

Onion Routing in Peer-to-Peer Networks for Co-operative Business: the ATHENA Project

Gerd Völksen
Siemens Corporate Technology
Munich, Germany
gerd.voelksen@siemens.com
www.ct.siemens.com



Content

- ATHENA Overview

- Onion Routing in Peer-to-Peer Networks for Business Processes
 - Business Scenario
 - Peer-to-Peer-based Business Process Enactment
 - Security Threat
 - Onion Routing
 - Results

- Future Work

ATHENA Overview: Vision and Mission



ATHENA builds upon the following Vision statement:

“By 2010, enterprises will be able to seamlessly interoperate with others.”

Following this vision statement, ATHENA's Mission is consequently:

“To be a main contributor in the European efforts to enabling enterprises to seamlessly interoperate.”

ATHENA Overview: Organizational Aspects

ATHENA is NOT a project, it's a PROGRAMME
FP 6, IST 507849, → www.athena-ip.org

Duration: February 2004 – January / March 2007

ATHENA is funded by the European Union

Total costs: ~ 26 M€

Funding: ~ 14 M€

Efforts: ~ 166 PY

Partners: SAP (Lead), AIDIMA, CNR-IASI, DFKI, EADS, ESI, FHG IPK, Fiat, Graisoft/ITREC, Gruppo Formula, IBM, IC Focus, INSEAD, Intracom, Siemens, TXT e-solutions, Uninova, University of Bordeaux, **Non-EU partners:** Computas/Troux/AKM, Sintef, University of St. Gallen, **Associated partners:** NIST, OAGI

A total of **23** partners

ATHENA Overview: Organizational Aspects

Action Line A: Research

- A1 Enterprise Modelling in the Context of Collaborative Enterprises
- A2 Cross-Organizational Business Processes
- A3 Knowledge Support and Semantic Mediation Solutions
- A4 Interoperability Framework and Services for Networked Enterprises
- A5 Planned and Customisable Service-Oriented Architectures
- A6 Model-driven and Adaptive Interoperability Architectures
- A7 Business Documents and Protocols
- A8 SME Interoperability in Practice

Action Line B: Community Building

- B1 Community Creation and EIC Establishment
- B2 Knowledge Sharing
- B3 Business Interoperability Research
- B4 Dynamic Requirement Definition
- B5 Piloting Including Technology Testing Coordination and Pilot Infrastructure
- B6 Training

Action Line C: Management Coordination

Administration, Coordination, Exploitation, Infrastructure

Onion Routing in Peer-to-Peer Networks for Business Processes

Add three ingredients ...

- A **Business Case** from the Project B5.5 Automotive Pilot Scenario: collaborative product design, strategic sourcing
- A **Peer-to-Peer Framework** from the Project A6 for Business Process enactment,
- **TOR (The Onion Router)**, developed by D. Chaum, 1981, <http://tor.eff.org/>

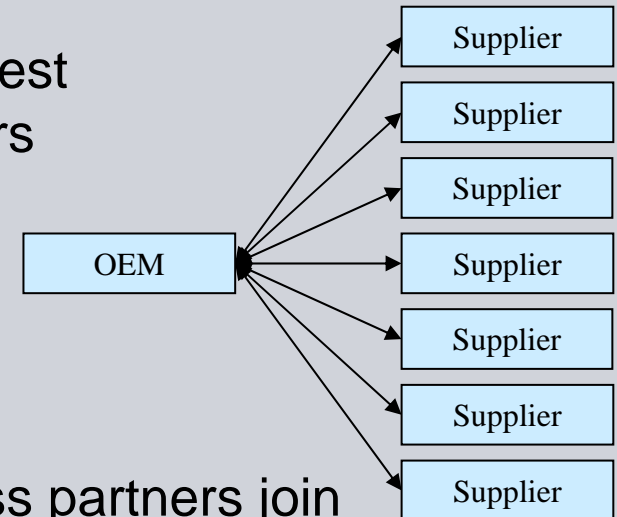


... to get anonymized messaging for cooperative distributed business computing in open Peer-to-Peer networks.

The Business Scenario

Collaborative Product Design in the automotive industry:

- OEM publishes Requests for Quotation
- Suppliers respond Quotes or Change Request
- Supplier network of partners and competitors



Characteristics of the supplier network

- No manual configuration when new business partners join
- Resilience when business partners leave/fail
- Robustness in case of system break-down
- No need for centralized coordination servers

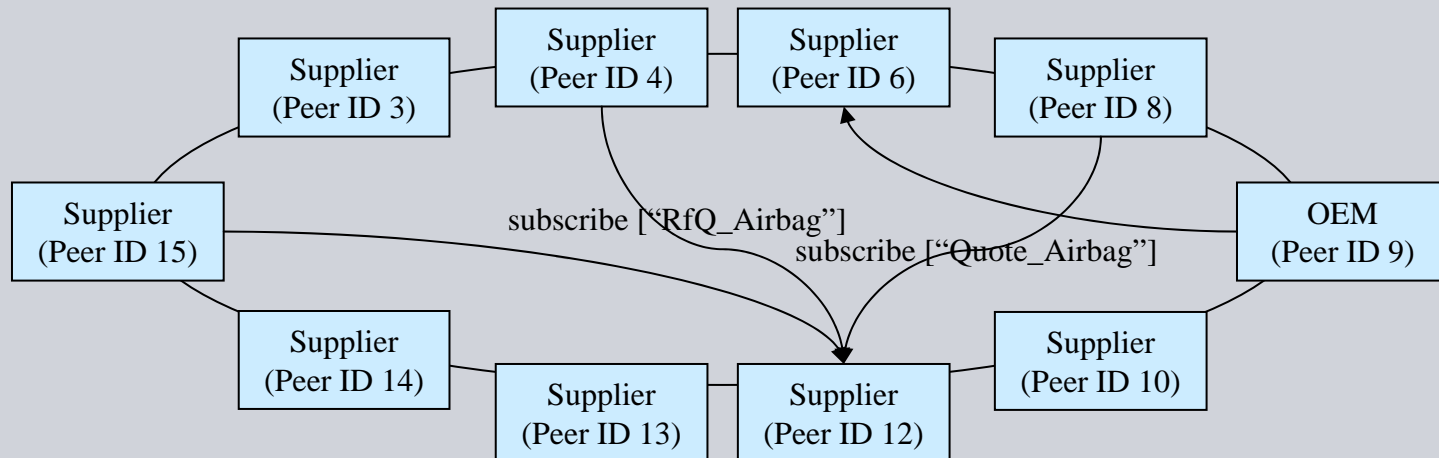
All partners provide peer systems in the network.

Peer-to-Peer-based Business Process Enactment

The P2P Business Process enactment is based on a

- Distributed Hash Table (DHT) approach:
 - Map keyword "Quote_Airbag" → Peer 12
 - Map keyword "RfQ_Airbag" → Peer 6
- Applying a publish subscribe mechanisms.

1. Subscription phase



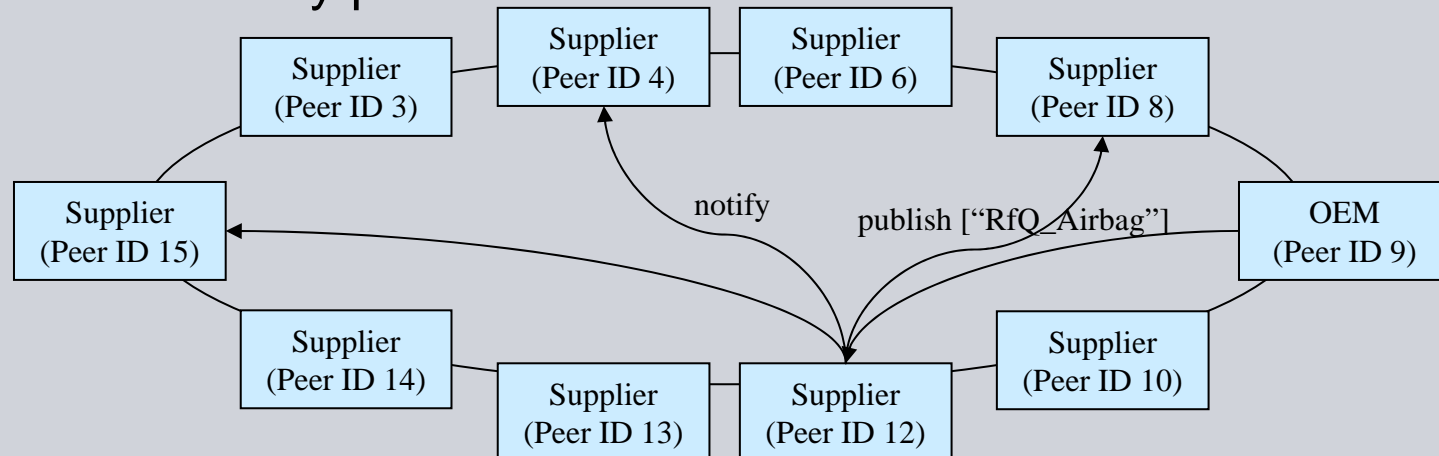
Peer-to-Peer-based Business Process Enactment

The P2P Business Process enactment is based on a

- Distributed Hash Table (DHT) approach:
 - Map keyword "Quote_Airbag" → Peer 12
 - Map keyword "RfQ_Airbag" → Peer 6
- Applying a publish subscribe mechanisms.

1. Subscription phase

2. Publish – Notify phase

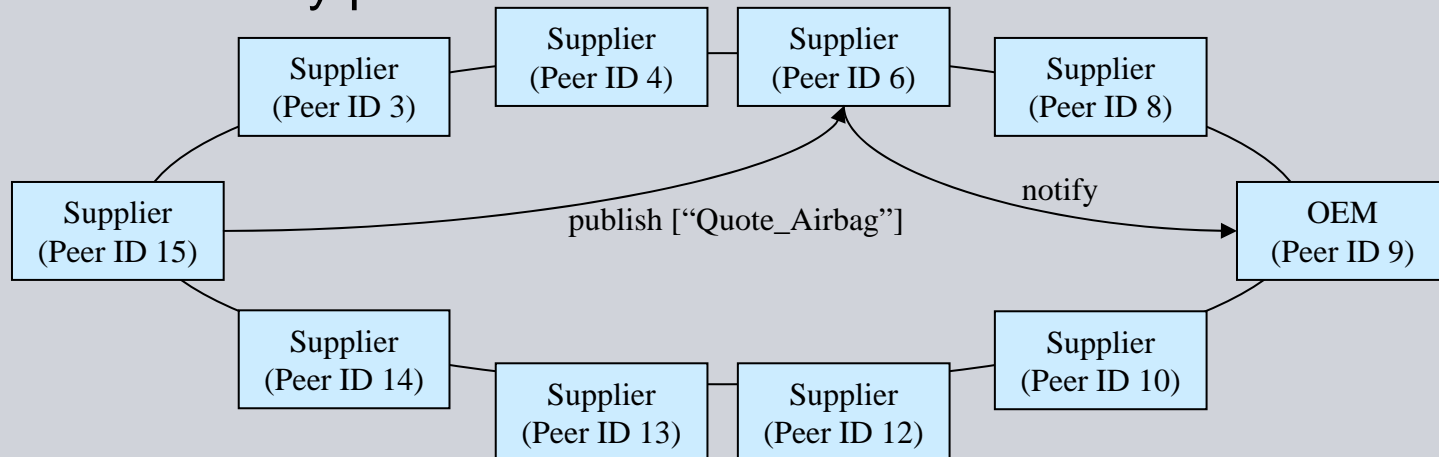


Peer-to-Peer-based Business Process Enactment

The P2P Business Process enactment is based on a

- Distributed Hash Table (DHT) approach:
 - Map keyword "Quote_Airbag" → Peer 12
 - Map keyword "RfQ_Airbag" → Peer 6
- Applying a publish subscribe mechanisms.

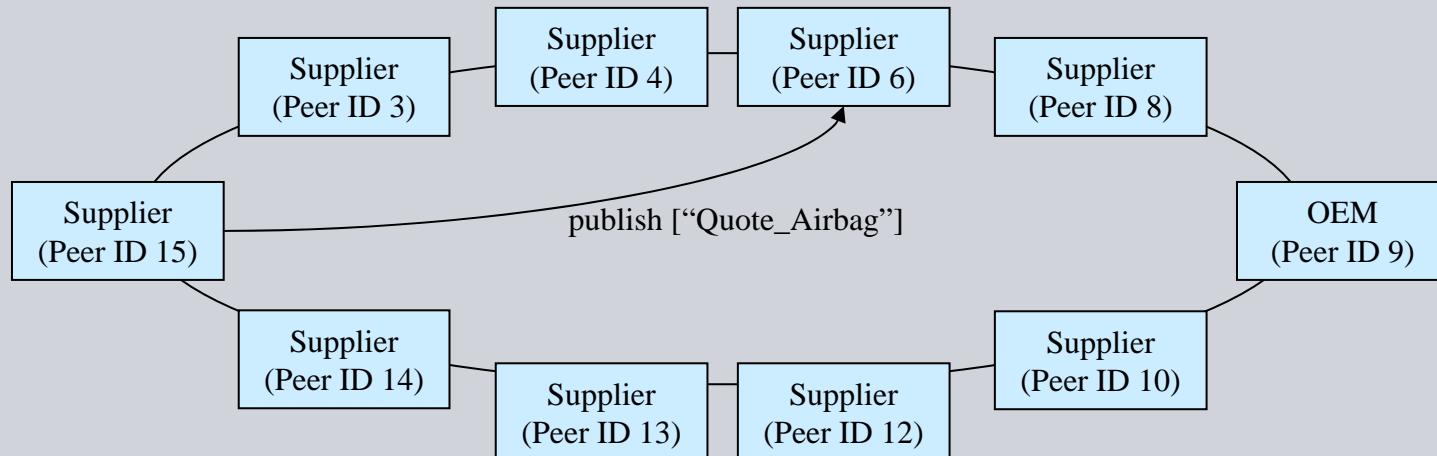
1. Subscription phase
2. Publish – Notify phase



The Security Threat

Imagine the supplier running peer 6 is an attacker. If the resource is encrypted for the OEM, the attacker still can ...

- ... observe whether a certain business competitor places a bid, and lower the price in reaction to this knowledge
- ... keep track of its competitors and raise the price in case none of them places a bid



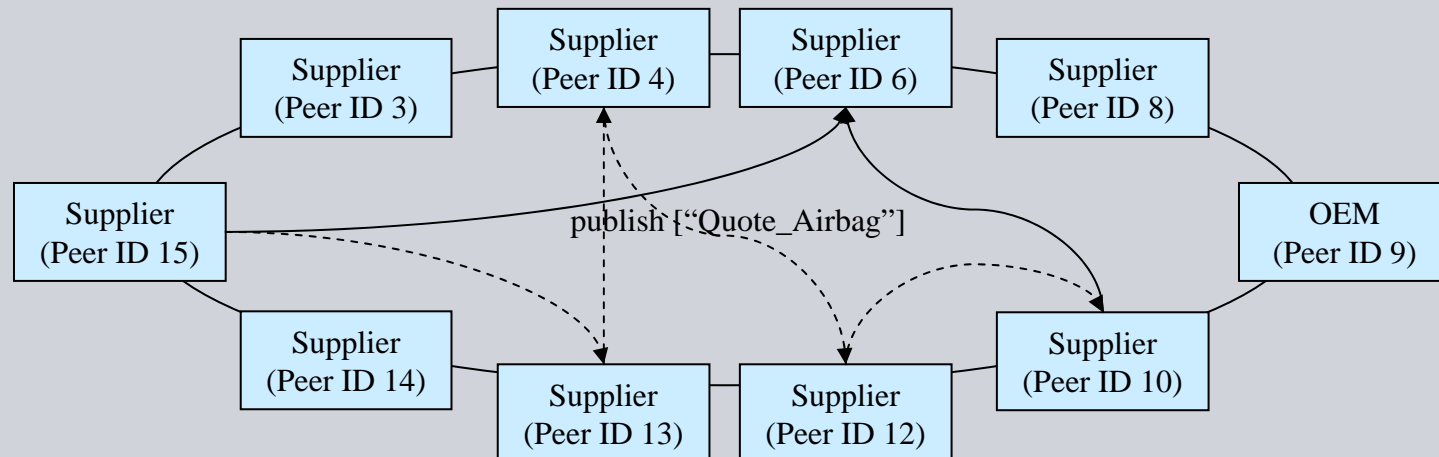
Onion Routing: the Solution

Preconditions:

Make sure every supplier may only run a single peer with a fixed peer identifier (preventing Sybil attacks).

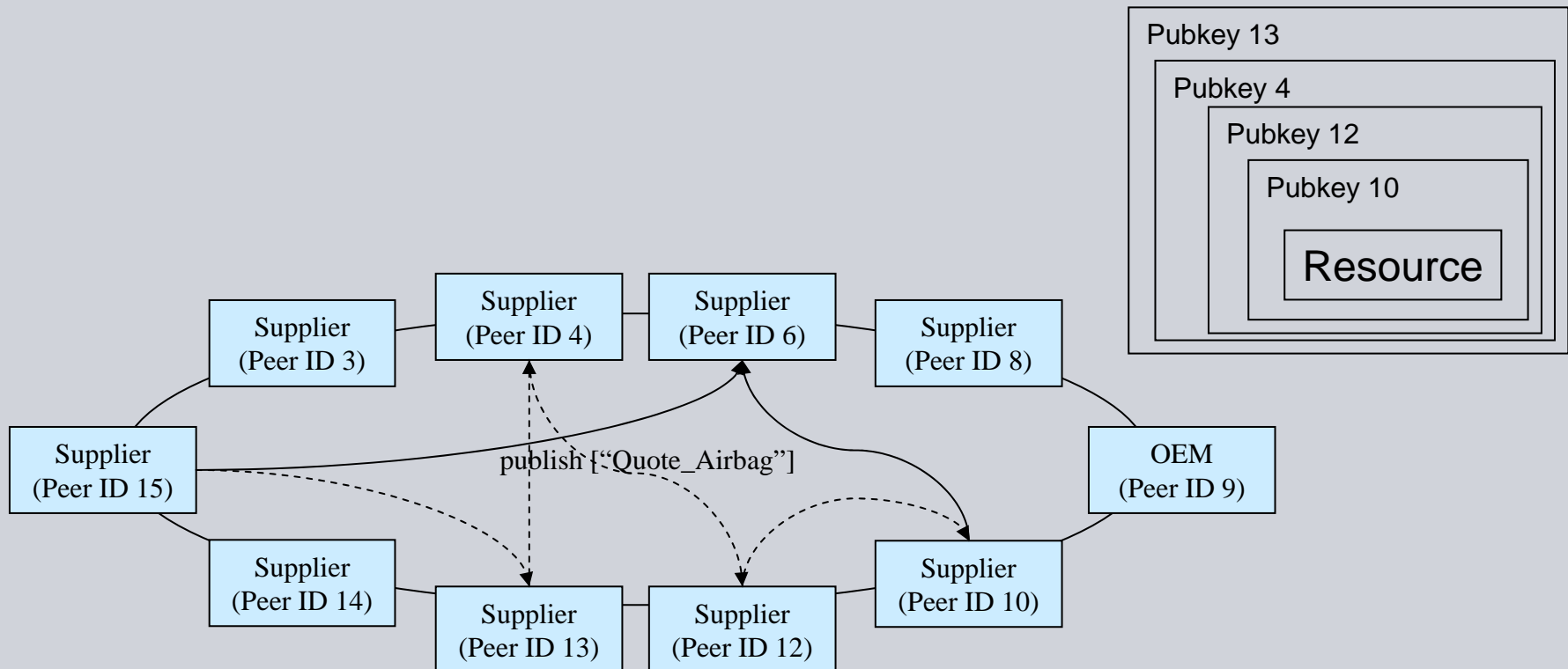
Onion Routing:

Do not publish resources directly, but send them via a random path (Routing) and encrypt the content accordingly (Onion).



Onion Routing: the Solution

- Using encryption layers, the peers on the path are not able to tell where a resource originally comes from and where it will finally go to.



Results

- Peer-to-peer has a lot of potential for business integration, but raises new security challenges.
- Security challenges in peer-to-peer based business collaboration can be addressed and solved.
- Analysis of the ATHENA Automotive Pilot scenario leads to a solution that can be applied in virtually any kind of peer-to-peer based auction scenario.
- The solution can be integrated with an existing public key infrastructure (e.g. underlying VPN).
- One step towards enabling networked businesses to benefit from resilience and self-organization offered by Peer-to-Peer.

Results

- Open issue: additional vulnerability scenarios need to be addressed, e.g. attacks on Chord's finger tables, effects of denial-of-service attacks.
- Security is always a trade-off. Future work must make Peer-to-Peer systems secure while still leaving the flexibility.
- Full paper
 - See: Stäber, Bartlang, Müller: "Using Onion Routing to Secure Peer-to-Peer Supported Business Collaboration", Proceedings of the eChallenges 2006
 - Review of features in current onion routing applications
 - Trade-offs and pitfalls
 - Related work, ideas for extending the solution
 - Best Paper Award at the eChallenges 2006

Future Work

Siemens will continue developing Peer-to-peer technology for various applications:

- Security features for Peer-to-Peer
- Distributed Peer-to-Peer-based repository using API Standard JSR 170
- Distributed Peer-to-Peer-based archiving systems
- Distributed monitoring and control
- Distributed diagnosis and alarm management

FP 7 proposals welcome

Thanks for listening

