UNCLASSIFIED

Serial No. CREG-100884
Effective Date: 19 November 2010

NSA/CSS COMMERCIAL SOLUTIONS CENTER
★ Partnering with Industry ★

Elliptic Curve Cryptography Patent License Agreement

Between

National Security Agency/Central Security Service
Commercial Solutions Center (NCSC)

And
OpenSSL Software Foundation, Inc.

PATENT LICENSE AGREEMENT

This Patent License Agreement ("Agreement") is made as of the date last signed below ("Effective Date") between OpenSSL Software Foundation, Inc. ("Company"), incorporated in the state of Maryland, with a principal place of business at 1829 Mount Ephraim Road, Adamstown, Maryland 21710-8521, U.S.A., and the United States Government ("USG") as represented by the National Security Agency, an instrumentality of the United States Government with a principal place of business at 9800 Savage Road, Ft. Meade, Maryland, 20755-6000, U.S.A.

WHEREAS, USG has licensed certain patents and patent applications in the field of elliptic curve cryptography from Certicom Corporation (Certicom), with the right to sublicense the same;

WHEREAS, USG desires to license the patents and patent applications in order to allow implementation of these patents and patent applications;

WHEREAS, Company desires a license to the patents and patent applications in order to implement these patents and patent applications; and,

WHEREAS, USG is willing to grant a license under the patents and patent applications in accordance with the terms and conditions set forth in this Agreement.

NOW, THEREFORE, in consideration of the mutual promises, terms, and conditions hereinafter set forth, the parties hereby agree as follows:

1. **Definitions.**

   A. "**End User**" means a person or entity granted the right to use any Licensed Product or Licensed Process solely for that person or entity's own use without right to license, resell, or otherwise redistribute such Licensed Product or Licensed Process to any other person or entity.

   B. "**Field of Use**" means the technology and methods necessary to implement, in an NSA Approved Product or a product for national security compliant with FIPS-140-2 or its successors, the Licensed Patents and Patent Applications with elliptic curves over *GF(p)*, where *p* is a prime number greater than 2^{255}.

   C. "**NSA Approved Product**" means a product that is approved by the NSA for use by:

      1.) U.S. Government agencies for protecting classified information, mission critical information, national security information or for protecting information under 10 U.S.C. 2315 or information contained in a "national security system" as defined by 40 U.S.C. 1452 and re-codified at 40 U.S.C. 11103; or,

2.) State and Local government agencies for protecting classified information, mission critical information, national security information or for protecting information under 10 U.S.C. 2315 or information contained in a "national security system" as defined by 40 U.S.C. 1452 and re-codified at 40 U.S.C. 11103; or,

3.) Foreign government agencies for protecting classified information, mission critical information, or national security information where interoperability with U.S. entities using an NSA Approved Product is a possibility or the aforementioned information originated in the U.S. Federal, State, or Local Government.

D. **"Licensed Patents and Patent Applications"** means the following United States and foreign patents and patent applications and any continuations, continuations in part, divisions, reissues, reexaminations, issuances, and foreign equivalents thereof:

1.) U.S. Pat. No. 5,761,305 entitled "Key Agreement and Transport Protocol with Implicit Signatures" issued on June 2, 1998;

2.) Can. Pat. Appl. Ser. No. 2176972 entitled "Key Agreement and Transport Protocol with Implicit Signature and Reduced Bandwidth" filed on May 16, 1996;

3.) U.S. Pat. No. 5,889,865 entitled "Key Agreement and Transport Protocol with Implicit Signatures" issued on March 30, 1999;

4.) U.S. Pat. No. 5,896,455 entitled "Key Agreement and Transport Protocol with Implicit Signatures" issued on April 20, 1999;

5.) U.S. Pat. No. 5,933,504 entitled "Strengthened Public Key Protocol" issued on August 3, 1999;

6.) Can. Pat. Appl. Ser. No. 2176866 entitled "Strengthened Public Key Protocol" filed on May 17, 1996;

7.) E.P. Pat. Appl. Ser. No. 96201322.3 entitled "Strengthened Public Key Protocol" filed on May 17, 1996;

8.) U.S. Pat. No. 5,999,626 entitled "Digital Signatures on a Smartcard" issued on December 7, 1999;

9.) Can. Pat. Appl. Ser. No. 2202566 entitled "Digital Signatures on a Smartcard" filed on April 14, 1997;

10.) E.P. Pat. Appl. No. 97106114.8 entitled "Digital Signatures on a Smartcard" filed on April 15, 1997;

11.) U.S Pat. No. 6,122,736 entitled "Key Agreement and Transport Protocol with Implicit Signatures" issued on September 19, 2000;

12.) Can. Pat. Appl. Ser. No. 2174261 entitled "Key Agreement and Transport Protocol with Implicit Signatures" filed on April 16, 1996;

13.) E.P. Pat. Appl. Ser. No. 96105920.1 entitled "Key Agreement and Transport Protocol with Implicit Signatures" filed on April 16, 1996;

14.) U.S. Pat. No. 6,141,420 entitled "Elliptic Curve Encryption Systems" issued on October 31, 2000;

15.) Can. Pat. Appl. Ser. No. 2155038 entitled "Elliptic Curve Encryption Systems" filed on July 31, 1995;

16.) E.P. Pat. Appl. Ser. No. 95926348.4 entitled "Elliptic Curve Encryption Systems" filed on July 31, 1995;

17.) U.S. Pat. No. 6,336,188 entitled "Authenticated Key Agreement" issued on January 1, 2002;

18.) U.S. Pat. No. 6,487,661 entitled "Key Agreement and Transport Protocol" issued on November 26, 2002;

19.) Can. Pat. Appl. Ser. No. 2174260 entitled "Key Agreement and Transport Protocol" filed on April 16, 1996;

20.) E.P. Pat. Appl. Ser. No. 96105921.9 entitled "Key Agreement and Transport Protocol" filed on April 21, 1996;

21.) U.S. Pat. No. 6,563,928 entitled "Strengthened Public Key Protocol" issued on May 13, 2003;

22.) U.S. Pat. No. 6,618,483 entitled "Elliptic Curve Encryption Systems" issued September 9, 2003;

23.) U.S. Pat. Appl. Ser. No. 09/434,247 entitled "Digital Signatures on a Smartcard" filed on November 5, 1999;

24.) U.S. Pat. Appl. Ser. No. 09/558,256 entitled "Key Agreement and Transport Protocol with Implicit Signatures" filed on April 25, 2000;

25.) U.S. Pat. Appl. Ser. No. 09/942,492 entitled "Digital Signatures on a Smartcard" filed on August 29, 2001 and published on July 18, 2002; and,

26.) U.S. Pat. Appl. Ser. No. 10/185,735 entitled "Strengthened Public Key Protocol" filed on July 1, 2000.

E. **"Licensed Process"** means any process which practices an invention claimed in the Licensed Patents and Patent Applications licensed under this Agreement and which if practiced in the absence of the license granted in this Agreement would infringe, contribute to, or induce the infringement of, at least one of the Licensed Patents and Patent Applications licensed under this Agreement.

F. **"Licensed Product"** means any product, article, toolkit, equipment, system, unit, or component part which employs or is produced by the practice of an invention claimed in the Licensed Patents and Patent Applications licensed under this Agreement and which if made, used, or sold in the absence of the license granted under this Agreement, would infringe, contribute to, or induce the infringement of at least one of the Licensed Patents and Patent Applications licensed under this Agreement.

2. **License Grant and Restrictions.**

USG Grant to the Company. The USG hereby grants to the Company a nonexclusive, nontransferable, worldwide, royalty-free license to the Patents and Patent Applications listed herein within the Field of Use to make, have made, and use Licensed Products and to practice the Licensed Processes in the Field of Use and to offer for sale, sell and import Licensed Products to End Users. All rights not expressly granted herein are reserved by the USG. Under no circumstances will anything in this Agreement be construed as granting, by implication, estoppel, or otherwise, a license to any USG technology or proprietary right other than the permitted use of the Licensed Patents and Patent Applications.

3. **Products.**

A. The product(s) covered by this Agreement are:

1.) The OpenSSL Toolkit

2.) The OpenSSL FIPS Object Module

Source code for both products is available at http://openssl.org/source/ and mirrors and is distributed under a BSD style open source license.

B. All of the above products have been determined to be within the Field of Use, as defined in section 1 of this Agreement.

4. **Warranties and Disclaimers.**

A. USG. USG warrants that it is authorized to enter into this Agreement and to grant the rights granted to the Company in Section 2.

B. Disclaimer. Nothing in this Agreement is or shall be construed as (i) a warranty or representation by the USG as to the validity or scope of the Licensed Patents and Patent Applications; (ii) any warranty or representation by the USG that anything made, used, sold, or otherwise disposed of under the license granted in this Agreement is or will be free from infringement of patents, copyrights, and other rights of third parties; or (iii) granting by implication, estoppel, or otherwise any license under patents licensed by the USG other than the Licensed Patents and Patent Applications defined in this Agreement, regardless of whether such patents are dominant or subordinate to the Licensed Patents and Patent Applications. EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, USG MAKES NO REPRESENTATIONS AND EXTENDS NO WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED. THERE ARE NO EXPRESSED OR IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR THAT THE USE OF THE LICENSED PRODUCTS OR LICENSED PROCESSES WILL NOT INFRINGE ANY PATENT, COPYRIGHT, TRADEMARK, OR OTHER RIGHTS.

5. **Marking and References.**

A. Patent. The Company agrees to mark all Licensed Products licensed under this Agreement, or in the event their size or configuration makes such marking impractical, their containers, packaging, or labels, as well as all literature describing the Licensed Products, with the appropriate patent numbers or patent application serial numbers.

B. No Use of Certicom Marks. The Company agrees not to identify or use any trademark, service mark, trade name, or symbol of Certicom or its affiliates, their employees, agents, officers, or directors without the prior written approval of Certicom.

6. **Limitation of Liability.**

NO LIABILITY. TO THE EXTENT PERMITTED BY APPLICABLE LAW, CERTICOM AND THE USG SHALL NOT BE LIABLE TO THE COMPANY, THE END USERS OF ANY LICENSED PRODUCT OR LICENSED PROCESS, OR ANY THIRD PARTIES FOR ANY DIRECT, CONSEQUENTIAL, INCIDENTAL, INDIRECT, PUNITIVE, OR SPECIAL DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, ANY DAMAGE OR INJURY TO BUSINESS EARNINGS, PROFITS, OR GOODWILL SUFFERED BY ANY PERSON ARISING FROM ANY USE OF THE LICENSED PATENTS AND PATENT APPLICATIONS, LICENSED PRODUCTS, AND/OR LICENSED PROCESSES, REGARDLESS OF WHETHER SUCH LIABILITY IS BASED ON BREACH OF CONTRACT, TORT, STRICT LIABILITY, BREACH OF WARRANTIES, INFRINGEMENT OF INTELLECTUAL PROPERTY, FAILURE OF ESSENTIAL PURPOSE OR OTHERWISE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. **Term and Termination.**

This Agreement and the rights and obligations established thereby shall remain in effect until the expiration of the last Licensed Patent and Patent Application licensed under this Agreement, or earlier if terminated by USG for any of the following reasons:

A. Breach of this Agreement by the Company; or,

B. Termination, by means other than expiration, of this Agreement by USG.

The determination of whether a breach has occurred remains within the sole discretion of the USG.

The Company may terminate this Agreement at any time. USG may terminate this Agreement when it is no longer able to approve the Company's product for use after it was once approved. Substantive changes in the product(s) may require another evaluation in order to maintain product approval. USG need not terminate this Agreement when the Company is working to regain approval. No termination by USG for substantive changes shall become effective unless USG notifies the Company of the reasons therefore and provides the Company with a reasonable period to cure the product for approval in good faith.

From and after termination of this Agreement, the Company shall cease and desist from all use of the Licensed Patents and Patent Applications licensed under this Agreement.

8. **Notices.**

All notices in connection with this Agreement shall be sent to the addresses stated at the beginning of this Agreement where the parties are identified (or to such other address as the party to receive the notice so designates by written notice to the other) and shall be: (i) deposited in the official mail system of the country of the sender, postage prepaid, certified or registered, return receipt requested; (ii) sent by overnight courier, charge prepaid; or (iii) delivered in person. Notices will be deemed to have been given at the time of actual delivery in person, six (6) business days after deposit in the official mail system of the country of the sender, or one (1) day after deposit with an overnight courier service.

9. **Miscellaneous.**

A. Governing Law. This Agreement shall be governed and construed by U.S. federal law, without regard to any conflicts of law principles.

B. No Waiver. No waiver of any breach of any provision of this Agreement shall constitute a waiver of any prior, concurrent, or subsequent breach of the same or any other provision hereof, and no waiver shall be effective, unless made in writing and signed by an authorized representative of the waiving party.

C. Severability. If any provision of this Agreement shall be held by a court of competent jurisdiction to be illegal, invalid, or unenforceable, the parties shall endeavor in good faith to agree to amendments that will preserve, as far as possible, the intentions expressed in this Agreement. If the parties fail to agree on such amendments, such invalid provision shall be severed from the remaining provisions, which shall remain in full force and effect.

D. Relationship. The relationship between the USG and the Company is solely that of independent contractors. Neither this Agreement nor any terms and conditions contained herein shall be construed as creating a partnership, joint venture, or agency relationship or as granting a franchise. Neither party shall have the authority to represent or bind the other.

E. Headings. Section headings are used in this Agreement for convenience of reference only and shall not affect the meaning of any provision of this Agreement.

F. Assignment. The license grant in Section 2 is personal to USG and the Company, and the Company shall not assign or transfer this Agreement.

G. Force Majeure. Neither party shall be held responsible for any delay or failure in performance of its obligations hereunder to the extent such delay or failure is caused by fire, flood, strike, civil, governmental, or military authority, act of terrorism, act of God, or other similar causes beyond its reasonable control and without the fault or negligence of the delayed or non-performing party or its subcontractors.

H. Export Compliance and Foreign Reshipment Liability. The patent and patent applications licensed under this Agreement, whether or not incorporated into Licensed Products or Licensed Processes, are subject to United States and Canadian export control laws and regulations that restrict exports, reexports, and disclosures to foreign persons of cryptographic items and are also subject to certain foreign laws that may restrict the export, reexport, import, and/or use of such items. Performance of this Agreement is expressly made subject to any export laws, regulations, orders, or other restrictions imposed by the United States of America, Canada, or any other country or government entity on the technology described in the Licensed Patents and Patent Applications under this Agreement, Licensed Products, Licensed Processes, or information relating to any of the above. Notwithstanding any other provision of this Agreement to the contrary, the Company under this Agreement shall not directly or indirectly import, export, or reexport any technology described in the Licensed Patents and Patent Applications, Licensed Products, Licensed Processes, or information pertaining thereto to any country or foreign person to which such import, export, or reexport is restricted or prohibited. If any country, government, or any agency thereof requires an export license or other governmental approval at the time of import, export, or reexport, the Company shall obtain such license approval before importing, exporting, or reexporting any technology described in the Licensed Patents and Patent Applications, Licensed Products, Licensed Processes, or information pertaining thereto. The Company unconditionally accepts full responsibility for their compliance with these requirements.

I. Language. This Agreement has been drawn up and shall be construed in accordance with the English language.

J. Counterparts. This Agreement may be executed in two or more counterparts, each of which shall be deemed to be an original and all of which together shall constitute one and the same instrument.

K. Facsimile Signature. This Agreement and any counterpart original thereof may be executed and transmitted by facsimile. The facsimile signature shall be valid and acceptable for all purposes as if it were an original.

IN WITNESS WHEREOF, each party has caused this Agreement to be executed by its duly authorized representatives:

OpenSSL Software Foundation, Inc. NATIONAL SECURITY AGENCY

UNCLASSIFIED

BY:	BY: Curtis W
Steve Marquess	Curtis W. Dukes
PRESIDENT	DIRECTOR, NSA/CSS COMMERCIAL SOLUTIONS CENTER
DATE: 2010-11-04	DATE: 19 November 2010