PROSTEP
integrate the future

Whitepaper

DATA SECURITY
AND KNOW-HOW PROTECTION

Our data is constantly exposed to the danger of being intercepted or stolen as it wends its way over global data networks. Data security measures and measures for protecting intellectual property should not, however, first be implemented when data is exchanged – companies must lay the foundation for these measures within their own organization. What is needed is a comprehensive security concept that specifies the protection objectives and the measures needed to achieve them based on analyses of possible threats and the probability of these threats materializing. In this context, consideration should be given to two different dimensions, namely protection against deliberate attacks and protection against human or technical error.

DATA SECURITY MADE IN GERMANY

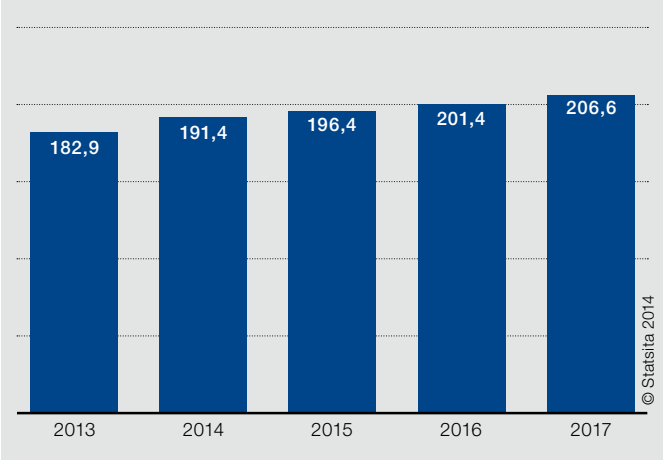
Content

Introduction/Abstract

The scandal surrounding the NSA‘s surveillance of Internet communications makes it clear just how vulnerable our data is as it wends its way over the global data networks. Data security measures and measures for protecting intellectual property (Intellectual Property Protection, IPP) should not, however, first be implemented when data is exchanged – companies must lay the foundation for these measures within their own organization. What is needed is a comprehensive security concept that specifies the protection objectives and the measures needed to achieve them based on analyses of possible threats and the probability of these threats materializing. In this context, consideration should be given to two different dimensions, namely protection against deliberate attacks (*security*) and protection against human or technical error (*safety*). The implementation of such a security concept requires integrated tools and services from a reliable software and system vendor that is familiar with its customers‘ processes.

The challenge of global data communication

The majority of today's business communication takes place via email. This significantly increases the risk of unintended data loss or deliberate theft. The misappropriation of sensitive internal business information can have catastrophic effects – it is said, for example, that the collapse of Lehman Brothers stock in the run-up to the global financial crisis was triggered by the unauthorized disclosure of an internal email. What this means for IT managers is that they not only have to protect emails and email systems from external threats (viruses,Trojans, etc.) but, at the same time, also ensure the integrity of the information sent, prevent the unintentional leaking of confidential information and guarantee the traceability of data communications in the event of legal disputes. Not an easy task in view of the growing volume of digital information.



Forecast of the number of emails sent daily around the world from 2013 to 2017 (in billions)

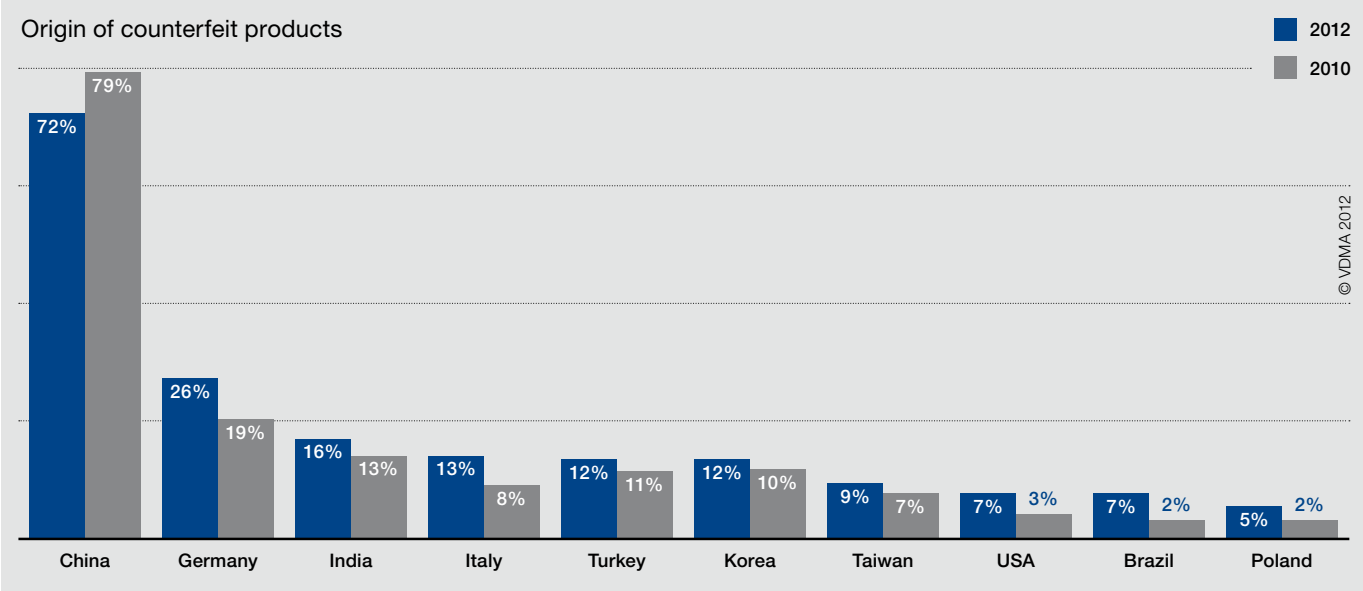
According to current surveys, approximately 191 billion emails are sent daily around the world. It is estimated that no more than 3 percent of these are encrypted, even if they include confidential information and/or attachments containing financial data, legal documents, patient data, copyrighted image and music data or sensitive product data. In principle, an email is no more secure than a postcard because, unlike conventional business letters, there is no signature or envelope that vouches for the authenticity of the sender and the reliability of the information. Even if they are encrypted, the encryption mechanisms offered by email programs only encrypt what is known as the body text of the email and not the attachments; and in any case – as the revelations of whistleblower Edward Snowden demonstrate – they are easy to crack.

Most vulnerable are the attachments, which often contain particularly sensitive information. This also applies, albeit not exclusively, to product data and the know-how it contains. Regardless of the threat posed to intellectual property protection and the security regulations in place at many companies, an alarmingly large amount of product data is still exchanged via email. This was demonstrated by a study conducted in 2011 by the Frauhofer IPK together with the PLM vendor CONTACT Software and the Association of German Engineers (VDI) involving over 1,400 engineers from a number of different industries. Even in the automotive industry, with the extremely high demands it places on know-how protection, 45 percent of those surveyed indicated that they use email to exchange CAD and product data with customers and suppliers.

The careless handling of product data is not the only reason that product piracy has increased so dramatically, but it is certainly one of the reasons. Current estimates by the German Association of Chambers of Industry & Commerce (Deutscher Industrie und Handelskammertag, DIHK) indicate that product piracy costs the German economy alone 50 billion euros every year – more than twice the amount than just a few years ago. According to the DIHK, two thirds of all counterfeit products come from China and Hong Kong, with a slight downward trend; the cases of counterfeits from Singapore and India, on the other hand, are increasing. The theft of intellectual property represents a major threat in particular for small and medium-sized companies, which cannot support heavyweight legal departments. The global competitive advantage derived from their expertise is eroded; if they act as suppliers, they may not be awarded series production contracts despite developing successful solutions or, as OEMs, may find their image tarnished by low-quality pirate copies.

Internal and external threats to data security

The above-mentioned figures compiled by the DIHK indicate that product piracy is wider spread in some countries than in others. Countries like China, which were late to industrialize and which have a legitimate interest in the transfer of knowledge and technology, place a different value on the protection of intellectual property. Companies from the West often have to enter into joint ventures with local companies in order to gain access to the respective market. This means that they are faced with the question of how to integrate these locations and subsidiaries in their IT infrastructure without exposing their intellectual property to possible attacks. Several automotive OEMs, for example, no longer allow sites in countries that pose a potential risk to directly access their IT systems but rather make the product data available to them on a separate platform.



The People's Republic of China remains the number one country of origin when it comes to product and brand piracy. Germany as country of origin was named by a quarter of the companies affected.

But there is no need to travel that far abroad to find the secret coves where product pirates are hiding. According to figures from the German Engineering Federation (VDMA), German companies come in second behind China as counterfeiters in the field of machinery and plant engineering. What is worse is the fact that, while China's share of counterfeit components, spare parts, etc. has decreased over the past two years, the share held by German counterfeiters has increased.

Risk posed by disloyal employees

Access to sensitive product data within a company is usually regulated by means of a (role-based) authorization concept, which is normally mapped in a product data management (PDM) or product lifecycle management (PLM) solution. How well it protects sensitive data also depends on how carefully employees handle permissions and passwords. In any event, the implementation of a security concept means that employees need to be educated about risks to data security and their awareness of their own behavior and that of their colleagues raised.

The greater threat to data security and intellectual property is namely not necessarily posed by intelligence services, hackers or other data pirates but rather by disgruntled, disloyal employees. Caution should in particular be exercised at overseas locations with numerous new employees and at locations with a high level of staff turnover. IT system administrators constitute a special risk group since they, as super users, are not subject to the authorization concept and have direct access to the information stored in the database. It is not surprising that it was a system administrator at one of the NSA's outside consultancy companies who revealed the secrets of the most secret of all American secret services. Several automotive suppliers have established a rule for their sensitive styling data stipulating that this data will only be replicated at other locations if requested by an authorized project member.

Engineering collaboration as an Achilles' heel

The protection of intellectual property during product development is particularly important to a company's competitiveness because the theft or misuse of information at this early stage may cost a company its time-to-market advantage. And this advantage is particularly crucial for the success or failure of a product, in particular in the fast-moving consumer goods sector. But at no other phase of the product lifecycle is intellectual property as vulnerable since the digitization of product development means that an increasing amount of product-related data has to be generated and made available to other departments, locations or even external partners in digital form so that downstream processes can be performed.

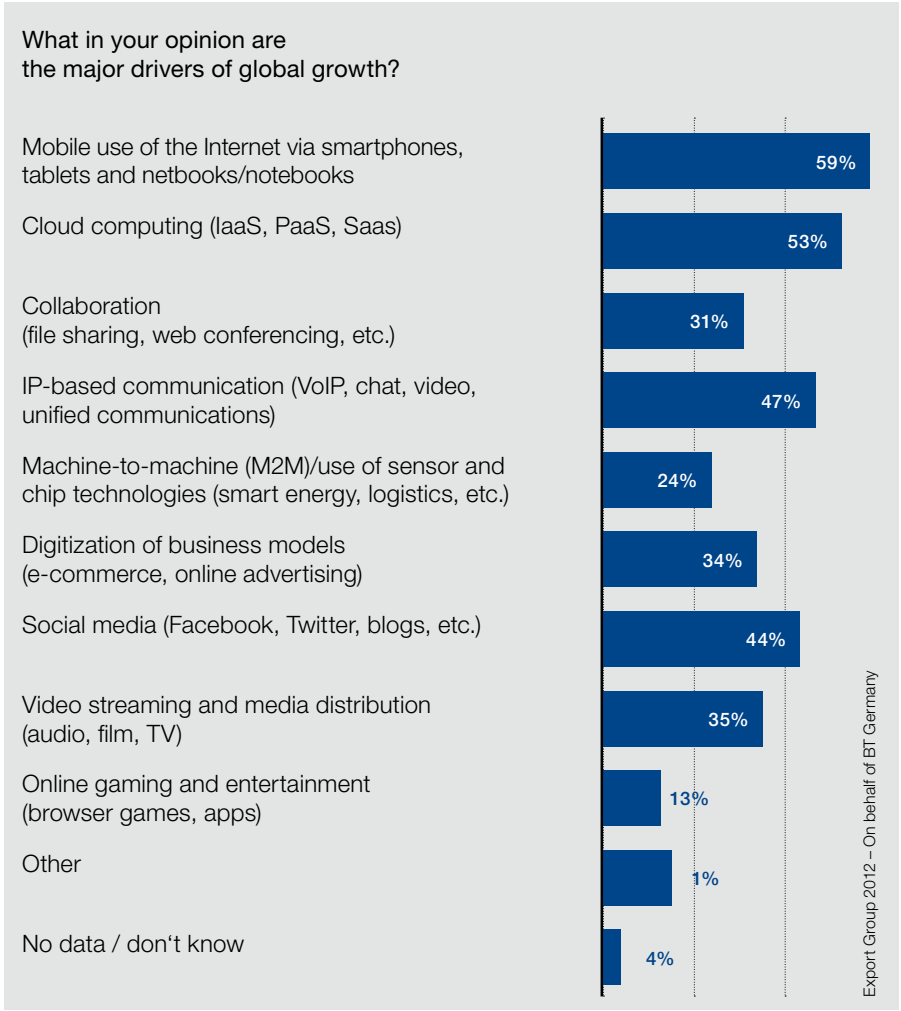
Digital product development has not only resulted in more data but also in data that contains an increasing amount of information in need of protection. Parametric CAD/CAM systems allow the design and manufacturing know-how stored in the heads of experienced engineers to be mapped in the form of rules or intelligent features to make it more easily accessible to younger users and utilize it to automate certain downstream processes. As a result, the CAD models to be exchanged inevitably include an increasing amount of content that cannot be allowed to fall into the wrong hands. In many cases, however, customers demand that their suppliers make the native CAD data available to enable them to process it more efficiently.

Collaboration with external partners is a data security Achilles' heel in two respects: Firstly because CAD data and other documents have to be exchanged via global data networks and are thus exposed to the prying eyes of intelligence services and other non-authorized persons; secondly, because the misuse of information by collaboration partners who are authorized to access this information cannot always be ruled out. The people responsible for data security must therefore give thought to which data should be exchanged in which formats and in which information depth with which partners. An important criterion in this context is the downstream processes for which the data is required. At the same time, they must ensure that data can be prepared according to these rules with as little time and effort as possible.

As a result of global collaboration and the trend toward outsourcing, the volume of product data being exchanged daily via data networks worldwide has dramatically increased in recent years and decades. In industries like the automotive or aviation industry in particular, product development today is distributed over a long chain of system suppliers, development offices and other suppliers. If they are to harmonize their work, they must transfer huge volumes of data and information within short time frames or allow the other partners in the development network direct access to their databases. A dangerous balancing act, especially for suppliers, since many project partners could be competitors when it comes to the next project.

Data explosion as a result of cloud computing

In addition to collaboration, cloud computing is contributing to the fact that the volume of data in the world's data networks is exploding and new security gaps are emerging. A study commissioned by BT Germany indicated that, according to high-ranking IT experts, the driving forces behind the rapid growth of global data are mobile Internet communication, cloud computing and Internet-based communication via VoIP, video, chat and the like. Mobile access to data gives rise to additional data security requirements that have to be taken into consideration when establishing IT architectures. At the same time, shifting data to the cloud raises the question as to how secure it is against attacks by secret services, hackers and other data pirates.



Data explosion as the result of mobile use and cloud computing

Many companies in Germany take a skeptical view of using the cloud to store sensitive data, or they are only willing to accept the idea in the form of a private cloud that can be operated by a trusted provider. The fact that major US American IT companies like Amazon, Google and Microsoft actively helped the NSA spy on their customers or were forced to help has only increased their skepticism. Under the USA Patriot Act, US companies and their foreign subsidiaries, but also non-American companies with servers in the USA, are obligated to provide security agencies with access to confidential data, which in case of doubt also includes the tools needed to decrypt it. To be on the safe side, many companies are therefore looking for German, or at least continental European, providers for their cloud-based services.

Definition of a comprehensive security concept

The starting point for a comprehensive security concept is an analysis of the threat and the potential impact of data loss or data theft. Which data in the company is particularly sensitive and which is particularly vulnerable? Based on these questions, there are a few basic things that need to be clarified first of all: for example, which data always has to be managed in-house, which data can be replicated at all locations (e.g. standard parts) and which cannot, which data can be stored in the cloud if necessary, which security-related requirements does the operator of a cloud infrastructure have to meet, which service providers are allowed access to the data, for example for data conversion and data exchange, and so on.

Assessing information protection

In order to clarify these and other questions relating to data security and know-how protection and define the necessary protection measures, IT experts recommend an initial assessment performed by an outside consultancy company. In addition to assessing the risks and defining the protection objectives, the aim of such an assessment is to raise the awareness of the people involved and, above all, that of executive management, which has to approve the funds required for the protective measures. Money whose return on investment is difficult to calculate because its very objective is to avert quantifiable damage.

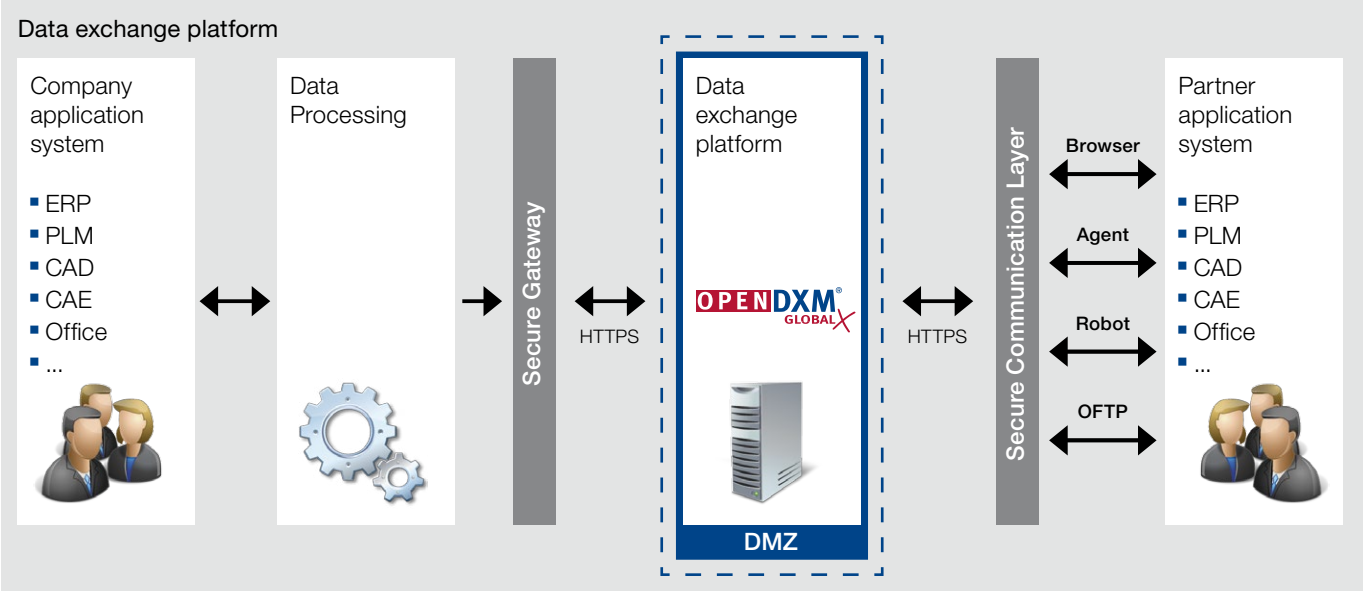
There are as many approaches to providing protection as there are potential risks. Therefore the focal points of the security concept should be specified within the framework of the assessment before qualitative and quantitative protection objectives for the individual application scenarios are worked out by key persons in workshops. After analysis and processing of the results, the consultants can provide the customer with clear recommendations for action and submit proposals for the appropriate course of action.

Implementing a security concept

The appropriate course of action could, for example, comprise developing a rough concept for the target process after examining the knowledge holders and knowledge transfer paths, as well as creating a topology of the risk areas and protection classes. A pilot implementation of certain key scenarios that can be played through with the users is recommended to ensure the feasibility of the concept and examine how the protective measures fit into operational workflows. This provides the basis for developing a specialist concept for implementation of the processes and their support in productive operation. It is important during implementation that training on how to use the new rules for know-how protection be provided and that mechanisms to keep track of compliance with the rules and their effectiveness be developed. If necessary, operation of the security solution can be outsourced to an external partner.

The basis for secure data communication

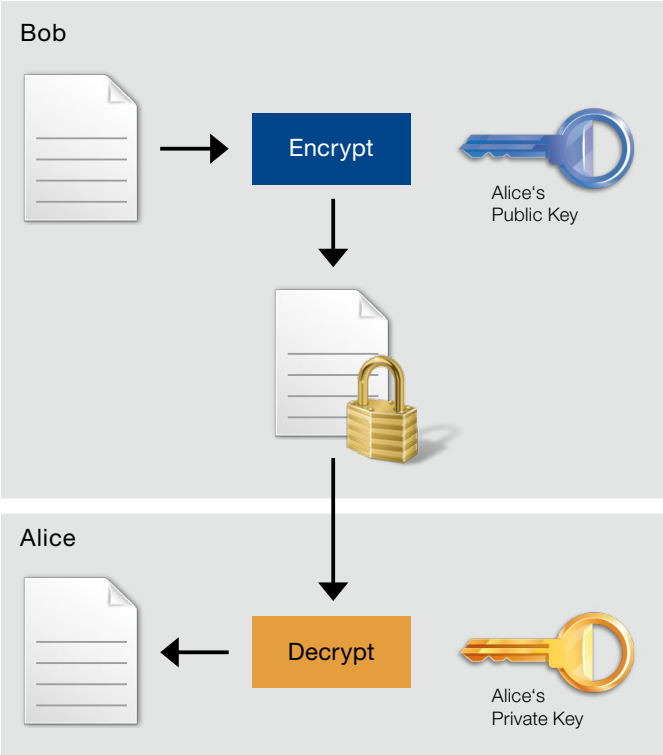
A prerequisite for secure data exchange is controlled data management within the company itself, for example through the use of a PDM/PLM solution or an integrated PDM/ERP system. As long as data is managed in a normal file directory without graduated access authorization, it is impossible to rule out the possibility that the wrong versions or data leaves the company without appropriate authorization. A key requirement for a secure data exchange platform is therefore that it can be seamlessly integrated in the existing IT landscape using appropriate interfaces. The OpenDXM GlobalX data exchange platform gives due consideration to this requirement by providing connectors to leading PDM/PLM and ERP systems and a Microsoft Outlook Integration component.



For practical purposes, a data exchange platform is installed on a separate server in the company's demilitarized zone (DMZ) that acts as the project owner; it can however also be hosted by an external provider. Regardless of the encryption of the data itself, data transfer to the platform and between the platform and recipient should be performed using an encrypted HTTPS connection. Combining encryption with other protection mechanisms, for example sending the data via a secure OFTP connection, may be of interest to companies in the automotive industry.

Multilevel data encryption

To provide maximum security, the data exchange platform should support a multilevel encryption concept. Ideally, the data to be exchanged is highly encrypted during upload using public/private key encryption, e.g. with keys of up to 4096 bits in length, and not decrypted until it is downloaded by the recipient, thus ensuring that the data is always stored on the data exchange platform's server in encrypted form. It is also advantageous if each individual document or data package can be protected with a separate, individually generated key. This allows users to assign certain files a higher security level, release them for a certain period of time only, or cancel their release at a later point in time.



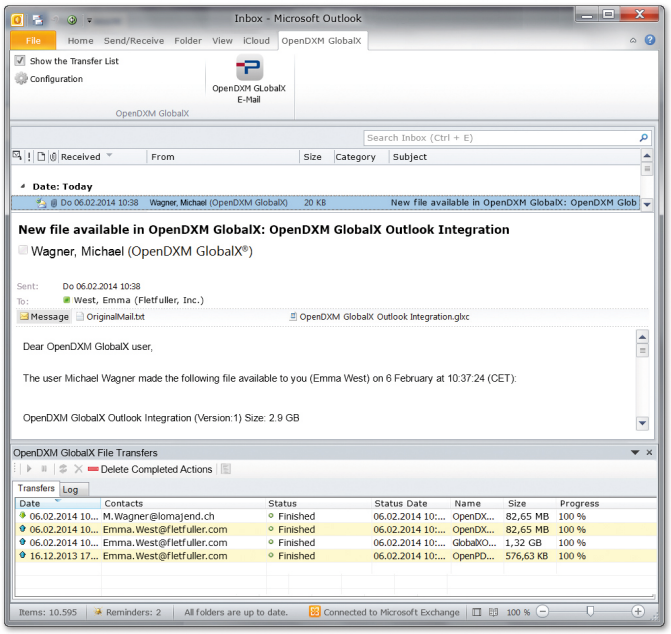
Multilevel data encryption

The level of encryption selected will have an impact on the question of who has ultimate control of the keys. In the case of normal encryption, the software manages the public and the private key and ensures that the data is automatically decrypted when it is downloaded so that the authorized recipient can read it. If, on the other hand, the person sending the data decides to use the highest level of security, i.e. personal encryption, the recipient must have a private key to which only they have access in order to read the data. The exchange solution should provide tools that enable the desired level of security to be defined ad hoc. A prerequisite for this is that new recipients can specify where they want to store the private key (e.g. on their own computer, a USB flash drive, a memory card, etc.), and with which password protection, during an online session.

An important requirement with a view to data security is the option of managing the encrypted data separately to the keys on decentralized servers. This separation not only minimizes data traffic over long distances but also offers the advantage that the data exchange platform together with key management can be operated in a country where intelligence agencies cannot simply demand that the keys be handed over. Without the keys, the encrypted data in the remote file vaults is of little use to them. In the case of personal encryption, they would even have to ask the individual recipients to hand over the keys.

Integration in email processes

Even the best encryption is useless if it is not used in the hustle and bustle of day-to-day business. It therefore makes sense to link the exchange of encrypted data with normal email processes. The data exchange platform's client application should be fully integrated in the user interface of the email program so that users can send large files or files containing sensitive content from their familiar work environment. It is important that the company or the system administrator be able to define uniform rules for determining which files are to be sent automatically via the platform. One criterion is, without doubt, file size in order to overcome the limitations of Outlook when sending large amounts of data. It may also be advisable to always make files with certain extensions or files intended for recipients in certain countries available in encrypted form. In addition to the option of giving users rules, it should also be possible for users to decide for themselves which data they want to send via the platform.



From the recipient's point of view, the data exchange platform must provide support for different scenarios. Companies that do not use a corresponding data exchange solution themselves favor an easy-to-use web portal for downloading data that is opened when they click on a link in the notification email; all that remains for them to do is enter the password. Companies that have their own Microsoft Outlook integration component want to be able to open the data directly in their email environment as they would any other attachment. Acceptance of the solution also depends on it being possible for data to be sent to recipients for whom no profile has yet been stored in the system. This means it must be possible to create an ad hoc account with limited rights, and preferably do so automatically.

With the OpenDXM GlobalX Outlook Integration component, encrypted data exchange is as easy as sending an email.

Controlled data access, even when on the go

A multilevel authentication concept is recommended if access to the data is to be controlled. If a password and key are not sufficient, a chip card, which must be supported by both the software and hardware, can also be used for authentication purposes. Insofar as the customer in question is already using an ADS/LDAP system for user login and authentication, they should also be able to use this system together with the data exchange platform to, for example, set up single sign-on. It must be possible to identify recipients using reliable procedures – before being given access to the data, for example, they have to have confirmed receipt of the data to the sender.

New requirements arise as the result of the popularity of mobile input devices such as iPads and iPhones, which users also want to use to access the data exchange platform. Appropriate applications or apps are therefore needed to provide access to user accounts and enable Office, PDF and graphic files to be downloaded and viewed offline. Even when it comes to mobile access, data security must be guaranteed at all times by means of explicit authentication and data encryption.

Monitoring and logging exchange operations

In certain industries, companies today are legally and/or contractually bound to document which information and documents were exchanged with which partners and when. The data exchange platform should therefore be able to store all information about the exchange operations in a database in an audit-proof manner so that it can be used, for example, for audit purposes. This makes it easier for companies to meet compliance requirements. Integration of the data exchange platform in the email application offers the advantage that the body text of the original email can be stored in the database together with the information about the exchange operations, thus making it possible to perform full-text searches according to sender, recipient, subject or other search criteria.

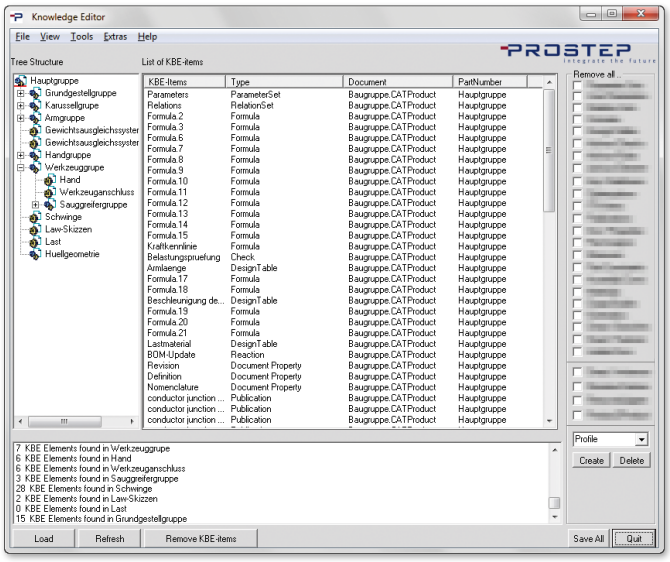
In addition to logging the exchange operations for audits, the application should also support control of day-to-day operation. This can be done, for example, by means of a clear graphical user interface that lists all the transfer operations with the data volume, number of users, transfer threads, etc. To ensure smooth operation, the system should inform the administrator of which keys are about to expire, which storage quotas for user accounts have been exhausted and so on. It is also advantageous if time-controlled maintenance functions are, for example, available for locking user accounts, specifying times for archiving and deletion and automatically executing the operations, thus reducing administrative overhead.

Increased security as the result of automated data preparation

With a view to protecting intellectual property, not only control of the exchange operations but also control of the information to be exchange plays an important role. Ideally, only the information required to perform the respective downstream operations should ever be made available or exchanged. Native CAD data is not required for many work steps – neutral formats with reduced information content or even lightweight viewing formats are perfectly sufficient. Manual selection of the information would, however, be much too complex and time-consuming, which is why certain automatic mechanisms for data preparation must be implemented in the exchange process. The definition of these automatic mechanisms requires precise knowledge of the processes within a company and across corporate borders. A competent team of consultants can provide valuable help in this context.

Hiding native CAD data

The embedding of an increasing amount of intelligence in the product data makes preparation of the information to be exchanged vital. If native CAD data needs to be exchanged because, for example, the customer demands it, all the elements that contain sensitive design and manufacturing know-how should be suppressed. Something that is easier said than done: Dumbing down “intelligent” CAD models across the board by removing these elements in their entirety is not the solution as these elements normally serve as references for other objects. Furthermore, data that has been modifed is often returned during the course of development, and the changes would then have to be incorporated in the original model by hand.



Among other things, the project software Knowledge Editor supports analysis of the CAD models to determine the knowledge they contain and protects company know-how by removing knowledge components from the CAD model.

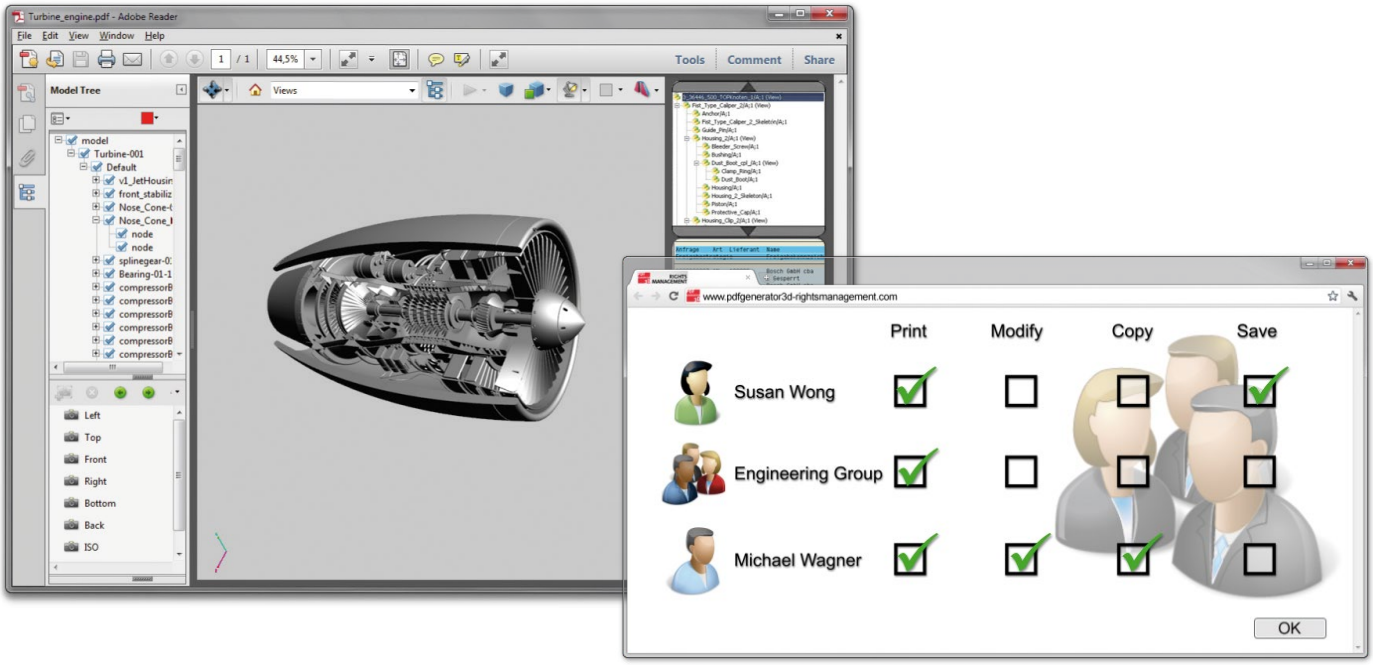
Therefore special tools like PROSTEP’s Knowledge Editor, which can be used to analyze the interrelationships and structures of CAD models with the objective of filtering out and hiding specific knowledge components, are needed. To minimize the time and effort needed for hiding, it is recommended that it be decided which exchange partners are to receive which information and which knowledge components are never to leave the company and then use the knowledge filter as a batch program. The knowledge components can be reattached when the exchange models are returned for modification with the help of appropriate program extensions.

Automatic generation of 3D PDF documents

Reconciling data security and seamless process continuity requires a certain balancing act. On the one hand, it should be possible to prepare information as required, on the other hand, this information should be available for everyone to use. Flexible solutions for preparing and distributing CAD and other product data within a company and the extended enterprise are needed if this balancing act is to be achieved. It should be possible to integrate them in both the PDM/PLM or PDM/ERP solutions and in the data exchange platform so that processes such as making data available can be automated with the help of intelligent document templates. PROSTEP addresses these requirements with its PDF Generator 3D.

A key requirement for cross-enterprise communication is the availability of data and information in a format that can be read by all those involved, if possible without the need to install additional software. 3D PDF documents can be viewed with the free Adobe reader, which is installed on practically every computer workstation, and offers the added advantage that 3D and 2D data can be combined, something that is required for many business processes. It is, of course, crucial that 3D models from all leading CAD systems can be embedded and interactively visualized.

A description of the functional scope and the many application options provided by 3D PDF technology is not the subject of this white paper (see the white paper on 3D PDF technology). Of primary interest in this context is the question of what it can contribute to data security and know-how protection. A prerequisite is that the information made available can be configured flexibly and that the use of this information downstream can be controlled even after the 3D PDF documents have been sent. It should therefore be possible to store corresponding rules in the application so that, for example, the level of detail and the resolution with which the CAD models are to be converted and embedded in the 3D PDFs can be specified. It is also important for data security purposes that the individual data and documents can be protected by passwords or digital signatures, even if they are combined in a single structured PDF portfolio for easier handling.



Graduated security mechanisms are required to configure access to 3D PDF documents user specifically and control the transfer and use of these documents once they have been sent. To do this, certain rights can be assigned to the 3D PDF document when it is created, for example the right to cut sections through the models and ascertain dimensions, which activate the corresponding Adobe reader function at the recipient's end. Others can be activated or deactivated later on. If necessary, the solution should be combined with a comprehensive digital rights management module in order to assign individual user rights. The recipient must use a key to log in to a certain secure server in order to be able to view, copy or print the 3D PDF document. Once user rights

have been defined, they can be granted for a limited period of time and can also be revoked again, thus allowing the owner to retain full control of their document even if the document is not located in their access area.

Automatic mechanisms are important tools for avoiding unintentional mistakes when transferring data and increasing data security. A key requirement in this context is the ability to define uniform templates for the transfer of certain information, which can be filled with certain metadata automatically, and that this data can be reintegrated in the backend systems. A prerequisite for this are appropriate interfaces to the backend systems and the ability to access this information with the help of Web services.

Automated data exchange

As far as processes are concerned, an essential requirement is the ability to integrate tools for data preparation and for the derivation of neutral formats in the IT infrastructure. This can be done by automatically converting the data and storing it in a secondary format in the PDM/PLM solution when there is a change in status, or by calling the conversion tool when a data exchange operation is triggered so that the data can be converted at runtime. The latter offers the advantage that the amount of data made available can be controlled dynamically depending on the recipient or recipient country involved.

Appropriate robot functions are needed to control conversion and the exchange of the data with the data exchange platform. All the user has to do is select the recipient and, if necessary, the desired target format; the software performs all other operations in the background. Provided that the appropriate interfaces are available, the data can also be sent directly from the PDM/PLM environment.

It might also be more efficient for capacity reasons or because special know-how is required to outsource data conversion and quality assurance to an external service provider, for example the cloud-based conversion service OpenDESC.com. In this case, the service provider must be integrated in the process like any other partner so that it receives the converted data via the platform in encrypted form and return it there in encrypted form or, if appropriate, make it available directly to the ultimate recipient.

PROSTEP‘s approach: Data Security Made in Germany

The growing demands relating to data security and know-how protection necessitate a comprehensive security concept that includes not only data exchange but also the processes for preparing data and making it available. In order to implement this concept, companies need innovative solutions for secure data exchange which, ideally, are integrated in the email application in addition to their traditional data management systems. They also need supplementary solutions for preparation of the data and for derivation of neutral formats in order to be able to control the scope of information made available. And they are dependent on the support of a competent software and system vendor that provides them with support during implementation of the various solution components.

PROSTEP AG’s objective is to set new standards worldwide with data security technology from Germany. The offering comprises the following tools and services:

- PROSTEP’s data exchange platform OpenDXM GlobalX is used by leading companies in the automotive industry and other industries around the world and, thanks to its Microsoft Outlook integration component and support for mobile and devices, also by users outside of the classic engineering field.
- PROSTEP’s PDF Generator 3D is the perfect addition to the data exchange platform and allows information to be made available for different business processes in a secure, uniform format that can be read by all those involved.
- PROSTEP’s Knowledge Editor makes it possible to analyze CAD models with the objective of filtering out specific knowledge components in order to protect company know-how when transferring data to customers or development partners.
- The competent team of consultants at PROSTEP AG provides customers with advice on analyzing potential security risks during data exchange and other business processes and provides them with support for integrating the different solution components in their enterprise applications.

PROSTEP AG
Dolivostrasse 11
64293 Darmstadt
Germany

Phone +49 6151 9287-0
Fax +49 6151 9287-326

info@prostep.com
www.prostep.com

Do you have any comments or questions?

We look forward to your feedback
at infocenter@prostep.com

PUBLICATION INFORMATION

Published by

PROSTEP AG

Responsible for the content

Joachim Christ

Edition 1, 2014