TrustZone®, TEE and Trusted Video Path Implementation Considerations

Michael Lu, Business Development Director, Trustonic Ltd.
Agenda

- Content Distribution Ecosystem Overview
  - Ecosystem overview
  - Relevance of TEE as Trusted Media Playback Platform
- TrustZone and Trusted Video Path implementation considerations
  - Secure video playback and architecture requirements
  - TrustZone Ready – Architecture Blueprints
  - Mali V500 and TZC400, additional IP required
  - Partner solutions
- Trustonic TEE and <t-play>
Content Distribution
Ecosystem Overview
Stakeholder and Assets needing protection

**Content Rights Holders**

- Media Content
- Usage Policy

**Content Aggregators and Service providers**

- *Media Content, Usage policy*
- Platform Metadata, User Info and Entitlements

**Content Protection Solution Providers**

- *Media Content, Usage Policy,*
- *Platform Metadata, User Info, Entitlements,*
- DRM secrets such as device/application keys, licenses etc.
TEE as Trusted Media Playback Platform

- The Device must implement a set of security features to enable protection of media content rendering path on the device, such that content decryption to decode, decompression and rendering/output to external links, is protected from unauthorised software and hardware components;

- The Device must implement a set of security features to enable robust DRM implementations to protect assets such as usage policy, account info, DRM application secrets and keys which allow media access;

- Device Security features and assets must be protected against tampering and modification by other unauthorized software and hardware components controlled by unauthorized software on the device.

- Device Security Features, where possible, should not adversely affect user experience, system renewability or increase significantly device implementation cost.
How TEE protects assets

<table>
<thead>
<tr>
<th>Sensitivity in DRM</th>
<th>TEE protection principles</th>
</tr>
</thead>
<tbody>
<tr>
<td>HW Root Of Trust</td>
<td>✓ Part of Secure Boot Process</td>
</tr>
<tr>
<td>Secure DRM Code Execution</td>
<td>✓ Hardware-based isolated environment</td>
</tr>
<tr>
<td>DRM Cryptography (e.g. DRM private keys)</td>
<td>✓ TEE secure storage and secure key management API</td>
</tr>
<tr>
<td>Secure DRM States Storage</td>
<td>✓ TEE secure storage</td>
</tr>
<tr>
<td>Secure date/time</td>
<td>✓ Secure clock management</td>
</tr>
<tr>
<td>Secure playback</td>
<td>✓ Secure configuration of Hardware Firewall</td>
</tr>
<tr>
<td>Link protection</td>
<td>✓ DTCP/IP and HDCP SW and configuration executed in TEE</td>
</tr>
</tbody>
</table>

- **Sensitivity in DRM**
  - HW Root Of Trust
  - Secure DRM Code Execution
  - DRM Cryptography (e.g. DRM private keys)
  - Secure DRM States Storage
  - Secure date/time
  - Secure playback
  - Link protection

- **TEE protection principles**
  - Part of Secure Boot Process
  - Hardware-based isolated environment
  - TEE secure storage and secure key management API
  - TEE secure storage
  - Secure clock management
  - Secure configuration of Hardware Firewall
  - DTCP/IP and HDCP SW and configuration executed in TEE
Standardisation through GlobalPlatform

- **GP Premium Content Task Force** supported by major studios. Intended Outputs are:
  - Standardise APIs for trusted video path access by DRM applications;
  - Provide a set of security features to enable robust DRM implementations;
  - Support downloadable and interoperable DRMs.
  - Certification and Compliance regime.
TrustZone and Trusted Video Path Implementation Considerations
Trusted Video Path Requirement

- End to end video path, from decryption to decode, decompression and rendering/output to external links, must be hardware isolated such that content is protected from unauthorised software processes and other hardware components;

- Memory buffers used in the processing, decoding, mixing and rendering of the content need to be protected by a hardware access control engine such that buffers are not accessible to other unauthorised software or hardware components. Output is only allowed to internal display or exported via protected links such as HDCP and DTCP.

- Firmware associated with decoders, mixers and renderers, and any software component such as DRM agents, directly used in setting up the protected memory path should be protected against tampering, including having critical components placed in secure processing space, or integrity checked and monitored at boot time and/or at runtime, or equivalent measures.
## What’s Required and where

<table>
<thead>
<tr>
<th>Premium Content</th>
<th>DRM</th>
<th>Video Codec</th>
<th>Display</th>
</tr>
</thead>
</table>

### Firmware protected against tampering
- Any SW component directly used in setting up protected memory path
- Decoders, mixers, renderers, DRM
- Critical components placed in secure processing space
- Integrity checked at boot time

### Unencrypted content protected
- After DRM protection removed
- Unencrypted content never accessible to processes running in HLOS
- Unencrypted content only ever written to protected memory

### Memory buffers protected by HW control
- All memory used in processing, decoding, mixing and rendering
- Sufficient memory for video bitstream and frame buffer
- Not accessible by HLOS or unauthorised HW or SW
- Output only to internal display or via protected export clients such as HDCP and DTCP
ARM TrustZone Architecture

- Hardware security to run “Trusted Apps”
- Secure OS isolated from HLOS by CPU HW
- HW protection from common SW Attacks
- Can be used to secure video path, Clock, RAM, SD/Storage, etc.
- Wide Adoption and standardisation

Apps which use TrustZone will have both a normal world App + a Trusted App

Standardized in GlobalPlatform

GP Client APIs allows communication between “Normal World & Secure World”

Trusted Apps have access to “Protected Memory” and Normal World memory
TrustZone Is System-wide Security

- **Trusted Base System Architecture – v1**
  - TrustZone-Enabled CPU Core
  - TrustZone-Aware L2 cache controller
  - TrustZone-Aware AXI Interconnect Fabric
  - Secure-World Memory (in addition to Normal World memory)
  - TrustZone-Aware Interrupt Controller
  - On-chip OTP protection for encryption and signature keys
  - On-SoC ROM protection for Trusted Boot Code
  - Off-SoC Memory Address Space Control
  - Secure Debug Control – Disable debug of Secure World
Components Needed for Trusted Media Path

- TEE Software (e.g. Trustonic TEE Solution)
- Video Decoder supporting TrustZone
- Memory Buffer Hardware Access Control Mechanism
- Display Controller Supporting TrustZone for local screen rendering
- HDCP/DTCP Link Protection for exporting content
TrustZone Ready Program

Desired Services

Market Requirements

Industry Factors

SoC Platform Assurance

SoC Checklist

TrustZone®
System Security by ARM

Security Design Blueprints

TEE Integration

Interoperability Standard APIs

SoC Platform Implementation

Industry Certification
ARM Mali-V500 – Mass Market HD Video

- System perspective to power reduction
  - 50% lower memory bandwidth with ARM Frame Buffer Compression (AFBC) in Video+Display
  - Small area Video for lowest cost and power
  - 1080p60 encode/decode to 4K120

- Optimized for real embedded systems
  - Latency tolerant design – no dropped frames
  - High quality IP from ARM

- Secure video path
  - Optimized for TrustZone secure media use cases

![Bandwidth Comparison](chart.png)
CoreLink™ TZC-400 TrustZone Controller

- Extends security to external DRAM
- Prevents illegal access to protected memory regions
- Protection from software attacks
- Part of TrustZone system
- Between CCI/NIC and DMC

Applications:
- **Secure Video Path for DRM**, **Trusted UI for secure payment**

<table>
<thead>
<tr>
<th>Master</th>
<th>Read</th>
<th>Write</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Master B</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Master C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Master D</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Address Map

- Region 0
- Region 1
- Region 2

- Supports multiple interfaces (1, 2 or 4)
- Secures 8 memory regions
- Enables a protected data pipe
- Setup read / write for specific masters
- Fast Path for low latency masters
- 256 outstanding transactions
Discretix Content Protection over TrustZone

Discretix Hardware Assisted Content Protection for Android Devices

- Pre-integrated and ready on all major Android platforms
- Integrated and deployed over Trustonic t-Base
- Key devices with Discretix below

Offering all the common Content Protection schemes:
- PlayReady for OTT and video services
- HDCP 2.x for Miracast™
- DTCP for DLNA
- CPRM for Japan Mobile TV

Key devices:
- LG Optimus G
- Samsung Galaxy Note 2
- Sharp SH-10D
- HTC One
- Samsung Galaxy S3
- Google Nexus 4
- Huawei HW-01E
- HTC Butterfly
- Sony Xperia V
- Samsung Galaxy Note 10.1
Complete Security Solutions for TrustZone and TEE

- **Content Protection and DRM**
  - tVault HDCP 2.2 (Wi-Fi Display / Miracast)
  - tVault DTCP-IP (DLNA enabled devices)
  - tVault DRM (PlayReady)

- **Platform Security**
  - Ellipsys-SB & Ellipsys-tBoot (Secure Boot)
  - Ellipsys-CA (Certification Authority)

- **Security protocol accelerators and processors**
  - Control interfaces support both secure and normal transactions
  - Reliable protection for sensitive data and transactions
  - High performance
  - Low power consumption
  - Efficient use of processing and bus resources
  - Intelligent data movement and controls
DRM Fusion - Content Protection from INSIDE Secure

- Fully integrated and supporting ARM® TrustZone® and TEEs
- PlayReady support for Android and Linux platforms
- Security enhanced with state-of-the-art hardware integration, obfuscation, anti-tampering and whitebox encryption
- Streaming support and file based content support including Smooth Streaming, HLS, MPEG-DASH and Ultraviolet
- HDCP and DTCP-IP solutions for local link content protection
- Studio approved technology with millions of users
- Available for Mobile Devices, STBs, Connected TVs and other devices
<t-play Trusted Media Playback Platform from Trustonic
<t-play – Trusted Media Playback Platform

For Content Rights Holders

• Higher bar of security for *premium content*
• Open Architecture for *greater content distribution opportunities*

For Service providers

• OTA *access* to Trusted Playback capabilities for premium services
• Payment and authentication integration for *new business models* and customer acquisition

For OEMs

• *Turnkey multi-DRM solution* for more content and time to market
• *Committed to independent assurance* - Most deployed and mature platform
• *Lower BOM cost* through downloadable DRM architecture
About Trustonic
Vision and Mission

Vision

Enriching, simplifying AND EXPANDING people’s digital lives by SECURING valued services on smart devices.

Our Mission

To be the trusted foundation of choice for all smart connected devices. Empowering our partners to enrich and simplify consumers’ lives through our technology, OPEN business model and VIBRANT application ecosystem.
t-play – Trusted Media Playback Platform

For Content Rights Holders
- Higher bar of security for *premium content*
- Open Architecture for *greater content distribution opportunities*

For Service Providers
- **OTA access** to Trusted Playback capabilities for premium services
- Payment and authentication integration for *new business models* and customer acquisition

For OEMs
- **Turnkey multi-DRM solution** for more content and time to market
- **Committed to independent assurance** - Most deployed and mature platform
- **Lower BOM cost** through downloadable DRM architecture
Simpler, faster, safer commerce

Merchant

Register Account 15 Seconds...

Enter Address 59 Seconds...

Select Address 1 Second...

Payment

Input Card Details 78 Seconds...

Authenticate 7 Seconds...

Select Account Enter PIN 6 Seconds...

1 Keystroke

1 Keystroke

23 Keystrokes

23 Keystrokes

5 Keystrokes

5 Keystrokes

32 Keystrokes

56 Keystrokes

9 Keystrokes

9 Keystrokes

2.5 Minutes 120 Keystrokes

7 Seconds 6 Keystrokes
Your Device at Work

Better User Experience and more functions

- Integrated into the device
- Remove need for complex passwords
- Certifiable for high assurance
- Expands to include biometrics

<table>
<thead>
<tr>
<th>2-FA Token</th>
<th>Security Function</th>
<th>Trusted Handset</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔</td>
<td>2 Factor Authentication</td>
<td>✔</td>
</tr>
<tr>
<td>✖</td>
<td>Secure Storage</td>
<td>✔</td>
</tr>
<tr>
<td>✖</td>
<td>Communication Security</td>
<td>✔</td>
</tr>
<tr>
<td>✖</td>
<td>Corporate Policy Enforcement</td>
<td>✔</td>
</tr>
<tr>
<td>$20</td>
<td>Annual Price per User</td>
<td>$TBD</td>
</tr>
</tbody>
</table>

28
Why Trustonic?

- Security software is meaningless without accessible TRUST
  - Only Trustonic provides both key management services and secure software essential for TRUST

- Trusted Execution Environments are not trivial things to develop
  - Trustonic has hundreds of man-years experience in developing commercial grade high assurance TEEs

- Trustonic has total ecosystem support for TEEs
  - Trustonic supports the leading Chip Makers
Assured content acquisition

Solutions deployed in more than 100m devices

Google, Samsung, HTC, Sony Ericsson, Motorola, Lenovo, Toshiba, Google, Fujitsu, Panasonic, Sharp, Barnes & Noble, Samsung Galaxy Nexus, Google Nexus 7, Samsung Galaxy S III, Samsung Galaxy Note II, Samsung Galaxy Note 10.1, Motorola Razr HD
Thank You

michael.lu@trustonic.com