

VIA ACE-CN X Security Service



VIA ACE-CN X Provides You with a Customized Security Service

ACE-CN X (pronounced as “ace connects”) is a service provided by VIA to help customers get the most out of VIA’s unique hardware-based encryption capabilities. This service aims to help customers connect with VIA’s resident security experts so customers can build their security infrastructure according to their requirements. With VIA’s built-in Advanced Cryptographic Engine (ACE), customers can enjoy high performance on-the-fly encryption.

The Advantages of Hardware Encryption

The development of smarter consumer devices and automated enterprise systems are leading to the increased need for higher security. However, today’s security infrastructure is heavily reliant upon software to make a system or network secure, and it produces a threat cycle that needs to be constantly maintained and updated.

The obvious answer is to have a security infrastructure that almost never needs to be updated. For example, such a security infrastructure would not have to rely on constantly evolving virus definition lists, spyware lists, lists of phishing websites. Such an infrastructure would probably require the use of encryption as its main modus operandi. But anyone who has used encryption knows how slow it can be.

It almost seems that the increase in security comes with a heavy trade off in computing performance. That’s because in most systems, all of the encryption is being handled by a regular CPU. And for a regular CPU to handle the complex instructions of powerful encryption algorithms, the process would most assuredly feel as slow as watching molasses drip in winter — even with a high performance double core CPU.

VIA’s CPUs have a built-in Advanced Cryptographic Engine (ACE). ACE is specially designed to handle powerful encryption algorithms such as AES, SHA-1, SHA-256, etc. Because ACE is designed specifically to handle encryption and decryption, data can be encrypted or decrypted like water running out of a faucet.



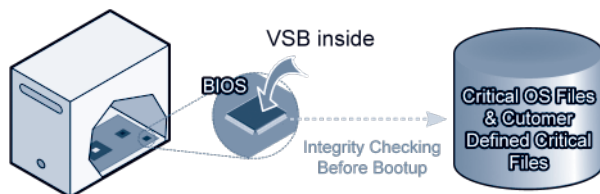
A Comprehensive and Fully Customizable Service

In this day and age, where almost every computer is connected to a network, security breaches are common but not desired. Data thieves use a number of ways to intrude and take information that may be confidential. Some online retailers have had entire databases of customer information stolen – compromising the privacy of millions of people.

1. Secure Boot-up

One example is to ensure a secure environment even before the OS loads. VIA Secure Boot (VSB) secures the computer at boot time to prevent the planting of fake system or application files.

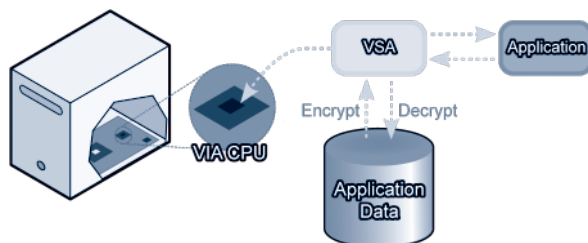
- Prevent hackers from stealing (or duplicating) system design and data to run on another system.
- Prevent hackers from planting malware or spyware to steal valuable information and customer data.
- OS support: Linux, Windows XP/XPe, Windows CE 5.0/6.0



2. On-the-fly Data Protection

All data used by or produced by an application are encrypted. VIA Secure Agent (VSA) can prevent hackers from stealing data by encrypting/decrypting application data on-the-fly without modification to the OS and applications.

- OS support: Linux, Windows XP/XPe



Applications

The flexible VIA ACE-CNXT service can be employed in a wide variety of scenarios where seamless data encryption is required. Data encryption can be used to protect valuable proprietary content in digital signage infrastructures. It can also be used to protect data encryption in remote access or VPN scenarios. Application and database repositories can be encrypted, making the threat of data theft redundant.

- Digital Signage
- Surveillance
- POS
- ATM
- Vehicle
- Automation Control
- Network Storage