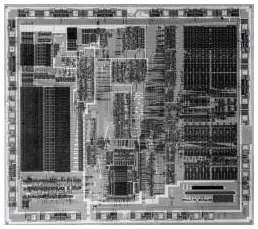
Design Center KM211

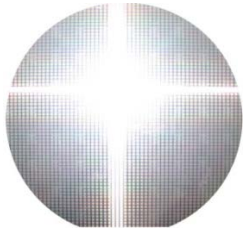
...from Idea – to Implementation!!!

IC Design Services & IP Development

Company

- Size: Highly professional team of 40+ engineers, with solid mass production experience
- Location: SEZ Zelenograd (Russian“Silicon valley”), Moscow Institute of Electronic Technology
- Background: former Design House of Angstrem fab
- Average Experience: 15+ years
- Key expertise:
  - ✓ Turnkey IC design
  - ✓ Proprietary microprocessors solutions & other IPs
  - ✓ SDK & Firmware



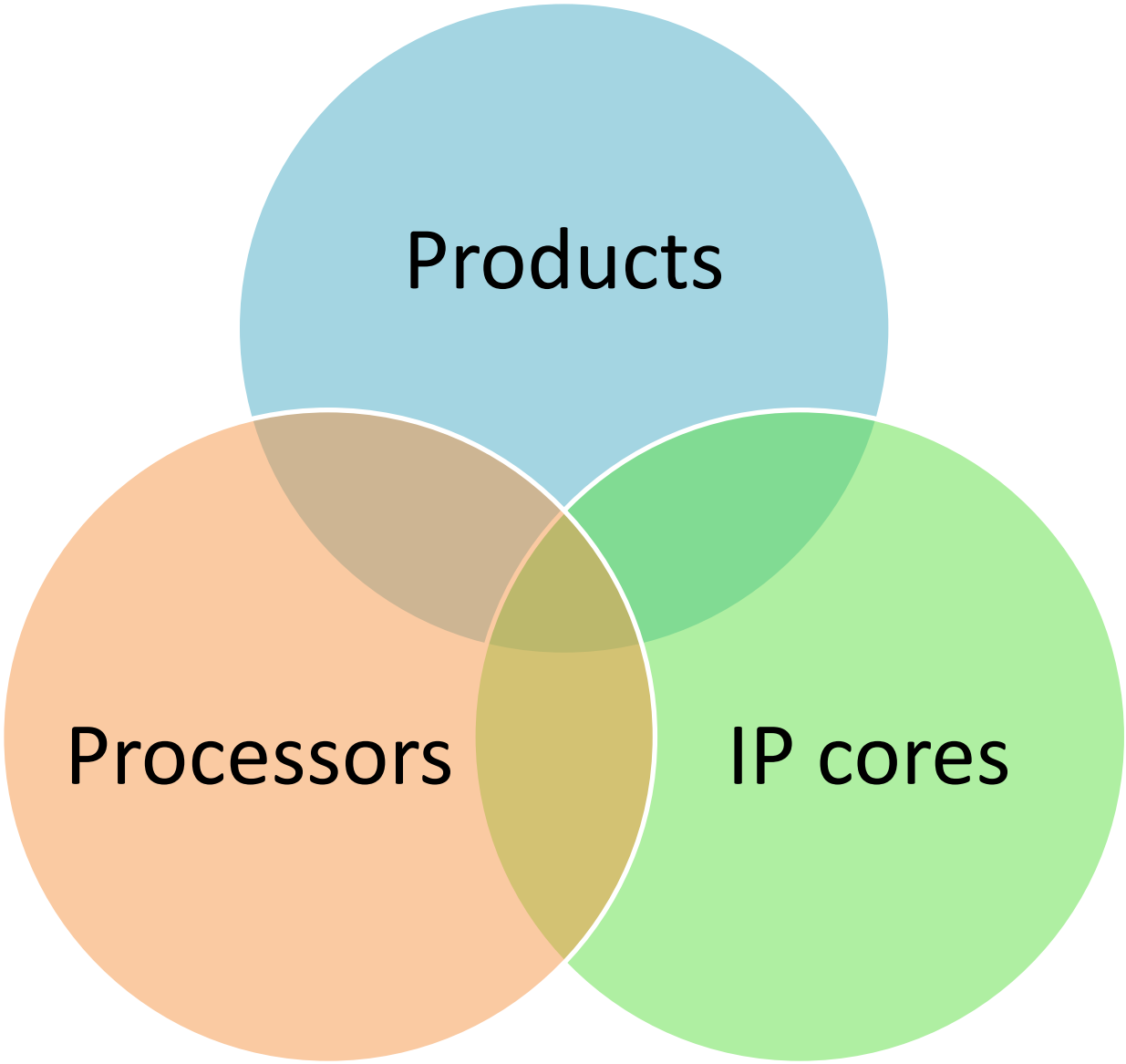


Key Expertise

- ASIC contract design
- **Value Chain Aggregator** services

  (TSMC representative since 2013/10)
- Own **CPU/DSP** architectures development
- **Smart cards/RFID** chips
- **Cryptography** and other **IP** cores
- Low-power designs
- Full **SDK, Toolchain** and **Firmware** support
- **Mass production:** cost, logistic optimization

General activities

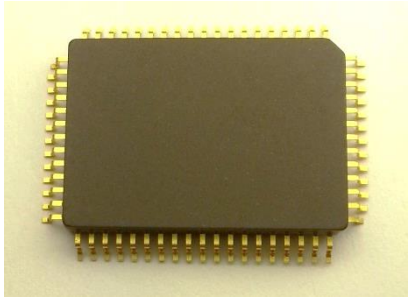


Processor Architectures

Architecture	Main Features	Applications
KROLIK 8/16/32-bit Microcontroller	• Low energy consumption under **28µW/MHz@90LP** • Class-leading performance **2.5 DMIPS/MHz -** better than Cortex-M3!!! • Small Die = Low cost: **33K gates 0.09mm^2**	• Smart-cards • Embedded controllers • Battery powered
KVARC 32-bit performance microprocessor	• IP Block library • Energy Efficiency • Linux or Free RTOS	• System-on-Chip • Personal navigation • Realtime applications
HYDRA DSP/Multimedia Engine	• Scalable Architecture • Performance up to **72** GFLOPS • Dynamic power consumption • up to 31 Application Specific Processors per die	• Multimedia application • Data processing • Networking

KROLIK 8/16/32 bit Microcontroller family

- Proprietary Harvard RISC architecture
- Very low power consumption: under **28µW/MHz***
- Class-leading performance of **2.5 DMIPS/MHz***
- Low gate-count and core size (**33K** gates and **0.09** mm^{2}*)
- Best of breed code density at GCC 4.7.2 & Eclipse SDK
- Secure OS & real-time FreeRTOS ported
- System and User modes of execution
- Memory access protection
- Secure architecture certification ready

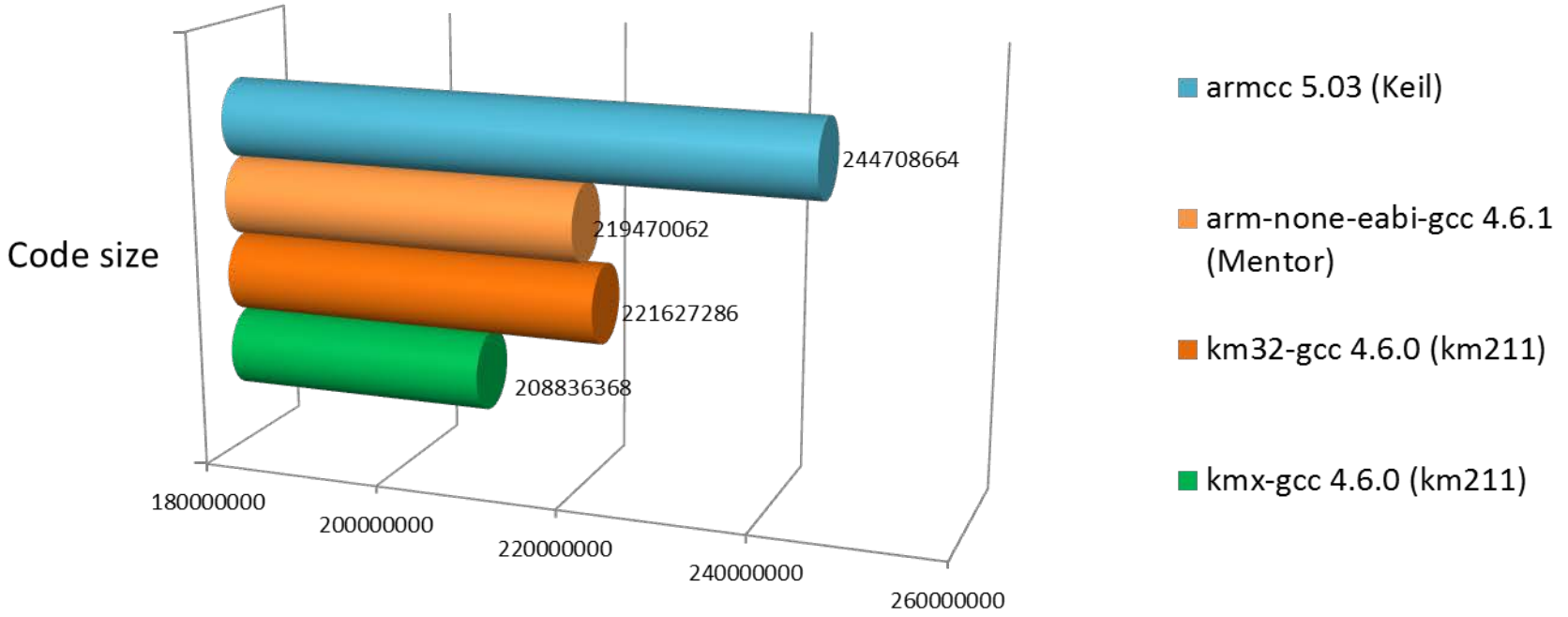


Unique combination of leading performance, minimal size (= minimal cost) and energy efficiency

**** results for KMX 32** @TSMC 90nm LP*

KROLIK 32 bit Code density

Comparison was made on compilers versions based on gcc 4.6.1-4.6.0*



ARM gcc 4.6.1 vs. KMx32 gcc 4.6.0 code gives 5% more size!!!

*-Detailed protocol is available

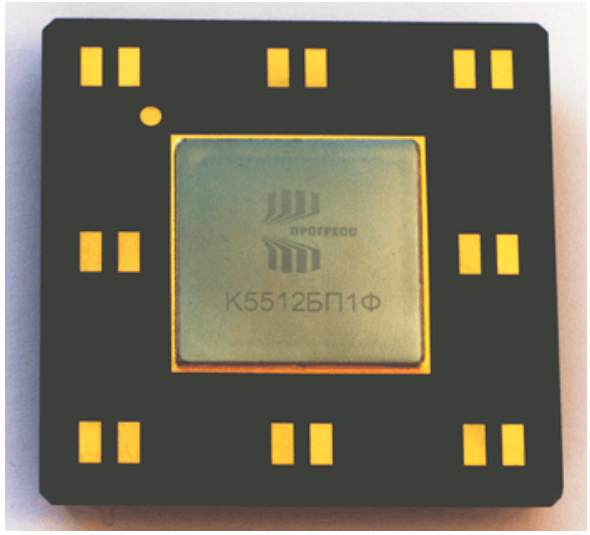
Competition comparison (low end cores)

Processor core		Cortex M3	Cortex M0	ARC 601	ARC 605	**KMX8**	**KMX32**
General characteristics	Performance, DMIPS/МГц	1.5	1	1.2	1.3	0.9[1]	**2.5**
	Coremark/MHz	3.3	2				**2.3**
	Operands size	32	32	32	32	8	32
	Pipeline length	3	3	5	5	3	3
	Code size (gcc 4.6.1)	100%					**95%**
130nm	Area, mm^2	0.38	0.17	0.175	0.24	0.178	0.27
	Dynamic consumption (uW/MHz)	84				**25**	63
	Work frequency, MHz	50	135			50	50
90nm	Area, mm^2	0.12[2]	0.04[2]	0,089		0.035	0.09[3]
	Area,%	100%	33%			29%	**75%**
	Dynamic consumption (uW/MHz)	32	16			12	**28**
	Work frequency, MHz					100+	100+

[1] – target value, not verified yet
[2] – minimal core configuration, no memories included, ARM web site info
[3] –with register file in maximum configuration, 70% area utilization

KVARC 32-bit MPU

- Silicon proven
- Options: MMU, Cache, TLB, Intellectual DMA, FPU
- DSP instruction set extension
- Fast interrupt switching of just 5 cycles
- **1.1** DMIPS/MHz
- **450** MHz clock frequency*
- **0.2** mm^2 @90nm core area*
- FreeRTOS, Linux 2.6, JAVA ported
- C-compiler GNU (GCC v 4.6.0), Eclipse based SDK
- Energy efficient 100 µW/MHz **, 8.5 DMIPS/MHz**
- Original architecture



* *Maximum @TSMC 90nm G*

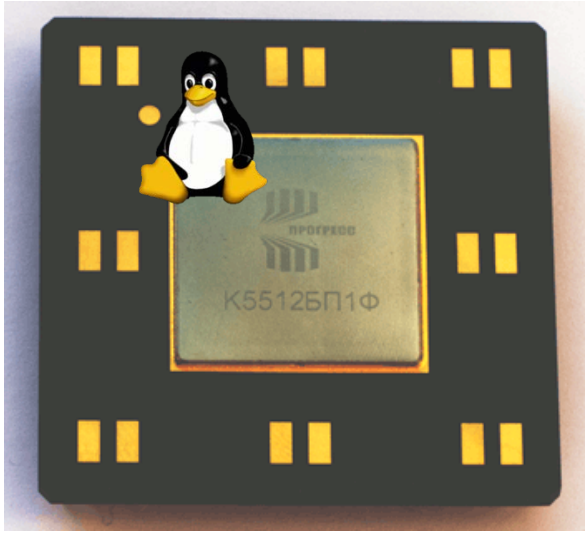
** *Estimated @TSMC 90nm LP*

KVARC environment.System-on-Chip ready

Linux with full user space environment.
Graphic/Video accelerator support

SDK, based on Eclipse for Linux and Windows developers
JTAG Debugger (**gdb**) support

FPGA Developer boards available



Memory controllers
- TSMC embedded flash
- ONFI flash controller (asynchronous mode)
- Compact Flash/IDE
- SDRAM, SRAM, NOR/NAND Flash

Cryptoaccelerators
- ECDSA/RSA
- AES/DES/SHA-1

FPU & Math units
- SD/DD IEEE 754-2008
- CRC-16/32 with any coefficients

Multimedia IP
- H.264 Codec
- AC97 / I^2S/ ITU 656 Video interfaces

Interfaces
- AMBA Support
- PCI 3.0
- SATA2
- USB 2.0 Host/Device

Additional on-chip IPs also available

Competition comparison (mid-range cores)

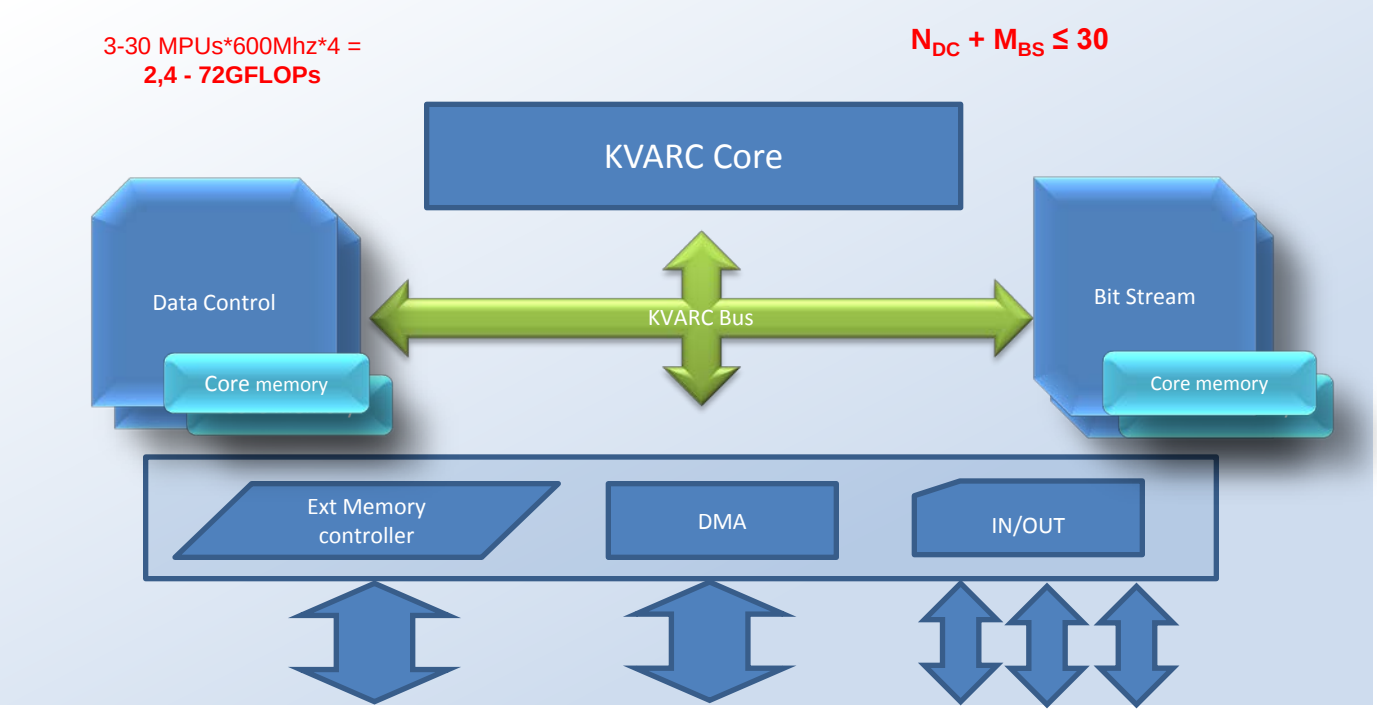
Processor core		ARM 926EJ	ARM 7-S	MIPS MIPS32 4k	**KM211 KMX32**	**KM211 KVARC**
General characteristics	Performance, DMIPS/MHz	1,1	0,74	1,3	2.5	1,1
	Operands size	32	32	32	32	32
	Pipeline length	5	3	5	3	5
130nm G	Work frequency, MHz	250	100	100	70	~270
TSMC 90nm	Area, mm^2	0.5	0.34		0.09	0.2
	Area,%	100%	68%		**18%**	**40%**
	Work frequency, MHz	250	204	300	100+	450

HYDRA Scalable DSP Platform

Modular scalable architecture;
Up to a **32** cores per chip:

- **KVARC** as CPU with Linux OS;
- **DC (Data Control core)** - DSP core that supports superscalar and vector modes, SIMD;
- **BS(Bit Stream core)** - for bit fields and the complex structured data streams

- **3** task optimized **instruction sets** in one chip;
- The unique configurability of the chip - a **set of operating cores** dependent on the task;
- Dynamic power control;
- **Ultra-low power consumption** due to specialization and cores compactness



HYDRA Engineering sample

32-bit KVARC control CPU

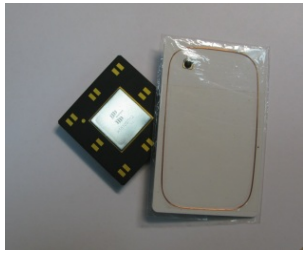
- 32 KB Instruction memory
- 16 KB data memory
- MMU, RTOS Support
- JTAG Debugger with 16KB trace

- **Two** 32-bit **DC cores**:
  64 KB SRAM per core
- **One** 32-bit **Bitstream (BS) core**
  with 80KB memory

- **Internal Bus controller**
- **Intellectual DMA Controller**
- **External Memory interface: FLASH/RAM**
- **Linux OS ported**
- **Clock and Power save controller**
- **Additional hardware accelerators and coprocessors**

Own products

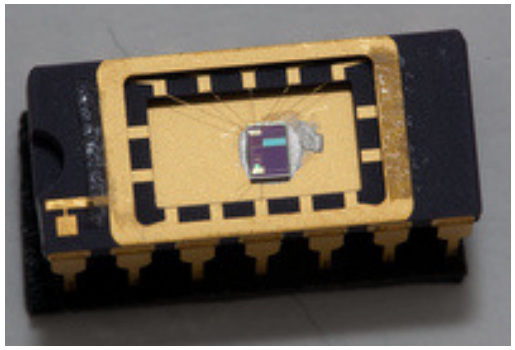
- SIM card with Secure OS
- Contactless Transport/ ID cards (MIFARE Classic, Ultralight)
- System-on-Chip
- Trusted Platform Module/Host Security Module chips
- Contact/contactless microprocessor based smart-card
- Biometric passport contactless smart-card (Russia)
- and more…



SIM card with HW Crypto accelerators

Main benefits

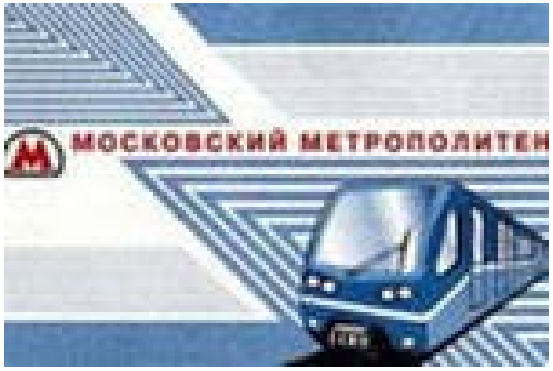
- Own secured 32-bit CPU core
- High Code Density
- True-RND
- Security sensors
- Secure OS porting in progress
- Certification (Russia) in progress
- Mass production at TSMC fab



- Up to 20MHz CPU clock
- 384 KB Flash
- 12 KB RAM
- DES/3DES
- GOST 34.10-2001/ECDSA digital signature
- Power:1.8/3/5 V

We have all success factors for smart cards business: secure processor cores, cryptography, SW and certification partners.

Contactless cards

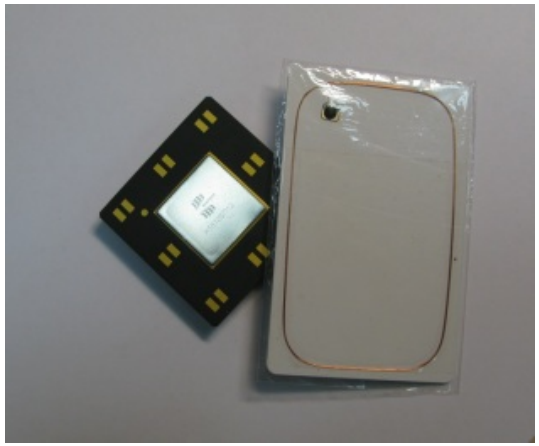


MIFARE Classic, Ultralight analogue

- ISO 14443 A interface
- ISO/IEC DIS 9798-2 authentication
- 1 KB EEPROM
- Die size: 0.2 mm^2

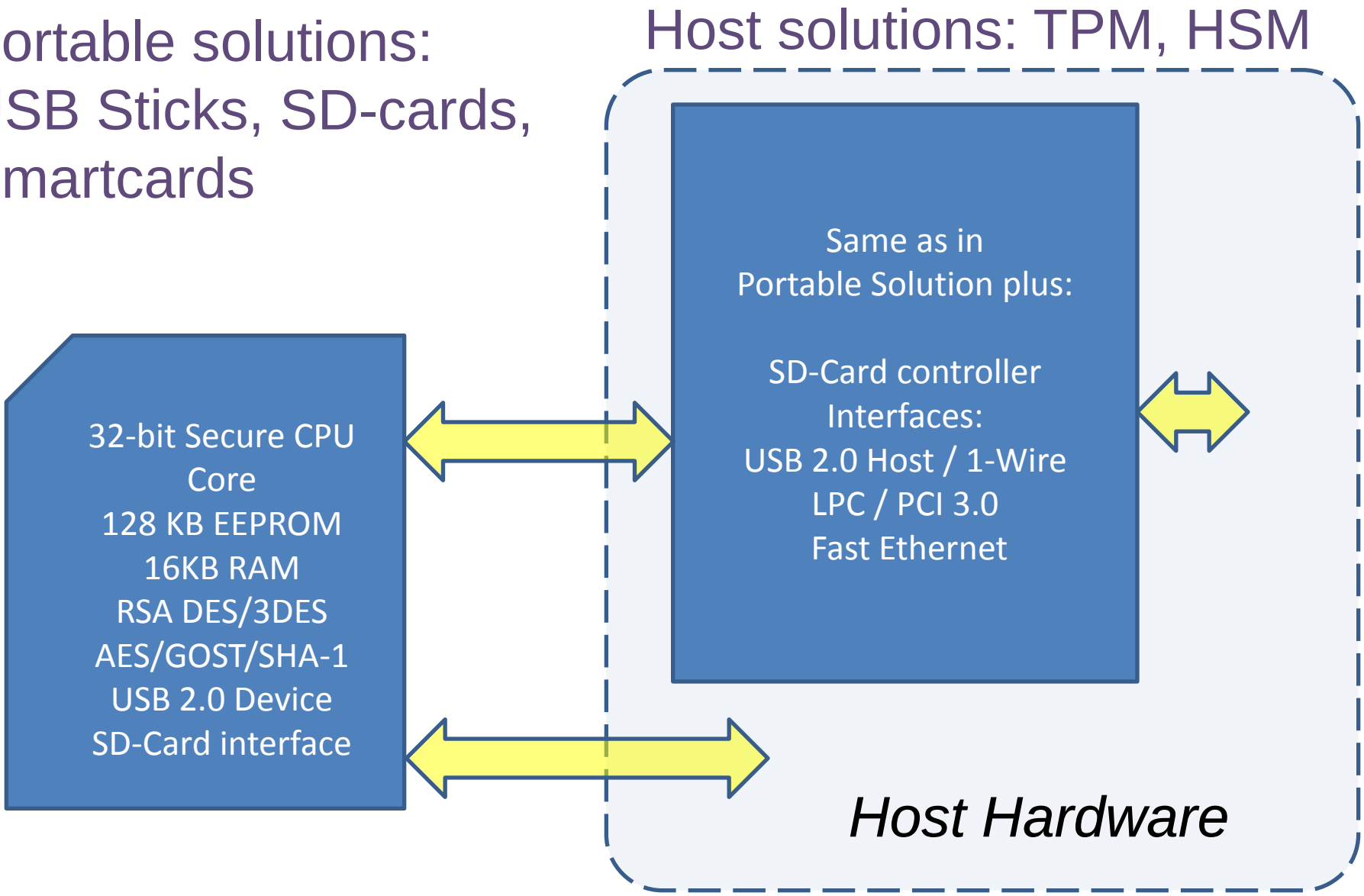
SLI/SLIX ICODE Analogue

- ISO 15693, ISO 18000-3 interface
- Collision detection
- Memory access control
- Unique serial number
- 1 KB EEPROM
- Die size: 0.2 mm^2



Trusted Platform/Host Security Module chips

Portable solutions:
USB Sticks, SD-cards,
Smartcards



Other IP Cores*

Crypto accelerators	Smart cards and RFID	Math coprocessors and accelerators
• ECDSA/RSA • AES/DES/SHA-1 • GOST 28147 • GOST 34.10 • GOST 34.11 • MIFARE Crypto1	• ISO 14443A/B • ISO 15693 • ISO 18000-3 • ISO 7816	• FPU SP/DP • H.264 codec • Divider • 16x16 MAC • CRC32 – programmable coeff. • CRC16 ($x^{16} + x^{12} + x^5 + 1$)

Interfaces		Memory controllers
• 1-Wire • Ethernet • USB 2.0 Host/Device • SATA2 • AC97 • TFT LCD • Touch Screen • JTAG Module	• PCI 3.0 • I^2C • I^2S • SPI • USART • ITU 656 Video	• TSMC embedded flash • ONFI flash controller (asynchronous mode) • Compact Flash/IDE • SDRAM, SRAM, NOR/NAND Flash

**** Additional information available under NDA***

Crypto and modular arithmetic IP Cores*

#	Algorithms	Description	Area/Gate count
1	DES/ 3DES	**Low** gate count, support of 3DES with key reload	7500mkm^2 @TSMC90LP 2,700 gates
3	DES/ 3DES/ GOST 28147-89	**Unified block** for two algorithms, additional memory could be mapped into CPU memory with direct access or as a standalone memory	8000 mkm^2 @TSMC90LP 3,000 gates
4	AES-128	S-tables that can be mapped to the CPU memory space or placed as a stand-alone block. If constant values can be used for S-tables then gate count can be reduced with no additional memory	7,300 gates
5	RSA/ DSA/ GOST 34.10-2001/ ECDSA	**Fast universal** block with 1024 bit data path for: RSA(1024) enc, dec, sign, check/DSA(1024/160) sign, check/GOST34.10-2001(256) sign, check/ ECDSA(160) sign, check	105,800 gates
6		**Slow universal** block with 1024 bit data path with same functionality as block #5	52,000 gates
7	GOST 34.10-2001/ ECDSA	**Small universal** block with 256 bit data path for GOST34.10-2001(256) sign, check/ ECSDA(160) sign, check	68,000 @90LP 25,000 gates
8	GOST P34.11-94/SHA-1	**Hash calculation** for 32bit datapath for GOST P34.11-94 and SHA-1	18,600 gates

**** Additional information available under NDA***

Contact Details

Design Center KM211, Ltd. (KM211) - www.km211.com
124498, Russia, Moscow, Zelenograd, proezd 4806, dom 5, stroenie 23
E-mail: *info@km211.com*
Tel: +7 (499) 940-03-56
Tel/Fax: +7 (499) 940-03-57

President
Alexander Lutsenko

CEO
Marat Rakhmatullin

R&D
Sergey Lubimov

VP Sales & Marketing
Dmitry Pustov