NAME

systemd-boot-system-token.service − Generate an initial boot loader system token and random seed

SYNOPSIS

systemd−boot−system−token.service

DESCRIPTION

systemd−boot−system−token.service is a system service that automatically generates a 'system token' to store in an EFI variable in the system's NVRAM and a random seed to store on the EFI System Partition ESP on disk. The boot loader may then combine these two randomized data fields by cryptographic hashing, and pass it to the OS it boots as initialization seed for its entropy pool. The random seed stored in the ESP is refreshed on each reboot ensuring that multiple subsequent boots will boot with different seeds. The 'system token' is generated randomly once, and then persistently stored in the system's EFI variable storage.

The systemd−boot−system−token.service unit invokes the **bootctl random−seed** command, which updates the random seed in the ESP, and initializes the 'system token' if it's not initialized yet. The service is conditionalized so that it is run only when all of the below apply:

- A boot loader is used that implements the **Boot Loader Interface**[1] (which defines the 'system token' concept).
- Either a 'system token' was not set yet, or the boot loader has not passed the OS a random seed yet (and thus most likely has been missing the random seed file in the ESP).
- The system is not running in a VM environment. This case is explicitly excluded since on VM environments the ESP backing storage and EFI variable storage is typically not physically separated and hence booting the same OS image in multiple instances would replicate both, thus reusing the same random seed and 'system token' among all instances, which defeats its purpose. Note that it's still possible to use boot loader random seed provisioning in this mode, but the automatic logic implemented by this service has no effect then, and the user instead has to manually invoke the **bootctl random−seed** acknowledging these restrictions.

For further details see **bootctl**(1), regarding the command this service invokes.

SEE ALSO

systemd(1), **bootctl**(1), **systemd-boot**(7)

NOTES

1. Boot Loader Interface
   https://systemd.io/BOOT_LOADER_INTERFACE