

## Leistungsstarke und sichere Identifikation auf 13,56 MHz



- ✓ **Schlüsselmaterial serienmässig vorkonfiguriert**
- ✓ **Kommunizieren über ISO 14443 A und ISO 15693**
- ✓ **Verwenden moderne Verschlüsselungsalgorithmen**
- ✓ **LEGIC advant und MIFARE DESFire EV2 vereint in einem Chip**

## Smartcard-IC mit erstklassiger Sicherheit

Die klassischen Smartcard-ICs für Identifikationsmedien wie Smartcards, Schlüssel oder Uhren. Sie werden in Projekten mit erhöhten Sicherheitsanforderungen verwendet. Dank der standardisierten Schlüsselverwaltung kommunizieren Leser- und Smartcard-ICs mühelos und trotzdem sicher.

### Leistungsstarke Smartcard-ICs

LEGICs advant Smartcard-ICs bieten leistungsstarke, zuverlässige und den Sicherheitsvorschriften entsprechende Qualität für kontaktlose RFID-Lösungen. Das von LEGIC perfekt abgestimmte Zusammenspiel zwischen Smartcard-IC und Leser-IC ermöglicht eine schnelle und nahtlose Integration in verschiedenste Anwendungen.

### Sicherheit & Verschlüsselung

Die Smartcard-ICs werden serienmässig mit vorkonfiguriertem, vertraulichem Schlüsselmaterial aus-

geliefert und können den Kundenbedürfnissen entsprechend individualisiert werden.

LEGIC advant verwendet moderne Verschlüsselungsalgorithmen und unterstützt mit dem MTSC (Master-Token System-Control) eine einzigartige Sicherheits- und Berechtigungslösung mit skalierbarer Sicherheit.

### Multiapplikation auf dem Medium Ihrer Wahl

LEGICs advant Smartcard-ICs sind das optimale Fundament für die Kombination von Anwendungen:

Von der Zutrittskontrolle und Zeiterfassung über bargeldloses Bezahlen bis hin zu Druckermanagement sowie eTicketing. Auch Anwendungen von Drittherstellern können auf dem Chip integriert werden. LEGIC advant erlaubt Ihnen die freie Wahl von Smartcards, Schlüsselanhängern oder Uhren als Identifikationsmedien.

### Ersatz für Hybridkarten

Dank der Verschmelzung von LEGIC advant und MIFARE DESFire auf einem Chip werden Hybridkarten der Vergangenheit angehören. Das Schlüsselmaterial ist schon installiert.

## ATC1024-MV110

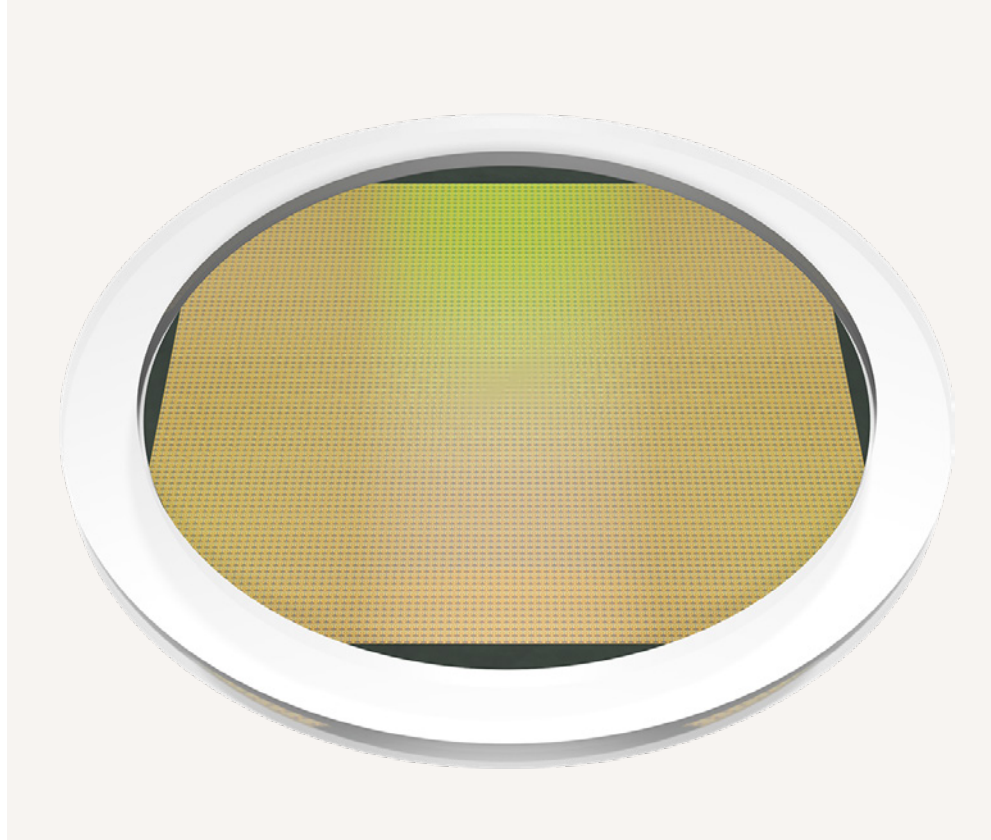
Die Lösung für grosse Lesedistanzen. Der Chip mit 1k Byte Speicher kommuniziert über ISO 15693 und ist der Smartcard-IC für einfache ID-Lösungen.

## ATC4096-MP311

Ideal für hohe Sicherheitsansprüche. Die Hardware ist nach Common Criteria EAL4+ zertifiziert, die Kommunikation erfolgt über ISO 14443 A. Bis zu 127 Anwendungen (4k Byte Speicher) auf einem Chip.

## ATC4096-MP312

Basierend auf dem NXP DESFire EV2 8K Chip, sind 3,3k Byte Speicher für zukünftige DESFire Applikationen reserviert. Der Chip ist kompatibel mit dem NXP AppXplorer und hat eine rund 20% grössere Lesedistanz als ein EV1 Chip.



## Technische Daten

	ATC1024-MV110	ATC4096-MP311	ATC4096-MP312
RF Standard	ISO 15693	ISO 14443 A	ISO 14443 A
Speichergrosse (Byte)	944	4096	4096 / DESFire EV2 (3328)
UID (Byte)***	8	7	7
Safe ID	Ja	Ja	Ja
Reichweite**	bis 70 cm	bis 9 cm	bis 11 cm
Schlüsselverwaltung (pro Applikation)	Master-Token System-Control	Master-Token System-Control	Master-Token System-Control / NXP AppXplorer / LEGIC Orbit
Datentransfer-Verschlüsselung	64 Bit Schlüssel	3DES	3DES / AES 128 ****
Datenspeicher-Verschlüsselung (pro Applikation)	3DES, DES, LEGIC Verschlüsselung	AES (128/256 Bit), 3DES, DES, LEGIC Verschlüsselung	AES (128/256 Bit), 3DES, DES, LEGIC Verschlüsselung
Max. mögliche Applikationen *	59	127	127 + (n x DESFire AID)
Speicher-Segmentierung	Dynamisch	Dynamisch	Dynamisch
Applikationssegment-Grösse	Variabel	Variabel	Variabel
Datenerhalt (mind.)	10 Jahre	10 Jahre	10 Jahre
EEPROM-Zyklen (mind.)	100 000	500 000	500 000
Baudraten (kbit/s)	bis 26.48	bis 424	bis 424
Lieferform	Wafer	MOA4 Modul, Wafer	MOA6 Modul, Wafer
Zertifizierte Hardware Plattform	-	CC EAL4+	CC EAL5+

\* Speicherangaben sind Nominalwerte. Die effektive max. Anzahl der Applikationen hängt vom Speicherbedarf der verwendeten Applikationen ab

\*\* Max. Leserreichweite ist abhängig von länderspezifischer Funkzulassung, Leser-Applikation, RF Standard, Antenne, Transponder und Umgebung

\*\*\* Abhängig von verwendeten Plattform

\*\*\*\* Wechselbares Schlüsselmaterial vorinstalliert (für einmalige, zukünftige Veränderung)