evidian

Federating & protecting roaming users' Web access

Bull
atos technologies

Summary

Enhancing roaming user's efficiency thanks to Web access

Roaming user's accesses to applications wherever they are located is a vital need for the enterprise activity. Mergers & acquisitions, offshoring, teleworking and the need to access information in real time are a necessity to maintain and increase the company's competitiveness.

Roaming users can be commercial advisors, distributors, suppliers, partners... who need, among other things, to:

- Access the Customer Relationship Management system in SaaS mode,
- place orders thanks to a single order entry system hosted in a private Cloud,
- Follow the situation of the customer's inventory on the internal IT system,
- Know the stock level through applications operated in the enterprise's data center,
- Ensure that a geographically distributed infrastructure is maintained.

If these people access online applications easily and securely, the enterprise's processes will be highly optimized.

This white paper describes the case of one of our customers, a Telecom operator. By optimizing internal processes, this operator succeeded in managing its demand growth while obtaining an increasingly important margin by:

- providing its customer advisers with a single interface to access the customer's information and inventory as well as stocks... in order for the operator to better identify the customer's need and offer him new products or services,
- informing technicians or sub-contractors at any time, through alerts and instructions for mending and following up its infrastructure's defective elements; in order to guarantee the best level in Quality of Service while optimizing associated costs.

It provides a pragmatic answer to the following questions:

- How to quickly offer a Web access to a customer adviser in a branch or a technician in the field with the level of security adapted to their respective missions?
- How to federate and secure Web accesses without modifying existing applications (internal or externalized): private Cloud, SaaS or hosted?
- How to prevent users from storing their application passwords, in professional or personal environments (workstations, tablets, smartphones and mobile terminals), and thus from introducing vulnerabilities?

The remainder of this document describes the needs and the solution facing these challenges, without any mandatory client component or any special feature on the mobile terminal.

Implementing new services through a corporate portal

Advising Customers and Selling New Services

The telecom operator has decided to implement a new global commercial service for single order entries for all its offers. Thanks to a global view of his customer's information, the customer adviser can promptly prepare additional proposals, whether he is in a branch or in a reseller's office.

The aim of this new service is to take advantage of the information related to his customer (products and services already subscribed) to offer him customized offers in real time.

A Global Service for All Sales Operations

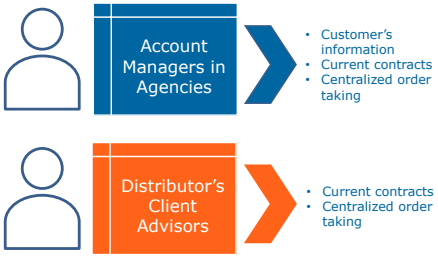
This new service must accelerate all the processes related to sales in the branches.

The sales department consults and manages customer information and subscribed contracts with the SalesForce CRM application accessible through the Web in the private Cloud or in SaaS mode.

The department in charge of mobile contracts provides access to contract terms of sale, subscription, mobile pack and order entries system thanks to a Web application hosted in a private data center. Other departments do the same in order to provide a Multi-play offer.

Internal advisers, in branches or external advisers on reseller premises, can update the single order entry system through the Web at the time of sale.

The operations performed, after a successful authentication, are thus perfectly identifiable "*who – where – when*", traceable and auditable by the company that wishes to control them.



Maintaining a Geographically Distributed Infrastructure

The telecom operator has decided to create a global service in charge of controlling and distributing the equipment required to maintain its infrastructure.

The aim of this new secure service is to manage and distribute the available equipment to its service providers reliably and quickly to accelerate maintenance operations.

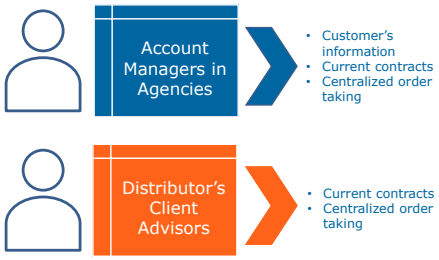
A global service for all maintenance operations

This new service must accelerate all the maintenance processes.

The department in charge of monitoring the movement of equipment can use the Web application to manage maintenance requests from the most appropriate service provider, based on equipment availability and contractual specifications.

The maintenance teams, internal or external service providers, can update the list of available maintenance equipment or obtain personal-related data, via the Web.

The company can follow up and control the maintenance operations.



Immediate Operational Gains

This new service optimizes the processes related to the sales and maintenance operations organization and the operations themselves.

Since branches, resellers and company agents have a secure direct access to Web applications, the commercial productivity and the maintenance operations management is improved and accelerated.

With direct order entry management via the Web, advisers in branches or on reseller premises, have a direct access to the all the customer's information, which increases the advisers' sales efficiency.

The fact that the different teams declare and monitor the equipment movements directly via the Web reduces the operation management cost and accelerates the decision-taking process.

Known Potential Risks Inherent to the Introduction of such a Service

Although the service generates immediate gains, it may involve some risks which must be controlled.

The data handled by the sales advisers and maintenance teams as part of this new service is essential to the operator's Quality of Service. A contract with missing or erroneous information, a special offer which should not be applied, an unjustified reimbursement operation, failing to update the stock inventory may have serious consequences on the turnover, maintenance deadlines and quality of service, i.e. business and income.

Moreover, some users, like resellers, access this new service from the Internet and from workstations which are not managed by the company, i.e. outside the protected intranet zone of the information system.

- The operator has no control on the security policy applied to the external service-providers' workstations or browsers.
- If the portal is not secured, the external service-providers could access all the company's applications via the Internet.
- The operator wishes to use the services in SaaS, Cloud and in a hosting company. However, it must control the authorized users' access to its Web applications.

Data protection and access via the Web were quickly identified as the key to the success of this new service

Use case: solution adopted by a telecom operator

Protecting and Managing Access

To protect its data, this operator has created a secure Web access-control point, including three functions:

- Network filtering through firewalls.
- User access control, with implementation of an authentication and access-authorization solution.
- Single Sign-On for the authorized Web applications.

Access-control and web-SSO functions are performed by the Web Access Manager (WAM) software.

Web Access Manager, your Web security infrastructure

Web Access Manager is a security solution that authenticates users and then checks, for each HTML request, the access rights for the requested URL.

Centralized access control

For each URL requested by a user, Web Access Manager checks the user's access rights and accepts or blocks the request, if necessary.

Web Access Manager is located at the forefront of the most protected zone of the information system. All application access requests must pass through this point, and all of them are filtered.

Guaranteeing the confidentiality of access

The company wished to implement an SSL communication. This HTTPS communication is implemented within Web Access Manager. Since only this frontal server is accessible from the Web, the company does not need to implement SSL on all Web application servers; there is no additional certificates management.

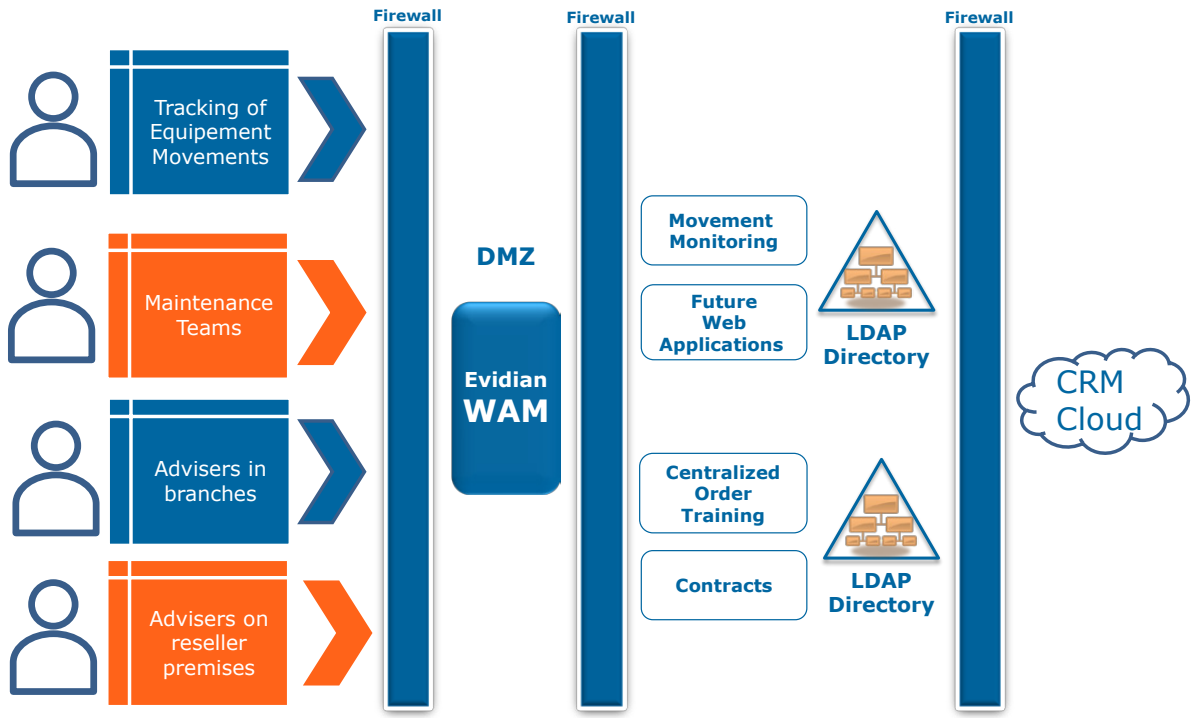
Simplifying access with Web SSO and a customized welcome page

Web Access Manager simplifies accesses thanks to:

- A primary authentication during user authentication.
- A customized welcome page displaying only the authorized applications.
- Automatic access to applications, with transparent secondary re-authentication to the application. This feature is also known as Single Sign-On (SSO).

Web Access Manager accelerates the deployment of new Web-based business services

The architecture of Web Access Manager has been a key factor in the secure deployment of new Web applications.



Web Access Manager Features	*Implementing new Web-based business services*
Integration with the operator's LDAP directory	Accelerates online creation of Web accesses 24/7
Robust authentication, SSO, URL and user IP address control	Guarantees information security and confidentiality
Non-intrusive reverse-proxy architecture (no module on the Web application servers)	Isolates the security functions from Web applications No modification of applications
Centralized administration	Simplifies the addition of new servers and Web applications
Web Access Manager Console	Allows a user's accesses to be blocked with just a few clicks
Centralized audit	Analyzes user activities

The Web application used to monitor the equipment movement was declared in Web Access Manager within less than 60 minutes (including tests).

Similarly, a new application (used to determine the eligibility to France Telecom's unbundling offer) was declared within a few dozen minutes in the Web Access Manager server.

All this without modifying any application

Control and secure user access with Web Access Manager

Usually, as companies go online, security enforcement falls to the administrators of each application. As applications are added, the security policies quickly become unmanageable. This kind of "*puzzle*" approach to security results both in security breaches and end-user frustration.

Enforce Access Control for All Applications

Web Access Manager allows you to define and manage which applications and resources users can access. Instead of having each resource manager control security on his servers, Web Access Manager centralizes access control management of Web resources.

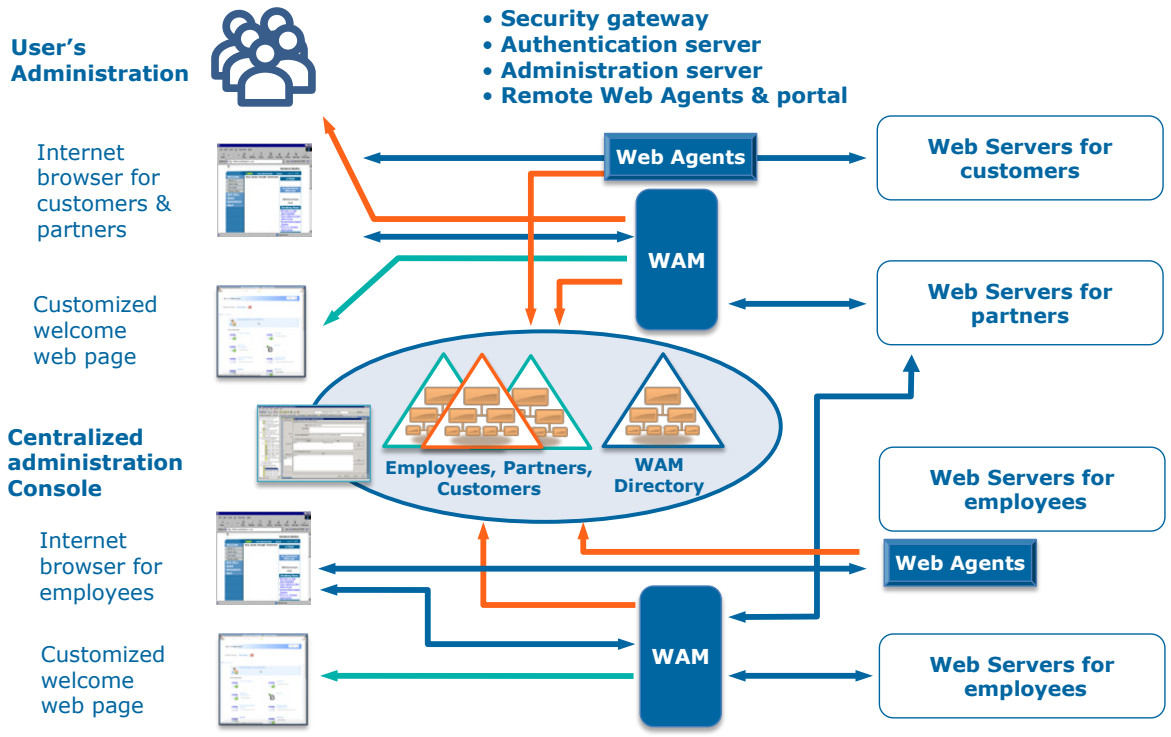
Through an easy-to-use console, an administrator can control user access dynamically. New employees can be added to the appropriate groups and gain access to multiple applications immediately. With Web Access Manager, former partners and employees can have their access to company services revoked with one click. In addition, Web Access Manager allows you to follow up all user activities. With Web Access Manager, you can implement a global security policy for all internal and external Web resources.

Control Access to Applications and URLs

The Web Access Manager URL access control modules can be placed either at a security gateway as a reverse proxy or on the applications themselves on the same servers.

Web Access Manager allows the implementation of four architecture types:

- Pure "*portal*" architecture in which the access control module is placed on the reverse proxy on a single gateway. This architecture is recommended since it has no impact on applications and servers.
- Pure "*local Web agent*" architecture in which the access control module is placed on the application servers to be protected.
- "*Remote Web agent*" architecture in which the access control is placed on a gateway and is dedicated to only one application and Web server. This architecture is recommended when applications to be protected are complex or generate many requests.
- Mixed "*Web agent/gateway*" architecture in which, depending on the security policy, network and application architecture and optimization of network flows, the control points can be located either on the reverse proxy or on the servers.



Web Access Manager Web agents Architecture

Dynamic authorizations

URL and application access authorizations can be computed dynamically using simple "*And*", "*Or*", "*Not*" rules applied to the user attributes available in the LDAP directory. These rules are centrally defined by the administrator and then applied by the access control modules.

User's authentication

Web Access Manager can authenticate users with different methods such as:

- Login and password
- Virtual keyboard enabling a user to enter his login and password by clicking on a keyboard displayed at random places on the PC screen. A virtual keyboard provides an additional protection against key loggers, without using a strong authentication device.
- One-Time Password:
  - Computed by a token
  - Sent by SMS
  - Sent by email
  - Computed by the QRentry smartphone application from a QR code
- Smart card with X.509 certificates
- Kerberos token (Windows® domain)
- SAML token (Service Provider / Identity Provider)
- Radius-based authentication
- Grid Card allowing each user to solve a challenge that cannot be replayed
- External authentication mechanisms such as CAS, OpenID, OAuth (authentication by Facebook, LinkedIn, Twitter, Google+) or pairing with any external mechanism using the Web Access Manager SDK.

Supervise the User Activity

Any proper access management policy requires monitoring. Web Access Manager tracks all user accesses or access attempts, in order to protect Web resources, and thus enabling security administrators to monitor who accessed which application and when.

Web Access Manager is compatible with log analysis tools such as NetIQ WebTrends. This makes it easier for administrators to analyze security audit reports.

Administer securely and quickly multiple Web accesses

- Separation between the security infrastructure and the applications.
- A non-intrusive solution on the servers, not requiring any specific developments.
- Offering high scalability and availability to follow the IT system's evolution.

Encrypt confidential data

To guarantee the confidentiality of the data exchanged on the Internet, the partners must open encrypted sessions. As more and more companies now work online, encrypting each Web application is becoming a problem, because not all applications can be encrypted.

With Web Access Manager, all communications with the browser can be encrypted. Customers, employees and partners can communicate confidently within the community of sites managed by Web Access Manager.

Protect Web resources against attacks

Web Access Manager helps prevent attacks against Web resources exposed on the Internet.

The Web Access Manager gateways hide the real address of Web resources. It modifies the Web applications' URL to prevent hackers from knowing the network architecture.

Web Access Manager also controls the entries for all Web accesses, making it easier to protect Web applications requiring an access code against worms or other attacks from the Internet.

Creating user accounts

Web Access Manager is consistently integrated into existing user management processes.

Using the enterprise LDAP directories

Web Access Manager reuses the user definition contained in the enterprise's different LDAP directories. The LDAP directories may be from different suppliers, have different structures and be located on different sites.

Account creation by the user

Depending on the existing security policy, a user may be authorized to create a personal account in a predefined LDAP directory, by connecting to Web Access Manager. The account can then be integrated by an administrator into the company's general access control policy.

Resetting a primary password

When a user forgets his primary password, Web Access Manager offers him the possibility to reset this primary password using a question/answer form. The user does not need any assistance from the help desk. The password creation policy defined by the company (number of characters, non-use of an already existing password, etc.) is then applied.

Using multiple identities

A user can access several domains using the same name. Each identity is then defined in a different LDAP directory. We then talk in terms of different domains. These different domains may, for instance, correspond to different enterprises, subsidiaries or organizations.

Web Access Manager enables the user to choose his domain during initial authentication. He is then granted the rights associated with the identity of the domain he has chosen.

Universal Single Sign-On

Traditional security solutions interfere with the user efficiency and experience. Web Access Manager's streamlined approach to security improves user loyalty. By facilitating navigation with Single Sign-On and improving the user experience with customized content, Web Access Manager improves user productivity and confidence.

Web Access Manager manages the connection to traditional Web applications, each using their own password, to applications using the domain password such as OWA, and to applications using the SAML protocol.

Improve the user experience and security with Single Sign-On

When users are expected to provide a password for each internal and external application, enforcing security can slow them down in their daily tasks. Managing multiple logins and passwords is time-consuming and frustrating.

Users find shortcuts such as choosing weak passwords or leaving them in conspicuous places. Password-related help-desk calls make up a significant part of its costs. Multiple passwords not only impede business by deteriorating the user experience and productivity, they also lead to security breaches.

With Web Access Manager, customers, partners or employees access internal and external Web resources with one user name and password. After an initial authentication performed by Web Access Manager, they can navigate freely among the resources they are allowed to access. Web Access Manager transparently provides each application with the corresponding login & password in the corresponding forms.

Single Sign-On to external Web sites

With the activity of organizations extending beyond the firewall across multiple domains, Single Sign-On also needs to follow the same path: Intranet portals often allow access to purchasing Websites or subscription services, extranets can cover multiple partner sites.

With Web Access Manager, portal managers can control their Web environment by adding and moving resources dynamically.

Users can access resources outside the enterprise without being prompted for another password. The Web Access Manager solution improves security, user experience and reduces help desk calls.

Web Access Manager acts also as a single gateway to SaaS or Cloud applications. The list of Cloud/SaaS services is available directly from the user's customized homepage and the same primary authentication is used for these applications using the SAML federation protocol.

Customize the end-user's Web environment

While navigating the Web is notoriously impersonal as users often have irrelevant links on their welcome page, Web Access Manager customizes the user experience, giving them the feeling of being part of a community.

With Web Access Manager, users in specific sectors of the industry located in predefined geographic areas can get access and customized information. Customers' and partners' access to services are secured on several levels. This ability to respond to user needs with Web Access Manager makes users feel like they are members of a trusted community. Single Sign-On strengthens this feeling by providing users with seamless navigation within authorized applications.

The user can choose to manage sensitive passwords himself

Passwords can be updated either by a central administrator or by the end-user. If the password is managed by the user, the administrator will not be able to access it.

Accessing a shared account

Several users can share a common account on a target application.

Group passwords may be transparent for end-users. Thus, an administrator can authorize members of a predefined group to access analyst reports without revealing the relevant company's password.

WAM extended to J2EE, SOA and Web Services Project Accesses

With a modular architecture, the SOA Access Manager module extends Web Access Manager functions by providing an integrated SSO solution to J2EE, SOA and Web Services environments.

Using a common authentication and administration server, Web Access Manager and SOA Access Manager cooperate to provide users with a Single Sign-On for Web environments as well as J2EE and Web Services environments.

Thanks to SAML technologies, SOA Access Manager simply extends the Web Access Manager access control functions to interconnect portals or Web applications to J2EE servers or to internal and external Web Services.

WAM Extended to non-Web access and legacy applications

Not all applications are Web-enabled. The Authentication Manager & Enterprise SSO solution (also known as Enterprise Access Management) can address non-Web applications; it completes Web Access Manager to provide a complete and integrated solution for securing and simplifying access to non-Web and legacy applications.

Keep Control of Security

- Centralized administration: minimize security costs and tasks.
- Flexible administration: add or revoke user rights in a few clicks.
- Central audit: track all connections to instantly know who has accessed what.

Instant security for a low cost of ownership

With Web Access Manager, you do not have to sacrifice convenience for security. Web Access Manager does not require any modification or additional components on user workstations or target systems. Today, the other solutions on the market are overcomplicated, requiring months to deploy and consuming precious IT resources.

A non-intrusive solution for easy deployment

Thanks to its non-intrusive architecture, Web Access Manager can be fully deployed in a matter of hours, enabling the extended company to change as quickly as the market does. Downloadable from the Web, Web Access Manager is a complete piece of software and is standard-based.

More effective administration

Web Access Manager enables portal or Web server managers to seamlessly manage access to any Web application without deploying any software, and without reorganizing the directories. There is no need to modify the existing administration processes or applications. Web Access Manager reuses the existing LDAP user directories to apply a security policy to the enterprise resources.

Moving forwards with Identity & Access Management applied to your Corporate Portal

Evidian Identity & Access Manager allows a complete management of the identity and access to services lifecycle. I&AM relies on the internal management of the authorization policy based on the roles and organizations of the enterprise, as well as a complete system of workflow, provisioning and control of the policy applied to applications and services.

Checkpoint for the extended enterprise

The Telecom operator's needs, which were described in this white paper, are shared by most of the companies or institutions that have to open their IT system to their roaming co-workers, thus extending their enterprise.

- The hospital now expects town and rural district doctors to access its information system with SAML tokens (Service Provider / Identity Provider).
- The community center opens registration services available to territorial officials wherever they work: swimming pools, canteens...
- The insurance company shares its business applications with its brokerage network.

The principles and recommendations outlined in this document are generic and transposable to these numerous professional use cases.

Evidian software suite

We offer our clients a complete, integrated and modular solution for digital identity management and access governance compatible with their security policies and the new regulatory requirements.

Evidian Identity Governance & Administration (IGA)

enables authorization governance and a complete management of the identity and access to services lifecycle, driven by a security policy and its approval workflows. IGA manages the four pillars of the Identity and Access Governance market: Identities, Policy, Process & Access. With IGA, only the right people access the right resources with the required rights for the right business reasons.

Evidian Web Access Manager

is designed to manage access federation to Web applications, secure user access. Indeed, mobile users and partners want to access their messages or company applications securely. WAM allows you to manage access to web applications and replace all user passwords with a single mean of authentication without modifying the applications.

Evidian Enterprise SSO

manages access to enterprise and personal applications on workstations as well as mobile devices, preventing the user from **memorizing and entering passwords**.

Evidian Authentication Manager

provides strong authentication on workstations and mobile devices: smartcard or token with certificate, contactless RFID cards, biometrics, One Time Password.

Evidian SafeKit

brings high availability and load balancing to applications.

About Atos & Bull

Atos SE (Societas Europaea) is a leader in digital transformation with circa 100,000 employees in 72 countries and pro forma annual revenue of circa € 12 billion. Serving a global client base, the Group is the European leader in Big Data, Cybersecurity, Digital Workplace and provides Cloud services, Infrastructure & Data Management, Business & Platform solutions, as well as transactional services through Worldline, the European leader in the payment industry. With its cutting edge technologies, digital expertise and industry knowledge, the Group supports the digital transformation of its clients across different business sectors: Defense, Financial Services, Health, Manufacturing, Media, Utilities, Public sector, Retail, Telecommunications, and Transportation. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and is listed on the Euronext Paris market. Atos operates under the brands Atos, Atos Consulting, Atos Worldgrid, Bull, Canopy, Unify and Worldline.

For more information, **visit atos.net**

Bull, the Atos technologies for the digital transformation

Bull is the Atos brand for its technology products and software, which are today distributed in over 50 countries worldwide. With a rich heritage of over 80 years of technological innovation, 2000 patents and a 700 strong R&D team supported by the Atos Scientific Community, it offers products and value-added software to assist clients in their digital transformation, specifically in the areas of Big Data and Cybersecurity.

Bull is the European leader in HPC and its products include bullx, the energy-efficient supercomputer; bullion, one of the most powerful x86 servers in the world developed to meet the challenges of Big Data; Evidian, the software security solutions for identity and access management; Trustway, the hardware security module and Hoox, the ultra-secure smartphone. Bull is part of Atos.

For more information, **visit bull.com**

CT_170220_LPM_W-Nomadic_Evidian_en1

IMPRIM'VERT®

This brochure is printed on paper combining 40% eco-certified fibers from sustainable forests management and 60% recycled fibers in line with current environment standards (ISO 14001).

Trusted partner for your **Digital Journey**

Atos