

EvoTech Technical Report

ETR-97-01a

Rapid development of a Cryptographic Module using

VASCO Data Security's Cryptech

CRY12C102 DES chip

by

William M. Conlon, P.E., Ph.D.
VP Business Development
EvoTech, Inc.

Abstract

A client desired a plug-in module to provide secure transmission of packets over the PSTN, using DES at full duplex E1 data rates.—EvoTech provided turn-key development of hardware and software, including definition, design, development, testing, and delivery of beta units.—EvoTech delivered the cryptographic module less than 5 months after the start of the project, successfully meeting cost and schedule requirements.

The project began with a technical investigation, wherein EvoTech identified and recommended hardware components and an architecture to meet the cost and schedule targets with minimal risk.—DES chips from VASCO, Newbridge Networks, and VLSI were evaluated for encryption speed, development risk, growth path, unit cost, and power consumption.—VASCO Data Security's Cryptech CRY12C102 DES chip was selected.

The hardware design effort included requirements specification, timing analysis, schematic capture, and management of board layout, fabrication and testing of beta units.—The design included a dual port RAM for the host interface, microcontroller, SRAM and FLASH memory.—A dual channel DMA controller and glue logic passed data to and from the encryption chip.

The firmware design effort included development of software requirements specifications, cryptographic API, drivers and applications software.—EvoTech's DSOS™ operating system, which provides Controlled Multi-tasking via Message Switching, enabled rapid development of a robust and compact (only 12k code space) embedded application.

This paper describes the technical requirements, design trade-off's, and methods used to achieve On-Time Delivery of this Real-Time embedded product.

Company Background

Incorporated in California in 1984, EvoTech, Inc. is an engineering design firm specializing in the **On-Time Development** of high volume products incorporating embedded software ("firmware").—Services provided by the Company include:

- **Turnkey product development**, involving both hardware and software development, and usually requiring aggressive development cycles;
- **Software Development**, especially for projects where high quality design documentation is important;
- **Software Process Improvement**, divided between cycle time improvement and safety critical software systems.

Industries served include telecommunications, semiconductor equipment, consumer electronics, and many companies using embedded systems in high-volume mission-critical applications.

In telecommunications, EvoTech focuses on Digital Subscriber Line (DSL) technologies, having completed more than 30 DSL designs for a variety of customers.—EvoTech also has extensive background in premises security systems, and has recently worked on several data security related projects, including the subject of this case study.

EvoTech's track record is built upon the Specification Driven Development life-cycle methodology for real-time systems.—Hierarchical Software State Machines (HSSM) provides the framework for the methodology resulting in Rapid Quality Product Development.—An exceptionally compact message switched kernel, DSOS™, provides rapid and deterministic Controlled Multitasking™ to enable efficient implementation of HSSM designs.

Project Background

EvoTech's client was in charge of data security product development at a multinational telecommunications company, and was already familiar with EvoTech's software development methodology.—The client asked EvoTech to provide an "engineering department in a box" for a new software engineering group.—To facilitate the adop-

tion of the new process, we proposed a pilot project to prove its effectiveness.—As the pilot project, the client suggested that we undertake turnkey development of a highly visible Packet Encryption Product (PEP), including both hardware and software.

The PEP was a first of its kind cryptographic module, intended as an add-in daughter board for a packet communications system.—It was required to provide DES encryption at full duplex E1 data rates, with minimal impact on the host processor.—Also it was required to work with a number of products, each somewhat different implementations of a so-called "standard interface" (3 different microprocessors, using different bus widths, and clock rates).

Moreover, the PEP had to meet a number challenging requirements on an aggressive schedule in order to be Beta tested at a customer site in only five months.—Accordingly, the investigation phase focused on identifying appropriate hardware and software components and designs that would minimize the development effort and risk of delay.—At the same time, it was necessary to consider the suitability of different designs with respect to the functionality that the client intended to add to the PEP in the future.—Finally, the PEP was cost-sensitive, so design concepts were also considered with respect to the potential for cost reduction.

Our first step was to undertake a technical investigation to study the project's feasibility, with the following deliverables.

- **Hardware Technical recommendations**, including design alternatives we considered (with cost/performance/risk tradeoffs identified), a proposed conceptual design with a block diagram, basic description, and preliminary bill of materials.
- **Software Technical recommendations**, including design alternatives, a proposed conceptual design (preliminary architecture), and recommendations for a cryptographic API and its implementation methods (protocol), including extensions for DES3 and compression.
- **Product Development Plan**, describing the strategy for delivering working units within four months.—This document also described the managerial and technical processes to be used to mitigate risks and to achieve on-time delivery with high pro-

duct quality.—The plan included a project schedule, list of deliverables, and cost estimate.

We concluded that the project was both technically and managerially feasible for EvoTech to undertake, and within three weeks, design work was underway.—Prototype boards with working firmware were delivered to the client on budget and on-time, five months after the initial discussions..

Requirements

The PEP was required to interface to 3 distinct Motorola based motherboards, with different processors, timing, and bus width.—A standard cryptographic API was to be developed to provide a standard software interface for security services.—The specific requirements are outlined below.

- **Packet encryption.**—The PEP was to provide packet encryption using DES CBC (Cipher Block Chaining) for variable size packets, with a typical length of 1600 bytes.—The PEP was to pad packets as necessary to multiples of 8 bytes long.
- **Data rate.**—Simultaneous encryption and decryption at E1 data rates were required for a total encryption rate of 4.096 Mbps.
- **Virtual channels.**—Separate secure connections were to be maintained for up to 1,024 Private Virtual Channels, each with their own key.
- **Key Management.**—Support for key exchange, key encrypting keys, tamper proofing, etc., was required.
- **Low cost.**—Unit costs less than \$150 in 1,000 unit quantities were desired.
- **Cryptographic API.**—A well-defined Applications Programming Interface was required to provide the software link between the PEP and the motherboard.
- **Future requirements.**—The client desired that the PEP design consider the need for several additional capabilities, including Triple DES encryption, data compression, and Loadware (firmware download).S

Hardware Design

Encryption throughput requirements dictate that a dedicated encryption chip be used.—Although extensive research was conducted to identify appropriate chips, most were

discarded because they were obsolete, too slow, or did not support all of the encryption modes.

- The Newbridge (Tundra) CA95C68/18/09 DES chip does not provide DES3 capability or OFB modes, so its future expansion capability is limited.—This chip has only an 8 bit interface, so memory bus bandwidth may become an issue.
- The VLSI VMS 110 does not support either OFB or CFB encryption in either block or byte modes, nor does it support triple DES.

Two candidates emerged: the VLSI VMS210 and the Cryptech CRY12C102.—There are a number of differences between the two encryption chips that had important implications with respect to technical risk, design effort, and schedule risk.

- **Microcontroller interface.**—The Cryptech chip must be controlled by an external microprocessor, which may be either on board the PEP, or on the Motherboard.—An on board processor would be Motorola based for the purpose of compatibility with the rest of the system.—The VLSI chip has an ARM6 RISC processor that is not compatible (either in H/W and S/W) with the Motorola based processors.—Development systems for the VLSI ARM6 implementation are limited.—
- **Field experience.**—The Cryptech chip is field proven, uses mature technology (reportedly 2 micron CMOS), and has an extensive published customer list.—One commercial application is an ISA bus DES/RSA encryption card for a personal computer, which EvoTech obtained as part of this technical evaluation.—The VLSI chip was brand new, not yet in production, and even the technical specifications were only available under a non-disclosure agreement.—Reportedly, of 3 prospective users of the VLSI chip, only 1 was past the prototype phase at the time of the evaluation.
- **Cost.**—The Cryptech chip was approximately half the cost of the VLSI chip, although this would be offset by the cost of an additional microcontroller to replace the ARM6 core in the VLSI chip.—
- **Package Size.**—The Cryptech chip is approximately one-half the size of the VLSI chip.—Some of this difference may be due to the unnecessary interfaces (ISA, PIO, MPEG2) included with the VLSI chip.—These interfaces suggest that the VLSI chip

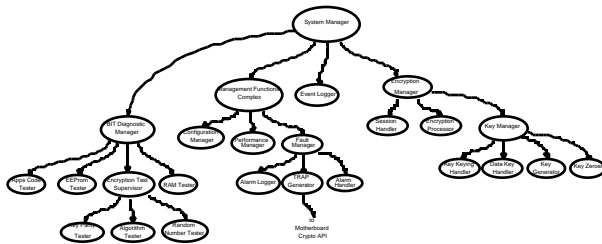
is designed for a multimedia application in a set top box, rather than for the straightforward encryption required of the PEP.

- **Memory Interface.**—The Cryptech chip is compatible with external DMA interfaces, or can be treated as a memory mapped peripheral.—The VLSI chip appeared to be relatively difficult to interface.

Recommendations. With the above considerations, EvoTech recommended, and the client accepted, selection of the Cryptech CRY12C102 DES encryption chip.

Software Design

The HSSM method was used to decompose the software requirements into a basic system architecture, as shown below.—This architecture was then increasingly elaborated, resulting in the definition of individual state machines, and their behavior.—



This object-like approach allows the system and its interactions to be **designed** by a software architect, while allowing programmers to implement and test individual software components.—This results in system integrity, faster and less expensive programming, and lower schedule risk.

The software deliverables received by the client included the following design documents:

- Software Requirements Specification
- Software Design Specification
- API and Protocol Specification
- Hardware/Software Interface Specification
- Event Analysis
- Source Code
- Unit Test Plan and Test Report
- Integration Test Report

Results

Total elapsed time from inception to delivery of working hardware and software was five months.—A total of 3,800 hours were required from the beginning of the investigation phase through delivery of the first Beta prototypes.—Approximately 800 hours were used for hardware design, 200 for project management, and the remainder for software design, implementation and test.

Thorough regression testing assured that the PEP performed as designed.—The PEP exceeded the throughput requirements for the typical packet size.—

The compact DSOS™ kernel and the memory efficient HSSM design methodology were key to the success of the project.—Total code size, including the DSOS kernel and all driver and applications code was approximately 12 kB, less than 10% of the available code space.— Software metrics indicate acceptable code complexity (less than 10), meaning the code is maintainable, and of high quality.

Summary

Critical success factors leading to the turnkey development of a high quality Packet Encryption Product included:

- Mitigation of technical risk by using proven hardware, including the Cryptech CRY12C102 DES chip.
- Use of proven software development methodologies, specifically Specification Driven Development.
- Experienced, effective project management.