IdenTrust
WE PUT THE TRUST IN IDENTITY

TrustID Business Certificate
Part I – Sponsoring Organization Authorization Form

This TrustID Business Certificate Authorization Agreement (this "Authorization Agreement") is made by and between IdenTrust Services, LLC, ("IdenTrust") a Delaware limited liability company with its principal place of business at 255 North Admiral Byrd Road, Salt Lake City, Utah 84116-3703 U.S.A (www.IdenTrust.com), and the Organization identified at the bottom of this Authorization Agreement ("Sponsoring Organization").

1. Effect of Trust ID Business Certificate Issuance

IdenTrust is a Certification Authority that issues digital certificates to employees, agents and other individuals (e.g., licensed professionals) affiliated with Sponsoring Organization ("Affiliated Individuals"). Each TrustID® business certificate identifies its named holder (i.e. its "Subject") as employed, associated or otherwise affiliated with the Organization. However, TrustID business certificates establish identity, not authority, and do not establish authority to bind the Organization—such authority would be established by other means between the parties relying on the digital certificate and Sponsoring Organization. Sponsoring Organization authorizes IdenTrust to issue a TrustID business certificate to the Affiliated Individual listed below. Prior to issuing a TrustID business certificate that identifies a person as affiliated with Sponsoring Organization, IdenTrust must confirm that the person is indeed affiliated with the Sponsoring Organization, and Sponsoring Organization agrees that the information it provides to IdenTrust concerning an Affiliated Individual's status with the Sponsoring Organization will be accurate, current and complete. Sponsoring Organization agrees to be bound by and accepts the terms and conditions of the attached TrustID Business Certificate Agreement that is presented to the Affiliated Individual on IdenTrust's web site during the application process. Sponsoring Organization further acknowledges and agrees that the act or omission of the Affiliated Individual with respect to a TrustID business certificate authorized hereunder will be deemed for all purposes to be the act or omission of Sponsoring Organization.

2. Certificate Renewal

Sponsoring Organization understands and acknowledges that the TrustID business certificate issued to the Affiliated Individual identified below will expire after its stated period of validity, and that prior to expiration the Affiliated Individual may apply for and receive a renewal TrustID business certificate to replace his or her expiring certificate. Sponsoring Organization hereby authorizes the Affiliated Individual to apply for and receive, and authorizes IdenTrust to issue, successive renewal TrustID business certificates, provided that the Affiliated Individual applies for the renewal TrustID business certificate within the required time frames for such renewal. Sponsoring Organization acknowledges and agrees that IdenTrust my require the Affiliated Individual to execute a new Certificate Agreement each time he or she applies for a renewal Certificate, and the Sponsoring Organization will be bound by the terms of each such Certificate Agreement.

3. Certificate Revocation

Sponsoring Organization must immediately request that the Certificate be revoked if: (i) it ever discovers or suspects that the Private Key corresponding to the Certificate has been or is in danger of being lost, disclosed, compromised or subjected to unauthorized use in any way, or (ii) any information in the Certificate is no longer accurate, current, or complete or becomes misleading, including if the Affiliated Individual is no longer affiliated with Sponsoring Organization.

4. Term and Termination

The terms of this Authorization Agreement shall run from the date indicated below until all TrustID business certificate issued to the Affiliated Individual, and all subsequent renewal Certificates, have been revoked, have expired or are no longer valid. If Sponsoring Organization desires to terminate this Authorization Agreement and all corresponding Certificate Agreements, then it must give notice to IdenTrust, in which case IdenTrust shall revoke all outstanding TrustID business certificates authorized hereunder.

5. Interpretation

Irrespective of the place of performance, this Authorization Agreement shall be construed, interpreted, and enforced in accordance with the substantive laws of the State of Utah, without regard to its conflicts of law principles. Capitalized terms used but not defined here in shall have the meanings indicated in the TrustID Business Certificate Agreement. If any provision hereof is found invalid, illegal or unenforceable, then the remaining provisions shall be construed to give maximum effect to the intent of the parties as evidenced by this Agreement.

Applicant: Carl James Adams-Collier ← (PRINT APPLICANT'S FIRST, MIDDLE, LAST NAME)

Applicant's Email: cjac@colliertech.org

Organization Name: Collier Technologies LLC

Headquarters Address: ~~85 Raccoon Point Road~~

Address Line 2: 17 Bartel Road

City, State, Zip: Eastsound, WA, 98245-1986

By: ____________________ ____________

Authorized Signer Signs Here Date
(eg. Local Registration Agent, Trusted Agent, Certificate Coordinator, Security Officer, Etc.)

C. J. Adams-Collier, Member
Print Name and Title of Authorized Sianer Here

IdenTrust

WE PUT THE TRUST IN IDENTITY

TrustID Business Certificate
Part II - Notary Form

Terms and Conditions

The undersigned applicant warrants, represents, and attests that all facts and information provided in Parts I and II are, to the best of the undersigned applicant's knowledge, accurate, current and complete and that he or she: a) Is authorized by his or her Organization to receive and use an ACES digital certificate to be issued by IdenTrust; b) Has read and accepts the personal identifying information set forth herein; c) Is who he or she represents himself or herself to be; and d) Has read, understood, and agrees to the responsibilities associated with being a Subscriber of an ACES Business Representative Certificate, including the terms and conditions found in the on-line ACES Business Representative Certificate Agreement. The applicant agrees to: 1) accurately represent him or herself in all communications with IdenTrust and Relying Parties; 2) protect his or her private key at all times; 3) immediately notify IdenTrust if he or she suspects his or her private key to have been compromised, stolen or lost; and 4) use his or her key only for authorized business as allowed by the ACES Program.

Identification - Complete this section entirely. Incomplete forms will be returned.

You must present 2 forms of ID for verification. At least one of the two must be a verifiable government-issued photo ID.

One verifiable government-issued Photo ID such as Passport, Driver's License, State ID Card w/ photo, Military ID card w/ photo, etc.

Photo ID

Doc. Type/ Title: U.S. Passport

Issuer: Seattle Passport Agency

Serial No: 0774 15086

Exact Name: Carl James Collier

Issue Date: 01 Dec 2004

Expir. Date: 30 Nov 2014

Other acceptable forms of ID include Certified Copy of Birth Certificate, Social Security Card, Student ID, Concealed Weapons Permit, Pilot's License, etc.

Second ID

Doc. Type/ Title: Washington Driver License

Issuer: Washington State Department of Licensing

Serial No: Colli-CJ-212NQ

Exact Name: Carl James Collier

Issue Date: 9-14-2009

Expir. Date: 8-20-2011

Signed By: ______________________ **(Subscriber to sign only in the presence of Notary)**

Print Name: Carl James Adams-Collier
First Name Middle Initial Last Name

Email Address: cjac@colliertech.org
(Same email address as provided online)

Notarial Acknowledgement

I ______________________ (name of notary/officer), registered in the state of __________, county of ______________ do hereby certify under PENALTY OF PERJURY under the laws of the State of ________ that the following information is true and correct:

1. On __________ (date), before me personally appeared ______________________ (name of signer), who proved to me on the basis of satisfactory evidence to be the person whose name is subscribed to the within instrument and acknowledged to me that he/she executed the same in his/her authorized capacity, and that by his/her signature on the instrument the person, or the entity upon behalf of which the person acted, executed the instrument.

2. I have seen and verified the forms of identification for which information is written above and hereby assert that said forms of ID do not appear to be altered, forged or modified in any way.

WITNESS my hand and official seal

Signature ______________________ (Seal)

Coalfire
IT Audit and Compliance

Audit required for 434-180-240 WAC

361 Centennial Parkway
Suite 150
Louisville, Colorado 80027
Tel: (303) 554-6333

Master Services and License Agreement

CLIENT:			
BILLING ADDRESS:			
CLIENT CONTACT:		CONTACT PHONE:	
CONTACT E-MAIL:		CONTACT FAX:	
PURCHASE ORDER NO.:		COALFIRE ACCOUNT MGR.:	Ryan McGowan

TERMS AND CONDITIONS

This Master Services and License Agreement, consisting of this cover page and the terms and conditions on the following pages hereof, together with any schedules attached hereto and incorporated herein by reference (the "Agreement"), is made and entered into as of the Effective Date set forth below by and between Coalfire Systems, Inc. ("Coalfire"), and the Client identified below ("Client"). Pursuant to the terms hereof, Client may purchase or license from Coalfire, and Coalfire agrees to sell or license to Client, the services identified and described in one or more service orders executed by each of Client and Coalfire from time to time (each, a "Service Order"), which are appended hereto and incorporated herein by reference and are, therefore, subject to the terms and conditions of this Agreement. Terms that are initially capitalized but not otherwise defined in a Service Order shall have the meaning given to such terms in this Agreement. In the event of a conflict or inconsistency between the terms and conditions of a Service Order and this Agreement, the terms of each Service Order shall control, but only with respect to the Services described therein. Each Service Order, together with the terms and conditions of this Agreement, shall constitute a separate contract.

CLIENT ACKNOWLEDGES THAT CLIENT HAS READ THIS AGREEMENT AND AGREES TO ALL ITS TERMS AND CONDITIONS. CLIENT FURTHER ACKNOWLEDGES THAT CLIENT IS NOT RELYING ON ANY REPRESENTATION, GUARANTEE, OR STATEMENT OTHER THAN AS EXPRESSLY SET FORTH IN THIS AGREEMENT.

EXECUTED BY CLIENT AND COALFIRE SYSTEMS, INC. INTENDING TO BE LEGALLY BOUND.

EFFECTIVE DATE:

CLIENT:		COALFIRE SYSTEMS, INC.	
X		X	
AUTHORIZED SIGNATURE (ABOVE)		AUTHORIZED SIGNATURE (ABOVE)	
NAME PRINTED:		NAME PRINTED:	Alan Ferguson
TITLE:		TITLE:	Vice President
DATE:		DATE:	

GENERAL TERMS AND CONDITIONS

1. Services and Deliverables. The services to be performed (the "Services"), and the deliverables to be delivered (the "Deliverables"), hereunder by Coalfire or by its subcontractors are those described in the applicable Service Order. Subject to the terms and conditions of this Agreement and the applicable Service Order, Coalfire may sell or license to Client, and Client may purchase or license one or more of the following Services:

(a) security assessment services, as further described in the Security Assessment Services Schedule;

(b) IT compliance assessment and management solutions and services, as further described in the Compliance Assessment and Management Solutions Schedule; or

(c) IT audit, control development, IT risk assessment, incident response and consulting services.

2. Fees, Expenses, Taxes.

(a) Fees. Client will pay Coalfire for Services provided hereunder at Coalfire's standard hourly billing rates or fees stated in the applicable Service Order, plus materials stated on any bill of materials that are part of a Service Order (collectively, the "Fees"). Client further agrees to reimburse Coalfire for reasonable travel and living expenses incurred by Coalfire in connection with the performance of Services. Expenses shall be billed in accordance with Coalfire's Travel and Expense Policy, available upon request.

(b) Payment. All Fees are non-refundable. Unless otherwise expressly stated in a Service Order, Coalfire's invoices are due and payable by Client in full within thirty (30) days from the invoice date. Undisputed invoiced amounts not paid when due will bear interest from the due date until paid at a rate of one percent (1.0%) per month or the maximum rate permitted by applicable law, whichever is less.

(c) Taxes. The Fees exclude all applicable sales, use, and other taxes, and all applicable export and import fees, customs duties and similar charges attributable to any use by Client of the Services, and Client will be responsible for payment of all such taxes (other than taxes based on Coalfire's income), fees, duties, and charges, and any related penalties and interest, arising from the payment of the Fees or the delivery, provision or license of the Services to Client.

3. Term, Termination.

(a) Term. This Agreement is effective upon the Effective Date and, unless earlier terminated in accordance with the terms hereof, shall continue in full force for an initial term of one (1) year (the "Initial Term"). Thereafter, this Agreement shall automatically renew for successive periods of one (1) year each (each, a "Renewal Term" and together with the Initial Term, the "Term") unless either party provides written notice of its intent not to renew at least thirty (30) days prior to the expiration of the then-current Initial Term or Renewal Term.

(b) Termination without Cause. Either party may terminate this Agreement at any time upon thirty (30) days' prior written notice to the other party, provided that with respect to outstanding Service Orders, termination shall be effective only upon completion or termination of the Service Order.

(c) Termination for Cause. Notwithstanding the above, if either party is in material breach of the Agreement, the non-breaching party may terminate the Agreement and any outstanding Service Order(s) upon thirty (30) days' prior written notice describing in reasonable detail the material breach, provided that the breaching party has not cured such material breach during the aforementioned notice period.

(d) Service Period. The period of performance of any Services provided hereunder shall be set forth in the applicable Service Order. To the extent that the period of performance for any Service extends beyond the Term of this Agreement, then this Agreement shall remain in full force and effect with respect to such Service until the expiration or termination of such Service Order.

(e) Effect of Termination. Upon the termination of this Agreement or a Service Order (i) by Client as set forth in Section 3(b) above, or (ii) by Coalfire due to Client breach as set forth in Section 3(c) above, then (1) all rights granted herein, including without limitation to the Software, as applicable, shall immediately revert to Coalfire and no residual rights will remain with Client, (2) Client and any Authorized Users (as such term is defined in **Schedule B**) shall immediately discontinue all access to and use of any Software (as such term is defined in **Schedule B**), (3) Client shall immediately return to Coalfire, or at Coalfire's request, destroy, any Confidential Information (as defined in Section 10, below) in Client's possession or control, (4) Client shall immediately pay all Fees associated with Client's account, and (5) upon request, certify to Coalfire in writing that Client has complied with the foregoing obligations. If the Services requested by Client in a Service Order include any PCI DSS assessments, then notwithstanding anything in this Agreement to the contrary, Client acknowledges and agrees that Coalfire is required to, and may, comply with the record retention policies of PCI DSS, including without limitation securing and maintaining digital and/or hard copies of case logs, audit results and work papers, notes, and any technical information that was created and/or obtained during the PCI DSS assessment for a minimum of three (3) years.

4. Client Acknowledgements, Cooperation.

(a) Client acknowledges and agrees that (i) any outcome of the Services involving compliance assessment is limited to a point-in-time examination of Client's compliance or non-compliance status with the applicable standards or industry best practices set forth in the Service Order and that the outcome of any audits, assessments or testing by, and the opinions, advice, recommendations and/or certification of, Coalfire do not constitute any form of representation, warranty or guarantee that Client's systems are 100% secure from every form of attack, and (ii) in examining Client's compliance or non-compliance status, Coalfire relies upon accurate, authentic and complete information provided by Client as well as use of certain sampling techniques.

(b) Client will reasonably cooperate with Coalfire and take all actions reasonably necessary to enable Coalfire to perform the Services contemplated herein in an effective and efficient manner. To that end, Client will provide on a timely basis all information, as well as access to systems and personnel, reasonably required to enable Coalfire to provide the Services. Client will remain responsible for the management of any third parties engaged by Client, which includes the quality, accuracy and timely provision of information and work by them. Client is responsible for informing Coalfire immediately of any changes to the information presented to Coalfire. If Client believes that Coalfire has misunderstood or failed to take account of relevant facts or circumstances, it will promptly inform Coalfire of such belief. Accordingly, Coalfire shall be entitled to assume that it is authorized to act on the instructions, oral, written or electronic, of any member of Client's staff unless expressly instructed otherwise.

(c) Client acknowledges and agrees that Client is responsible for selecting Services and Deliverables that allow Client to: (i) meet Client's business requirements; and (ii) comply with all federal, state and local laws, ordinances, code(s) and regulations and policies applicable to Client.

(d) Notwithstanding anything in this Agreement to the contrary, Client acknowledges and agrees that Coalfire may, without liability to Client or its Related Parties, take any and all actions reasonably necessary to comply with federal, state and local laws, ordinances, codes and regulations applicable to Coalfire. Coalfire shall use reasonable efforts to notify Client of any action taken pursuant to this Section based upon the circumstances solely to the extent that such notice is permitted under applicable law and authorized by appropriate authorities.

5. Warranties, Indemnification, Insurance.

(a) Coalfire Representations, Warranties and Covenants.

(i) Coalfire represents and warrants that (1) Coalfire and its employees, consultants and subcontractors ("Coalfire Personnel") performing Services have the necessary knowledge, skills, experience, qualifications, and resources to perform the Services in accordance with the Service Order, and (2) Coalfire will perform the Services and provide the Deliverables in accordance with the specified standards set forth in the applicable Service Order(s). If any portion of the Services or Deliverables do not conform to the forgoing in all material respects, and Client notifies Coalfire within sixty (60) days of completion of the Services and delivery of Deliverables, specifying in reasonable detail the reasons the Services or Deliverable do not conform, then Coalfire will work diligently to re-perform the nonconforming portion of the Services and redeliver the nonconforming portion of the Deliverables so that they conform to the Service Order in all material respects. If the preceding remedies are not fulfilled by Coalfire within a reasonable time, upon request by Client, Coalfire may terminate this Agreement and refund the price paid for the nonconforming portion of the Services and refund the price paid for nonconforming Deliverables that are returned to Coalfire. Coalfire will not be responsible for nonconformities arising from inaccurate, inauthentic or incomplete data or information provided by Client, or for failures or delays arising from lack of cooperation of Client.

(ii) Coalfire covenants that it and Coalfire Personnel performing the Services, while present at the facilities of Client, will comply with the written security and safety policies of Client that are provided to Coalfire in advance.

(b) Client Representations and Warranties. Client represents and warrants that, with respect to any and all data and other information disclosed or made available, or to be disclosed or made available, to Coalfire by it or by any third party acting on its behalf, (i) where such data and/or information is based on assumptions, Client will advise Coalfire of the same, and (ii) all such data and information is and will be accurate, authentic, complete and not misleading in any respect.

(c) Coalfire Indemnity Obligations.

(i) Coalfire shall defend, indemnify, and hold harmless Client and its affiliates and its and their respective officers, owners, directors, employees, contractors and agents (collectively, "Client Related Parties") from all losses, causes of action, claims, allegations, liabilities, costs, damages and expenses whatsoever (including, without limitation, reasonable attorneys' fees), regardless of the form of action ("Claim"), and shall promptly reimburse Client for, all Claims to the extent specifically attributable to a third party claim that the Services or Deliverables or Software, as applicable, infringe a third party copyright or trademark or misappropriates any third party trade secret, where such rights arise or are enforceable under the laws of the United States ("Claim of Infringement"). If, in Coalfire's opinion, any Service or Deliverable or Software, as applicable, infringes or misappropriates any intellectual property right of a third party, then Coalfire may procure the right for Client to continue to use the results of the Service or Deliverable or Software, or may re-perform the Service or replace the Deliverable or Software so that it is non-infringing and meets the original specifications in all material respects. If the preceding remedies are not reasonably available, as determined by Coalfire, Coalfire may terminate this Agreement or the applicable Service Order and refund the price paid for the infringing portion of the Deliverables that are returned to Coalfire or the Services. Notwithstanding the foregoing, Coalfire will have no obligation under this Section with respect to any Claim of Infringement based upon and that would not have occurred but for (1) any data, information or materials furnished by Client to Coalfire; (2) any use of the Services or Deliverables or Software not in accordance with this Agreement or in violation of any applicable law, or for purposes not intended by Coalfire, (3) any use of the Services or Deliverables or Software in combination with products, equipment, material, content, information or data not supplied by Coalfire where the combination is the basis of the claim, or (4) any modification of the Services or Deliverables or Software by any person other than Coalfire Personnel. In the foregoing cases (1) through (4), Client shall defend, indemnify and hold Coalfire and its affiliates and its and their respective officers, owners, directors, employees, contractors and agents (collectively, "Coalfire Related Parties") harmless with respect to such claims. The foregoing is the sole and exclusive remedy of Client and states the entire liability of Coalfire with respect to infringements or misappropriation of any proprietary rights by the Services or Deliverables or Software.

(ii) Coalfire shall defend, indemnify and hold harmless Client and Client Related Parties from and against any and all losses, causes of action, claims, allegations, liabilities, costs, damages and expenses whatsoever (including, without limitation, reasonable attorneys' fees), regardless of the form of action ("Claim"), and shall promptly reimburse Client for all Claims, to the extent arising out of Coalfire's or Coalfire's Related Parties' acts or omissions related to the subject matter of this Agreement that constitute gross negligence or willful misconduct.

(d) Client Indemnity Obligations. Client shall defend, indemnify and hold harmless Coalfire and Coalfire Related Parties from and against any and all losses, causes of action, claims, allegations, liabilities, costs, damages and expenses whatsoever (including, without limitation, reasonable attorneys' fees), regardless of the form of action ("Claim"), and shall promptly reimburse Coalfire for all Claims, arising out of or in connection with Client's Related Parties': (i) breach or alleged breach of any representation or warranty set forth in Section 5(b) of this Agreement, or (ii) acts or omissions (including negligence or strict liability) giving rise to any third party claim or action based on, arising out of or relating to Client's data or use of the Services or Deliverables in violation or alleged violation of any applicable law.

(e) Indemnification Procedures. Each party that seeks to be indemnified under Section 5(c) or 5(d) must: promptly notify in writing the indemnifying party of any such suit or claim; permit the indemnifying party to defend, compromise, or settle same; and provide all available information and reasonable assistance to the indemnifying party to enable the indemnifying party to do so.

(f) Insurance. The parties will each maintain (i) general liability insurance having a combined single limit of $2,000,000 and (ii) worker's compensation insurance as required by applicable laws. Additionally, Coalfire shall, at its sole cost and expense, maintain in effect at all times during the term of this Agreement, professional liability insurance coverage, provided on a Claims Made Form, having a limit of $2,000,000. Evidence of the insurance coverages required to be maintained by each party under this Agreement, represented by certificates of insurance issued by insurance carrier(s), must be furnished to the other party upon written request.

(g) Disclaimer. Except for the representations and warranties expressly stated in this Agreement or any Service Order, ALL SERVICES, DELIVERABLES AND THIRD-PARTY PRODUCTS ARE PROVIDED **AS IS**, WITHOUT WARRANTIES OR REPRESENTATIONS OF ANY KIND. THE PROVISIONS OF THIS SECTION 5 ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER REPRESENTATIONS AND WARRANTIES, WRITTEN OR ORAL, STATUTORY, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTY OF TITLE AND NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

6. Limitations of Liability. IN NO EVENT WILL CLIENT, ON THE ONE HAND, OR COALFIRE AND/OR ITS LICENSORS (INCLUDING WITHOUT LIMITATION THE PCI SECURITY STANDARD COUNCIL AND ITS MEMBERS AND ANY OTHER APPLICABLE STANDARDS ORGANIZATION) (EACH A "**COALFIRE LICENSOR**"), ON THE OTHER HAND, BE LIABLE TO THE OTHER, WHETHER IN CONTRACT, TORT OR ANY OTHER LEGAL THEORY (INCLUDING, WITHOUT LIMITATION, STRICT LIABILITY AND NEGLIGENCE), FOR LOST PROFITS OR REVENUES, LOSS OF USE OR LOSS OF DATA, OR FOR ANY INDIRECT, SPECIAL, EXEMPLARY, PUNITIVE, MULTIPLE, INCIDENTAL, CONSEQUENTIAL OR SIMILAR DAMAGES, ARISING OUT OF OR IN CONNECTION WITH THE SERVICES OR DELIVERABLES, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. WITH THE EXCEPTIONS OF COALFIRE'S INDEMNITY OBLIGATIONS UNDER SECTION 5(C) (COALFIRE INDEMNITY OBLIGATIONS), AND COALFIRE'S LIABILITY ARISING AS A RESULT OF BREACH OF SECTION 10 (CONFIDENTIALITY), IN NO EVENT WILL THE LIABILITY OF COALFIRE AND ALL COALFIRE LICENSORS EXCEED, IN THE AGGREGATE, AN AMOUNT EQUAL TO THE TOTAL AMOUNT OF FEES ACTUALLY PAID BY CLIENT TO COALFIRE UNDER THE APPLICABLE SERVICE ORDER. WITH RESPECT TO COALFIRE'S INDEMNITY OBLIGATIONS UNDER SECTION 5(C) (COALFIRE INDEMNITY OBLIGATIONS) AND COALFIRE'S LIABILITY ARISING AS A RESULT OF BREACH OF SECTION 10 (CONFIDENTIALITY), IN NO EVENT WILL THE LIABILITY OF COALFIRE AND ALL COALFIRE LICENSORS EXCEED, IN THE AGGREGATE, THE AMOUNT OF INSURANCE COVERAGE REQUIRED BY SECTION 5(F). No action regarding the Services or Deliverables, regardless of form, may be brought more than one (1) year after the first to occur of either (a) the conclusion of Services and delivery of any Deliverables under the Service Order, or (b) such party's knowledge of the event giving rise to such cause of action. This limitation on actions does not apply to confidentiality obligations or the limited license of Section 8 regarding Deliverables.

7. Place of Performance. The Services to be performed pursuant to a Service Order may be rendered at Client's, Coalfire's, or subcontractor's facilities or at other suitable locations mutually agreed by Coalfire and Client.

8. Ownership of Deliverables. The parties agree that all documentation provided as a Deliverable ("Documentation") will be the property of Client, *provided, however, that* Client acknowledges and agrees that Coalfire has certain Intellectual Property Rights (as defined below) covering the subject matter within such Documentation and that, except as provided in a written agreement from Coalfire, Client does not and will not receive any right, title or interest in or to such Intellectual Property Rights, with the sole exception of the license right to make a reasonable number of copies of the Documentation solely for Client's internal business purposes. Coalfire may freely use the ideas, concepts, know-how, and techniques that it develops during the course of providing Services and Deliverables under this Agreement or a Service Order. For purposes of this Section 8, "Intellectual Property Rights" means any and all copyright, trade secret, patent, patent application, trademark and other intellectual property rights worldwide.

9. Cancellation Policy. Coalfire and the Client may agree to a start date to commence services under a Service Order. Except as otherwise expressly provided for in a Service Order, once such start date is agreed to, Client agrees to furnish Coalfire with at least ten (10) business days prior written notice of Client's intention to delay or cancel a Coalfire staffing assignment under the associated Service Order. If Client delays or cancels a Coalfire staffing assignment without providing such 10 day notice, then Client agrees to pay Coalfire up to forty (40) hours at the hourly rate specified in the associated Service Order for each Coalfire personnel so delayed or cancelled. Coalfire agrees to use all reasonable means available to it to mitigate any losses that would otherwise be incurred in connection with such cancellation and to apply such mitigation to any amounts charged to Client.

10. Confidential Information.

(a) Defined. "Confidential Information", as used in this Agreement, means all information proprietary to a party or any of its customers or suppliers that is marked as confidential or that due to its nature is known or in good faith should be known to be confidential. Confidential Information of Client will be deemed to include, without limitation, all data to which Coalfire obtains access by performing the Services and any Deliverable containing such data. Confidential Information of Coalfire will be deemed to include, without limitation, its methodologies, templates, report, policy and plan formats, Deliverables (except Client's data), scripts and tools. The obligations of the party ("Receiving Party") that receives Confidential Information of the other party ("Disclosing Party") with respect to any particular portion of the Disclosing Party's Confidential Information shall not attach or shall terminate, as the case may be, when any of the following occurs (i) it was in the public domain or generally available to the public at the time of disclosure to the Receiving Party, (ii) it entered the public domain or became generally available to the public through no fault of the Receiving Party subsequent to the time of disclosure to the Receiving Party, (iii) it was or is furnished to the Receiving Party by a third parity having the right to furnish it with no obligation of confidentiality to the Disclosing Party, or (iv) it was independently developed by the Receiving Party by individuals not having access to the Confidential Information of the Disclosing Party.

(b) Obligations. The Receiving Party agrees not to disclose or use any Confidential Information of the Disclosing Party in violation of this Agreement and to use Confidential Information of the Disclosing Party solely for the purposes of this Agreement. Upon demand by the Disclosing Party, the Receiving Party shall return to the Disclosing Party all copies of the Disclosing Party's Confidential Information in the Receiving Party's possession or control and destroy all derivatives and other vestiges of the Disclosing Party's Confidential Information; provided that the Receiving Party may retain one archival copy solely for the purpose of administering its obligations under this Agreement.

(c) Need to Know. The Receiving Party may disclose Confidential Information of the Disclosing Party to Receiving Party's employees, officers, directors, representatives, subcontractors and consultants who have a reasonable need to know such Confidential Information for purposes of this Agreement. Before disclosing Confidential Information to any subcontractor or consultant, the Receiving Party will obtain the agreement, in writing, of such subcontractor or consultant to undertake non-disclosure obligations with respect to the Confidential Information similar to those set forth in this Section 10.

(d) Ownership. All Confidential Information of the Disclosing Party shall remain the exclusive property of the Disclosing Party.

(e) Injunction. Both parties agree that violation of any provision of this Section would cause the Disclosing Party irreparable injury for which it would have no adequate remedy at law, and that the Disclosing Party will be entitled to immediate injunctive relief prohibiting such violation, in addition to any other rights and remedies available to it. The Receiving Party also waives any requirement for the posting of a bond by Disclosing Party in an action for specific performance, or for a temporary or permanent injunction, to enforce this Section of the Agreement.

11. Use of Name and Publicity. Each party agrees that it will not, without prior written consent of the other party, use in advertising, publicity or otherwise the name of such party or any of its affiliates, or any partner or employee of such party or its affiliates, nor any trade name, trademark, service mark, logo or slogan of such party or its affiliates. Notwithstanding the preceding sentence and Section 10 above, and unless Client provides Coalfire with written notice to the contrary, Coalfire may identify Client as one of Coalfire's clients.

12. Notices. All notices and other communications required or permitted to be given or made pursuant to this Agreement will be in writing and deemed delivered one (1) day after being sent by a nationally recognized overnight courier service or three (3) days after being sent certified U.S. mail, return receipt requested, postage prepaid. All notices and other communications under this Agreement will be given to the party at the address indicated in this Agreement.

13. Non-solicitation and Contracting. During or for a period of twelve (12) months after conclusion of the Services set forth in a particular Service Order, neither party shall solicit to hire as an employee or independent contractor any employee of the other party without the prior written consent of such other party. Publications of open positions in media of general circulation, including without limitation websites, will not constitute solicitation by either party.

14. General.

(a) Assignment. Neither party may assign, subcontract or otherwise transfer any of its rights or obligations under this Agreement without the express written consent of the other party, such consent not to be unreasonably delayed, conditioned or withheld. Any attempted assignment or transfer in violation of the foregoing will be void. This Agreement shall be binding upon, and shall inure to the benefit of, the parties hereto and their respective permitted successors and assigns. For the purposes of this Agreement, a change of control shall not be considered an assignment, subcontract or transfer of rights hereunder.

(b) Attorneys' Fees. If any party shall commence any action or proceeding against the other in order to enforce the provisions of this Agreement or to recover damages as the result of the alleged breach of any of the provisions of this Agreement, then the prevailing party therein shall be entitled to recover all reasonable costs incurred in connection therewith, including reasonable attorneys' fees.

(c) Construction. The captions and headings contained herein are for purposes of convenience only and are not a part of this Agreement; all references to this Agreement and the words "herein", "hereof", "hereto" and "hereunder" and other words of similar import refer to this Agreement as a whole and not to any particular Section or other subdivision; and the words "including," "included" and "includes" mean inclusion without limitation. Client acknowledges that the terms of this Agreement result from substantial negotiation between the parties during which both parties had the opportunity to review and revise the terms of the Agreement. Accordingly, this Agreement shall not be construed against any party on the grounds that such party drafted this Agreement. Instead, this Agreement shall be interpreted as though drafted equally by the Parties. This Agreement and any Schedules and Service Orders attached hereto shall be construed as consistent with one another whenever possible; however, in the event of any conflict between any of the terms and conditions of this Agreement and the Schedules or Service Orders, the terms and conditions of the Schedules or Service Orders shall prevail, but only with respect to the Services described in such Schedule.

(d) Counterparts. This Agreement and any Service Order may be executed in any number of counterparts, each of which shall be deemed an original, and all of which together shall constitute one and the same agreement. Delivery of an executed counterpart of this Agreement and any Service Order by facsimile or any other reliable means shall be effective for all purposes as delivery of a manually executed original counterpart.

(e) Dispute Resolution. This Agreement is made under and will be construed in accordance with the laws of the State of Colorado, other than such laws, rules, regulations and case law that would result in the application of the laws of a jurisdiction other than the State of Colorado. This Agreement will not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded. The parties agree that exclusive venue for any dispute arising under or in connection with this Agreement shall be in the federal district court for the District of Colorado or the state court for the City and County of Denver, Colorado. Each party hereby agrees that such courts shall have in personam jurisdiction and venue with respect to such party, and each party hereby submits to the in personam jurisdiction and venue of such courts and waives any objection based on inconvenient forum.

(f) Electronic Signatures. Coalfire and Client agree, and hereby state their collective intent, to conduct transactions via electronic means. Accordingly, Client represents that Client's email system includes security measures of sufficient efficacy (e.g., password protection) that any electronic correspondence from such email address that refers to this Agreement and/or any Service Order shall: (i) constitute sufficient evidence to establish the identity of Client as the sender of such electronic correspondence; (ii) be effective as confirmation of Client and Coalfire's intent to conduct transactions by electronic means; (iii) be effective as delivery by Client of a manually executed counterpart to this Agreement and/or the Service Order referenced in the electronic correspondence; and (iv) indicate Client's acceptance of the terms of, and intent to authenticate and sign, this Agreement and/or the Service Order referenced in the electronic correspondence. For the avoidance of doubt, Client expressly agrees that any such response or confirmation issued by or on behalf of Client will constitute an electronic signature, enforceable under all applicable laws and shall be determined to have been sent by Client.

(g) Entire Agreement. This Agreement constitutes the entire agreement between the parties with respect to its subject matter and supersedes all prior proposals, agreements, negotiations, correspondence and other communications, whether written or oral, between Coalfire and Client.

(h) Force Majeure. Neither party shall be responsible to the other for any failure or delay in its performance under this Agreement (other than for failure or delay in the payment of money due and payable hereunder) to the extent said failures or delays are proximately caused by any condition beyond that party's reasonable control and occurring without its fault or negligence, including, without limitation, Acts of God, wars, insurrections, act of terrorism, riot, strike, fire, sabotage, flood, or other natural disaster, catastrophe, or other similar cause outside the reasonable control of the affected party.

(i) Independent Contractors. Coalfire and Client are independent contractors, each acting for its own account, and neither is authorized to make any commitment or representation, or incur any obligation, express or implied, on the other's behalf. In all matters relating to this Agreement, neither party or its employees or agents are, or will act as, employees of the other party within the meaning or application of any applicable laws.

(j) No Third Party Beneficiaries. No term or provision of this Agreement is intended to be, or shall be, for the benefit of any person, firm, organization or corporation not a party hereto, and no such third party shall have any right or cause of action hereunder.

(k) Remedies. Except as otherwise expressly provided in this Agreement, in addition to any remedies provided in this Agreement, the parties shall have all remedies provided at law or in equity. The rights and remedies provided in this Agreement or otherwise under applicable law shall be cumulative and the exercise of any particular right or remedy shall not preclude the exercise of any other rights or remedies in addition to, or as an alternative of, such right or remedy, except as expressly provided otherwise in this Agreement.

(l) Severability. In the event that a court of competent jurisdiction holds any provision of this Agreement invalid or unenforceable in any circumstances, the remainder of this Agreement, and the application of such provision in any other circumstances, will not be affected thereby. The parties authorize the court to modify any invalid or unenforceable provision to the extent necessary to make it enforceable under the circumstances.

(m) Survival. The rights and obligations of the parties set forth in Sections 2 (Fees, Expenses, Taxes), 3(e) (Effect of Termination), 4 (Client Acknowledgements, Cooperation), 5(c) (Coalfire Indemnity Obligations), 5(d) (Client Indemnity Obligations), 5(g) (Disclaimer), 6 (Limitations of Liability), 8 (Ownership of Deliverables), 10 (Confidential Information), 11 (Use of Name and Publicity), 13 (Non-Solicitation and Contracting) and 14 (General), and any other provision of this Agreement that by its nature is intended to survive, shall survive the expiration or termination of this Agreement for any reason whatsoever.

(n) Waiver. No forbearance, failure or delay in exercising any right, power or privilege impair any such right, power or privilege or be construed to be a waiver thereof. A waiver by any party of any of the covenants, conditions, or obligations to be performed by the other or any breach thereof shall not be construed to be a waiver of any succeeding breach thereof or of any other covenant, condition, or obligation herein contained. No change, waiver, or discharge hereof shall be valid unless in writing and signed by an authorized representative of the party against which such change, waiver, or discharge is sought to be enforced.

SCHEDULE A
SECURITY ASSESSMENT SERVICES

Assessment, Penetration Study and Computer Forensic Services.

1. Scope. If the Services requested by Client in a Service Order include technical security testing, penetration testing (including physical, ethical or network penetration assessment and testing) or computer forensic services, Coalfire will use various commercial, open source or proprietary testing tools, techniques and monitoring methods to evaluate the devices, software or resources (collectively "Systems") identified by the Client as within scope. Coalfire may, at its discretion, also use underground hacker tools that are employed by underground computer attackers. Coalfire is hereby authorized to perform those Services identified in any Service Order subject to this Agreement on Systems, including IP addresses, identified by the Client as within scope. Coalfire is not responsible for adverse consequences resulting from inaccurate information, including inaccurate IP Addresses, furnished by Client with respect to any System.

2. Additional Client Responsibilities. In connection with the Services performed by Coalfire under this Agreement and the applicable Service Order, Client shall:

(a) Access. Provide Coalfire with reasonable access to Client's designated project manager and technical resources for the Services for the duration of the engagement covered by the applicable Service Order. Client's project manager shall have the necessary knowledge and authority to make decisions concerning implementation of the Services, along with the technical resources and knowledge of the Client's environment to enable the methodology described herein.

(b) Identification. Identify and provide a description of the target Systems environment inventory and topology, including the number of servers at each site and their platforms as needed.

(c) Systems Information. Deliver to Coalfire, prior to the commencement of any Services, a list of the Systems, System names, networks, access points, hardware, software, devices (including wireless devices), and network and IP addresses of each of the foregoing in such form and format as is mutually agreed by the parties.

(d) No Interference. Upon request by Coalfire pursuant to the requirements of the Services identified in the applicable Service Order, configure all Systems so that they will not interfere with Coalfire's vulnerability scanning or testing.

(e) Disclosure. Disclose IP ranges considered in scope for the applicable Service Order prior to scanning or testing.

3. Authorization Window. Client shall give Coalfire reasonable access to the facilities (including, without limitation, Client's facilities and any facilities under the control of a third party such as data center providers) containing the Systems to perform the Services during a timeframe ("Authorization Window") mutually agreed upon between Client and Coalfire and designated in the applicable Service Order. Coalfire will coordinate with Client regarding scripts and auditing tools and so that Client, or any third party at Client's direction, can coordinate security access permissions or consents. Client understands and agrees that: (a) Client's failure to arrange for or provide Coalfire with any such access, permissions, or consents or the failure of Client to perform the responsibilities described in Section 2 may cause changes to the Services schedule, fees and expenses, Deliverables, level of effort required or otherwise impact Coalfire's performance of the Services described in the applicable Service Order, and (b) Coalfire shall have no liability in respect of its inability to perform its Services resulting therefrom.

4. Assumption of Risk. Client agrees to notify appropriate personnel within its organization and any contractors, suppliers and agents prior to scheduling, including without limitation any hosting, managed applications or services providers and data center providers and each of their respective designated client representatives, host masters, systems administrators, technical managers and/or security managers. Client assumes all risk for adverse consequences to the Systems resulting from the requested study and assessment. Coalfire and any Host will bear no responsibility for any adverse consequences to the Systems resulting from the requested study or assessment. Client releases and holds Coalfire, Coalfire Personnel harmless from any and all damages, losses and liabilities relating to the Systems arising as a consequence of the study and assessment. Adverse consequences to the Systems could include, without the limitation, the following: (a) Systems down time, (b) loss of business, (c) connectivity loss, (d) degradation of bandwidth, (e) Systems loss and crashes, and (f) information and access loss. If any IP Address is a broadcast address, router address or switch address, then Systems adversely affected could include all those connected to it. Also, older systems or components tend to cause more adverse consequences. NOTWITHSTANDING THE FOREGOING, SCETIONS 5 AND 6 OF THIS AGREEMENT REMAIN APPLICABLE IN DETERMINING THE RESPECTIVE LIABILITIES AND LIMITATIONS ON SAME AS TO BOTH PARTIES, AND NOTHING IN THIS SECTION 4 OF SCHEDULE A SHALL BE CONSTRUED AS AN ALTERATION OR LIMITATION OF SAME.

5. Reports. Notwithstanding the confidentiality provisions contained in the Agreement, Coalfire and Client agree that the results of any scanning reports may be disclosed to Client's employees, contractors, advisors, as Client, in its sole discretion, deems appropriate, so that Client may demonstrate the performance of such Services by Coalfire. Client understands and agrees that any certification by Coalfire as to the results of the application of any scanning or audit procedures are limited to Client's compliance or non-compliance with the applicable standards based solely upon the information and access provided or made available to Coalfire by Client, and are not intended to certify or provide any guarantee about the status of Client's security posture or to imply any other representations other than those specifically contained therein.

6. Client Representations and Warranties. Client represents and warrants to Coalfire that Client is the owner of and/or otherwise has the rights to the Client Systems, or that Client is authorized to instruct Coalfire to perform Services on such Client Systems pursuant to the applicable Service Order. Subject to the limitations set forth in Sections 5 and 6 of this Agreement, Client shall indemnify and hold harmless Coalfire from any damage, loss, liability, costs, fines, sanctions and expenses of any kind (including reasonable attorneys' fees) arising from the performance of the Services in accordance with the applicable Service Order on any computer system including but not limited to any computer, network, IP address, device including wireless devices on which Coalfire is instructed by Client to perform the Services.

7. PCI Assessment Services. If the Services requested by Client in a Service Order include a PCI "Assessment," then notwithstanding any agreement between the parties to the contrary and to meet compliance requirements imposed by the Payment Card Industry (PCI) Security Standards Council (SSC), the Client understands and agrees that, without further permission from the Client, Coalfire shall be permitted to submit the "Results" of such Assessment to a "Requesting Organization." The Results as defined herein shall include a Report on Compliance and, without limitation, any associated working papers, notes and other materials and information generated in connection with an Assessment, including a copy of this Agreement. As defined in this section, the terms "Assessment" and "Requesting Organization" shall have the meaning ascribed to those terms as stated in Appendix A to the PCI Security Standards Validation Requirements For Qualified Security Assessors (QSA), a copy of which can be located at https://www.pcisecuritystandards.org.

SCHEDULE B

Compliance Assessment and Management Solutions

1. Scope. If the Services requested by Client in a Service Order include any of Coalfire's hosted compliance assessment or management solutions Software modules, then the terms and conditions of this Schedule shall apply. For purposes of this Agreement, "Software" means the computer programs, software applications, modules and interactive computer service for compliance assessment and management solutions and its applicable documentation (if any), including without limitation, all related interfaces, functionality, web-services, supplements, add-on components, corrections, modifications, bug fixes, enhancements, updates, new versions or releases that Coalfire subsequently may make available to Licensee, to the extent that such items are not accompanied by an end user license agreement or other Terms of Use.

2. Software.

(a) License Grant. Subject to the terms and conditions of this Agreement and the Service Order(s) (including Client's obligation to pay all Fees when due), Coalfire hereby grants to Client a limited, personal, non-exclusive, non-transferable, revocable right and license, without right to grant sublicenses, during the License Term for Client to use, access and enjoy the benefits of the Software electronically via the Internet and use the Software solely within the license scope set forth in the applicable Service Order and solely for Client's internal business purposes. Coalfire shall make the Software available to Client via a digital information processing, transmission and storage system ("Server") maintained by or on behalf of Coalfire. Coalfire reserves the right to modify the Software at any time as business needs dictate in Coalfire's sole discretion; provided that the terms and conditions of this Agreement shall remain in effect and shall govern Client's use and obligations with respect to any modified Software. For purposes of this Agreement, "License Term" means the period of time designated in a Service Order during which Client is authorized to access and use the Software pursuant to the terms of this Agreement.

(b) License Restrictions. Any use of the Software not expressly permitted in this Agreement is prohibited. Client acknowledge that the Software and its structure, organization, and source code constitute valuable trade secrets of Coalfire and its suppliers. Client agree that Client shall not, nor shall Client permit, assist or encourage any third party to: (i) reproduce, allow use of or access to the Software or sell, rent, lease, use for service bureau use, sublicense or otherwise transfer or distribute the Software, in whole or in part, to any third parties; (ii) modify, translate, reverse engineer, decompile, or disassemble the Software or otherwise attempt to derive the source code for the Software; (iii) merge the Software with other software; (iv) copy, modify, adapt, alter, translate, enhance or otherwise modify or create derivative works of or from the Software; (v) alter, destroy or otherwise remove any proprietary notices or labels on or embedded within the Software; (vi) use the Software to develop any application or program having the same primary function as the Software or otherwise exercise any rights in or to the Software except as expressly permitted under Section 2(a) (License Grant); (vii) use, upload, post or transmit via or in connection with the Software any unlawful, threatening, abusive, false, libelous, defamatory, obscene, pornographic, profane, or otherwise infringing or objectionable information or content of any kind, including, without limitation, any use or transmissions constituting or encouraging conduct that would constitute a criminal offense, give rise to civil liability, or otherwise violate any applicable law, including violations of any patent, trade secret, copyright, trademark or other intellectual property right ("IP Rights"), privacy rights or any other rights of a third party; (viii) post or transmit into or via the Software any information, software, material or other content that is subject to an Open Source License or that contains a virus, cancelbot, Trojan horse, worm or other harmful components; or (ix) use the Software in violation of any terms and conditions of use governing access and use of the Software as set forth at the http/web address designated by Coalfire, as modified or amended from time to time in Coalfire's sole discretion (the "Terms of Use") or otherwise interfere, disrupt or attempt to gain unauthorized access to any computer system, server, network or account for which Client does not have authorization to access or at a level exceeding Client's authorization. In the event that the Terms of Use are modified by Coalfire subsequent to the execution of this Agreement and during the term of any outstanding Service Order wherein Client is granted a license for the use of such software, Coalfire will advise Client in writing of such modifications within thirty (30) days of same.

(c) No Implied Licenses. The Software is licensed, not sold. All rights not expressly granted in Section 2(a) (License Grant) are reserved by Coalfire, and nothing in this Agreement will be deemed to grant, by implication, estoppel or otherwise, a license under any of Coalfire's existing or future IP Rights.

(d) Suspension of Access & Service. Notwithstanding anything herein to the contrary and without prejudice to any other rights, upon any actual or alleged breach of this Agreement by Client, Coalfire reserves the right, in its sole discretion and upon notice (which notice may be in e-mail form), at any time, to: (i) remove or disable access to all or any portion of the Software; (ii) suspend Client's access to or use of the Software; and/or (iii) terminate this Agreement, in which case Coalfire shall have no liability of any kind for such termination, cancellation or suspension. Nothing in this Section is intended to preclude Coalfire from seeking immediate appropriate injunctive relief.

2. Equipment; Access; Availability.

(a) Equipment. Coalfire shall not be responsible for performance or operational issues experienced by Client with respect to access to or use of the Software. Client shall be solely responsible for, and Coalfire shall have no liability in connection with, providing, maintaining and ensuring compatibility of the Software with any hardware, third party software, electrical and other physical requirements to access and use the Software, including, without limitation, operating systems, telecommunications and digital transmission connections and links, routers, local area network servers, virus software, firewalls, or other equipment and services required to or desirable for access and use of the Software.

(b) Authorized Users. The Software enables Client to register, authorize and grant access to those employees, agents, contingent workers and authorized independent contractors of Client designated by Client (each, an "Authorized User"). Notwithstanding anything herein to the contrary, any breach of any terms or conditions of this Agreement by such Authorized Users shall be deemed to be a breach of this Agreement by Client. Client shall be responsible and liable for the acts or omissions of each such Authorized User as if such acts or omissions were Client's own acts or omissions.

(c) Access IDs. During the License Term, the Software shall permit Client to register, authorize and obtain unique and confidential login IDs, passwords and/or access codes ("Access IDs") to allow Client and its Authorized Users (in accordance with Section 2(b), above) to access the Software. Client shall maintain the confidentiality of its Access IDs and shall not disclose the Access IDs to any third party.

(d) Availability. Coalfire shall use commercially reasonable efforts to make the Software available to Authorized Users pursuant to the terms and conditions of this Agreement during the License Term. Client acknowledges that from time to time the Software may be inaccessible or inoperable for any reason, including, without limitation: (i) periodic maintenance procedures, enhancements, repairs or corrections with respect to the Software or Server, as determined by Licensor; (ii) equipment malfunctions; (iii) acts or omissions of Client and its Authorized Users, including but not limited to scheduled or unscheduled outages of the Authorized User's internet browser, known and persistent slow response time on Authorized User's internal network, problems with Authorized User's computer hardware or electricity; or (iv) causes beyond the reasonable control of Coalfire or that are not reasonably foreseeable by Coalfire, including interruption or failure of telecommunication or digital transmission links, delays or failures due to Client's Internet Service Provider, hostile network attacks or network congestion.

3. Support and Other Services.

Client acknowledges that Coalfire has no control over the stability and throughput speed of the Internet or availability of the Software on a continuous and uninterrupted basis. Subject to Client's performance of all of obligations hereunder, including the payment of all Fees when due, Coalfire shall provide Client with technical assistance as is reasonably necessary to initially install and implement the Software via telephone or remote web-based support (collectively, the "Support Services"). This Agreement does not otherwise entitle Client to receive object code, source code, on-site or additional installation, or training, technical support, telephone assistance, enhancements, updates or bug fixes for the Software. Coalfire, in its sole discretion, may provide Client with any such Support Services upon terms mutually agreed upon between the parties in a duly executed and delivered writing which shall be billed at Coalfire's standard rates and prices in effect from time to time or as mutually agreed between the parties in a Service Order or equivalent written agreement. Any software or other programs or materials provided to Client as part of the Support Services are considered part of the Software and shall be subject to the terms and conditions of this Agreement, unless otherwise mutually agreed upon by the parties in writing. If requested by Client, Coalfire, in its discretion, may provide consulting or professional services, which shall be billed at Coalfire's rates and prices pursuant to terms and conditions to be mutually agreed upon between the parties in writing.

4. Ownership; Further Restrictions.

(a) Ownership. Client acknowledge that: (i) the Software and all right, title and interest therein, including without limitation, all IP Rights in and to the Software, are the sole and exclusive property of Coalfire and its suppliers, (ii) Client receive no right, title or interest in or to the Software except as expressly set forth herein, and (iii) all title and IP Rights in and to any data or content that is not contained in the Software, but may be accessed through use of the Software, is the property of the respective content owners and this Agreement grants Client no rights to use such content. If Client, its Authorized Users or any of Client's Related Parties are deemed to have any ownership interest or other rights in the Software, including any and all derivative works, enhancements or other modifications thereto, then Client shall assign and/or cause such parties to assign, and Client does hereby assign, irrevocably and royalty-free, all of such ownership interest or other rights exclusively to Coalfire and Client shall, at Coalfire's reasonable request and expense, complete, execute and deliver any and all documents necessary to effect or perfect such assignments.

(b) Protection. Client shall use Client's reasonable best efforts, which shall be no less stringent than those efforts that Client uses to protect Client's own confidential information, trade secrets, technology, software or other similar proprietary property, to prevent any Software from being disclosed or used by any Authorized User or any of Client's Related Parties or other person in any manner that would violate this Agreement. In no event shall Client take any action that might encumber or expose the Software or the license rights granted in this Agreement to any claims, liens or other forms of encumbrance.

5. Security. NOTWITHSTANDING ANYTHING HEREIN TO THE CONTRARY, CLIENT SHALL BE SOLELY RESPONSIBLE FOR: (I) INPUTTING, LOADING OR OTHERWISE USING THE CLIENT DATA IN CONNECTION WITH THE SOFTWARE; (II) MAINTAINING INDEPENDENT ARCHIVAL AND BACKUP COPIES OF ALL CLIENT DATA; (III) ENSURING THE CONFIDENTIALITY OF CLIENT'S PASSWORDS, ACCESS IDS AND/OR MEMBER ACCOUNTS, WHICH SHALL BE ISSUED FOR THE LIMITED PURPOSE OF USING THE SOFTWARE PURSUANT TO THE TERMS HEREIN. COALFIRE SHALL HAVE NO LIABILITY TO CLIENT OR ANY OTHER PERSON FOR LOSS, DAMAGE OR DESTRUCTION OF CLIENT DATA. Client is solely responsible for any authorized or unauthorized access to and use of the Software via Client's or its Authorized Users' passwords and/or member accounts. If any of Client's or its Authorized Users' password are lost, stolen or otherwise compromised, Client shall promptly change the password or, if Client is unable to do so, Client shall notify Coalfire, whereupon Coalfire shall suspend use of such password and/or account and issue a replacement password. Notwithstanding anything herein to the contrary, Client hereby authorizes Coalfire to treat any person using Client's or any of its Authorized Users' passwords, Access IDs and/or member account as Client (even if such person is using such item(s) without Client's authorization), and any resulting transactions, Fees, obligations or liabilities shall be attributed to Client, until such time as Coalfire is notified by Client in writing of any unauthorized access arising under such conditions.

6. Warranties and Covenants.

(a) Client Warranty. Client represents, warrants and covenants to Coalfire that: (i) Client has the legal power and authority to enter into and perform Client's obligations under this Agreement; (ii) Client shall comply with all terms and conditions of this Agreement, including, without limitation, the License Restrictions set forth in Section 2(b); (iii) Client is the owner and/or the licensee of all IP Rights relating to the Client data and has the necessary rights to fulfill Client's obligations and/or otherwise perform under this Agreement; (iv) the Client data, and Client's use thereof in connection with the Software or as otherwise contemplated by this Agreement, does not, and shall not, infringe any third party's IP Rights, privacy rights, or other rights, and shall not otherwise violate any applicable law; and (v) Client shall not use the Software in violation of any applicable law and shall otherwise refrain from any act or omission that will cause Coalfire to be in violation of any applicable law regarding the use of the Software.

(b) Coalfire Warranty and Disclaimer. COALFIRE WARRANTS THAT (I) THE SOFTWARE SHALL PERFORM SUBSTANTIALLY IN ACCORDANCE WITH THE DATA SHEET ATTACHED TO THE APPLICABLE SERVICE ORDER(S); (II) COALFIRE HAS FULL CORPORATE AUTHORITY SUFFICIENT TO GRANT CLIENT THE LICENSES SET FORTH IN THIS AGREEMENT OR APPLICABLE SERVICE ORDER(S); AND (III) DURING THE TERM OF THIS AGREEMENT AND ANY APPLICABLE SERVICE ORDER(S), TO THE KNOWLEDGE OF COALFIRE AT THE TIME COALFIRE IS MAKING THE SOFTWARE AVAILABLE TO CLIENT, THE SOFTWARE SHALL BE FREE FROM VIRUSES, WORMS, TROJAN HORSES, BUILT-IN OR OTHER USE-DRIVEN DESTRUCTIVE MECHANISMS, OR OTHER INJURIOUS OR DAMAGING FORMULAS, INSTRUCTIONS OR OTHER MATERIALS (HEREINAFTER REFERRED TO SINGULARLY OR COLLECTIVELY AS "VIRUSES"). COALFIRE MAKES NO OTHER WARRANTY, EXPRESS OR IMPLIED, WITH RESPECT TO THIS AGREEMENT OR THE SOFTWARE, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE OR NONINFRINGEMENT AND/OR ANY WARRANTIES ARISING OUT OF A COURSE OF DEALING OR COURSE OF PERFORMANCE. WITHOUT LIMITING THE FOREGOING, COALFIRE DOES NOT WARRANT THAT THE SOFTWARE WILL MEET CLIENT'S REQUIREMENTS OR EXPECTATIONS OR THAT THE SOFTWARE, ANY COMMUNICATIONS SENT OR RECEIVED IN CONNECTION THEREWITH OR CLIENT'S USE OF THE SAME WILL BE UNINTERRUPTED, ERROR-FREE, VIRUS-FREE OR COMPLETELY SECURE, NOR DOES COALFIRE MAKE ANY WARRANTY AS TO ANY RESULTS THAT MAY BE OBTAINED BY USE OF THE SOFTWARE. COALFIRE SHALL HAVE NO LIABILITY FOR ANY INACCESSIBILITY OF THE SOFTWARE, ANY VIRUS, TRAPS OR OTHER HARMFUL CODE DIRECTLY OR INDIRECTLY TRANSMITTED BY OR THROUGH THE SOFTWARE (EXCEPT WHERE THE SAME WAS INTENTIONALLY OR KNOWINGLY TRANSMITTED BY COALFIRE WITHOUT CLIENT'S CONSENT), OR ANY DELAY OR FAILURE OF ANY TRANSMISSION, COMMUNICATION OR DATA SENT OR RECEIVED OR NOT SENT OR RECEIVED VIA THE SOFTWARE. COALFIRE MAKES NO REPRESENTATION OR WARRANTY OF ANY KIND WHATSOEVER WITH REGARD TO THE USE OF THE SOFTWARE BY CLIENT, INCLUDING WHETHER THE USE OF THE SOFTWARE BY CLIENT CONFORMS TO APPLICABLE LAWS. CLIENT SHALL BEAR SOLE RESPONSIBILITY TO DETERMINE WHETHER CLIENT'S USE OF THE SOFTWARE COMPLIES WITH APPLICABLE LAWS.

7. Compliance with Laws. Client shall at all times comply with all applicable laws and regulations in Client's use of the Software. Without limiting the generality of the foregoing, Client will not export or re-export the Software without all required United States and foreign government licenses. All rights to use the Software are granted on condition that such rights are forfeited if Client fails to comply with the terms of this Agreement. Client will defend, indemnify and hold harmless Coalfire and its Related Parties from and against any violation of such laws or regulations by Client or any of its Authorized Users or Related Parties.

8. Limitation of Liability. If the Services requested by Client in a Service Order include any of Coalfire's hosted compliance assessment or management solutions Software modules, then, solely with respect to the Software, this Section 8 shall apply. NEITHER COALFIRE NOR ITS RELATED PARTIES SHALL BE LIABLE FOR ANY CONSEQUENTIAL, INDIRECT, EXEMPLARY, SPECIAL, PUNITIVE OR INCIDENTAL DAMAGES, INCLUDING WITHOUT LIMITATION ANY LOST DATA OR LOST PROFITS, OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, ARISING FROM OR RELATING TO THIS AGREEMENT, THE USE OF OR INABILITY TO USE THE SOFTWARE, OR ANY COMMUNICATION OR DATA SENT OR RECEIVED OR NOT SENT OR RECEIVED VIA THE SOFTWARE, HOWEVER CAUSED AND UNDER ANY THEORY OF LIABILITY (INCLUDING CONTRACT, STATUTE, TORT OR NEGLIGENCE), EVEN IF COALFIRE OR ITS RELATED PARTIES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IF CLIENT IS DISSATISFIED WITH THE SOFTWARE, CLIENT'S SOLE AND EXCLUSIVE REMEDY HEREUNDER SHALL BE FOR CLIENT TO DISCONTINUE CLIENT'S USE OF THE SOFTWARE AND TERMINATE THIS AGREEMENT. NOTWITHSTANDING ANYTHING HEREIN TO THE CONTRARY, COALFIRE'S AND ITS RELATED PARTIES' TOTAL CUMULATIVE LIABILITY IN CONNECTION WITH THIS AGREEMENT SHALL IN NO EVENT EXCEED THE AMOUNT OF ANY FEES ACTUALLY PAID BY CLIENT TO COALFIRE FOR USE OF THE SOFTWARE HEREUNDER. CLIENT ACKNOWLEDGES THAT THE DISCLAIMERS AND LIMITATIONS HEREIN REFLECT A FAIR ALLOCATION OF RISK AND THAT COALFIRE WOULD NOT ENTER INTO THIS AGREEMENT WITHOUT SUCH LIMITATIONS ON ITS LIABILITY, AND CLIENT AGREES THAT THE FOREGOING DISCLAIMERS AND LIMITATIONS SHALL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF CERTAIN CATEGORIES OF DAMAGES, IN SUCH JURISDICTIONS, THE PARTIES AGREE THAT THE LIABILITY OF COALFIRE SHALL BE LIMITED TO THE FULLEST EXTENT PERMITTED BY SUCH JURISDICTION.

9. U.S. Government Restricted Rights Notice. The Software was developed at private expense and is a Commercial Item, as that term is defined in 48 CFR 2.101, consisting of Commercial Computer Software and Commercial Computer Software Documentation as such terms are used in 48 CFR 12.212 and 48 CFR 227.7202-1 through 227.7202-4, as applicable. The Software is licensed to U.S. Government end-users only as a Commercial Item and with only those rights granted to all other end-users pursuant to the terms and conditions herein.

10. Equitable Remedies. The parties acknowledge and agree that a breach or threatened breach of this Schedule's Section 2(a) (License Grant), 2(b) (License Restrictions), or 4 (Ownership; Further Restrictions) would result in irreparable harm to the non-breaching party or its suppliers for which a remedy at law would be inadequate, and therefore, such party shall have the right to seek to obtain injunctive relief upon any violation or threatened violation of the terms of the foregoing Sections without the necessity of posting bond or other security, in addition to all other rights and remedies available at law or in equity.

International Telecommunication Union

Application Form for Associates

National entities and organizations are invited to send this Form through the National Telecommunication Administration of the Member State in which the company has its headquarters, or directly to ITU if the Member State has assigned authority to the Secretary-General to approve the Application. Regional and international organizations may send it directly to the ITU Secretary-General.

In accordance with Article 19 of the Convention, the following company/organization:

Name: Collier Technologies, LLC

Chief Executive Officer: C. J. Adams- Collier

Main contact person (for subsequent correspondence): C. J. Adams-Collier Title: Member

Mailing address: ~~85 Raccoon Point Road~~ 17 Bartel Road 98245-1988

Tel.: (206)226-5809 Fax: E-mail: cjac@colliertech.org

Address and contact person (for invoicing) if different from contact person above: Chrystal Weinberg

20092 N. 272nd Lane Buckeye, AZ ~~85396~~ 85396-6899

wishes to become an Associate of: *(Please tick the appropriate box)*

□ ITU-R*) Study Group

□ ITU-T*) Study Group

☒ ITU-D*) Study Group CyberSecurity

* *For the period 2010-2011, the annual financial contribution for an Associate in ITU-R or ITU-T is CHF 10,600.–; in ITU-D it is CHF 3,975.– and CHF 1,987.50 for Associates from developing countries.*

Please note that denunciation will take effect at the end of six months from the date when notification is received by the Secretary-General. The contribution is due up to the last day of the month in which the denunciation takes effect.

in the category of: *(Please tick the appropriate box)*

☒ recognized operating agency

□ financial or development institution

□ scientific or industrial organization

□ other entity dealing with telecommunication matters

☒ regional and other international telecommunication, standardization, financial or development organization

Kindly indicate your sphere of activities: *(Please tick the appropriate box)*

☒ Network Operator

□ Voice Networks

□ Investment Bank

□ University

☒ Service Provider

□ Manufacturers

□ Telecommunication Consultancy

□ International Organization

☒ Internet Services

☒ Research Agency

□ Regulator

□ Other

I, the undersigned, have the power and authority to submit this application on behalf of my company/organization:

Name: C. J. Adams-Collier Title: Member

Date: 20120926T180811 Signature: C. J. Adams- Collier

Please make sure that you have given all the information requested.

ITU • Corporate Governance and Membership Division • Place des Nations • CH-1211 Geneva • Switzerland
Tel.: +41 22 730 5214/6018 • Fax: +41 22 730 6675 • E-mail: membership@itu.int • www.itu.int

Chapter 19.34 RCW
Washington electronic authentication act

WA
rev

RCW Sections

Notes:
Digital signature violations: RCW 9.38.060.

19.34.010
Purpose and construction.

This chapter shall be construed consistently with what is commercially reasonable under the circumstances and to effectuate the following purposes:

(1) To facilitate commerce by means of reliable electronic messages;

(2) To ensure that electronic signatures are not denied legal recognition solely because they are in electronic form;

(3) To provide a voluntary licensing mechanism for digital signature certification authorities by which businesses, consumers, courts, government agencies, and other entities can reasonably be assured as to the integrity, authenticity, and nonrepudiation of a digitally signed electronic communication;

(4) To establish procedures governing the use of digital signatures for official public business to provide reasonable assurance of the integrity, authenticity, and nonrepudiation of an electronic communication;

(5) To minimize the incidence of forged digital signatures and fraud in electronic commerce;

(6) To implement legally the general import of relevant standards; and

(7) To establish, in coordination with states and other jurisdictions, uniform rules regarding the authentication and reliability of electronic messages.

[1999 c 287 § 1; 1996 c 250 § 102.]

Notes:

Effective date -- 1999 c 287: "This act is necessary for the immediate preservation of the public peace, health, or safety, or support of the state government and its existing public institutions, and takes effect immediately [May 13, 1999]." [1999 c 287 § 20.]

19.34.020
Definitions.

Unless the context clearly requires otherwise, the definitions in this section apply throughout this chapter:

(1) "Accept a certificate" means to manifest approval of a certificate, while knowing or having notice of its contents. Such approval may be manifested by the use of the certificate.

(2) "Accept a digital signature" means to verify a digital signature or take an action in reliance on a digital signature.

(3) "Asymmetric cryptosystem" means an algorithm or series of algorithms that provide a secure key pair.

(4) "Certificate" means a computer-based record that:

(a) Identifies the certification authority issuing it;

(b) Names or identifies its subscriber;

(c) Contains the subscriber's public key; and

(d) Is digitally signed by the certification authority issuing it.

(5) "Certification authority" means a person who issues a certificate.

(6) "Certification authority disclosure record" means an online, publicly accessible record that concerns a licensed certification authority and is kept by the secretary.

(7) "Certification practice statement" means a declaration of the practices that a certification authority employs in issuing certificates.

(8) "Certify" means to declare with reference to a certificate, with ample opportunity to reflect, and with a duty to apprise oneself of all material facts.

(9) "Confirm" means to ascertain through appropriate inquiry and investigation.

(10) "Correspond," with reference to keys, means to belong to the same key pair.

(11) "Digital signature" means an electronic signature that is a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine:

(a) Whether the transformation was created using the private key that corresponds to the signer's public key; and

(b) Whether the initial message has been altered since the transformation was made.

(12) "Electronic" means electrical, digital, magnetic, optical, electromagnetic, or any other form of technology that entails capabilities similar to these technologies.

(13) "Electronic record" means a record generated, communicated, received, or stored by electronic means for use in an information system or for transmission from one information system to another.

(14) "Electronic signature" means a signature in electronic form attached to or logically associated with an electronic record, including but not limited to a digital signature.

(15) "Financial institution" means a national or state-chartered commercial bank or trust company, savings bank, savings association, or credit union authorized to do business in the state of Washington and the deposits of which are federally insured.

(16) "Forge a digital signature" means either:

(a) To create a digital signature without the authorization of the rightful holder of the private key; or

(b) To create a digital signature verifiable by a certificate listing as subscriber a person who either:

(i) Does not exist; or

(ii) Does not hold the private key corresponding to the public key listed in the certificate.

(17) "Hold a private key" means to be authorized to utilize a private key.

(18) "Incorporate by reference" means to make one message a part of another message by identifying the message to be incorporated and expressing the intention that it be incorporated.

(19) "Issue a certificate" means the acts of a certification authority in creating a certificate and notifying the subscriber listed in the certificate of the contents of the certificate.

(20) "Key pair" means a private key and its corresponding public key in an asymmetric cryptosystem, keys which have the property that the public key can verify a digital signature that the private key creates.

(21) "Licensed certification authority" means a certification authority to whom a license has been issued by the secretary and whose license is in effect.

(22) "Message" means a digital representation of information.

(23) "Notify" means to communicate a fact to another person in a manner reasonably likely under the circumstances to impart knowledge of the information to the other person.

(24) "Official public business" means any legally authorized transaction or communication among state agencies, tribes, and local governments, or between a state agency, tribe, or local government and a private person or entity.

(25) "Operative personnel" means one or more natural persons acting as a certification authority or its agent, or in the employment of, or under contract with, a certification authority, and who have:

(a) Duties directly involving the issuance of certificates, or creation of private keys;

(b) Responsibility for the secure operation of the trustworthy system used by the certification authority or any recognized repository;

(c) Direct responsibility, beyond general supervisory authority, for establishing or adopting policies regarding the operation and security of the certification authority; or

(d) Such other responsibilities or duties as the secretary may establish by rule.

(26) "Person" means a human being or an organization capable of signing a document, either legally or as a matter of fact.

(27) "Private key" means the key of a key pair used to create a digital signature.

(28) "Public key" means the key of a key pair used to verify a digital signature.

(29) "Publish" means to make information publicly available.

(30) "Qualified right to payment" means an award of damages against a licensed certification authority by a court having jurisdiction over the certification authority in a civil action for violation of this chapter.

(31) "Recipient" means a person who has received a certificate and a digital signature verifiable with reference to a public key listed in the certificate and is in a position to rely on it.

(32) "Recognized repository" means a repository recognized by the secretary under RCW 19.34.400.

(33) "Recommended reliance limit" means the monetary amount recommended for reliance on a certificate under RCW 19.34.280(1).

(34) "Repository" means a system for storing and retrieving certificates and other information relevant to digital signatures.

(35) "Revoke a certificate" means to make a certificate ineffective permanently from a specified time forward. Revocation is effected by notation or inclusion in a set of revoked certificates, and does not imply that a revoked certificate is destroyed or made illegible.

(36) "Rightfully hold a private key" means the authority to utilize a private key:

(a) That the holder or the holder's agents have not disclosed to a person in violation of RCW 19.34.240(1); and

(b) That the holder has not obtained through theft, deceit, eavesdropping, or other unlawful means.

(37) "Secretary" means the secretary of state.

(38) "Subscriber" means a person who:

(a) Is the subject listed in a certificate;

(b) Applies for or accepts the certificate; and

(c) Holds a private key that corresponds to a public key listed in that certificate.

(39) "Suitable guaranty" means either a surety bond executed by a surety authorized by the insurance commissioner to do business in this state, or an irrevocable letter of credit issued by a financial institution authorized to do business in this state, which, in either event, satisfies all of the following requirements:

(a) It is issued payable to the secretary for the benefit of persons holding qualified rights of payment against the licensed certification authority named as the principal of the bond or customer of the letter of credit;

(b) It is in an amount specified by rule by the secretary under RCW 19.34.030;

(c) It states that it is issued for filing under this chapter;

(d) It specifies a term of effectiveness extending at least as long as the term of the license to be issued to the certification authority; and

(e) It is in a form prescribed or approved by rule by the secretary.

A suitable guaranty may also provide that the total annual liability on the guaranty to all persons making claims based on it may not exceed the face amount of the guaranty.

(40) "Suspend a certificate" means to make a certificate ineffective temporarily for a specified time forward.

(41) "Time stamp" means either:

(a) To append or attach a digitally signed notation indicating at least the date, time, and identity of the person appending or attaching the notation to a message, digital signature, or certificate; or

(b) The notation thus appended or attached.

(42) "Transactional certificate" means a valid certificate incorporating by reference one or more digital signatures.

(43) "Trustworthy system" means computer hardware and software that:

(a) Are reasonably secure from intrusion and misuse; and

(b) Conform with the requirements established by the secretary by rule.

(44) "Valid certificate" means a certificate that:

(a) A licensed certification authority has issued;

(b) The subscriber listed in it has accepted;

(c) Has not been revoked or suspended; and

(d) Has not expired.

However, a transactional certificate is a valid certificate only in relation to the digital signature incorporated in it by reference.

(45) "Verify a digital signature" means, in relation to a given digital signature, message, and public key, to determine accurately that:

(a) The digital signature was created by the private key corresponding to the public key; and

(b) The message has not been altered since its digital signature was created.

[2000 c 171 § 50; 1999 c 287 § 2; 1997 c 27 § 30; 1996 c 250 § 103.]

Notes:

Effective date -- 1999 c 287: See note following RCW 19.34.010.

Effective date -- Severability -- 1997 c 27: See notes following RCW 19.34.030.

19.34.030
Secretary — Duties.

(1) The secretary must publish a certification authority disclosure record for each licensed certification authority, and a list of all judgments filed with the secretary, within the previous five years, under RCW 19.34.290.

(2) The secretary may adopt rules consistent with this chapter and in furtherance of its purposes:

(a) To license certification authorities, recognize repositories, certify operative personnel, and govern the practices of each;

(b) To determine the form and amount reasonably appropriate for a suitable guaranty, in light of the burden a suitable guaranty places upon licensed certification authorities and the assurance of quality and financial responsibility it provides to persons who rely on certificates issued by licensed certification authorities;

(c) To specify reasonable requirements for information to be contained in or the form of certificates, including transactional certificates, issued by licensed certification authorities, in accordance with generally accepted standards for digital signature certificates;

(d) To specify reasonable requirements for recordkeeping by licensed certification authorities;

(e) To specify reasonable requirements for the content, form, and sources of information in certification authority disclosure records, the updating and timeliness of the information, and other practices and policies relating to certification authority disclosure records;

(f) To specify the form of and information required in certification practice statements, as well as requirements regarding the publication of certification practice statements;

(g) To specify the procedure and manner in which a certificate may be suspended or revoked, as consistent with this chapter;

(h) To specify the procedure and manner by which the laws of other jurisdictions may be recognized, in order to further uniform rules regarding the authentication and reliability of electronic messages; and

(i) Otherwise to give effect to and implement this chapter.

(3) The secretary may act as a certification authority, and the certificates issued by the secretary shall be treated as having been issued by a licensed certification authority.

[1999 c 287 § 4; 1997 c 27 § 1; 1996 c 250 § 104.]

Notes:

Effective date -- 1999 c 287: See note following RCW 19.34.010.

Effective date -- 1997 c 27: "Sections 1 through 23, 25 through 27, and 29 through 34 of this act take effect January 1, 1998." [1997 c 27 § 35.]

Severability -- 1997 c 27: "If any provision of this act or its application to any person or circumstance is held invalid, the remainder of the act or the application of the provision to other persons or circumstances is not affected." [1997 c 27 § 36.]

19.34.040
Secretary — Fees — Disposition.

The secretary may adopt rules establishing reasonable fees for all services rendered by the secretary under this chapter, in amounts that are reasonably calculated to be sufficient to compensate for the costs of all services under this chapter, but that are not estimated to exceed those costs in the aggregate. All fees recovered by the secretary must be deposited in the state general fund.

[1997 c 27 § 2; 1996 c 250 § 105.]

Notes:

Effective date -- Severability -- 1997 c 27: See notes following RCW 19.34.030.

19.34.100
Certification authorities — Licensure — Qualifications — Revocation and suspension.

(1) To obtain or retain a license, a certification authority must:

(a) Provide proof of identity to the secretary;

(b) Employ only certified operative personnel in appropriate positions;

(c) File with the secretary an appropriate, suitable guaranty, unless the certification authority is a city or county that is self-insured or the department of information services;

(d) Use a trustworthy system;

(e) Maintain an office in this state or have established a registered agent for service of process in this state; and

(f) Comply with all further licensing and practice requirements established by rule by the secretary.

(2) The secretary may by rule create license classifications according to specified limitations, and the secretary may issue licenses restricted according to the limits of each classification.

(3) The secretary may impose license restrictions specific to the practices of an individual certification authority. The secretary shall set forth in writing and maintain as part of the certification authority's license application file the basis for such license restrictions.

(4) The secretary may revoke or suspend a certification authority's license, in accordance with the administrative procedure act, chapter 34.05 RCW, for failure to comply with this chapter or for failure to remain qualified under subsection (1) of this section. The secretary may order the summary suspension of a license pending proceedings for revocation or other action, which must be promptly instituted and determined, if the secretary includes within a written order a finding that the certification authority has either:

(a) Utilized its license in the commission of a violation of a state or federal criminal statute or of chapter 19.86 RCW; or

(b) Engaged in conduct giving rise to a serious risk of loss to public or private parties if the license is not immediately suspended.

(5) The secretary may recognize by rule the licensing or authorization of certification authorities by other governmental entities, in whole or in part, provided that those licensing or authorization requirements are substantially similar to those of this state. If licensing by another government is so recognized:

(a) RCW 19.34.300 through 19.34.350 apply to certificates issued by the certification authorities licensed or authorized by that government in the same manner as it applies to licensed certification authorities of this state; and

(b) The liability limits of RCW 19.34.280 apply to the certification authorities licensed or authorized by that government in the same manner as they apply to licensed certification authorities of this state.

(6) A certification authority that has not obtained a license is not subject to the provisions of this chapter, except as specifically provided.

[1999 c 287 § 5; 1998 c 33 § 1; 1997 c 27 § 3; 1996 c 250 § 201.]

Notes:

Effective date -- 1999 c 287: See note following RCW 19.34.010.

Effective date -- Severability -- 1997 c 27: See notes following RCW 19.34.030.

19.34.101
Expiration of licenses — Renewal — Rules.

Licenses issued under this chapter expire one year after issuance, except that the secretary may provide by rule for a longer duration. The secretary shall provide, by rule, for a system of license renewal, which may include requirements for continuing education.

[1997 c 27 § 4.]

Notes:

Effective date -- Severability -- 1997 c 27: See notes following RCW 19.34.030.

19.34.110
Compliance audits.

(1) A licensed certification authority shall obtain a compliance audit at such times and in such manner as directed by rule of the secretary. If the certification authority is also a recognized repository, the audit must include the repository.

(2) The certification authority shall file a copy of the audit report with the secretary. The secretary may provide by rule for filing of the report in an electronic format and may publish the report in the certification authority disclosure record it maintains for the certification authority.

[1999 c 287 § 6; 1997 c 27 § 5; 1996 c 250 § 202.]

Notes:

Effective date -- 1999 c 287: See note following RCW 19.34.010.

Effective date -- Severability -- 1997 c 27: See notes following RCW 19.34.030.

19.34.111
Qualifications of auditor signing report of opinion — Compliance audits under state auditor's authority.

(1) An auditor signing a report of opinion as to a compliance audit required by RCW 19.34.110 must:

(a) Be a certified public accountant, licensed under chapter 18.04 RCW or equivalent licensing statute of another jurisdiction; and

(b) Meet such other qualifications as the secretary may establish by rule.

(2) The compliance audits of state agencies and local governments who are licensed certification authorities, and the secretary, must be performed under the authority of the state auditor. The state auditor may contract with private entities as needed to comply with this chapter.

[1999 c 287 § 7; 1997 c 27 § 6.]

Notes:

Effective date -- 1999 c 287: See note following RCW 19.34.010.

Effective date -- Severability -- 1997 c 27: See notes following RCW 19.34.030.

19.34.120
Licensed certification authorities — Enforcement — Suspension or revocation — Penalties — Rules — Costs — Procedure — Injunctions.

(1) The secretary may investigate the activities of a licensed certification authority material to its compliance with this chapter and issue orders to a certification authority to further its investigation and secure compliance with this chapter.

(2) The secretary may suspend or revoke the license of a certification authority for its failure to comply with an order of the secretary.

(3) The secretary may by order impose and collect a civil penalty against a licensed certification authority for a violation of this chapter. The penalty shall not exceed ten thousand dollars per incident, or ninety percent of the recommended reliance limit of a material certificate, whichever is less. In case of a violation continuing for more than one day, each day is considered a separate

incident. The secretary may adopt rules setting forth the standards governing the exercise of the secretary's discretion as to penalty amounts. In the case of a state agency authorized by law to be a licensed certification authority, the sole penalty imposed under this subsection shall consist of specific findings of noncompliance and an order requiring compliance with this chapter and the rules of the secretary. Any penalty imposed under this chapter and chapter 34.05 RCW shall be enforceable in any court of competent jurisdiction.

(4) The secretary may order a certification authority, which it has found to be in violation of this chapter, to pay the costs incurred by the secretary in prosecuting and adjudicating proceedings relative to the order, and enforcing it.

(5) The secretary must exercise authority under this section in accordance with the administrative procedure act, chapter 34.05 RCW, and a licensed certification authority may obtain judicial review of the secretary's actions as prescribed by chapter 34.05 RCW. The secretary may also seek injunctive relief to compel compliance with an order.

[1999 c 287 § 8; 1997 c 27 § 7; 1996 c 250 § 203.]

Notes:

Effective date -- 1999 c 287: See note following RCW 19.34.010.

Effective date -- Severability -- 1997 c 27: See notes following RCW 19.34.030.

19.34.130
Certification authorities — Prohibited activities — Statement by secretary advising of certification authorities creating prohibited risks — Protest — Hearing — Disposition — Notice — Procedure.

(1) No certification authority, whether licensed or not, may conduct its business in a manner that creates an unreasonable risk of loss to subscribers of the certification authority, to persons relying on certificates issued by the certification authority, or to a repository.

(2) The secretary may publish brief statements advising subscribers, persons relying on digital signatures, or other repositories about activities of a certification authority, whether licensed or not, that create a risk prohibited by subsection (1) of this section. The certification authority named in a statement as creating or causing such a risk may protest the publication of the statement by filing a written defense of ten thousand bytes or less. Upon receipt of such a protest, the secretary must publish the protest along with the secretary's statement, and must promptly give the protesting certification authority notice and an opportunity to be heard. Following the hearing, the secretary must rescind the advisory statement if its publication was unwarranted under this section, cancel it if its publication is no longer warranted, continue or amend it if it remains warranted, or take further legal action to eliminate or reduce a risk prohibited by subsection (1) of this section. The secretary must publish its decision in the repository it provides.

(3) In the manner provided by the administrative procedure act, chapter 34.05 RCW, the secretary may issue orders and obtain injunctions or other civil relief to prevent or restrain a certification authority from violating this section, regardless of whether the certification authority is licensed. This section does not create a right of action in a person other than the secretary.

[1999 c 287 § 9; 1996 c 250 § 204.]

Notes:

Effective date -- 1999 c 287: See note following RCW 19.34.010.

19.34.200
Licensed certification authorities — Requirements.

(1) A licensed certification authority shall use only a trustworthy system to issue, suspend, or revoke certificates. A licensed certification authority shall use a recognized repository to publish or give notice of the issuance, suspension, or revocation of a certificate.

(2) A licensed certification authority shall publish a certification practice statement in accordance with the rules established by the secretary. The secretary shall publish the certification practice statements of licensed certification authorities submitted as part of the licensing process in a manner similar to the publication of the certification authority disclosure record.

(3) A licensed certification authority shall knowingly employ as operative personnel only persons who have not been convicted within the past seven years of a felony and have never been convicted of a crime involving fraud, false statement, or deception. For purposes of this subsection, a certification authority knowingly employs such a person if the certification authority knew of a conviction, or should have known based on information required by rule of the secretary. Operative personnel employed by a licensed certification authority must also be persons who have demonstrated knowledge and proficiency in following the requirements of this chapter. The secretary may provide by rule for the certification of operative personnel, and provide by rule for the manner in which criminal background information is provided as part of the certification process, as well as the manner in which knowledge and proficiency in following the requirements of this chapter may be demonstrated.

[1999 c 287 § 10; 1997 c 27 § 8; 1996 c 250 § 301.]

Notes:

Effective date -- 1999 c 287: See note following RCW 19.34.010.

Effective date -- Severability -- 1997 c 27: See notes following RCW 19.34.030.

19.34.210
Certificate — Issuance — Confirmation of information — Confirmation of prospective subscriber — Standards, statements, plans, requirements more rigorous than chapter — Revocation, suspension — Investigation — Notice — Procedure.

(1) A licensed certification authority may issue a certificate to a subscriber only after all of the following conditions are satisfied:

(a) The certification authority has received a request for issuance signed by the prospective subscriber; and

(b) The certification authority has confirmed that:

(i) The prospective subscriber is the person to be listed in the certificate to be issued;

(ii) If the prospective subscriber is acting through one or more agents, the subscriber duly authorized the agent or agents to have custody of the subscriber's private key and to request issuance of a certificate listing the corresponding public key;

(iii) The information in the certificate to be issued is accurate;

(iv) The prospective subscriber rightfully holds the private key corresponding to the public key to be listed in the certificate;

(v) The prospective subscriber holds a private key capable of creating a digital signature;

(vi) The public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the prospective subscriber; and

(vii) The certificate provides information sufficient to locate or identify one or more repositories in which notification of the revocation or suspension of the certificate will be listed if the certificate is suspended or revoked.

(c) The requirements of this subsection may not be waived or disclaimed by either the licensed certification authority, the subscriber, or both.

(2) In confirming that the prospective subscriber is the person to be listed in the certificate to be issued, a licensed certification authority shall make a reasonable inquiry into the subscriber's identity in light of:

(a) Any statements made by the certification authority regarding the reliability of the certificate;

(b) The reliance limit of the certificate;

(c) Any recommended uses or applications for the certificate; and

(d) Whether the certificate is a transactional certificate or not.

(3) A certification authority shall be presumed to have confirmed that the prospective subscriber is the person to be listed in a certificate where:

(a) The subscriber appears before the certification authority and presents identification documents consisting of at least one of the following:

(i) A current identification document issued by or under the authority of the United States, or such similar identification document issued under the authority of another country;

(ii) A current driver's license issued by a state of the United States; or

(iii) A current personal identification card issued by a state of the United States; and

(b) Operative personnel certified according to law or a notary has reviewed and accepted the identification information of the subscriber.

(4) The certification authority may establish policies regarding the publication of certificates in its certification practice statement, which must be adhered to unless an agreement between the certification authority and the subscriber provides otherwise. If the certification authority does not establish such a policy, the certification authority must publish a signed copy of the certificate in a recognized repository.

(5) Nothing in this section precludes a licensed certification authority from conforming to standards, certification practice statements, security plans, or contractual requirements more rigorous than, but nevertheless consistent with, this chapter.

(6) After issuing a certificate, a licensed certification authority must revoke it immediately upon confirming that it was not issued as required by this section. A licensed certification authority may also suspend a certificate that it has issued for a period not exceeding five business days as needed for an investigation to confirm grounds for revocation under this subsection. The certification authority must give notice to the subscriber as soon as practicable after a decision to revoke or suspend under this subsection.

(7) The secretary may order the licensed certification authority to suspend or revoke a certificate that the certification authority issued, if, after giving any required notice and opportunity for the certification authority and subscriber to be heard in accordance with the administrative procedure act, chapter 34.05 RCW, the secretary determines that:

(a) The certificate was issued without substantial compliance with this section; and

(b) The noncompliance poses a significant risk to persons relying on the certificate.

Upon determining that an emergency requires an immediate remedy, and in accordance with the administrative procedure act, chapter 34.05 RCW, the secretary may issue an order suspending a certificate for a period not to exceed five business days.

[1999 c 287 § 11; 1997 c 27 § 9; 1996 c 250 § 302.]

Notes:

Effective date -- 1999 c 287: See note following RCW 19.34.010.

Effective date -- Severability -- 1997 c 27: See notes following RCW 19.34.030.

19.34.220

Licensed certification authorities — Warranties, obligations upon issuance of certificate — Notice.

(1) By issuing a certificate, a licensed certification authority warrants to the subscriber named in the certificate that:

(a) The certificate contains no information known to the certification authority to be false;

(b) The certificate satisfies all material requirements of this chapter; and

(c) The certification authority has not exceeded any limits of its license in issuing the certificate.

The certification authority may not disclaim or limit the warranties of this subsection.

(2) Unless the subscriber and certification authority otherwise agree, a certification authority, by issuing a certificate, promises to the subscriber:

(a) To act promptly to suspend or revoke a certificate in accordance with RCW 19.34.250 or 19.34.260; and

(b) To notify the subscriber within a reasonable time of any facts known to the certification authority that significantly affect the validity or reliability of the certificate once it is issued.

(3) By issuing a certificate, a licensed certification authority certifies to all who reasonably rely on the information contained in the certificate, or on a digital signature verifiable by the public key listed in the certificate, that:

(a) The information in the certificate and listed as confirmed by the certification authority is accurate;

(b) All information foreseeably material to the reliability of the certificate is stated or incorporated by reference within the certificate;

(c) The subscriber has accepted the certificate; and

(d) The licensed certification authority has complied with all applicable laws of this state governing issuance of the certificate.

(4) By publishing a certificate, a licensed certification authority certifies to the repository in which the certificate is published and to all who reasonably rely on the information contained in the certificate that the certification authority has issued the certificate to the subscriber.

[1997 c 27 § 32; 1996 c 250 § 303.]

Notes:

Effective date -- Severability -- 1997 c 27: See notes following RCW 19.34.030.

19.34.230
Subscribers — Representations and duties upon acceptance of certificate.

(1) By accepting a certificate issued by a licensed certification authority, the subscriber listed in the certificate certifies to all who reasonably rely on the information contained in the certificate that:

(a) The subscriber rightfully holds the private key corresponding to the public key listed in the certificate;

(b) All representations made by the subscriber to the certification authority and material to the information listed in the certificate are true; and

(c) All material representations made by the subscriber to a certification authority or made in the certificate and not confirmed by the certification authority in issuing the certificate are true.

(2) By requesting on behalf of a principal the issuance of a certificate naming the principal as subscriber, the requesting person

certifies in that person's own right to all who reasonably rely on the information contained in the certificate that the requesting person:

(a) Holds all authority legally required to apply for issuance of a certificate naming the principal as subscriber; and

(b) Has authority to sign digitally on behalf of the principal, and, if that authority is limited in any way, adequate safeguards exist to prevent a digital signature exceeding the bounds of the person's authority.

(3) No person may disclaim or contractually limit the application of this section, nor obtain indemnity for its effects, if the disclaimer, limitation, or indemnity restricts liability for misrepresentation as against persons reasonably relying on the certificate.

(4) By accepting a certificate, a subscriber undertakes to indemnify the issuing certification authority for loss or damage caused by issuance or publication of a certificate in reliance on:

(a) A false and material representation of fact by the subscriber; or

(b) The failure by the subscriber to disclose a material fact;

if the representation or failure to disclose was made either with intent to deceive the certification authority or a person relying on the certificate, or with negligence. If the certification authority issued the certificate at the request of one or more agents of the subscriber, the agent or agents personally undertake to indemnify the certification authority under this subsection, as if they were accepting subscribers in their own right. The indemnity provided in this section may not be disclaimed or contractually limited in scope. However, a contract may provide consistent, additional terms regarding the indemnification.

(5) In obtaining information of the subscriber material to issuance of a certificate, the certification authority may require the subscriber to certify the accuracy of relevant information under oath or affirmation of truthfulness and under penalty of perjury.

[1996 c 250 § 304.]

19.34.231
Signature of a unit of government required — City or county as certification authority — Unit of state government prohibited from being certification authority — Exceptions.

***** CHANGE IN 2011 *** (SEE 1040.SL) *****

***** CHANGE IN 2011 *** (SEE 5931-S.SL) *****

(1) If a signature of a unit of state or local government, including its appropriate officers or employees, is required by statute, administrative rule, court rule, or requirement of the office of financial management, that unit of state or local government shall become a subscriber to a certificate issued by a licensed certification authority for purposes of conducting official public business with electronic records.

(2) A city or county may become a licensed certification authority under RCW 19.34.100 for purposes of providing services to local government, if authorized by ordinance adopted by the city or county legislative authority.

(3) A unit of state government, except the secretary and the department of information services, may not act as a certification authority.

[1999 c 287 § 12; 1997 c 27 § 10.]

Notes:

Effective date -- 1999 c 287: See note following RCW 19.34.010.

Effective date -- Severability -- 1997 c 27: See notes following RCW 19.34.030.

19.34.240
Private key — Control — Public disclosure exemption.

***** CHANGE IN 2011 *** (SEE** 1048-S.SL**) *****

(1) By accepting a certificate issued by a licensed certification authority, the subscriber identified in the certificate assumes a duty to exercise reasonable care to retain control of the private key and prevent its disclosure to a person not authorized to create the subscriber's digital signature. The subscriber is released from this duty if the certificate expires or is revoked.

(2) A private key is the personal property of the subscriber who rightfully holds it.

(3) A private key in the possession of a state agency or local agency, as those terms are defined by *RCW 42.17.020, is exempt from public inspection and copying under chapter 42.56 RCW.

[2005 c 274 § 235; 1997 c 27 § 11; 1996 c 250 § 305.]

Notes:

***Reviser's note:** RCW 42.17.020 was recodified as RCW 42.17A.005 pursuant to 2010 c 204 § 1102, effective January 1, 2012.

Part headings not law -- Effective date -- 2005 c 274: See RCW 42.56.901 and 42.56.902.

Effective date -- Severability -- 1997 c 27: See notes following RCW 19.34.030.

19.34.250
Suspension of certificate — Evidence — Investigation — Notice — Termination — Limitation or preclusion by contract — Misrepresentation — Penalty — Contracts for regional enforcement by agencies — Rules.

(1) Unless the certification authority provides otherwise in the certificate or its certification practice statement, the licensed certification authority that issued a certificate that is not a transactional certificate must suspend the certificate for a period not to exceed five business days:

(a) Upon request by a person whom the certification authority reasonably believes to be: (i) The subscriber named in the certificate; (ii) a person duly authorized to act for that subscriber; or (iii) a person acting on behalf of the unavailable subscriber; or

(b) By order of the secretary under RCW 19.34.210(7).

The certification authority need not confirm the identity or agency of the person requesting suspension. The certification authority may require the person requesting suspension to provide evidence, including a statement under oath or affirmation, regarding the requestor's identity, authorization, or the unavailability of the subscriber. Law enforcement agencies may investigate suspensions for possible wrongdoing by persons requesting suspension.

(2) Unless the certification authority provides otherwise in the certificate or its certification practice statement, the secretary may suspend a certificate issued by a licensed certification authority for a period not to exceed five business days, if:

(a) A person identifying himself or herself as the subscriber named in the certificate, a person authorized to act for that subscriber, or a person acting on behalf of that unavailable subscriber requests suspension; and

(b) The requester represents that the certification authority that issued the certificate is unavailable.

The secretary may require the person requesting suspension to provide evidence, including a statement under oath or affirmation, regarding his or her identity, authorization, or the unavailability of the issuing certification authority, and may decline to suspend the certificate in its discretion. Law enforcement agencies may investigate suspensions by the secretary for possible wrongdoing by persons requesting suspension.

(3) Immediately upon suspension of a certificate by a licensed certification authority, the licensed certification authority must give notice of the suspension according to the specification in the certificate. If one or more repositories are specified, then the licensed certification authority must publish a signed notice of the suspension in all the repositories. If a repository no longer exists or refuses to accept publication, or if no repository is recognized under RCW 19.34.400, the licensed certification authority must also publish the notice in a recognized repository. If a certificate is suspended by the secretary, the secretary must give notice as required in this subsection for a licensed certification authority, provided that the person requesting suspension pays in advance any fee required by a repository for publication of the notice of suspension.

(4) A certification authority must terminate a suspension initiated by request only:

(a) If the subscriber named in the suspended certificate requests termination of the suspension, the certification authority has confirmed that the person requesting suspension is the subscriber or an agent of the subscriber authorized to terminate the suspension; or

(b) When the certification authority discovers and confirms that the request for the suspension was made without authorization by the subscriber. However, this subsection (4)(b) does not require the certification authority to confirm a request for suspension.

(5) The contract between a subscriber and a licensed certification authority may limit or preclude requested suspension by the certification authority, or may provide otherwise for termination of a requested suspension. However, if the contract limits or precludes suspension by the secretary when the issuing certification authority is unavailable, the limitation or preclusion is effective only if notice of it is published in the certificate.

(6) No person may knowingly or intentionally misrepresent to a certification authority his or her identity or authorization in requesting suspension of a certificate. Violation of this subsection is a gross misdemeanor.

(7) The secretary may authorize other state or local governmental agencies to perform any of the functions of the secretary under this section upon a regional basis. The authorization must be formalized by an agreement under chapter 39.34 RCW. The secretary may provide by rule the terms and conditions of the regional services.

(8) A suspension under this section must be completed within twenty-four hours of receipt of all information required in this section.

[2000 c 171 § 51; 1999 c 287 § 13; 1997 c 27 § 12; 1996 c 250 § 306.]

Notes:

Effective date -- 1999 c 287: See note following RCW 19.34.010.

Effective date -- Severability -- 1997 c 27: See notes following RCW 19.34.030.

19.34.260
Revocation of certificate — Confirmation — Notice — Release from security duty — Discharge of warranties.

(1) A licensed certification authority must revoke a certificate that it issued but which is not a transactional certificate, after:

(a) Receiving a request for revocation by the subscriber named in the certificate; and

(b) Confirming that the person requesting revocation is the subscriber, or is an agent of the subscriber with authority to request the revocation.

(2) A licensed certification authority must confirm a request for revocation and revoke a certificate within one business day after receiving both a subscriber's written request and evidence reasonably sufficient to confirm the identity and any agency of the person requesting the revocation.

(3) A licensed certification authority must revoke a certificate that it issued:

(a) Upon receiving a certified copy of the subscriber's death certificate, or upon confirming by other evidence that the subscriber is dead; or

(b) Upon presentation of documents effecting a dissolution of the subscriber, or upon confirming by other evidence that the subscriber has been dissolved or has ceased to exist, except that if the subscriber is dissolved and is reinstated or restored before revocation is completed, the certification authority is not required to revoke the certificate.

(4) A licensed certification authority may revoke one or more certificates that it issued if the certificates are or become unreliable, regardless of whether the subscriber consents to the revocation and notwithstanding a provision to the contrary in a contract between the subscriber and certification authority.

(5) Immediately upon revocation of a certificate by a licensed certification authority, the licensed certification authority must give notice of the revocation according to the specification in the certificate. If one or more repositories are specified, then the licensed certification authority must publish a signed notice of the revocation in all repositories. If a repository no longer exists or refuses to accept publication, or if no repository is recognized under RCW 19.34.400, then the licensed certification authority must also publish the notice in a recognized repository.

(6) A subscriber ceases to certify, as provided in RCW 19.34.230, and has no further duty to keep the private key secure, as required by RCW 19.34.240, in relation to the certificate whose revocation the subscriber has requested, beginning at the earlier of either:

(a) When notice of the revocation is published as required in subsection (5) of this section; or

(b) One business day after the subscriber requests revocation in writing, supplies to the issuing certification authority information reasonably sufficient to confirm the request, and pays any contractually required fee.

(7) Upon notification as required by subsection (5) of this section, a licensed certification authority is discharged of its warranties based on issuance of the revoked certificate, as to transactions occurring after the notification, and ceases to certify as provided in RCW 19.34.220 (2) and (3) in relation to the revoked certificate.

[1997 c 27 § 13; 1996 c 250 § 307.]

Notes:

Effective date -- Severability -- 1997 c 27: See notes following RCW 19.34.030.

19.34.270
Certificate — Expiration.

(1) A certificate must indicate the date on which it expires.

(2) When a certificate expires, the subscriber and certification authority cease to certify as provided in this chapter and the certification authority is discharged of its duties based on issuance, in relation to the expired certificate.

[1996 c 250 § 308.]

19.34.280
Recommended reliance limit — Liability — Damages.

(1) By clearly specifying a recommended reliance limit in a certificate and in the certification practice statement, the issuing certification authority recommends that persons rely on the certificate only to the extent that the total amount at risk does not exceed the recommended reliance limit.

(2) Subject to subsection (3) of this section, unless a licensed certification authority waives application of this subsection, a licensed certification authority is:

(a) Not liable for a loss caused by reliance on a false or forged digital signature of a subscriber, if, with respect to the false or forged digital signature, the certification authority complied with all material requirements of this chapter;

(b) Not liable in excess of the amount specified in the certificate as its recommended reliance limit for either:

(i) A loss caused by reliance on a misrepresentation in the certificate of a fact that the licensed certification authority is required to confirm; or

(ii) Failure to comply with RCW 19.34.210 in issuing the certificate;

(c) Not liable for:

(i) Punitive or exemplary damages. Nothing in this chapter may be interpreted to permit punitive or exemplary damages that would not otherwise be permitted by the law of this state; or

(ii) Damages for pain or suffering.

(3) Nothing in subsection (2)(a) of this section relieves a licensed certification authority of its liability for breach of any of the warranties or certifications it gives under RCW 19.34.220 or for its lack of good faith, which warranties and obligation of good faith may not be disclaimed. However, the standards by which the performance of a licensed certification authority's obligation of good faith is to be measured may be determined by agreement or notification complying with subsection (4) of this section if the standards are not manifestly unreasonable. The liability of a licensed certification authority under this subsection is subject to the limitations in subsection (2)(b) and (c) of this section unless the limits are waived by the licensed certification authority.

(4) Consequential or incidental damages may be liquidated, or may otherwise be limited, altered, or excluded unless the limitation, alteration, or exclusion is unconscionable. A licensed certification authority may liquidate, limit, alter, or exclude consequential or incidental damages as provided in this subsection by agreement or by notifying any person who will rely on a certificate of the liquidation, limitation, alteration, or exclusion before the person relies on the certificate.

[1999 c 287 § 14; 1997 c 27 § 14; 1996 c 250 § 309.]

Notes:

Effective date -- 1999 c 287: See note following RCW 19.34.010.

Effective date -- Severability -- 1997 c 27: See notes following RCW 19.34.030.

19.34.290
Collection based on suitable guaranty — Proceeds — Attorneys' fees — Costs — Notice — Recovery of qualified right of payment.

(1)(a) If the suitable guaranty is a surety bond, a person may recover from the surety the full amount of a qualified right to payment against the principal named in the bond, or, if there is more than one such qualified right to payment during the term of the bond, a ratable share, up to a maximum total liability of the surety equal to the amount of the bond.

(b) If the suitable guaranty is a letter of credit, a person may recover from the issuing financial institution only in accordance with the terms of the letter of credit.

Claimants may recover successively on the same suitable guaranty, provided that the total liability on the suitable guaranty to all persons making qualified rights of payment during its term must not exceed the amount of the suitable guaranty.

(2) In addition to recovering the amount of a qualified right to payment, a claimant may recover from the proceeds of the guaranty, until depleted, the attorneys' fees, reasonable in amount, and court costs incurred by the claimant in collecting the claim,

provided that the total liability on the suitable guaranty to all persons making qualified rights of payment or recovering attorneys' fees during its term must not exceed the amount of the suitable guaranty.

(3) To recover a qualified right to payment against a surety or issuer of a suitable guaranty, the claimant must:

(a) File written notice of the claim with the secretary stating the name and address of the claimant, the amount claimed, and the grounds for the qualified right to payment, and any other information required by rule by the secretary; and

(b) Append to the notice a certified copy of the judgment on which the qualified right to payment is based.

Recovery of a qualified right to payment from the proceeds of the suitable guaranty is barred unless the claimant substantially complies with this subsection (3).

(4) Recovery of a qualified right to payment from the proceeds of a suitable guaranty are forever barred unless notice of the claim is filed as required in subsection (3)(a) of this section within three years after the occurrence of the violation of this chapter that is the basis for the claim. Notice under this subsection need not include the requirement imposed by subsection (3)(b) of this section.

[1996 c 250 § 310.]

19.34.291
Discontinuation of certification authority services — Duties of authority — Continuation of guaranty — Process to maintain and update records — Rules — Costs.

(1) A licensed certification authority that discontinues providing certification authority services shall:

(a) Notify all subscribers listed in valid certificates issued by the certification authority, before discontinuing services;

(b) Minimize, to the extent commercially reasonable, disruption to the subscribers of valid certificates and relying parties; and

(c) Make reasonable arrangements for preservation of the certification authority's records.

(2) A suitable guaranty of a licensed certification authority may not be released until the expiration of the term specified in the guaranty.

(3) The secretary may provide by rule for a process by which the secretary may, in any combination, receive, administer, or disburse the records of a licensed certification authority or a recognized repository that discontinues providing services, for the purpose of maintaining access to the records and revoking any previously issued valid certificates in a manner that minimizes disruption to subscribers and relying parties. The secretary's rules may include provisions by which the secretary may recover costs incurred in doing so.

[1997 c 27 § 15.]

Notes:

Effective date -- Severability -- 1997 c 27: See notes following RCW 19.34.030.

19.34.300
Satisfaction of signature requirements.

(1) Where a rule of law requires a signature, or provides for certain consequences in the absence of a signature, that rule is satisfied by a digital signature, if:

(a) The digital signature is verified by reference to the public key listed in a valid certificate issued by a licensed certification authority;

(b) The digital signature was affixed by the signer with the intention of signing the message; and

(c) The recipient has no knowledge or notice that the signer either:

(i) Breached a duty as a subscriber; or

(ii) Does not rightfully hold the private key used to affix the digital signature.

(2) Nothing in this chapter:

(a) Precludes a mark from being valid as a signature under other applicable law;

(b) May be construed to obligate a recipient or any other person asked to rely on a digital signature to accept a digital signature or to respond to an electronic message containing a digital signature except as provided in RCW 19.34.321; or

(c) Precludes the recipient of a digital signature or an electronic message containing a digital signature from establishing the conditions under which the recipient will accept a digital signature.

[1997 c 27 § 16; 1996 c 250 § 401.]

Notes:

Effective date -- Severability -- 1997 c 27: See notes following RCW 19.34.030.

19.34.305
Acceptance of digital signature in reasonable manner.

Acceptance of a digital signature may be made in any manner reasonable in the circumstances.

[1997 c 27 § 31.]

Notes:

Effective date -- Severability -- 1997 c 27: See notes following RCW 19.34.030.

19.34.310
Unreliable digital signatures — Risk.

Unless otherwise provided by law or contract, the recipient of a digital signature assumes the risk that a digital signature is forged, if reliance on the digital signature is not reasonable under the circumstances.

[1997 c 27 § 17; 1996 c 250 § 402.]

Notes:

Effective date -- Severability -- 1997 c 27: See notes following RCW 19.34.030.

19.34.311
Reasonableness of reliance — Factors.

The following factors, among others, are significant in evaluating the reasonableness of a recipient's reliance upon a certificate and upon the digital signatures verifiable with reference to the public key listed in the certificate:

(1) Facts which the relying party knows or of which the relying party has notice, including all facts listed in the certificate or incorporated in it by reference;

(2) The value or importance of the digitally signed message, if known;

(3) The course of dealing between the relying person and subscriber and the available indicia of reliability or unreliability apart from the digital signature; and

(4) Usage of trade, particularly trade conducted by trustworthy systems or other computer-based means.

[1997 c 27 § 18.]

Notes:

Effective date -- Severability -- 1997 c 27: See notes following RCW 19.34.030.

19.34.320
Digital message as written on paper — Requirements — Other requirements not affected — Exception from uniform commercial code.

A message is as valid, enforceable, and effective as if it had been written on paper, if it:

(1) Bears in its entirety a digital signature; and

(2) That digital signature is verified by the public key listed in a certificate that:

(a) Was issued by a licensed certification authority; and

(b) Was valid at the time the digital signature was created.

Nothing in this chapter shall be construed to eliminate, modify, or condition any other requirements for a contract to be valid, enforceable, and effective. No digital message shall be deemed to be an instrument under Title 62A RCW unless all parties to the transaction agree, including financial institutions affected.

[1997 c 27 § 19; 1996 c 250 § 403.]

Notes:

Effective date -- Severability -- 1997 c 27: See notes following RCW 19.34.030.

19.34.321
Acceptance of certified court documents in electronic form — Requirements — Rules of court on use in proceedings.

(1) A person may not refuse to honor, accept, or act upon a court order, writ, or warrant upon the basis that it is electronic in form and signed with a digital signature, if the digital signature was certified by a licensed certification authority or otherwise issued under court rule. This section applies to a paper printout of a digitally signed document, if the printout reveals that the digital signature was electronically verified before the printout, and in the absence of a finding that the document has been altered.

(2) Nothing in this chapter shall be construed to limit the authority of the supreme court to adopt rules of pleading, practice, or procedure, or of the court of appeals or superior courts to adopt supplementary local rules, governing the use of electronic messages or documents, including rules governing the use of digital signatures, in judicial proceedings.

[1997 c 27 § 20.]

Notes:

Effective date -- Severability -- 1997 c 27: See notes following RCW 19.34.030.

19.34.330
Digital message deemed original.

A digitally signed message shall be deemed to be an original of the message.

[1999 c 287 § 15; 1996 c 250 § 404.]

Notes:

Effective date -- 1999 c 287: See note following RCW 19.34.010.

19.34.340
Certificate as acknowledgment — Requirements — Exception — Responsibility of certification authority.

(1) Unless otherwise provided by law or contract, if so provided in the certificate issued by a licensed certification authority, a digital signature verified by reference to the public key listed in a valid certificate issued by a licensed certification authority satisfies the requirements for an acknowledgment under RCW 42.44.010(4) and for acknowledgment of deeds and other real property conveyances under RCW 64.04.020 if words of an express acknowledgment appear with the digital signature regardless of whether the signer personally appeared before either the certification authority or some other person authorized to take acknowledgments of deeds, mortgages, or other conveyance instruments under RCW 64.08.010 when the digital signature was created, if that digital signature is:

(a) Verifiable by that certificate; and

(b) Affixed when that certificate was valid.

(2) If the digital signature is used as an acknowledgment, then the certification authority is responsible to the same extent as a notary up to the recommended reliance limit for failure to satisfy the requirements for an acknowledgment. The certification authority may not disclaim or limit, other than as provided in RCW 19.34.280, the effect of this section.

[1997 c 27 § 21; 1996 c 250 § 405.]

Notes:

Effective date -- Severability -- 1997 c 27: See notes following RCW 19.34.030.

19.34.350
Adjudicating disputes — Presumptions.

In adjudicating a dispute involving a digital signature, it is rebuttably presumed that:

(1) A certificate digitally signed by a licensed certification authority and either published in a recognized repository, or made available by the issuing certification authority or by the subscriber listed in the certificate is issued by the certification authority that digitally signed it and is accepted by the subscriber listed in it.

(2) The information listed in a valid certificate and confirmed by a licensed certification authority issuing the certificate is

accurate.

(3) If a digital signature is verified by the public key listed in a valid certificate issued by a licensed certification authority:

(a) That digital signature is the digital signature of the subscriber listed in that certificate;

(b) That digital signature was affixed by that subscriber with the intention of signing the message;

(c) The message associated with the digital signature has not been altered since the signature was affixed; and

(d) The recipient of that digital signature has no knowledge or notice that the signer:

(i) Breached a duty as a subscriber; or

(ii) Does not rightfully hold the private key used to affix the digital signature.

(4) A digital signature was created before it was time stamped by a disinterested person utilizing a trustworthy system.

[1997 c 27 § 22; 1996 c 250 § 406.]

Notes:

Effective date -- Severability -- 1997 c 27: See notes following RCW 19.34.030.

19.34.351
Alteration of chapter by agreement — Exceptions.

The effect of this chapter may be varied by agreement, except:

(1) A person may not disclaim responsibility for lack of good faith, but parties may by agreement determine the standards by which the duty of good faith is to be measured if the standards are not manifestly unreasonable; and

(2) As otherwise provided in this chapter.

[1997 c 27 § 34.]

Notes:

Effective date -- Severability -- 1997 c 27: See notes following RCW 19.34.030.

19.34.360
Presumptions of validity/limitations on liability — Conformance with chapter.

The presumptions of validity and reasonableness of conduct, and the limitations on liability in this chapter do not apply to electronic records or electronic signatures except for digital signatures created in conformance with all of the requirements of this chapter and rules adopted under this chapter.

[1999 c 287 § 3.]

Notes:

Effective date -- 1999 c 287: See note following RCW 19.34.010.

19.34.400
Recognition of repositories — Application — Discontinuance — Procedure.

(1) The secretary must recognize one or more repositories, after finding that a repository to be recognized:

(a) Is a licensed certification authority;

(b) Includes, or will include, a database containing:

(i) Certificates published in the repository;

(ii) Notices of suspended or revoked certificates published by licensed certification authorities or other persons suspending or revoking certificates; and

(iii) Other information adopted by rule by the secretary;

(c) Operates by means of a trustworthy system, that may, under administrative rule of the secretary, include additional or different attributes than those applicable to a certification authority that does not operate as a recognized repository;

(d) Contains no significant amount of information that is known or likely to be untrue, inaccurate, or not reasonably reliable;

(e) Keeps a record of certificates that have been suspended or revoked, or that have expired, in accordance with requirements adopted by rule by the secretary; and

(f) Complies with other reasonable requirements adopted by rule by the secretary.

(2) A repository may apply to the secretary for recognition by filing a written request and providing evidence to the secretary sufficient for the secretary to find that the conditions for recognition are satisfied, in accordance with requirements adopted by rule by the secretary.

(3) A repository may discontinue its recognition by filing thirty days' written notice with the secretary, upon meeting any conditions for discontinuance adopted by rule by the secretary. In addition the secretary may discontinue recognition of a repository in accordance with the administrative procedure act, chapter 34.05 RCW, if the secretary concludes that the repository no longer satisfies the conditions for recognition listed in this section or in rules adopted by the secretary.

[1999 c 287 § 16; 1997 c 27 § 23; 1996 c 250 § 501.]

Notes:

Effective date -- 1999 c 287: See note following RCW 19.34.010.

Effective date -- Severability -- 1997 c 27: See notes following RCW 19.34.030.

19.34.410
Repositories — Liability — Exemptions — Liquidation, limitation, alteration, or exclusion of damages.

(1) Notwithstanding a disclaimer by the repository or a contract to the contrary between the repository, a certification authority, or a subscriber, a repository is liable for a loss incurred by a person reasonably relying on a digital signature verified by the public key listed in a certificate that has been suspended or revoked by the licensed certification authority that issued the certificate, if loss was incurred more than one business day after receipt by the repository of a request from the issuing licensed certification authority to publish notice of the suspension or revocation, and the repository had failed to publish the notice when the person relied on the digital signature.

(2) Unless waived, a recognized repository or the owner or operator of a recognized repository is:

(a) Not liable for failure to record publication of a suspension or revocation, unless the repository has received notice of publication and one business day has elapsed since the notice was received;

(b) Not liable under subsection (1) of this section in excess of the amount specified in the certificate as the recommended reliance limit;

(c) Not liable under subsection (1) of this section for:

(i) Punitive or exemplary damages; or

(ii) Damages for pain or suffering;

(d) Not liable for misrepresentation in a certificate published by a licensed certification authority;

(e) Not liable for accurately recording or reporting information that a licensed certification authority, or court clerk, or the secretary has published as required or permitted in this chapter, including information about suspension or revocation of a certificate;

(f) Not liable for reporting information about a certification authority, a certificate, or a subscriber, if the information is published as required or permitted in this chapter or a rule adopted by the secretary, or is published by order of the secretary in the performance of the licensing and regulatory duties of that office under this chapter.

(3) Consequential or incidental damages may be liquidated, or may otherwise be limited, altered, or excluded unless the limitation, alteration, or exclusion is unconscionable. A recognized repository may liquidate, limit, alter, or exclude damages as provided in this subsection by agreement, or by notifying any person who will rely on a digital signature verified by the public key listed in a suspended or revoked certificate of the liquidation, limitation, alteration, or exclusion before the person relies on the certificate.

[1999 c 287 § 17; 1997 c 27 § 33; 1996 c 250 § 502.]

Notes:

Effective date -- 1999 c 287: See note following RCW 19.34.010.

Effective date -- Severability -- 1997 c 27: See notes following RCW 19.34.030.

19.34.420
Confidentiality of certain records — Limited access to state auditor.

***** CHANGE IN 2011 *** (SEE** 5931-S.SL**) *****

(1) The following information, when in the possession of the secretary, the department of information services, or the state auditor for purposes of this chapter, shall not be made available for public disclosure, inspection, or copying, unless the request is made under an order of a court of competent jurisdiction based upon an express written finding that the need for the information outweighs any reason for maintaining the privacy and confidentiality of the information or records:

(a) A trade secret, as defined by RCW 19.108.010; and

(b) Information regarding design, security, or programming of a computer system used for purposes of licensing or operating a certification authority or repository under this chapter.

(2) The state auditor, or an authorized agent, must be given access to all information referred to in subsection (1) of this section for the purpose of conducting audits under this chapter or under other law, but shall not make that information available for public inspection or copying except as provided in subsection (1) of this section.

[1998 c 33 § 2.]

19.34.500
Rule making.

The secretary of state may adopt rules to implement this chapter beginning July 27, 1997, but the rules may not take effect until January 1, 1998.

[1997 c 27 § 24; 1996 c 250 § 603.]

Notes:

Severability -- 1997 c 27: See note following RCW 19.34.030.

19.34.501
Chapter supersedes and preempts local actions.

This chapter supersedes and preempts all local laws or ordinances regarding the same subject matter.

[1997 c 27 § 25.]

Notes:

Effective date -- Severability -- 1997 c 27: See notes following RCW 19.34.030.

19.34.502
Criminal prosecution not precluded — Remedies not exclusive — Injunctive relief availability.

This chapter does not preclude criminal prosecution under other laws of this state, nor may any provision of this chapter be regarded as an exclusive remedy for a violation. Injunctive relief may not be denied to a party regarding conduct governed by this chapter on the basis that the conduct is also subject to potential criminal prosecution.

[1997 c 27 § 26.]

Notes:

Effective date -- Severability -- 1997 c 27: See notes following RCW 19.34.030.

19.34.503
Jurisdiction, venue, choice of laws.

Issues regarding jurisdiction, venue, and choice of laws for all actions involving digital signatures must be determined according to the same principles as if all transactions had been performed through paper documents.

[1997 c 27 § 27.]

Notes:

Effective date -- Severability -- 1997 c 27: See notes following RCW 19.34.030.

19.34.900

Short title.

This chapter shall be known and may be cited as the Washington electronic authentication act.

[1996 c 250 § 101.]

19.34.901
Effective date — 1996 c 250.

(1) Sections 101 through 601, 604, and 605, chapter 250, Laws of 1996 take effect January 1, 1998.

(2) Sections 602 and 603, chapter 250, Laws of 1996 take effect July 27, 1997.

[2000 c 171 § 52; 1997 c 27 § 28; 1996 c 250 § 602.]

Notes:

Severability -- 1997 c 27: See note following RCW 19.34.030.

19.34.902
Severability — 1996 c 250.

If any provision of this act or its application to any person or circumstance is held invalid, the remainder of the act or the application of the provision to other persons or circumstances is not affected.

[1996 c 250 § 604.]

19.34.903
Part headings and section captions not law — 1996 c 250.

Part headings and section captions as used in this act do not constitute any part of the law.

[1996 c 250 § 605.]

Chapter 434-180 WAC
Electronic authentication

Last Update: 1/29/10

WAC Sections

PART 1

GENERAL PRINCIPLES

PART 2

CERTIFICATION AUTHORITY LICENSE APPLICATION, SUSPENSION, REVOCATION

PART 3

CERTIFICATION AUTHORITY STANDARDS AND PRACTICES

PART 4

RECOGNITION OF REPOSITORIES

PART 5

PROCEEDINGS BEFORE THE SECRETARY

DISPOSITIONS OF SECTIONS FORMERLY CODIFIED IN THIS CHAPTER

434-180-110 Office address, hours, and telephone number. [Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111, and 19.34.400. 00-21-087, § 434-180-110, filed 10/17/00, effective 11/17/00; 97-24-053, § 434-180-110, filed 11/26/97, effective 12/27/97.] Repealed by 04-04-018, filed 1/23/04, effective 2/23/04. Statutory Authority: RCW 23B.01.200(2), 24.03.007, [24.03.]008, 25.15.007, 19.09.020 (15), [19.09].315,19.77.115 , and 43.07.170.

434-180-235 Sufficient working capital. [Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-235, filed 11/26/97, effective 12/27/97.] Repealed by 98-16-031, filed 7/29/98, effective 8/29/98. Statutory Authority: Chapter 19.34 RCW, including RCW 19.34.030, 19.34.040, 19.34.100, 19.34.400, 19.34.500 and 1998 c 33.

434-180-100
Scope and purpose of chapter.

This chapter implements the Washington Electronic Authentication Act, codified as chapter 19.34 RCW.

[Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-100, filed 11/26/97, effective 12/27/97.]

434-180-120
Definitions.

For purposes of this chapter, all terms defined in RCW 19.34.020 have the meanings set forth in statute. Additionally, the following terms shall have the following meanings:

(1) "Operative personnel" means one or more natural persons acting as an agent of a licensed certification authority, or in the employment of, or under contract with, a licensed certification authority, and who have:

(a) Managerial or policy making responsibilities for such licensed certification authority; or

(b) Duties directly involving the issuance of certificates (including the identification of persons requesting a certificate from a certification authority), creation of private keys, or administration of a licensed certification authority's computing facilities.

(2) "Managerial or policy making responsibilities" means direct responsibility for the day-to-day operations, security and performance of those business activities that are regulated under chapter 19.34 of the Revised Code of Washington. If a licensed certification authority is a corporation, then it is presumed that the members of the board of directors, among others, exercise managerial or policy making responsibilities, unless the board delegates those duties in writing to one or more officers or employees of the corporation.

(3) "Presiding officer" means the secretary or an administrative law judge assigned to preside over an adjudicative hearing pursuant to this chapter.

(4) "X.509" means the specific set of technical standards identified by that name which were adopted by the international telecommunication union, formerly known as the international telegraph and telephone consultation committee. For purposes of these rules, all references to X.509 shall be construed as referring to version 3. Compliance with only versions 1 or 2 shall not be construed as compliance with X.509.

[Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-120, filed 11/26/97, effective 12/27/97.]

434-180-130
Fees.

Fees for services performed by the secretary of state are established in the following amounts:

(1) For application for a license as a certification authority:

(a) For the applicant's first year doing business as a licensed certification authority in this state: One thousand four hundred dollars;

(b) For the applicant's subsequent biennial renewal doing business as a licensed certification authority in this state: Two thousand eight hundred dollars.

(2) For recognition as a repository, in addition to the license issuance or renewal fee paid pursuant to this section:

(a) For the applicant's first year doing business as a recognized repository in this state: One thousand four hundred dollars;

(b) For the applicant's subsequent biennial renewal doing business as a recognized repository in this state: Two thousand eight hundred dollars.

(3) For recognition of a foreign license: One-half of the otherwise applicable fee as set forth under subsection (1) or (2) of this section.

(4) For qualification of operative personnel:

(a) For administering and scoring the examination required by WAC 434-180-215(3), fifty dollars per individual; and

(b) For qualifying operative personnel pursuant to WAC 434-180-215 and 434-180-220, other than (or in addition to) administering and scoring the examination, twenty-five dollars per individual.

[Statutory Authority: RCW 19.34.101, 19.34.500. 10-04-057, § 434-180-130, filed 1/29/10, effective 3/1/10. Statutory Authority: Chapter 19.34 RCW, including RCW 19.34.030, 19.34.040, 19.34.100, 19.34.400, 19.34.500 and 1998 c 33. 98-16-031, § 434-180-130, filed 7/29/98, effective 8/29/98. Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-130, filed 11/26/97, effective 12/27/97.]

434-180-200
Application for license as a certification authority.

Any person desiring to be licensed as a certification authority must file an application pursuant to this chapter demonstrating compliance with the requirements of RCW 19.34.100. To apply for a license, an applicant must submit all of the following:

(1) A completed application form as prescribed by WAC 434-180-210;

(2) The fee or fees provided by WAC 434-180-130;

(3) A certificate that shows the applicant as subscriber and is published in a recognized repository;

(4) A suitable guaranty, described by WAC 434-180-225, unless the applicant is a self-insured city, a self-insured county, or the department of information services of the state of Washington;

(5) Documentation, in the form of an information systems audit report, establishing that the applicant has the use of a trustworthy system as defined by WAC 434-180-360. The audit required by this subsection shall be performed pursuant to WAC 434-180-240, except that it is not required to establish anything more than that the applicant has the use of a trustworthy system;

(6) Materials establishing, to the satisfaction of the secretary that each person listed as operative personnel has qualified to act as operative personnel pursuant to WAC 434-180-215; and

(7) A written certification practice statement as described in WAC 434-180-330.

[Statutory Authority: Chapter 19.34 RCW, including RCW 19.34.030, 19.34.040, 19.34.100, 19.34.400, 19.34.500 and 1998 c 33. 98-16-031, § 434-180-200, filed 7/29/98, effective 8/29/98. Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-200, filed 11/26/97, effective 12/27/97.]

434-180-203
Designation of confidential information.

Any certification authority, recognized repository, or applicant for licensure or recognition who believes that any information submitted to the secretary is legally exempt from public disclosure, inspection, or copying pursuant to law may designate such records upon submission to the secretary. Such designation does not conclusively establish the application of any exemption, but will assist the secretary in correctly responding to requests for public records. Any designation shall specify the precise information the party regards as subject to an exemption, and precise statute establishing the exemption.

[Statutory Authority: Chapter 19.34 RCW, including RCW 19.34.030, 19.34.040, 19.34.100, 19.34.400, 19.34.500 and 1998 c 33. 98-16-031, § 434-180-203, filed 7/29/98, effective 8/29/98.]

434-180-205
Issuance of license or renewal.

The secretary shall, within a reasonable time, issue or renew a license as a certification authority if the applicant has:

(1) Submitted all documentation required by WAC 434-180-200 and 434-180-210; and

(2) The secretary has determined that the applicant meets all requirements for licensure.

(3) Issuance of a license shall be valid for a period of one year. Renewal of a license shall be valid for a period of two years. Failure to receive a notice of the need to renew a license is an insufficient reason for failing to file the required application for renewal.

[Statutory Authority: RCW 19.34.101, 19.34.500. 10-04-057, § 434-180-205, filed 1/29/10, effective 3/1/10. Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-205, filed 11/26/97, effective 12/27/97.]

434-180-210
Form.

Each application for a license, or renewal of a license, as a certification authority shall be submitted on a form prescribed by the secretary. The completed form shall contain the following:

(1) The name of the applicant;

(2) The applicant's uniform business identifier number, if any;

(3) The mailing address of the applicant, and a physical address if different;

(4) The telephone number of the applicant;

(5) The electronic mail address of the applicant;

(6) The name and address of the applicant's registered agent for service of process, other than the secretary. Address information shall include a physical address, but may additionally provide a mailing address if different;

(7) The names of all operative personnel; and

(8) The appointment of the secretary of state as the applicant's agent for service of process.

[Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-210, filed 11/26/97, effective 12/27/97.]

434-180-215
Certification of operative personnel.

The secretary shall not issue or renew a license as a certification authority unless the licensee documents that every individual employed or acting as operative personnel qualifies to act as operative personnel. This documentation shall include:

(1) Receipt of a completed form, signed by the individual under penalty of perjury, stating:

(a) The name (including all other names used in the past), date of birth, and business address of the individual;

(b) That the individual has not been convicted within the past seven years of a felony and has never been convicted of a crime involving fraud, false statement, or deception in any jurisdiction; and

(c) If the individual has resided in any nation other than the United States during the previous five years, the name of that nation and the period of residency.

(2) A criminal background check supporting the declaration required by subsection (1) of this section. This requirement is excused as to any individual for whom documentation satisfying this paragraph was submitted within the previous two years, even if the individual has changed employment. This check must include both of the following:

(a) A criminal background check compiled by a private sector provider, documenting a background check reasonably sufficient to disclose any criminal convictions within the previous seven years in any state or federal jurisdiction in the United States, its territories, or possessions, and any other jurisdiction specified pursuant to subsection (1)(c) of this section. This background check must contain information that is current to within thirty days of its date of submission; and

(b) The certified results of a criminal background check performed by the Washington state patrol or law enforcement agency where the operative personnel reside and are employed for the previous seven years, dated not more than thirty days prior to submission or such other jurisdictions as the secretary may reasonably request. Such check shall be performed using the individual's fingerprints.

(3) Satisfactory completion by the individual of a written examination demonstrating knowledge and proficiency in following the requirements of the Washington Electronic Authentication Act and these rules. The secretary shall develop an open book written test covering the subject matter of the act, and provide it upon request, which may include electronic access. The secretary may update or modify the test from time to time. The secretary shall indicate at the top of the test the percentage or number of questions that must be answered correctly in order to constitute satisfactory completion. No individual may take the examination more than once within a period of thirty days. A certification by the secretary that an individual has successfully completed this examination shall be valid for two years, and shall continue to satisfy the requirements of this subsection even if the individual changes employment.

(4) A licensed certification authority must remove a person from performing the functions of operative personnel immediately upon learning that the person has been convicted within the past seven years of a felony or has ever been convicted of a crime involving fraud, false statement, or deception, and must notify the secretary of this action within three

business days.

[Statutory Authority: Chapter 19.34 RCW and 1998 c 33. 99-02-047, § 434-180-215, filed 1/4/99, effective 2/4/99. Statutory Authority: Chapter 19.34 RCW, including RCW 19.34.030, 19.34.040, 19.34.100, 19.34.400, 19.34.500 and 1998 c 33. 98-16-031, § 434-180-215, filed 7/29/98, effective 8/29/98. Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-215, filed 11/26/97, effective 12/27/97.]

434-180-220
Qualification of newly designated operative personnel.

No licensed certification authority may assign any individual to perform the functions of operative personnel if that individual has not been certified by the secretary pursuant to WAC 434-180-215. Such certification may be obtained by application to the secretary at any time, without regard to the time at which the certification authority's license is subject to renewal.

[Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-220, filed 11/26/97, effective 12/27/97.]

434-180-225
Suitable guaranty.

(1) The suitable guaranty required for licensure as a certification authority may be in the form of either a surety bond executed by an insurer lawfully operating in this state, or an irrevocable letter of credit issued by a financial institution authorized to do business in this state.

(2) The suitable guaranty must be in an amount of at least fifty thousand dollars.

(3) As to form, the suitable guaranty must:

(a) Identify the insurer issuing the suitable guaranty or financial institution upon which it is drawn, including name, mailing address, and physical address, and identify by number or copy its licensure or approval as a financial institution, or in the case of an insurer, as an insurer in this state;

(b) Identify the certification authority on behalf of which it is issued;

(c) Be issued payable to the secretary for the benefit of persons holding qualified rights of payment against the licensed certification authority named as principal of the bond or customer of the letter of credit;

(d) State that it is issued for filing under the Washington Electronic Authentication Act; and

(e) Specify a term of effectiveness extending at least as long as the term of the license to be issued to the certification authority.

[Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-225, filed 11/26/97, effective 12/27/97.]

434-180-240
Compliance audits.

(1) A licensed certification authority shall obtain a compliance audit at least once every year. The auditor shall issue an opinion evaluating the degree to which the certification authority conforms to the requirements of this chapter and of chapter 19.34 RCW. If the certification authority is also a recognized repository, the audit must include the repository.

(2) For purposes of the opinion required by this section, the auditor shall exercise reasonable professional judgment as to

whether a condition that does not strictly comply with legal requirements is or is not material, taking into consideration the circumstances and context. Noncompliance as to any of the following shall be deemed material, in addition to any others the auditor may judge to be material:

(a) Any condition of noncompliance with statute or rule that relates to the validity of a certificate;

(b) Any employee performing the functions of operative personnel who has not qualified pursuant to WAC 434-180-215;

(c) Any material indication that the certification authority has used any system other than a trustworthy system.

(3) An audit may be performed by any licensed certified public accountant, or, in the case of a public agency, by the Washington state auditor. For purposes of this section, licensed certified public accountants include any person holding a certified public accountant certificate issued pursuant to chapter 18.04 RCW, or any licensee under any equivalent law of any other jurisdiction. Any auditor, or group of auditors, performing an audit pursuant to this section shall include at least one individual who has been issued a current and valid certificate as either a certified information systems auditor, by the information systems audit and control foundation, or as a certified information systems security professional, by the International Information Systems Security Certification Consortium. The names of all individuals possessing such certificates shall be disclosed in the audit report, or in a cover letter accompanying that report.

(4) The certification authority shall file a copy of the audit report with the secretary, prior to the date the certification authority must renew its license pursuant to WAC 434-180-205. At the certification authority's option, it shall be sufficient to file a portion of the report if that report summarizes all audit exceptions and conditions of noncompliance (including, but not limited to, those stated in subsection (2) of this section) stated in the full report, and bears the auditor's signature. The report may be filed electronically, if it is validly digitally signed by the auditor, using a licensed certification authority. The secretary shall publish the report, or summary, in the certification authority disclosure record it maintains for the certification authority.

[Statutory Authority: Chapter 19.34 RCW, including RCW 19.34.030, 19.34.040, 19.34.100, 19.34.400, 19.34.500 and 1998 c 33. 98-16-031, § 434-180-240, filed 7/29/98, effective 8/29/98. Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-240, filed 11/26/97, effective 12/27/97.]

434-180-245
Recognition of foreign licenses.

(1) A certification authority licensed as such by a governmental entity other than the state of Washington, may act as a licensed certification authority in Washington only if, in addition to meeting any other requirements established by law for the transaction of business, it either:

(a) Obtains a license as a certification authority from the secretary; or

(b) Provides to the secretary a certified copy of a license issued by a governmental entity whose licensing or authorization requirements the secretary has found to be substantially similar to those of Washington, together with the fee required by WAC 434-180-130. A license recognized under this subsection shall be valid in Washington only during the time it is valid in the issuing jurisdiction.

(2) The secretary may certify that the licensing or authorization requirements of another jurisdiction are substantially similar to those of Washington if, in order to obtain a license, the controlling law of the other jurisdiction requires that a licensed certification authority:

(a) Issue certificates based upon a system of public key cryptography using a trustworthy system. The law or administrative rule of another jurisdiction must establish standards determining what constitutes a trustworthy system. Those standards may differ from Washington's standards as set forth under WAC 434-180-360 as long as they are substantially similar in purpose and result;

(b) Provide a suitable guaranty in an amount of at least twenty-five thousand dollars;

(c) Employ as operative personnel only individuals who have demonstrated knowledge and proficiency in the requirements of the law regarding digital signatures, and who are free of felony criminal conviction for a minimum of seven years; and

(d) Be subject to a legally established system of enforcement of licensure requirements.

(3) If the requirements of another jurisdiction fail to be certified as substantially similar to those of Washington only because

they do not satisfy subsection (2)(c) of this section, then the secretary shall recognize the license of a particular certification authority licensed by that jurisdiction if the certification authority complies with subsection (1)(b) of this section and, in addition, employs as operative personnel only individuals whom the secretary has certified pursuant to WAC 434-180-215.

(4) The secretary shall publish in the *State Register*, and make available upon request, a list of those jurisdictions which the secretary has certified pursuant to subsection (2) of this section. If a jurisdiction is not included in the list most recently published in the *State Register*, the secretary shall consider whether certification of such jurisdiction should be added, upon request of either the jurisdiction or a certification authority licensed by that jurisdiction and upon receipt of an English language copy of the applicable laws and regulations of that jurisdiction.

[Statutory Authority: Chapter 19.34 RCW, including RCW 19.34.030, 19.34.040, 19.34.100, 19.34.400, 19.34.500 and 1998 c 33. 98-16-031, § 434-180-245, filed 7/29/98, effective 8/29/98. Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-245, filed 11/26/97, effective 12/27/97.]

434-180-250
Revocation or suspension of license.

(1) The secretary may revoke or suspend a license, pursuant to chapter 34.05 RCW, for failure to comply with any requirement of chapter 19.34 RCW or this chapter, for failure to remain qualified for a license pursuant to chapter 19.34 RCW or this chapter, or for failure to comply with a lawful order of the secretary.

(2) The secretary shall inform a licensed certification authority by written order, by mail directed to the mailing address or electronic mail address listed on the licensee's application, of a decision to revoke or suspend the license. The notification shall state when the revocation or suspension shall be effective, which shall not be less than thirty days following the issuance of the order except in the case of a summary suspension pursuant to WAC 434-180-255.

(3) If the licensee files an application for an adjudicative hearing, pursuant to WAC 434-180-500, prior to the effective date of revocation or suspension, the suspension or revocation shall not take effect until so ordered by the presiding officer, except in the case of a summary suspension pursuant to WAC 434-180-255.

[Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-250, filed 11/26/97, effective 12/27/97.]

434-180-255
Summary suspension of license.

The secretary may order the summary suspension of a license pending proceedings for revocation or other action, as described in RCW 19.34.100(4). A summary suspension of a license is effective immediately upon issuance.

[Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-255, filed 11/26/97, effective 12/27/97.]

434-180-260
Technical assistance program.

(1) This section describes the secretary's technical assistance program for licensed certification authorities, including recognized repositories. This section implements RCW 43.05.020, by providing for the dissemination of information to licensed certification authorities regarding the requirements of the Washington Electronic Authentication Act and this chapter. It is not intended as a method of providing general business advice to certification authorities, or technical information to the general public, although any member of the public may receive written materials described in this section upon request.

(2) The technical assistance program shall consist of the following:

(a) Technical assistance visits: The secretary, in his or her discretion, may conduct a technical assistance visit, as described by RCW 43.05.030, either by the request or the consent of a licensed certification authority. The secretary is not required to conduct a technical assistance visit.

(b) Printed information: The secretary shall develop, and make available upon request, printed information outlining the requirements of chapter 19.34 RCW and this chapter. This information should not be regarded as a comprehensive guide to conducting business as a certification authority.

(c) Information and assistance by telephone: A licensed certification authority or applicant for licensing or recognition, may contact the secretary's office by telephone during normal business hours at the number listed in WAC 434-180-110. The secretary's office shall provide information regarding the licensing and recognition requirements of chapter 19.34 RCW, and this chapter, but no representation or conclusion offered shall be binding upon the secretary.

(d) Training meetings: The secretary may, in his or her discretion, conduct meetings for the purpose of providing training regarding requirements for licensure or recognition.

(e) List of organizations providing technical assistance: The secretary shall compile, and make available upon request, a list of organizations, including private companies, that provide technical assistance to certification authorities. The secretary shall compile this list from information submitted by the organizations and shall not constitute an endorsement by the secretary of any organization.

(3) If the secretary determines, during or within a reasonable time after a technical assistance visit, that the licensed certification authority has violated any statute or rule, the secretary shall notify the certification authority in writing and specify a reasonable period of time to correct the violation before any civil penalty may be imposed. The notification shall include a copy of the specific statute or rule violated. After the expiration of a reasonable time period conveyed to the certification authority, the secretary may revisit the certification authority and issue civil penalties with regard to any uncorrected violations, for which notice was provided.

[Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-260, filed 11/26/97, effective 12/27/97.]

434-180-265
Civil penalties.

The secretary may, by order, impose and collect a civil monetary penalty against a licensed certification authority for a violation of chapter 19.34 RCW as provided by RCW 19.34.120.

(1) Penalties imposed under this section shall not exceed ten thousand dollars per incident, or ninety percent of the recommended reliance limit of a material certificate, whichever is less. In case of a violation continuing for more than one day, each day is considered a separate incident. In the case of a state agency authorized by law to become a licensed certification authority, the sole penalty imposed pursuant to this section shall consist of specific findings of noncompliance and an order requiring compliance with this chapter and the rules of the secretary. Any penalty imposed pursuant to this chapter and chapter 34.05 RCW shall be enforceable in the superior court.

(2) In assessing penalties under this section, the secretary shall:

(a) Issue to the licensed certification authority a notice of apparent noncompliance, specifying the provisions of statute or rule with which the certification authority is not in compliance and the range of possible sanctions;

(b) Specify a time period of not less than thirty days during which the certification authority may respond in writing to the notice of apparent noncompliance;

(c) If the certification authority does not respond in writing within the specified period, or obtain a written extension of that period, then the secretary may impose an order consistent with the notice, subject to review pursuant to WAC 434-180-500;

(d) If the certification authority does respond in writing:

(i) If the secretary deems the response to satisfactorily demonstrate compliance with the provisions referenced in the notice, then the secretary shall terminate this process without imposing any penalty;

(ii) If the secretary does not deem the response satisfactory, then the secretary may either:

(A) Issue a new or revised notice pursuant to (a) of this subsection; or

(B) Impose an order consistent with the notice, subject to review pursuant to WAC 434-180-500.

[Statutory Authority: Chapter 19.34 RCW. 99-02-048, § 434-180-265, filed 1/4/99, effective 2/4/99. Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-265, filed 11/26/97, effective 12/27/97.]

434-180-270
Criteria for determining penalty amounts.

In determining the appropriate penalty amount against a licensed certification authority for violation of chapter 19.34 RCW or this chapter, the secretary may consider the nature of the violation and the extent or magnitude of the severity of the violation, including:

(1) The damages arising from the violation including:

(a) The financial impact of the violation to any subscriber, relying party, or any other person;

(b) The amount of money obtained, or profit derived, by the certification authority as a result of the violation;

(c) The costs incurred by the state in enforcement, including reasonable investigative costs;

(d) The nonfinancial consequences of the violation, including harm to any subscriber, relying party, or other person;

(2) The nature of the violation, including whether it was continuing in nature, involved criminal conduct, or tended to significantly impair the reliability of any certificate or key pair;

(3) The presence of any aggravating circumstances, including whether the violator:

(a) Intentionally committed the violation with knowledge that the conduct constituted a violation;

(b) Attempted to conceal the violation;

(c) Was untruthful or uncooperative in dealing with the secretary or the secretary's staff;

(d) Had committed prior violations found by the secretary;

(e) Incurred no other sanction as a result of the violation;

(4) The presence of any mitigating circumstances, including whether the violator:

(a) Had taken any prior action to correct the violation or mitigate its consequences;

(b) Had previously paid any damages to any party resulting from the violation;

(c) Acted without intention to commit a violation; or

(d) Acted reasonably in light of any other mitigating factors deemed relevant by the secretary.

[Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-270, filed 11/26/97, effective 12/27/97.]

434-180-275
Recovery against suitable guaranty.

(1) To recover a qualified right to payment against a surety or issuer of a suitable guaranty, pursuant to RCW 34.10.290, the claimant must:

(a) File a signed notice of the claim with the secretary stating the name and address of the claimant, the amount claimed, the grounds for the qualified right to payment, the date of the occurrence of the violation forming the basis of the claim; and

(b) Append to the notice a certified copy of the judgment on which the qualified right to payment is based, except as provided in subsection (2) of this section.

(2) If the notice pursuant to subsection (1)(a) of this section is filed prior to entry of judgment, the secretary shall hold such notice on file, without further action, until the claimant files a copy of the judgment. If the secretary determines that the litigation identified in the notice has been finally resolved without a judgment providing the claimant with a qualified right to payment, the secretary may expunge the notice from his or her records. The secretary shall not expunge a notice until three years have elapsed since it was first filed.

(3) The secretary shall reject a notice for filing if the date of the occurrence of the violation is more than three years prior to the filing of the notice.

(4) If a notice and judgment are filed pursuant to subsection (1) of this section, the secretary shall provide the notice and judgment to the surety or issuer.

[Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-275, filed 11/26/97, effective 12/27/97.]

434-180-300
Form of certificates.

(1) Certificates issued by licensed certification authorities shall follow the Basic Certificate Field Standards specified in standard X.509, part one, section 4.1. Certificate data extension fields are optional. If certificate extension fields are used, usage must conform to the required guidelines referenced in X.509 section 4.1.2.1, section 4.2, and may be displayed on the certificate.

(2) Any certificate issued by a licensed certification authority that is to be used as an acknowledgment, as provided in RCW 19.34.340, shall include a certificate data extension field that specifies the reliance limit, if any, and a certificate data extension field that states that the certificate may be used as an acknowledgment.

[Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-300, filed 11/26/97, effective 12/27/97.]

434-180-310
Recordkeeping and retention.

(1) Every licensed certification authority shall make, keep, and preserve the following records:

(a) Such records as are necessary to demonstrate compliance with RCW 19.34.100 (1)(b), (c), (e), (f), and (g);

(b) Such records as are necessary to demonstrate compliance with RCW 19.34.210 (1)(a), (b), and (2);

(c) All notices of suspension of certificates pursuant to RCW 19.34.210(4), together with such other documents as required to demonstrate compliance with RCW 19.34.210;

(d) Such records as are necessary to demonstrate compliance with RCW 19.34.250(1);

(e) Such records as are necessary to demonstrate compliance with RCW 19.34.260 (1), (2), (3), (4), and (5); and

(f) Such records as are necessary to demonstrate compliance with RCW 19.34.290(1).

(2) Every licensed certification authority shall maintain a data base file which shall contain records of the identity of the subscriber named in each certificate issued by the certification authority, which identity is to include all the facts represented in the certificate, the date of issuance of the certificate, and number of the certificate.

(3) Every licensed certification authority shall maintain a date base file of every time-stamp issued by the certification authority, to include sufficient information so that the identity of the subscriber and the item being time stamped can be identified.

(4) Every licensed certification authority shall retain in a trustworthy fashion the following records for the following periods:

(a) All records identified in subsections (2) and (3) of this section for a period of at least ten years after the date a certificate is revoked or expired, or after a time-stamp is affixed; and

(b) All other records required to be retained under this section shall be retained for at least five years.

(5) Records may be kept in the form of paper-based documents, retrievable computer-based documents, or any form of reproduction approved by the state archivist for essential records pursuant to chapter 40.10 RCW. Such records shall be indexed, stored, preserved and reproduced so as to be accurate, complete, and accessible to an auditor. Certificate extension data, referenced in X.509 section 4.2, is not required to be part of any publicly accessible record.

[Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-310, filed 11/26/97, effective 12/27/97.]

434-180-320
Certification authority disclosure records.

(1) The secretary shall compile and maintain certification authority disclosure records for each certification authority that has been issued a current and valid Washington certification authority license. The secretary shall publish them in the secretary's repository and any other recognized repository the secretary deems appropriate. Each certification authority disclosure record shall include, at a minimum, the following:

(a) The information specified in WAC 434-180-210 (1), (2), (3), and (4);

(b) The name, mailing address, telephone number, and electronic mail address of the issuer or surety of the certification authority's suitable guaranty, and the expiration date of the guaranty;

(c) A copy of the certification practice statement filed with the secretary pursuant to WAC 434-180-330;

(d) A copy of the most recent audit report, or summary thereof, filed with the secretary pursuant to WAC 434-180-240;

(e) Information as to the current status of the certification authority's Washington license, including disclosure of any license revocation or suspension. If a suspension or revocation is currently subject to a pending administrative or judicial review, the record shall so note;

(f) Whether the certification authority operates a recognized repository, and, information sufficient to locate or identify any repository it either operates or utilizes;

(g) A list of all judgments filed with the secretary pursuant to WAC 434-180-275, within the previous five years; and

(h) Any other information specified by statute.

(2) The secretary shall update a certification authority disclosure record upon becoming aware that any item of information contained within it has changed or is not accurate.

(3) In compiling and maintaining certification authority disclosure records, the secretary shall utilize the records of the secretary's office, and is not obligated to conduct any affirmative investigation or review beyond the face of those records.

[Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-320, filed 11/26/97, effective 12/27/97.]

434-180-330
Certification practice statements.

Each licensed certification authority must file with the secretary a certification practice statement. This statement must declare the practices the certification authority uses in issuing, suspending, and revoking certificates. Additionally, it must set forth the following:

(1) If certificates are issued by class, the necessary criteria for each class of certificate, including the methods of subscriber identification applicable to each class;

(2) Disclosure of any warnings, liability limitations, warranty disclaimers, and indemnity and hold harmless provisions, if any, upon which the certification authority intends to rely;

(3) Disclosure of any and all disclaimers and limitations on obligations, losses, or damages, if any, to be asserted by the certification authority;

(4) A written description of all representations required by the certification authority of the subscriber for the subscriber's responsibility to protect the private key; and

(5) Disclosure of any mandatory dispute resolution process, if any, including any choice of forum and choice of law provisions.

[Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-330, filed 11/26/97, effective 12/27/97.]

434-180-340
Suspension or revocation of a certificate by the secretary.

(1) The secretary may order a licensed certification authority to suspend or revoke a certificate that the certification authority issued, if, after giving any required notice and opportunity for the certification authority and the subscriber to be heard in accordance with chapter 34.05 RCW, the secretary determines that:

(a) The certificate was issued without substantial compliance with RCW 19.34.210; and

(b) The noncompliance poses a significant risk to persons reasonably relying on the certificate.

(2) The secretary may issue an order, pursuant to RCW 19.34.210(5), suspending a certificate for a period not to exceed ninety-six hours upon determining that an emergency requires an immediate remedy. The secretary shall issue an order including such a finding, and mail it to the licensed certification authority at the mailing address listed in its application.

(3) The secretary may issue an order, pursuant to RCW 19.34.250(2), suspending a certificate for a period not to exceed ninety-six hours, unless the certificate provides otherwise or the certificate is a transactional certificate, under circumstances described by RCW 19.34.250 (2)(a) and (b). If, upon request by the secretary, the person requesting suspension fails to provide a statement under oath or affirmation regarding his or her identity or authorization to request suspension, the secretary shall not issue an order suspending the certificate unless he or she is satisfied that discretion to enter the order should be exercised because the circumstances provide a sufficient basis for confidence of the person's identity and authority.

[Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-340, filed 11/26/97, effective 12/27/97.]

434-180-350
Regional services for certificate suspension.

The secretary may enter into an agreement, pursuant to RCW 19.35.250(7) and chapter 39.34 RCW, authorizing a state or local agency to perform any of the functions of the secretary under RCW 19.34.250 or WAC 434-180-350 (2) or (3) upon a regional basis. The terms and conditions of such an agreement shall include, at a minimum:

(1) The identity of contracting parties;

(2) The region of the state for which the contract is effective;

(3) The duration of the agreement;

(4) The method by which the contracting agency shall inform the secretary of all actions taken pursuant to the agreement;

(5) The method by which any suspension pursuant to the agreement shall be made effective;

(6) The method by which the secretary shall reimburse the agency for its costs of performance under the agreement;

(7) A provision under which each party agrees to indemnify the other, to the extent permitted by law;

(8) The method by which the contract may be terminated prior to expiration, which shall include the right of either party to terminate the agreement immediately in the event of a loss or withdrawal of funding; and

(9) A method of resolving disputes under the agreement.

[Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-350, filed 11/26/97, effective 12/27/97.]

434-180-360
Trustworthy system.

A system shall be regarded as trustworthy if it materially satisfies the Common Criteria (CC) Protection Profile (PP) for Commercial Security 2 (CS2), (CCPPCS), developed by the National Institute of Standards and Technology (NIST). The determination whether a departure from CCPPCS is material shall be governed by WAC 434-180-240(2). For purposes of this chapter, CCPPCS shall be interpreted in a manner that is reasonable in the context in which a system is used and is consistent with other state and federal laws. Until such time as the referenced standard is adopted by NIST, the standard applicable for purposes of this chapter shall be the draft of CCPPCS dated July 13, 1998.

[Statutory Authority: Chapter 19.34 RCW and 1998 c 33. 99-02-047, § 434-180-360, filed 1/4/99, effective 2/4/99. Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-360, filed 11/26/97, effective 12/27/97.]

434-180-370
Procedure upon discontinuance of business.

A licensed certification authority that discontinues providing certification authority services without making other arrangements for preservation of the certification authority's records shall either:

(1) Revoke all valid certificates and return all records concerning them to the appropriate subscriber; or

(2) Submit such records to another licensed certification authority or authorities designated by the secretary.

[Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-370, filed 11/26/97, effective 12/27/97.]

434-180-400
Recognition of repositories.

The secretary shall recognize a repository upon determining that it satisfies all requirements set forth in RCW 19.34.400, and upon payment of the required fee and upon receipt and review of a completed form, provided by the secretary, containing the following:

(1) The name of the licensed certification authority, or applicant for licensure as a certification authority, requesting recognition of a repository;

(2) The applicant's uniform business identifier number, if any;

(3) The mailing address of the applicant, and a physical address if different;

(4) The telephone number of the applicant;

(5) The electronic mail address of the applicant; and

(6) A description of the data base and system architecture demonstrating that it satisfies the requirements of RCW 19.34.400(1) and WAC 434-180-420.

[Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-400, filed 11/26/97, effective 12/27/97.]

434-180-410
Revocation of recognition of a repository.

(1) This rule describes the secretary's procedure for revoking the recognition of a repository, without also revoking the license of the certification authority that operates the repository. Because a valid license as a certification authority is a statutory requirement for recognition of a repository, the secretary shall automatically revoke the recognition of any repository operated by a certification authority whose license is revoked, expired, or otherwise inoperative.

(2) The secretary may revoke recognition of a repository, pursuant to chapter 34.05 RCW, for failure to comply with any requirement of RCW 19.34.400 or this chapter, or for failure to comply with a lawful order of the secretary.

(3) The secretary shall inform a licensed certification authority that operates a recognized repository by written order, by mail directed to the mailing address listed on the licensee's application, of a decision to revoke recognition of the repository. The notification shall state when the revocation shall be effective, which shall not be less than thirty days following the issuance of the order.

(4) If the certification authority files an application for an adjudicative hearing, pursuant to WAC 434-180-500, prior to the effective date of revocation, the revocation shall not take effect until so ordered by the presiding officer.

[Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-410, filed 11/26/97, effective 12/27/97.]

434-180-420
Trustworthy system for recognized repositories.

A system shall be regarded as trustworthy for purposes of operating a recognized repository if it satisfies the requirements of WAC 434-180-360, and additionally it:

(1) Provides on-line access to the repository upon a continuous basis, with reasonable allowance for scheduled maintenance;

(2) Possesses the capacity to process transactions in a manner reasonably adequate for anticipated volume; and

(3) Provides for the periodic storage of data at a location other than the principal system utilized for the repository.

[Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-420, filed 11/26/97, effective 12/27/97.]

434-180-430
Contract for secretary of state repository publication.

The secretary may either directly operate, or contract for the operation of, a repository described in WAC 434-180-440. If the secretary contracts for the operation of the repository, with other than DIS, the contractor must be a licensed certification authority and must agree to operate the repository according to all requirements of chapter 19.34 RCW, including RCW 19.34.400. The contract may be rescinded for any reason that would form a basis for revoking recognition of a repository or for failure to meet the requirements of WAC 434-180-440.

[Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-430, filed 11/26/97, effective 12/27/97.]

434-180-440
Publication by the secretary of state.

(1) The secretary shall publish, either directly or under contract, any information required by chapter 19.34 RCW. Information published by the secretary shall include:

(a) The certification authority disclosure record for each certification authority licensed in Washington;

(b) A list of all judgments filed with the secretary within the previous five years pursuant to RCW 19.34.290;

(c) Any advisory statements published by the secretary regarding the activities of a licensed or unlicensed certification authority, together with any protest filed by the certification authority named in the statement and any final decision of the secretary regarding the issues raised in the statement, all as provided by RCW 19.34.130(2);

(d) Any information published by the secretary pursuant to WAC 434-180-450; and

(e) Any other information necessary or appropriate for publication pursuant to chapter 19.34 RCW or this chapter.

(2) The secretary may meet the requirements of this section through publication in the *State Register*, on the web site maintained by the secretary, or through any other medium suitable to providing public notice.

[Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111, and 19.34.400. 00-22-041, § 434-180-440, filed 10/25/00, effective 11/25/00; 97-24-053, § 434-180-440, filed 11/26/97, effective 12/27/97.]

434-180-450
Procedure upon discontinuance of business as repository.

A licensed certification authority that discontinues providing services as a recognized repository shall republish the records published in the repository in another recognized repository. If no other repository is available or willing to republish that information, the certification authority shall publish it in the secretary's repository.

[Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-450, filed 11/26/97, effective 12/27/97.]

434-180-500
Application for adjudicative proceedings.

Decisions and actions of the secretary pursuant to chapter 19.34 RCW and this chapter may be reviewed by filing an application of an adjudicative proceeding. An adjudicative proceeding shall be commenced when required by chapter 34.05 RCW, and may be commenced in the secretary's discretion upon such other occasions as may be permitted by statute. An application for an adjudicative proceeding may be on a form provided by the secretary for that purpose or in another paper or electronic writing signed by the applicant or the applicant's representative. The application for an adjudicative proceeding should specify the issue to be adjudicated in the proceeding.

[Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-500, filed 11/26/97, effective 12/27/97.]

434-180-510
Appointment of administrative law judge — Designation of procedural rules.

(1) The secretary hereby appoints the office of administrative hearings and the administrative law judges employed by that office to preside at all hearings that result from the commencement of adjudicative proceedings unless the secretary, by his or her own order, declares his or her intent to preside at a specific proceeding or the proceeding is an appeal of an initial order issued by an administrative law judge.

(2) All hearings shall be conducted in compliance with these rules, and with chapter 34.05 RCW. The secretary adopts chapter 10-08 WAC as the applicable rules of procedure, except where this chapter provides different, additional or conflicting procedures.

[Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-510, filed 11/26/97, effective 12/27/97.]

434-180-520
Pleadings in digital form.

(1) Unless the presiding officer directs otherwise, any party may file any pleading or other document in an adjudicative proceeding under this chapter in electronic form. If a pleading or document filed electronically requires a signature, that pleading or document shall be signed digitally, pursuant to a valid certificate issued by a licensed certification authority. The certification authority that issued the certificate shall not be a party to the adjudicative proceeding.

(2) Service of electronic pleadings or documents by electronic transmission is effective upon receipt, except that if sent after 5:00 p.m. on a business day or at any time on a weekend or state holiday, service is effective as of 8:00 a.m. on the following business day.

[Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-520, filed 11/26/97, effective 12/27/97.]

434-180-530
Service of process on the secretary.

Service of pleadings or documents upon the secretary or the presiding officer does not constitute service upon the attorney general as counsel to the secretary.

[Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-530, filed 11/26/97, effective 12/27/97.]

434-180-540
Stay of summary suspension.

(1) Upon summary suspension of a license by the secretary pursuant to this chapter and chapter 19.34 RCW, an affected certification authority may petition the secretary for a stay of suspension pursuant to RCW 34.05.467 and 34.05.550(1). Such petition must be received by the secretary within the time specified in RCW 34.05.467.

(2) Within seven days of receipt of a petition for stay, a hearing shall be held before an administrative law judge, or if an administrative law judge is not available during this period, before an individual designated by the secretary. The hearing shall be limited to consideration of whether a stay should be granted, or whether the terms of the suspension may be modified to

allow the conduct of limited activities under current licenses.

(3) Any hearing conducted pursuant to subsection (2) of this section shall be conducted under RCW 34.05.485, brief adjudicative proceedings. The agency record for the hearing shall consist of the information upon which the summary suspension was based and may be supplemented by any information obtained by the secretary subsequent to the date of the suspension order. The certification authority shall have the burden of demonstrating by a preponderance of the evidence that:

(a) The certification authority is likely to prevail upon the merits at hearing;

(b) Without relief, the certification authority will suffer irreparable injury. For purposes of this section, elimination of income from licensed activities shall not be deemed irreparable injury;

(c) The grant of relief will not substantially harm other

parties to the proceedings; and

(d) The threat to the public safety or welfare is not sufficiently serious to justify continuation of the suspension, or that modification of the terms of the suspension will adequately protect the public interest.

(4) The initial order granting or denying a stay shall be effective immediately upon service unless another date is specified in the order.

[Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-540, filed 11/26/97, effective 12/27/97.]

434-180-550
Review of orders regarding stay.

(1) Any party may petition the secretary for review of an initial order granting or denying a motion for a stay of suspension. A petition for review must be in writing and received by the secretary within twenty-one days of service of the initial order. If neither party has requested review within twenty-one days of service, the initial order shall be deemed the final order of the secretary for purposes of RCW 34.05.467.

(2) If the secretary receives a timely petition for review, he or she shall consider the petition promptly. Consideration on review shall be limited to the record of the hearing on stay.

(3) The secretary's order on the petition for review shall be effective upon service unless another date is specified in the order and is final pursuant to RCW 34.05.467. Final disposition of the petition for stay shall not affect subsequent administrative proceedings for suspension or revocation of a license.

[Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-550, filed 11/26/97, effective 12/27/97.]

434-180-560
Adjudicative proceedings — Appearance and practice before the secretary — Who may appear.

No person may appear in a representative capacity before the secretary or the designated administrative law judge other than the following:

(1) Attorneys at law duly qualified and entitled to practice before the supreme court of the state of Washington.

(2) A bona fide officer, authorized manager, partner, or full-time employee of a firm, association, partnership, LLC, or corporation who appears for such firm, association, partnership, corporation, or company.

(3) An individual appearing pro se.

(4) Such interpreters for persons with a limited understanding of the English language or hearing impaired persons as provided for in WAC 10-08-150.

(5) Such other persons as may be permitted by the secretary upon a showing by a party to the hearing of such a necessity or such a hardship as would make it unduly burdensome upon him to have a representative as set forth under subsections (1) and (2) of this section.

[Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-560, filed 11/26/97, effective 12/27/97.]

434-180-590
Brief adjudicative proceeding regarding certificate suspension.

(1) Pursuant to RCW 34.05.482, the secretary may use brief adjudicative proceedings where not violative of law, where in the judgment of the secretary protection of the public interest does not require the secretary to give notice and an opportunity to participate to persons other than the parties, and the issue and interests involved in the controversy do not warrant the use of the procedures of RCW 34.05.413 through 34.05.479.

(2) The secretary finds that prompt review of the suspension of a certificate pursuant to RCW 19.34.210(5), 19.34.250(2), or WAC 434-180-350 by the secretary or a state or local agency under contract with the secretary is appropriate for a brief adjudicative proceeding. The secretary adopts the provisions of RCW 34.05.482 through 34.05.494 for purposes of this category of proceedings.

(3) If any person affected by the suspension requests administrative review, the secretary shall immediately notify, by the most rapid means reasonably calculated to inform the recipient of the proceeding, the subscriber, the certification authority, and any other affected party who has requested notification or has requested the review, of the intent to conduct a proceeding pursuant to this section. Conduct of that review shall be in accordance with RCW 34.05.485 through 34.05.494.

(4) The suspension of a certificate by order of the secretary pursuant to RCW 19.34.210(5) and 19.34.250(2) shall lapse ninety-six hours after the suspension.

(5) The secretary may, in his or her discretion, conduct a full adjudicative proceeding if any affected party requests a full review of the suspension of a certificate pursuant to RCW 19.34.250(2). If a full adjudicative proceeding is held, the suspension lapses ninety-six hours after the suspension, but the review need not be completed within that time.

(6) If, by final order, the secretary determines that the suspension was in error, the certificate shall be deemed valid retroactively to the time of suspension.

[Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-590, filed 11/26/97, effective 12/27/97.]

CPS Updates

Quote 19.34.503 in Coice of laws subsection

In overview, mention that it was developed for use in an application to be filed ~~issued~~ with the Secretary of state

Current version
Located at URI
Above

CPS

From Wiki

Contents

Collier Technologies LLC CPS

Overview

This document will fill the role of Certification Practices Statement as described in 434-180-330 WAC once the CA is fully licensed by the state.

http://apps.leg.wa.gov/WAC/default.aspx?cite=434-180-330

This document may change without notice. Historical versions will be made available here:

git://git.colliertech.org/colliertech/state.git (http://git.colliertech.org/?p=state.git;a=blob;f=cps.txt)

Operative Personnel Responsibilities

Notary Public prerequisite

All Operative Personnel employed by Collier Technologies LLC, known here as the Certification Authority or CA, must also be licensed as notaries public by the local government where they reside during any act performed on behalf of the CA.

Demonstration of Proficiency

In addition to passing the Washington State Operative Personnel Exam, all OPs employed by the CA will demonstrate their proficiency by

```
a) creating a request for issuance as described in 19.34.210(1)
   RCW, known here as a Certificate Signing Request or CSR; and
b) signing CSR from (a) with a private key issued by the
   Certification Authority; and
c) publishing the public key corresponding to the CSR signed in
   (b) in a recognized repository as defined by 19.34.400 RCW
```

Use of private key

While holding the position of Operative Personnel for the CA, the OP will

```
a) utilize the private key corresponding to the CSR presented
   during the demonstration of proficiency exclusively for duties
   performed on behalf of the CA
b) not use the private key referenced in (a) for purposes other
   than those performed on behalf of the CA.
```

In the case that Operative Personnel contract or employment is terminated, certificates issued to Operative Personnel by the CA will be revoked starting midnight of the date of termination of contract or employment.

Private key data maintenance

Physical Storage

All private key data controlled by the CA and all Operative Personnel must be

```
a) stored on a solid-state device; and
b) kept within a locked safe except while
i) in use by OP acting on behalf of the CA; or
ii) being reviewed by auditors or customs personnel
```

Trustworthy system

All solid-state devices containing private key data controlled by the CA and all Operative Personnel may only be used

```
a) on a Trustworthy system, as defined in 19.34.020(43) RCW; and
b) with a system which remains always disconnected from any
   computer network
```

Dispute Resolution

- Choice of forum: San Juan County quote 19.34.503 RCW
- Choice of law: Revised Code of Washington 434-180-510 WAC

Certificate Classes

Trust Levels

Automated

The 'Automated' class of certificate requires minimal identity verification. The verification is performed by computer software which is maintained by operative personnel and includes a "Centi" reliance limit.

Core

The 'Core' class of certificate requires minimal identity verification. The verification is performed by operative personnel and includes a "Deci" recommended reliance limit.

Basic

The 'Basic' class of certificate requires identity verification through a trusted third party. Acceptable methods of identity verification include

- Bi-directional PGP trust paths of distance 3 or less with the CA's official PGP signing key
- A certificate published in a recognized repository along with proof of ownership of associated private key
- A driver's license or passport issued by an agent of the subject's local governmental authority
- A verification upon oath or affirmation as defined in 42.44.010(5) RCW which
  - identifies the affiant with a 300dpi or greater copy of one or more governmentally issued identification documents; and which
  - is signed and sealed by a public official licensed to perform notarial acts

Extended

Business

Enterprise

Requires of the subject the same identity verification and background checks as are required by the Secretary of State of Certification Authority Operative Personnel, described in 434-180-215 WAC

Recommended Reliance Limits

Centi

The minimal reliance limit. This is the reliance limit which will be assumed, should none be otherwise specified.

USD $0.01

Deci

This is the minimum reliance limit which will be assumed on all certificates created using manual intervention by operative personnel.

USD $0.10

Deca

USD $10.00

Hecto

USD $100.00

Kilo

USD $1,000.00

Mega

USD $10,000.00

Publication In Repository

after issuance, all certificates must be published in a recognized repository in addition to the repository ~~hosted~~ operated by Collier Technologies LLC

Retrieved from "http://wiki.loc.colliertech.org/index.php/CPS"

- This page was last modified on 1 August 2010, at 01:28. (UTC)

State of Washington

County of San Juan

Signed and sworn to (or affirmed) before me on __________/__________/__________
YYYY / Month / Day

by ______________________________.

____
(Signature)

____
Title

My appointment expires ______________________________

Text from Section 42.44.100 RCW

STATE OF WASHINGTON
SECRETARY OF STATE

ELECTRONIC AUTHENTICATION OPERATIVE PERSONNEL EXAM

INSTRUCTIONS

Please circle the correct answer in ink pen. Multiple answers will result in the question being marked as having been answered incorrectly. Select the best answer from the options given.

You must correctly answer at least 30 questions to pass.

The exam is open-book, and there is no time limit, but you may only take this exam one time within any thirty-day period. Any written materials may be referred to except for the operative personnel exam answer keys, whether the key has been prepared by this office or not. **You may not discuss this exam, the questions or your answers with any other person until you have submitted the test for grading**. Please return the test to:

OFFICE OF THE SECRETARY OF STATE
DIGITAL SIGNATURE PROGRAM
505 E. UNION
PO BOX 40234
OLYMPIA, WA 98504-0234

Be sure to include the examination grading fee of $50.00. Checks should be made payable to "Secretary of State."

Enter your name, address and telephone number in the space provided below:

First Carl Middle James Last Adams-Coller

Mailing Address 85 Raccoon Point Road

City Eastsound State or Country WA or San Juan

Zip or Postal Code 98245

Telephone Number (206) 226-5809

Test results will be mailed to the address listed above, and a copy of the exam results must be included in the Application for Certification as Digital Signature Operative Personnel.

✓

ELECTRONIC AUTHENTICATION
OPERATIVE PERSONNEL EXAM

1. Which of the following is not a stated purpose of the Washington Electronic Authentication Act?

10.1 → A. Facilitate commerce by means of reliable electronic messages.

[✓ B.] Promote access and communication between the public and government agencies.

10.5 → C. Minimize the incidence of forged or fraudulent digital signatures.

10.7 → D. Establish, in coordination with multiple states, uniform rules regarding the authentication and reliability of electronic messages.

2. Which of the following is <u>not</u> required by a certification authority to be licensed by the Washington Secretary of State?

200.1 [✓ A.] The certification authority's principal place of business must be located in the State of Washington.

100.1(d) → B. The certification authority must use a "trustworthy system" as defined under the Washington Electronic Authentication Act.

434-180-200 → C. The certification authority must be the subscriber of a certificate published in a recognized repository.

200.3
100.1(b) → D. The certification authority must employ individuals who have not been convicted of a crime involving fraud or dishonesty.

3. Which of the following statements is true?

A. A licensed certification authority may assign any individual to perform the functions of operative personnel, even if that individual has not been certified, for a reasonable period of time during the certification process so long as an application has been filed with the Washington Secretary of State.

B. A licensed certification authority may not assign any individual to perform the functions of operative personnel until it has notified the Washington Secretary of State of its intent to do so, and received the approval of the Washington Secretary of State, or at the time of licensing renewal.

100.1(b) [✓ C.] A licensed certification authority may not assign any individual to perform the functions of operative personnel if that individual has not been certified by the Washington Secretary of State.

D. None of the above.

4. If a licensed certification authority fails to comply with the Washington Electronic Authentication Act, the Act gives the Washington Secretary of State the authority to:

100.4 → [✓ A.] Revoke or suspend a certification authority's license.

B. Publish information about the violation in any newspaper.

C. Revoke the certification authority's business license.

D. Bring an action against the certification authority for violation of the Consumer Protection Act.

✓

5. If a certification authority fails to obtain a license from the Washington Secretary of State's office, the Washington Electronic Authentication Act provides that:

A. The certification authority may not issue certificates in the State of Washington.
B. The certification authority may not conduct any business in the State of Washington.
C. The certification authority will be liable for any loss caused by reliance on a certificate issued by such certification authority.
40.6 [✓ D.] The Washington Electronic Authentication Act does not apply to such certification authority, except as specifically provided.

6. The Washington Secretary of State may order the summary suspension of a certification authority license if the Washington Secretary of State includes within a written order a finding that the certification authority has:

A. Utilized its license in the commission of a violation of a state or federal criminal statute or of chapter 19.86 RCW.
40.4(b) [✓ B.] Engaged in conduct giving rise to a serious risk of loss to public or private parties if the license is not immediately suspended.
(5.5) [✓ C.] Either one of the above.
D. None of the above.

7. Which of the following is <u>not</u> required before a licensed certification authority may discontinue its services?

291.1(b) → A. The licensed certification authority must minimize to the extent commercially reasonable any disruption to the subscribers of valid certificates and relying parties.
[✓ B.] The licensed certification authority must sell all of its business to another licensed certification authority.
291.1(a) → C. The licensed certification authority must notify all subscribers listed on valid certificates listed by the certification authority.
291.1(c) → D. The licensed certification authority must make reasonable arrangements for preservation of the certification authority's records

8. Which of the following is <u>not</u> required before a licensed certification authority may issue a certificate to a subscriber?

210.1(a) → A. The certification authority has received a signed request by a prospective subscriber.
1(b)i → B. The certification authority has confirmed that the subscriber is the person to be listed in the certificate.
1(b)vii → C. The certificate provides information sufficient to locate the repositories in which notification of the revocation or suspension of the certificate would be listed.
[✓ D.] The certification authority has issued a password for the subscriber's private key.

9. In which of the following circumstances is a licensed certification authority <u>not</u> required to immediately revoke a certificate?

[✓ A.] The certification authority has decided to discontinue its business.
210.6 → B. The certification authority determines that the certificate was not issued as required by the Washington Electronic Authentication Act.
260.3(a) → C. The certification authority receives a certified copy of the subscriber's death certificate.
(b) → D. The subscriber is a corporation that has been dissolved.

✓

19.34.210 1.c
1.b.iv)

10. If the certification practice statement of a licensed certification authority provides that the certification authority does not verify that the private key held by the subscriber corresponds to the public key listed in the subscriber's certificate, that certificate is:

A. Valid under the Washington Electronic Authentication Act.
[✓ B.] Not valid under the Washington Electronic Authentication Act.
C. Valid under the Washington Electronic Authentication Act only if it includes the disclaimer. 1.C - Can not be disclaimed
D. None of the above.

11. After a subscriber accepts a certificate from a licensed certification authority, the licensed certification authority must: 19.34.220 19.34.210.4

Best answer from options given

A. Give to the subscriber the public and private keys, and password necessary to create a digital signature.
B. Must send information regarding the certificate to the Washington Office of the Secretary of State.
C. Must publish the certificate in a licensed or unlicensed repository.
[✓ D.] 4 Must publish a signed copy of the certificate in a recognized repository.

12. If the Washington Secretary of State decides to publish in a repository a statement regarding a licensed or unlicensed certification authority advising subscribers and relying parties about potential risks created by such certification authority: 19.34.130.2

A. The Secretary of State must first hold a hearing before publishing a statement.
B. The certification authority named in the statement may file a written defense of 1,000 words or less responding to the Washington Secretary of State.
[✓ C.] The certification authority named in the statement may file a written defense of 10,000 bytes or less.
D. The certification authority named in the statement may not file a statement in defense.

13. Under the Washington Electronic Authentication Act, a licensed certification authority, when issuing ~~using~~ a certificate, is not required to give which of the following warranties? 19.34.220

[✓ A.] The certificate is valid in all states which recognize digital signatures.
1.a B. The certificate contains no information known to the certification authority to be false.
1.b C. The certificate satisfies all material requirements of the Washington Electronic Authentication Act.
1.c D. The certification authority does not exceed any limits of its license in issuing the certificate.

14. Under the Washington Electronic Authentication Act, a licensed certification authority, upon issuance of a certificate, agrees to do which of the following: 19.34.220

A. Obtain cross-certification from other states authorizing the use of digital signatures.
B. Notify the subscriber of any changes in the Washington Electronic Authentication Act.
2.a [✓ C.] To act promptly to suspend or revoke a certificate in accordance with the Washington Electronic Authentication Act.
D. Monitor all signatures by the subscriber to make sure that the subscriber's private key has not been compromised.

PTR Record update CR 210 669 718

15. Under the Washington Electronic Authentication Act, a licensed certification authority, upon issuing a certificate to a subscriber, is <u>not</u> required to certify which of the following to parties who rely on such certificate: 19.34.220

[✓ A.] The subscriber, at the time of use, has control of his or her private key.

3.a 1.a B. The information in the certificate and listed as confirmed by the certification authority is accurate.

3.b C. All information foreseeable material to the reliability of the certificate is stated or incorporated by reference within the certificate.

3.c D. The subscriber has accepted the certificate.

16. If a potential subscriber (seeking a certificate from a licensed certification authority) states that it is an agent on behalf of another person or entity, the licensed certification authority may issue a certificate to such agent only if: 19.34.210.1

b.ii → A. The subscriber duly authorized the agent to have custody of the subscriber's private key.

b.ii → B. The subscriber duly authorized the agent to request issuance of a certificate listing the corresponding public key.

b.ii → [✓ C.] Only if A <u>and</u> B are satisfied.

D. None of the above, because an agent may not obtain a certificate on behalf of a principal.

19.34.240

17. If a subscriber publishes information about the subscriber's private key on a publicly assessable Web page, the Electronic Authentication Act and relevant administrative rules state that the subscriber may be found to be:

(5.5) [✓ A.] Liable for any losses incurred as a result of disclosure of information about the private key.

~~B.~~ ? Only liable if a court of law determines that the subscriber intentionally published information about the private key. (must specify in CPS)

C. Not liable from any loss relating to the disclosure of information about the private key in excess of $50.

[✓ D.] Not liable for any loss caused by disclosure of information about the private key.

18. Which of the following best describes the NIST CS-2 Protection Profile?

~~A.~~ A description of parameters available in defining a certificate profile.

~~B.~~ A generalized certificate structure.

[✓ C.] ✱ A baseline set of security functions and assurances.

~~D.~~ A set of uniform rules regarding the authenticity and reliability of electronic messages.

19. Immediately upon suspension of a certificate by a licensed certification authority, the licensed certification authority must:

A. Notify the Secretary of State.

B. Notify all relying parties.

[✓ C.] ? Give notice of the suspension according to the specifications in the certificate.

D. All of the above.

20. If a licensed certification authority commits a violation of chapter 19.34 RCW, which of the following actions may the Secretary take: 19.34.120, 434-180-265

A. Order the licensed certification authority to stop doing business in the State of Washington.

19.34.120 (3) → [✓ B.] Order that a civil penalty be imposed against the licensed certification authority.

C. Refuse to allow the licensed certification authority to apply for recognition of their repository. ~~434-180-340~~

D. None of the above.

21. If, upon suspension of a certificate by a licensed certification authority, the repository listed in the certificate no longer exists or refuses to accept publication of the suspension, the certification authority must: ~~19.34.120~~ 19.34.~~210~~ 4?? 434-180-400 19.34.240.4 450

A. Give notice of the suspension to the Secretary of State.

B. Give notice to the Secretary of State that repository no longer exists or refuses to accept publication.

C. ? Publish a notice of the suspension of the certificate in any recognized repository.

[✓ D.] ? None of the above. Can be overridden in CPS

22. Which of the following must be included in a certificate issued by a licensed certification authority?

A. Information sufficient to locate or identify one or more repositories in which notification of the revocation or suspension of the certificate will be listed if the certificate is suspended or revoked.

[✓ B.] The date on which the certificate expires. X.509 3.1

C. ? Both A and B.

~~D.~~ None of the above.

23. The NIST CS-2 Protection Profile makes a series of secure usage assumptions. These assumptions include:

A. That at least some of the system components are physically protected.

B. That authorized users will be able to connect to the system remotely over an unprotected network.

C. ? Both of the above.

[✓ D.] None of the above.

24. Which of the following is a true statement?

A. The licensed certification authority must confirm a request for revocation and revoke a certificate within four (4) hours after receiving a subscriber's written request.

B. A licensed certification authority must confirm a request for revocation and revoke a certificate within four (4) hours after receiving both a subscriber's written request and evidence reasonably sufficient to confirm the identity and agency of the person requesting the revocation.

C. A licensed certification authority must confirm a request for revocation and revoke a certificate within one (1) business day after receiving a subscriber's written request for revocation.

19.34.260.b [✓ D.] A licensed certification authority must confirm a request for revocation and revoke a certificate within one (1) business day after receiving both a subscriber's written request and evidence reasonably sufficient to confirm the identity and any agency of the person requesting the revocation.

19.34.280

25. What is the recommended reliance limit in a certificate?

A. The cumulative amount of transactions for which the subscriber may use the digital signature associated with the certificate.
B. The amount above which a transaction involving the digital signature is not valid.
2.a,b [✓ C.] The amount above which a licensed certification authority is not liable for a loss caused by reliance on a false or forged signature of the subscriber.
D. All of the above.

26. When a licensed certification authority conducts its operations within the terms of the Washington Electronic Authentication Act, that licensed certification authority is not liable for which of the following types of damages?

2.c.i A. Punitive damages.
B. Exemplary damages.
2.c.ii C. Damages for pain and suffering.
[✓ D.] All of the above.

27. Which of the following is not a security objective of the NIST CS-2 standards?

A. The system must ensure that all system users can subsequently be held accountable for actions which may impact upon the security of the system.
B. The system must provide a reasonable means for the acceptance of messages validated by a digital signature.
C. The system or its operators must provide a procedure for recovery in the event of a system failure or discontinuity of service.
[✓ D.] ? The system must limit user access to only those system resources for which the user has been granted access.

28. What is the effect of a valid digital signature under the Washington Electronic Authentication Act?
19.34.300

A. The digital signature is valid so long as the certificate corresponding to the digital signature has not expired.
1.a. [✓ B.] The digital signature satisfies any rule of law requiring a signature.
C. The digital signature is only valid if the contract is governed by Washington law.
D. None of the above.

29. If a subscriber, in the process of applying for a certificate from a licensed certification authority, instructs the certification authority in writing that he or she wishes to waive the requirement that the certification authority confirm that the private key held by the subscriber is capable of creating a digital signature, the licensed certification authority:
19.34.210 1.b. iv,v

A. May issue a certificate to such subscriber under those conditions.
[✓ B.] May not issue a certificate to such subscriber under those conditions.
C. May issue a certificate to such subscriber but only if the certificate includes information that the subscriber has waived the foregoing requirement.
D. None of the above.

30. A digital signature satisfies a rule of law requiring a signature if:
19.34.300

1.a A. The digital signature is verified by reference to the public key listed in a valid certificate issued by a licensed certification authority.
1.b B. The digital signature was affixed by the signer with the intention of signing the message.
1.c C. The recipient has no knowledge or notice that the signer either breached a duty as a subscriber or does not rightfully hold the private key used to affix the digital signature.
[✓ D.] All of the above are satisfied.

31. In which ways may recognition of a repository be discontinued?

19.34.400.3

A. Upon thirty (30) days written notice to the Secretary of State by the recognized repository.

B. The Secretary of State discontinues recognition of a repository in accordance with the Administrative Procedure~~s~~ Act.

[✓ C.] Either A or B.

D. None of the above.

32. Which of the following statements regarding the NIST CS-2 protection profile is <u>false</u>?

A. Systems that meet the CS-2 protection standards are not necessarily designed to enforce controls on the flow of information between objects at differing levels of information sensitivity.

B. In commercial environments, CS-2 compliant systems are considered to be suitable to protect information such that only designated groups of users may access the information.

C. CS-2 compliant systems are considered to be suitable to protect sensitive-but-unclassified information in government environments.

[✓ D.] ? None of the above.

33. When <u>must</u> a licensed certification authority revoke a certificate that it issued?

19.34.260

A. After receiving a request for revocation by the subscriber named in the certificate.

B. After receiving a request for revocation by the subscriber of any transactional certificate.

4.a → [✓ C.] After receiving a request for revocation by the subscriber named in the certificate and the licensed certification authority has confirmed that the person requesting revocation is the subscriber, or is an agent of the subscriber with authority to request revocation.

D. None of the above.

34. Which of the following types of records is a licensed certification authority required to preserve?

434-180-310 WAC

[✓ A.] Notices of suspension of certificates.

B. A database file containing records of the identity of every subscriber named in each certificate issued by the certification authority.

C. A database file of every time-stamp issued by the certification authority.

D. All of the above.

35. What is the purpose of the "Key Usage" extension as described in X.509?

X.509
4.2.1.3

A. Allows the certificate issuer to specify a different validity period for the private key than the certificate.

[✓ B.] Defines the purpose of the key contained in the certificate.

C. It contains a sequence of one or more policy information terms, each of which consists of an object identifier (OID) and optional qualifiers.

D. None of the above.

36. The published certification practice statement of a licensed certification authority is <u>not</u> required to contain which of the following?

434-180-330

[✓ A.] The price the certification authority is charging for each certificate in a given class.

2 → B. Any warnings, liability limitations or warranty disclaimers upon which the certification authority intends to rely.

5 → C. A disclosure of any mandatory dispute resolution process, if required by the certification authority.

1 → D. The methods of subscriber identification applicable to any class of certificate issued.

✓

37. A licensed certification authority's system is regarded as trustworthy where it:

434-180-360, 434-180-240

434-180-240 → A. Has been audited by a certified public accountant who is generally familiar with information technology systems.

434-180-360✓ B. Materially satisfies the common criteria protection profile for commercial security 2, as published by the National Institute of Standards and Technology.

[✓ C.] Both of the above.

D. None of the above.

38. What is one of the defined purposes of certificate extensions?

X.509 4.2

A. Allow for the general use of digital signatures over unprotected networks.

B. Provide unique identifiers to prevent the reuse of subject names over time.

[✓ C.] ? Provide methods for associating additional attributes with users or public keys.

D. None of the above.

39. The Authority Information Access extension in a certificate indicates:

X.509 4.2.2.1

A. The class of persons who are authorized to view the information contained in a certificate.

[✓ B.] How to access certification authority information and services for the issuer of the certificate in which the extension appears.

C. The object identifier which can be used to obtain a description of the certification authorities that have issued certificates superior in the public key infrastructure hierarchy to the certification authority that issued the certificate containing the extension.

D. None of the above.

40. In addition to the requirements of WAC 434-180-360, in order to be considered a trustworthy system a recognized repository must also: 434-180-420

(2) → A. Possess the capacity to process transactions in a manner reasonably adequate for anticipated volume.

(3) → B. Provide for the periodic storage of back-up data at a location other than that which houses the principal system utilized for the repository.

[✓ C.] Both of the above.

D. None of the above.

AFFIRMATION

I certify under penalty of perjury under the laws of the State of Washington that I have personally completed the foregoing examination, that I have not taken an examination for certification as operative personnel pursuant to Washington law within the past thirty days, and that the foregoing is true and correct.

Signature *Printed Name* *Date & Place*

See also
IETF RFC 4523

```
   ( 1.3.6.1.4.1.10126.1.5.3.2
        NAME 'x509serialNumber'
        DESC 'Unique integer for each certificate issued by a
              particular CA'
        EQUALITY integerMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 )
```

4.1.3 Signature algorithm

OID identifying the algorithm used by the CA in signing the certificate (see X.509(2000) 7, RFC3280 4.1.2.3) or the CRL.

```
   ( 1.3.6.1.4.1.10126.1.5.3.3
        NAME 'x509signatureAlgorithm'
        DESC 'OID of the algorithm used by the CA in
              signing the CRL or the certificate'
        EQUALITY objectIdentifierMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.38
        SINGLE-VALUE )
```

4.1.4 Issuer

String representation of the issuer's distinguished name (see X.509(2000) 7, RFC3280 4.1.2.4)

```
   ( 1.3.6.1.4.1.10126.1.5.3.4
        NAME 'x509issuer'
        DESC 'Distinguished name of the entity who has signed and
              issued the certificate'
        EQUALITY distinguishedNameMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
        SINGLE-VALUE )
```

Values of this attribute type must be encoded according to the syntax given in [RFC2253].

4.1.5 Validity

The "validity" attribute in an X.509 certificate (see X.509(2000) 7, RFC3280 4.1.2.5) consists of an ASN.1 sequence of two timestamps which define the begin and end of the certificate's validity period. This sequence has been split up into two separate attributes "x509validityNotBefore" and "x509validityNotAfter". The times are represented in string form as defined in [RFC2252].

```
( 1.3.6.1.4.1.10126.1.5.3.5
     NAME 'x509validityNotBefore'
     DESC 'Date on which the certificate validity period begins'
     EQUALITY generalizedTimeMatch
     ORDERING generalizedTimeOrderingMatch
     SYNTAX 1.3.6.1.4.1.1466.115.121.1.24
     SINGLE-VALUE )


( 1.3.6.1.4.1.10126.1.5.3.6
     NAME 'x509validityNotAfter'
     DESC 'Date on which the certificate validity period ends'
     EQUALITY generalizedTimeMatch
     ORDERING generalizedTimeOrderingMatch
     SYNTAX 1.3.6.1.4.1.1466.115.121.1.24
     SINGLE-VALUE )
```

Note that the field in the certificate may be in UTC or GeneralizedTime format. If in UTC format, the creator of this attribute MUST convert the UTC time into GeneralisedTime format when creating the attribute value.

4.1.6 Subject

String representation of the subject's distinguished name (see X.509(2000) 7, RFC3280 4.1.2.6).

```
( 1.3.6.1.4.1.10126.1.5.3.7
     NAME 'x509subject'
     DESC 'Distinguished name of the entity associated with this
           public-key'
     EQUALITY distinguishedNameMatch
     SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
     SINGLE-VALUE )
```

Values of this attribute type must be encoded according to the syntax given in [RFC2253].

4.1.7 Subject public key info algorithm

OID identifying the algorithm associated with the certified public key (see X.509(2000) 7, RFC3280 4.1.2.7).

```
   ( 1.3.6.1.4.1.10126.1.5.3.8
        NAME 'x509subjectPublicKeyInfoAlgorithm'
        DESC 'OID identifying the algorithm associated with the certified
              public key'
        EQUALITY objectIdentifierMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.38
        SINGLE-VALUE )
```

4.2 Attributes for selected extensions

As this specification intends to only facilitate applications in finding certificates, only those extensions have to be defined that might be searched for. Thus extensions described in [RFC3280] like the following are not dealt with here:

- o private key usage period extension
- o policy mappings extension
- o subject directory attributes extension
- o basic constraints extension
- o name constraints extensions
- o policy constraints extensions
- o inhibit any policy extension
- o freshest CRL extension
- o authority information access extension
- o subject information access extension

4.2.1 Authority key identifier extension

This attribute identifies the public key to be used to verify the signature on this certificate or CRL (see X.509(2000) 8.2.2.1, RFC3280 4.2.1.1). The key may be identified by an explicit key identifier in the keyIdentifier component, by identification of a certificate for the key (giving certificate issuer in the authorityCertIssuer component and certificate serial number in the authorityCertSerialNumber component), or by both explicit key identifier and identification of a certificate for the key.

4.2.1.1 Authority key identifier

```
   ( 1.3.6.1.4.1.10126.1.5.3.11
        NAME 'x509authorityKeyIdentifier'
        DESC 'Key Identifier field of the Authority Key Identifier
              extension'
        EQUALITY octetStringMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.40
        SINGLE-VALUE )
```

4.2.1.2 Authority cert issuer

```
   ( 1.3.6.1.4.1.10126.1.5.3.12
        NAME 'x509authorityCertIssuer'
        DESC 'Authority Cert Issuer field of the Authority Key Identifier
              extension'
        EQUALITY distinguishedNameMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.12
        SINGLE-VALUE )
```

In this specification, only the "Name" choice, encoded according to [RFC2253], of the "GeneralName" type may be used.

4.2.1.3 Authority cert serial number

```
   ( 1.3.6.1.4.1.10126.1.5.3.13
        NAME 'x509authorityCertSerialNumber'
        DESC 'Authority Cert Serial Number field of the
              Authority Key Identifier extension'
        EQUALITY integerMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
        SINGLE-VALUE )
```

4.2.2 Subject key identifier extension

This attribute identifies the public key being certified (see X.509(2000) 8.2.2.2, RFC3280 4.2.1.2). It enables distinct keys used by the same subject to be differentiated.

```
   ( 1.3.6.1.4.1.10126.1.5.3.14
        NAME 'x509subjectKeyIdentifier'
        DESC 'Key identifier which must be unique with respect to all
              key identifiers for the subject'
        EQUALITY octetStringMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.40
        SINGLE-VALUE )
```

4.2.3 Key usage extension

This attribute defines the purpose (e.g., encipherment, signature, certificate signing) of the key contained in the certificate (see X.509(2000) 8.2.2.3, RFC3280 4.2.1.3).

```
   ( 1.3.6.1.4.1.10126.1.5.3.15
        NAME 'x509keyUsage'
        DESC 'Purpose for which the certified public key is used'
        EQUALITY caseIgnoreMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
```

Values of this type are encoded according to the following BNF, so that each value corresponds to the respective bit in the ASN.1 "KeyUsage" bitstring:

```
   x509keyUsage-value ="digitalSignature" / "nonRepudiation" /
        "keyEncipherment" / "dataEncipherment" / "keyAgreement" /
        "keyCertSign" / "cRLSign" / "encipherOnly" / "decipherOnly"
```

4.2.4 Policy information identifier extension

This attribute contains OIDs which indicate the policy under which the certificate has been issued and the purposes for which the certificate may be used (see X.509(2000) 8.2.2.6, RFC3280 4.2.1.5).

```
   ( 1.3.6.1.4.1.10126.1.5.3.16
        NAME 'x509policyInformationIdentifier'
        DESC 'OID which indicates the policy under which the
              certificate has been issued and the purposes for which
              the certificate may be used'
        EQUALITY objectIdentifierMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.38
        SINGLE-VALUE )
```

4.2.5 Subject alternative name extension

The subject alternative name extension allows additional identities to be bound to the subject of the certificate (see X.509(2000) 8.3.2.1, RFC3280 4.2.1.7). Separate attribute types are defined for all choices of the ASN.1 type "GeneralName" except for "otherName", "x400Address" and "ediPartyName".

4.2.5.1 Subject RFC822 name

```
( 1.3.6.1.4.1.10126.1.5.3.17
     NAME 'x509subjectRfc822Name'
     DESC 'Internet electronic mail address of the entity
           associated with this public-key'
     EQUALITY caseIgnoreIA5Match
     SUBSTR caseIgnoreIA5SubstringsMatch
     SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

Values of this attribute must be encoded according to the syntax given in [RFC0822].

4.2.5.2 Subject DNS name

```
( 1.3.6.1.4.1.10126.1.5.3.18
     NAME 'x509subjectDnsName'
     DESC 'Internet domain name of the entity
           associated with this public-key'
     EQUALITY caseIgnoreIA5Match
     SUBSTR caseIgnoreIA5SubstringsMatch
     SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

Values of this attribute must be encoded as Internet domain names in accordance with [RFC1035].

4.2.5.3 Subject directory name

```
( 1.3.6.1.4.1.10126.1.5.3.19
     NAME 'x509subjectDirectoryName'
     DESC 'Distinguished name of the entity
           associated with this public-key'
     EQUALITY distinguishedNameMatch
     SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )
```

Values of this attribute type must be encoded according to the syntax given in [RFC2253].

4.2.5.4 Subject Uniform Resource Identifier

```
( 1.3.6.1.4.1.10126.1.5.3.20
     NAME  'x509subjectUniformResourceIdentifier'
     DESC 'Uniform Resource Identifier for the World-Wide Web
             of the entity associated with this public-key'
     EQUALITY caseExactIA5Match
     SUBSTR caseExactIA5SubstringsMatch
     SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

Values of this attribute must be encoded according to the syntax given in [RFC2396].

4.2.5.5 Subject IP address

```
( 1.3.6.1.4.1.10126.1.5.3.21
     NAME 'x509subjectIpAddress'
     DESC 'Internet Protocol address of the entity
           associated with this public-key'
     EQUALITY caseIgnoreIA5Match
     SUBSTR caseIgnoreIA5SubstringsMatch
     SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

Values of this attribute type must be stored in the syntax given in Appendix B of [RFC2373].

4.2.5.6 Subject registered ID

```
( 1.3.6.1.4.1.10126.1.5.3.22
     NAME 'x509subjectRegisteredID'
     DESC 'OID of any registered object identifying the entity
           associated with this public-key'
     EQUALITY objectIdentifierMatch
     SYNTAX 1.3.6.1.4.1.1466.115.121.1.38 )
```

registeredID is an identifier of any registered object assigned in accordance with ITU-T Rec. X.660.

4.2.6 Issuer alternative name extension

The issuer alternative names extension allows additional identities to be bound to the subject of the certificate or CRL (see X.509(2000) 8.3.2.2, RFC3280 4.2.1.8). Separate attribute types are defined for all choices of the ASN.1 type "GeneralName" except for "otherName", "x400Address" and "ediPartyName".

4.2.6.1 Issuer RFC 822 name

```
( 1.3.6.1.4.1.10126.1.5.3.23
     NAME 'x509issuerRfc822Name'
     DESC 'Internet electronic mail address of the entity who has
           signed and issued the certificate'
     EQUALITY caseIgnoreIA5Match
     SUBSTR caseIgnoreIA5SubstringsMatch
     SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

Values of this attribute must be encoded according to the syntax given in [RFC0822].

4.2.6.2 Issuer DNS name

```
( 1.3.6.1.4.1.10126.1.5.3.24
     NAME 'x509issuerDnsName'
     DESC 'Internet domain name of the entity who has
           signed and issued the certificate'
     EQUALITY caseIgnoreIA5Match
     SUBSTR caseIgnoreIA5SubstringsMatch
     SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

Values of this attribute must be encoded as Internet domain names in accordance with [RFC1035].

4.2.6.3 Issuer directory name

```
( 1.3.6.1.4.1.10126.1.5.3.25
     NAME 'x509issuerDirectoryName'
     DESC 'Distinguished name of the entity who has
           signed and issued the certificate'
     EQUALITY distinguishedNameMatch
     SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )
```

Values of this attribute type must be encoded according to the syntax given in [RFC2253].

4.2.6.4 Issuer Uniform Resource Identifier

```
   ( 1.3.6.1.4.1.10126.1.5.3.26
        NAME  'x509issuerUniformResourceIdentifier'
        DESC 'Uniform Resource Identifier for the World-Wide Web
                 of the entity who has signed and issued the certificate'
        EQUALITY caseExactIA5Match
        SUBSTR caseExactIA5SubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

Values of this attribute must be encoded according to the syntax given in [RFC2396].

4.2.6.5 Issuer IP address

```
   ( 1.3.6.1.4.1.10126.1.5.3.27
        NAME 'x509issuerIpAddress'
        DESC 'Internet Protocol address of the entity who has
              signed and issued the certificate'
        EQUALITY caseIgnoreIA5Match
        SUBSTR caseIgnoreIA5SubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

Values of this attribute type must be stored in the syntax given in Appendix B of [RFC2373].

4.2.6.6 Issuer registered ID

```
   ( 1.3.6.1.4.1.10126.1.5.3.28
        NAME 'x509issuerRegisteredID'
        DESC 'OID of any registered object identifying the entity who has
              signed and issued the certificate'
        EQUALITY objectIdentifierMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.38 )
```

registeredID is an identifier of any registered object assigned in accordance with ITU-T Rec. X.660.

4.2.7 Basic constraints extension

This attribute indicates whether the subject of the certificate is a CA (see X.509(2000) 8.4.2.1, RFC3280 4.2.1.10). If the value of this attribute is "TRUE", the certificate MUST be stored in the "cacertificate" attribute.

```
( 1.3.6.1.4.1.10126.1.5.3.29
     NAME 'x509basicConstraintsCa'
     DESC 'Identifies whether the subject of the certificate is a
           CA'
     EQUALITY booleanMatch
     SYNTAX 1.3.6.1.4.1.1466.115.121.1.7
     SINGLE-VALUE )
```

4.2.8 Extended key usage extension

This attribute indicates one or more purposes for which the certified public key may be used, in addition to or in place of the basic purposes indicated in the "x509keyUsage" attribute (see X.509(2000) 8.2.2.4, RFC3280 4.2.1.13). These purposes are identified by their OID.

```
( 1.3.6.1.4.1.10126.1.5.3.30
     NAME 'x509extKeyUsage'
     DESC 'Purposes for which the certified public key may be used,
           identified by an OID'
     EQUALITY objectIdentifierMatch
     SYNTAX 1.3.6.1.4.1.1466.115.121.1.38 )
```

4.2.9 CRL distribution points extension

This attribute identifies how the full CRL information for this certifacte can be obtained (see X.509(2000) 8.6.2.1, RFC3280 4.2.1.14).

```
( 1.3.6.1.4.1.10126.1.5.3.32
     NAME 'x509fullCRLDistributionPointURI'
     DESC 'URI type of DistributionPointName for the full CRL'
     EQUALITY caseExactIA5Match
```

```
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
```

In this specification, only the "uniformResourceIdentifier" choice of "distributionPoint.fullName" field is supported. If this attribute exists in an entry, both the "reasons" and "cRLIssuer" fields MUST be absent from the certificate, i.e. the CRL distributed by the distribution point contains revocations for all revocation reasons and the CRL issuer is identical to the certificate issuer.

Values of this attribute must be encoded according to the URI syntax given in [RFC2396].

4.3 Additional attributes

4.3.1 Certificate location

This attribute contains a pointer to the directory entry of a certificate. Thus it is possible to point to the certificate from an, e.g., white pages entry.

```
   ( 1.3.6.1.4.1.10126.1.5.4.74
        NAME 'x509certLocation'
        DESC 'Pointer to a x509certificate Entry'
        EQUALITY distinguishedNameMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )
```

4.3.2 Certificate holder

This attribute contains a pointer to the directory entry of the end entity to which this certificate was issued. Thus it is possible to link a certificate entry in a certificate repository to, e.g., a white pages entry of the subject.

```
   ( 1.3.6.1.4.1.10126.1.5.4.75
        NAME 'x509certHolder'
        DESC 'Pointer to the directory entry of the end entity to which this
                 certificate was issued'
        EQUALITY distinguishedNameMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )
```

4.3.3 X.509 user certificate

This attribute is used to store the complete certificate. Since it has to be single valued the multi valued attribute userCertificate [pkix-ldap-schema] cannot be used.

```
   ( 1.3.6.1.4.1.10126.1.5.4.76
         NAME 'x509userCert'
         DESC 'Complete x.509 user certificate'
         SUP userCertificate
         SINGLE-VALUE )
```

4.3.4 X.509 CA certificate

This attribute is used to store the complete CA certificate. Since it has to be single valued the multi valued attribute caCertificate [pkix-ldap-schema] cannot be used.

```
   ( 1.3.6.1.4.1.10126.1.5.4.77
         NAME 'x509caCert'
         DESC 'Complete x.509 CA certificate'
         SUP caCertificate
         SINGLE-VALUE )
```

4.4 X.509 PKC object class

This abstract object class contains the fields of an X.509 user certificate or CA certificate that are used in searches as attributes and in name forms. It is derived from the abstract objectclass x.509base as specified in [ldap-crl-schema] and is base for the two following object classes.

```
   ( 1.3.6.1.4.1.10126.1.5.4.2.3
        NAME 'x509PKC'
           SUP x509base
        ABSTRACT
        MUST ( x509serialNumber $ x509validityNotBefore $
              x509validityNotAfter $ x509subjectPublicKeyInfoAlgorithm )
        MAY  ( x509authorityKeyIdentifier $
           x509authorityCertIssuer $ x509authorityCertSerialNumber $
           x509subjectKeyIdentifier $ x509keyUsage $
           x509policyInformationIdentifier $
           x509subjectRfc822Name $ x509subjectDnsName $
           x509subjectDirectoryName $ x509subjectUniformResourceIdentifier $
           x509subjectIpAddress $
           x509subjectRegisteredID $
           x509issuerRfc822Name $ x509issuerDnsName $
           x509issuerDirectoryName $ x509issuerUniformResourceIdentifier $
           x509issuerIpAddress $
           x509issuerRegisteredID $
           x509extKeyUsage $
           x509FullcRLDistributionPointURI $ x509certHolder $
              x509issuerSerial $ x509basicConstraintsCa ) )
```

The attribute description of x509issuerSerial can be found in [ldap-ac-schema]

4.5 X.509 user certificate object class

This object class is for storing user certificates.

```
( 1.3.6.1.4.1.10126.1.5.4.2.4
      NAME 'x509userCertificate'
      SUP x509PKC
      STRUCTURAL
      MUST x509userCert
      MAY x509subject )
```

The attribute type x509subject is specified here as a MAY attribute. Nevertheless if this attribute is not used at least one of the following attributes MUST be filled in: x509subjectRfc822Name, x509subjectDnsName, x509subjectDirectoryName, x509subjectUniformResourceIdentifier, x509subjectIpAddress, or x509subjectRegisteredID.

4.6 X.509 CA certificate object class

This object class is for storing CA certificates.

```
( 1.3.6.1.4.1.10126.1.5.4.2.5
      NAME 'x509caCertificate'
      SUP x509PKC
      STRUCTURAL
      MUST ( x509caCert $ x509subject ) )
```

4.7 X.509 certificate holder object class

This auxiliary object class has an attribute that contains a pointer to an entry with x509certicate objectclass. Thus it is possible to link, e.g., an entry of a white pages directory to an entry in a certificate store.

```
   ( 1.3.6.1.4.1.10126.1.5.4.2.2
        NAME 'x509certificateHolder'
        AUXILIARY
        MAY  ( x509certLocation ) )
```

5. DIT structure and naming

If the schema presented in this document is used to store certificate information in a directory that contains entries for organizations, persons, services, etc., each certificate belonging to an entity SHOULD be stored as a direct subordinate to the entity's entry. In this case, these entries MUST be named by a multi-valued RDN formed by the certificate issuer and serial number, as this is the only way to enforce unique RDN under the siblings. This is expressed in the following two name forms:

```
   ( 1.3.6.1.4.1.10126.1.5.5.6
        NAME "x509userCertificateNameform"
        OC x509userCeriticate
        MUST ( x509serialNumber $ x509issuer ) )


   ( 1.3.6.1.4.1.10126.1.5.5.7
        NAME "x509caCertificateNameform"
        OC x509caCertificate
        MUST ( x509serialNumber $ x509issuer ) )
```

There are some LDAP implementations that don't support multi-valued RDNs. These can use following alternative two name forms:

```
   ( 1.3.6.1.4.1.10126.1.5.5.8
         NAME "x509userCertificateAltNameForm"
         OC x509userCertificate
         MUST x509issuerSerial )


   ( 1.3.6.1.4.1.10126.1.5.5.9
         NAME "x509PcaCertificateAltNameForm"
         OC x509caCertificate
         MUST x509issuerSerial )
```

The attribute description of x509issuerSerial can be found in [ldap-ac-schema]

For public directories of CAs that, besides the data stored in the certificates, do not hold any additional data about end entities the following DIT structure might be preferable. Entries for certificates are stored directly below the issuing CA's entry. In this case these entries SHOULD be named by the certificate serial number. This is expressed in the following two name forms:

```
( 1.3.6.1.4.1.10126.1.5.5.10
    NAME "x509userCertificateSerialNumberNameForm"
    OC x509userCertificate
    MUST x509serialNumber )


( 1.3.6.1.4.1.10126.1.5.5.11
    NAME "x509caCertificateSerialNumberNameForm"
    OC x509caCertificate
    MUST x509serialNumber )
```

Care must be taken when encoding DNs that contain an x509issuer attribute. Such a value is a string representation according to

[RFC2253]. These strings contain RFC2253 special characters and must therefore be escaped. For example, the issuer name in a certificate may be:

```
x509issuer: OU=VeriSign Trust Network,OU=(c) 1998 VeriSign\2c Inc. -
  For authorized use only,OU=Class 1 Public Primary Certification Au
  thority - G2,O=VeriSign\2c Inc.,C=US
```

When used in a DN, this will be appear as:

```
dn: x509serialNumber=123456+x509issuer=OU\3dVeriSign Trust Network
 \2cOU\3d(c) 1998 VeriSign\5c\2c Inc. - For authorized use only\2cOU\3d
 Class 1 Public Primary Certification Authority - G2\2cO\3dVeriSig
 n\5c\2c Inc.\2cC\3dUS,cn=Joe Example,...
```

6. Security Considerations

Attributes of directory entries are used to provide descriptive information about the real-world objects they represent which can be people, organizations, or devices. Most countries have privacy laws regarding the publication of information about people.

Without additional mechanisms such as Operation Signatures [RFC2649] which allow a client to verify the origin and integrity of the data contained in the attributes defined in this document, a client MUST NOT treat this data as authentic. Clients MUST only use - after proper validation - the data which they obtained directly from the certificate. Directory administrators MAY deploy ACLs which limit access to the attributes defined in this document to search filters.

Transfer of cleartext passwords is strongly discouraged where the underlying transport service cannot guarantee confidentiality and may result in disclosure of the password to unauthorized parties.

In order to protect the directory and its contents, strong authentication MUST have been used to identify the Client when an update operation is requested.

7. Open issues

There are still a number of todos with respect to this draft. Following work items will be dealt with in the next version of this draft:

- Section on IANA considerations

- Specification of an auxiliary object class with additional

attributes for storing a Qualified certificates as defined in RFC3039

- Specification of an auxiliary object class with attributes standardized elsewhere (e.g. RFC 2798) for additional certificate search possibilities, e.g. for the attribute mail.

- complete alignment with [ldap-ac-schema] and [ldap-crl-schema]

8. Acknowledgments

This document borrows from a number of IETF documents, including [certinfo-schema].

The authors wish to thank David Chadwick, Russ Housley, Mikhail Sahalayev, Michael Stroeder, and Kurt Zeilenga for their contributions to this document.

This work is part of the DFN Project "Ausbau und Weiterbetrieb eines Directory Kompetenzzentrums" funded by the German Ministry of Research (BMBF).

This document has been written in XML according to the DTD specified in RFC2629. xml2rfc has been used to generate an RFC2033 compliant plain text form. The XML source and a HTML version are available on request.

9. References

Normative references

[RFC0822] Crocker, D., "Standard for the format of ARPA Internet text messages", STD 11, RFC 822, August 1982.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2234] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 2234, November 1997.

[RFC2252] Wahl, M., Coulbeck, A., Howes, T. and S. Kille, "Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions", RFC 2252, December 1997.

[RFC2253] Wahl, M., Kille, S. and T. Howes, "Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names", RFC 2253, December 1997.

[RFC2256] Wahl, M., "A Summary of the X.500(96) User Schema for use with LDAPv3", RFC 2256, December 1997.

[RFC2373] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 2373, July 1998.

[RFC2396] Berners-Lee, T., Fielding, R. and L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax", RFC 2396, August 1998.

[RFC2798] Smith, M., "Definition of the inetOrgPerson LDAP Object Class", RFC 2798, April 2000.

[RFC3280] Housley, R., Polk, T., Ford, W. and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC 3280, April 2002.

[RFC3377] Hodges, J. and RL. Morgan, "Lightweight Directory Access Protocol (v3): Technical Specification", RFC 3377, September 2002.

[ldap-ac-schema] Chadwick, D. and M. Sahalayev, "Internet X.509 Public Key Infrastructure - LDAP Schema for X.509 Attribute Certificates", Internet Draft (work in progress), June 2003, <draft-ietf-pkix-ldap-ac-schema-01.txt>.

[ldap-crl-schema] Chadwick, D. and M. Sahalayev, "Internet X.509 Public Key Infrastructure - LDAP Schema for X.509 CRLs", Internet Draft (work in progress), June 2003, <draft-ietf-pkix-ldap-crl-schema-01.txt>.

[pkix-ldap-schema] Chadwick, D. and S. Legg, "Internet X.509 Public Key Infrastructure - LDAP Schema and Syntaxes for PKIs", Internet Draft (work in progress), June 2002, <draft-ietf-pkix-ldap-pki-schema-00.txt>.

Non-normative references

[RFC2312] Dusse, S., Hoffman, P., Ramsdell, B. and J. Weinstein, "S/MIME Version 2 Certificate Handling", RFC 2312, March 1998.

[RFC2649] Greenblatt, B. and P. Richard, "An LDAP Control and Schema for Holding Operation Signatures", RFC 2649, August 1999.

[RFC2651] Allen, J. and M. Mealling, "The Architecture of the Common Indexing Protocol (CIP)", RFC 2651, August 1999.

[RFC2654] Hedberg, R., Greenblatt, B., Moats, R. and M. Wahl, "A Tagged Index Object for use in the Common Indexing Protocol", RFC 2654, August 1999.

[X.509-2000] ITU, "Information Technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks", ITU-T Recommendation X.509, March 2000.

[certinfo-schema] Greenblatt, B., "LDAP Object Class for Holding Certificate Information", Internet Draft (expired), Februar 2000, <http://www.watersprings.org/pub/id/draft-greenblatt-ldap-certinfo-schema-02.txt>.

[componentmatch] Legg, S., "LDAP & X.500 Component Matching Rules", Internet Draft (work in progress), October 2002, <draft-legg-ldapext-component-matching-09.txt>.

[matchedval] Chadwick, D. and S. Mullan, "Returning Matched Values with LDAPv3", Internet Draft (work in progress), June 2002, <draft-ietf-ldapext-matchedval-06.txt>.

Authors' Addresses

Peter Gietz
DAASI International GmbH
Wilhelmstr. 106
Tuebingen 72074
DE

Phone: +49 7071 29 70336
EMail: peter.gietz@daasi.de
URI: http://www.daasi.de/

Norbert Klasen
Avinci
Halskestr. 38
Ratingen 40880
DE

EMail: norbert.klasen@avinci.de

Appendix A. Sample directory entries

A sample x509certificate directory entry for an intermediate CA certificate in LDIF format:

```
   dn: x509serialNumber=4903272,EMAILADDRESS=certify@pca.dfn.de,CN=DFN T
    oplevel Certification Authority,OU=DFN-PCA,OU=DFN-CERT GmbH,O=Deutsc
    hes Forschungsnetz,C=DE
   objectclass: x509caCertificate
   x509version: 2
   x509serialNumber: 4903272
   x509issuer: EMAILADDRESS=certify@pca.dfn.de,CN=DFN Toplevel Certifica
    tion Authority,OU=DFN-PCA,OU=DFN-CERT GmbH,O=Deutsches Forschungsnet
    z,C=DE
   x509validityNotBefore: 20020110170112Z
   x509validityNotAfter: 20060110170112Z
   x509subject: EMAILADDRESS=ca@daasi.de,OU=DAASI CA,O=DAASI Internation
    al GmbH,C=DE
   x509subjectPublicKeyInfoAlgorithm: 1.2.840.113549.1.1.1
   x509basicConstraintsCa: TRUE
   x509keyUsage: keyCertSign
   x509keyUsage: cRLSign
   x509subjectKeyIdentifier:: 5nrZFpVK4RKfIglqQ4N4JXBS4Bk=
   x509cLRdistributionPointURI: http://www.dfn-pca.de/certification/x509
    /g1/data/crls/root-ca-crl.crx
   x509cLRdistributionPointURI: http://www.dfn-pca.de/certification/x509
    /g1/data/crls/root-ca-crl.crl
```

```
   x509policyInformationIdentifier: 1.3.6.1.4.1.11418.300.1.1
   x509caCert:: MIIHTTCCBjWgAwIBAgIDStFoMA0GCSqGSIb3DQEBBQUAMI
    GsMQswCQYDVQQGEwJERTEhMB8GA1UEChMYRGV1dHNjaGVzIEZvcnNjaHVuZ3NuZXR6MR
    YwFAYD VQQLEw1ERk4tQ0VSVCBHbWJIMRAwDgYDVQQLEwdERk4tUENBMS0wKwYDVQQDE
    yRERk4gVG9 wbGV2ZWwgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkxITAfBgkqhkiG9w0B
    CQEWEmNlcnRpZnlAcGNhLmRmbi5kZTAeFw0wMjAxMTAxNzAxMTJaFw0wNjAxMTAxNzAx
    MTJaMF8xCzAJBgNVBAYTAkRFMSEwHwYDVQQKExhEQUFTSSBJbnRlcm5hdGlvbmFsIEdt
    YkgxETAPBgNVBAsTCERB QVNJIENBMRowGAYJKoZIhvcNAQkBFgtjYUBkYWFzaS5kZTC
    CASIwDQYJKoZIhvcNAQEBBQA DggEPADCCAQoCggEBAKmQBp+Gr28/qlEWjnJoiH3Awm
    hNEYMRWgXMXMMjM3S4mSmXZ8FZfTSPhi5O1zx5nyHecfl01fAO79Kpc6XkOTOl4iKBwu
    7+DM6my9Iizp2puhOQ6iuuchAIyJQPR0lfWAvvW+4n7Nf13Js5qFHvXBDqvgt6fud1l8
    XZ4nPWBSbs6OnB4EUDlRLx5fdCX2sEPQINKeu0INMtjHI6eGbspmahup0ArPA9RYZVjV
    q6ZHkh4205/JAhji9KtFifKCztXNTRMba7AHd2uS6GbF9+chGLPWGNZKtMhad1SvU7Zl
    w/ySHkFbBFZMu6x3kAVgwW8gKQa5qSFnMw/WTKATJRPekCAwEAAaOCA8Iwgg0+MA8GA1
    UdEwEB/wQFMAMBAf8wCwYDVR0PBAQDAgEGMB0GA1UdDgQWBBTmetkWlUrhEp8iCWpDg3
    glcFLgGTCB2wYDVR0jBIHTMIHQgBQGC/q1+Eh4oyCxCz7PoNDE0X990KGBsqSBrzCBrD
    ELMAkGA1UEBhMCREUxITAfBgNVBAoTGERldXRzY2hlcyBGb3JzY2h1bmdzbmV0ejEWMB
    QGA1UECxMNREZOLUNFUlQgR21iSDEQMA4GA1UECxMHREZOLVBDQTEtMCsGA1UEAxMkRE
    ZOIFRvcGxldmVsIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MSEwHwYJKoZIhvcNAQkBFh
    JjZXJ0aWZ5QHBjYS5kZm4uZGWCAxXP/TCBpQYDVR0fBIGdMIGaMEugSaBHhkVodHRwOi
    8vd3d3LmRmbi1wY2EuZGUvY2VydGlmaWNhdGlvbi94NTA5L2cxL2RhdGEvY3Jscy9yb2
    90LWNhLWNybC5jcngwS6BJoEeGRWh0dHA6Ly93d3cuZGZuLXBjYS5kZS9jZXJ0aWZpY2
    F0aW9uL3g1MDkvZzEvZGF0YS9jcmxzL3Jvb3QtY2EtY3JsLmNybDARBglghkgBhvhCAQ
    EEBAMCAQYwSwYJYIZIAYb4QgEIBD4WPGh0dHA6Ly93d3cuZGZuLXBjYS5kZS9jZXJ0aW
    ZpY2F0aW9uL3BvbGljaWVzL3g1MDlwb2xpY3kuaHRtbDCB+QYJYIZIAYb4QgENBIHrFo
```

```
 HoVGhpcyBjZXJ0aWZpY2F0ZSB3YXMgaXNzdWVkIGJ5IHRoZSBERk4tUENBLCB0aGUgVG
 9wCkxldmVsIENlcnRpZmljYXRpb24gQXV0aG9yaXR5IG9mIHRoZSBHZXJtYW4gUmVzZW
 FyY2gKTmV0d29yayAoRGV1dHNjaGVzIEZvcnNjaHVuZ3NuZXR6LCBERk4pLgpUaGUga2
 V5IG93bmVyJ3MgaWRlbnRpdHkgd2FzIGF1dGhlbnRpY2F0ZWQgaW4KYWNjb3JkYW5jZS
 B3aXRoIHRoZSBERk4tUENBIHg1MDkgUG9saWN5LjA3BglghkgBhvhCAQMEKhYoaHR0cH
 M6Ly93d3cuZGZuLXBjYS5kZS9jZ2kvY2hlY2stcmV2LmNnaTBkBgNVHSAEXTBbMFkGCy
 sGAQQB2RqCLAEBMEowSAYIKwYBBQUHAgEWPGh0dHA6Ly93d3cuZGZuLXBjYS5kZS9jZX
 J0aWZpY2F0aW9uL3BvbGljaWVzL3g1MDlwb2xpY3kuaHRtbDANBgkqhkiG9w0BAQUFAA
 OCAQEAU9GmwCW6LwsyHfC241afldqj/GULv8mfSkUEpK2OtYU1JAYFzmQx69iweOKHbg
 XZKZA2Wox+9AydIe98MJCSCOFKYjkzgXU4fEZbEgnZBo+/1+W2BoB6gFAWy77KVHgimA
 7AqCcfbObeyCmyfLg1ro8/KpE01OjNr0S+EfZ3gX9sezjVkCy12HBNQknz/hT2af25UU
 hyFTcvUY4xvlKAQpla29qyO28sfO93Qhkum6SU2XPlsKU+3lyqF33Xy84Y2z8ScVlsMu
 VWbUGtmVshnpT5K91n42pu/f0rLtkZDssEDbcLnQDLWEz1aUDkLC++4CeFJxC/Dd/SOr
 E0yR0hNQ=
```

A sample x509certificate directory entry for an end identity certificate in LDIF format:

```
dn: x509serialNumber=1581631808272310054353257112721713,EMAILADDRESS=
 certificate@trustcenter.de,OU=TC TrustCenter Class 1 CA,O=TC TrustCe
 nter for Security in Data Networks GmbH,L=Hamburg,ST=Hamburg,C=DE
objectclass: x509userCertificate
x509version: 2
x509serialNumber: 1581631808272310054353257112721713
x509issuer: EMAILADDRESS=certificate@trustcenter.de,OU=TC TrustCente
 r Class 1 CA,O=TC TrustCenter for Security in Data Networks GmbH,L=
 Hamburg, ST=Hamburg,C=DE
x509validityNotBefore: 20011030180757Z
x509validityNotAfter: 20021030180757Z
x509subject: EMAILADDRESS=norbert.klasen@daasi.de,CN=Norbert Klasen,C
 =DE
x509subjectPublicKeyInfoAlgorithm: 1.2.840.113549.1.1.1
x509userCert:: MIIDOTCCAqKgAwIBAgIOTfsAAAACxOstmlOu2TEwDQYJ
 KoZIhvcNAQEEBQAwgbwxCzAJBgNVBAYTAkRFMRAwDgYDVQQIEwdIYW1idXJnMRAwDgYD
 VQQHEwdIYW1idXJnMTowOAYDVQQKEzFUQyBUcnVzdENlbnRlciBmb3IgU2VjdXJpdHkg
 aW4gRGF0YSBOZXR3b3JrcyBHbWJIMSIwIAYDVQQLExlUQyBUcnVzdENlbnRlciBDbGFz
 cyAxIENBMSkwJwYJKoZIhvcNAQkBFhpjZXJ0aWZpY2F0ZUB0cnVzdGNlbnRlci5kZTAe
 Fw0wMTEwMzAxODA3NTdaFw0wMjEwMzAxODA3NTdaME4xCzAJBgNVBAYTAkRFMRcwFQYD
 VQQDEw5Ob3JiZXJ0IEtsYXNlbjEmMCQGCSqGSIb3DQEJARYXbm9yYmVydC5rbGFzZW5A
 ZGFhc2kuZGUwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAL8+XK98p4YjD7Wq7Apm
 hAN/j2tfVsFCS0ufy12vGpEtG4ny1tbbBORCJI8vIlDr2/vVTESl6UjzceloVUCib5V8
 55mKUVmLL9Ay4qQLFd4wAoRSPAu9DkfbR+ygjzaYq+MUKMwaB61sG6911xk/e2/IIq8/
```

```
IHKrRoYQGmHkaaJpAgMBAAGjgaowgacwMwYJYIZIAYb4QgEIBCYWJGh0dHA6Ly93d3cu
dHJ1c3RjZW50ZXIuZGUvZ3VpZGVsaW5lczARBglghkgBhvhCAQEEBAMCBaAwXQYJYIZI
AYb4QgEDBFAWTmh0dHBzOi8vd3d3LnRydXN0Y2VudGVyLmRlL2NnaS1iaW4vY2hlY2st
cmV2LmNnaS80REZCMDAwMDAwMDJDNEVCMkQ5QTUzQUVEOTMxPzANBgkqhkiG9w0BAQQF
AAOBgQCrAzuZzLztupeqcHa8OUOcnRuTacMpBEeICbZMKv6mN9rMYkAxFKerj/yXbdCE
8/3X3L00eGj+a8A7PumATiJSfmvYqa4EMZwHC2FFqPxYyAj+xVuSlL5AC4HGHu4SOCp/
UJu1xysoD16chOOLpj7+ZWZWLHIjA3zeXwUGl4kFvw==
```

Appendix B. Sample searches

This section details how clients should access the certstore. The searches are presented in LDAP URL format.

Retrieve all certificates for an end entity from a certstore using the first DIT structure:

```
ldap:///CN=Norbert%20Klasen,O=DAASI%20International%20GmbH,C=de?
     x509userCert?one?(objectClass=x509userCertificate)
```

Find a certificate in a trustcenter's certstore suitable for sending an encrypted S/MIME message to "norbert.klasen@daasi.de"

```
ldap:///O=TC%20TrustCenter%20for%20Security%20in%20Data%20Networks
     %20GmbH,L=Hamburg,ST=Hamburg,C=de?x509userCert?sub?
     ((&(objectClass=x509userCertificate)
       (x509subjectRfc822Name=norbert.klasen@daasi.de) )
      (|(x509keyUsage=keyEncipherment)(x509keyUsage=keyAgreement)
        (x509extendedKeyUsage=1.3.6.1.5.5.7.3.4)))
```

Find a CA certificate by its "subjectKeyIdentifier" obtained from the "keyIdentifier" field of the "autorityKeyIdentifier" extension in an end entity certificate:

```
ldap:///?caCertificate?sub?
     (&(objectClass=x509caCertificate)(x509subjectKeyIdentifier=%5CE6
      %5C7A%5CD9%5C16%5C95%5C4A%5CE1%5C12%5C9F%5C22%5C09%5C6A%5C43%
      5C83%5C78%5C25%5C70%5C52%5CE0%5C19))
```

Appendix C. Changes from previous Drafts

C.1 Changes in Draft 01

- Included new Attributes x509authorityKeyIdentifier, x509authorityCertissuer, x509authorityCertSerialNumber, x509certificateLocation, x509certificateHolder, and new objectclass x509certificateHolder

- Fixed bug in definition of objectclass x509certificate

- Changed references from RFC 2459 to RFC 3280 and included some respective language in 3.2.

- Changed references from RFC 2251 to RFC 3377 and deleted all references to LDAPv2.

- Deleted ";binary" in examples

- Included new section: Comparision with component matching approach

- Some changes in wording and section titles, and elimination of typos

- Changed order of authors, and one author's address

C.2 Changes in Draft 02

- abstract object class x509PKC

- aligned to [ldap-ac-schema] and [ldap-crl-schema]

C.3 Changes in Draft 03

- Changed Matching Rules from caseIgnoreMatch to caseIgnoreIA5Match etc.

- moved the references to RFC 3280 from the DESC part of the attribute definition to the text

- added some additional text about CIP in Introduction

- reworded text in Section 4.1.7

- changed x509userCert and x509caCert to be inherited from userCertificate and caCertificate respectively

- added clarification about x509subject and subject alternative names in section Section 4.5

- added attribute type x509issuerSerial to x509PKC object class

- added attribute type x509basicConstraintsCa to x509PKC object class

- renamed attributetype x509cRLDistributionPointURI to x509FullcRLDistributionPointURI

- devided references in normative and non normative

- deleted attributetype mail from x509PKC objectclass

- created separate Name Forms for x509userCertificate and x509caCertificate object classes.

- changed attributetype x509SerialNumber to MULTI-VALUE

- adjusted examples to new schema

- Fixed more typos

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.

Network Working Group
Internet-Draft
Expires: December 29, 2003

P. Gietz
DAASI International GmbH
N. Klasen
Avinci
June 30, 2003

An LDAPv3 Schema for X.509 Certificates
draft-klasen-ldap-x509certificate-schema-03

Status of this Memo

Comments and suggestions on this document are encouraged. They should be sent to the PKIX working group discussion list <ietf-pkix@imc.org> or directly to the authors.

This Internet-Draft will expire on December 29, 2003.

Copyright Notice

Abstract

This document describes an LDAP schema which can be used to implement a certificate store for X.509 certificates. Specifically, two structural object classes for X.509 user and CA certificates are defined. Key fields of a certificate are stored in LDAP attributes

so that applications can easily retrieve the certificates needed by using basic LDAP search filters. Multiple certificates for a single entity can be stored and retrieved.

Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

The following syntax specifications use the augmented Backus-Naur Form (ABNF) as described in [RFC2234].

Schema definitions are provided using LDAPv3 description formats [RFC2252]. Definitions provided here are formatted (line wrapped) for readability.

Table of Contents

1. Introduction

A key component in the wide-spread adoption of a PKI infrastructure is the general availability of public keys and their certificates. Today, certificates are often published in an X.500 compliant directory service. These directories are accessed by applications using the LDAP v3 [RFC3377] protocol. An LDAPv3 schema for PKI repository objects is specified in [pkix-ldap-schema], where a set of object classes, attribute types, syntaxes, and extended matching rules are defined. For storing certificates, the "userCertificate" and "cACertificate" attribute types are used. All certificates of an entity are stored as values in these multi-valued attributes. This solution has a serious drawback. In LDAP, the smallest granularity of data access is the attribute. The directory server will therefore always return the full list of certificates of an entry to clients dealing with certificates. If the number of certificates for an entity is large this will result in considerable overhead and burden to the client.

This document proposes to solve this problem by the use of the structural object classes x509userCertificate and x509caCertificate for storing certificates. Each certificate will be stored in a separate entry in the directory.

While it is a simple matter to modify the DIT in such a way that all certificate information is removed from the entries and placed in the container directly beneath the entries according to the definitions of this specification, it is less simple to simultaneously modify all of the applications that depend on certificates being stored in the entry. Thus, it may be desirable to duplicate the certificate information, by having it appear in the entry, as well as in the container beneath the entry for a short period of time, in order to allow for migration of the applications to the new LDAP schema. As in any situation in which information is duplicated, great care must be taken in order to ensure the integrity and consistency of the information.

Fields of certificates which are needed to identify a certificate and those which are often used in searching for an appropriate certificate, are extracted from the certificate and stored as attributes of the entry. Each attribute type uses existing LDAP syntax, so that no new matching rules need to be defined. Applications can thus search for specific certificates with simple LDAP filters. This approach could be named a metadata approach, since data (attributes) about data (certificate) are stored.

The use of simple attributes also makes a large scale widely distributed certificate repository service possible by using an

indexing service based on The Common Indexing Protocol (CIP) [RFC2651], which defines a protocol between index servers for exchanging indexobjects in order to facilitate query routing. The Tagged Index Object format as specified in [RFC2654] was specified to carry directory server information, by collecting the single attributetypes and values.

This document is one of a set following this approach comprising:

1. the LDAP schema for X.509 public key certificates (this document)

2. the LDAP schema for X.509 attribute certificates [ldap-ac-schema]

3. the LDAP schema for X.509 CRLs [ldap-crl-schema]

Two alternative approaches are discussed in the next two sections.

2. Comparison with Values Return Filter Control

In [matchedval] a control has been defined that allows for only a subset of values of a specified attribute to be returned from a matching entry, by defining a filter for the returned values. In this section, this approach is compared with the one proposed in this document.

The major benefit of the Values Return Filter Control is that it does not require any changes to the DIT.

There are several advantages in using the x509certificate object class. No special matching rules are needed to retrieve a specific certificate. Any field in the certificate can be used in the search filter. Even information that doesn't appear in the certificate can be used in a search filter. It is easier to remove certificates from the DIT, since the entire certificate BER/DER encoding does not have to be supplied in the modify operation. Searches that don't need extensible matching rules and Values Return Filter Control will perform faster.

Another advantage of the solution proposed here is that it will not be necessary to modify existing server implementations to support this schema. The extended matching rules proposed in [pkix-ldap-schema] would require substantial changes in the servers' indexing mechanisms. In contrast, servers implementing the x509certificate schema can easily leverage their indexing support for standard LDAPv3 syntaxes.

A CIP-based indexing system for a wide scale distributed certificate repository will rather be possible by using the solution proposed

here due to its dependency on attribute values.

3. Comparison with component matching approach

[componentmatch] defines a new mechanism for matching in complex syntaxes, by defining generic matching rules that can match any user selected component parts in an attribute value of any arbitrarily complex attribute syntax. We believe that this might be the proper way to solve search problems in the longer term, but that it will take a long time until such ASN.1 based mechanisms will be implemented in LDAP servers and clients. Even if this has happened the mechanism proposed here, will still be useful in the frame of CIP. A simple and easy to implement mechanism is needed today and this is what this memo wants to provide.

4. The x509certificate object classes and their attribute types

The description of all attributes with relevance to fields and extensions of an X.509 certificate include a respective reference to [X.509-2000] and to [RFC3280].

4.1 Attributes for mandatory fields of an X.509 certificate

4.1.1 X.509 version

X.509 Version of the encoded certificate (See X.509(2000) 7, RFC3280 4.1.2.1.) or of the CRL.

```
( 1.3.6.1.4.1.10126.1.5.3.1
        NAME 'x509version'
        DESC 'X.509 Version of the certificate, or of the CRL'
        EQUALITY integerMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
        SINGLE-VALUE )
```

Values of this attribute may either be 0, 1, 2 or 3 corresponding to X.509 v1, v2, v3, or v4.

4.1.2 Serial number

The serial number is an integer assigned by the CA to each certificate. It is unique for each certificate issued by a given CA (i.e., the issuer name and serial number uniquely identify a certificate). See X.509(2000) 7, RFC3280 4.1.2.2

↗Pam Floyd ↖ 19.34 RCW

Head of RCW 19.34 Dept [434.180.225 WAC]

Need Bond form for "Suitable guaranty"

WAC 434-180-225
Suitable guaranty.

(1) The suitable guaranty required for licensure as a certification authority may be in the form of either a surety bond executed by an insurer lawfully operating in this state, or an irrevocable letter of credit issued by a financial institution authorized to do business in this state.

(2) The suitable guaranty must be in an amount of at least fifty thousand dollars.

(3) As to form, the suitable guaranty must:

(a) Identify the insurer issuing the suitable guaranty or financial institution upon which it is drawn, including name, mailing address, and physical address, and identify by number or copy its licensure or approval as a financial institution, or in the case of an insurer, as an insurer in this state;

(b) Identify the certification authority on behalf of which it is issued;

(c) Be issued payable to the secretary for the benefit of persons holding qualified rights of payment against the licensed certification authority named as principal of the bond or customer of the letter of credit;

(d) State that it is issued for filing under the Washington Electronic Authentication Act; and

(e) Specify a term of effectiveness extending at least as long as the term of the license to be issued to the certification authority.

[Statutory Authority: RCW 19.34.030, 19.34.040, 19.34.100, 19.34.111 and 19.34.400. 97-24-053, § 434-180-225, filed 11/26/97, effective 12/27/97.]