Personas® - Managing digital identities

At the foundation level, Personas are essentially a pseudonym for an individual, offering the ability to adopt one of the many faces we all "wear" & present to other people throughout our daily lives.

This is as true for Octopus Personas as it is for other similar metaphors - but to assume this is the extent of their role in intelligent privacy is to fundamentally understate the core concepts that underpins this premise behind identity management.

Octopus Personas are not about identifying an individual, but about identifying an "*authoritative entity*", that subtle nuance offers a fundamentally different perspective on identity management.

For example, the "HR Director" Persona is never "owned" by "Steve" or "Mary" - the actual human HR Director, because they are individuals that perform the "role" of HR Director.

When a new HR Director is hired, their own personal "Work Persona" is granted the right to act on behalf of the HR Director role.

They are granted the rights to the cryptographic authority that allows them to "sign" & "identify" themselves in that role, but that is not "who" they are, it is merely a role they play for a prescribed period of time.

When a new employee is hired, they are hired by the authority of the "HR Director" not the individual who is playing that role.

When those individuals leave that role, their crypto keys are revoked and they can no longer act on behalf of that role, however, the cryptographic signatures generated by them on behalf of that role, are, and will continue to be valid when a new individual HR Director takes up that position.

Both the Persona of the individual who "is" the HR Director, and the Persona that represents the "role" of HR Director are "authorities" in their own right - one for the individual and one for the role or position - representing the company or organisation.

But unlike other digital trust technologies, there is no central authority to validate one Persona, nor is there a requirement to trust a mathematical chain of

signatures (eg. Blockchain). The trust & authority in a Persona, is based on the trust and authority conveyed to it by other Personas.

The authority a Persona offers is built from the other Personas that trust it, and in turn the trust others have in them. To coin the phrase popularised by Nassim Taleb, each Persona has "skin-in-the-game", and stands to lose their hard won reputational value should they behave or prove to be unworthy of the conveyed trust.

In this way, the authority of a Persona is conveyed not by some G.O.D. (Grand Organising Directorate), but by a chain of reputational trust - who trusts who. In the same way our daily lives trust is gained through interactions with others, so is the authority - and thus value of a Persona.

And so a "consensus" can be built of which digital identities can or should not be trusted. A Persona's trust will increase with age, as it "ages" it gathers more trust "votes" and thus so does it's value, and it stands to lose more by behaving in an "untrustworthy" way.

Once the concept of an abstract entity, such as a "role" is accepted as an "authority", there is no limit to what types of entities can be authorities.

For example, in the IoT world, how will I securely communicate with my washing machine, my house heating system, or my car?

Each in its own way requires the ability to not only identify itself, but ensure it's identity can be verified before interacting with it. A Persona can deliver this identity verification just as well for a machine as a human.

Whilst your washing machine may not be able to send deeply constructed prose as text messages, it can provide a structured mechanism to communicate with it.

As part of making a connection between two Personas, an encrypted "channel" is created over which both parties can exchange offers for their interaction along with cryptographic security keys, and the offer of a secure "Endpoint".

This allows, for example, the washing machine to "offer" itself as an "Endpoint" along with a specific user interface with a set of "commands" it understands. Instead of seeing a standard "message view" with the connection, the recipient might see a dashboard that allows the washing machine to be started and stopped and the temperature adjusted.

This interface the washing machine "offers" is not built into the Octopus app, and so in many ways works like an "app store", where web enabled devices can "offer" a web interface over which secure and verified communications can take place.

The logical progression from this is that the "Endpoint" - the other end of the Persona connection need not be a specific machine or device, but a service.

A user may choose to "trust" the Persona offered by their electricity company. The electricity company in-turn displays their current consumption in realtime in the

connection information. The Persona that the user connects to the electricity company with shares their account information with the electricity company, and that easily allows standard web APIs to return this data to their own "dashboard".

If I open the connection with my boss, I can send them a message, if I open the connection with my washing machine I can turn it off, if I open the connection with my utility company I can see my current bill.

Now the concept of a Persona has progressed from an individual, to a role, to a device and to a service, there is one final logical step.

Only the human backed Personas have any true intelligence behind them. But each Persona that connects with another has access to specific sets of private data and has the capacity to request & consume any amount of seemingly unrelated data. This is where Personas can become "*Intelligent Agents*".

Intelligent Agents

Along with the "offers" one Persona makes to another, it becomes a simple extension to offer a local IA - an "Intelligent Agent" to act on the Persona's behalf.

This IA is executed in the background of a security isolated thread on the user's device or web browser, and gains access to the data the user has shared with that Persona. This allows the IA to analyse the data offered locally and without breaching any data privacy. For example:

I connect with "Nike", and share my location & my shoe size with their Persona, the Nike IA is able to offer me available stock - in a store close to me.

I connect with "Mothercare", and share my child's birth certificate, and Mothercare's IA is able to offer me a range of clothes that fit my 5 year old son.

I connect with Starbucks, and their connection "Dashboard" allows me to choose my favourite coffee. Their IA knows I purchase coffee on the way to work each morning, so it dials ahead, places an order for the coffee in the nearest (open) shop on my way to work. It also has the ability to generate a payment Artefact that Starbucks is able to verify was issued by my Persona.

My car insurance is due to expire, but having shared my details with an insurance comparison IA, it is able to monitor my location, behaviour and its expiry date and offers me the best deal before it is due for renewal.

I want a cheap flight to the Maldives next month for the family, and so my flight scanner IA sends my mobile phone a Push Notification that it has just found the best deal & booked it for me - using the Passport I had shared with it and generated a payment Artefact as a deposit.

My Health IA has examined the data from my Fitbit, it's seen my blood pressure rise, that I haven't used my gym membership Artefact in the last 30 days and I buy far too much coffee from Starbucks. I booked an appointment with my GP next Wednesday on my way

home from work.

As AI becomes increasingly ubiquitous, AI will be used by companies to target theirs and others customers and users in both honest and less-honest ways.

When calling a company, we have all heard the line - “This call will be recorded for training and monitoring purposes”. But what happens when that “training and monitoring” is for an AI?

What happens when that AI realises that you, personally, respond with lower stress levels in your voice when called by a lady, in her mid-30s, with a soft Edinburgh accent? That you are most susceptible to a sales message on Monday afternoons between 2pm and 4pm?

You will need some form of defense, and your Persona’s intelligent agent will step in.

Acting on your behalf, it will answer your phone, it will protect your Mother from sales tactics targeting her pension or double glazing. It will protect your children from potential predators as well receiving or sending inappropriate content.

As the saying goes, don't bring a knife to a gunfight, and in a world where everyone has AI you need to be better equipped. Some vague privacy & security settings on social media just won’t cut it.

VaultChain was built from the ground up as a distributed graph dataset using RDF/JSON-LD linked data and can be extended to support any vocabulary or ontology that a service might require.

Standard web interfaces allow that data to be consumed and processed in interesting and imaginative ways.

Personas offer trust and identity and a simple mechanism to share and control the data being consumed.

Intelligent Agents keep data private and under the control of the owners, whilst allowing 3rd parties to offer new services and insights to their customers.