



CryptoServer

**Don't compromise when securing
your business process**

Utimaco Safeware Inc.

10 Lincoln Road
Suite 102
Foxboro, MA 02035
USA
Phone: +1 (508) 543 10 08
Fax: +1 (508) 543 10 09

Utimaco Safeware Ltd.

Ash House
Fairfield Avenue
Staines, Middlesex
TW 18 4AB
UK
Phone: +44 (17 84) 224 225
Fax: +44 (17 84) 224 229

Utimaco Safeware AG

Germanusstraße 4
52080 Aachen
Germany
Phone: +49 (241) 16 96-200
Fax: +49 (241) 16 96-199
hsm@utimaco.com

You will find more information about CryptoServer at:

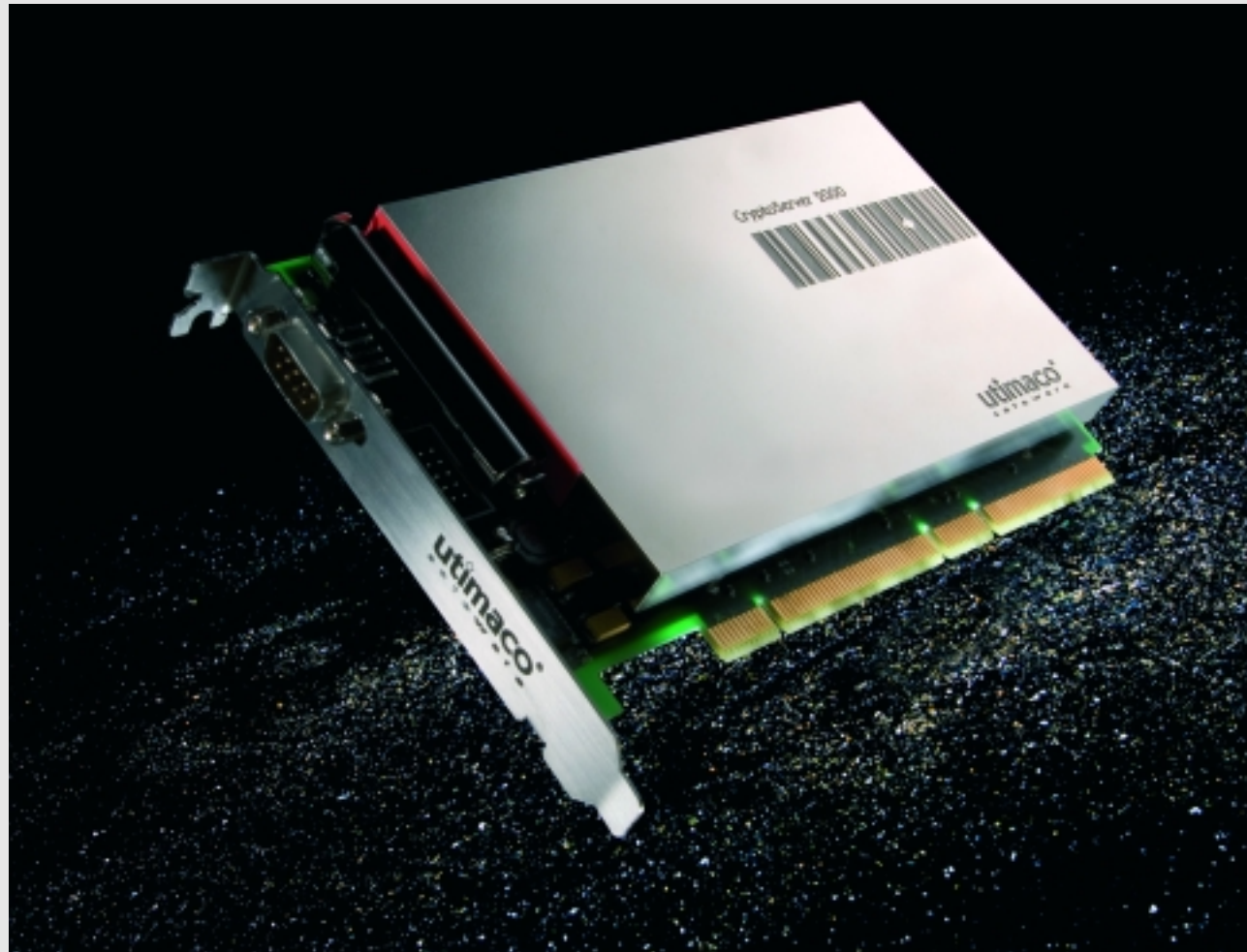
www.utimaco.com/hsm

utimaco[®]
safeware

© 2006 – Utimaco Safeware AG
All CryptoServer are registered trademarks of Utimaco Safeware AG. All other named trademarks are trademarks of the particular copyright holder.

utimaco[®]
safeware

IT security technology by Utimaco: Protecting the electronic assets of companies and government bodies



CryptoServer PCI



Utimaco Safeware has been developing security solutions since 1983. Today, Utimaco is one of the world's leading manufacturers of innovative and professional solutions for data security. The security technology and solutions developed by Utimaco protect the electronic data of companies and government bodies against unauthorized access and guarantee that business processes and administrative procedures in the electronic world are binding and confidential.

Customers and partners value the reliability, simplicity, and long-term investment security of the Utimaco security solutions. Utimaco stands for recognized product quality, user-friendly software, excellent support, and products that effectively meet market requirements.

For more information, visit our website at www.utimaco.com

Online transactions and digitalization optimize your business processes



Electronic business processes – increasingly under threat from security risks

The Internet has evolved from purely a means of communication to become the central interface of networked business processes. Nowadays a multitude of diverse transactions are processed and controlled electronically. In our daily lives, common examples include electronic financial transactions and online tax declarations, data entry and processing in CRM and ERP systems involving more than one company, organizing purchasing by e-procurement and e-sourcing,

e-mail correspondence, road pricing system, online shopping, virtual auctions and lottery games on the Internet, refilling prepaid cards, and the digital processing of patient data via electronic health cards.

The increasing use of Application Service Providers (ASPs) means that entire applications, and therefore parts of a company's electronic value-added chain, can be completely outsourced.

CryptoServer
Don't compromise when securing
your business process

Despite all of its benefits, the move to optimized electronic business processes also opens up vulnerable areas to data theft, industrial espionage, and attacks on IT infrastructures. As network boundaries become more fluid and applications become ever more complex, there is a corresponding increase in the number of security loopholes which offer potential attackers a wide range of opportunities for their misdeeds.

But it is not only the methods of attack used today, such as phishing or hacking, that are the problem. Increasingly, security risks and new points of attack can be traced back to simple carelessness or poorly implemented electronic processes.

Commercial and industrial espionage

The close technical organizational integration of staff, partners, and customers that is necessary in successful business processes also significantly increases security risks. In its annual report on IT security for 2005, the German Federal Ministry for Security in Information Technology (BSI) wrote, "The Internet is opening up new dimensions for

commercial and competitive espionage. The methods used to detect and manipulate data and services are becoming more and more professional. Technology and specialist knowledge are the classic targets for thieves, but gaining a competitive advantage by spying on offers, contracts, and pricing information is also on the increase. Snooping on corporate networks with the aim of gaining unauthorized knowledge of enterprise data will become more common in the next ten years". This warning from the BSI is based on several studies by the corporate consultants KPMG and PricewaterhouseCoopers (PwC) in the two previous years, which showed that over 70% of companies consider industrial espionage to be a threat, and that more than 80% of respondents expect the number of espionage attacks to rise in future. Moreover, the Institute of Directors (IoD), an association with headquarters in London, and more than 55,000 decision-makers world-wide from all sectors of industry all sectors of industry stated that among its members 60% of them had already suffered harm from the theft of information.

CryptoServer – Maximum security for your data

Because business-critical information of all kinds needs reliable protection against unauthorized access, manipulation, and theft, IT security is one of management's most important tasks today in business, in public administration (e-government), and in health-care (e-health).

New business processes, technologies, and legal requirements require new security strategies. In a dynamic competitive environment, the ability to quickly modify and extend security mechanisms as system landscapes grow and become more heterogeneous is no simple task. The Utimaco CryptoServer hardware security solutions provide optimum protection when you need efficient and cost-effective secure business processes or need to comply with legal and company-wide security requirements.

The basic idea behind a hardware security module

Today's cryptography guarantees the security of user data, so the way electronic transactions are processed completely meets demands for confidentiality, integrity, and identity (authenticity). However, the encrypted data are not protected effectively until the computer systems on which these cryptographic transactions are performed, and on which the keys that will be used in the future are saved, are also fully secured.

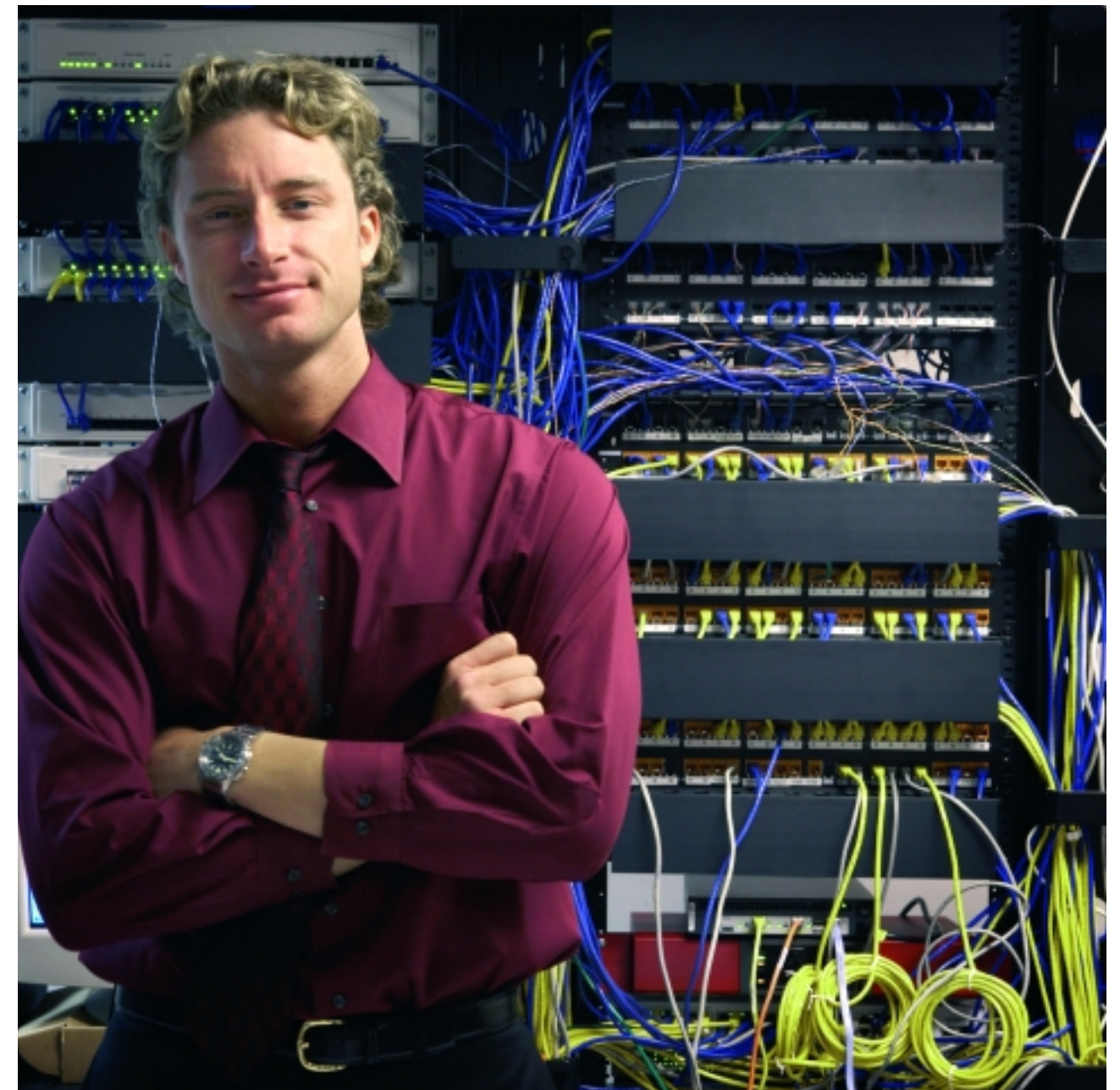
A solution to achieve this has been developed using HSM (referred to as both hardware security module and host security module)

technology. All current certification procedures for proving that IT security measures have been implemented, physically and logically, such as the American FIPS 140-2* standard, share these general basic characteristics:

- A computer must have reliable protection so that its data and programs can never be manipulated and accessed.
- Communication with the HSM's computing unit is via an interface that does not permit any attacks from the application interface.
- The HSM's computing unit is equipped with a protective system that immediately recognizes attacks from outside and actively reacts by deleting the saved information to guarantee data security.

Known as tamper-resistant hardware, this includes sensors for automatically recognizing attacks and circuits for performing appropriate countermeasures. The current generation of the CryptoServer hardware security modules provide measures for protecting against:

- Extracting and analyzing data
- Temperature attacks
- Mechanical attacks
- Chemical attacks
- Tampering using electrical current



Hardware security modules such as the CryptoServer can be used to save important, confidential, and business-critical enterprise data (such as corporate certificates, signature keys, encryption keys, etc.) safe from tampering and theft, and then process that data and make it available for use. This provides

a way for companies to create their own "zone of trust." In other words, hardware security modules provide comprehensive data security, even in environments such as external computing centers in which they have no direct control over or access to cryptographic identities and keys or their application.

* Federal Information Processing Standard (FIPS) 140-2 Level 3 is the international security standard for cryptography modules.

CryptoServer provides security in three dimensions

Ten years ago, in the first version of the Utimaco HSM, the most important issues were the basic architectures of the processors and memory module to be used and the design. With today's powerful digital signal-processor architectures, the focus is now on security circuits and the ways to optimize them.

In CryptoServer, Utimaco gives customers not only the benefit of its many years of experience in IT systems integration, but also a hardware security module that creates three-dimensional security:

- The security of keys and their applications in accordance with cryptographic procedures (with American FIPS 140-2 standard certification*).
- High fail-safe security and availability.
- High investment security due to its open and uniquely modular software concept, which enables CryptoServer to be upgraded to work with new or changed procedures, even in years to come.

Our product philosophy: your security in all three dimensions

Our experts in hardware security not only define security to mean cryptography or secure key memory – for them security also means certified hardware, availability, and reliability.

Hardware security must be achieved as cost-effectively as possible, whether in the case of largely standardized system landscapes such as Microsoft Server, for applications in which security tools and functions are integrated via PKCS #11 interfaces, or in payment traffic with clearly defined procedures.

A characteristic of the cost-efficiency of CryptoServer is its high level of flexibility and openness, which means it can be integrated smoothly into all business processes and specific IT architectures: both CryptoServer PCI and CryptoServer LAN base platforms work with all basic IT architectures. These two variants of the Utimaco HSM offer the following basic functionality:

- **CryptoServer PCI** is the best solution for users who configure and administer their own IT infrastructure and place greater emphasis on the security of their data and keys.

- **CryptoServer LAN** is suitable for users who implement dedicated server units in their IT architecture and require a clear division between technical functionality and the IT systems in use. With CryptoServer LAN you can implement role-based administration, because many company policies need to distinguish between their security, system, and network administrators.

Simply secure

Cryptography, certificates, PKCS interfaces – all these terms, abbreviations, and functional descriptions make it harder to understand, select, and implement IT security systems. Carrying out detailed in-house analysis of requirements and implementing complex certification procedures that have been tailored to meet the high protection potential of HSMs is both expensive and time-consuming.

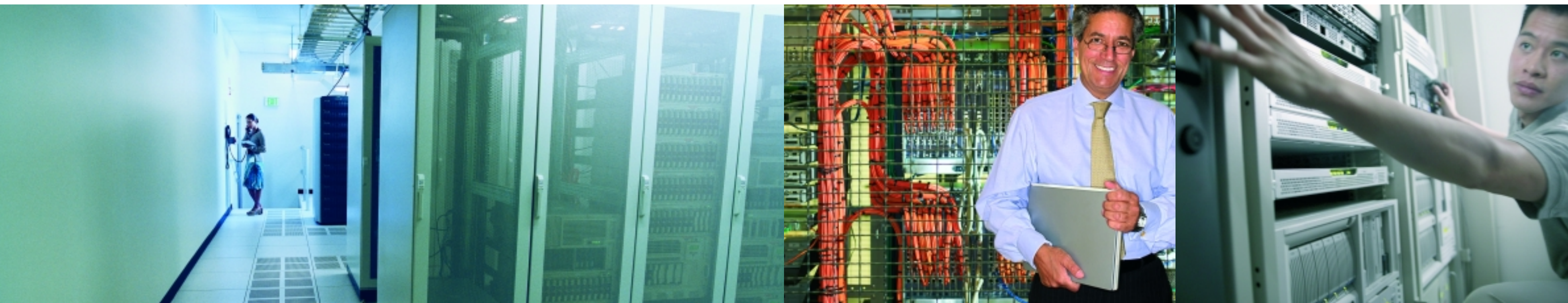
CryptoServer combines all of the necessary functions, procedures, and interfaces in a range of ready-to-use solution packages, all of which meet the requirements of the many various sectors of industry and business processes.

When selecting a product you are no longer forced to research cryptography and hardware security. Instead, you can choose an

optimized standard package that consists of certified hardware and software that has been tried, tested, and refined over many years of use. And if you want to add specific functions, CryptoServer can be retrofitted whenever you want and without having to upgrade hardware. To do this, Utimaco can turn to its extensive portfolio of protocols and applications from many already successfully completed projects.

CryptoServer

Don't compromise when securing your business process

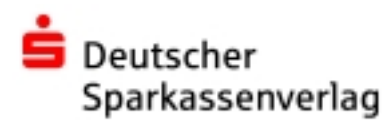


What users say about CryptoServer



"No payment traffic transaction is possible without very high standards of security. Security module technology is the core of a payment system. We decided to use CryptoServer 2000 because Utimaco offers the best platform and the most thorough security concept. With CryptoServer we can integrate existing and future requirements in all aspects of cashless payment traffic, both effectively and efficiently."

Peter Ortmann,
IT Security Product Manager at Atos Worldline GmbH



"The deciding factor in choosing Utimaco's hardware security module was the security of investment that resulted from working with an established, reliable and experienced partner. The CryptoServer is providing us with a security platform that will give us maximum reliability, flexibility, and upgradability."

Dr. Rüdiger Mock-Hecker,
Director of the card system department at the Deutscher Sparkassenverlag (DSV)



CryptoServer LAN