

### 1) Where in the CPU is UDPI's technology located?

UDPI is located between the Instruction Fetcher (or Instruction Register) and the Instruction Decoder.

### 2) How does UDPI work with the Instruction Decoder?

UDPI creates a virtual unique set of instructions. Firmware A in Processor A will look completely different from Firmware A in Processor B. The Firmware A goes through a special encoder that creates a logic set of instructions for Processor A, but these instructions will not work for Processor B. Only Processor A can properly decode its firmware.

### 3) Does the Program Counter (PC) in a processor have to be sequential with UDPI's security?

No, with UDPI the Program Counter (PC) does not have to be sequential. For example, to execute the same line in one processor the instruction might be GOTO 0x10010 compared to GOTO 0x2E400 in another. UDPI can randomize the process flow of a program, causing it to jump to different locations from one processor to another.

### 4) Does the level of security depend upon the bit-size of a microprocessor?

No. Larger processors have longer strings of instruction, and when there is a higher bit-count, more can be executed in one cycle. For example, a 4-bit micro would take many cycles to execute an instruction that a 32-bit could execute in one step. UDPI's ability to scramble data does not rely on how many bits the micro contains, allowing advanced security for 4-bit micros and beyond.

### 5) Can EPROM memory be scrambled with UDPI?

Yes, EPROM memory can be scrambled with UDPI and unique for each processor.

### 6) What affect does UDPI's security have on an opcode table?

UDPI scrambles data and as a result opcode tables appear "corrupted" or scrambled.

### 7) Does UDPI standardize processors?

No. UDPI's technology can be applied to any processor and layout on the market and the processor is in no way standardized by UDPI.

### 8) Can UDPI be compared to encryption-based securities?

No. UDPI is not an encryption. Currently security is deemed as being a trusted party, but does not involve much processor security. There may be trusted control over communicating with peripherals, but this security protects against “sniffers” trying to access data traveling from one place to another, rather than actually protecting intellectual property (IP) and data traveling within the microprocessor itself. UDPI protects this IP and is truly a tamper-proof and anti-cloning technology.

### 9) Does UDPI require a second chip for its security capabilities?

There is no separate security chip required for UDPI's security capabilities. The technology is hard-wired during manufacturing with no added BOM costs. Silicon protection is complete without the use of a second chip.