*Kazimierz Krupa**

INTEGRATED SYSTEMS' ARCHITECTURES AND SECURITY INSTRUMENTS

Corporate portal is an important element of companies' integrated operating system architecture. The portal is required to execute its tasks in effective and safe manner. Data encoding, individual access keys, scoring applications and many other special instruments are utilised to achieve this goal.

Selected architectures of integrated operating systems and tasks of information portals

New economy requires active business units should interact and communicate directly to other partners in the specific business chain. Precise customer-reorientation is also expected, which results in fundamental change to the process of adding value. With its increasing worth the information has become an independent value in the e-business. It is important then to integrate precisely all information systems, which could be helpful in getting customer's satisfaction (CRM, PRM) and receiving strategic signals that enable „to take the jump forward on the market". While creating the architecture of such systems we can use ready models describing their structure, or the methods of construction of information modules, or sophisticated computer programs. Such programs make it possible to develop the applications for rebuilding current process models and to „conquer" selected market segment. Complete reengineering of business processes is effectively supported by the architectures of integrated information systems: (CIMOSA (Open System Architecture for Computer Integrated Manufacturing), GRAI (Graphes de Resultats et Activites Interrelies), GIM (GRAI Integrated Methodology), PERE (Purdue Enterprise Reference Architecture), GERAM (Generalized Enterprise Reference Architecture and Methodology), IFIP (Information System Methodology), SOM semantic object modelling Ferstla and Sinza, ISA (Information System

---

* University Rzeszow, 35 959 Rzeszów, ul. Rejtana 16 C, tel. (0 prefiks) 17 27 61 347, E-mail: kkrupa@pf.pl

Architecture Kromer) or the ARIS (Architecture of Integrated Information Systems)[1] [7, 8, 9,14] method, which is very popular in Poland. Frequently, the information portal is the main component[2] of „new" information system of a New Economy company. Portals are tools providing free access to necessary data and information. Generally, based on criterion of

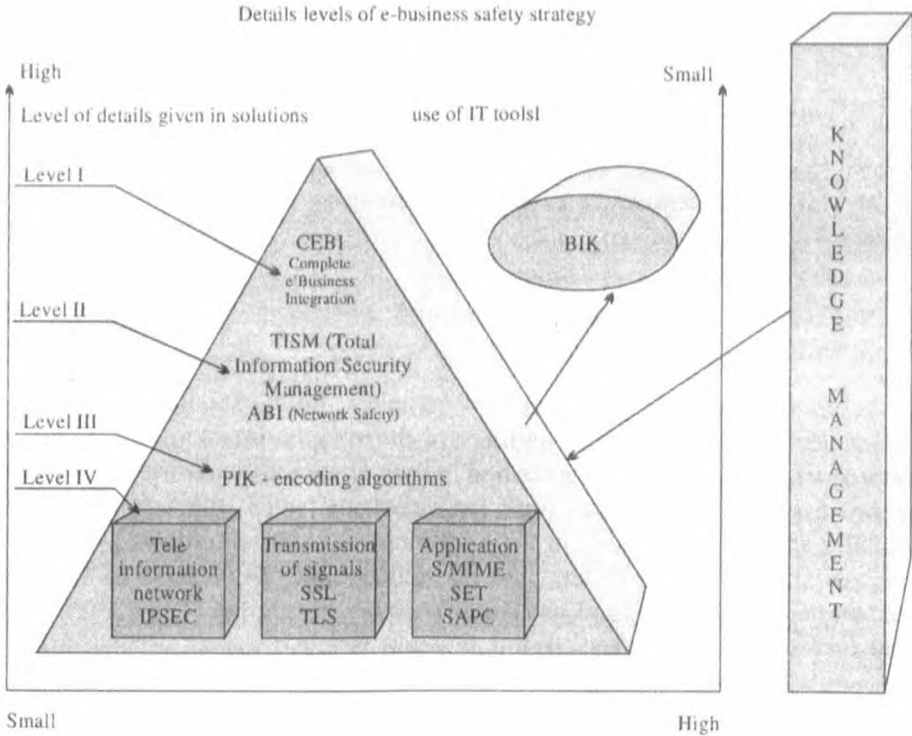Details levels of e-business safety strategy

Figure 1   Securities pyramid e-business
Source: Own elaborate

destination, one can distinguish open portals and dedicated (thematic) ones. Besides portals can be grouped on the basis of their tasks: general-use portals[3],

---

[1] See in www.Is-Scheer.de/produkte.html

[2] Created with the help of selected methodology.

[3] General-use portals allow (upon definition) quick, centralized and integrated access to the mechanisms of searching data in any databases, e-mail and news.

vortals[4], corporate portals (Enterprise Information Portal-EIP). EIP combines the most important features of all types of portals with problems access to corporate applications and databases. In the newest concepts it is also integrated with workflow and intelligent tools.

Typical classic task of the corporate portal is providing single-site control of information flow, especially:

➢ opportunity to classify and search objects,

➢ easy defining the authorisation for getting data and information,

➢ tools for data transmission to shared repositories,

➢ uniform on-line access to selected information,

➢ opportunity to provide data to data processing OLAP-class instruments,

➢ scalability, flexibility, „ecological" way of getting information[5].

IT tools to create corporate portals develop in frenetic pace. Their new expected capabilities are: personalised information, effective integration with business partners, sophisticated automatic assurance of full safety to business processes.

Safety tools of corporate portals

There are multiple facets of assuring top-level safety of information processing with the use of corporate portals' capabilities and flexibility. This issue is also exceptionally important, as attempts to attack e-transactions often take place. While preparing the strategy of information protection, one can utilise the TISM methodology, which initial element is to distinguish the types of information. Mr P. Musiał, IT/ITSec specialist, differentiates between compulsory, attractive and worthy information and thinks that there will be two the most important subjects in the nearest future, namely, the teleinformation operators who provide sophisticated digital products and teleinformation safety (mainly: securities and encoding digital products). Tools offering safe access to the data and their processing concentrate on complex solutions and information technology. List of possible solutions is shown by the securities pyramid (fig. 1). They are (detail levels of e-business safety strategy):

---

[4] Vortal is a vertical portal providing specialist information on strictly defined subject (on the basis of subscription)

[5] It is assumed that portals can be a valuable information source for Credit Information Office.

1. Complete E'Business Integration (CEBI), which among other things includes designing, implementation, integration and protecting information systems. CEBI tools are based on „best of breed" applications. Conforming to ComputerLand opinion, the CEBI supports functional areas of the Internet, e'commerce, e'procurement, CRM, PRM, Supply Chain Management, EDI. (high level of details given in solutions and small use of IT tools)[6].

2. Information Safety Policy (TISM) which (according to M. Byczkowski) consists of monitoring threats to the information, security and audit procedures for information safety level in e-business. Specialist tools supporting TISM are: SOWA, OKW, EMPI, BlackICE. The role of Network Safety Administrator (ABI) is similar to that played by TISM[7].

3. Infrastructure of Public Key (PIK - encoding algorithms), which consists of encoding keys, instruments for creation and receipt of certificates, tools for immediate cancellation of certificates in situations of any crisis or attack takes place, procedures and tools for confirming business partner identification.[8]. Data encoding algorithms are: IDEA (128-bit), RC2-40 (40-bit), RC4-40 (40-bit), RC4-128 (128-bit), DES (56-bit), DES-40 (40-bit), 3DES (168-bit), Fortezz (80-bit), certificates conforming to X.509 recommendation.

4. Protecting mechanisms at the level of: teleinformation network, transmission of signals, applications. The following can be used among others: TLS (Transport Layer Security), MIME (Multipurpose Internet Mail Extensions), S/MIME (Secure Multipurpose Internet Mail Extensions), SET (Secure Electronic Transaction) , IPSec (Internet Protocol Secure Standard), SSL (Secure Sockets Layer), BlackICE Defender, BlackICE Agent, BlackICE, Guard[9], Buster[10], Pro[11], ADO+ (ActveX Data Object NET).

---

[6] PRM makes it possible to market participants to use another link within the partner chain (apart from CRM). According to ChannelWave Company, PRM gives detailed knowledge on performance and effectiveness of particular business partners. This solution is especially designed for those whose substantial part of revenues comes from the indirect sale channels.

[7] See ABI and IB in www.kerberos.pl

[8] W. Ślusarczyk presents classic PIK infrastructure. It consists of (among others): certification policy, certification authorization, storing keys, canceling certificates, creation of two keys, creation of electronic signature, verification of this signature and confidential exchange of keys.

[9] For more information on ICE instruments to protect corporate networks see at www.networkice.com

Original and effective ADO+[12] protection consists of three modules. They are: presentation layer (WWW browser, DataSet, B2B solutions), business layer (integrated applications of ERP, CRM class, OLAP packages for information analysis, support to business sectors - CRM, workflow), data sources (databases of multiple formats including object databases, warehouses, data mining), knowledge databases. ADO+ interface allows controlled dealing with separated data resources and enables safe e-business (EMPI). Use of formatted XML and DataSet files facilitates communication between any scattered elements of the information system. Thus, DataSet permits utilisation of a range of any information sources, which - related to each other - can determine data hierarchy, if reasonable. During transmission ADO+ and DataSet determine automatically and independently which set of data should be exploited and select operations necessary to transfer this information (to the other server or database). These tools have "strongly defined types" so they support effectiveness and safety of corporate portals, especially when linked to SSL (Secure Sockets Layer). SSL is an element of open standard of data transmission protection[13]. It is a base for flexible TLS (Transport Layer Security) specification, developed by Internet Engineering Task Force (IETF). The Secure Sockets Layer procedure consists of four stages:

1. Session encoding.

2. Confirmation of identification.

3. Message transmission.

4. Maintaining cohesion of messages.

The very important problem of maintaining the cohesion of messages in the SSL is overcome by linking encoded messages and check numbers in transmission channels. To encode the information the SSL can use two methods: symmetrical method with secret private key known to both partners involved or asymmetrical method with two keys (private CA, public PIK). The Public key is known to everyone, but can be decoded only by an individual key. The SSL is one of the main elements enabling safe transmissions in global networks. Other elements used to protect against any attack are: SET (Secure Electronic Transactions) specialised in securing transactions where credit cards are used,

---

[10] It operates as a pr server and controls all HP calls. Moreover, it deletes all unnecessary coo files and other information.

[11] Protects users computers from cookies, applets, scripts, advertisements and animations.

[12] ADO+ built MS which is the upgraded interface for the architecture conforming to the standard.

[13] SSL was developed by Netscape Communications and currently its version no. 3.0. is available.

IPSec (Internet Protocol Secure Standard) identifying network instruments, S/MIME (Secure Multipurpose Internet Mail Extensions) protection EDI and e-mail. The figure 2 shows transmission safety triad in corporate portals[14]. The triad consists of:

➢ **Starting HTTPs procedure.** SSL is switched on automatically while the Internet browser is being started.

➢ **Handshake.** Staged procedure of negotiating the determinants of transmission session.

➢ **Security transportation.** Safe information exchange between transmission operators.

Closed safety cycle in corporate portals is formed by the following: idea of safety triad, tasks: "operator requests safe connection" and "end of safe transmission process in the corporate portal", questions: *"Was SSL successfully started?" "Is the exchange of information and data completed?"*, *"Were the negotiation successfully accomplished?"*. Requirements put on corporate portals are still growing[15].

---

[14] Doyle Shaun: *What is Missing from Campaign Management Today? SeUGI 19, Florence, maj, 2001*

[15] See *Business Objects Launches the Knowledge Exchange.* International Knowledge Management News no 23, 2001
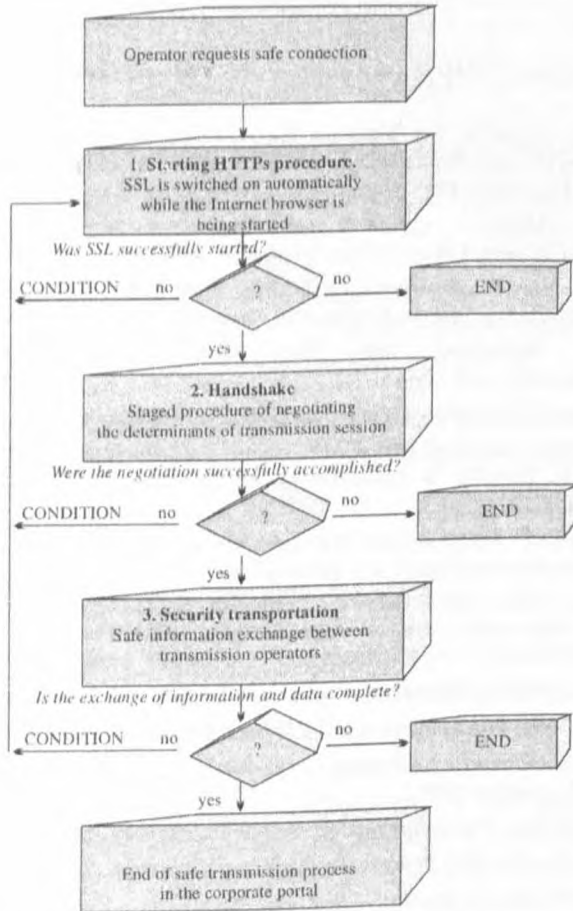
Figure 2   Transmission safety triad in corporate portals
Source: Own elaborate

Summary

It is assumed that modern portals will enable free access to any information expected by the business at the particular time, but they will also provide full safety to the transactions. Therefore, in order to execute complex tasks related to transmission safety and taking the heterogeneity of data sources into consideration it is necessary that each corporate portal should utilise many specialist tools for encoding and protecting from unauthorised access. One of effective instruments in this field is the SSL. The tests conducted shown that it is a flexible, universal instrument and allows effective protection of any data that can be transmitted via corporate portal.

References

1. CIMOSA Association, *CIMOSA –A Primer on Key Concepts.* Purpose and Business Value. Stuttgart, 1995

2. Doumeibgts G., Vallespir B., Marcotte F.: *A Proposal for an Integrated Model of a Manufacturing System: Application to the Re-engineering of an Assembly Shop.* Control Engineering Practice, no 3, 1995

3. Kosanke K.: *CIMOSA – Offene System Architektur.* W A.W. Scheer: Handbuch Informationsmanagement, Gabler Verlag, Wiesbaden, 1993

4. Kasanke K., Naccari F.: *Enterprise Engineering with CIMOSA,* European Workshop on Integrated Manufacturing Systems Engineering. Grenoble, np. 12-14, 1994

5. Krcmar H.; Bedeutung und Ziele von Informationssystem-Architekturen. Wirtschaftsinformatik, no 5, 1990

6. Krupa K.: *Portal informacyjny – inteligentne narzędzie zarządzania.* EiOP, nr 3, 2000

7. Krupa K.: *Struktura otwartych portali biznesowych i równoważona karta wyników* (wybrane aspekty). Red. R. Knosala. W Komputerowo zintegrowane zarządzanie. WNT, Warszawa, 2002

8. Li H., Williams Th.J.: *Explaining the Purdue Architecture and the Purdue Methodology Using the Axioms of Engineering Design.* Computer in Industry no 34, 1997

9. Olle T.W., Hagelstein J., Macdonald . G., Rolland C., Sol H.G., Van Assche F.J.M., Verrijn-Stuart A.A.: *Information Systems Methodologies: A Framework for Understanding.* Workingham, 1991

10. *Taking digital control applications into the future.* Technology Innovations, 2000

11. US Army Knowledge Portal. International Knowledge Management News no 23, 2001

12. Vernadat F.B.: *Enterprise Modeling and Integration: Principles and Applications.* Chapman&Hall, London, 1996

13. Vezzosi H.: ?-ST@Rt: Statistics in the Net. SeUGI 19, Florence, maj, 2001

14. Wagle D.; *The Case for ERP Systems.* The McKinsey Quarterly, no 2, 1998

15. Willams T.J.: *The Purdue Enterprise Reference Architecture.* Computers in Industry, no 24, 1994

16. Willams T.J.: *Development of GERAM, a Generic Enterprise* Reference Architecture and Enterprise Integration Methodology. W Ladet P., Vernadat F.B.: Integrated Manufacturing Systems Engineering. Chapman&Hall, London, 1995

17. http://home.netscape.com/security/techbriefs/ssl.html

18. http://www.microsoft.com/technet/chaptr14.asp

19. http://www.ietf.org/html.charters/tsl-charter.htm/

20. www.networkice.com

21. www./strategie/info.pl/wiedz/knowled.htm

22. www./strategie/pcg-6-portale-finansowe.htm

23. www.kerberos.pl

24. www.sas.com