

# Messaging is a business worth many billions of Euros annually

**High price of market data delivery is driven by high demands for resiliency and scalability. To open the competition and the market for SMEs, there is a need for developing a messaging framework that is both cost-effective and meets the scalability and resilience requirements with assurance against security vulnerabilities and erroneous input vulnerabilities.**

At the top end of the market in Investment banking it is estimated that market data delivery, which predominantly consists of messaging and, to a smaller degree of often simplistic Vision like applications, would cost top-tier Investment banks around Euro 600 per user per month. About half of this would go on the software license while the other half goes on support. This high price of both software and support is driven by high demands for resiliency and scalability (market data delivery is critical part of the infrastructure in investment banking). An average top tier bank is likely to need a few thousand licenses. There is a broad range of Publish/Subscribe messaging platforms and the whole industry offerings range in price and capability from a dozen or so thousands of Euros for simple, reliable messaging to a few dozens of Millions of Euros annually for resilient, highly scalable implementations for big clients. Messaging is a business worth many billions of Euros annually. At least half of this is coming from large companies. Two top criteria for the adoption of new messaging technology by big clients are resilience and scalability. With smaller clients, cost is the first priority, followed by resilience.

MOM (Message Oriented Middleware) increases the interoperability, portability, and flexibility of architectures by enabling applications to exchange messages with other programs without having to know what platform or processor the other application resides on within the network. MOM is typically asynchronous and peer-to-peer, but most implementations support synchronous message passing as well.

Furthermore, large organizations, e-government etc. buy a considerable amount of software from software companies or have bespoke (custom-made) software developed through software houses or develop specialized in-house components. Increasingly this software has web-client interfaces and business to business interfaces and use MOM as glue between components. While the components and the middleware may be developed according to the appropriate standards (E.g. ISO/IEC 15408), as is increasingly required in the European Union, they may still contain many security weaknesses that are only discovered the hard way, namely during operation. Also as new vulnerabilities become notified, the organizations need to check for these vulnerabilities in their systems

Currently most market leaders in the industry are from the US: Tibco, IBM, Sonic Software, Fiorano Software Inc, Vitria etc, to name a few. The European share is limited to a smaller proportion of the business. The best available systems have features to support scalability and resilience as they employ hot standby brokers with instant switch over and no data loss. However, once switch-over is performed these systems have no means to compensate for the reliability loss by automatically finding another source of redundancy. Also, they are relatively prone to the incidence of feed failures as they often do not take redundant feeds into account. It is often said that the existing state-of-the-art achieves arbitrary resilience by a brute-force approach. The state of the art is often outside of the reach of SMEs and even of large companies. Self healing is either rudimentary or non-existent. Consequently, existing MOM technologies are crude, not scalable and not suited for what will be required in the future. There is neither adequate robustness nor resilience appropriate for future real-time systems in particular.

The GEMOM (Genetic Message Oriented Secure Middleware) project is funded by the European Commission's Seventh Framework Programme (FP7), has started January 1, 2008, and will provide solutions to overcome these limitations to secure messaging. It focuses on the significant and measurable increase in the end-to-end intelligence, security and resilience of complex, distributed information systems. It will support a messaging infrastructure which will enable both far cheaper solutions as there is no need for heavy investment in infrastructure, and assurance against security vulnerabilities and erroneous input vulnerabilities to improve the reliability, robustness and dependability of critical infrastructures through specific research and development on distributed, real-time evolutionary and self-healing messaging. GEMOM resilience features will allow specialist, independent system actors, (viz. watchdogs, security and situation monitors, routers, and other optimisers) to remove or replace compromised nodes from the broader network instantly and without compromising higher level functionality and security.

The explosive growth of networking supported by the deployments of Service Oriented Architectures (SOA) and forthcoming GRID and/or Utility Computing are changing perception as to what the "computer" and even what simple application(s) are. We are entering an era where the "Network becomes the computer". The network is becoming the entity that executes even simple software tasks, not individual, known machines. Fluid, resilient and adaptive messaging of GEMOM fully supports this paradigm shift in the computing and IT evolution. The catalyst effect of having readily available services are likely to prompt more creativity as it would be easier to reuse functionality and so assemble new software systems. This easy access to a variety of services promises major qualitative and quantitative advancements in the evolution of information systems.

### **GEMOM consortium**

**Industry:** Q-Sphere Ltd (UK), Hewlett Packard (Italy), JRC Capital Management and Research GmbH (Germany), Datel Consulting International (Ireland), Diginus (UK), TXT eSolutions (Italy).

**Academia and Research Institutes:** Queen Mary University of London (UK), CNIT (Italy), Norwegian Computing Center (Norway), VTT (Finland).

**End user Applications:** Financial Market Data, Collaborative Business Portal, Distributed Linked Exchange, and Dynamic Road Management.

CNIT and Q-sphere are responsible for the administrative and scientific coordination, respectively. NR is hosting the first GEMOM technical meeting 03-05 March 2008 at NR.

Habtamu Abie and Jørn Inge Vestgården, Norwegian Computing Center