

SafeXcel™ IP Public Key Accelerators

## Silicon-proven Intellectual Property (IP)

### BENEFITS

- Silicon-proven
- ROM-based sequencer facilitates functional upgrades
- Fast and easy to integrate
- Simple user (Software I/O) interface
- World-class support

Semiconductor designers require ready-to-use hardware designs that are silicon-proven and reliable, yet flexible to accommodate a wide variety of design goals. As part of AuthenTec's extensive IP product portfolio, AuthenTec provides the SafeXcel™ IP Public Key Accelerators to meet these requirements. Designed for full scalability and an optimal performance over gate count ratio, they address the unique needs of semiconductor OEMs and provide a reliable and cost-effective IP solution that is easy to integrate into SoC designs. The SafeXcel IP Public Key Accelerators can be deployed in semiconductors that are used for Internet Protocol Security (IPsec), Secure Sockets Layer (SSL), and Transport Layer Security (TLS) protocol implementations, such as handheld devices, gateways, and certificate authority servers, and in smart cards. In general, they are used to dramatically increase the performance of computationally intensive public key algorithms such as RSA, DSA, ECC and Diffie-Hellman, and to increase the security of these implementations.

### Ease of Integration

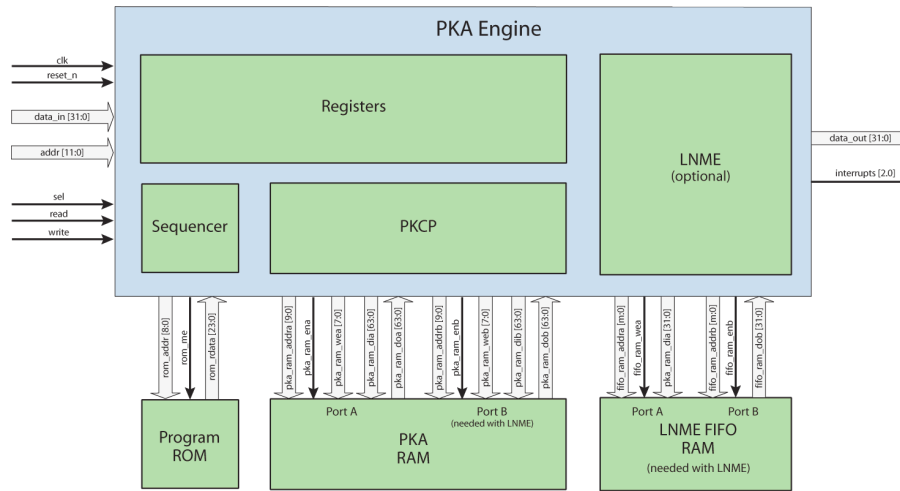
Years of experience in designing silicon security products made AuthenTec the leading vendor of complete, reliable, and high-quality IP products, featuring cost-efficient designs and user-friendly product interfaces. AuthenTec's global presence and expertise in security IP design enables us to provide our customers with 24/7 worldclass support that is unmatched in the industry—thereby supporting your design-in and ensuring the success of your project.

### Public Key Accelerators

The SafeXcel IP Public Key Accelerators contain a multiplier-based Public Key Crypto Processor (PKCP) and, in most configurations, a Large Number Multiplier and Exponentiator (LNME). The PKCP can implement add, subtract, multiply, divide, compare, copy, shift right, and shift left operations. The LNME performs Montgomery-based multiplications and exponentiations. A ROM-driven sequencer controls the PKCP and the LNME to perform complex operations such as large number modular exponentiations. The LNME consists of a selectable number of Processing Elements (PEs), operating simultaneously in a pipelined manner. The architecture and implementation of the LNME make the engine resistant against attacks that try to exploit power and timing characteristics of exponentiation operations.

### Configuration Flexibility

The SafeXcel IP Public Key Accelerator is available in numerous configurations. The Public Key Accelerator is available in a low gate count PKCP-only configuration, and in many configurations with the additional LNME. The number of PEs in the LNME can be selected between 4 and 54, allowing customers to make the best possible tradeoff between power consumption, gate count, and performance. The table shows the PKCP-only configuration, as well as three examples of configurations that include the additional LNME. Please contact AuthenTec for more information on the remaining configurations (with different number of PEs).



### SafeXcel IP Public-Key Accelerator Architecture

NAME	EIP-28B	EIP-28-PE4	EIP-28-PE17	EIP-28-PE33
CONFIGURATION	32 bit PKCP only	16 bit PKCP + LNME (4 PEs)	16 bit PKCP + LNME (17 PEs)	16 bit PKCP + LNME (33 PEs)
MAX CLOCK FREQUENCY <sup>1</sup>	240 MHz	250 MHz	230 MHz	230 MHz
APPROXIMATE GATE COUNT AT SYNTHESIS FREQUENCY EQUAL TO 75% OF THE MAX. CLOCK FREQUENCY	32 kGates	60 kGates	146 kGates	254 kGates
RSA-1024 PERFORMANCE <sup>2</sup>	NUMBER OF CYCLES <sup>3</sup>	3,919,118	1,559,831	395,130
	AT MAX CLOCK FREQUENCY	16.4 msec	6.3 msec	1.72 msec
ECC-ADD-384 PERFORMANCE <sup>4</sup>	NUMBER OF CYCLES	102,271	145,655	145,655
	AT MAX CLOCK FREQUENCY	0.43 msec	0.59 msec	0.64 msec
ECC-MUL-384 PERFORMANCE <sup>5</sup>	NUMBER OF CYCLES	5,997,832	2,300,939	1,452,289
	AT MAX CLOCK FREQUENCY	24.9 msec	9.21 msec	6.32 msec

1 Technology and synthesis dependent; based on the use of a basic design compiler and a high-speed 0.13µm technology.  
 2 1024-bit random exponent and modulus vectors; 50% of the exponent bits are '1'; no use of CRT.  
 3 Using 4 pre-calculated odd powers. Time includes pre-calculation and is slightly data-dependent (a few percent margin around the given values is to be expected—mostly due to actual exponent vector value). A higher number of odd powers increase performance but requires more PKA RAM working space.  
 4 Addition of points on a prime field elliptic curve. Added points differ – if they were the same a point doubling would be performed automatically. Prime modulus has 384 significant bits.  
 5 Multiplication of a point on a prime field elliptic curve by a scalar value. Prime modulus and scalar value both have 384 significant bits.

### SPECIFICATIONS

#### Features

- Support of RSA, RSA-CRT, DSA, DH and ECC
- Highly scalable architecture with selectable number of Processing Elements
- Standard modulus size: 2048 bits (wider vectors are optional)
- Resistant against power and timing analysis attacks
- Fully synchronous design

#### Deliverables

- Synthesizable Verilog RTL source code
- Self-checking RTL test bench, including test vectors and expected result vectors
- Simulation script
- Synthesis script
- User's Manual with technical specifications, including the programmer's interface
- Developer's Manual with step-by-step descriptions that allows developers to easily install, verify, and synthesize the design

#### HEADQUARTERS

AuthenTec, Inc.  
 100 Rialto Place, Suite 100  
 Melbourne, FL 32901 USA  
 +1-321-308-1300

For more information  
 about Embedded Security  
 Solutions:  
[embedded@authentec.com](mailto:embedded@authentec.com)

WORLDWIDE  
 REPRESENTATIVES NETWORK  
 A complete listing of  
 AuthenTec's network of  
 representatives is  
 available at our web site.

[www.authentec.com](http://www.authentec.com)