

## Gary Cywie & Sébastien Stormacq (Noble & Scheidecker et Sun Microsystems) : Identity Management – form an IT specialist's and a lawyer's perspective A cross interview where Noble & Scheidecker's Gary Cywie and Catherine Jardin give their legal views about the IT description of Identity Management outlined by Sébastien Stormacq, Senior Software Architect at Sun Microsystems Luxembourg.

What is Identity Management and what does it imply?

Gary Cywie (Noble & Scheidecker (MNKS)) : From a legal standpoint, besides questions relating to software (licensing, maintenance, etc.), ID Management mainly involves data protection issues, including general data protection laws as well as those specifically applicable to the electronic communications sector. Data protection rules apply in the case of processing of personal data, i.e. the use of information of any type relating to identified or identifiable persons. Such personal data processing triggers several obligations for the data controller (mainly prior information to regulator and data subjects) and rights for data subjects (mainly right to access and modify the data if not up to date). Additional obligations may apply when personal data of employees is processed. Beside the data protection aspect, confidentiality matters might be implied.

Sébastien Stormacq (Sun Microsystems Luxembourg) : Identity Management is a term that usually refers to four independent but complimentary technologies and processes. Directory Services are used to store user accounts in a highly performant and high-available fashion. Identity Provisioning is the process of managing user identities across a variety of IT systems and applications and managing users' entitlements to these systems. Access and Authorization management is the process of enforcing users entitlements. GRC (Governance, Risk, Control) allows a set of tools to reach a state of compliancy. This implies ensuring each and every employee receives the exact set of entitlements he/she needs for his/her role, enforce security through policies, meet compliancy obligations (running audit analysis and ad hoc reporting), and finally reducing costs (providing process automatization, eliminate duplicate effort, maximize self-service, ...).

What sector benefits of the Identity Management systems?

Sun : Identity Management processes are found at any company regardless of the sector. It is clear that companies with a large set of identities and/or a large set of systems will benefit more of an automated solution. On the Luxembourg market, Sun Microsystems' solutions are being used by large financial institutions, as well as European Institutions, Industry etc

MNKS : Any sector might benefit from ID management systems as a security tool to enforce confidentiality as persons (whether employees or providers for instance) would only have the entitlements they need for doing their specific job, without having access to other information. In the same logic, ID management may also be used as a sort of "Privacy enhancing technology". Moreover, ID management systems may help to comply with regulatory obligations of confidentiality imposed on certain specific sectors such as the banking and the insurance sectors for example.

Which department within an organization typically drives the need for an Identity Management solution?

Sun : Initial demand to rationalize the processes of managing identities and entitlements is usually coming either from Human Resources department, IT Security or Organization department, or it can be a requirement resulting from an Audit. Once the system is deployed, every single employee will see benefits. For example, end users will be able to access self-service pages to ask or revoke entitlements, perform password resets, all resulting in a reduction of the help desk team workload.

MNKS : If the company has one, the data protection officer or, as the case may be, the compliance officer would certainly see the benefits from an Identity Management solution. He would then pay attention to the prior formalities that the use of an ID management system might entail under data protection laws. In particular, the data processing may require either prior notification to or authorization from the "Commission nationale pour la protection des données". In case of any doubt, the company may contact directly the CNPD or ask a legal counsel to assist in determining which procedures must be undertaken and/or take care of the applicable administrative procedures.

What are the risks addressed by the ID System?

Sun : An Identity Management solution such as the one from Sun, allows a deep-level risk assessment and mitigation of a variety of problems that can occur with the entitlements awarded to the end-users. By scanning the data in a preventative or post-mortem fashion, the data can be validated against a set of configurable policies. As a result conflicting entitlements (e.g. detected via Segregation of Duty rules) will be detected and can be remediated or mitigated. Furthermore, Sun's GRC capabilities allow for certification cycles whereby the entitlements given to roles or users can be validated by data owners. This repeating certification cycle will help an organization to reach a state of compliancy reducing the risk of invalid entitlements being awarded. Actual versus Theoretical scans will remediate exceptional and erroneous entitlements that were given in the past, but are no longer acceptable according to newly set rules. Orphan accounts, i.e accounts no longer used because the employee or contractor left the organization, will be spotted by the system and may be terminated.

MNKS : The ID management system should ensure that access to an IT system of a company is being granted to each person (employee, provider or third party) in accordance with the internal policy or the legal and regulatory rules applicable to such company, that limits access to electronic information. This raises the confidentiality level in and limits

damages for the undertaking by restricting the risk of unauthorized access to (confidential) information or conduct of transactions by employees which are not entitled to execute them. Furthermore, an ID management system may help detecting and deleting dormant accounts which could for instance contain personal data of a former employee, which processing may have become unlawful (as the data controller may not store personal data for a longer period than necessary for achieving the purpose of the intended data processing).

How does a company obtain the ID System in practice? Sun : Sun's Microsystems is a one stop shop for Identity Solutions. Sun's solutions are based on open standards and open source software. The customer has a choice between a perpetual licensing/support model, or a subscription model, legal indemnification and support. Sun Microsystems' Professional Services and Partners can help organizations to deploy and implement an effective Identity Management solution on a very short time frame.

For more information, please visit the following web site <http://www.sun.com/identity>

MNKS : In practice, companies would receive a license from the provider of the ID management system. This usually implies entering into a license agreement which states the rights and obligations of the parties to the agreement. It should be noted that such agreement does generally not lead to any transfer of IP rights, but only to a right to use the product for a certain period of time and under the agreed conditions. In general, the provider of the ID management system would be responsible for the good operation of the system and the customer for the use that is made of the system, for instance in case of a fraudulent use (i.e. persons granting unauthorized access to other persons or to themselves). Additionally, the provider would be responsible for providing maintenance of the system (proactive maintenance with updates and upgrades as well as curative maintenance if a problem occurs).