with Micros-managed MPH require a minimum of two Trustwave employees to come together in order to derive the private key.

6.2.3 Private Key Escrow

Trustwave does not, nor has the facilities to, escrow private keys.

6.2.4 Private Key Backup

All private key backups for the certification authorities of the MPH shall be stored in password or PIN protected hardware (smart cards) in a form such that it requires at least two trusted and qualified Trustwave employees to come together in order to regenerate the private key.

All private key backups of the following three global root certification authorities – SGCA, XGCA, and STCA shall be stored in hardware such that it requires three people to come together in order to regenerate the private key.

6.2.5 Private Key Archival

Trustwave does not archive private keys, except as stipulated within section 6.1.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

All Micros managed certification authority key pairs that are transferred into or from a cryptographic module shall be:

1. Performed in accordance with a documented key movement ceremony that is videotaped. Following completion of the ceremony, all Trustwave employees present shall attest in signatory form to the adherence of the procedure. These records shall be kept for seven years; and
2. Performed by multiple (at least three) trusted and qualified Trustwave employees.

6.2.7 Private Key Storage on Cryptographic Module

See 6.2.1

6.2.8 Method of Activating Private Key

All End-Entities and Subscribers are solely responsible for protection of their private keys. All End-Entities and subscribers are responsible for protection of their private keys against loss, theft, modification, unauthorized disclosure, or unauthorized use. Micros and Trustwave maintain no role in the generation, protection, or maintenance of Subscriber private keys.

All MPH components require multiple individuals (at least two) to come together in order to activate a certification authority's private key. This is enforced by both operating system access control and hardware security module routines.

6.2.9 Method of Decertification, Deactivating Private Key

The private keys stored on hardware security modules are deactivated via the hosting operating systems and shut down and by lockout receivers associated with the HSM. Subscribers should also deactivate their private keys via logout and removal procedures when they are not in use.

6.2.10 Method of Destroying Private Key

At the conclusion of any certification authority's private key lifetime, the private key associated with the MPH component shall be destroyed following vendor recommended guidelines for the hardware security module.via incineration of the HSM.

6.2.11 Cryptographic Module Rating

See 6.2.1

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Trustwave retains copies of all Public Keys for archival in accordance with Section 5.5.

6.3.2 Certificate Validity Periods and Key Pair Usage Periods

All MPH certification authority Certificates and corresponding keys shall have maximum Validity Periods (not exceeding) of ten (10) years.

6.4 Activation Data

Trustwave deploys multiple levels of electronic and physical security controls in order to protect access to CA's private keys. Physical access to computer rooms containing CA private keys shall require at least two individuals to come together in order to deactivate the physical security controls protecting the room.

In addition, Trustwave deploys an "m out of n" secret sharing routine for electronic access to CA private keys, where "m" is greater than two and "n" is six. In other words, three of the six individuals possessing a component of the activation data must come together in order to gain access to a private key as stored in an HSM. Each of these six individuals shall have their own token necessary for insertion into the HSM in order to perform activities associated with the root certification authorities' private keys.

6.4.1 Activation Data Generation and Installation

Activation data associated with each of the tokens possessed by the six individuals capable of accessing root certification authority private keys was generated during initial installation and configuration of the hardware security modules.

6.4.2 Activation Data Protection

All activation data shall be stored on FIPS 140-2 level 3 smart cards associated with the HSM's.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

No stipulation.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Micros maintains within its corporate information security policy and program, significant management controls governing systems development. These controls are applied for all certification authority development activities.

6.6.2 Security Management Controls

Trustwave maintains both technical and procedural mechanisms to monitor change to all components within the MPH.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

The systems containing the MPH all reside in highly segmented networks constrained from both the Internet and Micros and Trustwave corporate networks via multiple levels of firewalls. Interaction with outside entities shall only be performed with servers located on a demilitarized zone (DMZ). Additionally, all networks associated with certification authority operations at Micros shall be monitored by a network intrusion detection system. All systems associated with certification authority activities shall be hardened with services restricted to only those necessary for certification authority operations. Any change associated with the MPH shall be documented and approved via a change management system.

6.8 Time-Stamping

No Stipulation.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

(Note: Textual printouts of each Micros root Certificate are included in Appendix A)

7.1.1 Version Number(s)

All Certificates within the MPH shall be X.509 version 3 Certificates.

7.1.2 Certificate Extensions

7.1.2.1 MPH Certification Authority Extensions

Basic constraints

1. All certification authority Certificates within the MPH shall include the basic constraints extension with a subject type equal to "CA" and its criticality set to "critical".
2. The CCA shall have the path length constraint set to "1".
3. Subordinate CAs underneath CCA shall have the path length constraint set to "0".

Key Usage

All certification authority Certificates within the MPH shall contain a key usage extension set for "Certificate signing" and "CRL signing." Additionally, this extension may contain the "off-line CRL signing" bit. This extension shall be marked as non-critical.

CRL Distribution Point

All certification authority Certificates within the MPH shall contain the location of the CRL retrieval location in the form of the "CRL distribution point" extension. Typically this extension will be in the form of an HTTP URL. This extension will be marked as "non-critical".

7.1.2.2 MISCA Client Certificate Extensions

All Certificates issued by the MISCA to a Subscriber shall include:

- Micros's OID in the certificate policies extension. Micros' OID for MISCA Internal SSL is 1.3.6.1.4.1.32036.3.3.3.3.4.3.3
- The basic Constraints extension, marked as Critical, with Subject Type=End Entity and Path Length Constraint=None
- The key usage, marked as non-critical, set to include Digital Signature and Key Encipherment. The non-repudiation bit shall not be set.
- The extended Key Usage, marked as non-critical, set equal to TLS Client Authentication (1.3.6.1.5.5.7.3.2). No other values within the enhanced Key Usage extension shall be set.
- The CRL Distribution Point extension, marked as non-critical, set equal to either http://crl.securetrust.com/XXXX.crl where XXXX represents either Micros CA or the Micros MISCA depending on the issuing root CA.

7.1.3 Algorithm Object Identifiers

All Certificates issued by certification authorities within the MPH shall use RSA signatures with SHA-1 hashes for their signatures in compliance with the Internet Engineering Task Force's Request for Comment ("RFC") 5280.

7.1.4 Name Forms

Micros Certificates are populated using X.500 naming conventions.

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

Each Certificate issued by Micros shall contain an OID reflecting Certificate type and its associated governance as defined in section 1.1.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL Profile

For each of the certification authorities within the MPH, CRL's conforming to RFC 5280 shall be issued on a daily basis containing:

- Version (set to "1" in order to indicate version 2);
- Issuer Signature Algorithm (SHA-1 with RSA Encryption {1 2 840 113549 1 1 5});
- Issuer Distinguished Name (the issuing certification authority);
- This Update in ISO 8601 format with UTC designation.
- Next Update in ISO 8601 format with UTC designation;
- The list of revoked Certificates including reason code;
- Serial Number;
- Revocation Date;
- RSA Signature of the CRL.

7.2.1 Version Number(s)

All certification authorities within the MPH shall issue version 2 CRLs.

7.2.2 CRL and CRL Entry Extensions

Each Certificate revocation list issued may contain:

- CRL Number (unique);
- Authority Key Identifier;
- CRL Entry Extensions;
- Invalidity Date (UTC - optional); and
- Reason Code (optional).

7.3 OCSP Profile

No stipulation. Reserved for future use.

7.3.1 Version Number(s)

No stipulation. Reserved for future use.

7.3.2 OCSP Extensions

No stipulation. Reserved for future use.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

An annual audit is performed by an independent external auditor to assess Trustwave's compliance with the standards set forth by the CA/Browser Forum. Included within this audit is the environment containing all of Micros's assets.

Material exceptions or deficiencies identified during an audit will result in a determination of actions to be taken. This determination is made by Trustwave management with input from the independent auditor. Trustwave management is responsible for developing and implementing a corrective action plan. Trustwave undergoes yearly audits using AICPA/CICA WebTrust for certification authorities, including extended validation criteria, for all components of the Trustwave managed MPH and complies with all requirements of the program.

8.1 Frequency or Circumstances of Assessment

Trustwave shall conduct the AICPA/CICA WebTrust audits on a yearly basis.

8.2 Identity/Qualifications of Assessor

The AICPA/CICA WebTrust audits shall be conducted by a certified public accounting firm with a sound foundation for conducting its audit business, that:

- Has no financial, business, or legal interest with Trustwave;
- Has demonstrated proficiency and competence in regards to public key infrastructure technology; and is
- Accredited by the American Institute of Certified Public Accountants (AICPA).

8.3 Assessor's Relationship to Assessed Entity

The public accounting firm conducts the AICPA/CICA WebTrust audits for Trustwave shall be completely independent of Trustwave.

8.4 Topics Covered by Assessment

The annual WebTrust audits shall include but are not limited to:

- CA business practices disclosure;
- Detailed validation process;
- Service integrity;
- CA environmental controls.

8.5 Actions Taken as a Result of Deficiency

For any deficiencies found by the WebTrust audit, Trustwave shall immediately develop a plan to implement remediation steps. This plan will be submitted to the Certification Practice Board and to the independent auditor within 30 days. Following acceptance of the plan, Trustwave shall immediately move to correct all deficiencies noted.

8.6 Communication of Results

All results of the WebTrust audit for Trustwave shall be communicated to the Certification Practice Board and to the Certification Operations Committee. Following review and approval by the Certification Practice Board, the results will be communicated to the Trustwave Board of Directors.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Micros shall not charge Subscribers and End-Entities for the issuance, reissuance, management, rekey, and renewal of Certificates.

9.1.2 Certificate Access Fees

Micros shall not charge a fee to make a Certificate available in a repository or available to a Relying Party.

9.1.3 Revocation or Status Information Access Fees

Micros shall not charge a fee to view the CRLs or to make the CRLs available in a repository or to a Relying Party. Micros shall not charge a fee for access to revocation information, Certificate status information, or time stamping in its repositories to third parties, including third parties that provide products and/or services that utilize such Certificate status information. Such access may, however, be provided with the prior written consent of Micros.

9.1.4 Fees for Other Services

Micros shall not charge a fee for access to this CPS. Any use made for purposes other than simply viewing the document, such as reproduction, redistribution, modification, or creation of derivative works is strictly prohibited without the express written consent of Trustwave.

9.1.5 Refund Policy

No Stipulation.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

Micros encourages customer, Subscribers, End-Entities, Relying Parties, and all other entities to maintain adequate insurance to protect against errors and omissions, professional liability, and general liability. Micros shall maintain commercially reasonable insurance.

9.2.2 Other Assets

Micros shall maintain adequate financial resources for their operations and duties, and shall be able to bear the risk of liability to Subscribers and Relying Parties.

9.2.3 Insurance or Warranty Coverage for End-Entities

No Stipulation.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following Subscriber documentation shall be maintained in confidence.

- CA application records, whether approved or disapproved;
- Certificate Application records;

- Subscriber Agreement;
- Private keys held by customers and subscribers and information needed to recover such Private Keys;
- Transactional records;
- Contingency planning and disaster recovery plans; and
- Security measures controlling the operations of Micros and Trustwave hardware and software and the administration of Certificate services and designated enrollment services.

9.3.2 Information Not Within the Scope of Confidential Information

This section is subject to applicable privacy laws. The following are not considered confidential:

- Certificates;
- Certificate revocation;
- Certificate status; and
- Micros certificate/CRL repositories and their contents.

9.3.3 Responsibility to Protect Confidential Information

Micros protects and secures confidential information from disclosure.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

Micros's privacy plan/policy may be found at http://www.Micros.com.

Trustwave's privacy plan/policy may be found at https://www.Trustwave.com.

9.4.2 Information Treated as Private

Non-public Subscriber information is treated as private.

9.4.3 Information Not Deemed Private

Subscriber information issued in the Certificates, Certificate directory, and online CRLs is not deemed private information, subject to applicable law.

9.4.4 Responsibility to Protect Private Information

Micros, customers, Subscribers, and End-Entities who receive private information shall protect it from disclosure to third parties and shall comply with all applicable laws.

9.4.5 Notice and Consent to Use Private Information

Unless otherwise stated in this CPS, Micros's and Trustwave's Privacy Policy, or agreements in writing, private information shall not be used without the written consent of the party who owns such information. This section is subject to applicable laws.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Micros and Trustwave shall be permitted to disclose confidential and/or private information if Trustwave reasonably determines that disclosure is required in response to a subpoena, court order, search warrant, judicial, administrative, discovery, or other legal process or directive. This section is subject to applicable laws.

9.4.7 Other Information Disclosure Circumstances

Refer to section 9.4.6.

9.5 Intellectual Property Rights

Micros retains all rights, title, and interest, including without limitation intellectual property rights to this CPS, CPs, and Micros's logos, trademarks and service marks; and

Trustwave retains all rights, title, and interest, including without limitation intellectual property rights to the following:

- roots keys and the root Certificates containing them;
- Certificates; and
- Revocation Information.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

Micros warrants that, to the best of Micros's knowledge:

- there are no material misrepresentations of fact with the Certificates;
- there are no errors in the information within the Certificates caused by Micros's failure to exercise reasonable care in approving, creating, issuing, and managing the Certificates;
- the Certificates comply with the material requirements of this CPS and the applicable CPs; and
- Micros's revocation services and its repositories materially comply with this CPS and the applicable CPs.

9.6.2 RA Representations and Warranties

RAs, including Micros, warrant that, to the best of their knowledge:

- there are no material misrepresentations of fact with the Certificates;
- there are no errors in the information within the Certificates caused by Micros's failure to exercise reasonable care in approving, creating, issuing, and managing the Certificates;
- the Certificates comply with the material requirements of this CPS and the applicable CPs; and
- Micros's revocation services, if applicable, and its repositories materially comply with this CPS and the applicable CPs.

9.6.3 Subscriber Representations and Warranties

Subscribers warrant that:

- Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created;
- Their private key is protected and that no unauthorized person has ever had access to the Subscriber's private key;
- All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true;
- All information supplied by the Subscriber and contained in the Certificate is true;

- The Certificate is being used exclusively for authorized and legal purposes consistent with this CPS, and
- The Subscriber is an end-user Subscriber and not a CA, and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise.

  Subscriber Agreements may include additional representations and warranties.

9.6.4 Relying Party Representations and Warranties

Relying Party Agreements require Relying Parties to acknowledge that they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate, that they are solely responsible for deciding whether or not to rely on such information, and that they shall bear the legal consequences and liability of their failure to perform the Relying Party obligations in terms of this CPS.

Relying Party Agreements may include additional representations and warranties.

9.7 Disclaimers of Warranties

EXCEPT FOR THE LIMITED WARRANTY DESCRIBED HEREIN AND TO THE GREATEST EXTENT PERMITTED BY APPLICABLE LAW, MICROS AND TRUSTWAVE EXPRESSLY DISCLAIM AND MAKE NO REPRESENTATION, WARRANTY OR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, WITH RESPECT TO THIS CPS, THE APPLICABLE CPS OR ANY CERTIFICATE ISSUED HEREUNDER, INCLUDING WITHOUT LIMITATION, ALL WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE OR USE OF A CERTIFICATE OR ANY SERVICE (INCLUDING, WITHOUT LIMITATION, ANY SUPPORT SERVICES) PROVIDED BY MICROS AND TRUSTWAVE AS DESCRIBED HEREIN. ALL WARRANTIES, REPRESENTATIONS, CONDITIONS, UNDERTAKINGS, TERMS AND OBLIGATIONS IMPLIED BY STATUTE OR COMMON LAW, TRADE USAGE, COURSE OF DEALING OR OTHERWISE ARE HEREBY EXCLUDED TO THE FULLEST EXTENT PERMITTED BY LAW. EXCEPT FOR THE LIMITED WARRANTY DESCRIBED HEREIN, MICROS AND TRUSTWAVE FURTHER DISCLAIM AND MAKE NO REPRESENTATION, WARRANTY OR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, TO ANY APPLICANT, SUBSCRIBER OR ANY RELYING PARTY THAT (1) THE SUBSCRIBER TO WHICH IT HAS ISSUED A CERTIFICATE IS IN THE FACT THE PERSON, ENTITY OR ORGANIZATION IT CLAIMS TO HAVE BEEN (2) A SUBSCRIBER IS IN FACT THE PERSON, ENTITY OR ORGANIZATION LISTED IN THE CERTIFICATE, OR (3) THAT THE INFORMATION CONTAINED IN THE CERTIFICATES OR IN ANY CERTIFICATE STATUS MECHANISM COMPILED, PUBLISHED OR OTHERWISE DISSEMINATED BY MICROS OR TRUSTWAVE, OR THE RESULTS OF ANY CRYPTOGRAMPHIC METHOD IMPLEMENTED IN CONNECTION WITH THE CERTIFICATES IS ACCURATE, AUTHENTIC, COMPLETE OR RELIABLE.

IT IS AGREED AND ACKNOWLEDGED THAT APPLICANTS AND SUBSCRIBERS ARE LIABLE FOR ANY MISREPRESENTATIONS MADE TO MICROS OR TRUSTWAVE OR RELIED UPON BY A RELYING PARTY. MICROS AND TRUSTWAVE DO NOT WARRANT OR GUARANTEE UNDER ANY CIRCUMSTANCES THE "NON-REPUDIATION" BY A SUBSCRIBER AND/OR RELYING PARTY OF ANY TRANSACTION OR CONTRACT ENTERED INTO BY THE SUBSCRIBER AND/OR RELYING PARTY INVOLVING THE USE OF OR RELIANCE UPON A CERTIFICATE.

IT IS UNDERSTOOD AND AGREED UPON BY SUBSCRIBERS AND RELYING PARTIES THAT IN USING AND/OR RELYING UPON A CERTIFICATE THEY ARE SOLELY RESPONSIBLE FOR THEIR RELIANCE UPON THAT CERTIFICATE AND THAT SUCH PARTIES MUST CONSIDER THE FACTS, CIRCUMSTANCES AND CONTEXT SURROUNDING THE TRANSACTION IN WHICH THE CERTIFICATE IS USED IN DETERMINING SUCH RELIANCE.

THE APPLICANTS, SUBSCRIBERS AND RELYING PARTIES AGREE AND ACKNOWLEDGE THAT CERTIFICATES HAVE A LIMITED VALIDITY PERIOD AND MAY BE REVOKED AT ANY TIME. SUBSCRIBERS AND RELYING PARTIES ARE UNDER AN OBLIGATION TO VERIFY WHETHER A CERTIFICATE IS EXPIRED OR HAS BEEN REVOKED. MICROS AND TRUSTWAVE HEREBY DISCLAIM ANY AND ALL LIABILITY TO SUBSCRIBERS AND RELYING PARTIES WHO DO NOT FOLLOW SUCH PROCEDURES, THIS CPS, THE TRUSTWAVE CPS, OR THE APPLICABLE CPS.

Micros and Trustwave provide no warranties with respect to another party's software, hardware, telecommunications or networking equipment utilized in connection with the use, issuance, revocation or management of Certificates or providing other services (including, without limitation, any support services) with respect to this CPS or the applicable CPs. Applicants, Subscribers and Relying Parties agree and acknowledge that Micros and Trustwave are not responsible or liable for any misrepresentations or incomplete representations of Certificates or any information contained therein caused by another party's application software or graphical user interfaces. The cryptographic key-generation technology used by Applicants, Subscribers and Relying Parties in conjunction with the Certificates may or may not be subject to the intellectual property rights of third-parties. It is the responsibility of Applicants, Subscribers and Relying Parties to ensure that they are using technology which is properly licensed or to otherwise obtain the right to use such technology

9.8 Limitations of Liability

IN NO EVENT SHALL THE CUMULATIVE OR AGGREGATE LIABILITY OF MICROS OR TRUSTWAVE TO APPLICANTS, SUBSCRIBER AND/OR ANY RELYING PARTY FOR ALL CLAIMS RELATED TO THE INSTALLATION OF, USE OF OR RELIANCE UPON A SPECIFIC CERTIFICATE INCLUDING WITHOUT LIMITATION ANY CAUSE OF ACTION OR CLAIM IN CONTRACT, TORT (INCLUDING NEGLIGENCE AND TORTIOUS INTERFERENCE WITH CONTRACT), STRICT LIABILITY, FOR BREACH OF A STATUTORY DUTY OR FIDUCIARY DUTY OR IN ANY OTHER WAY, EXCEED TWO THOUSAND U.S. DOLLARS ($2,000.00 USD). THE FOREGOING LIMITATIONS OF LIABILITY SHALL APPLY ON A CERTIFICATE-BY-CERTIFICATE BASIS, REGARDLESS OF THE NUMBER OF TRANSACTIONS OR CLAIMS RELATED TO EACH CERTIFICATE, AND SHALL BE APPORTIONED FIRST TO THE EARLIER CLAIMS TO ACHIEVE FINAL RESOLUTION.

MICROS AND TRUSTWAVE SHALL NOT BE LIABLE IN CONTRACT, TORT (INCLUDING NEGLIGENCE AND TORTIOUS INTERFERENCE WITH CONTRACT), STRICT LIABILITY, FOR BREACH OF A STATUTORY OR FIDUCIARY DUTY OR IN ANY OTHER WAY (EVEN IF FORSEEABLE AND/OR MICROS OR TRUSTWAVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) FOR: (I) ANY ECONOMIC LOSS (INCLUDING, WITHOUT LIMITATION, LOSS OF REVENUES, PROFITS, CONTRACTS, BUSINESS OR ANTICIPATED SAVINGS); (II) TO THE EXTENT ALLOWED BY APPLICABLE LAW, ANY LOSS OR DAMAGE RESULTING FROM DEATH OR INJURY OF SUBSCRIBER AND/OR ANY RELYING PARTY OR ANYONE ELSE; (III) NON-ECONOMIC LOSS OR ANY LOSS OF

GOODWILL OR REPUTATION; OR (IV) ANY OTHER INDIRECT, CONSEQUENTIAL, INCIDENTAL, MULTIPLE, SPECIAL, PUNITIVE, EXEMPLARY DAMAGES.

THIS SECTION “LIMITATIONS OF LIABILITY” SHALL APPLY WHETHER OR NOT SUCH LOSSES OR DAMAGES WERE WITHIN THE CONTEMPLATION OF THE PARTIES AT THE TIME OF THE APPLICATION FOR, INSTALLATION, USE, OR RELIANCE ON THE CERTIFICATE, OR AROSE OUT OF ANY OTHER MATTER OR SERVICES (INCLUDING, WITHOUT LIMITATION, ANY SUPPORT SERVICES) UNDER THIS CPS OR THE APPLICABLE CPS OR WITH REGARD TO THE USE OF OR RELIANCE ON THE CERTIFICATE.

IN THE EVENT THAT SOME JURISDICTIONS DO NOT PERMIT THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, THE ABOVE EXCLUSIONS OF INCIDENTAL AND CONSEQUENTIAL DAMAGES MAY NOT APPLY TO AN APPLICANT, SUBSCRIBER AND/OR A RELYING PARTY BUT SHALL BE GIVEN EFFECT TO THE FULLEST AND GREATEST EXTENT PERMITTED BY APPLICABLE LAW.

In no event will Micros or Trustwave be liable for any damages to Applicants, Subscribers, Relying Parties or any other party arising out of or related to the use or misuse of, or reliance on any Certificate issued under this CPS that: (i) has expired or been revoked; (ii) has been used for any purpose other than as set forth in the CPS; (iii) has been tampered with; (iv) has been Compromised or if the Key Pair underlying such Certificate or the cryptography algorithm used to generate such Certificate's Key Pair, has been Compromised by the action of any party other than Micros (including without limitation the Applicant, Subscriber or Relying Party); or (v) is the subject of misrepresentations or other misleading acts or omissions of any other party, including but not limited to Applicants, Subscribers and Relying Parties. In no event shall Micros or Trustwave be liable to the Applicant, Subscriber, Relying Party or other party for damages arising out of any claim that a Certificate infringes any patent, trademark, copyright, trade secret or other intellectual property right of any party.

The liability (and/or limitation thereof) of Subscribers shall be as set forth in the applicable Subscriber agreements.

The liability (and/or limitation thereof) of enterprise RAs and the applicable CA shall be set out in the agreement(s) between them.

The liability (and/or limitation thereof) of Relying Parties shall be as set forth in the applicable Relying Party Agreements.

9.9 Indemnities

Applicant, Subscriber and Relying Parties hereby agree to indemnify and hold Micros, Trustwave and their affiliates (including, but not limited to, its parent company, officers, directors, employees, agents, partner, successors and assigns) harmless from any claims, actions, or demands that are caused by the use, publication or reliance on a Certificate and that arises from (a) any false or misleading statement of fact by the Applicant (or any person acting on the behalf of the Applicant) (b) any failure by the Applicant or the Subscriber to disclose a material fact, regardless of whether such omission was made negligently or with the intent to deceive; (c) any failure on the part of the Subscriber to protect its Private Key and Certificate or to take the precautions necessary to prevent the Compromise, disclosure, loss, modification or unauthorized use of the Private Key or Certificate; (d) any failure on the part of the Subscriber to

promptly notify Micros and Trustwave, as the case may be, of the Compromise, disclosure, loss, modification or unauthorized use of the Private Key or Certificate once the Subscriber has constructive or actual notice of such event; (e) the Subscriber's failure to the comply with the Subscriber Agreement; or (f) the Relying Party's failure to comply with this CPS and the Relying Party Agreement, including without limitation the Relying Party's (i) failure to verify a Certificate in accordance with this CPS and the Relying Party Agreement; (ii) reliance on a Certificate that is unreasonable given the circumstances; and/or (iii) failure to verify whether a Certificate has expired or been revoked.

The applicable Subscriber and/or Relying Party Agreements may set forth additional indemnity obligations.

9.10 Term and Termination

9.10.1 Term

This CPS and the CPs, and any amendments thereto, are effective upon publication in Micros's Repository.

9.10.2 Termination

This CPS and the CPs, as may be amended from time to time, are effective until replace by a new version, which shall be published in Micros's Repository.

9.10.3 Effect of Termination and Survival

Upon Termination of this CPS or the applicable CPs, customers, Subscribers, and Relying Parties are bound by its terms for all Certificates issued, while it's effective, for the remainder of the validity periods of such Certificates.

9.11 Individual Notices and Communications with Participants

Micros, Subscribers, Applicants, Relying Parties and other participants will use commercially reasonable methods to communicate with each other.

9.12 Amendments

9.12.1 Procedure for Amendment

Refer to Section 1.5.4 hereof.

9.12.2 Notification Mechanism and Period

Micros reserves the right to amend this CPS and the applicable CPs without notification for amendments that are not material, subject to the written approval of Trustwave's Certification Practice Board. Micros's and Trustwave's decision to designate an amendment's materiality shall be within the sole discretion of Micros and Trustwave..

Updates, amendments, and new version of Micros CPS and the applicable CP's shall be posted in Micros's repository. Such publication shall serve as notice to all relevant entities.

9.12.3 Circumstances under Which OID Must be Changed

If Micros's Certification Practice Board determines that a change is necessary in the object identifier corresponding to a Certificate policy, the amendment shall contain new object identifiers for the Certificate policies corresponding to each such Certificate. Otherwise, amendments shall not require a change in Certificate policy object identifier.

9.13 Governing Law

This CPS is governed by and interpreted in accordance with the laws of the State of Maryland, USA, excepting the conflict of law rules of the State of Maryland, as if this contract were made and to be performed entirely within the State of Maryland. The parties mutually consent to exclusive jurisdiction and venue in the state and federal courts sitting in the State of Maryland.

9.14 Compliance with Applicable Law

This CPS and the applicable CPs is subject to applicable federal, state, local and foreign laws, rules, regulations including, but not limited to, restrictions on exporting or importing software, hardware, or information

9.15 Miscellaneous Provisions

9.15.1 Entire Agreement

This CPS, the applicable CPs, and the applicable Subscriber Agreement and Relying Party Agreement represent the entire agreement between any Subscriber or Relying Party and Micros and shall supersede any and all prior understandings and representations pertaining to its subject matter. In the event, however, of a conflict between this CPS and any other express agreement between a Subscriber or Relying Party with Micros with respect to a Certificate, including but not limited to a Subscriber Agreement, and Relying Party such other agreement shall take precedence.

9.15.2 Assignment

This CPS and its CPs shall not be assigned to any party without the express prior written consent of Micros and Trustwave.

9.15.3 Severability

If any provision of this CPS and/or the CPs shall be held to be invalid, illegal, or unenforceable, the validity, legality, or enforceability of the remainder of this CPS and the CPs shall remain in full force and effect.

9.15.4 Enforcement (Attorneys' Fees and Waiver of Rights)

The waiver or failure to exercise any right provided for in this CPS or the applicable CPs shall not be deemed a waiver of any further or future right under this CPS or the applicable CPs.

9.15.5 Force Majeure

Micros and Trustwave shall not be liable for any default or delay in the performance of its obligations hereunder to the extent and while such default or delay is caused, directly or indirectly, by fire, flood, earthquake, elements of nature or acts of God, acts of war, terrorism, riots, civil disorders, rebellions or revolutions, strikes, lockouts, or labor difficulties or any other similar cause beyond the reasonable control of Micros.

9.15.6 Other Provisions

No stipulation.

Appendix A –

Micros Root Certificate

Certificate:
Data:
Version: 3 (0x2)
Serial Number: 1800000005 (0x6b49d205)
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=US, ST=Illinois, L=Chicago, O=Trustwave Holdings, Inc., CN=Trustwave Organization Issuing CA, Level 2/emailAddress=ca@trustwave.com
Validity
Not Before: Apr 1 18:23:53 2010 GMT
Not After : Mar 29 18:23:53 2020 GMT
Subject: C=US, ST=Maryland, L=Columbia, O=Micros Systems, Inc., CN=Micros CA
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)
Modulus (2048 bit):
00:e2:1c:4c:5e:25:a3:53:4b:64:63:f5:ec:c3:11:
2e:df:cd:d1:e5:31:a5:16:08:67:04:43:0e:3a:33:
f0:5c:fd:9a:8c:a6:a4:a6:5d:3c:08:29:6c:0e:3d:
b7:5a:95:35:a1:62:4a:83:19:56:1d:49:0e:2e:e5:
4a:d5:57:83:c5:b7:ed:1a:b5:66:73:c5:24:4c:c1:
99:bf:2b:89:de:0c:1b:d3:d8:58:8e:9d:28:70:22:
84:ed:e1:29:3e:97:7b:ff:78:22:3b:90:d1:7a:11:
f1:b1:ae:c1:0d:6a:f4:f9:bd:2a:a7:1a:d5:ca:d5:
55:59:9c:cb:cc:5b:c7:b1:c9:2f:cf:6f:6c:19:6a:
af:8f:9d:52:18:f9:6b:05:8a:4a:b9:b9:e7:d0:a9:
d2:44:b2:bc:fa:ed:55:20:00:d0:78:0d:b5:34:27:
1e:e7:9e:f9:f3:9f:b2:b3:87:92:ef:0b:8c:7f:d9:
1e:65:ef:d1:d4:a7:8f:a2:7f:c4:12:80:f2:af:72:
41:4e:df:f2:8c:cb:f1:ec:7a:3a:f5:86:68:8f:de:
33:db:a4:2d:dc:2f:26:b8:78:ca:48:d6:f7:29:a2:
7b:7f:df:9c:84:40:9c:f1:ed:ae:52:a1:6c:1c:46:
b6:a8:5a:1e:77:62:db:f1:bd:05:46:da:b7:c9:d0:
d2:df
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints: critical
CA:TRUE, pathlen:1
X509v3 Subject Key Identifier:
C6:6B:91:57:43:4E:5B:93:15:CA:C2:14:40:9E:2C:43:7E:EF:18:18
X509v3 Authority Key Identifier:
keyid:92:08:64:B1:BB:9F:A4:91:5B:5E:AF:53:ED:E2:92:F3:DB:66:AD:31

X509v3 Key Usage:
Certificate Sign, CRL Sign

X509v3 Certificate Policies:
Policy: 1.3.6.1.4.1.35539.3.3.3.3.3
CPS: http://ssl.trustwave.com/CA/micros

Signature Algorithm: sha1WithRSAEncryption
b2:95:fc:57:27:08:25:b5:a8:a4:49:9f:0a:68:e9:0f:31:18:
68:c7:2b:44:e4:31:d9:a5:f2:00:bc:0b:6f:55:2d:32:d2:1f:
14:b4:3c:cf:92:85:f3:2c:39:c4:55:e6:aa:6b:87:8d:5a:8c:
17:3a:99:a3:24:4f:17:49:85:17:12:ad:e4:7e:f7:d1:3d:78:
c3:b9:4e:a7:6f:fe:29:97:ee:52:ad:8c:6d:fc:64:fa:c9:7e:
f1:ba:80:02:15:af:b8:c7:6d:87:a0:3a:09:23:ae:a1:f4:b5:
82:5e:5f:1c:58:b4:2d:49:c1:ab:04:cc:cf:64:b5:06:f0:78:
92:9e:03:85:f3:e0:f5:a5:92:4d:7f:c5:0f:c0:c5:99:47:ab:
67:4e:83:da:8e:d5:f0:82:84:e4:01:c5:96:28:c5:78:e5:b3:
ba:0c:4b:11:f2:89:3e:d6:a6:1a:74:8a:8c:36:27:b0:44:1f:
ad:cc:b6:87:0b:59:7e:41:bd:b1:07:88:0a:c9:17:01:e6:5d:
b7:01:0b:d5:51:53:21:25:1c:19:10:3a:89:d9:fd:f0:4d:30:
82:20:81:50:60:36:0f:9c:4f:67:f5:c7:aa:21:86:50:22:6a:
31:87:67:3c:a7:3c:93:6c:80:6f:8a:d6:bd:fb:86:29:ee:87:
01:5e:8c:9b

The Micros Internal SSL Root Certificate

Certificate:
Data:
Version: 3 (0x2
Serial Number: 1200020938 (0x4786ddca)
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=US, ST=Maryland, L=Columbia, O=Micros Systems, Inc., CN=Micros CA
Validity
Not Before: Apr 1 18:31:30 2010 GMT
Not After : Mar 29 18:31:30 2020 GMT
Subject: C=US, ST=Maryland, L=Columbia, O=Micros Systems, Inc., CN=Micros Internal CA
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)
Modulus (2048 bit):
00:9e:95:91:2c:28:3a:69:22:99:de:90:1d:e2:95:
d8:9b:2d:21:88:47:76:fb:23:ff:61:1c:e0:27:ae:
0f:2f:0a:71:ac:f9:0c:a2:28:4a:a5:75:33:9e:da:

```
            9a:94:f3:43:df:2e:13:d7:9d:a6:ef:c7:3b:22:08:
            d3:a7:e3:7e:9f:bd:16:2d:05:27:d5:58:19:9f:f6:
            7f:b4:0c:e2:0b:0e:18:ee:24:75:6f:a2:fb:a0:dd:
            3c:a7:1a:95:4f:29:ce:8b:fe:62:5e:6e:2a:5a:8b:
            b6:df:9b:68:8e:f4:e1:3d:f3:74:e3:9b:b1:f1:32:
            c9:7a:9f:2a:1b:b3:a2:1d:9c:f0:4a:7e:6c:24:b1:
            af:69:15:4b:d1:fe:2e:d7:e2:f5:79:db:c6:f8:d8:
            30:60:4e:44:c5:b2:c0:ab:05:5b:0b:30:3c:87:b0:
            0f:09:f1:4c:1b:91:56:6c:c9:74:0d:84:a1:25:76:
            e0:ea:08:4d:77:48:43:69:59:69:59:d5:1b:03:ba:
            32:a1:43:88:b9:a2:87:cd:86:57:01:31:4b:b3:b2:
            3c:60:4f:85:de:a0:2b:10:55:7f:04:aa:6a:f3:e1:
            95:9c:31:a0:7a:f0:4c:22:56:d9:9a:d1:73:d5:59:
            1e:2f:fc:0a:d9:28:35:42:7b:41:54:06:00:05:38:
            78:cd
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints: critical
        CA:TRUE, pathlen:0
      X509v3 Subject Key Identifier:
        4E:20:84:A2:D5:A4:81:A5:48:4E:2F:96:DB:21:3D:C0:B6:8D:DB:EF
      X509v3 Authority Key Identifier:
        keyid:C6:6B:91:57:43:4E:5B:93:15:CA:C2:14:40:9E:2C:43:7E:EF:18:18

      X509v3 Key Usage:
        Certificate Sign, CRL Sign
      X509v3 Certificate Policies:
        Policy: 1.3.6.1.4.1.35539.3.3.4.3.3
          CPS: http://ssl.trustwave.com/CA/micros

  Signature Algorithm: sha1WithRSAEncryption
    7c:b1:68:39:3b:7a:31:cf:24:3d:36:91:19:3d:a2:ba:b2:63:
    f3:ab:81:c4:3f:1b:4b:59:fa:cb:b2:6d:4b:73:56:cf:67:ea:
    eb:23:9a:6f:46:64:9c:21:f2:9a:17:9c:c5:c9:ef:67:a5:49:
    ba:59:fb:6c:eb:e5:34:73:aa:a1:9b:81:e6:9a:5e:88:44:b7:
    0d:ff:89:ee:a5:db:e3:9a:5c:20:11:b3:6c:92:29:9a:d6:b6:
    13:2a:c2:a0:20:c2:61:b9:1e:65:12:12:45:49:8b:51:a5:d2:
    a7:1c:25:7a:98:d1:b3:43:96:68:0e:17:e7:a0:36:ff:55:07:
    e7:a3:56:91:ca:ce:27:91:16:71:97:5b:7b:76:80:42:3d:3e:
    fd:d0:17:ac:2c:45:cd:bd:5a:76:37:d1:05:ac:b9:25:e2:f4:
    0b:56:23:a2:46:7b:05:bd:bf:02:1e:3d:90:c3:a2:41:24:1b:
    8f:07:43:f4:fa:3f:67:6a:66:a5:5f:31:65:33:4f:e1:93:fe:
    f2:17:9f:c8:1f:6a:c8:8c:98:36:2f:02:dd:9f:15:97:6b:bc:
    d6:f5:73:83:38:3a:e2:4d:80:9c:a9:d0:46:ba:25:76:6e:e1:
    8c:0f:62:76:95:8b:1c:e5:c1:13:74:0b:6c:3e:f8:05:28:64:
    a7:4c:72:12
```