

XXIII ENCUENTRO CLARCIEV HONDURAS 2026

**Credenciales verificables,
billetteras digitales y el papel de la
identificación digital**



Marta García Gomar

Chief Technology Officer, IDENTITY

Los servicios son digitales. La identidad no

Mandar una fotografía del documento no es digitalizarlo

Cada foto de tu cédula es una copia de tu identidad fuera de tu control



Expones todos tus datos para verificar uno



Quedan copias en servidores de terceros, sin revocación



Y una foto se falsifica con facilidad

+311%

documentos sintéticos con IA en un año

Sumsub · Q1 2025

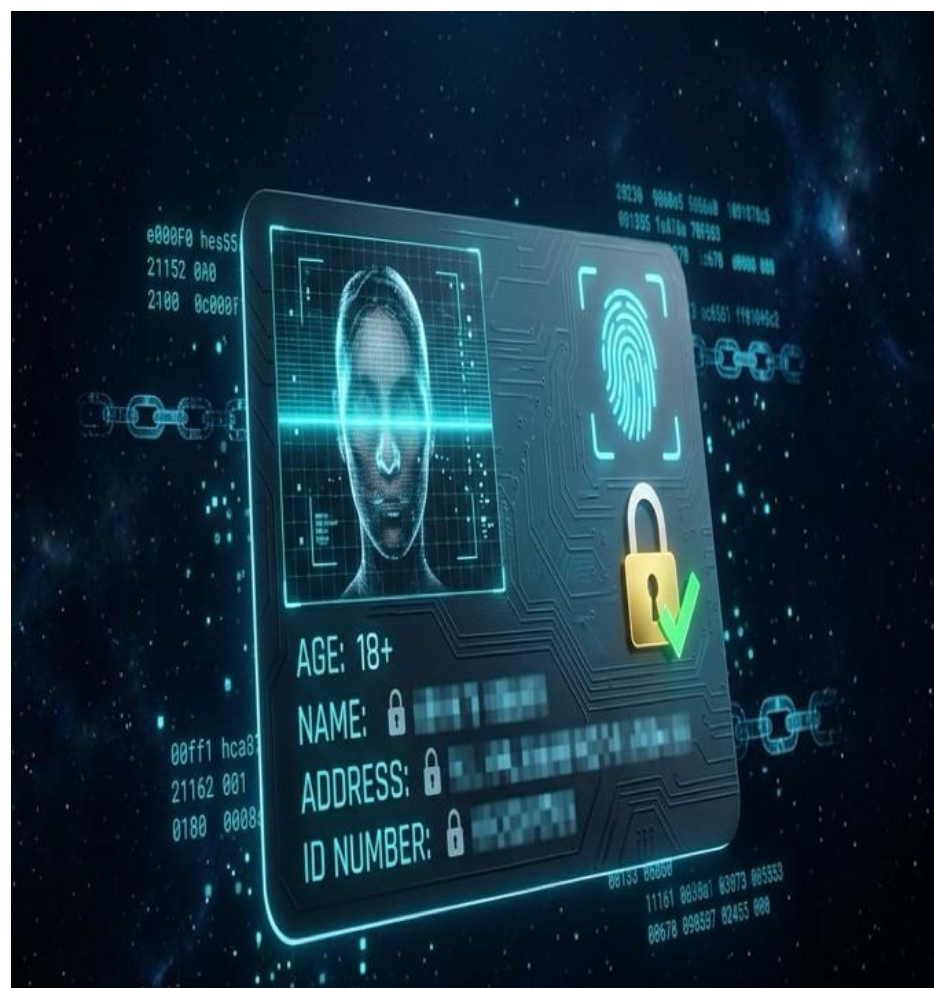
¿Qué necesita una identidad digital confiable?

01 ÍNTEGRA

Biometría vinculada
criptográficamente a la identidad

03 VERIFICABLE

Cualquiera puede verificar que la
emisión es del gobierno



02 AUTÉNTICA

Emitida y firmada por la entidad
de gobierno

04 PRESENTABLE

Se presenta en cualquier servicio
que se adhiera al estándar,
también desde el móvil

 CREDENCIAL FÍSICA CON CHIP

Se lee por NFC, pero no resuelve el problema

NO ES UNIVERSAL

-  Cara de fabricar y distribuir
-  Solo se entrega en oficinas del gobierno
-  El NFC no está disponible en todos los sitios

NO ES 100% SEGURA

-  Expone dirección y otros datos a la vista
-  Si se pierde, no se revoca fácilmente



LA SOLUCIÓN: CREDENCIALES VERIFICABLES EN EL MÓVIL

El gobierno emite una vez; los verificadores comprueban la firma sin consultarle



EL RETO: AUTENTICACIÓN UNIVERSAL Y CONFIABLE

En la emisión y en cada presentación posterior



El facial por sí solo ya no basta

- Vulnerable a deepfake: kits de IA disponibles por 12 \$ que suplantán un rostro en tiempo real, replicando los movimientos
- No es universal ni inclusiva: deja fuera a parte de la población



Multimodal: rostro + huella touchless

- Sin hardware adicional: basta la cámara del móvil
- Huella touchless blindada frente a la IA: no existen fotos de huellas en alta resolución en redes ni bases públicas
- Cubre a quien el facial deja fuera: universal de verdad



Depender de servidores y conexión

- Coste alto de desplegar, mantener y escalar la infraestructura
- Inviabile donde la conexión es mala o no llega
- Punto único de ataque: una base centralizada compromete a millones de golpe



Cotejo en el propio dispositivo

- Costo marginal cero: sin servidores biométricos que mantener ni escalar
- Funciona con conexión deficiente
- Los ataques no escalan: el template vive solo en el teléfono

[¡Gracias!

Marta García Gomar · CTO, IDENTITY · marta@identity.io