ATAES132A

32K AES Serial EEPROM Specification

SUMMARY DATASHEET

CryptoAuthentication

Ensures Things and Code are Real, Untampered, and Confidential

Secure Download and Boot
Authentication and Protect Code In-transit

Ecosystem Control
Ensure Only OEM/Licensed Nodes and Accessories Work

Anti-cloning
Prevent Building with Identical BOM or Stolen Code

Message Security
Authentication, Message Integrity, and Confidentiality of Network Nodes (IoT)

This is a summary document. The complete document is available on the Atmel website at www.atmel.com.

Features

- Crypto Element Device with Secure Hardware-based Key Storage
- 32Kb Standard Serial EEPROM Memory
  - Compatible with the Atmel® AT24C32D and the Atmel AT25320B
  - 16 User Zones of 2Kb Each
- High-security Features
  - AES Algorithm with 128-bit Keys
  - AES-CCM for Authentication
  - Message Authentication Code (MAC) Capability
  - Secure Storage for up to Sixteen 128-bit Keys
  - Encrypted User Memory Read and Write
  - Internal High-quality FIPS Random Number Generator (RNG)
  - 16 High-Endurance Monotonic EEPROM Counters
- Flexible User Configured Security
  - User Zone Access Rights Independently Configured
  - Authentication Prior to Zone Access
- Read/Write, Encrypted, or Read-only User Zone Options
- High-speed Serial Interface Options
  - 10MHz SPI (Mode 0 and 3)
  - 1MHz Standard I^2C Interface
- 2.5V to 5.5V Supply Voltage Range
- <250nA Sleep Current
- 8-pad UDFN and 8-lead SOIC Package Options
- Temperature Range: -40°C to +85°C

Benefits

- Easily Add Security by Replacing Existing Serial EEPROM
- Authenticate Consumables, Components, and Network Access
- Protect Sensitive Firmware
- Securely Store Sensitive Data and Enable Paid-for Features
- Prevent Contract Manufacturers from Overbuilding
- Manage Warranty Claims
- Securely Store Identity Data (i.e. Fingerprints and Pictures)

Description

The Atmel ATAES132A is a high-security, Serial Electrically-Erasable and Programmable Read-Only Memory (EEPROM) providing both authentication and confidential nonvolatile data storage capabilities. Access restrictions for the 16 user zones are independently configured, and any key can be used with any zone. In addition, keys can be used for standalone authentication. This flexibility permits the ATAES132A to be used in a wide range of applications.

The AES-128 cryptographic engine operates in AES-CCM mode to provide authentication, stored data encryption/decryption, and Message Authentication Codes. Data encryption/decryption can be performed for internally stored data or for small external data packets, depending upon the configuration. Data encrypted by one ATAES132A device can be decrypted by another, and vice versa.

The ATAES132A pinout is compatible with standard SPI and I^2C Serial EEPROMs to allow placement on existing PC boards. The SPI and I^2C instruction sets are identical to the Atmel Serial EEPROMs. The extended security functions are accessed by sending command packets to the ATAES132A using standard write instructions, and reading responses using standard read instructions. The ATAES132A secure Serial EEPROM architecture allows it to be inserted into existing applications.

The ATAES132A device incorporates multiple physical security mechanisms to prevent the release of the internally stored secrets. Secure personalization features are provided to facilitate third-party product manufacturing.

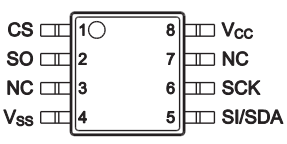
Pin Descriptions and Configurations

Table 1. Pin Descriptions

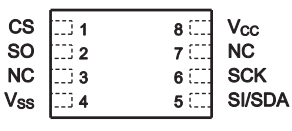
Name	Description
$\overline{CS}$	**SPI Chip Select Bar Input**
SO	**Serial Data Out**
NC	**No Connect**
V_{SS}	**Ground**
SI/SDA	**Serial Data In**
SCK	**Serial Clock Input**
NC	**No Connect**
V_{CC}	**Supply Voltage**

Table 2. Pin Configurations

8-lead SOIC
(Top View)



8-pad UDFN
(Top View)



Note: Drawings are not to scale.

1. Introduction

The ATAES132A is the first device in a family of high-security Serial EEPROMs using the Advanced Encryption Standard (AES) cryptographic algorithm. The ATAES132A provides 32Kb of EEPROM user data memory, sixteen 128-bit Key Registers, sixteen high-endurance monotonic EEPROM Counters, factory unique Die Identification Numbers, and a Configuration Memory. The Configuration Memory registers control access to the User Memory, as well as the restrictions on Key and Counter functionality.

The User Memory can be accessed directly with standard SPI or I^2C commands if a user zone is configured for open or read-only access. If the user zone security is activated, then the extended ATAES132A command set is used to access the contents of a user zone. The extended ATAES132A commands are executed by writing the command packet to the virtual memory using standard SPI or I^2C Write commands. The response packet is retrieved by reading it from the virtual memory using standard SPI or I^2C Read commands.

The ATAES132A packages are compatible with standard SPI and I^2C EEPROM footprints. This allows the ATAES132A to be inserted into many existing Serial EEPROM applications.

2. Security Features

All ATAES132A security features are optional. Each feature is enabled or disabled by programming configuration bits in the EEPROM Configuration Memory. Each user zone, Key, and Counter is separately and independently configured.

2.1 Architecture

ATAES132A contains all circuitry for performing authentication, encryption, and decryption using keys stored securely in the internal EEPROM. Since the secrets are stored securely in the ATAES132A, they do not have to be exchanged prior to executing cryptographic operations.

ATAES132A has fixed cryptographic functionality; it is not a microcontroller and cannot accept customer firmware. ATAES132A contains a hardware AES cryptographic engine and has a fixed command set. Although the functionality is fixed, it is also flexible because each feature is enabled or disabled by the customer by programming registers in the EEPROM Configuration Memory. After personalization is complete, fuses lock the configuration so it cannot be changed.

2.1.1 AES

The ATAES132A cryptographic functions are implemented with a hardware cryptographic engine using AES in CCM mode with a 128-bit key. AES-CCM mode provides both confidentiality and integrity checking with a single key. The integrity MAC includes both the encrypted data and additional authenticate-only data bytes, as described in each command definition. Each MAC is unique due to inclusion of a Nonce and an incrementing MacCount Register in the MAC calculation.

2.1.2 Hardware Security Features

The ATAES132A device contains physical security features to prevent an attacker from determining the internal secrets. ATAES132A includes tamper detectors for voltage, temperature, frequency, and light, as well as an active metal shield over the circuitry, internal memory encryption, and other various features. The ATAES132A physical design and cryptographic protocol are designed to prevent or significantly complicate most algorithmic, timing, and side-channel attacks.

2.2 Authentication

The authentication commands utilize AES-CCM to generate or validate a MAC value computed using an internally stored key. The command set supports both one-way and mutual authentication. One ATAES132A device can generate packets for authentication of a second ATAES132A device containing the same key. The internal authentication status register remembers only the most recent authentication attempt. A user zone can be configured to require prior authentication of a designated key before access to the user zone is permitted.

2.2.1 Key Authentication

Individual keys can be configured to require a successful authentication prior to use. This requirement can be used to prevent some kinds of exhaustive attacks on the keys. The authentication requirement can be chained to require authentication of several keys prior to allowing a particular operation. The internal Authentication Status Registers remember only the most recent authentication attempt.

3. Electrical Characteristics

3.1 Absolute Maximum Ratings*

Operating Temperature	-40°C to +85°C
Storage Temperature	-65°C to +150°C
Maximum Operating Voltage	6.0V
DC Output Current	5.0mA
Voltage on any pin	-0.7V to (V_{CC} + 0.7V)
HBM ESD	3kV minimum

Notice*: Stresses beyond those listed under “Absolute Maximum Ratings” may cause permanent damage to the device. This is a stress rating only, and the functional operation of the device at these or any other conditions beyond those indicated in the operational sections of this specification is not implied. Exposure to absolute maximum rating conditions for extended periods may affect device reliability.

3.2 Reliability

The ATAES132A is fabricated with the Atmel high reliability CMOS EEPROM manufacturing technology. The reliability ratings in Table 3-1 apply to each byte of the EEPROM memory.

Table 3-1. EEPROM Reliability(1)

Parameter	Min	Typical	Max	Units
Write Endurance (each byte)	100,000			Write Cycles
Data Retention (at 55°C)	10			Years
Data Retention (at 35°C)	30	50		Years
Read Endurance	Unlimited			Read Cycles

Note: 1. These specifications apply to every byte of the User Memory, Configuration Memory, and Key Memory. The Write Endurance specification also applies to the RNG EEPROM Seed Register.

3.3 DC Characteristics

3.3.1 Supply Characteristics

Table 3-2. Supply Voltage and Current Characteristics

Applicable over recommended operating range from T_A = -40°C to +85°C, V_{CC} = +2.5V to +5.5V (unless otherwise noted). (1)

Symbol	Parameter	Test Conditions	Min	Typ	Max	Units
V_{CC} (1)	Supply Voltage		2.50		5.50	V
I_{CC1}	Supply Current	V_{CC} = 3.3V at f_{max} (4) SO = Open(3), Read, Write, or AES operation.			6	mA
I_{CC2}	Supply Current	V_{CC} = 5.5V at f_{max} (4) SO = Open(3), Read, Write, or AES operation.			10	mA
I_{CC3}	Idle Current	V_{CC} = 3.3V or 5.5V at f_{max} (4) SO = Open(3), Waiting for a command.		600	800	µA
I_{SL1}	Sleep Current	V_{CC} = 3.3V; $\overline{CS}$ = V_{CC}(3), Sleep State		0.10	0.25	µA
I_{SL2}	Sleep Current	V_{CC} = 5.5V; $\overline{CS}$ = V_{CC}(3), Sleep State		0.25	0.50	µA
I_{SB1}	Standby Current	V_{CC} = 3.3V; $\overline{CS}$ = V_{CC}(3), Standby State		15	30	µA
I_{SB2}	Standby Current	V_{CC} = 5.5V; $\overline{CS}$ = V_{CC}(3), Standby State		20	40	µA

Notes:
1. Typical values are at 25˚C, and are for reference only. Typical values are not tested or guaranteed.
2. On power-up, V_{CC} must rise continuously from V_{SS} to the operating voltage, with a rise time no faster than 1V/µs.
3. All input pins must be held at either Vss or Vcc during this measurement. In SPI interface mode, the $\overline{CS}$ pin must be at V_{CC}. In I^2C interface mode, the $\overline{CS}$ pin may be in either state.
4. Measurement is performed at the maximum serial clock frequency. In the I^2C interface mode, f_{max} is 1MHz. In the SPI interface mode, f_{max} is 10MHz.
5. The ATAES132A does not support hot swapping or hot plugging. Connecting or disconnecting this device to a system while power is energized can cause permanent damage to the ATAES132A.

3.3.2 I/O Characteristics

Table 3-3. DC Characteristics

Applicable over recommended operating range from T_A = -40°C to +85°C, V_{CC} = +2.5V to +5.5V (unless otherwise noted).

Symbol	Parameter	Test conditions	Min	Max	Units
I_{LI}	Input Current	V_{IN} = 0V or V_{CC}	-3.0	3.0	µA
I_{LO}	Output Leakage	V_{OUT} = 0V or V_{CC}	-3.0	3.0	µA
V_{IL}(1)	Input Low-Voltage		-0.5	V_{CC} x 0.3	V
V_{IH} (1)	Input High-Voltage		V_{CC} x 0.7	V_{CC} + 0.5	V
V_{OL1}(2)	Output Low-Voltage, Except SI/SDA in I^2C Mode	I_{OL} = 3.0mA	0	0.4	V
V_{OH1}(2)	Output High-voltage, Except SI/SDA in I^2C Mode	I_{OH} = -3.0mA	V_{CC} − 0.8	V_{CC}	V
V_{OL2}	Output Low-voltage, SI/SDA Pin in the I^2C Mode *Only*	I_{OL} = 3.0mA	0	0.4	V

Notes:
1. V_{IL} min and V_{IH} max are for reference only, and are not tested.
2. In the I^2C interface mode, if Auth signaling is enabled, the SO pin functions as the AuthO output. When AuthO is high, the V_{OH1} specification applies. When AuthO is not high, the pin is in the high-impedance state; the V_{OL1} specification is not applicable.

3.4 AC Characteristics

Table 3-4. AC Characteristics

Applicable over recommended operating range from T_A = -40°C to + 85°C, V_{CC} = +2.5V to +5.5V.

Symbol	Parameter	Min	Max	Units
t_{WC1}	User Zone Write Cycle Time(1)	6.0	9.0	ms
t_{WC2}	Key Zone Write Cycle Time(1)	12.0	16.0	ms
	Command Response Time			

Note: 1. The write cycle time includes the EEPROM Erase, Write, and Automatic Data Write verification operations.

3.4.1 Power-Up, Sleep, Standby, and Wake-Up Timing

Table 3-5. Power-Up, Sleep, and Wake-Up Timing Characteristics(1)

Applicable over recommended operating range from T_A = -40°C to + 85°C, V_{CC} = +2.5V to +5.5V.

Symbol	Parameter	Min	Typ	Max	Units
$t_{PU.STATUS}$	Power-Up Time, Status		500	600	µs
$t_{PU.RDY}$	Power-Up Ready Time		1200	1500	µs
t_{SB}	Sleep Time, Entering the Standby State		65	100	µs
t_{SL}	Sleep Time, Entering the Sleep State		55	90	µs
$t_{WupSB.STATUS}$	Wake-Up Status Time, Standby State		50	100	µs
$t_{WupSB.RDY}$	Wake-Up Ready Time, Standby State		200	240	µs
$t_{WupSL.STATUS}$	Wake-Up Status, Sleep State		500	600	µs
$t_{WupSL.RDY}$	Wake-Up Ready Time, Sleep State		1200	1500	µs

Note: 1. All values are based on characterization and are not tested. Typical values are at 25˚C and are for reference only.

3.4.2 I²C Interface Timing

Table 3-6. AC Characteristics of I²C Interface

Applicable over recommended operating range from T_A = -40°C to + 85°C, V_{CC} = +2.5V to +5.5V, CL = 1 TTL Gate and 100pF (unless otherwise noted).

Symbol	Parameter	Min	Max	Units
f_{SCK}	SCK Clock Frequency		1	MHz
	SCK Clock Duty Cycle	30	70	percent
t_{HIGH}	SCK High Time	400		ns
t_{LOW}	SCK Low Time	400		ns
$t_{SU.STA}$	Start Setup Time	250		ns
$t_{HD.STA}$	Start Hold Time	250		ns
$t_{SU.STO}$	Stop Setup Time	250		ns
$t_{SU.DAT}$	Data in Setup Time	100		ns
$t_{HD.DAT}$	Data in Hold Time	0		ns
t_R	Input Rise Time(1)		300	ns
t_F	Input Fall Time(1)		100	ns
t_{AA}	Clock Low to Data Out Valid	50	550	ns
t_{DH}	Data Out Hold Time	50		ns
t_{BUF}	Time bus must be free before a new transmission can start.(1)	500		ns

Notes: 1. Values are based on characterization, and are not tested.

2. AC measurement conditions:
   - RL (connects between SDA and V_{CC}): 2.0kΩ (for V_{CC} +2.5V to +5.0V)
   - Input pulse voltages: 0.3V_{CC} to 0.7V_{CC}
   - Input rise and fall times: ≤ 50ns
   - Input and output timing reference voltage: 0.5V_{CC}

3.4.3 SPI Interface Timing

Table 3-7. AC Characteristics of SPI Interface

Applicable over recommended operating range from T_A = -40°C to + 85°C, V_{CC} = +2.5V to +5.5V, CL = 1 TTL Gate and 30pF (unless otherwise noted).

Symbol	Parameter	Min	Max	Units
f_{SCK}	SCK Clock Frequency	0	10	MHz
	SCK Clock Duty Cycle	30	70	percent
t_{WH}	SCK High Time	40		ns
t_{WL}	SCK Low Time	40		ns
t_{CS}	$\overline{CS}$ High Time	50		ns
t_{CSS}	$\overline{CS}$ Setup Time	50		ns
t_{CSH}	$\overline{CS}$ Hold Time	50		ns
t_{SU}	Data In Setup Time	10		ns
t_H	Data In Hold Time	10		ns
t_{RI}	Input Rise Time(1)		2	µs
t_{FI}	Input Fall Time(1)		2	µs
t_V	Output Valid	0	40	ns
t_{HO}	Output Hold Time	0		ns
t_{DIS}	Output Disable Time		50	ns

Note: 1. Values are based on characterization, and are not tested.

4. Ordering Information

To increase security, ATAES132A packages are not marked with the ordering code. The ATAES132A standard packages are marked with a trace code which is unique for each manufacturing lot. Contact Atmel for additional information.

A.1 Ordering Codes

Atmel Ordering Code	Interface Configuration	Conditioning	Package	Lead Finish	Temperature Range
ATAES132A-SHEQ	SPI	Bulk[1]	8S1	NiPdAu Lead-free/Halogen-free (Exceeds RoHS Requirments)	Industrial Temperature (-40°C to 85°C)
ATAES132A-SHER	I^2C				
ATAES132A-SHEQ-T	SPI	Tape and Reel[2]			
ATAES132A-SHER-T	I^2C				
ATAES132A-MAHEQ-T	SPI		8MA2		
ATAES132A-MAHER-T	I^2C				

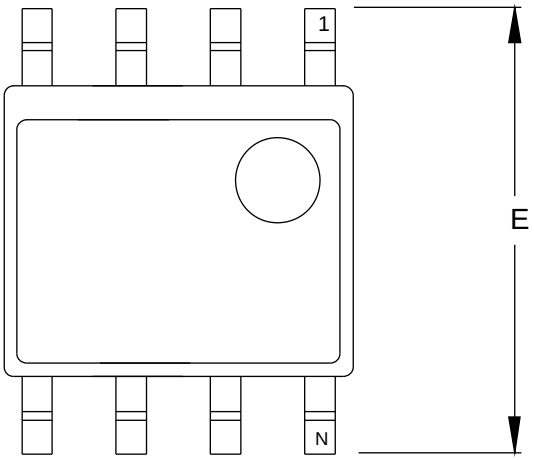
Notes: 1. Blank = Bulk
- SOIC = 100 per tube.

2. -T = Tape and Reel
- SOIC = 4,000 per reel.
- UDFN = 15,000 per reel.

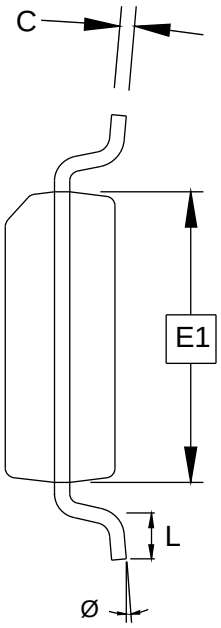
Package Type	
8S1	8-lead, 0.150” wide body, Plastic Gull Wing Small Outline, Green (JEDEC SOIC)
8MA2	8-pad, 2.0mm x 3.0mm x 0.6mm body, Thermally Enhanced Plastic Ultra Thin Dual Flat No Lead, Green (UDFN)

A.2 Mechanical Information

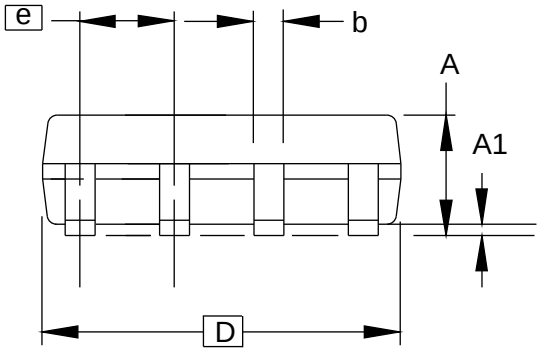
A.2.1 8S1 — 8-lead JEDEC SOIC



TOP VIEW



END VIEW



SIDE VIEW

Notes: This drawing is for general information only.
Refer to JEDEC Drawing MS-012, Variation AA
for proper dimensions, tolerances, datums, etc.

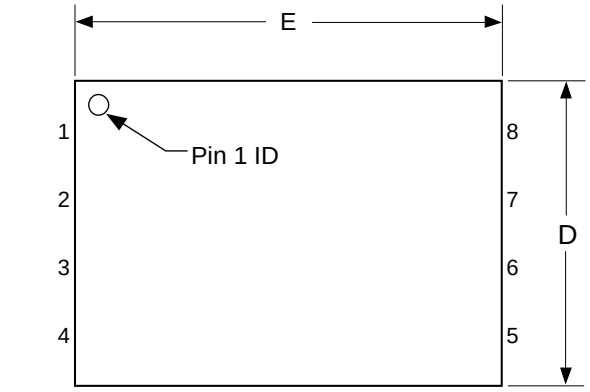
COMMON DIMENSIONS
(Unit of Measure = mm)

SYMBOL	MIN	NOM	MAX	NOTE
A	–	–	1.75	
A1	0.10	–	0.25	
b	0.31	–	0.51	
C	0.17	–	0.25	
D	4.90 BSC			
E	6.00 BSC			
E1	3.90 BSC			
e	1.27 BSC			
L	0.40	–	1.27	
Ø	0°	–	8°	

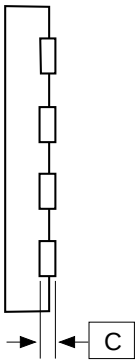
3/6/2015

Atmel Package Drawing Contact: packagedrawings@atmel.com	**TITLE** 8S1, 8-lead (0.150” Wide Body), Plastic Gull Wing Small Outline (JEDEC SOIC)	**GPC** SWB	**DRAWING NO.** 8S1	**REV.** H

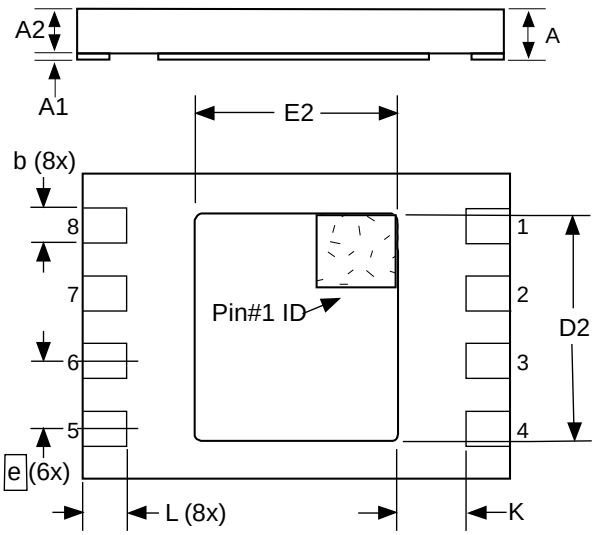
A.2.2 8MA2 — 8-pad UDFN



TOP VIEW



SIDE VIEW



BOTTOM VIEW

Notes:
1. This drawing is for general information only. Refer to Drawing MO-229, for proper dimensions, tolerances, datums, etc.
2. The Pin #1 ID is a laser-marked feature on Top View.
3. Dimensions b applies to metallized terminal and is measured between 0.15 mm and 0.30 mm from the terminal tip. If the terminal has the optional radius on the other end of the terminal, the dimension should not be measured in that radius area.
4. The Pin #1 ID on the Bottom View is an orientation feature on the thermal pad.

COMMON DIMENSIONS
(Unit of Measure = mm)

SYMBOL	MIN	NOM	MAX	NOTE
A	0.50	0.55	0.60	
A1	0.0	0.02	0.05	
A2	-	-	0.55	
D	1.90	2.00	2.10	
D2	1.40	1.50	1.60	
E	2.90	3.00	3.10	
E2	1.20	1.30	1.40	
b	0.18	0.25	0.30	3
C	1.52 REF			
L	0.30	0.35	0.40	
e	0.50 BSC			
K	0.20	-	-	

11/26/14

Atmel Package Drawing Contact: packagedrawings@atmel.com	**TITLE** 8MA2, 8-pad 2 x 3 x 0.6mm Body, Thermally Enhanced Plastic Ultra Thin Dual Flat No-Lead Package (UDFN)	**GPC** YNZ	**DRAWING NO.** 8MA2	**REV.** G

5. Revision History

Doc. Rev.	Date	Comments
8914AS	03/2015	Initial summary document release.

Atmel | Enabling Unlimited Possibilities®

Atmel Corporation 1600 Technology Drive, San Jose, CA 95110 USA **T:** (+1)(408) 441.0311 **F:** (+1)(408) 436.4200 | www.atmel.com

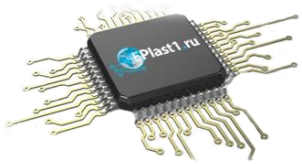
Компания «ЭлектроПласт» предлагает заключение долгосрочных отношений при поставках импортных электронных компонентов на взаимовыгодных условиях!

Наши преимущества:

- Оперативные поставки широкого спектра электронных компонентов отечественного и импортного производства напрямую от производителей и с крупнейших мировых складов;
- Поставка более 17-ти миллионов наименований электронных компонентов;
- Поставка сложных, дефицитных, либо снятых с производства позиций;
- Оперативные сроки поставки под заказ (от 5 рабочих дней);
- Экспресс доставка в любую точку России;
- Техническая поддержка проекта, помощь в подборе аналогов, поставка прототипов;
- Система менеджмента качества сертифицирована по Международному стандарту ISO 9001;
- Лицензия ФСБ на осуществление работ с использованием сведений, составляющих государственную тайну;
- Поставка специализированных компонентов (Xilinx, Altera, Analog Devices, Intersil, Interpoint, Microsemi, Aeroflex, Peregrine, Syfer, Eurofarad, Texas Instrument, Miteq, Cobham, E2V, MA-COM, Hittite, Mini-Circuits,General Dynamics и др.);

Помимо этого, одним из направлений компании «ЭлектроПласт» является направление «Источники питания». Мы предлагаем Вам помощь Конструкторского отдела:

- Подбор оптимального решения, техническое обоснование при выборе компонента;
- Подбор аналогов;
- Консультации по применению компонента;
- Поставка образцов и прототипов;
- Техническая поддержка проекта;
- Защита от снятия компонента с производства.



Как с нами связаться

Телефон: 8 (812) 309 58 32 (многоканальный)
Факс: 8 (812) 320-02-42
Электронная почта: org@eplast1.ru
Адрес: 198099, г. Санкт-Петербург, ул. Калинина, дом 2, корпус 4, литера А.