GetInfo

MakeCredentia

Host requests Device to report

Host requests gener

MSG	CBOR	INIT	PING	CANCEL	ERROR	KEEPALIVE	WINK	LOCK
No need to implement as the CTAPHID_MSG Command is for Backward Compatibility with U2F Devices	Receive the CBOR encoded message. Feed it to the CBOR decoder and then execute the encapsulated CTAP2 Command	Handle the INIT Command. Respond with the 8-bye Nonce, the 4-byte Channel ID and other metadata.	Echo back the n-byte payload to the client with the same command.	Requested by the Client to Cancel any outstanding requests on the active Channel ID.	Used by Authenticator to relay any and all Error Messages.	Used for indicating device is active while processing a CTAPHID_MSG command. No need to implement.	For Visual/Audible identification of a particular Authenticator device, when more than one device is attached to the client.	Places an exclusive lock for one channel to communicate with the device. Maximum locking duration is 10 seconds.

al	GetAssertion	GetNextAssertion	ClientPIN	
ration of a	Host requests cryptographic	Client uses this command to obtain the next per-credential	Host sends PIN to Device in	Host requ

Cancel

Reset

ate the Authenticator

Used by the client to reset an

Host requests Device to report version, extension, ID and capabilities

NO INPUT

versions
extensions
aaguid
options
maxMsgSize
pinProtocols

Host requests gener
new credential i
authenticato

clientDataHash
rp
user
pubKeyCredParams
excludeList
extensions
options
pinAuth
pinProtocol

ration of a n the or.	proof of user authentication as well as user consent to a given transaction.	obtain the next per-credential signature for a given authenticatorGetAssertion request.	Host sends PIN to Device in encrypted format while setting or changing a PIN.		Host reque to cancel a are retu	
authData fmt attSmt	rpId clientDataHash allowList extensions options pinAuth pinProtocol	credential authData signature user numberOfCredentials	NO INPUT	credential authData signature user	Get Retries Get Key Agreement Set PIN Change PIN Get PIN token	NO INPUT
					pinProtocol subCommand keyAgreement pinAuth newPinEnc pinHashEnc getKeyAgreement getRetries	KeyAgreement pinToken retries

ests the Authenticator
ll ongoing operations
rn to a ready state

Used by the client to reset an authenticator back to a factory default state

success/failure

NO INPUT

NO OUTPUT