

Nexor Statement of Capability

for

Collaborative Research into High Assurance Clouds

Ref: FP7 Call 5

May 2011

connect transform protect

NEXOR[®]

www.nexor.com



Executive Summary

Nexor provides an end-to-end capability to manage secure information exchange, enable cross domain interoperability, prevent data loss and promote collaborative working by building solutions to enforce corporate security policies. This specialist knowledge and technology has been developed over two decades.

Nexor is seeking to collaborate with parties interested in researching how cloud services can be used in secure environments. In particular, we are seeking partners who are bidding for EC FP7 Security Call 5 funding. We wish to offer our expertise and capability specifically to the capability project “Secure cloud computing for critical infrastructure”.

The secure exchange of information between a client computer and the cloud requires three key components:

- A **connection** needs to be established to enable a data flow
- The data needs to be **transformed** to ensure both computer systems correctly interpret the content
- The connection need to be **protected** to prevent the egress of confidential data and the ingress of harmful content.

Nexor’s portfolio of capability focuses on these three key areas. Our research and development is conducted in our CyberShield Secure™ development facility, which brings a high degree of trust and confidence to our projects.

This document presents Nexor’s interests, credentials and capability to would-be research partners.

For further discussions related to this research, please contact:

Colin Robbins

Chief Technology Officer

Phone: 0115 953 5541

Email: colin.robbins@nexor.com



Introduction

Context

Nexor is proud of its research heritage, spun out of communication research programmes at both Nottingham University and University College London. Our close association with research continues to this day with recent project engagements looking at tracking electronic classified assets and standardisation around governance, risk and compliance – all related to the high assurance market space.

Our research capability drives an innovative approach to interpreting new market requirements and technology trends, which has led to us being a frequent market leader.

Nexor is constantly looking to the future and seeking research engagements in the areas related to the connection, transformation and protection of classified information flows, working with universities to understand latest thinking and our customers and partners to solve real world problems. Currently, our customers are all looking at the opportunities cloud computing provides, but, being at the higher assurance end of the security market, our customers are concerned about security implications. Consequently, the following FP7 Call 5 topic is of specific interest to Nexor and the market in which we operate:

FP7 Call 5

Topic SEC-2012.2.5-2 Cyber resilience – Secure cloud computing for critical infrastructure - Capability Project

Description of topic: *Cloud computing will change computing environments as we know them today. With the increasing use of this model which provides computing functions as a utility, more and more sectors will incorporate cloud services in the computing environment, eventually reaching ICT services which are operating critical infrastructures (e.g. telecommunication networks). The advantages of this new technology cannot be neglected, and commercial pressure will contribute to a widespread adoption. The objective of this topic is to analyse and evaluate cloud computing technologies with respect to potential security weaknesses in sensitive environments, and to further develop new technologies for implementing high assurance clouds. Trustable cloud computing systems and scenarios have to be developed, to allow sensitive applications to leverage the potentials of this new technology. Work done on this topic has to take into account existing research on cloud computing technologies and take it beyond state-of-the-art level towards trustworthy cloud computing. Furthermore, it is necessary to assure the societal acceptance of solutions produced by the project. Important topics of research include, but are not limited to:*

- *Data confidentiality in the cloud: one has to analyse how distributed systems can be built with cloud services that provide end-to-end data confidentiality*
- *Security in large scale cross-organisational systems: how can existing security mechanisms like security policy enforcement,*



identity and access management, incident response handling or auditing be adopted in large scale cloud environments

- *Best practices for security in cloud computing for critical infrastructure ICT.*

Funding scheme: *Collaborative Project (small or medium-scale focused research project)*

Expected impact: *With the adoption of cloud computing in critical infrastructure, the results of this work should make sure that these new technologies do not introduce new weaknesses into these systems, but should increase knowledge of the impacts and consequences of these technologies. This will allow critical infrastructure operators and manufacturers to leverage their advantages without sacrificing system security. Furthermore testing, validation and demonstration of these technologies should be foreseen.¹*

Summary

In summary, meeting the needs of the call requires looking at the following three topics, related to the cloud:

- Confidentiality
- Security
- Best Practice

¹ Taken from draft FP7 text – subject to change.



The Research Challenge

The global drive towards the use of cloud-based services is gaining pace, with a strong customer pull. For example, the UK Government IT strategy confirms the intent for the Government to “push ahead with its agenda for data centre, network, software and asset consolidation and the shift towards cloud computing”.

However, the cloud raises serious security and privacy concerns, particularly in the high assurance space. For example:

- Are the service providers’ security controls as rigorous as those of an internal IT department and does the shared infrastructure lead to an aggregated risk (*confidentiality topic*)?
- How can end-to-end confidentiality be maintained, while the service provider systems can still access the data for processing. For example, simply encrypting documents in SharePoint gives confidentiality, but removes the ability for the document to be indexed and hence the user loses the search capability (*confidentiality topic*)?
- How can you manage what data is uploaded to and retrieved from the cloud, over what connection and to what end-point (*security & best practice topics*)?
- What federated identity management mechanisms should be used to validate claimed identities and how do you control what they are allowed access to (*security & best practice topics*)?
- How do you preserve the integrity of the data stored in the cloud – how does the reader know the data has not been modified (*security topic*)?

If a cloud service (public or private) is to be used for high assurance systems and critical infrastructure, solutions to these issues need to be found.

The diagram below gives an example of the complex set of communication paths that need to be considered in a relatively simple software-as-a-service (SaaS) outsource environment. How can each of these be suitably secured for restricted and above data? Similar problems exist for other cloud models.

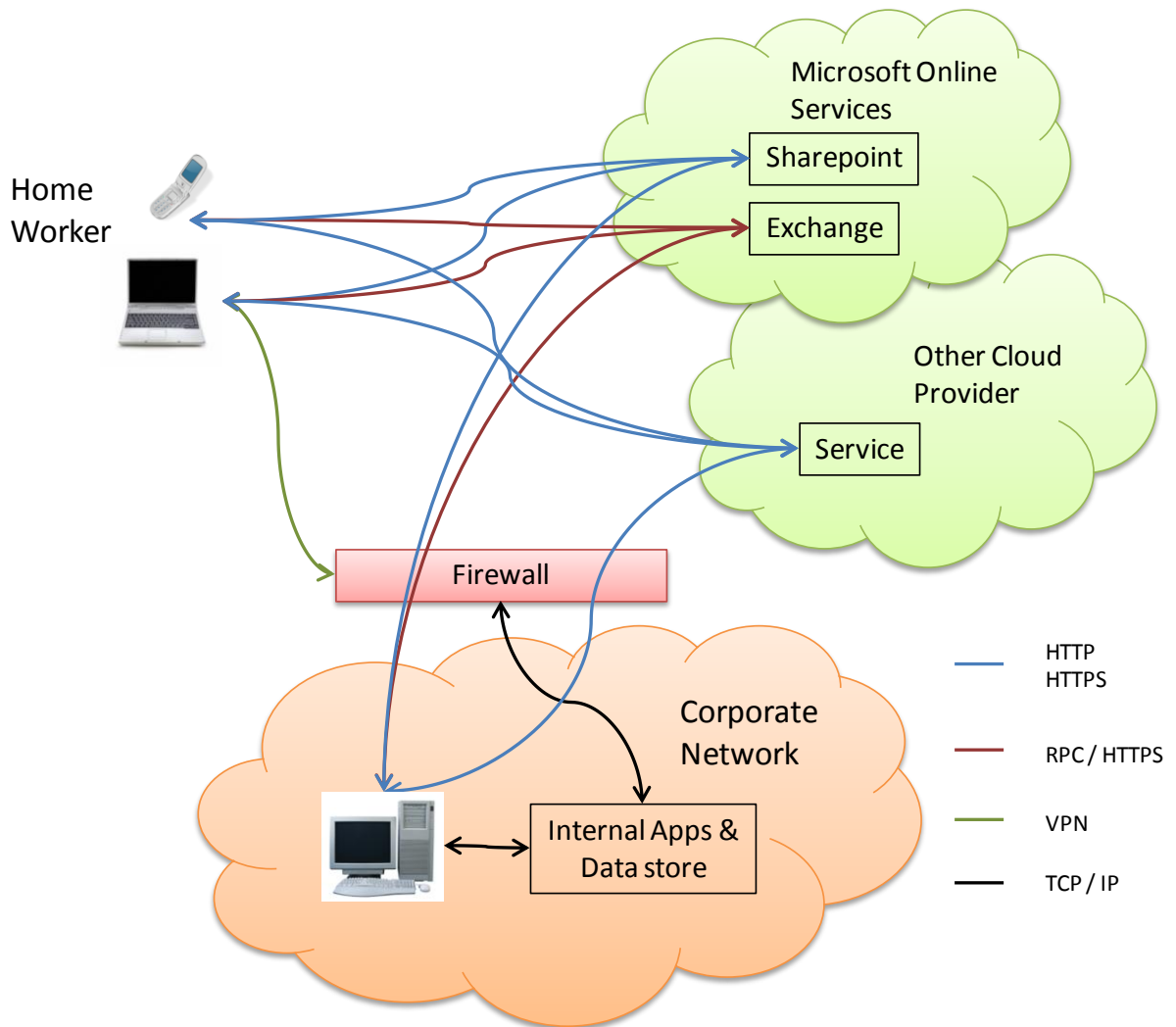


Figure 1. Simple Cloud Service
An example of a simple cloud outsource service, showing the multitude of different communication paths that need to be managed as part of a cloud security solution.

Traditional high assurance solutions based on guarding and content filtering can partly address these issues but significant challenges remain, which will be investigated as part of the FP7 call.



Nexor Interest in FP7 Call 5

Nexor's interest is to research the challenges of maintaining security and confidentiality in a cloud solution and to identify potential solutions, the solutions will need to enable and manage the multitude of different communication paths required by a cloud model to deliver user benefit. This research will lead to the identification of best practice that can be achieved in a secure cloud proposition. Nexor are also interested in working with partners to build prototype solutions meeting the identified best practice.

The following section describes Nexor's capability in detail, but in summary, our expertise puts us in an excellent position to contribute to solving the "high assurance cloud" problem by investigating:

- How is confidentiality of data in motion and data at rest maintained?
- How is data segregated?
- How secure connections are made and managed?
- How is integrity preserved?
- How do you control who gets access and from where?
- What is best practice?

We are seeking to join a consortium to contribute any or all of the following:

- Research papers and reports
- Market analysis
- Solution architecture and design
- Secure software development
- Solution testing
- Proof-of-concept hosting
- Promotional activities
- Exploitation channels.

Our existing customer base will be an excellent benchmark to investigate if the proposed solutions are viable, practical and workable.

In addition to the areas where Nexor has directly relevant technology as outlined above, we are interested in using our expertise and experience to research other challenging problems the Cloud presents. This includes, but is not limited to:

- **Multi-hosting:** How can you run systems for multiple customers in a single cloud, while managing the risk of data cross over between systems?
- **Data aggregation:** How can the issue of data aggregation be managed?



- **Data / application segregation:** How can the data sets be protected, such that the service provider can manage the application but not access the customer data?
- **Multi-level cloud:** How can different data classification levels be run in the same cloud?



Nexor Capability

Nexor connects, transforms and protects sensitive information in cyberspace. We provide an end-to-end capability to manage secure information exchange, enable cross domain interoperability, prevent data loss and promote collaborative working by building solutions to enforce corporate security policies. This specialist knowledge and technology has been developed over two decades and is readily tailored to provide a value for money contribution to applied research programmes.

Headquartered in Nottingham, Nexor is proud to count amongst its customers some of the world's largest government and military organisations, including the UK MoD and other UK Government departments, NATO, the US and Canadian military and intelligence agencies and several European defence departments.

Technology

Nexor's relevant technology expertise is focused on the secure exchange of information between client computer systems and the cloud:

- A **connection** needs to be established to enable a data flow
- The data needs to be **transformed** to ensure both computer systems correctly interpret the content
- The connection need to be **protected** to prevent the egress of confidential data and the ingress of harmful content.

Connect

A key challenge for cloud computing is how to intercept communication protocols such that it is transparent to the communicating parties while preserving all relevant information and not breaking any end-to-end security mechanisms. Our connect technology contains protocol libraries for the common communication protocols, security libraries that can manage encryption and digital signatures embedded in the protocols and application level-proxies to ensure that the protocol interactions between communication parties are seamless.

Transform

Communications between systems often requires transformation of content from that used by the sending party to something the receiving party can understand and correctly interpret. Examples include modification of the format or location of a security label, changing digital signature formats or reformatting the content itself.

Our technologies cover a wide range of protocols and content formats including email, instant messaging, file transfer and web.

In addition to providing communication interoperability, transformation services may be used as part of the security environment. Our technologies can be used to normalise a wide variety of file formats to a baseline subset, for example convert all inbound office documents to PDF or images to JPEG to reduce the risk of embedded malware. Similarly, our gateways may be used to perform redaction on the file content – removing sections of text that contain sensitive or confidential material.

Protect

Cyber security and information assurance are big concerns when connecting two systems. Questions arise such as:



- Will confidential data leak from one of the connected systems?
- Will a path be opened for an adversary to gain access to a connected system?

To protect against these risks, we have a range of technologies across the assurance spectrum:

- Email and data guards to provide high assurance that all data content has been checked and approved by a filter before passing between systems
- High assurance data diodes to guarantee one way information flows
- Medium assurance solutions to provide high assurance filter capability to mainstream third party products.

Nexor's filter technology operates in a flexible architecture enabling a suitable combination of our own and third party filters to approve content for data transfer. Our own filter components include Nexor Watchman, which locates and analyses security labels as well as providing dirty word scanning. Modules for virus scanning and deep content scanning of images and documents are also available.

Cloud

In summary, Nexor's relevant technology to securing a cloud environment includes:

- Application proxies with content filtering
- Data labelling controls
- Data loss prevention technology
- Malware detection capability
- Advanced data guard appliances and diodes
- Secure communication technology.



Nexor Research and Development Approach

Nexor approaches research projects in a very similar way to all projects we undertake. We have a strong methodology and cultural values that are supported by robust process to ensure consistency and quality of approach in everything we do. We have a track record of delivering on time and to budget, which our customers will testify to.

Secure Development

Nexor’s CyberShield Secure™ development facility provides capability to produce high assurance software, built on best practice secure software development. The CyberShield Secure™ lifecycle can be applied as both Agile and Waterfall development projects as well as prototype research concepts. In all cases, we ensure that security objectives are integrated with the requirements and that confidentiality, integrity and availability of the data and applications are kept under constant review.

Deployability

Nexor recognises that solving problems in research should extend beyond simply developing software. The full environment needs to be assessed to ensure the solution will be deployable and that all stakeholders understand what the solution will mean to them, how it will be used and what it can and cannot do. With significant experience of developing solutions for deployment, using best practice, Nexor ensures that all these aspects are built into the process. Our team of qualified security professional (CISSP, CSSLP, M Inst ISP) also ensure the solution meets all relevant Information Assurance needs.

Process

At Nexor, we ensure that our processes are aligned to the CMMI framework. We currently sit comfortably at Level 3 and have many of the organisational characteristics of Levels 4 and 5. Each continuous improvement project checks back to the CMMI model to steadily progress us through the levels. Additionally, Nexor was the first UK company to be awarded TickITplus certification.

Project Management

All Nexor assignments are managed using a proven and comprehensive service delivery methodology as shown below, with stages selected and adapted to the needs of the project.

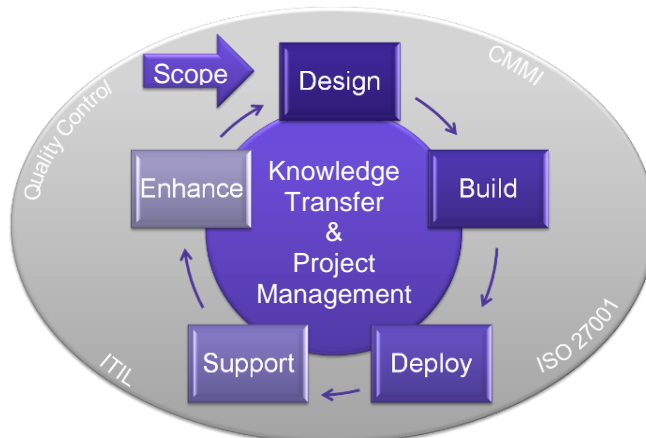


Figure 2: Nexor's Service Delivery Methodology Incorporating CMMi compliance and LEAN principles



Nexor is always pragmatic in its approach ensuring efficient and effective application of all policies and procedures. This means the delivery approach for each project will be appropriate, to ensure quality and consistency of delivery is maintained without being overly onerous.

Platforms

Secure and high assurance environments require the highest standards of robustness and resilience. On top of this, there is a balance to be achieved relating to performance, speed, functionality and accreditation. Nexor has focused on building expertise in a range of platforms and operating systems to cater for many circumstances, including:

- Windows
- SELinux
- STOP 6.



Track Record

Nexor can provide evidence of successful research and development projects of varying types and sizes as well as operational projects. Examples are:

Sample R&D Projects and Proofs-of-Concept

Cloud Guard Study

Nexor has undertaken a Cloud Guard study for a customer. In this project, Nexor has undertaken appropriate research, developed a prototype, conducted a demonstration and produced a report describing the guard capability to protect an organisation's sensitive information from being shared with a cloud service.

Information Tracking Research

This customer funded project is researching how protectively marked material can be monitored and tracked at points of ingress and egress to a network. A proof-of-concept has been built and is about to be market tested.

iGRC Research

Nexor has enhanced its guard appliances as part of a consortium to carry out research into, develop, build and test an innovative Integrated Governance, Risk and Compliance (iGRC) information infrastructure protection system. The project includes development and test of an interoperability protocol (GRCiP) to couple 'sensor' products within the network security supply chain to a GRC management suite for real-time control of threat modalities. The innovative aspect is to enhance existing COTS tools and combine them to not only respond to defined classes of threats and vulnerabilities within a GRC context, but also to adapt in a flexible manner to address new classes of these as they emerge. Risks to the security of information infrastructure that supports the UK's national infrastructure and its competitive standing will be minimised

Guard/Gateway Project

Nexor created an ISTAR Security Gateway for a major international demonstration. The gateway provided a mechanism to transfer ISTAR information between security domains. The gateway allowed one way transfer of information from a low domain into a high domain to provide critical information to that domain. To create the solution, Nexor integrated its own and third party technology including an email generation server, an email content checking server, high side and low side data diodes, a low bandwidth email gateway, secure image and video file transfer and streaming video with all the relevant infrastructure components into robust flight cases for use in an extremely harsh environment.



Sample Operational Projects

- IEG Study** Nexor is undertaking a study of the information exchange requirements for the European Defence Agency. An approach of this nature will be key in understanding how a high assurance cloud can be built – what data is to be held where and how is it to be accessed.
- Guard Project** In 2006, Nexor was awarded a framework contract and appointed as supplier of choice for the provision of high assurance mailguards for operational use by NATO Maintenance and Supply Agency (NAMSA) (<http://www.namsa.nato.int>). In advance of this award, Nexor worked in close collaboration with NAMSA to enhance Nexor Sentinel to offer boundary protection services for NATO mission systems. This project has been hailed a successful example of industry’s flexibility and responsiveness to the customer’s needs.
- Guard Project** When a UK agency recognised a requirement to prevent accidental data leakage, Nexor developed Nexor Watchman specifically to address this need. Watchman provides content checking and verification technology to prevent confidential information being transferred by unauthorised parties between specified domains. Watchman is standards-based and supports X.400 and SMTP
- Guard Project** After a thorough evaluation of the market, Nexor Sentinel 3 was selected by a North American Government agency to fulfil its cross domain guarding requirements. The customer onward recommended this solution to another agency that is using it in conjunction with Nexor gateway technology to provide a complete border solution.