

Compliant Cryptography in Quest vWorkspace – *MokaFive Suite*

© 2011 Quest Software, Inc.
ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software, Inc.

The information in this document is provided in connection with Quest products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest products. EXCEPT AS SET FORTH IN QUEST'S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software World Headquarters
LEGAL Dept
5 Polaris Way
Aliso Viejo, CA 92656
email: legal@quest.com

Refer to our Web site (www.quest.com) for regional and international office information.

Trademarks

Quest, Quest Software, the Quest Software logo, Imceda are trademarks and registered trademarks of Quest Software, Inc in the United States of America and other countries. For a complete list of Quest Software's trademarks, please see <http://www.quest.com/legal/trademark-information.aspx>. Other trademarks and registered trademarks are property of their respective owners.

June 14, 2011

Contents

Contents.....	3
Compliant Cryptography in Quest vWorkspace – <i>MokaFive Suite</i>	4
Executive Overview	4
About Quest vWorkspace – <i>MokaFive Suite</i>	4
Background on NIST’s Cryptographic Algorithm Validation Program	4
Data Protection and CAVP Certification	4
Summary	5
References	5
Disclaimer.....	5

Compliant Cryptography in Quest vWorkspace – *MokaFive Suite*

Executive Overview

This document describes the use of a NIST (National Institute of Standards and Technology) compliant cryptographic algorithms by Quest Software's Quest vWorkspace – *MokaFive Suite* product.

About Quest vWorkspace – *MokaFive Suite*

Not all employees have the same desktop and application requirements. Some need multiple applications to perform their job function; others may only need access to a small number of critical applications. Mobile computing or work-from-home access may be necessary for a remote workforce, and developers rely on huge amounts of computing power to run test analyses or crunch statistics. If you have a diverse workforce with varying workspace needs, no one virtualization technology is a “best fit” for your entire workforce.

Quest Software and MokaFive have teamed up to provide a desktop virtualization solution that enables customers to securely, centrally and affordably deliver Windows desktops and applications to employees in different roles, using the appropriate technology.

This solution enables desk-bound task workers to click into hosted sessions, office workers to log onto their personalized VDI sessions, as well as provides a virtual desktop to mobile executives and home workers.

Background on NIST's Cryptographic Algorithm Validation Program

In July 1995, NIST and the Communications Security Establishment Canada (CSEC) established the Cryptographic Algorithm Validation Program (CAVP). This program focuses on validation testing for NIST recommended, and FIPS approved, cryptographic algorithms. Vendors interested in validating the cryptographic implementations used within their products may select an accredited laboratory to conduct testing of these implementations. Upon successful completion of the testing, vendors get listed on NIST's validation list(s) on their website.

Quest vWorkspace – *MokaFive Suite* has made it a priority to use cryptographic implementations (algorithms and libraries) that have been successfully tested and certified under CAVP.

Data Protection and CAVP Certification

If encryption is enabled for a user, Quest vWorkspace – *MokaFive Suite* will encrypt all LivePC images (the locally hosted virtual machine) using AES (Advanced Encryption Standard) algorithm in CBC (cipher block chaining) mode. The administrator can, via a policy, choose the length of the AES keys (128- or 256-bits). A different initialization vector (IV) is used for each block of encrypted data. In addition, a level of tamper protection is provided for each block of data, such as to provide for data integrity and to prevent a replacement attack of blocks. A message authentication code (MAC) is computed based on the combination of the block's (unencrypted) data and certain other identifiers, using either SHA256 or SHA 512 as the digest algorithm.

Quest vWorkspace – *MokaFive Suite* uses the cryptographic Crypto++ software library. Each of the cryptographic algorithms referred to above, including AES, SHA256 and SHA512, are on the list of FIPS 140-2 approved cryptographic algorithms. Their implementations within the Crypto++ library have been validated and certified under CAVP. The URLs to their CAVP certificates are listed in the *References* section at the end of this document.

Summary

Quest vWorkspace – *MokaFive Suite* complies with CAVP by utilizing certified cryptographic implementations (algorithms and software library) that have been tested and certified under CAVP.

References

CAVP Homepage

<http://csrc.nist.gov/groups/STM/cavp/>

Crypto++ Homepage

<http://www.cryptopp.com>

CAVP Certificate for the AES implementation in Crypto++

<http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html#499>

CAVP Certificate for the SHA256 and SHA512 implementations in Crypto++

<http://csrc.nist.gov/groups/STM/cavp/documents/shs/shaval.htm#569>

Disclaimer

While efforts have been made by Quest to ensure that the information provided in this document is accurate, Quest makes no representation about the content and suitability of this information for any purpose. This information may be modified by Quest at any time. Nothing contained herein shall be construed as a warranty, express or implied, regarding the operation of Quest's products.