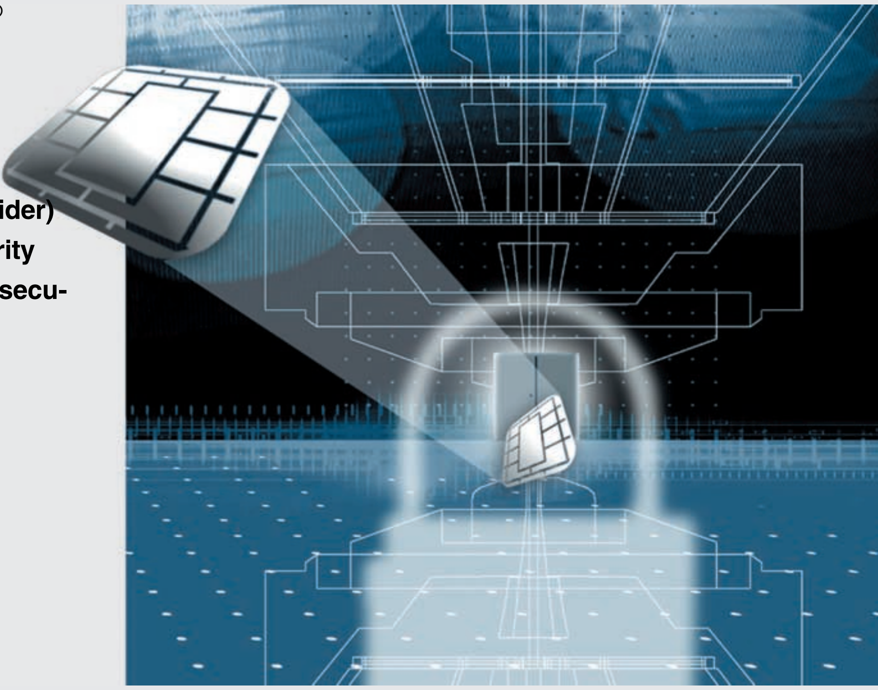
The ticket to HW-secured Microsoft® Windows® 2000 & Windows® XP Public Key Infrastructure



Infineon's SICRYPT® CSP (Crypto Service Provider) implemented on Infineon's chipcard- and security controller family SLE66P directly supports the security token enabled Microsoft® Windows® 2000 & Windows® XP Public Key Infrastructure (PKI). It can be implemented on smartcards as well as in USB-Tokens.

SICRYPT

Infineon Technologies SICRYPT® CSP offers:

- Full support of Microsoft® Windows® 2000 & Windows® XP Public Key Infrastructure
- A plug and play solution already included in the Microsoft® Windows® XP standard package
- A CSP compliant to Microsoft®'s Smart Card Cryptographic Provider (SCCP) requirements
- A technology based on Infineon's SLE66P security and chipcard controller family

Infineon's SICRYPT® CSP provides a ready to use technology for the Microsoft® Windows® 2000 & Windows® XP Public Key Infrastructure. The host SW stack, required to assure a proper communication between the host and the SICRYPT® CSP enabled smartcards and USB-tokens, is already implemented in the basic Windows® XP package.

Today the SICRYPT® CSP comes on the SLE66CX320P HW-platform. The USB enabled SLE66CUX640P HW-platform will follow soon.

Both HW-platforms offer sufficient E^{2}PROM capacity for additional on-chip file structures required for project specific SICRYPT® CSP solutions like e.g. an employee ID-card with PKI capability. Such on-chip file structures can be utilized by a host application.
The SICRYPT® CSP Software Development Kit (SDK) eases the customisation and implementation into the host application.

Infineon SICRYPT® CSP together with Infineon SLE66P security- and chipcard controller family enables card manufacturers to offer a complete and proven solution.
Take the opportunity!

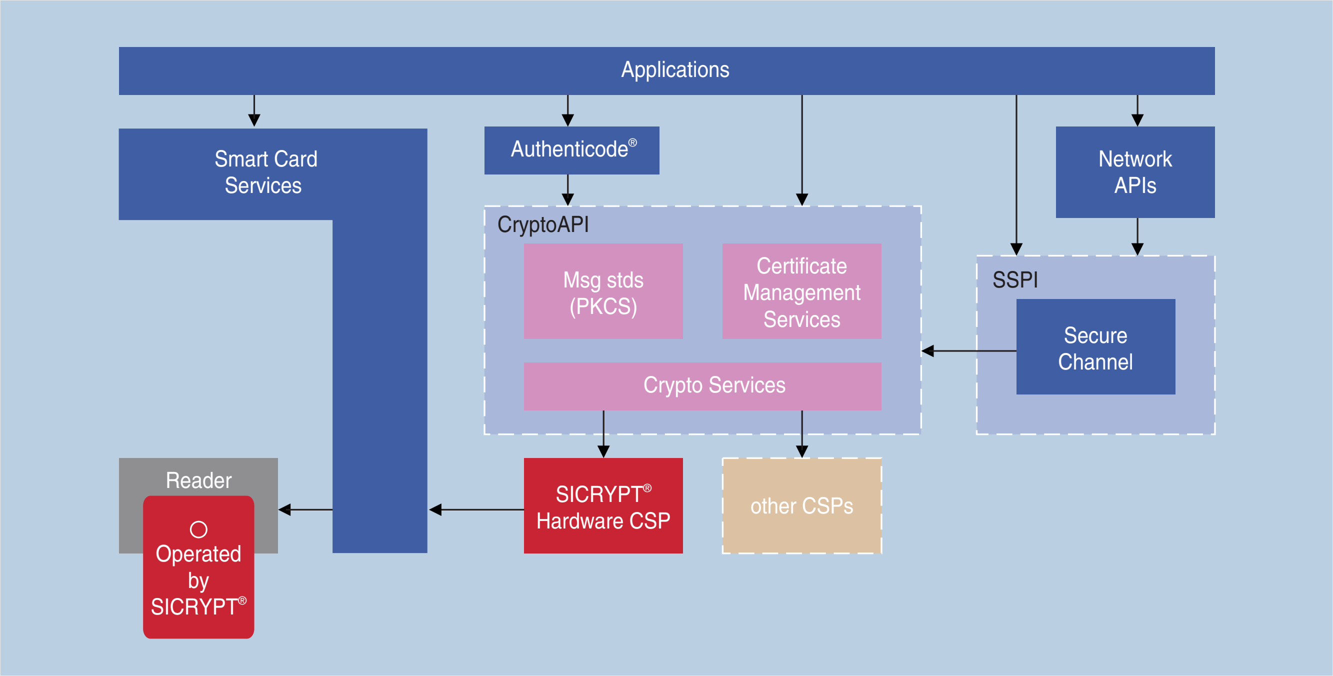
www.infineon.com/SICRYPT

SICRYPT® CSP

Infineon technologies

Never stop thinking.

SICRYPT® CSP utilized by Windows® 2000 & Windows® XP PKI Architecture



The need for hardware based IT-security is getting stronger day by day. Authentication, Privacy, Confidentiality and Integrity are the keywords. These properties are the basic needs to enable trusted communication and trusted e-business via open networks. IT-security solutions need to consider these requirements. “Public Key Infrastructure“ has become the synonym for a technology providing all these properties. This is true - especially when the private keys are stored in secure storage and computing devices like smart cards and secure USB-tokens.

The inherent PKI platform within Microsoft® Windows® 2000 & Windows® XP is fully smart card (or generally spoken security-token) enabled. Thus client authentication, public key interactive logon and secure email can fully leverage the enhanced security offered by smart cards and USB-tokens.

Client authentication involves identification and validation of a client to a server to establish a secure communication channel for e.g. finance transactions. Typically a secure protocol, such as Secure Sockets Layer (SSL) is used. The secure session is established using public-key authentication with key exchange to derive a unique session key. The smart card or secure USB-token enhances the public-key authentication process by serving as a secure store for the private-key material and as a cryptographic engine for performing a digital signature or key-exchange operation. Client authentication can be used via the Microsoft® Internet Explorer.

Public key interactive logon uses the public key certificate of the card to authenticate a user to a network. Thus only the cardholder is able to get access to the system. There are no passwords anymore which can be hacked. Additionally a Personal Identification Number (PIN) is used to authenticate the user to the card to avoid misuse of the card. Public Key interactive logon can be used via the Graphical Identification and Authentication GINA.

Secure email is a quite exciting public-key-enabled application because it allows users to share information confidentially and to trust that the integrity of the information was maintained during transit. A smart card significantly increases the level of integrity to secure email because it stores the private key on the card, protected by a PIN. Secure email is directly supported by Microsoft® Outlook® and Outlook® Express.

Further information see www.infineon.com/sicrypt

How to reach us:
http://www.infineon.com

Published by
Infineon Technologies AG,
St.-Martin-Strasse 53,
81541 München

Attention please!

The information herein is given to describe certain components and shall not be considered as warranted characteristics.

Terms of delivery and rights to technical change reserved.

We hereby disclaim any and all warranties, including but not limited to warranties of non-infringement, regarding circuits, descriptions and charts stated herein.

Infineon Technologies is an approved CECC manufacturer.

Information

For further information on technology, delivery terms and conditions and prices please contact your nearest Infineon Technologies Office in Germany or our Infineon Technologies Representatives worldwide.

Warnings

Due to technical requirements components may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies Office.

Infineon Technologies Components may only be used in life-support devices or systems with the express written approval of Infineon Technologies, if a failure of such components can reasonably be expected to cause the failure of that life-support device or system, or to affect the safety or effectiveness of that device or system. Life support devices or systems are intended to be implanted in the human body, or to support and/or maintain and sustain and/or protect human life. If they fail, it is reasonable to assume that the health of the user or other persons may be endangered.

Published by Infineon Technologies AG

Ordering No. B116-H0000-X-X-7600
Printed in Germany
PS 02022. NB