Soluciones de Seguridad de Freescale 2ª parte: Criptografía en procesadores de comunicaciones

Artículo cedido por el Dpto. Técnico de Freescale

Freescale Semiconductor
www.freescale.com

En este nuevo artículo de la serie, analizaremos otro aspecto importante en seguridad, como es el relacionado con la aceleración criptográfica orientada a las comunicaciones en red.
Los procesadores PowerQUICC de Freescale, desde sus comienzos incorporan estos periféricos de aceleración basados en hardware.
En el presente artículo se presentaran las diferentes arquitecturas de criptografía y se mostrará en más detalle la elegida por Freescale en sus implementaciones.
Para el análisis de resultados se particularizará para uno de los procesadores de la serie PowerQUICC II Pro, MPC8313E, mostrándose la implementación realizada en este procesador y los algoritmos soportados.
Para más información, visite www.freescale.com/networking

¿Qué es la criptografía?

La criptografía es el arte y la ciencia de codificar y decodificar información de forma que terceras personas no puedan hacerlo y por tanto acceder a la información en cuestión. Los aspectos a tener en cuenta en todo proceso criptográfico incluyen:

- Confidencialidad de la información durante el almacenamiento y la transmisión.
- Autenticación de los usuarios y de la información recibida o leída.
- Integridad de los datos
- No-repudio de transacciones.
- Disponibilidad de datos y recursos
- Acceso controlado a la información o los recursos

Los protocolos de seguridad utilizados en redes de comunicación hacer un uso intensivo de algoritmos criptográficos, para conseguir los objetivos anteriormente descritos. Dado que todo proceso criptográfico es desde un punto de vista computacional bastante intensivo, toda aceleración que se pueda ofrecer desde el propio microprocesador será bienvenido, si bien habrá diferentes aspectos que condicionarán las prestaciones que se puedan esperar de de los mismos, como veremos en siguientes apartados.

Descripción del MPC8313E y sus módulos criptográficos

Como hilo conductor en el presente articulo, utilizaremos como referencia el procesador MPC8313E de Freescale, que incorpora el núcleo Power e300c3, acompañado de 16 kBytes de memoria L1 caché de datos e instrucciones y MMU. Junto al núcleo principal, dispone de un núcleo de aceleración de cálculos criptográficos (SEC 2.2) que permite descargar a la CPU principal en algoritmos tales como DES, 3DES, Advanced Encryption Standard (AES), Secure Hash Algorithm (SHA)-1 y algoritmos MD-5. Además, el MPC8313E está provisto de dos controladores Ethernet 10-100-1000 Mbps, controlador de memoria DDR-1/DDR-2 SDRAM controlador PCI-2.3 de 32-bit, USB on-the-go (soporte de modo device y host) con USB 2.0 HS PHY, doble controlador I2C, DMA de 4x canales y puertos E/S. En la figura 1, puede verse un diagrama de bloques del dispositivo.

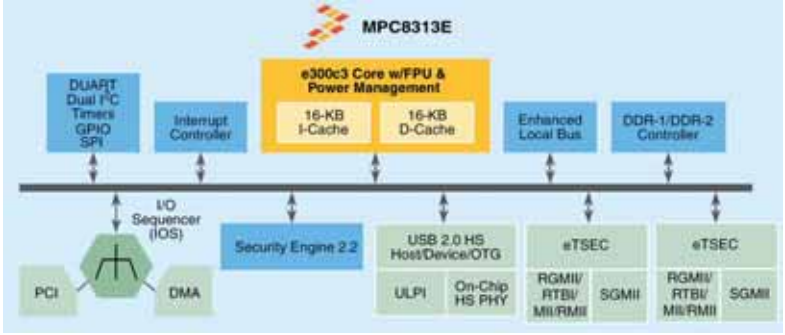

Figura 1. Diagrama de Bloques del MPC8313E

El motor de seguridad (Security Engine SEC 2.2) reside en el mapa de memoria de periféricos del procesador, de forma que cuando una aplicación requiera la ejecución de funciones criptográficas simplemente crea unos descriptores para el SEC que se encarga de la ejecución de dichas funciones. El SEC puede tomar control del bus, y tras la escritura de unos pocos registros por parte del procesador principal, el SEC se encarga de leer y escribir de la propia memoria del sistema hasta completar la tarea.

El controlador es capaz de transferir palabras de 64bits entre el bus y cualquier registro dentro del propio SEC.

El SEC está optimizado para el tratamiento de los algoritmos relacionados con IPSec, 802.11i, e iSCSI. Contiene un canal de encriptado para el manejo de los comandos para diferentes algoritmos, un controlador y un conjunto de Unidades de Ejecución Criptográfica (EUs):

- DEU (Data Encryption Standard Execution Unit), para el soporte del DES y 3DES

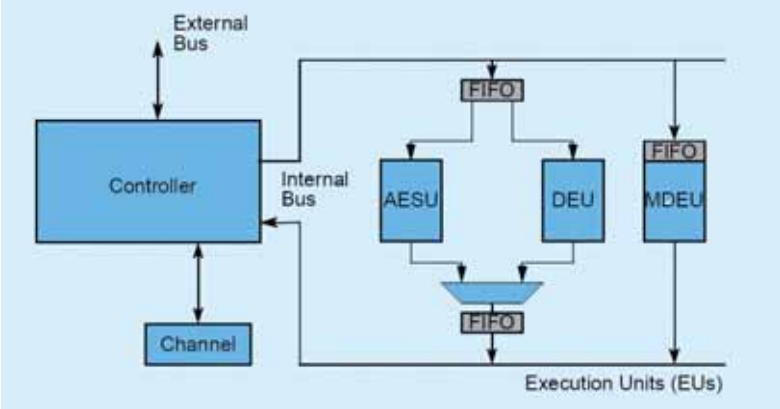

Figura 2. Arquitectura SEC 2.2 simplificada del MPC8313E

• AESU (Advanced Encryption Standard Unit), para el manejo de AES
• MDEU (Message Digest Execution Unit), para el tratamiento MD5, SHA1, SHA-256, y HMAC con cualquier algoritmo.

En la figura 2 se describe de forma simplificada la arquitectura del SEC 2.2.

Variables que inciden en las prestaciones criptográficas

Pueden existir enormes diferencias entre las prestaciones teóricamente alcanzables en un dispositivo dotado de capacidad de proceso criptográfico, y las que en realidad se alcanzan en una determinada aplicación, que es en definitiva para lo que se realiza. Por tanto, juzgar a priori cual es el resultado esperado no es tarea fácil. Alguna de las diferencias que encontraremos están directamente relacionadas con la propia arquitectura de aceleración utilizada. Otras están más relacionadas con el Stack de Protocolo de software usado, y por último algunas otras están relacionadas con limitaciones en los API o en los drivers usados.

En los próximos apartados, se identificarán y analizarán las variables que afectan a las prestaciones relacionadas con la seguridad desde un punto de vista de sistema, y cómo esas variables inciden en el tráfico de datos. De esta forma podremos predecir como va a comportarse un determinado dispositivo dotado de esta funcionalidad y poder compararlo con otros disponibles en el mercado.

Arquitecturas de Aceleración Criptográfica

Hay muchas posibilidades para implementar un acelerador criptográfico, pero todas ellas se agrupan en dos tipos de arquitecturas: Flow-through y Look-aside.

Aceleradores Flow-Through

Un acelerador Flow-through realiza la Operacion criptográfica a medida que los datos "fluyen" de una posición de almacenamiento o de localización a otra. En un sistema de almacenamiento, por ejemplo, podría ser de la memoria del sistema a un disco duro; en un sistema de comunicaciones en red, el flujo sería entre el interfaz de comunicaciones y el procesador. Un factor característico de los procesadores Flow-through es el nivel de autonomía frente a otros procesos situados tras él. Por ejemplo, en sistemas de red, los procesadores Flow-through son capaces de terminar paquetes IPsec, de forma que procesadores que reciban los datos tras el reciban ya solo paquetes IP. Terminar paquetes IPsec implica que el procesador criptográfico es capaz de clasificar paquetes, de forma que sea capaz de determinar si requiere procesamiento y caso de necesitarlo a qué túnel de seguridad pertenece. Estos procesadores han de ser capaces también de realizar el procesado de cabeceras y colas IPsec y de mantener la sesión de seguridad. Típicamente este tipo de implementaciones se realizan en ASICs o pseudo-procesadores de red, y por tanto su posibilidades de adaptación en los protocolos de seguridad son nulas o muy reducidas. Es por ello que su uso en procesadores empotrados es muy reducido, tanto por la mencionada falta de flexibilidad, como por el área de silicio requerido para su implementación. Este tipo de aceleradores se usan en aplicaciones SoC (System on a Chip). Un chipset para un MODEM de cable con estándar DOCSIS MAC/PHY puede implementar un acelerador Flow-Through, por ejemplo, para la aceleración de desencriptado DES, o una controladora SATA puede llevar integrado un acelerador AES para encriptado de sectores de disco. Estas funciones pueden llegar a ser configurables, pero no reprogramables.

Aceleradores Look-Aside

A diferencia de los aceleradores Flow-through, los aceleradores Look-aside tienen poca o nula autonomía. Esta arquitectura requiere de la presencia de una CPU o NPU que realice la clasificación de paquetes como prerrequisito necesario para el posterior procesado de seguridad. La CPU realiza además funciones propias del SO (buffering/manejo de memoria) y proceso del protocolo de red. Dado que los protocolos de seguridad de red con complejos y con múltiples opciones, como por ejemplo IPsec, estos requieren la continua consulta de bases de datos por paquete recibido. Esta consulta está definida por el tipo de algoritmo usado, así como las claves necesarias para su implementación. La vida de las claves ha de ser monitorizada así como el proceso de refresco de las mismas. Por tanto, es necesario desfragmentar el paquete antes de realizar el procesado criptográfico. En la CPU principal se ejecuta un driver para el acelerador criptográfico y de esta forma aliviar su carga de trabajo. Inicialmente estos cripto procesadores se encontraban en dispositivos separados, como el HiFN 7901 y el MPC180 de Motorola (actualmente Freescale) y conectados por bus PCI, pero la tendencia ha sido lógicamente a integrarlos junto con el procesador principal. Existen dos subcategorías principales:

Aceleradores de bajo nivel (Low-Level).

No existe una definición formal de aceleradores de bajo nivel, pero la más extendida sería la de considerar bajo este tipo aquellos que no contengan capacidad de DMA. Si el acelerador no puede capturar sus propios datos, en ese caso una DMA (posiblemente 2, una para captura de datos y otra para la cesión de los datos) ha de entregar o recoger los datos de la FIFO del cripto procesador. Si la FIFO del cripto dispone de algún mecanismo de señal de handshaking con la DMA externa (tales como DREQ), el traspaso de datos será más sencillo. Esto obligará al procesador principal a estar saltando entre lectura y escritura a la FIFO, y si los paquetes son de tamaño reducido el proceso se verá altamente dificultado. Si además algunos algoritmos requieren encriptación de paquetes y autenticación (como por ejemplo en 3DES-HMAC-SHA-1), las APU del cripto comienzan a funcionar de forma serie, síncrona y bloqueante, ya que han de realizar estas tareas en un determinado orden; esto obligaría a crear dos descriptores y tratar ambas operaciones como dos acciones separadas, cada una con su acceso a memoria (ya que se considera de bajo nivel) por lo que las prestaciones se ven reducidas.

Aceleradores de alto nivel (High-Level)

Como es de esperar, los aceleradores de alto nivel vienen definidos por la presencia de DMA, con la capacidad de realizar pipelining y de diseminar/reunir la información (scatter/gather). Estas arquitecturas evolucionaron como co-procesadores externos en buses periféricos como PCI, donde las latencias de acceso a memoria son altas, y el ancho de banda bajo. Los aceleradores de alto nivel facilitan el encriptado y la autenticación en una sola pasada, y en algunos casos proporcionan otros niveles de procesado del protocolo, para descargar aun más al procesador principal, como por ejemplo añadir cabeceras o colas del protocolo de seguridad. Esta es la implementación usada en los procesadores de comunicaciones PowerQUICC de Freescale. Veamos más en detalle alguna de sus características intrínsecas.

Flujo de información en Aceleradores Look-aside

Aun cuando pueda pensar que el flujo de información en sistemas con procesamiento de bajo nivel o de alto nivel pueden ser similar, en realidad no lo son, y existen notables diferencias en prestaciones y eficiencia.

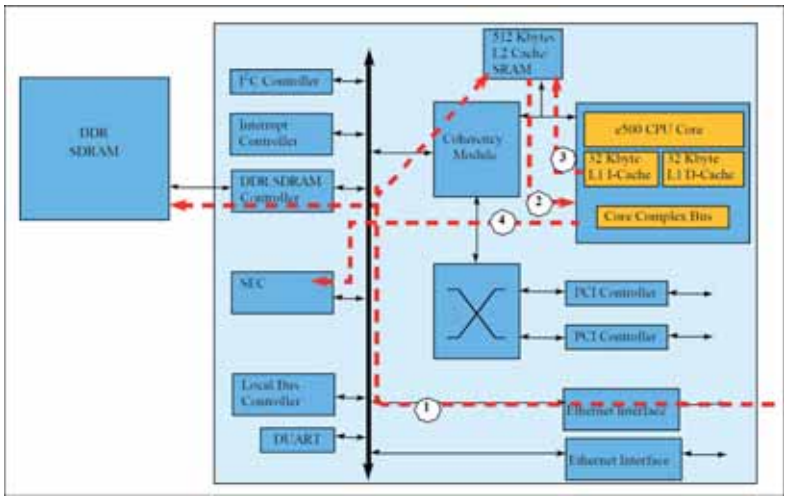

Figura 3. Pasos 1 a 4 en Arquitectura de seguridad Look-Aside

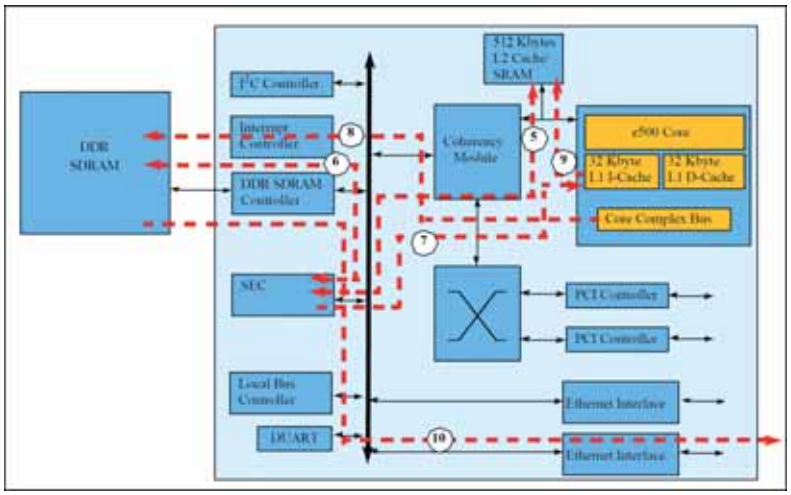

Figura 4. Pasos 5 a 10 en Arquitectura de seguridad Look-Aside

En las figuras 3 y 4 se ilustran los flujos de datos típicamente usados en procesadores de comunicaciones PowerQUICC III de Freescale con unidad SEC integrada, y que sería el más completo de los existentes. Los pasos son los siguientes:

1. Un paquete es recibido a través del interfaz Ethernet, y ubicado en un buffer de la memoria principal. Algunos dispositivos PowerQUICC disponen de optimizaciones específicas para este primer procesado.

2. Tras la notificación correspondiente (o vía polling) el paquete esta preparado para su procesado. La CPU lee la cabecera del mensaje - paquete para realizar su clasificación. En este ejemplo, se realizan una serie de chequeos en la cabecera para ubicarlos en diferentes tablas, y determinar si el paquete ha de ser protegido mediante IPsec, y mediante una asociación de seguridad en una base de datos se determina el túnel IPsec específico y los parámetros para el encapsulado del paquete.

3. La CPU crea un descriptor para el motor de seguridad (SEC) que incluye información de configuración, punteros a las claves, información de contexto, y otros datos que puedan ser necesarios para la operación criptográfica. La cantidad de proceso previo dependerá de las capacidades del acelerador. Por ejemplo, como se ha mencionado anteriormente, algunos cripto procesadores son capaces de añadir cabeceras IPsec durante su ejecución, y descargar por tanto de esta tarea a la CPU principal.

4. La CPU dirige un puntero al canal del cripto procesador (que como se ha explicado anteriormente, dispone de capacidad DMA).

5. El SEC captura el descriptor de la memoria principal.

6. El SEC se configura para realizar el procesado criptográfico en una sola pasada, tras capturar los datos necesarios para la misma (contexto, claves y datos de la memoria principal). Tras el proceso, escribe la información desencriptada en la memoria principal a medida que la va procesando.

7. El SEC interrumpe a la CPU principal bien cuando la operación ha se ha completado, o bien asigna un flag de "operación completada", para que sea la CPU principal la que detecte que está listo mediante un procedimiento de polling.

8. El core principal realiza un formateo final del paquete.

9. El core principal crea un descriptor de transmisión para el periférico Ethernet.

10. El interfaz Ethernet reenvía el parquet ya desencriptado.

La arquitectura Look-aside se ha convertido en predominante en procesamiento empotrado por los siguientes motivos:

- Por su coste, ya que se benefician de recursos ya incluidos en el propio SoC (tales como memoria, recursos de clasificación de datos y de mantenimiento del protocolo).
- Por la posibilidad de procesar los datos por software antes y después de la propia función criptográfica, de forma que se pueda acometer un abanico más amplio de posibilidades, tanto en tipos de instrucciones como en protocolo de seguridad. Es decir, por su flexibilidad.
- Por su versatilidad, ya que aun cuando puede tener prestaciones algo inferiores que arquitecturas Flow-through, aun así son más que suficientes para una amplia gama de aplicaciones.

Estos son los motives fundamentales para que la opción elegida en los procesadores de la familia PowerQUICC sea de tipo Look-aside.

Aspectos que influyen en mayor o menor medida las prestaciones de seguridad

En los siguientes apartados se analizan que aspectos tienen una influencia en las prestaciones de seguridad, desde el software, el propio SEC o el ancho de banda del bus.

Sobrecarga de Software por la aplicación o el Stack de Protocolo

Llamamos sobrecarga de la aplicación o del stack de protocolo a las instrucciones que el procesador principal ha de ejecutar para determinar que tipo de procesado criptográfico es que hay que realizar, y el formateo de los datos de cara a esa aplicación o protocolo de seguridad concreta. Esta sobrecarga es diferente a las esperadas por el driver especifico utilizado, ya que van a estar presentes independientemente de que exista o no aceleración. Esta sobrecarga es la responsable de la mayoría de la degradación de prestaciones y que más llama la atención al usuario cuando de pasa de una versión no securizada del protocolo (IP o TCP) a la versión dotada de seguridad (IPsec o SSL).

Unos protocolos tienen una incidencia mayor que otros. El porqué dependerá de la mayor o menor complejidad que requiera en la clasificación de paquetes para determinar si ha de ser securizado o no. La influencia de los stacks de protocolo dependerá del sistema operativo utilizado, y del stack propiamente dicho. Si bien no existen cálculos concluyentes al respecto, los resultados parecen indicar que la influencia del IPsec stack es mayor que la del propio sistema operativo. En el ejemplo realizado en el último apartado de este articulo, en la particularización para el MPC8313E, puede apreciarse con toda claridad este efecto.

Sobrecarga por los API criptográficos y Drivers de los dispositivos

Si bien no van a desarrollarse en el presente artículo la influencia de las APIs de seguridad y de los drivers de los procesadores SEC en las prestaciones que cabe esperar en el procesado criptográfico de la información, debe mencionarse que tanto unos como otros tienen una influencia. Como norma general ha de decirse que a medida que el tamaño de paquete de información aumenta, la influencia del API - driver disminuye, haciéndose más importante las prestaciones del propio SEC. Esto es especialmente cierto en aceleradores de bajo nivel, si bien los procesadores criptográficos de alto nivel tales como los integrados en la familia PowerQUICC presentan buenas prestaciones incluso con tamaños de paquete de datos elevados.

Prestaciones del cripto procesador

Tal como se ha indicado en el apartado anterior, las prestaciones del propio modulo SEC tienen una gran influencia en la prestación global del sistema, en especial con buffers de datos elevados. No debemos fijarnos en la velocidad de proceso del acelerador criptográfico, ya que no necesariamente a mayor velocidad las prestaciones obtenidas son mayores. Determinar las prestaciones del acelerador es simple de calcular, si bien es difícil de predecir la influencia del software en las mismas. Por tanto, la mayoría de los fabricantes únicamente publican como estimaciones de mejora de prestaciones por el uso del acelerador.

Ancho de banda del Bus

La cantidad de acho de banda requerido para implementar una aceleración criptográfica Look-aside es considerablemente mayor que si la aplicación no dispone de seguridad. Tanto si el buffer de datos a procesar es de mayor o menor tamaño, los datos han de ser movidos de una red o periférico a memoria, después de memoria al procesador criptográfico, y una vez procesados, movidos de vuelta a memoria y a la red o periférico de destino. Además se deben capturar claves u otras informaciones para realizar el proceso. En la tabla de la figura 5, se compara el consumo de ancho de banda requerido para un proceso IPv4 sin criptografía, comparado con uno IPsec modo ESP. En esta comparación no se tienen en cuenta incrementos que puedan producirse por otras consultas a tablas, captura de la instrucción, u otras lecturas o escrituras propias de la arquitectura.

IPv4 Forwarding	Bandwidth Consumed
Data In (Eth --> Memory)	Packet Size
Data Out (Memory --> Eth)	Packet Size
IPsec Forwarding	**Bandwidth Consumed**
Data In (Eth --> Memory)	Packet Size
Data Out (Memory --> Accelerator)	Packet Size
Key reads	36 bytes
Min additional Ctx reads/writes	28 bytes
Data Out (Accelerator --> Memory)	Packet Size + 56 bytes
Data Out (Memory --> Eth)	Packet Size + 70 bytes

Figura 5. Influencia absoluta en ancho de banda del bus

Dependiendo del tipo de operación de seguridad realizado y del tamaño del paquete de información procesado, la influencia porcentual queda recogida en la figura 6, en este caso de nuevo comparando una transferencia de datos IPsec modo ESP, frente a una sin seguridad de acuerdo a IPv4. Nótese que la influencia del tamaño del paquete de información se incrementa a partir de 1518 bytes, debido a la fragmentación que se produce.

Packet Size (B)	IPv4 Bus BW	IPsec Bus BW	Bus BW % Increase
64	128	446	348%
128	256	702	274%
256	512	1214	237%
390	780	1750	224$
512	1024	2238	219%
768	1536	3262	212%
1024	2048	4286	209%
1280	2560	5310	207%
1456	2912	6014	207%
1518	3036	6452	213%

Figura 6. Influencia porcentual en ancho de banda del bus

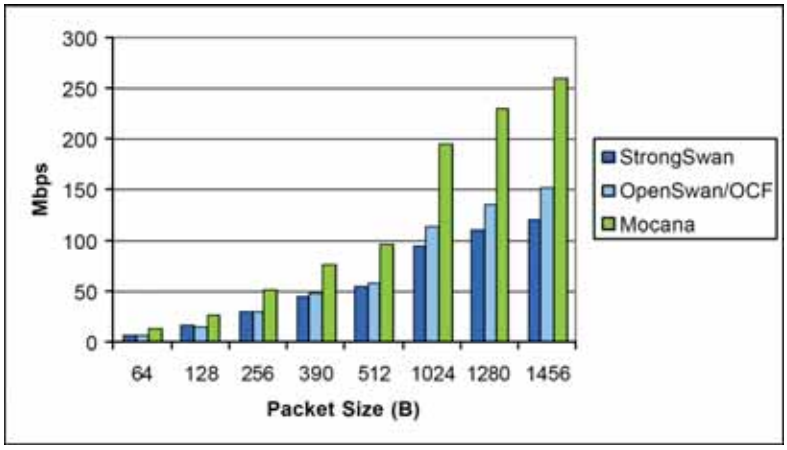

Figura 7. Test de rendimiento IPsec en MPC8313E

Las prestaciones en aceleradores Look-aside podrían verse comprometidas si no hubiese suficiente ancho de banda disponible para mantener al SEC plenamente utilizado. Es por ello que en la implementación utilizada en los PowerQUICC, el SEC esta conectado de forma permanente al bus para minimizar el la posibilidad de falta del acceso al bus por parte del cripto procesador.

Medidas de prestaciones criptográficas

Las prestaciones criptográficas pueden ser medidas a nivel del driver (mediante el uso de una rutina de test encriptando o desencriptando una matriz de datos aleatorio y el uso de una clave aleatoria).

La metodología utilizada en este caso, donde se han utilizado dos tarjetas MPC8313E RDB, ha sido mediante el uso de dos Smartbits SMB600, uno para la generación de paquetes y el segundo para su recepción y conteo. Se generan paquetes IPv4 en claro, a máxima velocidad y son dirigidos a uno de los puertos Ethernet de la primera tarjeta MPC8313E RDB. Ésta determina si el paquete deber ser encriptado de acuerdo a una sesión IPsec, realiza su encapsulación securizada de acuerdo al algoritmo 3DES-HMAC-SHA-1 (al ser este el más comúnmente utilizado) antes de mandarlo a través de un puerto Ethernet a una segunda tarjeta. Ésta lo recibe, clasifica la información tras comprobar que se trata de una sesión IPsec, desencapsula y descifra la información y enruta de nuevo la información en claro vía Ethernet al Smartbits.

En la figura 7 se muestra las prestaciones medidas en procesador PowerQUICC MPC8313E, de acuerdo al siguiente set up:

- 2x MPC8313E RDB
- e300 ejecutando a 333 MHz, DDR a 333 MHz, y procesador criptográfico SEC a 166 MHz
- SO: Linux 2.6.21
- IPsec Stacks: StrongSwan, OpenSwan, Mocana, todos ejecutando 3DES-HMAC-SHA-1

En ella se puede apreciar que el Stack IPsec de Mocana tiene un rendimiento superior que el resto en cualquier tamaño de paquete de datos: en torno a 1.7x frente a OpenSwan, y entre 1.6 y 2.2x superior a StrongSwan.

Conclusión

En el artículo se han descrito las claves del uso de criptografía aplicada a aplicaciones de comunicaciones. En él se han explicado los diferentes tipos de aceleradores que pueden utilizarse para descargar a la CPU de proceso y acelerar los procesos criptográficos. Se describen los aspectos que mayor influencia tienen en dichos aceleradores, particularizando para el caso de aceleradores Look-aside como los utilizados en los procesadores PowerQUICC de Freescale, además de resaltar la principal ventaja aportada: flexibilidad. Por último, se particulariza para el caso del procesador MPC8313E. Las prestaciones de seguridad alcanzadas gracias al uso de aceleradores de seguridad integrados descritos en el artículo proporcionan un complemento equilibrado con la relación de coste/prestaciones de la familia PowerQUICC de Freescale. Para más información, visite www.freescale.com/networking o consulte con la red de distribuidores de Freescale.