الإتحاد
الأفريقي

An Integrated, Prosperous
and Peaceful Africa

إطار الاتحاد الإفريقي للهويات الرقمية المتوافقة

FEBRUARY 2022

جدول المحتويات

الملخص التنفيذي 1

اختصارات 4

1. المعلومات الأساسية 5

1.1 السياق 5

1.2 حالة نظم الهويات في أفريقيا 6

1.3 مبادرات أخرى تعزز الاعتراف المتبادل والتشغيل المتوافق للهويات الرقمية في أفريقيا 8

1.4 السيادة الرقمية 10

2. المقدمة 12

2.1 الرؤية والأهداف وحالات الاستخدام الإرشادي 12

2.2 النطاق 14

2.3 إطار الثقة، وخصوصية البيانات، والتشغيل المتوافق والمعايير 15

3. الإطار 17

3.1 المبادئ التوجيهية 18

3.2 النموذج 19

3.3 عملية موثوق بها - إطار الثقة 21

3.4 خيارات التحقق المحتملة 24

4. خارطة طريق رفيعة المستوى للتنفيذ 27

4.1 المرحلة الأولى: اعتماد الإطار والبيئة التمكينية 27

4.2 المرحلة الثانية: تنفيذ الإطار واعتماد المواصفات التقنية للهوية الرقمية المتوافقة 30

4.3 المرحلة الثالثة: تطوير البنية التحتية لتمكين التحقق عن بُعد 30

5. افتراضات وتحديات ومخاطر عالية المستوى **32**

5.1 الافتراضات 32

5.2 التحديات العامة ومقترحات عالية المستوى للحد منها 32

5.3 المخاطر والآليات المقترحة للحد منها 33

6. الملحق **35**

6.1 تعريفات المصطلحات 35

الملخص التنفيذي

يفتقر مئات الملايين من الناس في أفريقيا إلى الهوية القانونية، وهناك عدد أكبر بكثير منهم لديهم بطاقات هوية لا تصلح للغرض المقصود منها في هذا العصر الرقمي؛ ونتيجة لذلك، فإنهم يواجهون تحديات في الوصول إلى الخدمات والفرص التي يتم إنشاؤها من خلال الرقمنة، ولذلك، فإن نظم الهوية الرقمية المتوافقة والموثوق بها والشاملة، والتي توفر للناس القدرة على التحقق من هويتهم القانونية دون اتصال بالإنترنت وعلى الإنترنت، يمكن أن تساعد على التصدي لتلك التحديات، ولها إمكانات كبيرة لتسريع رقمنة الاقتصادات والمجتمعات الأفريقية من خلال دعم تنظيم المشاريع والمساهمة في التنفيذ الناجح لمنطقة التجارة الحرة القارية الأفريقية، ولهذه الأسباب تقوم معظم البلدان الأفريقية حاليًا بتحديث نظمها الرقمية للهويات الشخصية وإن كانت في مراحل مختلفة.

ويحدد إطار عمل الهوية الرقمية المتوافقة رؤية تمكن جميع المواطنين الأفارقة من الحصول بسهولة وأمان على الخدمات العامة والخاصة التي يحتاجونها، عندما يحتاجون إليها، بغض النظر عن مواقعهم، ولهذا الغرض، يحدد الإطار المتطلبات المشتركة، والمعايير الدنيا، وآليات الحوكمة، وزيادة المواءمة بين الأطر القانونية مع الأهداف التالية:

1. السماح للمواطنين الأفارقة بإثبات هويتهم القانونية خارج الإنترنت وعلى الإنترنت للوصول إلى خدمات القطاعين العام والخاص في الدول الأعضاء في الاتحاد الأفريقي وبهذا تتم المساهمة في تحقيق تقدم متسارع نحو الوحدة القارية والتكامل من أجل النمو المستدام والتجارة وتبادل السلع والخدمات وحرية تنقل الأشخاص ورأس المال من خلال إنشاء أفريقيا المتحدة والتكامل الاقتصادي السريع من خلال منطقة التجارة الحرة القارية الأفريقية كما هو مذكور في الطموح 2 من أجندة 2063؛ بالإضافة إلى تمكين المواطنين الأفارقة من التحكم في بياناتهم الشخصية، بما في ذلك القدرة على الكشف بشكل انتقائي فقط عن المعلومات المطلوبة لمعاملة معينة؛ وينبغي أن تكون المعلومات الشخصية التي سيتم الكشف عنها ضئيلة وتتناسب مع المعاملة وأن تحتوي فقط على المعلومات ذات الصلة بتلك المعاملة بالذات مع الأخذ في الاعتبار الوضع الأفريقي الخاص وبما يتماشى مع أفضل الممارسات الدولية.

2. تعزيز الثقة والتوافق بين النظم الأساسية لتحديد الهوية للدول الأعضاء في الاتحاد الأفريقي.
ينص الإطار على نظام موحد على المستوى القاري للتمثيل الرقمي لإثباتات الهوية الصادرة عن مصادر موثوقة من الدول الأعضاء في الاتحاد الأفريقي، وضمان إمكانية توافق الهويات في جميع أنحاء القارة. سيتمكن الأفراد الذين يحملون بطاقة هوية من نظام وطني من الحصول على بيانات ثبوتية الهوية القانونية المتوافقة (IDC-ID) التي ستأخذ شكل بيانات يمكن التحقق منها. وسيتم تحديد معايير لإطار التشغيل التوافقي الذي سيحدد البيانات الرئيسية التي ستتوفر في الهوية الرقمية المتوافقة ومتطلبات التشفير للتوقيع الرقمي، هذه المعايير هي ما ستمنح الثقة في البيانات الثبوتية الرقمية التي أنشأت بموجب معايير إطار الثقة الذي يحدد الشروط والمعايير التي سيتم بموجبها إصدار البيانات الثبوتية هذه من قبل جهات موثوقة في الدول الأعضاء في الاتحاد الأفريقي.

للدول الأعضاء في الاتحاد الأفريقي الحرية في اختيار الطريقة التي تريد بها إصدار البيانات الثبوتية الرقمية هذه، مع إمكانية تخزينها في شكل رقمي بحت على تطبيق على الهاتف الذكي، أو الخوادم السحابية، أو بطاقة ذكية أو رابط إلى التمثيل الرقمي باستخدام باركود ذي بعد واحد أو ثنائي الأبعاد على وثيقة ورقية (مطبوع على بطاقة ورقية أو بلاستيكية). كما يمكن للدول الأعضاء أن تقرر استخدام هذه المعايير لتمثيل بيانات الهوية على المستوى الوطني، أو على مستوى المجتمعات الاقتصادية القارية أو الإقليمية أو حتى إصدارها بشكل منفصل لتُكمّل نظم الهوية الرقمية الموجودة من قبل.

يستند الإطار إلى تطوير نظم هوية أساسية قابلة للتشغيل المتوافق وشاملة وموثوق بها، وهذه النظم ستوفر العمود الفقري لمصادر البيانات الموثوقة للهوية القانونية للأفراد، وبالتالي تمكن بيانات إثبات الهوية الرقمية القابلة للتشغيل المتوافق من

---

[1] انظر ، اللائحةانظر اللائحة العامة لحماية البيانات في الاتحاد الأوروبي (GDPR) ،، 2016: https://gdpr.eu (GDPR) 2016:..

[2] ”المطالباتالمعلومات“ هي مجموعة من السمات حول المتعلقة بموضوع البيانات: على سبيل المثال ،، اسم العائلة أو تاريخ الميلاد.
”المطالبة المعلومات التي يمكن التحقق منها“ هي نسخة يمكن معرفة ما إذا تم إثبات التلاعب بها من هذه المعلومات والتي يمكن التحقق منها بشكل مشفر للتحقق من صحتها.

والتي هذه المعايير هي ما ستمنح الثقة في ستثبت الثقة في البيانات الثبوتية الرقمية كما التي أنشأت تم إنشاؤهابموجب معايير في إطار الثقة الذي يحدد الشروط والمعايير التي سيتم بموجبها إصدار البيانات الثبوتية هذه من قبل مصادر جهات موثوقة من في الدول الأعضاء في الاتحاد الأفريقي .

لالدول الأعضاء في الاتحاد الأفريقي حرة الحرية في اختيار الطريقة التي تريد بها إصدار البيانات الثبوتية الرقمية هذه. ، ويمكن مع إمكانية تخزينها في شكل رقمي بحت على تطبيق على الهاتف الذكي، أو خادم سحابة القائمةالخوادم السحابية، أو يمكن إنشاء بطاقة ذكية أو وصلة رابط إلى التمثيل الرقمي باستخدام الباركود واحد ذي بعد واحد أو ثنائيأو اثنين من الأبعاد على وثيقة ورقية (المطبوع ة على بطاقة ورقية أو الورق، بطاقة بلاستيكية). كما يمكن للدول الأعضاءهم أن تيقرروا إعادة استخدام هذها لمعاييار لتمثيل بيانات الهوية على المستوى الوطني، أو كجزء من حل الهوية الرقمية على مستوى المجتمعات الاقتصادية القارية أو الإقليمية أو حتى إصدارها بشكل منفصل استكمالا لتُكمّل لأنظمةنظم الهوية الرقمية الموجودة من قبل.

يوسيستند الإطار إلى تطوير نظم معرفية هوية أساسية قابلة للتشغيل المتبادل المتوافق وشاملة وموثوق بها، حيث وهذه النظم سأنها توفر العمود الفقري لمصادر موثوقة اللبيانات الموثوقة لالمتعلقة بالهوية القانونية للناسللأفراد، وبالتالي تمكن بيانات اعتمادبيانات إثبات الهوية الرقمية القابلة للتشغيل المتبادل المتوافق من تحقيق مستويات أعلى من الضمان. ، ولذلك تُشجع الدول الأعضاء في الاتحاد الأفريقي على تعزيز نظم الهوية التأسيسية الأساسية مع الأخذ في الاعتبار آليات الدعم مثل والمبادئ المتعلقة بتحديد الهوية لأغراض التنمية المستدامة . ويعتمد ويأخذ هذا الإطار أيضاأيضًا في اعتباره على ويعتمد على الجهود القارية الموازية التي تهدف إلى لخلق بيئة تمكينية تمكن منتهدف إلى حماية البيانات الشخصية، والحفاظ على الأمن السيبراني، وضمان حقوق الناسالأفراد، مع اعتماد اتفاقية مالابو للأمن السيبراني وحماية البيانات الشخصية والعمل الجاري لوضع إطار سياسة البيانات القارية.

يمكن إكمال استكمال إصدار بيانات اعتماد الهوية الرقمية القابلة للتشغيل المتداخلالمتوافقة (IDC-ID) مع ببنية تحتية تمكن تتيح حالات استخدامات أكثر تقدمًا مثل المصادقة عن بعد. ويسلط هذا الإطار الضوء على العديد من الخيارات التقنية المتاحة للدول الأعضاء في الاتحاد الأفريقي لتنفيذ هذه الطبقةالمرحلة، مثل ومن أمثلة هذه الخيارات اتحاد مقدمي خدمات الهوية الذين يقدمون آليات التوثيق لحاملي أوراق اعتماد الهوية الرقمية القابلة للتشغيل المتبادلالمتوافقة (IDC-ID)، أو تطوير حلول محفظة الهوية الرقمية أو أي نماذج أخرى تمكن من التشغيل المتبادلالتوافقي.؛ كما ستتمكن ستستطيع الدول الأعضاء في الاتحاد الأفريقي من السعي إلى مزيد من الاتفاق بشأن كيفية إنشاء هذه البنية التحتية لطبقة لمرحلة التوثيق، وإلى الشراكة مع الجماعات الاقتصادية الإقليمية وغيرها من المبادرات القارية التي تحقق تعمل بالفعل في على إدخال حلول أساسية قابلة للتشغيل المتبادل المتوافقلل ل الهوية الرقمية للوصول إلى الخدمات عن بعد.

ويستند ويعتمد نجاحتنفيذ الإطار المقترح عإلى افتراض فرضية أن الدول الأعضاء في الاتحاد الأفريقي ستعتمده وتصدق وتؤيدهعليه. وللقيام بذلك، يجب التخفيف من بعض المخاطر ومعالجتها ومواجهة بما فيهاالتحديات التي تم تحديدها للتخفيف من حدة التفرد المحتمل، وضعف الآليات الأمنية، وتلاشي الخصوصية الشخصية، وعدم اليقين بشأن الاستفادة من نظام الهوية الرقمية التأسيسيةالأساسية، والافتقار إلى القدرة التقنية والمالية، وجفاف وفقر مراكز البيانات في جميع أنحاء أفريقياأفريقيا (هامة لتخزين البيانات الحساسة)، ووجود أنظمةنظم هوية غير قابلة للتشغيل المتبادل التوافقي وأطر قانونية وتنظيمية عفا عليها الزمن، ويتم تناول هذه التحديات بمزيد من التعمق في القسم 5..

أقرت 30 منظمة دولية وإقليمية المبادئ العشرة لتحديد الهوية من أجل التنمية المستدامة ،، بما في ذلك المؤسسات الأفريقية مثل لجنة الأمم المتحدة الاقتصادية لأفريقيا ،، ومصرف التنمية الأفريقي ،، وأفريقيا الذكية ،، وكذلك اعتمدها عدد من البلدان الأفريقية. انظر: https://id4d.worldbank.org/principles.

الاتحاد الأفريقي (2014) ،، اتفاقية الأمن السيبراني وحماية البيانات الشخصية ،، انظر: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

وتتألف الوثيقة من الأقسام التالية:

1 **معلومات أساسية** عن عمل الاتحاد الأفريقي الذي أدى أدت إلى إنشاء هذه الوثيقة، ونظرة عامة عن حالة نظم ال الهويات في أفريقياأفريقيا، وسلسلة من المبادرات التي تعزز قابلية التشغيل المتوافق لالهوية الرقمية في القارة؛

2 **مقدمة** للرؤية والأهداف والنطاق وحالات الاستخدام المحتمل لإطار العمل البيني التوافقي المقترح. للمؤيد الرقمي للاتحاد الأفريقي؛

3 نظرة عامة على **العناصر الرئيسية التي تشكل الإطار**، ولا سيما المبادئ التوجيهية لتصميمه وتنفيذه، والنموذج المختار، والمكونات الرئيسية للإطار الذي يتعين يحتاج مزيدًا من التحديدزيادة تعريفه (مثل قواعد المشاركة، والتشغيل المتبادلالمتوافق، والمتطلبات التقنية)، فضلافضلًا عن ثلاثة خيارات بنيوية معمارية محتملة لإقامة طبقةللتوثيق تقبل مصادقة قابلة للتشغيل البينيالمتوافق.

4 وهناك خارطة طريق رفيعة المستوى توضح النهج المرحلي المقترح لتعريف لتحديد الإطار وتنفيذه، فضلافضلًا عن الإجراءات الملموسة التي قد ستتخذها الدول الأعضاء والاتحاد الأفريقي.

5 الافتراضات والتحديات والمخاطر الرفيعة الهامالمستوى التي يتعين التصدي لها والآليات الموصى بها للتخفيف من آثارها.

ولا يدعو الإطار إلى إنشاء نظام رقمي قاري موحد، بل يؤسس لإمكانية التشغيل المتبادل المتوافق بين أنظمةنظم الهويات الرقمية القائمة للدول الأعضاء في الاتحاد الأفريقي والذي يأخذ في الاعتبار السيادة الرقمية للدول الأعضاء في الاتحاد الأفريقي ، والاختلافات في الرقمية. نشر البنية التحتية، وتوافر السياسات واللوائح ذات الصلة ، والأنواع المختلفة لأنظمةنظم تحديد الهوية ،، وهشاشة ورد فعل السكان أثناء وبعد تنفيذ أنظمةنظم الهوية الرقمية القابلة للتشغيل البينيالمتوافق.

اختصارات

AfCFTA منطقة التجارة الحرة القارية الأفريقية - AfCFTA
AML/CFT - مكافحة غسل الأموال وتمويل الإرهاب ومكافحة تمويل الإرهاب
- واجهة برمجة تطبيقات - API
-الاتحاد الافريقي الاتحاد الافريقيالأفريقي - AU
AUC - مفوضية الاتحاد الأفريقي
-فرق الاستجابة لحوادث الكمبيوتر الحاسوب - CIRTs
-التسجيل المدني والإحصاءات الحيوية - CRVS
-هيئة حماية البيانات - DPA
-تقييم تأثير حماية البيانات - DPIA
-جماعة شرق إفريقياأفريقيا - EAC
-الجماعة الاقتصادية لدول غرب أفريقياأفريقيا - ECOWAS
المؤسسة الألمانية للتعاون الدولي - GIZ
النظام العالمي للاتصالات المتنقلة - GSMA
-وحدات أمان أاللجهزة - HSMs
-تكنولوجيا المعلومات والاتصالات - ICT
-بيانات البيانات الثبوتية للهوية الرقمية المتوافقةالاعتماد الرقمية القابلة للتشغيل البيني للهوية - IDC-ID
-الاتحاد الدولي للاتصالات السلكية واللاسلكية - ITU
-اعرف عميلك - KY
-مستوى الضمان - LOA
-إطار عمل الثقة لعموم إفريقياأفريقيا - PATF
-الجماعةت الاقتصادية الإقليمية - REC
الطرف المعول - RP
-التحالف الائتماني لأفريقياأفريقيا الذكية - SATA
- إطارالاتحاد الإطارالافريقي للتفعيل المتبادل للهويات الرقميةThe Framework
- لجنة الأمم المتحدة الاقتصادية لأفريقياأفريقيا - UNECA
غرب أفريقياأفريقيا التعريف الفريد للتكامل الإقليمي والشمول - WURI

See Annex I for working definitions.

1. المعلومات الأساسية

1.1 السياق

إن القدرة على إثبات هوية الشخص أمر ضروري لتمكينه من الحصول على الخدمات وممارسة الحقوق. وتقليدياوالمعمول به سابقًا هو ، يمكن إثبات الهوية على أساس الألفة والمظهر والشهادة من جانب الآخرين، الذين وهو أمر نجح يعملون في المجتمعات المحلية غير الرسمية الأصغر حجمًا وغير رسمية، ومع اتساع المجتمعات والاقتصادات وإضفاء الطابع الرسمي عليها وانإدماجها، أدخلت وثائق تفويض ثبوتية مادية ملموسة مثل بطاقات الهوية وجوازات السفر لإرساء الثقة. و، ومع ذلك، ومع تحول البلدان إلى المجتمعات والاقتصادات الرقمية، فإن الأوراق الثبوتية المادية الملموسة هذه ليست مفيدة جدا في لإثبات الهوية عبر الإنترنت وعند تنفيذ المعاملات الرقمية الأخرى مثل المدفوعات الرقمية وتبادل البيانات الشخصية. و، ولذلك، فإن الهويات الرقمية، التي تتمثل في الهويات التي تستخدم التكنولوجيات والنهج الحديثة لتمكين الناس من إثبات هويتهم والتحقق منها بأمان عبر الإنترنت، شرط مسبق للثقة على الإنترنت.

ويمكن أن يوفر تحديد الهوية، ولا سيما بطاقات الهوية الرقمية، مجموعة واسعة من الفوائد للبلدان، مثل الحكم الرشيد، والشمول المالي، والمساواة بين الجنسين وتمكين المرأة، وتعزيز الحماية الاجتماعية والرعاية الصحية ونتائج التعليم. وبالنسبة للأشخاص ، فإنها توفر أداة لتأكيد حقوقهم وأهليتهم للخدماتة سيرفيس والمعاملات. و، وبالمثل، فإنها توفر منصة للحكومات والشركات لتبسيط وتوسيع وابتكار وتجديد عملياتها عند تقديم الخدماتها من خلال استخدام الرقمنة والأتمتة، وخاصة عندما ينظر إليها للموضوع على أنها "كومة قناة رقمية" مع لتبادل البيانات الموثوق بها ومنصات الدفع الرقمية. ، وبالنظر إلى أن الإنترنت ليس لها حدود، فإن ال الهويات

الرقمية التي تصدر في بلد ما ومعترف بها في بلدان أخرى يمكن أن تكون أيضاأيضًا محركًا قويًا للتكامل الاجتماعي والاقتصادي، سواء على الصعيد الثنائي أو الإقليمي أو العالمي.

تحقق الهويات الرقمية أكبر قدر من الأمان والتأثير عندما تستند إلى الهوية القانونية للأفراد. و، وعادة ما تدار الهوية القانونية من خلال النظام البيئي الأساسي للهوية التأسيسية في بلد ما، بما في ذلك التسجيل المدني والهوية الوطنية وغيرها من النظم المماثلة. و، ومع ذلك، لا يزال مئات الملايين من الناس في أفريقياأفريقيا يفتقرون إلى الهوية التأسيسية الأساسية مثل الهوية الوطنية أو شهادة الميلاد. وفي هذا السياق، أعلنت الجمعية العامة ل الاتحاد الأفريقي في يوليو/تموز ٢٠١٦ أن ٢٠١٧ - ٢٠٢٦ هي هو العقد لإعادة وضع برنامج السجل المدني والمقاييس الحيوية كأولوية على أجندة التنمية على المستوى إعادة وضع إعادة وضع برنامج التنمية الإقليمية والقارية والوطني ة في أفريقياأفريقيا، وحثت الحكومات على الاستجابة باتخاذ الإجراءات المناسبة.

أجندة ٢٠٦٣م: إن أفريقياأفريقيا التي نريدها، وهوي الإطار الاستراتيجي للتنمية الاجتماعية - والاقتصادية والتحول في القارة في غضون فترة 50 عامًا، قد دعت إلى الهوية القانونية للجميع. وأقرت استراتيجية التحول الرقمي لأفريقياأفريقيا في الدورة العادية السادسة والثلاثين للمجلس التنفيذي للاتحاد الأفريقي في فبراير/شباط ٢٠٢٠ في أديس أبابا في، إثيوبيا (EX.CL/Dec. 1074 (XXXVI)؛ . كما أكد CL/Dec. 1074 (XXXVI) كما أكدت على أهمية الهوية الرقمية كلبنة بناء لإنشاء سوق رقمية موحدة (وهي مهمة يشاركها تشترك فيها أيضاأيضًا تحالف أفريقياأفريقيا الذكية) بما يتماشى مع اتفاقية التجارة الحرة القارية لأفريقياأفريقيا.

سلطت جائحة كوفيد الضوء على أهمية المداخن القنوات الرقمية لأن البلدان التي كانت موجودة لديها مثل هذه القنوات بشكل كامل أو جزئي قبل بدء الوباء كانت قادرة بشكل أفضل على تقديم المساعدة الاجتماعية بسرعة وفعالية وكانت أكثر مرونة عندما كان يجب نقل الخدمات الشخصية التي تتم في الواقع إلىعبر الإنترنت.

سلطت جائحة كوفيد الضوء على أهمية القنوات الرقمية لأن البلدان التي كانت موجودة لديها مثل هذه القنوات بشكل كامل أو جزئي قبل بدء الوباء كانت قادرة بشكل أفضل على تقديم المساعدة الاجتماعية بسرعة وفعالية وكانت أكثر مرونة عندما كان يجب نقل الخدمات الشخصية التي تتم في الواقع إلى عبر الإنترنت.

وأقرت استراتيجية التحول الرقمي لأفريقياأفريقيا أيضاأيضًا بأن تنمية الاقتصاد الرقمي والمجتمع الرقمي تعتمد على عوامل تمكين هامة، لا سيما بيئة تمكينية قوية فيما يتعلق بالأمن السيبراني وحماية البيانات، و. تضع اتفاقية مالابو للأمن السيبراني وحماية البيانات الشخصية لعام ٢٠١٤ ٢٠١٤ إطارًا قانونيًا وسياساتي وسياسيًا وتنظيميًا يدعم إنشاء بيئة رقمية آمنة للمعاملات الرقمية والتجارة الإلكترونية ونقل البيانات. و، وللأسف، لم يوقع بعد على هذا الإطار القانوني بعد ويصدق عليه العدد المطلوب من الدول الأعضاء في الاتحاد الأفريقي لكي يدخل حيز النفاذ، مما يحد من فعاليته فعليافي الواقع .، ولن يسهم هذا الإطار القانوني في تعزيز الثقة في الإطار والإدماج فحسب، بل سيخفف أيضاأيضًا من المخاطر المرتبطة بالمراقبة والتمييز غير المرخصين، ولا سيما بالنسبة للفئات الضعيفة أو المهمشة، فضلافضلًا عن ضمان مساءلة السلطات المنفذة.

1.2 حالة أنظمة نظم الهويات في افريقيا أفريقيا

تعد أنظمةنظم تحديد الهوية الموثوقة والشاملة أداة عامل تمكين للعديد من النتائج الإنمائية مثل القضاء على الفقر، والحكم الرشيد، والهجرة الآمنة والمنظمة، والحماية الاجتماعية، والمساواة بين الجنسين، وهي محرك مهم للتحول الرقمي. ونظرًا للحاجة الأساسية الملحة إلى تحديد الهوية والتوثيق عبر الإنترنت بشكل آمن ودقيق، فإن الهوية الرقمية وغيرها من خدمات الثقة - مثل التوقيعات الإلكترونية - تمثل الحدود التالية لبلدان القارة. و عندما يتم تمكينها من خلال البنية التحتية الرقمية التي تجلب تضع الأشخاص والمنظمات عبر على الإنترنت ،، يمكن سنتمكن من الاستفادة من خدمات المعرف الرقميالهوية الرقمية والثقة من قبل المنصات الحكومية والتجارية لتسهيل مجموعة متنوعة من المعاملات الرقمية ،، بما في ذلك المدفوعات الرقمية، و. على مستوى الدولة ،، يمكن أن تيعمل المعرّف الرقميالهوية الرقمية كمعرّف فريد للأنظمةنظم التي تتمحور حول المواطن مما يمكن من ديجعله قابلاً للتطبيق على دمج الأنظمةنظم. و، وتوفر منصات الهوية الرقمية والمدفوعات معًا الوسائل اللازمة للتحرك نحو مجتمع غير نقدي، مما يخلق مكاسب في الإنتاجية، ويقلل من الفساد والاحتيال، ويزيد من تحسين راحة المستخدمين.

في جميع أنحاء القارة، توجد مجموعة واسعة من أنواع أنظمةنظم الهويات مع ومستويات مختلفة من الروابط التنمية الإنمائية مع بتقديم الخدمات. و، وهناك بلدان أخرى كثيرة في مستويات متوسطة من التنمية مع وتوجد بهاوجود فجوات في التغطية بين السكان الفئات السكانية سريعة التأثرالضعفاء وقدراتها الرقمية الناشئة، في حين لا تزال نظم الهوية التأسيسيةأساسية غير موجودة أو ناشئة حديثًا في بعض الدول الأخرى. و، وبشكل عامعموما، زاد شهد عدد البلدان التي تنفذ تفعّل نظم بطاقات الهوية الوطنية زيادة هائلة خلال العقدين الماضيين، مدفوعًا بالرغبة في تحسين كفاءة واستهداف المدفوعات والتحويلات الحكومية، وتعزيز نزاهة الانتخابات وتحسين خدمات القطاع المالي (بما في ذلك عن طريق تسجيل بطاقة SIM او وعملية التحقق من هوية العملاء KYC) والانتخابات، وتعزيز الأمن العام وتعزيز الهجرة الآمنة والمنظمة. و، وهناك زخم مستمر لإصلاح وتحديث نهج تصميم النظام وتنفيذه بما مع وجود دليل على توسعيتماشى مع توسيع الأدلة على الممارسات الجيدة والدروس المستفادة من برامج ال هويةالهوية الناجحة[10].

. وخير مثال على ذلك رواندا التي شنت حملة لرقمنة اقتصادها وتمكين الطبقة المتوسطة من خلال اتخاذ إجراءات مثل الانتقال إلى اقتصاد غير نقدي، وهو ما تهدف الحكومة إلى تحقيقه من خلال اختراق نشر الهواتف المحمولة في كل مكان والوصول السريع إلى الإنترنت، وقد. انضمت رواندا إلى تحالف Better Than Cash، وهو شراكة عالمية ملتزمة بالانتقال من النقد إلى المدفوعات الرقمية، و. تحقق رواندا بالفعل زيادة في الكفاءة والإيرادات عن طريق بإلغاء تكاليف التحصيل وغيرها من النفقات. كما أصبحت الشركة الدولة رائدة في مجال المعرفة في المنطقة، وتتبادل أفضل الممارسات مع الآخرين الدول الأخرى المهتمةين باتباع مسار نهج مماثل[11].

---

[7] البنك الدولي ،، مجموعة بيانات ID4D العالمية ،، انظر: https://id4d.worldbank.org/global-dataset. ()

[8] AU (2014)،، اتفاقية الأمن السيبراني وحماية البيانات الشخصية ،، انظر: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

[9] اعتبارًا من يوليو 2021 ،، وقعت 14 دولة عضوًا من أصل 55 على اتفاقية مالابو (المرجع نفسه) ،، من بينها 10 دول أعضاء صدقت عليها. لدخول الاتفاقية حيز التنفيذ ،، يلزم تصديق ما لا يقل عن 15 دولة عضو.

وقد زادت القدرات الرقمية لأنظمةنظم الهوية بشكل كبير، على الرغم من أن التعريف الرقمي في سياق المعاملات عبر الإنترنت لا يزال في مراحله الأولى. و، وعلى مدى العقد الماضي، شرعت بلدان عديدة في بذل الجهود لتحديث نظم تحديد الهوية لديها، بهدف إنشاء منصة رقمية وإصدار وثائق تفويض ثبوتية تدعم مجموعة متنوعة من الاستخدامات والخدمات. و، وكثيرًا ما تنطوي هذه الإصلاحات على الانتقال من النظم الورقية إلى النظم الرقمية باستخدام التقاط جمع البيانات الإلكترونية وإدارة البيانات، وعادة أيضًا ما تتضمن وإدخال آليات التحقق من الهوية الرقمية والتوثيق ها عليها -– حتى الآن في الوقت الراهن، ومعظمها في سياق المعاملات الشخصية.

أغلبية البلدان الأفريقية (٨٥ %في المائة) لديها نظم وطنية للبطاقة الهوية تدعمها قاعدة بيانات إلكترونية، على الرغم من أن العديد منها لا يزال يعتمد على السجل والعمليات المدني والعمليات ة الورقية، وتوفر العديد من النظم فائدة محدودة لتقديم الخدمات. يتم جمع البيانات البيومترية الحيوية من قبل أكثر من ٧٠% في المئة من البلدان الأفريقية في وقت التسجيل لضمان تفرد الهويات. على الرغم من أن بعض البلدان - مثل كينيا وليسوتو ونيجيريا ورواندا وجنوب أفريقياأفريقيا - تقدم خدمات التحقق من الهوية الرقمية (للوزارات الحكومية والبنوك وما إلى ذلك) للتحقق من صحة معلومات الهوية أو الاوراق الثبوتية مقابل قاعدة بيانات مركزية، إلا أن المصادقة على معظم المعاملات لا تزال تعتمد على الفحص اليدوي لبطاقات الهوية المادية. و، ولا تزال حلول الهوية الرقمية التي تمكن من التوثيق الآمن للخدمات والمعاملات عبر الإنترنت في مراحلها الأولى في القارة، حيث لا تتوفر هذه الخدمات إلا في عدد قليل من البلدان (على سبيل المثال في جنوب أفريقياأفريقيا من قبل البنوك، في الرأس الأخضر، سيشيل لخدمات الحكومة الإلكترونية).

على الرغم من العديد من التحسينات وإطلاق أنظمةنظم جديدة في السنوات الأخيرة، تواجه البلدان الأفريقية وسكانها العديد من التحديات عندما يتعلق الأمر بتحديد الهوية. و، وتشمل بعض المجالات الرئيسية التي تتطلب التعزيز: إمكانية الوصول إلى أنظمةنظم الهوية، وقدرتها على دعم تقديم الخدمات بفعالية، وتنفيذ الضمانات التي تعزز الثقة وخصوصية البيانات.

ويشكل **ضمان إمكانية الوصول الشامل لنظم الهوية تحديًا مستمرًا.** و، وهناك ما يقدر بمليار شخص في جميع أنحاء العالم يفتقرون إلى وثائق الهوية الأساسية - ويقيم ما يقرب من نصف السكان هؤلاء في أفريقياأفريقيا؛ كما أن أفريقياأفريقيا هي موطن لثمانية ٨ من البلدان العشرة التي توجد فيها أكبر فجوات في الهوية بين الجنسين على الصعيد العالمي، كما أن تغطية الهوية بين البالغين في أفريقياأفريقيا جنوب الصحراء الكبرى أقل ب ١٠ نقاط مئوية بين النساء منها بين الرجال. و، وتبدأ التحديات في تحديد الهوية منذ الولادة: ١٠٠ مليون

طفل دون سن الخامسة في أفريقياأفريقيا لم يسجلوا عقب ولادتهم. وأسباب هذه الفجوات في التغطية متعددة وتشمل: ارتفاع التكاليف المباشرة و(خاصة) غير المباشرة للالتحاق، بما في ذلك تكاليف السفر إلى مواقع التسجيل البعيدة في كثير من الأحيان؛ والتكاليف غير المباشرة للالتحاق بالمدارس؛ و والمتطلبات المستندية والإدارية المعقدة للتسجيل؛ والطلب المحدود حيث توفر أنظمةنظم الهوية قيمة محدودة من حيث تسهيل الوصول إلى الخدمات.

كما أن **استخدام التكنولوجيات الحديثة زاد من التعقيد، ويشكل مخاطر جديدة.** فعلى سبيل المثال، لا تتكيف جميع الحلول بشكل جيد مع الاحتياجات والسياقات المحلية حيث قد يكون الاتصال بالإنترنت، أو الحصول على الكهرباء، أو محو الأمية الرقمية بين موظفي الخدمة المدنية أو عامة السكان محدودًا، وأيضًا عدم القدرة على تغيير الموردين هو مشكلة شائعة. قفل البائع هو مصدر قلق مشترك ، وغالباً ما تيرتبط مع بتكاليف التشغيل المرتفعة بشكل لا يمكن تحمله ،، ومحدودية التشغيل المتبادلالمتوافق المحدود لنظام الهوية ،، وانخفاض مستويات الرقابة الحكومية والفردية والتحكم في بيانات الهوية. و، وبالإضافة إلى ذلك، ومع زيادة اعتماد التكنولوجيات الرقمية في تحديد الهوية والتوثيق، فضلافضلاً عن التحول نحو الوثائق الثبوتية الرقمية، فإن الأشخاص ذوي المعرفة الرقمية المحدودة والوصول إلى الأجهزة المتصلة معرضون لخطر التخلف عن الركب.

---

[10]كشفت دراسة استقصائية أجريت عام 2018 لمسؤولين حكوميين أفارقة أن 60 في المائة من البلدان الأفريقية كانت تخطط لإطلاق نظام هوية أو تحديث النظام الحالي بحلول نهاية عام 2020.

[11](إطار الاستثمار الرقمي لأهداف التنمية المستدامة، الاتحاد الدولي للاتصالات/تحالف التأثير الرقمي (DIAL)، ٢٠١٩).

ومع رقمنةرقمنة الأنظمةنظم ومعالجة البيانات، ازدادت الحاجة إلى تنفيذ ضمانات فعالة لحماية البيانات وخصوصية الفرد أيضاأيضًا؛ كما. إ أن عدم كفاية الضمانات لحماية البيانات والخصوصية وحقوق المستخدمين - سواء كانت قانونية أو مؤسسية أو تكنولوجية - يمكن أن يجعل أنظمةنظم ال هويةالهوية عرضة للانتهاكات ويترك بيانات الأشخاص دون حماية. و، ولا يزال أمام العديد من البلدان طريق طويل في بناء أنظمةنظم هوية آمنة وموثوقة: فوفقاً ًا للأونكتاد، لم يعتمد سوى ٢٨ بلدًا (٥٠ %في المائة) في أفريقياأفريقيا تشريعات لحماية البيانات والخصوصية، و ٣٩ بلداً ًا (٧٠% في المائة) لديها تشريعات بشأن الجرائم السيبرانية. و، وحتى في الحالات التي توجد فيها هذه الأطر، فإن ترجمة الأحكام القانونية إلى ضوابط مؤسسية وتشغيلية وتقنية فعالة يمكن أن يشكل تحديًا. و، وحتى اليوم، لا عدد قليل من البلدان يخزن البياناتها ويديرها سوى عدد قليل من البلدان وفقاً ًا لأفضل الممارسات الدولية للحماية من السرقة أو فقدان البيانات عن غير قصد.

تواجه أنظمةنظم الهويات الرقمية نفس التحديات التي تواجهها تنمية نظم البيئاتة الرقمية؛ وتشمل هذه التحديات ،- ضمن أمور أخرى -، مسائل مشكلات التمويل، حيث أن دورات التمويل، (ولا سيما الدورات القائمة على المانحين والقائمة على المشاريع والمقيدة زمنيًا)، غالبًا ما تكون منفصلة عن دورات تطوير التكنولوجيا. و، وغالبًا ما يكون هناك نقص في التمويل المتاح لتوسيع نطاق تكنولوجيا المعلومات والاتصالات ، حيث تميل الأموال إلى أن تكون متاحة فقط لمراحل دورة حياة تطوير التكنولوجيا ، مع محدودية التمويل المتاح للتوسيع على المستوى الوطني، وبالإضافة إلى ذلك، فإن التخطيط في الصوامع واتخاذ القرارات عادة ما يكون على نقاط منفصلة بين مجموعات أصحاب المصلحةمما يؤدي إلى فرص محدودة للتنسيق بين مجموعات أصحاب المصلحة؛ التي والذي بدوره يحدتحد من إعادة استخدام الحلول الرقمية ويقتقوض إمكانية تطبيقها عبر البرامج والقطاعات. و، وكثيراً ًا ما تكون أوجه القصور في محو الأمية الرقمية بما فيها ، أي نقص القدرات في قيادة تكنولوجيا المعلومات والاتصالات، وفي اختيار وتصميم وتنفيذ وتوسيع نطاق وصيانة حلول تكنولوجيا المعلومات والاتصالات، مسألة هي موضوعات للنقاش بين الحكومات والعاملين في مجال التنمية. و. أخيرا، فإن غياب التمويل اللازم لتوسيع نطاق حلول تكنولوجيا المعلومات والاتصالات يشكل مصدر قلق كبير آخر، حيث يمكن عادة توفير الأموال لتمويل المراحل المبكرة من دورة حياة تطوير التكنولوجيا، ولكن مع توفر تمويل محدود للتوسع على المستوى الوطني (إطار الاستثمار الرقمي لأهداف التنمية المستدامة، الاتحاد الدولي للاتصالات/ تحالف التأثير الرقمي (DIAL)، ٢٠١٩).

1.3 مبادرات أخرى تعزز الاعتراف المتبادلالمتبادل والتشغيل المتبادلالمتوافق للهويات الرقمية في أفريقياأفريقيا

هناك عدد من المبادرات القائمة التكميلية القائمة للإطار تعزز بالفعل الاعتراف المتبادلالمتبادل والتشغيل المتبادلالمتوافق للهويات الرقمية في أفريقياأفريقيا. و، وتشمل هذه الخطوات، على سبيل المثال لا الحصر:

1.3.1 استراتيجية التحول الرقمي لأفريقياأفريقيا (٢٠٢٠-٢٠٣٠)

من المسلم به أن الهويات الرقمية هي واحد من خمسة مواضيع شاملة للاستراتيجية، التي تقدم أيضاً ًا عشر توصيات بشأن السياسات العامة وإجراءات مقترحة عبر موضوعين هما ضمان الإدماج والأمن والخصوصية وملكية البيانات، ودعم التشغيل المتبادلالمتوافق والحياد. و، وفي حين أن هذه التوصيات تغطي بشكل رئيسي تطوير أنظمةنظم الهوية الرقمية الوطنية، فإن إحدى التوصيات تدعو إلى إنشاء "هوية رقمية قارية قابلة للتشغيل المتبادلالمتوافق ومفتوحة، تسمح بالتحقق من الأفراد والتوثيق عليهم"، في حين تطلب توصية أخرى من مفوضية الاتحاد الأفريقي ولجنة الأمم المتحدة الاقتصادية لأفريقياأفريقيا وشركاء آخرين "العمل معاً ًا على وضع المعايير القارية والإقليمية، بما في ذلك بروتوكولات المصادقة، والحد الأدنى من حقول البيانات ،، وبروتوكولات إزالة الازدواجية، والصيغ البيومترية الحيوية، فضلافضلًا عن الصيغ الأخرى، واللوائح النموذجية، وغيرها من المعايير.

1.3.2 مبادرة لجنة الأمم المتحدة الاقتصادية لأفريقياأفريقيا بشأن الهوية الرقمية

أطلقت لجنة الأمم المتحدة الاقتصادية لأفريقياأفريقيا مبادرة بشأن الهوية الرقمية والتجارة والاقتصاد الرقمي، تعمل كمركز للتميز، تهدف إلى مواءمة المعايير ذات الصلة، واعتماد لوائح لحماية الأمن، وزيادة الاستثمارات، وتطوير قدرات ومهارات الجهات الفاعلة الرئيسية الفاعلة. وتدعم اللجنة الاقتصادية لمركز التميز الرقمي في أفريقياأفريقيا هدف العمل الهادف إلى إنشاء إطار قاري أفريقي منسق بشأن الرقالهويةم الرقمية، وتحديد وتشكيل السياسات والمعايير المتعلقة بالبطاقة الرقمية، وتوفير تنمية القدرات للدول الأعضاء، والجماعات الاقتصادية الإقليمية، والاتحاد الأفريقي. و، وأصدرت اللجنة الاقتصادية لأفريقياأفريقيا ورقة بيضاء عن إطار للعمل الرقمي المتبادلالمتوافق من خلال إنشاء إطار استئماني لعموم أفريقياأفريقيا (PATF).

1.3.3 تحالف افريقياأفريقيا الذكية -SMART AFRICA TRUST ALLIANCE أو (SATA)

مبادرة أفريقياأفريقيا الذكية هي مبادرة من رؤساء الدول الأفريقية لتسريع التنمية الاجتماعية والاقتصادية في أفريقياأفريقيا من خلال الاستفادة من تكنولوجيا المعلومات والاتصالات. في عام ٢٠٢٠، ترأست بنين مشروع رائد تحت مسمى أفريقياأفريقيا الذكية لوضع مخطط الهوية الرقمية، بدعم من فريق عامل ضم رواندا وتونس والاتحاد الأفريقي والاتحاد الدولي للاتصالات السلكية واللاسلكية والبنك الدولي وشبكة أوميديار الاستثمارية ولجنة الأمم المتحدة الاقتصادية لأفريقياأفريقيا والجمعية الدولية لشبكات الهاتف المحمول والمنتدى الاقتصادي العالمي والوكالة الألمانية للتعاون الدولي (GIZ) وعدة شركات خاصة. و، وقد اعتمده مجلس افريقياأفريقيا الذكية، بما في ذلك الدول الأعضاء فيه، والاتحاد الأفريقي والاتحاد الدولي للاتصالات، الذي يضم ٣٢ دولة. و، ويقترح المخطط أن يكون تحالف افريقياأفريقيا الذكية منصة لتسهيل التعرف الموثوق به على الالهويات الرقمية بين مجموعة من الجهات الفاعلة من خلال آليات إصدار الشهادات الموتحدة. ومن المتوقع أن تجري مشاريع تجريبية لتحالف افريقياأفريقيا الذكية بين بنين ورواندا وتونس وغيرها من الدول الأعضاء في أفريقياأفريقيا الذكية. و، وسوف يعمل تحالف افريقياأفريقيا الذكية كحل سريع وقابل للتكيف لتمكين التشغيل المتبادلالمتوافق بين مختلف مخططات الهوية العامة والخاصة في القارة. المزيد من التفاصيل ستكون متاحة على sata.smartafrica.org

1.3.4 برنامج غرب افريقياأفريقيا للهويات الفريدة من أجل تحقيق اللتكامل والإدماج الإقليمي (WURI)

برنامج غرب افريقياأفريقيا للهويات الفريدة من أجل تحقيق اللتكامل والإدماج الإقليمي (WURI) هو برنامج إقليمي يستفيد من التمويل من البنك الدولي لزيادة فرص الحصول على الخدمات في الدول الأعضاء المشاركة في الجماعة الاقتصادية لدول غرب أفريقياأفريقيا من خلال بناء نظم الهوية التأسيسيةالأساسية التي يمكن لجميع الأشخاص في أراضي البلد الوصول إليها -– دون بغض النظرمراعاة عن الجنسية أو الوضع القانوني - وهي مصممة مع مراعاة إمكانية التشغيل المتبادلالمتوافق عبر الحدود لفتح المجال أمام الوصول إلى الخدمات الاجتماعية، الخدمات الصحية والمالية وغيرها عبر الحدود. و، وانضمت ساحل العاج وغينيا ولجنة الجماعة الاقتصادية لدول غرب أفريقياأفريقيا إلى المرحلة الأولى خلال عام ٢٠١٨، وانضمت بنين وبوركينا فاسو والنيجر وتوغو إلى المرحلة الثانية خلال عام ٢٠٢٠. و، وتشمل المبادئ الرئيسية لبرنامج غرب افريقياأفريقيا للهويات الفريدة من أجل تحقيق اللتكامل والإدماج الإقليمي التسجيل الشامل للجميع، وتقليل البيانات إلى أدنى حد، والاوراق الثبوتية الأساسية التي تقدم بتكلفة صفرية للسكان.

1.3.5 بروتوكول السوق المشتركة لجماعة شرق افريقياأفريقيا

من خلال المادة ٨ من البروتوكول، التزمت الدول الست الشريكة لأفريقياأفريقيا في مجموعة شرق أفريقياأفريقيا بالعمل تدريجيا من أجل "... نظام موحد لإصدار وثائق هوية وطنية لمواطنيها". ويرتبط ذلك ارتباطًا وثيقًا بتحقيق أهداف البروتوكول الأخرى، بما في ذلك حرية حركة السلع (المادة ٦)، والأشخاص (المادة ٧)، والعملوالعمالة/العمال (المادة ١٠)، والخدمات (المادة ١٦)، ورأس المال (المادة ٢٤)، فضلافضلًا عن حقوق التأسيس والإقامة (المادتان ١٣ و ١٤ على التوالي). غير أن نظم الهوية الوطنية في مراحل مختلفة من التطوير. و، ومع ذلك، وبروح الهندسة المرونةالمتغيرة، وكبادرة من مشاريع التكامل الممر الوطني للممر، بدأت كينيا ورواندا وأوغندا في عام ٢٠١٤ بالاعتراف ببطاقات الهوية الوطنية لبعضها البعض كوثائق سفر صالحة فيما بينها. و، وفي إطار البرنامج الممر الوطني للاستفادة من هذه المسألة، جرت مناقشات للبناء على ذلك في حالات استخدام إضافية مثل الخدمات الإلكترونية، غير أن هذه الحالات لم تتحقق بعد. في عام ٢٠١٨، أجرت أمانة البنك الدولي و ومجموعة شرق أفريقياأفريقيا دراسة حول خيارات الاعتراف المتبادلالمتبادل بالهويات الوطنية في مجموعة شرق أفريقياأفريقيا التي اقترحت أربعة معالممراحل.

1.4 السيادة الرقمية و وسيادة البيانات

أفريقياأفريقيا، التي تضم ٥٥ دولة ذات سيادة، لديها ٥٥ اختصاصات قانونية يتعين النظر فيها. و، وتصف السيادة الرقمية طائفة من المفاهيم التقنية والتنظيمية المختلفة، تتراوح بين الموقع المادي للخوادم، وبناء الكابلات تحت سطح البحر، والقوانين والممارسات المتعلقة بحماية البيانات وفرض الضرائب على أسواق البيانات، التي تمكن الدول من اتخاذ قراراتها الخاصة بشأن الخيارات التكنولوجية وتنظيمها.

من أجل ضمان سيادة البيانات، تشجع الدول الأعضاء في الاتحاد الأفريقي على ما يلي:

لإنشاء أنظمةنظم تخزين آمنة للبيانات الشخصية (بما في ذلك البيانات الحساسة) من خلال تصميم وإنشاء مراكز بيانات وطنية والتي يجب أن توفر سيطرة الدولة على البيانات وتشمل على الأقل مساحة تخزين ومعالجة مخصصة حصريًا للبيانات الشخصية والحساسة. سيكون من الضروري أيضًاأيضًا وضع الضمانات المطلوبة (التقنية ،، على وجه الخصوص) لضمان أن البيانات المستخدمة في تبادل المعلومات عبر الحدود لا تتضمن بأي شكل من الأشكال البيانات الشخصية أو الحساسة التي قد تشكل معالجتها أو تخزينها مخاطر جسيمة على حقوق الأفراد أو سيادة الدول الأعضاء في الاتحاد الأفريقي.

بناء القدرات والبنية التحتية لتنمية المواهب الأفريقية ومجموعات المهارات لمواجهة التحديات الجديدة وتعزيز السيادة الرقمية. يُتوقع من الدول الأعضاء أن تأخذ زمام المبادرة في تطوير المهارات (بما في ذلك مهارات المرونة الإلكترونية) لجميع المواطنين والمقيمين ،، وينبغي أن تمكّن الناس من التحكم في بياناتهم الشخصية.

إقامة شراكة قائمة على الاحترام المتبادلالمتبادل والوضع والاستفادة لكلاالمربح ل الجانبين دون المساس بالسيادة والملكية الوطنية وتجنب التدخلات الأجنبية التي قد تؤثر سلبًا على الأمن القومي والمصالح الاقتصادية والتطورات الرقمية للدول الأعضاء في الاتحاد الأفريقي.

وسيسترشد الإطار بالقواعد السيادية التي تمثلها تضعها سلطاتة التسجيل وإصدار الهوية في كل دولة عضو في الاتحاد الأفريقي أو سلطاتها، وستعتمد الدول الأعضاء في الاتحاد الأفريقي هيكل الإدارةإداري يتضمن، بما في ذلك إنشاء مؤسسة تنسيق قارية للرقابة. و، وعلاوة على ذلك، فإن آليات المساءلة، بما في ذلك معالجة الالتزامات في حالة عدم الالتزامسوء السلوك، ستحددها وتصدق عليها الدول الأعضاء في الاتحاد الأفريقي، مما وبعد يشكل تتطوير الثقة القارية بين الدول ذات السيادة ذات المخططات المختلفة لتحديد الهوية الرقمية مهمة معقدة ولكنها قابلة للتحقيق وتتطلب تعاونًا بين أصحاب المصلحة المتعددين. و، ولتحقيق قابلية تبادل المعلومات المتعلقة بالهوية القانونية في البلدان الأفريقية المعنية، يجب الاعتراف بالقواسم المشتركة بين القواعد والمعايير الوطنية القائمة، استنادًا إلى مجموعة حد أدنىدنيا من المعايير التي ستسمح بالسيادة المحلية والثقة الكافية في نهج كل منها.

ولهذا الغرض، يتعين على الدول الأعضاء في الاتحاد الأفريقي تطوير أطرها القانونية وتعزيز قدراتها في ي مجال الإنفاذ القانون، ولا سيما قدرات سلطات حماية البيانات على رصد عمليات نقل البيانات عبر الحدود وإنفاذ القوانين واللوائح ذات الصلة في حالات الانتهاكات أو سوء الاستخدام.

وسيتبنى الإطار المقترح أحدث التكنولوجيات ويحترم تشريعات البلدان وأنظمتها. و، وينبغي ألا تكون الحكومات ملزمة باستخدام تكنولوجيات محددة. و، وينبغي أن يضمن استخدام المعايير والقواعد المفتوحة تنوعًا كبيرًا في الخيارات التكنولوجية من جانب الدول مع تيسير ملكية حقوق البلدان وإمكانية التشغيل المتبادلالمتوافق.

2. المقدمة

في عام ٢٠٢٠، اعتمدت الدول الأعضاء في الاتحاد الأفريقي استراتيجية التحول الرقمي لأفريقياأفريقيا (٢٠٢٠-٢٠٣٠) برؤية:

مجتمع واقتصاد رقمي متكامل وشامل واقتصاد في أفريقياأفريقيا يحسن نوعية حياة مواطني أفريقياأفريقيا، ويعزز القطاع الاقتصادي القائم، ويمكن من تنويعه وتنميتها، ويضمن الملكية الحقوق القارية لأفريقياأفريقيا كمنتج وليس كمستهلك في الاقتصاد العالمي فحسب.

ن تحقيق هذا الطموح – وكذلك طموح اتفاقية التجارة الحرة القارية الأفريقية القارية – يعتمد على تطوير أنظمةنظم الهوية الرقمية التأسيسيةالأساسية الشاملة والموثوق بها التي تمكن جميع الناس في أفريقياأفريقيا من إثبات هويتهم القانونية والتحقق منها بشكل موثوق وآمن عند التعامل شخصيًا وعبر الإنترنت، وتمكين مقدمي خدمات القطاعين العام والخاص من التعرف على أوراق اعتماد إثبات الهوية، بغض النظر عن المكان الذي تم إصدارها فيه في أفريقيامن أفريقيا. و، والأهم من ذلك، يجب تصميم أنظمةنظم الهوية الرقمية التأسيسيةالأساسية لتمكين الناس، وخاصة السكان المحرومين والمهمشين. و، وهذا سيمكن الجميع من المشاركة بشكل مجد في الاقتصاد الرقمي والمجتمع، وإطلاق العنان للوصول إلى الخدمات داخل البلدان وعبر الحدود، وتعزيز التجارة كجزء من اتفاقية التجارة الحرة القارية الأفريقية، وتعزيز الثقة في المجتمع الرقمي والاقتصاد الرقمي، والحد من الاحتيال وتكاليف ممارسة الأعمال التجارية.

والأهم من ذلك، يمكن لأنظمةنظم الهوية الرقمية التأسيسيةالأساسية أن تدعم أيضاأيضًا تطوير "أكوام قنوات رقمية" أوسع مع الدفع الرقمي ومنصات مشاركة البيانات الموثوقة لخلق فرص للابتكار للتجديد ومجموعة واسعة من المعاملات غير الورقية وغير الورقية وغير النقدية والتي لا تستلزم الحضور الشخصي في جميع أنحاء القارة. و، ومع ذلك، يتطلب ذلك أيضاأيضًا التخفيف بشكل شامل من المخاطر المتعلقة بالاستبعاد وحماية البيانات والأمن السيبراني والتكنولوجيا والتقيد بموردين معينين. و، ولهذه الأسباب، فإن المعرف الرقميالهوية الرقمية هيو واحد من خمسة مواضيع شاملة لاستراتيجية التحول الرقمي، مما يوفر التفويض الإلزام والإعداد لهذا الإطار.

2.1. الرؤية والأهداف وحالات الاستخدام الإرشاديالدلالي

تتمثل رؤية إطار الاتحاد الأفريقي للتشغيل المتبادلالمتوافق للهوية القانونية الرقمية في أن جميع المواطنون الأفارقة يمكنهم بسهولة وأمان الوصول إلى الخدمات التي يحتاجونها، عندما يحتاجونها الاقتضاء، من مقدمي الخدمات من القطاعين العام والخاص على حد سواء، مما سيشجع المشاركة الشاملة والهادفة في الاقتصاد والمجتمع الرقميين الأوسع نطاقًا ويسمح للخدمات بالعمل بثقة ويقين وضمان أكبر.

ولهذا الغرض، يحدد الإطار المتطلبات المشتركة، والحد الأدنى من المعايير الدنيا والقواعد، وآلية الحوكمة، وزيادة المواءمة بين الأطر القانونية مع الأهداف التالية:

1. السماح لجميع المواطنين الأفارقة بالتحقق من هويتهم القانونية خارج الإنترنت وعبر الإنترنت للوصول إلى خدمات القطاعين العام والخاص في جميع الدول الأعضاء في الاتحاد الأفريقي وبهذا يساهمون المشاركة هناك من خلال المساهمة في تحقيق تقدم متسارع نحو الوحدة القارية والتكامل من أجل النمو المستدام والتجارة وتبادل السلع والخدمات وحرية حركة الأشخاص ورؤوس الأموال من خلال إنشاء إفريقياأفريقيا الموحدة والتكامل الاقتصادي السريع من خلال منطقة التجارة الحرة القارية الأفريقية كما هو مذكور في الطموح 2 من أجندة 2063 .؛

2. تمكين المواطنين من التحكم في بياناتهم الشخصية، بما في ذلك القدرة على الكشف بشكل انتقائي فقط عن السمات المطلوبة لمعاملة معينة؛

3. تعزيز الثقة والتشغيل المتبادلالمتوافق فيما بين نظم تحديد الهوية التأسيسيةالأساسية للدول الأعضاء في الاتحاد الأفريقي.

ولا يدعو الإطار إلى إنشاء نظام رقمي قاري موحد، بل يؤسس لإمكانية التشغيل المتبادلالمتوافق لنظم الهويات الرقمية القائمة للدول الأعضاء في الاتحاد الأفريقي والذي يأخذ في الاعتبار السيادة الرقمية للدول الأعضاء في الاتحاد الأفريقي ،، والاختلافات في إطلاق البنية التحتية الرقمية ،، وتوافر السياسات واللوائح ذات الصلة ،، وأنظمةنظم تحديد المستويات المختلفة وهشاشة السكان أثناء وبعد تنفيذ أنظمةنظم الهوية الرقمية.

ومن الأهمية بمكان أن يتم تطوير هذا الإطار بما يتماشى مع أفضل الممارسات والمعايير الدولية التي تهدف إلى حماية البيانات الشخصية والحفاظ على الأمن السيبراني وضمان حقوق الناس. مع اعتماد اتفاقية مالابو للأمن السيبراني وحماية البيانات الشخصية والعمل الجاري لوضع إطار سياسة البيانات القارية، اتخذ الاتحاد الأفريقي خطوة هامة لإقامة بيئة رقمية موثوقة للمعاملات عبر الإنترنت من خلال اعتماد مجموعة مشتركة من القواعد التي تحكم نقل البيانات الشخصية عبر الحدود عبر القارة ومواءمة الأطر الوطنية لحماية البيانات والأمن السيبراني.

ويمكن للإطار القاري **تيسير الوصول إلى الخدمات في جميع البلدان المشاركة عن طريق بتمكين** الأشخاص والشركات من التحقق من الوثائق الثبوتية وغيرها من الحقائق دون الكشف عن البيانات الشخصية. و، ويشمل ذلك إمكانية التحقق من هويتهم عند الوصول إلى الخدمات عبر الإنترنت (مثل الخدمات الحكومية) في بلد آخر مع هوية رقمية دون الحاجة إلى التسجيل في حلول الهوية التأسيسيةالأساسية المحلية المعترف بها من قبل مقدمي الخدمات الأجانب. كما يُسهل الاعتراف بالهوية الرقمية وقابليتها للتشغيل المتبادلالمتوافق تبادل الاوراقالأوراق الثبوتية والبيانات الموثوق بها والموافقة عليها عند التقدم بطلب للحصول على الخدمات عندما يتطلب القانون مثل هذا التحقق (مثل إثبات التأمين وحالة التطعيم التأهيلي) مما يمكن الناس من توفير الوقت والحد من الروتين.

كما يمكن **أن يعزز هذا من سلامة نزاهة المدفوعات عبر الحدود والخدمات المالية في أفريقياأفريقيا وإمكانية الوصول إليها، وأن يخلق فرصًا** للابتكارللتجديد.؛ ف إن ضعف أنظمةنظم الهوية التي لا يعول يعتمد عليها، وغياب مواءمة تنسيق القوانينعد يخلق يضع العقبات مخاطر أمام مكافحة غسل الأموال/ مكافحة تمويل الإرهاب، مما يفرض حواجز أمام التبادلات عبر الحدود، ويرفع تكاليف الخدمات (مثل التحويلات المالية) ويعوق الابتكار.، و يمكن أن تسهل الهوية الرقمية تحديد هوية العملاء والتحقق منهم عند الصعود إلى الطائرة، ودعم عمليات عملية التحقق من هوية العملاء (KYC) والمساعدة في مراقبة المعاملات بغرض الكشف عن المعاملات المشبوهة والإبلاغ عنها. و، ولن يسهل الاعتراف المتبادلالمتبادل على المهاجرين إرسال الأموال إلى أوطانهم من خلال تخفيف عبء عملية التحقق من هوية العملاء (KYC) وعبء التوثيق فحسب، بل سيساعد أيضاأيضًا على خفض التكاليف، مما يساعد أفريقياأفريقيا على المضي أكثر نحو تحقيق الغاية هدف (١٠ ج) من أهداف التنمية المستدامة (10ج) المحددة عند 3 في المائة بحلول عام ٢٠٣٠.

ويمكن لإطار العمل القاري أيضاأيضًا أن يعزز التجارة والتجارة الإلكترونية بزيادة الثقة في المعاملات التجارية عبر الإنترنت وأن يسهل المعاملات التجارية والتجارة عبر أفريقياأفريقيا. و، وفي عام ٢٠٢٠، لم تمثل التجارة بين البلدان الأفريقية سوى ١٦ ,.٦% في المائة فقط من الناتج المحلي الإجمالي لأفريقياأفريقيا. ، وقد أطلقت تم إطلاق اتفاقية التجارة الحرة القارية الأفريقية في عام ٢٠١٩ لإطلاق فرص جديدة للتجارة والتجارة الإلكترونية بحلول عام ٢٠٣٠، و. يمكن أن يساعد الاعتراف عبر الحدود بالهويات الرقمية عبر الحدود في تعزيز عمليات التحقق من هوية المشترين والبائعين، وخاصة بالنسبة للسلع المقيدة التي تباع عبر الإنترنت. كما تتيح تمكن التوقيعات الإلكترونية ل ١٠٠٪ على الإنترنت، والمعاملات غير الورقية، والتي تمكن الشركات والعملاء من توفير الوقت وزيادة الأمن من خلال الحد من مخاطر الاحتيال في الهوية. كما أنه يبسط ممارسة الأعمال التجارية عبر الحدود، من خلال تمكين الشركات من إدارة تفاعلها تعاملاتها مع الحكومة رقميًا، على سبيل المثال مثل تقديم الإعلان الإقراراتعن الضريبية الضرائب، والمشاركة في إجراءات الشراءالتوريدات، وطلب رقم ضريبة القيمة المضافة وتطبيق التصاريح.

2.2 النطاق

لتحقيق هذه الأهداف، سيحدد الإطار ما يلي:

- نوع المعلومات/البيانات التي يمكن تبادلها في شكل حد أدنى من مجموعة البيانات لمعلومات الهوية التأسيسيةالأساسية؛
- طريقة إثبات هوية من أصدر البيانات وأنه يمكن الوثوق به؛
  - o إنشاء وضع إجراءاتعملية للتعريف بال لتوصيل مصادر الموثوقة لبيانات الهوية في كل دولة عضو في الاتحاد الأفريقي؛
  - o تحديد كيفية التحقق من صحة المطالبة البيانات الرقمية؛
- المعايير والعمليات التي تصف كيفية مشاركة البيانات من قبل المستخدمين والتحقق منها من قبل الآخرين في بيئة غير متصلة بعلى الإنترنت وخارجه.

تحدد هذه الوثيقة أسس إطار الثقة والتشغيل البينيالمتوافق لأنظمةنظم الهوية الرقمية عبر القارة الأفريقية. ، وستيحدد الحد الأدنى من المتطلبات اللازمة لضمان قابلية التشغيل البينيالمتوافق بين أنظمةنظم المعرف الرقميالهوية الرقمية الحالية والمستقبلية. تشير قابلية التشغيل البينيالمتوافق إلى قدرة الأطراف المختلفة في الإطار - مثل أنظمةنظم الهوية الرقمية وأنظمةنظم الأطراف المعتمدة المعوّلة - على التواصل والتفاعل بشكل فعال على المستويين التقني والدلالي.، و يمكن أن تسهل إمكانية التشغيل البينيالمتوافق الاعتراف المتبادلالمتبادل ،، وهو بناء أساس قانوني ،، ولكنها ليست شرطًا أساسيًا ولا تيضمن الاعتراف المتبادلالمتبادل. ولا يحدد إطار العمل نظام معرف رقميهوية رقمية

موحد لأفريقياأفريقيا ولا يتناول الاتفاقيات التجارية واتفاقيات المسؤولية بين الدول الأعضاء المشاركة.

العديد من البلدان الأفريقية لديها بالفعل أنظمةنظم الهوية الرقمية على قدم وساققائمة بالفعل وبعضها قد أدخلت قدرات التوثيق الرقمي. و، ويوفر الإطار المتطلبات مشتركة العامة لتشارك لمشاركة بيانات الهوية الأساسية والعمليات التي يمكن أن تكون قابلة للتشغيل المتبادلالمتوافق ومقبولة في الدول الأفريقية الأعضاء الأخرى، بينما تحتفظ الدول الأعضاء بالسيطرة الكاملة وحرية اختيار تصميم نظمها الوطنية. و.

سيكمل الإطار الأنشطة المرتبطة ببروتوكول المعاهدة المؤسسة للجماعة الأفريقية الاقتصادية إنشاء الجماعة الاقتصادية الأفريقية المتعلقة بحرية تنقل الأشخاص وحق الإقامة والحق في التأسيس، ولن يساهم في ازدواجيتها، ومؤتمر الوزراء الافريقيين الأفارقة المسؤولين عن التسجيل المدني والبرنامج الأفريقي للتعجيل بتحسين نظام التسجيل المدني والإحصاءات الحيوية. و، ويجب أنينبغي تُنسيق عملية تنفيذ الإطار تنسيقًا وثيقًا مع هذه المبادرة وغيرها من المبادرات ذات الصلة، مثل استكشاف الهجرة كحالة استخدام إضافية للهويات الرقمية في الوقت المناسب، وضمان تحسين تغطية وجودة نظم نظام التسجيل المدني والإحصاءات الحيوية كمدخلات هامة لنظم الهويات الرقمية الاساسية.

2.3. إطار الثقة، وخصوصية البيانات، والتشغيل المتبادل المتوافق والمعايير

ينبغي أن تعزز نظم الهوية الثقة بين مختلف الأطراف المشاركة، وأن تكفل مراعاة الحقوق القانونية لكل من المستخدمين الأفراد ووكالات ومؤسسات التشغيل، وتعزيز الاستخدام الأخلاقي لنظم الهوية. و، **ولضمان هذه الثقة، يجب تعريف مجموعة من القواعد التي توقع عليها جميع الأطراف وتلتزم بها**، وهي إطار الثقة.

وفي حين تعمل التكنولوجيا كعوامل تمكين رئيسية، تركز أطر الثقة أيضاأيضًا على العملية والإجراءات. و، وينبغي أن يحدد إطار الثقة القوي بوضوح ما يلي:

يستند إطار العمل على مبدأ التشغيل المتبادلالمتوافق. و، ولتيسير التشغيل المتبادلالمتوافق، يجب أن يكون كيانجهة ما قادرًا على الثقة بكيانجهة آخر ولا يستند فقط إلى سلامة العمليات التقنية (مثل إثبات التشفير، وما إلى ذلك)، ولكن أيضاأيضًا فيما يتعلق بمصدر البيانات التي يجري تقاسمها مشاركتها (مثل عمليات جمعها وإسناد سجل معين إلى فرد معين).

لا تتطلب قابلية التشغيل المتبادلالمتوافق أن تكون أنظمةنظم معرف الأساسالهوية الأساسية موحدة، بل ببساطة أن يتم اتباع معايير معينة مشتركة ومفتوحة معينة. و، وبموجب الإطار، يمكن لكل بلد مشارك إنشاء أنظمةنظام الهوية أنظمةأساسية مكيفة مع الاحتياجات والتقاليد والتشريعات المحلية، طالما تم اتباع معايير معينة تمكن من التشغيل المتبادلالمتوافق. تضع ينتج عن المعايير المفتوحة بروتوكولات تبادل مفهومة عالميا بشكل عام ومتسقة، وأنظمةنظم اختبار، وتدابير جودة، وممارسات جيدة فيما يتعلق بالتقاط بجمع بيانات الهوية القانونية وتخزينها ونقلها واستخدامها، فضلافضلًا عن شكل وسمات أوراق بيانات اعتماد إثبات الهوية القانونية وبروتوكولات التوثيق.

وعند النظر في إمكانية التشغيل المتبادلالمتوافق لأوراق لبيانات اعتماد إثبات الهوية القانونية الرقمية والمصادقة والتوثيق في جميع أنحاء القارة، سيكون من المهم النظر في المعايير المفتوحة لمطالبات لبيانات الهوية، وكيفية إصدارها، وكيفية توصيل نقل الثقة بين الكياناتالجهات المشاركة في إطار الثقة. و، وغالبًا ما تنشأ هذه المطالباتالبيانات، التي ستشكل الأساس للهوية الرقمية القانونية، من مصادر موثوقة مثل الوكالات الحكومية؛ كما يجب تحديد آلية مصادقة توثيق لتمكين حاملي الهوية الرقمية القانونية من مشاركة هذه المطالبات البيانات مع مقدمي الخدمات بشكل مناسب، وضمان أن يكون الكشف عن البيانات ثنائيًا وأن أي بيانات وصفية يتم تعميتها، وحماية خصوصية وحقوق الأفراد في جميع الأوقات.

وسيحدد هذا الإطار كيف يمكن إرساء الثقة في هذه المطالبات البيانات التي يمكن التحقق منها، وكيفي تة عمل عناصر ومعايير إدارة البيانات. و، ويمكن أن يكون التنفيذ التقني للحل مدفوعًا بالسوق التي ستكون قادرة على الاستفادة من إطار الثقة لتطوير حلول معرف هوية رقمية مبتكرة. و، ويضع الإطار خصوصية البيانات ومراجعة والتدقيقالحسابات وحماية البيانات في المركز ويضع إجراءات تتسم بال شفافيةا تيُنطبق على جميع الأطراف المعوّلة المعنية بشأن لكيفية طلب البيانات وجمعها ونقلها وتخزينها ويتبع معايير مقبولة جيدا على نطاق واسع لبشأن إجراءات تبادل المعلومات/البيانات. أهمية الرمز المميز في تقليل فرص جمع البيانات والاستنساخ والاحتيال ،، من خلال تقديم حامل الهوية ،، مع وظيفة إصدار الهويات افتراضية ،، من أجل حماية الهويات الفعلية نفسها هو جانب إضافي سيتم زيادة تفصيله لتعزيز خصوصية البيانات على المستوى الوطني / القاري.

3. الإطار

يقترح إطار الاتحاد الافريقيالأفريقي للتشغيل المتبادلالمتوافق للهوية الرقمية أن يحدد على المستوى القاري نهجا منهجًا منسقًا للأفراد لتبادل مطالباتبيانات الهوية الرقمية الصادرة عن السلطات الموثوق بها مع مقدمي الخدمات من أجل إثبات هويتهم القانونية في بيئة متصلة بالإنترنت وخارجها. و، ويتمثل في الاتفاق على **معيار موحد لتمثيل الأدلة القائمة علىإثباتات الهوية القانونية الموجودة بالفعل والصادرة عن الدول الأعضاء في الاتحاد الأفريقي في صيغة رقمية.** ويمكن التحقق من صحة الوثائق البيانات الثبوتية هذه من أجل ضمان مستوى عالٍ من الثقة والأمن.

لا توجد قيود على نظم الهوية التأسيسيةالأساسية الوطنية في كيفية عملها أو أنواع الوثائق البيانات الثبوتية التي تستخدمها لتوثيق هوية الأفراد؛ ولكل بلد السيادة في هذا الصدد. و، والغرض من الإطار هو تهيئة الظروف للتشغيل المتبادلالمتوافق على نطاق قاري بناء على النظم القائمة حيثما وجدت، وتوسيع نطاقها بدلًا من تقييد استخدامها لتوسيع نطاقها.

وستتخذ وثائق الهويات الرقمية القابلة للتشغيل المتبادلالمتوافقة الصادرة تمشيًا مع الإطار الاتحاد الأفريقي شكل مطالبة بيانات يمكن التحقق منها تكون مكملة لنظم الهوية التأسيسيةالأساسية الوطنية القائمة ومشاريع التعاون الإقليمي؛، دون استبدال نظم تحديد الهوية الرقمية المحلية للدول الأعضاء في الاتحاد الأفريقي. **و، وتظل الدول الأعضاء في الاتحاد الأفريقي حرة في اختيار الطريقة التي تريد بها إصدار بيانات إثبات الهوية الرقمية هذه.** و، ويمكن تخزينها في شكل رقمي بحت على تطبيق الهاتف الذكي، خادم سحابة القائمةأو الخوادم السحابية، أو بطاقة ذكية أو رابط إلى التمثيل الرقمي باستخدام باركود ذي بعد واحد أو ثنائي يمكن إنشاء بطاقة ذكية أو وصلة إلى التمثيل الرقمي باستخدام الباركود واحد أو اثنين من الأبعاد على وثيقة ورقية (المطبوعة على الورقبطاقة ورقية أو، بطاقة بلاستيكية).

وسيستند الإطار إلى تطوير نظم هوية قابلة للتشغيل المتبادلالمتوافق وشاملة وموثوق بها، حيث وهذه النظمأنها توفر العمود الفقري لمصادر موثوقة لالبيانات الموثوقة المتعلقة لبالهوية القانونية للناسللأفراد، وبالتالي تمكن وثائق الهويةات القانونية الرقمية القابلة للتشغيل المتبادلالمتوافقة من تحقيق مستويات أعلى من الضمان. و، ولذلك تُشجع الدول الأعضاء في الاتحاد الأفريقي على تعزيز نظم بطاقات الهوية الخاصة بها، اعتمادًا على ومبادئ تحديد الهوية لأغراض التنمية المستدامة.، و يمكن النظر في حلول بديلة للحصول على بيانات الهويات القانونية الرقمية القابلة للتشغيل المتبادلالمتوافقة للأشخاص المستبعدين حاليًا من نظام الهوية.

ويمكن استخدام معايير الهوية الرقمية القانونية القابلة للتشغيل المتبادلالمتوافقة على المستوى المحلي أو أن ت دعم حالات الاستخدام عبر الحدود. فعلى سبيل المثال، يمكن اعتماد المعيار من أجل:

- تمثيل بيانات الهوية الرقمية التأسيسيةالأساسية على المستوى الوطني بشأن في وثائق إثباتات الهوية الرقمية الصادرة حديثًا أو المحدثة؛ أو
- تمثيل بيانات المعرف الرقميالهوية الرقمية الأساسية على مستوى الجماعات الاقتصادية القارية أو الإقليمية؛
- إصدارها بشكل منفصل استكمالًا لأنظمةنظم ال معرف رقميةهوية تأسيسيةأساسية موجودة من قبل.

وتيشكل عناصر التشغيل المتبادلالمتوافق والثقة والشمولية التذي تُيعرّف بأنها جزء من هذا الإطار منطلقًا لإطار وبنية تحتية قارية أكثر شمولا لتحديد الهوية الرقمية والتوثيق الرقمي في القارة.

3.1. المبادئ التوجيهية

تسترشد سيتم الاسترشاد بالمبادئ التالية عند بتنفيذ الإطار اللتشغيل المتبادلالمتوافق عبر الحدود:

1. الشفافية في الحوكمة والتشغيل
2. يمكن سهولة الوصول إليها بسهولة، فعالية من حيث التكلفة ماليا المالية والقابلية للتطبيق على نطاق واسع،
3. تعزيز واحترام ودعم حقوق الإنسان وحريتها ودعمها
4. ضمان السلامة التقنية، بما في ذلك الهوية الفريدة والآمنة والقابلية للتوسع والدقيقة
5. ضمان سيادة الدول الأعضاء. ضمان السيادة على البيانات وخاصة انتماء بيانات الهوية الرقمية ينتمي إلى أفريقياأفريقيا وتيظل في تحت السيطرتهاة عليها:
6. أن تكون قابلة للتشغيل المتبادلالمتوافق بين الدول الأعضاء في الاتحاد الأفريقي
7. استخدام معايير مفتوحة ومنع احتكار البائعالموردين أو الاقتصار على تقنيات بعينهاوالتكنولوجيا قفل في
8. حماية الخصوصية وتمكين الناس من التحكم في بياناتهم الشخصية بما في ذلك تناسب البيانات من خلال تصميم النظام
9. حماية خصوصية البيانات والأمنها والحقوقها من خلال إطار قانوني وتنظيمي شامل
10. 1إنشاء ولايات ومسؤوليات مؤسسية واضحة والمساءلة

وبالنظر إلى أن الإطار يعتمد على مصادر موثوقة، مثل نظم تحديد الهوية القانونية، فإن ونوعية هذه النظم وتغطيتها ، فإن لها بالتالي تأثيرا على تنفيذ الإطاره. فالاستبعاد من هذه النظم والتحديات الأخرى مثل ضعف الأمن، على سبيل المثال، سيؤدي إلى نفس الشيء من حيث القدرة على إصدار البيانات الثبوتية واستخدامها على النحو الصحيح.

ولذلك، ينبغي للدول الأعضاء في الاتحاد الأفريقي أن تفي بالتزاماتها لضمان حصول جميع الأشخاص الموجودين في على أراضيها على هوية قانونية، تمشيًا مع اتفاقية حقوق الطفل وغيرها من الصكوك القانونية الدولية والإقليمية. و، وعلاوة على ذلك، تشجع هذه الجهات الدول بقوة أيضاأيضًا على التقيد بالقواعد والمبادئ الدولية القائمة ذات الصلة، وضمان أن تكون المصادر الموثوقة، ولا سيما نظم تحديد الهوية القانونية، شاملة للجميع، وحامية لبيانات الناس وحقوقهم، ومصممة لدعم التكامل الاقتصادي والمجتمعي القاري.

3.2. النموذج

يقترح الإطار التنفيذ على ثلاث مراحل:

1

اعتماد الإطار عمل الاتحاد الأفريقي ودعم وتطوير الإطار عمل التشريعي تالتمكيني؛

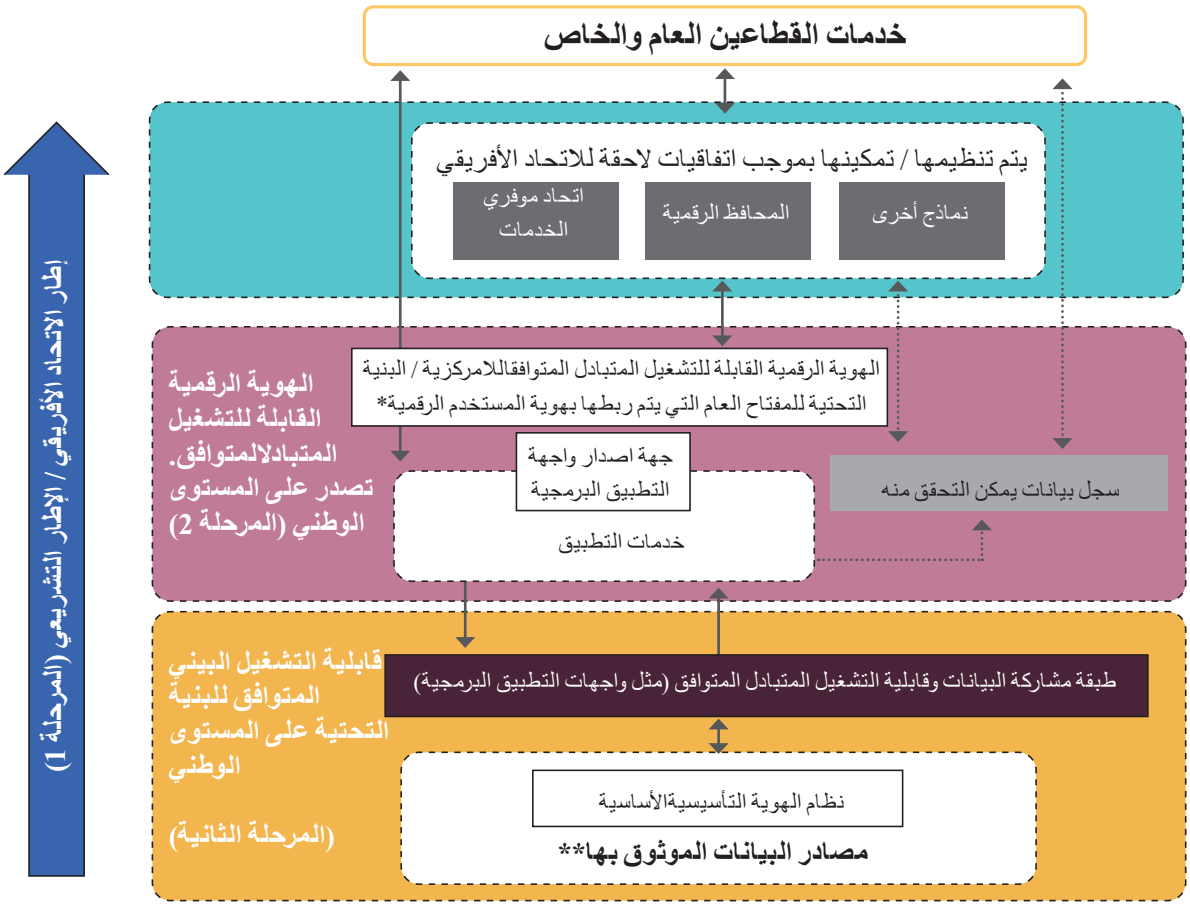
2

تنفيذ الإطار واعتماد المواصفات التقنية لوثائق للبيانات الثبوتية الرقمية المتوافقة اللهويةهوية الرقمية القابلة للتشغيل المتبادل؛

3

توسيع نطاق تنفيذ الالإطار ولتوفير بنية تحتية تمكن من حالات استخدام أكثر تقدمًا مثل التوثيق عن بعد.

الشكل 1 - نهج منهج التنفيذ المرحلي للإطار



* سيتم مواصلة مناقشة تفاصيل تنفيذ المرحلة الثانية مع الدول الأعضاء في الاتحاد الأفريقي بعد ذلك
** ستقرر الدول الأعضاء مصادر البيانات الموثوق بها التي تنطوي ستقصرعلى أنظمةنظم الهويات الأساسية الخاصة بها عليها

يجب أن تضمن بيانات الهوية الرقمية القابلة للتشغيل المتبادل أن السلطة المسؤولة عن اصدارها لا تعلم أي من الخدمات التي يمكن للأفراد الوصول إليها باستخدام هوياتهم الرقمية، ولكن يمكن التحقق من صحة وثائق الهوية. وهذا يوفر ضمانات من حيث حماية البيانات والخصوصية والمزيد من التحكم للفرد في كيفية استخدام بياناته.

يجب أن تضمن بيانات الهوية الرقمية المتوافقة أن السلطة المسؤولة عن إصدارها لا تعلم أي من الخدمات قد حصل عليها الأفراد عند استخدام هوياتهم الرقمية، ولكن يمكن التحقق من صحة البيانات الثبوتية للهوية، وهذا يوفر ضمانات لحماية البيانات والخصوصية وتمنح الفرد المزيد من التحكم في كيفية استخدام بياناته.

طبقة ستمكن البنية التحتية ستمكن من استخدامات أكثر تقدمًا و وسوف تنطوي تعمل عن طريقعلى ربط البيانات الهوية الثبوتية الصادرة بتنسيق بيانات الهوية الرقمية القابلة للتشغيل المتبادلالمتوافقة باللأفراد الفعلييننفي الواقع. و، وهناك عدة خيارات تقنية متاحة للدول الأعضاء في الاتحاد الأفريقي لتنفيذ هذه الطبقةالبنية، التي يمكن أن تتألف من اتحاد لمقدمي خدمات الهوية الذين يقدمون آليات التوثيق لحاملي الوثائق الهوياتالثبوتية الرقمية القابلة للتشغيل المتبادلالمتوافقة للهوية أو تطوير حلول محافظ الهوية الرقمية أو أي نماذج أخرى تمكن من التشغيل المتبادلالمتوافق، و. يمكن لكل تطبيق من هذه التطبيقات تقديم خدمات نهج تقليل البيانات وخدمات والكشف الانتقائي في لحالات الاستخدام المحددة ،، على سبيل المثال مشاركة نقاط البيانات ذات الصلة فقط من بطاقة الهوية وتقرير الائتمان للحصول على قرض ،، أو السعي للحصول على استحقاق مزايا اجتماعية أو صحية ،، أو الحصول على معاش تقاعدي ،، أو التقدم بطلب للحصول على منح دراسية أو إخفاء الحد الأدنى من مجموعة بيانات الهوية الرقمية القابلة للتشغيل المتبادلالمتوافقة (الاسم وتاريخ الميلاد) إلى إثبات بيانات أخرى (18+ عامًا أو 21+ عامًا أو الاجابةالإجابة بنعم / لا).

1.3.1 استراتيجية

يجب أن تفي مصادر البيانات الموثوق بها بالمعايير التي وضعها الإطار الاتحاد الأفريقي لجودة البيانات وسلامتها. و، وفي كثير من الحالات، يمكن تحقيق ذلك من خلال نظام هوية تأسيسي أساسي (تقرر الدول الأعضاء مصادر بياناته الموثوقة) يمكنه أن يقدم دليلًا على الهوية القانونية.

يصور الشكل 1 توسيع نطاق الوصول إلى الأنظمةنظم الوطنية الحالية ومصادر البيانات الموثوق بها من خلال طبقة تبادل البيانات وقابلية التشغيل المتبادلالمتوافق استنادًا إلى المعايير والبروتوكولات التي تمكن إصدار الهوية الرقمية المتوافقة الموثوق بها بها، وسيُلزم القابلة للتشغيل المتبادل. موفرو الخدمات با للتحقق من بيانات الهوية القانونية واستردادها عند إنشاء البيانات اعتمادبيانات الثبوتية لالهوية الرقمية الأساسية.

تصور يمثلطبقة إصدار الهوية الرقمية القابلة للتشغيل المتبادلالمتوافقة الإصدار الموحد للبيانات الثبوتية لالهوية الرقمية القابلة للتشغيل المتبادلالمتوافقة استنادًا إلى مصدر بيانات موثوق به لنظام هوية أساسي/ وطني.، وسيكون لكل جهة مسؤولة عن إصدار هوية (واحدة على الأقل لكل دولة عضو مشاركةمن الدول المشاركة) عدد من الوظائف الرئيسية تشمل (على سبيل المثال لا الحصر) ما يلي:

- واجهة التطبيق بالبرمجية لجهة الإصدار التي تمكن المحافظ والأنظمةنظم الأخرى من لطلب واسترجاع الاوراق البيانات الثبوتية
- سجل بيانات يمكن التحقق منه ويمكن التحقق من إبطال البينات الثبوتيةالالهويات والتحقق من إلغاء الهوية.
- إدارة مفتاح مفاتيح التشفير
- الرؤية الوضوح وإمكانية تدقيق استخدام البيانات الثبوتية والمراجعة لاستخدام بيانات الهوية لحامل البيانات الهوية الثبوتية الرقمية القابلة للتشغيل المتبادلالمتوافقة
- توفير بيانات وصفية إلى لجانب كل بيانات الهوية الصادرة لوصف تصف الجودة، والمنشأ ومستوى الثقة المقترنة ببيانات بالهوية الصادرة

3.2.2 المستوى الوطني ومتطلبات التشغيل المتبادلالمتوافق

لا يشترط إعادة هندسة تصميم نظم الهوية القائمة محليًا بالفعلعلى الصعيد المحلي لتحقيق قابلية التشغيل المتبادلالمتوافق على المستوى القاري. و، وبدلًا من ذلك، ستعتمد سيتم تطبيق معايير قابلية البيانات للتشغيل المتبادلالمتوافق ،، والتشغيل التقني المتبادلالمتوافق التقني عن طريق واجهة التطبيق البرمجية والبروتوكولات، والتمثيل التقني للبيانات الهويةالثبوتية ، و.سيكون إصدار وثائقالبيانات الثبوتية الهوية، وإنشائها، منفصلًا ان منطقيا عن النظم الوطنية القائمة، ولكنهما ستكيكونان تحت سيطرة الوكالات هيئات المسؤولة على الصعيد الوطني.

وقد لا تتطلب الثقة التقنية، التي تستند إلى تشفير متقدم إلى بنية PKI قارية، مرفق وطني للهياكل الأساسية أو بنية تحتية وطنية فائقة أخرى، بل قد تنبع بدلًا من ذلك قد تنشأ من تفضيل الدولة العضو في الاتحاد الأفريقي و/أو القدرة قدرتها على استخدام مرفق بنية PKI الهياكل الأساسية الوطنية (حيثما إذا كانت مستخدمةاستخدم) أو البدائل أخرى المعترف بها قانونًا. و، وستواصل كل دولة عضو في الاتحاد الأفريقي ممارسة سيادتها الوطنية في تصميم نظم الهوية الوطنية، بما في ذلك كيفية عمل تلك النظم على العمل نحو متوافقالمشترك مع إطار الاتحاد الأفريقي.

3.2.3 معايير مشاركة مصادر البيانات الموثوق بها

سيتم وضع تحديد معايير في إطار الاتحاد الأفريقي للجودة والأمان والموثوقية والحد الأدنى من مستوى الضمان المرتبط بكل مصدر بيانات موثوق به في الإطار. و، وينبغي أن تقدم أنظمةنظم الدول الأعضاء أدلة على أنها قد وصلت إلى الحد الأدنى من متطلبات المشاركة قبل أن تتمكن من المشاركة في إطار الاتحاد الأفريقي و إصدار بيانات ثبوتية متوافقة مع متطلبات الهوية الرقمية القابلة للتشغيل المتبادلالمتوافقة. و، وسيتم تحديد طبيعة هذه المعايير بموافقة الدول الأعضاء في الاتحاد الأفريقي.

3.3. عملية موثوق بها - إطار الثقة

ينبغي أن يصف إطار الثقة قواعد واضحة لمشاركة الكيانات الجهات (مثل جهة اصدار إصدار الهوية وحامليها ومتحققيهاوكيفية التحقق منها)، ولتشغيل الإطار، والمتطلبات التقنية للتشغيل المتبادلالمتوافق للبيانات الثبوتية الموثوق بها.

وسيمكن ذلك جميع الكيانات الجهات من الثقة في الوثائق التي يقدمها أصحاب الهوية استنادًا إلى الثقة التي أنشأتها السلطة المصدرة (لوثائق الهوية) والعمليات التي وافق كل كيانجهة على الالتزام بها في إطار الثقة.

ومن المتوقع أن تقوم الدول الأعضاء بصياغة الأقسام الرئيسية التالية كجزء من إطار الثقة.

3.3.1 معايير

تعريف واضح لكل كيان جهة (مثل الجهة المصدرة لوثائق الهوية)، والمسؤوليات الملقاة على عاتقها للحفاظ على الثقة مثل الإدارة الآمنة والآمنة للبيانات والخدمات، والإبلاغ عن الحوادث.

ومن بين الأدوار الرئيسية المتوقع إدراجها في إطار الثقة ما يلي:

- **السلطات الموثوق بها** هي مصادر موثوقة للبيانات لإثبات الهوية القانونية كما أقرتها الدول الأعضاء في الاتحاد الأفريقي.

- **جهات الاصدارالإصدار** هم هي الجهاتالكيانات المسؤولة عن إصدار إثبات الهوية القانونية في الشكل الرقمي الموحد بموجب الإطار إلى الحائزحامل الهوية. و، ويمكن للسلطات الموثوق بها إما أن تصدر الوثائق الثبوتية بنفسها أو أن تفوض كيانا جهة آخر أخرى تيتمتع بمهارات أكثر ملاءمة (مثل وكالة تكنولوجيا المعلومات والاتصالات، والقطاع الخاص).
- **صاحب حامل الهوية** الرقمية القابلة للتشغيل المتبادلالمتوافقة هو الشخص الذي يمتلك وثيقة ثبوتيةبطاقة اعتماد رقمية واحدة أو أكثر.، يمكن أن يكون حامل الهوية - ولكن ليس دائما - موضوع سمات بينات الهوية المشتركة التي تتم مشاركتها من خلالعبر الهوية الرقمية القابلة للتشغيل المتبادلالمتوافقة.
- **المتحقق جهة التحقق** هيو طرف معتمد (مثل مقدم الخدمة العامة أو الخاصة) يريد التحقق من ادعاء بينات هوية موضوع شخص معين.
- **يمكن لمقدمي خدمات الهوية ومقدمي** بيانات الوثائق الثبوتيةالهوية ومزودي ومقدمي خدمة المحافظة الرقمية المساهمة بشكل أكبر في النظام البيئي من خلال توفير مصادق نظام مصادقة لربط هوية حاملها بالبيانات الثبوتية وبالتالي تمكين حالات الاستخدام الأكثر تقدمًا والتي تتطلب مصادقة عن بعد.

قد يكون من الضروري إنشاء هيئة إشرافية مستقلة من قبل الدول الأعضاء لضمان أن تظل الكيانات الجهات المشاركة ممتثلة للقواعد المنصوص عليها في إطار الثقة وتعيين ولتحديد الحد الأدنى من الأدوات والتقنيات المطلوبة للامتثال. يجب أيضًاأيضًا تكليف الهيئة الإشرافية بمهمة زيادة الوعي بمهارات المرونة الإلكترونية عبر القارة لضمان استدامة الإطار. العمل

3.3.2 قواعد المشاركة

قد تتضمن قواعد المشاركة الحد الأدنى من المتطلبات القانونية أو التشغيلية أو التنظيمية المطلوبة لكيان لجهة موثوق بها تيقدم خدمة ما تحتف ي إطار الثقة. على سبيل المثال، قد يطلب من المصدر الحصول على اتفاقية تصريح رسمية للعمل (من مصدر موثوق / وكالة جهة حكومية).

قد يطلب من الخدمات التي تقبل الهوية الرقمية القابلة للتشغيل المتبادلالمتوافقة تأكيد امتثالها مع أساسيات متطلبات حماية البيانات الأساسية والخصوصية وسبل الانتصاف التعويض (لحاملي الهوية).
وقد يطلب يتطلب الأمر أيضاأيضًا من مذكرة التفاهم لضمان موافقة جميع الكيانات الجهات العاملة على شروط إطار الثقة.

3.3.3 الحوكمة

سيلزم أن تضع تحدد آليات الإدارة الحوكمة التي ستصدق عليها الدول الأعضاء في الاتحاد الأفريقي قواعد إطار الثقة وتحافظ عليها، وأن توافق على إدخال أي تغييرات على متطلبات التشغيل المتبادلالمتوافق، وأن تفوض المسؤولية عن صياغة/تطوير أي تغييرات في الإطار إلى المجموعات الفرعية المعنية بالإدارة بالحوكمة حسب الاقتضاء.

وقد يكون من الضروري إنشاء هيئة إشراف مستقلة من قبل الدول الأعضاء في الاتحاد الأفريقي لضمان أن تظل الكيانات الجهات المشاركة ممتثلة للقواعد التي يحددها إطار الثقة. وينبغي أن تكون هذه الهيئة مسؤولة أيضاأيضًا عن ضمان الامتثال الرسمي للمعايير من قبل جميع الأطراف للمعايير رسميا،، وفي حالة انحرافها عن ذلك، يتم تدقيقها أو محاسبتها حسبما يعتبر تقتضي الضرورةيا على سبيل المثال في حالة خرق البيانات.

وينبغي أن تكون حماية الأفراد ذات أهمية قصوى. و، وينبغي تمكين أن تتمكن الهيئة الإشرافية من تلقي الشكاوى التي قدمها أصحاب الهوية الرقمية القابلة للتشغيل المتبادلالمتوافقة والمتضررين من سوء الممارسة أو خرق البيانات أو تزوير الهوية أو غيرها من الحوادث المتعلقة بالهوية الرقمية والتصرف واتخاذ إجراءات بناء على ذلكيها. و، وينبغي أن تيكون كون هذه الهيئة أيضاأيضًا مركز

نقطة تنسيق لآليات الانتصاف التعويض حتى وإن كان هذا مجرد دور تنسيقي وينبغي أن تكون نصيرًا للأفراد وحقوقهم.

3.3.4 متطلبات التشغيل المتبادلالمتوافق

3.3.4.1 مستويات الضمان

وسيلة لتعزيز مستوى من الثقة في البيانات التي يقدمها حامل الهوية إلى المتحققجهة التحقق. و، وينبغي أن يحدد الإطار الشروط التي يمكن بموجبها تحقيق كل مستوى على أساس التحقق من الهوية من قبل مصدر موثوق به، وعملية الإصدار، ووسائل الاحتفاظ بوثيقة الهوية وتقديمها.

3.3.4.2 الحد الأدنى من مجموعة البيانات

الحد الأدنى من البيانات المتعلقة بحامل الهوية كما هو منصوص عليه في وثائق الهوية، ينبغي أن تكون كافية لتحديد هوية الفرد في معظم المعاملات المشتركة مع احترام الحاجة إلى تقليل البيانات إلى أدنى حد ممكن.، ويمكن توفير السمات الموجودة في الحد الأدنى من مجموعة البيانات من قبل كيان جهات موثوقة به مختلفة.

ويجوز للجهة المسؤولة أن تحدد كيف يمكن إدراج مطالباتبيانات إضافية (مجموعات بيانات) اختياريًا ضمن إطار الثقة. و، وينبغي أن يخضع أي إصدار لبيانات للوثائق الهوية الثبوتية لنفس الشروط والقواعد التي تخضع لها جهات اصدار إصدار الهويات الأساسية ، لا سيما المتطلبات الفنية.

3.3.5 المتطلبات التقنية

3.3.5.1 الأمن

ينبغي تحديد متطلبات الأمان الأساسية لكل كيانجهة تيقدم خدمة كجزء من البنية التحتية للهوية.

3.3.5.2 دليل التشفير

سيتم التحقق من الوثائق الثبوتية من خلال تضمين توقيع رقمي تم إنشاؤه من قبل سلطة الاصدار. التحقق من صحة التوقيع بمثابة دليل تشفيري على أن المطالبة البيانات التي قدمها حامل البيانات الوثائق الثبوتية يمكن الوثوق بها. وللتحقق من التوقيع الرقمي سيكون المفتاح العام مطلوبًا. و، ويمكن توفير المفتاح العمومي من خلال نهج لا مركزي أو مركزي يحدد كجزء من إطار الثقة ومتطلباته التقنية.

3.3.5.3 صيغة الأوراق الوثاق الثبوتية

ينبغي تحديد المواصفات التقنية لإنشاء بيانات الوثائق ثبوتية ونقلها بالاعتماد على المعايير القائمة مثل وثائق ثبوتية قابلة للتحقق منها (W3C) حيثما ينطبق ذلك.

- الهويات الرقمية القابلة للتشغيل المتبادلالمتوافقة هي مجموعة من مطالباتبيانات الهوية القانونية (مثل السمات) والعلاقاتة التي تصدرها تقوم بها جهة الاصدارالإصدار والتي يمكن التحقق منها تشفيريًا. و، وبشكل أكثر تحديدًا، تتيتضمن:
  - بيانات وصفية ثبوتية حول نوع بيانات الهوية الصادرة وتاريخ الإصدار واسم جهة الاصدار؛
  - معلومات عن موضوع المطالبة البيانات والمطالبة والبيانات الفعلية لبالهوية القانونية (مثل تاريخ الميلاد).
  - إثبات صحتها الصحة والذي عادة ما يكون توقيعًا رقميًا.

يمكن لصاحب الهوية الرقمية القابلة للتشغيل المتبادلالمتوافقة أن **يقدم بعض المعلومات التي يمكن التحقق منها** لهوية رقمية واحدة أو أكثر قابلة للتشغيل المتبادلالمتوافق بالطريقة التي يمكن بها التحقق من صحة المطالبة البيانات (مثل الكشف الانتقائي).

3.4 خيارات التحقق المحتملة

يمكن اعتماد عدة نهج هيكلية بنيوية تتيح التثبت من حامل الهوية الرقمية القابلة للتشغيل المتبادلالمتوافقة ،، عند مستوى معين من الضمان. يمكن أن تتعايش جميع الخيارات التالية وتنفذ على مستويات مختلفة من التعاون (مثلًا فيما بين جهات قطاعية محددة أو على مستوى الجماعات الاقتصادية الإقليمية).

ويمكن استكشاف خيارات إضافية، حسب توافر تكنولوجيات أخرى ذات ممارسات تنفيذ مثبتة.

3.4.1 الخيار الأول – المحافظ الرقمية الشخصية

يتكون هذا الخيار من تزويد الأفراد والشركات بمحفظة رقمية شخصية تحتوي على إثبات يمكن التحقق منه لسمات الهوية القانونية التي يمكن استخدامها لإثبات الهوية القانونية أو مشاركة حقائق محددة مع مزود الخدمة. يشير الخيار الهيكلي البنيوي هذا إلى حالات استخدام وثائق ثبوتية قابلة للتحقق منها (W3C).

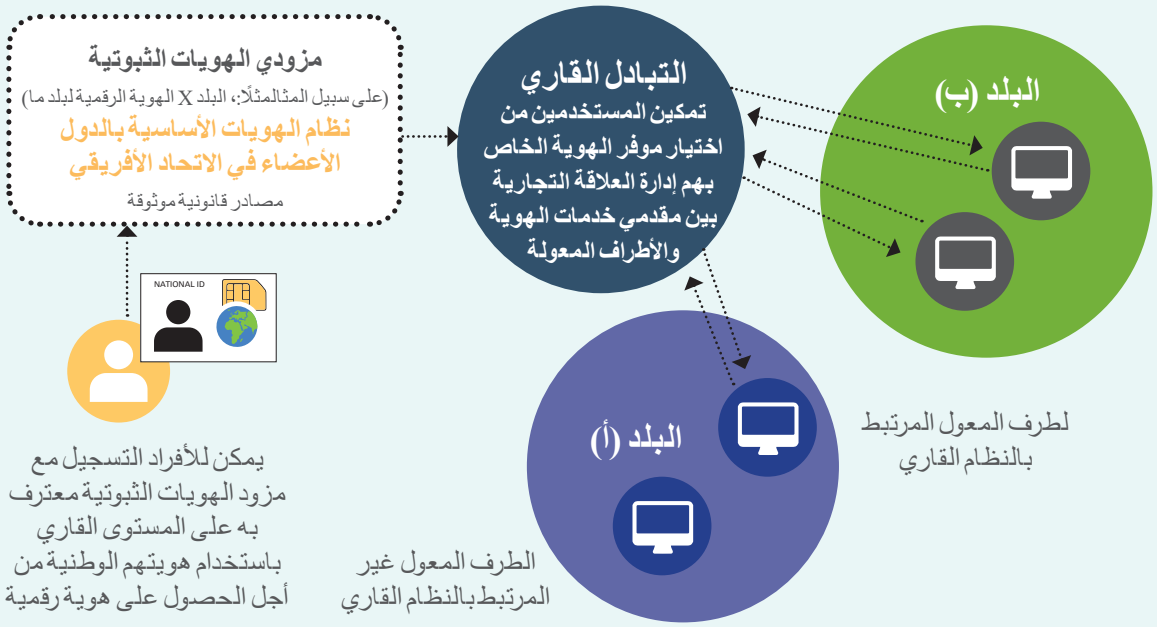
الشكل 2 – نظرة عامة على الخيار 1 - المحافظ الرقمية الشخصية

1. اختيار الفرد لأحد مزودي محفظة الهوية من أجل تخزين هويته الرقمية القابلة للتشغيل المتبادلالمتوافقة ،، وهنا تعد عملية الإعداد التنظيم أمرًا ضروريًا.
2. يتلقى الفرد بيانات ثبوتية هوية رقمية قابلة للتشغيل المتبادلالمتوافق يمكن التحقق منها (مثل الهوية وإثبات العنوان) من مصدر موثوق به ويخزنها في محفظة رقمية
3. في نفس وقت الإصدار، تسجل السلطة المعنية طبعة رقمية للمطالبة للبيانات في بنية تحتية لا مركزية للمفتاح العام مع مراعاة خصوصية المواطنين.
4. يمكن للأفراد تقديم مطالبة البيانات إلى مقدم الخدمة (مثل التأمين) مثل إثبات العنوان باستخدام محفظته أو محفظتها (بواسطة رمز الاستجابة السريعة أو QR Code ،، أو البلوتوث ،، أو التواصل قريب المدى أو NFC).
5. يمكن لمقدم الخدمة أن يتحقق في البنية التحتية اللامركزية للمفتاح العام من صحة المطالبة البيانات وأن سلطة معترف بها قد أصدرتها.

3.4.2 الخيار الثاني – الاتحاد القاري للهويات الرقمية

بموجب هذا النموذج، سيتمكن كل مقيم أفريقي من الصعود إلى الطائرةمن المشاركة عن طريق باستخدام مقدم وثائق ثبوتية أساسية على المستوى القاري من اختياره.

الشكل 3 – نظرة عامة على الخيار الثاني – الاتحاد القاري للهويات الرقمية



*ستقرر الدول الأعضاء مصادر البيانات الموثوقة التي تستلزم نظم تحديد الهوية الأساسية الخاصة بها

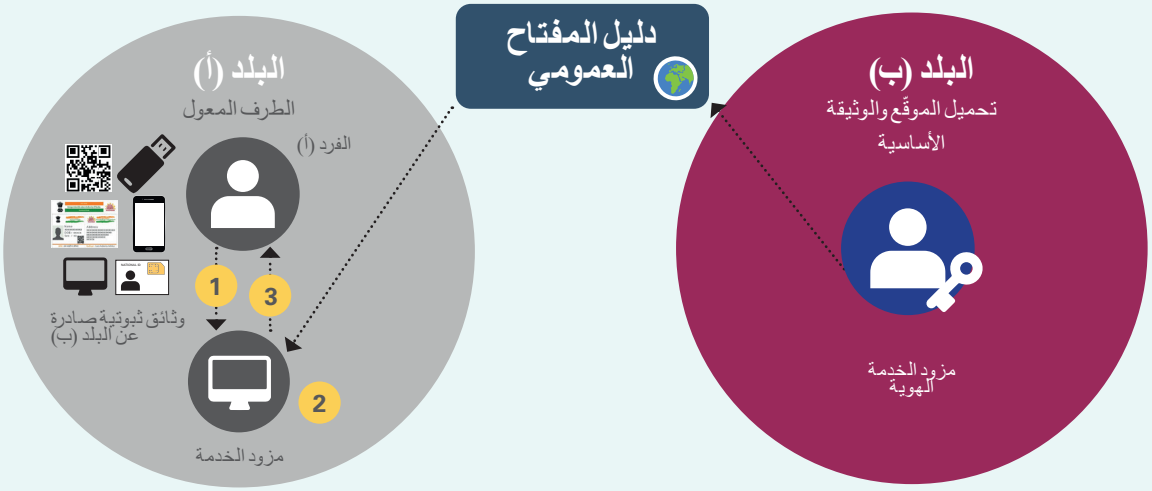
1. يتم تأسيس اتحاد قاري لمقدمي وثائق الهوية الأساسية: يمكن أن يوفر مشغلو شركاتي الاتصالات والبنوك والحكومات، الخ ... يمكن أن توفر خدمات التحقق.
2. يتم إنشاء نقطة اتصال قارية واحدة لجميع مقدمي الوثائق الثبوتية المشاركين والأطراف المعولة التي ترغب في المصادقة على الأفراد.
3. للمشاركة؛ يمكن للأفراد استخدام هويتهم الرقمية القابلة للتشغيل المتبادلالمتوافقة على متن الطائرة، و الصادرة من مقدم وثائق ثبوتية من اختيارهم، يمكن لموفري الوثائق الثبوتية التحقق من صحة الهوية الرقمية القابلة للتشغيل المتبادلالمتوافقة.
4. عند التحقق بنجاح، يقوم موفرو الوثائق الثبوتية بإصدار وسيلة تحقق للفرد.
5. يمكن للفرد استخدام وسيلة التحقق الخاصة به للوصول إلى الخدمات عبر الإنترنت والخدمات الشخصية الموصلة المرتبطة بنقطة الاتصال القارية.

3.4.3 الخيار الثالث – وثائق ثبوتية موقعة رقميًا

يتيح هذا النموذج المصادقة من خلال التحقق من بيانات الهوية القانونية الموقعة رقميًا باستخدام مفتاح عمومي، بالإضافة إلى وسيلة إضافية لمشاركة صورة حاملها.

الشكل 4 - نظرة عامة على الخيار 3 - وثائق ثبوتية موقعة رقمياً

عملية التحقق



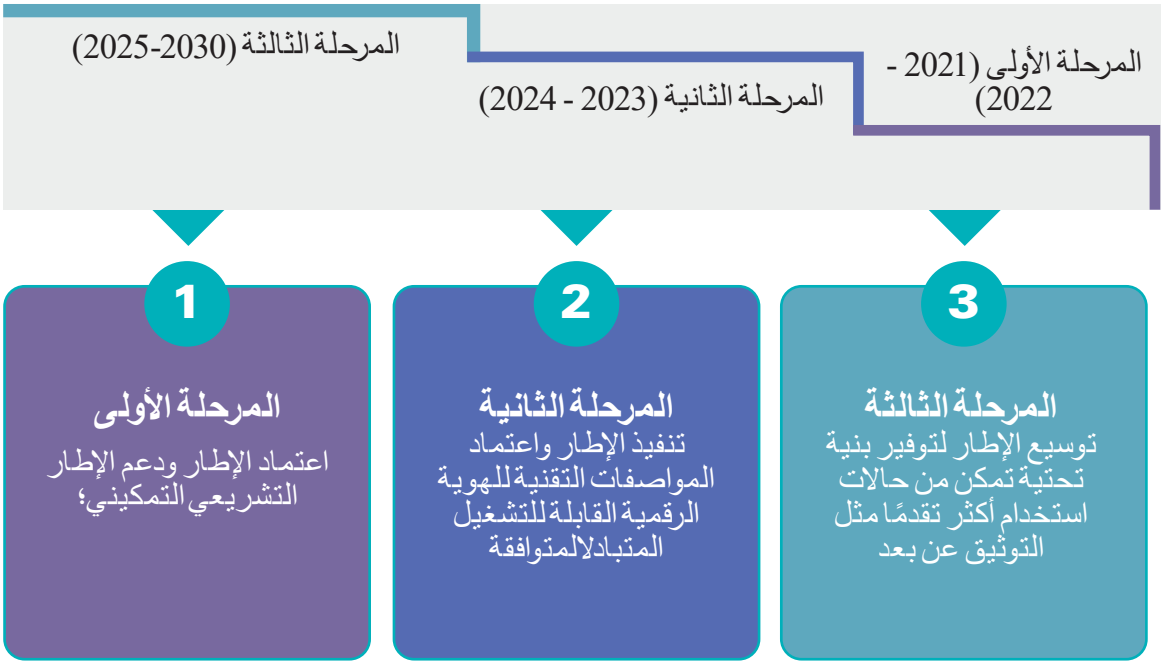
تتفق *ستقرر الدول الأعضاء مصادر البيانات الموثوقة التي تستلزم أنظمة تحديد الهوية التأسيسية الخاصة بها

1. البلدان تتفق على معيار (مثل رمز الاستجابة السريعة أو QR Code) وتوقع المصادر الرسمية توقع على الوثائق الثبوتية باستخدام نظام التشفير (عن طريق مفتاح خاص)
2. تتقاسم المصادر الرسمية مفتاحها العمومي العام في دليل للمفاتيح العامة ستصدق الدول الأعضاء في الاتحاد الأفريقي على إدارتهحوكمته، ويتدار على المستوى القاري.
3. تنشئ البلدان خدمة مستقلة تمكن من مشاركة نسخة من صورة حامل الهوية الرقمية القابلة للتشغيل المتبادلالمتوافقة ويمكن الوصول إليها عن طريق واجهة تطبيق برمجية آمنة من أجل توثيق هوية حاملها. و، وللعمل دون الاتصال بشبكة بالإنترنت، ويمكن أيضاأيضًا لمجموعة من البلدان (مثل الجماعات الاقتصادية الإقليمية) أن تتفق على إصدار وثائق ثبوتية مادية تحتوي على صورة لصاحب لحامل الهويةالتسجيل.
4. تصدر المصادر الرسمية في الدول أشكالًا موحدة من الهوية الرقمية القابلة للتشغيل المتبادلالمتوافقة للأفراد
5. يتم إنشاء برنامج تحقق (تطبيق أو موقع ويب) لتمكين مقدمي الخدمات من التحقق من صحة وسلامة التوقيع على الهوية الرقمية القابلة للتشغيل المتبادلالمتوافقة.
6. يمكن للأفراد استخدام هويتهم الرقمية القابلة للتشغيل المتبادلالمتوافقة للتحقق رقميًا من هويتهم القانونية من قبل الأطراف المعولة العامة أو الخاصة في بلدهم أو في الخارج ولالحصول على الخدمات.
7. يتوقع من كل دولة عضو أن تحافظ على التخزين الآمن مثل وحدات أمان الأجهزة (HSMs) واللمفاتيح الخاصة والشهادات المرجعية وخوارزميات التجزئة في وحدات تخزين آمنة مثل وحدات أمان الأجهزة لاستخدامها في التشفير و والتحقق من النزاهة

4. خارطة طريق رفيعة المستوى للتنفيذ

لتسريع الطريق نحو تحقيق الأهداف الطموحة لهذا الإطار، ينبغي للدول الأعضاء في الاتحاد الأفريقي أن تزيد من تعاونها من أجل صقل تفاصيل الإطار التقني والمرجعي والمعايير المشتركة والعمليات المشتركة.

ويقسم المقترح هو إلى تقسيم تنفيذ الإطار إلى ثلاث مراحل، كما هو مبين في الرسم المخطط التاليالبياني أدناه:



وفي كل مرحلة، سيتم التخطيط لفرص التشاور مع الدول الأعضاء في الاتحاد الأفريقي والمجتمع المدني وأصحاب المصلحة في النظام البيئي اللهوية من أجل ضمان أن يظل الإطار وتنفيذه متوافقين مع احتياجات الأفراد والسياقات المحلية. و، وستنشر الوثائق الرئيسية وتوفر نافذة زمنية مناسبة للمساهمات.

4.1. المرحلة الأولى: اعتماد الإطار والبيئة التمكينية

تقديم مشروع الإطار إلى الدورة العادية الرابعة للجنة التقنية المتخصصة المعنية بالاتصالات وتكنولوجيا المعلومات والاتصالات لاعتماده وتأييد أجهزة السياسات. 1

بعد إقرار هذه الوثيقة، سيتم زيادة تحديد تفاصيل إطار الثقة وسيتم تنفيذ الأنشطة التالية على وجه

الخصوص:

- خلق الوعي
- دراسة جدوى حول المشهد الحالي لنظام الهوية الرقمية في إفريقياأفريقيا
- إنشاء إطار عمل استشاري للجهات الفاعلة في النظام البيئي الرقمي بهدف حماية مصالح كل جهة فاعلة
- إنشاء صكوك أدوات قانونية وتنظيمية
- تحديد قواعد المشاركة
- إنشاء آليات ومنتديات الحوكمة لتبادل أفضل الممارسات في جميع مراحل عملية التنفيذ؛
- تحديد النصوص الأحكام القانونية التي يجب دمجها في البيئات القانونية المحلية للدول الأعضاء في الاتحاد الأفريقي من أجل تنفيذ الإطار ،، بما في ذلك الضمانات المناسبة بشأن الأمن السيبراني وحماية البيانات ،
- التصديق على اتفاقية مالابو بشأن الأمن السيبراني وحماية البيانات الشخصية
- اعتماد إطار قاري لسياسة البيانات
- والتي قد تشمل التصديق على اتفاقية مالابو بشأن الأمن السيبراني وحماية البيانات الشخصية اعتماد إطار سياسة البيانات القارية
- تعيين الدول الأعضاء في الاتحاد الأفريقي لأفرقة لفرق خبراء لتحديد الالمتطلبات التشغيلية والتقنية ومتطلبات التشغيل المتوافقة.
- إنشاء هياكل مؤسسية مستقل على المستوى الوطني (سلطات حماية البيانات - مراقبة سلطات التصديقالاعتماد، – فرق الاستجابة لحوادث الحاسوبومعلومات العملاء. نظام تتبع التسجيل(وتعزيز التعاون بين المؤسسات الوطنية.
- تطوير مبادرات بناء القدرات
- دعم نشر البنية التحتية الرقمية بما في ذلك مراكز البيانات على المستوى الوطني والإقليمي و/ القاري والتي اللازمة لتتطلب دعم واستدامة تشغيل أنظمةنظم الهوية الرقمية.
- حشد الموارد

من أجل ضمان نجاح الإطار، ستحدد سلسلة من حالات الاستخدام التي تمثل أكبر قدر من الفرص المتاحة للقارة. و، ويمكن لمجموعة من الدول الأعضاء في الاتحاد الأفريقي أن تتعاون أكثر بشكل أكبر لاختبار حالات الاستخدام المحددة وتجريبهاومعالجتها، إلى جانب أصحاب المصلحة الإضافيين حسب الحاجة.

وينبغي إجراء تقييم للتكاليف والفوائد الرئيسية للإطار المقترح وخيارات التوثيق اللاحقة من أجل توفير المزيد من الوضوح بشأن احتياجات التمويل لإبلاغ للالدول الأعضاء في الاتحاد الأفريقي لتكون القرارات على بينةبصنع القرار. و، وفي الوقت الراهن، من المتوقع أن يؤدي الامتثال لمعيار منسق لتمثيل معلومات الهوية إلى تكاليف محدودة للدول الأعضاء في الاتحاد الأفريقي، حيث يمكن إدماجه كشرط تقني في لمشاريع الرقمنة القائمة في نظم الهوية التأسيسيةالأساسية الخاصة بها. و، ومع ذلك،

من المتوقع أن يؤدي إنشاء البنية التحتية للمصادقة إلى تكاليف إضافية، و يتطلب تعريف نماذج الأعمال اعتمادًا على أنواع أصحاب المصلحة المعنيين، يتطلب تعريف نماذج الأعمال. و، وفيما يتعلق بهذه المرحلة، سيتعين إجراء تقييم مفصل للأثر من أجل ضمان أن تظل خيارات التوثيق المقترحة شاملة.

وبالتوازي مع في موازاة ذلك، تلتزم الدول الأعضاء في الاتحاد الأفريقي بما يلي:

- تطوير وتنفيذ الأطر القانونية والتنظيمية التمكينية المنسقة التي تبني الثقة في أنظمةنظم الهوية الرقمية التأسيسيةالأساسية الرقمية.
- تطوير تشريعات ولوائح منسقة للبيانات الشخصية تعمل على تمكين الأفراد ،، مع الحفاظ على سيادة البيانات ؛
- إطلاق نشر البنية التحتية الرقمية بما في ذلك البنية التحتية للبيانات (مراكز البيانات الوطنية) التي تعتبر الأساس لنشر نظام الهوية الرقمية
- التصديق على اتفاقية الاتحاد الأفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية (إذا لم يتم ذلك حتى الآن) والإسراع في دخولها حيز التنفيذ والعمل على تسريع إنشاء سلطات رقابية ل حماية البيانات للرقابة في البلدان المشاركة ؛
- تطوير الاستراتيجية الوطنية للأمن السيبراني و إنشاء فرق الاستجابة لحوادث الكمبيوتر الحاسوب (CIRTs) للتخفيف من المخاطر والتهديدات المتعلقة بالهجمات الإلكترونية وسرقة البيانات وسوء التعامل مع المعلومات الحساسة
- اعتماد إطار الاتحاد الأفريقي القاري لسياسة البيانات القارية. الذي يدعو إلى إنشاء أنظمةنظم المعرف الرقميهوية رقمية وتنفيذها بشكل متماسك بما يتماشى مع إطار عمل حوكمة البيانات الشامل الذي يضمن أن يتم الجمع بين البيانات الإدارية العامة التي تنطوي عليها أنظمةنظم التعريف الهوية الرقمية و إعادة تعيينها باستخدام الضمانات المناسبة. و، وينبغي أن تمكن هذه الجهات الأفراد وأن تحمي الخصوصية على الإنترنت كحق أساسي (بما في ذلك اختيار المستخدم والتحكم فيه،، والموافقة المستنيرة/المجديةالهادفة، وسيادة البيانات/ملكيتها، وما إلى ذلك)؛
- إطلاق و/أو توسيع نطاق الجهود الرامية إلى تعزيز نظم الهوية التأسيسيةالأساسية، لضمان أن تكون شاملة وموثوقة، بما يتماشى مع المعايير والمبادرات ذات الصلة مثل البرنامج الأفريقي للتحسين السريع للتسجيل المدني ونظم الإحصاءات الحيوية (البرنامج الأفريقي المعني بالتعجيل بتحسين التسجيل المدني والإحصاءات الحيوية) ومبادئ تحديد الهوية لأغراض التنمية المستدامة.

وستستكمل هذه المراحل المرحلة باعتماد الدول الأعضاء في الاتحاد الأفريقي للالصيغة المكتملة للإطار.

4.2. المرحلة الثانية: تنفيذ الإطار واعتماد المواصفات التقنية للهوية الرقمية القابلة للتشغيل المتبادلالمتوافقة

وتتمثل المرحلة الثانية في إنشاء إطار الثقة وآليات الحوكمة والتعاون وتقديم المواصفات التقنية لإدخال معرف مركز البيانات الدوليالهوية الرقمية المتوافقة الذي سيشمل:

- تطوير الحد الأدنى من معايير وقواعد دنيا لقابلية التشغيل البينيالمتوافق
- ملامح عزو ملفات التعريف لمجموعة الحد الأدنى منالسمة لمجموعة البيانات الدنيا (تنسيقات البيانات) والبيانات الوصفية المرتبطة بها
- شكل العرض (مثل الباركود الثنائي الابعاد، ووثائق ثبوتية يمكن التحقق منها)
- مستوى الضمان (كنقطة مرجعية للتشغيل المتبادلالمتوافق)
- عناصر التشفير الخاصة بتوقيع البيانات والتكويد
- بروتوكولات التحقق لحالات الاستخدام عبر الإنترنت وخارجها

وبعد ذلك ويمكن لمجموعة من الدول الأعضاء في الاتحاد الأفريقي وضع نموذج للتنفيذ (التطبيق أو الموقع الشبكي) للتحقق الأساسي الأولي من الهوية الرقمية القابلة للتشغيل المتبادلالمتوافقة لاختبار قابلية البيانات الثبوتية للتشغيل البينيالمتوافق، ودعم إثباتات الهوية القانونية التي يمكن التحقق منها ويعتمد ال. تنفيذ تنفيذ على الخصوصية والأمن حسب المتأصلالتصميم.

ويمكن وستحتاج الأطراف المشاركة إلىالنظر في الاتفاق على تعريف الحلول البديلة للحصول على هوية رقمية قابلة للتشغيل المتبادلالمتوافق للأشخاص المستبعدين حاليًا من أي نظام معرف هوية أساسيتأسيسي.

إضافة إلى ذلك، سيتم تحديد مبادرات الاتحاد الأفريقي الجارية الأخرى التي يمكن أن تبني تستفيد منعلى الإطار (مثل إطار المؤهلات القارية الأفريقية)

وستختتم المرحلة الثانية بتعريف خطة عمل واضحة لتعريف البنية التحتية للمصادقة كجزء من المرحلة 3الثالثة.

4.3. المرحلة الثالثة: تطوير البنية التحتية لتمكين التحقق عن بُعد

ستبدأ المرحلة الثالثة بتنفيذ إطار الثقة المحدد كجزء من المرحلة الثانية:

يمكن إكمال الطبقة التي تمثل إصدار الهوية الرقمية القابلة للتشغيل المتداخلالمتوافقة في مرحلة ثانية مع بنية تحتية تمكن حالات استخدام أكثر تقدمًا مثل المصادقة عن بعد. وستمكن طبقة المصادقة هذه الأفراد من إثبات هويتهم رقميًا من خلال ممارسة التحكم في عامل مصادقة واحد أو أكثر (مثل الرمز البيومتري أو رمز PIN) المرتبط يرتبط بهويتهم القانونية التي تم التحقق منها مسبقا ،، أي الهوية الرقمية القابلة للتشغيل المتبادلالمتوافقة. و.

وهناك عدة خيارات تقنية متاحة للدول الأعضاء في الاتحاد الأفريقي لتنفيذ هذه الطبقة، مثل

اتحاد لمقدمي خدمات الهوية الذين يوفرون آليات التوثيق لحاملي الهوية الرقمية القابلة للتشغيل المتبادلالمتوافقة، أو تطوير حلول محفظة الهوية الرقمية أو أي نماذج أخرى تمكن من التشغيل المتبادلالمتوافق. و، ويمكن لكل تطبيق من هذه التطبيقات تقديم نهج خدمات تقليل البيانات ووخدمات الكشف الانتقائي في لحالات الاستخدام المحددة ،، على سبيل المثال مشاركة نقاط البيانات ذات الصلة فقط من بطاقة الهوية وتقرير الائتمان للحصول على قرض ،، أو السعي للحصول على استحقاق مزايا اجتماعية أو صحية ،، أو الحصول على معاش تقاعدي ،، أو التقدم بطلب للحصول على منح دراسية أو إخفاء الحد الأدنى من مجموعة بيانات الهوية الرقمية القابلة للتشغيل المتبادلالمتوافقة (الاسم وتاريخ الميلاد) إلى إثبات بيانات أخرى (18+ عامًا ا أو 21+ عامًا أو الإجابة بنعم / لا).

كما ستتمكن الدول الأعضاء في الاتحاد الأفريقي من السعي إلى مزيد من الاتفاق بشأن كيفية إنشاء هذه البنية التحتية لطبقة التوثيق، والشراكة مع الجماعات الاقتصادية الإقليمية وغيرها من المبادرات القارية التي تحقق بالفعل في إدخال حلول قابلة للتشغيل المتبادلالمتوافق للهوية الرقمية للوصول إلى الخدمات عن بعد. و، وفي الواقع، ستتمكن الدول الأعضاء والمنظمات من الاستفادة من التمثيل الموحد لمعلومات الهوية على أساس معياري في شكل رقمي موثوق وآمن وبناء خدمات إضافية فوقه.

وستواصل الدول الأعضاء في الاتحاد الأفريقي التعاون لتعزيز إطار الثقة وآليات الإدارة الحوكمة والتعاون عقب الاتفاق على الهياكل الأساسية الإضافية التالية:

- التنسيق مع المبادرات الأخرى الرامية إلى إقامة إمكانية التشغيل المتبادلالمتوافق على المستوى القاري (مثل تحالف افريقياأفريقيا الذكية والمجموعات الاقتصادية الإقليمية)
- الاتفاق على أفضل خيار هيكلي بنيوي (مثل الاتحاد القاري، المحافظ الرقمية وما إلى ذلك) لتطوير مهمة التوثيق عن بعد التي من شأنها أن تبني على البيانات الثبوتية الرقمية القابلة للتشغيل المتبادل (تعتمد على الهوية الرقمية القابلة للتشغيل المتبادلالمتوافقة).

وستختتم المرحلة الثالثة بخطة عمل واضحة بشأن تنفيذ طبقة التوثيق وفقا للخيار الهيكلي البنيوي الذي سيتم الاتفاق عليه بين الدول الأعضاء في الاتحاد الأفريقي والمنظمات التابعة له.

5. افتراضات وتحديات ومخاطر عالية المستوى

5.1 الافتراضات

ستعتمد الدول الأعضاء الإطار وتتعاون وتلتزم بتنفيذ الإصلاحات القانونية والتنظيمية اللازمة.

5.2 التحديات العامة ومقترحات عالية المستوى للحد منها

يلخص الجدول أدناه التحديات العامة وآليات مقترحة للحد منها:

#	التحديات	آليات التخفيف المقترحة
١	الاقصاء وضعف الأمن وتآكل حماية البيانات الشخصية	إسقاط تطبيق المبادئ المحددة في الإطار (٣.١٣.1) وتعزيز الأطر القانونية وحماية أمن البيانات الأمنية والبنية التحتية في الدول الأعضاء في الاتحاد الأفريقي.
٢	إحجام الدول الأعضاء في الاتحاد الأفريقي عن اعتماد الإطار وتنفيذه	رفع مستوى الوعي حول فائدة إطار التشغيل المتبادلالمتوافق على المستويين المحلي والقاري ودوره في تعزيز نظام الهويات الأساسية
٣	نقص القدرات التقنية والمالية لدى الدول الأعضاء في الاتحاد الأفريقي	تعزيز القدرات وتعزيز تبادل المعارف بين الأقران بين الدول الأعضاء في الاتحاد الأفريقي، فضلافضلًا عن النظر في فعالية الحلول التكنولوجية من حيث التكلفة التي سيتم الاتفاق عليها في المرحلتين ٢ و٣الثانية والثالثة
٤	عدم كفاية مراكز البيانات على الصعيد الوطني/الإقليمي/القارية	بناء مراكز بيانات وطنية/إقليمية/وطنية قارية وتعزيز استخدامها في من قبل أفريقياأفريقيا.

5.3. المخاطر والآليات المقترحة للحد منها

يلخص الجدول أدناه المخاطر والآليات المقترحة للحد منها

#	التحديات	آليات التخفيف المقترحة
١	عدم وجود تعريف مناسب للمعايير المشتركة وعدم فهم الدول الأعضاء في الاتحاد الأفريقي وعدم اتباع واعتماد معايير مشتركة	تعريف المعايير والاتصالات ذاتها للدول الأعضاء في الاتحاد الأفريقي أثناء التنفيذ والرصد المنتظم من قبل هيئة أفريقية موثوقة وممكنة تحظى بدعم وتأييد جميع الدول الأعضاء من نفس القبيل لضمان الالتزام بالمعايير. مناقشات وورش عمل مركزة مع أصحاب المصلحة لضمان تعريف واضح لمعايير استراتيجية التنفيذ المختارة. قياس استراتيجية التنفيذ المعيارية القائمة على المعايير للدولة العضو في في الاتحاد الأفريقي مقابل برامج معرف الهوية الوطنية معيارية الأساسية في الدول الأخربمماثلة قائمة على أساس معياري عبر الدول الأعضاء في الاتحاد الأفريقي.
٢	يؤدي تدني مستويات الثقة بين السلطات الوطنية التي تتمتع بقدرات إنفاذ غير متجانسة إلى بطء استيعاب الإطار على نطاق قاري كبير. بالإضافة إلى ذلك ،، فإن عدم رغبة الدول الأعضاء في قبول هيئة إشرافية فوق وطنية ، يؤدي إلى إبطاء تنفيذ إطار الثقة.	يجب أن يستهدف الإطار المواءمة والاعتراف المتبادلالمتوافق كهدف طويل الأجل ولكن يظل مفتوحًا لتطوير حلول مرنة ورشيقة ،، والتي يمكن أن تخلق آليات تدقيق مشتركة بين الدول الراغبة في بناء الثقة فيما بينها مع الحفاظ على السيادة - من خلال الاعتراف من جانب واحد بشهادات الثقة.
٣	فالحل والفوائد والخيارات لا تكيف بشكل جيد مع البيئة أو المعلومات المحلية، ولا يستخدم الأشخاص الحل الذي يؤدي إلى ضعف الاستيعاب وارتفاع التكاليف في نهاية المطاف دون فائدة تذكر.	تطوير هياكل تصميم قوية تركز على المستخدمين لتحديد الحلول التي يسهل استخدامها ويمكن للجميع الوصول إليها؛ تطوير آليات نشر قوية عبر الدول الأعضاء في الاتحاد الأفريقي تضم جميع الجهات الفاعلة المحلية ذات التفكير الفكر المماثل.
٤	تتخذ ستقرر الدول الأعضاء قرارًا بشأن التكنولوجيا المناسبة أثناء مرحلة التنفيذ ،، ولكن إذا اختارت تكنولوجيا البنية التحتية للمفاتيح العموميةالعامة فإن ،قد يثبت غياب مؤسسة التصديق على المستوى القاري وعدم وجود إدارة غير كافية لمتطلبات التشفير للتوقيع الرقمي يمكن أن يكون عائقا في إنشاء نظام التشغيل المتبادلالمتوافق.	إنشاء إطار قانوني يمكن من إنشاء مؤسسة تنسيق على المستوى القاري يدعمها هيكل حوكمة عادل مسؤول عن سيادة كل دولة عضو لتنفيذ وإدارة التوقيعات الرقمية وإصدارها وإلغاءها واستبدالها وتحديثها في الوقت المناسب. إنشاء هيكل تنظيم مفصل وديناميكي لتمكين إدارة التوقيع الرقمي / البنية التحتية للمفتاح العام عبر مرحلة التنفيذ والعمليات.
٥	بسبب البيانات غير صحيحة وغير مكتملة، قد تتأثر استراتيجية تصميم وتنفيذ بعض مكونات التشغيل المتبادلالمتوافق مثل التوقيعات الرقمية. كما أن التأخير في تبادل البيانات والمعلومات ذات الصلة للمواطن أو المقيم يمكن أن يؤثر على توقيت المشروع.	عقد اجتماعات مع الوكالات الحكومية لجمع البيانات المتعلقة بالتنفيذ في الثغرات المعلوماتية عن طريق الاستفادة من خبرة الخبراء من خلال التعلم من نظير إلى نظيرالنظراء لتشجيع التعاون والملكية الإقليمية والقارية. رصد الجداول الزمنية للمشروعات والمعالم الرئيسية لمنع التأخير. و، ومن الضروري أيضاأيضًا أن يكون هناك جدول زمني مفصل وشامل للتنفيذ تم الاتفاق عليه من قبل الدول الأعضاء في الاتحاد الأفريقي وأصحاب المصلحة الرئيسيينالرئيسيين،

٦	غياب إرشادات واضحة المعالم لإدارة التغيير لضمان أن يظل الإطار متوافقًا مع الممارسات والاحتياجات والتطوير التكنولوجي الحالي.:	وضع عملية قوية ومحددة جيدًا لإدارة التغيير كجزء من إطار الحوكمة
٧	تتخذ الدول الأعضاء قرارًا بشأن التكنولوجيا المناسبة أثناء مرحلة التنفيذ ،، ولكن إذا اختارت تكنولوجيا البنية التحتية للمفاتيح العموميةالعامة ،، قد لا تتوصل وكالات التصديق في أفريقياأفريقيا إلى توافق في الآراء بشأن إدارة الهياكل الأساسية للمفتاح العام على مستوى بدء التنفيذ على نطاق القارة. ثانيا، قد لا تكون هناك توافقات في الآراء بشأن إنشاء تبادل للتوقيعات الرقمية.	إما أن تقوم أما الدول الأعضاء في الاتحاد الأفريقي فإما أن تقوم بإنشاء مؤسسة تصديق جديدة لإدارة البنية التحتية للمفتاح العام على مستوى القارة أو أن تقر آلية لوضع الوكالات القائمة على منصة مشتركة.
٨	عدم وجود الحد الأدنى من البيئة التمكينية القانونية اللازمة على المستويين الوطني والإقليمي.	على الدول الأعضاء في الاتحاد الأفريقي الإسراع في تنفيذ الأطر القانونية والتنظيمية المنسقة المطلوبة.

6. الملحق

6.1. تعريفات المصطلحات

السمة هي نوعية خاصية أو صفة أو سمة مسماة متأصلة في شخص أو شيء من هذا القبيل أو نسبت إليه في أنظمةنظم الهوية، تشمل سمات الهوية الشائعة الاسم والعمر والجنس ومكان الميلاد والعنوان وبصمات الأصابع والصورة والتوقيع ورقم الهوية وما إلى ذلك.

التوثيق والمصادقة هو عملية إثبات الثقة بأن الشخص هو ما يدعيه أنه. تتضمن المصادقة الرقمية بشكل عام شخصًا يقدم إلكترونيًا "عاملًا" أو أكثر "لتأكيد" هويته - أي لإثبات أنه نفس الشخص الذي تم إصدار الهوية أو الاعتماد له في الأصل. يمكن أن تتضمن هذه العوامل شيئا يعرفه الشخص (على سبيل المثال، كلمة مرور أو رقم تعريف شخصي) أو لديه (على سبيل المثال، بطاقة هوية أو رمز مميز أو بطاقة SIM متنقلة)، أو أنه (على سبيل المثال، بصمات أصابعه).

التفويض هو عملية تحديد الإجراءات التي يمكن تنفيذها أو الخدمات التي يمكن الوصول إليها على أساس الهوية المؤكدة والمصادق عليها.

المصدر جهات الإصدار الرسمية هيو مصدر موثوق للمعلومات الهوية وهو مستودع أو نظام يحتوي على سمات عن الفرد ويعتبر المصدر الرئيسي أو الأكثر موثوقية لهذه المعلومات. في حالة عدم تطابق نظامين أو أكثر أو وجود بيانات متعارضة، تعتبر البيانات الموجودة ضمن مصدر البيانات الموثوق به هي الأكثر دقة .

المطالبة البيانات هي مؤهل أو إنجاز أو جودة أو جزء من المعلومات حول خلفية الموضوع مثل الاسم أو هيئة الجهات الحكومية أو عنوان المنزل أو الشهادة الجامعية.

الموافقة على بالنسبة اللأشخاص المسجلة بياناتهم تعني أي إشارة حرة ومحددة ومطلعة لا لبس فيها لرغبات الشخص المعني بالبيانات التي يدل بها، ببيان أو بعمل إيجابي واضح، على الاتفاق على معالجة البيانات الشخصية المتعلقة به.

وثائق ثبوتية هي مستند أو كائن أو بنية بيانات تضمن هوية الشخص بمن خلال طريقة ما من الثقة والمصادقة. تتضمن الأنواع الشائعة من الوثائقبيانات اعتماد الثبوتية لالهوية - على سبيل المثال لا الحصر - بطاقات الهوية أو الشهادات أو الأرقام أو كلمات المرور أو بطاقات SIM. وفي في حالة هذا الإطار، البيانات الوثائق الثبوتية هي مطالبة بيانات يمكن التحقق منها تسمى الهوية الرقمية القابلة للتشغيل المتبادلالمتوافقة..

وحدة التحكم بالبيانات تعني أي شخص طبيعي أو اعتباري، عام أو خاص، أي منظمة أو جمعية أخرى والتي وحدها أو بالاشتراك مع الآخرين، تقرر جمع ومعالجة البيانات الشخصية وتحدد الأغراض.

حماية البيانات تنظم كيفية استخدام البيانات أو معالجتها ومن قبل من، وتضمن للمواطنين حقوقاهم بالنسبة لب على بياناتهم. و، وهو مهم بشكل خاص في ضمان الكرامة الرقمية، حيث يمكنه معالجة اختلال توازن القوى المتأصل بين "مواضيع الشخص موضوع البيانات" والمؤسسات أو الأشخاص الذين جمعوا البيانات بشكل مباشر.

هيئة حماية البيانات هي سلطات عامة مستقلة تراقب وتشرف، من خلال سلطات التحقيق والتصحيح، على تطبيق قانون حماية البيانات. و، وهي تقدم مشورة الخبراء بشأن قضايا حماية البيانات وتتعامل مع الشكاوى التي قد تكون انتهكت القانون.

الأشخاص الشخص المسجلة موضوع البيانات هم تعني أي شخص طبيعي يخضع لمعالجة البياناته الشخصية.

الكرامة الرقمية تعني (في سياق الهوية الرقمية) أن الهوية البشرية وراء الهوية الرقمية لها خصوصية وبياناتها محمية..

نظام الهوية الرقمية (ID) هو نظام تعريف هوية يستخدم التكنولوجيا الرقمية طوال دورة حياة الهوية، بما في ذلك التقاط جمع البيانات والتحقق من صحتها وتخزينها ونقلها؛ وإدارة البيانات الثبوتية؛ والتحقق من الهوية والمصادقة.

الهوية الرقمية هي مجموعة من السمات التي تم التقاطها جمعها وتخزينها إلكترونيًا و /و أو الاوراقالوثائق الثبوتية التي تحدد بشكل فريد الشخص.

التوقيع الرقمي هو عملية مفتاح غير متماثلة حيث يتم استخدام المفتاح الخاص لتوقيع البيانات رقميًا ويتم استخدام المفتاح العام للتحقق من التوقيع. توفر التوقيعات الرقمية حماية الأصالة وحماية السلامة وعدم التنصل، ولكن ليس حماية السرية.

القناة الرقمية في سياق التقنيات الرقمية هي مجموعة من التقنيات البرمجية أو البنى التحتية الرقمية التي تعمل معًا لدعم حالة استخدام

نظام الهوية الأساسية هو نظام تحديد الهوية الذي أنشئ في المقام الأول لإدارة معلومات الهوية لعامة السكان وتقديم الوثائق الثبوتية التي تستخدم كدليل على الهوية من أجل الوصول إلى الخدمات العامة والخاصة مثل التعليم والرعاية الصحية والحماية الاجتماعية والخدمات المالية، وما إلى ذلك. و، ولأغراض هذا الإطار، ستقرر الدول الأعضاء في الاتحاد الأفريقي مصادر البيانات الموثوقة التي تنطوي تعتمد عليهاعلى نظمها للوثوق الأساسية.

أنظمةنظام الهوية العملية الوظيفية هوي نظام تعريف هوية تم إنشاؤه لإدارة تحديد الهوية والتوثيق والتفويض لخدمة أو معاملة معينة مثل التصويت وإدارة الضرائب والبرامج الاجتماعية والتحويلات والخدمات المالية وغيرها. يمكن قبول أوراق اعتماد الهوية الوظيفية - مثل بطاقات هوية الناخبين وسجلات الصحة والتأمين وأرقام الهوية الضريبية وبطاقات التموين ورخص القيادة وما إلى ذلك - بشكل شائع كدليل على الهوية لأغراض أوسع خارج عن نيتها هدفها الأصلية ،، خاصة عندما لا يكون هناك نظام هوية تأسيسيأساسي.

التنسيق يضمن التوحيد في النظم من خلال استخدام الحد الأدنى من المعايير الدنيا لتيسير التشغيل المتبادلالمتوافق والأطر القانونية والثقة (مثلًا، مستويات الضمان) لوضع القواعد وبناء الثقة في النظم المعنية.

هوية هي هو اختصار لأوراق الهوية أو وثيقة الهوية في بعض المناطق.

نظام التعريف هو قواعد البيانات والعمليات والتكنولوجيا والبنية التحتية والاوراق والوثائق الثبوتية والأطر القانونية المرتبطة بالتقاط بجمع وإدارة واستخدام بيانات الهوية الشخصية لغرض عام أو محدد.

تحديد الهوية هي عملية تحديد هوية الشخص أو تحديده أو التعرف عليه.

الهوية هي الإحداثيات الاجتماعية النسبية التي تميز الفرد عن الآخر. يمكن أن تتغير الهوية اعتمادًا على الجهات الفاعلة أو الإعداد المكان الذي يجد فيه الأفراد أنفسهم وبالتالي فهي ليست ثابتة ولا مطلقة.

مزود الهوية هو كيانجهة موثوق به - على سبيل المثال، وكالة حكومية أو شركة خاصة - يصدر ويدير الهويات القانونية والاوراق والوثائق الثبوتية وعمليات المصادقة طوال دورة حياة الهوية.

التشغيل المتبادلالمتوافق هي قدرة وحدات الوظائف المختلفة – على سبيل المثال. مثل أنظمةنظم أو قواعد بيانات أو الأجهزة أو التطبيقات على العمل معًا - لتوصيل أو تنفيذ برامج أو نقل البيانات بطريقة تتطلب من المستخدم أن يكون لديه معرفة قليلة أو معدومة بتلك الوحدات الوظيفية.

مستوى الضمان هو القدرة على تحديد، مع مستوى معين من اليقين أو التأكيد، أن المطالبة بيانات بهوية معينة لمن قبل شخص أو كيانجهة ما يمكن الوثوق بها لتكون في الواقع هوية المطالب "الحقيقية". المستوى العام للتأكد هو وظيفة درجة من درجة الثقة بأن هوية مقدم الطلب المطالب بها هي هويته الحقيقية (مستوى ضمان الهوية) ،، وقوة عملية المصادقة (مستوى ضمان المصادقة) ،، و و- عند إذا كان استخدام هوية اتحادية - بروتوكول التأكيد المستخدم من قبل الاتحاد لتوصيل معلومات المصادقة والسمة (مستوى ضمان الاتحاد) .).

المعايير المفتوحة هي معايير متاحة لعامة الناس ويتم تطويرها (أو الموافقة عليها) والحفاظ وصيانتها معليها من خلال عملية تعاونية ومدفوعة بتوافق الآراء. و، وتيسر "المعايير المفتوحة" إمكانية التشغيل المتبادلالمتوافق وتبادل البيانات فيما بين مختلف المنتجات أو الخدمات، وهي معدة لاعتمادها على نطاق واسع.

البيانات الشخصية تعني أي معلومات تتعلق بشخص طبيعي محدد أو يمكن التعرف عليه يمكن من خلالها التعرف على هذا الشخص، بشكل مباشر أو غير مباشر، بشكل خاص بالإشارة إلى رقم تعريف أو أكثر من العوامل المحددة له/ لها البدنية، الفسيولوجية، العقلية، الاقتصادية، الثقافية أو الاجتماعية.

الخصوصية والأمن عن طريق التصميمالمتأصل يعني تضمين آليات الخصوصية والأمن بشكل استباقي في تصميم وتشغيل المنتجات والخدمات سواء غير تكنولوجيا المعلومات وأنظمةنظم تكنولوجيا المعلومات والبنية التحتية الشبكية والممارسات التجارية. و، وهذا يتطلب مراعاة حوكمة الخصوصية والأمان طوال العملية الهندسية ودورة حياة المنتج بأكمله.

تقييم تأثير حماية البيانات هي عملية تهدف إلى تحديد المخاطر الناشئة عن معالجة البيانات الشخصية وتقليل هذه المخاطر إلى أقصى حد ممكن وفي أقرب وقت ممكن. و، وتعد هذه القوانين أدوات هامة للحد من المخاطر، وإثبات الامتثال لقوانين ولوائح حماية البيانات.

معالجة البيانات الشخصية تعني أي عملية أو مجموعة من العمليات التي يتم تنفيذها بناء على البيانات الشخصية، سواء بوسائل تلقائية مثل جمع أو تسجيل أو تنظيم أو تخزين أو تكييف أو تغيير أو استرجاع أو نسخ أو نسخ أو استشارة أو استخدام أو الكشف عن طريق الإرسال أو النشر أو توفير المحاذاة أو الجمع والقفل والتشفير والمحو أو تدمير البيانات الشخصية.

إثبات الهوية القانونية هو هي شهادة ميلاد أو بطاقة هوية أو وثائق هوية رقمية، معترف بها كدليل على الهوية القانونية بموجب القانون الوطني ووفقا للقواعد والمبادئ الدولية. الناشئة

الطرف المعول هو كيانجهة تيعتمد على البيانات الثبوتية وآليات المصادقة التي يوفرها نظام الهوية، عادة لمعالجة معاملة أو منح الوصول إلى المعلومات أو إلى نظام.

إطار الثقة يشير إلى متطلبات الأعمال التجارية والتقنية والتشغيلية والقانونية لنظام الهوية لتعزيز التشغيل المتبادلالمتوافق بين مختلف الأطراف المشاركة.

العرض التمثيل القابل للتحقق هو عرض تمثيل للبيانات ضد التلاعب (البيانات المستمدة من بيانات ثبوتية واحدة أو أكثر يمكن التحقق منها) مشفرة بطريقة يمكن من خلالها الوثوق بتأليف بالبيانات بعد عملية التحقق من التشفير. على سبيل المثال، نُهج الكشف الانتقائي التي تقوم بتوليف بانتقاء البيانات ولا تنقل بيانات ثبوتية أصلية التي يمكن التحقق منها.

التحقق يُعرف بأنه عملية التحقق من سمات هوية محددة أو تحديد صحة الوثائق الثبوتية من أجل تيسير الإذن بخدمة معينة.

الإتحاد
الأفريقي

Bureau of the Chairperson
African Union Headquaters
P.O. Box 3243, Roosevelt Street
W21K19, Addis Ababa, Ethiopia
Tel: +251 (0) 11 551 77 00
Fax: +251 (0) 11 551 78 44
www.au.int