

# Stiftung SIC Java Crypto-Software Development Kit

## Licence Agreement

Valid from January 1, 2017

The Stiftung SIC (Stiftung Secure Information and Communication Technologies, Inffeldgasse16a, A-8010 Graz, Austria / Europe) hereafter referred to as "Stiftung SIC" offers to grant licences for the SOFTWARE defined below according to the following conditions:

### 1. DEFINITIONS

For the purpose of this Licence Agreement, the following definitions are valid:

- a. "**LICENSEE**" refers to the person, organisation or company, to whom the licenses are granted under this license agreement.
- b. The term "**SOFTWARE**" refers to IAIK Java Crypto Software in any form (source code, object code or other) including documentation. The SOFTWARE is the sole property of Stiftung SIC and protected by Austrian, International Copyright Law, e.g. the Revised Berne Convention, and the US Copyright Act.
- c. "**IAIK Java Crypto Software**" means either IAIK-JCE, iSaSiLk or any other Java-based Crypto-Software development kit which usually consists of source code (if applicable, for source licences only), Java byte code or any other form of object code. The Software and additional tools are distributed in documentation, manuals, user guides, sample application code, tools - including any revisions, patches and updates delivered or downloaded by the LICENSEE.
- d. "**IAIK Java Crypto Software Runtime Modules**" means the runtime object code modules provided with, or derived from, an IAIK-Java-Crypto Software Development Kit, which are usually distributed as a Java-Archive in JAR or ZIP-Format, or in any other format suitable for use by application programmes or other software.
- e. "**IAIK-Crypto Software based Application**" means any computer programme created by the LICENSEE using any of the IAIK-Toolkits, including applications offered using the "Software as a Service" model, but with the exception of other server software, which is considered as a different category.
- f. "**Server software**" means IAIK-Crypto Software based applications run on a server. Examples for server software are applets, midlets, servlets, CGI-scripts or software that is run on a server, with the exception of applications offered using the "Software as a Service" model.
- g. "**To publish**" means that an application is retrievable or accessible from a certain server, but not installed on another machine.

### 2. GRANTING of LICENCES

o Free Trial License:

The SOFTWARE can be downloaded from the INTERNET and used free of charge for thirty days of inspection and testing purposes. The test version may not be used for actual applications or commercial usage and must not be redistributed via any medium. Once the testing period is concluded this license automatically expires, whereupon all copies of the SOFTWARE at the LICENSEE`s premises must be destroyed.

Upon payment received by Stiftung SIC in accordance with the price list (without deductions), the licensee is granted one the following licenses specified below:

o Developers Licence:

Stiftung SIC grants the LICENSEE a non-exclusive, non-transferable, non-sublicensable licence to use the number of copies of each of the IAIK-Toolkits identified below for the development of IAIK-Crypto Software- based applications or server software only. Any attempt to use an IAIK-Toolkit for any other purpose, including, but not limited to, the creation of a toolkit, or inclusion in a different toolkit, is not permitted. The number of developer licences acquired entitles the equivalent number of LICENSEE employees to develop IAIK-Crypto Software-based applications using the IAIK Crypto-Software. For unlimited licences, all employees of the LICENSEE are allowed to use the IAIK Crypto-Software. These licences are not transferable to contractors or any other persons, organisation or companies outside the LICENSEE organisation, excluding the following scenario: A developer license can be transferred to a subcontractor in case of necessity during the course of a project, and if the results of the project are subsequently only owned by the LICENSEE: In this case the LICENSEE is allowed to transfer the purchased developer license to a subcontractor exclusively for developing software for this project and only for the time span of the project. In this case it must be guaranteed that either the LICENSEE or the subcontractor – and not both - use the Software. To be even clearer, the subcontractor may not use the licenses for his own developments outside the project nor may he own, sell or redistribute the results of the projects in any other way.

The LICENSEE may produce as many additional copies of the elements of the Stiftung SIC-Toolkit as he has purchased licences. He may also produce as many copies of the runtime modules as needed for the development of IAIK Crypto Software based applications. The IAIK Toolkit may also be stored on a Network-Server, if the appropriate number of licences has been acquired. The LICENSEE may also produce one additional copy of each IAIK-Toolkit for backup or archival purposes. No other right to reproduce the SOFTWARE is granted.

o Runtime Licence:

Stiftung SIC grants the LICENSEE a non-exclusive, non-sublicensable licence to run the respective number of IAIK-Crypto Software-based applications that have been developed by the LICENSEE under a developer Licence or, when the application is offered using the “Software as a Service” model, to allow the respective number of users to use the service. These licences are transferable to customers or other third parties, which means that if the customer or other third party acquires a certain number of licences for IAIK-Crypto Software-based applications from the LICENSEE, the respective number of runtime licences is transferred to the customer. If the LICENSEE grants his customers an unlimited number of runtime licences, the LICENSEE also needs an unlimited runtime licence from Stiftung SIC.

o Server Licence:

Stiftung SIC grants the LICENSEE a non-exclusive, non-sublicensable licence to run IAIK-Crypto based applications on a server or to publish IAIK-Crypto based applications on the respective number of servers. An application that is published on more than one server needs as many licences as the number of servers on which it is published. These licences are transferable to customers or other third parties, so that if the customer or other third party acquires a certain number of licences for servers using IAIK-Crypto Software from the LICENSEE, the respective number of server licences is transferred to the customer. If the LICENSEE grants his customer unlimited licences, the LICENSEE also needs an unlimited server licence from Stiftung SIC.

o Source Code Licence:

Full licences contain the source code of IAIK Java Crypto-Software. This source code is only provided for inspection purposes and Stiftung SIC does **not** grant the LICENSEE any licence to use that source code beyond inspection. The only exception to this is when the LICENSEE purchases an additional *unlimited source code developer toolkit license add-on*. This add-on adds the right to modify the source code. The LICENSEE is required to order any unlimited developer toolkit license together with the unlimited source code developer toolkit license. Stiftung SIC has no obligation to support code

that has been changed and it is also the responsibility of the LICENSEE to care for integrating updates. The object code (class files, jar files, or equivalent) resulting from compiling the (modified) source code may be redistributed with the IAIK-Crypto Software based Application, but has to be obfuscated at a level comparable to the original IAIK Software. Redistribution of the (original or modified) source code is NOT permitted! In case of termination, the LICENSEE must destroy all copies of the source code.

### **3. LIMITATIONS for all LICENCES:**

LICENSEES must not attempt to reverse engineer, decompile, disassemble, reverse translate or in any other manner decode the computer programs in the IAIK toolkit in order to derive the source code from there, other than in cases where the LICENSEE has requested Stiftung SIC in writing to urgently supply interface information needed and has not received this information within four weeks.

#### **ATTENTION:**

THIS LICENSE AGREEMENT DOES NOT INCLUDE LICENSING OF THE INCLUDED ALGORITHMS, when appropriate. Please see [http://jce.iaik.tugraz.at/sic/sales/patent\\_issues\\_algorithms](http://jce.iaik.tugraz.at/sic/sales/patent_issues_algorithms) for a summary of the license/patent status situation of algorithms used in IAIK-JCE. It is the sole responsibility of the licensees to ensure the legality of using the IAIK crypto software in their countries. Stiftung SIC declares that to the best of its knowledge all parts of the IAIK-Toolkits have been developed by Austrian citizens, except for the HTTP implementation (w3c\_http.jar) delivered with the iSaSilk distribution and free third party libraries (like Apache Xalan or Xerces) that may be delivered with the toolkits for convenience. The implementation of the Camellia cipher algorithm core has been provided by NTT (Nippon Telegraph and Telephone Corporation), the core of the optional native AES-NI part has been provided by Intel® Corporation (see [ThirdPartyLicenses.pdf](#) for more information).

### **4. TERMS of LICENSE:**

Upon receipt of order and payment, Stiftung SIC will ship the SOFTWARE to the LICENSEE. The licence allows free downloads of new updates, starting at the time of shipment and for the total period of one year, unless terminated earlier, as specified later in this agreement. The LICENSEE has the right to receive free updates or new versions of the SOFTWARE for one year and may use the versions received within that year and the related server or runtime licenses for an unlimited time. Upon payment the download period of purchased licenses, i.e. developer licenses and related runtime and server licenses, may be prolonged annually thereafter. Following termination of the download period, the LICENSEE may continue using the software provided, but will not get patches or new versions. If the LICENSEE has not purchased an unlimited number of runtime and server licences, the conditions stated in article 2 (concerning runtime licences) and article 13 (concerning audit rights) remain valid beyond the terms of this agreement.

### **5. PRICES and PAYMENT:**

The LICENSEE shall pay Stiftung SIC for the Licences acquired at the agreed price or as stated in our Price List. All prices are understood to be ex-works Graz and duty unpaid. Invoices have to be paid net within 30 days of date of invoice. Payments overdue shall be charged subsequently with past due interest of 1.25% per month, as of the first day of their falling overdue. Prices are subject to change without notice.

### **6. DELIVERY:**

For non-EU LICENSEES - except of Australia, Canada, Japan, New Zealand, Norway, Switzerland, United States of America (for those the general export authorisation No. EU001 is valid). Conditions and requirements for use of this authorisation are:

1. This general export authorisation EU001 may not be used if the exporter has been informed by the competent authorities of the Member State in which he is established that the items in question are or may be intended, in their entirety or in part, for use in connection with the development, production, handling, operation, maintenance, storage, detection, identification or dissemination of chemical, biological or nuclear weapons or other nuclear explosive devices or the development, production, maintenance or storage of missiles capable of delivering such weapons, or if the exporter is aware that the items in question are intended for such use.

2. This general authorisation may not be used if the exporter has been informed by the competent authorities of the Member State in which he is established that the items in question are or may be intended for a military end-use as defined in Article 4(2) of the Regulation in a country subject to an EU, OSCE or UN arms embargo, or if the exporter is aware that the items in question are intended for such use.

3. This general authorisation may not be used when the relevant items are exported to a customs free zone or free warehouse which is located in a destination covered by this authorisation. Stiftung SIC must acquire an individual export license. LICENSEES must provide Stiftung SIC with all information necessary to acquire such an individual export license and Stiftung SIC will do everything in its power for not delaying this process. Either the LICENSEES can download the ordered software or Stiftung SIC will ship one copy of the ordered Software to the LICENSEE on CD-ROM within 30 days of receipt of an order based on this Agreement. Costs for shipment will be charged to LICENSEE. For international orders, the LICENSEE may have to pay additional duties or taxes according to his country's practices. If the LICENSEE refuses to accept the package because of country-specific duties or taxes, the credit card will still be charged the shipping costs plus a 20% restoring fee. Please note that shipments must have a street address. Freight cannot be delivered to a P.O. box.

#### **7. INSPECTION:**

By ordering, the LICENSEE confirms that he has tested the SOFTWARE as downloaded from the INTERNET and has found it to be suitable for his needs. The LICENSEE acknowledges that the SOFTWARE is not built for usage in hazardous environments.

#### **8. WARRANTY:**

Stiftung SIC guarantees that the SOFTWARE is free of any computer virus or other malicious hidden routines that would intentionally cause damage to or corrupt data, storage media or equipment. For proving the integrity of the SOFTWARE, Stiftung SIC may calculate a SHA-1 hash value over the distribution file and publish it on its web site. It is the duty of the LICENSEE to verify this hash value. If the hash value cannot be verified, Stiftung SIC declines any warranties on that software, and the licensee should immediately (or within 30 days of delivery at the latest), contact Stiftung SIC for verification and reshipment.

The SOFTWARE is provided "as is" and except for the declaration and warranty stated in this Section, Stiftung SIC makes no representations, conditions or warranties, either express or implied, relative to the IAIK-Toolkit or services provided hereunder, including all implied conditions or warranties of merchantability and fitness for a particular purpose and all conditions with respect to intellectual property infringement. Stiftung SIC may, but shall not be obliged to, fix errors in any IAIK-Toolkit.

#### **9. PROPRIETARY INFORMATION and CONFIDENTIALITY:**

The LICENSEE acknowledges that the SOFTWARE remains the property of, and is confidential to, Stiftung SIC and incorporates trade secrets of Stiftung SIC, and that Stiftung SIC shall have the exclusive right to any copyrights or patents in respect of the SOFTWARE. The LICENSEE agrees to maintain the confidentiality of the SOFTWARE.

The LICENSEE further agrees that (with the exception of paragraph 2 above), he shall not make any disclosure of the SOFTWARE (including copies thereof or methods or concepts utilised therein) to any person or entity, other than employees of the LICENSEE, to whom such disclosure is necessary in order to use the SOFTWARE as provided herein. The LICENSEE shall appropriately notify each employee to whom any such disclosure is made. Such disclosure must be made in confidence and shall be kept in confidence by the employee in question.

The LICENSEE agrees to use diligent and determined efforts to secure and protect the SOFTWARE and copies thereof in a manner consistent with their proprietary character and the maintenance of LICENSOR`s rights therein, and without limitation thereof, to take appropriate action, by instruction or agreement with its employees who are permitted access to the SOFTWARE or copies thereof, or otherwise, to satisfy its obligations as hereby stated.

#### **10. TERMINATION:**

Stiftung SIC may terminate this Agreement without prior notice, if the LICENSEE 1. neglects or fails to perform or observe, or correct a breach of its obligations to Stiftung SIC; 2. goes out of business, files a bankruptcy petition or has such a petition filed involuntarily against it or becomes insolvent; 3. develops, sells, licenses or distributes or attempts to develop, sell, license or distribute any software based on the IAIK-Toolkit which is outside the scope of the limited rights granted herein, to any third party. In the event of such a termination, the LICENSEE shall immediately return the original of the SOFTWARE to Stiftung SIC and destroy all copies. If the SOFTWARE has been delivered electronically, the LICENSEE shall delete all electronic versions from his systems and ensure that all backup copies are destroyed as well.

#### **11. LIABILITY:**

To the maximum extent allowed by applicable law Stiftung SIC shall not be liable for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or other pecuniary loss) arising out of the use of or inability to use the IAIK-Toolkit, even if Stiftung SIC has been advised of the possibility of such damages.

#### **12. EXPORT RESTRICTIONS:**

In some countries, the IAIK-Toolkits may be subject to export and import restrictions. Their re-export may require the approval of the competent authorities. The LICENSEE shall be liable for the observance of any control regulation and explicitly agrees to hold Stiftung SIC fully harmless.

#### **13. AUDIT RIGHTS:**

The LICENSEE has to keep records regarding the number of copies of each IAIK-Toolkit made and/or in use, as well as of runtime licences distributed to his customers. A suitable person selected by Stiftung SIC may inspect these records in the name of Stiftung SIC to verify these figures. Such inspections will be made only upon reasonable notice, during normal business hours and no more often than once a year.

#### **14. WAIVER:**

Invalidity, on legal grounds, of any term of this Agreement does not render the Agreement as a whole invalid.

#### **15. SURVIVAL:**

Irrespective of expiration or termination of this Agreement, the provisions of Articles 2, 4, 5, 10, 13 shall survive the termination or the expiry of this Agreement.

**16. GOVERNING LAW, ARBITRATION:**

This Agreement is governed by Austrian law.

**17. ASSIGNMENT:**

The LICENSEE shall not assign this Agreement without the prior written consent of Stiftung SIC.