SecureMSM™ SECURITY SUITE

SecureMSM™ Security Suite

Overview

Wireless mobile devices have evolved into mobile computing platforms, complete with all the benefits available to computing platforms on the fixed-line Internet. Communication activities such as rich media distribution make security a critical feature for the revenue-generating applications and content consumers expect from 3G wireless devices.

To deliver trusted services, QUALCOMM has taken a leading role in the development of security solutions for chipsets. The SecureMSM™ security suite is a key component of QUALCOMM's Launchpad™ suite, providing operators, manufacturers and wireless users confidence in the integrity and security of the wireless network and the wireless device. New, attractive services are enabled by maintaining the confidentiality and integrity of value-added services, in addition to providing protection for the distribution of premium digital media.

The introduction of a rich digital rights management (DRM) platform into QUALCOMM's chipsets enables new and compelling business models. QUALCOMM's SecureMSM governs access to sensitive personal data for m-commerce services such as online payment, digital content and position location data. In addition, SecureMSM enables the delivery of secured services including strong identification and authentication capabilities to deliver protected wireless networks for enterprises with mobile workers. Operators will see increased average revenue per user (ARPU) as a result of the value-added, secure services that are readily deployable with the SecureMSM security suite.

QUALCOMM offers the building blocks that enable secure transactions between the wireless devices and the network. Available to both browsers and wireless applications written with QUALCOMM's BREW® system or Java® applications, SecureMSM software conforms to open, public standards and is also compatible with Web and WAP servers worldwide. SecureMSM software is integrated into select QUALCOMM Mobile Station Modem™ (MSM™) chipset solutions.

SecureMSM™ SECURITY SUITE

SecureMSM Security Suite Benefits

- Provides increased ARPU through provision of value-added premium content delivery services
- Introduces premium content forwarding such as superdistribution and peer-to-peer distribution by consistently governing rights assigned to content
- Enables saving of premium protected content to removable storage as well as backup to PC by leveraging the Open Mobile Alliance™ (OMA™) DRM version 1.0 specification
- Provides fast encryption and decryption with minimal performance or battery drain penalties through acceleration of critical protocols, public key algorithms, ciphers and message digests in the digital signal processor (DSP) and hardware
- Delivers trusted services to support multiple DRM mechanisms and vendors through a general content management framework
- Opens new service opportunities such as gifting or sending custom greetings with premium content mixed with user-generated voice, text or images
- Offers third-party application developers the means to easily integrate support for premium content through the BREW API
- Uses a common platform — applications that currently use DRM and trust agent will work on future MSM platforms

SecureMSM Security Suite Features

- Content protection removable media (CPRM)
- DRM agent supports open DRM implementations, including the three methods of OMA DRM version 1.0
  - Forward lock
  - Combined delivery
  - Separate delivery
- Supports OMA DRM v2.0
  - Rights Object Acquisition Protocol (ROAP)
  - OMA domain support
  - Unconnected device support
  - Export to CPRM capability
  - DRM Content Format v2.0 (DCF and Packetized-DCF)
- Secure execution of applications
- Fine granularity of permissions on executable content and API access control

- Secure boot ensures integrity of mobile device software
- Secure file system ensures integrity and confidentiality of sensitive data

Supported algorithms, ciphers, digests

- Protocols
  - SSL, TLS, IPSec, WTLS
- Public key algorithms
  - RSA, Diffie-Helman (Anonymous, Ephemeral)
- Ciphers
  - DES, 3DES, RC4, AES-128, C2
- Message digests
  - MD5, SHA-1, SHA-256

Launchpad Suite of Technologies

The Launchpad suite of applications technologies offers wireless operators and manufacturers a cost-effective, scalable and timely solution for providing advanced wireless data services. This seamlessly integrated solution enables advanced next-generation applications and services that incorporate multimedia, position location, connectivity, customized user interface and storage capabilities. Launchpad features are available for each QUALCOMM chipset, closely matching the specific functionality and cost-target objectives agreed upon in joint product planning with manufacturers and wireless service operators worldwide.

QUALCOMM's Complete Solution — Our Commitment to Our Partners

QUALCOMM CDMA Technologies is enabling the future of communications. We work closely with our manufacturer and operator partners to develop solutions that meet market needs today and provide the technology foundation for the wireless communications of tomorrow. Our world-class CDMA engineers create detailed reference designs to accelerate testing and deployment for our partners. And our chipsets and system software are fully integrated and able to bring advanced features and functionality to today's wireless devices. With QUALCOMM CDMA Technologies, manufacturers and operators can offer sophisticated wireless solutions that succeed in the global marketplace.