

## smart security component

silicon

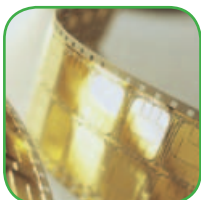
hardware security

100%

processor



### smart security component<sup>®</sup>



charismathics<sup>®</sup> provides affordable, easy to use and flexible identity solutions for the issuance and personalization of hardware tokens and smart cards.

Our smart security component is an integrated platform made up of a PKI smart card chip and the charismathics CSP, PKCS#11 and tokenD interfaces. This unique solution provides complete independence with maximum flexibility when selecting your smart card chip platform and operating system for use with identity management applications. The result is an enabling technology supporting all major smart card platforms that integrates into all PKI and client application environments. charismathics makes it possible to utilize smart tokens in new ways for secure mobile computing and secure data storage.

Never before has it been so easy to integrate a new authentication solution into an existing infrastructure.

### Overview:

- smart card chips for end-to-end security applications
- 3D-independence
- secure key generation and key pair storage
- plugs into all standard software applications
- quick integration with software and customized file structures

### Benefits

- smart card chip based technology for true data encryption, secure key generation and key pair storage
- seamless integration with existing PKI environments for smooth hardware upgrades
- support for all standard software applications such as MS Explorer, Firefox, MS Outlook, Entourage, Mail.app, Safari, etc.
- multiple smart card chip platform support
- quick integration with software and customized file structures
- support of pre-boot environments (Check Point, McAfee, PGP, Secude, Sophos)

### Product Integration Support

charismathics supplies a wide range of integrated circuits for PKI environments to the world market. Experience in security hardware integration as well as expertise to custom manufacture products meeting your specific requirements and certifications make our bundle of hardware and software unique. We offer simple, yet complete packages which maximize your price to value ratio. With our large buying power and our top level supplier relationships, charismathics can meet the demands for large quantities with rapid deliveries.

charismathics

## 3D-independence on platforms, vendors and applications

The smart security component optionally comes with our smart security interface<sup>®</sup>, the middleware which allows the use of a smart card security chip with the operating system of your choice. With smart security interface it is possible to use more than one smart card operating system on a single client at the same time. The middleware provides a single CSP, PKCS#11 and

tokenD module supporting multiple card profiles for literally any smart card related project. Digital certificates are made available for applications, like Outlook and Notes, as well as Firefox, Entourage, Mail.app and Novell. The smart security interface supports all major operating systems, including Macintosh, Linux and Solaris.

## A Selection of our PKI Smart Card Platforms

|                           | CardOS  | JCOP   | Oberthur<br>Cosmo ID  | jTOP   | TCOS   | SmartCafe<br>Expert   | Kona   |
|---------------------------|---|--|---|--|--|---|--|
| chip vendor               | Infineon  | NXP  | NXP<br>Atmel  | Infineon   | NXP<br>Infineon  | NXP<br>Infineon   | NXP<br>Samsung   |
| co-Processor              | yes   | yes  | yes   | yes  | yes  | yes   | yes  |
| delivery form             | wafer/<br>wafer/frame   | wafer/<br>wafer/frame  | wafer/<br>wafer/frame   | wafer/<br>wafer/frame  |  | wafer/<br>wafer/frame   | wafer/<br>wafer/frame  |
|                           | contact<br>module   | contact<br>module  | contact<br>module   | contact<br>module  | contact<br>module  | contact<br>module   | contact<br>module  |
|                           | contactless<br>module   | contactless<br>module  | contactless<br>module   | contactless<br>module  | contactless<br>module                                      | contactless<br>module   | contactless<br>module  |
|                           | dual<br>interface<br>module   | dual<br>interface<br>module  | dual<br>interface<br>module   | dual<br>interface<br>module  | dual<br>interface<br>module                                | dual<br>interface<br>module   | dual<br>interface<br>module                                    |
| EEPROM<br>Memory Size     | 36kB/68kB   | 36kB/72kB/<br>144kB  | 16kB/36kB<br>72kB/64kB<br>128kB/144kB                                       | 36kB/68kB  | 36kB/72kB  | 16kB to<br>144kB  | 36kB/72kB  |
| applets                   | n/a   | EMV, ICAO,<br>PKI  | EMV, ICAO,<br>PKI   | ICAO,<br>PKI   | n/a  | EMV,<br>PKI   | EMV,<br>PKI  |
| USB<br>interface          | no  | optional   | optional  | no   | optional   | optional  | optional   |
| contactless<br>operation  | optional<br>ISO<br>14443b,<br>T=CL  | optional<br>ISO<br>14443a/b,<br>T=CL   | optional<br>ISO<br>14443a/b,<br>T=CL  | optional<br>ISO<br>14443a/b,<br>T=CL   | optional<br>ISO<br>14443a/b,<br>T=CL                       | optional<br>ISO<br>14443a/b,<br>T=CL  | optional<br>ISO<br>14443a/b,<br>T=CL                           |
| RSA                       | up to<br>2048bit  | up to<br>2048bit   | up to<br>2048bit  | up to<br>2048bit   | up to<br>2048bit   | up to<br>2048bit  | up to<br>2048bit   |
| ECDSA                     | up to 384bit  | up to 256bit   | upto 256bit   | no   | up to 256bit   | up to 256bit  | no   |
| SHA-2xx                   | CardOS 4.4<br>only  | yes  | v5.4<br>and v7.0  | no   | no   | no  | no   |
| families                  | 4.2B/4.3B<br>4.2C/4.4   | JCOP<br>v21/31/41<br>J2A/J3A/J4A   | v5.2/5.4/5.5<br>v7.0  | jTOP v2<br>jTOP 15   | v3.0   | v3.0/3.1/3.2<br>v5.0  | v10<br>v25/26<br>v132  |
| product<br>certifications | chip<br>EAL 5+<br>software<br>CC EAL 4+<br>SigG<br>CWA 14169<br>Type3<br>IAS<br>CNS | chip<br>CC EAL 5+<br>software<br>EAL 4+<br>EMV<br>certified<br>(with<br>NXP applets)<br>ICAO | chip<br>CC EAL 5+<br>software<br>CC EAL 4+<br>SSCD<br>FIPS 140-2<br>level 3 | chip<br>CC EAL 5+<br>software<br>CC EAL 4+/5+<br>VISA approval<br>Mastercard<br>certified ICAO | chip<br>CC EAL 5+<br>software<br>CC EAL 5+<br>SigG<br>ICAO | chip<br>CC EAL 5+<br>software<br>CC EAL 4+<br>SSCD<br>FIPS 140-2<br>level 3 | chip<br>CC EAL 5+<br>software<br>CC EAL 4+<br>VISA<br>approval |

**charismathics**

the middleware company

charismathics gmbh  
47 Sendlinger St  
Munich, Germany 80331

www.charismathics.com  
sales@charismathics.com

phone +49 (89) 3090-6700

**charismathics**

the middleware company

charismathics inc.  
2033 Gateway Place Suite 500  
San Jose, CA 95110, USA

www.charismathics.com  
sales@charismathics.com

phone +1 (408) 573 6440

charismathics