IGEL AND DIGITTRADE HELP SECURE AND OPTIMIZE USER ENDPOINT DEVICES

IGEL OS is built on a secure Linux distribution with an extremely small attack surface. It is designed for easy, intelligent, and secure access to virtual applications, desktops, and cloud workspaces. IGEL OS turns any compatible x86-64 device or thin client into a secure IGEL-managed endpoint.

BENEFIT FROM A SECURE, TRUSTED OS

A read-only, modular OS keeps endpoints as lean as possible and minimizes the attack surface of the device.

SHIFT WINDOWS FROM ENDPOINTS TO THE DATA CENTER OR CLOUD

Moving Windows from endpoints to the data center or cloud simplifies management and keeps apps and data centralized for better security.

MANAGE AND MONITOR ALL ENDPOINTS WITH A SMALL TEAM

The IGEL Universal Management Suite (UMS) offers support for up to 300,000 endpoint devices from a single console.

DELIVER SIMPLE AND EFFICIENT REMOTE SUPPORT

Secure shadowing enables technical support teams to assist users no matter where they are — on the government/agency LAN, off-network, or anywhere else.

USE OF AN ENCRYPTED USB-C FLASH DRIVE WITH KEYBOARD FOR PIN ENTRY

IGEL OS supports the Kobra VS Stick from Digittrade, a BSI-certified USB flash drive with approval for applications up to the classification levels VS-NfD, NATO Restricted, and EU Restricted.

CUSTOMIZED LEVELS OF IT SECURITY

IGEL OS supports a wide range of partner solutions to extend security, which can be easily switched on as required, e.g. data encryption, multi-factor authentication, or solutions to implement many security, compliance, and regulatory requirements.

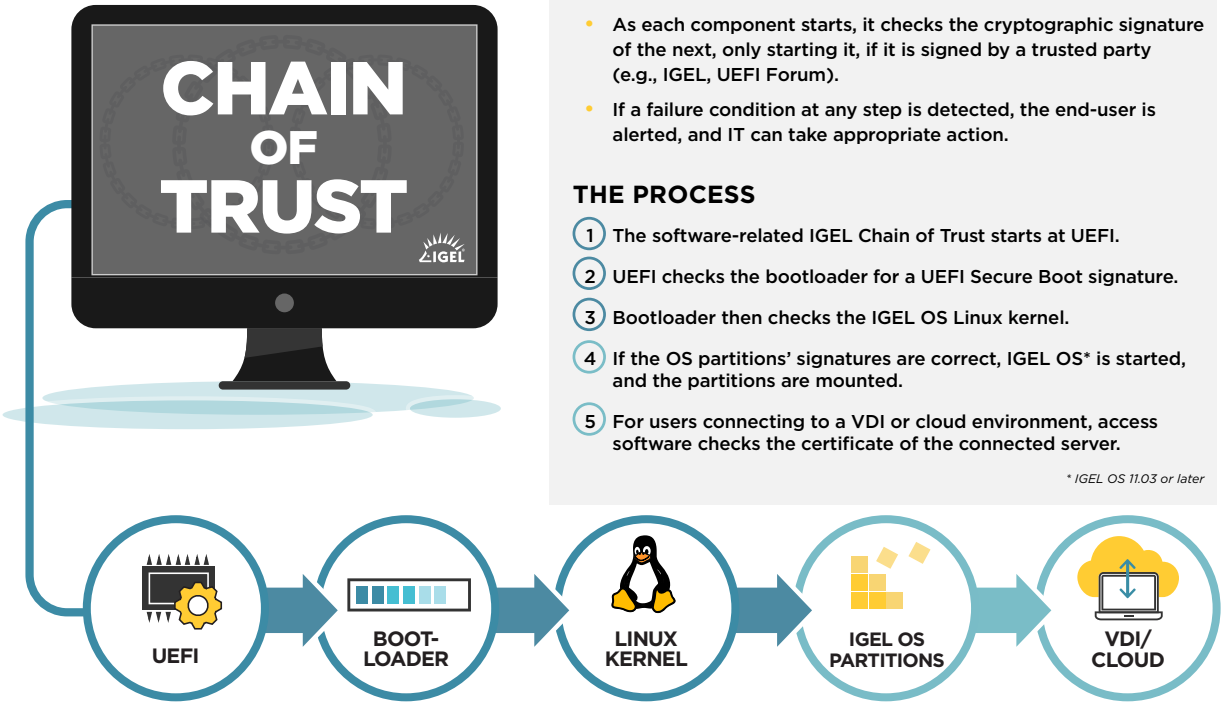
THE IGEL CHAIN OF TRUST

- Ensures all components of a VDI/cloud workspace scenario are secure and trustworthy.
- As each component starts, it checks the cryptographic signature of the next, only starting it, if it is signed by a trusted party (e.g., IGEL, UEFI Forum).
- If a failure condition at any step is detected, the end-user is alerted, and IT can take appropriate action.

THE PROCESS

1. The software-related IGEL Chain of Trust starts at UEFI.
2. UEFI checks the bootloader for a UEFI Secure Boot signature.
3. Bootloader then checks the IGEL OS Linux kernel.
4. If the OS partitions' signatures are correct, IGEL OS* is started, and the partitions are mounted.
5. For users connecting to a VDI or cloud environment, access software checks the certificate of the connected server.

** IGEL OS 11.03 or later*



KOBRA VS STICK - A secure solution for authorities and companies

The KOBRA VS Stick is an encrypted USB-C flash drive that enables data protection-compliant storage and secure transport of sensitive business and private data. It is easy to use and offers secure protection of all stored data.

- **Full-Disk Encryption**
  256-bit AES hardware encryption in XTS mode with 2 x 256-bit crypto keys
- **Access Control**
  Access is gained by entering a user PIN
- **Crypto Key Management**
  Self-management of cryptographic keys: creation, modification, and destruction

Technical details:

- Simple operation, maintenance, and free support
- USB 3.0 & 2.0 compatible
- Pre-boot authentication and boot capability
- Operating systems independent and bootable
- Read/write speed: up to 120 MB/s

Transfer rate:

- USB 3.0 max. 5 GBit/S
- USB 2.0 max. 480 MBit/s

Encryption:

- 256-bit AES hardware encryption in XTS mode with 2 x 256-bit crypto keys

REQUEST A DEMO
IGEL.COM/DEMO

IGEL
next-gen EDGE OS
for cloud workspaces