Question: How to enable dm-verity on Android-N when A/B partitions feature enabled ?

[**Answer**]

We have a CR-1116507 for it. Generally, need to apply 3 changes in code,
1. Add keyring certification for verity.
2. Enable the config SYSTEM_TRUSTED_KEYS.
3. Update command line required for dm-verity.

For example, on MSM8998, these changes would be as below.

- https://source.codeaurora.org/quic/la/kernel/msm-4.4/commit/certs/verity.x509.pem?h=kernel.lnx.4.4.r13-rel&id=8aa8a192db72fd0750e50d46f7536bc99599b406

```
diff --git a/certs/verity.x509.pem b/certs/verity.x509.pem
new file mode 100644
index 0000000..86399c3
--- /dev/null
+++ b/certs/verity.x509.pem
@@ -0,0 +1,24 @@
+-----BEGIN CERTIFICATE-----
+MIID/TCCAuWgAwIBAgIJAJcPmDkJqolJMA0GCSqGSIb3DQEBBQUAMIGUMQswCQYD
+VQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNTW91bnRhaW4g
+VmlldzEQMA4GA1UECgwHQW5kcm9pZDEQMA4GA1UECwwHQW5kcm9pZDEQMA4GA1UE
+AwwHQW5kcm9pZDEiMCAGCSqGSIb3DQEJARYTYW5kcm9pZEBhbmRyb2lkLmNvbTAe
+Fw0xNDExMDYxOTA3NDBaFw00MjAzMjQxOTA3NDBaMIGUMQswCQYDVQQGEwJVUzET
+MBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNTW91bnRhaW4gVmlldzEQMA4G
+A1UECgwHQW5kcm9pZDEQMA4GA1UECwwHQW5kcm9pZDEQMA4GA1UEAwwHQW5kcm9p
+ZDEiMCAGCSqGSIb3DQEJARYTYW5kcm9pZEBhbmRyb2lkLmNvbTCCASIwDQYJKoZI
+hvcNAQEBBQADggEPADCCAQoCggEBAOjreE0vTVSRenuzO9vnaWfk0eQzYab0gqpi
+6xAzi6dmD+ugoEKJmbPiuE5Dwf21isZ9uhUUu0dQM46dK4ocKxMRrcnmGxydFn6o
+fs3ODJMXOkv2gKXL/FdbEPdDbxzdu8z3yk+W67udM/fW7WbaQ3DO0knu+izKak/3
+T41c5uoXmQ81UNtAzRGzGchNVXMmWuTGOkg6U+0I2Td7K8yvUMWhAWPPpKLtVH9r
+AL5TzjYNR92izdKcz3AjRsI3CTjtpiVABGeX0TcjRSuZB7K9EK56HV+OFNS6I1NP
+jdD7FIShyGlqqZdUOkAUZYanbpgeT5N7QL6uuqcGpoTOkalu6kkCAwEAAaNQME4w
+HQYDVR0OBBYEFH5DM/m7oArf4O3peeKO0ZIEkrQPMB8GA1UdIwQYMBaAFH5DM/m7
+oArf4O3peeKO0ZIEkrQPMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEB
+AHO3NSvDE5jFvMehGGtS8BnFYdFKRIglDMc4niWSzhzOVYRH4WajxdtBWc5fx0ix
+NF/+hVKVhP6AIOQa+++sk+HIi7RvioPPbhjcsVlZe7cUEGrLSSveGouQyc+j0+m6
+JF84kszIl5GGNMTnx0XRPO+g8t6h5LWfnVydgZfpGRRg+WHewk1U2HlvTjIceb0N
+dcoJ8WKJAFWdcuE7VIm4w+vF/DYX/A2Oyzr2+QRhmYSv1cusgAeC1tvH4ap+J1Lg
```

```
+UnOu5Kh/FqPLLSwNVQp4Bu7b9QFfqK8Moj84bj88NqRGZgDyqzuTrFxn6FW7dmyA
+yttuAJAEAymk1mipd9+zp38=
+-----END CERTIFICATE-----
--
```

- https://source.codeaurora.org/quic/la/kernel/msm-4.4/commit/certs/Makefile?h=kernel.lnx.4.4.r13-rel&id=8aa8a192db72fd0750e50d46f7536bc99599b406

```
diff --git a/certs/Makefile b/certs/Makefile
index 28ac694..f30d601 100644
--- a/certs/Makefile
+++ b/certs/Makefile
@@ -17,6 +17,10 @@ AFLAGS_system_certificates.o := -I$(srctree)
quiet_cmd_extract_certs = EXTRACT_CERTS $(patsubst "%",%,$(2))
cmd_extract_certs = scripts/extract-cert $(2) $@ || ( rm $@; exit 1)
+ifeq ($(CONFIG_SYSTEM_TRUSTED_KEYS),"verity.x509.pem")
+SYSTEM_TRUSTED_KEYS_SRCPREFIX := $(srctree)/certs/
+endif
+
targets += x509_certificate_list
$(obj)/x509_certificate_list: scripts/extract-cert $(SYSTEM_TRUSTED_KEYS_SRCPREFIX)$(
SYSTEM_TRUSTED_KEYS_FILENAME) FORCE
$(call if_changed,extract_certs,$(SYSTEM_TRUSTED_KEYS_SRCPREFIX)$(
CONFIG_SYSTEM_TRUSTED_KEYS))
--
```

- https://source.codeaurora.org/quic/la/kernel/msm-4.4/commit/arch/arm64/configs/msmcortex-perf_defconfig?h=kernel.lnx.4.4.r13-rel&id=7b1c893c09599e995333048957bb99d4d343a70e

```
diff --git a/arch/arm64/configs/msmcortex-perf_defconfig b/arch/arm64/configs/
msmcortex-perf_defconfig
index f64ca9a..65d4fa8 100644
--- a/arch/arm64/configs/msmcortex-perf_defconfig
+++ b/arch/arm64/configs/msmcortex-perf_defconfig
@@ -628,6 +628,7 @@ CONFIG_CRYPTO_DEV_QCOM_MSM_QCE=y
CONFIG_CRYPTO_DEV_QCEDEV=y
CONFIG_CRYPTO_DEV_OTA_CRYPTO=y
CONFIG_CRYPTO_DEV_QCOM_ICE=y
+CONFIG_SYSTEM_TRUSTED_KEYS="verity.x509.pem"
CONFIG_ARM64_CRYPTO=y
CONFIG_CRYPTO_SHA1_ARM64_CE=y
CONFIG_CRYPTO_SHA2_ARM64_CE=y
```

--

- https://source.codeaurora.org/quic/la/kernel/msm-4.4/commit/arch/arm64/configs/msmcortex_defconfig?h=kernel.lnx.4.4.r13-rel&id=7b1c893c09599e995333048957bb99d4d343a70e

```
diff --git a/arch/arm64/configs/msmcortex_defconfig b/arch/arm64/configs/msmcortex_defconfig
index f08cd3b..db8617c 100644
--- a/arch/arm64/configs/msmcortex_defconfig
+++ b/arch/arm64/configs/msmcortex_defconfig
@@ -694,6 +694,7 @@ CONFIG_CRYPTO_DEV_QCOM_MSM_QCE=y
CONFIG_CRYPTO_DEV_QCEDEV=y
CONFIG_CRYPTO_DEV_OTA_CRYPTO=y
CONFIG_CRYPTO_DEV_QCOM_ICE=y
+CONFIG_SYSTEM_TRUSTED_KEYS="verity.x509.pem"
CONFIG_ARM64_CRYPTO=y
CONFIG_CRYPTO_SHA1_ARM64_CE=y
CONFIG_CRYPTO_SHA2_ARM64_CE=y
--
```

- https://source.codeaurora.org/quic/la/abl/tianocore/edk2/commit/QcomModulePkg/Library/BootLib/UpdateCmdLine.c?h=uefi.lnx.1.0.r13-rel&id=109199d787251924779e5295486a649cccca4828

```
diff --git a/QcomModulePkg/Library/BootLib/UpdateCmdLine.c b/QcomModulePkg/Library/BootLib/UpdateCmdLine.c
index f876f89..31a04ef 100644
--- a/QcomModulePkg/Library/BootLib/UpdateCmdLine.c
+++ b/QcomModulePkg/Library/BootLib/UpdateCmdLine.c
@@ -57,6 +57,7 @@ STATIC CONST CHAR8 *AlarmBootCmdLine = " androidboot.alarmboot=true";
STATIC CHAR8 *AndroidSlotSuffix = " androidboot.slot_suffix=";
STATIC CHAR8 *MultiSlotCmdSuffix = " rootwait ro init=/init";
STATIC CHAR8 *SkipRamFs = " skip_initramfs";
+STATIC CHAR8 *DmVerityCmd = " root=/dev/dm-0 dm=\"system none ro,0 1 android-verity";
STATIC CHAR8 *SystemPath;
/* Assuming unauthorized kernel image by default */
@@ -273,11 +274,12 @@ STATIC UINT32 GetSystemPath(CHAR8 **SysPath)
return 0;
}
- if (!AsciiStrCmp("EMMC", RootDevStr))
- AsciiSPrint(*SysPath, MAX_PATH_SIZE, " root=/dev/mmcblk0p%d", Index);
- else
- AsciiSPrint(*SysPath, MAX_PATH_SIZE, " root=/dev/sd%c%d", LunCharMapping[Lun],
+ if (!AsciiStrCmp("EMMC", RootDevStr)) {
+ AsciiSPrint(*SysPath, MAX_PATH_SIZE, " /dev/mmcblk0p%d\"", Index);
+ } else {
+ AsciiSPrint(*SysPath, MAX_PATH_SIZE, " /dev/sd%c%d\"", LunCharMapping[Lun],
GetPartitionIdxInLun(PartitionName, Lun));
+ }
DEBUG((EFI_D_VERBOSE, "System Path - %a \n", *SysPath));
@@ -407,6 +409,10 @@ EFI_STATUS UpdateCmdLine(CONST CHAR8 * CmdLine,
if (!Recovery)
CmdLineLen += AsciiStrLen(SkipRamFs);
+ }
+
+ if (VerifiedBootEnbled()) {
+ CmdLineLen += AsciiStrLen(DmVerityCmd);
SysPathLength = GetSystemPath(&SystemPath);
if (!SysPathLength)
@@ -528,7 +534,7 @@ EFI_STATUS UpdateCmdLine(CONST CHAR8 * CmdLine,
STR_COPY(Dst,Src);
}
- if (MultiSlotBoot && !AsciiStrStr(CmdLine, "root=")) {
+ if (MultiSlotBoot) {
/* Slot suffix */
Src = AndroidSlotSuffix;
if (HaveCmdLine) --Dst;
@@ -550,9 +556,15 @@ EFI_STATUS UpdateCmdLine(CONST CHAR8 * CmdLine,
Src = MultiSlotCmdSuffix;
if (HaveCmdLine) --Dst;
STR_COPY(Dst, Src);
+ }
+ if (VerifiedBootEnbled() && !AsciiStrStr(CmdLine, "root=")) {
/* Suffix System path in command line*/
if (*SystemPath) {
+ Src = DmVerityCmd;
+ if (HaveCmdLine) --Dst;
+ STR_COPY(Dst, Src);
+
Src = SystemPath;
if (HaveCmdLine) --Dst;
STR_COPY(Dst, Src);
```

- -