	P192 K163 B163	P224 K233 B233	P256 K283 B283	P384 K409 B409	P521 K571 B571
Hash algorithm	SHA-1	SHA-224	SHA-256	SHA-384	SHA-512
Hash length	160	224	256	384	512
KDF	Concatenation KDF				
Derived Key Material length	320	448	512	768	1024
MacKey length	80	112	128	192	256
MacTag length	160	224	256	384	512
ID_U	"ALICE"				
ID_V	"BOBBY"				
Message Strings (Unilateral)	KC_1_U KC_1_V				
Message Strings (Bilateral)	KC_2_U KC_2_V				

OtherInfo for KDF

AlgorithmID	123456789ABCDEF0
PartyUInfo	414C494345313233
PartyVInfo	424F424259343536
SupPubInfo	not used

OtherInfo for KDF (StaticUnifiedModel) requires the PartyUInfo to contain a nonce therefore the value is:

PartyUInfo = 414C494345313233 || nonceU_byte_len || nonceU

FullUnifiedCDH(P-192)
---
dsU is
        20F234D3 2CD7EDD8 BFC5BD96 DAE60859 3E38E894 2324FDE8

QsU_x is
        896C0B5E E70F55B3 B463101C 1BFB86D3 A7C6C5DA 354F6214

QsU_y is
        40B85F14 4536C6F5 4BC85BED 3820A74A BF58BC78 2D1DB241

dsV is
        0F9E539A E24C3A90 5B4ED7CE 4E2EBAD4 E4B77491 2623284B

QsV_x is
        09F9D21C 7FD98D09 7B4C3AE7 64300040 3DB445B7 49C4B441

QsV_y is
        43CB6933 62FD117C 79F255D9 DD6BBE75 F43BE57D 14E28685

deU is
        323FA316 9D8E9C65 93F59476 BC142000 AB5BE0E2 49C43426

QeU_x is
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612

QeU_y is
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A

deV is
        631F95BB 4A67632C 9C476EEE 9AB695AB 240A0499 307FCF62

QeV_x is
        519A1216 80E00454 66BA21DF 2EEE47F5 973B5005 77EF13D5

QeV_y is
        FF613AB4 D64CEE3A 20875BDB 10F953F6 B30CA072 C60AA57F

---

no Key Confirmation
Zs is
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D

Ze is
        AD420182 633F8526 BFE954AC DA376F05 E5FF4F83 7F54FEBE

Z is
        AD420182 633F8526 BFE954AC DA376F05 E5FF4F83 7F54FEBE
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
                         6FEF442F C17A7E2B 0C9DECE0 E47A5748
        ACB46AF1 98D76747 0F28A104 B56130AE B01009A4 5682A5E1

KeyData is
                         6FEF442F C17A7E2B 0C9DECE0 E47A5748
        ACB46AF1 98D76747 0F28A104 B56130AE B01009A4 5682A5E1

Scheme Initiator, Key Confirmation Provider: U to V
Zs is
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D

Ze is

```
        AD420182 633F8526 BFE954AC DA376F05 E5FF4F83 7F54FEBE


Z is
        AD420182 633F8526 BFE954AC DA376F05 E5FF4F83 7F54FEBE
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                            6FEF
        442FC17A 7E2B0C9D ECE0E47A 5748ACB4 6AF198D7 67470F28
        A104B561 30AEB010 09A45682 A5E17D62 1894ADB8 ADDCFE57


MacData is
                         4B435F31 5F55414C 49434542 4F424259
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A
        519A1216 80E00454 66BA21DF 2EEE47F5 973B5005 77EF13D5
        FF613AB4 D64CEE3A 20875BDB 10F953F6 B30CA072 C60AA57F


MacKey is
                                       6FEF 442FC17A 7E2B0C9D


Mtag is
                 9FC2821F 2F0314E6 7D4ED678 F9F53409 E50F0B6C


KeyData is
                         ECE0E47A 5748ACB4 6AF198D7 67470F28
        A104B561 30AEB010 09A45682 A5E17D62 1894ADB8 ADDCFE57




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
Zs is
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D
```

```
Ze is
        AD420182 633F8526 BFE954AC DA376F05 E5FF4F83 7F54FEBE


Z is
        AD420182 633F8526 BFE954AC DA376F05 E5FF4F83 7F54FEBE
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                            6FEF
        442FC17A 7E2B0C9D ECE0E47A 5748ACB4 6AF198D7 67470F28
        A104B561 30AEB010 09A45682 A5E17D62 1894ADB8 ADDCFE57


MacData is
                         4B435F31 5F56424F 42425941 4C494345
        519A1216 80E00454 66BA21DF 2EEE47F5 973B5005 77EF13D5
        FF613AB4 D64CEE3A 20875BDB 10F953F6 B30CA072 C60AA57F
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A


MacKey is
                                       6FEF 442FC17A 7E2B0C9D


Mtag is
                 8CFF7B69 2AD54B6E 72310512 31EC449D 177B75B5


KeyData is
                         ECE0E47A 5748ACB4 6AF198D7 67470F28
        A104B561 30AEB010 09A45682 A5E17D62 1894ADB8 ADDCFE57




------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
Zs is
```

```
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D


Ze is
        AD420182 633F8526 BFE954AC DA376F05 E5FF4F83 7F54FEBE


Z is
        AD420182 633F8526 BFE954AC DA376F05 E5FF4F83 7F54FEBE
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                            6FEF
        442FC17A 7E2B0C9D ECE0E47A 5748ACB4 6AF198D7 67470F28
        A104B561 30AEB010 09A45682 A5E17D62 1894ADB8 ADDCFE57


U2V
----------------
MacData is
                          4B435F32 5F55414C 49434542 4F424259
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A
        519A1216 80E00454 66BA21DF 2EEE47F5 973B5005 77EF13D5
        FF613AB4 D64CEE3A 20875BDB 10F953F6 B30CA072 C60AA57F


MacKey is
                                       6FEF 442FC17A 7E2B0C9D


Mtag is
                0C095ACF 86073288 9A1AE24E E016A615 0DEEC052


V2U
----------------
MacData is
                          4B435F32 5F56424F 42425941 4C494345
        519A1216 80E00454 66BA21DF 2EEE47F5 973B5005 77EF13D5
        FF613AB4 D64CEE3A 20875BDB 10F953F6 B30CA072 C60AA57F
```

CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612
68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A

MacKey is
6FEF 442FC17A 7E2B0C9D

Mtag is
5A0177D4 BF7EA587 E1A463BC 8A621FE8 F1DAAF5E

KeyData is
ECE0E47A 5748ACB4 6AF198D7 67470F28
A104B561 30AEB010 09A45682 A5E17D62 1894ADB8 ADDCFE57

FullMQV(P-192)
---
dsU is
20F234D3 2CD7EDD8 BFC5BD96 DAE60859 3E38E894 2324FDE8

QsU_x is
896C0B5E E70F55B3 B463101C 1BFB86D3 A7C6C5DA 354F6214

QsU_y is
40B85F14 4536C6F5 4BC85BED 3820A74A BF58BC78 2D1DB241

dsV is
0F9E539A E24C3A90 5B4ED7CE 4E2EBAD4 E4B77491 2623284B

QsV_x is
09F9D21C 7FD98D09 7B4C3AE7 64300040 3DB445B7 49C4B441

QsV_y is
43CB6933 62FD117C 79F255D9 DD6BBE75 F43BE57D 14E28685

deU is

```
        323FA316 9D8E9C65 93F59476 BC142000 AB5BE0E2 49C43426


QeU_x is
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612


QeU_y is
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A


deV is
        631F95BB 4A67632C 9C476EEE 9AB695AB 240A0499 307FCF62


QeV_x is
        519A1216 80E00454 66BA21DF 2EEE47F5 973B5005 77EF13D5


QeV_y is
        FF613AB4 D64CEE3A 20875BDB 10F953F6 B30CA072 C60AA57F




------------------------------------------------------------
no Key Confirmation
Z is
        AE64AB2B 2B75A94C F8EF24DA 2456BD3A A36DB614 29EA5521


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                         CC965A52 D05C949E 52C035FD 03530DB7
        EAA40870 2C9D3521 1E672154 12459151 BA2262BD 1E28E56B


KeyData is
                         CC965A52 D05C949E 52C035FD 03530DB7
        EAA40870 2C9D3521 1E672154 12459151 BA2262BD 1E28E56B
```

```
-----------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
Z is
        AE64AB2B 2B75A94C F8EF24DA 2456BD3A A36DB614 29EA5521


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                          CC96
        5A52D05C 949E52C0 35FD0353 0DB7EAA4 08702C9D 35211E67
        21541245 9151BA22 62BD1E28 E56BC8BB 2271AEE7 295E6A21


MacData is
                         4B435F31 5F55414C 49434542 4F424259
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A
        519A1216 80E00454 66BA21DF 2EEE47F5 973B5005 77EF13D5
        FF613AB4 D64CEE3A 20875BDB 10F953F6 B30CA072 C60AA57F


MacKey is
                                      CC96 5A52D05C 949E52C0


Mtag is
                 BE70E818 DBCCECBD A421D5B7 DA5F0EE9 CDD62A9A


KeyData is
                         35FD0353 0DB7EAA4 08702C9D 35211E67
        21541245 9151BA22 62BD1E28 E56BC8BB 2271AEE7 295E6A21




-----------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
Z is
        AE64AB2B 2B75A94C F8EF24DA 2456BD3A A36DB614 29EA5521
```

```
OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                            CC96
        5A52D05C 949E52C0 35FD0353 0DB7EAA4 08702C9D 35211E67
        21541245 9151BA22 62BD1E28 E56BC8BB 2271AEE7 295E6A21


MacData is
                         4B435F31 5F56424F 42425941 4C494345
        519A1216 80E00454 66BA21DF 2EEE47F5 973B5005 77EF13D5
        FF613AB4 D64CEE3A 20875BDB 10F953F6 B30CA072 C60AA57F
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A


MacKey is
                                      CC96 5A52D05C 949E52C0


Mtag is
                 9A20EA41 CE077751 1D774AC0 C3FC896E 9A5FA16E


KeyData is
                         35FD0353 0DB7EAA4 08702C9D 35211E67
        21541245 9151BA22 62BD1E28 E56BC8BB 2271AEE7 295E6A21




-----------------------------------------------------------

Scheme Initiator, Key Confirmation Bilateral
Z is
        AE64AB2B 2B75A94C F8EF24DA 2456BD3A A36DB614 29EA5521


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                            CC96
```

```
        5A52D05C 949E52C0 35FD0353 0DB7EAA4 08702C9D 35211E67
        21541245 9151BA22 62BD1E28 E56BC8BB 2271AEE7 295E6A21


U2V
----------------
MacData is
                         4B435F32 5F55414C 49434542 4F424259
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A
        519A1216 80E00454 66BA21DF 2EEE47F5 973B5005 77EF13D5
        FF613AB4 D64CEE3A 20875BDB 10F953F6 B30CA072 C60AA57F


MacKey is
                                       CC96 5A52D05C 949E52C0


Mtag is
                6C5F6913 A3BF1F7F 16386259 5C50B64B A3DE1A72


V2U
----------------
MacData is
                         4B435F32 5F56424F 42425941 4C494345
        519A1216 80E00454 66BA21DF 2EEE47F5 973B5005 77EF13D5
        FF613AB4 D64CEE3A 20875BDB 10F953F6 B30CA072 C60AA57F
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A


MacKey is
                                       CC96 5A52D05C 949E52C0


Mtag is
                B79F0184 B82652A0 E7AB0B68 2956AB3B 2330F57B


KeyData is
                         35FD0353 0DB7EAA4 08702C9D 35211E67
        21541245 9151BA22 62BD1E28 E56BC8BB 2271AEE7 295E6A21
```

EphemeralUnifiedCDH(P-192)
---
deU is
        323FA316 9D8E9C65 93F59476 BC142000 AB5BE0E2 49C43426

QeU_x is
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612

QeU_y is
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A

deV is
        631F95BB 4A67632C 9C476EEE 9AB695AB 240A0499 307FCF62

QeV_x is
        519A1216 80E00454 66BA21DF 2EEE47F5 973B5005 77EF13D5

QeV_y is
        FF613AB4 D64CEE3A 20875BDB 10F953F6 B30CA072 C60AA57F

---
no Key Confirmation
Z is
        AD420182 633F8526 BFE954AC DA376F05 E5FF4F83 7F54FEBE

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
                          5F17B665 72C57B03 34BB241C E6CB3A9D
        585E5C36 257DC087 5DEE4843 56E92FAB CCE2D388 ABF7EAF0

KeyData is
                          5F17B665 72C57B03 34BB241C E6CB3A9D

585E5C36 257DC087 5DEE4843 56E92FAB CCE2D388 ABF7EAF0

OnePassUnifiedCDH(P-192)
---
dsU is
20F234D3 2CD7EDD8 BFC5BD96 DAE60859 3E38E894 2324FDE8

QsU_x is
896C0B5E E70F55B3 B463101C 1BFB86D3 A7C6C5DA 354F6214

QsU_y is
40B85F14 4536C6F5 4BC85BED 3820A74A BF58BC78 2D1DB241

dsV is
0F9E539A E24C3A90 5B4ED7CE 4E2EBAD4 E4B77491 2623284B

QsV_x is
09F9D21C 7FD98D09 7B4C3AE7 64300040 3DB445B7 49C4B441

QsV_y is
43CB6933 62FD117C 79F255D9 DD6BBE75 F43BE57D 14E28685

deU is
323FA316 9D8E9C65 93F59476 BC142000 AB5BE0E2 49C43426

QeU_x is
CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612

QeU_y is
68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A

```
no Key Confirmation
Zs is
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D


Ze is
        78B3A426 67DFF154 E395367B 744CBB50 67C03D08 A96D9086


Z is
        78B3A426 67DFF154 E395367B 744CBB50 67C03D08 A96D9086
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                         73D683F6 751BC092 B68F8DB2 45FBBCF8
        74A1EF99 B15E85C1 5097D9EC 246869A2 DDC8083B 52BA25FC


KeyData is
                         73D683F6 751BC092 B68F8DB2 45FBBCF8
        74A1EF99 B15E85C1 5097D9EC 246869A2 DDC8083B 52BA25FC




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
        F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309


Zs is
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D


Ze is
        78B3A426 67DFF154 E395367B 744CBB50 67C03D08 A96D9086


Z is
        78B3A426 67DFF154 E395367B 744CBB50 67C03D08 A96D9086
```

```
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                            73D6
        83F6751B C092B68F 8DB245FB BCF874A1 EF99B15E 85C15097
        D9EC2468 69A2DDC8 083B52BA 25FC5032 25D8C464 84EA6B82


MacData is
                          4B435F31 5F55414C 49434542 4F424259
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A
        F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309


MacKey is
                                       73D6 83F6751B C092B68F


Mtag is
                 78C36193 A4ED0347 F8791C75 0DBB3360 E3691BBD


KeyData is
                          8DB245FB BCF874A1 EF99B15E 85C15097
        D9EC2468 69A2DDC8 083B52BA 25FC5032 25D8C464 84EA6B82




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
NonceU is
        F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309


Zs is
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D


Ze is
```

```
        78B3A426 67DFF154 E395367B 744CBB50 67C03D08 A96D9086


Z is
        78B3A426 67DFF154 E395367B 744CBB50 67C03D08 A96D9086
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                            73D6
        83F6751B C092B68F 8DB245FB BCF874A1 EF99B15E 85C15097
        D9EC2468 69A2DDC8 083B52BA 25FC5032 25D8C464 84EA6B82


MacData is
                          4B435F31 5F56424F 42425941 4C494345
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A


MacKey is
                                       73D6 83F6751B C092B68F


Mtag is
                 93439CD1 94CAEB81 3ECEEFFF D8FC8A5F 9D8BD4E5


KeyData is
                          8DB245FB BCF874A1 EF99B15E 85C15097
        D9EC2468 69A2DDC8 083B52BA 25FC5032 25D8C464 84EA6B82




------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
NonceV is
        F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309


Zs is
```

```
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D


Ze is
        78B3A426 67DFF154 E395367B 744CBB50 67C03D08 A96D9086


Z is
        78B3A426 67DFF154 E395367B 744CBB50 67C03D08 A96D9086
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                            73D6
        83F6751B C092B68F 8DB245FB BCF874A1 EF99B15E 85C15097
        D9EC2468 69A2DDC8 083B52BA 25FC5032 25D8C464 84EA6B82


U2V
----------------
MacData is
                         4B435F32 5F55414C 49434542 4F424259
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A
        F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309


MacKey is
                                       73D6 83F6751B C092B68F


Mtag is
                C12D5D7E 9318520B 9143CEF0 600D1E2E 1BD2C06D


V2U
----------------
MacData is
                         4B435F32 5F56424F 42425941 4C494345
        F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A
```

MacKey is
                                        73D6 83F6751B C092B68F

Mtag is
                33550A01 43DA603D E0843426 378CEDD0 E6D49C69

KeyData is
                          8DB245FB BCF874A1 EF99B15E 85C15097
        D9EC2468 69A2DDC8 083B52BA 25FC5032 25D8C464 84EA6B82

OnePassMQV(P-192)
----
dsU is
        20F234D3 2CD7EDD8 BFC5BD96 DAE60859 3E38E894 2324FDE8

QsU_x is
        896C0B5E E70F55B3 B463101C 1BFB86D3 A7C6C5DA 354F6214

QsU_y is
        40B85F14 4536C6F5 4BC85BED 3820A74A BF58BC78 2D1DB241

dsV is
        0F9E539A E24C3A90 5B4ED7CE 4E2EBAD4 E4B77491 2623284B

QsV_x is
        09F9D21C 7FD98D09 7B4C3AE7 64300040 3DB445B7 49C4B441

QsV_y is
        43CB6933 62FD117C 79F255D9 DD6BBE75 F43BE57D 14E28685

deU is
        323FA316 9D8E9C65 93F59476 BC142000 AB5BE0E2 49C43426

QeU_x is
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612

QeU_y is
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A

---
no Key Confirmation
Z is
        28D8AB53 9969B2C3 5979A92F D6462417 7A7191FF E70DE82D

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
                         B291C225 89BF6962 261ECD0A 37E0AA82
        BABD90BC 9EBDFEB2 479A6859 59EB317F FCB74243 8F0FE879

KeyData is
                         B291C225 89BF6962 261ECD0A 37E0AA82
        BABD90BC 9EBDFEB2 479A6859 59EB317F FCB74243 8F0FE879

Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
        F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309

Z is
        28D8AB53 9969B2C3 5979A92F D6462417 7A7191FF E70DE82D

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

```
DerivedKeyMaterial is
                                                              B291
        C22589BF 6962261E CD0A37E0 AA82BABD 90BC9EBD FEB2479A
        685959EB 317FFCB7 42438F0F E879844C AD2594C3 15CAF548


MacData is
                         4B435F31 5F55414C 49434542 4F424259
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A
        F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309


MacKey is
                                       B291 C22589BF 6962261E


Mtag is
                 B77CCEB3 AB54B2EA CD2DC61C 06A31CC1 6392D3CB


KeyData is
                         CD0A37E0 AA82BABD 90BC9EBD FEB2479A
        685959EB 317FFCB7 42438F0F E879844C AD2594C3 15CAF548




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
NonceU is
        F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309


Z is
        28D8AB53 9969B2C3 5979A92F D6462417 7A7191FF E70DE82D


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                              B291
        C22589BF 6962261E CD0A37E0 AA82BABD 90BC9EBD FEB2479A
```

```
        685959EB 317FFCB7 42438F0F E879844C AD2594C3 15CAF548


MacData is
                         4B435F31 5F56424F 42425941 4C494345
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A


MacKey is
                                      B291 C22589BF 6962261E


Mtag is
                 07EBCB09 B4850F10 E3ABCFE4 D9825913 DBC65BA5


KeyData is
                         CD0A37E0 AA82BABD 90BC9EBD FEB2479A
        685959EB 317FFCB7 42438F0F E879844C AD2594C3 15CAF548




-------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
NonceV is
        F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309


Z is
        28D8AB53 9969B2C3 5979A92F D6462417 7A7191FF E70DE82D


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                          B291
        C22589BF 6962261E CD0A37E0 AA82BABD 90BC9EBD FEB2479A
        685959EB 317FFCB7 42438F0F E879844C AD2594C3 15CAF548


U2V
----------------
```

```
MacData is
                        4B435F32 5F55414C 49434542 4F424259
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A
        F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309


MacKey is
                                     B291 C22589BF 6962261E


Mtag is
                CD5B865D 6B5C4ED0 6F50D438 5EDDA5EB 87BE7907


V2U
----------------
MacData is
                        4B435F32 5F56424F 42425941 4C494345
        F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A


MacKey is
                                     B291 C22589BF 6962261E


Mtag is
                D5B5AA11 A2679DA4 6556463E 4F4B4390 D3EA7337


KeyData is
                        CD0A37E0 AA82BABD 90BC9EBD FEB2479A
        685959EB 317FFCB7 42438F0F E879844C AD2594C3 15CAF548




OnePassDiffieHellmanCDH(P-192)
------------------------------------------------------------
dsV is
        0F9E539A E24C3A90 5B4ED7CE 4E2EBAD4 E4B77491 2623284B


QsV_x is
```

```
        09F9D21C 7FD98D09 7B4C3AE7 64300040 3DB445B7 49C4B441


QsV_y is
        43CB6933 62FD117C 79F255D9 DD6BBE75 F43BE57D 14E28685


deU is
        323FA316 9D8E9C65 93F59476 BC142000 AB5BE0E2 49C43426


QeU_x is
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612


QeU_y is
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A




------------------------------------------------------------
no Key Confirmation
Z is
        78B3A426 67DFF154 E395367B 744CBB50 67C03D08 A96D9086


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                         1811595A AE8280AE 98CAC5D7 D8ABCFB8
        12EF12BA F7241C8C DAC23476 F82967A9 B0A87754 98F39B63


KeyData is
                         1811595A AE8280AE 98CAC5D7 D8ABCFB8
        12EF12BA F7241C8C DAC23476 F82967A9 B0A87754 98F39B63




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
Z is
```

```
        78B3A426 67DFF154 E395367B 744CBB50 67C03D08 A96D9086


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                            1811
        595AAE82 80AE98CA C5D7D8AB CFB812EF 12BAF724 1C8CDAC2
        3476F829 67A9B0A8 775498F3 9B633200 E1C0DF52 C65BC142


MacData is
                         4B435F31 5F56424F 42425941 4C494345
        CD46489E CFD6C105 E7B3D325 66E2B122 E249ABAA DD870612
        68887B48 77DF51DD 4DC3D6FD 11F0A26F 8FD38443 17916E9A


MacKey is
                                      1811 595AAE82 80AE98CA


Mtag is
                650B63C0 625A62AF FC741CAF 57F945EE F1F7B36C


KeyData is
                         C5D7D8AB CFB812EF 12BAF724 1C8CDAC2
        3476F829 67A9B0A8 775498F3 9B633200 E1C0DF52 C65BC142




StaticUnifiedCDH(P-192)
------------------------------------------------------------
dsU is
        20F234D3 2CD7EDD8 BFC5BD96 DAE60859 3E38E894 2324FDE8


QsU_x is
        896C0B5E E70F55B3 B463101C 1BFB86D3 A7C6C5DA 354F6214


QsU_y is
        40B85F14 4536C6F5 4BC85BED 3820A74A BF58BC78 2D1DB241
```

```
dsV is
        0F9E539A E24C3A90 5B4ED7CE 4E2EBAD4 E4B77491 2623284B


QsV_x is
        09F9D21C 7FD98D09 7B4C3AE7 64300040 3DB445B7 49C4B441


QsV_y is
        43CB6933 62FD117C 79F255D9 DD6BBE75 F43BE57D 14E28685




------------------------------------------------------------
no Key Confirmation
NonceU is
        F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309


Z is
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D


OtherInfo is
                                                          1234
        56789ABC DEF0414C 49434531 3233C000 F8C1FC06 6B3EABFE
        0048466C A80DFDFB A3B9F7C3 73173309 424F4242 59343536


DerivedKeyMaterial is
                          97D227DD 8E001BFC 58AC4933 1C2233D8
        8128422F 35D247F1 68A2813B AAECB3AA E0F84155 7885E446


KeyData is
                          97D227DD 8E001BFC 58AC4933 1C2233D8
        8128422F 35D247F1 68A2813B AAECB3AA E0F84155 7885E446




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
```

```
NonceU is
        F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309


NonceV is
        81DB7325 97393873 89E51893 EFAD98A0 F0442D34 A531DC53


Z is
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D


OtherInfo is
                                                          1234
        56789ABC DEF0414C 49434531 3233C000 F8C1FC06 6B3EABFE
        0048466C A80DFDFB A3B9F7C3 73173309 424F4242 59343536


DerivedKeyMaterial is
                                                        97D2
        27DD8E00 1BFC58AC 49331C22 33D88128 422F35D2 47F168A2
        813BAAEC B3AAE0F8 41557885 E446E549 0A21E789 7277A6D7


MacData is
                         4B435F31 5F55414C 49434542 4F424259
        F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309
        81DB7325 97393873 89E51893 EFAD98A0 F0442D34 A531DC53


MacKey is
                                      97D2 27DD8E00 1BFC58AC


Mtag is
                525878C5 3D2851E1 1355A221 DBA01855 99B13388


KeyData is
                         49331C22 33D88128 422F35D2 47F168A2
        813BAAEC B3AAE0F8 41557885 E446E549 0A21E789 7277A6D7



------------------------------------------------------------
```

Scheme Responder, Key Confirmation Provider: V to U
NonceV is
        81DB7325 97393873 89E51893 EFAD98A0 F0442D34 A531DC53

NonceU is
        F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309

Z is
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D

OtherInfo is
                                                            1234
        56789ABC DEF0414C 49434531 3233C000 F8C1FC06 6B3EABFE
        0048466C A80DFDFB A3B9F7C3 73173309 424F4242 59343536

DerivedKeyMaterial is
                                                          97D2
        27DD8E00 1BFC58AC 49331C22 33D88128 422F35D2 47F168A2
        813BAAEC B3AAE0F8 41557885 E446E549 0A21E789 7277A6D7

MacData is
                         4B435F31 5F56424F 42425941 4C494345
        F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309

MacKey is
                                      97D2 27DD8E00 1BFC58AC

Mtag is
                 9EBA877C 4B6D62AE 22A9ED34 5280F5B1 A28421FF

KeyData is
                         49331C22 33D88128 422F35D2 47F168A2
        813BAAEC B3AAE0F8 41557885 E446E549 0A21E789 7277A6D7

```
Scheme Initiator, Key Confirmation Bilateral
NonceU is
        F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309


NonceV is
        81DB7325 97393873 89E51893 EFAD98A0 F0442D34 A531DC53


Z is
        0FB12A1B 3BEBF263 EE216413 ED06A84A 12EB5111 59F1337D


OtherInfo is
                                                            1234
        56789ABC DEF0414C 49434531 3233C000 F8C1FC06 6B3EABFE
        0048466C A80DFDFB A3B9F7C3 73173309 424F4242 59343536


DerivedKeyMaterial is
                                                          97D2
        27DD8E00 1BFC58AC 49331C22 33D88128 422F35D2 47F168A2
        813BAAEC B3AAE0F8 41557885 E446E549 0A21E789 7277A6D7


U2V
----------------
MacData is
                          4B435F32 5F55414C 49434542 4F424259
        F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309
        81DB7325 97393873 89E51893 EFAD98A0 F0442D34 A531DC53


MacKey is
                                       97D2 27DD8E00 1BFC58AC


Mtag is
                F563A1FF F1D386F2 AD2A5FAE 42D60BE7 5858ABD0


V2U
----------------
MacData is
                          4B435F32 5F56424F 42425941 4C494345
```

81DB7325 97393873 89E51893 EFAD98A0 F0442D34 A531DC53
F8C1FC06 6B3EABFE 0048466C A80DFDFB A3B9F7C3 73173309

MacKey is

97D2 27DD8E00 1BFC58AC

Mtag is

C64C12EF 4D9FDB90 0B24EA6C 92E7E4B4 CB07E81E

KeyData is

49331C22 33D88128 422F35D2 47F168A2
813BAAEC B3AAE0F8 41557885 E446E549 0A21E789 7277A6D7

FullUnifiedCDH(P-224)
----
dsU is
                                                        A273DD64
        3AB8A64B 4B6E1FF9 C7ECF18E BC1F62DE 33450A9E 32E8A504

QsU_x is
                                                        FAD43A96
        46721C46 52F13752 345FC2D5 25515A55 A170E685 314810E1

QsU_y is
                                                        E05BE902
        7238C138 7F7C5575 ED425324 32929EFB C2C37293 1253F3D2

dsV is
                                                        723A6551
        09089ED0 EDB4E630 72A82640 9F9C6204 635169F0 681F7514

QsV_x is
                                                        0898B1C4
        B9308496 45F2E605 00DA0492 0CB70272 3E4E13F6 64C99B0B

QsV_y is
                                                        0D91CF88
        A13435E4 D126DA64 352C75F2 B80C65F9 43D6F65A 6AC20F0B

deU is
                                                        B558EB6C
        288DA707 BBB4F8FB AE2AB9E9 CB62E3BC 5C7573E2 2E26D37F

QeU_x is
                                                        49DFEF30
        9F81488C 304CFF5A B3EE5A21 54367DC7 833150E0 A51F3EEB

QeU_y is
                                                        4F2B5EE4

5762C4F6 54C1A0C6 7F54CF88 B016B51B CE3D7C22 8D57ADB4

deV is
AC3B1ADD
3D9770E6 F6A708EE 9F3B8E0A B3B480E9 F27F85C8 8B5E6D18

QeV_x is
6B3AC96A
8D0CDE6A 5599BE80 32EDF10C 162D0A8A D219506D CD42A207

QeV_y is
D491BE99
C213A7D1 CA3706DE BFE305F3 61AFCBB3 3E2609C8 B1618AD5

---

no Key Confirmation
Zs is
9F18FF54
F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9

Ze is
52272F50
F46F4EDC 91515690 92F46DF2 D96ECC3B 6DC1714A 4EA949FA

Z is
52272F50 F46F4EDC
91515690 92F46DF2 D96ECC3B 6DC1714A 4EA949FA 9F18FF54
F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
7756BCFD EF3EE69F
6AC23CD2 DC607D01 FA8CE1B2 4F5CAAAA 48E04B81 63E1733A
ED7A040E 73F2B542 368F0054 8B163C3D C96D7009 9916F16B

KeyData is
                                                7756BCFD EF3EE69F
        6AC23CD2 DC607D01 FA8CE1B2 4F5CAAAA 48E04B81 63E1733A
        ED7A040E 73F2B542 368F0054 8B163C3D C96D7009 9916F16B

Scheme Initiator, Key Confirmation Provider: U to V
Zs is
                                                        9F18FF54
        F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9

Ze is
                                                        52272F50
        F46F4EDC 91515690 92F46DF2 D96ECC3B 6DC1714A 4EA949FA

Z is
                                                52272F50 F46F4EDC
        91515690 92F46DF2 D96ECC3B 6DC1714A 4EA949FA 9F18FF54
        F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
            7756 BCFDEF3E E69F6AC2 3CD2DC60 7D01FA8C E1B24F5C
        AAAA48E0 4B8163E1 733AED7A 040E73F2 B542368F 00548B16
        3C3DC96D 70099916 F16B96DE 6EF4948D 3C2EF037 E45DCD43

MacData is
                                                4B435F31 5F55414C
        49434542 4F424259 49DFEF30 9F81488C 304CFF5A B3EE5A21
        54367DC7 833150E0 A51F3EEB 4F2B5EE4 5762C4F6 54C1A0C6
        7F54CF88 B016B51B CE3D7C22 8D57ADB4 6B3AC96A 8D0CDE6A
        5599BE80 32EDF10C 162D0A8A D219506D CD42A207 D491BE99
        C213A7D1 CA3706DE BFE305F3 61AFCBB3 3E2609C8 B1618AD5

MacKey is
                              7756 BCFDEF3E E69F6AC2 3CD2DC60

Mtag is
                                                        9EE6013E
        119F3782 BF892E92 9E04D14D D24BDD0F 28FB87FC BE37803E

KeyData is
                                               7D01FA8C E1B24F5C
        AAAA48E0 4B8163E1 733AED7A 040E73F2 B542368F 00548B16
        3C3DC96D 70099916 F16B96DE 6EF4948D 3C2EF037 E45DCD43

Scheme Responder, Key Confirmation Provider: V to U
Zs is
                                                        9F18FF54
        F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9

Ze is
                                                        52272F50
        F46F4EDC 91515690 92F46DF2 D96ECC3B 6DC1714A 4EA949FA

Z is
                                               52272F50 F46F4EDC
        91515690 92F46DF2 D96ECC3B 6DC1714A 4EA949FA 9F18FF54
        F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
            7756 BCFDEF3E E69F6AC2 3CD2DC60 7D01FA8C E1B24F5C
        AAAA48E0 4B8163E1 733AED7A 040E73F2 B542368F 00548B16
        3C3DC96D 70099916 F16B96DE 6EF4948D 3C2EF037 E45DCD43

MacData is
                                                4B435F31 5F56424F
        42425941 4C494345 6B3AC96A 8D0CDE6A 5599BE80 32EDF10C
        162D0A8A D219506D CD42A207 D491BE99 C213A7D1 CA3706DE
        BFE305F3 61AFCBB3 3E2609C8 B1618AD5 49DFEF30 9F81488C
        304CFF5A B3EE5A21 54367DC7 833150E0 A51F3EEB 4F2B5EE4
        5762C4F6 54C1A0C6 7F54CF88 B016B51B CE3D7C22 8D57ADB4

MacKey is
                             7756 BCFDEF3E E69F6AC2 3CD2DC60

Mtag is
                                                        32FB2425
        20A67C16 52658556 16754B36 488841C8 B141EDB9 2F2B8400

KeyData is
                                                7D01FA8C E1B24F5C
        AAAA48E0 4B8163E1 733AED7A 040E73F2 B542368F 00548B16
        3C3DC96D 70099916 F16B96DE 6EF4948D 3C2EF037 E45DCD43

Scheme Initiator, Key Confirmation Bilateral
Zs is
                                                        9F18FF54
        F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9

Ze is
                                                        52272F50
        F46F4EDC 91515690 92F46DF2 D96ECC3B 6DC1714A 4EA949FA

Z is
                                                52272F50 F46F4EDC
        91515690 92F46DF2 D96ECC3B 6DC1714A 4EA949FA 9F18FF54
        F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

```
DerivedKeyMaterial is
            7756 BCFDEF3E E69F6AC2 3CD2DC60 7D01FA8C E1B24F5C
         AAAA48E0 4B8163E1 733AED7A 040E73F2 B542368F 00548B16
         3C3DC96D 70099916 F16B96DE 6EF4948D 3C2EF037 E45DCD43


U2V
----------------
MacData is
                                              4B435F32 5F55414C
         49434542 4F424259 49DFEF30 9F81488C 304CFF5A B3EE5A21
         54367DC7 833150E0 A51F3EEB 4F2B5EE4 5762C4F6 54C1A0C6
         7F54CF88 B016B51B CE3D7C22 8D57ADB4 6B3AC96A 8D0CDE6A
         5599BE80 32EDF10C 162D0A8A D219506D CD42A207 D491BE99
         C213A7D1 CA3706DE BFE305F3 61AFCBB3 3E2609C8 B1618AD5


MacKey is
                              7756 BCFDEF3E E69F6AC2 3CD2DC60


Mtag is
                                                      3C1B7182
         FF32DC91 BCD26B90 223CDC27 34EBF8CC 236EB944 857153B2


V2U
----------------
MacData is
                                              4B435F32 5F56424F
         42425941 4C494345 6B3AC96A 8D0CDE6A 5599BE80 32EDF10C
         162D0A8A D219506D CD42A207 D491BE99 C213A7D1 CA3706DE
         BFE305F3 61AFCBB3 3E2609C8 B1618AD5 49DFEF30 9F81488C
         304CFF5A B3EE5A21 54367DC7 833150E0 A51F3EEB 4F2B5EE4
         5762C4F6 54C1A0C6 7F54CF88 B016B51B CE3D7C22 8D57ADB4


MacKey is
                              7756 BCFDEF3E E69F6AC2 3CD2DC60


Mtag is
                                                      7DFA15A7
         5550A8FD F01AF1EF 77FB9547 7E49D672 6CFD3BD1 079428CA
```

KeyData is
                                                7D01FA8C E1B24F5C
        AAAA48E0 4B8163E1 733AED7A 040E73F2 B542368F 00548B16
        3C3DC96D 70099916 F16B96DE 6EF4948D 3C2EF037 E45DCD43

FullMQV(P-224)
----
dsU is
                                                        A273DD64
        3AB8A64B 4B6E1FF9 C7ECF18E BC1F62DE 33450A9E 32E8A504

QsU_x is
                                                        FAD43A96
        46721C46 52F13752 345FC2D5 25515A55 A170E685 314810E1

QsU_y is
                                                        E05BE902
        7238C138 7F7C5575 ED425324 32929EFB C2C37293 1253F3D2

dsV is
                                                        723A6551
        09089ED0 EDB4E630 72A82640 9F9C6204 635169F0 681F7514

QsV_x is
                                                        0898B1C4
        B9308496 45F2E605 00DA0492 0CB70272 3E4E13F6 64C99B0B

QsV_y is
                                                        0D91CF88
        A13435E4 D126DA64 352C75F2 B80C65F9 43D6F65A 6AC20F0B

deU is
                                                        B558EB6C
        288DA707 BBB4F8FB AE2AB9E9 CB62E3BC 5C7573E2 2E26D37F

```
QeU_x is
                                                        49DFEF30
        9F81488C 304CFF5A B3EE5A21 54367DC7 833150E0 A51F3EEB


QeU_y is
                                                        4F2B5EE4
        5762C4F6 54C1A0C6 7F54CF88 B016B51B CE3D7C22 8D57ADB4


deV is
                                                        AC3B1ADD
        3D9770E6 F6A708EE 9F3B8E0A B3B480E9 F27F85C8 8B5E6D18


QeV_x is
                                                        6B3AC96A
        8D0CDE6A 5599BE80 32EDF10C 162D0A8A D219506D CD42A207


QeV_y is
                                                        D491BE99
        C213A7D1 CA3706DE BFE305F3 61AFCBB3 3E2609C8 B1618AD5




-------------------------------------------------------------
no Key Confirmation
Z is
                                                        DEF3B660
        18D14DCD FFF1C251 174C6825 82709092 5AA823EF A0F99812


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                5924621F C51249E4
        48BBF95B B47E6B6B 6406F8E1 A1E1C046 C6B4F49C 4DD866F3
        F76A47C4 C996BCA3 0B02789A 023DFCB4 1270EAB2 A1F10B00


KeyData is
```

                                                5924621F C51249E4
        48BBF95B B47E6B6B 6406F8E1 A1E1C046 C6B4F49C 4DD866F3
        F76A47C4 C996BCA3 0B02789A 023DFCB4 1270EAB2 A1F10B00

Scheme Initiator, Key Confirmation Provider: U to V
Z is
                                                        DEF3B660
        18D14DCD FFF1C251 174C6825 82709092 5AA823EF A0F99812

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
            5924 621FC512 49E448BB F95BB47E 6B6B6406 F8E1A1E1
        C046C6B4 F49C4DD8 66F3F76A 47C4C996 BCA30B02 789A023D
        FCB41270 EAB2A1F1 0B00A4E0 3C6F0379 624382F0 3C4F340A

MacData is
                                                4B435F31 5F55414C
        49434542 4F424259 49DFEF30 9F81488C 304CFF5A B3EE5A21
        54367DC7 833150E0 A51F3EEB 4F2B5EE4 5762C4F6 54C1A0C6
        7F54CF88 B016B51B CE3D7C22 8D57ADB4 6B3AC96A 8D0CDE6A
        5599BE80 32EDF10C 162D0A8A D219506D CD42A207 D491BE99
        C213A7D1 CA3706DE BFE305F3 61AFCBB3 3E2609C8 B1618AD5

MacKey is
                                5924 621FC512 49E448BB F95BB47E

Mtag is
                                                        6FA28E3D
        AB50C637 65039C64 ED28C014 AF9AE6FB FC0E633A 4748CAE4

KeyData is
                                                6B6B6406 F8E1A1E1
        C046C6B4 F49C4DD8 66F3F76A 47C4C996 BCA30B02 789A023D
        FCB41270 EAB2A1F1 0B00A4E0 3C6F0379 624382F0 3C4F340A

```
-------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
Z is
                                                        DEF3B660
        18D14DCD FFF1C251 174C6825 82709092 5AA823EF A0F99812


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
            5924 621FC512 49E448BB F95BB47E 6B6B6406 F8E1A1E1
        C046C6B4 F49C4DD8 66F3F76A 47C4C996 BCA30B02 789A023D
        FCB41270 EAB2A1F1 0B00A4E0 3C6F0379 624382F0 3C4F340A


MacData is
                                               4B435F31 5F56424F
        42425941 4C494345 6B3AC96A 8D0CDE6A 5599BE80 32EDF10C
        162D0A8A D219506D CD42A207 D491BE99 C213A7D1 CA3706DE
        BFE305F3 61AFCBB3 3E2609C8 B1618AD5 49DFEF30 9F81488C
        304CFF5A B3EE5A21 54367DC7 833150E0 A51F3EEB 4F2B5EE4
        5762C4F6 54C1A0C6 7F54CF88 B016B51B CE3D7C22 8D57ADB4


MacKey is
                              5924 621FC512 49E448BB F95BB47E


Mtag is
                                                        A22C1AC7
        613C91C9 E3F85F55 7DA051FC 59C42F35 53132A10 DB641373


KeyData is
                                               6B6B6406 F8E1A1E1
        C046C6B4 F49C4DD8 66F3F76A 47C4C996 BCA30B02 789A023D
        FCB41270 EAB2A1F1 0B00A4E0 3C6F0379 624382F0 3C4F340A
```

```
-----------------------------------------------------------

Scheme Initiator, Key Confirmation Bilateral
Z is
                                                        DEF3B660
        18D14DCD FFF1C251 174C6825 82709092 5AA823EF A0F99812


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
            5924 621FC512 49E448BB F95BB47E 6B6B6406 F8E1A1E1
        C046C6B4 F49C4DD8 66F3F76A 47C4C996 BCA30B02 789A023D
        FCB41270 EAB2A1F1 0B00A4E0 3C6F0379 624382F0 3C4F340A


U2V
----------------
MacData is
                                            4B435F32 5F55414C
        49434542 4F424259 49DFEF30 9F81488C 304CFF5A B3EE5A21
        54367DC7 833150E0 A51F3EEB 4F2B5EE4 5762C4F6 54C1A0C6
        7F54CF88 B016B51B CE3D7C22 8D57ADB4 6B3AC96A 8D0CDE6A
        5599BE80 32EDF10C 162D0A8A D219506D CD42A207 D491BE99
        C213A7D1 CA3706DE BFE305F3 61AFCBB3 3E2609C8 B1618AD5


MacKey is
                              5924 621FC512 49E448BB F95BB47E


Mtag is
                                                        A18A79FC
        B60D7368 ABA1D3FC 80D3D745 2678EA16 0734453A 208FAF61


V2U
----------------
MacData is
                                            4B435F32 5F56424F
        42425941 4C494345 6B3AC96A 8D0CDE6A 5599BE80 32EDF10C
        162D0A8A D219506D CD42A207 D491BE99 C213A7D1 CA3706DE
        BFE305F3 61AFCBB3 3E2609C8 B1618AD5 49DFEF30 9F81488C
```

```
        304CFF5A B3EE5A21 54367DC7 833150E0 A51F3EEB 4F2B5EE4
        5762C4F6 54C1A0C6 7F54CF88 B016B51B CE3D7C22 8D57ADB4


MacKey is
                             5924 621FC512 49E448BB F95BB47E


Mtag is
                                                    DB375DC5
        2BA00B86 1B5F365D 41CDED7D 3AAFCE42 576F1301 1183AC41


KeyData is
                                                6B6B6406 F8E1A1E1
        C046C6B4 F49C4DD8 66F3F76A 47C4C996 BCA30B02 789A023D
        FCB41270 EAB2A1F1 0B00A4E0 3C6F0379 624382F0 3C4F340A




EphemeralUnifiedCDH(P-224)
----------------------------------------------------------
deU is
                                                    B558EB6C
        288DA707 BBB4F8FB AE2AB9E9 CB62E3BC 5C7573E2 2E26D37F


QeU_x is
                                                    49DFEF30
        9F81488C 304CFF5A B3EE5A21 54367DC7 833150E0 A51F3EEB


QeU_y is
                                                    4F2B5EE4
        5762C4F6 54C1A0C6 7F54CF88 B016B51B CE3D7C22 8D57ADB4


deV is
                                                    AC3B1ADD
        3D9770E6 F6A708EE 9F3B8E0A B3B480E9 F27F85C8 8B5E6D18


QeV_x is
                                                    6B3AC96A
        8D0CDE6A 5599BE80 32EDF10C 162D0A8A D219506D CD42A207
```

```
QeV_y is
                                                        D491BE99
        C213A7D1 CA3706DE BFE305F3 61AFCBB3 3E2609C8 B1618AD5




------------------------------------------------------------
no Key Confirmation
Z is
                                                        52272F50
        F46F4EDC 91515690 92F46DF2 D96ECC3B 6DC1714A 4EA949FA


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                8F61E07C 6B90ECD0
        15E5DED9 ED3B82B8 229786BD FB039289 CC666FAD 99E0D042
        A3F19045 8335A703 26486A23 43DBB074 0984604F 1E715BEE


KeyData is
                                                8F61E07C 6B90ECD0
        15E5DED9 ED3B82B8 229786BD FB039289 CC666FAD 99E0D042
        A3F19045 8335A703 26486A23 43DBB074 0984604F 1E715BEE




OnePassUnifiedCDH(P-224)
------------------------------------------------------------
dsU is
                                                        A273DD64
        3AB8A64B 4B6E1FF9 C7ECF18E BC1F62DE 33450A9E 32E8A504


QsU_x is
                                                        FAD43A96
        46721C46 52F13752 345FC2D5 25515A55 A170E685 314810E1
```

```
QsU_y is
                                                        E05BE902
        7238C138 7F7C5575 ED425324 32929EFB C2C37293 1253F3D2


dsV is
                                                        723A6551
        09089ED0 EDB4E630 72A82640 9F9C6204 635169F0 681F7514


QsV_x is
                                                        0898B1C4
        B9308496 45F2E605 00DA0492 0CB70272 3E4E13F6 64C99B0B


QsV_y is
                                                        0D91CF88
        A13435E4 D126DA64 352C75F2 B80C65F9 43D6F65A 6AC20F0B


deU is
                                                        B558EB6C
        288DA707 BBB4F8FB AE2AB9E9 CB62E3BC 5C7573E2 2E26D37F


QeU_x is
                                                        49DFEF30
        9F81488C 304CFF5A B3EE5A21 54367DC7 833150E0 A51F3EEB


QeU_y is
                                                        4F2B5EE4
        5762C4F6 54C1A0C6 7F54CF88 B016B51B CE3D7C22 8D57ADB4




------------------------------------------------------------
no Key Confirmation
Zs is
                                                        9F18FF54
        F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9


Ze is
                                                        59141E22
```

```
        76D41EDA D4E6D088 5C363DCF E91FCC0C 1726D11C FB3AA35B


Z is
                                                59141E22 76D41EDA
        D4E6D088 5C363DCF E91FCC0C 1726D11C FB3AA35B 9F18FF54
        F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                92EA706A 6FCE4DD2
        0D0B918B C1076EEE 1FBCD591 37429C8B 56B201D3 D7255180
        E8F11FF1 DBB34C10 310028E0 29708B05 0A834422 934109BD


KeyData is
                                                92EA706A 6FCE4DD2
        0D0B918B C1076EEE 1FBCD591 37429C8B 56B201D3 D7255180
        E8F11FF1 DBB34C10 310028E0 29708B05 0A834422 934109BD




-------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
                                                        4327ABCA
        DC176812 553A2E13 F68080BE D1BC6A1A 4F6FBB12 345EC9F9


Zs is
                                                        9F18FF54
        F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9


Ze is
                                                        59141E22
        76D41EDA D4E6D088 5C363DCF E91FCC0C 1726D11C FB3AA35B


Z is
                                                59141E22 76D41EDA
```

```
        D4E6D088 5C363DCF E91FCC0C 1726D11C FB3AA35B 9F18FF54
        F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
            92EA 706A6FCE 4DD20D0B 918BC107 6EEE1FBC D5913742
        9C8B56B2 01D3D725 5180E8F1 1FF1DBB3 4C103100 28E02970
        8B050A83 44229341 09BD0362 8FC0BA70 8AA035DB B2D8C4F0


MacData is
                                                        4B435F31
        5F55414C 49434542 4F424259 49DFEF30 9F81488C 304CFF5A
        B3EE5A21 54367DC7 833150E0 A51F3EEB 4F2B5EE4 5762C4F6
        54C1A0C6 7F54CF88 B016B51B CE3D7C22 8D57ADB4 4327ABCA
        DC176812 553A2E13 F68080BE D1BC6A1A 4F6FBB12 345EC9F9


MacKey is
                               92EA 706A6FCE 4DD20D0B 918BC107


Mtag is
                                                        083B64E0
        F6BAAA1D D69B4545 E42CEF3F 9C292D80 0DCA76D1 7E71E687


KeyData is
                                                6EEE1FBC D5913742
        9C8B56B2 01D3D725 5180E8F1 1FF1DBB3 4C103100 28E02970
        8B050A83 44229341 09BD0362 8FC0BA70 8AA035DB B2D8C4F0




-----------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
NonceU is
                                                        4327ABCA
        DC176812 553A2E13 F68080BE D1BC6A1A 4F6FBB12 345EC9F9
```

```
Zs is
                                                        9F18FF54
        F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9


Ze is
                                                        59141E22
        76D41EDA D4E6D088 5C363DCF E91FCC0C 1726D11C FB3AA35B


Z is
                                            59141E22 76D41EDA
        D4E6D088 5C363DCF E91FCC0C 1726D11C FB3AA35B 9F18FF54
        F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
            92EA 706A6FCE 4DD20D0B 918BC107 6EEE1FBC D5913742
        9C8B56B2 01D3D725 5180E8F1 1FF1DBB3 4C103100 28E02970
        8B050A83 44229341 09BD0362 8FC0BA70 8AA035DB B2D8C4F0


MacData is
        4B435F31 5F56424F 42425941 4C494345 49DFEF30 9F81488C
        304CFF5A B3EE5A21 54367DC7 833150E0 A51F3EEB 4F2B5EE4
        5762C4F6 54C1A0C6 7F54CF88 B016B51B CE3D7C22 8D57ADB4


MacKey is
                              92EA 706A6FCE 4DD20D0B 918BC107


Mtag is
                                                        2762D05E
        EE45EB61 B2DEA75E C0F9A1A2 B93B1859 E74AEAD8 6CBBC6B2


KeyData is
                                            6EEE1FBC D5913742
        9C8B56B2 01D3D725 5180E8F1 1FF1DBB3 4C103100 28E02970
        8B050A83 44229341 09BD0362 8FC0BA70 8AA035DB B2D8C4F0
```

```
-----------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
NonceV is
                                                        4327ABCA
        DC176812 553A2E13 F68080BE D1BC6A1A 4F6FBB12 345EC9F9


Zs is
                                                        9F18FF54
        F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9


Ze is
                                                        59141E22
        76D41EDA D4E6D088 5C363DCF E91FCC0C 1726D11C FB3AA35B


Z is
                                            59141E22 76D41EDA
        D4E6D088 5C363DCF E91FCC0C 1726D11C FB3AA35B 9F18FF54
        F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
            92EA 706A6FCE 4DD20D0B 918BC107 6EEE1FBC D5913742
        9C8B56B2 01D3D725 5180E8F1 1FF1DBB3 4C103100 28E02970
        8B050A83 44229341 09BD0362 8FC0BA70 8AA035DB B2D8C4F0


U2V
----------------
MacData is
                                                        4B435F32
        5F55414C 49434542 4F424259 49DFEF30 9F81488C 304CFF5A
        B3EE5A21 54367DC7 833150E0 A51F3EEB 4F2B5EE4 5762C4F6
        54C1A0C6 7F54CF88 B016B51B CE3D7C22 8D57ADB4 4327ABCA
        DC176812 553A2E13 F68080BE D1BC6A1A 4F6FBB12 345EC9F9
```

MacKey is
92EA 706A6FCE 4DD20D0B 918BC107

Mtag is
0954AFC0
2B5F3F3E 06FE2FF2 120D8695 C7D4BF77 7285B7CC F5691371

V2U

MacData is
4B435F32
5F56424F 42425941 4C494345 4327ABCA DC176812 553A2E13
F68080BE D1BC6A1A 4F6FBB12 345EC9F9 49DFEF30 9F81488C
304CFF5A B3EE5A21 54367DC7 833150E0 A51F3EEB 4F2B5EE4
5762C4F6 54C1A0C6 7F54CF88 B016B51B CE3D7C22 8D57ADB4

MacKey is
92EA 706A6FCE 4DD20D0B 918BC107

Mtag is
CEFD1BF6
C74C966F 97B632FB 26E2129B 2AED8022 2CCE396E B95091C1

KeyData is
6EEE1FBC D5913742
9C8B56B2 01D3D725 5180E8F1 1FF1DBB3 4C103100 28E02970
8B050A83 44229341 09BD0362 8FC0BA70 8AA035DB B2D8C4F0

OnePassMQV(P-224)
---
dsU is
A273DD64
3AB8A64B 4B6E1FF9 C7ECF18E BC1F62DE 33450A9E 32E8A504

QsU_x is
FAD43A96
46721C46 52F13752 345FC2D5 25515A55 A170E685 314810E1

QsU_y is

```
                                                        E05BE902
        7238C138 7F7C5575 ED425324 32929EFB C2C37293 1253F3D2
```

dsV is

```
                                                        723A6551
        09089ED0 EDB4E630 72A82640 9F9C6204 635169F0 681F7514
```

QsV_x is

```
                                                        0898B1C4
        B9308496 45F2E605 00DA0492 0CB70272 3E4E13F6 64C99B0B
```

QsV_y is

```
                                                        0D91CF88
        A13435E4 D126DA64 352C75F2 B80C65F9 43D6F65A 6AC20F0B
```

deU is

```
                                                        B558EB6C
        288DA707 BBB4F8FB AE2AB9E9 CB62E3BC 5C7573E2 2E26D37F
```

QeU_x is

```
                                                        49DFEF30
        9F81488C 304CFF5A B3EE5A21 54367DC7 833150E0 A51F3EEB
```

QeU_y is

```
                                                        4F2B5EE4
        5762C4F6 54C1A0C6 7F54CF88 B016B51B CE3D7C22 8D57ADB4
```

---

no Key Confirmation
Z is

```
                                                        C94E2263
        B99BEB56 46CA803A B625A9F8 734BD00E C9533680 8DCC8732
```

```
OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                62C37171 C44BE767
        4004DF4E B111664A 39C2E7AB 31C36CA0 0AA6996B CA481767
        09F68F9A B0C361C4 A34AACC4 ABE7A89B E78C547D 6829D25E


KeyData is
                                                62C37171 C44BE767
        4004DF4E B111664A 39C2E7AB 31C36CA0 0AA6996B CA481767
        09F68F9A B0C361C4 A34AACC4 ABE7A89B E78C547D 6829D25E




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
                                                        4327ABCA
        DC176812 553A2E13 F68080BE D1BC6A1A 4F6FBB12 345EC9F9


Z is
                                                        C94E2263
        B99BEB56 46CA803A B625A9F8 734BD00E C9533680 8DCC8732


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
            62C3 7171C44B E7674004 DF4EB111 664A39C2 E7AB31C3
        6CA00AA6 996BCA48 176709F6 8F9AB0C3 61C4A34A ACC4ABE7
        A89BE78C 547D6829 D25EAFD6 1602000B A871D962 B4BC59C5


MacData is
                                                        4B435F31
        5F55414C 49434542 4F424259 49DFEF30 9F81488C 304CFF5A
        B3EE5A21 54367DC7 833150E0 A51F3EEB 4F2B5EE4 5762C4F6
        54C1A0C6 7F54CF88 B016B51B CE3D7C22 8D57ADB4 4327ABCA
        DC176812 553A2E13 F68080BE D1BC6A1A 4F6FBB12 345EC9F9
```

```
MacKey is
                              62C3 7171C44B E7674004 DF4EB111


Mtag is
                                                      EBED799A
        91765BD7 A2D0CAE9 E7006E21 66058613 ED56873D 00EA3AF7


KeyData is
                                                664A39C2 E7AB31C3
        6CA00AA6 996BCA48 176709F6 8F9AB0C3 61C4A34A ACC4ABE7
        A89BE78C 547D6829 D25EAFD6 1602000B A871D962 B4BC59C5




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
NonceU is
                                                      4327ABCA
        DC176812 553A2E13 F68080BE D1BC6A1A 4F6FBB12 345EC9F9


Z is
                                                      C94E2263
        B99BEB56 46CA803A B625A9F8 734BD00E C9533680 8DCC8732


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
            62C3 7171C44B E7674004 DF4EB111 664A39C2 E7AB31C3
        6CA00AA6 996BCA48 176709F6 8F9AB0C3 61C4A34A ACC4ABE7
        A89BE78C 547D6829 D25EAFD6 1602000B A871D962 B4BC59C5


MacData is
        4B435F31 5F56424F 42425941 4C494345 49DFEF30 9F81488C
        304CFF5A B3EE5A21 54367DC7 833150E0 A51F3EEB 4F2B5EE4
        5762C4F6 54C1A0C6 7F54CF88 B016B51B CE3D7C22 8D57ADB4
```

```
MacKey is
                            62C3 7171C44B E7674004 DF4EB111


Mtag is
                                                        0D63208B
        C4ED7839 4C5FC832 DC7B51E2 F702CB05 FB297813 688336C0


KeyData is
                                               664A39C2 E7AB31C3
        6CA00AA6 996BCA48 176709F6 8F9AB0C3 61C4A34A ACC4ABE7
        A89BE78C 547D6829 D25EAFD6 1602000B A871D962 B4BC59C5




------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
NonceV is
                                                        4327ABCA
        DC176812 553A2E13 F68080BE D1BC6A1A 4F6FBB12 345EC9F9


Z is
                                                        C94E2263
        B99BEB56 46CA803A B625A9F8 734BD00E C9533680 8DCC8732


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
            62C3 7171C44B E7674004 DF4EB111 664A39C2 E7AB31C3
        6CA00AA6 996BCA48 176709F6 8F9AB0C3 61C4A34A ACC4ABE7
        A89BE78C 547D6829 D25EAFD6 1602000B A871D962 B4BC59C5


U2V
----------------
MacData is
                                                        4B435F32
        5F55414C 49434542 4F424259 49DFEF30 9F81488C 304CFF5A
        B3EE5A21 54367DC7 833150E0 A51F3EEB 4F2B5EE4 5762C4F6
```

```
        54C1A0C6 7F54CF88 B016B51B CE3D7C22 8D57ADB4 4327ABCA
        DC176812 553A2E13 F68080BE D1BC6A1A 4F6FBB12 345EC9F9


MacKey is
                            62C3 7171C44B E7674004 DF4EB111


Mtag is
                                                    B2E7A535
        1609EEFF B9DC6DDD 3A09FE05 F972F8E0 EEF1B4F8 9AF0834A


V2U
----------------
MacData is
                                                    4B435F32
        5F56424F 42425941 4C494345 4327ABCA DC176812 553A2E13
        F68080BE D1BC6A1A 4F6FBB12 345EC9F9 49DFEF30 9F81488C
        304CFF5A B3EE5A21 54367DC7 833150E0 A51F3EEB 4F2B5EE4
        5762C4F6 54C1A0C6 7F54CF88 B016B51B CE3D7C22 8D57ADB4


MacKey is
                            62C3 7171C44B E7674004 DF4EB111


Mtag is
                                                    47F5EE5E
        51BA83C3 CB5F94BD D07742D1 38B37764 437F8923 874FCC9F


KeyData is
                                                664A39C2 E7AB31C3
        6CA00AA6 996BCA48 176709F6 8F9AB0C3 61C4A34A ACC4ABE7
        A89BE78C 547D6829 D25EAFD6 1602000B A871D962 B4BC59C5




OnePassDiffieHellmanCDH(P-224)
------------------------------------------------------------
dsV is
                                                    723A6551
        09089ED0 EDB4E630 72A82640 9F9C6204 635169F0 681F7514
```

```
QsV_x is
                                                        0898B1C4
        B9308496 45F2E605 00DA0492 0CB70272 3E4E13F6 64C99B0B


QsV_y is
                                                        0D91CF88
        A13435E4 D126DA64 352C75F2 B80C65F9 43D6F65A 6AC20F0B


deU is
                                                        B558EB6C
        288DA707 BBB4F8FB AE2AB9E9 CB62E3BC 5C7573E2 2E26D37F


QeU_x is
                                                        49DFEF30
        9F81488C 304CFF5A B3EE5A21 54367DC7 833150E0 A51F3EEB


QeU_y is
                                                        4F2B5EE4
        5762C4F6 54C1A0C6 7F54CF88 B016B51B CE3D7C22 8D57ADB4




-------------------------------------------------------------
no Key Confirmation
Z is
                                                        59141E22
        76D41EDA D4E6D088 5C363DCF E91FCC0C 1726D11C FB3AA35B


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                D9DAD952 FDA8BE9B
        1C3F0962 D5B21DC8 F87E85B1 D3521242 2E4458FC 1600B2D4
        5528EC66 ED6BB75E 8714B4EF BA31CD10 B0CEB5CF 74C480FA


KeyData is
```

                                                D9DAD952 FDA8BE9B
        1C3F0962 D5B21DC8 F87E85B1 D3521242 2E4458FC 1600B2D4
        5528EC66 ED6BB75E 8714B4EF BA31CD10 B0CEB5CF 74C480FA

Scheme Responder, Key Confirmation Provider: V to U
Z is
                                                        59141E22
        76D41EDA D4E6D088 5C363DCF E91FCC0C 1726D11C FB3AA35B

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
            D9DA D952FDA8 BE9B1C3F 0962D5B2 1DC8F87E 85B1D352
        12422E44 58FC1600 B2D45528 EC66ED6B B75E8714 B4EFBA31
        CD10B0CE B5CF74C4 80FAA515 716881E3 658C6202 B97D4E01

MacData is
        4B435F31 5F56424F 42425941 4C494345 49DFEF30 9F81488C
        304CFF5A B3EE5A21 54367DC7 833150E0 A51F3EEB 4F2B5EE4
        5762C4F6 54C1A0C6 7F54CF88 B016B51B CE3D7C22 8D57ADB4

MacKey is
                                D9DA D952FDA8 BE9B1C3F 0962D5B2

Mtag is
                                                        AB02D5F4
        32638AA2 339EE0B5 07A31345 24EC7A1C 67A398A6 9D3BF981

KeyData is
                                                1DC8F87E 85B1D352
        12422E44 58FC1600 B2D45528 EC66ED6B B75E8714 B4EFBA31
        CD10B0CE B5CF74C4 80FAA515 716881E3 658C6202 B97D4E01

StaticUnifiedCDH(P-224)
---
dsU is
A273DD64
3AB8A64B 4B6E1FF9 C7ECF18E BC1F62DE 33450A9E 32E8A504

QsU_x is
FAD43A96
46721C46 52F13752 345FC2D5 25515A55 A170E685 314810E1

QsU_y is
E05BE902
7238C138 7F7C5575 ED425324 32929EFB C2C37293 1253F3D2

dsV is
723A6551
09089ED0 EDB4E630 72A82640 9F9C6204 635169F0 681F7514

QsV_x is
0898B1C4
B9308496 45F2E605 00DA0492 0CB70272 3E4E13F6 64C99B0B

QsV_y is
0D91CF88
A13435E4 D126DA64 352C75F2 B80C65F9 43D6F65A 6AC20F0B

---
no Key Confirmation
NonceU is
4327ABCA
DC176812 553A2E13 F68080BE D1BC6A1A 4F6FBB12 345EC9F9

Z is
9F18FF54
F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9

```
OtherInfo is
                                                    1234 56789ABC
        DEF0414C 49434531 3233E000 4327ABCA DC176812 553A2E13
        F68080BE D1BC6A1A 4F6FBB12 345EC9F9 424F4242 59343536


DerivedKeyMaterial is
                                                  3A15B245 C1EA216C
        5FEB3768 EABFB0F1 144477D4 AB41AC6C C6E73717 08B21A9B
        FC99DEBB 82AD4852 68037AC2 1FEF9BA5 54283FE3 6114230C


KeyData is
                                                  3A15B245 C1EA216C
        5FEB3768 EABFB0F1 144477D4 AB41AC6C C6E73717 08B21A9B
        FC99DEBB 82AD4852 68037AC2 1FEF9BA5 54283FE3 6114230C




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceU is
                                                    4327ABCA
        DC176812 553A2E13 F68080BE D1BC6A1A 4F6FBB12 345EC9F9


NonceV is
                                                    A863E43A
        B0C1163A 741A10AE F27BD6BE 6E8E3E45 0B8BCE01 DF0DA8B2


Z is
                                                    9F18FF54
        F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9


OtherInfo is
                                                    1234 56789ABC
        DEF0414C 49434531 3233E000 4327ABCA DC176812 553A2E13
        F68080BE D1BC6A1A 4F6FBB12 345EC9F9 424F4242 59343536


DerivedKeyMaterial is
            3A15 B245C1EA 216C5FEB 3768EABF B0F11444 77D4AB41
```

```
        AC6CC6E7 371708B2 1A9BFC99 DEBB82AD 48526803 7AC21FEF
        9BA55428 3FE36114 230C2C72 8DBDB69A 34153BF1 BAA71580


MacData is
        4B435F31 5F55414C 49434542 4F424259 4327ABCA DC176812
        553A2E13 F68080BE D1BC6A1A 4F6FBB12 345EC9F9 A863E43A
        B0C1163A 741A10AE F27BD6BE 6E8E3E45 0B8BCE01 DF0DA8B2


MacKey is
                            3A15 B245C1EA 216C5FEB 3768EABF


Mtag is
                                                    78EA5BF9
        DC24A78E A6D94FA1 46A8BC6F 5E29B63F 6B85695C 27425489


KeyData is
                                               B0F11444 77D4AB41
        AC6CC6E7 371708B2 1A9BFC99 DEBB82AD 48526803 7AC21FEF
        9BA55428 3FE36114 230C2C72 8DBDB69A 34153BF1 BAA71580




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
NonceV is
                                                    A863E43A
        B0C1163A 741A10AE F27BD6BE 6E8E3E45 0B8BCE01 DF0DA8B2


NonceU is
                                                    4327ABCA
        DC176812 553A2E13 F68080BE D1BC6A1A 4F6FBB12 345EC9F9


Z is
                                                    9F18FF54
        F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9


OtherInfo is
                                                1234 56789ABC
```

```
        DEF0414C 49434531 3233E000 4327ABCA DC176812 553A2E13
        F68080BE D1BC6A1A 4F6FBB12 345EC9F9 424F4242 59343536


DerivedKeyMaterial is
            3A15 B245C1EA 216C5FEB 3768EABF B0F11444 77D4AB41
        AC6CC6E7 371708B2 1A9BFC99 DEBB82AD 48526803 7AC21FEF
        9BA55428 3FE36114 230C2C72 8DBDB69A 34153BF1 BAA71580


MacData is
                 4B435F31 5F56424F 42425941 4C494345 4327ABCA
        DC176812 553A2E13 F68080BE D1BC6A1A 4F6FBB12 345EC9F9


MacKey is
                             3A15 B245C1EA 216C5FEB 3768EABF


Mtag is
                                                    8D3DCDAF
        B2E7F89B 2ACFC757 828BC46C E708C8AC 0D59DE08 95779651


KeyData is
                                               B0F11444 77D4AB41
        AC6CC6E7 371708B2 1A9BFC99 DEBB82AD 48526803 7AC21FEF
        9BA55428 3FE36114 230C2C72 8DBDB69A 34153BF1 BAA71580




-------------------------------------------------------------

Scheme Initiator, Key Confirmation Bilateral
NonceU is
                                                    4327ABCA
        DC176812 553A2E13 F68080BE D1BC6A1A 4F6FBB12 345EC9F9


NonceV is
                                                    A863E43A
        B0C1163A 741A10AE F27BD6BE 6E8E3E45 0B8BCE01 DF0DA8B2


Z is
```

                                                        9F18FF54
        F8872307 3F64A695 3D04914F 45A23EEE 7CFC4667 080AA0F9

OtherInfo is
                                                    1234 56789ABC
        DEF0414C 49434531 3233E000 4327ABCA DC176812 553A2E13
        F68080BE D1BC6A1A 4F6FBB12 345EC9F9 424F4242 59343536

DerivedKeyMaterial is
            3A15 B245C1EA 216C5FEB 3768EABF B0F11444 77D4AB41
        AC6CC6E7 371708B2 1A9BFC99 DEBB82AD 48526803 7AC21FEF
        9BA55428 3FE36114 230C2C72 8DBDB69A 34153BF1 BAA71580

U2V

MacData is
        4B435F32 5F55414C 49434542 4F424259 4327ABCA DC176812
        553A2E13 F68080BE D1BC6A1A 4F6FBB12 345EC9F9 A863E43A
        B0C1163A 741A10AE F27BD6BE 6E8E3E45 0B8BCE01 DF0DA8B2

MacKey is
                            3A15 B245C1EA 216C5FEB 3768EABF

Mtag is
                                                        701F901A
        59DB352A 63F83B7A 4AB75B70 E1676941 38F2A82E D877DA3E

V2U

MacData is
        4B435F32 5F56424F 42425941 4C494345 A863E43A B0C1163A
        741A10AE F27BD6BE 6E8E3E45 0B8BCE01 DF0DA8B2 4327ABCA
        DC176812 553A2E13 F68080BE D1BC6A1A 4F6FBB12 345EC9F9

MacKey is
                            3A15 B245C1EA 216C5FEB 3768EABF

Mtag is

```
                                                        CDF6A578
        6125F911 209D68F0 F58F16F5 ACEED698 A21394AE 4DA3C33D


KeyData is
                                               B0F11444 77D4AB41
        AC6CC6E7 371708B2 1A9BFC99 DEBB82AD 48526803 7AC21FEF
        9BA55428 3FE36114 230C2C72 8DBDB69A 34153BF1 BAA71580
```

FullUnifiedCDH(P-256)
---
dsU is
5DCDF2A3 3538D7CF
93A3680D 4CB4E86A 6814DA67 AC5D8323 EDBAAA59 FAAA2DE4

QsU_x is
E960C4EA 199B35D5
4CA122BB D85A61A3 0015FB9C 1FA43BE5 C04B4642 7D5206AB

QsU_y is
4EF04F38 77329ACF
60A13454 CC169266 6497DD57 B8705B0F C9459649 7E433532

dsV is
8FED7843 1D82558D
9006C3DE B06AB58D 9DCCC971 06875C67 25D5F166 255BA90A

QsV_x is
1B1631C5 DC76D378
A914C967 29D0A594 D54B4F58 845B1D4A 4B6BE739 CA4A18EA

QsV_y is
4F85E4C9 26EE5323
90AA7CD4 14943537 25E6E804 714AA69D 67072F65 DB625E07

deU is
81426414 5F2F56F2
E96A8E33 7A128499 3FAF432A 5ABCE59E 867B7291 D507A3AF

QeU_x is
2AF502F3 BE8952F2
C9B5A8D4 160D09E9 7165BE50 BC42AE4A 5E8D3B4B A83AEB15

QeU_y is
EB0FAF4C A986C4D3

8681A0F9 872D79D5 6795BD4B FF6E6DE3 C0F5015E CE5EFD85

deV is
2CE1788E C197E096
DB95A200 CC0AB26A 19CE6BCC AD562B8E EE1B5937 61CF7F41

QeV_x is
B120DE4A A3649279
5346E8DE 6C2C8646 AE06AAEA 279FA775 B3AB0715 F6CE51B0

QeV_y is
9F1B7EEC E20D7B5E
D8EC685F A3F071D8 37270270 92A84113 85C34DDE 5708B2B6

---

no Key Confirmation
Zs is
227684E7 1F5C313F
ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F

Ze is
DD0F5396 219D1EA3
93310412 D19A08F1 F5811E9D C8EC8EEA 7F80D21C 820C2788

Z is
DD0F5396 219D1EA3 93310412 D19A08F1
F5811E9D C8EC8EEA 7F80D21C 820C2788 227684E7 1F5C313F
ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
C08B3DE2 4F1A381E 7A5675A2 A6523B08
F354605E EE46B9F3 9EADB1E9 7534416D 98B43CAE 8AB04AFD
53DEB37F 44022352 C3FBDE1E 2F2CEC53 1CFC324F DD0FCCA6

```
KeyData is
                          C08B3DE2 4F1A381E 7A5675A2 A6523B08
        F354605E EE46B9F3 9EADB1E9 7534416D 98B43CAE 8AB04AFD
        53DEB37F 44022352 C3FBDE1E 2F2CEC53 1CFC324F DD0FCCA6



------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
Zs is
                                                227684E7 1F5C313F
        ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F


Ze is
                                                DD0F5396 219D1EA3
        93310412 D19A08F1 F5811E9D C8EC8EEA 7F80D21C 820C2788


Z is
                          DD0F5396 219D1EA3 93310412 D19A08F1
        F5811E9D C8EC8EEA 7F80D21C 820C2788 227684E7 1F5C313F
        ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                C08B3DE2 4F1A381E
        7A5675A2 A6523B08 F354605E EE46B9F3 9EADB1E9 7534416D
        98B43CAE 8AB04AFD 53DEB37F 44022352 C3FBDE1E 2F2CEC53
        1CFC324F DD0FCCA6 9B778342 70D4ED54 6720F5EF 269C95C2


MacData is
        4B435F31 5F55414C 49434542 4F424259 2AF502F3 BE8952F2
        C9B5A8D4 160D09E9 7165BE50 BC42AE4A 5E8D3B4B A83AEB15
        EB0FAF4C A986C4D3 8681A0F9 872D79D5 6795BD4B FF6E6DE3
        C0F5015E CE5EFD85 B120DE4A A3649279 5346E8DE 6C2C8646
        AE06AAEA 279FA775 B3AB0715 F6CE51B0 9F1B7EEC E20D7B5E
        D8EC685F A3F071D8 37270270 92A84113 85C34DDE 5708B2B6
```

MacKey is
                        C08B3DE2 4F1A381E 7A5675A2 A6523B08

Mtag is
                                            5CFD5CC4 D489476E
        65EE2E20 DF948DF9 A6B311B7 270CBEA1 9E309760 ECF2F4E4

KeyData is
                        F354605E EE46B9F3 9EADB1E9 7534416D
        98B43CAE 8AB04AFD 53DEB37F 44022352 C3FBDE1E 2F2CEC53
        1CFC324F DD0FCCA6 9B778342 70D4ED54 6720F5EF 269C95C2

Scheme Responder, Key Confirmation Provider: V to U
Zs is
                                            227684E7 1F5C313F
        ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F

Ze is
                                            DD0F5396 219D1EA3
        93310412 D19A08F1 F5811E9D C8EC8EEA 7F80D21C 820C2788

Z is
                        DD0F5396 219D1EA3 93310412 D19A08F1
        F5811E9D C8EC8EEA 7F80D21C 820C2788 227684E7 1F5C313F
        ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
                                            C08B3DE2 4F1A381E
        7A5675A2 A6523B08 F354605E EE46B9F3 9EADB1E9 7534416D
        98B43CAE 8AB04AFD 53DEB37F 44022352 C3FBDE1E 2F2CEC53
        1CFC324F DD0FCCA6 9B778342 70D4ED54 6720F5EF 269C95C2

```
MacData is
        4B435F31 5F56424F 42425941 4C494345 B120DE4A A3649279
        5346E8DE 6C2C8646 AE06AAEA 279FA775 B3AB0715 F6CE51B0
        9F1B7EEC E20D7B5E D8EC685F A3F071D8 37270270 92A84113
        85C34DDE 5708B2B6 2AF502F3 BE8952F2 C9B5A8D4 160D09E9
        7165BE50 BC42AE4A 5E8D3B4B A83AEB15 EB0FAF4C A986C4D3
        8681A0F9 872D79D5 6795BD4B FF6E6DE3 C0F5015E CE5EFD85


MacKey is
                         C08B3DE2 4F1A381E 7A5675A2 A6523B08


Mtag is
                                            206CBE5D 40AAAC1E
        678ED3F7 C248F4BF D3B1AE0E 60B3089A C179AAB7 B1D4FF55


KeyData is
                         F354605E EE46B9F3 9EADB1E9 7534416D
        98B43CAE 8AB04AFD 53DEB37F 44022352 C3FBDE1E 2F2CEC53
        1CFC324F DD0FCCA6 9B778342 70D4ED54 6720F5EF 269C95C2




------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
Zs is
                                            227684E7 1F5C313F
        ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F


Ze is
                                            DD0F5396 219D1EA3
        93310412 D19A08F1 F5811E9D C8EC8EEA 7F80D21C 820C2788


Z is
                         DD0F5396 219D1EA3 93310412 D19A08F1
        F5811E9D C8EC8EEA 7F80D21C 820C2788 227684E7 1F5C313F
        ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F
```

```
OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                            C08B3DE2 4F1A381E
        7A5675A2 A6523B08 F354605E EE46B9F3 9EADB1E9 7534416D
        98B43CAE 8AB04AFD 53DEB37F 44022352 C3FBDE1E 2F2CEC53
        1CFC324F DD0FCCA6 9B778342 70D4ED54 6720F5EF 269C95C2


U2V
----------------
MacData is
        4B435F32 5F55414C 49434542 4F424259 2AF502F3 BE8952F2
        C9B5A8D4 160D09E9 7165BE50 BC42AE4A 5E8D3B4B A83AEB15
        EB0FAF4C A986C4D3 8681A0F9 872D79D5 6795BD4B FF6E6DE3
        C0F5015E CE5EFD85 B120DE4A A3649279 5346E8DE 6C2C8646
        AE06AAEA 279FA775 B3AB0715 F6CE51B0 9F1B7EEC E20D7B5E
        D8EC685F A3F071D8 37270270 92A84113 85C34DDE 5708B2B6


MacKey is
                          C08B3DE2 4F1A381E 7A5675A2 A6523B08


Mtag is
                                            91C619A8 7851D80A
        1142688B 0CDDC3A1 A2B20147 CA2C0ECF 04265EAF 8448DA3B


V2U
----------------
MacData is
        4B435F32 5F56424F 42425941 4C494345 B120DE4A A3649279
        5346E8DE 6C2C8646 AE06AAEA 279FA775 B3AB0715 F6CE51B0
        9F1B7EEC E20D7B5E D8EC685F A3F071D8 37270270 92A84113
        85C34DDE 5708B2B6 2AF502F3 BE8952F2 C9B5A8D4 160D09E9
        7165BE50 BC42AE4A 5E8D3B4B A83AEB15 EB0FAF4C A986C4D3
        8681A0F9 872D79D5 6795BD4B FF6E6DE3 C0F5015E CE5EFD85


MacKey is
                          C08B3DE2 4F1A381E 7A5675A2 A6523B08
```

```
Mtag is
                                                F3267D2F E5CDBCEF
        E763E96E C3974832 1B32B0EF 737D97A2 74DE6502 88107E41


KeyData is
                            F354605E EE46B9F3 9EADB1E9 7534416D
        98B43CAE 8AB04AFD 53DEB37F 44022352 C3FBDE1E 2F2CEC53
        1CFC324F DD0FCCA6 9B778342 70D4ED54 6720F5EF 269C95C2




FullMQV(P-256)
------------------------------------------------------------
dsU is
                                                5DCDF2A3 3538D7CF
        93A3680D 4CB4E86A 6814DA67 AC5D8323 EDBAAA59 FAAA2DE4


QsU_x is
                                                E960C4EA 199B35D5
        4CA122BB D85A61A3 0015FB9C 1FA43BE5 C04B4642 7D5206AB


QsU_y is
                                                4EF04F38 77329ACF
        60A13454 CC169266 6497DD57 B8705B0F C9459649 7E433532


dsV is
                                                8FED7843 1D82558D
        9006C3DE B06AB58D 9DCCC971 06875C67 25D5F166 255BA90A


QsV_x is
                                                1B1631C5 DC76D378
        A914C967 29D0A594 D54B4F58 845B1D4A 4B6BE739 CA4A18EA


QsV_y is
                                                4F85E4C9 26EE5323
        90AA7CD4 14943537 25E6E804 714AA69D 67072F65 DB625E07


deU is
```

```
                                                81426414 5F2F56F2
        E96A8E33 7A128499 3FAF432A 5ABCE59E 867B7291 D507A3AF


QeU_x is
                                                2AF502F3 BE8952F2
        C9B5A8D4 160D09E9 7165BE50 BC42AE4A 5E8D3B4B A83AEB15


QeU_y is
                                                EB0FAF4C A986C4D3
        8681A0F9 872D79D5 6795BD4B FF6E6DE3 C0F5015E CE5EFD85


deV is
                                                2CE1788E C197E096
        DB95A200 CC0AB26A 19CE6BCC AD562B8E EE1B5937 61CF7F41


QeV_x is
                                                B120DE4A A3649279
        5346E8DE 6C2C8646 AE06AAEA 279FA775 B3AB0715 F6CE51B0


QeV_y is
                                                9F1B7EEC E20D7B5E
        D8EC685F A3F071D8 37270270 92A84113 85C34DDE 5708B2B6




------------------------------------------------------------
no Key Confirmation
Z is
                                                83050B73 1021FDBD
        B13FFE9F DE0373A8 C917C6FA 8106636C 1E1F7D15 64566219


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                            D71E0F55 D4EF4431 816EE299 715EA93D
        D116BDC8 803D66EA FEF37A07 5DB6A2A4 6AEF2BC5 D38A77EE
        40D34283 58580E87 99A4F70A E7353D69 AD2C964A 113ABFDD
```

KeyData is
                        D71E0F55 D4EF4431 816EE299 715EA93D
        D116BDC8 803D66EA FEF37A07 5DB6A2A4 6AEF2BC5 D38A77EE
        40D34283 58580E87 99A4F70A E7353D69 AD2C964A 113ABFDD

Scheme Initiator, Key Confirmation Provider: U to V
Z is
                                                83050B73 1021FDBD
        B13FFE9F DE0373A8 C917C6FA 8106636C 1E1F7D15 64566219

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
                                                D71E0F55 D4EF4431
        816EE299 715EA93D D116BDC8 803D66EA FEF37A07 5DB6A2A4
        6AEF2BC5 D38A77EE 40D34283 58580E87 99A4F70A E7353D69
        AD2C964A 113ABFDD 8129D8D2 3847448A 934B832D E3DFCFA8

MacData is
        4B435F31 5F55414C 49434542 4F424259 2AF502F3 BE8952F2
        C9B5A8D4 160D09E9 7165BE50 BC42AE4A 5E8D3B4B A83AEB15
        EB0FAF4C A986C4D3 8681A0F9 872D79D5 6795BD4B FF6E6DE3
        C0F5015E CE5EFD85 B120DE4A A3649279 5346E8DE 6C2C8646
        AE06AAEA 279FA775 B3AB0715 F6CE51B0 9F1B7EEC E20D7B5E
        D8EC685F A3F071D8 37270270 92A84113 85C34DDE 5708B2B6

MacKey is
                        D71E0F55 D4EF4431 816EE299 715EA93D

Mtag is
                                                19B74E52 B5966E9C
        49A31324 36F17A7F 51EF40D0 15F677B7 B8F3B7BB 455CE8D0

KeyData is
                        D116BDC8 803D66EA FEF37A07 5DB6A2A4
        6AEF2BC5 D38A77EE 40D34283 58580E87 99A4F70A E7353D69
        AD2C964A 113ABFDD 8129D8D2 3847448A 934B832D E3DFCFA8

Scheme Responder, Key Confirmation Provider: V to U
Z is
                                                83050B73 1021FDBD
        B13FFE9F DE0373A8 C917C6FA 8106636C 1E1F7D15 64566219

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
                                                D71E0F55 D4EF4431
        816EE299 715EA93D D116BDC8 803D66EA FEF37A07 5DB6A2A4
        6AEF2BC5 D38A77EE 40D34283 58580E87 99A4F70A E7353D69
        AD2C964A 113ABFDD 8129D8D2 3847448A 934B832D E3DFCFA8

MacData is
        4B435F31 5F56424F 42425941 4C494345 B120DE4A A3649279
        5346E8DE 6C2C8646 AE06AAEA 279FA775 B3AB0715 F6CE51B0
        9F1B7EEC E20D7B5E D8EC685F A3F071D8 37270270 92A84113
        85C34DDE 5708B2B6 2AF502F3 BE8952F2 C9B5A8D4 160D09E9
        7165BE50 BC42AE4A 5E8D3B4B A83AEB15 EB0FAF4C A986C4D3
        8681A0F9 872D79D5 6795BD4B FF6E6DE3 C0F5015E CE5EFD85

MacKey is
                        D71E0F55 D4EF4431 816EE299 715EA93D

Mtag is
                                                D638EDCF F42CAE22
        BDF90E84 FA3E9CE2 55CC8FCD CA176B8B CC42A5F0 7B3E77B0

KeyData is
                        D116BDC8 803D66EA FEF37A07 5DB6A2A4

```
        6AEF2BC5 D38A77EE 40D34283 58580E87 99A4F70A E7353D69
        AD2C964A 113ABFDD 8129D8D2 3847448A 934B832D E3DFCFA8



-------------------------------------------------------------

Scheme Initiator, Key Confirmation Bilateral
Z is
                                                83050B73 1021FDBD
        B13FFE9F DE0373A8 C917C6FA 8106636C 1E1F7D15 64566219


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                D71E0F55 D4EF4431
        816EE299 715EA93D D116BDC8 803D66EA FEF37A07 5DB6A2A4
        6AEF2BC5 D38A77EE 40D34283 58580E87 99A4F70A E7353D69
        AD2C964A 113ABFDD 8129D8D2 3847448A 934B832D E3DFCFA8


U2V
----------------
MacData is
        4B435F32 5F55414C 49434542 4F424259 2AF502F3 BE8952F2
        C9B5A8D4 160D09E9 7165BE50 BC42AE4A 5E8D3B4B A83AEB15
        EB0FAF4C A986C4D3 8681A0F9 872D79D5 6795BD4B FF6E6DE3
        C0F5015E CE5EFD85 B120DE4A A3649279 5346E8DE 6C2C8646
        AE06AAEA 279FA775 B3AB0715 F6CE51B0 9F1B7EEC E20D7B5E
        D8EC685F A3F071D8 37270270 92A84113 85C34DDE 5708B2B6


MacKey is
                          D71E0F55 D4EF4431 816EE299 715EA93D


Mtag is
                                                37690854 0BECD752
        958AB6CD 70AEF7DE 21091A9C C4B51B1F 64FBE347 8CBE0C84


V2U
```

```
----------------
MacData is
        4B435F32 5F56424F 42425941 4C494345 B120DE4A A3649279
        5346E8DE 6C2C8646 AE06AAEA 279FA775 B3AB0715 F6CE51B0
        9F1B7EEC E20D7B5E D8EC685F A3F071D8 37270270 92A84113
        85C34DDE 5708B2B6 2AF502F3 BE8952F2 C9B5A8D4 160D09E9
        7165BE50 BC42AE4A 5E8D3B4B A83AEB15 EB0FAF4C A986C4D3
        8681A0F9 872D79D5 6795BD4B FF6E6DE3 C0F5015E CE5EFD85


MacKey is
                        D71E0F55 D4EF4431 816EE299 715EA93D


Mtag is
                                          8ACB634F 83232041
        0F1AE1DA 4359D31B E87D3E62 2791D904 0B3A3687 948A24EE


KeyData is
                        D116BDC8 803D66EA FEF37A07 5DB6A2A4
        6AEF2BC5 D38A77EE 40D34283 58580E87 99A4F70A E7353D69
        AD2C964A 113ABFDD 8129D8D2 3847448A 934B832D E3DFCFA8




EphemeralUnifiedCDH(P-256)
------------------------------------------------------------
deU is
                                          81426414 5F2F56F2
        E96A8E33 7A128499 3FAF432A 5ABCE59E 867B7291 D507A3AF


QeU_x is
                                          2AF502F3 BE8952F2
        C9B5A8D4 160D09E9 7165BE50 BC42AE4A 5E8D3B4B A83AEB15


QeU_y is
                                          EB0FAF4C A986C4D3
        8681A0F9 872D79D5 6795BD4B FF6E6DE3 C0F5015E CE5EFD85


deV is
                                          2CE1788E C197E096
```

```
        DB95A200 CC0AB26A 19CE6BCC AD562B8E EE1B5937 61CF7F41


QeV_x is
                                                B120DE4A A3649279
        5346E8DE 6C2C8646 AE06AAEA 279FA775 B3AB0715 F6CE51B0


QeV_y is
                                                9F1B7EEC E20D7B5E
        D8EC685F A3F071D8 37270270 92A84113 85C34DDE 5708B2B6




------------------------------------------------------------
no Key Confirmation
Z is
                                                DD0F5396 219D1EA3
        93310412 D19A08F1 F5811E9D C8EC8EEA 7F80D21C 820C2788


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                            4C664A9B CA73D981 9538F659 B4B675C7
        2FB95AC2 F86527D9 8254F85E 1041CBFA 386EEA63 B4DA8803
        B31383B5 44D33A0B C781F7C2 F66A8CF4 1DE148E2 D3328173


KeyData is
                            4C664A9B CA73D981 9538F659 B4B675C7
        2FB95AC2 F86527D9 8254F85E 1041CBFA 386EEA63 B4DA8803
        B31383B5 44D33A0B C781F7C2 F66A8CF4 1DE148E2 D3328173




OnePassUnifiedCDH(P-256)
------------------------------------------------------------
dsU is
                                                5DCDF2A3 3538D7CF
        93A3680D 4CB4E86A 6814DA67 AC5D8323 EDBAAA59 FAAA2DE4
```

```
QsU_x is
                                                E960C4EA 199B35D5
        4CA122BB D85A61A3 0015FB9C 1FA43BE5 C04B4642 7D5206AB


QsU_y is
                                                4EF04F38 77329ACF
        60A13454 CC169266 6497DD57 B8705B0F C9459649 7E433532


dsV is
                                                8FED7843 1D82558D
        9006C3DE B06AB58D 9DCCC971 06875C67 25D5F166 255BA90A


QsV_x is
                                                1B1631C5 DC76D378
        A914C967 29D0A594 D54B4F58 845B1D4A 4B6BE739 CA4A18EA


QsV_y is
                                                4F85E4C9 26EE5323
        90AA7CD4 14943537 25E6E804 714AA69D 67072F65 DB625E07


deU is
                                                81426414 5F2F56F2
        E96A8E33 7A128499 3FAF432A 5ABCE59E 867B7291 D507A3AF


QeU_x is
                                                2AF502F3 BE8952F2
        C9B5A8D4 160D09E9 7165BE50 BC42AE4A 5E8D3B4B A83AEB15


QeU_y is
                                                EB0FAF4C A986C4D3
        8681A0F9 872D79D5 6795BD4B FF6E6DE3 C0F5015E CE5EFD85




------------------------------------------------------------
no Key Confirmation
Zs is
```

```
                                                227684E7 1F5C313F
        ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F


Ze is
                                                F9C34B92 ACEA12A0
        C50760E5 9D06C01F 72A0A5CD 8B1BFDD7 3DC8109A 8F8151B3


Z is
                         F9C34B92 ACEA12A0 C50760E5 9D06C01F
        72A0A5CD 8B1BFDD7 3DC8109A 8F8151B3 227684E7 1F5C313F
        ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                         C9FE943A B7241197 98158A10 E50DF332
        4593317C C9CBE7CD D4F99D11 B45E0C3B BAA16916 9C6D949A
        87450F4D 83B67C54 ADB69BEC D6271E83 5E22A058 7919484F


KeyData is
                         C9FE943A B7241197 98158A10 E50DF332
        4593317C C9CBE7CD D4F99D11 B45E0C3B BAA16916 9C6D949A
        87450F4D 83B67C54 ADB69BEC D6271E83 5E22A058 7919484F




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
                                                817807C9 E8826EE1
        CFB2F373 26D32195 585BD75A 5140460F D9BC7139 82B4D7DA


Zs is
                                                227684E7 1F5C313F
        ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F


Ze is
```

```
                                                F9C34B92 ACEA12A0
        C50760E5 9D06C01F 72A0A5CD 8B1BFDD7 3DC8109A 8F8151B3


Z is
                        F9C34B92 ACEA12A0 C50760E5 9D06C01F
        72A0A5CD 8B1BFDD7 3DC8109A 8F8151B3 227684E7 1F5C313F
        ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                C9FE943A B7241197
        98158A10 E50DF332 4593317C C9CBE7CD D4F99D11 B45E0C3B
        BAA16916 9C6D949A 87450F4D 83B67C54 ADB69BEC D6271E83
        5E22A058 7919484F FD288D71 BB78F910 B980487C 0631603B


MacData is
                        4B435F31 5F55414C 49434542 4F424259
        2AF502F3 BE8952F2 C9B5A8D4 160D09E9 7165BE50 BC42AE4A
        5E8D3B4B A83AEB15 EB0FAF4C A986C4D3 8681A0F9 872D79D5
        6795BD4B FF6E6DE3 C0F5015E CE5EFD85 817807C9 E8826EE1
        CFB2F373 26D32195 585BD75A 5140460F D9BC7139 82B4D7DA


MacKey is
                        C9FE943A B7241197 98158A10 E50DF332


Mtag is
                                                12DEF174 D12ADC8A
        2EAFB7B4 90B9CB10 F7514FDE 21EA2A5C E856EA63 D78E94C3


KeyData is
                        4593317C C9CBE7CD D4F99D11 B45E0C3B
        BAA16916 9C6D949A 87450F4D 83B67C54 ADB69BEC D6271E83
        5E22A058 7919484F FD288D71 BB78F910 B980487C 0631603B
```

```
------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
NonceU is
                                                817807C9 E8826EE1
        CFB2F373 26D32195 585BD75A 5140460F D9BC7139 82B4D7DA


Zs is
                                                227684E7 1F5C313F
        ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F


Ze is
                                                F9C34B92 ACEA12A0
        C50760E5 9D06C01F 72A0A5CD 8B1BFDD7 3DC8109A 8F8151B3


Z is
                        F9C34B92 ACEA12A0 C50760E5 9D06C01F
        72A0A5CD 8B1BFDD7 3DC8109A 8F8151B3 227684E7 1F5C313F
        ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                C9FE943A B7241197
        98158A10 E50DF332 4593317C C9CBE7CD D4F99D11 B45E0C3B
        BAA16916 9C6D949A 87450F4D 83B67C54 ADB69BEC D6271E83
        5E22A058 7919484F FD288D71 BB78F910 B980487C 0631603B


MacData is
                                                4B435F31 5F56424F
        42425941 4C494345 2AF502F3 BE8952F2 C9B5A8D4 160D09E9
        7165BE50 BC42AE4A 5E8D3B4B A83AEB15 EB0FAF4C A986C4D3
        8681A0F9 872D79D5 6795BD4B FF6E6DE3 C0F5015E CE5EFD85


MacKey is
                        C9FE943A B7241197 98158A10 E50DF332


Mtag is
```

```
                                                50DDD00D 351C9953
        9380B9E5 06005963 2E48FC1E 4E392E69 B7A20E0D 25078FAE


KeyData is
                            4593317C C9CBE7CD D4F99D11 B45E0C3B
        BAA16916 9C6D949A 87450F4D 83B67C54 ADB69BEC D6271E83
        5E22A058 7919484F FD288D71 BB78F910 B980487C 0631603B




------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
NonceV is
                                                817807C9 E8826EE1
        CFB2F373 26D32195 585BD75A 5140460F D9BC7139 82B4D7DA


Zs is
                                                227684E7 1F5C313F
        ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F


Ze is
                                                F9C34B92 ACEA12A0
        C50760E5 9D06C01F 72A0A5CD 8B1BFDD7 3DC8109A 8F8151B3


Z is
                            F9C34B92 ACEA12A0 C50760E5 9D06C01F
        72A0A5CD 8B1BFDD7 3DC8109A 8F8151B3 227684E7 1F5C313F
        ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                C9FE943A B7241197
        98158A10 E50DF332 4593317C C9CBE7CD D4F99D11 B45E0C3B
        BAA16916 9C6D949A 87450F4D 83B67C54 ADB69BEC D6271E83
        5E22A058 7919484F FD288D71 BB78F910 B980487C 0631603B
```

```
U2V
----------------
MacData is
                        4B435F32 5F55414C 49434542 4F424259
        2AF502F3 BE8952F2 C9B5A8D4 160D09E9 7165BE50 BC42AE4A
        5E8D3B4B A83AEB15 EB0FAF4C A986C4D3 8681A0F9 872D79D5
        6795BD4B FF6E6DE3 C0F5015E CE5EFD85 817807C9 E8826EE1
        CFB2F373 26D32195 585BD75A 5140460F D9BC7139 82B4D7DA


MacKey is
                        C9FE943A B7241197 98158A10 E50DF332


Mtag is
                                            41F50954 02FAA2D8
        17F0F865 03B5285D E6088DEC 4875230A 78EEE770 4CB4D96B


V2U
----------------
MacData is
                        4B435F32 5F56424F 42425941 4C494345
        817807C9 E8826EE1 CFB2F373 26D32195 585BD75A 5140460F
        D9BC7139 82B4D7DA 2AF502F3 BE8952F2 C9B5A8D4 160D09E9
        7165BE50 BC42AE4A 5E8D3B4B A83AEB15 EB0FAF4C A986C4D3
        8681A0F9 872D79D5 6795BD4B FF6E6DE3 C0F5015E CE5EFD85


MacKey is
                        C9FE943A B7241197 98158A10 E50DF332


Mtag is
                                            8C200B72 CF72375D
        30702D0B B9E3A398 1D4EA7EF F558928F 2F2F8DE5 52E016C3


KeyData is
                        4593317C C9CBE7CD D4F99D11 B45E0C3B
        BAA16916 9C6D949A 87450F4D 83B67C54 ADB69BEC D6271E83
        5E22A058 7919484F FD288D71 BB78F910 B980487C 0631603B
```

OnePassMQV(P-256)
---

dsU is
                                                5DCDF2A3 3538D7CF
        93A3680D 4CB4E86A 6814DA67 AC5D8323 EDBAAA59 FAAA2DE4

QsU_x is
                                                E960C4EA 199B35D5
        4CA122BB D85A61A3 0015FB9C 1FA43BE5 C04B4642 7D5206AB

QsU_y is
                                                4EF04F38 77329ACF
        60A13454 CC169266 6497DD57 B8705B0F C9459649 7E433532

dsV is
                                                8FED7843 1D82558D
        9006C3DE B06AB58D 9DCCC971 06875C67 25D5F166 255BA90A

QsV_x is
                                                1B1631C5 DC76D378
        A914C967 29D0A594 D54B4F58 845B1D4A 4B6BE739 CA4A18EA

QsV_y is
                                                4F85E4C9 26EE5323
        90AA7CD4 14943537 25E6E804 714AA69D 67072F65 DB625E07

deU is
                                                81426414 5F2F56F2
        E96A8E33 7A128499 3FAF432A 5ABCE59E 867B7291 D507A3AF

QeU_x is
                                                2AF502F3 BE8952F2
        C9B5A8D4 160D09E9 7165BE50 BC42AE4A 5E8D3B4B A83AEB15

QeU_y is
                                                EB0FAF4C A986C4D3
        8681A0F9 872D79D5 6795BD4B FF6E6DE3 C0F5015E CE5EFD85

```
------------------------------------------------------------
no Key Confirmation
Z is
                                            D67DA92B 55FCB46A
        A03E23E5 42F4184C E93C534D 4BE9E9AC F3327355 3DD47A5B


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                         139A77DD 97F7C9A3 D14F30B7 C27A0330
        2F392FED 08FC8839 9FF07B8B D2E34554 08F20BBC 72322228
        50F5C90A 14F52346 23C4D985 6F8C86A6 AACD2879 C4B5A626


KeyData is
                         139A77DD 97F7C9A3 D14F30B7 C27A0330
        2F392FED 08FC8839 9FF07B8B D2E34554 08F20BBC 72322228
        50F5C90A 14F52346 23C4D985 6F8C86A6 AACD2879 C4B5A626




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
                                            817807C9 E8826EE1
        CFB2F373 26D32195 585BD75A 5140460F D9BC7139 82B4D7DA


Z is
                                            D67DA92B 55FCB46A
        A03E23E5 42F4184C E93C534D 4BE9E9AC F3327355 3DD47A5B


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                            139A77DD 97F7C9A3
```

```
        D14F30B7 C27A0330 2F392FED 08FC8839 9FF07B8B D2E34554
        08F20BBC 72322228 50F5C90A 14F52346 23C4D985 6F8C86A6
        AACD2879 C4B5A626 4104CC9E A0DEF14F 11345D1F 0174389C


MacData is
                         4B435F31 5F55414C 49434542 4F424259
        2AF502F3 BE8952F2 C9B5A8D4 160D09E9 7165BE50 BC42AE4A
        5E8D3B4B A83AEB15 EB0FAF4C A986C4D3 8681A0F9 872D79D5
        6795BD4B FF6E6DE3 C0F5015E CE5EFD85 817807C9 E8826EE1
        CFB2F373 26D32195 585BD75A 5140460F D9BC7139 82B4D7DA


MacKey is
                         139A77DD 97F7C9A3 D14F30B7 C27A0330


Mtag is
                                           8C795D0E 97C8EF29
        C7A63AFE B581D6E7 53A75551 61255355 F26F35B2 56604CDD


KeyData is
                         2F392FED 08FC8839 9FF07B8B D2E34554
        08F20BBC 72322228 50F5C90A 14F52346 23C4D985 6F8C86A6
        AACD2879 C4B5A626 4104CC9E A0DEF14F 11345D1F 0174389C




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
NonceU is
                                           817807C9 E8826EE1
        CFB2F373 26D32195 585BD75A 5140460F D9BC7139 82B4D7DA


Z is
                                           D67DA92B 55FCB46A
        A03E23E5 42F4184C E93C534D 4BE9E9AC F3327355 3DD47A5B


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536
```

```
DerivedKeyMaterial is
                                                139A77DD 97F7C9A3
        D14F30B7 C27A0330 2F392FED 08FC8839 9FF07B8B D2E34554
        08F20BBC 72322228 50F5C90A 14F52346 23C4D985 6F8C86A6
        AACD2879 C4B5A626 4104CC9E A0DEF14F 11345D1F 0174389C


MacData is
                                                4B435F31 5F56424F
        42425941 4C494345 2AF502F3 BE8952F2 C9B5A8D4 160D09E9
        7165BE50 BC42AE4A 5E8D3B4B A83AEB15 EB0FAF4C A986C4D3
        8681A0F9 872D79D5 6795BD4B FF6E6DE3 C0F5015E CE5EFD85


MacKey is
                           139A77DD 97F7C9A3 D14F30B7 C27A0330


Mtag is
                                                518F4660 3D6E107A
        1C21EFDB 8D52028B FF32400A A8BF8763 876DEDFE 410003A3


KeyData is
                           2F392FED 08FC8839 9FF07B8B D2E34554
        08F20BBC 72322228 50F5C90A 14F52346 23C4D985 6F8C86A6
        AACD2879 C4B5A626 4104CC9E A0DEF14F 11345D1F 0174389C




------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
NonceV is
                                                817807C9 E8826EE1
        CFB2F373 26D32195 585BD75A 5140460F D9BC7139 82B4D7DA


Z is
                                                D67DA92B 55FCB46A
        A03E23E5 42F4184C E93C534D 4BE9E9AC F3327355 3DD47A5B


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536
```

```
DerivedKeyMaterial is
                                                139A77DD 97F7C9A3
        D14F30B7 C27A0330 2F392FED 08FC8839 9FF07B8B D2E34554
        08F20BBC 72322228 50F5C90A 14F52346 23C4D985 6F8C86A6
        AACD2879 C4B5A626 4104CC9E A0DEF14F 11345D1F 0174389C


U2V
----------------
MacData is
                        4B435F32 5F55414C 49434542 4F424259
        2AF502F3 BE8952F2 C9B5A8D4 160D09E9 7165BE50 BC42AE4A
        5E8D3B4B A83AEB15 EB0FAF4C A986C4D3 8681A0F9 872D79D5
        6795BD4B FF6E6DE3 C0F5015E CE5EFD85 817807C9 E8826EE1
        CFB2F373 26D32195 585BD75A 5140460F D9BC7139 82B4D7DA


MacKey is
                        139A77DD 97F7C9A3 D14F30B7 C27A0330


Mtag is
                                                9C14D68B A0421C8D
        70863331 AE7A6571 8575724C 49E6D27F 82DA2F9E BF8B53ED


V2U
----------------
MacData is
                        4B435F32 5F56424F 42425941 4C494345
        817807C9 E8826EE1 CFB2F373 26D32195 585BD75A 5140460F
        D9BC7139 82B4D7DA 2AF502F3 BE8952F2 C9B5A8D4 160D09E9
        7165BE50 BC42AE4A 5E8D3B4B A83AEB15 EB0FAF4C A986C4D3
        8681A0F9 872D79D5 6795BD4B FF6E6DE3 C0F5015E CE5EFD85


MacKey is
                        139A77DD 97F7C9A3 D14F30B7 C27A0330


Mtag is
                                                ACB99F03 D04B3310
        8C49EFB1 5566DD7C 2D567035 A55F2B71 FA015271 F42E8A68
```

```
KeyData is
                          2F392FED 08FC8839 9FF07B8B D2E34554
        08F20BBC 72322228 50F5C90A 14F52346 23C4D985 6F8C86A6
        AACD2879 C4B5A626 4104CC9E A0DEF14F 11345D1F 0174389C



OnePassDiffieHellmanCDH(P-256)
------------------------------------------------------------
dsV is
                                            8FED7843 1D82558D
        9006C3DE B06AB58D 9DCCC971 06875C67 25D5F166 255BA90A


QsV_x is
                                            1B1631C5 DC76D378
        A914C967 29D0A594 D54B4F58 845B1D4A 4B6BE739 CA4A18EA


QsV_y is
                                            4F85E4C9 26EE5323
        90AA7CD4 14943537 25E6E804 714AA69D 67072F65 DB625E07


deU is
                                            81426414 5F2F56F2
        E96A8E33 7A128499 3FAF432A 5ABCE59E 867B7291 D507A3AF


QeU_x is
                                            2AF502F3 BE8952F2
        C9B5A8D4 160D09E9 7165BE50 BC42AE4A 5E8D3B4B A83AEB15


QeU_y is
                                            EB0FAF4C A986C4D3
        8681A0F9 872D79D5 6795BD4B FF6E6DE3 C0F5015E CE5EFD85



------------------------------------------------------------
no Key Confirmation
Z is
                                            F9C34B92 ACEA12A0
```

```
        C50760E5 9D06C01F 72A0A5CD 8B1BFDD7 3DC8109A 8F8151B3


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                         C5BAF92F 8EBBE330 4A6CF682 764BDC7F
        55947A16 DCDB572A 0A0D20A0 5A47BBC4 37FC7C97 C2700009
        C8837D75 754E5796 CDFF537F 62D87E7F 5D2B6DF6 837367A8


KeyData is
                         C5BAF92F 8EBBE330 4A6CF682 764BDC7F
        55947A16 DCDB572A 0A0D20A0 5A47BBC4 37FC7C97 C2700009
        C8837D75 754E5796 CDFF537F 62D87E7F 5D2B6DF6 837367A8




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
Z is
                                            F9C34B92 ACEA12A0
        C50760E5 9D06C01F 72A0A5CD 8B1BFDD7 3DC8109A 8F8151B3


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                            C5BAF92F 8EBBE330
        4A6CF682 764BDC7F 55947A16 DCDB572A 0A0D20A0 5A47BBC4
        37FC7C97 C2700009 C8837D75 754E5796 CDFF537F 62D87E7F
        5D2B6DF6 837367A8 ECE5365E 3F286630 B1D592D7 3906AD5C


MacData is
                                            4B435F31 5F56424F
        42425941 4C494345 2AF502F3 BE8952F2 C9B5A8D4 160D09E9
        7165BE50 BC42AE4A 5E8D3B4B A83AEB15 EB0FAF4C A986C4D3
        8681A0F9 872D79D5 6795BD4B FF6E6DE3 C0F5015E CE5EFD85
```

MacKey is
                        C5BAF92F 8EBBE330 4A6CF682 764BDC7F

Mtag is
                                          0913AAAB 61FBE46A
        F3BDCA05 8690A909 214144EC 8370C5EA C376EA45 38EE01FD

KeyData is
                        55947A16 DCDB572A 0A0D20A0 5A47BBC4
        37FC7C97 C2700009 C8837D75 754E5796 CDFF537F 62D87E7F
        5D2B6DF6 837367A8 ECE5365E 3F286630 B1D592D7 3906AD5C

StaticUnifiedCDH(P-256)
----
dsU is
                                          5DCDF2A3 3538D7CF
        93A3680D 4CB4E86A 6814DA67 AC5D8323 EDBAAA59 FAAA2DE4

QsU_x is
                                          E960C4EA 199B35D5
        4CA122BB D85A61A3 0015FB9C 1FA43BE5 C04B4642 7D5206AB

QsU_y is
                                          4EF04F38 77329ACF
        60A13454 CC169266 6497DD57 B8705B0F C9459649 7E433532

dsV is
                                          8FED7843 1D82558D
        9006C3DE B06AB58D 9DCCC971 06875C67 25D5F166 255BA90A

QsV_x is
                                          1B1631C5 DC76D378
        A914C967 29D0A594 D54B4F58 845B1D4A 4B6BE739 CA4A18EA

QsV_y is
                                          4F85E4C9 26EE5323

```
        90AA7CD4 14943537 25E6E804 714AA69D 67072F65 DB625E07



------------------------------------------------------------
no Key Confirmation
NonceU is
                                                817807C9 E8826EE1
        CFB2F373 26D32195 585BD75A 5140460F D9BC7139 82B4D7DA


Z is
                                                227684E7 1F5C313F
        ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F


OtherInfo is
                                         1234 56789ABC DEF0414C
        49434531 32330001 817807C9 E8826EE1 CFB2F373 26D32195
        585BD75A 5140460F D9BC7139 82B4D7DA 424F4242 59343536


DerivedKeyMaterial is
                            D34157A9 2C809C89 3E78FED7 AFDEA43C
        FCC7F7E5 58CA9000 6E088BB4 74807F24 0843FE79 01A7CCF6
        911177D2 A3E3FB36 321D9789 D01E656E CA32C417 968118A9


KeyData is
                            D34157A9 2C809C89 3E78FED7 AFDEA43C
        FCC7F7E5 58CA9000 6E088BB4 74807F24 0843FE79 01A7CCF6
        911177D2 A3E3FB36 321D9789 D01E656E CA32C417 968118A9



------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceU is
                                                817807C9 E8826EE1
        CFB2F373 26D32195 585BD75A 5140460F D9BC7139 82B4D7DA


NonceV is
                                                604063F3 8D0FCEFB
```

```
        132880D3 29415F5A 701EFD62 6E35E72B F38A29DF 2FD653C3


Z is
                                            227684E7 1F5C313F
        ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F


OtherInfo is
                                       1234 56789ABC DEF0414C
        49434531 32330001 817807C9 E8826EE1 CFB2F373 26D32195
        585BD75A 5140460F D9BC7139 82B4D7DA 424F4242 59343536


DerivedKeyMaterial is
                                            D34157A9 2C809C89
        3E78FED7 AFDEA43C FCC7F7E5 58CA9000 6E088BB4 74807F24
        0843FE79 01A7CCF6 911177D2 A3E3FB36 321D9789 D01E656E
        CA32C417 968118A9 23B4925A 0989E5B5 60A38121 36A0B617


MacData is
                                            4B435F31 5F55414C
        49434542 4F424259 817807C9 E8826EE1 CFB2F373 26D32195
        585BD75A 5140460F D9BC7139 82B4D7DA 604063F3 8D0FCEFB
        132880D3 29415F5A 701EFD62 6E35E72B F38A29DF 2FD653C3


MacKey is
                         D34157A9 2C809C89 3E78FED7 AFDEA43C


Mtag is
                                            11358781 D1E2865F
        8206A688 ACFBCE80 F8D78325 2D6C0DB9 988D656D 92EB083B


KeyData is
                         FCC7F7E5 58CA9000 6E088BB4 74807F24
        0843FE79 01A7CCF6 911177D2 A3E3FB36 321D9789 D01E656E
        CA32C417 968118A9 23B4925A 0989E5B5 60A38121 36A0B617



-------------------------------------------------------------
```

Scheme Responder, Key Confirmation Provider: V to U
NonceV is
                                                604063F3 8D0FCEFB
        132880D3 29415F5A 701EFD62 6E35E72B F38A29DF 2FD653C3

NonceU is
                                                817807C9 E8826EE1
        CFB2F373 26D32195 585BD75A 5140460F D9BC7139 82B4D7DA

Z is
                                                227684E7 1F5C313F
        ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F

OtherInfo is
                                        1234 56789ABC DEF0414C
        49434531 32330001 817807C9 E8826EE1 CFB2F373 26D32195
        585BD75A 5140460F D9BC7139 82B4D7DA 424F4242 59343536

DerivedKeyMaterial is
                                                D34157A9 2C809C89
        3E78FED7 AFDEA43C FCC7F7E5 58CA9000 6E088BB4 74807F24
        0843FE79 01A7CCF6 911177D2 A3E3FB36 321D9789 D01E656E
        CA32C417 968118A9 23B4925A 0989E5B5 60A38121 36A0B617

MacData is
        4B435F31 5F56424F 42425941 4C494345 817807C9 E8826EE1
        CFB2F373 26D32195 585BD75A 5140460F D9BC7139 82B4D7DA

MacKey is
                        D34157A9 2C809C89 3E78FED7 AFDEA43C

Mtag is
                                                7EE04628 20045443
        52E6A270 37B64D7F 39DAC02F A69A462E 14E89AF8 74BAEBC2

KeyData is
                        FCC7F7E5 58CA9000 6E088BB4 74807F24
        0843FE79 01A7CCF6 911177D2 A3E3FB36 321D9789 D01E656E

```
        CA32C417 968118A9 23B4925A 0989E5B5 60A38121 36A0B617



-------------------------------------------------------------

Scheme Initiator, Key Confirmation Bilateral
NonceU is
                                                817807C9 E8826EE1
        CFB2F373 26D32195 585BD75A 5140460F D9BC7139 82B4D7DA


NonceV is
                                                604063F3 8D0FCEFB
        132880D3 29415F5A 701EFD62 6E35E72B F38A29DF 2FD653C3


Z is
                                                227684E7 1F5C313F
        ADC91E52 9807E314 7D53145B 15ABD6ED 416AD35C D7E6838F


OtherInfo is
                                          1234 56789ABC DEF0414C
        49434531 32330001 817807C9 E8826EE1 CFB2F373 26D32195
        585BD75A 5140460F D9BC7139 82B4D7DA 424F4242 59343536


DerivedKeyMaterial is
                                                D34157A9 2C809C89
        3E78FED7 AFDEA43C FCC7F7E5 58CA9000 6E088BB4 74807F24
        0843FE79 01A7CCF6 911177D2 A3E3FB36 321D9789 D01E656E
        CA32C417 968118A9 23B4925A 0989E5B5 60A38121 36A0B617


U2V
----------------
MacData is
                                                4B435F32 5F55414C
        49434542 4F424259 817807C9 E8826EE1 CFB2F373 26D32195
        585BD75A 5140460F D9BC7139 82B4D7DA 604063F3 8D0FCEFB
        132880D3 29415F5A 701EFD62 6E35E72B F38A29DF 2FD653C3


MacKey is
```

```
                        D34157A9 2C809C89 3E78FED7 AFDEA43C


Mtag is
                                                 BC463927 0152563D
        FE332A90 77F13CD0 7D11D268 BFA9D1E4 C357E016 2E442A13


V2U
----------------
MacData is
                                                 4B435F32 5F56424F
        42425941 4C494345 604063F3 8D0FCEFB 132880D3 29415F5A
        701EFD62 6E35E72B F38A29DF 2FD653C3 817807C9 E8826EE1
        CFB2F373 26D32195 585BD75A 5140460F D9BC7139 82B4D7DA


MacKey is
                        D34157A9 2C809C89 3E78FED7 AFDEA43C


Mtag is
                                                 955BA1CD 519C6218
        4A1A8EDA DA578889 F1F2304D 91542FCF 3B163EE6 11FA0221


KeyData is
                        FCC7F7E5 58CA9000 6E088BB4 74807F24
        0843FE79 01A7CCF6 911177D2 A3E3FB36 321D9789 D01E656E
        CA32C417 968118A9 23B4925A 0989E5B5 60A38121 36A0B617
```

FullUnifiedCDH(P-384)
---
dsU is
AA46C475 14D92CB6 F565A3AE 500944F6 760D9E74 F646D3D8
9FD09E76 85C41C1F 8DCEC4D7 FA5F91E2 23624A0B EF2FEF93

QsU_x is
B6E49C4B 30E3E642 843D84F4 8ED7D5FE 7254A0BD 057137EE
77F1F9EE D74DB4C8 C43B2010 65B8009E 9A925F3D 7040BDFF

QsU_y is
F502B3F9 841EA18B D8045102 CA2ED057 19CBC63F A338252D
EB0A1154 7B948938 265509B3 E2F4C848 4C7FA78F 321A1A15

dsV is
E7B8C2B3 E5422ACF C314D93D AD7B0025 730A0B38 0F13E4FE
03BDC0E0 0D9D63DA DF4AD600 EBFAA552 57B6DADC B772BB3A

QsV_x is
42B512E1 5235D548 457B651D 9AC448E7 8872DB45 854C4D48
F0F8FCDF 31579B43 0977406B 2008B94E D061D61B BF6B1BBB

QsV_y is
BFB3ED9E 7A69D765 EFDA14DE 7D0D8ECF 9B8BB3A0 3821EE88
8F5B45E9 DF755F55 292F9263 C765C463 B3FE786E 0C909A9D

deU is
D27335EA 71664AF2 44DD14E9 FD126071 5DFD8A79 65571C48
D709EE7A 7962A156 D706A90C BCB5DF29 86F05FEA DB9376F1

QeU_x is
793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66

QeU_y is
C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0

```
        6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128


deV is
        52D1791F DB4B70F8 9C0F00D4 56C2F702 3B612526 2C36A7DF
        1F802311 21CCE3D3 9BE52E00 C194A413 2C4A6C76 8BCD94D2


QeV_x is
        5CD42AB9 C41B5347 F74B8D4E FB708B3D 5B36DB65 915359B4
        4ABC1764 7B6B9999 789D72A8 4865AE2F 223F12B5 A1ABC120


QeV_y is
        E171458F EAA939AA A3A8BFAC 46B404BD 8F6D5B34 8C0FA4D8
        0CECA163 56CA9332 40BDE872 3415A8EC E035B0ED F36755DE




------------------------------------------------------------
no Key Confirmation
Zs is
        88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
        7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030


Ze is
        5EA1FC4A F7256D20 55981B11 0575E0A8 CAE53160 137D904C
        59D926EB 1B8456E4 27AA8A45 40884C37 DE159A58 028ABC0E


Z is
        5EA1FC4A F7256D20 55981B11 0575E0A8 CAE53160 137D904C
        59D926EB 1B8456E4 27AA8A45 40884C37 DE159A58 028ABC0E
        88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
        7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        8E6E265F 2082F14D 34DA23E1 032C9024 834AF015 72B66477
        82411BDD CB84A5DA EE117BA6 FBA6D0EB 2808EF8A B07005EE
```

```
        ABE52D2E FD31121C 7BF9D5FA FC40E00C 6D6DBF39 EF43FE97
        15C7202C DC2DB7E8 2B88D748 EB84258B F84D8582 F2BFD940


KeyData is
        8E6E265F 2082F14D 34DA23E1 032C9024 834AF015 72B66477
        82411BDD CB84A5DA EE117BA6 FBA6D0EB 2808EF8A B07005EE
        ABE52D2E FD31121C 7BF9D5FA FC40E00C 6D6DBF39 EF43FE97
        15C7202C DC2DB7E8 2B88D748 EB84258B F84D8582 F2BFD940




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
Zs is
        88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
        7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030


Ze is
        5EA1FC4A F7256D20 55981B11 0575E0A8 CAE53160 137D904C
        59D926EB 1B8456E4 27AA8A45 40884C37 DE159A58 028ABC0E


Z is
        5EA1FC4A F7256D20 55981B11 0575E0A8 CAE53160 137D904C
        59D926EB 1B8456E4 27AA8A45 40884C37 DE159A58 028ABC0E
        88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
        7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        8E6E265F 2082F14D 34DA23E1 032C9024 834AF015 72B66477
        82411BDD CB84A5DA EE117BA6 FBA6D0EB 2808EF8A B07005EE
        ABE52D2E FD31121C 7BF9D5FA FC40E00C 6D6DBF39 EF43FE97
        15C7202C DC2DB7E8 2B88D748 EB84258B F84D8582 F2BFD940
        8FF3FB6C AF48423D 583E7F9B AC45DE1A F19F3610 8ADB13F7


MacData is
                        4B435F31 5F55414C 49434542 4F424259
```

793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66
C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128
5CD42AB9 C41B5347 F74B8D4E FB708B3D 5B36DB65 915359B4
4ABC1764 7B6B9999 789D72A8 4865AE2F 223F12B5 A1ABC120
E171458F EAA939AA A3A8BFAC 46B404BD 8F6D5B34 8C0FA4D8
0CECA163 56CA9332 40BDE872 3415A8EC E035B0ED F36755DE

MacKey is
8E6E265F 2082F14D 34DA23E1 032C9024 834AF015 72B66477

Mtag is
48D78F1B A30800FD 7FA839ED 950A5FDD F885A572 A4EE2F41
C75B577B 39FEDC4E C8412235 A4F05EC0 B614B2EB D15FE6EE

KeyData is
82411BDD CB84A5DA EE117BA6 FBA6D0EB 2808EF8A B07005EE
ABE52D2E FD31121C 7BF9D5FA FC40E00C 6D6DBF39 EF43FE97
15C7202C DC2DB7E8 2B88D748 EB84258B F84D8582 F2BFD940
8FF3FB6C AF48423D 583E7F9B AC45DE1A F19F3610 8ADB13F7

Scheme Responder, Key Confirmation Provider: V to U
Zs is
88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030

Ze is
5EA1FC4A F7256D20 55981B11 0575E0A8 CAE53160 137D904C
59D926EB 1B8456E4 27AA8A45 40884C37 DE159A58 028ABC0E

Z is
5EA1FC4A F7256D20 55981B11 0575E0A8 CAE53160 137D904C
59D926EB 1B8456E4 27AA8A45 40884C37 DE159A58 028ABC0E
88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030

```
OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        8E6E265F 2082F14D 34DA23E1 032C9024 834AF015 72B66477
        82411BDD CB84A5DA EE117BA6 FBA6D0EB 2808EF8A B07005EE
        ABE52D2E FD31121C 7BF9D5FA FC40E00C 6D6DBF39 EF43FE97
        15C7202C DC2DB7E8 2B88D748 EB84258B F84D8582 F2BFD940
        8FF3FB6C AF48423D 583E7F9B AC45DE1A F19F3610 8ADB13F7


MacData is
                        4B435F31 5F56424F 42425941 4C494345
        5CD42AB9 C41B5347 F74B8D4E FB708B3D 5B36DB65 915359B4
        4ABC1764 7B6B9999 789D72A8 4865AE2F 223F12B5 A1ABC120
        E171458F EAA939AA A3A8BFAC 46B404BD 8F6D5B34 8C0FA4D8
        0CECA163 56CA9332 40BDE872 3415A8EC E035B0ED F36755DE
        793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
        0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66
        C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
        6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128


MacKey is
        8E6E265F 2082F14D 34DA23E1 032C9024 834AF015 72B66477


Mtag is
        2A4E289B B91D49E2 C11FA97A 52BB78B2 CCAAC949 FD218381
        442B3840 168F33F3 09728F38 BC93972B F1C121ED D0F5D01E


KeyData is
        82411BDD CB84A5DA EE117BA6 FBA6D0EB 2808EF8A B07005EE
        ABE52D2E FD31121C 7BF9D5FA FC40E00C 6D6DBF39 EF43FE97
        15C7202C DC2DB7E8 2B88D748 EB84258B F84D8582 F2BFD940
        8FF3FB6C AF48423D 583E7F9B AC45DE1A F19F3610 8ADB13F7




-------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
Zs is
```

```
        88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
        7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030


Ze is
        5EA1FC4A F7256D20 55981B11 0575E0A8 CAE53160 137D904C
        59D926EB 1B8456E4 27AA8A45 40884C37 DE159A58 028ABC0E


Z is
        5EA1FC4A F7256D20 55981B11 0575E0A8 CAE53160 137D904C
        59D926EB 1B8456E4 27AA8A45 40884C37 DE159A58 028ABC0E
        88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
        7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        8E6E265F 2082F14D 34DA23E1 032C9024 834AF015 72B66477
        82411BDD CB84A5DA EE117BA6 FBA6D0EB 2808EF8A B07005EE
        ABE52D2E FD31121C 7BF9D5FA FC40E00C 6D6DBF39 EF43FE97
        15C7202C DC2DB7E8 2B88D748 EB84258B F84D8582 F2BFD940
        8FF3FB6C AF48423D 583E7F9B AC45DE1A F19F3610 8ADB13F7


U2V
----------------
MacData is
                        4B435F32 5F55414C 49434542 4F424259
        793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
        0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66
        C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
        6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128
        5CD42AB9 C41B5347 F74B8D4E FB708B3D 5B36DB65 915359B4
        4ABC1764 7B6B9999 789D72A8 4865AE2F 223F12B5 A1ABC120
        E171458F EAA939AA A3A8BFAC 46B404BD 8F6D5B34 8C0FA4D8
        0CECA163 56CA9332 40BDE872 3415A8EC E035B0ED F36755DE


MacKey is
        8E6E265F 2082F14D 34DA23E1 032C9024 834AF015 72B66477
```

```
Mtag is
        4B86C08B FEF2B461 8FDA5905 4CE94123 35C8E24F 089356FC
        4CC07E78 832577D3 2565588B 16D48691 2A18185A 81CDEDB1


V2U
----------------
MacData is
                         4B435F32 5F56424F 42425941 4C494345
        5CD42AB9 C41B5347 F74B8D4E FB708B3D 5B36DB65 915359B4
        4ABC1764 7B6B9999 789D72A8 4865AE2F 223F12B5 A1ABC120
        E171458F EAA939AA A3A8BFAC 46B404BD 8F6D5B34 8C0FA4D8
        0CECA163 56CA9332 40BDE872 3415A8EC E035B0ED F36755DE
        793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
        0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66
        C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
        6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128


MacKey is
        8E6E265F 2082F14D 34DA23E1 032C9024 834AF015 72B66477


Mtag is
        AD9D7DD1 A85FD7F8 F2F3128C 732C84F5 6853A630 4FC60D57
        E1A11B24 F6A55E72 B43EE727 DDBB159F 9CD76A4E 175A75BA


KeyData is
        82411BDD CB84A5DA EE117BA6 FBA6D0EB 2808EF8A B07005EE
        ABE52D2E FD31121C 7BF9D5FA FC40E00C 6D6DBF39 EF43FE97
        15C7202C DC2DB7E8 2B88D748 EB84258B F84D8582 F2BFD940
        8FF3FB6C AF48423D 583E7F9B AC45DE1A F19F3610 8ADB13F7




FullMQV(P-384)
------------------------------------------------------------
dsU is
        AA46C475 14D92CB6 F565A3AE 500944F6 760D9E74 F646D3D8
        9FD09E76 85C41C1F 8DCEC4D7 FA5F91E2 23624A0B EF2FEF93


QsU_x is
        B6E49C4B 30E3E642 843D84F4 8ED7D5FE 7254A0BD 057137EE
```

77F1F9EE D74DB4C8 C43B2010 65B8009E 9A925F3D 7040BDFF

QsU_y is
F502B3F9 841EA18B D8045102 CA2ED057 19CBC63F A338252D
EB0A1154 7B948938 265509B3 E2F4C848 4C7FA78F 321A1A15

dsV is
E7B8C2B3 E5422ACF C314D93D AD7B0025 730A0B38 0F13E4FE
03BDC0E0 0D9D63DA DF4AD600 EBFAA552 57B6DADC B772BB3A

QsV_x is
42B512E1 5235D548 457B651D 9AC448E7 8872DB45 854C4D48
F0F8FCDF 31579B43 0977406B 2008B94E D061D61B BF6B1BBB

QsV_y is
BFB3ED9E 7A69D765 EFDA14DE 7D0D8ECF 9B8BB3A0 3821EE88
8F5B45E9 DF755F55 292F9263 C765C463 B3FE786E 0C909A9D

deU is
D27335EA 71664AF2 44DD14E9 FD126071 5DFD8A79 65571C48
D709EE7A 7962A156 D706A90C BCB5DF29 86F05FEA DB9376F1

QeU_x is
793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66

QeU_y is
C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128

deV is
52D1791F DB4B70F8 9C0F00D4 56C2F702 3B612526 2C36A7DF
1F802311 21CCE3D3 9BE52E00 C194A413 2C4A6C76 8BCD94D2

QeV_x is
5CD42AB9 C41B5347 F74B8D4E FB708B3D 5B36DB65 915359B4
4ABC1764 7B6B9999 789D72A8 4865AE2F 223F12B5 A1ABC120

```
QeV_y is
        E171458F EAA939AA A3A8BFAC 46B404BD 8F6D5B34 8C0FA4D8
        0CECA163 56CA9332 40BDE872 3415A8EC E035B0ED F36755DE




------------------------------------------------------------
no Key Confirmation
Z is
        25329E26 86FFA271 D821F39C 1D3CD1FA F0D5CA3E 0BF60F30
        57D62674 036DE771 50EDCE94 B28E5D21 1F8DFF9C 4C1199AB


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        1DF6B2E9 313FEE5A B5F7B447 57AB1F9C 061EB276 96F3C0F3
        F42D63B8 752801BE 1CCE0D03 AB484B7A 26F2DAD0 47FD20B5
        D2B79935 518D47C1 B1FD69B7 B118DE21 CB8ABC6C B0C07020
        AAD2CBB3 B24B6497 CFCBE174 07D619EA EBD49141 BCB3A42C


KeyData is
        1DF6B2E9 313FEE5A B5F7B447 57AB1F9C 061EB276 96F3C0F3
        F42D63B8 752801BE 1CCE0D03 AB484B7A 26F2DAD0 47FD20B5
        D2B79935 518D47C1 B1FD69B7 B118DE21 CB8ABC6C B0C07020
        AAD2CBB3 B24B6497 CFCBE174 07D619EA EBD49141 BCB3A42C




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
Z is
        25329E26 86FFA271 D821F39C 1D3CD1FA F0D5CA3E 0BF60F30
        57D62674 036DE771 50EDCE94 B28E5D21 1F8DFF9C 4C1199AB


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536
```

```
DerivedKeyMaterial is
        1DF6B2E9 313FEE5A B5F7B447 57AB1F9C 061EB276 96F3C0F3
        F42D63B8 752801BE 1CCE0D03 AB484B7A 26F2DAD0 47FD20B5
        D2B79935 518D47C1 B1FD69B7 B118DE21 CB8ABC6C B0C07020
        AAD2CBB3 B24B6497 CFCBE174 07D619EA EBD49141 BCB3A42C
        9103992A 26E24A91 09E4AE20 5272C3D4 1F479F8B 1BF6E931


MacData is
                         4B435F31 5F55414C 49434542 4F424259
        793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
        0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66
        C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
        6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128
        5CD42AB9 C41B5347 F74B8D4E FB708B3D 5B36DB65 915359B4
        4ABC1764 7B6B9999 789D72A8 4865AE2F 223F12B5 A1ABC120
        E171458F EAA939AA A3A8BFAC 46B404BD 8F6D5B34 8C0FA4D8
        0CECA163 56CA9332 40BDE872 3415A8EC E035B0ED F36755DE


MacKey is
        1DF6B2E9 313FEE5A B5F7B447 57AB1F9C 061EB276 96F3C0F3


Mtag is
        A139D711 09C0EFC1 6609A7A1 9425156F 726FA351 E80DEC4D
        2BC15183 ECCE8B41 1004983D 9CF996DA FFF152E7 1BD70B0A


KeyData is
        F42D63B8 752801BE 1CCE0D03 AB484B7A 26F2DAD0 47FD20B5
        D2B79935 518D47C1 B1FD69B7 B118DE21 CB8ABC6C B0C07020
        AAD2CBB3 B24B6497 CFCBE174 07D619EA EBD49141 BCB3A42C
        9103992A 26E24A91 09E4AE20 5272C3D4 1F479F8B 1BF6E931




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
Z is
        25329E26 86FFA271 D821F39C 1D3CD1FA F0D5CA3E 0BF60F30
        57D62674 036DE771 50EDCE94 B28E5D21 1F8DFF9C 4C1199AB
```

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
        1DF6B2E9 313FEE5A B5F7B447 57AB1F9C 061EB276 96F3C0F3
        F42D63B8 752801BE 1CCE0D03 AB484B7A 26F2DAD0 47FD20B5
        D2B79935 518D47C1 B1FD69B7 B118DE21 CB8ABC6C B0C07020
        AAD2CBB3 B24B6497 CFCBE174 07D619EA EBD49141 BCB3A42C
        9103992A 26E24A91 09E4AE20 5272C3D4 1F479F8B 1BF6E931

MacData is
                        4B435F31 5F56424F 42425941 4C494345
        5CD42AB9 C41B5347 F74B8D4E FB708B3D 5B36DB65 915359B4
        4ABC1764 7B6B9999 789D72A8 4865AE2F 223F12B5 A1ABC120
        E171458F EAA939AA A3A8BFAC 46B404BD 8F6D5B34 8C0FA4D8
        0CECA163 56CA9332 40BDE872 3415A8EC E035B0ED F36755DE
        793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
        0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66
        C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
        6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128

MacKey is
        1DF6B2E9 313FEE5A B5F7B447 57AB1F9C 061EB276 96F3C0F3

Mtag is
        1DF9E920 5DB9591F DECB0DC6 892B1AD9 CFC9C38A 27D7F345
        9CB2CBDC 95B92672 480DCB77 2861656B A9C9E5BD 7D5A1467

KeyData is
        F42D63B8 752801BE 1CCE0D03 AB484B7A 26F2DAD0 47FD20B5
        D2B79935 518D47C1 B1FD69B7 B118DE21 CB8ABC6C B0C07020
        AAD2CBB3 B24B6497 CFCBE174 07D619EA EBD49141 BCB3A42C
        9103992A 26E24A91 09E4AE20 5272C3D4 1F479F8B 1BF6E931

Scheme Initiator, Key Confirmation Bilateral
Z is

```
        25329E26 86FFA271 D821F39C 1D3CD1FA F0D5CA3E 0BF60F30
        57D62674 036DE771 50EDCE94 B28E5D21 1F8DFF9C 4C1199AB


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        1DF6B2E9 313FEE5A B5F7B447 57AB1F9C 061EB276 96F3C0F3
        F42D63B8 752801BE 1CCE0D03 AB484B7A 26F2DAD0 47FD20B5
        D2B79935 518D47C1 B1FD69B7 B118DE21 CB8ABC6C B0C07020
        AAD2CBB3 B24B6497 CFCBE174 07D619EA EBD49141 BCB3A42C
        9103992A 26E24A91 09E4AE20 5272C3D4 1F479F8B 1BF6E931


U2V
----------------
MacData is
                        4B435F32 5F55414C 49434542 4F424259
        793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
        0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66
        C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
        6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128
        5CD42AB9 C41B5347 F74B8D4E FB708B3D 5B36DB65 915359B4
        4ABC1764 7B6B9999 789D72A8 4865AE2F 223F12B5 A1ABC120
        E171458F EAA939AA A3A8BFAC 46B404BD 8F6D5B34 8C0FA4D8
        0CECA163 56CA9332 40BDE872 3415A8EC E035B0ED F36755DE


MacKey is
        1DF6B2E9 313FEE5A B5F7B447 57AB1F9C 061EB276 96F3C0F3


Mtag is
        096852B0 1E118249 E4B7A1E1 9BE128AC 147EB34B 19B0135B
        D61D33EC FC5CBEC1 EE6079AA 965C1C6A C2FEAEBF BB41E846


V2U
----------------
MacData is
                        4B435F32 5F56424F 42425941 4C494345
        5CD42AB9 C41B5347 F74B8D4E FB708B3D 5B36DB65 915359B4
        4ABC1764 7B6B9999 789D72A8 4865AE2F 223F12B5 A1ABC120
        E171458F EAA939AA A3A8BFAC 46B404BD 8F6D5B34 8C0FA4D8
```

```
        0CECA163 56CA9332 40BDE872 3415A8EC E035B0ED F36755DE
        793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
        0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66
        C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
        6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128


MacKey is
        1DF6B2E9 313FEE5A B5F7B447 57AB1F9C 061EB276 96F3C0F3


Mtag is
        F91066DE D3765AFA FE5006C6 E6B193EF B3EAB284 8B7042CC
        37EA3302 8D52AE92 3BC9FBF1 F943FE06 CAF93CCD 01740218


KeyData is
        F42D63B8 752801BE 1CCE0D03 AB484B7A 26F2DAD0 47FD20B5
        D2B79935 518D47C1 B1FD69B7 B118DE21 CB8ABC6C B0C07020
        AAD2CBB3 B24B6497 CFCBE174 07D619EA EBD49141 BCB3A42C
        9103992A 26E24A91 09E4AE20 5272C3D4 1F479F8B 1BF6E931




EphemeralUnifiedCDH(P-384)
------------------------------------------------------------
deU is
        D27335EA 71664AF2 44DD14E9 FD126071 5DFD8A79 65571C48
        D709EE7A 7962A156 D706A90C BCB5DF29 86F05FEA DB9376F1


QeU_x is
        793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
        0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66


QeU_y is
        C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
        6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128


deV is
        52D1791F DB4B70F8 9C0F00D4 56C2F702 3B612526 2C36A7DF
        1F802311 21CCE3D3 9BE52E00 C194A413 2C4A6C76 8BCD94D2
```

```
QeV_x is
        5CD42AB9 C41B5347 F74B8D4E FB708B3D 5B36DB65 915359B4
        4ABC1764 7B6B9999 789D72A8 4865AE2F 223F12B5 A1ABC120


QeV_y is
        E171458F EAA939AA A3A8BFAC 46B404BD 8F6D5B34 8C0FA4D8
        0CECA163 56CA9332 40BDE872 3415A8EC E035B0ED F36755DE




------------------------------------------------------------
no Key Confirmation
Z is
        5EA1FC4A F7256D20 55981B11 0575E0A8 CAE53160 137D904C
        59D926EB 1B8456E4 27AA8A45 40884C37 DE159A58 028ABC0E


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        95824CDC 9774A4F2 5A9DD4C2 C18A604E 0F103E54 0E80EBD7
        8DD260C1 520C6E54 3C558DFB 429CCC81 FDD3DDE2 3A5DD1A6
        89813FF1 17E2A33E 52A7DAE0 996F857E 99B2B5C7 4365642A
        FE953EAB 155766B9 C78AE255 A74622CE DD505304 3FA716EE


KeyData is
        95824CDC 9774A4F2 5A9DD4C2 C18A604E 0F103E54 0E80EBD7
        8DD260C1 520C6E54 3C558DFB 429CCC81 FDD3DDE2 3A5DD1A6
        89813FF1 17E2A33E 52A7DAE0 996F857E 99B2B5C7 4365642A
        FE953EAB 155766B9 C78AE255 A74622CE DD505304 3FA716EE




OnePassUnifiedCDH(P-384)
------------------------------------------------------------
dsU is
        AA46C475 14D92CB6 F565A3AE 500944F6 760D9E74 F646D3D8
        9FD09E76 85C41C1F 8DCEC4D7 FA5F91E2 23624A0B EF2FEF93
```

```
QsU_x is
        B6E49C4B 30E3E642 843D84F4 8ED7D5FE 7254A0BD 057137EE
        77F1F9EE D74DB4C8 C43B2010 65B8009E 9A925F3D 7040BDFF


QsU_y is
        F502B3F9 841EA18B D8045102 CA2ED057 19CBC63F A338252D
        EB0A1154 7B948938 265509B3 E2F4C848 4C7FA78F 321A1A15


dsV is
        E7B8C2B3 E5422ACF C314D93D AD7B0025 730A0B38 0F13E4FE
        03BDC0E0 0D9D63DA DF4AD600 EBFAA552 57B6DADC B772BB3A


QsV_x is
        42B512E1 5235D548 457B651D 9AC448E7 8872DB45 854C4D48
        F0F8FCDF 31579B43 0977406B 2008B94E D061D61B BF6B1BBB


QsV_y is
        BFB3ED9E 7A69D765 EFDA14DE 7D0D8ECF 9B8BB3A0 3821EE88
        8F5B45E9 DF755F55 292F9263 C765C463 B3FE786E 0C909A9D


deU is
        D27335EA 71664AF2 44DD14E9 FD126071 5DFD8A79 65571C48
        D709EE7A 7962A156 D706A90C BCB5DF29 86F05FEA DB9376F1


QeU_x is
        793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
        0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66


QeU_y is
        C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
        6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128




------------------------------------------------------------
no Key Confirmation
Zs is
```

88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030

Ze is
B2672A91 6BE1EC91 F6A2C618 74735152 B081949C 1FF53D1E
0BC2BC29 87985A40 7AD10961 0AC0990F 8ED2867E AC2D34DF

Z is
B2672A91 6BE1EC91 F6A2C618 74735152 B081949C 1FF53D1E
0BC2BC29 87985A40 7AD10961 0AC0990F 8ED2867E AC2D34DF
88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
BBB8BB84 83D17952 2D15241A 237D6C08 BD3C0161 CD3349EF
9F685494 DA85750C E7B5B585 621DDF3E 161BA9EB 253E61B4
82117082 1EC98372 C50DA5A1 B5480CCB A738E877 A2FC9081
A1C20484 9A93431A 4B959596 8340D8D1 98E64BA0 68F3856C

KeyData is
BBB8BB84 83D17952 2D15241A 237D6C08 BD3C0161 CD3349EF
9F685494 DA85750C E7B5B585 621DDF3E 161BA9EB 253E61B4
82117082 1EC98372 C50DA5A1 B5480CCB A738E877 A2FC9081
A1C20484 9A93431A 4B959596 8340D8D1 98E64BA0 68F3856C

Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988

Zs is
88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030

Ze is
        B2672A91 6BE1EC91 F6A2C618 74735152 B081949C 1FF53D1E
        0BC2BC29 87985A40 7AD10961 0AC0990F 8ED2867E AC2D34DF

Z is
        B2672A91 6BE1EC91 F6A2C618 74735152 B081949C 1FF53D1E
        0BC2BC29 87985A40 7AD10961 0AC0990F 8ED2867E AC2D34DF
        88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
        7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
        BBB8BB84 83D17952 2D15241A 237D6C08 BD3C0161 CD3349EF
        9F685494 DA85750C E7B5B585 621DDF3E 161BA9EB 253E61B4
        82117082 1EC98372 C50DA5A1 B5480CCB A738E877 A2FC9081
        A1C20484 9A93431A 4B959596 8340D8D1 98E64BA0 68F3856C
        2DD07262 81DAC0DD 7818DADC A7A4A8E4 4C540319 811CA08E

MacData is
                        4B435F31 5F55414C 49434542 4F424259
        793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
        0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66
        C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
        6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128
        F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
        ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988

MacKey is
        BBB8BB84 83D17952 2D15241A 237D6C08 BD3C0161 CD3349EF

Mtag is
        30AFDA64 2BCE5992 D861FDEC 68ACD4A7 EA07B9DD F6B5326A
        82608A4F 2A228E52 7F729393 D5A3C13D 4ACE2201 372FA071

KeyData is

9F685494 DA85750C E7B5B585 621DDF3E 161BA9EB 253E61B4
82117082 1EC98372 C50DA5A1 B5480CCB A738E877 A2FC9081
A1C20484 9A93431A 4B959596 8340D8D1 98E64BA0 68F3856C
2DD07262 81DAC0DD 7818DADC A7A4A8E4 4C540319 811CA08E

Scheme Responder, Key Confirmation Provider: V to U
NonceU is
F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988

Zs is
88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030

Ze is
B2672A91 6BE1EC91 F6A2C618 74735152 B081949C 1FF53D1E
0BC2BC29 87985A40 7AD10961 0AC0990F 8ED2867E AC2D34DF

Z is
B2672A91 6BE1EC91 F6A2C618 74735152 B081949C 1FF53D1E
0BC2BC29 87985A40 7AD10961 0AC0990F 8ED2867E AC2D34DF
88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
BBB8BB84 83D17952 2D15241A 237D6C08 BD3C0161 CD3349EF
9F685494 DA85750C E7B5B585 621DDF3E 161BA9EB 253E61B4
82117082 1EC98372 C50DA5A1 B5480CCB A738E877 A2FC9081
A1C20484 9A93431A 4B959596 8340D8D1 98E64BA0 68F3856C
2DD07262 81DAC0DD 7818DADC A7A4A8E4 4C540319 811CA08E

MacData is
4B435F31 5F56424F 42425941 4C494345

793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66
C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128

MacKey is
BBB8BB84 83D17952 2D15241A 237D6C08 BD3C0161 CD3349EF

Mtag is
C8A6E9F3 F376380B 42DE44B5 270536AA 81969EE9 DCDBEB05
81C0E644 A7F31274 4B0E47C8 44C11B4A E7F05350 C9A46E93

KeyData is
9F685494 DA85750C E7B5B585 621DDF3E 161BA9EB 253E61B4
82117082 1EC98372 C50DA5A1 B5480CCB A738E877 A2FC9081
A1C20484 9A93431A 4B959596 8340D8D1 98E64BA0 68F3856C
2DD07262 81DAC0DD 7818DADC A7A4A8E4 4C540319 811CA08E

Scheme Initiator, Key Confirmation Bilateral
NonceV is
F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988

Zs is
88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030

Ze is
B2672A91 6BE1EC91 F6A2C618 74735152 B081949C 1FF53D1E
0BC2BC29 87985A40 7AD10961 0AC0990F 8ED2867E AC2D34DF

Z is
B2672A91 6BE1EC91 F6A2C618 74735152 B081949C 1FF53D1E
0BC2BC29 87985A40 7AD10961 0AC0990F 8ED2867E AC2D34DF
88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030

```
OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        BBB8BB84 83D17952 2D15241A 237D6C08 BD3C0161 CD3349EF
        9F685494 DA85750C E7B5B585 621DDF3E 161BA9EB 253E61B4
        82117082 1EC98372 C50DA5A1 B5480CCB A738E877 A2FC9081
        A1C20484 9A93431A 4B959596 8340D8D1 98E64BA0 68F3856C
        2DD07262 81DAC0DD 7818DADC A7A4A8E4 4C540319 811CA08E


U2V
----------------
MacData is
                        4B435F32 5F55414C 49434542 4F424259
        793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
        0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66
        C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
        6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128
        F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
        ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988


MacKey is
        BBB8BB84 83D17952 2D15241A 237D6C08 BD3C0161 CD3349EF


Mtag is
        8BAE5D2C F589947A D2619F1A D07FC5F0 5DF4685F AF36DFD7
        3F70D1C6 10C98890 D97FE138 023CE4B7 47C7FC2F 84610FB6


V2U
----------------
MacData is
                        4B435F32 5F56424F 42425941 4C494345
        F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
        ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988
        793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
        0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66
        C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
        6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128
```

MacKey is
        BBB8BB84 83D17952 2D15241A 237D6C08 BD3C0161 CD3349EF

Mtag is
        FB92A939 E1E6B83F D74FA8D2 29DD7219 E238E900 C917C8E1
        F570E908 007A97E3 E72F1EAC F8259620 67AE57A2 BE873EE7

KeyData is
        9F685494 DA85750C E7B5B585 621DDF3E 161BA9EB 253E61B4
        82117082 1EC98372 C50DA5A1 B5480CCB A738E877 A2FC9081
        A1C20484 9A93431A 4B959596 8340D8D1 98E64BA0 68F3856C
        2DD07262 81DAC0DD 7818DADC A7A4A8E4 4C540319 811CA08E

OnePassMQV(P-384)
---
dsU is
        AA46C475 14D92CB6 F565A3AE 500944F6 760D9E74 F646D3D8
        9FD09E76 85C41C1F 8DCEC4D7 FA5F91E2 23624A0B EF2FEF93

QsU_x is
        B6E49C4B 30E3E642 843D84F4 8ED7D5FE 7254A0BD 057137EE
        77F1F9EE D74DB4C8 C43B2010 65B8009E 9A925F3D 7040BDFF

QsU_y is
        F502B3F9 841EA18B D8045102 CA2ED057 19CBC63F A338252D
        EB0A1154 7B948938 265509B3 E2F4C848 4C7FA78F 321A1A15

dsV is
        E7B8C2B3 E5422ACF C314D93D AD7B0025 730A0B38 0F13E4FE
        03BDC0E0 0D9D63DA DF4AD600 EBFAA552 57B6DADC B772BB3A

QsV_x is
        42B512E1 5235D548 457B651D 9AC448E7 8872DB45 854C4D48
        F0F8FCDF 31579B43 0977406B 2008B94E D061D61B BF6B1BBB

```
QsV_y is
        BFB3ED9E 7A69D765 EFDA14DE 7D0D8ECF 9B8BB3A0 3821EE88
        8F5B45E9 DF755F55 292F9263 C765C463 B3FE786E 0C909A9D


deU is
        D27335EA 71664AF2 44DD14E9 FD126071 5DFD8A79 65571C48
        D709EE7A 7962A156 D706A90C BCB5DF29 86F05FEA DB9376F1


QeU_x is
        793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
        0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66


QeU_y is
        C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
        6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128




------------------------------------------------------------
no Key Confirmation
Z is
        EE9D0DAC 7A2FFA32 F77933D0 91026A94 5D913FDA EB4B8020
        1E19DF45 C1902316 F95BB133 654C8002 D88BF81B EF2F4F6A


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        B95685CB 37D2439F C1EFA320 2A137842 88F4EAD2 D52FBFA0
        0C3017E6 E4979AB7 ECA63546 3374B707 DEB8C25A 6511F5FF
        EB03920C D04F856B 83C78BD9 A35B5EE7 89636982 88C2642C
        2CF15381 CA210529 43551A30 CB5D1847 C4403CEC 5D2807D6


KeyData is
        B95685CB 37D2439F C1EFA320 2A137842 88F4EAD2 D52FBFA0
        0C3017E6 E4979AB7 ECA63546 3374B707 DEB8C25A 6511F5FF
        EB03920C D04F856B 83C78BD9 A35B5EE7 89636982 88C2642C
        2CF15381 CA210529 43551A30 CB5D1847 C4403CEC 5D2807D6
```

```
------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
        F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
        ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988


Z is
        EE9D0DAC 7A2FFA32 F77933D0 91026A94 5D913FDA EB4B8020
        1E19DF45 C1902316 F95BB133 654C8002 D88BF81B EF2F4F6A


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        B95685CB 37D2439F C1EFA320 2A137842 88F4EAD2 D52FBFA0
        0C3017E6 E4979AB7 ECA63546 3374B707 DEB8C25A 6511F5FF
        EB03920C D04F856B 83C78BD9 A35B5EE7 89636982 88C2642C
        2CF15381 CA210529 43551A30 CB5D1847 C4403CEC 5D2807D6
        D19FABD8 4414764F 513FDD8A 1E45EB79 D8CC4BD2 8792C812


MacData is
                         4B435F31 5F55414C 49434542 4F424259
        793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
        0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66
        C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
        6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128
        F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
        ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988


MacKey is
        B95685CB 37D2439F C1EFA320 2A137842 88F4EAD2 D52FBFA0


Mtag is
        87C99855 88B8D0F9 7F4DC1D8 5E25D6B0 1820DB34 4FBF3468
        FACAE44B 977BFE73 FB9AA595 9539A0C7 CC6DD154 8610F058
```

KeyData is
0C3017E6 E4979AB7 ECA63546 3374B707 DEB8C25A 6511F5FF
EB03920C D04F856B 83C78BD9 A35B5EE7 89636982 88C2642C
2CF15381 CA210529 43551A30 CB5D1847 C4403CEC 5D2807D6
D19FABD8 4414764F 513FDD8A 1E45EB79 D8CC4BD2 8792C812

Scheme Responder, Key Confirmation Provider: V to U
NonceU is
F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988

Z is
EE9D0DAC 7A2FFA32 F77933D0 91026A94 5D913FDA EB4B8020
1E19DF45 C1902316 F95BB133 654C8002 D88BF81B EF2F4F6A

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
B95685CB 37D2439F C1EFA320 2A137842 88F4EAD2 D52FBFA0
0C3017E6 E4979AB7 ECA63546 3374B707 DEB8C25A 6511F5FF
EB03920C D04F856B 83C78BD9 A35B5EE7 89636982 88C2642C
2CF15381 CA210529 43551A30 CB5D1847 C4403CEC 5D2807D6
D19FABD8 4414764F 513FDD8A 1E45EB79 D8CC4BD2 8792C812

MacData is
4B435F31 5F56424F 42425941 4C494345
793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66
C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128

MacKey is
B95685CB 37D2439F C1EFA320 2A137842 88F4EAD2 D52FBFA0

Mtag is

```
        D75DECD4 5AFF89A8 D1F1224A 587AA819 2F9F9C85 50145776
        BC55AFC0 C6B6081C 165FD393 61C45F4A BA4B557F 5FF0AC9F


KeyData is
        0C3017E6 E4979AB7 ECA63546 3374B707 DEB8C25A 6511F5FF
        EB03920C D04F856B 83C78BD9 A35B5EE7 89636982 88C2642C
        2CF15381 CA210529 43551A30 CB5D1847 C4403CEC 5D2807D6
        D19FABD8 4414764F 513FDD8A 1E45EB79 D8CC4BD2 8792C812




------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
NonceV is
        F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
        ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988


Z is
        EE9D0DAC 7A2FFA32 F77933D0 91026A94 5D913FDA EB4B8020
        1E19DF45 C1902316 F95BB133 654C8002 D88BF81B EF2F4F6A


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
        B95685CB 37D2439F C1EFA320 2A137842 88F4EAD2 D52FBFA0
        0C3017E6 E4979AB7 ECA63546 3374B707 DEB8C25A 6511F5FF
        EB03920C D04F856B 83C78BD9 A35B5EE7 89636982 88C2642C
        2CF15381 CA210529 43551A30 CB5D1847 C4403CEC 5D2807D6
        D19FABD8 4414764F 513FDD8A 1E45EB79 D8CC4BD2 8792C812


U2V
----------------
MacData is
                        4B435F32 5F55414C 49434542 4F424259
        793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
        0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66
        C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
        6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128
        F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
```

```
        ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988


MacKey is
        B95685CB 37D2439F C1EFA320 2A137842 88F4EAD2 D52FBFA0


Mtag is
        EEFF3280 6231D206 46383A7F BBF244E2 FF823922 BBDF9EFF
        72FA7908 3E3DBBA1 308A3583 BD65B5FC BAB91282 3E2D7DBF


V2U
----------------
MacData is
                         4B435F32 5F56424F 42425941 4C494345
        F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
        ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988
        793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
        0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66
        C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
        6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128


MacKey is
        B95685CB 37D2439F C1EFA320 2A137842 88F4EAD2 D52FBFA0


Mtag is
        65609F84 0027D9B1 3035EA69 450C4DBE 49A0D34A BFFE2FEA
        EAF67FCC E1093264 A90D2BDF 317FA9C7 D90EE22B 1D916E57


KeyData is
        0C3017E6 E4979AB7 ECA63546 3374B707 DEB8C25A 6511F5FF
        EB03920C D04F856B 83C78BD9 A35B5EE7 89636982 88C2642C
        2CF15381 CA210529 43551A30 CB5D1847 C4403CEC 5D2807D6
        D19FABD8 4414764F 513FDD8A 1E45EB79 D8CC4BD2 8792C812




OnePassDiffieHellmanCDH(P-384)
------------------------------------------------------------
dsV is
        E7B8C2B3 E5422ACF C314D93D AD7B0025 730A0B38 0F13E4FE
```

03BDC0E0 0D9D63DA DF4AD600 EBFAA552 57B6DADC B772BB3A

QsV_x is
42B512E1 5235D548 457B651D 9AC448E7 8872DB45 854C4D48
F0F8FCDF 31579B43 0977406B 2008B94E D061D61B BF6B1BBB

QsV_y is
BFB3ED9E 7A69D765 EFDA14DE 7D0D8ECF 9B8BB3A0 3821EE88
8F5B45E9 DF755F55 292F9263 C765C463 B3FE786E 0C909A9D

deU is
D27335EA 71664AF2 44DD14E9 FD126071 5DFD8A79 65571C48
D709EE7A 7962A156 D706A90C BCB5DF29 86F05FEA DB9376F1

QeU_x is
793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66

QeU_y is
C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128

---

no Key Confirmation
Z is
B2672A91 6BE1EC91 F6A2C618 74735152 B081949C 1FF53D1E
0BC2BC29 87985A40 7AD10961 0AC0990F 8ED2867E AC2D34DF

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
9F14D953 BE79A0F0 19FBEC23 0574FEF2 0FDD37E7 68E01C3E
B5EDDD24 BB2682D9 44731656 7DAA372E FA5CB467 61F50402
A7D7B473 A280DE54 C56D7FE8 56BBD745 52148D85 D7625678
56B080E0 DABE441D 59520D45 14017736 5F9CACF1 1B54DB2E

KeyData is
        9F14D953 BE79A0F0 19FBEC23 0574FEF2 0FDD37E7 68E01C3E
        B5EDDD24 BB2682D9 44731656 7DAA372E FA5CB467 61F50402
        A7D7B473 A280DE54 C56D7FE8 56BBD745 52148D85 D7625678
        56B080E0 DABE441D 59520D45 14017736 5F9CACF1 1B54DB2E

Scheme Responder, Key Confirmation Provider: V to U
Z is
        B2672A91 6BE1EC91 F6A2C618 74735152 B081949C 1FF53D1E
        0BC2BC29 87985A40 7AD10961 0AC0990F 8ED2867E AC2D34DF

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
        9F14D953 BE79A0F0 19FBEC23 0574FEF2 0FDD37E7 68E01C3E
        B5EDDD24 BB2682D9 44731656 7DAA372E FA5CB467 61F50402
        A7D7B473 A280DE54 C56D7FE8 56BBD745 52148D85 D7625678
        56B080E0 DABE441D 59520D45 14017736 5F9CACF1 1B54DB2E
        730EA8FB BFA8FE4A 6227F998 CC4DBA63 6136F159 001059CF

MacData is
                        4B435F31 5F56424F 42425941 4C494345
        793148F1 787634D5 DA4C6D90 74417D05 E057AB62 F82054D1
        0EE6B040 3D627954 7E6A8EA9 D1FD7742 7D016FE2 7A8B8C66
        C6C41294 331D23E6 F480F4FB 4CD40504 C947392E 94F4C3F0
        6B8F398B B29E4236 8F7A6859 23DE3B67 BACED214 A1A1D128

MacKey is
        9F14D953 BE79A0F0 19FBEC23 0574FEF2 0FDD37E7 68E01C3E

Mtag is
        545245CD CFB724EB 57BA7FD0 B7B21A3D EC7B953E 54A1ABE6
        696D912C 0277EC2E C2830F0B 7E53F58D C2B368A0 5A58093F

KeyData is
	B5EDDD24 BB2682D9 44731656 7DAA372E FA5CB467 61F50402
	A7D7B473 A280DE54 C56D7FE8 56BBD745 52148D85 D7625678
	56B080E0 DABE441D 59520D45 14017736 5F9CACF1 1B54DB2E
	730EA8FB BFA8FE4A 6227F998 CC4DBA63 6136F159 001059CF

StaticUnifiedCDH(P-384)
---
dsU is
	AA46C475 14D92CB6 F565A3AE 500944F6 760D9E74 F646D3D8
	9FD09E76 85C41C1F 8DCEC4D7 FA5F91E2 23624A0B EF2FEF93

QsU_x is
	B6E49C4B 30E3E642 843D84F4 8ED7D5FE 7254A0BD 057137EE
	77F1F9EE D74DB4C8 C43B2010 65B8009E 9A925F3D 7040BDFF

QsU_y is
	F502B3F9 841EA18B D8045102 CA2ED057 19CBC63F A338252D
	EB0A1154 7B948938 265509B3 E2F4C848 4C7FA78F 321A1A15

dsV is
	E7B8C2B3 E5422ACF C314D93D AD7B0025 730A0B38 0F13E4FE
	03BDC0E0 0D9D63DA DF4AD600 EBFAA552 57B6DADC B772BB3A

QsV_x is
	42B512E1 5235D548 457B651D 9AC448E7 8872DB45 854C4D48
	F0F8FCDF 31579B43 0977406B 2008B94E D061D61B BF6B1BBB

QsV_y is
	BFB3ED9E 7A69D765 EFDA14DE 7D0D8ECF 9B8BB3A0 3821EE88
	8F5B45E9 DF755F55 292F9263 C765C463 B3FE786E 0C909A9D

---
no Key Confirmation

```
NonceU is
        F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
        ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988


Z is
        88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
        7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030


OtherInfo is
                                                          1234
        56789ABC DEF0414C 49434531 32338001 F19737D1 F8452AC6
        3510BC35 D3444440 F4DC2C8A EEDBF0F9 ADBA62C9 1DBF5FB7
        DEC1DBDA 032C7F8C E54ACF60 2F922988 424F4242 59343536


DerivedKeyMaterial is
        973A6753 E146E77B 32F134EF 72394029 C0686DC4 3BB6D9EF
        E3291C4A 38399224 CD519938 122C6472 FAF19EE1 4997A2A7
        3A607E72 C639ABD9 A405E086 D1BB79B8 CD9E7C97 B5D8FD56
        DD35593C 8376A0A5 39863BB0 53201319 FCBEFC7C DD5450CB


KeyData is
        973A6753 E146E77B 32F134EF 72394029 C0686DC4 3BB6D9EF
        E3291C4A 38399224 CD519938 122C6472 FAF19EE1 4997A2A7
        3A607E72 C639ABD9 A405E086 D1BB79B8 CD9E7C97 B5D8FD56
        DD35593C 8376A0A5 39863BB0 53201319 FCBEFC7C DD5450CB




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceU is
        F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
        ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988


NonceV is
        5A452352 1700C41A AED50DE4 BA622E46 FADAC9BE 771DBD0F
        95664DF2 D4116AD2 B58136C2 87DE481D A491F4AC 2CAA687F


Z is
```

```
        88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
        7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030


OtherInfo is
                                                          1234
        56789ABC DEF0414C 49434531 32338001 F19737D1 F8452AC6
        3510BC35 D3444440 F4DC2C8A EEDBF0F9 ADBA62C9 1DBF5FB7
        DEC1DBDA 032C7F8C E54ACF60 2F922988 424F4242 59343536


DerivedKeyMaterial is
        973A6753 E146E77B 32F134EF 72394029 C0686DC4 3BB6D9EF
        E3291C4A 38399224 CD519938 122C6472 FAF19EE1 4997A2A7
        3A607E72 C639ABD9 A405E086 D1BB79B8 CD9E7C97 B5D8FD56
        DD35593C 8376A0A5 39863BB0 53201319 FCBEFC7C DD5450CB
        33BDBE3F 58C025CE 51B9196A DB386F8F 5FEB7DF7 AB7433B9


MacData is
                         4B435F31 5F55414C 49434542 4F424259
        F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
        ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988
        5A452352 1700C41A AED50DE4 BA622E46 FADAC9BE 771DBD0F
        95664DF2 D4116AD2 B58136C2 87DE481D A491F4AC 2CAA687F


MacKey is
        973A6753 E146E77B 32F134EF 72394029 C0686DC4 3BB6D9EF


Mtag is
        7638E87E 6D616F2B 3DE4A120 EF20CCAC 21AFD521 69B9E100
        FD426AB7 3AE8A2E7 D9C564F9 E2F9D8C2 27A600DC 1297050C


KeyData is
        E3291C4A 38399224 CD519938 122C6472 FAF19EE1 4997A2A7
        3A607E72 C639ABD9 A405E086 D1BB79B8 CD9E7C97 B5D8FD56
        DD35593C 8376A0A5 39863BB0 53201319 FCBEFC7C DD5450CB
        33BDBE3F 58C025CE 51B9196A DB386F8F 5FEB7DF7 AB7433B9




-------------------------------------------------------------
```

Scheme Responder, Key Confirmation Provider: V to U
NonceV is
        5A452352 1700C41A AED50DE4 BA622E46 FADAC9BE 771DBD0F
        95664DF2 D4116AD2 B58136C2 87DE481D A491F4AC 2CAA687F

NonceU is
        F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
        ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988

Z is
        88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
        7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030

OtherInfo is
                                                        1234
        56789ABC DEF0414C 49434531 32338001 F19737D1 F8452AC6
        3510BC35 D3444440 F4DC2C8A EEDBF0F9 ADBA62C9 1DBF5FB7
        DEC1DBDA 032C7F8C E54ACF60 2F922988 424F4242 59343536

DerivedKeyMaterial is
        973A6753 E146E77B 32F134EF 72394029 C0686DC4 3BB6D9EF
        E3291C4A 38399224 CD519938 122C6472 FAF19EE1 4997A2A7
        3A607E72 C639ABD9 A405E086 D1BB79B8 CD9E7C97 B5D8FD56
        DD35593C 8376A0A5 39863BB0 53201319 FCBEFC7C DD5450CB
        33BDBE3F 58C025CE 51B9196A DB386F8F 5FEB7DF7 AB7433B9

MacData is
                            4B435F31 5F56424F 42425941 4C494345
        F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
        ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988

MacKey is
        973A6753 E146E77B 32F134EF 72394029 C0686DC4 3BB6D9EF

Mtag is
        E39200D9 02F1193F F39B7FB3 683F1BB0 D8945BD2 9D1F6E38
        4B71684A 7B1B92B6 005EB0BA 76FE53B4 3E604498 9820C623

```
KeyData is
        E3291C4A 38399224 CD519938 122C6472 FAF19EE1 4997A2A7
        3A607E72 C639ABD9 A405E086 D1BB79B8 CD9E7C97 B5D8FD56
        DD35593C 8376A0A5 39863BB0 53201319 FCBEFC7C DD5450CB
        33BDBE3F 58C025CE 51B9196A DB386F8F 5FEB7DF7 AB7433B9



------------------------------------------------------------

Scheme Initiator, Key Confirmation Bilateral
NonceU is
        F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
        ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988


NonceV is
        5A452352 1700C41A AED50DE4 BA622E46 FADAC9BE 771DBD0F
        95664DF2 D4116AD2 B58136C2 87DE481D A491F4AC 2CAA687F


Z is
        88769CB7 2FC5AC45 7CD58E89 089B196A 70BF533C 6DC91C9C
        7E1741DB 5E7AB6B0 849F01DE A65FEDD0 6C77187C D88ED030


OtherInfo is
                                                          1234
        56789ABC DEF0414C 49434531 32338001 F19737D1 F8452AC6
        3510BC35 D3444440 F4DC2C8A EEDBF0F9 ADBA62C9 1DBF5FB7
        DEC1DBDA 032C7F8C E54ACF60 2F922988 424F4242 59343536


DerivedKeyMaterial is
        973A6753 E146E77B 32F134EF 72394029 C0686DC4 3BB6D9EF
        E3291C4A 38399224 CD519938 122C6472 FAF19EE1 4997A2A7
        3A607E72 C639ABD9 A405E086 D1BB79B8 CD9E7C97 B5D8FD56
        DD35593C 8376A0A5 39863BB0 53201319 FCBEFC7C DD5450CB
        33BDBE3F 58C025CE 51B9196A DB386F8F 5FEB7DF7 AB7433B9


U2V
----------------
MacData is
                          4B435F32 5F55414C 49434542 4F424259
```

```
        F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
        ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988
        5A452352 1700C41A AED50DE4 BA622E46 FADAC9BE 771DBD0F
        95664DF2 D4116AD2 B58136C2 87DE481D A491F4AC 2CAA687F


MacKey is
        973A6753 E146E77B 32F134EF 72394029 C0686DC4 3BB6D9EF


Mtag is
        EB224525 C906CBF9 FF252E37 AF00020E 93D397B5 014A6051
        4062C08F 3949DBD7 D097F22D 691CCC87 7DB2FE64 746F9CEA


V2U
----------------
MacData is
                         4B435F32 5F56424F 42425941 4C494345
        5A452352 1700C41A AED50DE4 BA622E46 FADAC9BE 771DBD0F
        95664DF2 D4116AD2 B58136C2 87DE481D A491F4AC 2CAA687F
        F19737D1 F8452AC6 3510BC35 D3444440 F4DC2C8A EEDBF0F9
        ADBA62C9 1DBF5FB7 DEC1DBDA 032C7F8C E54ACF60 2F922988


MacKey is
        973A6753 E146E77B 32F134EF 72394029 C0686DC4 3BB6D9EF


Mtag is
        1DD2EC31 FFBF133F 9F1908E1 E3F2F206 05EC5675 5D168381
        499D7296 7AD75398 C5DAE6D0 B6DE4EB1 819D199D D77F51A0


KeyData is
        E3291C4A 38399224 CD519938 122C6472 FAF19EE1 4997A2A7
        3A607E72 C639ABD9 A405E086 D1BB79B8 CD9E7C97 B5D8FD56
        DD35593C 8376A0A5 39863BB0 53201319 FCBEFC7C DD5450CB
        33BDBE3F 58C025CE 51B9196A DB386F8F 5FEB7DF7 AB7433B9
```

FullUnifiedCDH(P-521)
----
dsU is
                    017D 1527DCC7 C046E4D3 04600ED0 D3A625F6
        AA46C475 14D92CB6 A6416C1B 8978B3E6 E9796830 6FFC49D0
        0371CCBD 4B796AA3 6547A6ED 3E78BBDF F2CFF34C E4C57FC9

QsU_x is
                    00D0 C2D9A667 F85A3C27 0C838535 04616791
        F3052858 3CF2D5CD D35D4E77 D440FE51 01DFC0E1 953983A9
        C1D7C330 7E6213FB CEB3D113 460D7B45 BBACAE5D 54B68166

QsU_y is
                    01C8 A85F0367 B3B1F4DE 8A74021E 08E13EA5
        65EF012E 647DD317 3B21DD6B B9987155 73063EBB 3152CAA7
        91ABD47F D31FB528 799413F8 DFF76E28 64E9870A 262ECACB

dsV is
                    00A0 752E306C ECD87AB0 E4830DA1 44F8038C
        E7B8C2B3 E5422ACF 9AAA6CCF 21818316 9A4CCA2A D577A64E
        6D86DCBF F5C1727A 11FD1CB8 E3A53842 B84005FD A9AC7F36

QsV_x is
                    0128 C16B23A4 259C9FE4 257C1DA4 3C7735C4
        3337929E 0FD86CC2 A778975B 67184CC2 825F6E66 7876D404
        BBF03E04 1F8FAD2F CCC036CD 5448B64E 9BD7DF6F 537659BB

QsV_y is
                    0108 089A6431 FED52344 DD5859A0 E5432D16
        9BEE36F5 3F857AED 08A69FE3 07B1C94B 8ABDCF65 0C4D1297
        29D69FB7 7D1CC1CD 651C676B 309CE018 C9771EAB 9CA5A754

deU is
                    0113 F82DA825 735E3D97 276683B2 B74277BA
        D27335EA 71664AF2 430CC4F3 3459B966 9EE78B3F FB9B8683
        015D344D CBFEF6FB 9AF4C6C4 70BE2545 16CD3C1A 1FB47362

QeU_x is
01EB B34DD757 21ABF8AD C9DBED17 889CBB97
65D90A7C 60F2CEF0 07BB0F2B 26E14881 FD4442E6 89D61CB2
DD046EE3 0E3FFD20 F9A45BBD F6413D58 3A2DBF59 924FD35C

QeU_y is
00F6 B632D194 C0388E22 D8437E55 8C552AE1
95ADFD15 3F92D749 08351B2F 8C4EDA94 EDB0916D 1B53C020
B5EECAED 1A5FC38A 233E4830 587BB2EE 3489B3B4 2A5A86A4

deV is
00CE E3480D86 45A17D24 9F2776D2 8BAE6169
52D1791F DB4B70F7 C3378732 AA1B2292 8448BCD1 DC2496D4
35B01048 066EBE4F 72903C36 1B1A9DC1 193DC2C9 D0891B96

QeV_x is
010E BFAFC6E8 5E08D24B FFFCC1A4 511DB0E6
34BEEB1B 6DEC8C59 39AE4476 6201AF62 00430BA9 7C8AC6A0
E9F08B33 CE7E9FEE B5BA4EE5 E0D81510 C24295B8 A08D0235

QeV_y is
00A4 A6EC300D F9E257B0 372B5E7A BFEF0934
36719A77 887EBB0B 18CF8099 B9F4212B 6E30A141 9C18E029
D36863CC 9D448F4D BA4D2A0E 60711BE5 72915FBD 4FEF2695

---

no Key Confirmation
Zs is
0138 A672B695 8BD784E5 D7FA8373 8AC68F9B
3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4

Ze is
00CD EA89621C FA46B132 F9E4CFE2 261CDE2D
4368EB56 56634C7C C98C7A00 CDE54ED1 866A0DD3 E6126C9D
2F845DAF F82CEB1D A08F5D87 521BB0EB ECA77911 169C20CC

```
Z is
                                  00CDEA89 621CFA46 B132F9E4
        CFE2261C DE2D4368 EB565663 4C7CC98C 7A00CDE5 4ED1866A
        0DD3E612 6C9D2F84 5DAFF82C EB1DA08F 5D87521B B0EBECA7
        7911169C 20CC0138 A672B695 8BD784E5 D7FA8373 8AC68F9B
        3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
        F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                              2D4A46A1 7099BAA8
        330BC59D 4A1CF5AE 3A3075B4 C62BB26E 7FC98924 726D274C
        09646F44 08E6858C 43B42DAE D015EF26 1708D55E F24DAA7D
        3EA3D1C4 A08CFD24 DB6000A5 B8A67DE7 46F3D3F4 FF348515
        8FD3B691 55791DF4 6747D4DB BE17C4B5 58462E26 BE5ED35F
        E680E297 1422C3B0 1B17E167 FC437F84 869D8549 537B3338


KeyData is
                                              2D4A46A1 7099BAA8
        330BC59D 4A1CF5AE 3A3075B4 C62BB26E 7FC98924 726D274C
        09646F44 08E6858C 43B42DAE D015EF26 1708D55E F24DAA7D
        3EA3D1C4 A08CFD24 DB6000A5 B8A67DE7 46F3D3F4 FF348515
        8FD3B691 55791DF4 6747D4DB BE17C4B5 58462E26 BE5ED35F
        E680E297 1422C3B0 1B17E167 FC437F84 869D8549 537B3338




-----------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
Zs is
                     0138 A672B695 8BD784E5 D7FA8373 8AC68F9B
        3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
        F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4


Ze is
                     00CD EA89621C FA46B132 F9E4CFE2 261CDE2D
        4368EB56 56634C7C C98C7A00 CDE54ED1 866A0DD3 E6126C9D
        2F845DAF F82CEB1D A08F5D87 521BB0EB ECA77911 169C20CC
```

Z is
                                00CDEA89 621CFA46 B132F9E4
        CFE2261C DE2D4368 EB565663 4C7CC98C 7A00CDE5 4ED1866A
        0DD3E612 6C9D2F84 5DAFF82C EB1DA08F 5D87521B B0EBECA7
        7911169C 20CC0138 A672B695 8BD784E5 D7FA8373 8AC68F9B
        3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
        F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
                        2D4A46A1 7099BAA8 330BC59D 4A1CF5AE
        3A3075B4 C62BB26E 7FC98924 726D274C 09646F44 08E6858C
        43B42DAE D015EF26 1708D55E F24DAA7D 3EA3D1C4 A08CFD24
        DB6000A5 B8A67DE7 46F3D3F4 FF348515 8FD3B691 55791DF4
        6747D4DB BE17C4B5 58462E26 BE5ED35F E680E297 1422C3B0
        1B17E167 FC437F84 869D8549 537B3338 50F0B78E 5CAD4ED6
        E0635DAE 1DCCA0EB 448F3BD1 3A0CDDB9 BE162CDF 3EF23175

MacData is
                        4B435F31 5F55414C 49434542 4F424259
        01EBB34D D75721AB F8ADC9DB ED17889C BB9765D9 0A7C60F2
        CEF007BB 0F2B26E1 4881FD44 42E689D6 1CB2DD04 6EE30E3F
        FD20F9A4 5BBDF641 3D583A2D BF59924F D35C00F6 B632D194
        C0388E22 D8437E55 8C552AE1 95ADFD15 3F92D749 08351B2F
        8C4EDA94 EDB0916D 1B53C020 B5EECAED 1A5FC38A 233E4830
        587BB2EE 3489B3B4 2A5A86A4 010EBFAF C6E85E08 D24BFFFC
        C1A4511D B0E634BE EB1B6DEC 8C5939AE 44766201 AF620043
        0BA97C8A C6A0E9F0 8B33CE7E 9FEEB5BA 4EE5E0D8 1510C242
        95B8A08D 023500A4 A6EC300D F9E257B0 372B5E7A BFEF0934
        36719A77 887EBB0B 18CF8099 B9F4212B 6E30A141 9C18E029
        D36863CC 9D448F4D BA4D2A0E 60711BE5 72915FBD 4FEF2695

MacKey is
                                                2D4A46A1 7099BAA8
        330BC59D 4A1CF5AE 3A3075B4 C62BB26E 7FC98924 726D274C

Mtag is
                        39AB0A29 E9A2E245 D6897BF7 CF51D6ED

```
        7AA59EBE E1E86820 F96B1804 1B158070 6D1911FA CDCCC8B6
        5B1328BD C0EB6AE0 F2C91A0C B53CDBBE 0D298A54 413D49F2


KeyData is
                                            09646F44 08E6858C
        43B42DAE D015EF26 1708D55E F24DAA7D 3EA3D1C4 A08CFD24
        DB6000A5 B8A67DE7 46F3D3F4 FF348515 8FD3B691 55791DF4
        6747D4DB BE17C4B5 58462E26 BE5ED35F E680E297 1422C3B0
        1B17E167 FC437F84 869D8549 537B3338 50F0B78E 5CAD4ED6
        E0635DAE 1DCCA0EB 448F3BD1 3A0CDDB9 BE162CDF 3EF23175




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
Zs is
                    0138 A672B695 8BD784E5 D7FA8373 8AC68F9B
        3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
        F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4


Ze is
                    00CD EA89621C FA46B132 F9E4CFE2 261CDE2D
        4368EB56 56634C7C C98C7A00 CDE54ED1 866A0DD3 E6126C9D
        2F845DAF F82CEB1D A08F5D87 521BB0EB ECA77911 169C20CC


Z is
                                00CDEA89 621CFA46 B132F9E4
        CFE2261C DE2D4368 EB565663 4C7CC98C 7A00CDE5 4ED1866A
        0DD3E612 6C9D2F84 5DAFF82C EB1DA08F 5D87521B B0EBECA7
        7911169C 20CC0138 A672B695 8BD784E5 D7FA8373 8AC68F9B
        3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
        F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                          2D4A46A1 7099BAA8 330BC59D 4A1CF5AE
        3A3075B4 C62BB26E 7FC98924 726D274C 09646F44 08E6858C
        43B42DAE D015EF26 1708D55E F24DAA7D 3EA3D1C4 A08CFD24
```

```
        DB6000A5 B8A67DE7 46F3D3F4 FF348515 8FD3B691 55791DF4
        6747D4DB BE17C4B5 58462E26 BE5ED35F E680E297 1422C3B0
        1B17E167 FC437F84 869D8549 537B3338 50F0B78E 5CAD4ED6
        E0635DAE 1DCCA0EB 448F3BD1 3A0CDDB9 BE162CDF 3EF23175


MacData is
                         4B435F31 5F56424F 42425941 4C494345
        010EBFAF C6E85E08 D24BFFFC C1A4511D B0E634BE EB1B6DEC
        8C5939AE 44766201 AF620043 0BA97C8A C6A0E9F0 8B33CE7E
        9FEEB5BA 4EE5E0D8 1510C242 95B8A08D 023500A4 A6EC300D
        F9E257B0 372B5E7A BFEF0934 36719A77 887EBB0B 18CF8099
        B9F4212B 6E30A141 9C18E029 D36863CC 9D448F4D BA4D2A0E
        60711BE5 72915FBD 4FEF2695 01EBB34D D75721AB F8ADC9DB
        ED17889C BB9765D9 0A7C60F2 CEF007BB 0F2B26E1 4881FD44
        42E689D6 1CB2DD04 6EE30E3F FD20F9A4 5BBDF641 3D583A2D
        BF59924F D35C00F6 B632D194 C0388E22 D8437E55 8C552AE1
        95ADFD15 3F92D749 08351B2F 8C4EDA94 EDB0916D 1B53C020
        B5EECAED 1A5FC38A 233E4830 587BB2EE 3489B3B4 2A5A86A4


MacKey is
                                             2D4A46A1 7099BAA8
        330BC59D 4A1CF5AE 3A3075B4 C62BB26E 7FC98924 726D274C


Mtag is
                         1F9E2BC0 F3AE6550 53D3A462 B5EB9333
        BDB8BCB3 1E193748 EAA73689 A1BD5649 F6612926 6F097365
        74ACD563 3157F95C 6B9636FB 721A9BFB 08E91A8C 74CD324D


KeyData is
                                             09646F44 08E6858C
        43B42DAE D015EF26 1708D55E F24DAA7D 3EA3D1C4 A08CFD24
        DB6000A5 B8A67DE7 46F3D3F4 FF348515 8FD3B691 55791DF4
        6747D4DB BE17C4B5 58462E26 BE5ED35F E680E297 1422C3B0
        1B17E167 FC437F84 869D8549 537B3338 50F0B78E 5CAD4ED6
        E0635DAE 1DCCA0EB 448F3BD1 3A0CDDB9 BE162CDF 3EF23175




------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
Zs is
```

```
                    0138 A672B695 8BD784E5 D7FA8373 8AC68F9B
         3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
         F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4


Ze is
                    00CD EA89621C FA46B132 F9E4CFE2 261CDE2D
         4368EB56 56634C7C C98C7A00 CDE54ED1 866A0DD3 E6126C9D
         2F845DAF F82CEB1D A08F5D87 521BB0EB ECA77911 169C20CC


Z is
                                   00CDEA89 621CFA46 B132F9E4
         CFE2261C DE2D4368 EB565663 4C7CC98C 7A00CDE5 4ED1866A
         0DD3E612 6C9D2F84 5DAFF82C EB1DA08F 5D87521B B0EBECA7
         7911169C 20CC0138 A672B695 8BD784E5 D7FA8373 8AC68F9B
         3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
         F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4


OtherInfo is
         12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                           2D4A46A1 7099BAA8 330BC59D 4A1CF5AE
         3A3075B4 C62BB26E 7FC98924 726D274C 09646F44 08E6858C
         43B42DAE D015EF26 1708D55E F24DAA7D 3EA3D1C4 A08CFD24
         DB6000A5 B8A67DE7 46F3D3F4 FF348515 8FD3B691 55791DF4
         6747D4DB BE17C4B5 58462E26 BE5ED35F E680E297 1422C3B0
         1B17E167 FC437F84 869D8549 537B3338 50F0B78E 5CAD4ED6
         E0635DAE 1DCCA0EB 448F3BD1 3A0CDDB9 BE162CDF 3EF23175


U2V
----------------
MacData is
                           4B435F32 5F55414C 49434542 4F424259
         01EBB34D D75721AB F8ADC9DB ED17889C BB9765D9 0A7C60F2
         CEF007BB 0F2B26E1 4881FD44 42E689D6 1CB2DD04 6EE30E3F
         FD20F9A4 5BBDF641 3D583A2D BF59924F D35C00F6 B632D194
         C0388E22 D8437E55 8C552AE1 95ADFD15 3F92D749 08351B2F
         8C4EDA94 EDB0916D 1B53C020 B5EECAED 1A5FC38A 233E4830
         587BB2EE 3489B3B4 2A5A86A4 010EBFAF C6E85E08 D24BFFFC
         C1A4511D B0E634BE EB1B6DEC 8C5939AE 44766201 AF620043
         0BA97C8A C6A0E9F0 8B33CE7E 9FEEB5BA 4EE5E0D8 1510C242
```

95B8A08D 023500A4 A6EC300D F9E257B0 372B5E7A BFEF0934
36719A77 887EBB0B 18CF8099 B9F4212B 6E30A141 9C18E029
D36863CC 9D448F4D BA4D2A0E 60711BE5 72915FBD 4FEF2695

MacKey is
2D4A46A1 7099BAA8
330BC59D 4A1CF5AE 3A3075B4 C62BB26E 7FC98924 726D274C

Mtag is
332623B6 15C0AF2C EF5C1D66 70670B3E
6D01479C EF6041AD 617A5DA9 53E6211F 89E98E1A F3002302
817FAE27 6E92547F 79266D58 82B7732D 6B46A203 08445842

V2U

MacData is
4B435F32 5F56424F 42425941 4C494345
010EBFAF C6E85E08 D24BFFFC C1A4511D B0E634BE EB1B6DEC
8C5939AE 44766201 AF620043 0BA97C8A C6A0E9F0 8B33CE7E
9FEEB5BA 4EE5E0D8 1510C242 95B8A08D 023500A4 A6EC300D
F9E257B0 372B5E7A BFEF0934 36719A77 887EBB0B 18CF8099
B9F4212B 6E30A141 9C18E029 D36863CC 9D448F4D BA4D2A0E
60711BE5 72915FBD 4FEF2695 01EBB34D D75721AB F8ADC9DB
ED17889C BB9765D9 0A7C60F2 CEF007BB 0F2B26E1 4881FD44
42E689D6 1CB2DD04 6EE30E3F FD20F9A4 5BBDF641 3D583A2D
BF59924F D35C00F6 B632D194 C0388E22 D8437E55 8C552AE1
95ADFD15 3F92D749 08351B2F 8C4EDA94 EDB0916D 1B53C020
B5EECAED 1A5FC38A 233E4830 587BB2EE 3489B3B4 2A5A86A4

MacKey is
2D4A46A1 7099BAA8
330BC59D 4A1CF5AE 3A3075B4 C62BB26E 7FC98924 726D274C

Mtag is
F752AFAE F5E2F786 008BA46F 9524516B
D4F80388 C35FB7A5 CEA8F38A EEDAED09 AABFC450 2EC99150
F53C2FC8 791FB613 FCE28F7E 97FC1C65 17CC8A4F 803209F9

KeyData is
09646F44 08E6858C

```
        43B42DAE D015EF26 1708D55E F24DAA7D 3EA3D1C4 A08CFD24
        DB6000A5 B8A67DE7 46F3D3F4 FF348515 8FD3B691 55791DF4
        6747D4DB BE17C4B5 58462E26 BE5ED35F E680E297 1422C3B0
        1B17E167 FC437F84 869D8549 537B3338 50F0B78E 5CAD4ED6
        E0635DAE 1DCCA0EB 448F3BD1 3A0CDDB9 BE162CDF 3EF23175



FullMQV(P-521)
------------------------------------------------------------
dsU is
                    017D 1527DCC7 C046E4D3 04600ED0 D3A625F6
        AA46C475 14D92CB6 A6416C1B 8978B3E6 E9796830 6FFC49D0
        0371CCBD 4B796AA3 6547A6ED 3E78BBDF F2CFF34C E4C57FC9


QsU_x is
                    00D0 C2D9A667 F85A3C27 0C838535 04616791
        F3052858 3CF2D5CD D35D4E77 D440FE51 01DFC0E1 953983A9
        C1D7C330 7E6213FB CEB3D113 460D7B45 BBACAE5D 54B68166


QsU_y is
                    01C8 A85F0367 B3B1F4DE 8A74021E 08E13EA5
        65EF012E 647DD317 3B21DD6B B9987155 73063EBB 3152CAA7
        91ABD47F D31FB528 799413F8 DFF76E28 64E9870A 262ECACB


dsV is
                    00A0 752E306C ECD87AB0 E4830DA1 44F8038C
        E7B8C2B3 E5422ACF 9AAA6CCF 21818316 9A4CCA2A D577A64E
        6D86DCBF F5C1727A 11FD1CB8 E3A53842 B84005FD A9AC7F36


QsV_x is
                    0128 C16B23A4 259C9FE4 257C1DA4 3C7735C4
        3337929E 0FD86CC2 A778975B 67184CC2 825F6E66 7876D404
        BBF03E04 1F8FAD2F CCC036CD 5448B64E 9BD7DF6F 537659BB


QsV_y is
                    0108 089A6431 FED52344 DD5859A0 E5432D16
        9BEE36F5 3F857AED 08A69FE3 07B1C94B 8ABDCF65 0C4D1297
        29D69FB7 7D1CC1CD 651C676B 309CE018 C9771EAB 9CA5A754
```

```
deU is
                    0113 F82DA825 735E3D97 276683B2 B74277BA
        D27335EA 71664AF2 430CC4F3 3459B966 9EE78B3F FB9B8683
        015D344D CBFEF6FB 9AF4C6C4 70BE2545 16CD3C1A 1FB47362


QeU_x is
                    01EB B34DD757 21ABF8AD C9DBED17 889CBB97
        65D90A7C 60F2CEF0 07BB0F2B 26E14881 FD4442E6 89D61CB2
        DD046EE3 0E3FFD20 F9A45BBD F6413D58 3A2DBF59 924FD35C


QeU_y is
                    00F6 B632D194 C0388E22 D8437E55 8C552AE1
        95ADFD15 3F92D749 08351B2F 8C4EDA94 EDB0916D 1B53C020
        B5EECAED 1A5FC38A 233E4830 587BB2EE 3489B3B4 2A5A86A4


deV is
                    00CE E3480D86 45A17D24 9F2776D2 8BAE6169
        52D1791F DB4B70F7 C3378732 AA1B2292 8448BCD1 DC2496D4
        35B01048 066EBE4F 72903C36 1B1A9DC1 193DC2C9 D0891B96


QeV_x is
                    010E BFAFC6E8 5E08D24B FFFCC1A4 511DB0E6
        34BEEB1B 6DEC8C59 39AE4476 6201AF62 00430BA9 7C8AC6A0
        E9F08B33 CE7E9FEE B5BA4EE5 E0D81510 C24295B8 A08D0235


QeV_y is
                    00A4 A6EC300D F9E257B0 372B5E7A BFEF0934
        36719A77 887EBB0B 18CF8099 B9F4212B 6E30A141 9C18E029
        D36863CC 9D448F4D BA4D2A0E 60711BE5 72915FBD 4FEF2695




------------------------------------------------------------
no Key Confirmation
Z is
                    01BE 3D4F8058 EF18D790 2A263CEF 57325EAE
        C9B9D6D6 411800FA 0518A173 DA7AEC8E 984B2AFA 782C2506
        639AFB54 092D56E1 2C02AE2B 943B22C3 8763DBC7 DE3BDFC1
```

```
OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                            E7946061 588EA80B
        9FE8FF31 515B007B 12EE2988 633DE0ED 71EBCD33 B605F8C2
        EAD28CBC D07BAA3D FFCC7BA3 51860A90 D8E28699 BCF1866D
        46CBC313 01CBBB2B C44125FC B6B5B974 E59B2010 90898AC1
        511261EB 392EBD23 53B7A3EA 65F1CF67 54BB5519 C190C47D
        8AE32B51 78293EBA 66C7E633 BACEF480 9A349F0C 1663EADC


KeyData is
                                            E7946061 588EA80B
        9FE8FF31 515B007B 12EE2988 633DE0ED 71EBCD33 B605F8C2
        EAD28CBC D07BAA3D FFCC7BA3 51860A90 D8E28699 BCF1866D
        46CBC313 01CBBB2B C44125FC B6B5B974 E59B2010 90898AC1
        511261EB 392EBD23 53B7A3EA 65F1CF67 54BB5519 C190C47D
        8AE32B51 78293EBA 66C7E633 BACEF480 9A349F0C 1663EADC




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
Z is
                    01BE 3D4F8058 EF18D790 2A263CEF 57325EAE
        C9B9D6D6 411800FA 0518A173 DA7AEC8E 984B2AFA 782C2506
        639AFB54 092D56E1 2C02AE2B 943B22C3 8763DBC7 DE3BDFC1


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                          E7946061 588EA80B 9FE8FF31 515B007B
        12EE2988 633DE0ED 71EBCD33 B605F8C2 EAD28CBC D07BAA3D
        FFCC7BA3 51860A90 D8E28699 BCF1866D 46CBC313 01CBBB2B
        C44125FC B6B5B974 E59B2010 90898AC1 511261EB 392EBD23
        53B7A3EA 65F1CF67 54BB5519 C190C47D 8AE32B51 78293EBA
        66C7E633 BACEF480 9A349F0C 1663EADC 73A64A8A EF283A37
        E0CA305E 0A9124D7 221F5D67 3DDB7B12 CB0A8516 9BFD17C9
```

MacData is
                        4B435F31 5F55414C 49434542 4F424259
        01EBB34D D75721AB F8ADC9DB ED17889C BB9765D9 0A7C60F2
        CEF007BB 0F2B26E1 4881FD44 42E689D6 1CB2DD04 6EE30E3F
        FD20F9A4 5BBDF641 3D583A2D BF59924F D35C00F6 B632D194
        C0388E22 D8437E55 8C552AE1 95ADFD15 3F92D749 08351B2F
        8C4EDA94 EDB0916D 1B53C020 B5EECAED 1A5FC38A 233E4830
        587BB2EE 3489B3B4 2A5A86A4 010EBFAF C6E85E08 D24BFFFC
        C1A4511D B0E634BE EB1B6DEC 8C5939AE 44766201 AF620043
        0BA97C8A C6A0E9F0 8B33CE7E 9FEEB5BA 4EE5E0D8 1510C242
        95B8A08D 023500A4 A6EC300D F9E257B0 372B5E7A BFEF0934
        36719A77 887EBB0B 18CF8099 B9F4212B 6E30A141 9C18E029
        D36863CC 9D448F4D BA4D2A0E 60711BE5 72915FBD 4FEF2695

MacKey is
                                            E7946061 588EA80B
        9FE8FF31 515B007B 12EE2988 633DE0ED 71EBCD33 B605F8C2

Mtag is
                        8AA7CAEA EC472789 1C57399C 291BC2E1
        538A85DC EC4BC42E 9C48B37C 3F42B4E5 2FB2F152 A655D1A7
        33F3D43D A91EA799 952B197F DF6E8DF8 6CD1FE47 09E1AE15

KeyData is
                                            EAD28CBC D07BAA3D
        FFCC7BA3 51860A90 D8E28699 BCF1866D 46CBC313 01CBBB2B
        C44125FC B6B5B974 E59B2010 90898AC1 511261EB 392EBD23
        53B7A3EA 65F1CF67 54BB5519 C190C47D 8AE32B51 78293EBA
        66C7E633 BACEF480 9A349F0C 1663EADC 73A64A8A EF283A37
        E0CA305E 0A9124D7 221F5D67 3DDB7B12 CB0A8516 9BFD17C9

Scheme Responder, Key Confirmation Provider: V to U
Z is
                    01BE 3D4F8058 EF18D790 2A263CEF 57325EAE
        C9B9D6D6 411800FA 0518A173 DA7AEC8E 984B2AFA 782C2506
        639AFB54 092D56E1 2C02AE2B 943B22C3 8763DBC7 DE3BDFC1

```
OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                         E7946061 588EA80B 9FE8FF31 515B007B
        12EE2988 633DE0ED 71EBCD33 B605F8C2 EAD28CBC D07BAA3D
        FFCC7BA3 51860A90 D8E28699 BCF1866D 46CBC313 01CBBB2B
        C44125FC B6B5B974 E59B2010 90898AC1 511261EB 392EBD23
        53B7A3EA 65F1CF67 54BB5519 C190C47D 8AE32B51 78293EBA
        66C7E633 BACEF480 9A349F0C 1663EADC 73A64A8A EF283A37
        E0CA305E 0A9124D7 221F5D67 3DDB7B12 CB0A8516 9BFD17C9


MacData is
                         4B435F31 5F56424F 42425941 4C494345
        010EBFAF C6E85E08 D24BFFFC C1A4511D B0E634BE EB1B6DEC
        8C5939AE 44766201 AF620043 0BA97C8A C6A0E9F0 8B33CE7E
        9FEEB5BA 4EE5E0D8 1510C242 95B8A08D 023500A4 A6EC300D
        F9E257B0 372B5E7A BFEF0934 36719A77 887EBB0B 18CF8099
        B9F4212B 6E30A141 9C18E029 D36863CC 9D448F4D BA4D2A0E
        60711BE5 72915FBD 4FEF2695 01EBB34D D75721AB F8ADC9DB
        ED17889C BB9765D9 0A7C60F2 CEF007BB 0F2B26E1 4881FD44
        42E689D6 1CB2DD04 6EE30E3F FD20F9A4 5BBDF641 3D583A2D
        BF59924F D35C00F6 B632D194 C0388E22 D8437E55 8C552AE1
        95ADFD15 3F92D749 08351B2F 8C4EDA94 EDB0916D 1B53C020
        B5EECAED 1A5FC38A 233E4830 587BB2EE 3489B3B4 2A5A86A4


MacKey is
                                                 E7946061 588EA80B
        9FE8FF31 515B007B 12EE2988 633DE0ED 71EBCD33 B605F8C2


Mtag is
                         94CDE460 990F798F 070120D1 1E84893F
        75A6E8DD 3BF7ED88 A37BA3DF AEBEBC2C 63E6A3FC BA69C41A
        F8F0B6E8 342B9578 E4475B71 DBC92F2E 47BCFD6A C397DF05


KeyData is
                                                 EAD28CBC D07BAA3D
        FFCC7BA3 51860A90 D8E28699 BCF1866D 46CBC313 01CBBB2B
        C44125FC B6B5B974 E59B2010 90898AC1 511261EB 392EBD23
        53B7A3EA 65F1CF67 54BB5519 C190C47D 8AE32B51 78293EBA
        66C7E633 BACEF480 9A349F0C 1663EADC 73A64A8A EF283A37
```

E0CA305E 0A9124D7 221F5D67 3DDB7B12 CB0A8516 9BFD17C9

Scheme Initiator, Key Confirmation Bilateral
Z is
01BE 3D4F8058 EF18D790 2A263CEF 57325EAE
C9B9D6D6 411800FA 0518A173 DA7AEC8E 984B2AFA 782C2506
639AFB54 092D56E1 2C02AE2B 943B22C3 8763DBC7 DE3BDFC1

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
E7946061 588EA80B 9FE8FF31 515B007B
12EE2988 633DE0ED 71EBCD33 B605F8C2 EAD28CBC D07BAA3D
FFCC7BA3 51860A90 D8E28699 BCF1866D 46CBC313 01CBBB2B
C44125FC B6B5B974 E59B2010 90898AC1 511261EB 392EBD23
53B7A3EA 65F1CF67 54BB5519 C190C47D 8AE32B51 78293EBA
66C7E633 BACEF480 9A349F0C 1663EADC 73A64A8A EF283A37
E0CA305E 0A9124D7 221F5D67 3DDB7B12 CB0A8516 9BFD17C9

U2V

MacData is
4B435F32 5F55414C 49434542 4F424259
01EBB34D D75721AB F8ADC9DB ED17889C BB9765D9 0A7C60F2
CEF007BB 0F2B26E1 4881FD44 42E689D6 1CB2DD04 6EE30E3F
FD20F9A4 5BBDF641 3D583A2D BF59924F D35C00F6 B632D194
C0388E22 D8437E55 8C552AE1 95ADFD15 3F92D749 08351B2F
8C4EDA94 EDB0916D 1B53C020 B5EECAED 1A5FC38A 233E4830
587BB2EE 3489B3B4 2A5A86A4 010EBFAF C6E85E08 D24BFFFC
C1A4511D B0E634BE EB1B6DEC 8C5939AE 44766201 AF620043
0BA97C8A C6A0E9F0 8B33CE7E 9FEEB5BA 4EE5E0D8 1510C242
95B8A08D 023500A4 A6EC300D F9E257B0 372B5E7A BFEF0934
36719A77 887EBB0B 18CF8099 B9F4212B 6E30A141 9C18E029
D36863CC 9D448F4D BA4D2A0E 60711BE5 72915FBD 4FEF2695

MacKey is

```
                                                E7946061 588EA80B
        9FE8FF31 515B007B 12EE2988 633DE0ED 71EBCD33 B605F8C2


Mtag is
                        929585B7 A0144071 35759347 4CA4B4DC
        9A56DD61 4F15400C EB305EFE 84C0BA0B 2D2BB87C AF153EBC
        7105AB31 59E7B7AD 1FA69669 7C137B56 2AD8C314 5E3B2730


V2U
----------------
MacData is
                        4B435F32 5F56424F 42425941 4C494345
        010EBFAF C6E85E08 D24BFFFC C1A4511D B0E634BE EB1B6DEC
        8C5939AE 44766201 AF620043 0BA97C8A C6A0E9F0 8B33CE7E
        9FEEB5BA 4EE5E0D8 1510C242 95B8A08D 023500A4 A6EC300D
        F9E257B0 372B5E7A BFEF0934 36719A77 887EBB0B 18CF8099
        B9F4212B 6E30A141 9C18E029 D36863CC 9D448F4D BA4D2A0E
        60711BE5 72915FBD 4FEF2695 01EBB34D D75721AB F8ADC9DB
        ED17889C BB9765D9 0A7C60F2 CEF007BB 0F2B26E1 4881FD44
        42E689D6 1CB2DD04 6EE30E3F FD20F9A4 5BBDF641 3D583A2D
        BF59924F D35C00F6 B632D194 C0388E22 D8437E55 8C552AE1
        95ADFD15 3F92D749 08351B2F 8C4EDA94 EDB0916D 1B53C020
        B5EECAED 1A5FC38A 233E4830 587BB2EE 3489B3B4 2A5A86A4


MacKey is
                                                E7946061 588EA80B
        9FE8FF31 515B007B 12EE2988 633DE0ED 71EBCD33 B605F8C2


Mtag is
                        CC624E00 604233DA A807A33C 0662C7D4
        91317C12 F079851F 3805F602 11EEAFB5 E986E2A2 DD422259
        B7A9E32C 68C8AC9E 1BA7F641 04E70399 BAE6FA39 4F4E5896


KeyData is
                                                EAD28CBC D07BAA3D
        FFCC7BA3 51860A90 D8E28699 BCF1866D 46CBC313 01CBBB2B
        C44125FC B6B5B974 E59B2010 90898AC1 511261EB 392EBD23
        53B7A3EA 65F1CF67 54BB5519 C190C47D 8AE32B51 78293EBA
        66C7E633 BACEF480 9A349F0C 1663EADC 73A64A8A EF283A37
        E0CA305E 0A9124D7 221F5D67 3DDB7B12 CB0A8516 9BFD17C9
```

EphemeralUnifiedCDH(P-521)
---
deU is
0113 F82DA825 735E3D97 276683B2 B74277BA
D27335EA 71664AF2 430CC4F3 3459B966 9EE78B3F FB9B8683
015D344D CBFEF6FB 9AF4C6C4 70BE2545 16CD3C1A 1FB47362

QeU_x is
01EB B34DD757 21ABF8AD C9DBED17 889CBB97
65D90A7C 60F2CEF0 07BB0F2B 26E14881 FD4442E6 89D61CB2
DD046EE3 0E3FFD20 F9A45BBD F6413D58 3A2DBF59 924FD35C

QeU_y is
00F6 B632D194 C0388E22 D8437E55 8C552AE1
95ADFD15 3F92D749 08351B2F 8C4EDA94 EDB0916D 1B53C020
B5EECAED 1A5FC38A 233E4830 587BB2EE 3489B3B4 2A5A86A4

deV is
00CE E3480D86 45A17D24 9F2776D2 8BAE6169
52D1791F DB4B70F7 C3378732 AA1B2292 8448BCD1 DC2496D4
35B01048 066EBE4F 72903C36 1B1A9DC1 193DC2C9 D0891B96

QeV_x is
010E BFAFC6E8 5E08D24B FFFCC1A4 511DB0E6
34BEEB1B 6DEC8C59 39AE4476 6201AF62 00430BA9 7C8AC6A0
E9F08B33 CE7E9FEE B5BA4EE5 E0D81510 C24295B8 A08D0235

QeV_y is
00A4 A6EC300D F9E257B0 372B5E7A BFEF0934
36719A77 887EBB0B 18CF8099 B9F4212B 6E30A141 9C18E029
D36863CC 9D448F4D BA4D2A0E 60711BE5 72915FBD 4FEF2695

---
no Key Confirmation
Z is

```
                    00CD EA89621C FA46B132 F9E4CFE2 261CDE2D
        4368EB56 56634C7C C98C7A00 CDE54ED1 866A0DD3 E6126C9D
        2F845DAF F82CEB1D A08F5D87 521BB0EB ECA77911 169C20CC


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                            C642987D 025C5B37
        80D9CC99 82B785B2 CCD78A16 20B41B83 3B78F149 FE823A23
        CE7B2712 7E8E07A1 F4CC7D1C E5D8849D FC82B411 BACBC476
        B2E0C1A8 9025A16E 45956081 87DC2F82 CCC4C5E3 FC3504D8
        5BE8497A 2B240AAD 7A5ACA6C 42691F08 9F9D072A 0A66CF43
        BBEB5F84 13D923C9 F77515E5 8E5989F3 7D09E6D2 922C2B57


KeyData is
                                            C642987D 025C5B37
        80D9CC99 82B785B2 CCD78A16 20B41B83 3B78F149 FE823A23
        CE7B2712 7E8E07A1 F4CC7D1C E5D8849D FC82B411 BACBC476
        B2E0C1A8 9025A16E 45956081 87DC2F82 CCC4C5E3 FC3504D8
        5BE8497A 2B240AAD 7A5ACA6C 42691F08 9F9D072A 0A66CF43
        BBEB5F84 13D923C9 F77515E5 8E5989F3 7D09E6D2 922C2B57




OnePassUnifiedCDH(P-521)
-----------------------------------------------------------
dsU is
                    017D 1527DCC7 C046E4D3 04600ED0 D3A625F6
        AA46C475 14D92CB6 A6416C1B 8978B3E6 E9796830 6FFC49D0
        0371CCBD 4B796AA3 6547A6ED 3E78BBDF F2CFF34C E4C57FC9


QsU_x is
                    00D0 C2D9A667 F85A3C27 0C838535 04616791
        F3052858 3CF2D5CD D35D4E77 D440FE51 01DFC0E1 953983A9
        C1D7C330 7E6213FB CEB3D113 460D7B45 BBACAE5D 54B68166


QsU_y is
                    01C8 A85F0367 B3B1F4DE 8A74021E 08E13EA5
        65EF012E 647DD317 3B21DD6B B9987155 73063EBB 3152CAA7
```

```
        91ABD47F D31FB528 799413F8 DFF76E28 64E9870A 262ECACB


dsV is
                    00A0 752E306C ECD87AB0 E4830DA1 44F8038C
        E7B8C2B3 E5422ACF 9AAA6CCF 21818316 9A4CCA2A D577A64E
        6D86DCBF F5C1727A 11FD1CB8 E3A53842 B84005FD A9AC7F36


QsV_x is
                    0128 C16B23A4 259C9FE4 257C1DA4 3C7735C4
        3337929E 0FD86CC2 A778975B 67184CC2 825F6E66 7876D404
        BBF03E04 1F8FAD2F CCC036CD 5448B64E 9BD7DF6F 537659BB


QsV_y is
                    0108 089A6431 FED52344 DD5859A0 E5432D16
        9BEE36F5 3F857AED 08A69FE3 07B1C94B 8ABDCF65 0C4D1297
        29D69FB7 7D1CC1CD 651C676B 309CE018 C9771EAB 9CA5A754


deU is
                    0113 F82DA825 735E3D97 276683B2 B74277BA
        D27335EA 71664AF2 430CC4F3 3459B966 9EE78B3F FB9B8683
        015D344D CBFEF6FB 9AF4C6C4 70BE2545 16CD3C1A 1FB47362


QeU_x is
                    01EB B34DD757 21ABF8AD C9DBED17 889CBB97
        65D90A7C 60F2CEF0 07BB0F2B 26E14881 FD4442E6 89D61CB2
        DD046EE3 0E3FFD20 F9A45BBD F6413D58 3A2DBF59 924FD35C


QeU_y is
                    00F6 B632D194 C0388E22 D8437E55 8C552AE1
        95ADFD15 3F92D749 08351B2F 8C4EDA94 EDB0916D 1B53C020
        B5EECAED 1A5FC38A 233E4830 587BB2EE 3489B3B4 2A5A86A4




------------------------------------------------------------
no Key Confirmation
Zs is
                    0138 A672B695 8BD784E5 D7FA8373 8AC68F9B
        3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
```

```
        F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4


Ze is
                    0104 F83D9416 E8BB0FEB CBAC67FE CA3F23A1
        54E9ECE9 CE152A38 1308754A E68B575A 67D0BA3E 7FAB218C
        74C58BEF DB2E494D 510158A2 5EF077C1 D1C89E58 5F1C44F7


Z is
                                  0104F83D 9416E8BB 0FEBCBAC
        67FECA3F 23A154E9 ECE9CE15 2A381308 754AE68B 575A67D0
        BA3E7FAB 218C74C5 8BEFDB2E 494D5101 58A25EF0 77C1D1C8
        9E585F1C 44F70138 A672B695 8BD784E5 D7FA8373 8AC68F9B
        3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
        F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                                                 A649B1A5 7457DCB4
        15134A13 B4D9973D 13E48BA9 3B22A7A1 ED9F09EA BB493978
        A5E301CF 7FCF1D12 37E26111 8CBED7AD E92EF2ED 856A6309
        3182B539 40BE7572 E914505F A51461C4 F4B889C0 8BFB0442
        0C994ED1 05EB68B9 8EAF6E42 41E84F8F 3A4C8BF8 A62B694F
        05FC5338 65A7B6AB EEC2D8A2 25019C14 6B17A14E AB572BD0


KeyData is
                                                 A649B1A5 7457DCB4
        15134A13 B4D9973D 13E48BA9 3B22A7A1 ED9F09EA BB493978
        A5E301CF 7FCF1D12 37E26111 8CBED7AD E92EF2ED 856A6309
        3182B539 40BE7572 E914505F A51461C4 F4B889C0 8BFB0442
        0C994ED1 05EB68B9 8EAF6E42 41E84F8F 3A4C8BF8 A62B694F
        05FC5338 65A7B6AB EEC2D8A2 25019C14 6B17A14E AB572BD0




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
                    0020 905F7F3A 0298275E 33482000 1D90F0B2
```

```
        F19737D1 F8452AC5 54BEEB7A ECB9A566 5E43DF31 3C361B1A
        9DC118D1 570D001F 3369934C 33DC782E D003C8FA 6F04553D


Zs is
                    0138 A672B695 8BD784E5 D7FA8373 8AC68F9B
        3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
        F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4


Ze is
                    0104 F83D9416 E8BB0FEB CBAC67FE CA3F23A1
        54E9ECE9 CE152A38 1308754A E68B575A 67D0BA3E 7FAB218C
        74C58BEF DB2E494D 510158A2 5EF077C1 D1C89E58 5F1C44F7


Z is
                                  0104F83D 9416E8BB 0FEBCBAC
        67FECA3F 23A154E9 ECE9CE15 2A381308 754AE68B 575A67D0
        BA3E7FAB 218C74C5 8BEFDB2E 494D5101 58A25EF0 77C1D1C8
        9E585F1C 44F70138 A672B695 8BD784E5 D7FA8373 8AC68F9B
        3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
        F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                         A649B1A5 7457DCB4 15134A13 B4D9973D
        13E48BA9 3B22A7A1 ED9F09EA BB493978 A5E301CF 7FCF1D12
        37E26111 8CBED7AD E92EF2ED 856A6309 3182B539 40BE7572
        E914505F A51461C4 F4B889C0 8BFB0442 0C994ED1 05EB68B9
        8EAF6E42 41E84F8F 3A4C8BF8 A62B694F 05FC5338 65A7B6AB
        EEC2D8A2 25019C14 6B17A14E AB572BD0 B3A85D44 9099783D
        4F192877 B712A0BD 12B53459 A8342F13 4D5C5717 AA34ECC5


MacData is
            4B43 5F315F55 414C4943 45424F42 425901EB B34DD757
        21ABF8AD C9DBED17 889CBB97 65D90A7C 60F2CEF0 07BB0F2B
        26E14881 FD4442E6 89D61CB2 DD046EE3 0E3FFD20 F9A45BBD
        F6413D58 3A2DBF59 924FD35C 00F6B632 D194C038 8E22D843
        7E558C55 2AE195AD FD153F92 D7490835 1B2F8C4E DA94EDB0
        916D1B53 C020B5EE CAED1A5F C38A233E 4830587B B2EE3489
```

B3B42A5A 86A40020 905F7F3A 0298275E 33482000 1D90F0B2
F19737D1 F8452AC5 54BEEB7A ECB9A566 5E43DF31 3C361B1A
9DC118D1 570D001F 3369934C 33DC782E D003C8FA 6F04553D

MacKey is
A649B1A5 7457DCB4
15134A13 B4D9973D 13E48BA9 3B22A7A1 ED9F09EA BB493978

Mtag is
BA11042B 74ED409A 83E73B0C A1C64A58
E07B31BA 35B86FEF 8B7AD787 F683F557 77EF0E35 04BEB56E
0FEB75BC 824428A6 775E5BB0 D29B0CC2 1BFC3B72 1D10DC55

KeyData is
A5E301CF 7FCF1D12
37E26111 8CBED7AD E92EF2ED 856A6309 3182B539 40BE7572
E914505F A51461C4 F4B889C0 8BFB0442 0C994ED1 05EB68B9
8EAF6E42 41E84F8F 3A4C8BF8 A62B694F 05FC5338 65A7B6AB
EEC2D8A2 25019C14 6B17A14E AB572BD0 B3A85D44 9099783D
4F192877 B712A0BD 12B53459 A8342F13 4D5C5717 AA34ECC5

Scheme Responder, Key Confirmation Provider: V to U
NonceU is
0020 905F7F3A 0298275E 33482000 1D90F0B2
F19737D1 F8452AC5 54BEEB7A ECB9A566 5E43DF31 3C361B1A
9DC118D1 570D001F 3369934C 33DC782E D003C8FA 6F04553D

Zs is
0138 A672B695 8BD784E5 D7FA8373 8AC68F9B
3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4

Ze is
0104 F83D9416 E8BB0FEB CBAC67FE CA3F23A1
54E9ECE9 CE152A38 1308754A E68B575A 67D0BA3E 7FAB218C
74C58BEF DB2E494D 510158A2 5EF077C1 D1C89E58 5F1C44F7

Z is
                                0104F83D 9416E8BB 0FEBCBAC
        67FECA3F 23A154E9 ECE9CE15 2A381308 754AE68B 575A67D0
        BA3E7FAB 218C74C5 8BEFDB2E 494D5101 58A25EF0 77C1D1C8
        9E585F1C 44F70138 A672B695 8BD784E5 D7FA8373 8AC68F9B
        3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
        F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
                        A649B1A5 7457DCB4 15134A13 B4D9973D
        13E48BA9 3B22A7A1 ED9F09EA BB493978 A5E301CF 7FCF1D12
        37E26111 8CBED7AD E92EF2ED 856A6309 3182B539 40BE7572
        E914505F A51461C4 F4B889C0 8BFB0442 0C994ED1 05EB68B9
        8EAF6E42 41E84F8F 3A4C8BF8 A62B694F 05FC5338 65A7B6AB
        EEC2D8A2 25019C14 6B17A14E AB572BD0 B3A85D44 9099783D
        4F192877 B712A0BD 12B53459 A8342F13 4D5C5717 AA34ECC5

MacData is
                                                    4B435F31
        5F56424F 42425941 4C494345 01EBB34D D75721AB F8ADC9DB
        ED17889C BB9765D9 0A7C60F2 CEF007BB 0F2B26E1 4881FD44
        42E689D6 1CB2DD04 6EE30E3F FD20F9A4 5BBDF641 3D583A2D
        BF59924F D35C00F6 B632D194 C0388E22 D8437E55 8C552AE1
        95ADFD15 3F92D749 08351B2F 8C4EDA94 EDB0916D 1B53C020
        B5EECAED 1A5FC38A 233E4830 587BB2EE 3489B3B4 2A5A86A4

MacKey is
                                                A649B1A5 7457DCB4
        15134A13 B4D9973D 13E48BA9 3B22A7A1 ED9F09EA BB493978

Mtag is
                        CB211DDE F1CADA90 2EC21C58 165E89AC
        D51FF0FB 8D42B87D 6BF20733 155C9F5A 1C48D948 0DDC1A81
        D53E3E1D 13EE9DFE BB2745C5 E2F42800 29309F5F 73C1DFD3

KeyData is

                                                A5E301CF 7FCF1D12
        37E26111 8CBED7AD E92EF2ED 856A6309 3182B539 40BE7572
        E914505F A51461C4 F4B889C0 8BFB0442 0C994ED1 05EB68B9
        8EAF6E42 41E84F8F 3A4C8BF8 A62B694F 05FC5338 65A7B6AB
        EEC2D8A2 25019C14 6B17A14E AB572BD0 B3A85D44 9099783D
        4F192877 B712A0BD 12B53459 A8342F13 4D5C5717 AA34ECC5

Scheme Initiator, Key Confirmation Bilateral
NonceV is
                    0020 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB7A ECB9A566 5E43DF31 3C361B1A
        9DC118D1 570D001F 3369934C 33DC782E D003C8FA 6F04553D

Zs is
                    0138 A672B695 8BD784E5 D7FA8373 8AC68F9B
        3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
        F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4

Ze is
                    0104 F83D9416 E8BB0FEB CBAC67FE CA3F23A1
        54E9ECE9 CE152A38 1308754A E68B575A 67D0BA3E 7FAB218C
        74C58BEF DB2E494D 510158A2 5EF077C1 D1C89E58 5F1C44F7

Z is
                                    0104F83D 9416E8BB 0FEBCBAC
        67FECA3F 23A154E9 ECE9CE15 2A381308 754AE68B 575A67D0
        BA3E7FAB 218C74C5 8BEFDB2E 494D5101 58A25EF0 77C1D1C8
        9E585F1C 44F70138 A672B695 8BD784E5 D7FA8373 8AC68F9B
        3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
        F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4

OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
                            A649B1A5 7457DCB4 15134A13 B4D9973D
        13E48BA9 3B22A7A1 ED9F09EA BB493978 A5E301CF 7FCF1D12

```
        37E26111 8CBED7AD E92EF2ED 856A6309 3182B539 40BE7572
        E914505F A51461C4 F4B889C0 8BFB0442 0C994ED1 05EB68B9
        8EAF6E42 41E84F8F 3A4C8BF8 A62B694F 05FC5338 65A7B6AB
        EEC2D8A2 25019C14 6B17A14E AB572BD0 B3A85D44 9099783D
        4F192877 B712A0BD 12B53459 A8342F13 4D5C5717 AA34ECC5


U2V
----------------
MacData is
            4B43 5F325F55 414C4943 45424F42 425901EB B34DD757
        21ABF8AD C9DBED17 889CBB97 65D90A7C 60F2CEF0 07BB0F2B
        26E14881 FD4442E6 89D61CB2 DD046EE3 0E3FFD20 F9A45BBD
        F6413D58 3A2DBF59 924FD35C 00F6B632 D194C038 8E22D843
        7E558C55 2AE195AD FD153F92 D7490835 1B2F8C4E DA94EDB0
        916D1B53 C020B5EE CAED1A5F C38A233E 4830587B B2EE3489
        B3B42A5A 86A40020 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB7A ECB9A566 5E43DF31 3C361B1A
        9DC118D1 570D001F 3369934C 33DC782E D003C8FA 6F04553D


MacKey is
                                               A649B1A5 7457DCB4
        15134A13 B4D9973D 13E48BA9 3B22A7A1 ED9F09EA BB493978


Mtag is
                         8D8FBD76 2F350C8D B1D5D6E9 3E259DAF
        69679568 275C55A7 E58076A7 2EF06D4C 02005E1E 4647B9E6
        716A9F4E CABC1E10 E91D1E2B 57D05DD4 132DB133 4945112C


V2U
----------------
MacData is
            4B43 5F325F56 424F4242 59414C49 43450020 905F7F3A
        0298275E 33482000 1D90F0B2 F19737D1 F8452AC5 54BEEB7A
        ECB9A566 5E43DF31 3C361B1A 9DC118D1 570D001F 3369934C
        33DC782E D003C8FA 6F04553D 01EBB34D D75721AB F8ADC9DB
        ED17889C BB9765D9 0A7C60F2 CEF007BB 0F2B26E1 4881FD44
        42E689D6 1CB2DD04 6EE30E3F FD20F9A4 5BBDF641 3D583A2D
        BF59924F D35C00F6 B632D194 C0388E22 D8437E55 8C552AE1
        95ADFD15 3F92D749 08351B2F 8C4EDA94 EDB0916D 1B53C020
        B5EECAED 1A5FC38A 233E4830 587BB2EE 3489B3B4 2A5A86A4
```

```
MacKey is
                                                A649B1A5 7457DCB4
        15134A13 B4D9973D 13E48BA9 3B22A7A1 ED9F09EA BB493978


Mtag is
                         6713A8C4 B3567D00 CD75FF1A 6E053049
        F5455FD0 B2BAA262 9135CD12 B8D79A01 B2C56CCA D66C0AC0
        75D65028 48D20C2D DC65FB53 4DFD29F7 504CC145 1A17B67F


KeyData is
                                                A5E301CF 7FCF1D12
        37E26111 8CBED7AD E92EF2ED 856A6309 3182B539 40BE7572
        E914505F A51461C4 F4B889C0 8BFB0442 0C994ED1 05EB68B9
        8EAF6E42 41E84F8F 3A4C8BF8 A62B694F 05FC5338 65A7B6AB
        EEC2D8A2 25019C14 6B17A14E AB572BD0 B3A85D44 9099783D
        4F192877 B712A0BD 12B53459 A8342F13 4D5C5717 AA34ECC5




OnePassMQV(P-521)
-------------------------------------------------------------
dsU is
                      017D 1527DCC7 C046E4D3 04600ED0 D3A625F6
        AA46C475 14D92CB6 A6416C1B 8978B3E6 E9796830 6FFC49D0
        0371CCBD 4B796AA3 6547A6ED 3E78BBDF F2CFF34C E4C57FC9


QsU_x is
                      00D0 C2D9A667 F85A3C27 0C838535 04616791
        F3052858 3CF2D5CD D35D4E77 D440FE51 01DFC0E1 953983A9
        C1D7C330 7E6213FB CEB3D113 460D7B45 BBACAE5D 54B68166


QsU_y is
                      01C8 A85F0367 B3B1F4DE 8A74021E 08E13EA5
        65EF012E 647DD317 3B21DD6B B9987155 73063EBB 3152CAA7
        91ABD47F D31FB528 799413F8 DFF76E28 64E9870A 262ECACB


dsV is
                      00A0 752E306C ECD87AB0 E4830DA1 44F8038C
        E7B8C2B3 E5422ACF 9AAA6CCF 21818316 9A4CCA2A D577A64E
        6D86DCBF F5C1727A 11FD1CB8 E3A53842 B84005FD A9AC7F36
```

QsV_x is
0128 C16B23A4 259C9FE4 257C1DA4 3C7735C4
3337929E 0FD86CC2 A778975B 67184CC2 825F6E66 7876D404
BBF03E04 1F8FAD2F CCC036CD 5448B64E 9BD7DF6F 537659BB

QsV_y is
0108 089A6431 FED52344 DD5859A0 E5432D16
9BEE36F5 3F857AED 08A69FE3 07B1C94B 8ABDCF65 0C4D1297
29D69FB7 7D1CC1CD 651C676B 309CE018 C9771EAB 9CA5A754

deU is
0113 F82DA825 735E3D97 276683B2 B74277BA
D27335EA 71664AF2 430CC4F3 3459B966 9EE78B3F FB9B8683
015D344D CBFEF6FB 9AF4C6C4 70BE2545 16CD3C1A 1FB47362

QeU_x is
01EB B34DD757 21ABF8AD C9DBED17 889CBB97
65D90A7C 60F2CEF0 07BB0F2B 26E14881 FD4442E6 89D61CB2
DD046EE3 0E3FFD20 F9A45BBD F6413D58 3A2DBF59 924FD35C

QeU_y is
00F6 B632D194 C0388E22 D8437E55 8C552AE1
95ADFD15 3F92D749 08351B2F 8C4EDA94 EDB0916D 1B53C020
B5EECAED 1A5FC38A 233E4830 587BB2EE 3489B3B4 2A5A86A4

---

no Key Confirmation
Z is
0142 29035D7F 7F1F6331 0B786136 5902C246
ED7ABF91 F13A5D38 12588D67 AECF74D5 4DA191F8 A2938F53
71772870 853C9228 85875BBC 8A5103AB ED01D10C E2B9F381

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

```
DerivedKeyMaterial is
                                                3F753BE6 F4789EF7
        118B0A21 9B14B011 484791A0 1A0D32D3 0585F595 55B61063
        68FBF512 FE36483B 8EBF4945 BBE2D2D9 278D9BBE CCF18F26
        A0CE02A6 8DBB57E7 749E0542 F225E2AC 1A1BC554 742B1810
        6A3E4508 C757F13C B86D2DD9 845357C2 AB460A67 A2652DBC
        FB409A2A C0E8F29A 41BAAB96 773216B6 A0127A56 69FA8577


KeyData is
                                                3F753BE6 F4789EF7
        118B0A21 9B14B011 484791A0 1A0D32D3 0585F595 55B61063
        68FBF512 FE36483B 8EBF4945 BBE2D2D9 278D9BBE CCF18F26
        A0CE02A6 8DBB57E7 749E0542 F225E2AC 1A1BC554 742B1810
        6A3E4508 C757F13C B86D2DD9 845357C2 AB460A67 A2652DBC
        FB409A2A C0E8F29A 41BAAB96 773216B6 A0127A56 69FA8577




------------------------------------------------------------
Scheme Initiator, Key Confirmation Provider: U to V
NonceV is
                    0020 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB7A ECB9A566 5E43DF31 3C361B1A
        9DC118D1 570D001F 3369934C 33DC782E D003C8FA 6F04553D


Z is
                    0142 29035D7F 7F1F6331 0B786136 5902C246
        ED7ABF91 F13A5D38 12588D67 AECF74D5 4DA191F8 A2938F53
        71772870 853C9228 85875BBC 8A5103AB ED01D10C E2B9F381


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                          3F753BE6 F4789EF7 118B0A21 9B14B011
        484791A0 1A0D32D3 0585F595 55B61063 68FBF512 FE36483B
        8EBF4945 BBE2D2D9 278D9BBE CCF18F26 A0CE02A6 8DBB57E7
        749E0542 F225E2AC 1A1BC554 742B1810 6A3E4508 C757F13C
        B86D2DD9 845357C2 AB460A67 A2652DBC FB409A2A C0E8F29A
        41BAAB96 773216B6 A0127A56 69FA8577 5274B1D9 603A560E
        F94E8641 43A458AD 6BDF9083 7BB2ACD6 FDF48123 2BF66CC4
```

```
MacData is
            4B43 5F315F55 414C4943 45424F42 425901EB B34DD757
         21ABF8AD C9DBED17 889CBB97 65D90A7C 60F2CEF0 07BB0F2B
         26E14881 FD4442E6 89D61CB2 DD046EE3 0E3FFD20 F9A45BBD
         F6413D58 3A2DBF59 924FD35C 00F6B632 D194C038 8E22D843
         7E558C55 2AE195AD FD153F92 D7490835 1B2F8C4E DA94EDB0
         916D1B53 C020B5EE CAED1A5F C38A233E 4830587B B2EE3489
         B3B42A5A 86A40020 905F7F3A 0298275E 33482000 1D90F0B2
         F19737D1 F8452AC5 54BEEB7A ECB9A566 5E43DF31 3C361B1A
         9DC118D1 570D001F 3369934C 33DC782E D003C8FA 6F04553D


MacKey is
                                                 3F753BE6 F4789EF7
         118B0A21 9B14B011 484791A0 1A0D32D3 0585F595 55B61063


Mtag is
                           6E07FA4C E93B7E89 24BBBD0D C61AE9E0
         B2907CCB B2DF2469 6C80BA0C 7E0229D0 F5929E85 FE1EF024
         65FA9DEF 8FA1D8CC 3AEB08B9 C9206E8D 6DE6AE99 B81C1757


KeyData is
                                                 68FBF512 FE36483B
         8EBF4945 BBE2D2D9 278D9BBE CCF18F26 A0CE02A6 8DBB57E7
         749E0542 F225E2AC 1A1BC554 742B1810 6A3E4508 C757F13C
         B86D2DD9 845357C2 AB460A67 A2652DBC FB409A2A C0E8F29A
         41BAAB96 773216B6 A0127A56 69FA8577 5274B1D9 603A560E
         F94E8641 43A458AD 6BDF9083 7BB2ACD6 FDF48123 2BF66CC4




------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
NonceU is
                      0020 905F7F3A 0298275E 33482000 1D90F0B2
         F19737D1 F8452AC5 54BEEB7A ECB9A566 5E43DF31 3C361B1A
         9DC118D1 570D001F 3369934C 33DC782E D003C8FA 6F04553D


Z is
                      0142 29035D7F 7F1F6331 0B786136 5902C246
```

```
        ED7ABF91 F13A5D38 12588D67 AECF74D5 4DA191F8 A2938F53
        71772870 853C9228 85875BBC 8A5103AB ED01D10C E2B9F381


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                         3F753BE6 F4789EF7 118B0A21 9B14B011
        484791A0 1A0D32D3 0585F595 55B61063 68FBF512 FE36483B
        8EBF4945 BBE2D2D9 278D9BBE CCF18F26 A0CE02A6 8DBB57E7
        749E0542 F225E2AC 1A1BC554 742B1810 6A3E4508 C757F13C
        B86D2DD9 845357C2 AB460A67 A2652DBC FB409A2A C0E8F29A
        41BAAB96 773216B6 A0127A56 69FA8577 5274B1D9 603A560E
        F94E8641 43A458AD 6BDF9083 7BB2ACD6 FDF48123 2BF66CC4


MacData is
                                                    4B435F31
        5F56424F 42425941 4C494345 01EBB34D D75721AB F8ADC9DB
        ED17889C BB9765D9 0A7C60F2 CEF007BB 0F2B26E1 4881FD44
        42E689D6 1CB2DD04 6EE30E3F FD20F9A4 5BBDF641 3D583A2D
        BF59924F D35C00F6 B632D194 C0388E22 D8437E55 8C552AE1
        95ADFD15 3F92D749 08351B2F 8C4EDA94 EDB0916D 1B53C020
        B5EECAED 1A5FC38A 233E4830 587BB2EE 3489B3B4 2A5A86A4


MacKey is
                                            3F753BE6 F4789EF7
        118B0A21 9B14B011 484791A0 1A0D32D3 0585F595 55B61063


Mtag is
                         0B6E0BC7 95CFEF22 0326AA13 6DEB0779
        CBA2A842 721CCD74 80B1F98F 7ADA003C 8111D8BF E0AA540C
        E4F1A392 A00F8685 4B96BD55 9C7DB7E3 E0D0D776 4F399775


KeyData is
                                            68FBF512 FE36483B
        8EBF4945 BBE2D2D9 278D9BBE CCF18F26 A0CE02A6 8DBB57E7
        749E0542 F225E2AC 1A1BC554 742B1810 6A3E4508 C757F13C
        B86D2DD9 845357C2 AB460A67 A2652DBC FB409A2A C0E8F29A
        41BAAB96 773216B6 A0127A56 69FA8577 5274B1D9 603A560E
        F94E8641 43A458AD 6BDF9083 7BB2ACD6 FDF48123 2BF66CC4
```

```
------------------------------------------------------------
Scheme Initiator, Key Confirmation Bilateral
NonceV is
                    0020 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB7A ECB9A566 5E43DF31 3C361B1A
        9DC118D1 570D001F 3369934C 33DC782E D003C8FA 6F04553D


Z is
                    0142 29035D7F 7F1F6331 0B786136 5902C246
        ED7ABF91 F13A5D38 12588D67 AECF74D5 4DA191F8 A2938F53
        71772870 853C9228 85875BBC 8A5103AB ED01D10C E2B9F381


OtherInfo is
        12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536


DerivedKeyMaterial is
                         3F753BE6 F4789EF7 118B0A21 9B14B011
        484791A0 1A0D32D3 0585F595 55B61063 68FBF512 FE36483B
        8EBF4945 BBE2D2D9 278D9BBE CCF18F26 A0CE02A6 8DBB57E7
        749E0542 F225E2AC 1A1BC554 742B1810 6A3E4508 C757F13C
        B86D2DD9 845357C2 AB460A67 A2652DBC FB409A2A C0E8F29A
        41BAAB96 773216B6 A0127A56 69FA8577 5274B1D9 603A560E
        F94E8641 43A458AD 6BDF9083 7BB2ACD6 FDF48123 2BF66CC4


U2V
----------------
MacData is
            4B43 5F325F55 414C4943 45424F42 425901EB B34DD757
        21ABF8AD C9DBED17 889CBB97 65D90A7C 60F2CEF0 07BB0F2B
        26E14881 FD4442E6 89D61CB2 DD046EE3 0E3FFD20 F9A45BBD
        F6413D58 3A2DBF59 924FD35C 00F6B632 D194C038 8E22D843
        7E558C55 2AE195AD FD153F92 D7490835 1B2F8C4E DA94EDB0
        916D1B53 C020B5EE CAED1A5F C38A233E 4830587B B2EE3489
        B3B42A5A 86A40020 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB7A ECB9A566 5E43DF31 3C361B1A
        9DC118D1 570D001F 3369934C 33DC782E D003C8FA 6F04553D
```

```
MacKey is
                                                3F753BE6 F4789EF7
        118B0A21 9B14B011 484791A0 1A0D32D3 0585F595 55B61063


Mtag is
                         7F400BD7 E1E64884 309B256E 2CA57375
        EEFB825E EB117058 0BB4FADC 2DC23484 ADEAAE61 79BC6292
        BDC84C22 8ABC28BF 99B1064D 4842C6CD D20F1244 19A03AC1


V2U
----------------
MacData is
            4B43 5F325F56 424F4242 59414C49 43450020 905F7F3A
        0298275E 33482000 1D90F0B2 F19737D1 F8452AC5 54BEEB7A
        ECB9A566 5E43DF31 3C361B1A 9DC118D1 570D001F 3369934C
        33DC782E D003C8FA 6F04553D 01EBB34D D75721AB F8ADC9DB
        ED17889C BB9765D9 0A7C60F2 CEF007BB 0F2B26E1 4881FD44
        42E689D6 1CB2DD04 6EE30E3F FD20F9A4 5BBDF641 3D583A2D
        BF59924F D35C00F6 B632D194 C0388E22 D8437E55 8C552AE1
        95ADFD15 3F92D749 08351B2F 8C4EDA94 EDB0916D 1B53C020
        B5EECAED 1A5FC38A 233E4830 587BB2EE 3489B3B4 2A5A86A4


MacKey is
                                                3F753BE6 F4789EF7
        118B0A21 9B14B011 484791A0 1A0D32D3 0585F595 55B61063


Mtag is
                         63017ABC 7778F87D 061C9247 B2E58A18
        9102C27B 100B00D3 FBD132D4 677F26B9 58A6C5E7 4C050F82
        7C5E5A72 A7F7AFF2 E9745287 EF1D8DB9 C199C9BA 180FB0D5


KeyData is
                                                68FBF512 FE36483B
        8EBF4945 BBE2D2D9 278D9BBE CCF18F26 A0CE02A6 8DBB57E7
        749E0542 F225E2AC 1A1BC554 742B1810 6A3E4508 C757F13C
        B86D2DD9 845357C2 AB460A67 A2652DBC FB409A2A C0E8F29A
        41BAAB96 773216B6 A0127A56 69FA8577 5274B1D9 603A560E
        F94E8641 43A458AD 6BDF9083 7BB2ACD6 FDF48123 2BF66CC4
```

OnePassDiffieHellmanCDH(P-521)
---
dsV is
00A0 752E306C ECD87AB0 E4830DA1 44F8038C
E7B8C2B3 E5422ACF 9AAA6CCF 21818316 9A4CCA2A D577A64E
6D86DCBF F5C1727A 11FD1CB8 E3A53842 B84005FD A9AC7F36

QsV_x is
0128 C16B23A4 259C9FE4 257C1DA4 3C7735C4
3337929E 0FD86CC2 A778975B 67184CC2 825F6E66 7876D404
BBF03E04 1F8FAD2F CCC036CD 5448B64E 9BD7DF6F 537659BB

QsV_y is
0108 089A6431 FED52344 DD5859A0 E5432D16
9BEE36F5 3F857AED 08A69FE3 07B1C94B 8ABDCF65 0C4D1297
29D69FB7 7D1CC1CD 651C676B 309CE018 C9771EAB 9CA5A754

deU is
0113 F82DA825 735E3D97 276683B2 B74277BA
D27335EA 71664AF2 430CC4F3 3459B966 9EE78B3F FB9B8683
015D344D CBFEF6FB 9AF4C6C4 70BE2545 16CD3C1A 1FB47362

QeU_x is
01EB B34DD757 21ABF8AD C9DBED17 889CBB97
65D90A7C 60F2CEF0 07BB0F2B 26E14881 FD4442E6 89D61CB2
DD046EE3 0E3FFD20 F9A45BBD F6413D58 3A2DBF59 924FD35C

QeU_y is
00F6 B632D194 C0388E22 D8437E55 8C552AE1
95ADFD15 3F92D749 08351B2F 8C4EDA94 EDB0916D 1B53C020
B5EECAED 1A5FC38A 233E4830 587BB2EE 3489B3B4 2A5A86A4

---
no Key Confirmation
Z is
0104 F83D9416 E8BB0FEB CBAC67FE CA3F23A1
54E9ECE9 CE152A38 1308754A E68B575A 67D0BA3E 7FAB218C

74C58BEF DB2E494D 510158A2 5EF077C1 D1C89E58 5F1C44F7

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
C0F84A40 108F717A
B9B7270C B8483BFA 4B2769E3 420C7259 C5E9FF93 F806C623
878B2215 E5784481 5B7AA0B6 BF36B690 BDCAE103 F1A24DB3
C6C3B58F 10B3A545 CD718E8B 358E1EE2 F9707D5F 54C8693A
E313F1C2 0737706B DDC7813C F0AB701F 27DC1382 8DB5FAC8
28455FF9 4AD3E1ED BA60FA73 5112F751 755ACF29 2AAF0D52

KeyData is
C0F84A40 108F717A
B9B7270C B8483BFA 4B2769E3 420C7259 C5E9FF93 F806C623
878B2215 E5784481 5B7AA0B6 BF36B690 BDCAE103 F1A24DB3
C6C3B58F 10B3A545 CD718E8B 358E1EE2 F9707D5F 54C8693A
E313F1C2 0737706B DDC7813C F0AB701F 27DC1382 8DB5FAC8
28455FF9 4AD3E1ED BA60FA73 5112F751 755ACF29 2AAF0D52

Scheme Responder, Key Confirmation Provider: V to U
Z is
0104 F83D9416 E8BB0FEB CBAC67FE CA3F23A1
54E9ECE9 CE152A38 1308754A E68B575A 67D0BA3E 7FAB218C
74C58BEF DB2E494D 510158A2 5EF077C1 D1C89E58 5F1C44F7

OtherInfo is
12345678 9ABCDEF0 414C4943 45313233 424F4242 59343536

DerivedKeyMaterial is
C0F84A40 108F717A B9B7270C B8483BFA
4B2769E3 420C7259 C5E9FF93 F806C623 878B2215 E5784481
5B7AA0B6 BF36B690 BDCAE103 F1A24DB3 C6C3B58F 10B3A545
CD718E8B 358E1EE2 F9707D5F 54C8693A E313F1C2 0737706B
DDC7813C F0AB701F 27DC1382 8DB5FAC8 28455FF9 4AD3E1ED
BA60FA73 5112F751 755ACF29 2AAF0D52 2CD329F4 B4266D87

```
        217A098B B81B8A26 9DD3A410 78668E31 74C0E4B9 D0A1F216


MacData is
                                                          4B435F31
        5F56424F 42425941 4C494345 01EBB34D D75721AB F8ADC9DB
        ED17889C BB9765D9 0A7C60F2 CEF007BB 0F2B26E1 4881FD44
        42E689D6 1CB2DD04 6EE30E3F FD20F9A4 5BBDF641 3D583A2D
        BF59924F D35C00F6 B632D194 C0388E22 D8437E55 8C552AE1
        95ADFD15 3F92D749 08351B2F 8C4EDA94 EDB0916D 1B53C020
        B5EECAED 1A5FC38A 233E4830 587BB2EE 3489B3B4 2A5A86A4


MacKey is
                                               C0F84A40 108F717A
        B9B7270C B8483BFA 4B2769E3 420C7259 C5E9FF93 F806C623


Mtag is
                          9A8B208D 0DBB8215 E8E3F003 3F626C5C
        28B9953D 20E6B824 1DBB13EB 31557C04 9ABFCC60 D9990DEB
        ABF29DBF D3780D8A D3786313 CA4609CE 4A37F833 086A3CF8


KeyData is
                                               878B2215 E5784481
        5B7AA0B6 BF36B690 BDCAE103 F1A24DB3 C6C3B58F 10B3A545
        CD718E8B 358E1EE2 F9707D5F 54C8693A E313F1C2 0737706B
        DDC7813C F0AB701F 27DC1382 8DB5FAC8 28455FF9 4AD3E1ED
        BA60FA73 5112F751 755ACF29 2AAF0D52 2CD329F4 B4266D87
        217A098B B81B8A26 9DD3A410 78668E31 74C0E4B9 D0A1F216




StaticUnifiedCDH(P-521)
-----------------------------------------------------------
dsU is
                     017D 1527DCC7 C046E4D3 04600ED0 D3A625F6
        AA46C475 14D92CB6 A6416C1B 8978B3E6 E9796830 6FFC49D0
        0371CCBD 4B796AA3 6547A6ED 3E78BBDF F2CFF34C E4C57FC9


QsU_x is
                     00D0 C2D9A667 F85A3C27 0C838535 04616791
        F3052858 3CF2D5CD D35D4E77 D440FE51 01DFC0E1 953983A9
```

```
        C1D7C330 7E6213FB CEB3D113 460D7B45 BBACAE5D 54B68166


QsU_y is
                    01C8 A85F0367 B3B1F4DE 8A74021E 08E13EA5
        65EF012E 647DD317 3B21DD6B B9987155 73063EBB 3152CAA7
        91ABD47F D31FB528 799413F8 DFF76E28 64E9870A 262ECACB


dsV is
                    00A0 752E306C ECD87AB0 E4830DA1 44F8038C
        E7B8C2B3 E5422ACF 9AAA6CCF 21818316 9A4CCA2A D577A64E
        6D86DCBF F5C1727A 11FD1CB8 E3A53842 B84005FD A9AC7F36


QsV_x is
                    0128 C16B23A4 259C9FE4 257C1DA4 3C7735C4
        3337929E 0FD86CC2 A778975B 67184CC2 825F6E66 7876D404
        BBF03E04 1F8FAD2F CCC036CD 5448B64E 9BD7DF6F 537659BB


QsV_y is
                    0108 089A6431 FED52344 DD5859A0 E5432D16
        9BEE36F5 3F857AED 08A69FE3 07B1C94B 8ABDCF65 0C4D1297
        29D69FB7 7D1CC1CD 651C676B 309CE018 C9771EAB 9CA5A754




------------------------------------------------------------
no Key Confirmation
NonceU is
                    0020 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB7A ECB9A566 5E43DF31 3C361B1A
        9DC118D1 570D001F 3369934C 33DC782E D003C8FA 6F04553D


Z is
                    0138 A672B695 8BD784E5 D7FA8373 8AC68F9B
        3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
        F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4


OtherInfo is
                12345678 9ABCDEF0 414C4943 45313233 09020020
        905F7F3A 0298275E 33482000 1D90F0B2 F19737D1 F8452AC5
```

54BEEB7A ECB9A566 5E43DF31 3C361B1A 9DC118D1 570D001F
3369934C 33DC782E D003C8FA 6F04553D 424F4242 59343536

DerivedKeyMaterial is

502F5BC5 F0934777
2ECCB85C D867B79D 223D080A AD76E94B F9A6405D 5E9EBE81
5AC18328 52CC526F 21E850C7 113402B5 B1B8CF67 78CE4F43
AE3741BC 55B709D6 0B7DDE38 D0AC5501 2024E212 C714FB0C
39C122DA F6136D8E A2CC4359 F597A606 E99566A4 3E515AD7
23008707 1409F0FD 6A7D0F2E 230791B9 90F6A12C 5DD5E9F3

KeyData is

502F5BC5 F0934777
2ECCB85C D867B79D 223D080A AD76E94B F9A6405D 5E9EBE81
5AC18328 52CC526F 21E850C7 113402B5 B1B8CF67 78CE4F43
AE3741BC 55B709D6 0B7DDE38 D0AC5501 2024E212 C714FB0C
39C122DA F6136D8E A2CC4359 F597A606 E99566A4 3E515AD7
23008707 1409F0FD 6A7D0F2E 230791B9 90F6A12C 5DD5E9F3

Scheme Initiator, Key Confirmation Provider: U to V
NonceU is

0020 905F7F3A 0298275E 33482000 1D90F0B2
F19737D1 F8452AC5 54BEEB7A ECB9A566 5E43DF31 3C361B1A
9DC118D1 570D001F 3369934C 33DC782E D003C8FA 6F04553D

NonceV is

002A 26EAF7F8 44D4C41E 622F4AA9 17AB5F06
5A452352 1700C41A 5234B396 83680BCE F996099C 67FE5B46
6C1BAD07 A6C7F0F1 BBBFA3E2 A538CEA8 5A3C5936 3BEC365D

Z is

0138 A672B695 8BD784E5 D7FA8373 8AC68F9B
3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4

OtherInfo is

12345678 9ABCDEF0 414C4943 45313233 09020020

```
        905F7F3A 0298275E 33482000 1D90F0B2 F19737D1 F8452AC5
        54BEEB7A ECB9A566 5E43DF31 3C361B1A 9DC118D1 570D001F
        3369934C 33DC782E D003C8FA 6F04553D 424F4242 59343536


DerivedKeyMaterial is
                         502F5BC5 F0934777 2ECCB85C D867B79D
        223D080A AD76E94B F9A6405D 5E9EBE81 5AC18328 52CC526F
        21E850C7 113402B5 B1B8CF67 78CE4F43 AE3741BC 55B709D6
        0B7DDE38 D0AC5501 2024E212 C714FB0C 39C122DA F6136D8E
        A2CC4359 F597A606 E99566A4 3E515AD7 23008707 1409F0FD
        6A7D0F2E 230791B9 90F6A12C 5DD5E9F3 4E9CE662 1224DBED
        54E0005C 2AC6F95A 30808D45 EE4C8AB6 FFC5FBAC BE07CDEB


MacData is
                                                    4B435F31
        5F55414C 49434542 4F424259 0020905F 7F3A0298 275E3348
        20001D90 F0B2F197 37D1F845 2AC554BE EB7AECB9 A5665E43
        DF313C36 1B1A9DC1 18D1570D 001F3369 934C33DC 782ED003
        C8FA6F04 553D002A 26EAF7F8 44D4C41E 622F4AA9 17AB5F06
        5A452352 1700C41A 5234B396 83680BCE F996099C 67FE5B46
        6C1BAD07 A6C7F0F1 BBBFA3E2 A538CEA8 5A3C5936 3BEC365D


MacKey is
                                           502F5BC5 F0934777
        2ECCB85C D867B79D 223D080A AD76E94B F9A6405D 5E9EBE81


Mtag is
                         A12E81CA 6179767B 1F9849C2 F0200354
        6C404E9E B7FCB6AD 2A567DB7 B19BBCF5 A4838DDD C791CD8B
        28D70C36 FBADD63E B1D35A75 E31194FD 6BE45449 D1452D49


KeyData is
                                           5AC18328 52CC526F
        21E850C7 113402B5 B1B8CF67 78CE4F43 AE3741BC 55B709D6
        0B7DDE38 D0AC5501 2024E212 C714FB0C 39C122DA F6136D8E
        A2CC4359 F597A606 E99566A4 3E515AD7 23008707 1409F0FD
        6A7D0F2E 230791B9 90F6A12C 5DD5E9F3 4E9CE662 1224DBED
        54E0005C 2AC6F95A 30808D45 EE4C8AB6 FFC5FBAC BE07CDEB
```

```
------------------------------------------------------------
Scheme Responder, Key Confirmation Provider: V to U
NonceV is
                    002A 26EAF7F8 44D4C41E 622F4AA9 17AB5F06
        5A452352 1700C41A 5234B396 83680BCE F996099C 67FE5B46
        6C1BAD07 A6C7F0F1 BBBFA3E2 A538CEA8 5A3C5936 3BEC365D


NonceU is
                    0020 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB7A ECB9A566 5E43DF31 3C361B1A
        9DC118D1 570D001F 3369934C 33DC782E D003C8FA 6F04553D


Z is
                    0138 A672B695 8BD784E5 D7FA8373 8AC68F9B
        3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
        F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4


OtherInfo is
                12345678 9ABCDEF0 414C4943 45313233 09020020
        905F7F3A 0298275E 33482000 1D90F0B2 F19737D1 F8452AC5
        54BEEB7A ECB9A566 5E43DF31 3C361B1A 9DC118D1 570D001F
        3369934C 33DC782E D003C8FA 6F04553D 424F4242 59343536


DerivedKeyMaterial is
                        502F5BC5 F0934777 2ECCB85C D867B79D
        223D080A AD76E94B F9A6405D 5E9EBE81 5AC18328 52CC526F
        21E850C7 113402B5 B1B8CF67 78CE4F43 AE3741BC 55B709D6
        0B7DDE38 D0AC5501 2024E212 C714FB0C 39C122DA F6136D8E
        A2CC4359 F597A606 E99566A4 3E515AD7 23008707 1409F0FD
        6A7D0F2E 230791B9 90F6A12C 5DD5E9F3 4E9CE662 1224DBED
        54E0005C 2AC6F95A 30808D45 EE4C8AB6 FFC5FBAC BE07CDEB


MacData is
                                    4B43 5F315F56 424F4242
        59414C49 43450020 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB7A ECB9A566 5E43DF31 3C361B1A
        9DC118D1 570D001F 3369934C 33DC782E D003C8FA 6F04553D


MacKey is
```

```
                                                502F5BC5 F0934777
        2ECCB85C D867B79D 223D080A AD76E94B F9A6405D 5E9EBE81


Mtag is
                            332E2BED 457524D1 B542DF81 38F54D95
        AEC9D484 C579996F 871BAEFC B503972F ED5A34B9 99D4FD28
        63A018CA CC05BB83 3F1E0521 43904468 80AA12E5 59C3E57A


KeyData is
                                                5AC18328 52CC526F
        21E850C7 113402B5 B1B8CF67 78CE4F43 AE3741BC 55B709D6
        0B7DDE38 D0AC5501 2024E212 C714FB0C 39C122DA F6136D8E
        A2CC4359 F597A606 E99566A4 3E515AD7 23008707 1409F0FD
        6A7D0F2E 230791B9 90F6A12C 5DD5E9F3 4E9CE662 1224DBED
        54E0005C 2AC6F95A 30808D45 EE4C8AB6 FFC5FBAC BE07CDEB




------------------------------------------------------------

Scheme Initiator, Key Confirmation Bilateral
NonceU is
                        0020 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB7A ECB9A566 5E43DF31 3C361B1A
        9DC118D1 570D001F 3369934C 33DC782E D003C8FA 6F04553D


NonceV is
                        002A 26EAF7F8 44D4C41E 622F4AA9 17AB5F06
        5A452352 1700C41A 5234B396 83680BCE F996099C 67FE5B46
        6C1BAD07 A6C7F0F1 BBBFA3E2 A538CEA8 5A3C5936 3BEC365D


Z is
                        0138 A672B695 8BD784E5 D7FA8373 8AC68F9B
        3423B483 F9BF539E 71141E45 DBFB7AFE D18B11C0 028B13F1
        F860EF43 C480F4DA CDA20810 59D3978C 999D5D1A DE3454E4


OtherInfo is
                    12345678 9ABCDEF0 414C4943 45313233 09020020
        905F7F3A 0298275E 33482000 1D90F0B2 F19737D1 F8452AC5
        54BEEB7A ECB9A566 5E43DF31 3C361B1A 9DC118D1 570D001F
```

```
        3369934C 33DC782E D003C8FA 6F04553D 424F4242 59343536


DerivedKeyMaterial is
                         502F5BC5 F0934777 2ECCB85C D867B79D
        223D080A AD76E94B F9A6405D 5E9EBE81 5AC18328 52CC526F
        21E850C7 113402B5 B1B8CF67 78CE4F43 AE3741BC 55B709D6
        0B7DDE38 D0AC5501 2024E212 C714FB0C 39C122DA F6136D8E
        A2CC4359 F597A606 E99566A4 3E515AD7 23008707 1409F0FD
        6A7D0F2E 230791B9 90F6A12C 5DD5E9F3 4E9CE662 1224DBED
        54E0005C 2AC6F95A 30808D45 EE4C8AB6 FFC5FBAC BE07CDEB


U2V
----------------
MacData is
                                                    4B435F32
        5F55414C 49434542 4F424259 0020905F 7F3A0298 275E3348
        20001D90 F0B2F197 37D1F845 2AC554BE EB7AECB9 A5665E43
        DF313C36 1B1A9DC1 18D1570D 001F3369 934C33DC 782ED003
        C8FA6F04 553D002A 26EAF7F8 44D4C41E 622F4AA9 17AB5F06
        5A452352 1700C41A 5234B396 83680BCE F996099C 67FE5B46
        6C1BAD07 A6C7F0F1 BBBFA3E2 A538CEA8 5A3C5936 3BEC365D


MacKey is
                                            502F5BC5 F0934777
        2ECCB85C D867B79D 223D080A AD76E94B F9A6405D 5E9EBE81


Mtag is
                         858013F9 A125A145 CDE0839A 16109570
        01E5CE24 137679E1 73DBAF5C 2853C810 81C746BD AEF5AC60
        F7CE18F0 D532AE82 9BAD7FCB B64D92DE 40C13B3B B8F21769


V2U
----------------
MacData is
                                                    4B435F32
        5F56424F 42425941 4C494345 002A26EA F7F844D4 C41E622F
        4AA917AB 5F065A45 23521700 C41A5234 B3968368 0BCEF996
        099C67FE 5B466C1B AD07A6C7 F0F1BBBF A3E2A538 CEA85A3C
        59363BEC 365D0020 905F7F3A 0298275E 33482000 1D90F0B2
        F19737D1 F8452AC5 54BEEB7A ECB9A566 5E43DF31 3C361B1A
        9DC118D1 570D001F 3369934C 33DC782E D003C8FA 6F04553D
```

MacKey is

```
                                            502F5BC5 F0934777
        2ECCB85C D867B79D 223D080A AD76E94B F9A6405D 5E9EBE81
```

Mtag is

```
                         0FBB421D 3538D824 DBA92CFB EE51D96D
        9420F397 5AA02313 BE8F5D6F 72696C09 486A377A FF68F8E8
        1609DCEC A874B2C2 07547A42 58956874 6B1F8E1E E70EC90C
```

KeyData is

```
                                            5AC18328 52CC526F
        21E850C7 113402B5 B1B8CF67 78CE4F43 AE3741BC 55B709D6
        0B7DDE38 D0AC5501 2024E212 C714FB0C 39C122DA F6136D8E
        A2CC4359 F597A606 E99566A4 3E515AD7 23008707 1409F0FD
        6A7D0F2E 230791B9 90F6A12C 5DD5E9F3 4E9CE662 1224DBED
        54E0005C 2AC6F95A 30808D45 EE4C8AB6 FFC5FBAC BE07CDEB
```