Minority Report:

IDESG Functional Model Representation of the Identity Ecosystem Final Deliverable August 2014

Excerpted from

A Living Context for the Human Identity Ecosystem

Ann Racuya-Robbins

The U.S. National Institute of Standards and Technology (NIST) hosts the National Program Office (NPO) of the National Strategy for Trusted Identities in Cyberspace (NSTIC). The NSTIC calls for a vibrant Identity Ecosystem where identity solutions adhere to four Guiding Principles. To achieve this Ecosystem, NSTIC has formed the Identity Ecosystem Steering Group (IDESG), and one of its committees is the Security Committee.

In the context of the current state of the Functional Model Representation of the Identity Ecosystem (IEFM) produced by the Security Committee of the IDESG, a question is posed, "W*hat is a Functional Model*?"

Simply stated it is a tool for engineering and understanding systems directed towards engineers particularly Information and Communications Technology (ICT) engineers. As such it intentionally attempts to simplify elements of the model to describe more narrowly the scope of its discourse. It describes by omission what it is not. This methodology comes from mathematical thought. These simplifications can be called functions. A Functional Model exemplified in IEFM is a representation of how a system of functions is organized.

This kind of system advantages the solving of computational problems through mathematical steps. It advantages computational problem solving, and automata, sometimes referred to as patterns or data patterns. Overall this kind of system advantages complexity through iteration in ICT engineering. In our current era of Big Data this iteration can help reveal human behavior which may be used for good and ill.

*

In commercial development and standards settings organizations like NIST this kind of Functional Model can be used as a tool to bring together varying and competing companies, technologies and stakeholders—groups of people and organizations with a common desired end. It can also be a part of the way a democracy governs commercial activities and

itself including citizen services and defense. A goal of using this Functional Model tool is to find a way through standards to allow entities and stakeholders to compete for a share of a new or emerging commercial market while stimulating innovation and economic development. In this case the emerging market is based in part on the buying and selling of human attributes (characteristics). It is widely known in ICT environments that "human attributes are the new money" as Anil John of FICAM said. From that standpoint it can seem like a good idea to create more and more attributes to be bought and sold even if the individual human whose attributes are being bought and sold for profit receive little or none of the revenue and may likely not even know that their personal attributes are earning profits for someone else.

The NSTIC Guiding Principles are intended to protect individual human interests through the unique role of Privacy Evaluation and Privacy Protections including civil liberties and human rights in systems. There is however, no discussion to date in the Functional Model of this important, pivotal and foundational issue —no discussion of to whom does this money belong? Individual human users are referred to as actors and roles. The status of individual human user in terms of rights is vague and may even be deferred to organizations that can limit individual human standing through organizational policy.

Yet the IEFM in its current form can be seen as a system that manipulates human rights and human identity attributes (characteristics) for governmental and commercial purposes many of which the human individual is unaware. Today there is no way for individual human beings to determine if the system being represented here is or will ever be just or just enough to inspire voluntary participation by human individuals.

This current state of affairs is most clearly symbolized by the fact that the representation, icon, image, or graphic of the individual human user has been banned from the IEFM. More importantly it can be said that this Functional Model does not have enough of the right kind information for human individuals to determine if this system is or will ever be just. A large part of the reason for this is that the IEFM even the NSTIC Guided Identity Ecosystem generates vast amounts of iterative complexity that is well suited to computation problem solving rather than adaptive complexity such as in human conversation best suited to human imagination, creativity, innovation and labor.

This vast amount of iterative complexity is very costly and requires large interlocking bureaucracies to manage.

*

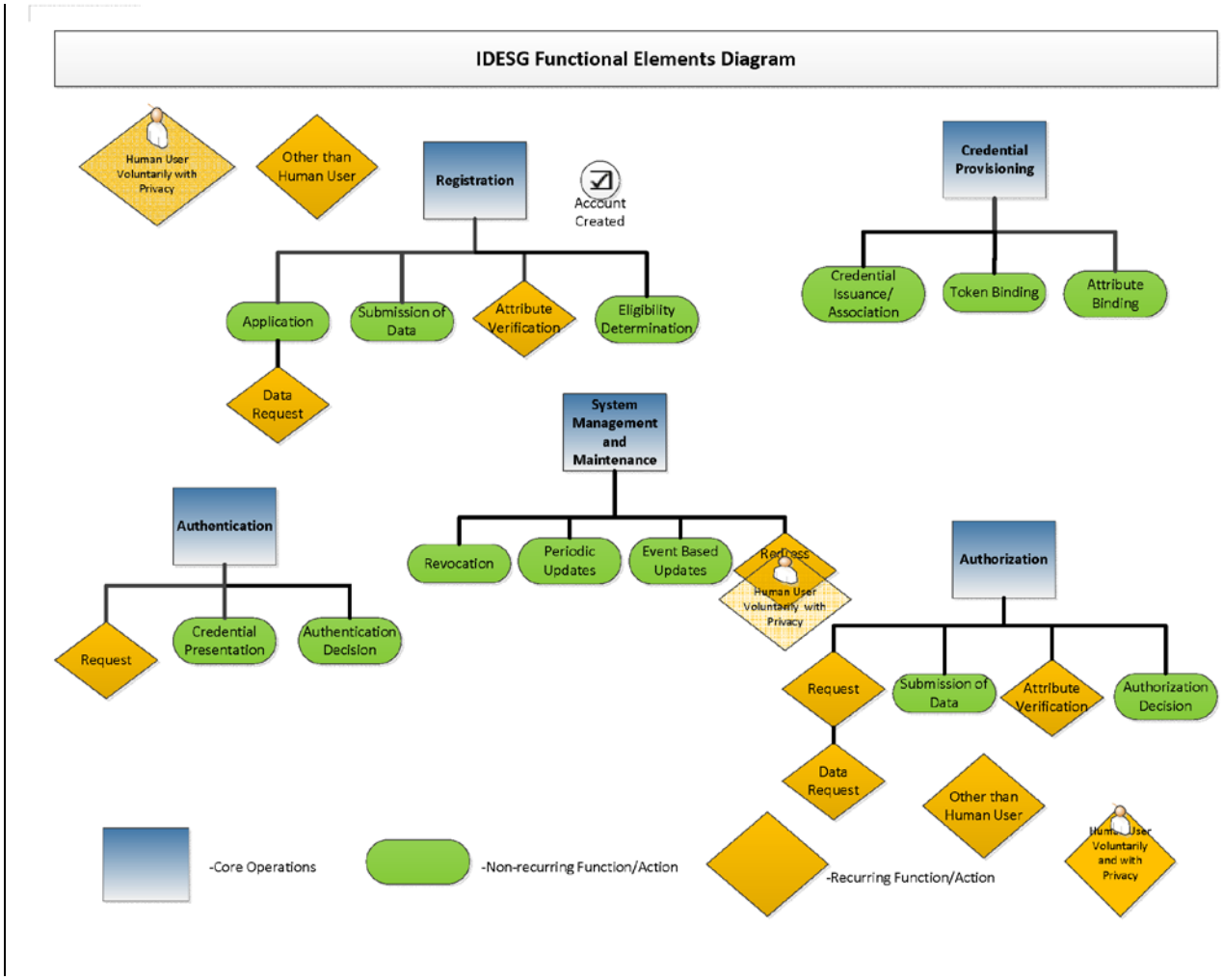
An Alternative Approach

The following approach will be unfolding in the IDESG Security Committee Interactions Model.

In a nutshell this approach ties the NSTIC Guided Identity Ecosystem Framework Project to human rights including the US Bill of Rights and the Consumer Bill of Rights (2012) among others and articulates individual human responsibilities to that system of rights. Through conversation it asks and answers what different parties want.

*

Below are a couple of artefacts I created which include the agency of individual human user.



Core Operations	Functions	Description	MITRE Report Definitions	Intel Presentation
Registration		Set of processes voluntarily entered into that establishes the identity of a Human User to the extent necessary prior to creating the digital identity and issuing a credential.	Identity Enrollment-Set of processes that establishes the identity of a human user entity prior to creating the digital identity in the human resources system or other identity store with the subsequent issuance of a credential that can be presented by the entity to prove their identity.	Identity Lifecycle Management; Registration
	Application	Process by which a potential human user requests initiation of registration.	None	N/A
	Data Request	Process by which a Human User is notified of the attributes required for determining eligibility to create the digital identity.	None	N/A
	Submission of Data	Process for collecting human user identity data once an application has been received and data has been requested.	Background Investigation- Process for collecting identity data and accepting individuals as contractors or associates. Background investigation process once an applicant has been selected to support a particular contract that results in the creation of a digital identity within the agency's human resource(s) (HR) application.	N/A
	Attribute Verification	Process of confirming or denying that the human user claimed identity attributes are correct and meet the pre-determined requirements for accuracy, assurance, etc. to the required levels of assurance	Identity Verification & Validation- The process of confirming or denying that a claimed identity is correct and meets the pre-determined requirements by comparing the credential(s) (something you know, something you have, something you are) with previously proven information.	N/A
	Eligibility Determination	A decision that a human user does or does not meet the pre-determined requirements of eligibility for an entitlement.	Fitness Determination- A decision by an agency that an individual has or does not have the required level of character and conduct necessary to perform work for or on behalf of a Federal agency as an employee in the excepted service (other than in an excepted service position where the incumbent can be noncompetitively converted to competitive service) or as a contractor employee.	N/A
Provisioning		The process to bind an established digital identity with a credential.	Digital Identity Lifecycle Management - The process to bind an entity's established identity with a token (either hardware or software, to include username and password), issuance, renewals, suspension, and revocation.	Identity Lifecycle Management; Provisioning
	Token Binding	The process of binding a physical or electronic token to acredential.	The process of binding an identity to a physical or electronic credential.	N/A
	Token Issuance/Association	Process by which possession of a token is transferred to a non human user.	Issuance- Process by which possession of a credential is passed to an entity. Service characteristics vary by credential type.	N/A
	Attribute Binding	The process of binding pre-determined human user and non human user? attributes to a credential.	Credential Production- The process of binding an identity to a physical or electronic credential.	N/A
Authentication		Process of determining the validity of one or more credentials used to claim a digital identity.	Authentication- Authentication is the process of verifying that a claimed identity is genuine and based on valid credentials.	Authentication
	Request	Process by which authentication is initiated by a non human entity.	None	N/A
	Credential Presentation	Process by which a human user submits a digital credential for the purposes of authentication.	None	N/A
	Authentication Decision	The decision to accept or not accept the results of the authentication process.	None	N/A
Authorization		Authorization is the process of granting or denying specific human user's digital identity requests for access to resources.	Authorization- Authorization is the process of granting or denying specific requests for access to resources.	Authorization, Access Control, SSO, ID Federation
	Request	Process by which authorization is initiated by a non human user	None	N/A
	Data Request	Process by which a non human user is notified of the attributes required for determining access to a specific resource; typically, these attributes for authorization have not been bound to the credential or previously available to the organization making the authorization decision.	None	N/A
	Submission of Data	Process for collecting human user or non human user attributes required to make a determination regarding authorization.	None	N/A
	Attribute Verification	The process of confirming or denying that human user claimed attributes are correct and meet the pre-determined non human requirements for authorization; typically, these attributes for authorization have not been bound to the credential or previously available to the organization making the authorization decision.	Background Investigation- Process for collecting identity data and accepting individuals as contractors or associates. Background investigation process once an applicant has been selected to support a particular contract that results in the creation of a digital identity within the agency's human resource(s) (HR) application.	N/A
	Authorization Decision	The non human user's decision to accept or not accept the results of the authorization process.	Identity Verification & Validation- The process of confirming or denying that a claimed identity is correct and meets the pre-determined requirements by comparing the credential(s) (something you know, something you have, something you are) with previously proven information.	N/A
System Management and Maintenance		Process of creating, maintaining, deactivating and deleting digital identities, credentials, and tokens within a system.	Local Digital Identity Creation and Management- Process of creating, maintaining, deactivating and deleting digital identities for entities in the identity store.	Identity Lifecycle Management
	Revocation	The process by which a non human being user issuing authority renders a human being user issued credential useless for authentication to a specific digital identity.	None	Identity Lifecycle Management; Revocation and De-provisioning
	Periodic Updates	Periodic scheduled background update to determine eligibility for an entitlement. Requires new data?	Background Update- Periodic scheduled background update to determine fitness in relation to physical and logical access policy.	Identity Lifecycle Management; Revocation and De-provisioning
	Event Based Updates	Background update to determine eligibility for an entitlement as a result of changes in a user's status (e.g., change in marital status, end of subscription, etc.) requires new data?	Background Update- Periodic scheduled background update to determine fitness in relation to physical and logical access policy.	Identity Lifecycle Management; Revocation and De-provisioning
	Redress	The voluntary process by which human users and non human users reconcile errors that occur during the operations and processes of an identity (eco?) system.	None	None