



**Data Input**



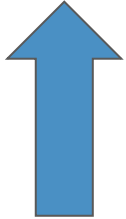
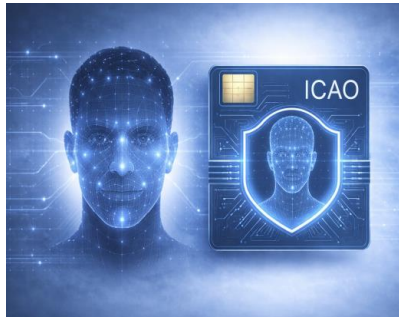
**Biometric Verification**



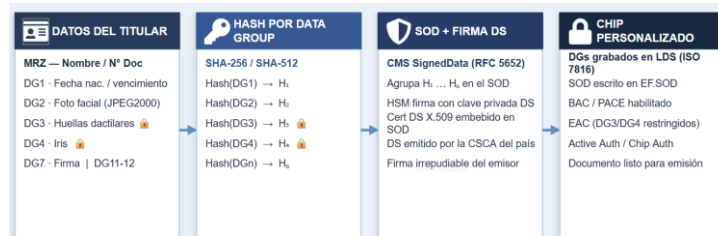
**Secure Output**



# Verificación de identidad (1 a 1 ) Identificación (1 a N)



# Proceso de Personalización , ocurre solo una vez en la emision del documento



**DATOS DEL TITULAR**  
(MRZ, foto, biometría) ↓

## SISTEMA DE PERSONALIZACIÓN

1. Genera DG1 a DGn con los datos del titular
2. Calcula hash SHA de cada DG
3. Construye el SOD con todos los hashes
4. Solicita firma al HSM (clave privada DS)
5. HSM retorna SOD firmado
6. Graba todos los DGs + SOD en el chip
7. Aplica controles de acceso (BAC/PACE, EAC)

## CHIP PERSONALIZADO

Datos del titular en DGs - SOD firmado por DS - Cert DS embebido

## PUBLICACIÓN -

Cert DS → PKD ICAO  
CSCA PKD ICAO



## CSCA — Country Signing CA

- Autoridad raíz PKI del país emisor
- Firma y emite los certificados DS



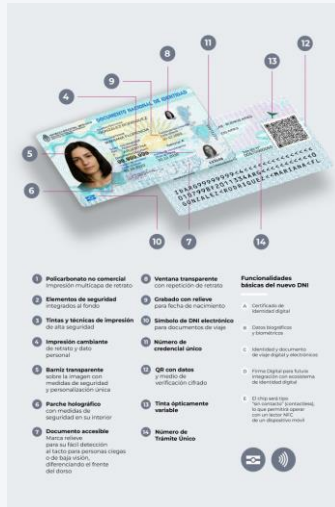
## DS — Document Signer

- Cert X.509 emitido y firmado por la CSCA
- Clave privada residente en HSM — nunca sale en claro
- Vigencia corta: 3 a 12 meses por diseño de seguridad
- Cert DS embebido dentro del SOD en el chip



## PKD ICAO — Public Key Directory

- Repositorio central administrado por ICAO (Montreal)
- Países emisores publican: CSCA cert + DS certs
- Países verificadores sincronizan vía LDAP
- Protocolo PKD LDAP + CRL (revocación de certificados)
- +70 países participantes — base de confianza global



## Verificación de autenticidad y vigencia de eDNI (Presencial y Remota)

