

UEFI Secure Boot

Secure Boot is een bijzondere component van UEFI, die ten doel heeft bescherming te bieden tegen malware die zich in het bootproces heeft genesteld voordat het besturingssysteem wordt geladen, in het bijzonder rootkits en bootkits. Het is een late toevoeging op initiatief van Microsoft. De eerste UEFI specificatie met Secure Boot is versie 2.2 van november 2010, maar pas met de komst van Windows 8 in oktober 2012 werd het echt werkzaam.

Presentatie over UEFI Secure Boot

Op 5 september 2016 gaf Hans Lunsing bij HCC afdeling Leiden, locatie Leiderdorp, een presentatie over Secure Boot. Deze is [van de website van HCC!Zuid-Holland](#) te downloaden. U moet er wel even voor inloggen.

Nuttige links met informatie over UEFI Secure Boot

Hier volgen een aantal webpagina's waarop nuttige informatie over UEFI Secure Boot kan worden gevonden. Helaas is het meeste alleen in het Engels.

www.rodsbooks.com/.../secureboot.html	In addition to implementing a new boot protocol, UEFI adds a new feature that can improve system security, but that also has the potential to cause a great deal of confusion and trouble: <i>Secure Boot</i> . As the name implies, Secure Boot is intended as a security feature. By its very nature, though, Secure Boot can also make it harder to boot Linux, particularly on commodity PCs that ship with Windows pre-installed. This page provides an overview of what Secure Boot is and how the Linux community is responding to it.
www.rodsbooks.com/.../controlling-sb.html	This page is written for more advanced users who want to take <i>full</i> control of their Secure Boot features. Reasons to take this type of control are covered in the Why Read This Page? section of this page.
UEFI boot: how does that actually work then?	This blog post by Adam Williamson is intended to dispel a few common myths and help regular people understand UEFI and Secure Boot a bit better. Secure Boot is not magic. It's incredibly complicated, but the <i>theory</i> isn't very complicated. It's actually a pretty clever mechanism. But what it does can be described very, very simply. It says that the firmware can contain a set of signatures, and refuse to run any EFI executable which is not signed with one of those signatures.
Microsoft about Secure Boot	Secure Boot is a security standard developed by members of the PC industry to help make sure that your PC boots using only software that is trusted by the PC manufacturer. Support for Secure Boot was introduced in Windows 8.
ArchLinux about Secure Boot	This article focuses on how to set up Secure Boot in Arch Linux.
openSUSE about UEFI and Secure Boot	About UEFI and Secure Boot in relation to openSUSE.
Fedora about UEFI	This page attempts to explain some of the things to take into consideration when installing Fedora on systems with UEFI firmwares. It is not a comprehensive description of UEFI theory or practice, but an attempt to provide the most basic information you may need to know.
UEFI Secure Boot Guide by Fedora	Gids voor het begrijpen van en omgaan met UEFI Secure Boot (draft). Nederlandstalig.
Ubuntu about Secure Boot	This page provides information about testing Secure Boot.