The roles and goals of identity management in future Smart Cities – Gert Botha, CEO Hiving Technology
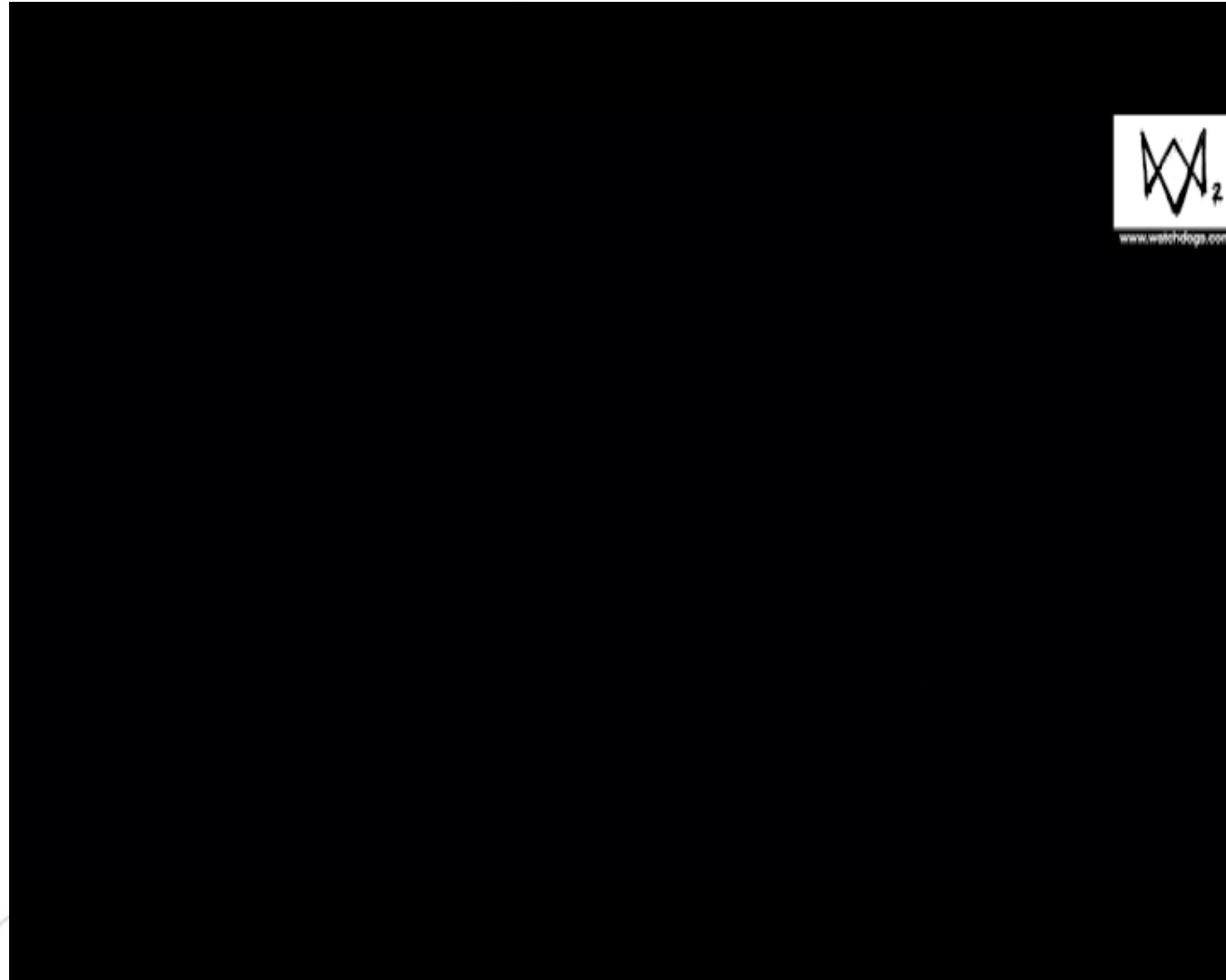
Futuristic animation extracted from Watchdog 2 by Ubisoft.

- Compromised security and privacy
- Massive duplication of data
- **IoT** mostly unsecured with reactive security practices
- No unified identity and poor quality data make progress to the next computing era impossible
- The Internet is an untrusted source
- Reactive
- Legal

Trusted Identity!!

- **Trusted Identity** is the **missing key** in enabling the progression of computing into the next phase. This entails linking the physical, digital and virtual worlds into a seamless user experience as predicted by the Gartner (2016) and some of its counterparts.

- **Deep root of trust element** on an independent identification device has the ability to:
    - identify people and things in a unified manner;
    - Enabling a seamless user experience across all aspects of life while collecting data and building context owned by the person or legal entity but made available to service providers by permission;
    - linking things to a person or legal entity from an ownership perspective;
    - keeping privacy and security intact.
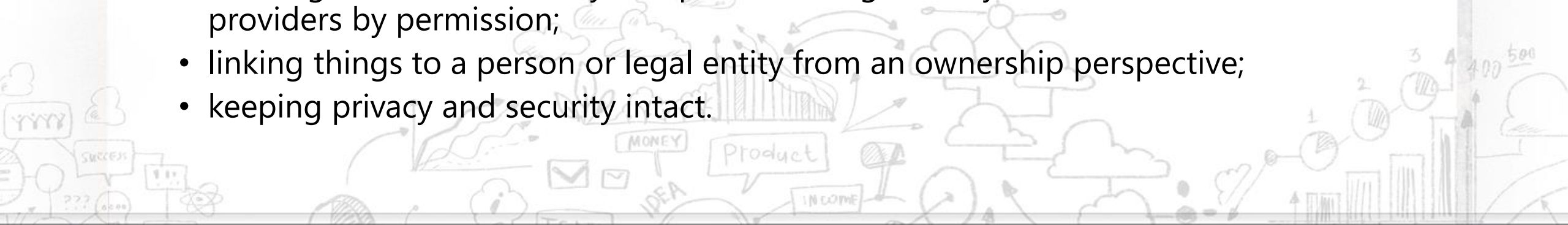
What is the success criteria?

In the McKinsey & Company report 'Unlocking the potential of the Internet of Things' and as such smart connected cities are:

"with policy actions to encourage *interoperability*, ensure *security*, and protect *privacy* and property rights, the Internet of Things can begin to reach its full potential."

Success Criteria
Interoperability
Security
Privacy
Unified Identity

Identity in Citizen Centric Engagement

Unified Identity Requirement

- Must be physical and digital
- Must be ambient
- Must be private and secure
- Must be application agnostic
- Must have a deep root of trust element

Smart City Framework that delivers:

- Privacy and Security

- Individualised services centred on people in a city, nation or global context

- Protecting personal and owner's data through trusted applications

- Using identity and location as the universal trigger for a seamless user experience

Trust

Single Identity enables a unique Citizen Centric Implementation Framework

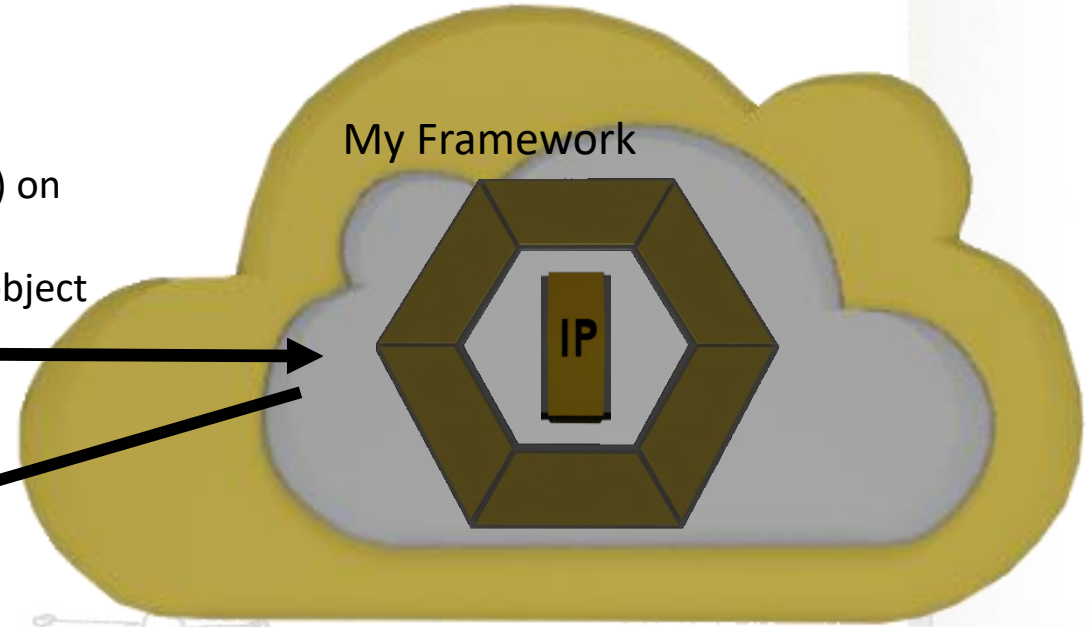# Identification and Data Management

Location data is added to the identity string

One ID

Location

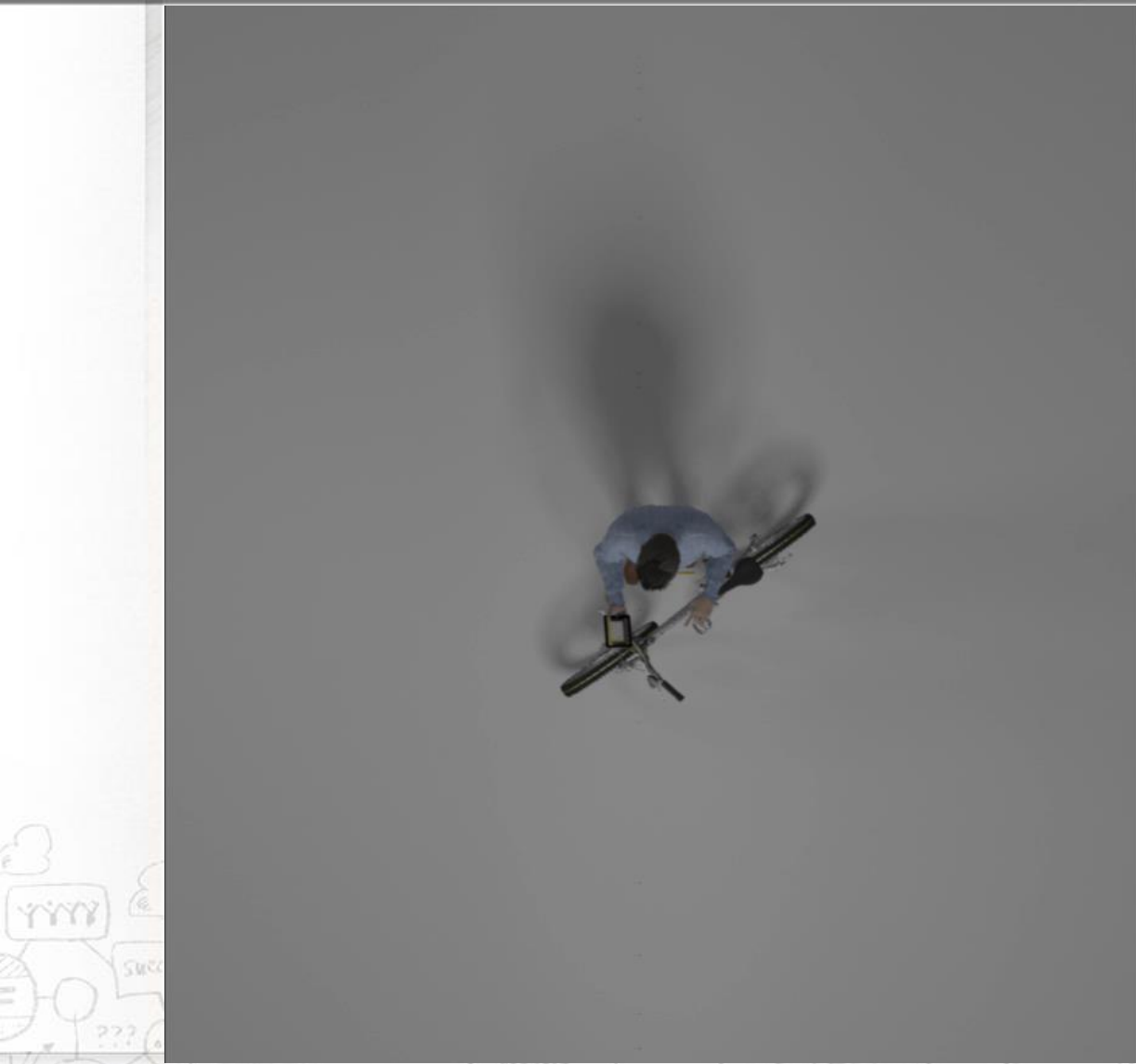Enables a single place (IP) on the cloud to store data about the person or object

My Framework

IP

Trigger rule based actions or experiences according to predefined location rules

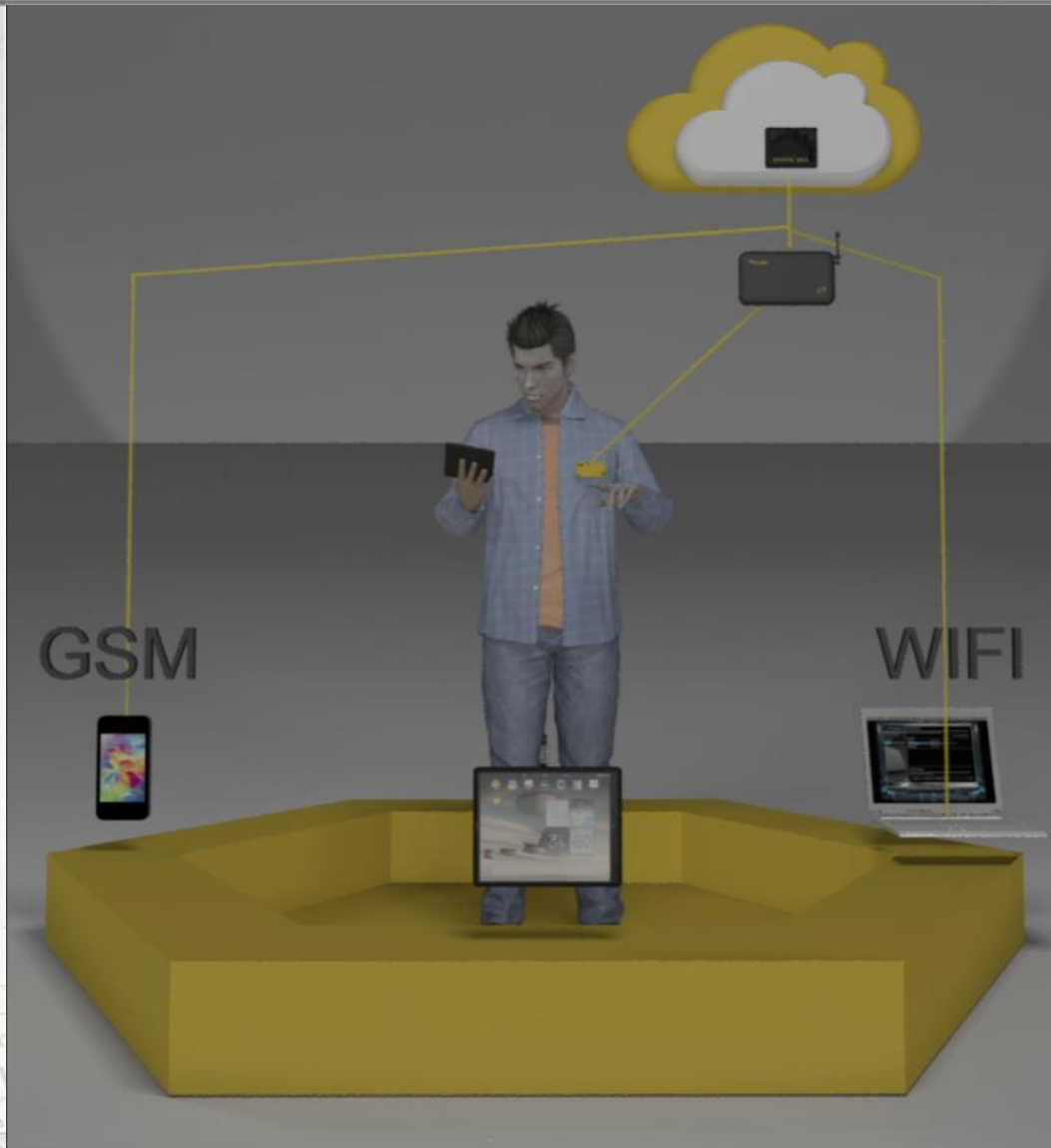- Unified identity suited for people and things.

Unified Identity – One common identifier for everything

- Unified identity suited for people and things.
- Every personal endpoint has its own unsecure identity.

- Unified identity suited for people and things.

- Every personal endpoint has its own unsecure identity.

- Utilise One ID as a deep root of trust element across all endpoints. Using physical identity as the single digital identity.

- Unified identity suited for people and things.

- Every personal endpoint has its own unsecure identity.

- Utilise One ID as a deep root of trust element across all endpoints. Using physical identity as the single digital identity.

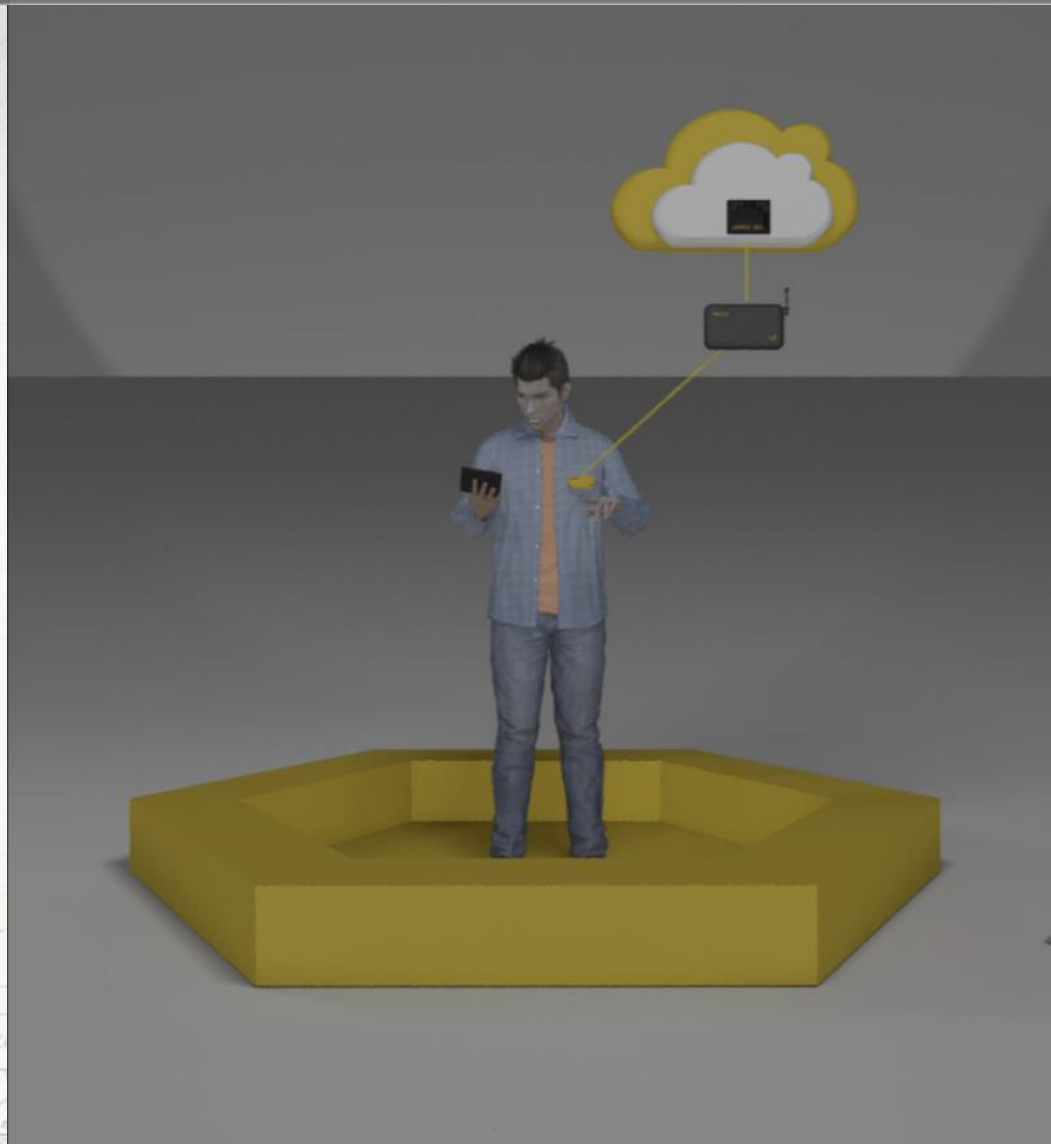- Connecting a responsible person to all communication through endpoints.

- Everything related to the person can be grouped with the person

- Everything related to the person can be grouped with the person
  - Family

- Everything related to the person can be grouped with the person
  - Family
  - Properties and Content

- Everything related to the person can be grouped with the person
  - Family
  - Properties and Content
  - My Business or My Job

- Everything related to the person can be grouped with the person
  - Family
  - Properties and Content
  - My Business or My Job

- Data about these objects and people even though they have their own One ID's is grouped to a responsible person or legal entity

- Everything related to the person can be grouped with the person
  - Family
  - Properties and Content
  - My Business or My Job

- Data about these objects and people even though they have their own One ID's is grouped to a responsible person or legal entity

- Millions of these groupings can exist independent of each other with the One ID pointing the identity data to the IP address specified on the One ID

Group People and Things – Establish Ownership & Responsibility

- Everything related to the person can be grouped with the person.
  - Family
  - Properties and Content
  - My Business or My Job

- Data about these objects and people even though they have their own One ID's is grouped to a responsible person or legal entity.
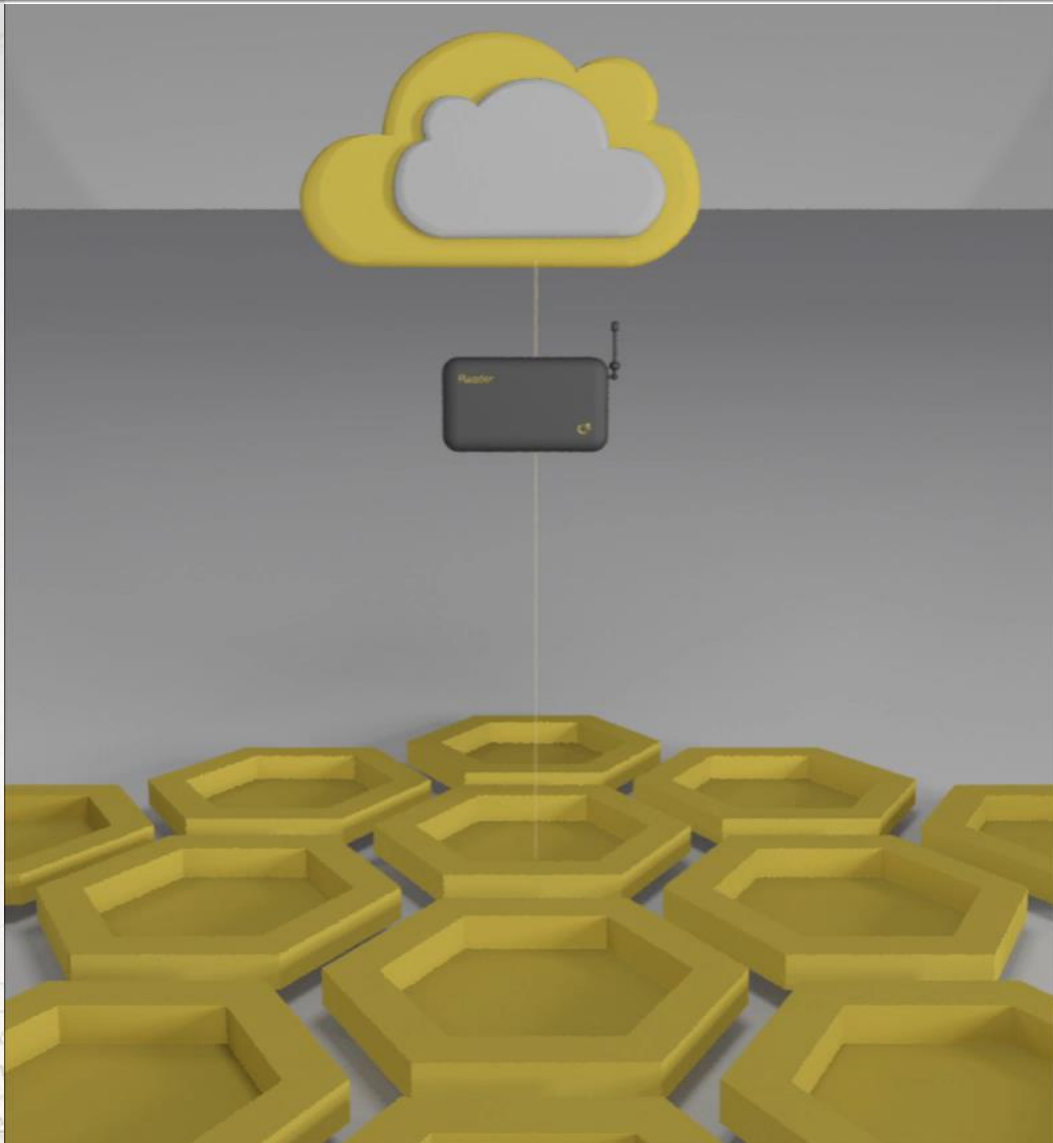
- Millions of these groupings can exist independent of each other with the One ID pointing the identity data to the IP address specified on the One ID.

- These groups can again be grouped into a Smart Nation for a specific country.

My Trusted Data

- Everything related to the person can be grouped with the person
    - Family
    - Properties and Content
    - My Business or My Job
- Data about these objects and people even though they have their own One ID's is grouped to a responsible person or legal entity
- Millions of these groupings can exist independent of each other with the One ID pointing the identity data to the IP address specified on the Hive One ID
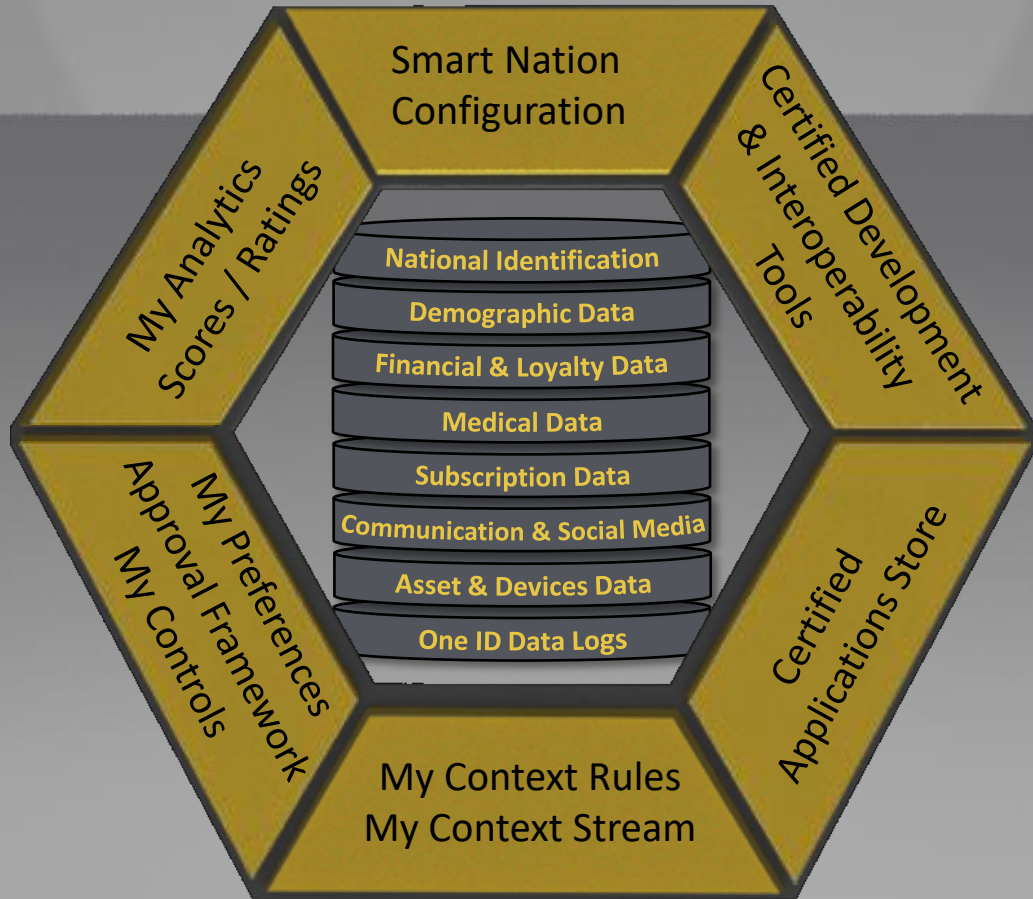- These groups can again be grouped into a Smart Nation for a specific country
- A One ID is associated with a trusted data set about the person or legal entity. This data is owned and managed by the person or entity

- Trusted data can be anything related to the person, object (thing) or the legal entity.

- The data is secured and access to the data can only be obtained through trusted applications and tools regulated by different rules and preferences:
  - Context Rules generate automated actions depending on the context data stream. Different rules apply to different locations.
  - Preferences, approvals and controls are user definable and allows for a unique experience.
  - Smart Nation rules can be configured that will apply to and override the personal framework.
  - Certified Development and Interoperability Tools
  - Certified Smart Nation and User Applications
  - Analytics are done and the ratings are provided rather than raw data.

- The Context Data Stream of the person, the context stream of his/her things with the deep root of trust element of the One ID creates an unbreakable security foundation.
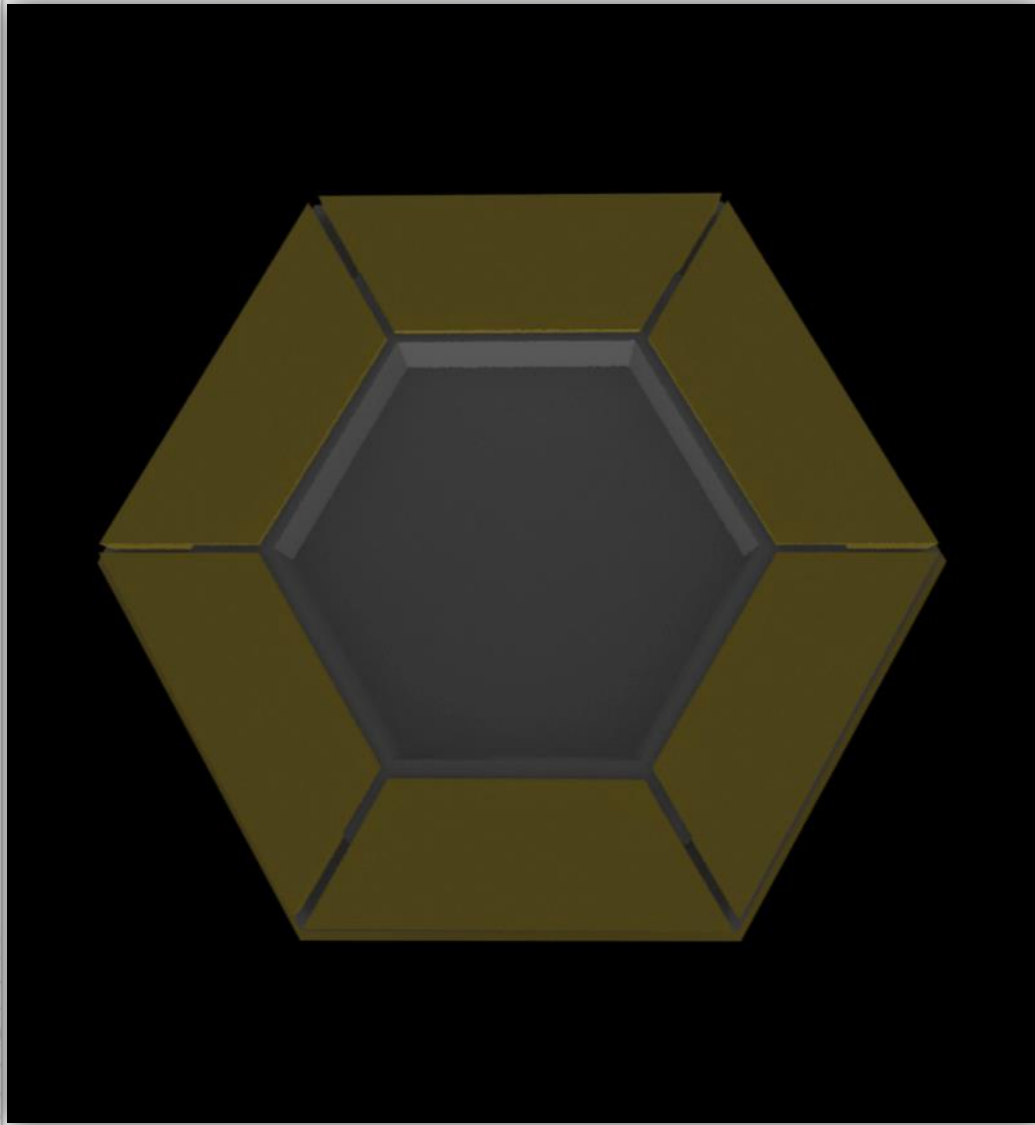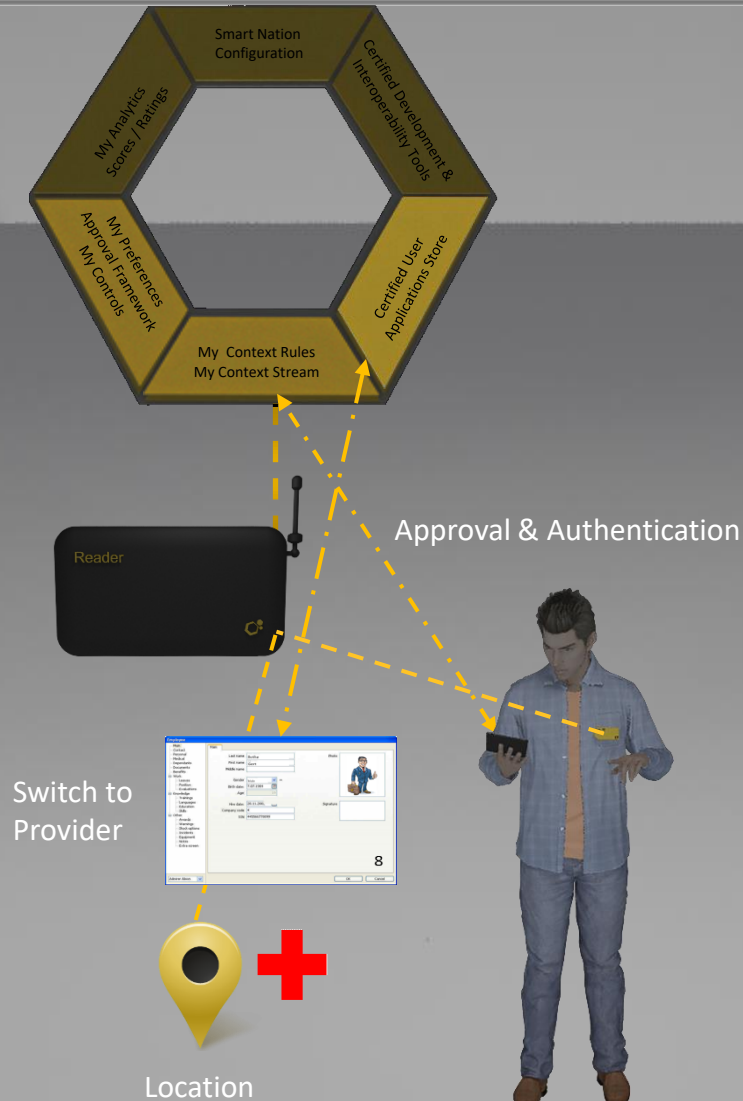
- Every One ID points to an IP address on the Internet.

- A Context data stream is created wherever people and objects are seen.

- The context triggers rules and actions automatically as the person or object gets detected.
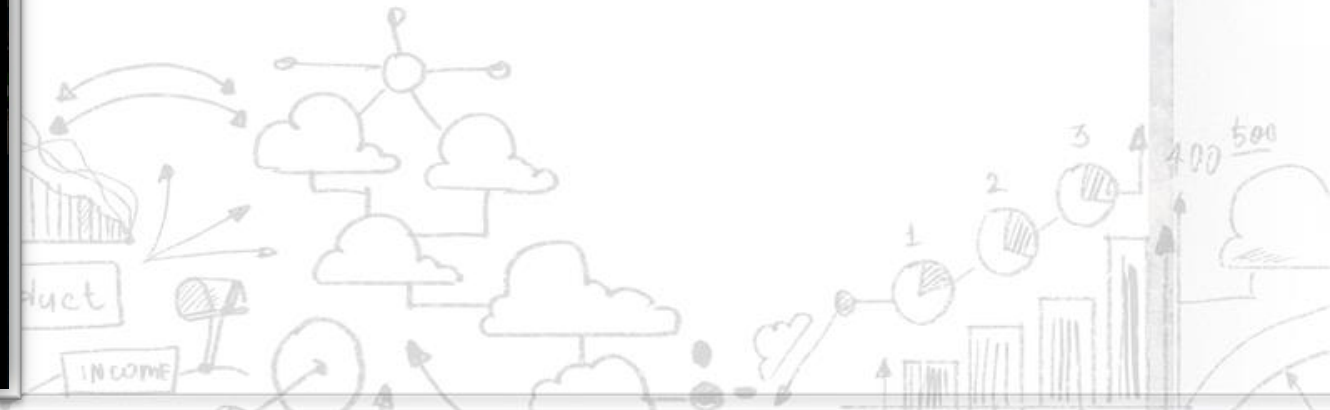
Citizen Centric Delivery in Action

- The person walks up to a medical admissions counter.

- The person is identified via the One ID and the data is combined with the Location data.

- The Context Rules according to the approvals framework sends a message to the person's phone to authorise the data that will be made available.

- Once authorised the trusted application is triggered that makes the data available to the admissions staff.

- Similarly a unique user experience can be created in virtually all situations.

Additional Examples:

- Obtain government services
- Pay for goods and services
- Pay for public transport
- Personalised shopping experience
- Access Control
- Crowd Management
- Vehicle Identification
- More............

Summary

- Unified identity with a deep route of trust not only solve Smart City challenges but offer a solution to IoT Security

- Identity enable ownership and responsibility of things

- Authentication always include a person or legal entity. Location and the presence of other things can be used for additional authentication

- Authenticated identity of all digital interactions has the potential to resolve cyber security challenges

Questions