Crypto DR Domain Services Specification

Revision 1.0

April 28, 2008

Gary Morton

1 Crypto DR

The ability to dynamically add or remove hardware crypto providers from a logical domain is driven from the LDOM manager through this domain service. Separate services will be defined for the Modular Arithmetic Unit (MAU) and the Control Word Queue (CWQ) hardware components.

1.1 Service ID

The following service IDs should be added to the Domain Services registry for the Crypto DR service.

Service ID	Description
"dr-crypto-mau"	Dynamic reconfiguration for MAU
"dr-crypto-cwq"	Dynamic reconfiguration for CWQ

The same DR service messages will be used for both services. Each message will consist of a fixed message header and payload as described below. Overall, the Crypto DR service messages will be very similar to the CPU DR messages.

1.2 Crypto DR Message Header

All Crypto DR messages begin with the same header. The payload that follows the header is specific to a particular message type.

Offset	Size	Field Name	Description
0	8	req_num	Request number
8	4	msg_type	Message type
12	4	num_records	Number of records

The Crypto DR protocol consists of a command sent to the client guest which then responds with a reply indicating the success or failure of the request.

1.3 Crypto DR Message Types

The following message types are defined for the Crypto DR domain service:

- Request messages

Type	Value	ASCII	Definition
DR_CRYPTO_CONFIG	0x43	'C'	configure new crypto unit
DR_CRYPTO_UNCONFIG	0x55	'U'	unconfigure crypto unit
DR_CRYPTO_FORCE_UNCONFIG	0x46	'F'	forcibly unconfigure crypto unit
DR_CRYPTO_STATUS	0x53	'S'	Request status for a crypto unit

- Response messages

Type	Value	ASCII	Definition
DR_CRYPTO_OK	0x6f	'o'	Request completed ok
DR_CRYPTO_ERROR	0x65	'e'	Request failed

1.3.1 Crypto DR Request Payload

The Crypto DR requests all use the same payload format, which is a list of records of virtual CPU IDs within a guest. Because there is no crypto unit ID defined in the guest, a virtual CPU ID which maps to the desired crypto unit is passed as the identifier. There should be one virtual CPU ID specified per targeted crypto unit.

The payload is as follows:

Offset	Size	Field name	Description
0	4	id0	Virtual CPU ID
4	4	id1	Virtual CPU ID
8	4	id2	Virtual CPU ID
			... etc.

1.3.2 Request Number

The request number is a monotonically increasing value that uniquely identifies each request. Responses to requests are expected to use the same request number so they can be paired with the original request. Requests are to be processed in the order received.

1.3.3 DR_CRYPTO_CONFIG request

This command requests that a guest attempt to configure and bring online the crypto units associated with the set of virtual CPU ID supplied in the request message. In order to be successful, the crypto unit and associated virtual CPUs must already exist in the guest's Machine Description (MD). If both of these conditions are not satisfied, an error is returned.

1.3.4 DR_CRYPTO_UNCONFIG request

This command requests that the guest attempt to offline and unconfigure the targeted crypto units. An associated virtual CPU ID is supplied in the request message to identify the crypto unit. In order to be successful, the crypto unit and associated virtual CPUs must already exist in the guest's Machine Description (MD). If both of these conditions are not satisfied, an error is returned.

1.3.5 DR_CRYPTO_FORCE_UNCONFIG request

This command requests that the guest forcibly attempt to offline and unconfigure the targeted crypto units. However, there is no still guarantee that the guest will be able to successfully complete the request.

1.3.6 DR_CRYPTO_STATUS

The command requests the configuration status for specific crypto units.

1.3.7 DR CRYPTO OK response payload

The DR CRYPTO OK response uses the following format. The response header is followed by an array of status reports, one for each crypto unit targeted in the command request. Each status report provides information on the result of the requested operation. Because there is no crypto unit ID, the virtual CPU ID is carried in the status report.

The crypto unit status reports have the following format:

Offset	Size	Field name	Description
0	4	cpuid	Virtual CPU ID

4	4	result	Result of the operation
8	4	status	Status of the crypto unit

1.3.8 DR CRYPTO OK result codes

The result field in the per crypto unit response record conveys the result of the requested operation for that crypto unit. The result codes are defined as follows:

Name	Value	Definition
DR_CRYPTO_RES_OK	0x0	Operation succeeded
DR_CRYPTO_RES_FAILURE	0x1	Operation failed
DR_CRYPTO_RES_BAD_CPU	0x2	CPU not in MD
DR_CRYPTO_RES_BAD_CRYPTO	0x3	Crypto unit not in MD

1.3.9 DR CRYPTO OK status codes

The status field in the per crypto unit response record conveys the configuration status for the targeted crypto unit. The status codes are defined as follows:

Name	Value	Definition
DR_CRYPTO_STAT_NOT_PRESENT	0x0	Crypto unit not in MD
DR_CRYPTO_STAT_UNCONFIGURED	0x1	Crypto unit is not configured
DR_CRYPTO_STAT_CONFIGURED	0x2	Crypto unit is configured

1.3.10 DR Crypto Error Response

The message type DR_CRYPTO_ERROR is returned as the response to a malformed request message. No additional payload is provided.

1.4 Operational Overview

1.4.1 Offlining a Crypto Unit

When the LDOM manager decides to offline a crypto unit (or multiple crypto units), it will build DR_CRYPTO_UNCONFIG domain service messages, including a list of virtual CPU IDs, each associated with the specific crypto unit being taken offline. This message must be sent and acknowledged in advance of any change to the machine description.

The domain service peers in the guest must guarantee that all jobs have completed for that crypto unit and that no additional work will be scheduled before responding successfully.

1.4.2 Onlining a Crypto Unit

When the LDOM manager decides to online a crypto unit, if it is a new crypto unit, the guest must first get an MD update which includes information about the new crypto unit. Once that has occurred, the LDOM manager will build DR_CRYPTO_CONFIG domain service messages, including a list of virtual CPU IDs, each associated with the specific crypto unit being brought online.

The domain service peers in the guest will re-read the MD and configure in the new crypto unit based on the virtual CPU IDs included in the DR_CRYPTO_CONFIG message payload. Once the configuration has completed, the response will be returned to the LDOM manager.