Schutz von Daten und KnowHow im Agile EDM System mit EAC Add-On

Dr.-Ing. Helmut Maier, Dipl.-Ing. Matthias Mayer
Dr. Maier CSS GmbH & Co.KG
Stutensee, Technologie Region Karlsruhe, Deutschland

Schlüsselworte:

Agile, PLM, PDM, EDM, EAC, Access Control, Intellectual Property, Produktpiraterie, Markenschutz, Zugriffskontrolle, Berechtigung,

Einleitung

Eine Umfrage des VDMA Frankfurt beziffert die jährlichen Umsatzverluste im deutschen Maschinen- und Anlagenbau durch Produktplagiate und Know-How-Piraterie auf mehr als 6 Milliarden Euro. Die VDMA Umfrage aus 2010 benennt 68 Prozent der 3.000 VDMA-Mitglieder, die von Produktpiraterie betroffen sind. Unter den befragten Firmen geben 59% an, dass sie Geheimhaltung/Zugriffsschutz als präventive Schutzmaßnahme neben anderen treffen wollen.

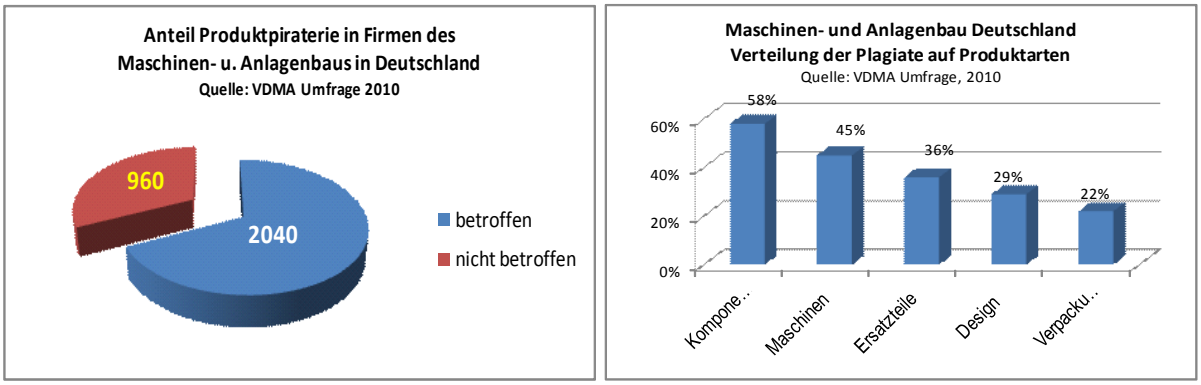


Abb. 1: Produktpiraterie – Auszug aus den Ergebnissen der VDMA Umfrage 2010

Agile EDM verwaltet Produktdaten über den gesamten Produktlebenszyklus und kontrolliert die Zugriffsberechtigung jedes einzelnen Benutzers. Das Agile EDM Add-On Modul EAC – Extended Access Control – erweitert die Möglichkeiten der gezielten Zugriffskontrolle auf Stammdaten, Stücklisten, Unterlagen oder Projektinhalte beliebig für Geschäftseinheiten, Standorte, Abteilungen, Projektteams, Kunden oder Lieferanten.

EAC lässt sich in einer bestehenden Agile EDM Anwendung leicht einrichten. Der Aufwand für Installation, Pflege und Update ist gering. Das bestehende Customizing bleibt fast unberührt. Vorhandene Schnittstellen zu CAD, ERP oder zu anderen Applikationen werden von EAC mit überwacht.

Wirksamer Schutz von Daten und KnowHow im Agile PLM System mit EAC

Produktdaten sind wertvoll und müssen wirksam geschützt werden. Durch die globale Zusammenarbeit eines Unternehmens wird die Zugriffskontrolle auf Produktdaten und Unterlagen von unterschiedlichen Geschäftspartnern, Geschäftseinheiten, Teams und Standorten aus extrem wichtig. Datenbanken mit umfangreichen Design- und Produktdaten sind inzwischen beliebter Angriffspunkt für Produktpiraten. Ungeschützte Visualisierung mit oftmals einfachen Shareware/Freeware Viewern machen es den Produktpiraten leicht, schnell an sensible Entwicklungsdaten und Designs zu gelangen. Ohne ausgefeiltes Konzept für dedizierten Zugriffsschutz bieten sie eine große Schwachstelle.

Mandantenfähigkeit im PLM wird immer wichtiger, damit Geschäftsbereiche ihre PLM Daten autark im Agile PLM System verwalten können. Anstelle des Einrichtens von mehreren PLM-Umgebungen kann dies durch den EAC-Modul erreicht werden.

Mit dem EAC Add-On werden die Agile Standards für den Zugriffsschutz werden noch um verschärfte, objektbezogene Zugriffskontrollen und Benutzerberechtigungen erweitert. So kann der Zugriff auf Produktdaten und -strukturen einerseits flexibel, andererseits aber dennoch sehr restriktiv behandelt werden.

Das Funktionsprinzip von EAC basiert einerseits auf einer sogenannten Access-Liste an den zu schützenden PLM-Objekten wie bspw. Unterlagen, CAD-Dokumente, Artikelstämme, Stücklisten oder Projekte und Unterprojekte sowie andererseits auf der Festlegung von Berechtigungsgruppen. Diese können statisch nach Geschäftsbereichen, Standorten oder Abteilungen definiert sein oder dynamisch nach Projektteams, Lieferanten oder Kunden gebildet werden. In jedem Fall benötigt der Anwender natürlich eine eindeutige Autorisierung im Agile EDM System mit individuellem (und möglichst periodisch wechselndem) Passwort.

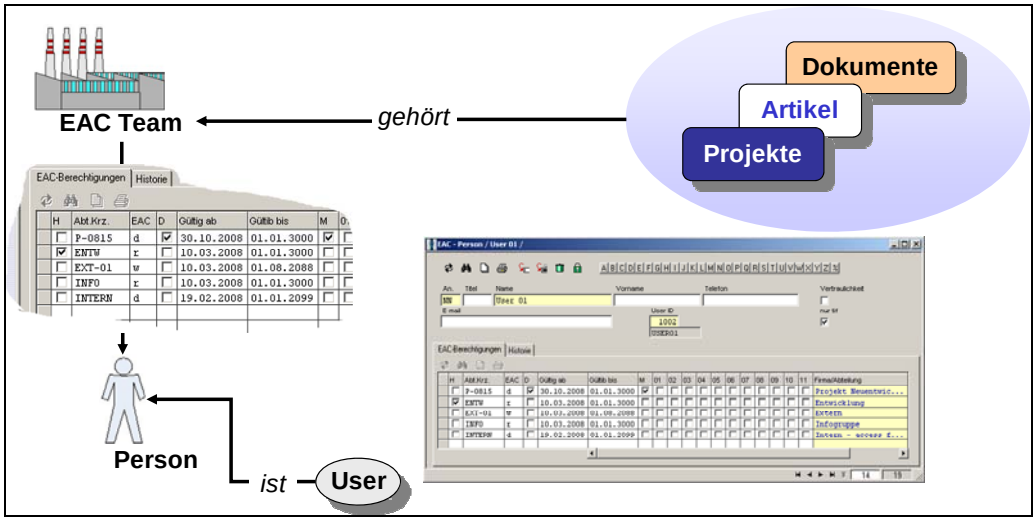


Abb. 2: Zuordnung von organisatorischen Einheiten, Benutzern und PLM-Daten und -strukturen

Grundlage für EAC sind Zuordnung des Anwenders zu Teams, Abteilungen oder sonstigen Geschäftsbereichen sowie die Zuordnung von Artikeln, Modellen, Zeichnungen, Unterlagen und Projekten zu diesen organisatorischen Einheiten. EAC kontrolliert jede PLM Entität und ihre Beziehungen zueinander. Zusammenarbeit und Informationsaustausch mit anderen Standorten, Lieferanten oder Kunden werden vereinfacht. EAC macht die Abläufe in Engineering und Logistik sicherer.

EAC lässt sich in einer bestehenden Agile PLM Anwendung leicht einrichten. Aufwand für Installation, Pflege und Update ist gering. Das bestehende Customizing bleibt fast unberührt. Vorhandene Schnittstellen zu CAD, ERP oder zu anderen Applikationen werden von EAC mit überwacht. EAC Lizenzen beziehen sich auf Applikationsserver oder auch auf Firmenstandorte.

Berechtigungsgruppen werden unterschieden nach organisatorischer Einheit, Team oder Info-Gruppen. Eine Gruppe kann sich aus Kategorien von operativen oder von informellen Benutzern zusammensetzen:

- Operative Benutzer haben Lese-, Schreib- und Löschrechte. Informelle Benutzer haben in der Regel nur Leserecht.

- Das Einrichten eines neuen Benutzers mit Username und Passwort sowie dessen grundlegende Berechtigungen übernimmt in den meisten PLM-Installationen immer noch der PLM-Administrator. Für die Anforderung, einen neuen Benutzer anzulegen, wird oftmals ein firmenspezifischer Workflow mit entsprechender Checkliste für die Festlegung seines Rechteprofils benutzt.

- Darüber hinaus können Gruppen- oder Teammanager festgelegt werden, die für das Anlegen von Gruppen und für die Administration der Teammitglieder und deren Berechtigungen innerhalb der Gruppe zuständig sind. Ein Teammanager benötigt keine PLM Administrator Rechte.

- Ein Benutzer kann Mitglied in mehreren Gruppen sein und unterschiedliche Rechte je Gruppe haben. Ein operativer Benutzer ist immer genau einer Home-Group zugeordnet. Er kann sich selbst oder durch den Teammanger dann einem Arbeitsteam (default work team) zuordnen.

- Die Zuordnung eines Benutzers zu einer Gruppe hat eine zeitlich begrenzte Gültigkeit, die vom Teammanager festgelegt wird und die jederzeit verlängert oder gelöscht werden kann. Der Benutzer hat dann mit sofortiger Wirkung keinen Zugriff mehr innerhalb dieser Gruppe.

- Für PLM Objekte, die jeder Benutzer sehen darf, wie bspw. Liefervorschriften oder Normblätter, ist ein Team WORLD definiert, dem keine Personen zugeordnet werden. PLM Objekte, die dem Team WORLD zugeordnet sind, sind somit für jeden Benutzer im System sichtbar, sofern er die PLM Basisrechte dazu hat. Falls ein PLM Objekt nicht mehr öffentlich sein soll, wird es einfach aus WORLD entfernt und in eine andere EAC Gruppe geschoben.

Die Verwaltung der Benutzer, deren Zuordnung zu Gruppen und deren Berechtigungen in diesen Gruppen wird über eine relativ einfach zu bedienenden Maske durch den Gruppen-Administrator oder Teammanager vorgenommen.

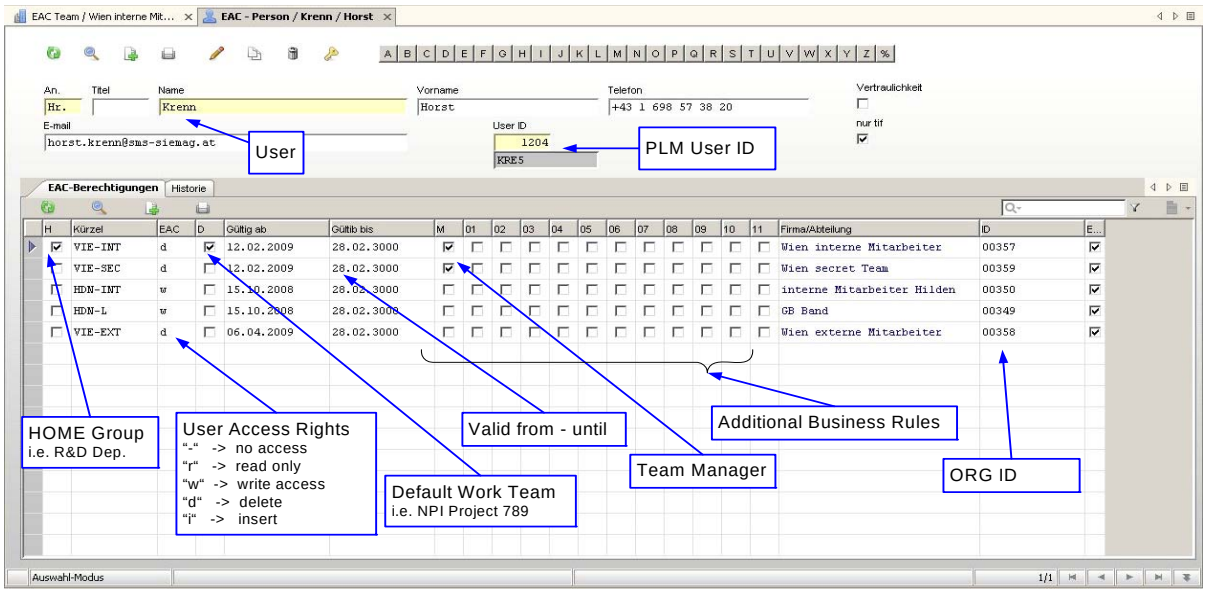
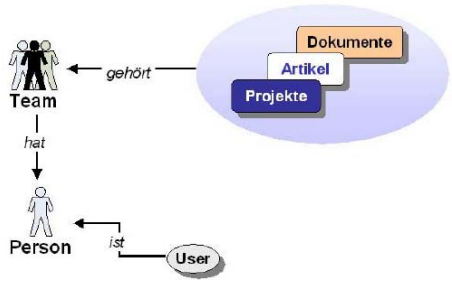


Abb. 3: PLM Maske, mit der Benutzer, Rechte, Gruppenzuordnungen und Regeln festgelegt werden

Falls die einfache Zuordnung und Festlegung der Rechte nicht ausreicht, können Regeln zugeordnet werden, die im Zusammenhang mit dem Benutzer und der betreffenden Zuordnung zur Gruppe stehen (siehe Abbildung 3 oben).

Mit EAC wird die Basis-Zugriffskontrolle des PLM Systems nicht aufgehoben. Hat auf Grund dieser Rechte ein User kein Recht für ein Element, so kann dies durch EAC nicht übergangen werden. EAC erweitert allerdings die Zugriffskontrolle durch feinere Abstimmung auf die zu kontrollierenden PLM-Objekte wie Artikel, Dokumente, Projekte und den dazu gehörenden Strukturen im Kontext mit Zuordnung zu organisatorischen Einheiten des Unternehmens und übergreifenden Teams.



Ein zu schützendes PLM Objekt besitzt sowohl eine eindeutige Berechtigungsgruppe (Home Group), als auch weitere Zuordnungen von Berechtigungsgruppen, denen ebenfalls unterschiedliche Rechte bezüglich dieses PLM Objekts zugeordnet sind.

Welche Aktion das Mitglied eines Teams mit diesem PLM Objekt ausführen darf, ist in der unten dargestellten Maske der EAC Benutzerverwaltung vom jeweiligen Teammanger festgelegt worden.

Abb. 4: Zuordnung von PLM Objekten zu Teams bzw. Benutzern

Über ihre objektspezifische EAC Accessliste werden die PLM Objekte für diejenigen Gruppen markiert, die auf dieses Objekt zugreifen dürfen. Die EAC Accessliste kann an jedem Objekt entweder in der Formular- oder in der Listmaske editiert werden, das heißt, Rechte können sehr schnell zusätzlich zugeordnet oder auch wieder weggenommen werden. Das ist bspw. interessant, wenn kurzfristig eine Entwicklung oder Fertigung von einem Standort auf den anderen verlegt werden soll, aber nach bestimmter Zeit wieder wegfällt.

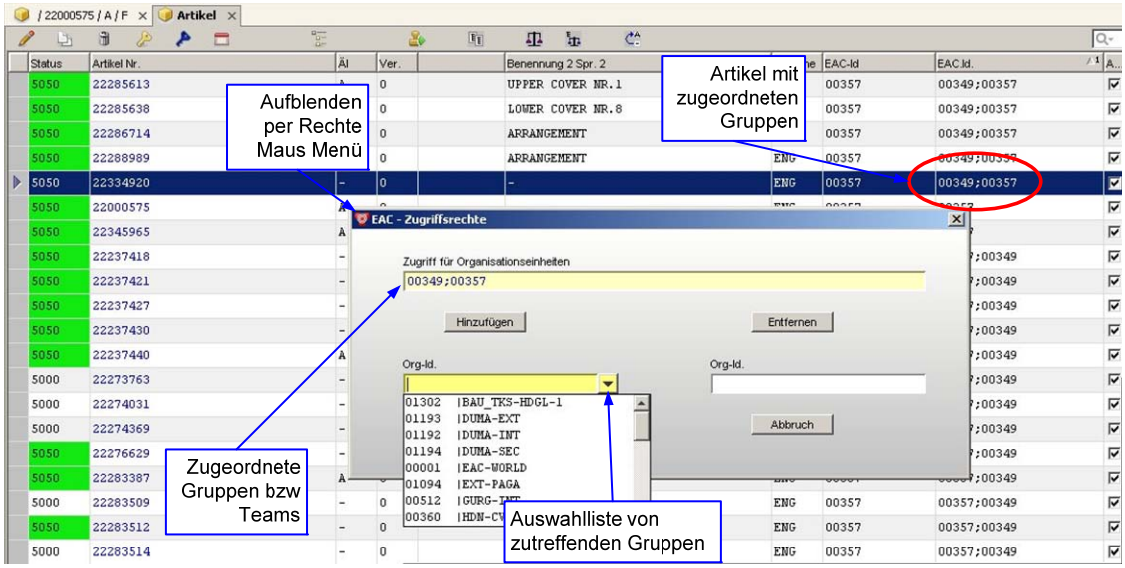


Abb. 5: Einfaches Zuordnen von Berechtigungsgruppen zu einem PLM Objekt (hier Artikel)

Zum einfacheren Handling können Teams allen Elementen entlang einer PLM Objektstruktur wie bspw einer 3D CAD Dokumentstruktur in einem Vorgang zugeordnet werden. Änderungen der Berechtigungsdefinitionen werden in der Historientabelle des PLM Objekts automatisch vermerkt. Somit sind Vorgänge und ausführende Benutzer dokumentiert und jederzeit nachvollziehbar.

Die Suchfunktion im PLM System ist angepasst. Nach Gruppen-Idents kann gesucht werden. Die Trefferliste der Suchfunktion zeigt nur diejenigen Objekte an, für die der Benutzer eine entsprechende Zugriffsberechtigung hat. Beim Selektieren und Laden einer 3D CAD Dokumentstruktur prüft EAC, ob der Benutzer auf alle Objekte der Struktur ein Zugriffsrecht hat (mindestens LESEN). Falls irgendein Objekt in der Struktur für seinen Zugriff gesperrt ist, wird die gesamte Struktur nicht geladen. Der Benutzer bekommt von EAC eine entsprechende Meldung mit der Anzahl der Objekte angezeigt, auf die er keinen Zugriff hat.

Die EAC Funktionen lassen sich PLM technisch und organisatorisch leicht in den laufenden PLM Betrieb einbinden. Der Schulungsaufwand für Administratoren und Benutzer ist minimal. Mit EAC ist die Verwaltung und Zuordnung der Benutzerrechte übersichtlich und für den Tagesbetrieb ohne zu große Zusatzaufwände beherrschbar. Insbesondere die Organisation der Teams kann in die Fachbereiche des Unternehmens verlagert werden. Das erhöht im Fachbreich die Flexibilität und entlastet gleichzeitig die PLM Administration.

Die EAC Teamdefinition im PLM System kann Schritt für Schritt und von Fachbereich zu Fachbereich eingeführt werden. Die Berechtigungen lassen sich jederzeit ergänzen oder entfernen. Durch den Projektbezug und die zeitliche Gültigkeit der EAC Rechte wird automatisch verhindert, dass unberechtigte Benutzer auch lange Zeit danach noch Zugriff auf Projekte und Daten hätten.

Innerhalb kurzer Zeit profitiert das Unternehmen von der intensiveren Kontrolle über die Zugriffe auf Daten und über Visualisierung von sensiblen Entwicklungsdaten. Das Intellektuelle Eigentum des Unternehmens kann durch Agile EDM mit dem EAC Add-On noch besser geschützt werden, als bisher. Firmen setzen das ein, um so den Zugriff auf Daten für externe Personen, Zulieferanten, Praktikanten oder für Standorte einzuschränken, um somit bestimmte Daten des Produkts oder einer neuen Entwicklung vor fremdem Zugriff zu schützen. Das sichert die Wettbewerbsfähigkeit und reduziert das Risiko der Datenpiraterie erheblich.

Der Nutzen für das Unternehmen ist monetär bewertbar. Die Amortisationszeit für diese Investition ist sehr kurz. EAC stellt so eine äußerst wirtschaftliche Zusatzlösung zum Agile EDM System dar.

--- *** ---

Kontaktadresse für Agile e6 EAC:

Dr.-Ing. Helmut Maier,
Dipl.-Ing. Matthias Mayer

Dr. Maier CSS GmbH & Co.KG
Am Sohlweg 6
DE 76297 Stutensee

Telefon: +49 (0) 7244 947-100
Fax: +49 (0) 7244 947-105
E-Mail helmut.maier@maiercss.de, matthias.mayer@maiercss.de
Internet: www.maiercss.de