

Certificate Coordinator Agreement

This Certificate Coordinator Agreement (this “Agreement”) is made and entered into, as of the Effective Date, by and between IdenTrust Services LLC (“IdenTrust”), a Certification Authority, and

 (“Organization”).

RECITALS

- A. IdenTrust is a Certification Authority that issues, manages and revokes Certificates.
- B. Organization desires to designate employees or agents to act as Certificate Coordinators who may coordinate and/or perform one or more procedures related to Key Recovery, Renewal and Revocation of Certificates that were purchased with funds provided by Organization.
- C. IdenTrust and Organization enter into this Agreement as authorized by contract number T00-MST-001 between IdenTrust and the State of Washington, acting through the Department of Information Services, an agency of the Washington State Government (“DIS”).

AGREEMENT

THEREFORE, IdenTrust and Organization (the “Parties”) hereby agree as follows:

1. Appointment of Authorizing Official(s).

Organization shall appoint individuals to serve as its Primary Authorizing Official and other Authorizing Officials, and shall identify such individuals on a Schedule 1, in the form attached hereto, executed by Organization and delivered to IdenTrust. A Primary Authorizing Official will have authority on behalf of Organization to communicate with IdenTrust regarding all matters relating to this Agreement, including the authority to add or remove Authorizing Officials by notifying IdenTrust in writing. If at any time there are no currently named Authorizing Officials for Organization, the person signing this Agreement on behalf of Organization shall be its Primary Authorizing Official. Authorizing Officials will have the authority on behalf of Organization to appoint one or more other individuals as Certificate Coordinators who will have authority to obtain and use a Washington State High Assurance Level Certificate on behalf of the Organization.

2. Certificate Coordinator(s).

2.1 Appointment of Certificate Coordinator.

Organization may appoint Certificate Coordinators who may coordinate and/or perform one or more procedures related to recovery of archived confidentiality keys (“Key Recovery”), Renewal, or Revocation of Certificates. Other activities may include the delivery and collection of Hardware Tokens and information to and from Subscribers of Certificates purchased with funds provided by Organization. Certificate Coordinators shall be, and shall remain, the employees and agents of Organization and not IdenTrust. Subject to the terms of this Agreement, Organization may select its own manner of operation and IdenTrust is not responsible for the acts or omissions of, or the supervision, direction, or control of, Organization's Certificate Coordinators.

2.2 Appointment Process.

For purposes of authenticating communications with Certificate Coordinators, if they do not currently have a valid Washington State High Assurance Certificate, applicants shall be required to submit an application for same in accordance with IdenTrust's procedures for the issuance of such Certificates. Such application procedures shall include provisions that Certificate Coordinators agree with IdenTrust to protect their Private Keys and perform their duties with due diligence as set forth in the Washington State High Assurance Level Subscriber Agreement, the Certificate Policy, and this Agreement. Each Certificate Coordinator shall be appointed by Organization through submission to IdenTrust of an Authorization Form, signed by an Authorizing Official of the Organization.

2.3 Protection of Certificate Coordinator Private Keys.

Organization agrees that, in regard to each High Assurance Level Certificate issued to Certificate Coordinators, Organization will require all Certificate Coordinators to reasonably safeguard and maintain Private Keys (and any Activation Data used to protect Private Keys) in strict confidence, including without limitation, reasonable security measures to prevent unauthorized access to, or disclosure, loss, modification, compromise, or use of, Private Keys and the computer systems or media on which the Private Keys are stored. Organization is solely responsible for enforcing any restrictions it may impose upon the Certificate Coordinators' use of their High Assurance Level Certificates and will notify IdenTrust in the event such unauthorized acts occur and take such additional actions as specified in Section 2.4.

2.4 Supervision of Authorizing Officials and Certificate Coordinators.

Organization agrees to supervise Certificate Coordinators and to act promptly and halt any unauthorized actions by Authorizing Officials or Certificate Coordinators that may compromise the security or trustworthiness of the Public Key Infrastructure (PKI). Organization agrees to notify IdenTrust if an individual leaves the Organization or is no longer authorized to act as a Certificate Coordinator. Disciplinary steps may include, but are not limited to, notifying IdenTrust of potential key compromises, requesting revocation of any High Assurance Level Certificate issued to a Certificate Coordinator that has been used for an unauthorized purpose, and/or the immediate removal of the individual from the role of Certificate Coordinator or Authorizing Official.

3. Certificate Coordinator Resources.

Upon IdenTrust's receipt of (i) a fully executed copy of this Agreement, and (ii) the completion of the necessary Identification and Authentication of Organization's Primary Authorizing Official, IdenTrust will provide Organization with the hardware, software, forms, instructions, handbooks and other materials necessary to perform Certificate Coordinator functions. Organization may make copies of such documentation to the extent required for its use. Notwithstanding the foregoing, Organization agrees to distribute such documentation only to those individuals within Organization who have a need to know (e.g., Certificate Coordinators) and to keep such documentation secure for the trustworthy operation of the PKI.

Organization agrees to pay the applicable fee as set forth in the Schedule A, *Authorized Product and Price List*, of the Master Contract (DIS Contract Number T00-MST-001), for the Certificate Coordinator service, the issuance of each High Assurance Level Certificate for Certificate Coordinators, and any associated hardware resources necessary to perform Certificate Coordinator functions (e.g., hardware tokens, smart cards, card readers, etc.) in accordance with the applicable fee schedule.

4. Certificate Coordinator Functions.

4.1 Certificate Coordinators as Points of Contact with Subscribers.

For the purpose of determining which certificates have been purchased with funds provided by Organization, IdenTrust shall maintain records of certificates purchased using order numbers or voucher numbers issued to Organization by IdenTrust under a valid purchase order or other written purchase authorization. Subscribers may also inform IdenTrust in writing at the time of application for a certificate, or thereafter, that the Subscriber's certificate is being or was purchased with funds provided by Organization, and such Subscribers' certificates shall be added to IdenTrust's record of certificates purchased with funds provided by Organization. Certificate Coordinators may engage in the functions identified in subsections 4.2 and 4.3 herein only for Subscribers' certificates identified in IdenTrust's records in accordance with the above terms as having been purchased by Organization. In the event that Organization transfers, no longer holds, relinquishes or otherwise loses its right to control revocation or confidentiality key recovery of any Subscriber's certificate, it shall immediately notify IdenTrust when it learns of any such loss of the right to control such revocation or key recovery, so that IdenTrust may remove the Subscriber's certificate from the record of certificates for which the Organization may exercise Certificate Coordinator functions.

4.2 Certificate Revocation.

IdenTrust will revoke a Certificate upon receiving an Authenticated Instruction from a Certificate Coordinator to revoke a certificate purchased with funds provided by the Organization. Provided that the Certificate Coordinator has properly followed the revocation procedures established by IdenTrust for Certificate Coordinators, IdenTrust may rely conclusively upon, and shall incur no liability to Organization for acting in accordance with, any Authenticated Instructions to revoke a Certificate received from a Certificate Coordinator. Organization will be responsible for defining any additional rights, duties or obligations it deems necessary among Organization, Certificate Coordinators and Subscribers not inconsistent with this Agreement or applicable Certificate Policies or Subscriber Agreements.

4.3 Key Recovery for Confidentiality Keys.

Upon the receipt of an Authenticated Instruction from a Certificate Coordinator of Organization, IdenTrust will initiate a Key Recovery of the Confidentiality Key corresponding to a Certificate purchased with funds provided by the Organization. Provided that the Certificate Coordinator has properly followed the key recovery procedures established by IdenTrust for Certificate Coordinators, IdenTrust may rely conclusively upon, and shall incur no liability to Organization for acting in accordance with, any Authenticated Instructions to recover a Confidentiality Key received from a Certificate Coordinator. Organization will be responsible for defining any additional rights, duties or obligations it deems necessary among Organization, Certificate Coordinators and Subscribers not inconsistent with this Agreement, or applicable Certificate Policies or Subscriber Agreements applicable to the certificates for which the Certificate Coordinator has administrative responsibility.

5. Definitions

Activation Data: User IDs, passphrases, PINs, or shared secrets used to safeguard the Private Key from unauthorized viewing or use.

Authenticated Instruction: An instruction received by IdenTrust from a Certificate Coordinator whose identity has been authenticated by IdenTrust using systems and processes established by IdenTrust for such authentication, including but not necessarily limited to the validation of the Certificate Coordinator's High Assurance Level Certificate.

Authorizing Official: The person who signs this Agreement on behalf of Organization or a person who has been appointed by a Primary Authorizing Official, and thereby has the authority to appoint Certificate Coordinators on behalf of Organization, as further described in Sections 1 and 2 of this Agreement.

Certificate: A computer-based record or electronic message issued by an entity that: (i) identifies the entity issuing it; (ii) names or identifies a Certificate holder; (iii) contains the Public Key of the Certificate holder; (iv) identifies the Certificate's Validity Period; and (v) is digitally signed by the issuing entity. A Certificate includes not only its actual content but also all documents expressly referenced or incorporated in it.

Certificate Coordinator: A person who has been appointed by an Authorizing Official of the Organization, to perform the functions described in Section 4 of this Agreement.

Effective Date: The date of the last signature applied to this Agreement.

High Assurance Level Certificate: A Washington State High Assurance Certificate issued to a Subscriber pursuant to the terms set forth in Sections 1.1.2 and 3.1.8 of the State of Washington Certificate Policy and associated Certification Practice Statement.

Primary Authorizing Official: The person who signs this Agreement on behalf of Organization or a person employed by Organization who has the authority to appoint Authorizing Officials and Certificate Coordinators on behalf of Organization, as further described in Sections 1 and 2 of this Agreement.

Private Key: The key of a Key Pair kept secret by its holder and used to create Digital Signatures and to decrypt messages or files that were encrypted with the corresponding Public Key.

Public Key: The key of a Key Pair publicly disclosed by the holder of the corresponding Private Key and used by the recipient to verify Digital Signatures created with the corresponding Private Key and to encrypt messages or files to be decrypted with the corresponding Private Key.

Public Key Infrastructure: The hardware, software, people, processes and policies that employ Digital Signature technology to enable a verifiable association between the public component of an asymmetric Public Key and a specific Subscriber.

Subscriber: A person to whom a Certificate has been issued by IdenTrust. Certificate Coordinators perform the functions described in Section 4 of this Agreement for Subscribers who hold Certificates purchased with funds provided by Organization.

6. Notices

Any notices permitted or required under this Agreement will be in writing, and will be deemed given (i) when actually received, (ii) on the date of receipt as shown by proof of receipt, if sent by independent courier or by registered certified mail (return receipt requested), (iii) on the date sent when sent by facsimile with confirmation of receipt, or (iv) when available at the e-mail address of the receiving party if sent by e-mail with confirmation of receipt, at the applicable address indicated below:

To IdenTrust: IdenTrust Services, LLC Attention: Legal Department 255 North Admiral Byrd Road Salt Lake City, Utah 84116-3703 U.S.A.	OR	E-mail to legal@identrust.com OR Fax: 801-924-8138
--	----	---

To Organization: To the Primary Authorizing Official at the postal address, facsimile number, or e-mail address specified in Schedule 1.

Either party may from time to time change its address for notification purposes by giving the other prior notice, in conformance with this Section, of the new address and the date upon which it shall become effective.

SCHEDULE 1 - AUTHORIZING OFFICIALS

Primary Authorizing Official for Organization: _____

Name: _____ Title: _____

Business Address: _____

STREET ADDRESS SUITE/MAILSTOP

CITY STATE ZIP COUNTRY

Mailing Address: _____
(if different) STREET ADDRESS SUITE/MAILSTOP

CITY STATE ZIP COUNTRY

Phone: _____ FAX: _____ E-mail: _____

Authorizing Official:

Name: _____ Title: _____

Business Address: _____

STREET ADDRESS SUITE/MAILSTOP

CITY STATE ZIP COUNTRY

Mailing Address: _____
(if different) STREET ADDRESS SUITE/MAILSTOP

CITY STATE ZIP COUNTRY

Phone: _____ FAX: _____ E-mail: _____

Authorizing Official:

Name: _____ Title: _____

Business Address: _____

STREET ADDRESS SUITE/MAILSTOP

CITY STATE ZIP COUNTRY

Mailing Address: _____
(if different) STREET ADDRESS SUITE/MAILSTOP

CITY STATE ZIP COUNTRY

Phone: _____ FAX: _____ E-mail: _____
