Security Guidelines for AudioCodes Native Teams Android-based Devices

Introduction

AudioCodes Native Teams devices are Android-based and purpose-built for Teams calling and meetings, with customizations specifically designed to enhance security and reduce the attack surface.

AudioCodes prioritizes device security, ensuring that its Android-based devices offer a higher level of protection compared to standard Android devices.

For more details, please refer to the information provided later in this document.

When analyzing the security of the device, the following levels should be addressed:

- Authentication and security with regards to Microsoft Teams connectivity and use
- Android system level security
- Hardware level security

Microsoft Teams Security Guidelines

- With regards to AudioCodes Native Teams devices, AudioCodes recommends the following:
  - Use the **Sign-in with other device** option; using this mode, the user does not type the password on their device but instead obtains a code to be used to sign-in on their PC/laptop; the device obtains a private token that enables it to access Teams cloud; this token, unlike a password, allows only that device which obtained it to reuse it. The token is stored on the secured file system.
  - Leverage Multi-Factor Authentication (MFA) to improve sign-in security.
  - IT can consider reducing the expiration time of the sign-in for devices which are connected remotely (outside the organization network) vs. devices on the organization's premises.
- AudioCodes recommends that customers visit Microsoft's technical pages and learn more on security guidelines and policies for Microsoft Teams adoption:
  - Overview of security and compliance - Microsoft Teams | Microsoft Docs
  - Identity models and authentication for Microsoft Teams - Microsoft Teams | Microsoft Docs
  - Sign into Microsoft Teams - Microsoft Teams | Microsoft Docs

Android Level Security Hardening

This section describes the major changes performed on the system/Android level that were incorporated into the AudioCodes Native Teams device to improve its security.

Google Play Services

Google Play services were removed from the AudioCodes Native Teams device software. No access to any Google store or Play services is allowed.

AudioCodes Native Teams device update of the Android software and application is securely performed via special software components that connect to Teams Admin Center or to AudioCodes' Device Manager over a secured channel.

Running Android in Kiosk Mode

AudioCodes Native Teams devices run in Android Kiosk mode.

Only specific Microsoft apps and AudioCodes-signed apps that were certified and approved in the certification process can run when the device is in Kiosk mode. Even if a malicious user manages to install a new unauthorized app on the file system, the user will be blocked from launching it. The launcher on the AudioCodes Native Teams device will only run apps that are approved, and this cannot be changed in runtime.

Screen Lock

AudioCodes Native Teams phones use a screen lock mechanism to prevent any malicious user/users from gaining access to Calendar information and / or Active Directory list of employees and / or triggering unauthorized Teams calls from the device. After enabling screen lock, the device automatically locks after a preconfigured period; a code is required to unlock the device and resume full operation.

Remote Configuration Management

The AudioCodes Native Teams device does not have an embedded WEB server. Configuration and management is performed using one of the following remote interfaces:

- Microsoft Teams Admin Center (for Native Teams devices) over HTTPS protocols – this is enabled after successful sign-in authentication process.
- AudioCodes Device Manager (part of AudioCodes OVOC suite) over HTTPS.

Secured Access to AudioCodes Management System

The AudioCodes Native Teams device connection to AudioCodes management systems (for example, Device Manager and Redirect Service) require trusted TLS authentication.

Signed Builds

AudioCodes enhances security by signing the builds of its Native Teams devices for release. This process ensures:

- **Signed APKs**: Verifies that applications on the device are authentic and untampered.
- **Signed Platform Images**: Confirms that the operating system images are secure and trusted.
- **Signed OTA Updates**: Guarantees that over-the-air updates are legitimate and safe to install.

These measures protect against unauthorized modifications, providing users with a secure and reliable experience on AudioCodes Native Teams devices.

Apps Signature Verification

Applications on AudioCodes Native Teams devices must be signed by either AudioCodes or Microsoft. The device verifies that apps are signed by these trusted entities. This app signing process prevents malicious users from replacing a legitimate Microsoft-signed / AudioCodes-signed app with a counterfeit app that lacks the private key known only to Microsoft / AudioCodes.

Data Security

AudioCodes Native Teams devices use Android Application Sandbox so that each application can access only its own data and is isolated from other applications. This prevents a malicious app from accessing the code or the data of other applications in the system.

Data Deletion

The device deletes all business data on the applications when restored to factory settings, ensuring data security.

Device File System Encryption

The AudioCodes Native Teams device file system is encrypted to protect the data stored on the device. This encryption ensures that even if a device is lost or stolen, data remains secure and inaccessible to unauthorized users.

Device Certificate

AudioCodes Native Teams devices are shipped with a unique certificate which is signed by AudioCodes Root CA (see *Appendix A – AudioCodes Root CA Certificate*).

Certificate enrollment can be utilized to apply and manage customer-specific certificates. This process allows customers to use their own certificates for enhanced security and compliance with their internal policies.

Keystore

With AudioCodes Native Teams devices, the certificate keys are stored in TrustZone (TEE).

Password Complexity

AudioCodes Native Team devices enforce a password replacement of the default device administrator upon initial login. For security reasons, the new password must be a complex password consisting of at least 8 characters and containing letters, numbers, and special symbols.

Android Security Updates

In addition to all the above, AudioCodes continuously reviews and integrates Android security updates. For reference, go to https://source.android.com/security/bulletin/2019-10-01 .

Hardware Level Security Hardening

Disabling USB Port

The USB port of AudioCodes Native Teams phones can be disabled by the administrator. Once the device's USB port is disabled, the phone cannot detect a plugged-in USB device. Additionally, all USB-related settings are removed from the phone's user interface.

Debugging Interface

On AudioCodes devices, UART serial port, ADB, Telnet, and other device debugging interfaces are blocked, ensuring protection against unauthorized access and potential data risks.

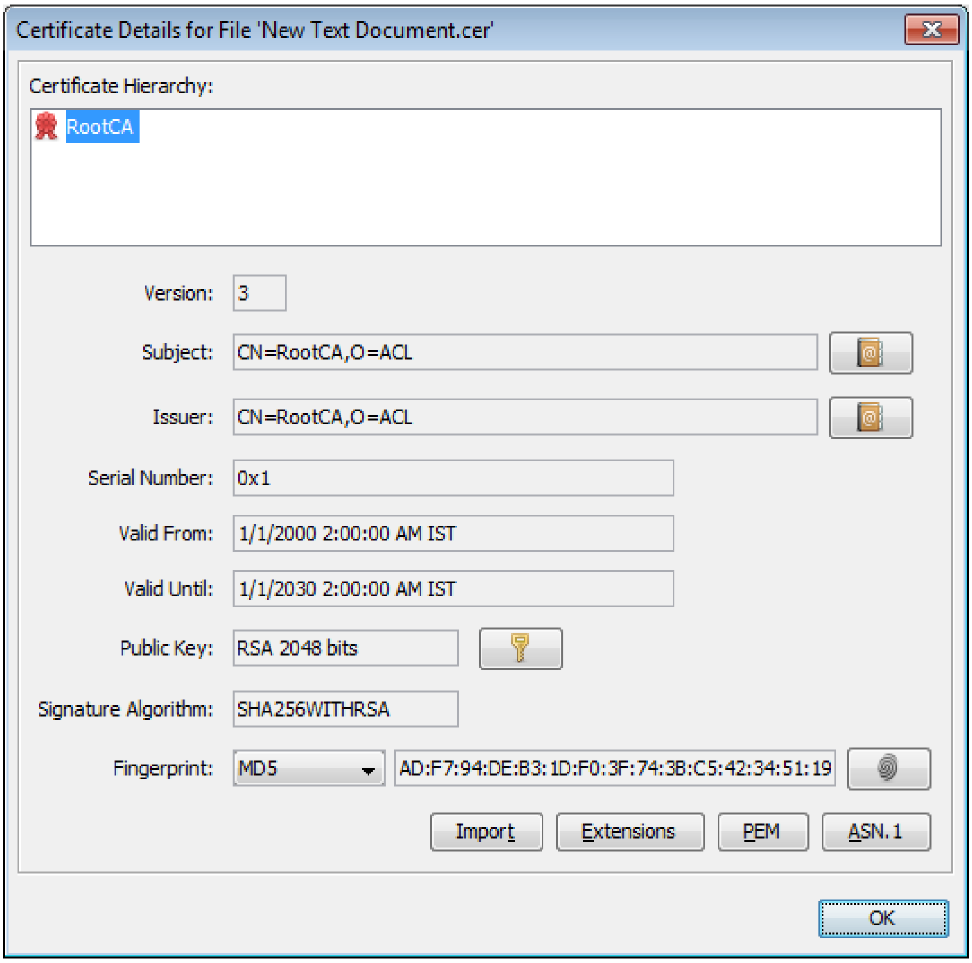
AudioCodes Native Teams devices leverage SSH as a limited debugging interface (for example, bug reporting, configuration changes, and firmware updates).

- On AudioCodes devices SSH is disabled by default.
- AudioCodes recommends changing the Admin password from the default, prior to a SSH debug session. It can be done via Teams Admin Center or AudioCodes Device Manager (OVOC).
- When debugging of a specific device is required, the user can enable SSH on specific device/s, access SSH with the new Admin password for debugging phase and disable SSH once debugging has been completed.

Additional Links

- AudioCodes Security Vulnerability Handling for SBCs, OVOC, Phones & ARM (Android-Level Security Hardening)
- AudioCodes Data Processing Policy

Appendix A – AudioCodes Root CA Certificate



Certificate Details for File 'New Text Document.cer'

Certificate Hierarchy:

RootCA

Version: 3

Subject: CN=RootCA,O=ACL

Issuer: CN=RootCA,O=ACL

Serial Number: 0x1

Valid From: 1/1/2000 2:00:00 AM IST

Valid Until: 1/1/2030 2:00:00 AM IST

Public Key: RSA 2048 bits

Signature Algorithm: SHA256WITHRSA

Fingerprint: MD5 AD:F7:94:DE:B3:1D:F0:3F:74:3B:C5:42:34:51:19

```
-----BEGIN CERTIFICATE-----
MIIDMTCCAhmgAwIBAgIBATANBgkqhkiG9w0BAQsFADAfMQwwCgYDVQQKEwNBQ0wx
DzANBgNVBAMTBlJvb3RDQTAeFw0wMDAxMDEwMDAwMDBaFw0zMDAxMDEwMDAwMDBa
MB8xDDAKBgNVBAoTA0FDTDEPMA0GA1UEAxMGUm9vdENBMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEA6GK495KUCXAm/UE17G4/cjnZN4LNaxYEYzbfZL0a
EhgSKYt/LQ+iUcDhojsneusNgrcGkpwKklKsGsvGWmSRNULV01CW+TX2VJN73+hh
V0uzhyOIYAUhbDaoqNM6Kp5b7sJ1ew4Ig9kfd/ma9Czl5koESLlw/inLj/r+rD96
mUcPElWrKspv7Qy4I14fsK/yMArixRopTL1munVVPpSFM9Jh8IY3JHyr5CQJXKKs
EhGAJsnHaRqsR2Su3X/WtslgEF+cvP34pxhlhFL29nMfnaFATSS3rgGaFlSvl1ZS
esLMqkWjp9cqGYrvt7K61sYnvMMb+o/KbWqVokXb+Fr7bwIDAQABo3gwdjAMBgNV
HRMEBTADAQH/MB0GA1UdDgQWBBQDXySn9hz15lDraZ+iXddZGReB+zBHBgNVHSME
QDA+gBQDXySn9hz15lDraZ+iXddZGReB+6EjpCEwHzEMMAoGA1UEChMDQUNMMQ8w
DQYDVQQDEwZSb290Q0GCAQEwDQYJKoZIhvcNAQELBQADggEBAI0rUywommWWJnH3
JOfKiS3+VnX5hJITZymvWanMXUz/6FonHccPXEBYTrUYwhiWx3dwELAFXDFKkxMp
0KKWZ4F39cAOLRjqhzya+xUeeJ9HQZCXYAJ6XgvTfN2BtyZk9Ma8WG+H1hNvvTZY
QLbWsjQdu4eFniEufeYDke1jQ6800LwMlFlc59hMQCeJTenRx4HdJbJV86k1gBUE
A7fJT1ePrRnXNDRz6QtADWoX3OmN7Meqen/roTwvLpEP22nYwvB28dq3JetlQKwu
XC4gwI/o8K2wo3pySLU9Y/vanxXCr0/en5l3RDz1YpYWmQwHA8jJIu8rxdhr+VNQ
Zv6R/Ys=
-----END CERTIFICATE----
```