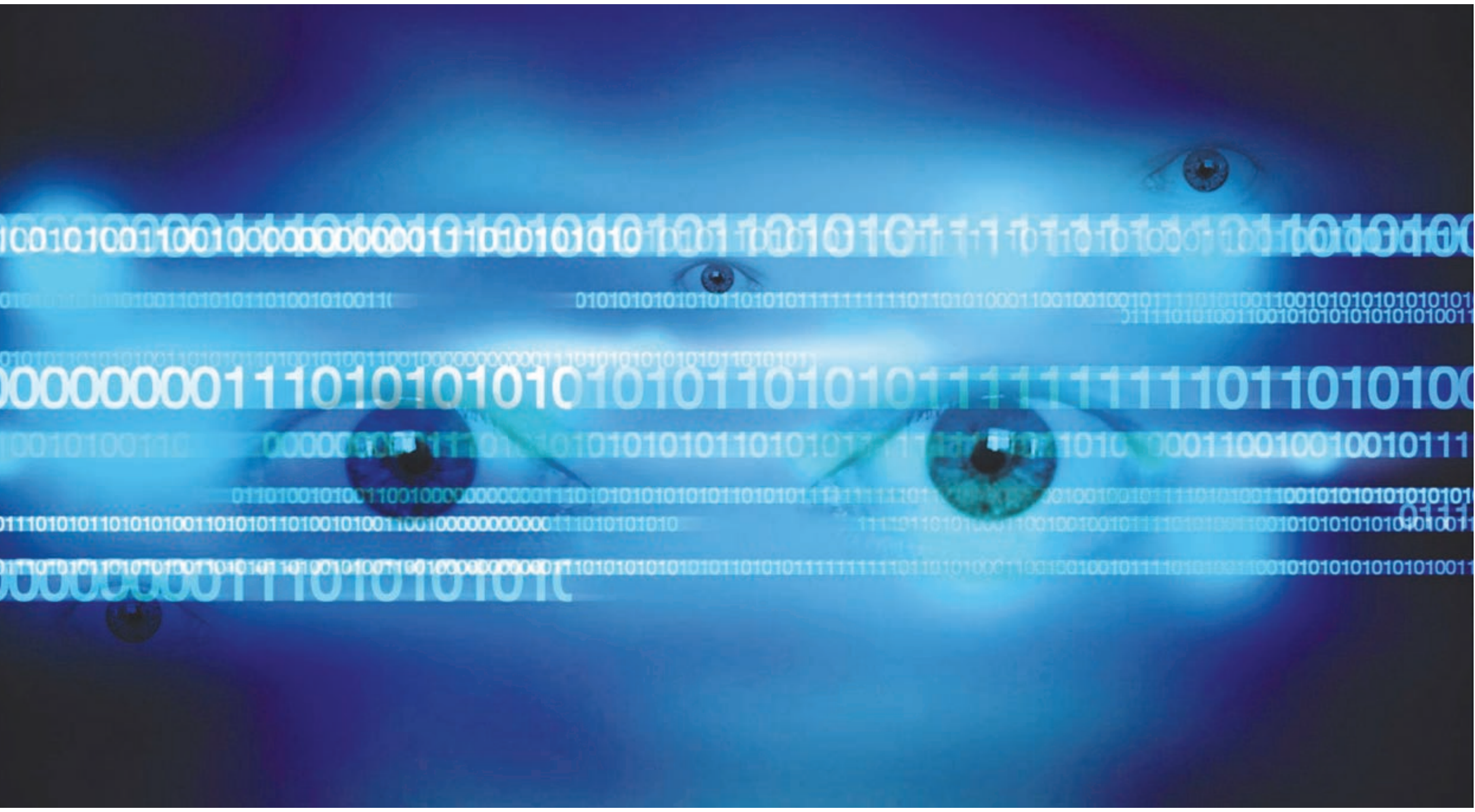
PLM IT REPORT

Reprint from No. 3 | May 2014 |

Product data deserves greater **protection**

www.plm-it-business.de

Product data deserves greater protection



The real value of a company is not to be found in gold or money, but in its data. The data embodies the intellectual property that gives a company its competitive edge. And it's not only the Chinese that have recognized it. The intelligence agencies in the West also appear to believe that no methods are taboo as they strive to access confidential information under the guise of combating terrorism. In an age of global collaboration, the protection of intellectual property has become a serious challenge.

Money and data have one thing in common: They need to circulate in order to grow. Even though the importance of intellectual property protection (IPP) is well understood, sensitive product information is generally less well protected when it is exchanged than money is during the course of financial transactions. The revelations made by whistleblower Edward Snowden have highlighted how easy it is to intercept data on its journey through the global data networks and how easy we make life for those involved in data espionage by exchanging information without any protection mechanisms whatsoever. We are inviting industrial espionage.

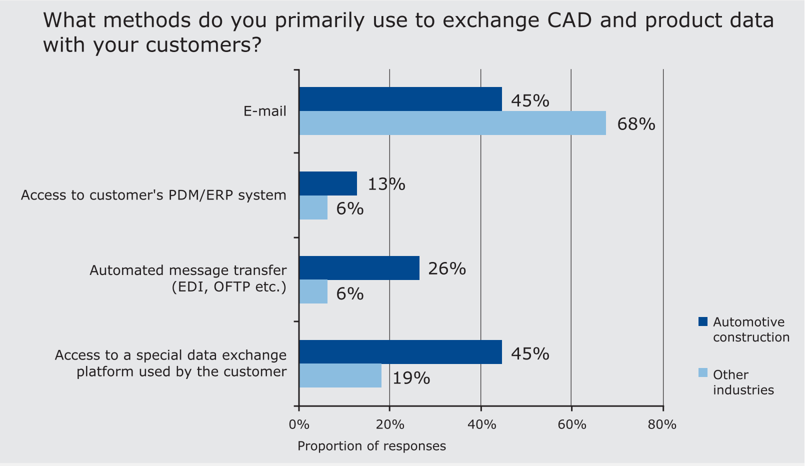
Despite all the security concerns and the data protection regulations that are in place in many companies, an alarming quantity of product data is still sent by email. These were the findings of a survey of over 1400 engineers from a wide range of industries carried out by the Fraunhofer IPK in conjunction with the PLM vendor CONTACT Software and the VDI. Even in the automotive industry, which is known for its strict requirements in respect of intellectual property protection, 45 percent of those surveyed said that they exchanged CAD data and product data with customers and suppliers by email. In other words, with no form of encryption, because the encryption mechanisms incorporated in the mail clients only cover the body of the mail, and not the attachments.

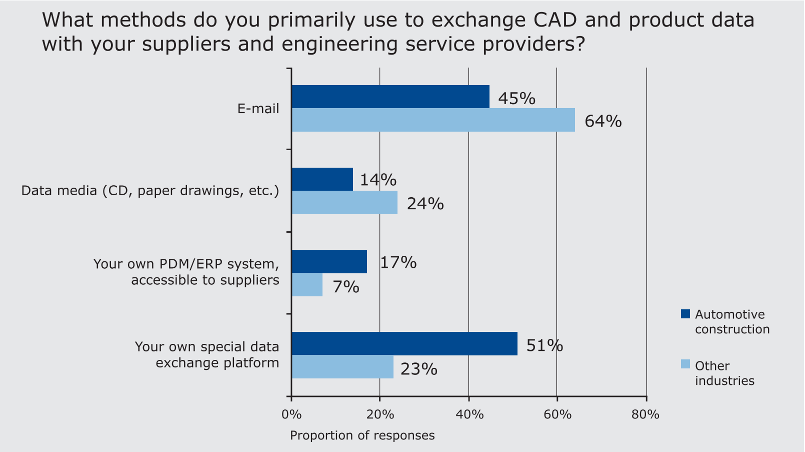
Secure data exchange via email

But it doesn't have to be that way, and one option is to use a data exchange solution such as OpenDXM GlobalX that can be fully integrated in Outlook. Although users continue to send data with their familiar email client as before, attachments of a given size, with certain filename extensions and/or to recipients in particular countries are automatically redirected to an exchange platform, where they are encrypted and made available for downloading. The rules are defined by the company concerned and stored together with the encryption mechanisms on a central server. If required, this server can also perform additional processing such as virus checking or conversion.

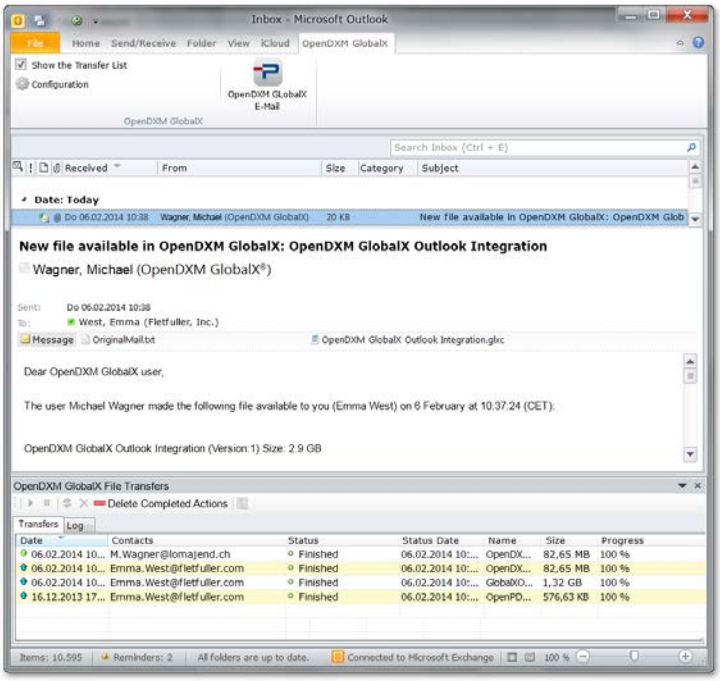
When it is uploaded, the data to be exchanged is encrypted using public-private-key cryptography methods with an encryption strength of up to 4096 bits, thus ensuring a high level of security. Unlike the supposedly secure SSL method used for transferring data to Web servers, which is relatively easy to crack. According to reports in the press, the NSA and the British intelligence agency GCHQ have developed a whole raft of different measures and technologies to overcome the encryption used in SSL connections and virtual private networks (VPNs) and intercept data before it is encrypted or after it has been decrypted. There are many different ways of combining encryption with other protection mechanisms, such as the use of a secure OFTP connection for sending data, which is of particular interest for companies in the automotive industry. Users can also assign higher security levels to individual files, only release them for a certain period or subsequently revoke release of the files.

The exchange platform supports different levels of encryption. In the case of normal encryption, the software manages the public and private keys and ensures that the data is automatically decrypted when it is downloaded by the recipient, so that the authorized recipient can read it. If the person sending the data decides to use the maximum security level of personal encryption, the recipient must be in possession of a private key that only they have access to in order to read the data. The exchange solution makes it possible to define not only new exchange partners, but also the required security level on an ad hoc basis. When personal encryption is used, a wizard in the software prompts the recipient to specify a storage location for the private key during an online session and to protect this location with a separate password.





From the survey „Kollaborative Produktentwicklung und digitale Werkzeuge. Defizite heute – Potenziale morgen" (Collaborative product development and digital tools. Today's shortcomings – Tomorrow's potential) by CONTACT Software, Fraunhofer IPK and VDI.



New file available in OpenDXM GlobalX: OpenDXM GlobalX Outlook Integration

Wagner, Michael (OpenDXM GlobalX®)

Sent: Do 06.02.2014 10:38
To: West, Emma (Fletfuller, Inc.)

Dear OpenDXM GlobalX user,

The user Michael Wagner made the following file available to you (Emma West) on 6 February at 10:37:24 (CET):

OpenDXM GlobalX Outlook Integration (Version:1) Size: 2.9 GB

Date	Contacts	Status	Status Date	Name	Size	Progress
06.02.2014 10...	M.Wagner@lomajend.ch	Finished	06.02.2014 10:...	OpenDX...	82,65 MB	100 %
06.02.2014 10...	Emma.West@fletfuller.com	Finished	06.02.2014 10:...	OpenDX...	82,65 MB	100 %
06.02.2014 10...	Emma.West@fletfuller.com	Finished	06.02.2014 10:...	GlobalXO...	1,32 GB	100 %
16.12.2013 17...	Emma.West@fletfuller.com	Finished	06.02.2014 10:...	OpenPD...	576,63 KB	100 %

Integration of OpenDXM GlobalX in Outlook makes encrypted data exchange as simple as sending an email.

Where are the keys? That is the question

The question of where the keys reside is far from trivial. It is not just the indiscriminate interception of data on the transatlantic glass fiber cables that has alarmed European businesses. They are even more worried about the fact that American IT giants such as Amazon, Google and Microsoft have helped or have been forced to help the NSA to spy on their customers. The USA Patriot Act obliges companies incorporated under American law and their overseas subsidiaries, as well as foreign companies operating servers in the USA, to allow the security authorities access to confidential data, including, in cases of doubt, the means of decrypting this data. The secretiveness of the American intelligence agencies means that nobody knows for sure whether they only assess this data for intelligence purposes or also for commercial purposes.

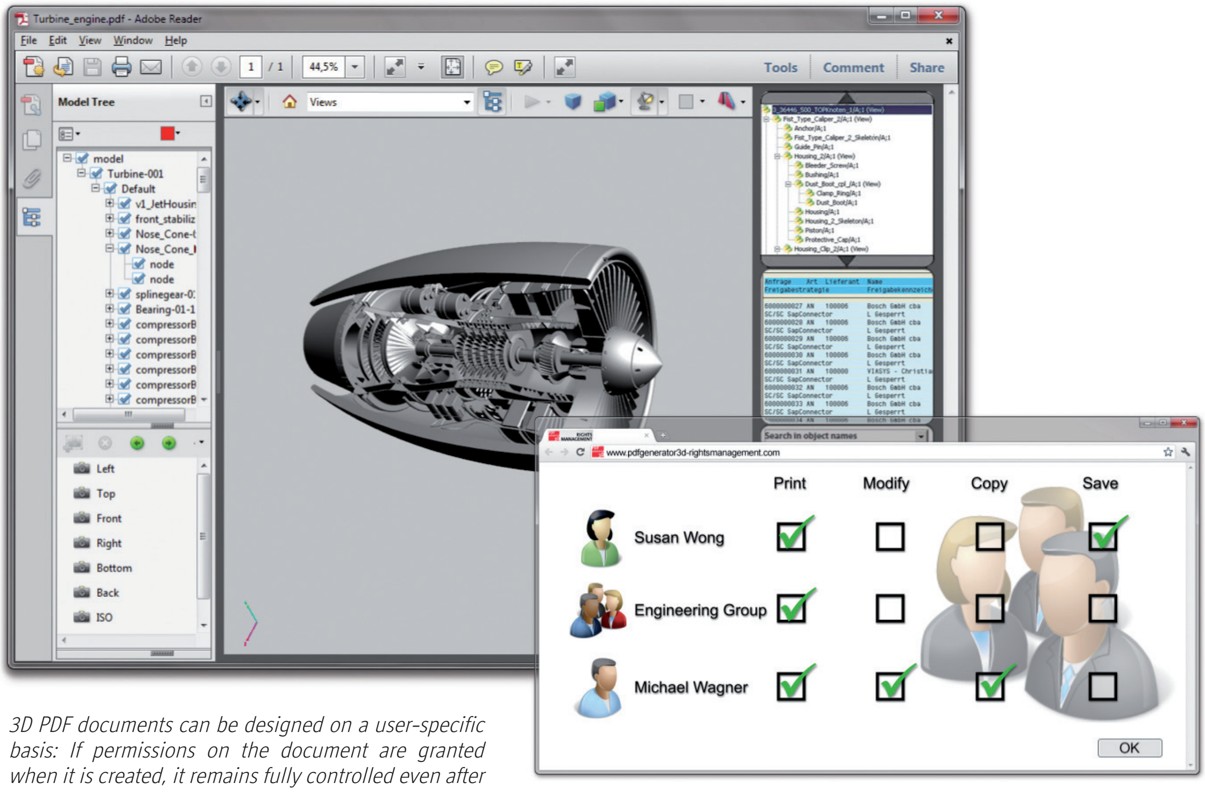
The remarkable thing is that this American legislation is nothing new. It passed into law shortly after the terror attacks on the World Trade Center on 11 September 2001. But the dramatic impact has only become clear in the light of the revelations about the machinations of the NSA and their colleagues. This has been a stab in the back for American providers of cloud-based solutions. In the meantime, telecommunications companies and other providers have been overwhelmed by inquiries from companies who want to move their data clouds to Europe, where far stricter data protection regulations apply. In concrete terms, this means Directive 95/46EG, although the European Court has ruled that this has not been implemented correctly in Germany.

But in terms of intellectual property protection, the crucial thing is not where the encrypted data resides, but whether the keys are safe from the prying eyes of the intelligence agencies and other parties involved in data espionage. In order to optimize data traffic over great distances, the data can be stored or replicated on local servers in the USA or elsewhere, after all, it is encrypted at all times. But to read the data, the recipient has to log in on the central data exchange server, which needs to be located in a country with stricter data protection regulations where intelligence agencies cannot simply demand the keys. And if the data is additionally personally encrypted, the agencies would also have to get their hands on the recipient‘s private key.

Protection behind the firewall as well

But it is not enough only to look for data security risks emanating from hackers and product pirates on the other side of the firewall. Another thing that Snowden has shown is that the greatest risk for data security lies in people and one‘s own staff, including the staff of partner companies. After all, it was the system administrator of an external consultancy contracted by the NSA who revealed the secrets of the most secretive of all American secret services. This means that protection of intellectual property cannot focus on data exchange alone. Instead, it has to start with the way in which sensitive data is handled within a company and its associates.

Companies with development locations distributed across the globe have to start thinking about what project data is needed at what locations and, in cases of doubt, they must make only this data available. Staff turnover in the emerging economies of Asia is higher, so it is not always possible to rely on the loyalty of the employees. A sophisticated role and permissions management system with multilevel user authentication is needed to control precisely which employees at which locations or in which partner companies are permitted



	Print	Modify	Copy	Save
Susan Wong	☑	□	□	☑
Engineering Group	☑	□	□	□
Michael Wagner	☑	☑	☑	□

OK

3D PDF documents can be designed on a user-specific basis: If permissions on the document are granted when it is created, it remains fully controlled even after it has been sent.
Images: PROSTEP

to access what data. Combining existing ADS/LDAP systems with the data exchange solution reduces the effort involved in defining user permissions and allows single-sign-on user authentication.

Data integrity in the global development networks in the automotive or aerospace industries is exposed to considerable risks as the composition of these networks often changes from project to project. The partners have to exchange large volumes of information in order to coordinate their work. This increases the risk of data getting into the wrong hands. Companies therefore need tools that allow them to control the level of detail in the data they provide.

The use of „intelligent“ development tools means that the CAD models contain a considerable amount of design and manufacturing know-how. The solution cannot be to simply dumb down the models. Instead, it must be possible for the exchange partners to explicitly suppress information in a graduated way depending on the recipient of the data or the processes it is needed for. For coordination purposes, it is generally sufficient to convert the data to a lightweight, neutral format such as 3D-PDF. Server solutions such as PROSTEP PDF Generator 3D are able to do this fully automatically while providing comprehensive protection functions. If the data is then to be used again in downstream processes, it is often necessary to revert to the native data format in which sensitive data has been masked.

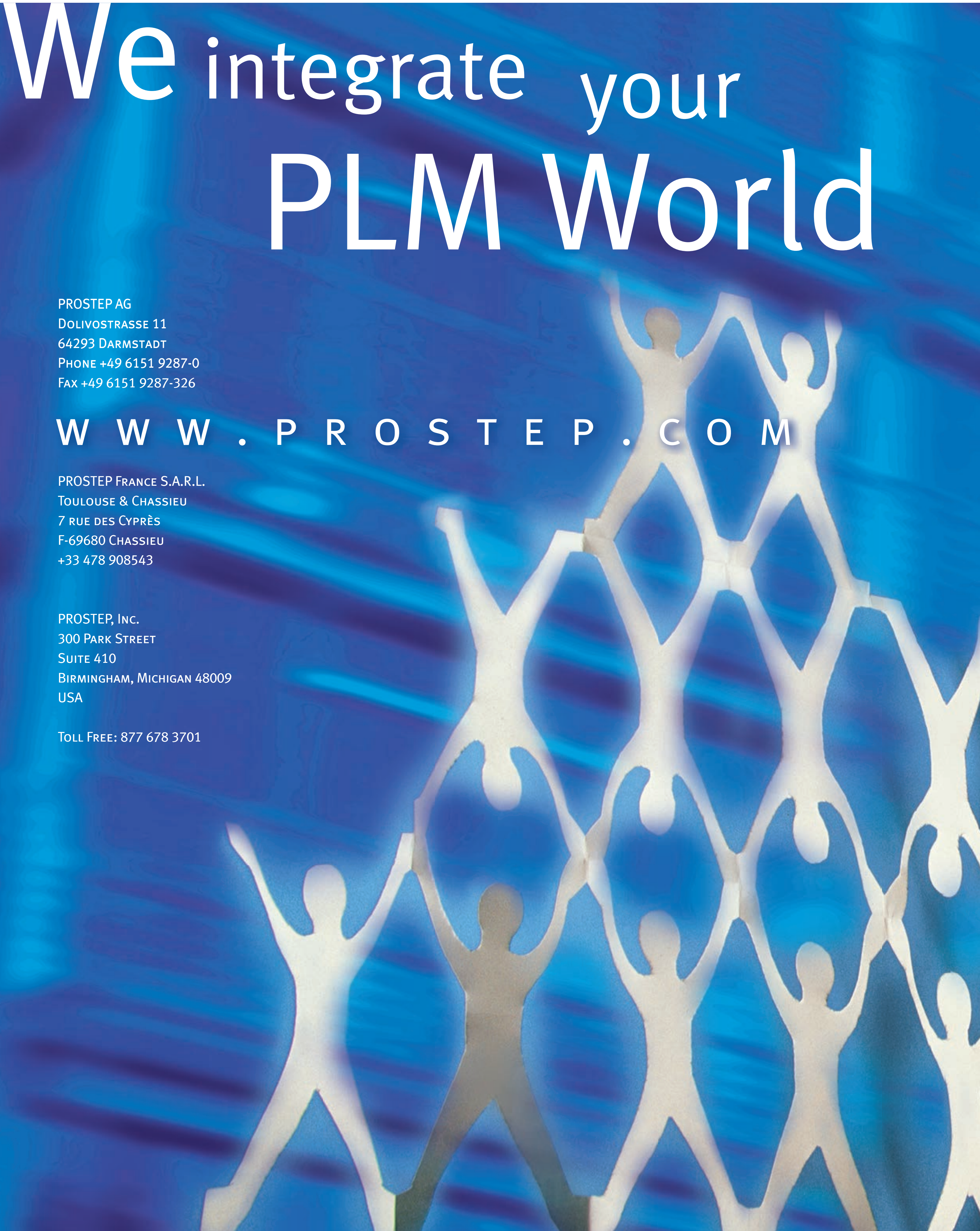
Given the quantity of data exchanged nowadays in the development networks of the automotive or aerospace industries, it is no longer feasible for selection of the information that is to be exchanged and data preparation to be done by hand. From the perspective of data security, it is therefore crucial that the tools for converting or masking data can be fully integrated in the data exchange process. This is the only way to allow automation of the processing operations and avoid user errors when choosing the scope of the information to be exchanged. In other words, maximum data protection requires a combination of different technologies and a comprehensive package of measures that takes account of internal as well as external risks. -sg-

Michael Wendenburg, Sevilla
(www.wendenburg.net)

PROSTEP AG, Darmstadt,
Phone +49 6151 9287-0,
www.prostep.com

PROSTEP
integrate the future

We integrate your PLM World



PROSTEP AG
Dolivostrasse 11
64293 Darmstadt
Phone +49 6151 9287-0
Fax +49 6151 9287-326

WWW.PROSTEP.COM

PROSTEP France S.A.R.L.
Toulouse & Chassieu
7 rue des Cyprès
F-69680 Chassieu
+33 478 908543

PROSTEP, Inc.
300 Park Street
Suite 410
Birmingham, Michigan 48009
USA

Toll Free: 877 678 3701