Introduction and Concepts of Identification Systems

Session Objectives

- Consider the concept of *Interaction*
- Consider the concept of *Trust*
- Define Identity and its major facets
  - *Differential-identity*
  - *Experiential-identity*
- Consider Credentials
  - *Markers*
  - *Certificates*
- Define the processes of Identification Systems
  - *Enrolment*
  - *Authentication*
  - *Authorization*
- Consider how Trust derives from Identity

What is the Purpose of an Identification System?

To establish ***trust*** within an interaction

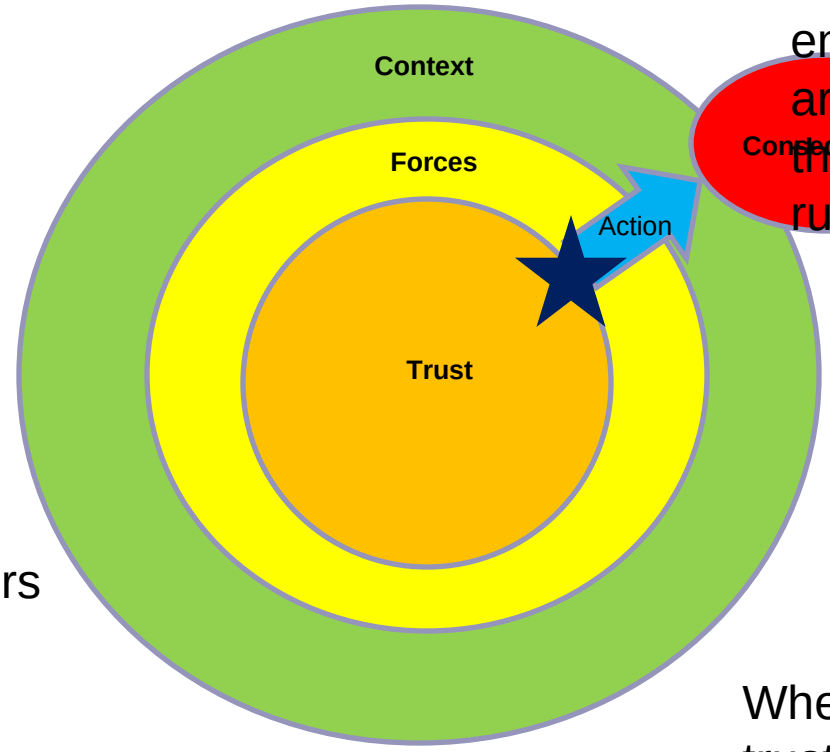
What is an ***interaction***?

The application of a force,
i.e. an ***action***,
between two or more entities,
resulting in a ***consequence***.

Interaction mechanics

An interaction is bounded by a context.

The context encompasses the interacting entities, the forces through which they interact and all of the parameters which influence the interaction.



The action may engage forces that are physical or forces that are social; i.e. rules, laws, etc.

Trust is a measure of the probability that a specific action will result in the desired consequence.

When the assessment of trust suggests an acceptable probability of the desire outcome, an action is evoked.

The resulting consequence concludes the interaction. Whether it is the desired consequence is the measure of validity of the assessment of trust.

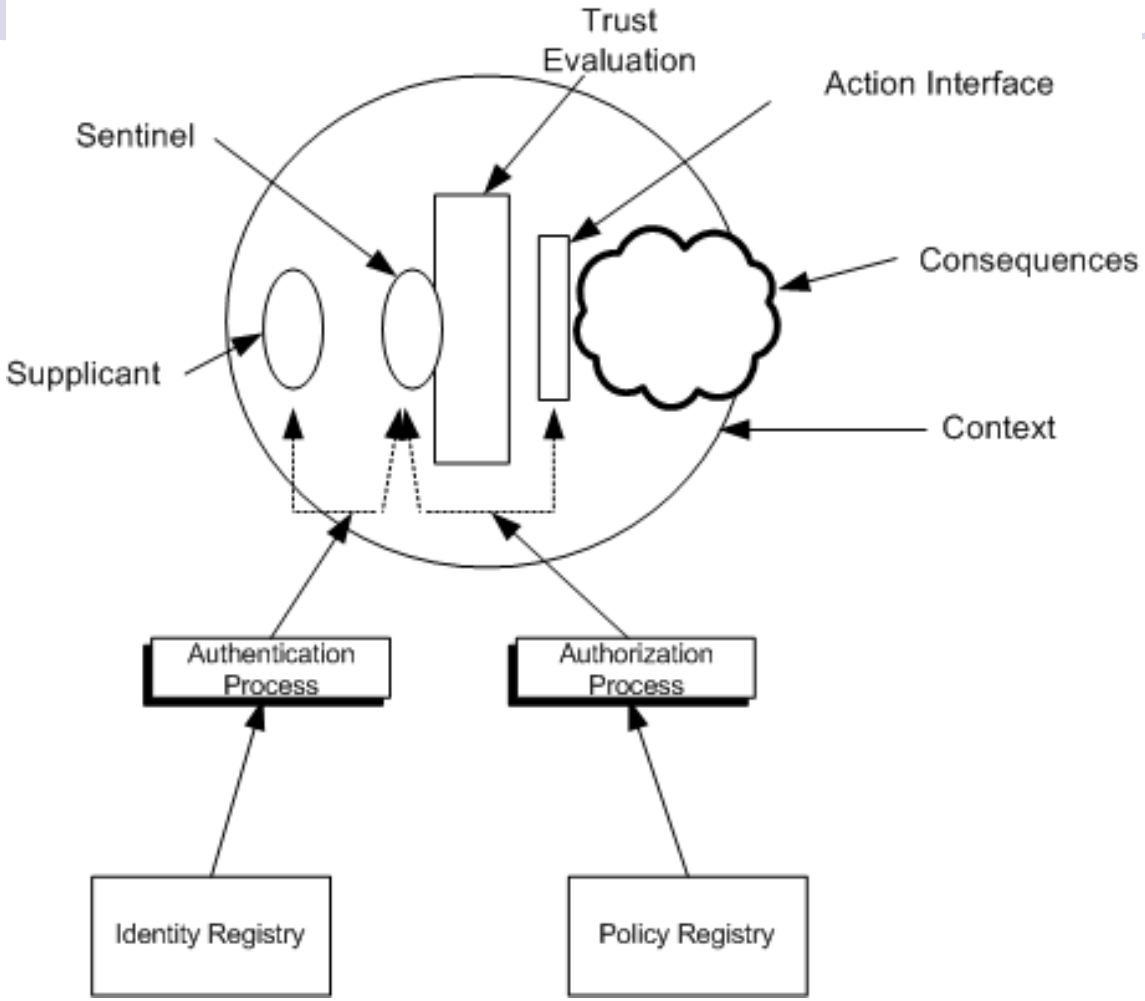
Elements of an Interaction

- Context – constraining association
  - Policy (forces, capabilities and social rules)
  - Interacting individuals
  - Initial conditions (trust) for action stimulus
- Action – application of force within context
  - physical (natural forces)
  - organic (physiological capabilities)
  - social (social rules)
- Consequence – result of action

Parties to an Interaction

- Sentinel – the guardian of an interaction
- Supplicant – one who seeks leave from the sentinel to engage in an interaction
- Symmetric Interaction – an interaction in which all parties act both as sentinel as well as supplicant

Overview of Interaction Mechanics



How do we establish trust for personal interactions?

Through mechanisms that we'll find translate directly to the digital world!

- Privacy – participants control all aspects of the interaction
- Secrecy – participants can exclude other parties from the interaction
- Authentication - participants can establish each other's identities
- Authorization - capabilities can be limited based on identity
- Information Integrity - information can be trusted; it doesn't change
- Non-Repudiation - participation & decisions can be documented
- Trust derived from reputation

Secrecy


No one can hear us as we talk to each other.
I guess not, since we're stuck in this box!

Authentication

Authorization

Information Integrity

Non Repudiation

Trust based on reputation

What is Trust?

Probability of a **specific** interaction consequence

How do we establish trust in individuals?

- We ***identify*** them.
- We engage in actions based on their capabilities.
- We grant them access based on their characteristics, capabilities and/or authority.
- We anticipate consequences based on their reputation.

Identity

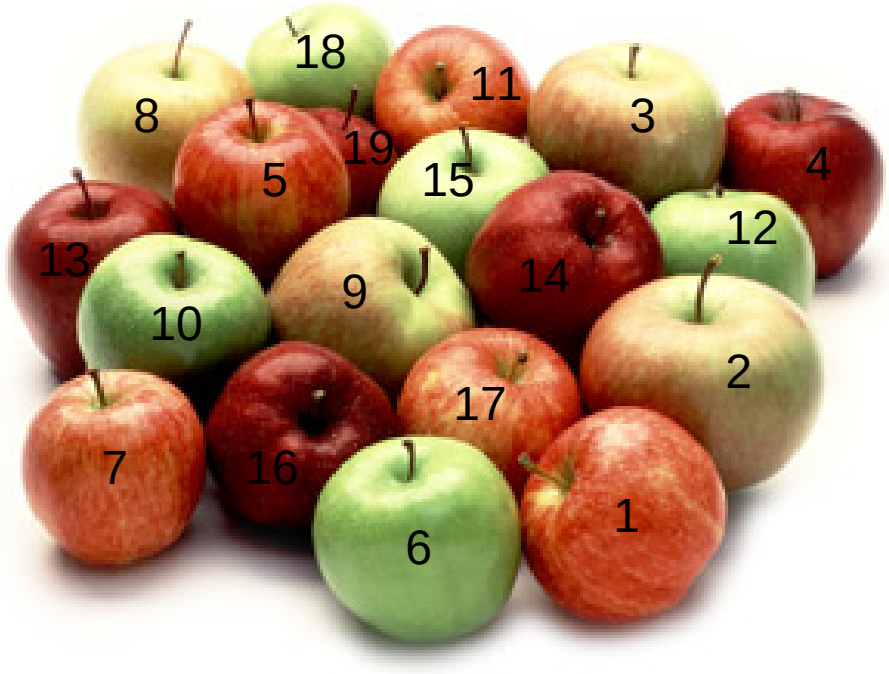
Who are you?

Two Major Facets of Identity

- **Differential Identity** – distinguish the members of an identification system

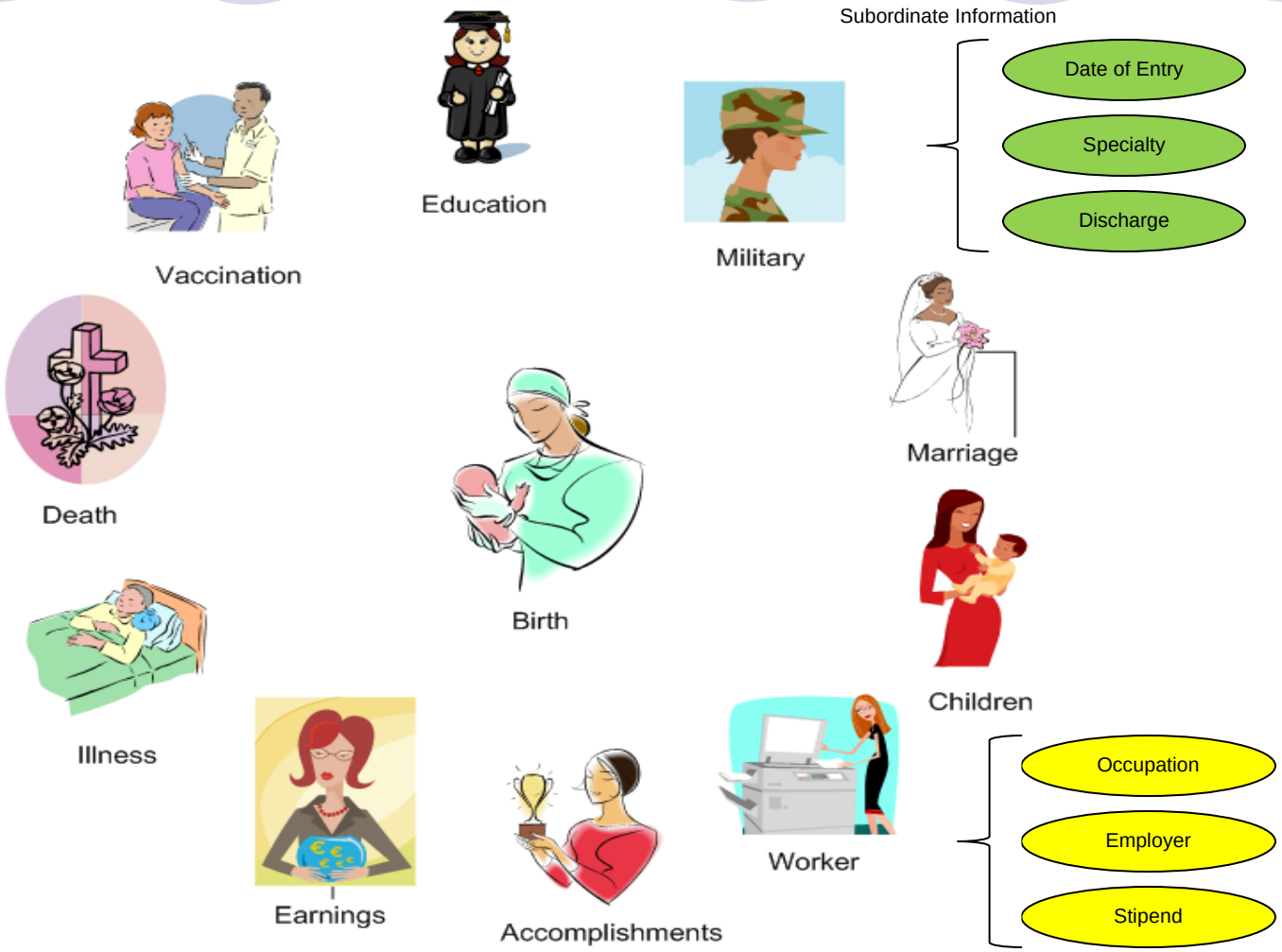
- **Experiential Identity** – the association of interaction consequences with differential identity

Differential-identity



Differential-identity distinguishes entities only to the extent that they can be counted.

Experiential-identity



How do we establish differential-identity or experiential-identity?

Credentials

The simple machines of identification systems

Two types of credentials

- **Markers** – secrets or biometric characteristics used to establish differential-identity

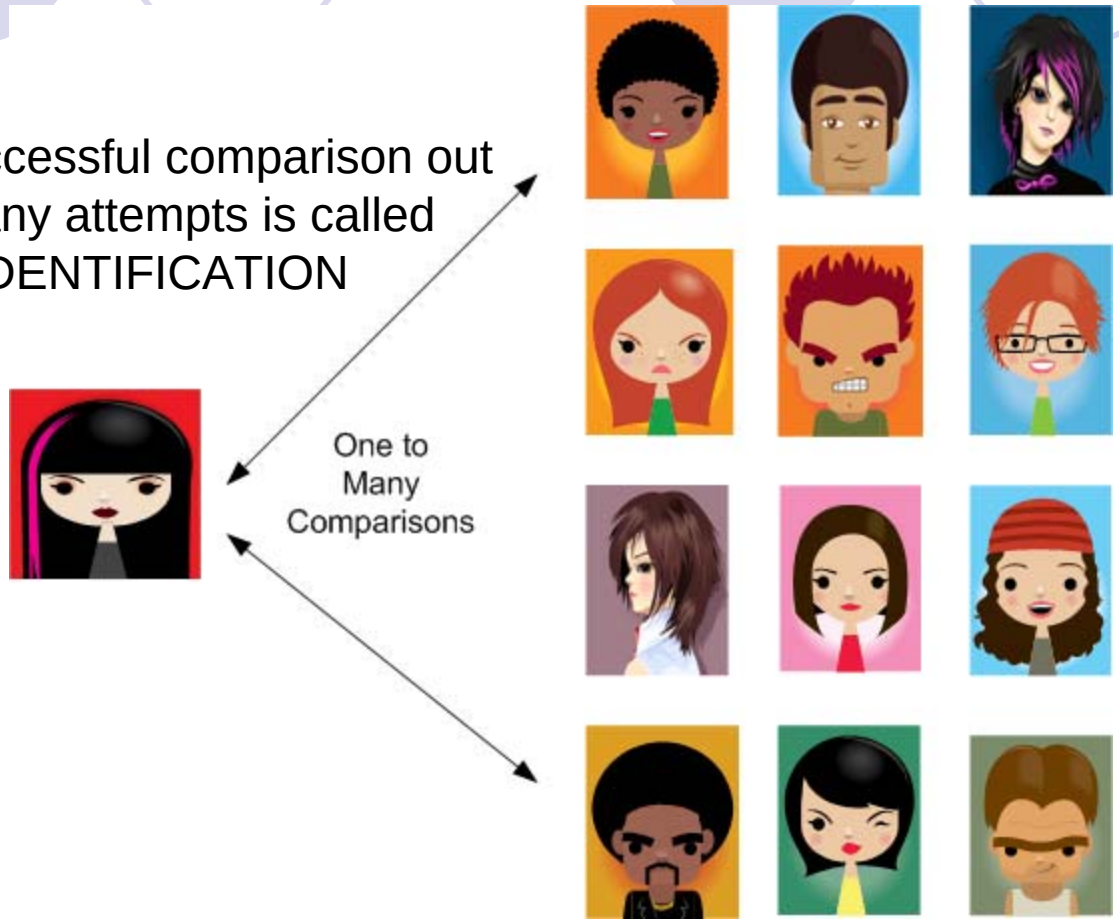
- **Certificates** – messaging mechanisms that rigorously convey information and hence can be used to establish and convey experiential-identity

Characteristics of a *good* marker

- Unique to a specific individual
- Immutable over the individual's lifetime
- Non-invasive to measure
- Cost effective to measure
- Capable of trustworthy one-to-many test
- Capable of trustworthy one-to-one test
- Can ONLY be provided by the individual
- Minimal forensic value (Identity only!)

Why a one-to-many test?

One successful comparison out of many attempts is called IDENTIFICATION



IDENTIFICATION is the basis of ENROLMENT in an Identification System

Why a one-to-one test?

An unsuccessful comparison means differential-identity is UNAUTHENTICATED

A successful comparison means differential-identity is AUTHENTICATED

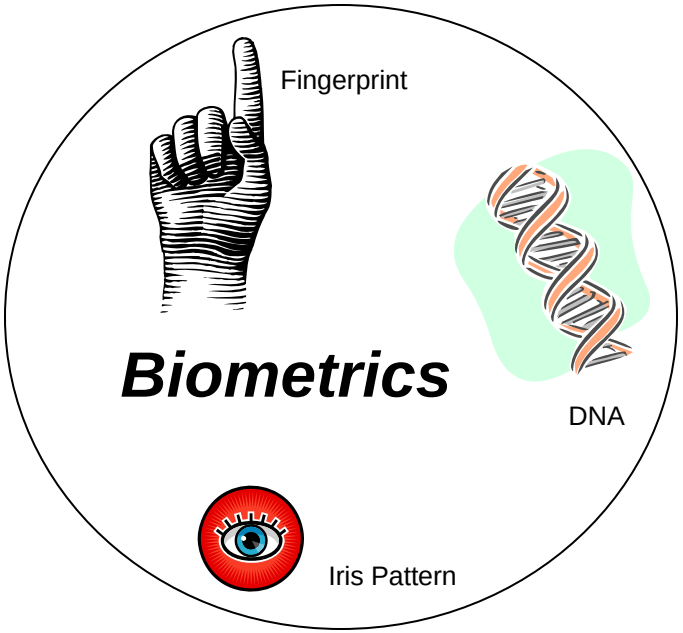
Some Common Markers

Signature

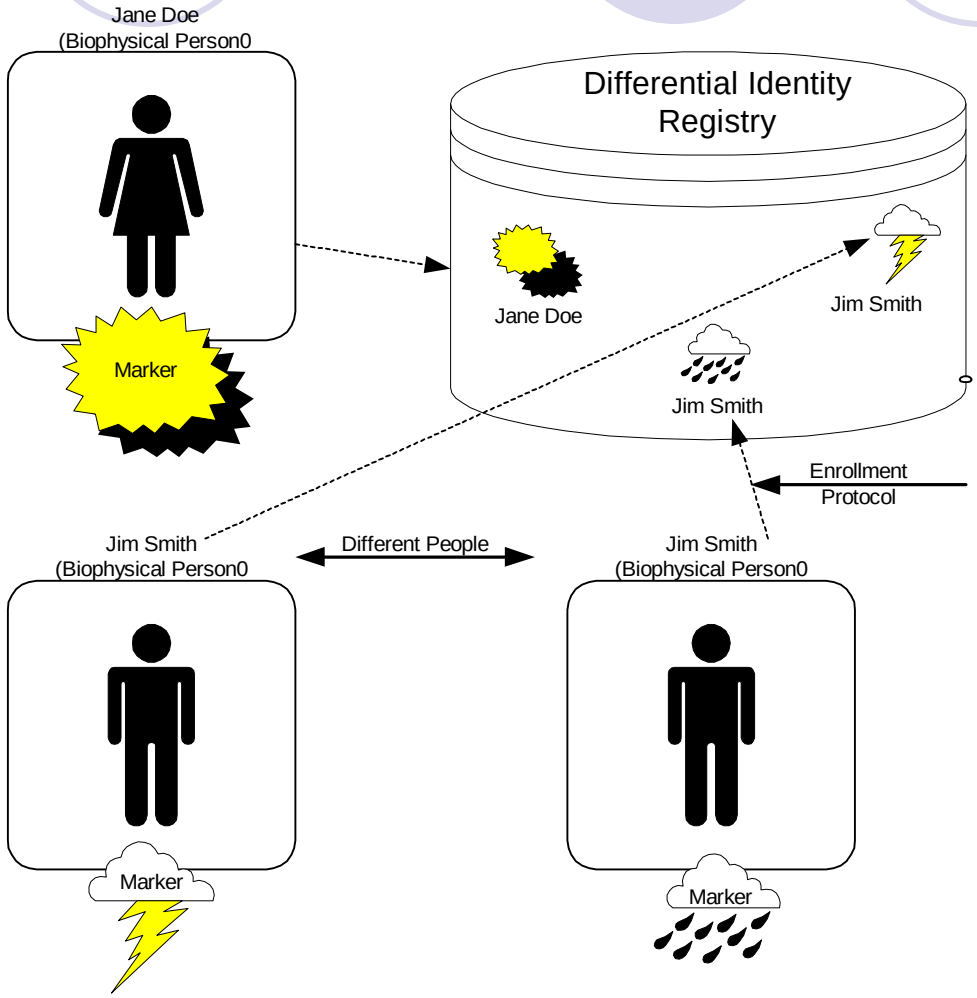
Key

Signet

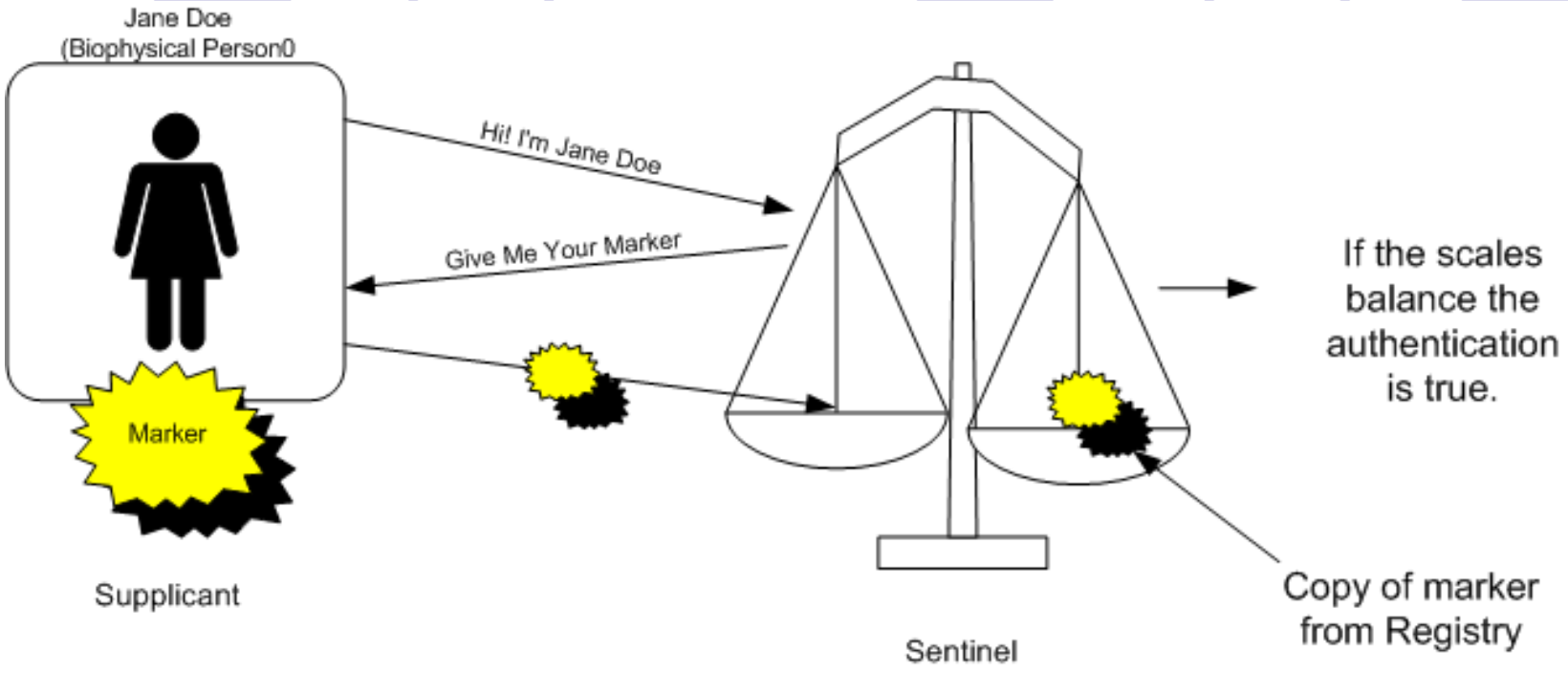
Face
Picture



Basic aspects of enrolment

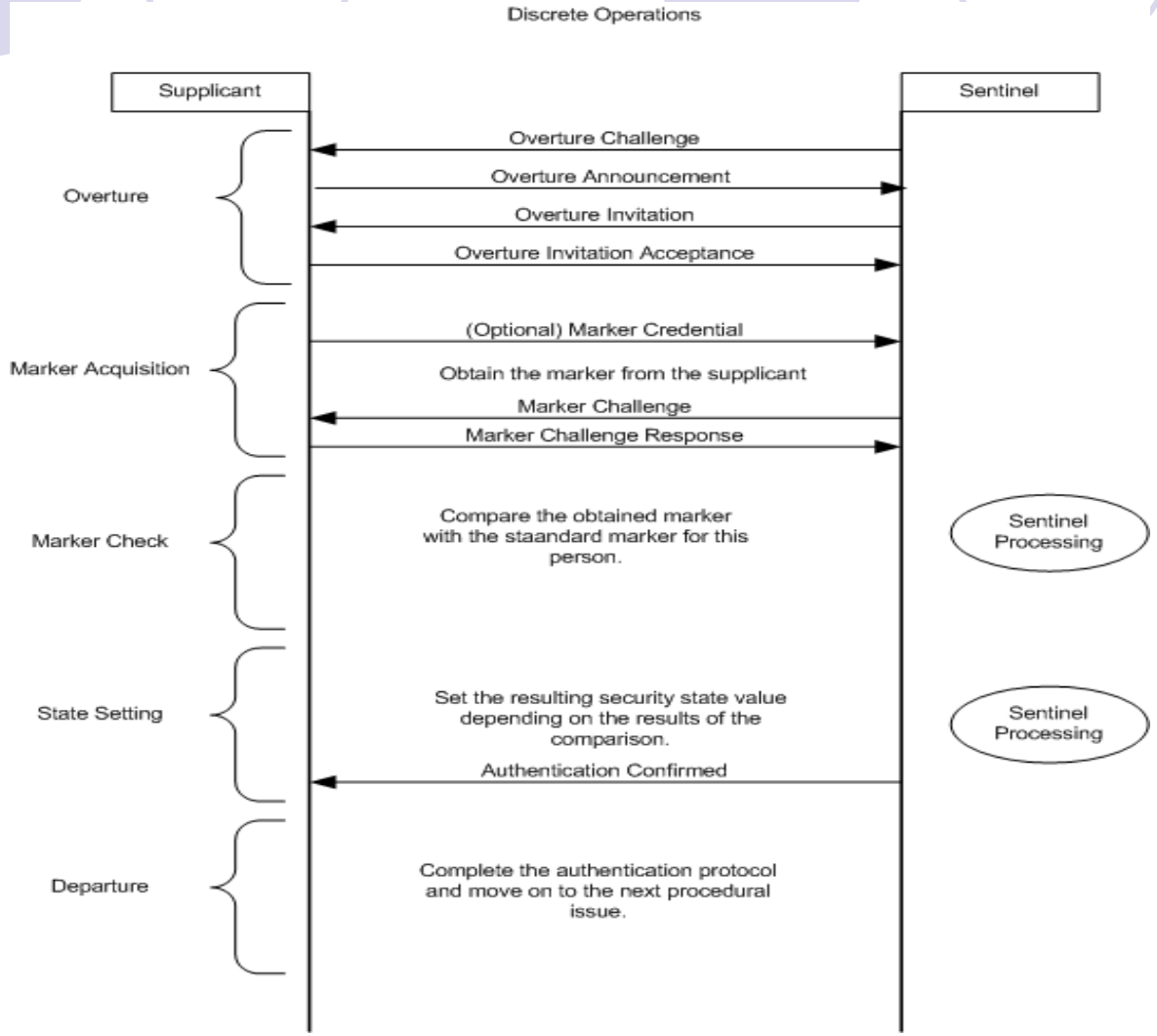


Trust from Authentication



Connection between Marker and Biphysical Person is critical. In general, marker must either be a secret, known only to the supplicant and the sentinel, or it must be a unique, non-counterfeitable characteristic of the biophysical person.

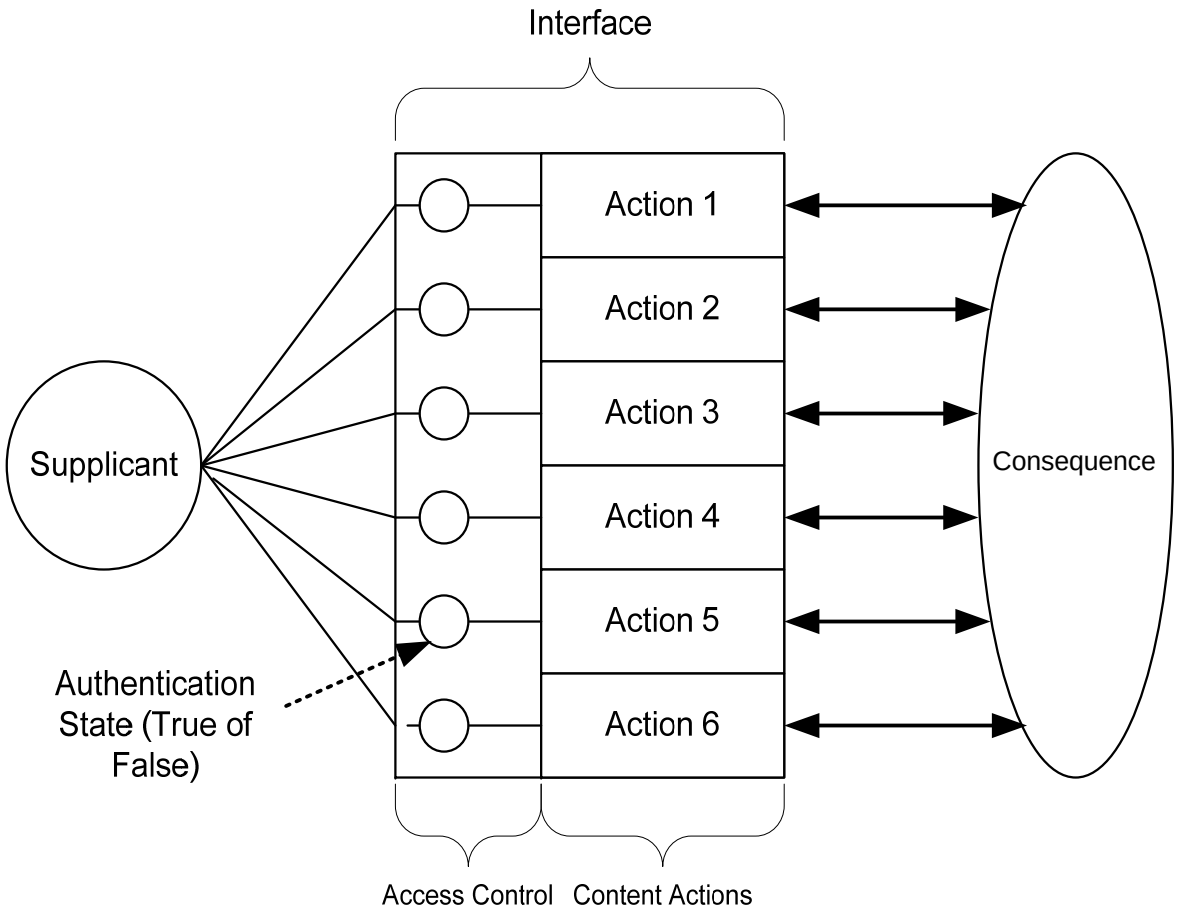
Generic Overview of Authentication



Authorization

- Permission to engage in some specific action during an interaction
- Authorization (permission) can be applied to actions directly
- Authorization can be applied to actions indirectly through other attributes
- Authorization is typically conveyed with a digital certificate (credential)

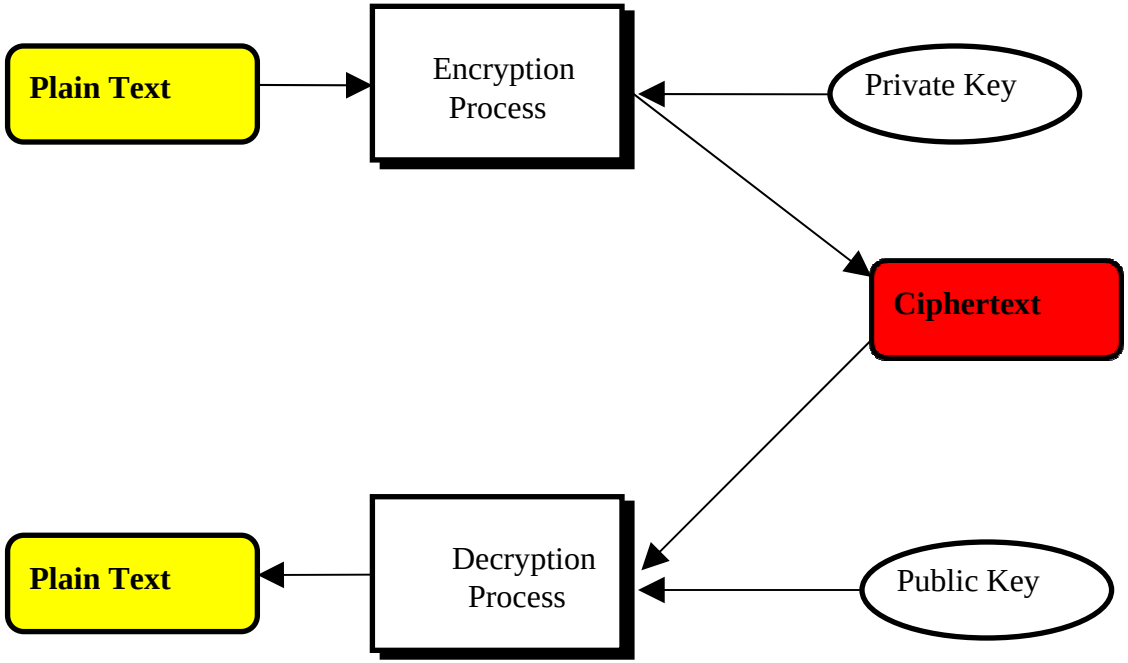
Generic overview of Authorization



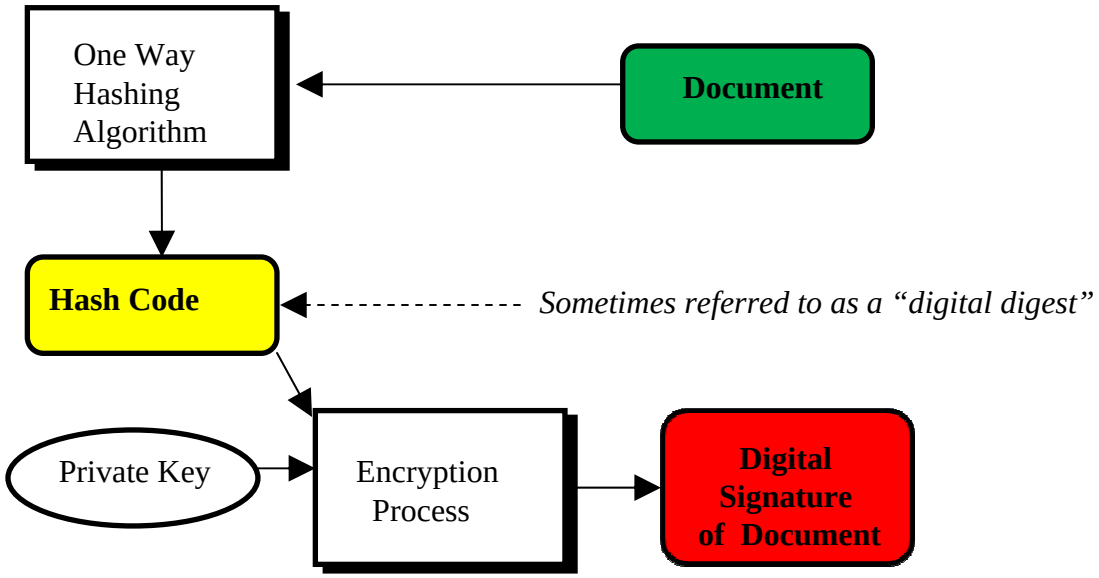
And….. We make use of cryptography.

Cryptography – means of communication in the face of adversaries.

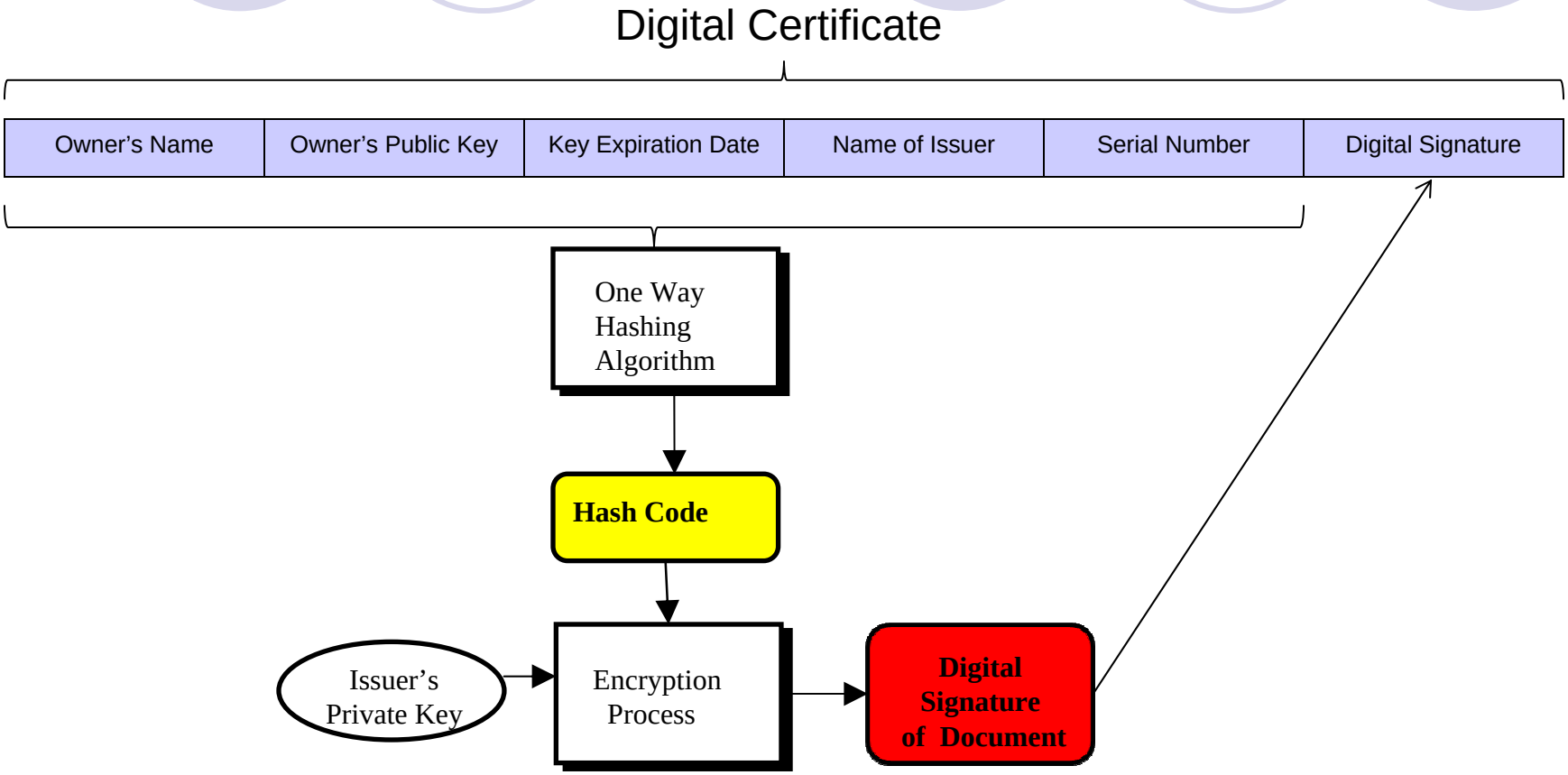
Asymmetric Key Encryption



Digital Signature

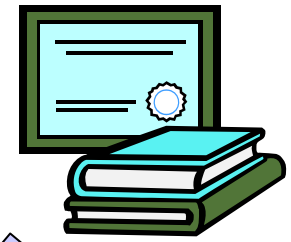


A Public Key Certificate



How do we connect experience to identity?

A Trusted Party

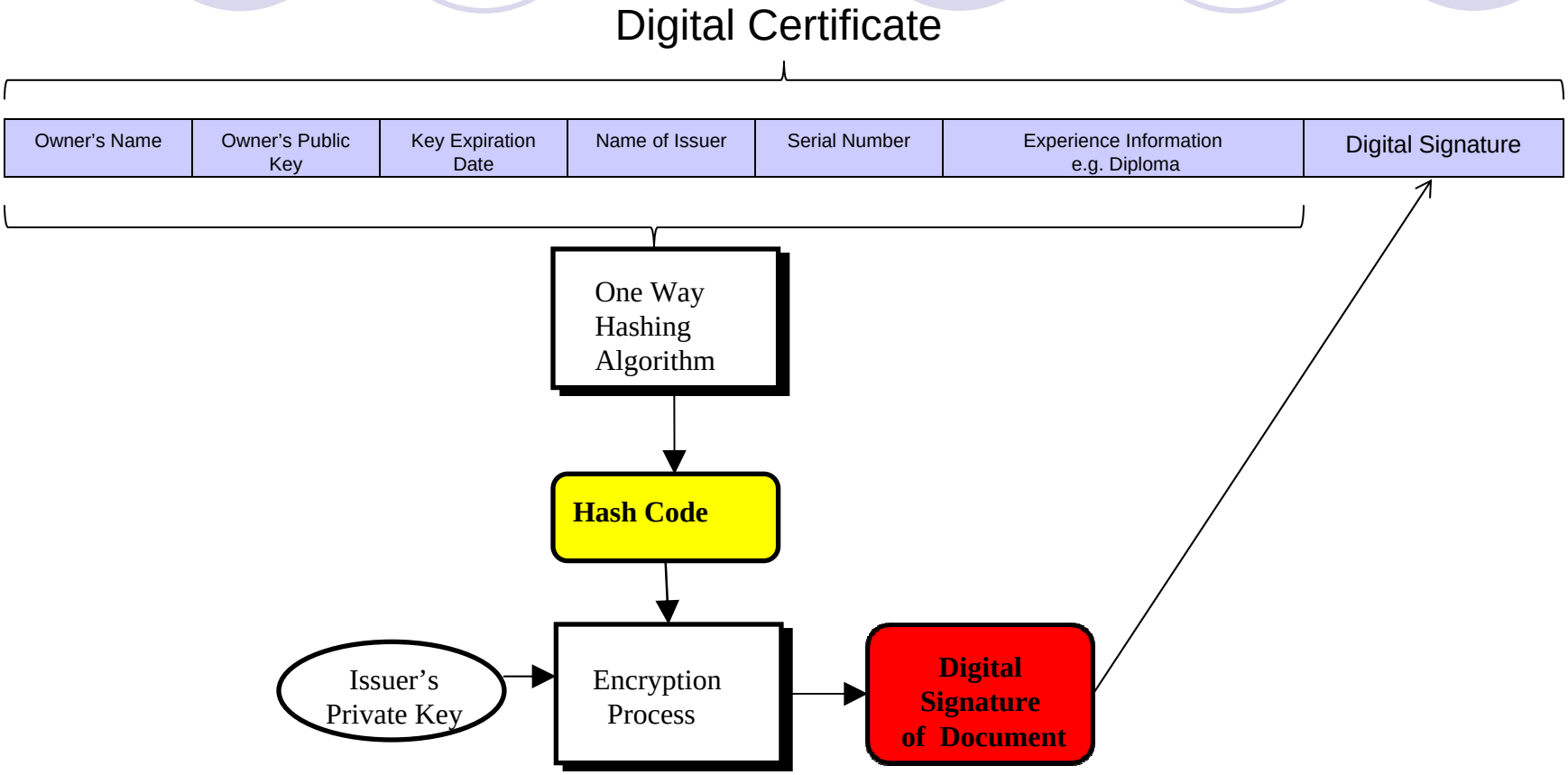


Authenticates
Differential-identity

Signs a certificate attesting
To both facts

Authenticates an
Experience
(e.g. Graduation)

An “Experience” Certificate



How do we establish trust for digital interactions?

Through mechanisms that have their foundation in the personal world!

- Secrecy – interaction is shielded through encryption
- Authentication – through differential-identity and protocols
- Authorization – through experiential-identity and PKI
- Information Integrity – through digital signatures and certificates
- Non-Repudiation – through digital signatures and certificates
- Trust derived from reputation based on experiential-identity and PKI

How do we provide the various mechanisms we've just considered?

THROUGH TOKEN BASED IAS SYSTEMS

QUESTIONS?