

Envelope	InitHello	RespHello	InitConf																																																																																																																																
<p>bytes</p> <table border="1"> <tr> <td>COOKIE_WIRE_DATA</td><td></td><td></td><td></td></tr> <tr> <td>type</td><td>1</td><td></td><td></td></tr> <tr> <td>reserved</td><td>3</td><td></td><td></td></tr> <tr> <td>payload</td><td>n</td><td></td><td></td></tr> <tr> <td>mac</td><td>16</td><td></td><td></td></tr> <tr> <td>cookie</td><td>16</td><td></td><td></td></tr> <tr> <td></td><td></td><td></td><td></td></tr> <tr> <td>envelope</td><td>$n + 36$</td><td></td><td></td></tr> </table>	COOKIE_WIRE_DATA				type	1			reserved	3			payload	n			mac	16			cookie	16							envelope	$n + 36$			<p>type=0x81</p> <table border="1"> <tr> <td>sidi</td><td>4</td><td></td><td></td></tr> <tr> <td>epki</td><td>800</td><td></td><td></td></tr> <tr> <td>sctr</td><td>188</td><td></td><td></td></tr> <tr> <td>pidiC</td><td>$32 + 16 = 48$</td><td></td><td></td></tr> <tr> <td>auth</td><td>16</td><td></td><td></td></tr> <tr> <td></td><td></td><td></td><td></td></tr> <tr> <td>payload</td><td>1056</td><td></td><td></td></tr> <tr> <td>+ envelope</td><td>1092</td><td></td><td></td></tr> </table>	sidi	4			epki	800			sctr	188			pidiC	$32 + 16 = 48$			auth	16							payload	1056			+ envelope	1092			<p>type=0x82</p> <table border="1"> <tr> <td>sidi</td><td>4</td><td></td><td></td></tr> <tr> <td>sidi</td><td>4</td><td></td><td></td></tr> <tr> <td>ecti</td><td>768</td><td></td><td></td></tr> <tr> <td>scti</td><td>188</td><td></td><td></td></tr> <tr> <td>biscuit</td><td>$76 + 24 + 16 = 116$</td><td></td><td></td></tr> <tr> <td>auth</td><td>16</td><td></td><td></td></tr> <tr> <td></td><td></td><td></td><td></td></tr> <tr> <td>payload</td><td>1096</td><td></td><td></td></tr> <tr> <td>+ envelope</td><td>1132</td><td></td><td></td></tr> </table>	sidi	4			sidi	4			ecti	768			scti	188			biscuit	$76 + 24 + 16 = 116$			auth	16							payload	1096			+ envelope	1132			<p>type=0x83</p> <table border="1"> <tr> <td>sidi</td><td>4</td><td></td><td></td></tr> <tr> <td>sidi</td><td>4</td><td></td><td></td></tr> <tr> <td>biscuit</td><td>$76 + 24 + 16 = 116$</td><td></td><td></td></tr> <tr> <td>auth</td><td>16</td><td></td><td></td></tr> <tr> <td></td><td></td><td></td><td></td></tr> <tr> <td>payload</td><td>140</td><td></td><td></td></tr> <tr> <td>+ envelope</td><td>176</td><td></td><td></td></tr> </table>	sidi	4			sidi	4			biscuit	$76 + 24 + 16 = 116$			auth	16							payload	140			+ envelope	176		
COOKIE_WIRE_DATA																																																																																																																																			
type	1																																																																																																																																		
reserved	3																																																																																																																																		
payload	n																																																																																																																																		
mac	16																																																																																																																																		
cookie	16																																																																																																																																		
envelope	$n + 36$																																																																																																																																		
sidi	4																																																																																																																																		
epki	800																																																																																																																																		
sctr	188																																																																																																																																		
pidiC	$32 + 16 = 48$																																																																																																																																		
auth	16																																																																																																																																		
payload	1056																																																																																																																																		
+ envelope	1092																																																																																																																																		
sidi	4																																																																																																																																		
sidi	4																																																																																																																																		
ecti	768																																																																																																																																		
scti	188																																																																																																																																		
biscuit	$76 + 24 + 16 = 116$																																																																																																																																		
auth	16																																																																																																																																		
payload	1096																																																																																																																																		
+ envelope	1132																																																																																																																																		
sidi	4																																																																																																																																		
sidi	4																																																																																																																																		
biscuit	$76 + 24 + 16 = 116$																																																																																																																																		
auth	16																																																																																																																																		
payload	140																																																																																																																																		
+ envelope	176																																																																																																																																		

EmptyData	Data	CookieReply	biscuit																																																																																																								
<p>type=0x84</p> <table border="1"> <tr> <td>sid</td><td>4</td><td></td><td></td></tr> <tr> <td>ctr</td><td>8</td><td></td><td></td></tr> <tr> <td>auth</td><td>16</td><td></td><td></td></tr> <tr> <td></td><td></td><td></td><td></td></tr> <tr> <td>payload</td><td>28</td><td></td><td></td></tr> <tr> <td>+ envelope</td><td>64</td><td></td><td></td></tr> </table>	sid	4			ctr	8			auth	16							payload	28			+ envelope	64			<p>type=0x85</p> <table border="1"> <tr> <td>sid</td><td>4</td><td></td><td></td></tr> <tr> <td>ctr</td><td>8</td><td></td><td></td></tr> <tr> <td>data</td><td>variable + 16</td><td></td><td></td></tr> <tr> <td></td><td></td><td></td><td></td></tr> <tr> <td>payload</td><td>variable + 28</td><td></td><td></td></tr> <tr> <td>+ envelope</td><td>variable + 64</td><td></td><td></td></tr> </table>	sid	4			ctr	8			data	variable + 16							payload	variable + 28			+ envelope	variable + 64			<p>type=0x86</p> <table border="1"> <tr> <td>type(0x86)</td><td>1</td><td></td><td></td></tr> <tr> <td>reserved</td><td>3</td><td></td><td></td></tr> <tr> <td>sid</td><td>4</td><td></td><td></td></tr> <tr> <td>nonce</td><td>24</td><td></td><td></td></tr> <tr> <td>cookie</td><td>$16 + 16 = 32$</td><td></td><td></td></tr> <tr> <td></td><td></td><td></td><td></td></tr> <tr> <td>payload</td><td>64</td><td></td><td></td></tr> </table>	type(0x86)	1			reserved	3			sid	4			nonce	24			cookie	$16 + 16 = 32$							payload	64			<table border="1"> <tr> <td>pidi</td><td>32</td><td></td><td></td></tr> <tr> <td>biscuit_no</td><td>12</td><td></td><td></td></tr> <tr> <td>ck</td><td>32</td><td></td><td></td></tr> <tr> <td></td><td></td><td></td><td></td></tr> <tr> <td>biscuit</td><td>76</td><td></td><td></td></tr> <tr> <td>+ nonce</td><td>100</td><td></td><td></td></tr> <tr> <td>+ auth code</td><td>116</td><td></td><td></td></tr> </table> <p>data nonce auth code</p>	pidi	32			biscuit_no	12			ck	32							biscuit	76			+ nonce	100			+ auth code	116		
sid	4																																																																																																										
ctr	8																																																																																																										
auth	16																																																																																																										
payload	28																																																																																																										
+ envelope	64																																																																																																										
sid	4																																																																																																										
ctr	8																																																																																																										
data	variable + 16																																																																																																										
payload	variable + 28																																																																																																										
+ envelope	variable + 64																																																																																																										
type(0x86)	1																																																																																																										
reserved	3																																																																																																										
sid	4																																																																																																										
nonce	24																																																																																																										
cookie	$16 + 16 = 32$																																																																																																										
payload	64																																																																																																										
pidi	32																																																																																																										
biscuit_no	12																																																																																																										
ck	32																																																																																																										
biscuit	76																																																																																																										
+ nonce	100																																																																																																										
+ auth code	116																																																																																																										