



¿Qué es la Identidad Digital (ID)?

Mesa de Investigación de la
Secretaría del GAFIC
03 de noviembre de 2021.





La identidad oficial es la especificación de una persona física única que es:



Basado en características de la persona que establecen la singularidad de una persona en la población o contexto(s) particular(s).



Reconocido por un país para fines reglamentarios y otros fines oficiales.



Generalmente depende de alguna forma de registro, documentación o certificación proporcionada o emitida por el gobierno que constituye evidencia de los atributos básicos para establecer y verificar la identidad oficial.





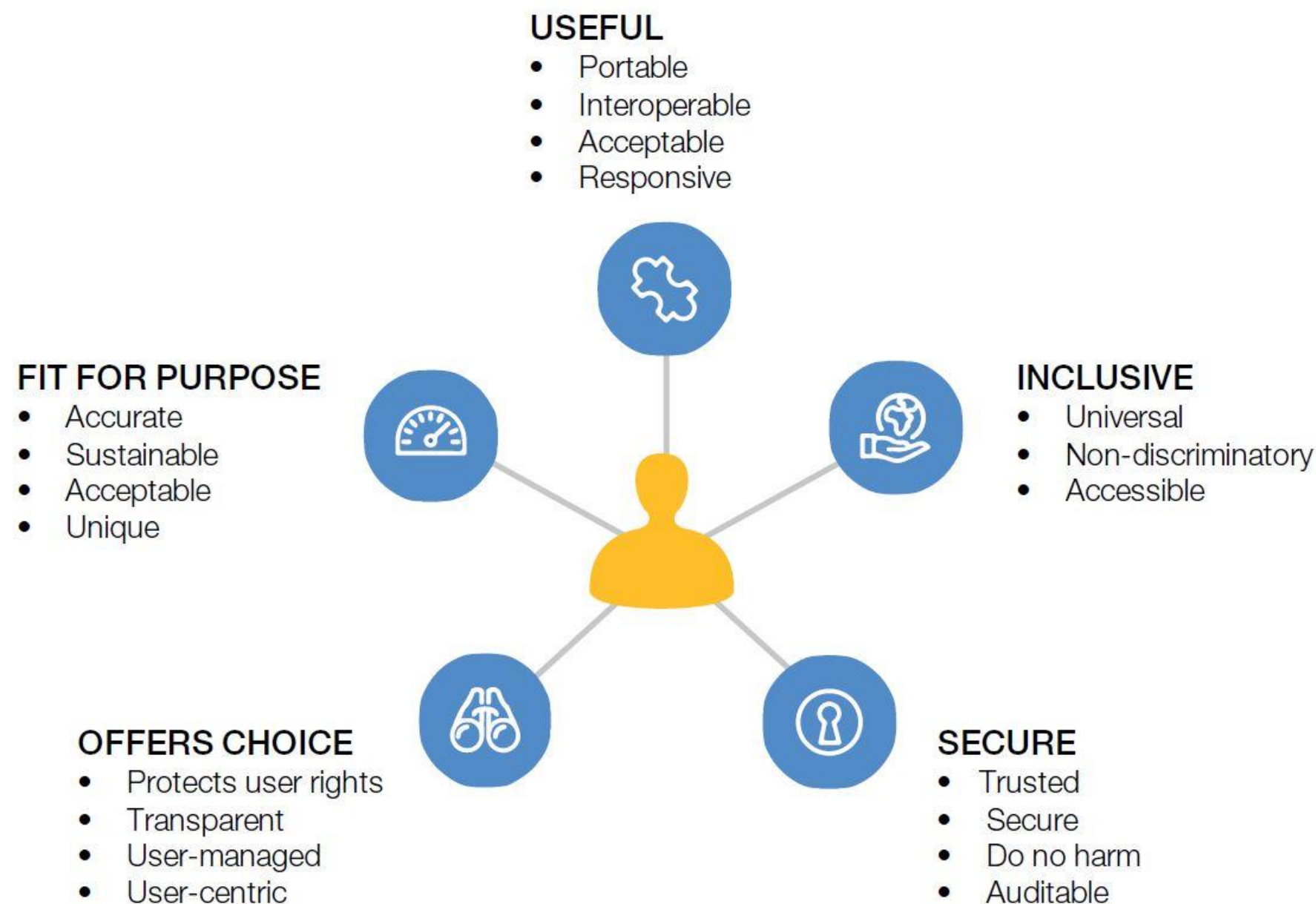
¿Qué es la Identidad Digital (ID)?



- Una identidad digital se puede definir como un conjunto de registros digitales que verifican que una persona es quien dice ser y le permite realizar transacciones en el mundo digital moderno. (1)
- Una identificación digital se puede autenticar de forma remota a través de canales digitales, lo que se puede hacer independientemente de la entidad emisora de la identificación. La identificación digital también se puede aplicar independientemente de la tecnología específica utilizada para realizar la autenticación digital, que puede variar desde el uso de datos biométricos hasta contraseñas, PIN o dispositivos inteligentes y tokens de seguridad. (2)



Cinco Elementos de una Buena Identificación Digital



¿Qué es un sistema de identificación digital?



- La Guía del GAFI sobre Identificación Digital señala que los sistemas de identificación digital utilizan medios electrónicos para afirmar y probar la identidad oficial de una persona en línea (digital) y/o en entornos personales en varios niveles de garantía. (1)
- Los niveles de garantía miden el nivel de confianza en la confiabilidad e independencia de un sistema de identificación digital y sus componentes.
- La Guía de Sistemas de Identificación del Banco Mundial también describe que los sistemas de identificación digital son aquellos que utilizan tecnología digital durante todo el ciclo de vida de la identidad, incluso para la captura, validación, almacenamiento y transferencia de datos; gestión de credenciales; y verificación y autenticación de identidad. (2)





Aplicación de los Estándares del GAFI a DDC (R.10) y sistemas de identificación digital



Identificación y verificación

- R. 10 (a) requiere que las entidades identifiquen al cliente y verifiquen la identidad de ese cliente, utilizando "documentos, datos o información de fuentes independientes y confiables".
- R. 10 no impone ninguna restricción sobre la forma (documental / física o digital) que pueden tomar las pruebas de identidad, "documentos fuente, información o datos".
- Las entidades deben vincular la identidad verificada de un cliente con el individuo de alguna manera "confiable", pero la forma en que esto se hace depende del marco legal de cada jurisdicción para la DDC.
- El requisito de que los "documentos, datos o información de origen" digitales deben ser "fiabes, independientes" significa que el sistema de identificación digital utilizado para realizar la DDC se basa en la tecnología, la gobernanza adecuada, los procesos y los procedimientos que proporcionan el nivel adecuado de confianza de que el sistema produce resultados precisos.





Aplicación de los Estándares del GAFI a DDC (R.10) y Sistemas de Identificación Digital



Enfoque Basado en Riesgos (RBA)

- Las entidades reguladas deben aplicar un RBA para determinar el alcance de las medidas de DDC que se utilizarán para la identificación /verificación del cliente. Estos deben ser proporcionales al tipo y nivel de riesgos de LA / FT.

Debida diligencia continua sobre la relación comercial

- R. 10 (d) requiere la debida diligencia y el escrutinio continuos de las transacciones realizadas durante el curso de la relación comercial.
- La autenticación mediante un sistema de identificación digital establece la confianza de que una persona es la misma persona a la que se le realizó una prueba de identidad y se le emitieron las credenciales pertinentes.
- La autenticación digital continua de la identidad del cliente vincula a esa persona con su actividad financiera y puede fortalecer la capacidad de llevar a cabo una diligencia debida y un monitoreo de transacciones significativos y continuos.





Beneficios de los Sistemas de Identificación Digital para el Cumplimiento ALA / CFT



Fortalecer la Diligencia Debida del Cliente (DDC)

- Los sistemas de identificación digital pueden mejorar la confiabilidad, seguridad, privacidad, conveniencia y eficiencia de identificar a las personas de los servicios financieros, en beneficio de los clientes, las entidades reguladas y la integridad del sector financiero.
- Minimizar las debilidades en las medidas de control humano: reducir el error humano y el juicio subjetivo.
- Mejorar la experiencia del cliente y generar ahorros de costos: experiencias más eficientes y fáciles de usar para los clientes potenciales y menores costos para las entidades reguladas.
- Monitoreo de transacciones: puede facilitar la identificación y reporte de transacciones sospechosas, porque ayuda a la entidad regulada a establecer que la persona que accede a una cuenta.
- Puede permitir que las entidades reguladas capturen información adicional para obtener una comprensión detallada del comportamiento del cliente.





Beneficios de los Sistemas de Identificación Digital para el Cumplimiento ALA / CFT



Inclusión Financiera

- Permite a las personas económicamente excluidas que carecen de acceso a los documentos de identidad oficiales tradicionales y los utilizan para obtener servicios financieros en situaciones apropiadas de bajo riesgo.
- Los sistemas de identificación digital pueden llegar a poblaciones excluidas en áreas remotas para respaldar la prueba / inscripción segura de identidad no cara a cara para la identificación / verificación del cliente.
- Los sistemas de identificación digital pueden facilitar los pagos de gobierno a persona (G2P), el pago de salarios y pensiones del gobierno y la asistencia para salvar vidas en contextos humanitarios.





Desafíos de los Sistemas de Identificación Digital para el Cumplimiento ALA / CFT



Riesgos de inscripción y pruebas de identidad

- Puede resultar en identificaciones digitales que son "falsas" (es decir, obtenidas bajo premisas falsas a través de un acto intencionalmente malicioso).
- La información de identidad robada o falsificada se puede utilizar para facilitar actividades ilícitas, como el fraude y el robo.
- La prueba de identidad y / o la autenticación de personas a través de Internet pueden crear riesgos relacionados con ciberataques y posibles robos de identidad a gran escala.
- Estos riesgos se mitigan al tener un nivel de garantía de identidad adecuado.





Desafíos de los Sistemas de Identificación Digital para el Cumplimiento ALA / CFT



Riesgos de la gestión del ciclo de vida de la autenticación y la identidad

- Los diferentes tipos de autenticadores / procesos pueden ser vulnerables a los riesgos que permiten a los malos actores utilizar la identidad legítima de un individuo para que una parte que confía acceda a bienes y servicios.
- La mayoría de las vulnerabilidades de autenticación se explotan sin el conocimiento del propietario, pero el abuso también puede implicar el intercambio deliberado de credenciales de identidad con fines ilícitos.
- Los riesgos relacionados con los esfuerzos ALA/CFT incluyen autenticadores de contraseñas, autenticadores biométricos y riesgos desconocidos a través de cambios en el diseño técnico.





Desafíos de los Sistemas de Identificación Digital para el Cumplimiento ALA / CFT



- Problemas de conectividad: la falta de una infraestructura confiable puede socavar los sistemas de identificación digital. Sin embargo, los sistemas de identificación digital pueden diseñarse para admitir transacciones tanto en línea como fuera de línea.
- Marcos nacionales para la identidad oficial: las deficiencias en la confiabilidad de la evidencia de identidad documental en la que se basan los sistemas de identificación digital pueden afectar los riesgos a los que están expuestos estos sistemas.
- Desafíos de la Protección de Datos y la Privacidad (DPP): las salvaguardas de DPP son importantes para reducir el riesgo de robo de identidad y los riesgos de ciberseguridad que podrían socavar la confiabilidad del sistema de identificación digital.
- La Recomendación 2 del GAFI propone que las autoridades ALA/CFT y DPP deben buscar cooperar y coordinarse para asegurar la compatibilidad de los requisitos y reglas de DPP.



¡Gracias!

Mesa de Investigación de la Secretaría del GAFIC

cfatf@cfatf.org

<http://www.cfatf-gafic.org>

