



# WIDEVINE<sup>®</sup>

CYPHER FOR DIGITAL MEDIA

## HARDWARE AND SOFTWARE REQUIREMENTS

VERSION: 1.0

---

Widevine Technologies

901 5<sup>th</sup> Ave, Suite 3400

Seattle, WA 98164 USA

[www.widevine.com](http://www.widevine.com)

206.254.3000 *voice*

206.254.3001 *fax*

[sales@widevine.com](mailto:sales@widevine.com)



## CONTENTS

<b>1. Purpose.....</b>	<b>4</b>
<b>2. Hardware Requirements.....</b>	<b>5</b>
<b>3. Software Requirements .....</b>	<b>5</b>
<b>4. Security Recommendations.....</b>	<b>6</b>
4.1. Content Source.....	6
4.2. Cypher Encryption Appliances.....	7
<b>5. Tested Hardware Configuration .....</b>	<b>9</b>
5.1. HP DL360 G7.....	9
5.2. HP DL360 G6.....	10
<b>6. Tested Software Configuration .....</b>	<b>11</b>
6.1. RPM List .....	11

© 2011 Widevine Technologies, Inc. All Rights Reserved. Widevine, Widevine Cypher, Cypher Virtual SmartCard, Cypher VOD, Cypher DCP, Cypher Broadcast, Cypher for the PC, Widevine MediaProtect, Widevine Cypher Express, Widevine Mensor, Encryption On The Fly, Encrypts Streaming Media On The Fly, Encrypts Streaming Media, and Content Security from Hollywood to the Home are either registered trademarks or trademarks of Widevine Technologies, Inc. and its subsidiaries in the United States and/or other countries. All other trademarks and trade names are the property of their respective owners. No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features or functionality will be provided on an if and when available basis. Widevine reserves the right to substitute hardware component vendors and quantities in order to meet the customer specific environment and based on component availability. Note that the descriptions of Widevine Technologies' patents and other intellectual property herein are intended to provide illustrative, non-exhaustive examples of some of the areas to which the patents and applications are currently believed to pertain, and is not intended for use in a legal proceeding to interpret or limit the scope or meaning of the patents or their claims, or indicate that a Widevine patent claim(s) is materially required to perform or implement any of the listed items. Widevine patents include but are not limited to: U.S. Patent No. 7,007,170 B2; 6,449,719 B1; 6,965,993 B2; 7,043,473; 7,150,045; 7,165,175; 7,299,292; and Korean Patent No. 10-0749947-0000; 00-747755-0000; and Taiwan Patent No. R.O.C I268080

## Revision History

Version	Date	Description	By
1.0	01/27/2011	Initial release	Alex Lee

## 1. PURPOSE

The purpose of this document is to describe the hardware and software requirements to run the Widevine Digital Media system.

## 2. HARDWARE REQUIREMENTS

	Minimum	Recommended
<b>Processor</b>	Intel x86 Dual-Core	Quad-Core or better
<b>Memory</b>	1 GB	4+ GB
<b>Networking</b>	Fast Ethernet (100mbps)	Gigabit Ethernet (1000mbit)
<b>Storage</b>	20 GB	100+ GB

## 3. SOFTWARE REQUIREMENTS

Supported Operating Systems:

- RedHat Enterprise Linux 5 (32-bit)

Required packages:

- httpd
- net-snmp
- syslog-ng

Storage allocation:

- Recommended 80 GB or more in /usr
  - Widevine software uses /usr exclusively.

## 4. SECURITY RECOMMENDATIONS

### 4.1. CONTENT SOURCE

The content source is not protected by Cypher and must be secured via other methods.

If at all possible, content should not be in the clear. If this cannot be avoided, the following recommendations apply.

In current implementations clear content typically exists in the content head end at a storage device called the catcher. An aggregator to the head end typically transmits content. This transmission is often performed via satellite and the transport is encrypted. When it arrives at the Head End an Integrated Receiver Decoder (IRD) will decrypt the content and place in the clear on the catcher. During the provisioning process from the catcher to the content delivery server the content may be encrypted again. This method leaves an attack point in the catcher. This process requires physical protection. If at all possible all Cypher Components should be in a physically secure facility:

- It is recommended that clear content be located in a facility with physical access control. Personnel with access to this content should be kept to a minimum and should be subjected to background checks and other measures typically employed to establish a trusted employee.
- The Clear Content facility should be an enclosed space with limited access. The door locks are keyed to a master, which has a much more restricted distribution than the standard “building master” keys normally used. Access to this key is restricted to pre-designated persons.
- Routine access to the data center is may be via a proximity card activated security system. Every authorized user is issued their own access card and all accesses are logged by the security system. The hardware controlling the security system should be mounted inside the data center.
- Each entrance should have a mantrap (except for the loading dock), a security kiosk, physical barriers (concrete barricades) and CCTV cameras to ensure each person entering the facility is identified.
- Crew requiring badges to enter the facility should be required to produce picture ID in exchange for the badge allowing access. Security kiosks should have access to read the badge database. The badge database should have pictures of each user and their corresponding badge. Badges should be picture IDs.

- A log of equipment and content being placed in and removed from the facility must be kept at each guard desk listing what was removed, when and by whom.
- The person whom they are visiting at all times MUST escort visitors. Visitors MUST NOT be allowed access to the facility without written approval from data center management.

There are two alternatives to the above. One option is to create a physically secure rack in the data center instead of an entire room or facility. In this rack you would want to house the IRD, the catcher's mitt and the Cypher encryption appliance. All network connections between these items should be physically contained in the rack. The idea is content is encrypted as it goes into the rack and as it comes out. Physical access to the rack should follow the general guidelines above.

The second alternative is to pre-encrypt the content with Cypher at the aggregator and not decrypt until it reaches the client device. Often this option may not be desired.

The following Network Security measures are recommended for the Content Source:

- We recommend a firewall between the content source and the Cypher appliance.
- We recommend a firewall between the content source and any external networks.
- We recommend the use of network and host based intrusion detection systems for the content source

All firewalls and intrusion detection products should be compliant with industry standards, kept up to date with all patches and updates released by the vendor, and where possible, products that are certified by an independent testing lab should be selected. Firewalls must be configured to the most restrictive profile consistent with the traffic that travels across them.

### 4.2. CYPHER ENCRYPTION APPLIANCES

The following Network Security measures are recommended for the Cypher Encryption Appliances:

- We recommend a firewall between the Cypher Encryption Appliances and the Internet.
- We recommend a firewall between the Cypher Encryption Appliances and the Corporate network
- We recommend a firewall between the Cypher Encryption Appliances and third-party appliances

- We recommend the use of network and host based intrusion detection systems for the Cypher Encryption Appliances

All firewalls and intrusion detection products should be compliant with industry standards, kept up to date with all patches and updates released by the vendor and where possible, products that are certified by an independent testing lab should be selected. Firewalls must be configured to the most restrictive profile consistent with the traffic that travels across them.



## 5. TESTED HARDWARE CONFIGURATION

Below are verified and validated configurations.

### 5.1. HP DL360 G7

Part Number	Description
<b>579237-B21</b>	HP Proliant DL360G7 CTO Chassis
<b>588080-L21</b>	HP L5630 DL360G7 FIO Kit (Quad-Core Intel® Xeon® Processor L5630 (2.13GHz, 12M L3 Cache, 40 Watts, DDR3-1066MHz, HT Turbo 1/1/2/2)
<b>500670-B21</b>	HP 2GB 1x2GB PC3-10600 ECC Unbuffered CAS 9 Dual Rank x8 DRAM Memory Kit
<b>500670-B21</b>	HP 2GB 1x2GB PC3-10600 ECC Unbuffered CAS 9 Dual Rank x8 DRAM Memory Kit
<b>588080-B21</b>	HP L5630 DL360G7 FIO Kit (Quad-Core Intel® Xeon® Processor L5630 (2.13GHz, 12M L3 Cache, 40 Watts, DDR3-1066MHz, HT Turbo 1/1/2/2)
<b>500670-B21</b>	HP 2GB 1x2GB PC3-10600 ECC Unbuffered CAS 9 Dual Rank x8 DRAM Memory Kit
<b>500670-B21</b>	HP 2GB 1x2GB PC3-10600 ECC Unbuffered CAS 9 Dual Rank x8 DRAM Memory Kit
	HP P410i/ZM (SAS Array Controller)
<b>507125-B21</b>	HP 146GB 6G SAS 10K rpm 2.5-inch Dual Port Enterprise Hard Disk Drive
<b>507125-B21</b>	HP 146GB 6G SAS 10K rpm 2.5-inch Dual Port Enterprise Hard Disk Drive
	(2) Embedded HP NC382i Dual Port Multifunction Gigabit Server Adapters (4-Ports)
<b>Drive Config</b>	RAID-1

## 5.2. HP DL360 G6

<b>484184-B21</b>	HP ProLiant DL360 G6 Server°
<b>507682-L21</b>	Quad-Core Intel® Xeon® Processor E5504 (2.00GHz, 4M Cache, 80 Watts, 800MHz)°
<b>500656-4GB</b>	HP 4GB PC3-10600R 2x2GB 2Rank Memory
<b>507682-B21</b>	Quad-Core Intel® Xeon® Processor E5504 (2.00GHz, 4M Cache, 80 Watts, 800MHz)°
<b>500656-4GB</b>	HP 4GB PC3-10600R 2x2GB 2Rank Memory
	Embedded P410i (SAS Array Controller)
<b>418367-B21</b>	HP 146GB Hot Plug 2.5 SAS Dual Port 10,000 rpm Hard Drive°
<b>418367-B21</b>	HP 146GB Hot Plug 2.5 SAS Dual Port 10,000 rpm Hard Drive°
	Embedded HP NC382T Dual Port Multifunction Gigabit Server Adapter
<b>412648-B21</b>	HP NC360T PCI Express Dual Port Gigabit Server Adapter - Low Profile°
<b>500172-2PS</b>	2 HP 1200W 12V Hotplug ACC Power Supplies
<b>Drive Config</b>	RAID-1

## 6. TESTED SOFTWARE CONFIGURATION

Below are the validated and verified operating system software components.

Operating system: RedHat Enterprise Linux 5 (Update 4)

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/mapper/system-root					
	3.9G	831M	2.9G	23%	/
/dev/mapper/system-tmp					
	3.9G	137M	3.6G	4%	/tmp
/dev/mapper/system-usr					
	92G	6.3G	81G	8%	/usr
/dev/mapper/system-var					
	9.7G	222M	9.0G	3%	/var
/dev/cciss/c0d0p1	487M	23M	439M	5%	/boot
tmpfs	4.0G	0	4.0G	0%	/dev/shm

### 6.1. RPM LIST

```

acl-2.2.39-3.el5
acpid-1.0.4-9.el5
acpid-1.0.4-9.el5_4.1
aide-0.13.1-4.el5
amtu-1.0.6-1.el5
anacron-2.3-45.el5
apr-1.2.7-11.el5_3.1
apr-util-1.2.7-7.el5_3.2
at-3.1.8-82.fc6
attr-2.4.32-1.1
audit-1.7.13-2.el5
audit-libs-1.7.13-2.el5
authconfig-5.3.21-6.el5
basesystem-8.0-5.1.1
bash-3.2-24.el5
bc-1.06-21
beecrypt-4.1.2-10.1.1
bind-libs-9.3.6-4.P1.el5_4.1
bind-utils-9.3.6-4.P1.el5_4.1
binutils-2.17.50.0.6-12.el5
bzip2-1.0.3-4.el5_2
bzip2-libs-1.0.3-4.el5_2
ccid-1.3.8-1.el5
chkconfig-1.3.30.1-2
conman-0.1.9.2-8.el5
coolkey-1.1.0-6.el5
coreutils-5.97-23.el5_4.1

```

cpio-2.6-23.el5  
cracklib-2.8.9-3.3  
cracklib-dicts-2.8.9-3.3  
crontabs-1.10-8  
cryptsetup-luks-1.0.3-5.el5  
curl-7.15.5-2.1.el5\_3.5  
cyrus-sasl-2.1.22-5.el5  
cyrus-sasl-lib-2.1.22-5.el5  
cyrus-sasl-plain-2.1.22-5.el5  
db4-4.3.29-10.el5  
dbus-1.1.2-12.el5  
dbus-glib-0.73-8.el5  
dbus-libs-1.1.2-12.el5  
Deployment\_Guide-en-US-5.2-11  
desktop-file-utils-0.10-7  
device-mapper-1.02.32-1.el5  
device-mapper-event-1.02.32-1.el5  
device-mapper-multipath-0.4.7-30.el5\_4.4  
dhclient-3.0.5-21.el5  
dialog-1.0.20051107-1.2.2  
diffutils-2.8.1-15.2.3.el5  
distcache-1.4.5-14.1  
dmidecode-2.10-2.el5  
dmraid-1.0.0.rc13-53.el5  
dmraid-events-1.0.0.rc13-53.el5  
dos2unix-3.1-27.2.el5  
e2fsprogs-1.39-23.el5  
e2fsprogs-libs-1.39-23.el5  
ed-0.2-39.el5\_2  
elfutils-libelf-0.137-3.el5  
ethtool-6-3.el5  
expat-1.95.8-8.3.el5\_4.2  
expect-5.43.0-5.1  
file-4.17-15.el5\_3.1  
filesystem-2.4.0-2  
findutils-4.2.27-6.el5  
fipscheck-1.2.0-1.el5  
fipscheck-lib-1.2.0-1.el5  
firstboot-tui-1.4.27.7-1.el5  
ftp-0.17-35.el5  
gawk-3.1.5-14.el5  
gdbm-1.8.0-26.2.1  
glib2-2.12.3-4.el5\_3.1  
glibc-2.5-42.el5\_4.2  
glibc-common-2.5-42.el5\_4.2  
gnu-efi-3.0c-1.1  
gnupg-1.4.5-14  
gnutls-1.4.1-3.el5\_3.5  
gpm-1.20.1-74.1  
grep-2.5.1-55.el5  
groff-1.18.1.1-11.1  
grub-0.97-13.5  
gzip-1.3.5-10.el5  
hal-0.5.8.1-52.el5

hesiod-3.1.0-8  
hmacalc-0.9.6-1.el5  
hp-health-8.3.2.2-1  
hp-ilo-8.3.0-119.custom.rhel5  
hponcfg-2.2.0-5  
hp-snmp-agents-8.3.0.27-25  
htmlview-4.0.0-2.el5  
httpd-2.2.3-31.el5\_4.2  
hwdata-0.213.16-1.el5  
ifd-egate-0.05-15  
info-4.8-14.el5  
initscripts-8.45.30-2.el5  
iproute-2.6.18-10.el5  
iptables-1.3.5-5.3.el5\_4.1  
iptables-ipv6-1.3.5-5.3.el5\_4.1  
iptstate-1.4-1.1.2.2  
iputils-20020927-46.el5  
irqbalance-0.55-15.el5  
jre-1.6.0\_03-fcs  
jwhois-3.2.3-8.el5  
kbd-1.12-21.el5  
kernel-PAE-2.6.18-164.9.1.el5  
kernel-PAE-2.6.18-164.el5  
keyutils-libs-1.2-1.el5  
kpartx-0.4.7-30.el5\_4.4  
krb5-libs-1.6.1-36.el5  
krb5-workstation-1.6.1-36.el5  
ksh-20080202-14.el5  
kudzu-1.2.57.1.21-1  
less-394-6.el5  
lftp-3.7.11-4.el5  
libacl-2.2.39-3.el5  
libaio-0.3.106-3.2  
libattr-2.4.32-1.1  
libcap-1.10-26  
libgcc-4.1.2-46.el5\_4.1  
libgcrypt-1.4.4-5.el5  
libgpg-error-1.4-2  
libhugetlbfs-1.3-3.el5  
libidn-0.6.5-1.1  
libselineux-1.33.4-5.5.el5  
libsepol-1.15.2-2.el5  
libstdc++-4.1.2-46.el5\_4.1  
libsysfs-2.0.0-6  
libtermcap-2.0.8-46.1  
libusb-0.1.12-5.1  
libuser-0.54.7-2.1.el5\_4.1  
libutempter-1.1.4-4.el5  
libvolume\_id-095-14.21.el5  
libX11-1.0.3-11.el5  
libXau-1.0.1-3.1  
libXdmcp-1.0.1-2.1  
libXext-1.0.1-2.1  
libxml2-2.6.26-2.1.2.8

libxml2-python-2.6.26-2.1.2.8  
libXp-1.0.0-8.1.el5  
lm\_sensors-2.10.7-4.el5  
logrotate-3.7.4-9  
lsof-4.78-3  
lvm2-2.02.46-8.el5\_4.2  
lynx-2.8.5-28.1.el5\_2.1  
lzo2-2.02-3.el5.rf  
m2crypto-0.16-6.el5.6  
mailcap-2.1.23-1.fc6  
MAKEDEV-3.23-1.2  
man-1.6d-1.1  
man-pages-2.39-12.el5  
mcstrans-0.2.11-3.el5  
mdadm-2.6.9-2.el5  
mingetty-1.07-5.2.2  
mkinitrd-5.1.19.6-54  
mktemp-1.5-23.2.2  
mlocate-0.15-1.el5.2  
mod\_perl-2.0.4-6.el5  
mod\_python-3.2.8-3.1  
mod\_ssl-2.2.3-31.el5\_4.2  
module-init-tools-3.3-0.pre3.1.54.el5  
mtr-0.71-3.1  
nano-1.3.12-1.1  
nash-5.1.19.6-54  
nc-1.84-10.fc6  
ncurses-5.5-24.20060715  
net-snmp-5.3.2.2-7.el5\_4.2  
net-snmp-libs-5.3.2.2-7.el5\_4.2  
net-snmp-utils-5.3.2.2-7.el5\_4.2  
net-tools-1.60-78.el5  
newt-0.52.2-12.el5\_4.1  
nload-0.7.2-1.el5.rf  
nmap-4.11-1.1  
nspr-4.7.6-1.el5\_4  
nss-3.12.3.99.3-1.el5\_3.2  
nss-tools-3.12.3.99.3-1.el5\_3.2  
ntp-4.2.2p1-9.el5\_4.1  
ntsysv-1.3.30.1-2  
numactl-0.9.8-8.el5  
OpenIPMI-2.0.16-5.el5\_4.1  
OpenIPMI-libs-2.0.16-5.el5\_4.1  
openldap-2.3.43-3.el5  
openssh-4.3p2-36.el5\_4.3  
openssh-clients-4.3p2-36.el5\_4.3  
openssh-server-4.3p2-36.el5\_4.3  
openssl-0.9.8e-12.el5  
openvpn-2.0.9-1.el5.rf  
pam-0.99.6.2-6.el5  
parted-1.8.1-23.el5  
passwd-0.73-1  
pax-3.4-1.2.2  
pciutils-2.2.3-7.el5

pcre-6.6-2.el5\_1.7  
pcsc-lite-1.4.4-0.1.el5  
pcsc-lite-libs-1.4.4-0.1.el5  
perl-5.8.8-27.el5  
perl-BSD-Resource-1.28-1.fc6.1  
perl-String-CRC32-1.4-2.fc6  
pkinit-nss-0.7.6-1.el5  
pm-utils-0.99.3-10.el5  
popt-1.10.2.3-18.el5  
postgresql-libs-8.1.18-2.el5\_4.1  
prelink-0.4.0-2.el5  
procmail-3.22-17.1  
procps-3.2.7-11.1.el5  
psacct-6.3.2-44.el5  
psmisc-22.2-7  
python-2.4.3-27.el5  
python-elementtree-1.2.6-5  
python-iniparse-0.2.3-4.el5  
python-sqlite-1.1.7-1.2.1  
python-urlgrabber-3.1.0-5.el5  
quota-3.13-1.2.5.el5  
rdate-1.4-8.el5  
rdist-6.1.5-44  
readline-5.1-3.el5  
redhat-logos-4.9.16-1  
redhat-menus-6.7.8-3.el5  
redhat-release-5Server-5.4.0.3  
redhat-release-notes-5Server-29  
rhel-instnum-1.0.9-1.el5  
rhpl-0.194.1-1  
rootfiles-8.1-1.1.1  
rpm-4.4.2.3-18.el5  
rpm-libs-4.4.2.3-18.el5  
rpm-python-4.4.2.3-18.el5  
rsync-2.6.8-3.1  
screen-4.0.3-1.el5\_4.1  
sed-4.1.5-5.fc6  
sendmail-8.13.8-2.el5  
setarch-2.0-1.1  
setserial-2.17-19.2.2  
setup-2.5.58-7.el5  
setuptools-1.19.2-1  
sgpio-1.2.0\_10-2.el5  
shadow-utils-4.0.17-14.el5  
slang-2.0.6-4.el5  
sntl-sud-7.0.0-0  
sos-1.7-9.27.el5  
specspo-13-1.el5  
sqlite-3.3.6-5  
stunnel-4.15-2.el5.1  
sudo-1.6.9p17-5.el5  
symlinks-1.2-24.2.2  
sysfsutils-2.0.0-6  
sysklogd-1.4.1-44.el5

syslog-ng-2.1.4-1.el5  
sysstat-7.0.2-3.el5  
system-config-network-tui-1.3.99.18-1.el5  
system-config-securitylevel-tui-1.6.29.1-2.1.el5  
SysVinit-2.86-15.el5  
tar-1.15.1-23.0.1.el5  
tcl-8.4.13-4.el5  
tcpdump-3.9.4-14.el5  
tcp\_wrappers-7.6-40.7.el5  
telnet-0.17-39.el5  
termcap-5.5-1.20060701.1  
time-1.7-27.2.2  
tmpwatch-2.9.7-1.1.el5.2  
traceroute-2.0.1-5.el5  
tree-1.5.0-4  
tzdata-2009o-2.el5  
udev-095-14.21.el5  
udftools-1.0.0b3-0.1.el5  
unix2dos-2.2-26.2.3.el5  
unzip-5.52-3.el5  
usbutils-0.71-2.1  
usermode-1.88-3.el5.2  
util-linux-2.13-0.52.el5  
vconfig-1.9-2.1  
vim-minimal-7.0.109-6.el5  
vixie-cron-4.1-76.el5  
vsftpd-2.0.5-16.el5\_4.1  
wget-1.11.4-2.el5\_4.1  
which-2.16-7  
wireless-tools-28-2.el5  
words-3.0-9.1  
xinetd-2.3.14-10.el5  
xorg-x11-filesystem-7.1-2.fc6  
yum-3.2.22-20.el5  
yum-metadata-parser-1.1.2-3.el5  
yum-security-1.1.16-13.el5  
yum-utils-1.1.16-13.el5  
zip-2.31-2.el5  
zlib-1.2.3-3