

Quantum Protect Open-Source Licenses

Imprint

Copyright 2025	Utimaco IS GmbH Germanusstr. 4 D-52080 Aachen, Germany
Phone	AMERICAS: +1-844-UTIMACO (+1 844-884-6226) EMEA: +49 800-627-3081 APAC: +81 800-919-1301
Internet	https://support.utimaco.com
Email	support@utimaco.com
Document version	1.0.0
Date	2025-03-17
Status	Final
Document No.	n/a
Author	Utimaco
All Rights reserved	<p>No part of this documentation may be reproduced in any form (printing, photocopy or according to any other process) without the written approval of Utimaco IS GmbH or be processed, reproduced or distributed using electronic systems.</p> <p>Utimaco IS GmbH reserves the right to modify or amend the documentation at any time without prior notice. Utimaco IS GmbH assumes no liability for typographical errors and damages incurred due to them. Any mention of the company name Utimaco in this document refers to the Utimaco IS GmbH.</p> <p>All trademarks and registered trademarks are the property of their respective owners.</p>

Contents

Introduction.....	3
License Text	3
LMS/HSS	3
XMSS / XMSS-MT	3
Crystals-Dilithium.....	4
Crystals-Kyber	4

Introduction

The Utimaco QuantumProtect package is using some Open-Source components. This document lists the Open-Source components, their type of use and includes the license text.

License Text

LMS/HSS

Source: <https://github.com/cisco/hash-sigs>

Copyright (c) 2017 Cisco Systems, Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the Cisco Systems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

XMSS / XMSS-MT

Source: <https://github.com/XMSS/xmss-reference>

This reference implementation was written by Andreas Hülsing and Joost Rijneveld. All included code is available under the CC0 1.0 Universal Public Domain Dedication.

Crystals-Dilithium

Source: <https://github.com/pq-crystals/dilithium>

Public Domain (<https://creativecommons.org/share-your-work/public-domain/cc0/>);
or Apache 2.0 License (<https://www.apache.org/licenses/LICENSE-2.0.html>).

For Keccak and the random number generator we are using public-domain code from sources
and by authors listed in comments on top of the respective files.

Crystals-Kyber

Source: <https://github.com/pq-crystals/kyber>

Public Domain (<https://creativecommons.org/share-your-work/public-domain/cc0/>);
or Apache 2.0 License (<https://www.apache.org/licenses/LICENSE-2.0.html>).

For Keccak and the random number generator we are using public-domain code from sources
and by authors listed in comments on top of the respective files.