



HiPQ & HiAQ

# Security Technology White Paper

Issue	01
Date	2016-10-29

**Copyright © HiSilicon Technologies Co., Ltd. 2016. All rights reserved.**

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of HiSilicon Technologies Co., Ltd.

## **Trademarks and Permissions**



**HISILICON**, and other HiSilicon icons are trademarks of HiSilicon Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

## **Notice**

The purchased products, services and features are stipulated by the contract made between HiSilicon and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

## **HiSilicon Technologies Co., Ltd.**

Address: Huawei Industrial Base  
Bantian, Longgang  
Shenzhen 518129  
People's Republic of China

Website: <http://www.hisilicon.com>

Email: [support@hisilicon.com](mailto:support@hisilicon.com)



# About This Document

## Purpose

This document is intended for developers and provides precautions on network security when HiSilicon PQ Tools and HiSilicon AQ Tools are used.

## Related Versions

The following table lists the product versions related to the HiSilicon PQ Tools.

Product Name	Version
Hi3519	V100R001
Hi3519	V101R001
Hi3516C	V300R001
Hi3516A	V100R001
Hi3516D	V100R001
Hi3518E	V200R001
Hi3518E	V201R001
Hi3516C	V200R001

The following table lists the product versions related to the HiSilicon AQ Tools.

Product Name	Version
Hi3518E	V200R001
Hi3518E	V201R001
Hi3516C	V200R001



## Change History

Changes between document issues are cumulative. Therefore, the latest document issue contains all changes made in previous issues.

### Issue 01 (2016-10-29)

This issue is the first official release.



# Contents

<b>About This Document.....</b>	<b>i</b>
<b>Contents .....</b>	<b>iii</b>
<b>1 Introduction.....</b>	<b>1</b>
<b>2 HiPQ .....</b>	<b>2</b>
2.1 Basic Architecture .....	2
2.2 Security Attacks and Threats .....	3
2.3 Security Dimensions .....	3
2.4 Security Domains .....	4
<b>3 HiAQ.....</b>	<b>5</b>
3.1 Basic Architecture .....	5
3.2 Security Attacks and Threats .....	6
3.3 Security Dimensions .....	6
3.4 Security Domains .....	7
<b>4 Conclusions .....</b>	<b>8</b>
<b>5 Acronyms and Abbreviations.....</b>	<b>9</b>



---

## Figures

---

<b>Figure 2-1</b> HiPQ basic architecture .....	2
<b>Figure 2-2</b> HiPQ and peripheral interaction diagram .....	3
<b>Figure 3-1</b> HiAQ basic architecture .....	5
<b>Figure 3-2</b> HiAQ and peripheral interaction diagram.....	6



# 1 Introduction

---

The HiSilicon PQ Tools (HiPQ for short) and HiSilicon AQ Tools (HiAQ for short) are debugging tools used based on the HiMPP (MPP for short) media software development kit (SDK). Set up in local area network (LAN), the two tools are used to implement the data exchange between the board and the PC.

- The HiPQ includes online on-demand and online tuning functions.
  - The online on-demand uses the media functional module based on MPP development to implement online on-demand preview and basic configuration preview.
  - The online tuning, based on MPP development, has functions of adjusting the attributes of the picture quality-related modules, assisting in calibrating ISP initialization parameters, and capturing ISP adjustment information to locate image signal processor (ISP) and audio problems.
- The HiAQ includes online tuning function.

The online tuning, based on MPP development, has functions of adjusting the attributes of the audio quality-related modules and capturing the audio adjustment information to locate audio problems.

Basic application scenarios are as follows:

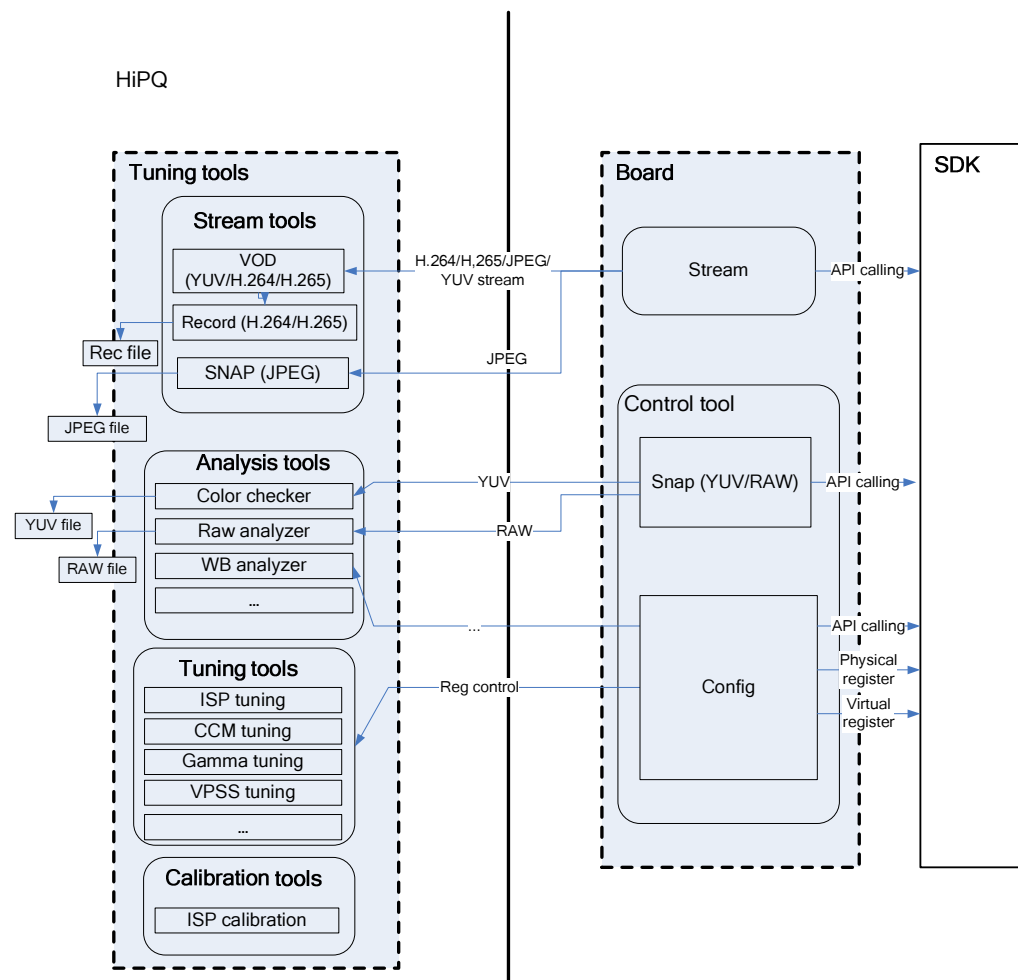
- During product development based on HiMPP media SDK, the HiPQ and HiAQ can be used to adjust parameters.
- During product development based on HiMPP media SDK, the HiPQ and HiAQ can be used to capture location information for developers to locate picture- or audio-related problems.



# 2 HiPQ

## 2.1 Basic Architecture

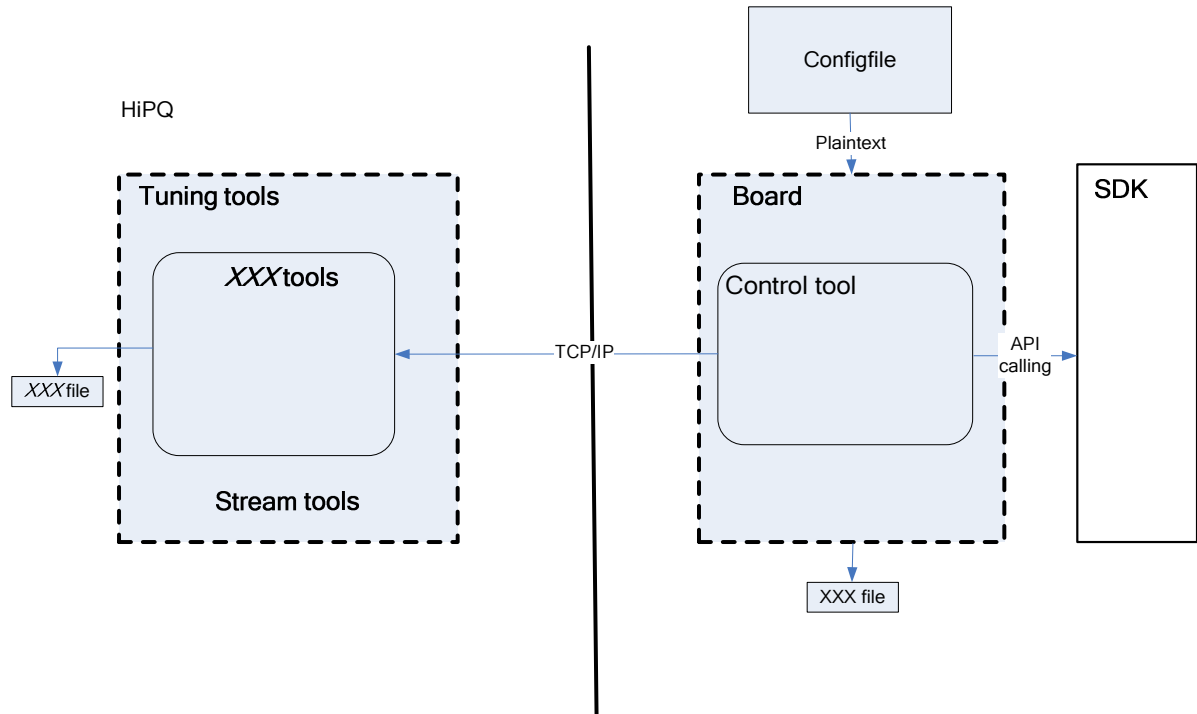
Figure 2-1 HiPQ basic architecture





## 2.2 Security Attacks and Threats

**Figure 2-2** HiPQ and peripheral interaction diagram



The HiPQ consists of executable program at the server end and executable program at the client end. Data is transmitted between the two ends over LAN TCP/IP. During network construction:

- **For the online tuning part, the server** reads the port number from the plaintext configuration files and then performs monitoring operation. The server stores binary files (XXX.bin file and XXX.raw file) during running.
- **For the online tuning part, the client** specifies the sending port number when started and then implements command and data exchanges. The client stores and fetches data (RAW data, YUV data, and ISP parameters) obtained from the server during running.

For the online on-demand part, the server reads some default media parameters from the plaintext configuration files and specifies port 80 to implement monitoring operation fixedly. The client stores the recording files (XXX.h264 files and XXX.h265 files) and snapshot files (XXX.jpg files) during running.

## 2.3 Security Dimensions

### 2.3.1 Login Control

The HiPQ is run based on MPP environment construction, including board preparation, boot burning, kernel burning, rootfs burning, and network setting. Before the HiPQ is run, the number of the monitoring port for online tuning needs to be configured. The port number is



stored in the **config.cfg** file in the HiPQ running directory. Modify the port parameter in the **Default** field. The default monitoring port number is 4321. For the online on-demand part, the port number is 80 fixedly. Before occupying port 80, check whether this port is occupied by other processes.

## 2.3.2 Permission Control

To log in to the HiPQ client, users need to enter the IP address and port number of the board to be logged in to. The port number for the online on-demand is 80, and users do not need to enter the port number.

## 2.3.3 Storage Security

The HiPQ stores the intermediate files to and fetches them from the board or PC according to different application conditions during running. The access path of the intermediate files on the server is configurable, and the configuration items are stored in plaintext in **config.cfg** file under the **HiPQ running directory**. For some intermediate files on the client, such as *XXX.yuv* or *XXX.raw*, you need to select an access path. For intermediate files like data reports, such as *XXX.jpg*, the default access path is the current client running directory.

## 2.3.4 Interaction Security

The HiPQ can run over LAN only. It uses LAN TCP/IP to implement network transmission.

## 2.3.5 Data Transmission Security

During data transmission, the HiPQ uses simple flags to identify whether the packet is sent by HiPQ. The packet integrity is verified using simple algorithms to preliminarily identify whether packet loss occurs on the network.

# 2.4 Security Domains

## 2.4.1 Management

The HiPQ is used during product development only, and is not recommended in products.

## 2.4.2 Control

The HiPQ is used during product development only, and users need to protect the access of the port number, board IP address, and sensitive intermediate information.

## 2.4.3 Application Environment

The HiPQ can only be used in LAN.



# 3 HiAQ

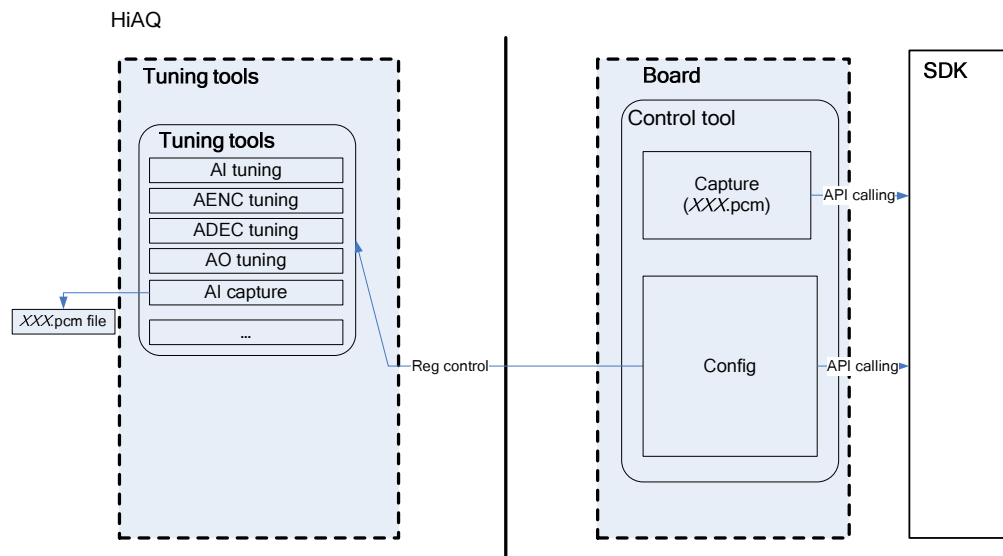


## NOTE

This section only applies to the Linux version of the Hi3518E V20X series chips.

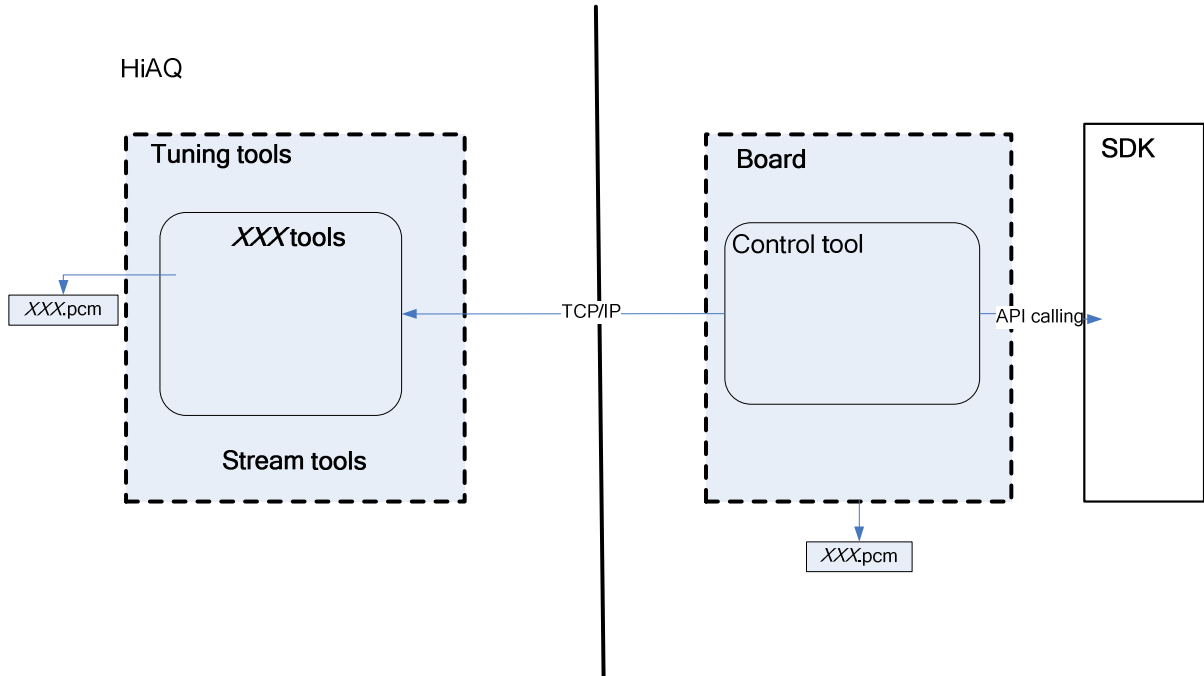
## 3.1 Basic Architecture

Figure 3-1 HiAQ basic architecture



## 3.2 Security Attacks and Threats

**Figure 3-2** HiAQ and peripheral interaction diagram



The HiAQ consists of executable program at the server end and executable program at the client end. Data is transmitted between the two ends over LAN TCP/IP. During network construction:

- **For the online tuning part, the server** reads the port number from the plaintext configuration files and then performs monitoring operation. The server writes binary files (XXX.pcm files) during running.
- **For the online tuning part, the client** specifies the sending port number when started and then implements command and data exchanges. The client stores and fetches data (XXX.pcm data) obtained from the server during running.

## 3.3 Security Dimensions

### 3.3.1 Login Control

The HiAQ is run based on MPP environment construction, including board preparation, boot burning, kernel burning, rootfs burning, and network setting. Before the HiAQ is run, the monitoring port number needs to be configured. The port number needs to be added at the end of the **HiAQTool.sh** script, to be specific, `./HiAQTool.sh port number`.

### 3.3.2 Permission Control

To log in to the HiAQ client, users need to enter the IP address and port number of the board to be logged in to.



### 3.3.3 Storage Security

The HiAQ stores the intermediate files to and fetches them from the board or PC according to different application conditions during running. The access path of the intermediate file on the server is program running directory. For intermediate files on the client, such as XXX.pcm, you need to select an access path.

### 3.3.4 Interaction Security

The HiAQ can run over LAN only. It uses LAN TCP/IP to implement network transmission.

### 3.3.5 Data Transmission Security

During data transmission, the HiAQ uses simple flags to identify whether the packet is sent by HiAQ. The packet integrity is verified using simple algorithms to preliminarily identify whether packet loss occurs on the network.

## 3.4 Security Domains

### 3.4.1 Management

The HiAQ is used during product development only, and is not recommended in products.

### 3.4.2 Control

The HiAQ is used during product development only, and users need to protect the access of the port number, board IP address, and sensitive intermediate information.

### 3.4.3 Application Environment

The HiAQ can only be used in LAN.



# 4 Conclusions

---

- The HiPQ and HiAQ are debugging tools, which are used only during product development.
- The data of the user-developed product needs to be protected by product developers.
- The software package of the tools includes the executable files and configuration files. For software package related to mass production, you need to delete all executable files and configuration files, and tool descriptions in the documents.



# 5 Acronyms and Abbreviations

---

**Table 5-1** Acronyms and abbreviations

Acronym or Abbreviation	Full Name
ISP	image signal processor
LAN	local area network
MPP	media processing platform
SDK	software development kit