

# Security and Trust Services APIs For the Java™ 2 Platform, Micro Edition

Cryptographic Operations and Smart Card Communication For Mobile Devices



## Key Feature Highlights

- Provides user certificate management and authentication services for mobile devices
- Allows a Java™ 2 Platform, Micro Edition (J2ME™) application to communicate with applications running on a smart card
- Enables the development of new, rich applications that provide value-added services to end users
- Lowers the cost of developing, maintaining, and debugging applications by increasing developer productivity
- Ensures faster downloads and maximizes memory footprint through standards-based APIs

Today's wireless handsets and other mobile devices are merging voice, multimedia, data, and connectivity services onto a single handheld platform. The mobility and increasing computing power of these devices enable developers to deploy new, sophisticated, value-added services. For example, location-based information services allow a traveler to use an Internet-enabled phone to find the nearest hotel or obtain train schedules. Through mobile commerce applications, drivers will be able to pay for gas through a wireless handset when they fill up at a gas station.

The success of these applications requires a high level of security and trust. Because the mobile device essentially becomes its owner's digital identity, there must be some method for authenticating the user and ensuring that the device can be trusted. Providing secure data access over a mobile network and reducing fraud in mobile payment systems is absolutely critical.

### Security For Application-Based Services

To perform trusted operations, applications running Java™ 2 Platform, Micro Edition (J2ME™ platform) rely on the security services provided in a smart card or similar device to ensure that the cryptographic keys are stored securely and that the cryptographic computations are performed securely. To address the security requirements of J2ME applications running on mobile devices, the Security and Trust Services APIs for the Java 2 Platform, Micro Edition — Java Specification Request (JSR) 177), also known as SATSA — has been developed through the Java Community Process™ (JCP™) program. Created by an expert group comprised of leading mobile device manufacturers, wireless operators, and mobile software vendors, the specification defines APIs that provide several capabilities to J2ME platforms: Application-level digital signatures, basic user credential management, cryptographic operations, and smart card communication.

### User Verification For Secure Transactions

To complete a mobile shopping transaction, an online merchant needs to verify that the wireless subscriber has authorized the transaction. The merchant also must send a receipt or confirmation to the subscriber. The best method of authenticating users and authorizing transactions is obtaining a digital signature from the user's device. SATSA provides a digital signing service that allows a J2ME application to generate digital signatures that conform to the Cryptographic Message Syntax (CMS) format.

The user's identity is usually bound to a public key through a public key certificate. SATSA also has related user credential management functions that allow the device to manage the certificate on the user's behalf. Using a SATSA API, the device can generate a certificate enrollment request that can be sent to a certificate authority. User credential management also allows a J2ME application to add or delete a user certificate to or from a certificate store.

## Security and Trust Services APIs For the Java™ 2 Platform, Micro Edition

### Securing Mobile Data Through Encryption

Large amounts of data are managed within today's wireless networks. Much of this data comprises personal information or communication that must be handled in a secure, encrypted form. To enable this capability, SATSA also includes a general-purpose cryptography library that provides a subset of the Java 2 Platform, Standard Edition (J2SE™) cryptography API. It supports basic cryptographic operations, such as signature verification, encryption, and decryption, that allow a J2ME application to provide secure data communication, data protection, and content management.

### Enabling Access To Existing Security Services

Digital signature generation and credential management rely on a security element for storing sensitive data — private keys, public key certificates, and other personal information. The security element also performs cryptographic computations to support payment protocols, data integrity, and data confidentiality, and is most commonly implemented as a smart card.

Smart cards provide a secure, programmable environment that can run applications such as custom and enabling security services. J2ME applications can use these services to handle many types of value-added services, including mobile commerce, banking, stock trading, and gaming. The services can be continually upgraded with new or improved applications that are installed on a smart card. To leverage the

security services deployed on a smart card, SATSA provides access methods for a J2ME application to communicate with the card.

### New Opportunities For Richer Services

By providing secure services, SATSA expands the range of applications developers can create for mobile platforms. Because developers can use SATSA to communicate with the smart card, they can access user information with which they can drive new applications — such as account access and bill payment — through the wireless handset, or coupon and loyalty programs.

### Increased Productivity Through Standards-Based APIs

SATSA offers a standard method of creating secure services in the Java application environment. Mobile devices that support the specification will have built-in security and trust functions. Because the secure services are platform-provided, developers do not need to create their own versions. SATSA APIs free developers to focus on other aspects of the applications, increasing their productivity and reducing programming, maintenance, and debugging costs.

### Reduced Application Footprint

Because memory is one of the largest costs in a wireless handset, applications ideally should have as small a footprint as possible. SATSA specifies the security and trust services available to all applications on a compliant platform; thus,

only one occurrence of these services exists in memory and can be shared by each application. The smaller footprint means that applications are faster to download, and more applications can be stored in the device.

### Serious Software Made Simple

Sun provides a complete portfolio of affordable, interoperable, and open software systems designed to help you maximize the utilization and efficiency of your IT infrastructure. Sun's portfolio consists of Solaris™ and Linux software for SPARC® and x86 platforms, the N1™ Grid platform for dynamic and utility computing, and the Sun Java System — five integrated software systems for the data center, the desktop, the developer, mobile devices, and identity implementations.

### For More Information

To learn more about the Security and Trust Services APIs for the Java 2 Platform, Micro Edition, please visit the following Web sites:

- J2ME: [java.sun.com/j2me](http://java.sun.com/j2me)
- JSR 177: [jcp.org/en/jsr/detail?id=177](http://jcp.org/en/jsr/detail?id=177)
- Java Community Process: [jcp.org](http://jcp.org)

### Learn More

Get the inside story on the trends and technologies shaping the future of computing by signing up for the Sun Inner Circle program. You'll receive a monthly newsletter packed with information, plus access to a wealth of resources. Register today at [sun.com/joinic](http://sun.com/joinic).

Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA Phone 1-650-960-1300 or 1-800-555-9SUN Web [sun.com](http://sun.com)



**Sun Worldwide Sales Offices:** Argentina +5411-4317-5600, Australia +61-2-9844-5000, Austria +43-1-60563-0, Belgium +32-2-704-8000, Brazil +55-11-5187-2100, Canada +905-477-6745, Chile +56-2-3724500, Colombia +571-629-2323, Commonwealth of Independent States +7-502-935-8411, Czech Republic +420-2-3300-9311, Denmark +45 4556 5000, Egypt +202-570-9442, Estonia +372-6-308-900, Finland +358-9-525-561, France +33-134-03-00-00, Germany +49-89-46008-0, Greece +30-1-618-8111, Hungary +36-1-489-8900, Iceland +354-563-3010, India-Bangalore +91-80-2298989/2295454; New Delhi +91-11-6106000; Mumbai +91-22-697-8111, Ireland +353-1-8055-666, Israel +972-9-9710500, Italy +39-02-641511, Japan +81-3-5717-5000, Kazakhstan +7-3272-466774, Korea +822-2193-5114, Latvia +371-750-3700, Lithuania +370-729-8468, Luxembourg +352-49 11 33 1, Malaysia +603-21161888, Mexico +52-5-258-6100, The Netherlands +00-31-33-45-15-000, New Zealand-Auckland +64-9-976-6800; Wellington +64-4-462-0780, Norway +47 23 36 96 00, People's Republic of China-Beijing +86-10-6803-5588; Chengdu +86-28-619-9333, Guangzhou +86-20-8755-5900; Shanghai +86-21-6466-1228; Hong Kong +852-2202-6688, Poland +48-22-8747800, Portugal +351-21-4134000, Russia +7-502-935-8411, Saudi Arabia +9661 273 4567, Singapore +65-6438-1888, Slovak Republic +421-2-4342-9485, South Africa +27 11 256-6300, Spain +34-91-767-6000, Sweden +46-8-631-10-00, Switzerland-German 41-1-908-90-00; French 41-22-999-0444, Taiwan +886-2-8732-9933, Thailand +662-344-6888, Turkey +90-212-335-22-00, United Arab Emirates +9714-3366333, United Kingdom +44 (0)1252 420000, United States +1-800-555-9SUN or +1-650-960-1300, Venezuela +58-2-905-3800, or online at [sun.com/store](http://sun.com/store)

**SUN** © 2004 Sun Microsystems, Inc. All rights reserved. Sun, Sun Microsystems, the Sun logo, Java, the Java Coffee Cup logo, Java Community Process, JCP, J2ME, J2SE, N1, Solaris, and The Network Is The Computer are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc. UNIX is a registered trademark in the United States and other countries, exclusively licensed through X/Open Company, Ltd. Information subject to change without notice. 06/04 R1.0