



RFID Towards Digital Evidence



**A discussion on the use of RFID and encryption
to create digital evidence within the scope of
real-world process environments.**

Ver 1.0

8 January 2006

Bertus Pretorius

Chief Systems Architect iPico

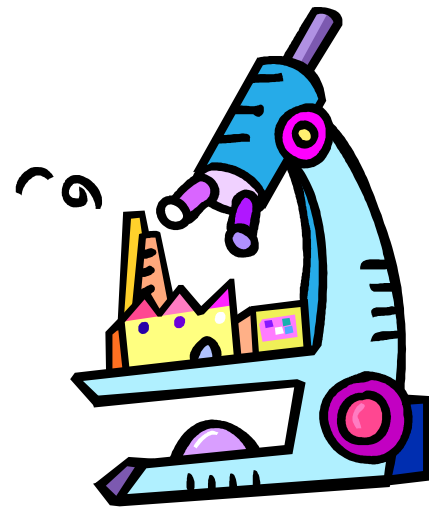
Chairman: Standards SA – SC71H (EVI)

Chairman: Standards SA – SC71K (Autold)

Head of Delegation SA: JTC1/SC31



- Definitions
- What is Digital Evidence
- The Case for Digital Evidence
 - Supply Chain
 - Vehicles
 - Product & Source Authenticity
- The Operational Environment
- Privacy
- Pro's and Con's of RFID
- Encryption
- Conclusion



These definitions is within the scope of the presentation.

- Risk: the chance of a negative outcome towards a material loss
- Integrity: the assurance towards correctness as presented
- Authenticity: the integrity, as a whole, as issued or created
- Authority: the ultimate legal-person responsible
- Confidentiality: a defined limited
- Item: anything, which can be identified uniquely; people...artefact
- People: all humans
- Artefact: all non-human items
- Set: a grouping, which can be identified uniquely
- Real-world: the tangible 3-D world with live in
- Scrutiny: multiple verifications from a different viewpoint

- Digital recording of an occurrence, which can be held in court
 - to a specific risk profile
 - to a deterministic integrity profile
 - Thus the recording and storage method must stand scrutiny before the data can be analysed
- Digital Evidence proves:
 - That a specific Real-World-Occurrence did take place
 - Place, which could included the state of the place
 - Legal entities, both actively participating or not
 - Date & Time
 - Items
 - That a specific Real-World-Item is what it claims to be
 - Integrity of the item
 - Integrity of the source of the item → trail of accountability
- Demographics of digital evidence
 - Usually remote
 - Usually off-line
 - Usually used in local decision making

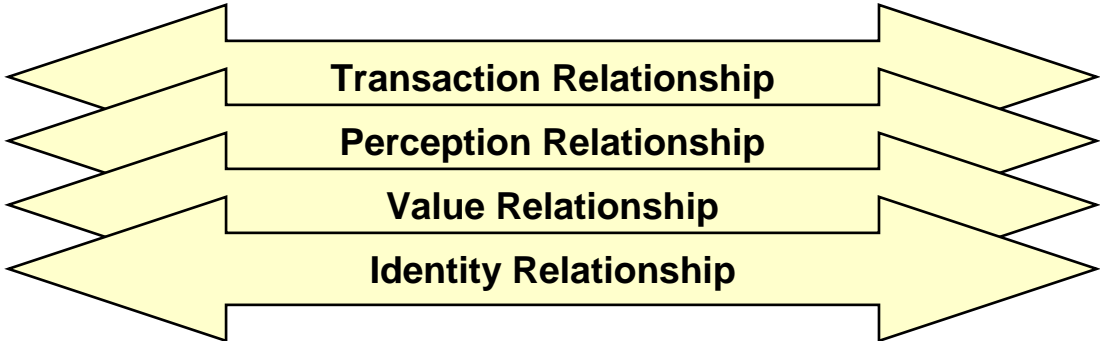
Positive identification of items is the key to digital evidence

Real Item
Person, Article

**Representation
of an item**
Identifier (tag)

Systems
DB, Portals

ICT & Marks

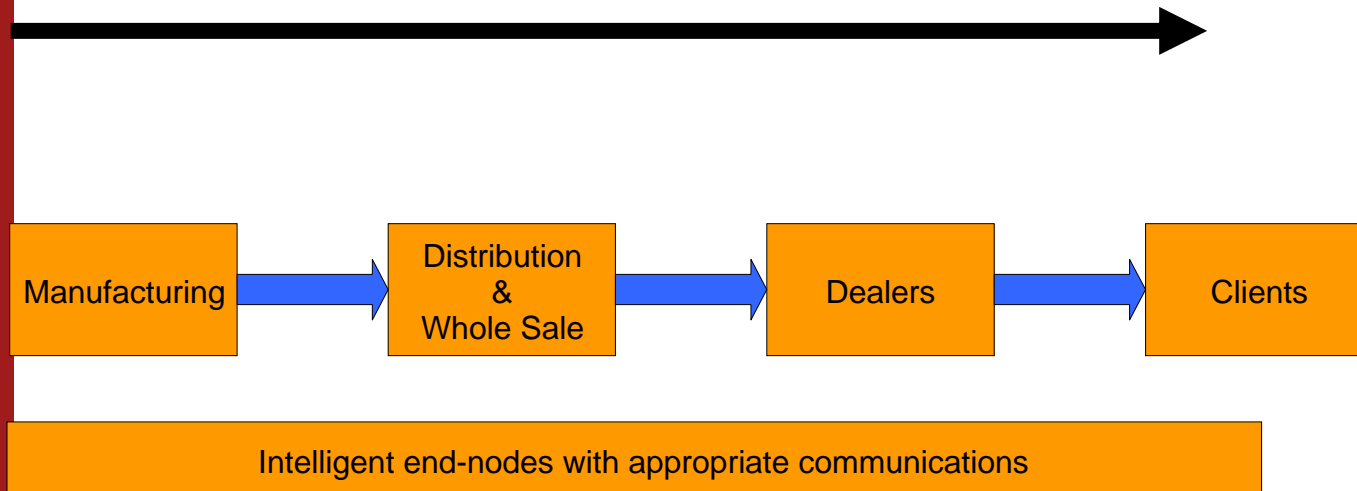


Digital Evidence in the Supply Chain

Brand owner requires control over supply chain activities to

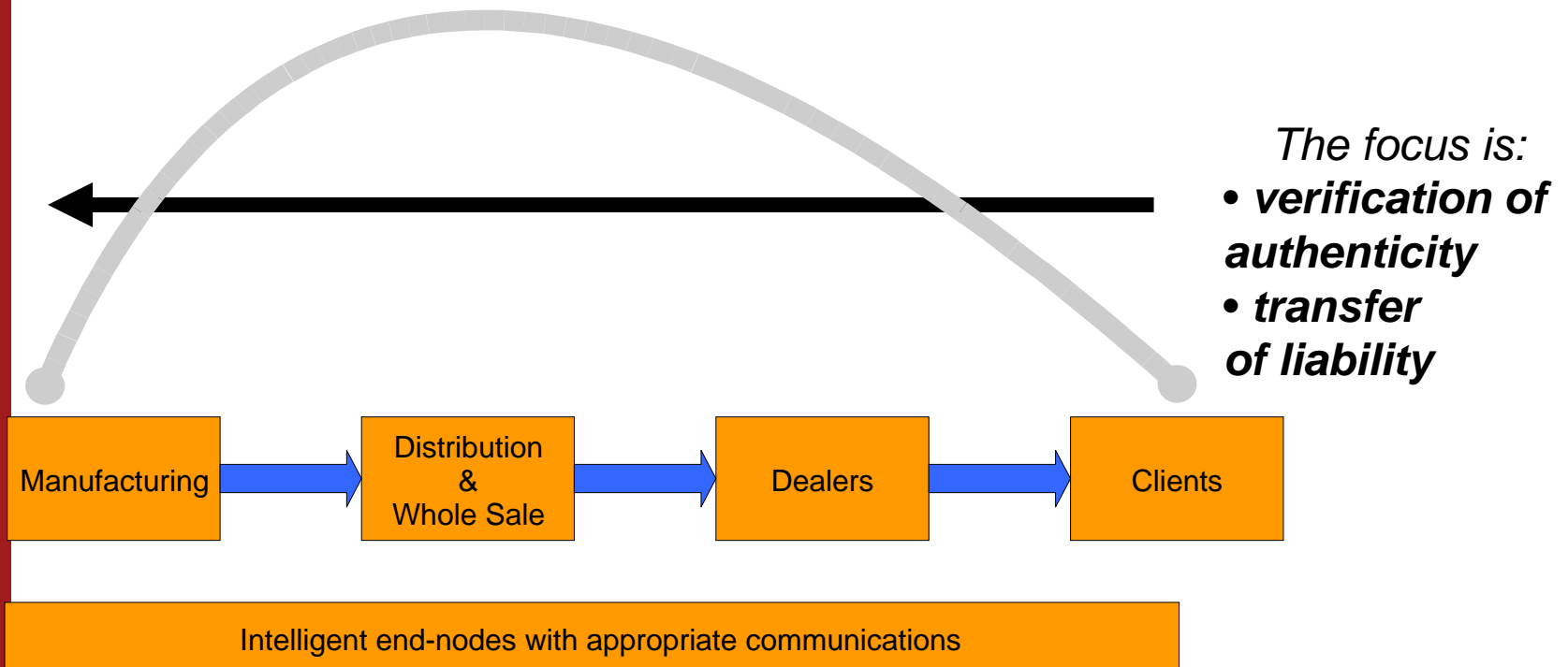
- protect brand integrity
- eliminate counterfeit goods
- prevent illegal trade

*The focus is:
monitoring the
transfer
of goods*

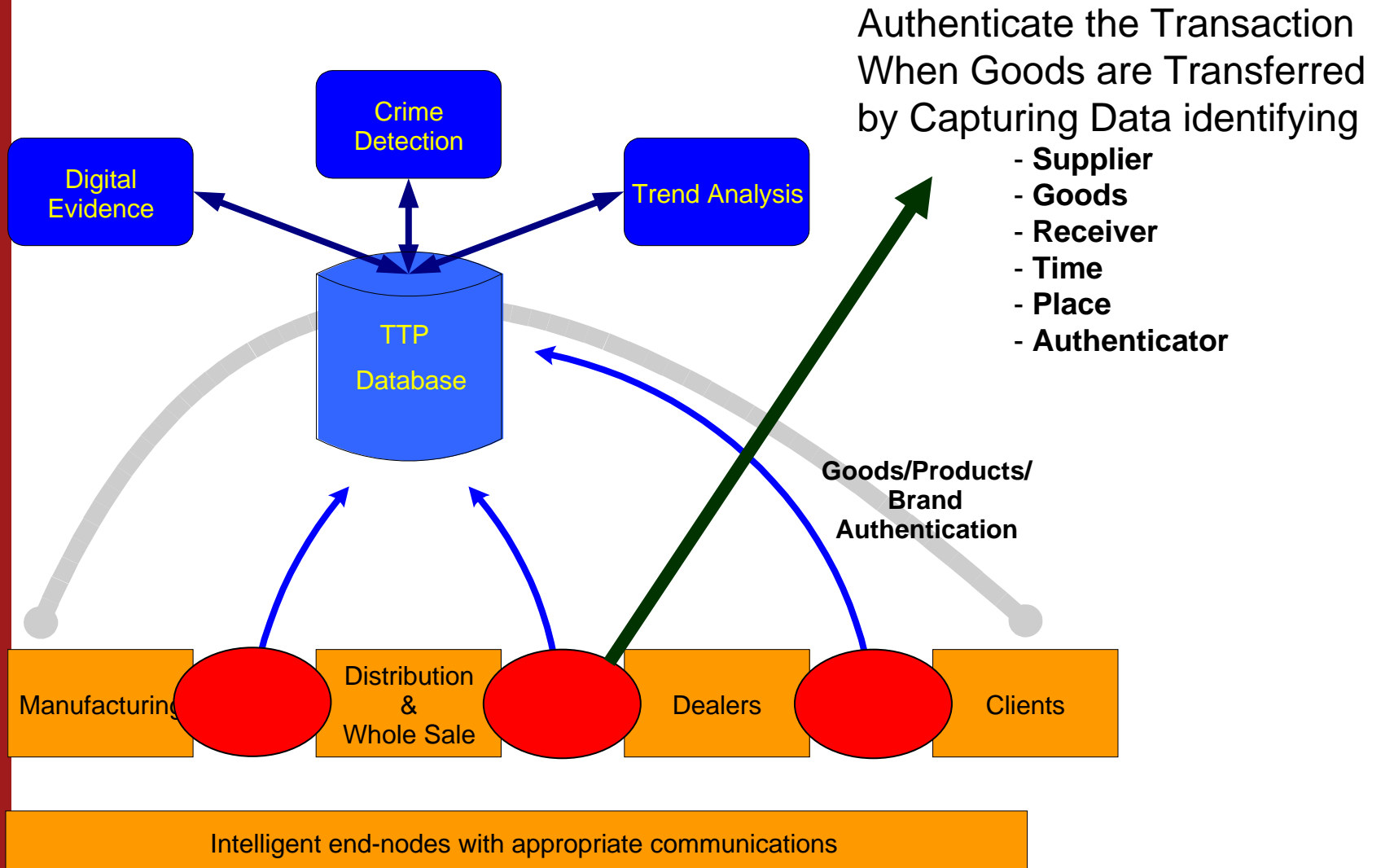


Digital Evidence in the Supply Chain

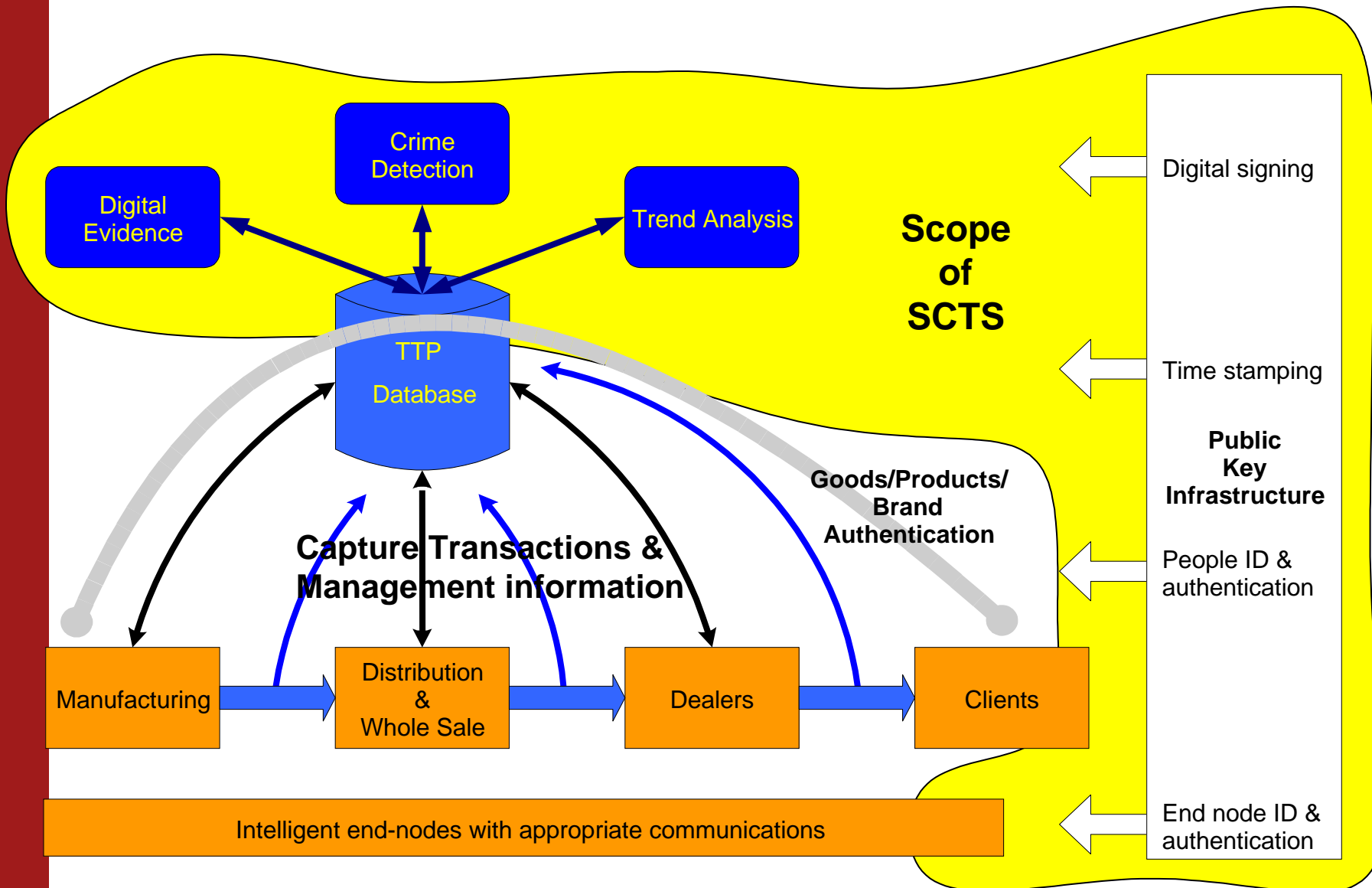
Brand user requires reassurance regarding authenticity of goods
- this must be guaranteed by a Trusted Third Party (TTP)



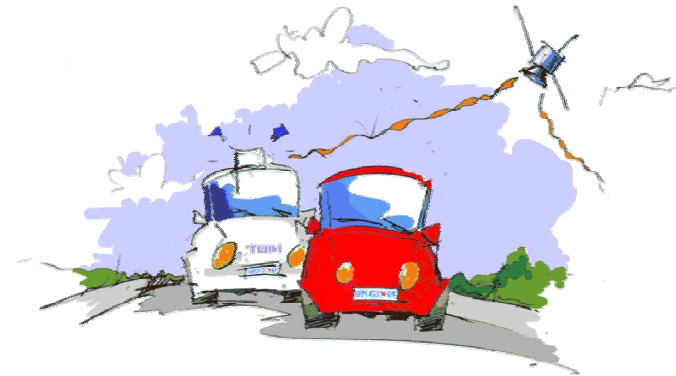
Digital Evidence in the Supply Chain



Digital Evidence in the Supply Chain



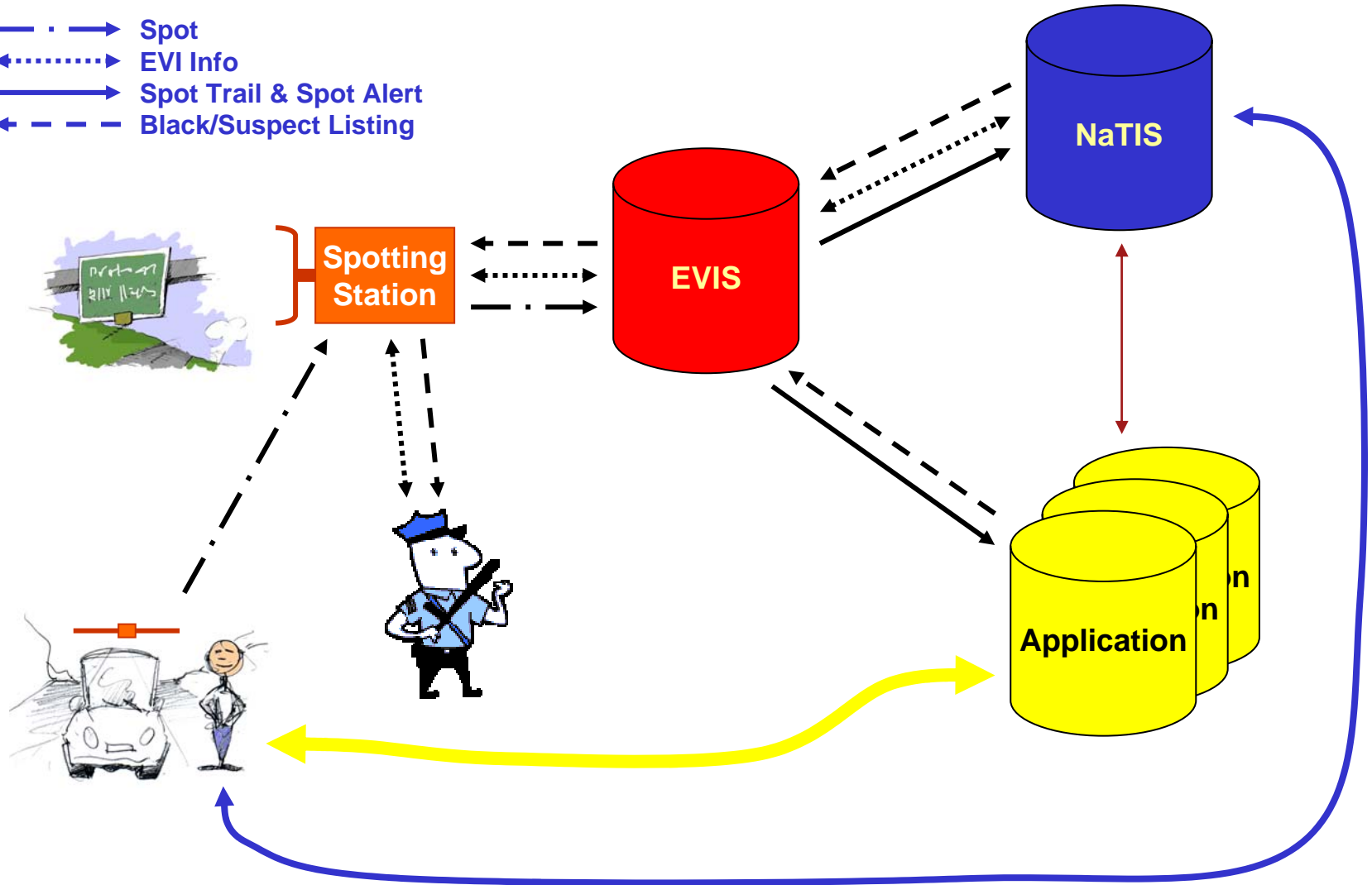
- Basic premises of EVI
 - If all vehicles must carry an Electronic Registration Device [ERD],
 - then the following vehicles are assumed to be illegal,
 - vehicles that does not read (broken or no ERD)
 - vehicles with an ERD that does not match
 - vehicles identified to be illegal (black listed; suspect)
 - vehicles not spotted according to real-world space-time
 - These vehicles, in use, will stand out at the roadside!
- prosecution of the **illegals** without harassment of the **legals** by identification of the **legals** with the **illegals** paying
- EVI is a trust service
 - Providing high integrity vehicle spot-trails
 - On road alerts → black listing
 - Application leverage



Example of an ERD



- · — · → Spot
- ← ······ ← EVI Info
- Spot Trail & Spot Alert
- ← - - - - ← Black/Suspect Listing



- Face value documents
 - Vehicle licenses
 - Certificates and legal documents
 - Way-bills

Note the use of both 2-D barcodes & RFID is applicable
- Proof of source
 - Anti-piracy of products; optical disks, pharmaceuticals, tires, etc.
 - Container seals

Note the potential to control issuing and registration fraud
- Proof of delivery
 - Digital evidence of the right goods at the right person

Note that both the recipient and items can be digitally linked
- Transfer of liability, thus controlling human processes

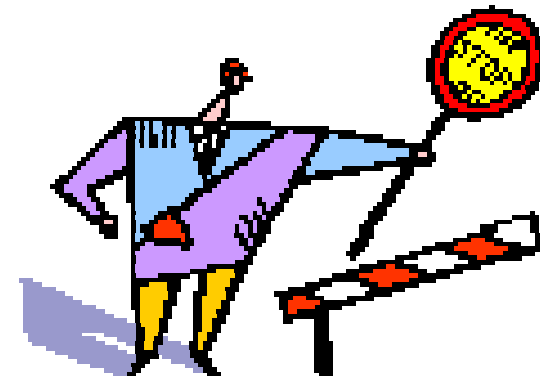
Note in all these cases we only require an end-to-end encryption method

- Electronic suspect selection within process free-flow
 - Suspect lists
 - Contradictory information
 - Real-world anomalies (behavioural scrutiny)
 - “Civil disobedience” *due to a lack of traceability*
- Physical inspection after suspect selection or ad hoc
 - Self inspection
 - Cloning detection
 - Tamper detection
- Digital data & physical verification in gating scenarios
 - Strong digital signatures
 - Item “*finger prints*” or “*DNA*”
- Forensic level verification

Timely detection of breach of integrity is the important aspect

Auto-Identification Requirements

- Spotting of processes in operation
 - Can not stop the process
 - Free-Flow spotting
- Spotting of items, vehicles, people, animals, ect.
 - A large variant on the number of tags in the beam
 - A large variant on the time tags spend in the beam
 - High-speed dynamic populations of tags in the beam
- Deployment cost
 - Re-use infrastructure
 - Optimise networking and data manipulation costs
 - Note that spotting points are often off-line
 - Minimise requirement to change
- Must be used in anti-crime efforts
 - High integrity ChipID for authenticity
 - Supports encrypted code structures

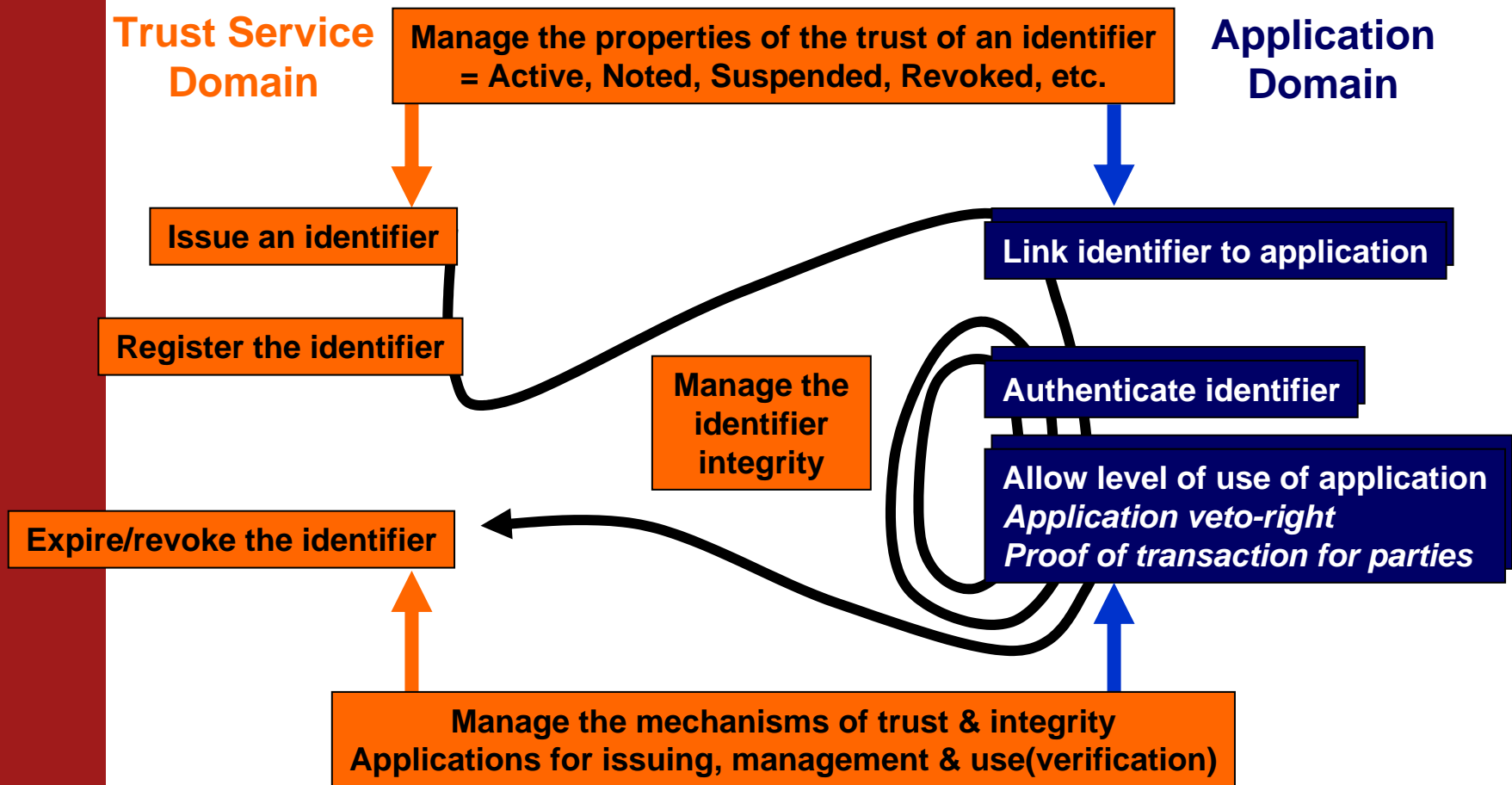


- Various active lobby groups
 - Need to balance the rights of the individual
 - Privacy vs. Protection
 - National security risk perception influence
- RFID threat can be limited by passive technologies
 - limit in range (max 10 meters)
 - line of sight (paint the reader yellow)
 - limit of data transfer (low data rates & storage due to power limit)
 - physical tamper evident
 - clone restrictive
- Data control
 - Effective regulations
 - Effective enforcement of regulations
 - Limited content within single databases.

Assume we deal only with an identifier RFID tag

- Tag must have a unique ChipID
 - allow for item linking to the tag
 - allow for issuing fraud control and detection
- Requires at least 256 bits on tag
 - 64 bits for a ChipID – written by the chip manufacturer
 - this allows for effective control since there are limited chip manufacturers
 - bad chip imitations tend not to work well as passive devices
 - 20 bits for source identity index
 - 172 bits for a ECC short message signature containing an 96bit “EIC”
- Tag needs to be reliably read in 5ms to allow for effective;
 - multi-read
 - free-flow at high speeds
- Requires a cost efficient reader
 - This is a function of the air-protocol (read-only reader)
- Requires the spectrum to allow for high density free-flow tag scrutiny
 - Readers must be co-location & co-channel

Lifecycle of an Identifier



- It is possible to control human behaviour using digital methods
 - without infringing on privacy
 - or stopping processes
 - in creating digital evidence
 - and accountability
- It is possible to verify digital evidence in an off-line manner
- Integrity of identity is the key & the only prerequisite
- RFID can be used to achieve it
 - Requires an unique ChipID
 - Requires short message digital signatures
 - Requires scrutiny
 - Requires cost efficient verification tools (RFID Readers)
 - Requires enough spectrum, which is optimised using Read-Only RFID with non-modulating or Tag-Talk-Only [TTO] RFID readers
- This in all requires a regulatory framework for:
 - the public key infrastructure, which includes encryption methods
 - remote connectivity & data transfer, storage, manipulation & access
 - dedicated spectrum environment



Thank You

i Píco