

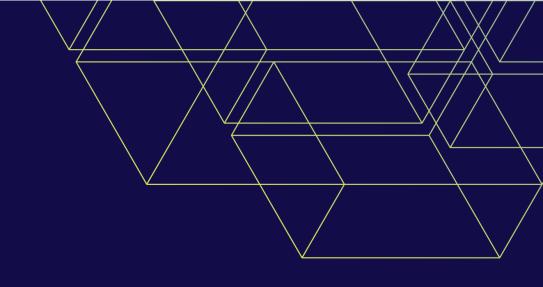
Storage Developer Conference September 22-23, 2020

**Securing SMB3 over RDMA** 

Wen Xin Microsoft Corp.

#### **Overview**

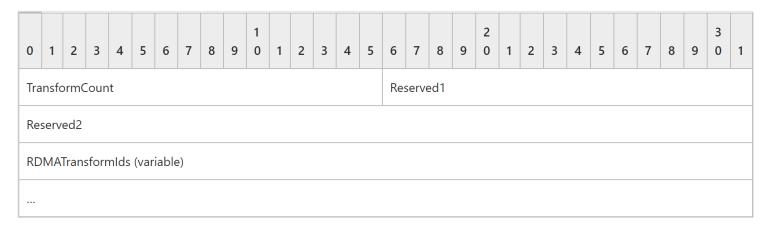
- Crypto transform over direct data placement.
- RDMA Encryption
  - Shipped in Mn (20H1) release.
  - Includes 256-bit AES algorithms.
- RDMA Signing
  - Feature complete.
  - Includes AES-GMAC algorithm.



# **Protocol Updates**

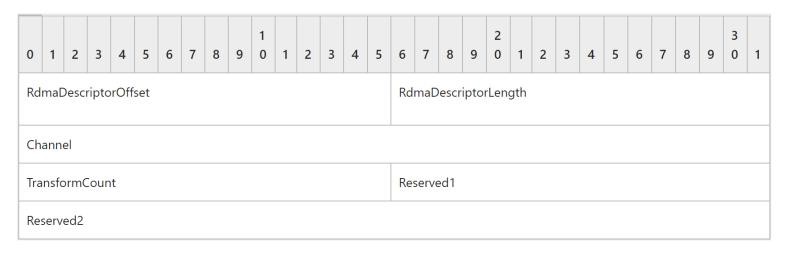
### **Protocol Update - Negotiate**

#### RDMA\_TRANSFORM\_CAPABILITIES



### **Protocol Update – RDMA Channel**

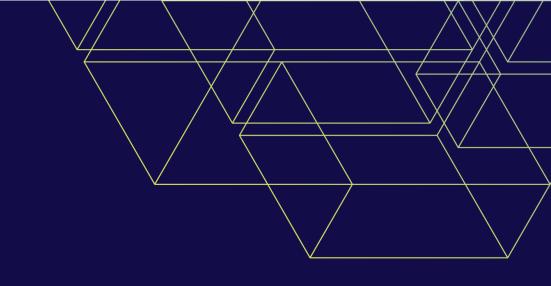
SMB2\_CHANNEL\_RDMA\_TRANSFORM



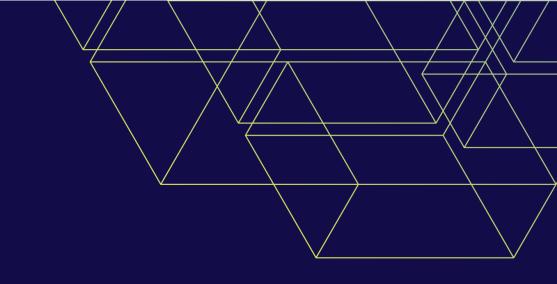
## **Protocol Update – RDMA Encryption**

SMB2\_CHANNEL\_RDMA\_TRANSFORM

0	1	2	3	4	5	6	7	8	9	1	1	2	3	4	5	6	7	8	9	2	1	2	3	4	5	6	7	8	9	3	1
Tra	TransformType S														SignatureLength																
No	NonceLength F														Reserved																
Signature (variable)																															
Reserved1																															
No	Nonce (variable)																														
Pad	ddin	g (va	ariab	ole)																											



#### **Performance**



## Demo