AN15078

Enable SELinux with dm-verity Protected RootFS

Rev. 1.0 — 7 July 2026 **Application note**

Document information

Information	Content
Keywords	AN15078, i.MX 93 EVK, SELinux, dm-verity
Abstract	This application note describes how to combine SELinux and dm-verity on an i.MX 93 EVK image built with the NXP Yocto BSP.

1 Introduction

This application note describes how to combine SELinux and dm-verity on an i.MX 93 EVK image built with the NXP Yocto BSP. The implementation produces a verified read-only root filesystem while keeping selected system directories writable through overlayfs. It also documents the required first-boot labeling flow before switching SELinux from permissive mode to enforcing mode.

The main objective is to keep the root filesystem immutable and continuously verified while still allowing the system to maintain writable state in directories, such as /etc, /root, /var, and /home. The implementation is intended for BSP enablement, security evaluation, and product teams that need a baseline for combining integrity protection with mandatory access control.

2 Platform environment

The reference implementation uses the following baseline.

Table 1. Environment

Item	Value
Board	i.MX 93 EVK
BSP	lf-6.18.2, 2026 Q1 release
Manifest branch	imx-linux-whinlatter
Manifest file	imx-6.18.2-1.0.0.xml
Yocto machine	imx93evk
Yocto distro	fsl-imx-xwayland
Root filesystem image	imx-image-core
Verified rootfs type	ext4

3 Security model

Dm-verity validates block contents of the root filesystem through a hash tree. The protected root filesystem is mounted read only through a device-mapper node, so runtime writes cannot silently change verified rootfs contents.

SELinux enforces policy decisions based on process and object labels. On this image, the MLS policy provider is selected and SELinux userspace tools are included in imx-image-core.

Overlayfs supplies the writable state that a Linux system still needs when the base root filesystem is read-only. The lower directories come from the verified rootfs, while the upper and work directories are stored on a separate ext4 data partition. The first boot must run in permissive mode because the newly created overlay upper directories are initially unlabeled. After restorecon labels those directories, the system can reboot with SELinux enforcing mode enabled.

4 Reference software package contents

The reference software package provides the minimal BSP changes needed for the integration.

Table 2. Package content

Area	Provided change
meta-imx	Image and kernel recipe patch

Table 2. Package content*...continued*

Area	Provided change
`linux-imx`	Kernel defconfig patch
`meta-security`	`dm-verity env` generation patch
`meta-security-imx-dmverity`	`initramfs`, `overlayfs`, and WIC patch
Build configuration	`local.conf` fragment
Validation evidence	Boot and command log

In this document, paths inside the provided package are shown as `<reference_software_package>/...`.

5 Yocto integration

Follow below steps to build a Yocto image with `SELinux` and `dm-verity` support.

5.1 Initialize the BSP

Create the Yocto workspace and initialize the BSP source tree.

```
mkdir yocto
cd yocto
repo init -u https://github.com/nxp-imx/imx-manifest \
    -b imx-linux-whinlatter \
    -m imx-6.18.2-1.0.0.xml
repo sync
DISTRO=fsl-imx-xwayland MACHINE=imx93evk \
    source imx-setup-release.sh -b build-xwayland-93-6.18.2/
```

5.2 Add security layers

Add the `dm-verity` integration layer and the `SELinux`/security layers.

```
cd yocto/sources
git clone https://github.com/nxp-imx/meta-security-imx-dmverity.git
cd meta-security-imx-dmverity
git switch lf-6.18.y-1.0.0

cd ../../build-xwayland-93-6.18.2/
bitbake-layers add-layer ../sources/meta-security-imx-dmverity/
bitbake-layers add-layer ../sources/meta-security
bitbake-layers add-layer ../sources/meta-selinux
```

5.3 Apply BSP changes

To apply BSP changes, perform the following steps:

1. Apply the image and kernel integration patch to `meta-imx`.

```
cd yocto/sources/meta-imx
git apply <reference_software_package>/sources/meta-imx/meta-imx-enable-
selinux.patch
mkdir -p meta-imx-bsp/recipes-kernel/linux/files/
cp <reference_software_package>/sources/meta-imx/meta-imx-bsp/recipes-kernel/
linux/files/0001-enable-selinux-for-6.18.2.patch \
```

```
meta-imx-bsp/recipes-kernel/linux/files/
```

The kernel `defconfig` patch enables the security features required by `SELinux`.

```
CONFIG_AUDIT=y
CONFIG_NETWORK_SECMARK=y
CONFIG_EXT4_FS_SECURITY=y
CONFIG_SECURITY=y
CONFIG_SECURITYFS=y
CONFIG_SECURITY_NETWORK=y
CONFIG_SECURITY_SELINUX=y
CONFIG_SECURITY_SELINUX_BOOTPARAM=y
CONFIG_SECURITY_SELINUX_DEVELOP=y
CONFIG_SECURITY_SELINUX_AVC_STATS=y
CONFIG_AUDIT_GENERIC=y
```

2. Apply the `dm-verity` environment fix.

```
cd yocto/sources/meta-security
git apply <reference_software_package>/sources/meta-security/meta-security-
fix-verity-env.patch
```

This change strips unit annotations such as [bytes] from generated values before they are written to `/usr/share/misc/dm-verity.env`.

3. Apply the `overlayfs` and `initramfs` update.

```
cd yocto/sources/meta-security-imx-dmverity git apply
 <reference_software_package>/sources/meta-security-imx-dmverity/meta-
security-imx-dmverity-add-home-and-increase-overlayfs.patch
```

The overlay configuration becomes:

```
NEW_DIRS="root etc var work home" OVERLAY_DIRS="root etc var home"
```

The WIC data partition used for `overlayfs` is changed from 32 MB to 128 MB.

5.4 Configure the image

To configure the image, perform the following steps:

1. Append the configuration below to the build directory `conf/local.conf`.

```
DISTRO_FEATURES:append = " acl xattr pam selinux"
PREFERRED_PROVIDER_virtual/refpolicy ?= "refpolicy-mls"

DISTRO_FEATURES:append = " security"
INITRAMFS_IMAGE = "dm-verity-image-initramfs"
DM_VERITY_IMAGE = "imx-image-core"
DM_VERITY_IMAGE_TYPE = "ext4"
IMAGE_CLASSES += "dm-verity-img dm-verity-verify-roothash"
DM_VERITY_SEPARATE_HASH = "1"
INITRAMFS_IMAGE_BUNDLE = "1"
IMAGE_BOOT_FILES:append = "${KERNEL_IMAGETYPE}-initramfs-${MACHINE}.bin"
WKS_FILES = "imx-imx-boot-bootpart-dmverity-hash-overlay.wks.in"
OVERLAYFS_UUID = "94a69ec6-abb5-41e1-b0b1-bfd15e004d66"
```

2. Build the image.

```
bitbake imx-image-core
```

6 Boot-time configuration

To boot the device with proper configuration, perform the following steps:

1. Flash the generated WIC image.

```
uuu -b emmc_all tmp/deploy/images/imx93evk/imx-image-core-
imx93evk.rootfs.wic.zst
```

2. Use the `initramfs-bundled` kernel image for `dm-verity` boot. On first boot, add `enforcing=0` so the system can create and label overlay-backed directories.

```
u-boot=> editenv image
edit: Image-initramfs-imx93evk.bin
u-boot=> editenv mmcargs edit: setenv bootargs ${jh_clk} ${mcore_clk}
 console=${console} root=${mmcroot} rootrw=UUID="94a69ec6-abb5-41e1-b0b1-
bfd15e004d66" enforcing=0
u-boot=> editenv fdt_addr_r
edit: 0x87000000
u-boot=> saveenv
u-boot=> boot
```

The `rootrw= UUID` must match `OVERLAYFS_UUID` in `local.conf`.

7 Labeling and enforcing-mode bring-up

To check the status and recover the filesystem, perform the following steps:

1. After first boot, confirm that SELinux is enabled and currently permissive.

```
sestatus
```

Expected key fields:

```
SELinux status:                 enabled
Loaded policy name:             mls
Current mode:                   permissive
Mode from config file:          enforcing
Policy MLS status:              enabled
```

2. Confirm that the verified root filesystem and overlay directories are mounted.

```
df -h
mount | grep overlay
```

Expected rootfs and overlay indicators:

```
/dev/mapper/rootfs  1.8G  1.4G  271M  84% /
overlay             119M  2.1M  108M   2% /root
overlay             119M  2.1M  108M   2% /etc
overlay             119M  2.1M  108M   2% /var
overlay             119M  2.1M  108M   2% /home
```

The first boot can show unlabeled files in overlay-backed directories.

```
ls -Z /etc/ld.so.cache
```

Example before relabeling:

```
system_u:object_r:unlabeled_t:s0 /etc/ld.so.cache
```

3. Relabel the persistent overlay-backed directories.

```
restorecon -RF /etc
```

```
restorecon -RF /root
restorecon -RF /home
restorecon -RF /var
```

4. Confirm that labels were restored.

```
ls -Z /etc/ld.so.cache
```

Expected example:

```
system_u:object_r:ld_so_cache_t:s0 /etc/ld.so.cache
```

5. Reboot and switch to enforcing mode.

```
u-boot=> editenv mmcargs
edit: setenv bootargs ${jh_clk} ${mcore_clk} console=${console} root=
${mmcroot} rootrw=UUID="94a69ec6-abb5-41e1-b0b1-bfd15e004d66" enforcing=1
u-boot=> saveenv
u-boot=> boot
```

8 Verification checklist

The boot log must show `dm-verity` initialization.

```
device-mapper: verity: sha256 using "sha256-lib"
```

The SELinux policy must load successfully.

```
systemd[1]: Successfully loaded SELinux policy
```

After rebooting with `enforcing=1`, `sestatus` must report enforcing mode.

```
SELinux status:                 enabled
Loaded policy name:             mls
Current mode:                   enforcing
Mode from config file:          enforcing
```

The root filesystem should remain backed by `/dev/mapper/rootfs`, and `/root`, `/etc`, `/var`, and `/home` should remain mounted as `overlayfs`. The label check should continue to show normal SELinux types instead of `unlabeled_t`.

9 Recommendations

Use permissive mode only for initial policy and label bring-up. Before production, review AVC messages, remove unnecessary permissive behavior, and keep only required SELinux policy allowances.

Keep the verified root filesystem immutable after image generation. Application state should be directed to intentionally writable partitions or overlay-backed paths.

Treat `OVERLAYFS_UUID` as a deployment parameter. The value in Yocto configuration, U-Boot boot arguments, and the WIC layout must remain synchronized.

Size the overlay partition according to product write volume, log retention requirements, and update strategy. Avoid using the overlay partition as a general-purpose data store unless it is sized and monitored for that role.

10 Acronyms and definitions

Table 3. Acronyms and definitions

Acronym	Definition
AVC	Access Vector Cache
BSP	Board Support Package
DM	Device Mapper
DTB	Device Tree Blob
EVK	Evaluation Kit
GPT	GUID Partition Table
MLS	Multi-Level Security
SELinux	Security-Enhanced Linux
UUID	Universally Unique Identifier
UUU	Universal Update Utility
WIC	OpenEmbedded Image Creator

11 Related documentation

Table 4 lists and explains the additional documents and resources that you can refer to for more information.

Table 4. Related documentation

Document	Link / how to access
NXP i.MX Linux Reference Manual	RM00293
NXP i.MX Linux Yocto Project User's Guide	UG10164
Yocto Project Development Tasks Manual	Yocto Project Development Tasks Manual — The Yocto Project 6.0-tip documentation
SELinux Project documentation	meta-selinux - Layer enabling SELinux support

12 Note about the source code in the document

Example code shown in this document has the following copyright and BSD-3-Clause license:

Copyright 2026 NXP 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 must be provided with the distribution.
3. Neither the name of the copyright holder 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 HOLDER 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.

13 Revision history

Section 13 summarizes the revisions to this document.

Table 5. Revision history

Document ID	Release date	Description
AN15078 v.1.0	7 July 2026	Initial public release

Legal information

Definitions

Draft — A draft status on a document indicates that the content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included in a draft version of a document and shall have no liability for the consequences of use of such information.

Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at https://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Suitability for use in non-automotive qualified products — Unless this document expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications.

In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

HTML publications — An HTML version, if available, of this document is provided as a courtesy. Definitive information is contained in the applicable document in PDF format. If there is a discrepancy between the HTML document and the PDF document, the PDF document has priority.

Translations — A non-English (translated) version of a document, including the legal information in that document, is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — Customer understands that all NXP products may be subject to unidentified vulnerabilities or may support established security standards or specifications with known limitations. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately.

Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP.

NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

NXP B.V. — NXP B.V. is not an operating company and it does not distribute or sell products.

Trademarks

Notice: All referenced brands, product names, service names, and trademarks are the property of their respective owners.

NXP — wordmark and logo are trademarks of NXP B.V.

Contents

1 Introduction 2
2 Platform environment 2
3 Security model 2
4 Reference software package contents 2
5 Yocto integration 3
5.1 Initialize the BSP 3
5.2 Add security layers 3
5.3 Apply BSP changes 3
5.4 Configure the image 4
6 Boot-time configuration 5
7 Labeling and enforcing-mode bring-up 5
8 Verification checklist 6
9 Recommendations 6
10 Acronyms and definitions 7
11 Related documentation 7
12 Note about the source code in the document 7
13 Revision history 8
Legal information 9