Security Guidelines

AudioCodes Native Teams Android-based Devices

Introduction

AudioCodes' Native Teams devices are Android-based devices purpose-built and customized for Teams calling and meeting and designed to enhance security as part of the default use.

Though customers might perceive Android-based systems as prone to security issues, security is much less of a concern on these devices because they're purpose-built for Teams meeting and calling.

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

- Authentication and security with regards to Teams connectivity and use
- Android level / system of the device

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 in to 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.

AudioCodes Inc.
200 Cottontail Lane, Suite A101E, Somerset, NJ 08873
Tel: +1-732-469-0880 Fax: +1-732-469-2298

International Headquarters
1 Hayarden Street, Airport City, Lod 7019900
P.O.Box 255, Ben Gurion Airport, Israel 7019900
Tel: +972-3-976-4000 Fax: +972-3-976-4040

Contact
www.audiocodes.com/contact
Website
www.audiocodes.com

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 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

Android Kiosk Lockdown software is software that locks down Android devices to allow only essential apps, by disabling access to Home/Launcher. Using Android Kiosk Lockdown software, the Android devices can be converted into public kiosk terminals or secured work devices.

- Only specific Microsoft apps and AudioCodes-signed apps that were certified and approved in the certification process, can run under Kiosk mode; even if a malicious user manages to install a new unauthorized app on the file system, the launcher on the AudioCodes Native Teams device will only run those specific approved apps and this cannot be changed in run time (only with a new software code provided by AudioCodes).

Screen Lock

AudioCodes Native Teams devices 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.

AudioCodes Private Key

The system software on AudioCodes Native Teams devices is signed with AudioCodes private key – users can replace the complete software only with new software that is also signed by the AudioCodes private key. This prevents the user from replacing the complete OTA package of the device with any new system software, unless this software has been fully signed by AudioCodes.

Android Debug Bridge (ADB)

AudioCodes disables the Android Debug Bridge (ADB) application and keeps the Teams app running in the front all the time, which means there is no way to install other Apps from unknown sources and sideloading.

App Signing

Android requires all apps to be digitally-signed with a developer key before installation; currently, the AudioCodes Native Teams device verifies that the apps are signed by Microsoft. App signing prevents malicious user/users from replacing a Microsoft-signed app with an app

that "pretends" to be Microsoft but which lacks the private key that is known only to Microsoft.

Web Browser

The AudioCodes Native Teams device does not include a web browser. Users cannot browse to the public internet or internal intranet; all web services are customized to connect to Office 365 services and AudioCodes managed services such as One Voice Operations Center (OVOC). Without a web browser, malicious user/users will not be able to access the device and browse from it as a trusted device into the customer network.

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.
- Debugging interface over SSH. Note that SSH **MUST** be disabled by default and enabled only per specific case for debugging-purposes only.

AudioCodes Device Manager Validation

The AudioCodes Native Teams device validates AudioCodes' Device Manager identity using known Root CA:

- The device is shipped with known Root CAs installed. See Appendix A– AudioCodes Root CA Certificate.
- For the initial connection phase, the AudioCodes Device Manager should access the device using a known CA.
- Once a successful secured connection has been established between the device and the Device Manager, the user can replace the root CA on the Device Manager and on the device and re-establish the connection leveraging any private root CA.

Sandboxing

AudioCodes Native Teams devices use Android Application Sandbox so that each application can access 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.

Device File System

The AudioCodes Native Teams device file system is encrypted on C470 / C435 and C450-DBW devices – customers may enforce a policy of device encryption via Microsoft Intune.

Keystore

With AudioCodes Native Teams devices, the certificate keys are encrypted on the device file system.

Device Certificate

AudioCodes Native Teams devices are shipped with a unique certificate which is signed by AudioCodes Root CA.

Data Protection

AudioCodes Native Teams devices run Android which has integral procedures for protecting and securing user data.

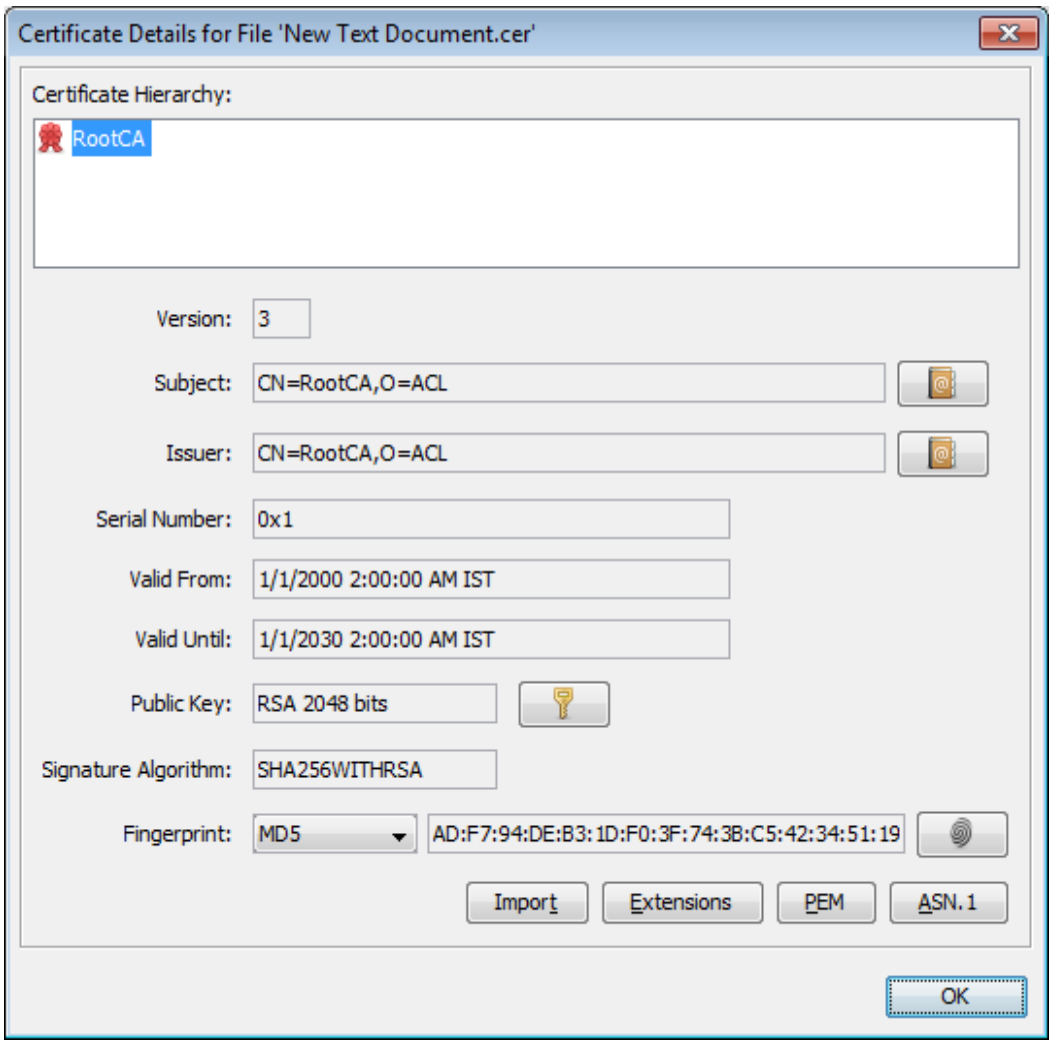
Debugging Interface

- AudioCodes Native Teams devices leverage SSH as a debugging interface.
- AudioCodes recommends that customers disable SSH on the device – this can be done via the AudioCodes Device Manager (OVOC).
- AudioCodes recommends changing the Admin password from the default, which 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.

Android Security Updates

In addition to all the above, AudioCodes regularly adopts and integrates the Android security updates. For reference see https://source.android.com/security/bulletin/2019-10-01).

Appendix A– AudioCodes Root CA Certificate




```
-----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----
```


AudioCodes Inc.
200 Cottontail Lane, Suite A101E, Somerset, NJ 08873
Tel: +1-732-469-0880 Fax: +1-732-469-2298

International Headquarters
1 Hayarden Street, Airport City, Lod 7019900
P.O.Box 255, Ben Gurion Airport, Israel 7019900
Tel: +972-3-976-4000 Fax: +972-3-976-4040

Contact
www.audiocodes.com/contact

Website
www.audiocodes.com