



Building Radio frequency IDentification solutions for the Global Environment

BRIDGE Webinar – Discovery Services: Design, Security, Integration and Standardisation





Outline

- About BRIDGE
- Discovery Service Design
- Security Framework
- Standardisation activity
- Integration with Track and Trace Applications
- Q&A



BRIDGE in a few words

- A 3 years project
- Started on July 1st 2006
- 30 Partners
- 15 work packages
- Total budget: €13 millions
- European Union funding: € 7,5 millions



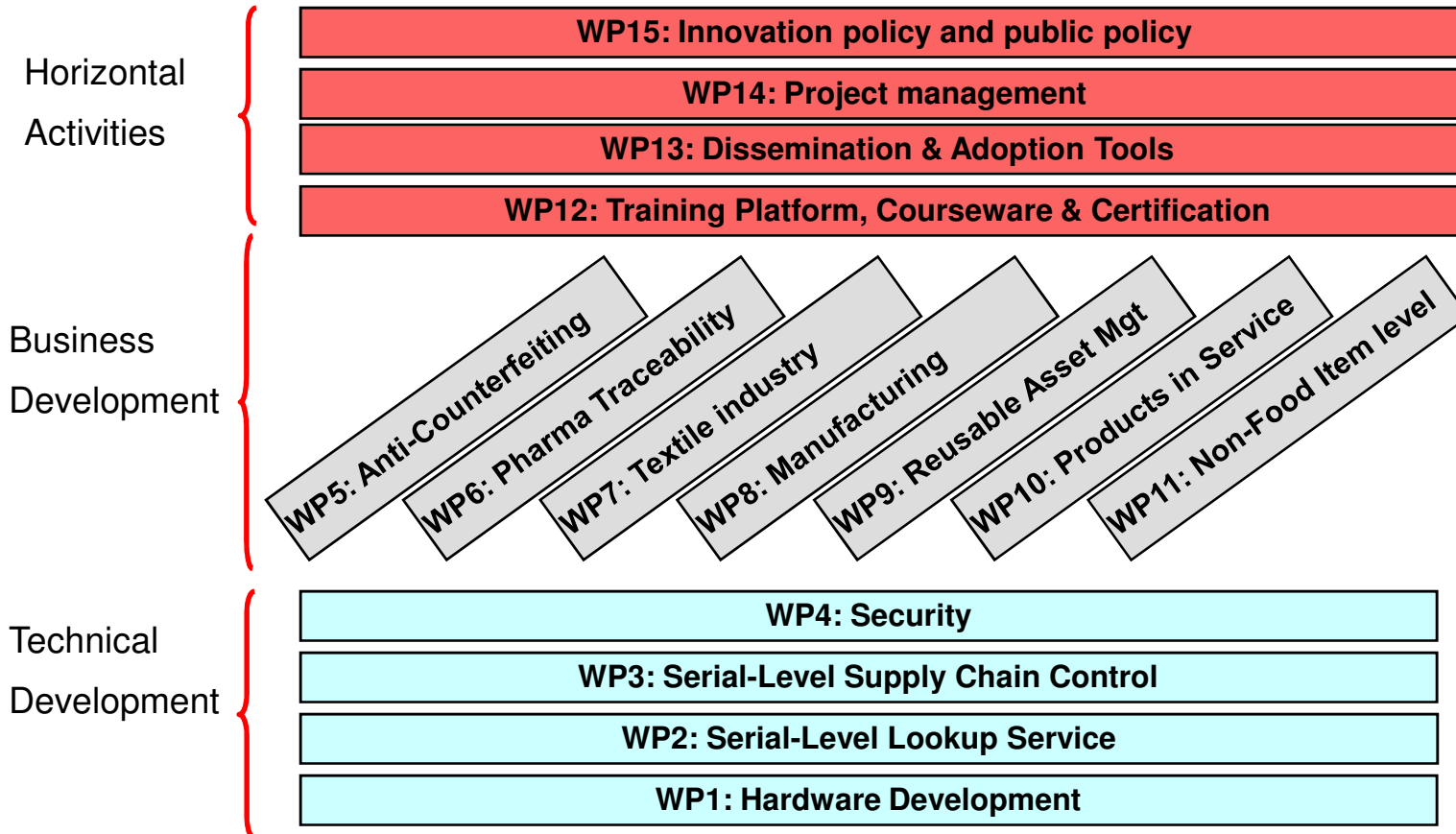
BRIDGE Partners

GS1	Labs/ Universities	End users	Solution Providers
Global Office (Coordinator) China France Germany Poland Spain UK	Cambridge ETH Zürich Fudan TUG Graz UPC Barcelona	Bénédicta Carrefour gardeur Kaufhof Nestlé UK Northland Sony	AIDA Centre AT4 wireless BT CAEN Confidex Domino JJ Associates Melior SAP UPM Raflatac Verisign UK
7	5	7	11





Building Radio frequency Identification solutions for the Global Environment





BRIDGE Discovery Services

Design and Prototype

Miguel Angel Guijarro

Bridge-at4wireless@at4wireless.com

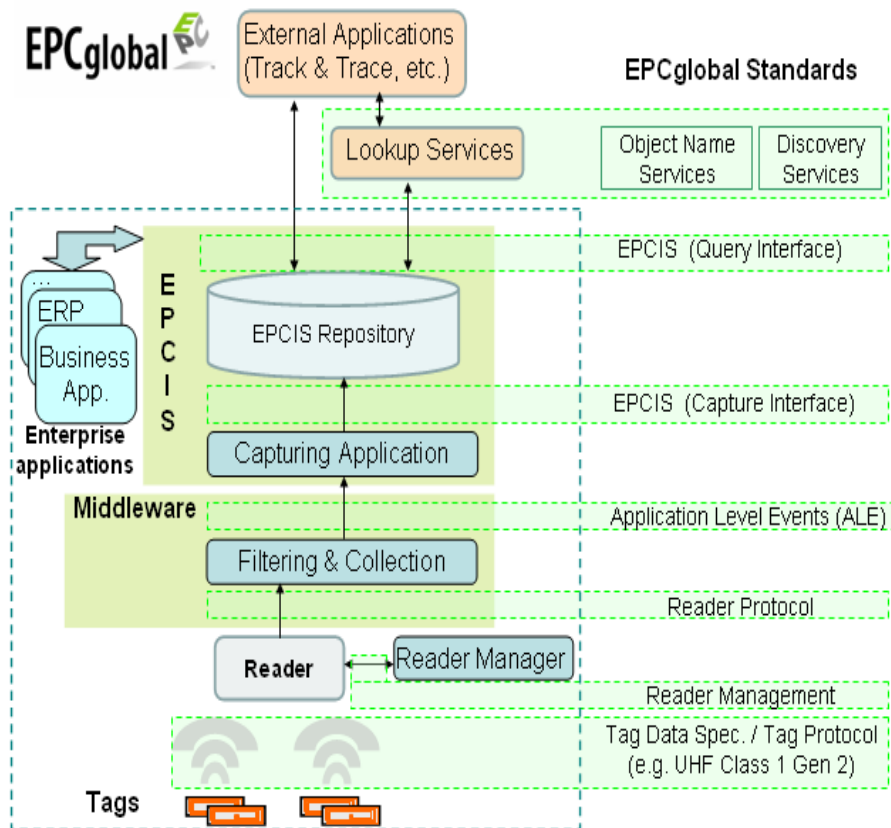
AT4 wireless

21st May 2008





Discovery Service Design: Motivation



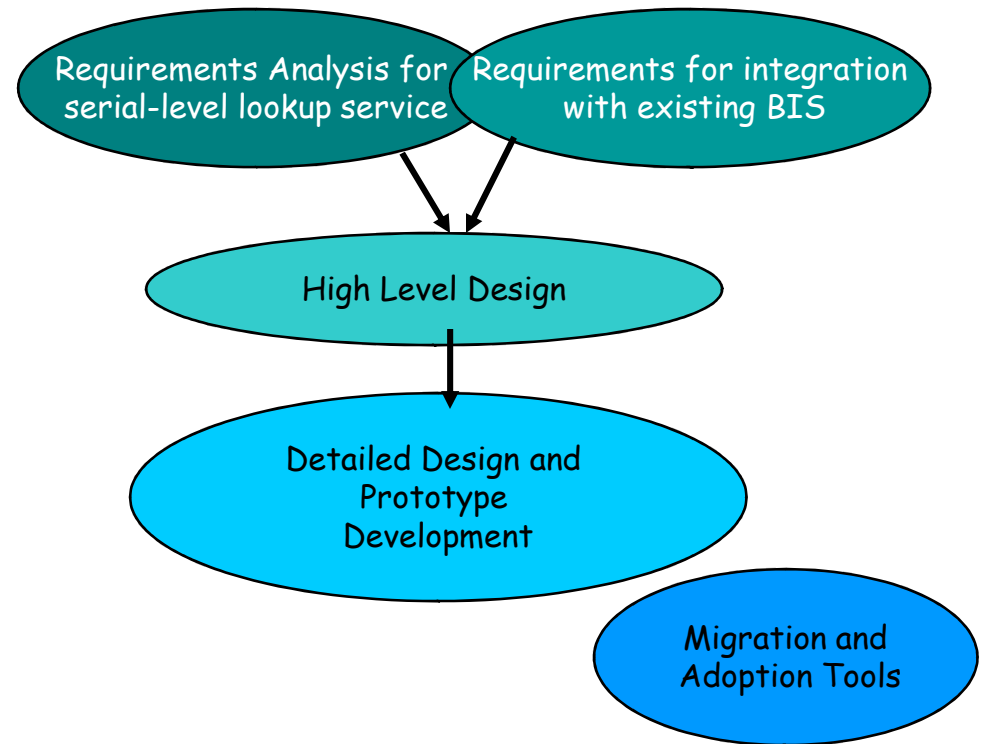
- At the time the project was defined, the EPCglobal ratified ONS standard provided a method for accessing manufacturing information about a product class
- However, there was no standard for finding multiple sources of item-level information
- Serial-level lookup services or Discovery Services were envisaged as the last layer in the EPCglobal architecture
- Also, they were conceived as being complementary to another standard, EPCIS, which was ratified in April 2007





Discovery Service Design: Steps

- 1) Gather Requirements from RFID community with special focus on integration with current IT systems
- 2) Develop a high level design for DS
- 3) Implement a prototype
- 4) Contribute to standardization, promote value of RFID and EPC standards

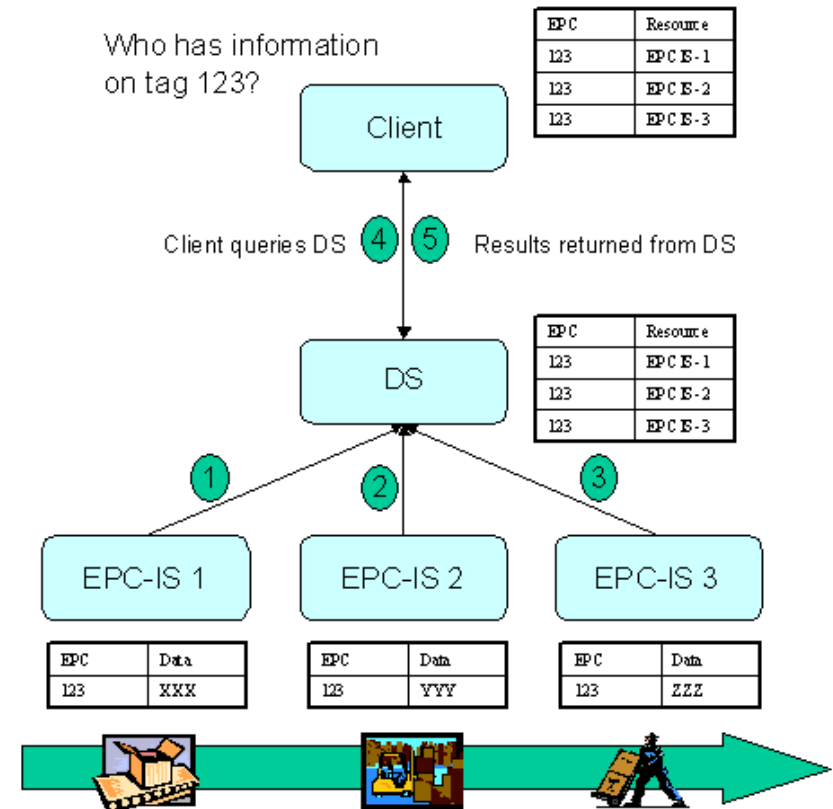




Discovery Service Design: Requirements & Design

Conclusions

- Security and access control policies are key for success of the service
- Design model is
 - Synchronous response to queries
 - Respond with a list of pointers to sources of information (not replication – ownership of data remains in SC companies)
 - Independent of external components and compatible with EPCIS interface standard





Discovery Services

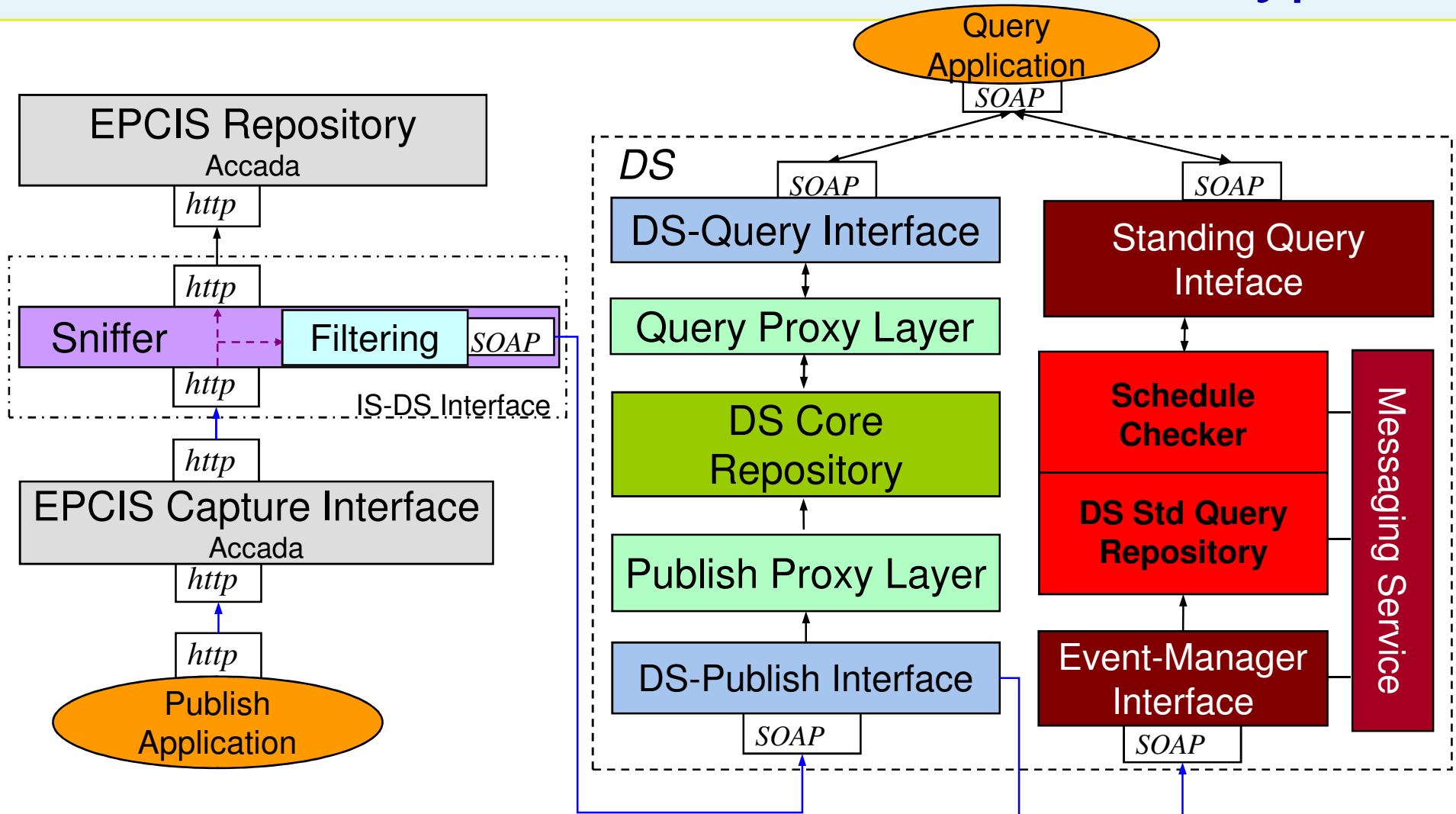
High-level design - key features

- We considered different interaction models between client, Discovery Service and resource - in terms of impact on performance and security (protecting confidentiality of both client and resource)
- Our internal data model borrows some data fields and ideas from EPCIS events - but we don't necessarily return the complete events that were published - just a time-ordered list of links with minimal meta-data. The meta-data in our DS records/events is primarily to provide 'hooks' for defining and enforcing access control policies, so you can say for example "I'll share receipt info with my suppliers - but not with my customers"
- We don't embed URLs within records because URLs can become broken. Instead, we embed the URL in a PublisherProfile and embed its ID within the DS record. If the URL has to change, a new updated PublisherProfile with the same ID can replace the old one, without voiding the DS records.
- We include a serviceType field (like in ONS) to indicate the kind of service to expect at each URL (e.g. EPCIS, DS, web service, HTML, XML)





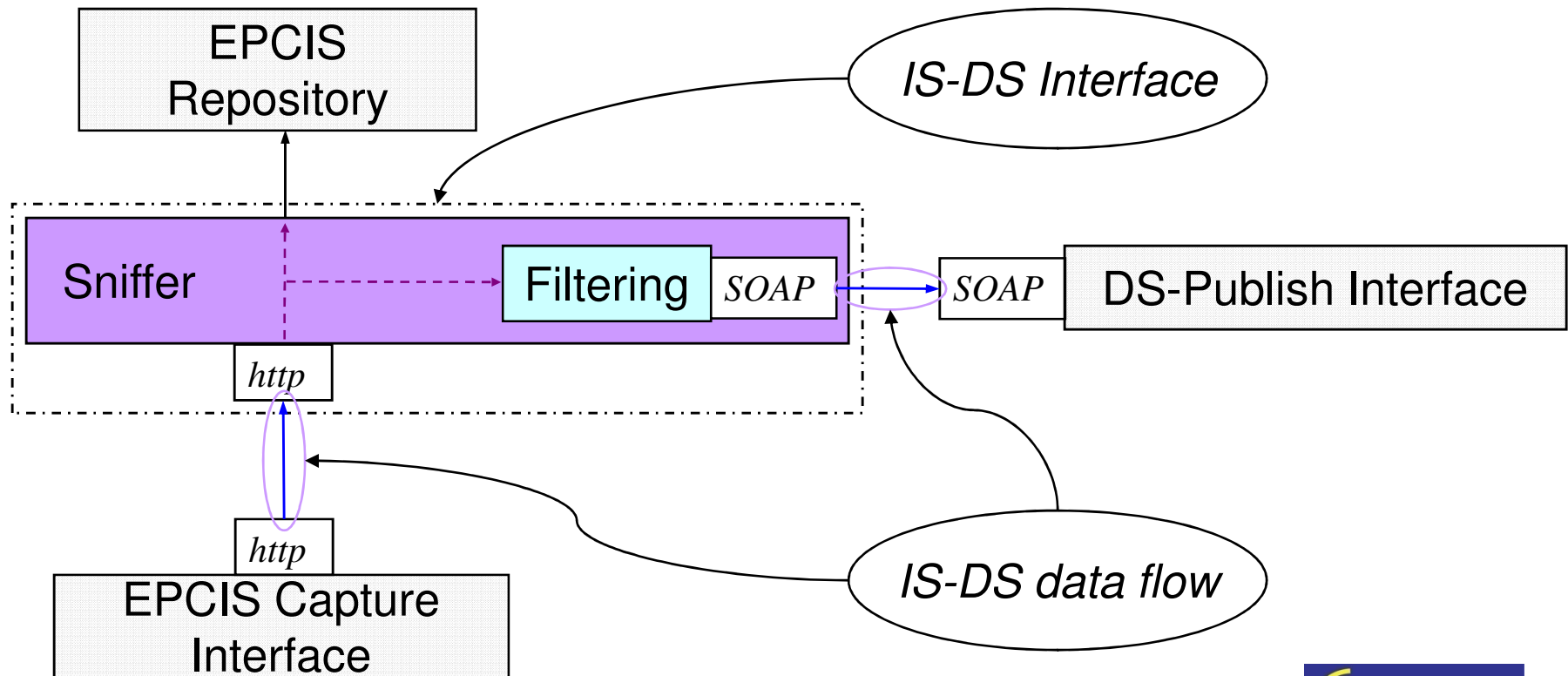
Discovery Service Design: Architecture of Prototype





Discovery Service Design: IS – DS interface

- IS-DS Interface feeds DS repository with relevant filtered data
- IS-DS Interface connects EPCIS and DS and shall be transparent to EPCIS





Discovery Service Design: Conclusions

- Four public deliverables available in www.bridge-project.eu
 - D2.1 Requirements Requirement document of serial-level lookup service for various industries
 - D2.2 Working prototype of serial-level lookup service
 - D2.3 Integration of Serial-level Data into Existing Business Information Systems
 - D2.4 High Level Design
- DS Prototype is made public as LGPL, in addition, service will be hosted along BRIDGE time frame (until June 2009) and is open for use by external parties. DS V2.1.2 is ready since January 2008
- Applications based on Discovery Services could provide following benefits:
 - Traceability of individual items, not only shipments (i.e. saving time and money locating possible faulty products already distributed - i.e. selective recalls)
 - Track and trace throughout the lifecycle of products, not only up to the point of sale
 - Detailed information about all movements along supply chains
 - Detection of potential counterfeiting
 - New services for customers





Discovery Services & Security

Trevor Burbridge
BT Networks Research Centre
21st May 2008

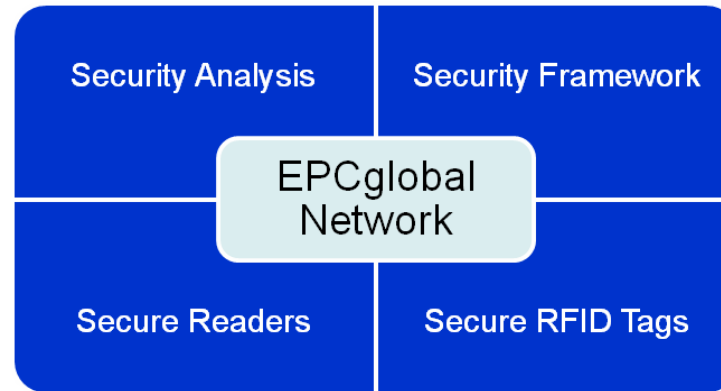




BRIDGE WP4: Security

Security Analysis
to gather end user requirements

Secure Readers
to enable multi-party services



Security Framework
enables data sharing while protecting integrity and confidentiality

Secure Tags protect confidentiality & privacy and enables product authentication

EPCglobal network
enables interoperability across multiple locations

- WP4 lead: 
- WP4 members:   
     





Starting Design Principles

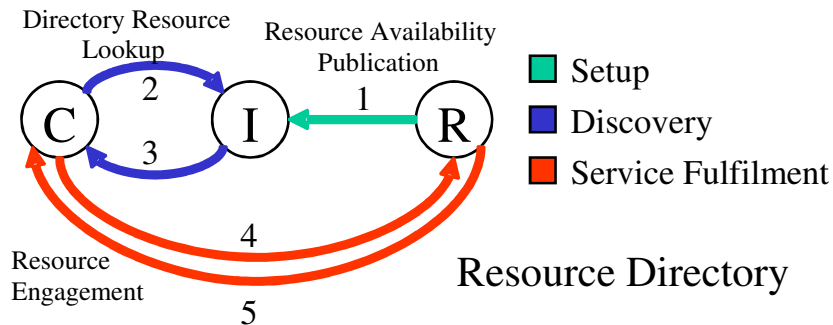
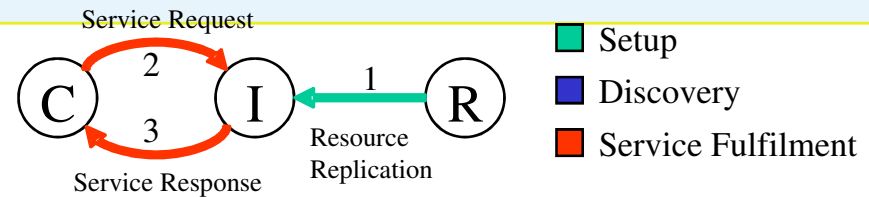
- Publishers continue to own their data
- Discovery Service can enforce some community behaviour
- Clients require confidentiality
- Choice of Discovery Service(s)
- No enforced network routing path or data hosting location (e.g. ONS)
- Autonomous domain instead of unified inter-network
 - No clear requirement (can reach multiple autonomous DSs), security harder (propagation of security policies)
- Lightweight & scalable (do not replicate EPCIS roles)



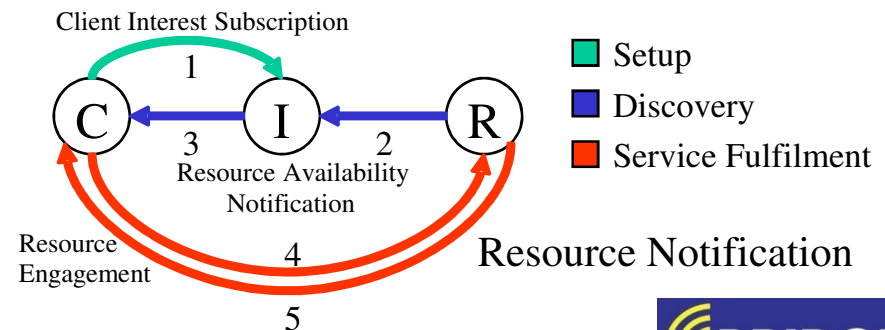
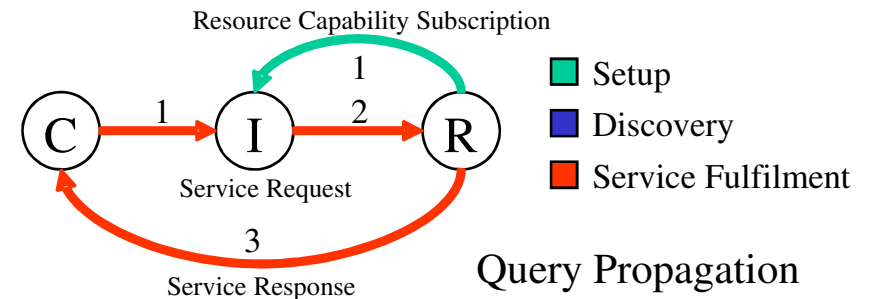


Communication Models

- Can characterise by:
 - Push vs. pull (two links)
 - Data vs. reference
 - Needs vs. resources



Protects both client and publisher confidentiality





Approach to Security

- Use existing standards
 - RFID services not operated in isolation
- Build flexible access control technology substrate
 - Data, service logic and security policy separated
- Work with business to identify real uses/requirements and security policies
- Narrow and optimise enforcement technology
- Provide management tools and policy automation



Security Design

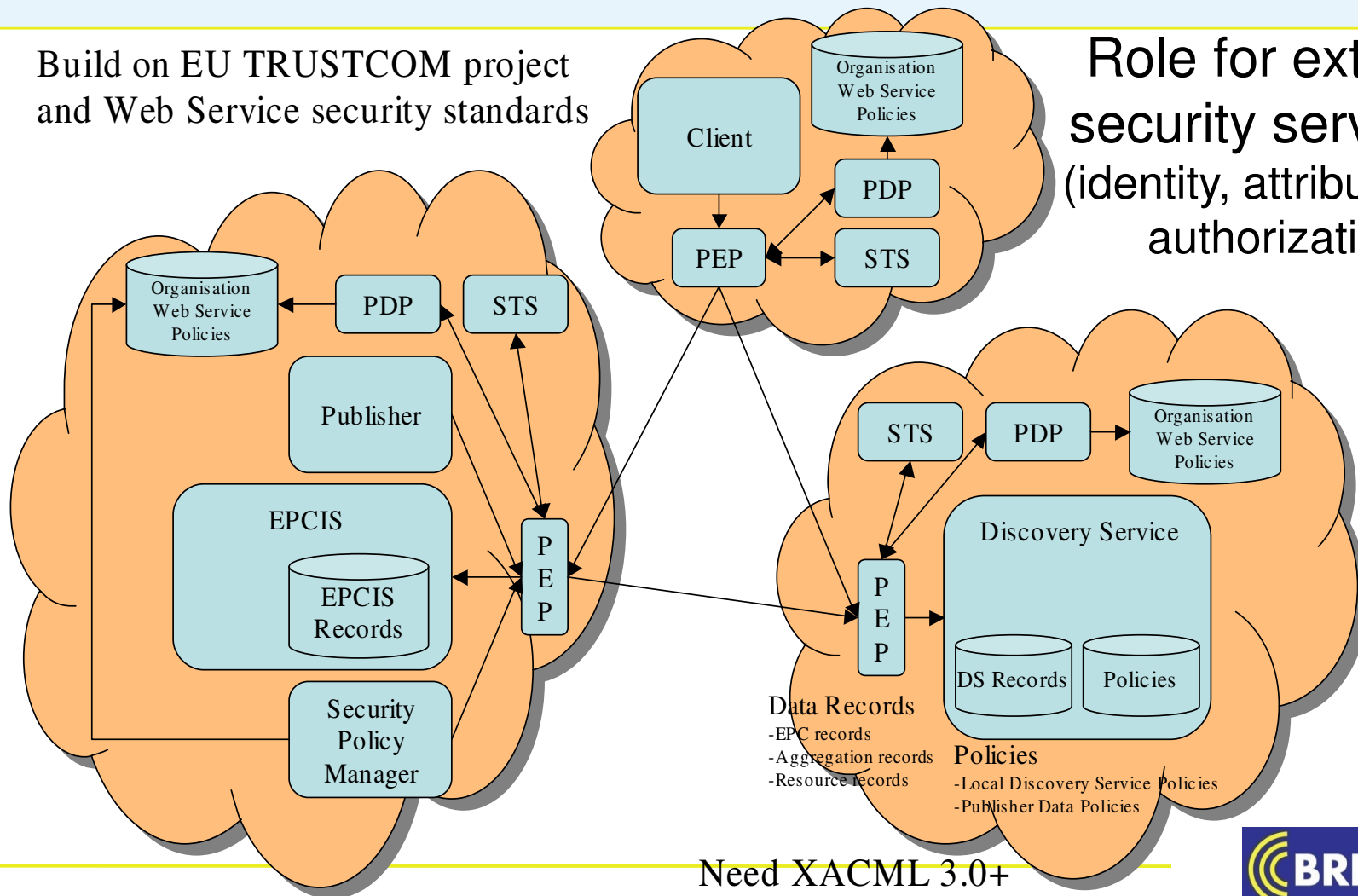
- Consider: Authentication, Authorisation, Access Control, Confidentiality, Integrity, Non-Repudiation, Availability, Accountability/Audit
- **Access control** is the largest outstanding problem for the Discovery Service (due to multi-ownership of data and granular access requirements)
- In Resource Directory model access control policies can be considered as a subset of the EPCIS policy
- Access control of reading/writing/deleting records (EPC, aggregation, resources) and policies
- Need to manage EPCIS/DS and other (partners!) policies together to avoid conflicts



Security Framework

Build on EU TRUSTCOM project and Web Service security standards

Role for external security services?
(identity, attribute/role, authorization)



Need XACML 3.0+

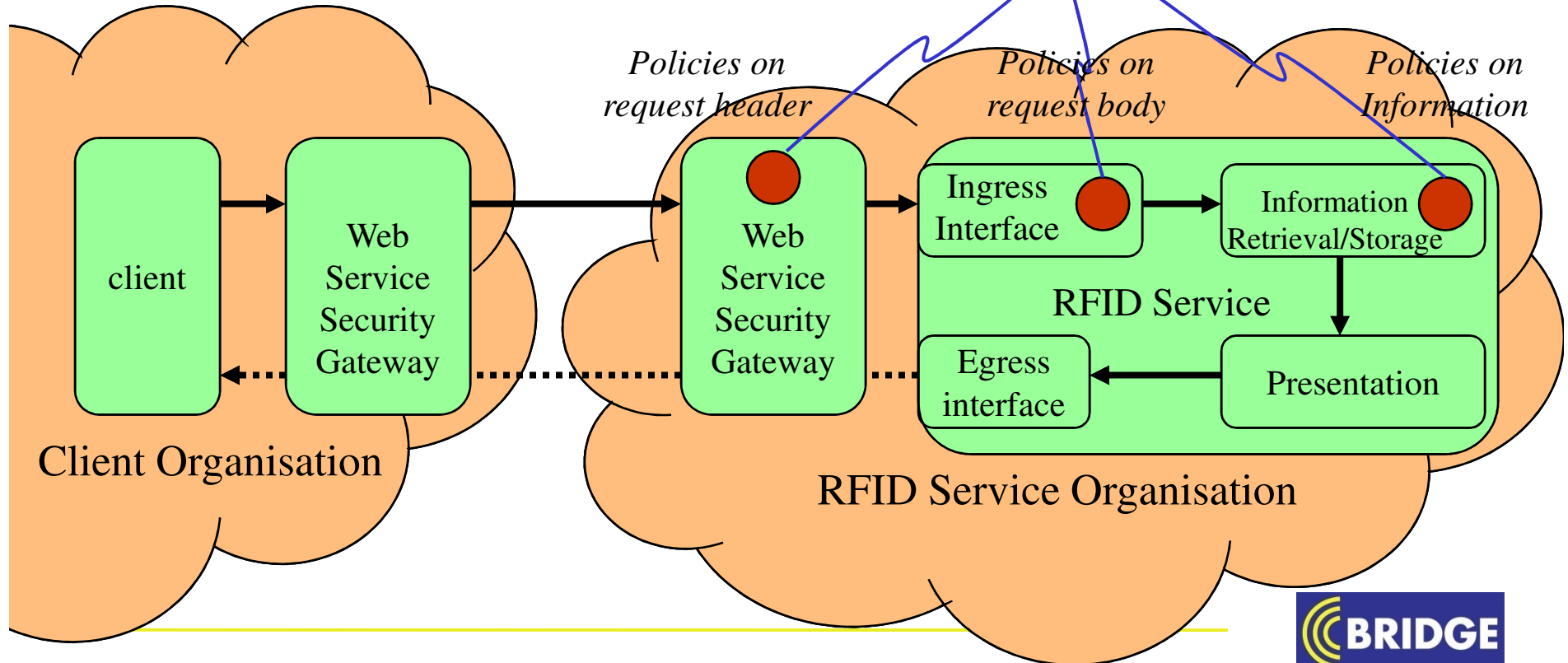




Enforcement Points

Modification of query at ingress not feasible due to potential large number of applicable policies

Main Access Control Enforcement Options for RFID Service





Policy Capabilities

- Publisher Control
- Mandated Community Policies
- Group Separation (of Publishing)
 - Achieve groups through policies rather than separation of data at publishing
- Emergency Policies
 - Assertion of supply chain events e.g. product recall
- Delegation
 - Ability to delegate management without access?
 - Delegation through assertions or policies?



Policy Attributes

- **Subject**
 - Identity, role, group, organisation, country?
- **Context**
 - Supply chain event, load, query time/date?
- **Resource**
 - EPC, bizStep, disposition, record time/date?



Further Security Questions

- Data retention
 - Delete and/or void action (can have both and restrict DS instance using security policies)
 - If preventing deletion, also need to prevent removal of access rights!
- Introduction of unknown parties
 - Permit/deny/introduce policy evaluation
- DS as Authorisation Authority (single sign-on)
- Semantic policy languages
 - E.g. “customers who purchased an item”
- Automated policy distribution (EPCIS publisher extension?)



BRIDGE contributions to standardization activities

Mark Harrison

Auto-ID Lab, University of Cambridge

21st May 2008



UNIVERSITY OF
CAMBRIDGE





BRIDGE contributions to DS standardization activities

- Members of BRIDGE WP2,3,4 have been actively participating in activities towards standardization at EPCglobal and also within the IETF and have contributed public deliverables from WP2 to both activities.
- The EPCglobal Data Discovery JRG is gathering use cases and analyzing these to extract technical & security requirements.
- The ESDS activity aims to develop a generic protocol for handling dynamic referrals, which can be used for Discovery Services in supply chains / product lifecycle, as well as for other purposes.
- We are trying to help ensure that there is good communication between these two activities, to minimize duplication of effort and divergence - and to try to ensure that work on an ESDS protocol within IETF considers requirements from EPCglobal and aims to provide something useful that can be further developed by an EPCglobal technical work group in the future.





BRIDGE contributions to EPCglobal Data Discovery JRG

- In the EPCglobal Data Discovery JRG, members of BRIDGE WP2 compiled a detailed questionnaire that has been refined by the DD JRG group and is being used as the basis for analysis of use cases from end-users, in order to extract technical, performance and security requirements.
- We join the bi-weekly DD JRG calls and try to ask relevant questions and provide clarifications where needed.



BRIDGE contributions to ESDS@IETF.org

- In April 2007, while we were nearing the end of the BRIDGE high-level design task, Michael Young and Frank Thompson (Afilias) published three internet drafts concerning a draft protocol for Extensible Supply Chain Discovery Services (ESDS).
- Via face-to-face meetings and discussion on the ESDS mailing list (esds@ietf.org), we have contributed feedback on their internet drafts, posted the BRIDGE requirements documents and high-level design documents to the mailing list and (together with Frank Thompson) begun a comparison between their draft protocol and the BRIDGE high-level design work.
- BRIDGE D2.2 appendix has a table comparing the two designs.
- Feedback from BRIDGE has already resulted in some revisions of the ESDS draft documents
- Mark Harrison (WP3 lead, WP2 member) co-chaired the first ESDS 'Birds of a Feather' kick-off meeting at the 71st IETF meeting, in Philadelphia, March 2008.





Beyond Discovery Services: a framework for enhanced track & trace

Mark Harrison

Auto-ID Lab, University of Cambridge

21st May 2008



UNIVERSITY OF
CAMBRIDGE





WP3 Serial-level supply chain control / Framework for enhanced track & trace

Main objective: Gather event data from across the supply chain / product lifecycle, analyse it, and enhance business processes and decision-making ability

Develop 'tracking model' algorithms to be able to:

- estimate the location of products in the supply chain
- analyse delays or deviations from expected routes
- predict when/where objects will be seen next

Leader:

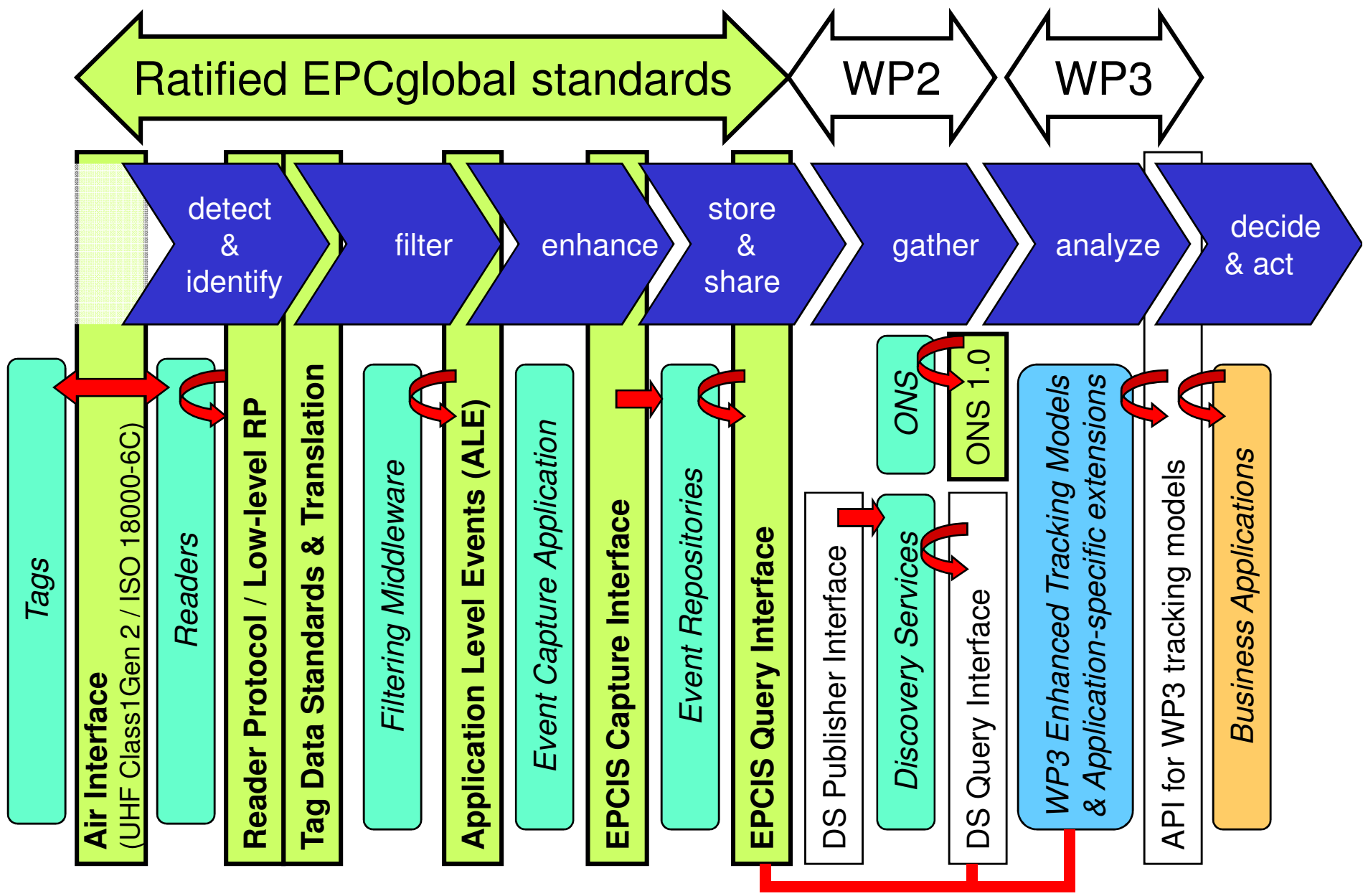


**UNIVERSITY OF
CAMBRIDGE**

Partners:



EPC Network architecture - with extensions by





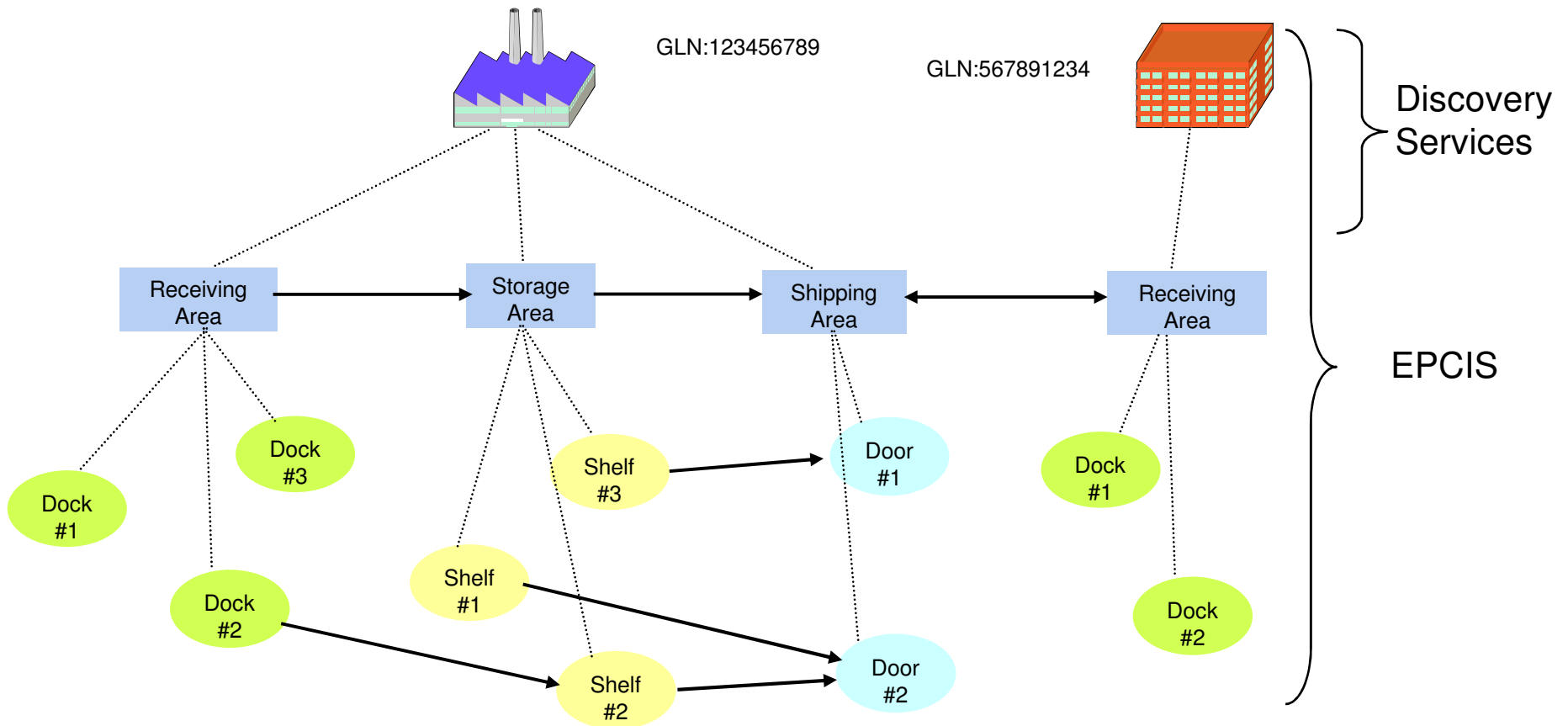
BRIDGE WP3 (Enhanced Track & Trace)

- Cambridge Auto-ID Lab led task 3.1
 - Serial-level Inventory Control model
 - Gathering of event data from across supply chain (via Discovery Services and EPC Information Services)
 - Supply chain network modeling (as hierarchy of nodes)
 - Use of probabilistic algorithms and first-order Markov models to 'learn and predict' the movement of objects
- Technical details reported in public document D3.1 (see BRIDGE website <http://www.bridge-project.eu>)
- Currently involved in collaborative development (together with BT and SAP) of an extensible software prototype to support various pilot and trial activities in various industry sectors across the BRIDGE project



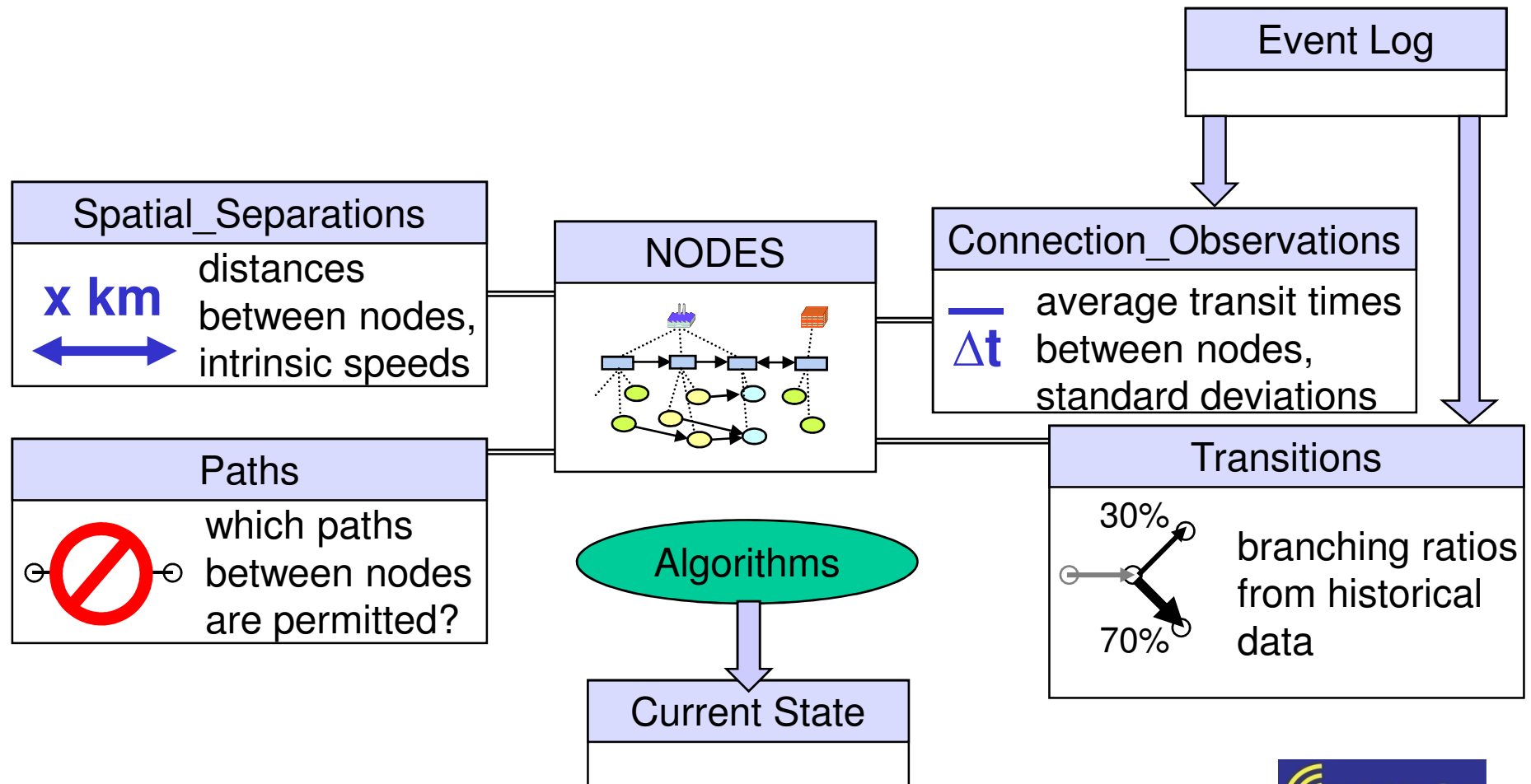


Supply Chain Network Model





Overview of database design





Non-probabilistic query methods

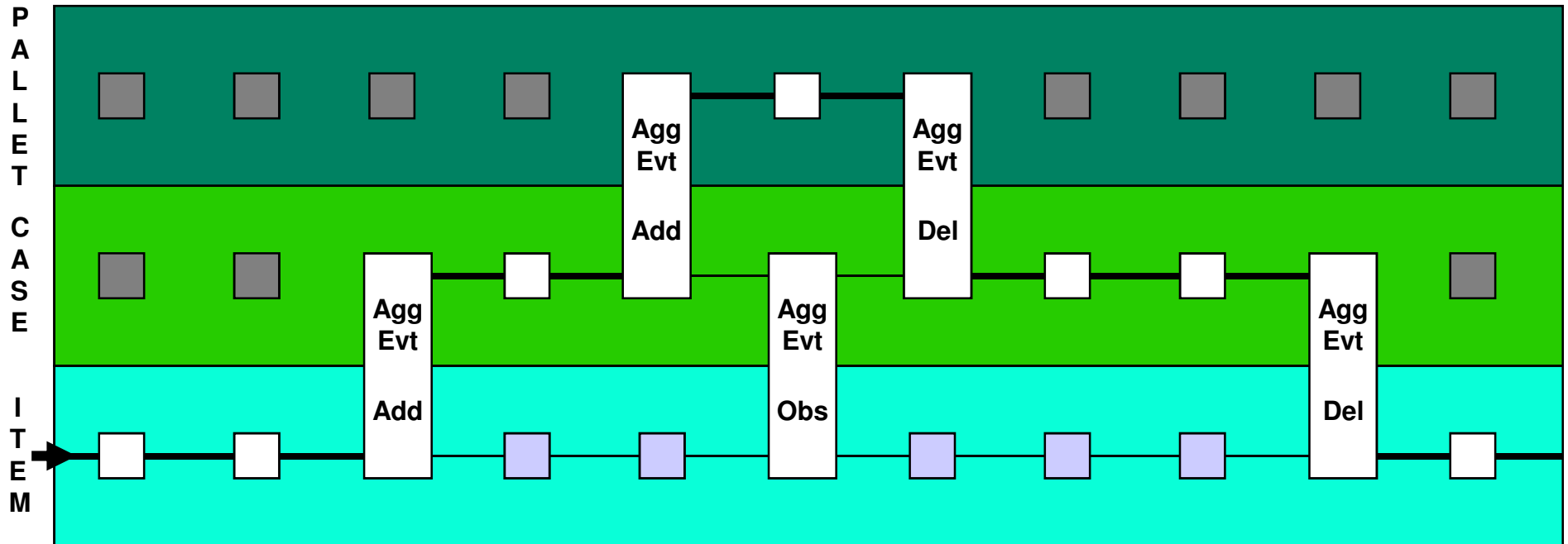
- **Where was it last observed? (tracking)**
- **Where are all the places it was observed? (trace)**

Additional complications: changes of aggregation happen!

- **Items packed into cases, cases loaded onto pallets, pallets form shipments / are loaded into containers**
- **Components being assembled into composite products**
- **Disaggregation - unloading, disassembly, break down of bulk products into smaller units (e.g. for retail)**



Following changes of aggregation



Item packed into case
Need to track case ID

Case removed from pallet
Need to track case ID

Case packed onto pallet
Need to track pallet ID

Item removed from case
Resume tracking item ID

time →

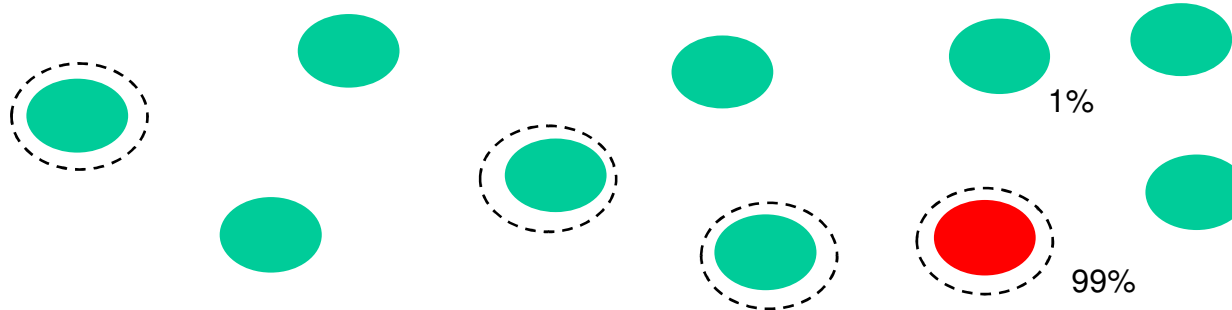




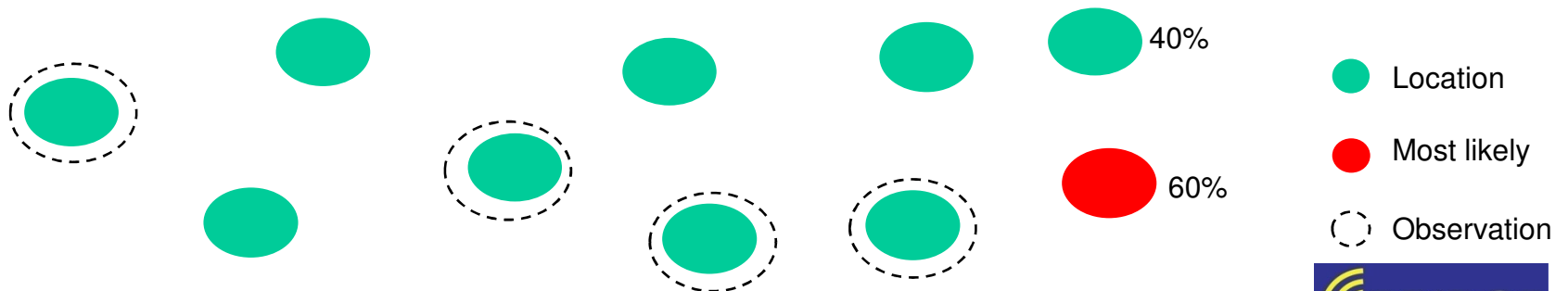
Probabilistic algorithms: Filling in the 'gaps'

Probabilistic reasoning enables:

- Filtering: **Where is it?** Estimate current location given observations so far



- Prediction: **Where will it be next?** Estimate future location given observations so far



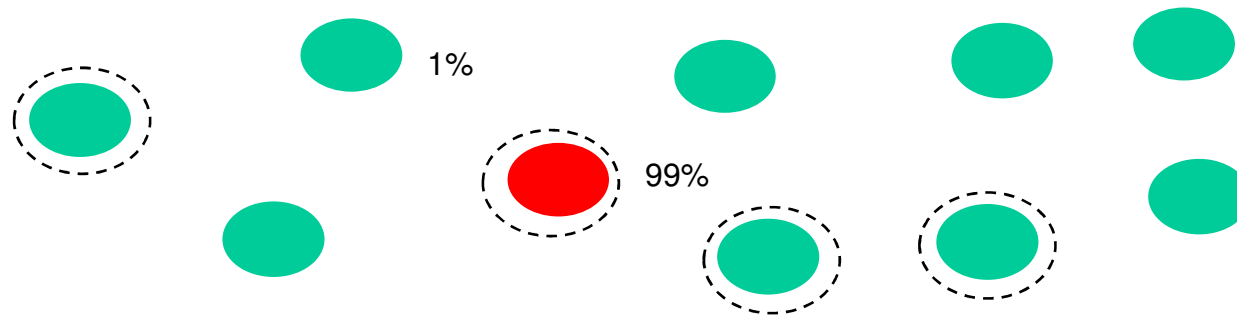
- Location
- Most likely
- Observation



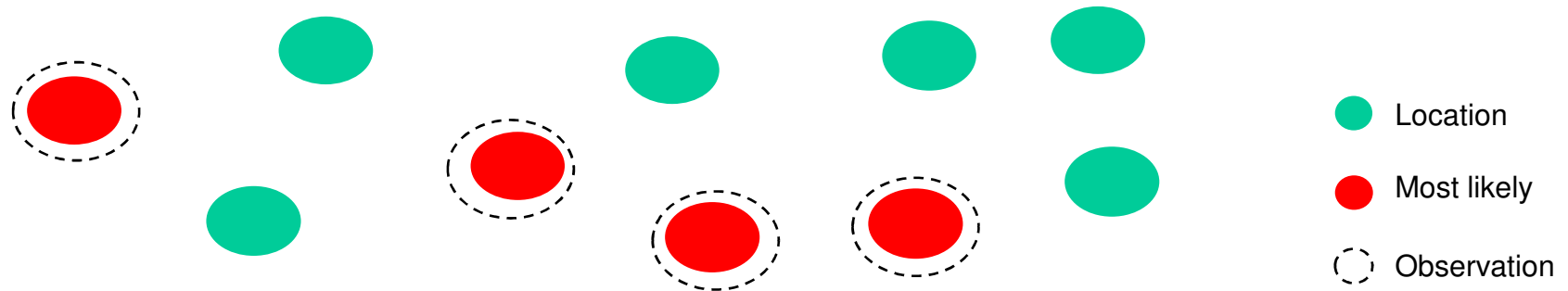


Probabilistic algorithms: Filling in the 'gaps'

- Smoothing: **Where has it been?** Estimate past location given observations so far

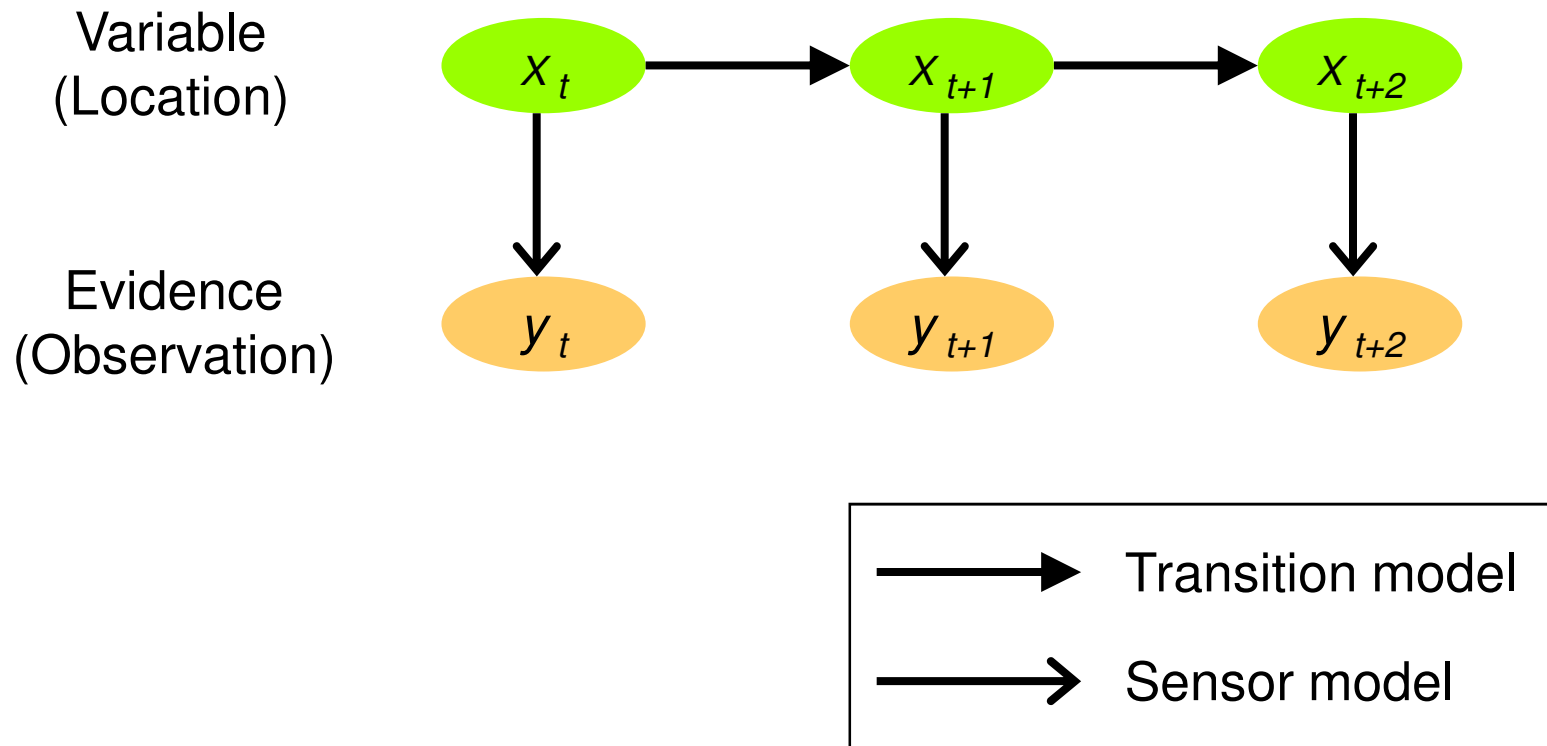


- **Where did it go through?** Estimate the most likely path that an item has followed given observations so far



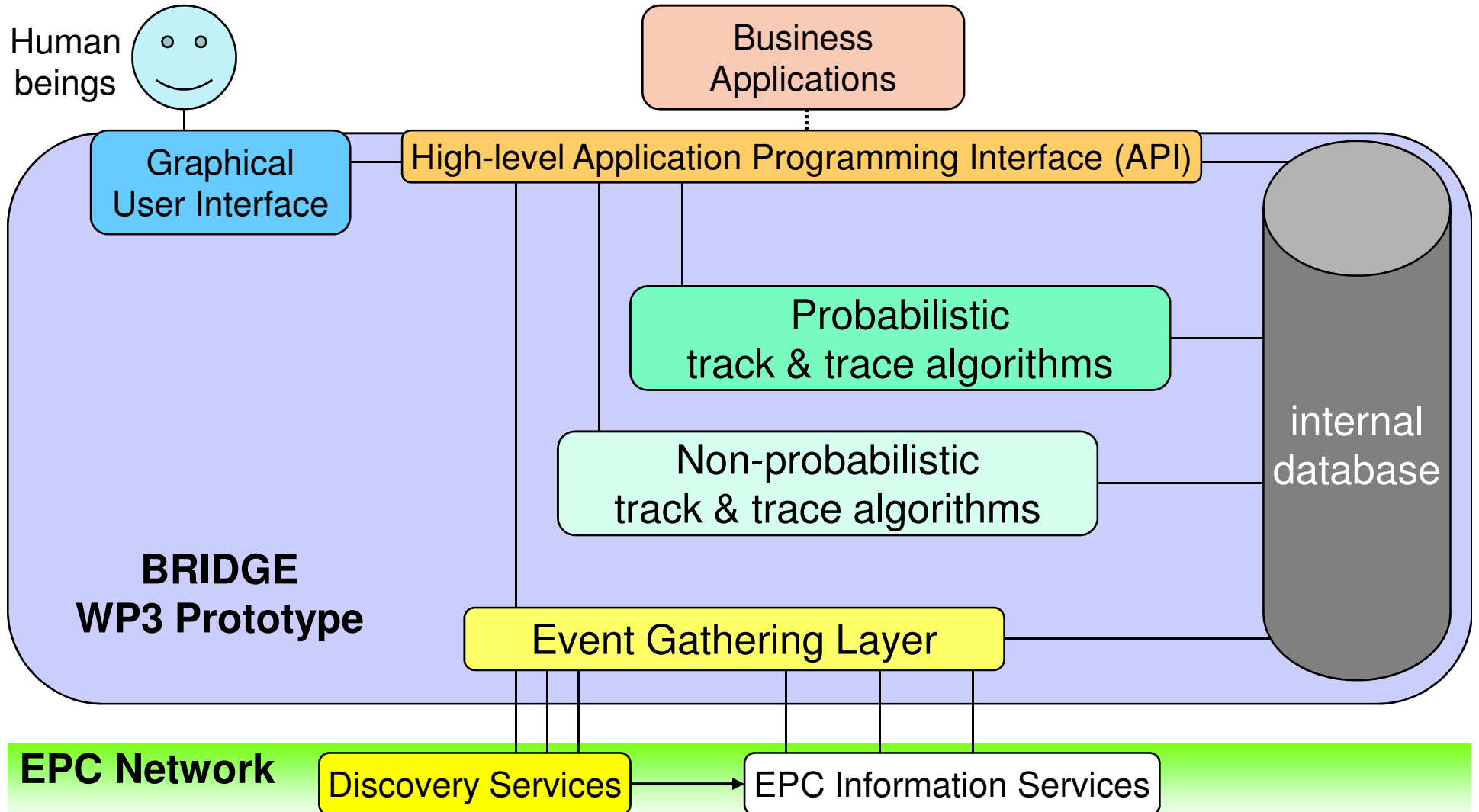


Probabilistic algorithms: Models and Algorithms





WP3 software prototype for enhanced serial-level track & trace

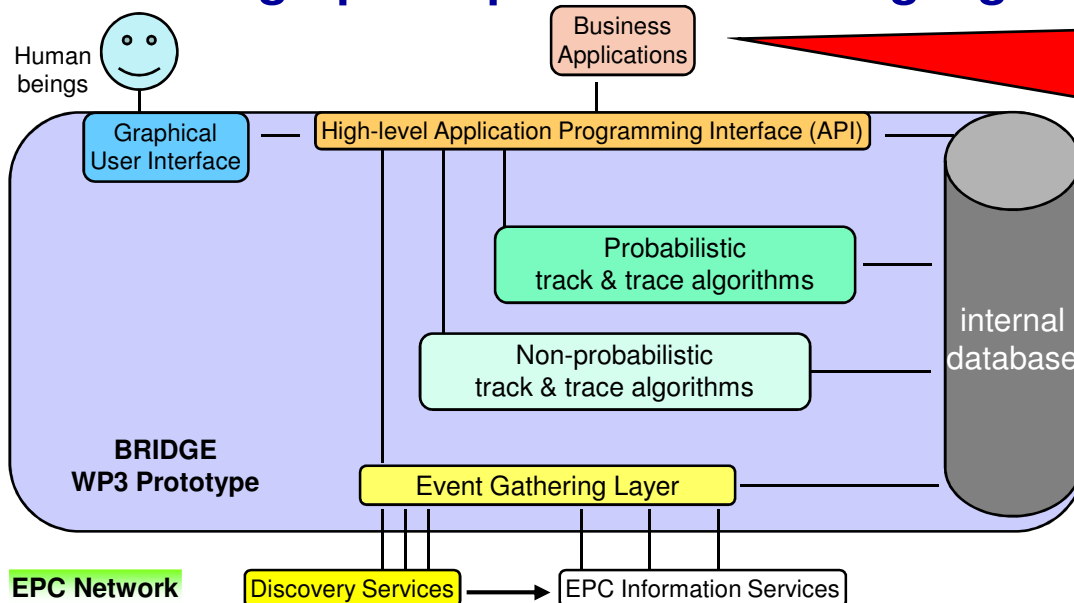




Application Programming Interface

Goal: Interface to WP3's Tracking Infrastructure

- support wide range of **business applications**
- **expose tracking model** through API and convenience functions
- exception handling & alerting
- trigger event collection from distributed sources
- choreograph sequence of tracking algorithms



Targeted Recall,
Diversion, Shrinkage,
Lost & Found,
Asset Tracking,
Condition Monitoring,
Reconciliation, ...





WP3 software will be able to answer the following:

- Where was the object observed?
(including tracking of parent(s) or children as necessary)
- Where is it likely to be now?
- What is the probability that the object will arrive at location X by time T?
- After how much elapsed time is the probability of arriving at location X greater than threshold probability P?
- Which path is the object likely to have taken?
- Alert me if my shipment is likely to arrive late at its destination
- Alert me to where delays are happening in the supply chain
- Alert me to inconsistencies (e.g. duplicate IDs at distant locations, similar times)
- Alert me to deviations from permitted paths (including 'insertions')





Contact us

- **BRIDGE Project Website:** <http://www.bridge-project.eu>

Email : info@bridge-project.eu

- **Presenters**

Henri Barthel, BRIDGE Project coordinator

henri.barthel@gs1.org

Miguel Angel Guijarro, AT4 wireless, WP2 Leader:

Bridge-at4wireless@at4wireless.com

Mark Harrison, Cambridge University, WP3 Leader:

mark.harrison@cantab.net

Trevor Burbridge, BT, WP4 Leader

trevor.burbridge@bt.com

