

SmartMIPS™ アーキテクチャー

スマート・カード・エクステンションズ



確実に多用途な スマートカードのための 次世代アーキテクチャ

今日のスマートカードは複数のアプリケーションをサポートし、妥協を許されないレベルのセキュリティを提供しなければなりません。世界トップのスマートカード・ベンダー、Gemplus SAと共同開発したMIPS32.アーキテクチャのSmartMIPSエクステンションは、完全なソリューションを提供し、比類なきセキュリティと暗号化性能を実現します。

SmartMIPSアーキテクチャは、暗号エンハンスメント、保証されたメモリ・スペース、コード圧縮およびバーチャル・マシン・パフォーマンス・エンハンスメントを結合させ、安価で低消費電力の完全なスマートカード・プロセッサ・ソリューションを可能にしました。

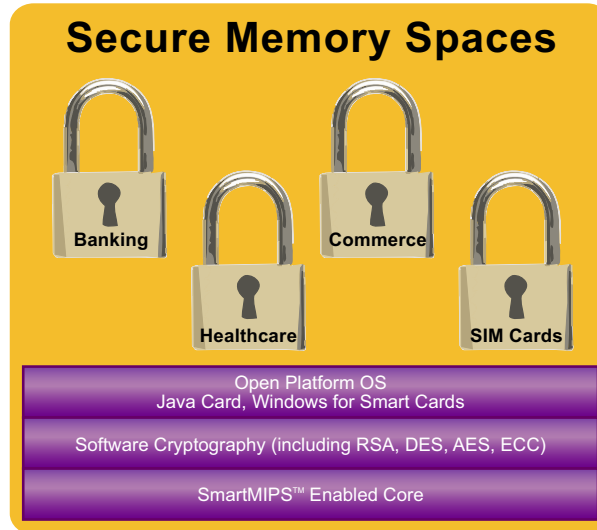
安全確実なスマートカードパフォーマンス

SmartMIPSアーキテクチャは、ソフトウェア暗号化と高度なセキュリティ特長というパワフルな組合せによって情報の保護とアプリケーションの柔軟性を改善し、多用途スマートカードの業界標準アーキテクチャとなっています。

- SmartMIPSアーキテクチャの暗号エンハンスメントは、公開/秘密鍵データのセキュリティ・アルゴリズムを高速化するため、専用のコプロセッサが不要になり、ダイサイズと全体的システムコストを削減します。
- ソフトウェア暗号化によって暗号化アルゴリズムのフィールド・アップデートが容易になります。このため、セキュリティ・アルゴリズムに、仮に違反があっても、実際のカードを回収する必要がありません。
- 高速化されたソフトウェア暗号化は、アプリケーション毎にアルゴリズム(例、RSA、DES、AES、楕円曲線暗号化(ECC)等)を選択することを可能にします。
- 保証されたメモリ・リソースは、アプリケーションによって繊細な消費者データを保護し、不正アプリケーションによる無断データ・アクセスを防止します。
- コード圧縮技術によってメモリ使用が最小化され、メモリ・リソースの不足を防止します。
- サンマイクロシステムズのJava Card.技術やマイクロソフトのWindows for Smart Cards等の主要OSをサポートし、高速化するように設計されています。

SmartMIPS™ アーキテクチャ・スマートカードエクステンション

SmartMIPSアーキテクチャ：
低消費電力で多機能な
スマートカードプロセッサのための
ハイパフォーマンスな暗号化
およびセキュリティー



保証されたメモリ・スペースは、アプリケーションを要約化し、繊細な顧客情報を保護、かつてないレベルのセキュリティーをスマートカードにもたらしめます。

SmartMIPSアーキテクチャの特長

- 高速化されたソフトウェア暗号化
- Java Card
- Windows for Smart Cards
- コード圧縮
- 保証されたメモリ・スペース

MIPSアーキテクチャの利点

業界標準の32ビットMIPSアーキテクチャは、低リスクの最先端技術を提供します。200以上のソフトウェアおよびIPソリューションにサポートされたアーキテクチャは、商品化時間を短縮しながら技術革新を可能にします。隆盛を誇るMIPSコミュニティーが、製品開発のために、豊富なエコシステムを提供します。

MIPSテクノロジーのソフトウェア暗号化戦略

専用のハードウェアとしてコプロセッサを使用する今日のセキュリティー技術は、次世代の多機能スマートカードには不十分です。より長い鍵とAESや楕円曲線暗号等の、より新しく、より安全なアルゴリズムに対する要求は、固定機能のハードウェア・ブロックで可能な以上に、フレキシブルな暗号ソリューションを必要とします。

SmartMIPSアーキテクチャの高性能なソフトウェア準拠暗号化エンハンスメントでは、幅広いアルゴリズムから選択できるようになっており、アルゴリズムを変更する際には、配布されたスマートカードを交換せず、再使用することが可能です。SmartMIPSアーキテクチャは、RSA、DES、AESおよび楕円曲線暗号を含む非常に様々なアルゴリズムをサポートする設計となっています。SmartMIPSアーキテクチャは、次世代の多機能スマートカードが要求するフレキシビリティを提供します。

翻訳言語アクセラレーションをサポート

多機能スマートカードには翻訳言語をサポートするプラットフォームが必要です。この戦略は、移植可能で安全確実なフレームワークを多用途スマートカードに提供します。しかし、この要求を満たす翻訳言語は複数が競合しています。MIPSテクノロジーは、どれか一つの翻訳言語ではなく、翻訳全般を高速化する方法でSmartMIPSアーキテクチャを拡張することによって、ライセンシーに最大限のフレキシビリティを提供することを選びました。

保証されたメモリ・スペース

スマートカードは、その完全性を傷つけようとするあらゆる方法の攻撃を受けます。スマートカードのアーキテクチャは、システムのセキュリティー全体を高めなければならず、脆い点があってはなりません。またアーキテクチャは、安全確実なプログラミングとOSをサポートしていなければなりません。SmartMIPSアーキテクチャは、安全確実なプログラミングと検証可能な安全確実なOSをサポートするために必要な全てのメモリ管理メカニズムを提供するように特に設計されています。ユーザコードはシステムコードから分離されており、アプリケーションはそれ自体のメモリ領域でカプセル化することができ、実行/読出し/書き込み専用のページ保護属性を個別にプログラムすることが可能です。

MIPS
TECHNOLOGIES

MIPS Technologies, Inc.
1225 Charleston Road
Mountain View, CA 94043-1353
phone: (650) 567-5000
fax: (650) 567-5158

ミップス・テクノロジーズ
〒105-0001
東京都港区虎ノ門3-7-8
ランディック第2虎ノ門ビル3F
TEL: 03-5733-9541
FAX: 03-5733-9545

www.mips.jp

