

Enterprise Rights Management

RECOMMENDATION

Enterprise Rights Management
Version 1.1



Abstract

This document provides recommendations for the adoption of ERM technology especially for the cross-enterprise exchange of sensitive data such as product data or bidding documents. It describes a reference process for the introduction and use of the technology as well as a reference system architecture. Where applicable, standards are proposed for the interfaces between the systems involved.

Disclaimer

ProSTEP iViP Recommendations (PSI Recommendations) are recommendations that are available for anyone to use. Anyone using these recommendations is responsible for ensuring that they are used correctly.

This PSI Recommendation gives due consideration to the prevailing state-of-the-art technology at the time of publication. Anyone using PSI Recommendations must assume responsibility for his or her actions and acts at their own risk. The ProSTEP iViP Association and the parties involved in drawing up the PSI Recommendation assume no liability whatsoever.

We request that anyone encountering an error or the possibility of an incorrect interpretation when using the PSI Recommendation contact the ProSTEP iViP Association (psi-issues@prostep.com) immediately so that any errors can be rectified.

Copyright

- I. All rights to this ProSTEP iViP Recommendation, in particular the copyright rights of use and sale such as the right to duplicate, distribute or publish the recommendation remain exclusively with the ProSTEP iViP Association and its members.
- II. The recommendation may be duplicated and distributed unchanged, for example, for use in the context of creating software or services.
- III. It is not permitted to change or edit this recommendation.
- IV. A suitable notice indicating the copyright owner and the restrictions on use must always appear.

Table of Contents

1 Preamble	1
2 Multi-level Approach	2
3 Use Cases and Main Requirements	2
3.1 Protection Level One	2
3.1.1 Use case: internal data exchange	3
3.1.2 Use case: document access	4
3.1.3 Use case: document from content system	5
3.2 Protection Level Two	5
3.2.1 Cross-company ERM use	6
3.2.2 Use case: content integration	6
3.3 Protection Level Three	7
3.3.1 Use case: multi-tier use	8
4 Reference Infrastructure and Architecture	9
4.1 ERM infrastructure in the context of the zone model	9
4.2 ERM reference architecture	10
4.3 Communication between parties involved in ERM data exchange	12
4.3.1 Direct communication between data exchange partners	12
4.3.2 Indirect Communication between Data Exchange Partners	13
4.4 Watched folders for automatic ERM-based folder protection	14
4.5 PDM integration	14
4.6 Identity management	16
4.6.1 Extranet scenario	16
4.6.2 Federated identity management scenario	17
4.7 Role-based assignment of rights	18
4.7.1 Role-based assignment of rights in Protection Level One and Two	18
4.7.2 Role-based assignment of rights in Protection Level Three	20
4.8 Minimal set of rights	22
5 Reference Process	24
5.1 Introduction and methodology	24
5.1.1 Introduction for reference processes	24
5.1.2 The Big Picture	24
5.1.3 Modeling methodology	25
5.1.4 Overview of ERM introduction and ERM usage	26
5.2 ERM administrative process	26
5.2.1 Preliminary tasks for ERM introduction	28
5.3 Processes for certain use cases	31
5.3.1 Data exchange	31
5.3.2 Providing documents received from partner to a third party	32
Glossary	36
References	37
Annex A : Cross-enterprise ID Solution Outline	38
Annex B : Cross-enterprise ID Technical Recommendation	38
Annex C : Reference Processes	38

Figures

Figure 1: Protected data cannot reach unauthorized users	1
Figure 2: ERM in the context of the zone model	9
Figure 3: Reference architecture	10
Figure 4: Function of and interaction between the ERM components	11
Figure 5: Direct communication between the parties involved in ERM data exchange	12
Figure 6: Indirect communication between the parties involved in ERM data exchange	13
Figure 7: Extranet scenario	17
Figure 8: Federated identity management scenario	17
Figure 9: Administration of users and roles in a multi-tier scenario – stage 1	19
Figure 10: Authentication of a user in stage 1	20
Figure 11: Administration of users and roles in a multi-tier scenario – stage 2	20
Figure 12: Authentication of a user in a multi-tier environment– stage 2	21
Figure 13: The Big Picture for reference processes	24
Figure 14: Modeling methodology for reference processes	25
Figure 15: Simplified overview of ERM introduction and ERM usage	26
Figure 16: 'ERM administrative processes' process diagram	27
Figure 17: 'Preliminary tasks for ERM introduction' process diagram	29
Figure 18: 'Data exchange' process diagram	31
Figure 19: General use case involving three main actors	33
Figure 20: 'Providing documents received from partner to third party – Alternative' process diagram	24

Tables

Table 1 Symbols used for modeling reference processes	24
---	----

Abbreviations, definitions, references

CAD	Computer Aided Design
DLP	Data Leakage Prevention
DMS	Document Management System
DMZ	Demilitarized Zone
DX	Data Exchange
EDM	Electronic Data Management
EDX/EDI	Electronic Data Exchange/Interchange
ERM	Enterprise Rights Management
GUI	Graphical User Interface
IdM	Identity Management System
OEM	Original Equipment Manufacturer
PDM	Product Data Management
PLM	Product Lifecycle Management
PoC	Proof of Concept
RBAC	Role-based Access Control
SADT	Structured Analysis and Design Technique
SSO	Single Sign-On
TDM	Technical Data Management