ASTRO® 25
INTEGRATED VOICE AND DATA

KVL 400
KEY VARIABLE LOADER
ADVANCED SECURENET
USER GUIDE

January 2013

6871018P35-F

Copyrights

Disclaimer

Please note that certain features, facilities, and capabilities described in this document may not be applicable to or licensed for use on a particular system, or may be dependent upon the characteristics of a particular mobile subscriber unit or configuration of certain parameters. Please refer to your Motorola contact for further information.

Trademarks

European Union (EU) Waste of Electrical and Electronic Equipment (WEEE) directive

The European Union's WEEE directive requires that products sold into EU countries must have the crossed out trash bin label on the product (or the package in some cases).

As defined by the WEEE directive, this cross-out trash bin label means that customers and end-users in EU countries should not dispose of electronic and electrical equipment or accessories in household waste.

Customers or end-users in EU countries should contact their local equipment supplier representative or service centre for information about the waste collection system in their country.

Document History

Version	Description	Date
6871018P35-A	Original release of the *KVL 4000 Key Variable Loader Advanced SECURENET User Guide*	May 2010
6871018P35-B	Updated as follows: • Added the following sections: – "Performing the OS Hardening" – "Unlocking the Operator Account" – "Setting the PDA USB Mode" – "KVL 4000 Disaster Recovery" – "Radio Frequency Interference Requirements - European Union - EMC Directive 2004/108/EC" • Updated Figure 1-11 KVL 4000 - Charging. • Updated to include the Radio Authentication operating mode.	November 2010
6871018P35-C	Updated as follows: • Changed "Motorola, Inc." to "Motorola Solutions, Inc." • Changed document layout.	July 2011
6871018P35-D	Added/updated the following sections: • "MOTOROLA SOLUTIONS, INC. END USER LICENSE AGREEMENT" • "PUBLICLY AVAILABLE SOFTWARE LIST – KVL SOFTWARE INSTALLATION WIZARD" • "PUBLICLY AVAILABLE SOFTWARE LIST – PDA" • "Personal Digital Assistant" • "Applying Enhanced Security Settings Through the KVL Software Installation Wizard" • "Applying Transparent Security Settings Through the KVL Software Installation Wizard" • "Connecting the KVL to a Radio or Another Target Device" • "Launching the KVL Application" • "Setting Up Passwords on the KVL"	March 2012

Version	Description	Date
	• "Selecting the Password Masking Mode" • "Managing Encryption Keys" • "Loading Keys into Target Devices" • "KVL 4000 Disaster Recovery" • "Troubleshooting KVL Application and/or VPN Software Failure" • "Motorola System Support Center and Radio Support Center" • "North America Parts Organization" • "KVL 4000 – Orderable Parts" Updated the following figures: • Figure 1-1 KVL 4000 Key Variable Loader • Figure 1-2 Personal Digital Assistant (PDA) • Figure 1-12 Today Screen	
6871018P35-E	Updated the following sections: • "Personal Digital Assistant" • "Applying Enhanced Security Settings Through the KVL Software Installation Wizard" • "Applying Transparent Security Settings Through the KVL Software Installation Wizard" • "Launching the KVL Application" • "Exiting the KVL Application" • "Entering the User-Defined System Key" • "Changing the User-Defined System Key" • "Setting Up the KVL to Use the Default System Key" • "Setting the PDA USB Mode" Updated the following figures: • Figure 1-2 Personal Digital Assistant (PDA) • Figure 1-11 Today Screen	November 2012
6871018P35-F	Updated the following sections: • "Applying Enhanced Security Settings Through the KVL Software Installation Wizard"	January 2013

Version	Description	Date
	• “Applying Transparent Security Settings Through the KVL Software Installation Wizard” • “Exiting the KVL Application”	

Contents

List of Figures

List of Tables

List of Procedures

About the KVL 4000 Key Variable Loader Advanced SECURENET User Guide

This manual provides step-by-step instructions for using the Key Variable Loader (KVL) to create and store encryption keys, and then load them into other Motorola secure equipment, such as radios, fixed encryption units, digital interface units (DIUs), and others.

This manual is intended for use by experienced technicians familiar with similar types of equipment. Technicians should understand encryption concepts and be familiar with other types of Motorola encryption equipment.

Depending on the options ordered, the KVL has the capability of being configured to operate in the Advanced SECURENET® (ASN) mode, ASTRO® 25, and/or Radio Authentication mode. The KVL menu system, functionality, and operating characteristics are different depending which operating mode is active.

This manual describes the Advanced SECURENET® operating mode.

IMPORTANT

The Advanced SECURENET® operating mode only supports Physical ID (PID) based key management.

What Is Covered in This Manual?

This manual consists of the following chapters:

- Chapter 1 Introduction
- Chapter 2 KVL 4000 – Performing Initial Programming
- Chapter 3 Managing Encryption Keys
- Chapter 4 Loading Keys into Target Devices
- Chapter 5 Managing Keys in Target Devices
- Chapter 6 Sharing Keys Between KVLs
- Chapter 7 Managing Log Records
- Chapter 8 Converting Encryption Keys
- Chapter 9 Troubleshooting

Helpful Background Information

Motorola offers various courses designed to assist in learning about the system. For information, go to http://www.motorolasolutions.com/training to view the current course offerings and technology paths.

Related Information

Refer to the following documents for associated information:

Related Information	Purpose
Standards and Guidelines for Communication Sites	Provides standards and guidelines that should be followed when setting up a Motorola communications site. Also known as R56 manual. This may be purchased on CD 9880384V83, by calling the North America Parts Organization at 800-422-4210 (or the international number: 302-444-9842).
System Documentation Overview	For an overview of the ASTRO® 25 system documentation, open the graphical user interface for the ASTRO® 25 system documentation set and select the **System Documentation Overview** link. This opens a file that includes: • ASTRO® 25 system release documentation descriptions • ASTRO® 25 system diagrams • ASTRO® 25 system glossary For an additional overview of the system, review the architecture and descriptive information in the manuals that apply to your system configuration.
MC55 Enterprise Digital Assistant User Guide (72E-108859)	Describes how to use the MC55 EDA.
MC55 Quick Start Guide (72-127603)	Describes how to get the MC55 EDA up and running.
KVL 4000 Quick Start Guide	Provides basic information on the KVL 4000.
KVL 4000 Key Variable Loader ASTRO 25 User Guide	Provides step-by-step instructions for using the Key Variable Loader (KVL) to create and store encryption keys, and then load them into other Motorola secure equipment, such as radios, fixed encryption units, digital interface units (DIUs), and others. This manual describes the ASTRO® 25 mode of operation.
KVL 4000 Key Variable Loader Radio Authentication User Guide	Provides step-by-step instructions for using the Key Variable Loader (KVL) to create and store authentication keys, and then load them into Motorola radios.
KVL 4000 FLASHPort Upgrade User Guide	Provides instructions for upgrading the Key Variable Loader (KVL), radios, and other target devices. It also provides instructions for applying security settings on the KVL, installing and activating VPN software, as well as provides troubleshooting information.
KVL 3000 Plus Key Variable Loader User's Guide (6881132E29)	Provides information for the KVL 3000 Plus Key Variable Loader.

MOTOROLA SOLUTIONS, INC. END USER LICENSE AGREEMENT

Motorola Solutions, Inc. (“Motorola”) is willing to license the Motorola PDA and Security Adapter Software and the accompanying documentation to you (“Licensee” or “you”) for use with a Motorola KVL4000 only on the condition that you accept all the terms in this End User License Agreement (“Agreement”).

IMPORTANT: READ THE FOLLOWING TERMS AND CONDITIONS BEFORE USING THE ACCOMPANYING PRODUCT.

IF YOU DO NOT AGREE TO THIS AGREEMENT, DO NOT USE THE SOFTWARE OR COPY THE SOFTWARE, INSTEAD, YOU MAY, FOR A FULL REFUND, RETURN THIS PRODUCT TO THE LOCATION WHERE YOU ACQUIRED IT OR PROVIDE WRITTEN VERIFICATION OF DELETION OF ALL COPIES OF THE SOFTWARE. ANY USE OF THE SOFTWARE, INCLUDING BUT NOT LIMITED TO USE ON A KVL 4000 THAT INCLUDES MOTOROLA PDA AND SECURITY ADAPTER, WILL CONSTITUTE YOUR AGREEMENT TO THIS END USER LICENSE AGREEMENT.

1. Definitions

In this Agreement, the word “Software” refers to the set of instructions for computers, in executable form and in any media, (which may include diskette, CD-ROM, downloadable internet, hardware, or firmware) licensed to you. The word “Documentation” refers to electronic or printed manuals and accompanying instructional aids licensed to you. The word “Product” refers to the specific combination of Software and Documentation that you have licensed and which has been provided to you under this Agreement.

2. Grant of License

Motorola grants you a personal, non-exclusive, non-assignable, nontransferable license to use the Products subject to the Conditions of Use set forth in Section 2 and the terms and conditions of this Agreement. Any terms or conditions appearing on the face or reverse side of any purchase order, purchase order acknowledgment or other order document that are different from, or in addition to, the terms of this Agreement will not be binding on the parties, even if payment is accepted.

3. Conditions of Use

Any use of the Products outside of the conditions set forth in this Agreement is strictly prohibited and will be deemed a breach of this Agreement.

3.1 Only you, your employees or agents may use the Products. You will take all necessary steps to insure that your employees and agents abide by the terms of this Agreement.

3.2 You will use the Products: (i) only for your internal business purposes; (ii) only as described in the Products; and (iii) in strict accordance with this Agreement.

3.3 You may install and use the Products on a single Motorola PDA and KVL 4000 security adapter, provided that the use is in conformance with the terms set forth in this Agreement.

3.4 Portions of the Products are protected by United States copyright laws, international treaty provisions, and other applicable laws. Therefore, you must treat the Products like any other copyrighted material (e.g., a book or musical recording) except that you may either: (i) make 1 copy of the transportable part of the Products (which typically is supplied on diskette, CD-ROM, or downloadable internet), solely for back-up purposes; or (ii) copy the

transportable part of the Products to a PC hard disk, provided you keep the original solely for back-up purposes. If the Documentation is in printed form, it may not be copied. If the Documentation is in electronic form, you may print out 1 copy, which then may not be copied. With regard to the copy made for backup or archival purposes, you agree to reproduce any Motorola copyright notice, and other proprietary legends appearing thereon. Such copyright notice(s) may appear in any of several forms, including machine-readable form, and you agree to reproduce such notice in each form in which it appears, to the extent it is physically possible to do so. Unauthorized duplication of the Software or Documentation constitutes copyright infringement, and in the United States is punishable in federal court by fine and imprisonment.

3.5 You will not transfer, directly or indirectly, any product, technical data or software to any country for which the United States Government requires an export license or other governmental approval without first obtaining such license or approval.

4. Title; Restrictions

If you transfer possession of any copy of the Products to another party outside of the terms of this agreement, your license is automatically terminated. Title and copyrights to the Products and any copies made by you remain with Motorola and its licensors. You will not, and will not permit others to: (i) modify, translate, decompile, bootleg, reverse engineer, disassemble, or extract the inner workings of the Software or Documentation, (ii) copy the look-and-feel or functionality of the Software or Documentation; (iii) remove any proprietary notices, marks, labels, or logos from the Software or Documentation; (iv) rent or transfer all or some of the Software or Documentation to any other party without Motorola's prior written consent; or (v) utilize any computer software or hardware which is designed to defeat any copy protection device, should the Products be equipped with such a protection device. If the Products are provided on multiple types of media (such as diskette, CD-ROM, downloadable internet), then you will only use the medium which best meets your specific needs, and will not loan, rent, lease, or transfer the other media contained in the package without Motorola's written consent. Unauthorized copying of the Software or Documentation, or failure to comply with any of the provisions of this Agreement, will result in automatic termination of this license.

5. Confidentiality

You acknowledge that all Products contain valuable proprietary information and trade secrets and that unauthorized or improper use of the Products will result in irreparable harm to Motorola for which monetary damages would be inadequate and for which Motorola will be entitled to immediate injunctive relief. Accordingly, you will limit access to the Products to those of your employees and agents who need to use the Products for your internal business purposes, and you will take appropriate action with those employees and agents to preserve the confidentiality of the Products, using the same degree of care to avoid unauthorized or improper disclosure as you use for the protection of your own proprietary software, but in no event less than reasonable care.

You have no obligation to preserve the confidentiality of any proprietary information that: (i) was in the public domain at the time of disclosure; (ii) entered the public domain through no fault of yours; (iii) was given to you free of any obligation to keep it confidential; (iv) is independently developed by you; or (v) is disclosed as required by law provided that you notify Motorola prior to such disclosure and provide Motorola with a reasonable opportunity to respond.

6. Right to Use Motorola's Name

Except as required in Section 3.4 above, you will not, during the term of this Agreement or thereafter, use any trademark of Motorola, or any word or symbol likely to be confused with any Motorola trademark, either alone or in any combination with another word or words.

7. Payment

The rights granted hereunder are contingent upon payment for the Product. All payments are due next 30 days from the date of the invoice.

8. Transfer

In the case of Software designed to operate on Motorola equipment, you may not transfer the Software to another party except: (i) if you are an end-user, when you are transferring the Software together with the Motorola equipment on which it operates; or (ii) if you are a Motorola licensed distributor, when you are transferring the Software either together with such Motorola equipment or are transferring the Software as a licensed duly paid for upgrade, update, patch, new release, enhancement or replacement of a prior version of the Software. If you are a Motorola licensed distributor, when you are transferring the Software permitted in this Agreement, you agree to transfer the Software with a license agreement having terms and conditions no less restrictive than those contained in this Agreement. All such transfers of Software are strictly subject to the conditions precedent that the other party agrees to accept the terms and conditions of this License, and you destroy and copy of the Software you do not transfer to that party. You may not sublicense or otherwise transfer, rent or lease the Software without Motorola's written consent. You may not transfer the Software in violation of any laws, regulations, export controls or economic sanctions imposed by the U.S. Government.

9. Upgrades and Updates

If the Products are licensed to you as an upgrade or update to a product previously licensed to you, you must destroy the Products previously licensed to you, including any copies, within 30 days of your receipt of the update or upgrade.

10. Maintenance and Support

Motorola is not responsible for maintenance or support of the Software under this Agreement. By accepting the license granted under this Agreement, you agree that Motorola will be under no obligation to provide any support, maintenance or service in connection with the Software. Any maintenance and support of the Software and equipment on which it resides will be provided under the terms of a separate agreement.

11. Limited Warranty

All diskettes or CD-ROMS on which the Products are furnished (“Media”) are warranted to be free from manufacturing and material defects for 90 days after the shipment date of the Products to you. Media that becomes defective during such period will be repaired or, at Motorola's option, replaced. This limited warranty is contingent upon proper use of the Media and does not cover Products which have been tampered with, modified, or subjected to unusual physical or electrical stress. Tampering with or removal of any factory seal or label on any Media voids this warranty and releases Motorola from any and all liability.

12. Disclaimer

EXCEPT FOR THE ABOVE EXPRESS LIMITED WARRANTY, MOTOROLA DISCLAIMS ALL WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, OR IN ANY COMMUNICATION WITH YOU. MOTOROLA SPECIFICALLY DISCLAIMS ANY WARRANTY INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILTY, NONINFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE. THE PRODUCTS ARE PROVIDED “AS IS”. MOTOROLA DOES NOT WARRANT THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS, OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR FREE, OR THAT DEFECTS IN THE SOFTWARE WILL BE CORRECTED. MOTOROLA MAKES NO WARRANTY WITH RESPECT TO THE CORRECTNESS, ACCURACY, OR RELIABILITY OF THE SOFTWARE AND DOCUMENTATION. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

13. Remedies

The entire liability of Motorola, and your exclusive remedy under the warranty provided in this Agreement will be, at Motorola's option, to repair or replace any Media found to be defective within the warranty period, or to refund the purchase price and terminate this Agreement. To seek such a remedy, you must return the entire Product to Motorola, with a copy of the original purchase receipt, within the warranty period.

14. Limitation of Liability

THE TOTAL LIABILITY OF MOTOROLA UNDER THIS AGREEMENT FOR DAMAGES WILL NOT EXCEED THE TOTAL AMOUNT PAID BY YOU FOR THE PRODUCT LICENSED UNDER THIS AGREEMENT. IN NO EVENT WILL MOTOROLA OR ANY OF THE LICENSORS BE LIABLE IN ANY WAY FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL OR PUNITIVE DAMAGES OF ANY NATURE, INCLUDING WITHOUT LIMITATION, LOST BUSINESS PROFITS, OR LIABILITY OR INJURY TO THIRD PERSONS, WHETHER FORESEEABLE OR NOT, REGARDLESS OF WHETHER MOTOROLA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE LIMITATIONS IN THIS PARAGRAPH WILL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY. Some jurisdictions do not permit limitations of liability for incidental or consequential damages, so the above exclusions may not apply to you.

15. U.S. Government

If you are acquiring the Product on behalf of any unit or agency of the U.S. Government, the following applies. Use, duplication, or disclosure of the Products is subject to the restrictions set forth in subparagraphs (c) (1) and (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 (JUNE 1987), if applicable, unless being provided to the Department of Defense. If being provided to the Department of Defense, use, duplication, or disclosure of the Products is subject to the restricted rights set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 (OCT 1988), if applicable. Software and Documentation may or may not include a Restricted Rights notice, or other notice referring specifically to the terms and conditions of this Agreement. The terms and conditions of this Agreement will each continue to apply, but only to the extent that such terms and conditions are not inconsistent with the rights provided to you under the aforementioned provisions of the FAR and DFARS, as applicable to the particular procuring agency and procurement transaction.

16. Term of License

Your right to use the Products will terminate immediately without notice upon a breach of this Agreement by you. Within 30 days after termination of this Agreement, you will certify to Motorola in writing that through your best efforts, and to the best of your knowledge, the original and all copies, in whole or in part, in any form, of the Software and all related material and Documentation, have been destroyed, except that, with prior written consent from Motorola, you may retain one copy for archival or backup purposes. You may not sublicense, assign or transfer the license or the Product, except as expressly provided in this Agreement. Any attempt to otherwise sublicense, assign or transfer any of the rights, duties or obligations hereunder is null and void.

17. Governing Law

This Agreement is governed by the laws of the United States of America to the extent that they apply and otherwise by the laws of the State of Illinois.

18. Assignment

This Agreement may not be assigned by you without Motorola's prior written consent.

19. Survival of Provisions

The parties agree that where the context of any provision indicates an intent that it survives the term of this Agreement, then it will survive.

20. Entire Agreement

This Agreement contains the parties' entire agreement regarding your use of the Products and may be amended only in writing signed by both parties, except that Motorola may modify this Agreement as necessary to comply with applicable laws.

21. Third-Party Software

The Software may contain one or more items of Third-Party Software supplied by other third-party suppliers. The terms of this Agreement govern your use of any Third-Party Software UNLESS A SEPARATE THIRD-PARTY SOFTWARE LICENSE IS INCLUDED, IN WHICH CASE YOUR USE OF THE THIRD-PARTY SOFTWARE WILL THEN BE GOVERNED BY THE SEPARATE THIRD-PARTY LICENSE.

22. Open Source Software

The Software may contain one or more items of Open Source or other Publicly Available Software. For information regarding licenses, acknowledgements, required copyright notices, and other usage terms, see Open Source Software Legal Notices, page xxiii.

Open Source Software Legal Notices

This media, or Motorola Solutions Product, may include Motorola Solutions Software, Commercial Third-Party Software, and Publicly Available Software.

The Motorola Solutions Software that may be included on this media, or included in the Motorola Solutions Product, is Copyright (c) by Motorola Solutions, Inc., and its use is subject to the licenses, terms and conditions of the agreement in force between the purchaser of the Motorola Solutions Product and Motorola Solutions, Inc.

The Commercial Third-Party Software that may be included on this media, or included in the Motorola Solutions Product, is subject to the licenses, terms and conditions of the agreement in force between the purchaser of the Motorola Solutions Product and Motorola Solutions, Inc., unless a separate Commercial Third-Party Software License is included, in which case, your use of the Commercial Third-Party Software will then be governed by the separate Commercial Third-Party License.

The Publicly Available Software that may be included on this media, or in the Motorola Solutions Product, is listed below. The use of the listed Publicly Available Software is subject to the licenses, terms and conditions of the agreement in force between the purchaser of the Motorola Solutions Product and Motorola Solutions, Inc., as well as the terms and conditions of the license of each Publicly Available Software package. Copies of the licenses for the listed Publicly Available Software, as well as all attributions, acknowledgements, and software information details, are included below. Motorola Solutions is required to reproduce the software licenses, acknowledgments and copyright notices as provided by the Authors and Owners, thus, all such information is provided in its native language form, without modification or translation.

The Publicly Available Software in the list below is limited to the Publicly Available Software included by Motorola Solutions. The Publicly Available Software included by Commercial Third Party Software or Products, that is used in the Motorola Solutions Product, are disclosed in the Commercial Third-Party Licenses, or via the respective Commercial Third-Party Publicly Available Software Legal Notices.

For instructions on how to obtain a copy of any source code being made publicly available by Motorola Solutions related to software used in this Motorola Solutions Product you may send your request in writing to:

MOTOROLA SOLUTIONS, INC.
Government & Public Safety Business
Publicly Available Software Management
1301 E. Algonquin Road
Schaumburg, IL 60196
USA

In your request, please include the Motorola Solutions Product Name and Version, along with the Publicly Available Software specifics, such as the Publicly Available Software Name and Version.

Note that source code for the Publicly Available Software may be resident on the Motorola Solutions Product Installation Media, or on supplemental Motorola Solutions Product Media. Please reference and review the entire Motorola Solutions Publicly Available Software Legal Notices and End User License Agreement for the details on location and methods of obtaining the source code.

Note that dependent on the license terms of the Publicly Available Software, source code may not be provided. Please reference and review the entire Motorola Solutions Publicly Available Software Legal Notices and End User License Agreement for identifying which Publicly Available Software Packages will have source code provided.

To view additional information regarding licenses, acknowledgments and required copyright notices for Publicly Available Software used in this Motorola Solutions Product, please select “Legal Notices” display from the GUI (if applicable), or review the Legal Notices and End User License Agreement File/README, on the Motorola Solutions Product Install Media, or resident in the Motorola Solutions Product.

PUBLICLY AVAILABLE SOFTWARE LIST – KVL SOFTWARE INSTALLATION WIZARD

Name:	RAPI2
Version:	1.2
Description:	A managed wrapper to access the features exposed by the COM interfaces for the Remote API 2. These classes allow the developer to access information, files, and the registry on a device connected through ActiveSync from desktop applications.
Software Site:	http://rapi2.codeplex.com
Source Code:	No Source Code Distribution Obligations. The Source Code may be obtained from the original Software Site.
License:	MIT Type of License

Copyright (c) 2008 David Hall

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS“, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Credits:	See License

==========

Name:	NLOG
Version:	2.0
Description:	NLog is a logging platform for .NET with rich log routing and management capabilities. It makes it easy to produce and manage high-quality logs for application.
Software Site:	http://nlog.codeplex.com http://nlog-project.org
Source Code:	No Source Code Distribution Obligations. The Source Code may be obtained from the original Software Site.
License:	BSD Type of License

Copyright (c) 2004-2009, Jaroslaw Kowalski
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 Jaroslaw Kowalski 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 OWNER 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.

Credits: See License

PUBLICLY AVAILABLE SOFTWARE LIST – PDA

Name:	NLOG
Version:	2.0
Description:	NLog is a logging platform for .NET with rich log routing and management capabilities. It makes it easy to produce and manage high-quality logs for application.
Software Site:	http://nlog.codeplex.com http://nlog-project.org
Source Code:	No Source Code Distribution Obligations. The Source Code may be obtained from the original Software Site.
License:	BSD Type of License

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 Jaroslaw Kowalski 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 OWNER 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.

Credits: See License

==========

Name:	Smart Device Framework - Community Edition
Version:	2.3.0.39
Description:	Extentions, to the NET Compact Framework core libraries, which enables calls to OS services.
Software Site:	http://www.opennetcf.com/Products/SmartDeviceFramework.aspx
Source Code:	No Source Code Distribution Obligations. The Community Edition of the Smart Device Framework is only provided in Binary form from the Software Authors. Source Code can be obtained via commercially licensing the Software.
License:	OpenNETCF Shared Source License

NOTICE

This license governs use of the accompanying software (“Software”), and your use of the Software constitutes acceptance of this license.

Subject to the restrictions below, you may use the Software for any commercial or noncommercial purpose, including distributing derivative works.

SECTION 1: DEFINITIONS

A. “OpenNETCF” refers to OpenNETCF Consulting, LLC, a limited liability corporation organized and operating under the laws of the state of Maryland.

B. “SDF” refers to the OpenNETCF Smart Device Framework, which is an OpenNETCF software product.

C. “SOFTWARE” refers to the source code, compiled binaries, installation files documentation and any other materials provided by OpenNETCF.

SECTION 2: LICENSE

You agree that:

A. You are NOT allowed to combine or distribute the SOFTWARE with other software that is licensed under terms that seek to require that the SOFTWARE (or any intellectual property in it) be provided in source code form, licensed to others to allow the creation or distribution of derivative works, or distributed without charge.

B. You may NOT distribute the SOFTWARE in source code form to any other person, company, government, group or entity.

C. You may NOT decompile, disassemble, reverse engineer or otherwise attempt to extract, generate or retrieve source code from any compiled binary provided in the SOFTWARE.

D. You will (a) NOT use OpenNETCF's name, logo, or trademarks in association with distribution of the SOFTWARE or derivative works unless otherwise permitted in writing; and (b) you WILL indemnify, hold harmless, and defend OpenNETCF from and against any claims or lawsuits, including attorneys fees, that arise or result from the use or distribution of your modifications to the SOFTWARE and any additional software you distribute along with the SOFTWARE.

E. The SOFTWARE comes “as is”, with no warranties. None whatsoever. This means no express, implied or statutory warranty, including without limitation, warranties of merchantability or fitness for a particular purpose or any warranty of title or non-infringement.

F. Neither OpenNETCF nor its suppliers will be liable for any of those types of damages known as indirect, special, consequential, or incidental related to the SOFTWARE or this license, to the maximum extent the law permits, no matter what legal theory its based on. Also, you must pass this limitation of liability on whenever you distribute the SOFTWARE or derivative works.

G. If you sue anyone over patents that you think may apply to the SOFTWARE for a person's use of the SOFTWARE, your license to the SOFTWARE ends automatically.

H. The patent rights, if any, granted in this license only apply to the SOFTWARE, not to any derivative works you make.

I. The SOFTWARE is subject to U.S. export jurisdiction at the time it is licensed to you, and it may be subject to additional export or import laws in other places. You agree to comply with all such laws and regulations that may apply to the SOFTWARE after delivery of the SOFTWARE to you.

J. If you are an agency of the U.S. Government, (i) the SOFTWARE is provided pursuant to a solicitation issued on or after December 1, 1995, is provided with the commercial license rights set forth in this license, and (ii) the SOFTWARE is provided pursuant to a solicitation issued prior to December 1, 1995, is provided with Restricted Rights as set forth in FAR, 48 C.F.R. 52.227-14 (June 1987) or DFAR, 48 C.F.R. 252.227-7013 (Oct 1988), as applicable.

K. Your rights under this license end automatically if you breach it in any way.

L. This license contains the only rights associated with the SOFTWARE and OpenNETCF reserves all rights not expressly granted to you in this license. © 2006 OpenNETCF Consulting, LLC. All rights reserved.

Credits: See License Above

PUBLICLY AVAILABLE SOFTWARE LIST – SECURITY ADAPTER

Name: Buffer Management Source Code from OpenBSD Operating System, as well as, OpenSSH Project.

Version: N/A

Description: This Package was included by Commercial Third Party Software Development Kit, from WindRiver-Interpeak, within the Motorola Product.

Software Site:	http://www.openbsd.org
License:	The utilized Code is under BSD Type of License

Author: Tatu Ylonen <ylo@cs.hut.fi>
Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland
All rights reserved.
Functions for manipulating fifo buffers (that can grow if needed).

As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible with the protocol description in the RFC file, it must be called by a name other than "ssh" or "Secure Shell".

Copyright (c) 1983, 1990, 1992, 1993, 1995
The Regents of the University of California.
All rights reserved.

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

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. 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.
3. Neither the name of the University 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 REGENTS 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 REGENTS 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.

Credits:	OpenBSD Project, http://www.openbsd.org Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland

==========

Name:	C Support Libraries and Headers
Version:	N/A
Description:	The Packages were included by Commercial Third Party Software Development Kit, from Blunk MicroSystems, within the Motorola Product. Copyright 2009, Blunk Microsystems, ALL RIGHTS RESERVED
Software Site:	http://www.blunkmicro.com

Source Code:	No Source Code Distribution Obligations
License:	The utilized Code is under BSD and MIT Type of Licenses

sccl.c, vscanf.c

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms, and that any documentation related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

xscanf.c

This code is derived from software contributed to Berkeley by Chris Torek.

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

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. 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.
3. Neither the name of the University 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 REGENTS 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 REGENTS 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.

stdint.h

Permission to use, copy, modify, and distribute this software is freely granted, provided that this notice is preserved.

Credits:	N/A

PUBLICLY AVAILABLE SOFTWARE COMMON LICENSES

No Common Licenses included.

Commercial Warranty and Service Limited Warranty

MOTOROLA COMMUNICATION PRODUCTS

I. WHAT THIS WARRANTY COVERS AND FOR HOW LONG:

MOTOROLA SOLUTIONS, INC. (“MOTOROLA”) warrants the MOTOROLA manufactured Communication Products listed below (“Product”) against defects in material and workmanship under normal use and service for a period of time from the date of purchase as scheduled below:

KVL 4000 Key Variable Loader	One (1) Year
Product Accessories	One (1) Year

MOTOROLA, at its option, will at no charge either repair the Product (with new or reconditioned parts), replace it (with a new or reconditioned Product), or refund the purchase price of the Product during the warranty period provided it is returned in accordance with the terms of this warranty. Replaced parts or boards are warranted for the balance of the original applicable warranty period. All replaced parts of Product shall become the property of MOTOROLA.

This express limited warranty is extended by MOTOROLA to the original end user purchaser only and is not assignable or transferable to any other party. This is the complete warranty for the Product manufactured by MOTOROLA. MOTOROLA assumes no obligations or liability for additions or modifications to this warranty unless made in writing and signed by an officer of MOTOROLA. Unless made in a separate agreement between MOTOROLA and the original end user purchaser, MOTOROLA does not warrant the installation, maintenance or service of the Product.

MOTOROLA cannot be responsible in any way for any ancillary equipment not furnished by MOTOROLA which is attached to or used in connection with the Product, or for operation of the Product with any ancillary equipment, and all such equipment is expressly excluded from this warranty. Because each system which may use the Product is unique, MOTOROLA disclaims liability for range, coverage, or operation of the system as a whole under this warranty.

II. GENERAL PROVISIONS:

This warranty sets forth the full extent of MOTOROLA's responsibilities regarding the Product. Repair, replacement or refund of the purchase price, at MOTOROLA's option, is the exclusive remedy.

THIS WARRANTY IS GIVEN IN LIEU OF ALL OTHER EXPRESS WARRANTIES. IMPLIED WARRANTIES, INCLUDING WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ARE LIMITED TO THE DURATION OF THIS LIMITED WARRANTY. IN NO EVENT SHALL MOTOROLA BE LIABLE FOR DAMAGES IN EXCESS OF THE PURCHASE PRICE OF THE PRODUCT, FOR ANY LOSS OF USE, LOSS OF TIME, INCONVENIENCE, COMMERCIAL LOSS, LOST PROFITS OR SAVINGS OR OTHER INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE ORINABILITY TO USE SUCH PRODUCT, TO THE FULL EXTENT SUCH MAY BE DISCLAIMED BY LAW.

III. STATE LAW RIGHTS:

SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES OR LIMITATION ON HOW LONG AN IMPLIED WARRANTY LASTS, SO THE ABOVE LIMITATION OR EXCLUSIONS MAY NOT APPLY.

This warranty gives specific legal rights, and there may be other rights which may vary from state to state.

IV. HOW TO GET WARRANTY SERVICE:

You must provide proof of purchase (bearing the date of purchase and Product item serial number) in order to receive warranty service and, also, deliver or send the Product item, transportation and insurance prepaid, to an authorized warranty service location. Warranty service will be provided by MOTOROLA through one of its authorized warranty service locations. If you first contact the company which sold you the Product (e.g., dealer or communication service provider), it can facilitate your obtaining warranty service. You can also call MOTOROLA at 1-800-927-2744 in the US/Canada.

V. WHAT THIS WARRANTY DOES NOT COVER:

1. Defects or damage resulting from use of the Product in other than its normal, customary or authorized manner.
2. Defects or damage from misuse, accident, water, neglect or act of God.
3. Defects or damage from improper testing, operation, maintenance, installation, alteration, modification, or adjustment not provided or authorized in writing by MOTOROLA.
4. Breakage or damage to antennas unless caused directly by defects in material workmanship.
5. A Product subjected to unauthorized Product modifications, disassembles or repairs (including, without limitation, the addition to the Product of non-MOTOROLA supplied equipment) which adversely affect performance of the Product or interfere with MOTOROLA's normal warranty inspection and testing of the Product to verify any warranty claim.
6. Product which has had the serial number removed or made illegible.
7. Rechargeable batteries if:
   - any of the seals on the battery enclosure of cells are broken or show evidence of tampering.
   - the damage or defect is caused by charging or using the battery in equipment or service other than the Product for which it is specified.
8. Freight costs to the repair depot.
9. A Product which, due to illegal or unauthorized alteration of the software/firmware in the Product, does not function in accordance with MOTOROLA's published specifications or the FCC type acceptance labeling in effect for the Product at the time the Product was initially distributed from MOTOROLA.
10. Scratches or other cosmetic damage to Product surfaces that does not affect the operation of the Product.
11. Normal and customary wear and tear.

VI. PATENT AND SOFTWARE PROVISIONS:

MOTOROLA will defend, at its own expense, any suit brought against the end user purchaser to the extent that it is based on a claim that the Product or parts infringe a United States patent, and MOTOROLA will pay those costs and damages finally awarded against the end user purchaser in any such suit which are attributable to any such claim, but such defense and payments are conditioned on the following:

1. that MOTOROLA will be notified promptly in writing by such purchaser of any notice of such claim;
2. that MOTOROLA will have sole control of the defense of such suit and all negotiations for its settlement or compromise; and
3. should the Product or parts become, or in MOTOROLA's opinion be likely to become, the subject of a claim of infringement of a United States patent, that such purchaser will permit MOTOROLA, at its option and expense, either to procure for such purchaser the right to continue using the Product or parts or to replace or modify the same so that it becomes non-infringing or to grant such purchaser a credit for the Product or parts as depreciated and accept its return. The depreciation will be an equal amount per year over the lifetime of the Product or parts as established by MOTOROLA.

MOTOROLA will have no liability with respect to any claim of patent infringement which is based upon the combination of the Product or parts furnished hereunder with software, apparatus or devices not furnished by MOTOROLA, nor will MOTOROLA have any liability for the use of ancillary equipment or software not furnished by MOTOROLA which is attached to or used in connection with the Product. The foregoing states the entire liability of MOTOROLA with respect to infringement of patents by the Product or any parts thereof.
Laws in the United States and other countries preserve for MOTOROLA certain exclusive rights for copyrighted MOTOROLA software such as the exclusive rights to reproduce in copies and distribute copies of such MOTOROLA software. MOTOROLA software may be used in only the Product in which the software was originally embodied and such software in such Product may not be replaced, copied, distributed, modified in any way, or used to produce any derivative thereof. No other use including, without limitation, alteration, modification, reproduction, distribution, or reverse engineering of such MOTOROLA software or exercise of rights in such MOTOROLA software is permitted. No license is granted by implication, estoppel or otherwise under MOTOROLA patent rights or copyrights.

VII. GOVERNING LAW:

This Warranty is governed by the laws of the State of Illinois, U.S.A.

SERVICE

Proper repair and maintenance procedures will assure efficient operation and long life for this product. A Motorola maintenance agreement will provide expert service to keep this and all other communication equipment in perfect operating condition. A nationwide service organization is provided by Motorola to support maintenance services. Through its maintenance and installation program, Motorola makes available the finest service to those desiring reliable, continuous communications on a contract basis. For a contract service agreement, please contact your nearest Motorola service or sales representative, or an authorized Motorola dealer.

Repair Service Advantage (RSA) Service Agreements is a post-warranty service offering that provides for the repair of this product. The service agreement is renewable annually for as long as Motorola supports the equipment. For more information about RSA Service Agreements, contact the Motorola Radio Support Center at 800-247-2346 or your Customer Support Manager.

1 Introduction

1.1 MC55A0 PDA Reference

See the *MC55 Enterprise Digital Assistant User Guide* (72E-108859) (available at http://www.motorola.com/enterprisemobility/manuals) for the following information:

- Inserting/replacing the battery
- Charging the battery (Security Adapter disconnected)
- Changing the power settings (setting the timeout for turning off the display to conserve battery power)

SUGGESTION

Set up the PDA so that it turns itself off when it is not in use to preserve the KVL 4000 battery life.

- Changing the backlight settings:
  - Setting the display backlight time-out
  - Adjusting brightness
- Setting date and time for timestamping logs
- Turning KVL sounds on/off
- Troubleshooting the MC55
- MC55 performance specifications

1.2 Overview of the KVL 4000

The KVL 4000 Key Variable Loader is a portable, handheld, rugged device whose most basic function is to transfer encryption keys to a target device. Encryption keys can be entered manually by the KVL user, auto-generated by the KVL, or obtained from or shared with another KVL. Keys can be transferred to secure mobile and portable radios, infrastructure devices, and system test equipment.

The KVL 4000 provides a User Interface for entering encryption keys, downloading them from an external source, and transferring them to target devices. It also provides internal processing and memory for secure key storage, as well as interfaces for data communication.

1.2.1 KVL 4000 Components

The KVL 4000 consists of the two main components:

- **Personal Digital Assistant (PDA)**
- **Security Adapter**

Figure 1-1 KVL 4000 Key Variable Loader

1.2.1.1 Personal Digital Assistant

The Personal Digital Assistant (PDA) is the host component of the KVL 4000, responsible for controlling all operations of the device. It is a Motorola rugged handheld computer operating Windows Mobile 6.5. The PDA model used as part of the KVL 4000 is MC55A0.

Figure 1-2 Personal Digital Assistant (PDA)

Table 1-1 PDA Controls and Ports Used in the KVL Operation

Callout Number	Item	Description
1	Charging/Battery Status LED	Blinks when the battery is charging; solid when the battery is charged.
2	Touch screen	Navigate through the UI by tapping or dragging items on the screen.
3	Volume Up Key	Press to turn the volume of the KVL sounds up.
4	Volume Down Key	Press to turn the volume of the KVL sounds down.
5	Action Button	You can use it instead of your finger to initiate an action.
6	End Key	Press to return to the KVL main screen.
7	Side Up Navigation Key	You can use it instead of your finger to scroll up a list.
8	Side Down Navigation Key	You can use it instead of your finger to scroll down a list.
9	Backspace Key	Press to delete digits entered with the PDA keypad.

Table 1-1 PDA Controls and Ports Used in the KVL Operation (cont'd.)

Callout Number	Item	Description
10	Shift Key	Press twice to access and lock capital letters.
11	PDA Keypad	Use it for all cases when alphanumeric text entry is required.
12	Orange Key	Press twice to access and lock the secondary layer of characters.
13	Power Button	Press to power on or suspend the KVL; press and hold for 5 seconds to reboot.
14	I/O Connector	Use to connect the PDA to the Security Adapter or to a PC through the USB Programming Cable.
15	Stylus	You can use it instead of your finger to tap and drag items on the screen.

NOTE

For more information on the PDA, see the *MC55 Enterprise Digital Assistant User Guide* (72E-108859) (available at http://www.motorola.com/enterprisemobility/manuals).

1.2.1.2 Security Adapter

The Security Adapter is an integral component of the KVL 4000, providing secure storage of encryption keys, cryptographic operations, and port access for the KVL 4000.

CAUTION

Always make sure to exit the KVL application on the PDA before disconnecting the Security Adapter. Otherwise, you may lose any unsaved work or cause data corruption.

Figure 1-3 Security Adapter – Ports and Interfaces

Table 1-2 Security Adapter Ports and Interfaces

Number	Item	Description
1	Key load Port	Serves as the interface to all target devices for key loading and upgrade operations.
2	Tricolored LED	Serves as the diagnostic status indicator for the KVL. The available states are: • Momentary Red – before security adapter self tests • Fast Flashing Amber – during security adapter self tests (power up) • Momentary Green – after successful security adapter self tests • Solid Red – fatal error / hardware failure
3	Charging Port	Connect the charger to charge the PDA battery.
4	DB9 Port (RS–232)	Serves as the interface to a PC/Printer for transferring/printing log records.

Table 1-2 Security Adapter Ports and Interfaces (cont'd.)

Number	Item	Description
5	USB Port	Serves as the interface to all expansion adapters used by the KVL.
6	Locking Tabs	Attach the Security Adapter to the PDA and slide the two locking tabs up until they both lock into position.
7	PDA Interface Port	Serves as the interface to any attached host (the primary host for the Security Adapter is the PDA).

1.2.2 KVL 4000 – Key Features

The KVL 4000 offers the following features:

- Manual and automatic generation of encryption keys
- Password protection (Administrator and Operator security levels)
- Secure storage of a total of 1,024 encryption keys (Traffic and Shadow combined)
- Configuration of system- and user-specific settings
- Support of the KVL and Crypto Module upgrades
- Support of the following encryption algorithms:
  - AES-256
  - DES
  - DVI-XL
  - DVP-XL
- Key Management Support for radios that support 12 kbps Advanced SECURENET®
- Support of the following encryption standards:
  - FIPS 46-3
  - FIPS 140-2
  - FIPS 197
- USB, DB9 (RS-232), and Key load Ports
- Sharing encryption keys between two KVLs
- Maintenance of log records of KVL activities

NOTE

The KVL supports any combination of algorithms.

1.2.3 KVL 4000 Sounds

Table 1-3 Sounds Played by the KVL 4000

Sound name	Description
attention	Played for any case when your attention is needed.
bad bonk	Played when you enter an invalid digit when entering a value.
completed	Played when an action or a process (such as loading keys) is completed.
connected	Played when you connect an external device (such as a radio) to the KVL.

For information on how to turn the sounds on or off, see the *MC55 Enterprise Digital Assistant User Guide* (72E-108859) (available at http://www.motorola.com/enterprisemobility/manuals).

1.2.4 Using the KVL 4000

Secure communications systems are designed to provide coded (encrypted) voice and data signals between some or all links in the system (including RF links and network links). In order to do this, each device, such as a radio or fixed encryption unit, is loaded with a multi-digit encryption variable (a key). This key is used by the encryption algorithm, such as AES or DES, built into the device to mathematically encrypt all transmitted voice and data signals, and decode all encrypted received voice and data signals.

Only devices in the system with the same algorithm and encryption key can decode the encrypted signal and carry on communications with each other. Talkgroups can therefore be created by controlling the assignment of encryption keys to specific groups of radios.

1.2.4.1 Types of Keys

The KVL stores two basic types of encryption keys:

- **Traffic Keys** – Used by subscriber units to encrypt/decrypt voice and data communications
- **Shadow Keys** – Used by the KVL to provide an additional level of encryption to the encryption keys

Both types of keys are stored in the KVL memory in an encrypted format and are protected from tampering.

1.2.4.2 Entering and Loading Keys – Overview

Encryption keys are entered into the KVL memory locations (slots). The keys may then be transferred (loaded) to a target device, such as a secure radio.

A two-step process is required for most encryption keys:

- Create (enter) the multi-digit encryption key into the KVL memory. See 3.1 Entering Encryption Keys Manually, page 3-1 or 3.2 Auto-Generating Encryption Keys, page 3-2.

- Connect the KVL to a target device, such as a radio, and transfer the key to the target device. See 1.4.4 Connecting the KVL to a Target Device, page 1-13 and Chapter 4 Loading Keys into Target Devices.

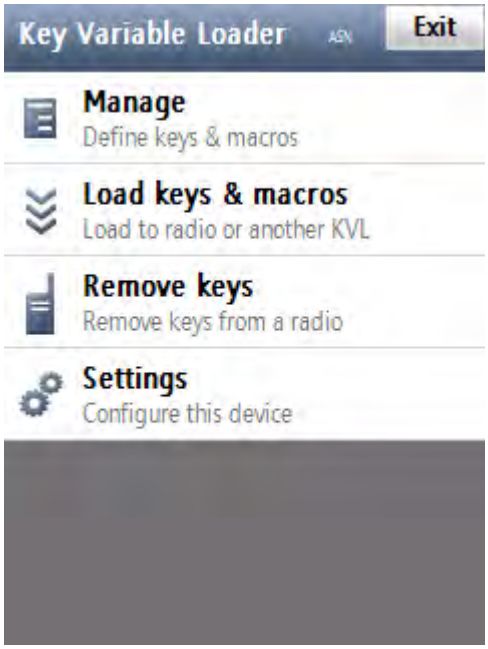
1.3 KVL User Interface

You navigate through the KVL UI and perform operations by:

- Selecting list items, buttons, and tabs
- Entering data
- Dragging sliders
- Scrolling through lists

You can navigate through the KVL UI using your finger. Alternatively, you can use the stylus attached to the side of the PDA, or press hard controls on the PDA.

Figure 1-4 KVL Main Screen



1.4 Getting Started

This section covers the following topics:

1.4.1 Applying Enhanced Security Settings Through the KVL Software Installation Wizard

Prerequisites:

- Ensure that you have the USB Programming Cable.
- For Windows XP, ensure that Microsoft ActiveSync is installed on your PC.
- For Windows Vista and Windows 7, ensure that Microsoft Windows Mobile Device Center is installed on your PC.

When and where to use:
By default, the KVL uses Transparent Security Settings. If required by your organization's policies, follow this procedure to apply Enhanced Security Settings.

NOTE

Applying Enhanced Security Settings causes the KVL to:

- prevent installation and launching of any unsigned applications
- disable the use of wireless modem (Bluetooth and WiFi are disabled)
- require you to set a password on the Operating System

Procedure Steps

1 If the KVL Application software is running, exit or log out of the KVL.

2 Disconnect the Security Adapter from the PDA.

3 Connect the PDA to a PC using the USB Programming Cable.

Figure 1-5 PDA and PC – Connected

Step result: For Windows XP, the ActiveSync application starts. For Windows Vista and Windows 7, the Windows Mobile Device Center starts.

NOTE

If ActiveSync or Windows Mobile Device Center do not start automatically, perform 9.4 Setting the PDA USB Mode, page 9-5 to put the PDA into the **USB Client** or **USB OTG** mode.

4 Insert the CD provided by Motorola and run the Setup.exe file to start the KVL Software Installation Wizard.

Step result: The End User License Agreement screen appears.

5 Click **Accept**.

6 In the window that appears, select the check box next to **Your device is using Transparent Security Settings (default)**, and click **Next**. The Enhanced Security Settings will be applied after the KVL application reinstallation/upgrade.

NOTE

During the process, the PDA may restart several times.

Step result: When the process is completed, a message appears, asking you to configure your device according to the security policy.

7 Check your PDA screen and follow the instructions to renew your password settings.

8 When you have entered and confirmed the password on your PDA, click **OK** on the message on your PC.

Step result: The Enhanced Security Settings are applied successfully.

9 Click **Next** → **Exit** to close the KVL Software Installation Wizard.

10 Disconnect the USB Programming Cable from the PDA.

11 Connect the Security Adapter to the PDA.

NOTE

If the Security Adapter is not detected automatically, perform 9.4 Setting the PDA USB Mode, page 9-5 to put the PDA into the **USB Host** or **USB OTG** mode.

1.4.2 Applying Transparent Security Settings Through the KVL Software Installation Wizard

Prerequisites:

- Ensure that you have the USB Programming Cable.
- For Windows XP, ensure that Microsoft ActiveSync is installed on your PC.
- For Windows Vista and Windows 7, ensure that Microsoft Windows Mobile Device Center is installed on your PC.

Procedure Steps

1 If the KVL Application software is running, exit or log out of the KVL.

2 Disconnect the Security Adapter from the PDA.

3 Connect the PDA to a PC using the USB Programming Cable.

Step result: For Windows XP, the ActiveSync application starts. For Windows Vista and Windows 7, the Windows Mobile Device Center starts.

NOTE

If ActiveSync or Windows Mobile Device Center do not start automatically, perform 9.4 Setting the PDA USB Mode, page 9-5 to put the PDA into the **USB Client** or **USB OTG** mode.

4 Insert the CD provided by Motorola and run the Setup.exe file to start the KVL Software Installation Wizard.

Step result: The End User License Agreement screen appears.

5 Click **Accept**.

6 In the window that appears, clear the check box next to **Your device is using Enhanced Security Settings**, and click **Next**. The Transparent Security Settings will be applied after the KVL application reinstallation/upgrade.

NOTE

During the installation process, the PDA may restart several times.

7 When the process is completed, click **Next** → **Exit** to close the KVL Software Installation Wizard.

Step result: The Transparent Security Settings are applied successfully.

8 Disconnect the USB Programming Cable from the PDA.

9 Connect the Security Adapter to the PDA.

NOTE

If the Security Adapter is not detected automatically, perform 9.4 Setting the PDA USB Mode, page 9-5 to put the PDA into the **USB Host** or **USB OTG** mode.

1.4.3 Connecting the PDA and the Security Adapter

Procedure Steps

1 Connect the PDA and the Security Adapter.

Figure 1-6 PDA and Security Adapter – Connecting

2 To secure the Adapter, slide the locking tabs up fully until a click is felt indicating they are in the locked position. If either slide is not in the locked position, an orange dot is visible.

Figure 1-7 PDA and Security Adapter – Connected

3 If the Security Adapter is not detected automatically after powering on the PDA, perform 9.4 Setting the PDA USB Mode, page 9-5 to put the PDA into the **USB Host** or **USB OTG** mode.

1.4.4 Connecting the KVL to a Target Device

This section covers the following topics:

1.4.4.1 Connecting the KVL to a Radio or Another Target Device

You can load encryption keys into the following devices:

- Secure ASTRO® 25 Single Key Target Radios
- Secure ASTRO® 25 Multiple Key Target Radios
- SECURENET/Advanced SECURENET Mobile Radios
- SECURENET/Advanced SECURENET Portable Radios
- Another KVL unit (see 1.4.4.2 Connecting Two KVL Units, page 1-15)
- Radio Network Controller (RNC)
- Digital Interface Unit (DIU)
- Console Interface Unit (CIU)
- Key Management Center (KMC)

Procedure Steps

1 For information on what cables/adaptors to use with particular target devices, see Table B-5 Interface Cables in B KVL 4000 – Orderable Parts, page B-1.

2 Connect the KVL and the Target Device using an appropriate key load cable and an adaptor (if required).

Figure 1-8 KVL and Radios – Connected (Example)

1.4.4.2 Connecting Two KVL Units

Prerequisites:
Ensure you have the KVL to KVL cable.

Procedure Steps

1 Take the KVL to KVL cable (TKN8209).

2 Connect two KVLs through their key load ports.

Figure 1-9 Two KVL Units – Connected

NOTE

The KVL 4000 is also compatible with the previous models of the KVL.

1.4.5 Charging the KVL 4000

Prerequisites:
Ensure that you have:

- Power Supply
- AC Line Cord (See B KVL 4000 – Orderable Parts, page B-1 for the list of compatible AC Line Cords.)

Procedure Steps

1 Connect one end of the AC Line Cord to the power source.

2 Connect the other end of the AC Line Cord to the power supply.

3 Connect the power supply to the KVL through the Charging Port on the Security Adapter.

Step result: The KVL starts charging. The middle LED on the PDA is blinking to indicate the KVL is being charged. Once the device is fully charged, the LED becomes solid.

Figure 1-10 KVL 4000 - Charging

1.4.6 Launching the KVL Application

Procedure Steps

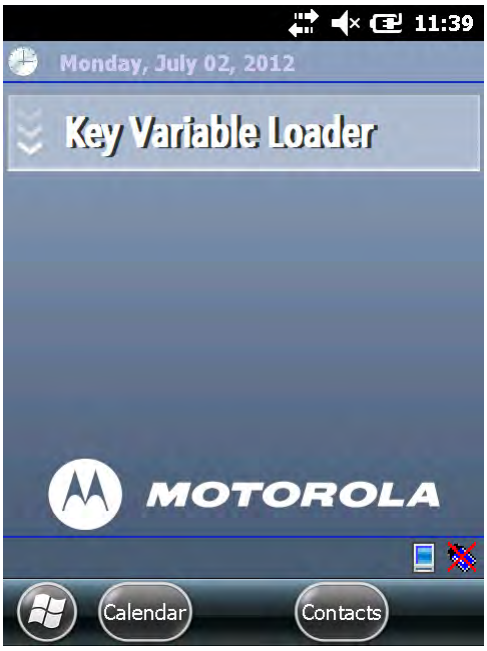
1 If the device is not already powered on, press the **Power** button on the PDA.

NOTE

If you reboot the device, the KVL application launches automatically.

Step result: The KVL powers on and the **Today** screen appears.

Figure 1-11 Today Screen



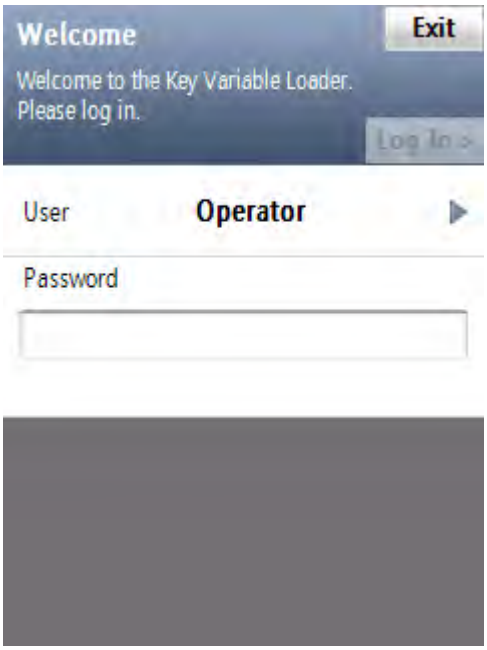
2 Tap the **Key Variable Loader** button.

NOTE

If the PDA and the Security Adapter are not compatible, a notification appears.

Step result: If there are no passwords defined for your KVL, the KVL application launches and the KVL main screen appears. Otherwise, the **Welcome** screen appears.

Figure 1-12 Welcome Screen



NOTE

- To change the user level, tap **User** (the current user level is presented). The available values are **Operator** and **Administrator**.
- To exit the KVL application, tap **Exit**.

NOTE

If you launch the KVL first time after reinstalling/upgrading the KVL application, upgrading Security Adapter software, or applying Security Settings on the KVL, the End User License Agreement screen appears. To continue, select **Accept >**.

3 In the **Password** field, type your password using the keypad and tap **Log In >**.

Step result: The KVL main screen appears.

NOTE

If you log on as an Administrator and there are upgrades available for the Security Adapter or a target device, the **Upgrades available** screen appears. For more information on upgrades, see the *KVL 4000 FLASHPort Upgrade User Guide*.

NOTE

If you log on as an Operator and enter an incorrect password 3 times, your account is locked. Wait 15 minutes to try again, or contact an Administrator to unlock your account (see 9.3 Unlocking the Operator Account, page 9-5).

1.4.7 Exiting the KVL Application

When and where to use:
Use these steps to exit the KVL application.

IMPORTANT

To avoid unnecessary drain on the battery, always exit the KVL application before turning off the unit with the **Power** button.

Procedure Steps

1 Navigate to the KVL main screen.

NOTE

You can do it by pressing the End Key on the PDA (see 1.2.1.1 Personal Digital Assistant, page 1-2).

2 Tap **Exit**.

NOTE

If you have passwords defined for your KVL, the button says **Log Off** instead.

Step result: Depending on whether you have passwords defined or not, the **Exit** or the **Log off** screen appears.

Figure 1-13 Exit Screen

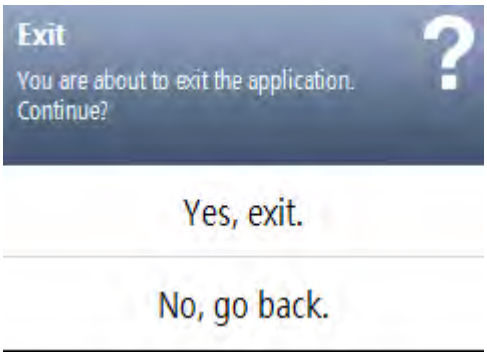
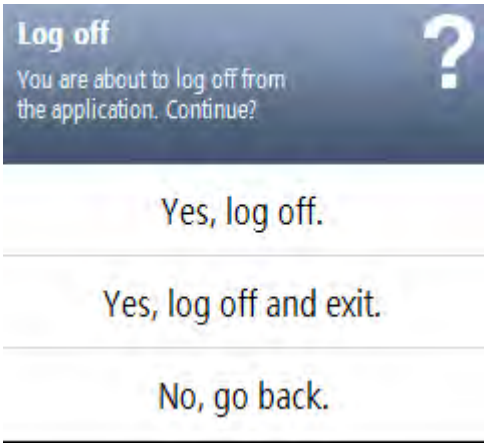


Figure 1-14 Log Off Screen



3 Select **Yes, exit** or **Yes, log off and exit**.

Step result: You exit the application and the **Today** screen appears.

2 KVL 4000 – Performing Initial Programming

Before using your KVL to enter and load encryption keys, set several parameters that determine how the KVL operates.

2.1 KVL 4000 User Preference Parameters

The user preference parameters and settings are not required for operation of the KVL, but instead provide a way of customizing certain functions to suit your individual needs.

2.1.1 Setting the KVL Log Off Time

For security reasons, you can set the period of inactivity after which you are logged off from the KVL.

Prerequisites:
This option is only available if you have set passwords on your KVL. Only an Administrator can set or change the KVL log off time.

Procedure Steps

1 Log on to the KVL application as an Administrator.

2 On the KVL main screen, select **Settings** → **Security** → **Inactivity**.

Step result: The list of available duration appears, with the currently set duration highlighted.

NOTE

To return to the previous screen without changing the current duration, tap **Cancel**.

3 Tap the desired duration.

Step result: The duration is changed.

4 Tap **Done** on the consecutive screens to return to the KVL main screen.

2.1.2 Setting the KVL Screen Color Scheme

You can set the KVL screen to one of the two color schemes: Day Time, or Night Time. These schemes define the text and background colors of the KVL screen. By default, the KVL screen is set to the Day Time scheme.

When and where to use:
Use these steps to set the KVL screen color scheme.

Figure 2-1 KVL Screen in Day Time Color Scheme (Example)

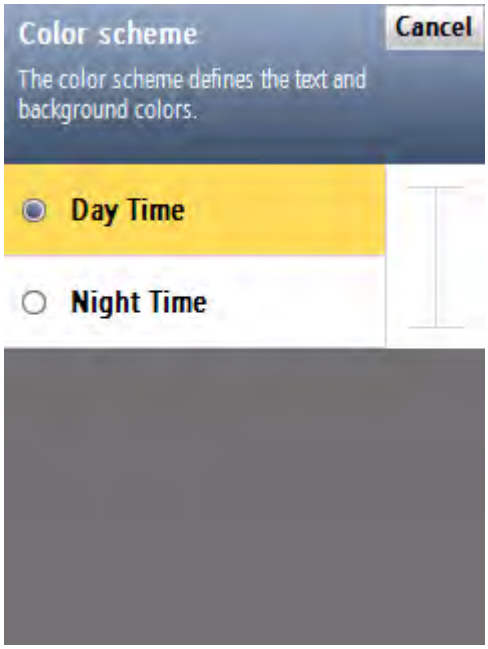
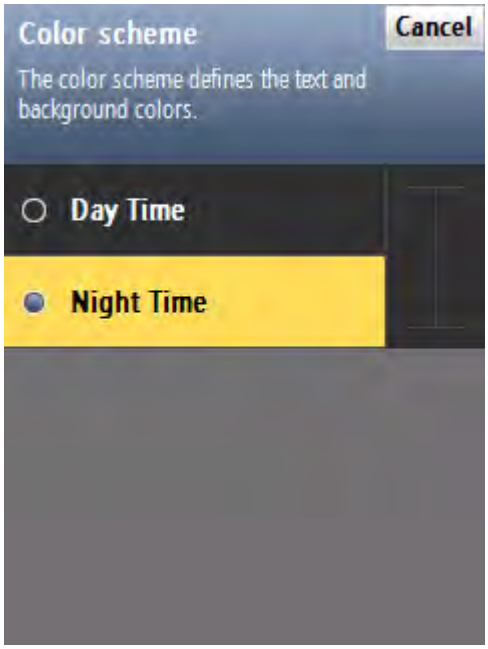


Figure 2-2 KVL Screen in Night Time Color Scheme (Example)



Procedure Steps

1 On the KVL main screen, select **Settings → General → Color scheme**.

Step result: The list of color scheme options appears, with the one currently used highlighted.

Tap **Cancel** to return to the previous screen without changing the current mode.

2 Tap the desired color scheme.

Step result: The color scheme is changed.

3 Tap **Done** on the consecutive screens to return to the KVL main screen.

2.1.3 Turning Sharing On/Off

In addition to loading keys into target devices, the KVL can also share its keys with another KVL. In order to share keys, the sharing feature must be turned on in both the source and target KVL.

Prerequisites:
Only an Administrator can turn sharing on or off.

Procedure Steps

1 On the KVL main screen, select **Settings → Security → Sharing**.

Step result: A list of available values appears (On/Off), with the currently set value highlighted.

2 Select the desired value.

3 Tap **Done** on the consecutive screens to return to the KVL main screen.

2.1.4 Managing Passwords

The KVL provides two levels of security access:

- **Administrator**
- **Operator**

The Administrator has access to all functions and features. The Operator does **NOT** have access to the following functions and features:

- performing KVL and target devices upgrades
- adding, deleting, and editing keys and macros

- converting keys
- setting and changing the KVL inactivity timeout
- changing FIPS mode
- changing System Key
- changing Sharing mode
- changing Administrator password
- clearing passwords
- clearing log records

Without password protection, all users have access to all of the KVL functions.

2.1.4.1 Setting Up Passwords on the KVL

This section covers the following topics:

2.1.4.1.1 Setting Up the Operator Password

When and where to use:
Use these steps to set up the Operator password.

NOTE

You cannot set just Administrator or Operator passwords, but must set both, if the password feature is desired.

Procedure Steps

1 On the KVL main screen, select **Settings → Security → Passwords → Define passwords → Operator**.

Step result: The **New password** and **Repeat password** entry fields appear.

2 In the **New password** entry field, type the password of your choice using the PDA keypad.

NOTE

The password must contain between 15 and 30 characters, including at least 1 special character, 1 numeric character, and 1 uppercase character. The following special characters are acceptable: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

NOTE

As you type the password, dynamic hints about password rules appear.

3 In the **Repeat password** entry field, type the password again.

Step result: If the passwords match, the **Done** button is enabled.

NOTE

To abort the operation at any time, tap **Cancel**.

4 Tap **Done**.

Step result: The password has been set up.

5 Tap **Done** on the consecutive screens to return to the KVL main screen.

IMPORTANT

If the Operator password is forgotten, the Administrator can assign a new Operator password.

2.1.4.1.2 Setting Up the Administrator Password

When and where to use:
Use these steps to set up the Administrator password.

NOTE

You cannot set just Administrator or Operator passwords, but must set both, if the password feature is desired.

Procedure Steps

1 On the KVL main screen, select **Settings → Security → Passwords → Define passwords → Administrator**.

Step result: The **New password** and **Repeat password** entry fields appear.

2 In the **New password** entry field, type the password of your choice using the PDA keypad.

NOTE

The password must contain between 15 and 30 characters, including at least 1 special character, 1 numeric character, and 1 uppercase character. The following special characters are acceptable: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

NOTE

As you type the password, dynamic hints about password rules appear.

3 In the **Repeat password** entry field, type the password again.

Step result: If the passwords match, the **Done** button is enabled.

NOTE

To abort the operation at any time, tap **Cancel**.

4 Tap **Done**.

Step result: The password has been set up.

5 Tap **Done** on the consecutive screens to return to the KVL main screen.

2.1.4.2 Changing Passwords on the KVL

This section covers the following topics:

2.1.4.2.1 Changing the Operator Password (Operator Access Level)

When and where to use:
Use this procedure if you have the Operator level of access.

Procedure Steps

1 Log on as an Operator.

Step result: The KVL main screen appears.

2 Select **Settings** → **Security** → **Password**.

Step result: The **Operator** screen appears, with the **Current password**, **New password**, and **Repeat password** entry fields.

3 In the **Current password** entry field, type the current password using the PDA keypad.

4 In the **New password** entry field, type the password of your choice using the PDA keypad.

NOTE

The password must contain between 15 and 30 characters, including at least 1 special character, 1 numeric character, and 1 uppercase character. The following special characters are acceptable: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

NOTE

As you type the password, dynamic hints about password rules appear.

5 In the **Repeat password** entry field, type the password again.

Step result: If the passwords match, the **Done** button is enabled.

NOTE

To abort the operation at any time, tap **Cancel**.

6 Tap **Done**.

Step result: The password has been changed.

7 Tap **Done** on the consecutive screens to return to the KVL main screen.

2.1.4.2.2 Changing the Operator Password (Administrator Access Level)

When and where to use:
Use this procedure if you have the Administrator level of access.

Procedure Steps

1 Log on as an Administrator.

If you are prompted for upgrades, select **No, not now**.

Step result: The KVL main screen appears.

2 Select **Settings → Security → Passwords → Update passwords → Operator**.

Step result: The **Current password**, **New password**, and **Repeat password** entry fields appear.

3 In the **Current password** entry field, type the current password using the PDA keypad.

4 In the **New password** entry field, type the password of your choice using the PDA keypad.

The password must contain between 15 and 30 characters, including at least 1 special character, 1 numeric character, and 1 uppercase character. The following special characters are acceptable: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

As you type the password, dynamic hints about password rules appear.

5 In the **Repeat password** entry field, type the password again.

Step result: If the passwords match, the **Done** button is enabled.

To abort the operation at any time, tap **Cancel**.

6 Tap **Done**.

Step result: The password has been changed.

7 Tap **Done** on the consecutive screens to return to the KVL main screen.

2.1.4.2.3 Changing the Administrator Password

Prerequisites:
Only an Administrator can change the Administrator password.

Procedure Steps

1 Log on as an Administrator.

If you are prompted for upgrades, select **No, not now**.

Step result: The KVL main screen appears.

2 Select **Settings → Security → Passwords → Update passwordsAdministrator**.

Step result: The **Current password**, **New password**, and **Repeat password** entry fields.

3 In the **Current password** entry field, type the current password using the PDA keypad.

4 In the **New password** entry field, type the new password.

The password must contain between 15 and 30 characters, including at least 1 special character, 1 numeric character, and 1 uppercase character. The following special characters are acceptable: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

As you type the password, dynamic hints about password rules appear.

5 In the **Repeat password** entry field, type the new password again.

Step result: If the passwords match, the **Done** button is enabled.

To abort the operation at any time, tap **Cancel**.

6 Tap **Done**.

Step result: The password has been changed.

7 Tap **Done** on the consecutive screens to return to the KVL main screen.

If you forget the Administrator password, you must perform a system reset before the KVL can be used again. Since a system reset erases all stored keys and returns the KVL settings to the factory defaults, you must enter all keys again.

2.1.4.3 Clearing KVL Passwords

Prerequisites:
Only an Administrator can clear passwords.

Procedure Steps

1 Log on as an Administrator.

NOTE

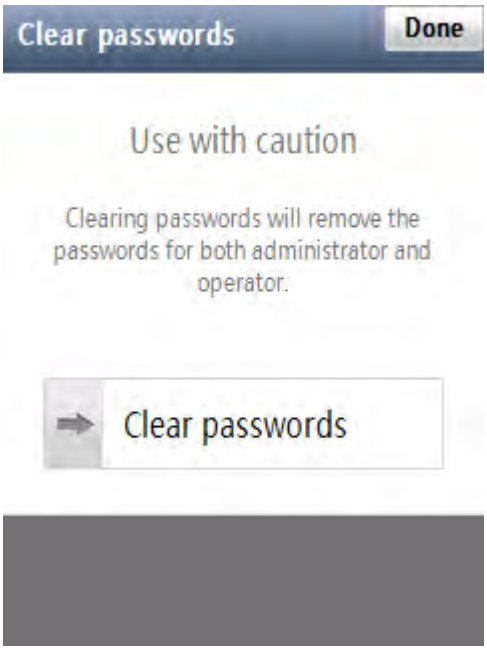
If you are prompted for upgrades, select **No, not now**.

Step result: The KVL main screen appears.

2 Select **Settings → Security → Passwords → Clear passwords**.

Step result: A screen with the **Clear passwords** slider appears.

Figure 2-3 Clear Passwords Screen



3 Touch the slider and drag it from left to right. Alternatively, highlight the slider, and use the navigation key on the PDA to move it.

CAUTION

Clearing passwords removes the passwords for both administrator and operator.

Step result: The passwords have been cleared.

4 Tap **Done** on the consecutive screens to return to the KVL main screen.

2.1.4.4 Selecting the Password Masking Mode

There are two masking modes available for the KVL passwords: all characters masked, or the last character non masked.

Procedure Steps

1 On the KVL main screen, select **Settings → Security → Masking mode**.

Step result: A screen with the list of available options appears.

2 Select the masking mode of your choice.

Step result: The masking mode is selected and you return to the previous screen.

3 Tap **Done** on the consecutive screens to return to the KVL main screen.

2.2 KVL 4000 System-Dependent Parameters

Set the parameters in this section depending on the particular system (ASN, ASTRO® 25, or Radio Authentication) in which the KVL is operating.

2.2.1 KVL 4000 – Switching Between the Modes of Operation

The KVL provides three modes of operation: ASN (Advanced SECURENET®), ASTRO® 25, and Radio Authentication. The KVL is shipped from the factory to power on in the ASTRO® 25 mode. Then, the KVL powers on in the mode it was operating in when it was last powered off.

Prerequisites:
This procedure is applicable if your KVL is configured to operate in more than one mode of operation.

When and where to use:
Use these steps to switch between the modes of operation.

IMPORTANT

In the Radio Authentication mode, the KVL operates in FIPS Level 2 only. Before changing the mode of operation to Radio Authentication, ensure FIPS Level 2 is set for the mode the KVL is currently operating in.

Procedure Steps

1 On the KVL main screen, select **Settings → System**.

Step result: A list of available modes appears (ASN, ASTRO® 25, and Radio Authentication), with the currently used mode highlighted.

To return to the previous screen without changing the mode, tap **Cancel**.

2 Tap the desired mode of operation.

Step result: The mode is changed.

3 Tap **Done** to return to the KVL main screen.

2.2.2 Setting the Baud Rate for RS-232 Communication

When using the KVL DB9 Port (RS-232) to communicate with external equipment (such as a KMF, or a modem), select the proper baud rate.

Procedure Steps

1 On the KVL main screen, select **Settings → General → Baud Rate**.

Step result: A list of available values appears, with the currently set value highlighted. You can choose from the following values:

- 9600
- 19200
- 57600
- 115200

To return to the previous screen without changing the current value, tap **Cancel**.

2 Tap the desired value.

3 Tap **Done** on the consecutive screens to return to the KVL main screen.

2.2.3 Changing the FIPS Mode

The KVL can operate in a mode that is compliant with the U.S. Federal Information Processing Standard (FIPS) guidelines. To be FIPS-compliant, set passwords on your KVL.

Prerequisites:
Only an Administrator can change the FIPS mode.

When and where to use:
Use these steps to change the FIPS mode.

Changing the FIPS mode erases all keys, Store and Forward messages, target devices to update, and sets the System Key to its default value.

Procedure Steps

1 On the KVL main screen, select **Settings → Security → FIPS mode**.

Step result: The list of available values appears, with the currently selected value highlighted.

NOTE

The available values are:

- **Level 3 (High Security)**
- **Level 2 (Standard)**

IMPORTANT

Use **Level 3** for high security. If FIPS Level 3 is active, the Sharing setting is disabled and cannot be turned on.

IMPORTANT

In the Radio Authentication mode, the KVL operates in FIPS Level 2 only. Before changing the mode of operation to Radio Authentication, ensure FIPS Level 2 is set for the mode the KVL is currently operating in.

2 Select the desired value.

Step result: A **Warning** screen appears, informing that changing the FIPS mode will remove all keys.

3 Select **Yes, change FIPS mode** if you are sure that you want to continue.

Step result: The FIPS mode is changed.

4 Tap **Done** on the consecutive screens to return to the KVL main screen.

2.2.4 Managing the System Key (DVI-XL Only)

The KVL requires a 128-digit System Key to communicate in DVI-XL systems. Each KVL is shipped from the factory with a default System Key.

IMPORTANT

Changing the System Key causes all keys defined with the DVI-XL algorithm (including the UKEK for ASTRO® 25) to be erased (includes DVI-XL keys in both ASN and ASTRO® 25 memory).

2.2.4.1 Entering the User-Defined System Key

Prerequisites:
Only an Administrator can enter the System Key.

When and where to use:
Instead of using the default System Key, you can enter your own System Key.

Changing the System Key deletes all associated keys.

Procedure Steps

1 On the KVL main screen, select **Settings** → **Security** → **System Key**.

2 Select the **Enter Key** tab.

3 Perform one of the following actions:

- Select **Auto** to generate the key automatically.
- Enter the key manually using the Hex keypad.

At any time, you can tap the key entry bar to go to the key review screen.

4 Tap **Done**.

Step result: A warning message appears, informing that changing the system key will delete all keys associated with the system key.

5 Tap **Yes, change system key** to confirm the change.

Step result: The System Key is changed.

6 Tap **Done** on the consecutive screens to return to the KVL main screen.

2.2.4.2 Changing the User-Defined System Key

When and where to use:
Use these steps to change the System Key you have previously entered.

Changing the System Key deletes all associated keys.

Procedure Steps

1 On the KVL main screen, select **Settings → Security → System Key**.

2 Tap the **New >** key.

Step result: A Key Data Info Field and a Hex Entry Keypad appear.

3 Perform one of the following actions:

- Select **Auto** to generate the key automatically.
- Enter the key manually using the Hex keypad.

At any time, you can tap the key entry bar to go to the key review screen.

4 Tap **Done**.

Step result: A warning message appears, informing that changing the system key will delete all keys associated with the system key.

5 Tap **Yes, change system key** to confirm the change.

Step result: The System Key is changed.

6 Tap **Done** on the consecutive screens to return to the KVL main screen.

2.2.4.3 Setting Up the KVL to Use the Default System Key

Procedure Steps

1 On the KVL main screen, select **Settings → Security → System Key**.

2 Tap the **Use default** tab.

Step result: A message appears, informing that the default system key will be used.

3 Tap **Done**.

Step result: A warning message appears, informing that changing the system key will delete all keys associated with the system key.

4 Tap **Yes, change system key** to confirm the change.

Step result: The default System Key is restored.

5 Tap **Done** on the consecutive screens to return to the KVL main screen.

3 Managing Encryption Keys

IMPORTANT

The Advanced SECURENET® operating mode only supports Physical ID (PID) based key management.

3.1 Entering Encryption Keys Manually

Prerequisites:
Only an Administrator can enter keys.

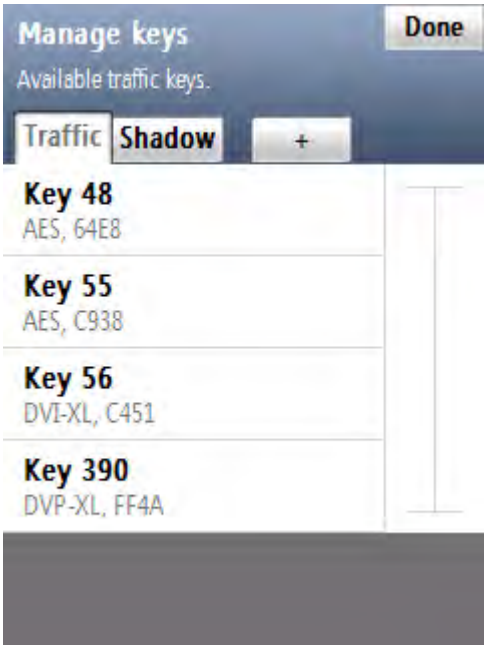
When and where to use:
Use these steps to manually enter a Traffic Key or a Shadow Key into the KVL internal key database.

Procedure Steps

1 On the KVL main screen, select **Manage → Keys**.

Step result: The **Manage keys** screen appears.

Figure 3-1 Manage Keys Screen – Entering a Key (Example)



2 Choose if you want to enter **Traffic** or **Shadow** keys – select the appropriate tab.

3 Tap the + button to define a new key.

4 Select **Enter manually** to enter keys one by one.

5 Select **Algorithm** and choose one of the algorithms from the list.

6 Select **Physical ID** and type a number in 0–511 range to set the key location.

7 Tap **Done** when ready.

8 Select **Logical ID** and type a number in 0000–FFFF hexadecimal range.

9 Tap **Done** when ready.

10 Tap **Enter Key >**.

11 Enter the encryption key using the keypad. The specific byte number is displayed as you enter the key numbers.

NOTE

At any time, you can review the digits you have entered by tapping anywhere on the Key Data Info field. This brings up a Review key screen.

NOTE

For DES keys only: As you enter each digit of the encryption key, the KVL checks it for validity. If you enter an invalid number, it flashes red. In this case, tap **< Del** and correct the number. Every two numbers entered for the key represent a byte of data that must have odd-parity for DES keys. For non-DES keys: Encryption key validity is checked only after you entered the entire key and tapped **Done**.

12 Once you have entered the key, tap **Done** to confirm, or **Next Key** to confirm and enter a new key with the same parameters.

13 Tap **Done** to return to the KVL main screen.

3.2 Auto-Generating Encryption Keys

Prerequisites:
Only an Administrator can enter keys.

When and where to use:
Use these steps to quickly generate multiple encryption keys.

Procedure Steps

1 On the KVL main screen, select **Manage → Keys**.

Step result: The **Manage keys** screen appears.

Figure 3-2 Manage Keys Screen – Entering a Key (Example)

2 Choose if you want to enter **Traffic** or **Shadow** keys – select the appropriate tab.

3 Tap the + button to define a new key.

4 Select **Auto generate** to generate multiple keys quickly.

5 Enter the number of keys to auto generate and tap **Next Step**.

NOTE

You can generate a maximum of 100 keys at a time.

6 Select **Algorithm** and choose one of the algorithms from the list.

7 Select **Initial PID** and type a number in 0–511 range to set the first key location.

8 Tap **Done** when ready.

9 Select **Initial LID** and type a number in 0000–FFFF hexadecimal range.

10 Tap **Done** when ready.

11 Tap **Generate >**.

Step result: A progress animation appears, indicating that the keys are being generated. When the process is completed, you return to the **Manage keys** screen.

12 Tap **Done** to return to the KVL main screen.

3.3 Using Macros

Macros allow you to group several keys stored in the KVL memory and map each one to a specific target slot. You can then load the entire group of keys to the target device in a single operation. This is especially useful when loading the same group of keys to several target devices, such as a fleet of radios.

The KVL supports up to four macros, each consisting of up to 16 Traffic keys and one Common Shadow Key (CSK).

3.3.1 Creating a Macro

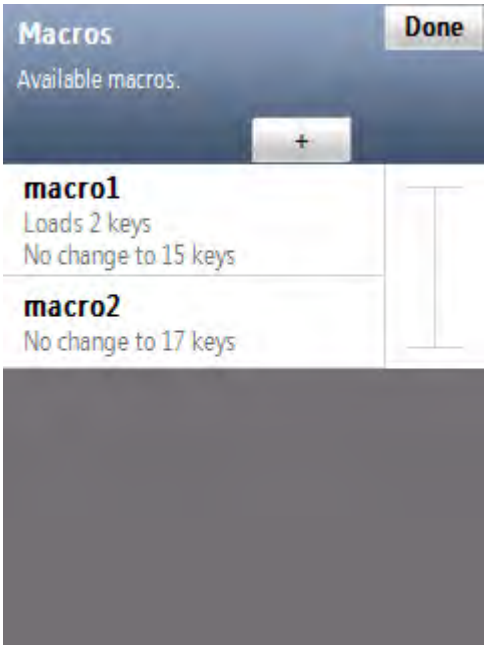
Prerequisites:
Only an Administrator can create macros.

Procedure Steps

1 On the KVL main screen, select **Manage → Macros**.

Step result: The **Macros** screen appears with a list of available macros.

Figure 3-3 Macros Screen – Creating a Macro (Example)



2 Tap the + button to define the parameters of a new macro.

NOTE

You can create up to 4 macros. When you have defined all 4 macros, the + button becomes grayed out.

3 Enter the name of the macro using the PDA keypad.

NOTE

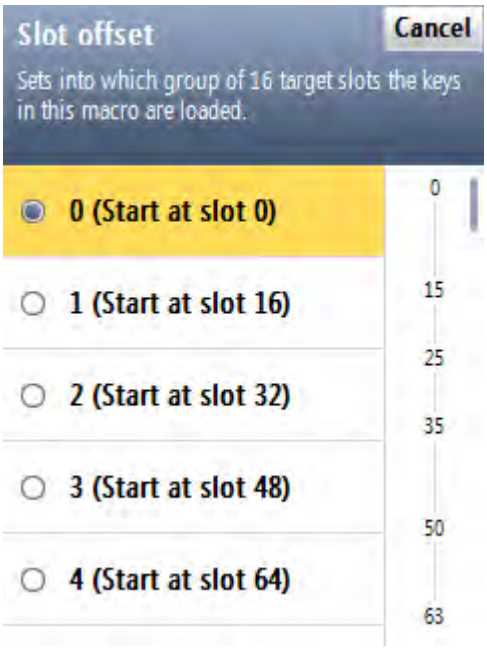
You can enter up to 8 characters, including spaces.

4 Select **Slot offset** to indicate into which group of 16 target slots the keys in this macro will be loaded.

NOTE

You can choose from group 0 to group 63.

Figure 3-4 Slot Offset Screen



5 Select the desired group.

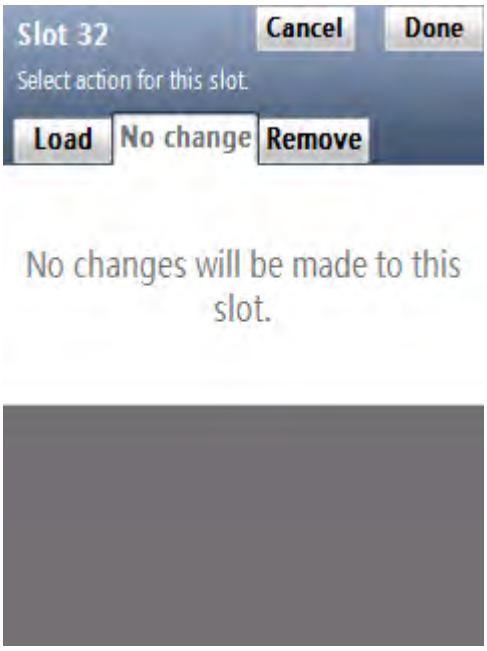
6 Select the desired target slot number.

NOTE

Each group consists of 16 slots for Traffic keys and one slot for Common Shadow Key (CSK).

Step result: A screen for this slot appears.

Figure 3-5 Slot Screen – Example



7 Select the **Load** tab.

Step result: A Hex keypad appears.

8 Enter the slot number for the Traffic key stored in the KVL that you wish to map to the currently selected target slot, and tap **Done** when ready.

NOTE

You may also select the **No change** tab or **Remove** tab. Selecting **No change** results in no changes being made to the key residing in the selected target slot when a load operation is performed. Selecting **Remove** results in erasing the key residing in the selected target slot when a load operation is performed.

9 Repeat step 6 through step 8 until you have mapped the desired number of source and target keys (up to 16).

10 Scroll down the screen and select **CSK** to load the Common Shadow Key.

11 Repeat step 7 and step 8 for the CSK.

12 Tap **Done** when ready.

Step result: The new macro is saved and appears in the list.

13 Tap **Done** to return to the previous screen.

14 Tap the + button to define a new macro, or tap **Done** to return to the KVL main screen.

3.4 Editing Keys

You can modify Traffic and Shadow Keys stored in the KVL memory.

Prerequisites:
Only an Administrator can modify keys.

When and where to use:
Use these steps to modify an Encryption Key.

Procedure Steps

1 On the KVL main screen, select **Manage → Keys**.

Step result: The **Manage keys** screen appears with a list of available keys.

Figure 3-6 Manage Keys Screen – Modifying a Key (Example)

2 Choose if you want to modify the **Traffic** or **Shadow** keys – select the appropriate tab.

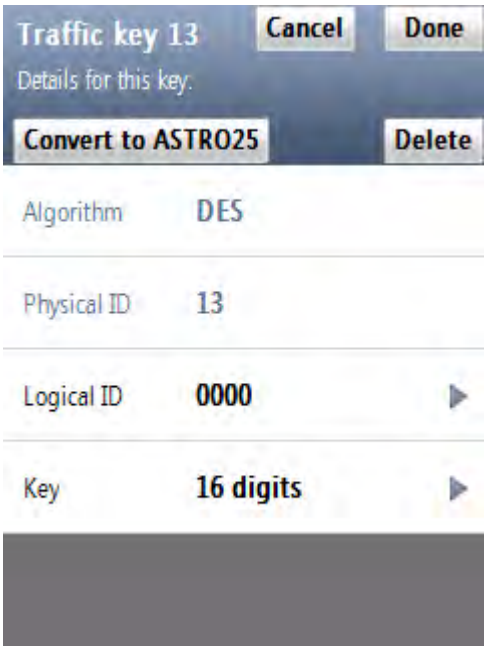
3 Locate and select the key you want to modify on the list of available keys.

NOTE

You can use the smart bar on the right side of the screen to scroll through the list or quickly jump within the list to a selected area. If the list fits completely on the screen, the smart bar is disabled.

Step result: A screen with details for the key appears.

Figure 3-7 Key Details Screen – Example



NOTE

The **Algorithm** and **Physical ID** entries are read-only.

4 Select and modify **Logical ID** using the Hex keypad. Type the hexadecimal number to set the new Logical ID.

5 Tap **Done** when ready.

Step result: You return to the screen with the key details.

6 Select **Key**.

Step result: A Hex keypad appears.

Figure 3-8 Enter Key Screen – Example

7 Tap **Auto** to generate the key automatically, or enter the key using the Hex keypad.

NOTE

For DES keys only: As you enter each digit of the encryption key, the KVL checks it for validity. If you enter an invalid number, it flashes red and a **bad bonk** sound is played. In this case, tap **< Del** and correct the number. Every two numbers entered for the key represent a byte of data that must have odd-parity for DES keys. For non-DES keys: Encryption key validity is checked only after you entered the entire key and tapped **Done**.

8 Once you have entered the key, tap **Done** to confirm.

Step result: The key has been modified.

9 Tap **Done** on the consecutive screens to return to the KVL main screen.

3.5 Deleting Keys

You can erase an Encryption Key (Traffic or Shadow) stored in a specific key slot in the KVL memory. Deleting permanently erases the Encryption Key currently stored in the slot. The slot is then considered to be undefined and may be used to hold another Encryption Key.

Prerequisites:
Only an Administrator can delete keys.

When and where to use:
Use these steps to delete an Encryption Key.

Procedure Steps

1 On the KVL main screen, select **Manage** → **Keys**.

Step result: The **Manage keys** screen appears.

Figure 3-9 Manage Keys Screen – Deleting a Key (Example)

2 Choose if you want to delete a **Traffic** or **Shadow** key – select the appropriate tab.

3 From the list of available keys, select the key you want to delete.

NOTE

You can use the smart bar on the right side of the screen to scroll through the list or quickly jump within the list to a selected area. If the list fits completely on the screen, the smart bar is disabled.

4 Tap **Delete**.

Step result: The key has been deleted.

NOTE

If you want to restore the deleted key, tap **Undo** before leaving the confirmation screen.

5 Tap **Accept** to confirm and return to the list of keys.

6 Tap **Done** to return to the KVL main screen.

4 Loading Keys into Target Devices

You can load encryption keys into one of the following devices:

- Secure ASTRO® 25 Single Key Target Radios
- Secure ASTRO® 25 Multiple Key Target Radios
- SECURENET/Advanced SECURENET Mobile Radios
- SECURENET/Advanced SECURENET Portable Radios
- Another KVL unit (see Chapter 6 Sharing Keys Between KVLs)
- Radio Network Controller (RNC)
- Digital Interface Unit (DIU)
- Console Interface Unit (CIU)
- Key Management Center (KMC)

IMPORTANT

The Advanced SECURENET® operating mode only supports Physical ID (PID) based key management.

4.1 Loading Traffic Keys

Prerequisites:
There are encryption keys in the KVL database.

When and where to use:
Use these steps to load a Traffic Key into a target device.

Procedure Steps

1 On the KVL main screen, select **Load keys & macros → Load keys**.

Step result: The **Load keys** screen appears, with the **Traffic** tab open.

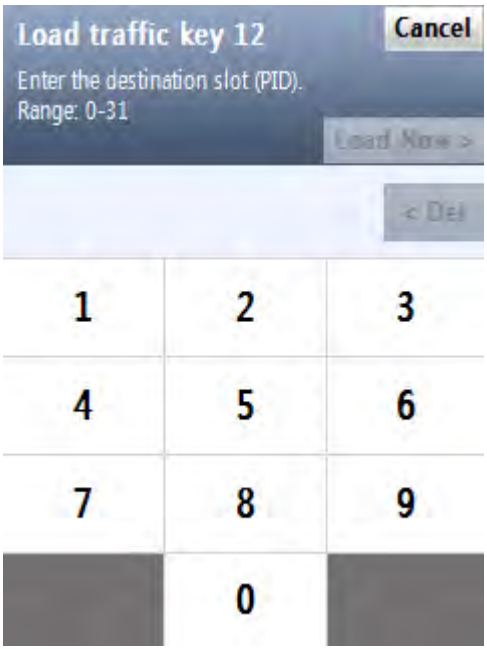
Figure 4-1 Load Keys Screen – Loading a Traffic Key (Example)

2 Connect the radio to the KVL using an appropriate key load cable. (See 1.4.4.1 Connecting the KVL to a Radio or Another Target Device, page 1-13.)

3 Select the key you want to load.

Step result: A screen with the decimal keypad appears.

Figure 4-2 PID Entry Screen – Example



4 Enter the destination slot (PID) for this key using the decimal keypad.

NOTE

This screen appears only if the connected radio has more than one destination slot.

NOTE

The Physical ID (PID) range is dynamically generated based on a query for the radio's capacity.

5 Tap **Load now >**.

Step result: The key has been loaded to the desired destination. The **completed** sound is played and you return to the **Load keys** screen (the key that you have loaded now has a green check mark next to it).

Figure 4-3 Traffic Key Loaded – Example

6 Select another key to load and repeat step 4 through step 5, or tap **Done**.

NOTE

If you want to load the same key to another radio, disconnect the current radio, connect another one, and perform step 3 through step 5.

7 Tap **Done** to return to the KVL main screen.

4.2 Loading Shadow Keys

You can load a Shadow key to either a Common Shadow Key (CSK) slot or a Unique Shadow Key (USK) slot in the target device.

Prerequisites:
Shadow Keys are only applicable for target devices in MDC OTAR systems.

When and where to use:
Use these steps to load a Shadow key into a target device.

Procedure Steps

1 On the KVL main screen, select **Load keys & macros → Load keys**.

Step result: The **Load keys** screen appears with a list of available Traffic keys.

Figure 4-4 Load Keys Screen – Loading a Shadow Key (Example)

2 Select the **Shadow** tab.

Step result: The list of Shadow keys appears.

NOTE

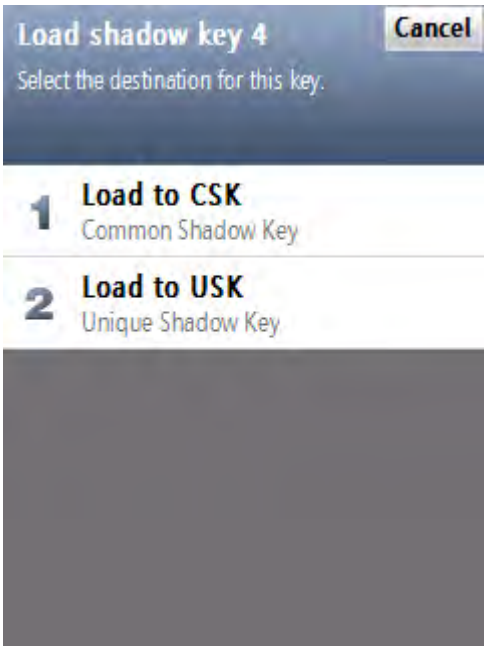
You can use the smart bar on the right side of the screen to scroll through the list or quickly jump within the list to a selected area. If the list fits completely on the screen, the smart bar is disabled.

3 Connect the radio to the KVL using an appropriate key load cable. (See 1.4.4.1 Connecting the KVL to a Radio or Another Target Device, page 1-13.)

4 Select the key you want to load.

Step result: The list of available destinations for the key appears.

Figure 4-5 Load Shadow Key Screen – Example



5 Select the destination for this key. Choose either **Load to CSK** or **Load to USK**.

NOTE

If the radio has no CSK and USK slots, an error message is displayed.

Step result: The key has been loaded to the desired destination.

Figure 4-6 Shadow Key Loaded – Example

6 Select another key to load and repeat step 5, or tap **Done**.

NOTE

If you want to load the same key to another radio, disconnect the current radio, connect another one, and perform step 4 through step 5.

7 Tap **Done** to return to the KVL main screen.

4.3 Loading a Macro

Prerequisites:
There are macros in the KVL database.

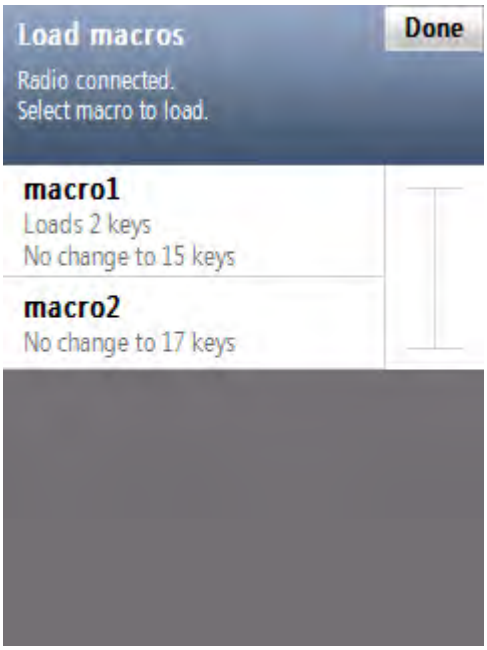
When and where to use:
Use these steps to load a macro into a target device.

Procedure Steps

1 On the KVL main screen, select **Load keys & macros → Load macros**.

Step result: The list of available macros appears.

Figure 4-7 Load Macros Screen – Example



2 Connect the radio to the KVL using an appropriate key load cable. (See 1.4.4.1 Connecting the KVL to a Radio or Another Target Device, page 1-13.)

3 Select the macro you want to load to the target device.

Step result: A progress animation appears, indicating that the macro is being loaded. When the process is completed, a **completed** sound is played and you return to the **Load macros** screen.

4 Select another macro to load, or tap **Done**.

NOTE

If you want to load the same macro to another radio, disconnect the current radio, connect another one, and select the macro you want to load.

5 Tap **Done** to return to the KVL main screen.

5 Managing Keys in Target Devices

5.1 Removing Keys from Target Devices

KVL allows you to erase an encryption key (Traffic or Shadow) stored in a specific key slot in a secure target device, such as a radio. This feature permanently erases the encryption key currently stored in the slot. The slot is then considered to be undefined and may be used to hold another encryption key.

5.1.1 Removing Traffic Keys from a Target Device

Prerequisites:
There are encryption keys in the KVL internal database.

Procedure Steps

1 Connect the radio to the KVL using an appropriate key load cable. (See 1.4.4.1 Connecting the KVL to a Radio or Another Target Device, page 1-13.)

2 Select **Remove keys** on the KVL main screen.

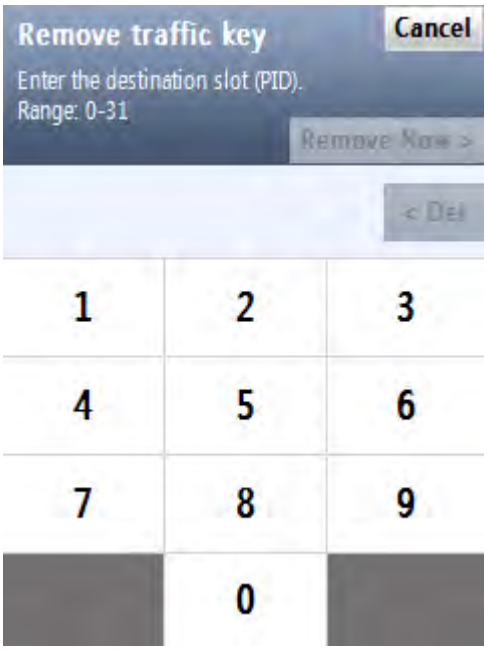
Step result: A list of available options appears.

Figure 5-1 Remove Keys Screen

3 Select **Traffic key**.

Step result: The **Remove traffic key** screen appears with a decimal keypad.

Figure 5-2 Remove Traffic Key Screen



NOTE

This screen is only displayed when the radio has more than one destination slot.

4 Enter the destination slot (PID) of the key you want to remove using the decimal keypad.

NOTE

The range is dynamically generated based on a query for the radio's capacity.

5 Tap **Remove now >**.

Step result: The Traffic key has been removed and a confirmation message appears.

6 Tap **Ok, done** to return to the **Remove keys** screen, or **Remove another** to remove another key.

7 Tap **Done** to return to the KVL main screen.

5.1.2 Removing Shadow Keys from a Target Device

Prerequisites:
There are encryption keys in the KVL internal database.

Procedure Steps

1 Connect the radio to the KVL using an appropriate key load cable. (See 1.4.4.1 Connecting the KVL to a Radio or Another Target Device, page 1-13.)

2 Select **Remove keys**.

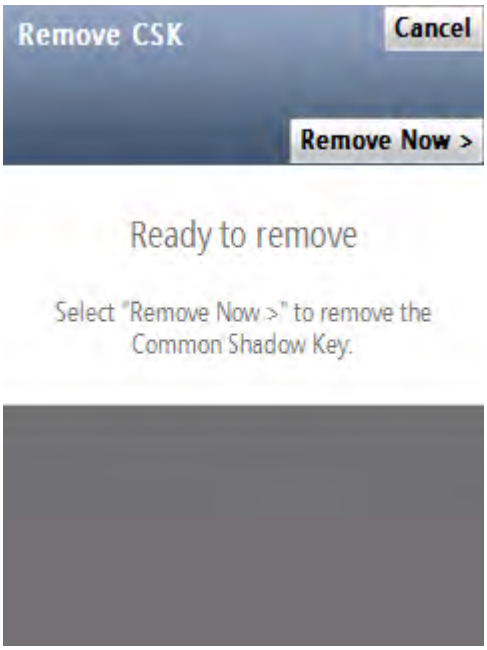
Step result: A list of available options appears.

Figure 5-3 Remove Keys Screen – Removing a Shadow Key

3 Select **CSK** if you want to remove a Common Shadow Key, or **USK** if you want to remove a Unique Shadow Key.

Step result: A confirmation screen appears.

Figure 5-4 Remove CSK Screen



4 Select **Remove Now >**.

Step result: The key has been removed and a confirmation screen appears.

5 Tap **OK** to return to the **Remove keys** screen.

6 Remove another key, or disconnect the radio and tap **Done** to return to the KVL main screen.

6 Sharing Keys Between KVLs

In addition to loading keys into target devices, the KVL can also load (share) its keys with another KVL of the same or earlier model.

The following sharing functions are supported:

- Sharing a single key - The source KVL can share a selected key with another KVL.
- Sharing a macro - The source KVL can share its macros (and the keys associated with these macros) with another KVL.
- Sharing all keys and all macros - The source KVL can share all of its keys (including Traffic keys, Shadow keys, and macros) with another KVL.

The following rules apply to sharing:

- Sharing must be turned ON in both the source and target KVL. See 2.1.3 Turning Sharing On/Off, page 2-3.)
- The target KVL must be on its main screen.
- Sharing cannot be performed between a KVL in ASN mode and a KVL in ASTRO® 25 mode. (To change the mode of operation, see 2.2.1 KVL 4000 – Switching Between the Modes of Operation, page 2-11.)
- Only key data and macros are shared. KVL configuration settings and log records for the target KVL remain unchanged.
- Sharing can be performed between two KVLs of the same or different models. Either may be the source or target.

6.1 Sharing a Single Key

Prerequisites:
In order to share a selected key, the target KVL must support the algorithm of the key being shared.

Procedure Steps

1 On the KVL main screen, select **Load keys & macros → Load keys**.

Step result: The list of Traffic keys appears.

Figure 6-1 Load Keys Screen – Sharing a Key (Example)

NOTE

If you want to share a Shadow key, select the **Shadow** tab.

2 Connect the target KVL using the KVL to KVL cable. (See 1.4.4.2 Connecting Two KVL Units, page 1-15.)

NOTE

For the sharing operation to work, the target KVL must have the sharing function turned on and must be on its main screen.

3 Select the key you want to share.

4 Tap **Load now >**.

Step result: The key has been shared with the target KVL.

5 Select another key to share, or disconnect the KVLs and tap **Done** on the consecutive screens to return to the KVL main screen.

6.2 Sharing a Macro and Associated Keys

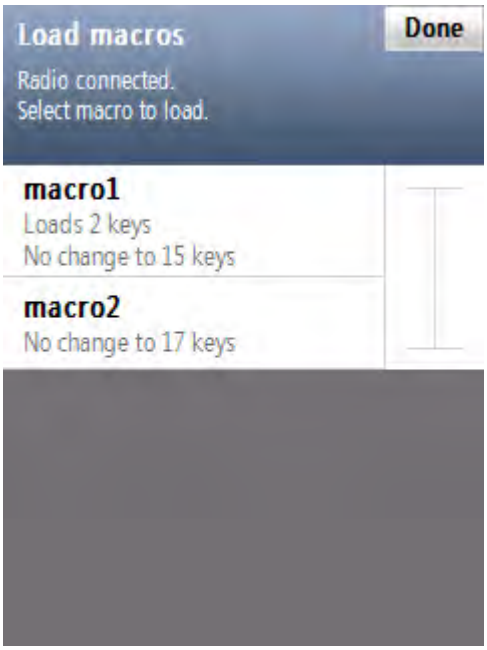
Prerequisites:
There are macros in the KVL internal database.

Procedure Steps

1 On the KVL main screen, select **Load keys & macros → Load macros**.

Step result: A list of available macros appears.

Figure 6-2 Load Macros Screen – Sharing a Macro (Example)



2 Connect the target KVL using the KVL to KVL cable. (See 1.4.4.2 Connecting Two KVL Units, page 1-15.)

NOTE

For the sharing operation to work, the target KVL must have the sharing function turned on and must be on its main screen.

3 Select the macro you want to share.

Step result: A progress animation appears, indicating that the macro is being loaded. When the operation has completed successfully, you return to the list of macros and the list item for the loaded macro receives a check mark.

4 Select another macro to share, or disconnect the KVLs and tap **Done** on the consecutive screens to return to the KVL main screen.

6.3 Sharing All Keys and All Macros

Prerequisites:
In order to share all keys and macros, the target KVL must support the same algorithms as the source KVL.

- **Example 1:** The source KVL is equipped with DES and DVP-XL, and there is at least one key defined for each algorithm. The target KVL must also be equipped with DES and DVP-XL.
- **Example 2:** The source KVL is equipped with AES, DES, and DVP-XL, but there are keys defined only for AES. The target KVL must also be equipped with at least AES.

Procedure Steps

1 Select **Load keys & macros** on the KVL main screen.

2 Connect the target KVL using the KVL to KVL cable. (See 1.4.4.2 Connecting Two KVL Units, page 1-15.)

NOTE

For the sharing operation to work, the target KVL must have the sharing function turned on and must be on its main screen.

3 Select **Load all to Another KVL**.

Step result: The confirmation screen appears.

4 Tap **Load Now >**.

Step result: A progress animation appears, indicating that the keys and macros are being shared. When the operation has completed successfully, a confirmation screen appears and a **completed** tone is played.

5 Disconnect the KVLs and connect another KVL to load keys and macros to, or tap **Done** on the consecutive screens to return to the KVL main screen.

7 Managing Log Records

The KVL maintains a running record of the most recent 100 successful key load operations.

The format of each log record entry on the list is as follows:

- First line: Date/Time
- Second line: Role/Action Performed
- Third line: Entity Name/CKR ID/PID/Target ID

Log records can be:

- Viewed and scrolled on the KVL screen.
- Exported to a PC for printing or saving to a file.
- Cleared (erased) from the KVL memory.

7.1 Organization of Log Records

The log records are stored chronologically in a 100-location continuous buffer, with the most recent log record displayed first each time you access the log records.

Each new log record created is appended to the beginning of the buffer, with each existing log record moving down one position.

When the buffer is full (100 entries maximum), the next new log record is appended to the beginning, the existing log records move down one position, and the oldest log record is overwritten.

7.2 Accessing Log Records

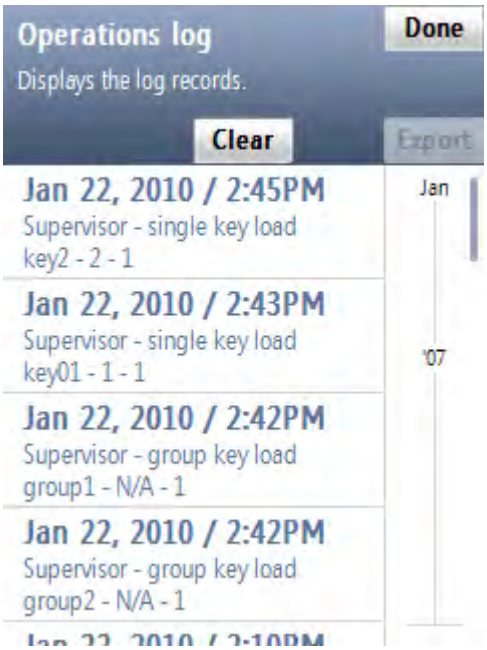
Prerequisites:
There are log records in the KVL memory.

Procedure Steps

1 On the KVL main screen, select **Settings → Operations log**.

Step result: The list of log records appears.

Figure 7-1 Operations Log (Example)



NOTE

You can scroll through the list or quickly jump to a selected area using the smart bar on the right side of the screen.

2 When you have finished viewing log records, tap **Done** on the consecutive screens to return to the KVL main screen.

7.3 Clearing Log Records

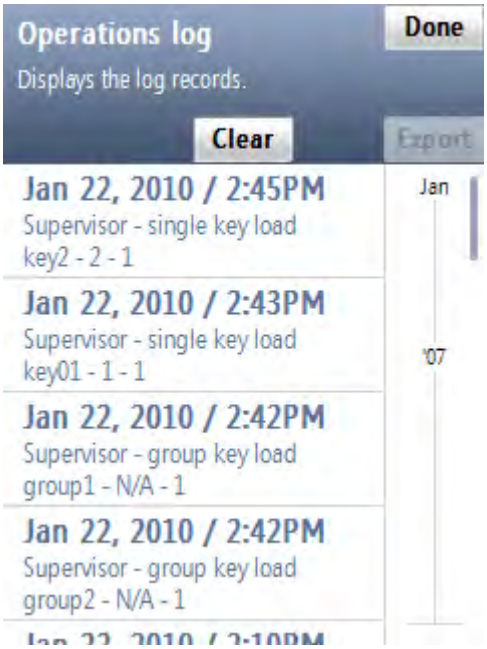
Prerequisites:
Only an Administrator can clear log records.

Procedure Steps

1 On the KVL main screen, select **Settings → Operations log**.

Step result: The list of log records appears.

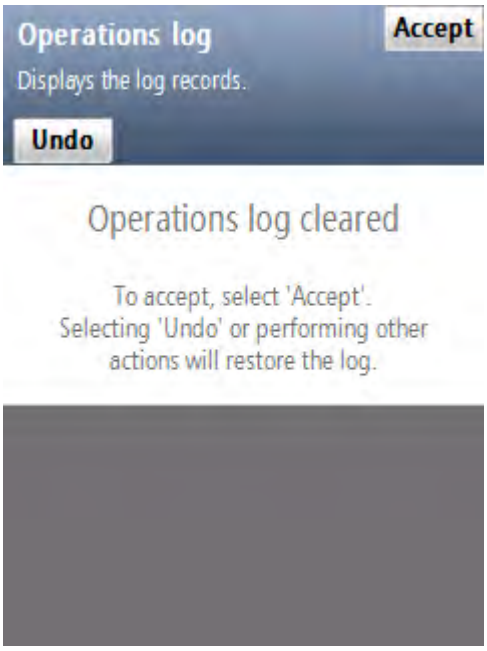
Figure 7-2 Operations Log – Clear (Example)



2 Select the **Clear** button.

Step result: A confirmation screen appears.

Figure 7-3 Clearing Logs – Confirmation Screen



NOTE

To restore the log, tap **Undo**.

3 Tap **Accept** to confirm.

IMPORTANT

Only the logs for the current mode of operation (ASN, ASTRO® 25, or Radio Authentication) are cleared.

Step result: The log records have been cleared.

4 Tap **Done** to return to the KVL main screen.

7.4 Exporting Log Records to a PC

You can connect the KVL to a COM port on a PC (typically a laptop) and export log records to the PC. You can then print log records from the PC or save them on the PC as a file.

Prerequisites:
A communications program, such as Microsoft HyperTerminal, must be running on the PC in order to export log records.

Procedure Steps

1 Connect an appropriate cable between the KVL DB9 Port (RS-232) and a COM port on the PC. Depending on the cable type, you may need to use a gender changer.

NOTE

Ensure that the baud rate set up in the KVL matches the baud rate in the communications program.

2 Launch a communications program on the PC (such as Microsoft HyperTerminal or equivalent). Set up the program as follows:

- No parity
- 8 bits
- 1 stop bit
- Translate line feeds <LF> to Carriage Return and Line Feed <CR><LF>
- 80 character width

3 On the KVL main screen, select **Settings → Operations log → Print → Print Now>**.

Step result: A progress animation appears, indicating that the log records are being exported to the PC. When the log records have been exported successfully, you return to the list of log records.

4 Tap **Done** on the consecutive screens to return to the KVL main screen.

8 Converting Encryption Keys

NOTE

This chapter is applicable only if your KVL is configured to work in both ASN and ASTRO® 25 modes of operation.

If your KVL is configured to work in both ASN and ASTRO® 25 modes of operation, you can convert encryption keys between these two modes. Converting keys allows you to copy an ASN Traffic or Shadow key from its ASN memory location (stored to a PID and containing a LID) and load it into an empty ASTRO® 25 TEK or KEK memory location (stored to a CKR and containing a KID), and the other way around.

8.1 When to Convert Keys

Converting keys is used most commonly for copying keys between ASN and ASTRO® 25 in the KVL memory.

There may be occasions when you have an existing key in an ASN memory location and wish to duplicate it for use on an ASTRO® 25 target. By converting the key from the ASN memory to ASTRO® 25 memory within the KVL, you save the effort of recreating the key in the ASTRO® 25 memory and reentering the encryption key data. You may also convert keys from the ASTRO® 25 memory and load them into the ASN memory.

8.2 Key Converting Restrictions and Guidelines

Observe the following restrictions and guidelines when converting keys:

- Only keys with AES, DES, DVP-XL, and DVI-XL algorithms can be converted.
- Keys of the same algorithm type stored in ASN memory cannot have duplicate KIDs.
- Traffic Keys (ASN) can be converted only to Traffic Encryption Keys (TEK) locations in ASTRO® 25 memory (and the other way around); Shadow Keys (ASN) can be converted only to Key Encryption Keys (KEK) locations in ASTRO® 25 memory (and the other way around).
- Keys can be converted only to an empty memory location; overwriting is not allowed.
- Keys must be converted one at a time.

8.3 Converting a Key from ASN to ASTRO 25

Prerequisites:
Only an Administrator can convert keys.

Procedure Steps

1 On the KVL main screen, select **Manage → Keys**.

Step result: The **Manage keys** screen appears, with a list of available Traffic keys.

Figure 8-1 Manage Keys Screen – Converting ASN Key (Example)

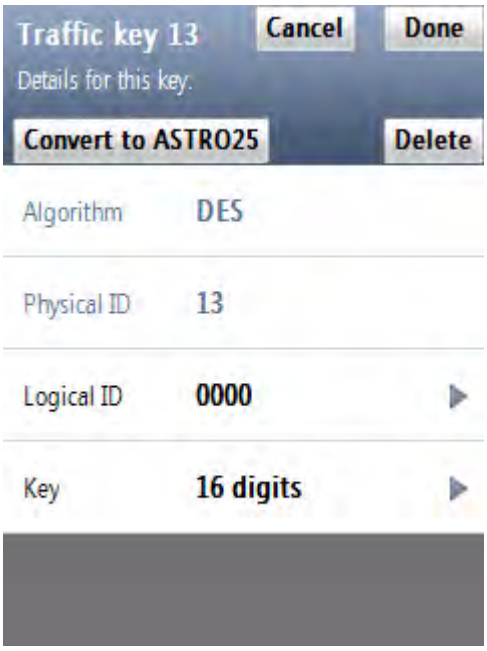
NOTE

To see the list of available Shadow keys, select the **Shadow** tab. You can use the smart bar on the right side of the screen to scroll through the list or quickly jump within the list to a selected area. If the list fits completely on the screen, the smart bar is disabled.

2 Select the desired key.

Step result: A screen with details for the selected key appears.

Figure 8-2 Converting to ASTRO 25 (Example)



3 Select **Convert to ASTRO25**.

Step result: If you have made changes to the key, you are prompted to confirm conversion. Otherwise, you are prompted to provide details for the ASTRO® 25 key.

4 From the list of available algorithms, select the algorithm for the key.

Step result: A screen with the decimal keypad appears, prompting you to enter the CKR ID for the key.

5 Enter the CKR ID using the decimal keypad.

NOTE

If you are converting a Traffic key, the valid CKR range is 1-4095. If you are converting a Shadow key, the valid CKR range is 61440-65535.

6 Tap **Convert >**.

Step result: A screen appears, informing that the conversion has completed successfully.

7 Tap **OK**.

8 Tap **Done**.

9 If you want to convert another key, perform step 2 through step 8 for this key. Otherwise, tap **Done** to return to the KVL main screen.

8.4 Converting a Key from ASTRO 25 to ASN

Prerequisites:
Only an Administrator can convert keys.

Procedure Steps

1 Select **Manage keys** on the KVL main screen.

Step result: A list of available keys appears.

Figure 8-3 Manage Keys Screen – Converting ASTRO 25 Key (Example)

NOTE

You can use the smart bar on the right side of the screen to scroll through the list or quickly jump within the list to a selected area. If the list fits completely on the screen, the smart bar is disabled.

2 Select the desired key.

Step result: A screen with details for the selected key appears.

Figure 8-4 Converting to ASN (Example)

3 Select **Convert to ASN**.

Step result: If you have made changes to the key, you are prompted to confirm conversion. Otherwise, a screen with the decimal keypad appears, prompting you to enter the Physical ID for the key.

4 Enter the PID for the key using the decimal keypad.

NOTE

The valid PID range is 0–511.

5 Tap **Convert >**.

Step result: A screen appears, informing that the conversion has completed successfully.

6 Tap **OK**.

7 If you want to convert another key, perform step 2 through step 6 for this key. Otherwise, tap **Done** to return to the KVL main screen.

9 Troubleshooting

9.1 Error Messages

Error messages displayed by the KVL can be divided into two types:

- **User Entry Errors** – Displayed in response to an illegal or disallowed action (such as entering an invalid value, entering a duplicate LID, and so on). See 9.1.1 User Entry Errors, page 9-1.
- **Operational Errors** – Displayed during normal operation in response to a user-initiated action, such as attempting to load a key to a target device. See 9.1.2 Operational Errors, page 9-2.

9.1.1 User Entry Errors

This section lists all possible user entry errors along with their probable causes and remedies.

Table 9-1 User Entry Errors

Error/Status Message	Probable Cause	Remedy
`Algorithm mismatch`	(Displayed for a single algorithm mismatch.) 1. During key loading, the KVL does not have the same algorithm as the radio. 2. During sharing, the KVLs do not have the same algorithm.	1. Use the KVL that has the same algorithm as the radio. 2. Purchase an appropriate algorithm and add it to the KVL or radio.
`[X] algorithm mismatches.`	(Displayed for more than one algorithm mismatch.) 1. During key loading, the KVL does not have the same algorithms as the radio. 2. During sharing, the KVLs do not have the same algorithms.	1. Use the KVL that has the same algorithms as the radio. 2. Purchase appropriate algorithms and add them to the KVL or radio.
`Oops Shadow key cannot be loaded. No Shadow keys on radio.`	Displayed when you try to load a Shadow key to a radio that does not support Shadow keys or MDC OTAR.	Use a radio that supports Shadow keys or MDC OTAR.

Table 9-1 User Entry Errors (cont'd.)

Error/Status Message	Probable Cause	Remedy
`Oops Traffic key cannot be loaded. Not enough slots available`	Displayed when you try to load a Traffic key to a radio that does not have enough Traffic key slots available.	Change the destination slot for your key loading to a smaller value. (A radio can have 1, 8, or 16 slots for keys.)
`Error Key could not be converted. Enter another CKR value.`	Displayed when you have entered a duplicate CKR value while attempting to convert an ASN PID key to an ASTRO® 25 CKR Key.	Enter another CKR value.
`Error Key could not be converted. Enter another PID value.`	Displayed when you have entered a duplicate PID value while attempting to convert an ASTRO® 25 CKR Key to an ASN PID key.	Enter another PID value.
`Error The key entered is weak. Enter a strong key.`	Displayed when you have entered key that has been determined to be cryptographically weak and unworthy for use in the system.	Try entering another key.
`Oops Red key transfers are not allowed in FIPS Level 3 mode.`	Displayed when an unencrypted (red) key transfer is initiated while in FIPS Level 3 mode, where only encrypted (black) key loading is allowed.	Use a radio that supports encrypted (black) key loading only, or change FIPS to Level 2.
`Error Duplicate Logical ID found.`	A key with this LID already exists in the KVL database.	Enter another LID value.
`Error Duplicate Physical ID found.`	A key with this PID already exists in the KVL database.	Enter another PID value.
`Error Duplicate Name found.`	The name you have entered for the key already exists.	Enter another name.

9.1.2 Operational Errors

This section lists all operational errors along with their probable causes and remedies.

For most of the operational errors, the cause is a faulty cable connection between the KVL and the target device. Ensure that the connection is good and try the operation again. If it still fails, contact Support (see 9.9 Contacting Motorola, page 9-13).

Table 9-2 Operational Errors

Error/Status Message	Probable Cause	Remedy
`Out of memory`	The KVL internal database is full and cannot store any more data.	Delete any items stored in the KVL to make room for new data. This includes items such as unused keys and log records.
`Load failed Cannot load beyond the radio's capacity.`	Displayed when the item to load points to a page or number of keys that is beyond the capacity of the radio. This situation can only happen if you switched radios after the KVL discovered the radios key capacity.	Do not switch radios while you are on the PID selection screen and do not select a key PID that is beyond the capacity of the connected radio.
`Error Load All could not be performed. {Out of memory}`	The destination radio or KVL cannot hold any more keys.	Remove any keys in the destination radio or KVL to make room for the keys that the KVL is trying to send.
`Error Load All could not be performed. {Algorithm mismatch}`	Displayed for a single algorithm mismatch during a share operation when the source KVL is trying to send a key to the destination KVL that has an algorithm that the destination KVL does not support.	Do not attempt to share keys with an algorithm that is not supported by the destination KVL.
`Error Load All could not be performed. {[X] algorithm mismatches.}`	Displayed for more than one algorithm mismatch during a share operation when the source KVL is trying to send a key to the destination KVL that has algorithms that the destination KVL does not support.	Do not attempt to share keys with algorithms that are not supported by the destination KVL.
`Unable to load Shadow keys The connected radio does not support Shadow keys.`	Displayed when a radio is connected, but no Shadow key destination slots are available. The radio does not support MDC OTAR.	Use a radio that supports Shadow keys or MDC OTAR.
`Error Database has been corrupted.`	The KVL has suffered an event that left its database corrupted and the resulting data cannot be trusted.	Perform a System Reset or exit the application.
`Error Security adapter not connected. Check connection.`	The Security Adapter got disconnected.	Reattach the Security Adapter and select **Retry connection**.
`Check radio's algorithm` (Displayed as a key subtitle)	An algorithm issue occurred.	Check the connection to the radio and make sure that the radio supports the algorithm of the key being loaded.

Table 9-2 Operational Errors (cont'd.)

Error/Status Message	Probable Cause	Remedy
`Not supported by radio` (Displayed as a key subtitle)	An algorithm is not supported.	Check the connection to the radio and make sure that the radio supports the algorithm of the key being loaded.
The KVL 3000/3000 Plus is emitting continuous success tones when connected to the KVL 4000 for sharing.	The KVL 4000 is trying to determine if the KVL 3000/3000 Plus is connected or disconnected.	Turn off the sound for the KVL 3000/3000 Plus.

9.2 Performing a System Reset

Resetting causes the KVL to erase the UKEKs, all stored keys, key groups, log records, and passwords, and reset the configuration settings to the factory defaults. For KVLs equipped for triple mode operation (ASN, ASTRO® 25, and Radio Authentication), resetting erases UKEKs, ASN keys, ASTRO® 25 keys, all stored radio – key pairs, macros, key groups, log records, and passwords.

Procedure Steps

1 On the KVL main screen, select **Settings → System reset**. Alternatively, if user authentication is set on your KVL, press the Windows key on the PDA and hold it for 5 seconds to go to the System Reset screen.

CAUTION

Use this option with caution as a system reset resets the KVL to its original state. All settings are reset and all data is deleted.

2 Drag the Reset System slider from left to right. Alternatively, highlight the slider and use the navigation key on the PDA to move it.

Step result: The system is being reset. When the action is completed, you are logged out of the KVL application and the Welcome screen appears.

Figure 9-1 KVL System Reset Slider – Subsequent States

9.3 Unlocking the Operator Account

Prerequisites:
Only an Administrator can unlock the Operator account.

Procedure Steps

1 Select **Settings → Security → Unlock operator account → Yes, unlock now**.

Step result: The Operator account is unlocked.

2 Tap **Done** on the consecutive screens to return to the KVL main screen.

9.4 Setting the PDA USB Mode

When and where to use:
Sometimes, the PDA may not automatically detect whether it should work in a Host mode (when connected to the Security Adapter), or in a Client mode (when connected to a PC). In such a case, use these steps to set the PDA USB mode manually.

Procedure Steps

1 On the Today screen, select  .

2 Select **Settings → System → USBConfig**.

3 Perform one of the following actions:

- If there are two options available (**USB Host** and **USB Client**), then select **USB Host** if you need to connect the PDA to the Security Adapter, or select **USB Client** if you need to connect the PDA to a PC.
- If there are three options available (**USB Host**, **USB Client**, and **USB OTG**), then select **USB OTG** to allow the KVL to auto detect whether it is connected to the Security Adapter or a PC.

9.5 KVL 4000 Disaster Recovery

Table 9-3 KVL 4000 Disaster Recovery

Event	Remedy
Hardware failure	Replace the device and reenter all the lost data. Refer to this manual to configure your KVL with all the necessary parameters.

Table 9-3 KVL 4000 Disaster Recovery (cont'd.)

Event	Remedy
	SUGGESTION Keep non-sensitive data in a secure location so that you can restore it quickly when needed.
KVL application failure	Reinstall the KVL application. See "Running the KVL Software Installation Wizard" in the *KVL 4000 FLASHPort Upgrade User Guide*.

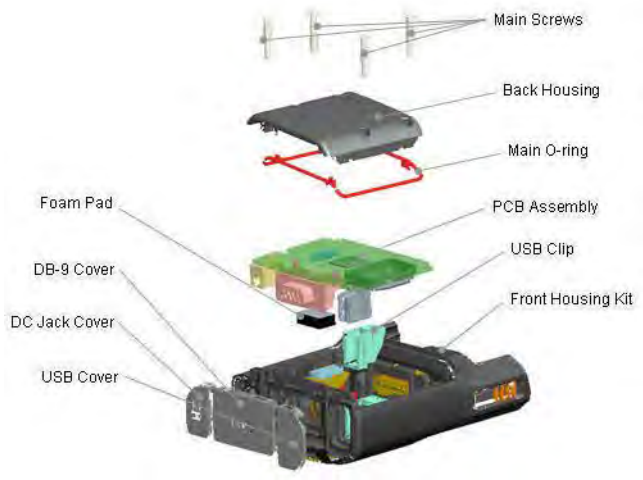
9.6 Troubleshooting KVL Application and/or VPN Software Failure

If you are experiencing problems with the KVL and/or NCP applications, follow "Running the KVL Software Installation Wizard" in the *KVL 4000 FLASHPort Upgrade User Guide* to reinstall the applications.

9.7 Disassembling the Security Adapter

When and where to use:
Use these steps to disassemble the Security Adapter.

Figure 9-2 Security Adapter – Exploded View



CAUTION

Make sure to exit the KVL application on the PDA before disconnecting the Security Adapter. Otherwise, you may lose any unsaved work or cause data corruption.

Procedure Steps

1 Remove the self-tapping screws and then remove the back housing.

Figure 9-3 Removing Back Housing

2 Remove the dust covers from the tongue features on the front housing.

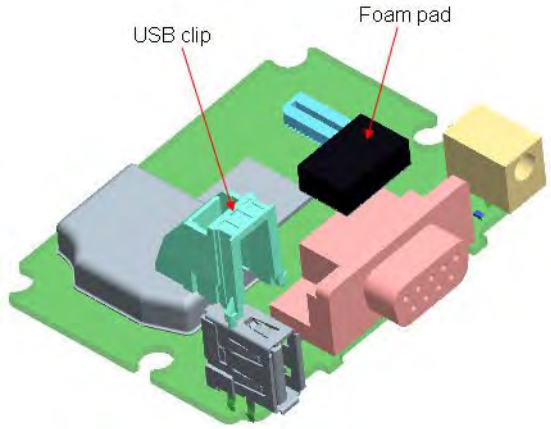
Figure 9-4 Removing Dust Covers

3 Remove the connectors from the front housing connector holes, disconnect the 30-pins board-to-board connector from the flex to the PCB, and remove the PCB assembly from the front housing.

Figure 9-5 Removing PCB Assembly

4 Remove the USB clip from the USB connector and the foam pad from the DB-9 connector on the PCB assembly.

Figure 9-6 Removing USB Clip and Foam Pad

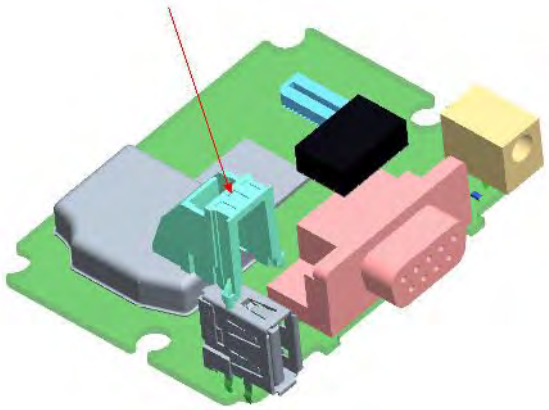


9.8 Assembling the Security Adapter

Procedure Steps

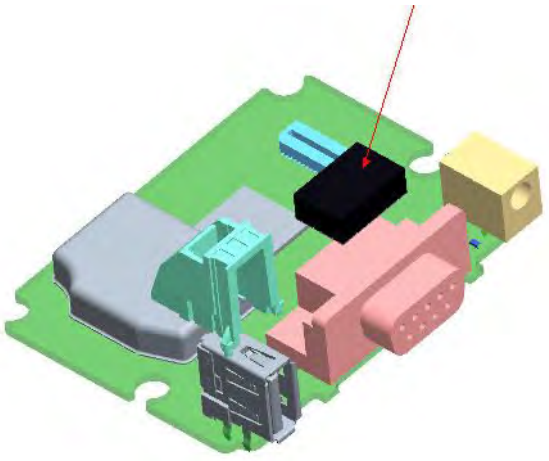
1 Attach the USB clip to the USB connector on the PCB.

Figure 9-7 Assembling USB Clip



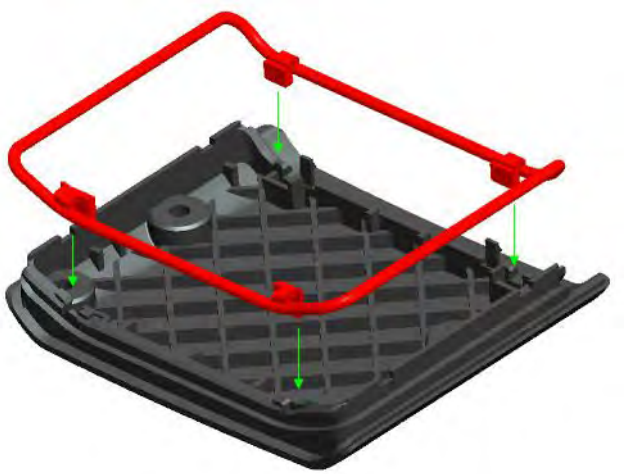
2 Attach the foam pad on top of the DB-9 connector. Ensure that the foam pad is aligned to the middle of the DB-9 face.

Figure 9-8 Assembling Foam Pad



3 Dress the O-ring to the O-ring groove at the back housing. Ensure that the O-ring tabs are slotted to the back housing features. Orient the O-ring so that its tabs' size matches the back housing features' size.

Figure 9-9 Assembling O-Ring



4 Connect the 30-pins board-to-board connector from the flex to the PCB.

Figure 9-10 Assembling Front Housing – PCB

5 Slot the connectors through the front housing connector holes.

Figure 9-11 Assembling Front Housing – Connectors

6 Place the PCB assembly to the front housing. Ensure the PCB sits properly on screw bosses.

Figure 9-12 Assembling Front Housing – PCB Placed

7 Slot in the dust cover retention holes through the tongue features on the front housing.

Figure 9-13 Assembling Dust Covers

8 Press down the back housing to the front housing vertically. Before closing the back housing, verify that the USB clip is assembled correctly.

Figure 9-14 Assembling Back Housing to Front Housing

9 Tighten the back housing with the self-tapping screws (tightening torque: 7 lbf.in).

Figure 9-15 Tightening Back Housing

10 Press the dust covers until they are flush with the front housing.

Figure 9-16 Pressing Dust Covers

Result:
The assembly is complete.

9.9 Contacting Motorola

This section contains information about calling Motorola for help.

9.9.1 Motorola System Support Center and Radio Support Center

After collecting the required information and writing a detailed problem report, contact one of the following support centers to help with the problem:

- Motorola System Support Center (SSC):
  - North America: 800-221-7144
  - International: 302-444-9800

NOTE

The Motorola System Support Center (SSC) provides technical support, return material authorization (RMA) numbers, and confirmations for troubleshooting results. Call the System Support Center for information about returning faulty equipment or ordering replacement parts.

- Motorola Radio Support Center:
  - Phone: 800-247-2346
  - Fax: 800-318-0281

NOTE

The Motorola Radio Support Center repairs mobile and portable radios, and related RF equipment.

9.9.2 North America Parts Organization

The North America Parts Organization is your source for manuals, replacement parts, and assemblies.

Table 9-4 North America Parts Organization Telephone Numbers

Purpose	Telephone Number
For ordering	• 800-422-4210 (US and Canada orders) • 302-444-9842 (International orders)
For Fax Orders	800-6226210 (US and Canada orders)
For help identifying an item or part number	800-422-4210; select choice 3 from the menu

Appendix A: KVL 4000 – Performance Specifications

Table A-1 Physical Characteristics

Item	Description
KVL (PDA + Security Adapter)	Height: 216 mm (8.5 in)
	Width: 84 mm (3.3 in)
	Depth: 39 mm (1.5 in)
	Weight: 473 g

Table A-2 Encryption

Supported Encryption Protocols	12 kbps Advanced SECURENET®
	9.6 kbps Secure ASTRO® (VSELP Vocoder)
	9.6 kbps Secure APCO Project 25 (IMBE Vocoder)
Encryption Keys	1,024 Total Traffic and Shadow Keys (ASN)
	Traffic Encryption Keys (TEK) and Key Encryption Keys (KEK) (ASTRO® 25)
Standards	FIPS 46-3
	FIPS 140-2
	FIPS 197

Table A-3 Supported Algorithms

Algorithm	ASN	ASTRO 25	KMF (ASTRO 25 Only)	Radio Authentication
DES	✓	✗	✗	✗
DES-XL	✗	✓	✓	✗
DES-OFB	✗	✓	✓	✗
DVI-XL	✓	✓	✓	✗
DVP-XL	✓	✓	✓	✗
AES-128	✗	✗	✗	✓
AES-256	✓	✓	✓	✗
ADP	✗	✓	✗	✗

NOTE

In the ASN mode, the KVL GUI does not distinguish between DES, DES-XL, and DES-OFB, but you can load keys for all DES types by selecting the DES option.

NOTE

ADP does not support the following features related to OTAR:

- Store & Forward
- KEK Key loading
- Tactical OTAR
- Remote Control Head Key loading

Table A-4 Electromagnetic Compatibility

EN 55022 Class A
EN 55024
FCC Part 15 Class A

Table A-5 Regulatory Compliance and Approvals

Safety	EN 60950-1
	UL 60950-1
	cUL 60950-1

Appendix B: KVL 4000 – Orderable Parts

Table B-1 KVL 4000 Model

Item	Count	Part Number
MC55 Kit (see Table B-2 MC55 Kit)	1	NNTN7864
Security Adapter Super Tanapa (see Table B-3 Security Adapter Super Tanapa)	1	NTN2564
KVL 4000 Documentation CD	1	CLN8627
KVL 4000 Quick Start Guide	1	6871015P34
DB9 Gender Changer	1	2871926H02
Packing Kit	1	HBN5096

Table B-2 MC55 Kit

Item	Count	Part Number
MC55 PDA	1	MC55A0-P30SWQQA79R
Power Supply	1	PWRS-14000-249S
Battery (2400 mAH)	1	BTRY-MC55EAB00
MC55 Quick Start Guide	1	72-127603-02
MC55 Regulatory Guide	1	72-108860-02

Table B-3 Security Adapter Super Tanapa

Item	Count	Part Number
Front Housing Assembly (see Table B-4 Front Housing Assembly – Orderable Parts)	1	01009328004
PCB Assembly Kit	1	NNTN7650
Back Housing	1	15009431001
Main O-ring	1	32009316001
Self tapping screw Dia. 3 x 18 mm	4	03009288001
USB Cover	1	32012053001
DB-9 Cover	1	32012052001
DC Jack Cover	1	32012051001
Foam Pad	1	75009419001
USB Clip	1	42009269001

Table B-4 Front Housing Assembly – Orderable Parts

Item	Count	Part Number
MX Dust Cover	1	32012050001

Table B-5 Interface Cables

Item	Part Number	Used with	Adaptor Required
Key Load Cable	TKN8531	XTL 5000/2500	TRN7414 (W Control Head) HKN6182 (M/O Control Head)
		XTS 5000/3000/2500	NTN8613
		ASTRO Spectra	TRN7414
		APX 7500/6500	HKN6182
		APX 7000/6000/4000	NNTN7869
		RNC, DIU, MGEG, MCC 7500 Console, KMF, PDEG, CDEM, KMF CryptR	n/a
	CKN6886	XTS 4000	n/a
	TDN9390	XTS 5000/3000/2500	n/a
	WPLN6904	APX 7000/6000/4000	n/a
	TKN1039	CRYPTR micro	n/a
OTAR / Radio Authentication Cable	HKN6183	APX 7500/6500, XTL 5000/2500, ASTRO Spectra	n/a
	NKN1027	XTS 4000	n/a
	RKN4106	XTS 5000/3000/2500	n/a
	WPLN6905	APX 7000/6000/4000	n/a
KVL To KVL Cable	TKN8209	KVL 3000/3000 Plus/4000	n/a
USB Programming Cable	25-108022-02R	PDA to PC	n/a
MINI-B to Type-A USB Cable	25-68596-01R	USB to Ethernet Adapter	n/a
Other	CKN6324	Serial Modem	n/a
	TKN8210	Service Monitor	n/a

Table B-6 Optional Accessories

Item	Part Number
AC Line Cord US	50-16000-182R
AC Line Cord cEE7/16 Plug	50-16000-255R
AC Line Cord BS 1363 Plug	50-16000-670R
AC Line Cord GB 2099-1-1996 Plug	50-16000-664R
AC Line Cord AS3112 Plug	50-16000-666R
AC Line Cord Brazil	50-16000-726R

Table B-6 Optional Accessories (cont'd.)

Item	Part Number
MultiMobile™ USB Modem V.92/56K	DSMT9234MUCDCXR
CradlePoint Technology USB to Ethernet Adapter	PS6U1UPE
3600mAH Battery	BTRY-MC55EAB02

Appendix C: Radio Frequency Interference Requirements

C.1 Radio Frequency Interference Requirements – USA

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user is required to correct the interference at his own expense.

C.2 Radio Frequency Interference Requirements – Canada

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numrique de la classe A est conforme la norme NMB-003 du Canada.

C.3 Radio Frequency Interference Requirements – European Union – EMC Directive 2004/108/EC

This is an EMC Class A product.

This product may cause interference if used in residential areas. Such use must be avoided unless the user takes special measures to reduce magnetic emissions to prevent interference to the reception of radio and television broadcast.

Appendix D: Acronyms

Table D-1 Acronyms

Item	Description
ADP	Advanced Digital Privacy
AES	Advanced Encryption Standard
AME	Assured Mobile Environment
ASN	Advanced SECURENET
CKR	Common Key Reference
CSK	Common Shadow Key
DES	Data Encryption Standard (Cipher)
DES-OFB	Data Encryption Standard-Output Feedback
DES-XL	Data Encryption Standard-Counter Addressing
DIU	Digital Interface Unit
DVI-XL	Digital Voice International-Range Extension
DVP	Digital Voice Protection
DVP-XL	Digital Voice Protection-Range Extension
FIPS	Federal Information Processing Standard
I/O	Input/Output
KID	Key ID
KEK	Key Encryption Key
KMF	Key Management Facility
KMM	Key Management Message
SEK	Signaling Encryption Key
KVL	Key Variable Loader
LED	Light Emitting Diode
LID	Logical ID
MDC	Motorola Data Communications
MGEG	Motorola Gold Elite Gateway
MNP	Message Number Period
OTAR	Over-the-Air Rekeying
PID	Physical ID
RNC	Radio Network Controller
RSI	Radio Set Identifier
TEK	Traffic Encryption Key
UKEK	Unique Key Encryption Key

Table D-1 Acronyms (cont'd.)

Item	Description
USK	Unique Shadow Key
VPN	Virtual Private Network
WACN	Wide Area Communications Network