The Identity Toolbox
CONCEPT NOTE

June 3rd, 8:30-18:30 (InF3, InF7, InF11, InF15)

The Identity Toolbox provides best practices and latest developments—policy, technical, business practices–around key capabilities that must be in place and deployed by any identity system irrespective of the application or sector. In totality it is expected to cover advances in enrollment and onboarding, authentication, biometrics, mobile, cloud platforms, machine learning, artificial intelligence, PKI, plus document and data security. Experiences from border management, elections, health, education, civil registration, passports and visas, among others may be presented as examples to illustrate the power of the core capabilities advancements.

This track was developed in response to a huge demand from African identity stakeholders seeking actionable knowledge. A **MUST ATTEND** track with highest quality expertise!

The sessions for this Track are as follows:

Session 1 (InF3): Inclusive Trusted Enrollment and Onboarding
Enrollment continues to be one of the most important (and often costliest activities) in the development of an identity program. It is fraught with several challenges that include access to the population in non-urban and challenging locations, data transmission issues, integrity of collected data and validation, etc. The task is made even more challenging by the need that enrollment be inclusive, so that no one is left behind, and is often done under very tight time frames--as is often seen in voter registration or social inclusion programs.

The session will share field experiences and best practice strategies for affecting inclusive and trustworthy enrollment of large-scale populations.

Moderator for this session TBC.

Session II (InF7): Authentication Platforms
An authentication platform is a corner stone in the use of identity systems for service delivery and for empowering the daily actions of end-users. Authentication of user identity as a capability, is difficult to achieve because it has to meet several challenges and constraints. For example (i) It has to be frictionless, so that it is always available and easy to use and does not slow down transactions, (ii) It has to work robustly so that it can deliver the level of trust and security needed, without disenfranchising users through high false rejection rates, (iii) It has to be privacy respecting by design, so that it assures the public that the authentication platform will not lead to surveillance of behavior, neither by government agencies nor by the private sector (iv) It needs to work seamlessly across all platforms—mobile, offline, online, via kiosks, point of sale, etc— so it can provide a uniform user experience that improves engagement. Of course, it has to do all of this while remaining low cost and widely available through appropriate APIs and standard based interfaces that encourage the development

of a myriad of applications within an ecosystem to ensure commercial viability and sustainability. The session will address this core capability from several viewpoints, technological, business, and policy, and will illustrate the advances, through successful country case deployments, that make it possible to deploy authentication platforms that overcome all of the stated challenges.

Moderator for this session TBC.

Session III (InF11): Secure Identity Credentials

Secure identity credentials, as opposed to an identity number in a centralized population register— continue to rise in importance, even as the world continues to undergo digital transformation and dematerialization of interactions. There are several reasons for this. The principal one among them comes from privacy concerns. A secure identity credential that is in the hands of the end user—in physical form—or that is under the control of the end user—in virtual form— can be used to affect transactions without the need to connect to a centralized database, which can prevent behavioral surveillance and tracking. In addition, populations that do not fully trust the digital medium continue to demand physical credentials, which are a source of pride and provide evidence of belonging. With the emphasis on distributed and offline authentication, the security of the credential becomes paramount. A credential needs to be robust against tampering, counterfeiting and all other forms of fraud, since it is the token that unlocks a world of access. Of course, this has to be achieved while remaining cost effective, given that the cost of credentials is proportional to the size of the population.

The session will holistically explore the subject of secure credentials, examining the available options including physical and virtual credentials, and the expectations for its production, and the experiences that have already accumulated with this most familiar form of identity proofing. It will address the mechanisms for securing it, producing it, delivering it, using it and managing it throughout its lifecycle. The discussion will necessarily cover smart cards, mobile credentials, PKI, security printing, holograms, among other mechanisms for token security.

Moderator for this session TBC.

Session IV (InF15): Digital Public Goods Initiatives

The Global Digital Public Goods Alliance defines a public good as a good that is both non-excludable (no one can be prevented from consuming this good) and non-rivalrous (the consumption of this good by anyone does not reduce the quantity available to others). These are goods with benefits that extend to all countries, people, and generations and are available across national borders everywhere without any licensing fees. They hold a particular promise in the context of development and for developing countries, especially in Africa.

This session will explore some of the most prominent initiatives in this domain as they pertain to identity. These include MOSIP (Modular Open Source Identity Platform) and OpenCRVS initiatives that promise to provide a game changer for the domain of civil registration and identity management.

Moderator for this session TBC.