

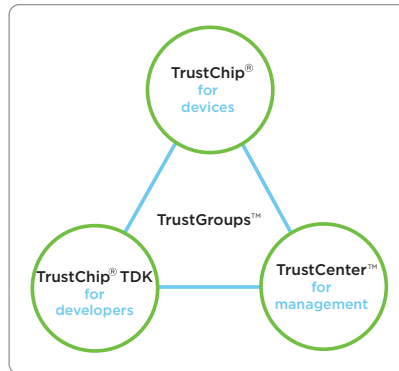
## A self-contained engine for end-to-end device and user security.

The KoolSpan TrustChip is a fully hardened, self-contained security engine that deploys in combination with a software library. Together, they provide high-performance protection wherein the TrustChip insulates key management from threats that can reside in open platform, mobile and legacy host devices. This self-contained structure ensures that any network-aware device, or any application running on the device, can become fully secured end to end, simply, easily and without limits of scale.



### The TrustChip Developer Kit

KoolSpan provides a TrustChip Developer Kit (TDK) that makes it easy for developers to secure their applications. With a few simple function calls, an enterprise application, voice application or control network application can be entirely protected across any network connection. The TDK enables an application developer to easily integrate security without the complexity or expertise typical of a strong security solution. To enable rapid



**The TrustChip Platform**

prototyping, the TDK contains all TrustChip functions entirely in software. Once the application is fully tested and debugged and ready for a final build, the TDK “hardware” switch is set and the cryptography is then anchored by the TrustChip itself.

### Security at the core

TrustChip, designed from the ground up, contains a hardened 32-bit processor with an embedded AES GCM encryption core. The NAND flash memory is fully encrypted, so even direct intrusive attempts cannot compromise user data.



### Key Features

- microSD form factor
- SD 2.0 compliant
- On-chip key management
- Simplified interface to any host processor
- Insulates key management from host environment
- Internal TrustGroup management
- 124 megabytes of user storage
- Highly resistant to invasive and non-invasive attacks
- Collapses complexity of security
- Hardware-based solution
- No infrastructure necessary for mutual authentication
- Sophisticated cryptography for low-powered devices
- Supports multiple applications simultaneously
- Portable to other OEM hardware packages
- Reference design available
- Architecture provides no limits of scale
- Smart use of trusted tokens
- Multi-factor authentication

Functionality	TrustChip-enabled Capabilities
Key Management	<ul style="list-style-type: none"> <li>• Uses TrustGroups for peer-to-peer authentication</li> <li>• Hardware anchor ensures system integrity</li> <li>• Double-bind key management environment</li> </ul>
Authentication	<ul style="list-style-type: none"> <li>• Peer-to-peer authentication using TrustGroups</li> <li>• Multiple TrustGroups can easily be established</li> <li>• Unlimited membership to TrustGroups provides unlimited scale</li> </ul>
Encryption	<ul style="list-style-type: none"> <li>• Embedded AES GCM 256-bit core</li> <li>• PRNG</li> <li>• Supports multiple independent secure contexts</li> </ul>
Memory	<ul style="list-style-type: none"> <li>• 124 megabytes of user storage</li> <li>• Key store fully protected and secured at all times</li> <li>• Holds dozens of TrustGroups</li> </ul>

**Build natural security associations with TrustGroups**

TrustGroups are used in the TrustChip for peer-to-peer authentication. Organizations can create one or more TrustGroups, which are then securely distributed to specific TrustChips. TrustGroups can have unlimited membership and therefore have no issues of scale. A TrustGroup is designed specifically for peer-to-peer authentication without network infrastructure where latency can be introduced.

When two users or devices connect, TrustGroup IDs are exchanged and both peers automatically determine which common TrustGroup to use to establish security. Authentication is fast and secure. From the authentication process, encryption keys are automatically and independently

calculated on both sides of the connection. With KoolSpan, there is never a key exchange.

**Micro form factor implementation**

TrustChip is implemented in an industry standard SD 2.0 interface. Recognized by common electronic devices such as smartphones and digital cameras, the SD 2.0 interface eliminates the need to develop complex drivers and modifications to the device firmware and operating system. The TrustChip microSD can be plugged into a miniSD slot, standard-sized SD slot or USB port by using a simple adapter. In all cases, the TrustChip is viewed as memory to the host device and as a security engine to applications enabled to use it via the TDK.

**Security Processor Features**

- Hardened protection
- On-chip key management
- Tamper resistant
- On-chip AES core
- Tamper evident
- 32-bit processor
- Standard microSD interface to host devices
- Complete development environment available

**Features**

- Edge-of-network operation
  - No external authentication server
  - No real-time support necessary
  - Seamless peer-to-peer authentication
- Multi-factor authentication
- No limits of scale
- User management features include:
  - Permanent electronic serial number uniquely identifies device
  - Securely add/remove TrustGroups from TrustChip's
- Native to wired and wireless network
- Automatic AES session key generation
  - Keyless exchange

**Benefits**

- Single solution for authentication and encryption services
- Hardened endpoint key management
- The TrustChip integrates:
  - 32-bit processor
  - Real-time authentication database
  - SD 2.0 secure digital interface
- Fully scalable architecture
- Power: 3.3v I/O, 1.2v core

**For More Information**

Please call 240.880.4400, or go to [www.koolspan.com](http://www.koolspan.com)