# Enabling Protected Processor Identification Number (PPIN) on Lenovo ThinkSystem Servers

## Planning / Implementation

Both Intel and AMD processors all have serial number assigned to them, known as the Protected Processor Identification Number (PPIN). This number makes it easy to identify a specific CPU, which is particularly useful in troubleshooting scenarios.

PPIN is calculated based on the physical characteristics of different chips and added in the factory using fuses on the silicon die. Fuses are one-time programmable devices on a chip used to configure or set specific functionalities during the chip manufacturing process. Once set, the fuses cannot be altered, ensuring PPIN uniqueness and security within the same CPU series. However, the uniqueness of the PPIN number is only guaranteed within the same series of CPUs. In different CPU series, PPIN numbers may be duplicated. PPIN is unique to physical cores, logical cores on the same physical core share the same PPIN.

The algorithm developed by CPU vendors calculates a unique PPIN number based on the hardware characteristics of the processor and other factors. Typically, the generated PPIN is linked to the processor's unique serial number.

The software can communicate with the processor through specific instructions or interfaces and request to obtain the PPIN number. This usually requires the operating system or application program to provide corresponding functional interfaces. Through the specified interface, the software can read the PPIN number from the processor.

Linux kernel version 5.18 and later introduces a new sysfs interface to acquire PPIN number. Users can acquire PPIN by reading `/sys/devices/system/cpu/cpuX/topology/ppin` when enabling PPIN feature.

## PPIN setup in UEFI

The PPIN feature can be enabled by following steps:

1. In System Setup (F1 at boot), enter the UEFI System Configuration and Boot Management as shown in Figure 1:

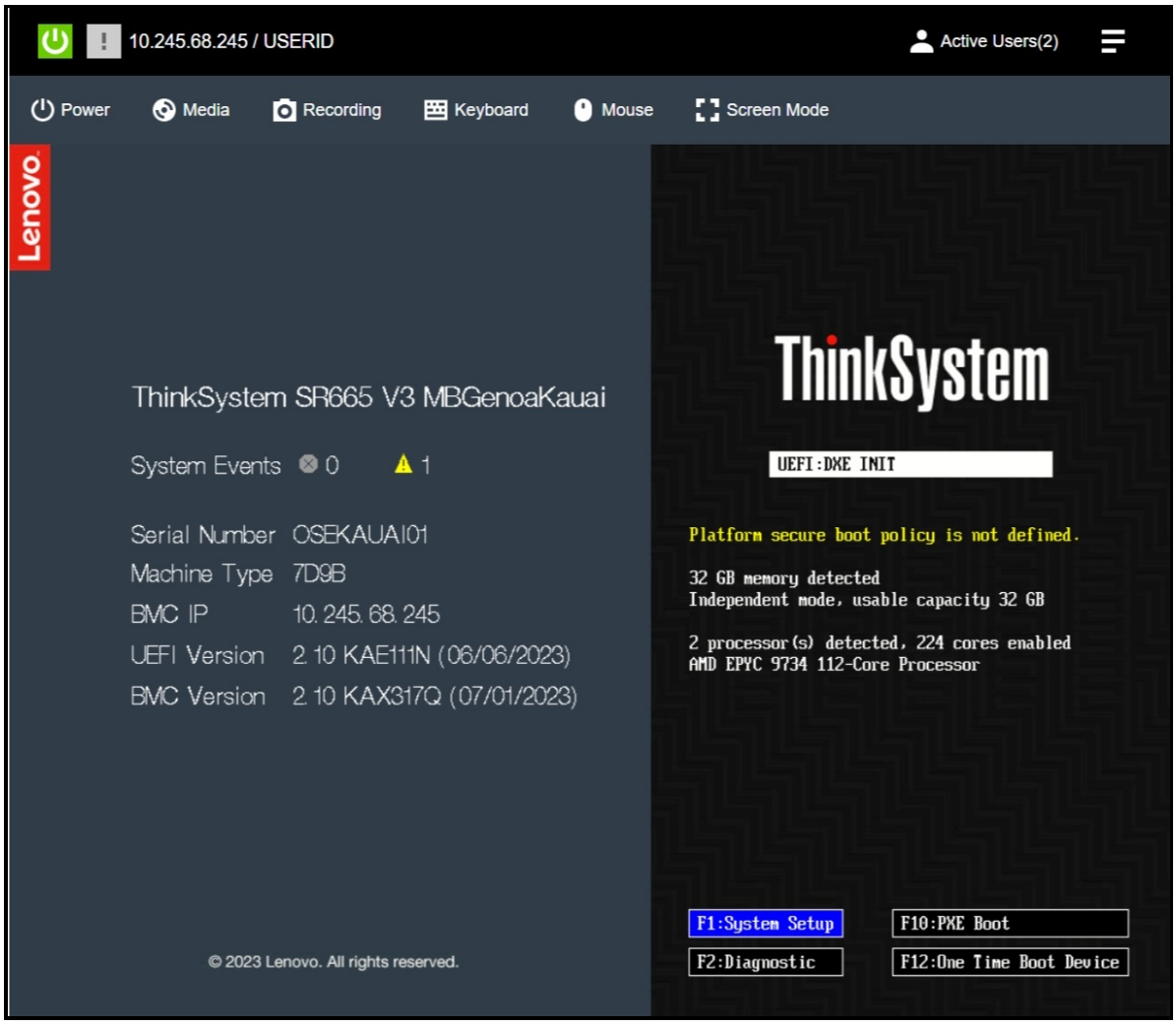


Figure 1. Boot Management in Lenovo System Setup

2. From the BIOS setup menu path, select **System Information > AMD CBS GN > CPU Common Options** and set **PPIN Opt-in** to **Enable** to enable the PPIN feature as shown in Figure 2.

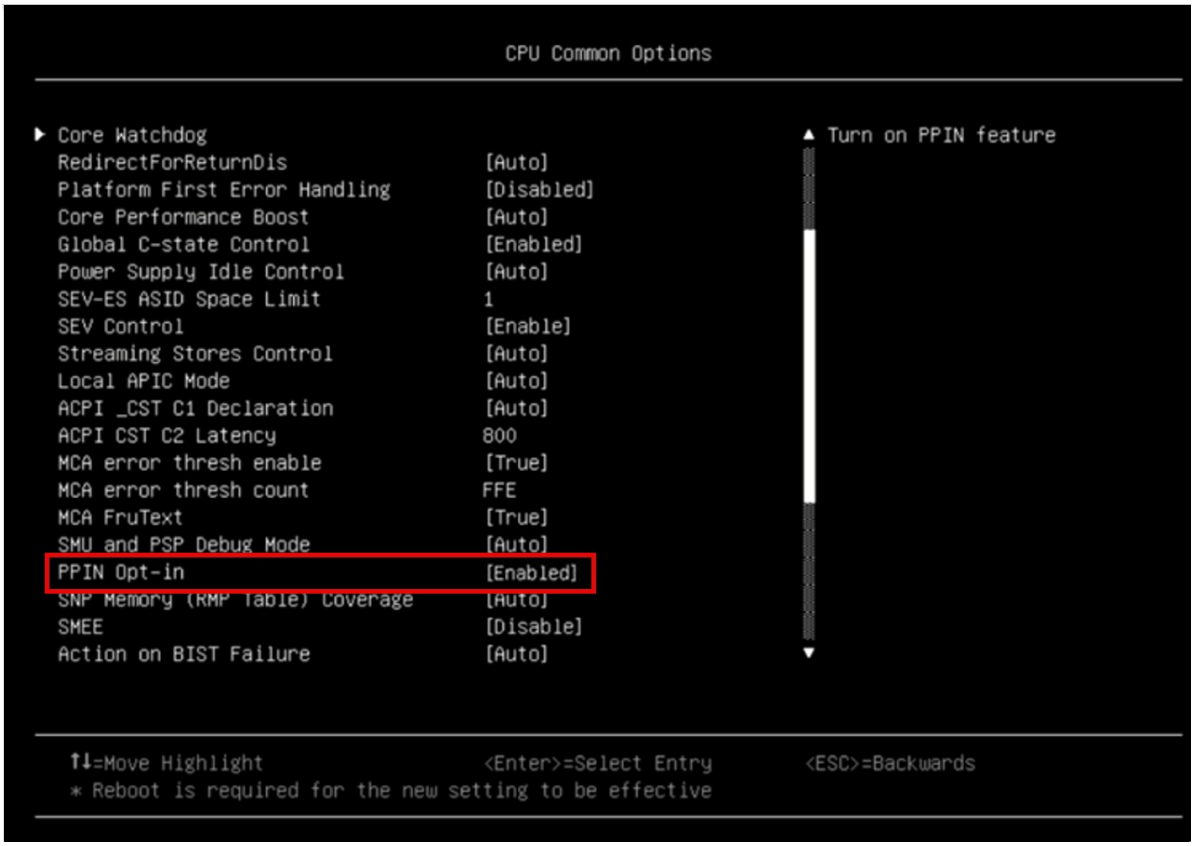


Figure 2. PPIN feature in Lenovo System Setup

3. Save your changes and exit the UEFI System Configuration menu.
4. Once the kernel boots up, you can acquire each of processor's PPIN number by reading the kernel sysfs interface at `/sys/devices/system/cpu/cpuX/topology/ppin`. Each processor has own unique PPIN number.
   Alternatively, you can acquire it via XCC/XCC2 using OneCLI commands. See the following page for details:
   https://pubs.lenovo.com/sr630-v3/enable_intel_on_demand#reading-ppin

Note: In some platform, PPIN Opt-in is hidden, it is enabled by default.

## PPIN working model in the Linux kernel

PPIN working model is shown as in Figure 3.

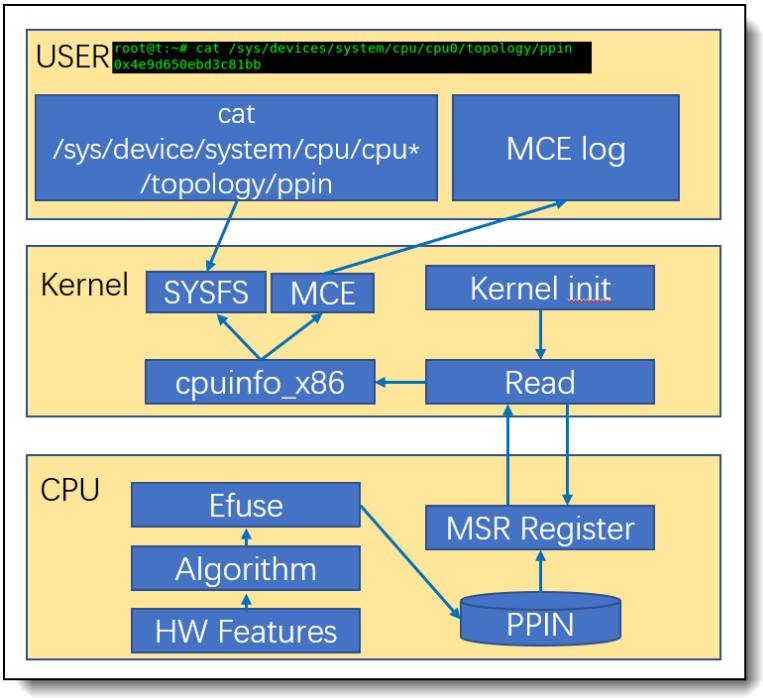


Figure 3. PPIN working model

At the hardware level, when PPIN is enabled, the PPIN algorithm generates PPIN based on hardware features and stores it in efuse. When the CPU powers on, this is directly reflected in the CPU's MSR registers.

At the kernel level, during CPU initialization, the kernel reads the values from the MSR registers and stores PPIN into the software cpuinfo_x86 structure. The PPIN in this structure is then provided to the created sysfs and MCE (Machine Check Error) software components.

At the user level, PPIN can be obtained through both active and passive methods. In the active method, users can retrieve PPIN by reading `/sys/device/system/cpu/cpuX/topology/ppin`. In the passive method, MCE generally adopts a passive approach. When the system detects an error, it triggers MCE and inputs PPIN information into MCE log files. However, this paper mainly describes how to obtain PPIN using the active method.

## Support scope

The Linux kernel supports PPIN starting from Version 5.18.

All ThinkSystem servers with Intel Xeon Scalable processors or AMD EPYC processors support PPIN.

## Troubleshooting

If you cannot acquire PPIN number under the `/sys/devices/system/cpu/cpuX/topology/ppin`, you can use the following steps to do troubleshooting.

1. Check kernel version
   Use the command `uname -a` to check whether your kernel version >= 5.18. If not, upgrade kernel please.
2. Check CPU platform
   Use `lscpu` command to check whether your CPU platform supports PPIN feature. For Intel platform, it needs Xeon or later platforms to support this feature. For AMD platform, it needs EPYC or later platforms.
3. Check whether PPIN feature is enabled
   For Intel if PPIN feature is enabled, `lscpu | grep ppin` has the `intel_ppin` flag as shown in Figure 4:

```
root@Whitleylijia:/root# lscpu | grep ppin
Stepping:            6
Flags:               fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm pbe
syscall nx pdpe1gb rdtscp lm constant_tsc art arch_perfmon pebs bts rep_good nopl xtopology nonstop_tsc cpuid aperfmperf pni pclmulqdq dtes64
 monitor ds_cpl vmx smx est tm2 ssse3 sdbg fma cx16 xtpr pdcm pcid dca sse4_1 sse4_2 x2apic movbe popcnt tsc_deadline_timer aes xsave avx f16
c rdrand lahf_lm abm 3dnowprefetch cpuid_fault epb cat_l3 intel_ppin ssbd mba ibrs ibpb stibp ibrs_enhanced tpr_shadow flexpriority ept vpid
ept_ad fsgsbase tsc_adjust bmi1 avx2 smep bmi2 erms invpcid cqm rdt_a avx512f avx512dq rdseed adx smap avx512ifma clflushopt clwb intel_pt av
x512cd sha_ni avx512bw avx512vl xsaveopt xsavec xgetbv1 xsaves cqm_llc cqm_occup_llc cqm_mbm_total cqm_mbm_local split_lock_detect wbnoinvd d
therm ida arat pln pts hwp_epp vnmi avx512vbmi umip pku ospke avx512_vbmi2 gfni vaes vpclmulqdq avx512_vnni avx512_bitalg tme avx512_vpopcntd
q la57 rdpid fsrm md_clear pconfig flush_l1d arch_capabilities
```

Figure 4. CPU flags for Intel ppin

For AMD, if PPIN feature is enabled, `lscpu | grep ppin` has the `amd_ppin` flag as shown in Figure 5:

```
localhost:~ # lscpu | grep ppin
Stepping:                        1
Flags:                           fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 ht sysc
all nx mmxext fxsr_opt pdpe1gb rdtscp lm constant_tsc rep_good amd_lbr_v2 nopl nonstop_tsc cpuid extd_apicid aperfmperf rapl pni pclmulqdq mo
nitor ssse3 fma cx16 pcid sse4_1 sse4_2 x2apic movbe popcnt aes xsave avx f16c rdrand lahf_lm cmp_legacy svm extapic cr8_legacy abm sse4a mis
alignsse 3dnowprefetch osvw ibs skinit wdt tce topoext perfctr_core perfctr_nb bpext perfctr_llc mwaitx cpb cat_l3 cdp_l3 invpcid_single hw_p
state ssbd mba perfmon_v2 ibrs ibpb stibp ibrs_enhanced vmmcall fsgsbase bmi1 avx2 smep bmi2 erms invpcid cqm rdt_a avx512f avx512dq rdseed a
dx smap avx512ifma clflushopt clwb avx512cd sha_ni avx512bw avx512vl xsaveopt xsavec xgetbv1 xsaves cqm_llc cqm_occup_llc cqm_mbm_total cqm_m
bm_local avx512_bf16 clzero irperf xsaveerptr rdpru wbnoinvd amd_ppin cppc arat npt lbrv svm_lock nrip_save tsc_scale vmcb_clean flushbyasid
decodeassists pausefilter pfthreshold avic v_vmsave_vmload vgif x2avic v_spec_ctrl vnmi avx512vbmi umip pku ospke avx512_vbmi2 gfni vaes vpcl
mulqdq avx512_vnni avx512_bitalg avx512_vpopcntdq la57 rdpid overflow_recov succor smca fsrm flush_l1d
```

Figure 5. CPU flags for AMD ppin

## References

For more information, see the following web pages:

- Linux kernel 5.18
  https://kernelnewbies.org/Linux_5.18
- Convenient Intel PPIN Reporting To Come With Linux 5.18
  https://www.phoronix.com/news/Intel-PPIN-Linux-5.18
- AMD Plumbing Linux Support For Reading The CPU's Protected Processor Identification Number (PPIN)
  https://www.phoronix.com/news/AMD-PPIN-Processor-ID-Linux

## Author

**Dong Wang** is a Linux engineer in the Lenovo Infrastructure Solution Group in Beijing, China.

Thanks to the following people for their contributions to this project:

- Adrian Huang, Lenovo OS engineer, Lenovo ISG, Taiwan

## Related product families

Product families related to this document are the following:

- Processors

## Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area. Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service. Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc.
8001 Development Drive
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary. Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk. Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.



This document, LP1890, was created or updated on February 24, 2024.

Send us your comments in one of the following ways:

- Use the online Contact us review form found at:
  https://lenovopress.lenovo.com/LP1890
- Send your comments in an e-mail to:
  comments@lenovopress.com

This document is available online at https://lenovopress.lenovo.com/LP1890.

## Trademarks

Lenovo and the Lenovo logo are trademarks or registered trademarks of Lenovo in the United States, other countries, or both. A current list of Lenovo trademarks is available on the Web at https://www.lenovo.com/us/en/legal/copytrade/.

The following terms are trademarks of Lenovo in the United States, other countries, or both:
Lenovo®
ThinkSystem®

The following terms are trademarks of other companies:

Intel® and Xeon® are trademarks of Intel Corporation or its subsidiaries.

Linux® is the trademark of Linus Torvalds in the U.S. and other countries.

Other company, product, or service names may be trademarks or service marks of others.