DIAGRAMA NOISE IK (HANDSHAKE)

ALICE

Claves Efímeras: e_priv_A, e_pub_A

Claves Estáticas: s_priv_A, $\underbrace{s\_pub\_A}_{\text{mDNS}}$

BOB

Claves Efímeras: e_priv_B, e_pub_B

Claves Estáticas: s_priv_B, $\underbrace{s\_pub\_B}_{\text{mDNS}}$

$$CK_0 = \textbf{Hash}(\text{“\textbf{DNIe-IM-V2-Signed}”})$$

$$1^\circ \begin{cases} CK_1, K_S = \textbf{KDF}(CK_0, \textbf{DH}(e\_priv\_A, s\_pub\_B)) \\ CK_2, K_{PA} = \textbf{KDF}(CK_1, \textbf{DH}(s\_priv\_A, s\_pub\_B)) \end{cases} \qquad \left. \begin{array}{r} CK_1, K_S = \textbf{KDF}(CK_0, \textbf{DH}(s\_priv\_B, e\_pub\_A)) \\ CK_2, K_{PA} = \textbf{KDF}(CK_1, \textbf{DH}(s\_priv\_B, s\_pub\_A)) \end{array} \right\} 2^\circ$$

$$4^\circ \begin{cases} CK_3, \sim = \textbf{KDF}(CK_2, \textbf{DH}(e\_priv\_A, e\_pub\_B)) \\ CK_4, K_{PB} = \textbf{KDF}(CK_3, \textbf{DH}(s\_priv\_A, e\_pub\_B)) \end{cases} \qquad \left. \begin{array}{r} CK_3, \sim = \textbf{KDF}(CK_2, \textbf{DH}(e\_priv\_B, e\_pub\_A)) \\ CK_4, K_{PB} = \textbf{KDF}(CK_3, \textbf{DH}(e\_priv\_B, s\_pub\_A)) \end{array} \right\} 3^\circ$$

$$K_{B \to A}, K_{A \to B} = \textbf{KDF}(CK_4)$$

ALICE INICIA HANDSHAKE

0x01 **1B**	**Size** **4B**	**IdxA** **4B**	e_pub_A **32B**	s_pub_A **32B**	**Tag** **16B**	**JSON: Cert X.509** **+ Firma de e-pub-A**	**Tag** **16B**

ChaCha20Poly1305(K_S) **ChaCha20Poly1305**(K_{PA})

BOB RESPONDE HANDSHAKE

0x02 **1B**	**Size** **4B**	**IdxB** **4B**	**IdxA** **4B**	e_pub_B **32B**	**JSON: Cert X.509** **+ Firma de e-pub-B**	**Tag** **16B**

ChaCha20Poly1305(K_{PB})