



CREDENCIALES VERIFICABLES, BILLETERAS DIGITALES Y EL ROL DE LA IDENTIFICACIÓN DIGITAL

Julio Custodio de Melo | Infineon Technologies



La confianza digital se está convirtiendo en
infraestructura.

CONFIAR

PORTÁTIL · VERIFICABLE · BAJO CONTROL

La pregunta ya no es solo «¿quién es usted?», sino «¿qué puede demostrar?». Las credenciales contienen afirmaciones firmadas; las billeteras median su uso; la identificación digital las vincula con una persona y una fuente oficial.

TRES PIEZAS

Cada una resuelve un problema distinto.

Juntas, permiten reutilizar la confianza entre servicios.

1

IDENTIFICACIÓN DIGITAL
Establece quién es la persona y con qué nivel de garantía.

2

CREDENCIAL VERIFICABLE
Transporta atributos firmados por un emisor reconocido.

3

BILLETERA DIGITAL
Protege claves y media el consentimiento y la presentación.

NO ES UN PDF

La apariencia no demuestra el origen; verificar exige criptografía, autoridad y estado.

1

AFIRMACIONES FIRMADAS

La integridad y la procedencia pueden comprobarse automáticamente.

2

EMISOR AUTORIZADO

El verificador evalúa si el emisor puede realizar la afirmación.

3

ESTADO + PRIVACIDAD

La validez sigue siendo verificable; se pueden revelar menos datos.



MODELO DE CONFIANZA

Tres actores comparten un marco de confianza.

La gobernanza indica cuándo confiar.

1

EMISOR

Firma solo las afirmaciones que está autorizado a realizar.

2

TITULAR

Controla credenciales, claves y la decisión de presentarlas.

3

VERIFICADOR

Comprueba procedencia, integridad, vínculo, validez y estado.



RECIBIR
emisores
confiables



PROTEGER
claves +
credenciales



CONSENTIR
quién solicita
qué



PRESENTAR
solo lo
necesario

BILLETERA

La billetera es el agente de confianza de la persona.

No debe sustituir los registros oficiales ni crear un historial central de cada interacción ciudadana.

IDENTIDAD

La billetera solo es confiable cuando la prueba de identidad, la autenticación y la recuperación también lo son.

1

REGISTRO

Vincular a la persona y sus atributos con evidencias y registros confiables.

2

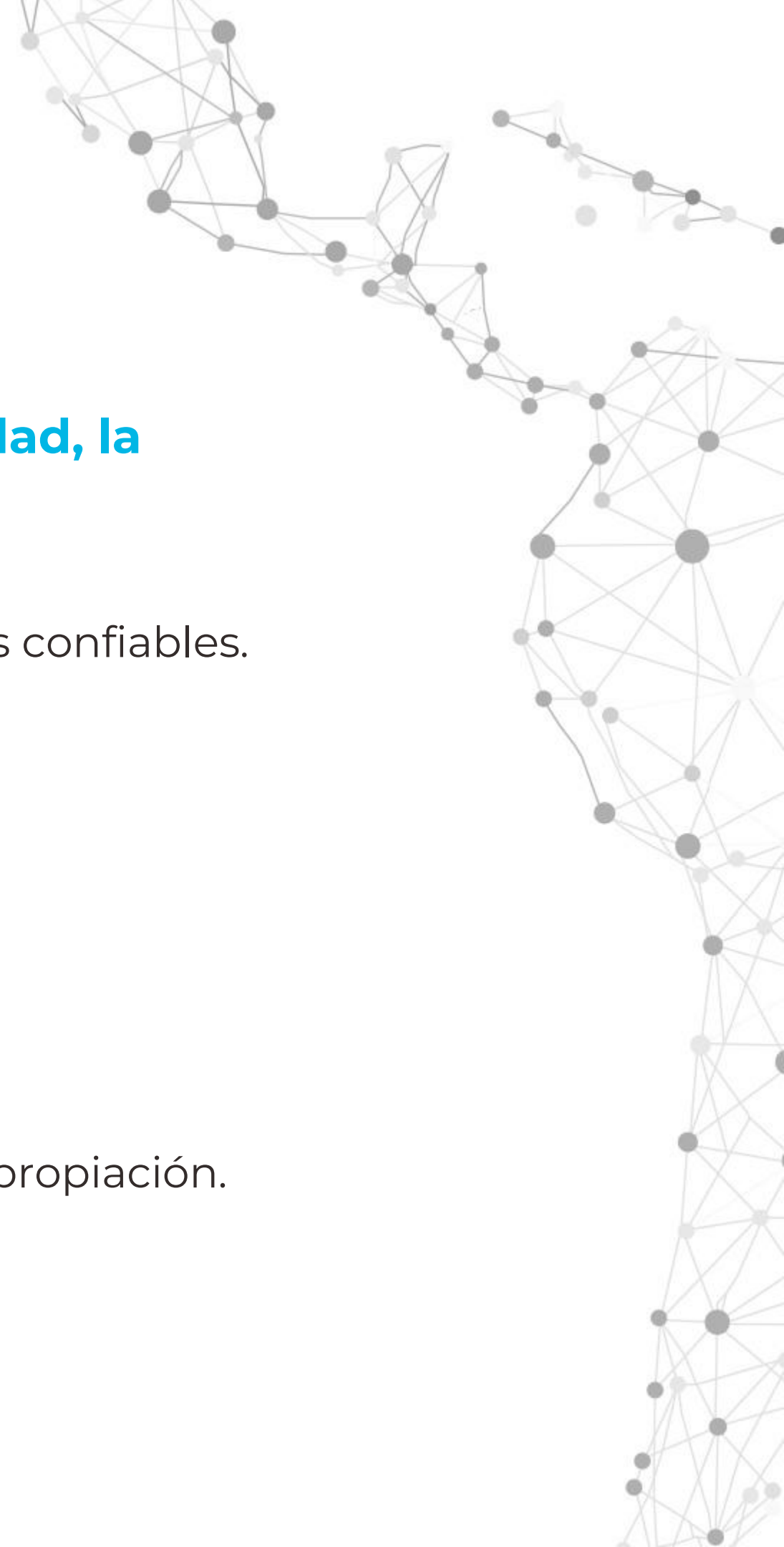
AUTENTICACIÓN

Garantizar que solo el titular acceda y presente credenciales.

3

RECUPERACIÓN

Restaurar el acceso tras una pérdida o ataque sin facilitar la apropiación.





EMITIR
Identificar +
firmar



GUARDAR
Proteger
credencial +
claves



PRESENTAR
Consentir +
minimizar
datos



VERIFICAR
Prueba +
validez +
estado

RECORRIDO

Del documento oficial al servicio digital en cuatro pasos seguros.

EXCESO

Un servicio pregunta: «¿Esta persona es mayor de 18 años?».

El ciudadano muestra nombre, fecha, número, foto y otros datos.

El verificador recibe y puede conservar datos que el servicio nunca necesitó.

MINIMIZADO

Presentar «mayor de 18: sí» con emisor, validez y prueba criptográfica.

MENOS DATOS
en circulación

MENOR IMPACTO
ante incidentes

PROPÓSITO CLARO
para la persona

ESTÁNDARES

Un catálogo de estándares todavía no es un perfil interoperable.

1

DATOS + PRUEBAS

W3C VC 2.0, SD-JWT VC, Data Integrity e ISO mdoc.

2

EMISIÓN + PRESENTACIÓN

OpenID4VCI y OpenID4VP por web, QR, NFC y BLE.

3

CONFIANZA + ESTADO

Esquemas, garantía, listas, expiración, suspensión y revocación.



PRIVACIDAD

Una pantalla de consentimiento no basta; la privacidad debe estar en la arquitectura.

1

MINIMIZAR

Solicitar y revelar solo lo que el servicio realmente necesita.

2

VINCULAR EL PROPÓSITO

Identificar al verificador, el uso declarado y la retención prevista.

3

PRESERVAR LA ELECCIÓN

Limitar la correlación; ofrecer alternativas, corrección y reparación accesible.





SERVICIOS
PÚBLICOS
Identidad,
beneficios +
trámites



EDUCACIÓN
+ TRABAJO
Diplomas,
licencias +
historial



SERVICIOS
FINANCIERO
S
KYC
reutilizable +
prevención
del fraude



MOVILIDAD +
ACCESO
Permisos,
boletos +
autenticación

LATAM

Cuatro frentes pueden generar
valor tangible con credenciales
reutilizables y verificables.

SEGURIDAD

Perspectiva de Infineon · las claves privadas y las operaciones sensibles no deben depender solo del software o de la nube.

1

HARDWARE SEGURO

Los elementos seguros y el hardware certificado protegen claves y respaldan garantías auditadas.

2

CONFIANZA OPERATIVA

NFC, USB, tarjetas y factores integrados sirven a recorridos móviles, físicos e híbridos.

3

RESISTENCIA AL FRAUDE

Una raíz física de confianza dificulta la extracción de claves, la clonación y el robo de identidad.

INFINEON

PROTECCIÓN DE LA RAÍZ
Elementos seguros y controladores
certificados protegen claves y
operaciones criptográficas aisladas.

FORMATO + AUTENTICACIÓN
USB, NFC, tarjetas y factores integrados
admiten MFA, biometría y recorridos
híbridos.

EL ROL DE INFINEON

Infineon habilita la capa de confianza en hardware que
conecta identidad digital, dispositivo y servicio final.

SECORA™ ID KEY
autenticación segura

TEGRION™
controladores de seguridad

CIPURSE™ + JAVA CARD™
transporte + identidad pública



CONFIAR. DERECHOS.

