ISSN:0975-9646

Human Digitization: Authentication Profiles in Digital Information Rights Management Systems

K. M. Moorning

Department of Computer Information Systems, The City University of New York
New York, New York, United States of America

Abstract — **This article emphasizes a new layer to information rights management as it applies to security, privacy and confidentiality of field level data elements. In the interconnected economy, consumers and corporations develop an electronic relationship where commercial and online applications provide convenient access to account data. As consumer use of digital information systems become widespread, the greater the need to protect their proprietary information with more secure authentication protocols. Human Digitization ("HD") involves creating a customer profile at the onset of the data collection and encoding each data element with an access key. The use of authentication profiles in digital information rights management systems mitigates unauthorized data access and provides protection on three levels: 1) internal-employee access, 2) external-customer access, and 3) computer-program access.**

***Keywords* — Authentication, Information Privacy, Data Profiles, Information Rights Management, Digital Rights Management, Information Security, Data Breach, Human Digitization, Identity Theft**

I. Introduction

Sharing of data electronically makes customers more sophisticated in their privacy expectations, hoping that organizations have adopted acceptable information exchange procedures. Initially, as e-commerce transactions became widespread, rather than being proactive and guided by internally agreed upon moral principles, organizations' privacy behaviors were largely reactive and driven by external pressures (Goodhue & Straub, 1991). Today, the decentralized technology environment contributes to a different organizational privacy problem known as data breaches (Culnan & Clark Williams, 2009).

Unnecessary insider access to private information is one of the biggest threats to corporate transaction processing. Data privacy deals with "the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and disposal of personal information." (American Institute of Certified Public Accountants, Inc. and Canadian Institute of Chartered Accountants, 2009). Information misuse and unauthorized access can potentially threaten an individual's credibility, cause severe financial losses, and subsequently threaten the organization's legitimacy in its interactions with consumers, shareholders, and regulators (Greenaway & Chan, 2005).

The United States Privacy Rights Clearinghouse reported that since January 2005, more than 246 million records containing sensitive personal information have been exposed due to data breaches. Although new laws have been enacted which require affected organizations to provide notice if they suffer a breach, the laws do little to identify criteria for minimizing such breaches. They are especially difficult to detect and prevent because in many cases an insider has the proper authority to access customer information. Government interventions have painted breaches as an important information management issue that continues to challenge organizations.

Most research on information privacy does not address broader managerial challenges and social issues such as how firms treat personally identifiable information internally. An analysis by Verizon Business of more than 500 forensic investigations of U.S. breaches involving more than 230 million records found that nearly 90 percent could have been prevented had reasonable security measures been implemented. Nine out of 10 of the breaches involved a system that had unknown network connections or accessibility, including data storage on systems which the organization did not know existed (Baker, Hylender, & Valentine, 2008).

II. Digital Information Rights Management System

An Information Rights Management ("IRM") system is a collection of coding protocols which protect customer information from unauthorized access and distribution. The IRM system will only share information with duly authorized and cleared personnel based on a rights management process. Unlike Digital Rights Management ("DRM") systems which protect music and video files from unlawful duplication, IRM systems are typically used to protect information mainly in textual and transactional systems. DRM systems operate as file locks are not as dynamic as IRM systems which continually evaluate rights as each layer of information is accessed.

In some DRM systems, a Display-Only File Servers present a viable solution against information theft by insiders. They store files on a protected server and prevents bits of the files from physically leaving the server. In other words, once a file is checked into the server, its digital content can never be directly taken out. Because of the isolation of digital content from end users, the rights management in this architecture can be less complicated, due to the access control policies of the underlying operating system of the server (Tzi-cker Chiueh, 2004).

Compared with basic DRM systems, those which implement display only controls prevent even authorized insiders from accessing content bits and leaking them. The limitation to this protocol is that users having access can still read or write to these files indirectly through standard applications. This process solves the problem of sending information directly from the network to unauthorized sources, but does not solve the problem of access to data elements irrelevant to the specific transaction. A natural bridge between the two types of would be a properly encoded Digital Information Rights Management System ("DIRMS") that combines the functionality of both the IRM and DRM systems. The DIRMS would allow the flow of sensitive information to those authorized while limiting the unauthorized duplication and dissemination of such information to those without clearances.

DIRMS place emphasis on protecting each element of proprietary information, i.e., the combination of personally identifiable information and sensitive information, which can be used to directly or indirectly identify an individual. Personally identifiable information includes name, home address, email address, social security or identification number, and may include physical characteristics that uniquely identify one individual. Sensitive information includes medical conditions, financial status, gender, racial or ethnic origin, political opinions, religious or philosophical beliefs, sexual preferences, current and former employers, criminal offenses, family members and others with whom the customer has a relationship that may be used to indirectly identify an individual. Since each of these data elements may be sold and re-used without discretion, proprietary information needs new rules for disclosure.

In DIRMS, each layer or element of data has an encrypted code to protect and control access to the information, keep the information within the secure environment and guard the information from programmatic attacks. The main area of application of DIRMS is to clear rights for content accessed and transmitted on digital networks. The system subject to concerns about privacy is the best, and perhaps the only way to monitor use of content sent through digital networks, since the usage itself is monitored through rights management and an identification system. In fact, usage monitoring has long been a key issue in the discussions between rights holders and access providers (Gervais, 1999). Simply put, employers limit their liability in cases of employee misuse, as it restricts those who would normally have access to private information.

III. Privacy Principles

Unnecessary insider access to private information is one of the biggest threats to corporate transactions. Information theft is considered the most damaging in terms of financial loss. It is especially difficult to detect and prevent, because in many cases the insider has the proper authority to access the stolen information. Therefore, information privacy is an important information management issue that continues to challenge organizations.

The global nature of the e-commerce means regulatory actions in one country affect the rights and obligations of customers around the world. Generally Accepted Privacy Principles (GAPPs) were developed from a business perspective to reference significant local, national, and international privacy regulations. Each principle is supported by objective, measurable criteria that form the basis for effective management of privacy risk and compliance in an organization. Within the context of GAPPs, the organization's privacy notice is supposed to indicate the criteria for collecting, using, retaining, disclosing, and disposing personal information in conformity with the commitments set forth in the GAPPs. Table 1 below outlines the ten GAPPs adopted to protect customer information.

Table I – Generally Accepted Principles

PRINCIPLE	DEFINITION/EXPECTATION OF ENTITY
Management	defines documents, communicates, and assigns accountability for its privacy policies and procedures
Notice	provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed
Choice & Consent	describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information
Collection	collects personal information only for the purposes identified in the notice
Use, Retention & Disposal	limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent while retaining personal information long enough to fulfil the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information
Access	provides individuals with access to their personal information for review and update
Disclosure to Third Parties	discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual
Security for Privacy	protects personal information against unauthorized access (both physical and logical)
Quality	maintains accurate, complete, and relevant personal information for the purposes identified in the notice

Source: American Institute of Certified Public Accountants, Inc.

IV. Threats to Privacy

Although Electronic Data Interchange (EDI) represents an opportunity to improve business processes and business controls, challenges are expected (Magutu, Lelei, & Nanjira, 2010). The goal is to improve operational efficiency, enhance information quality, while maintaining reductions in processing time of critically important business information. Privacy and confidentiality are difficult to maintain during EDI because each interchange involves a plurality of data elements. A special kind of threat, called insider attack, cannot be stopped effectively by traditional methods like firewalls and intrusion detection systems and is receiving more and more attention from system administrators and security researchers. Insider attack is more dangerous than external attack because the attackers are already inside the security perimeter and therefore are considered more trustworthy than those outside.

Unlike the external attacker who tries to infiltrate into an organization through the network, people inside an organization, such as a company employee, have more opportunities to interact with the sensitive digital information, and thus are more likely to have the information disclosed to non-trusted parties, either unintentionally or deliberately. For example, a disgruntled employee may save sensitive information to USB drive and sell it to a competitor company. In addition, they have more knowledge about the internal security mechanism and sometimes even have the authority to bypass the associated security checks without raising alerts. Among all insider attacks, information theft is considered the most damaging in terms of potential financial loss (Yu & Chiueh, 2004).

V. Authentication Profiles

Human Digitization ("HD") is the coding of private information at the data level creating multiple key codes for access. Customer profiles are locked and secure, only accessible in authenticated transactions, leaving sensitive and irrelevant personal private information intact. Organizations with large reservoirs of customer information, must find a way to encode the data so that the market for breached data is annihilated.

Computational algorithms for each stratum of private information are developed, assigning identification numbers based on verified credentials, and adding a data checking access layer. When consumers and organizations use the Internet and other electronic communication or collaboration systems for transaction processing, an associated stratum code is entered for each field on an individual's profile. Each personally identifiable piece of information has a separate code. Alternatively, the use or reuse of each data element requires a separate code.

Upon opening an account, all personally identifiable and sensitive proprietary data is collected and encoded in the DIRMS. Customers are provided with a HD profile as soon as the fiduciary relationship commences. As transactions are performed, further exposure to actual data elements is unnecessary because transactions are processed electronically. The authentic customer already has the information, and an employee does not need access to it. Updates to personal information would be performed through a separate, secured and documented process.

Unique data codes protect the privacy and security of identifiable and sensitive information. Identifiable data has a higher standard of protection since it uniquely identifies one customer. Sensitive information is personal information about the customer but does not uniquely identify the person unless mapped to other data elements. As transactions are performed, the customer provides the codes, not the data values. Table II below illustrates a sample coding process for individual data elements using HD techniques.

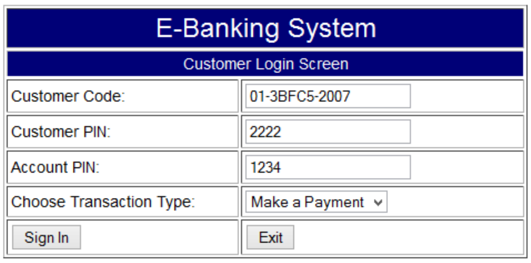
Table II – Human Digitization Coding

Data Element	Identifiable or Sensitive	Sample Data	HDC
Customer Code	I	01-3BFC5-2007	--
Account Number	I	3BFC5-01	--
Customer Name	I	John Smith	12A
Home Address	I	12 Main Street,	B14
Telephone	I	515.555.1212	37Z
Email	I	jsmith@someorg.com	L0X
Social Security	I	123456789	9A1
Employer	S	Revell Industries	XZ2
Work Address	S	24 Broad Street,	77Z
Salary	S	$87,000	65R
Gender	S	Male	LS7
Race/Ethnicity	S	American	92P
Credit Card	I	1234567890123456	FH7

The entire record is coded and stored in the DIRMS as: **013BFC52007-3BFC501-12A- B14-37Z-L0X-9A1-XZ2-77Z-65R- LS7-92P**. The digital format of the data is even more lengthy, and unreadable by non-technical person. The codes do not represent encryption of the data, but a key to access that specific data element when properly authenticated. Two back-end secure servers are involved, one containing coded, digital data, and the other containing the encrypted, personal data.

VI. Transaction Processing

Upon entering a valid customer code and account personal identification number ("PIN"), a transaction is initiated. Each customer has a distinct PIN, as well as each account, so the coding process requires a multi-PIN approach. Exposure to sensitive or personally identifiable information is determined by the transaction type, but only revealed upon entering the correct code. For a payment transaction, the only items needed are the payment date and payment amount. Figures 1-2 below show a sample process of an online payment transaction. In the actual system, PIN would show as asterisks.

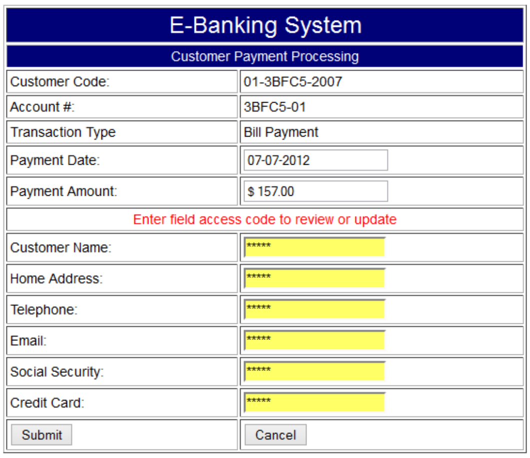


E-Banking System

Customer Login Screen

Customer Code:	01-3BFC5-2007
Customer PIN:	2222
Account PIN:	1234
Choose Transaction Type:	Make a Payment

Figure 1 – E-Commerce Transaction (Online)



E-Banking System

Customer Payment Processing

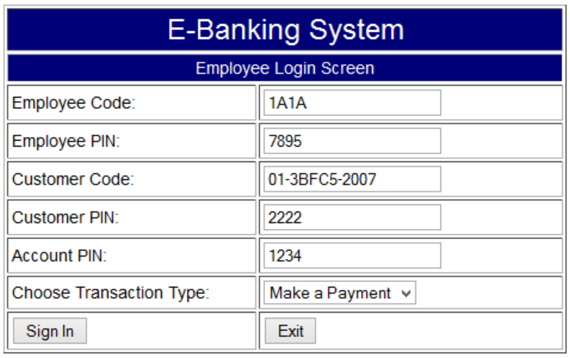
Customer Code:	01-3BFC5-2007
Account #:	3BFC5-01
Transaction Type	Bill Payment
Payment Date:	07-07-2012
Payment Amount:	$ 157.00

Enter field access code to review or update

Customer Name:	*****
Home Address:	*****
Telephone:	*****
Email:	*****
Social Security:	*****
Credit Card:	*****

FIGURE 2 – E-COMMERCE TRANSACTION (ONLINE) – BILL PAYMENT

Customer service employees do not need access to un-coded information to perform financial transactions. Figures 3-4 below shows a sample process of a transaction initiated by a customer service representative:

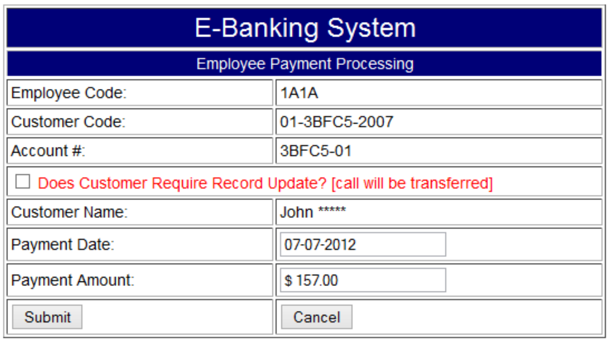


E-Banking System

Employee Login Screen

Employee Code:	1A1A
Employee PIN:	7895
Customer Code:	01-3BFC5-2007
Customer PIN:	2222
Account PIN:	1234
Choose Transaction Type:	Make a Payment

FIGURE 3 – E-COMMERCE TRANSACTION (CUSTOMER SERVICE)



E-Banking System

Employee Payment Processing

Employee Code:	1A1A
Customer Code:	01-3BFC5-2007
Account #:	3BFC5-01

☐ Does Customer Require Record Update? [call will be transferred]

Customer Name:	John *****
Payment Date:	07-07-2012
Payment Amount:	$ 157.00

FIGURE 4 – E-COMMERCE TRANSACTION (CUSTOMER SERVICE)

VII. METADATA

The main purposes for this type of DIRMS development is the lack of systematized processes for access to consumer's private information. Metadata used to be "data about data", but now it includes data, information and knowledge about data and information of an organization. It refers to the interpretation of data elements such as: Where is the data stored? Who created it? What elements does a record contain? When was it created? When was it changed? Who accessed it? These and other questions arise out of need for data control. Metadata management provides organizations with the visibility needed to manage data in a complex environment. For our transaction code algorithm, the metadata elements are the items collected for information security analysis.

Table III below represents the metadata captured when a customer service represents initiates an account transaction. The purpose for access is based on the transaction type. The rights associated with the access are matched to the credentials code. Employee access has two forms: (LA) Limited Access generally used for customer service and staff management, and (FA) Full Access for database administrators. When capturing transactions, the DIRMS will evaluate which data elements are being accessed and how access policies are implemented within the system to safeguard customer information.

TABLE III – METADATA FOR THE PAYMENT TRANSACTION

Metadata Element	Sample Pattern
Employee Code	1A1A
Transaction Rights (Access Level)	LA
Customer Code	01-3BFC5-2007
Account Number	3BFC5-01
Date Code	07072012
Transaction Opened Time Code	1630
Transaction Closed Time Code	1640
Transaction Code	P

The metadata record for the payment transaction is decoded below in Table IV below.

TABLE IV – METADATA FOR AN UPDATE TRANSACTION

METADATA CODE	Algorithm Pattern
1A1ALA-013BFC52007-07072012-16301640-P	● Accessed by Employee - 1A1A ● Access Level - LA ● Account Region - 013 ● Account Number - 3BFC5 ● Account Open Year - 2007 ● Date - July 7, 2012 ● Record Open Time - 4:30pm ● Record Closed Time - 4:40pm ● Transaction Type – Payment

Table V below represents the metadata captured when sensitive data has been viewed and edited. Internal system checks can flag transaction codes and information changes. For instance, red flags will be raised if span between the open time and close time is significantly too long for the type of access. Another flag on updates would be too many being performed by employees instead of customers. Employee updates should correspond to some financial transaction occurring simultaneously. Some data elements updates, such as name, address and social security number would require documentation proof.

TABLE V – METADATA FOR AN UPDATE TRANSACTION

Meta-Data Element	Sample Pattern
Employee Code	4ZF2
Transaction Rights (Access Level)	FA
Customer Code	01-3BFC5-2007
Account Number	3BFC5-01
Date Code	07072012
Transaction Opened Time Code	1615
Transaction Closed Time Code	1625
Transaction Code	U
Proprietary Field	5
Privacy Level	S

The metadata record for the update transaction is decoded below in Table VI, and Table VII represents the corresponding metadata table of all transactions.

TABLE VI – METADATA FOR AN UPDATE TRANSACTION

METADATA CODE	Algorithm Pattern
4ZF2FA-013BFC52007-07072012-16451655-U-5-S	● Accessed by Employee – 4ZF2 ● Access Level - FA ● Account Region - 013 ● Account Number - 3BFC5 ● Account Open Year - 2007 ● Date - July 7, 2012 ● Record Open Time - 4:15pm ● Record Closed Time - 4:25pm ● Transaction Type – Update ● Transaction Field – Credit Card ● Privacy Level - Sensitive

TABLE VII – METADATA TRANSACTION CODES

METADATA TRANSACTIONS
1A1ALA-013BFC52007-07072012-16301640-P
4ZF2FA-013BFC52007-07072012-16451655-U-5-S

VIII. SUMMARY AND CONCLUSION

With HD coding, companies may strengthen methods for investing trust in otherwise anonymous digital transactions. Information systems and technology can be properly harnessed to serve virtuous purposes, with tremendous potential to improve human and organizational performance. Organizations will be able to facilitate more secure and controlled relationships with employees and partners through the adoption of this sophisticated information system. Field-level (data elements) security gives organizations control over who is permitted to read, modify, print or redistribute individual information even if they filter beyond the firewall. Designating role-based permissions on information down to the level of individual sections would automatically redact confidential data if a permission level did not entitle him or her to view it. Server-based, cross-enterprise identity management systems would interface with external DIRMS to automatically present the right version of a consumer's profile to the accessor, concealing that which is designated confidential or inappropriate for that role or relationship.

IX. FURTHER RESEARCH

More research has to be performed with respect to governing electronic transactions. Global legislation is needed to set rules for customer profiles and data retention especially across Internet channels. The need for internal and external regulatory compliance will transform electronic transaction practices. Protocols should be established for providing organizational transaction processing identifications numbers (TPID) to coincide with their federal or corporate tax ID number. When fiduciary transactions are encumbered, the TPID is registered in the electronic data interchange authenticating whether the organization can perform such transactions. The TPID code will also determine who can use, reuse or share information with third party clients. Legislation governing electronic funds transfers, electronic data interchange and Internet privacy would need to conform to more secure encryption and decoding process.

Corporations, in turn must view DIRMS as a business process. All transaction process systems need to restrict proprietary data for safety purposes. Future research for reviewing privacy agreements is needed. Sending notification of data breaches is insufficient to preventing insider attacks. Additional factors would have to be included in an information access analysis. New managerial information security roles can harness compliance as an opportunity to escalate customer trust, raise organizational awareness, and better align security measures with business objectives.

REFERENCES

[1] American Institute of Certified Public Accountants, Inc. and Canadian Institute of Chartered Accountants. (2009). *Generally Accepted Privacy Principles*. American Institute of CPAs.

[2] Baker, W., Hylender, C. D., & Valentine, J. A. (2008). 2008 *Data Breach Investigations Report*. New York: Verizon Business.

[3] Culnan, M., & Clark Williams, C. (2009). *How Ethics can Enhance Organizational Privacy: Lessons from the ChoicePoint and TJX Data Breaches*. Management Information Systems Quarterly, 33(4), 673-687.

[4] Gervais, D. J. (1999). *Electronic Rights Management and Digital Identifier Systems*. Journal of Electronic Publishing, 3(4).

[5] Goodhue, D. L., & Straub, D. W. (1991). *Security Concerns of System Users: A Study of Perceptions of the Adequacy of Security. Information & Management*, 20(1), pp. 13-27.

[6] Greenaway, K. E., & Chan, Y. E. (2005). *Theoretical Explanations of Firms' Information Privacy Behaviors*. Journal of the Association for Information Systems, 6(6), pp. 171-198.

[7] Magutu, P. O., Lelei, J. K., & Nanjira, A. O. (2010). *The Benefits and Challenges of Electronic Data Interchange*. African Journal of Business and Management, 1, 212-236.

[8] Tzi-cker Chiueh, A. M. (2004). *Display-Only File Server: A Solution against Information Theft Due to Insider Attack*. Stony Brook University: Stony Brook, NY.

[9] Yu, Y., & Chiueh, T.C. (2004). *Enterprise Digital Rights Management: Solutions against Information Theft by Insiders*. Architecture, 1-26.