



**SECURING INTER-ORGANIZATIONAL WORKFLOWS IN
HIGHLY DYNAMIC ENVIRONMENTS THROUGH BIOMETRIC
AUTHENTICATION**

Journal:	<i>18th European Conference on Information Systems</i>
Manuscript ID:	ECIS2010-0352.R1
Submission Type:	Research Paper
Keyword:	Business process management, Information security/privacy, Interorganizational systems, IT compliance



SECURING INTER-ORGANIZATIONAL WORKFLOWS IN HIGHLY DYNAMIC ENVIRONMENTS THROUGH BIOMETRIC AUTHENTICATION

Senk, Christian, University of Regensburg, Universitätsstraße 31, 93053 Regensburg,
Germany, christian.senk@wiwi.uni-regensburg.de

Abstract

High flexibility demands of business processes in an inter-organizational context potentially conflict with existing security needs, mainly implied by regulative and legal requirements. In order to comply with these it has to be ensured that access to information within the workflow is restricted to authorized participants. Furthermore, the system might be required to prove this retrospectively. In highly flexible environments, particularly when documents leave the owner's security domain, the scope of trust must be expendable throughout the workflow. Usage control provides practical concepts. However, user authentication remains a major vulnerability. In order to ensure effective access control the possibility of process-wide enforcement of strong authentication is needed. Inherently, strong user authentication can be realized applying biometrics, though practical reasons still slow the broad application of biometric authentication methods in common workflow scenarios. This work proposes the combination of usage control and typing biometrics to secure inter-organizational workflows in highly dynamic environments. On the one hand, usage control provides high flexibility for document-centric workflows but relies on the enforcement of strong authentication. On the other hand, authentication based on typing is flexible in both deployment and application. Furthermore, the inherent privacy problem of biometrics is significantly weakened by the proposed approach.

Keywords: biometric authentication, identity management, access control, usage control, business process flexibility, business process compliance

1 INTRODUCTION

Due to various factors, enterprises and their business processes (BP) across different industries face steadily increasing demands in flexibility and efficiency (Ghattas and Soffer 2009; Pütz et al. 2009). Simultaneously, service-oriented technologies are becoming more and more mature and business-oriented and thus enable the automation of highly flexible business processes (hBP) both within organizational boundaries and, increasingly, beyond them (Ghattas and Soffer 2009; Lotz et al. 2008); BP are termed highly flexible when they indicate either fragmentary predictability or inherent context sensibility (Pütz et al. 2009). Inter-organizational BP especially imply new security issues (Ghattas and Soffer 2009; Hafner and Breu 2009). As autonomous and legally independent entities with varying security standards co-operate in executing one BP, the security of the end-to-end process depends on its weakest element within the federation (Hafner and Breu 2009). Various legal and regulatory specifications (e.g. German federal data protection act, Sarbanes-Oxley Act) imply obligatory security goals requiring the implementation of appropriate controls that “constrain the behavior of business processes” accordingly (Lotz et al. 2008, p. 383). This includes not only the protection of the processed information but also the accountability and legal liability of the BP and the involved tasks performed by business users (Dierstein 2004). At the technical level this makes high demands on the workflow and the supporting infrastructure, especially in inter-organizational scenarios. In this context the effectiveness of both user authentication and access control (AC) is inherently limited by the need for trust (Reiser 2008). This challenge applies even more in flexible business environments (Ghattas and Soffer 2009; Hommel 2007; Lotz et al. 2008). AC in the context of hBP requires a flexible inter-organizational infrastructure that provides effective and transparent mechanisms for the enforcement of the resource owner’s policies based on authorization models like RBAC, ABAC, TBAC, T-RBAC or RTFW. For this purpose, strong user authentication is essential and must be enforceable at the technical level. Common password-based methods are easy to implement but inherently insecure, as a digital identity is bound to a secret and not to a person. So the authentication process can easily be bypassed at the organizational level. Token-based approaches improve the situation but reduce structural flexibility. Natural personal reference can be realized with biometric authentication methods. They are potentially more secure and more practicable than other approaches (Jain and Ross 2007) and thus steadily gain practical relevance (van Graevenitz 2006; Weber 2008). As the applicability of biometric methods highly depends on the requirements of the respective environment, a specific evaluation of available methods in the context of hBP is required.

The main contribution of this work is the proposal of the combination of usage control and typing biometrics for increased control in the context of inter-organizational hBP. An integrated approach for effective access control in the context of hGB does not yet exist. Therefore, available paradigms for identity and access management as well as selected biometric authentication methods are evaluated according to relevant literature. Subsequently, the proposed approach is introduced and discussed.

The paper is structured as follows. In section 2 basic paradigms for identity and access management are analyzed. Section 3 outlines the drawbacks of traditional authentication methods and suggests biometric approaches instead. The applicability of various biometric authentication methods is discussed in section 4. Section 5 describes a combined approach for usage control and typing biometrics to secure inter-organizational data-centric workflows in highly dynamic environments, which are discussed in section 6. Future research directions are depicted in section 7.

2 APPROACHES FOR ACCESS CONTROL

2.1 Basic requirements in the context of highly flexible business processes

Inter-domain resource control. Workflows involve the automated transfer of information and tasks to different participants (users) according to a set of procedural rules (Workflow Management

Coalition 1999). In collaboration scenarios workflows of different and potentially heterogeneous security domains are interfaced and resources are shared between them (Ghattas and Soffer 2009; Hafner and Breu 2009). Resources can basically be services which partly or entirely automate single tasks, or documents that are transferred automatically for manual processing. It is assumed that exactly one domain, the resource owner, accounts for a particular information resource (Policy Administration Point, PAP). Thus, the use of information must steadily follow the owner's security policy. In service-oriented workflows, the resource (e.g. Webservice) is generally protected by its owner. An external access request is intercepted by the owner's security domain. Based on available attributes about user, requested action, resource, and context as well as on the corresponding policy, an AC decision is made and enforced autonomously. As the resource's owner keeps both policy enforcement point (PEP) and policy decision point (PDP) under control, solely externally sourced attributes remain potential vulnerabilities. By contrast, document- or data-centric workflows involve the physical distribution of document files. PEP and PDP usually move with the document. Thus, the access to the resource cannot be controlled effectively by implication, and the assertion of compliance with the owner's policy basically relies on trust. Summing up, an AC model for hBP must provide effective and transparent policy enforcement and the reduction of trust dependencies along inter-organizational (a) service-oriented and (b) document-centric workflows.¹

Structural flexibility. hBP are characterized by two types of flexibility: (1) behavioural flexibility and (2) structural flexibility. Behavioral flexibility refers to the ability of BP to adapt the control flow using existing value net structures. Structural flexibility additionally implicates the necessity for structural changes. Consequently, federated structures in the context of hBP are highly dynamic and trust relationships between the resource owner's and the external user's domains should be established instantly. From a technical point of view high interoperability is necessary.

2.2 Access control paradigms for inter-organizational workflows

According to the literature, several paradigms for AC can be deduced from existing identity management models. The paradigms are introduced in the following and evaluated against the former specified basic requirements in the context of hBP.

Owner-centric Identity and Access Management (IAM). As the structure of non-flexible BP is established ex ante, they can be secured by embedding them into a static security context controlled in a centralized manner by the designated process owner. For instance, an automotive manufacturer might run one IAM system that includes the identities of both internal employees and external users from suppliers or other business partners. In the context of hBP ownership relationships are much more complex. Thus, identities would be necessary in several security domains and probably registered and administered redundantly, which would involve great effort and potentially cause inconsistencies (Hommel 2007). Although control is theoretically high for service-oriented workflows, structural flexibility and scalability are limited with this approach. Moreover, document-centric workflows cannot be secured in a feasible way.

Global IAM. This approach assumes that all members of a federation share one security domain for identity and access management. Due to various legal and political reasons, this approach seems highly unattractive for organizations. Thus, flexibility is rated low.

Federated Identity Management (FIM). FIM is a concept for distributed identity management (Hommel 2007; Reiser 2008). Every user belongs to at least one home organization, known as an identity provider (IDP). External resources are provided by service providers (SP). When an external user requests access to an SP's resource, the SP bases the AC decision on information obtained from the user's IDP. So, the SP, protecting a resource according to a specific policy, does not need to keep

¹ in line with the basic model of the eXtensible Access Control Markup Language (XACML) (OASIS 2005)

identity data on every possible user within the federation, but relies on the information provided by the user's home entity. In order to strengthen trust relationships, terms of quality and availability of exchanged user attributes are specified in contracts between the participating organizations of a federation. FIM-based AC provides high structural flexibility as AC and identity management are technically and logically decoupled. Assuming syntactic and semantic consistency regarding applied FIM protocols new organizations can easily join the federation and participate in the execution of the hBP. The approach is feasible for service-oriented scenarios. PDP and PEP remain in the security domain of the resource owner. Nevertheless, the effectiveness of the AC highly depends on the authenticity and correctness of the externally provided user information.

User-Centric Identity Management (UCIM). UCIM describes an approach that allows each user to manage an arbitrary number of their own digital identities. As the user autonomously certifies and modifies his or her attributes, their authenticity is inherently weak. Though UCIM provides high structural flexibility, it is not applicable for the establishment of a strong trust chain.

	Service-oriented workflows		Document-centric workflows	
	Control	Flexibility	Control	Flexibility
Owner-centric IAM	high	low	high	low
Global IAM	high	low	high	low
FIM	medium	high	not applicable	not applicable
UCIM	low	high	not applicable	not applicable

Table 1. Comparative evaluation of identity and access management paradigms

The results are summarized in Table 1. AC based on federated identities is rated best for service-oriented workflows, assuming that user attributes provided are authentic. Nevertheless, document-centric workflows cannot be secured effectively as PDP and PEP move out of the trusted domain.

2.3 Usage Control

In order to address this problem, Usage CONtrol (UCON) is introduced by Sandhu and Park (2003) but has not yet been examined in the context of BP or hBP. UCON explicitly addresses the (continuous) AC to physically distributed data resources like documents (Pretschner et al. 2006). UCON is based on the concept of Trusted Computing and the deployment of Reference Monitors (RM). RM are tamper-proof and revisable components deployed in the resource consumer's security domain in order to act as PEP (Müller 2008). Resources are distributed in a protected form in order to guarantee that they can only be accessed through an RM. RM ensure the enforcement of resource-specific policies (licenses) which are centrally managed and distributed by the resource owner (PAP) (Sandhu and Park 2004; Zhang et al. 2008).

In addition to classical authorization issues, licenses include so-called obligations to specify more abstract constraints like the validity of the license, the automated notification of the resource owner each time the resource is used, the number of allowed uses, ability to re-distribute etc. (Nauman et al. 2009; Pretschner et al. 2006). This allows the highly flexible configuration of the relationship between resource owner and RM. Depending on control objectives, once provided with resource and license, the RM may have full autonomy or, in contrast, the license might require the RM to obtain a policy update for each request. Thus, assuming the authenticity and correctness of available attribute information, particularly regarding user attributes, the potential inter-domain control is high. UCON is a generic concept that principally allows the integration of traditional and workflow-specific authorization models with enhancements regarding the continuity of the access decision and the mutability of relevant attributes (Nauman et al. 2009). Moreover, Danwei et al. (2009) introduce an architecture for UCON in Cloud Computing environments based on XACML and the OASIS' FIM-related standard Security Assertion Markup Language (SAML). Due to loose and asynchronous coupling between owner and consumer high structural flexibility is provided assuming the RM is both easily distributable and deployable in the consumer's security domain. Therefore, the RM must be software-based and interoperable with existing IDP.

2.4 Evaluation

In the context of inter-organizational hBP, FIM shows best results in both resource control and structural flexibility regarding service-oriented workflows. Indeed, the effective protection of distributed document-based resources requires the expandability of trusted domains. With UCON a promising approach with high flexibility potentials exists. For interoperability reasons RM must be able to communicate with relevant IDP. The benefit of the application of FIM standards in this context is obvious. However, the effectiveness of inter-domain control of both approaches highly depends on the authenticity and correctness of the attribute information taken into account for the actual AC decision. This is assumed to be a major problem for user attributes. Consequently, besides the technical security of exchanged attributes, strong authentication methods must be enforced along the comprehensive workflow to ensure the effectiveness of the applied AC mechanism.

3 TOWARD STRONG AUTHENTICATION

Authentication in general is the process binding a subject to an identity by means of distinguished processable characteristics; the sum of these characteristics builds an identity. For effective AC reliable authentication of legitimated users is a basic requirement (Schläger 2008). Otherwise, potential attackers could simply assume the identity of an arbitrary subject and bypass authorization restrictions. In legally regulated business environments (e.g. health care) BP require strong authentication. The strength of authentication is implicated by the confidence of a digital identity being consistent with the logically allocated “real” one. Principally, this can be proven by knowledge, possession, or property/biometrics (Jain and Ross 2007; Smith 2002). These factors feature different advantages and drawbacks in regard to the desired strength of authentication. The overall strength can be increased by combining two or more factors (multifactor authentication).

3.1 Traditional authentication methods

Knowledge-based authentication. Generally, authentication by proof of knowledge is based on mutual secrets between subject and authenticator. The identity of a subject is thus logically bound to this secret. Most common is the use of static secrets in particular for password- (PW) or PIN-based methods. Such methods are technically easy and economical to implement and practical in application. Moreover, knowledge is highly portable as it should be memorized by the user at all times. However, it is also inherently insecure. Though PW with high average information content potentially provide appropriate security from a theoretical point of view, this security can be bypassed at the organizational level. As PW security depends on length and complexity, more secure PW are harder for the user to remember. Consequently, employees tend to write PW down or use one for several applications. This significantly increases the threat of compromises that may even remain unaware. Alternative methods are based on cultural or dynamic secrets. Whereas cultural secrets like birth date or social security number are not even confidential, such authentication mechanisms are weak in principle. Though methods based on dynamic secrets like transaction authentication numbers (TAN) or one-time PW can be used for stronger authentication, they face substantial practical problems: the usually physical synchronization and storage of the secrets as they usually cannot be remembered by the user. (Oppliger 2002; Smith 2002) A major drawback for all knowledge-based methods, especially from a legal point of view, is that secrets can easily be shared across different users. On that account many authors agree that solely knowledge-based authentication does not provide appropriate security for many practical use cases (St. Clair et al. 2006). Thus, alternative authentication mechanisms must be taken into account (Benatar 2006; Pope and Bartmann 2009; Smith 2002).

Token-based authentication. Possession-based authentication basically relies on the proof of holding a particular hardware device (token), e.g. a smart card or a USB token. Thus, analog to knowledge-based approaches, the authentication process cannot guarantee the authenticity of the token-associated user attributes as the device may be transferred (either on purpose or unintentionally) to other persons.

Another disadvantage lies in the high expenses for tokens and the required infrastructure. Moreover, the portability of tokens might be limited in any case due to their size. One advantageous characteristic of tokens is the possibility of replacing them in the case of a detected compromise. Nevertheless, the associated costs as well as the inherent transferability remain major disadvantages of possession-based authentication methods, so the applicability for distributed environments is limited (Benatar 2006; Oppliger 2002; Pope and Bartmann 2009; Smith 2002).

As shown above, due to inherent transferability, knowledge- and possession-based methods are highly susceptible to various malicious attacks. Thus, these traditional authentication methods leave problems that biometric approaches are potentially able to solve (Pope and Bartmann 2009, Jain and Ross 2007).

3.2 General aspects of biometric authentication

Biometrics basically relies on the measurement of specific biological characteristics in order to recognize individuals (Jain and Ross 2007). Thus, biometric authentication is defined as the automated identification or verification of a person by means of unique anatomical or behavioral features (Maltoni et al. 2009). A basic requirement is previous enrollment. Therefore, a user registers his or her biometric feature, which is stored by the system provider and henceforth used as a reference. The authentication itself relies on the comparison of a provided biometric sample with the former registered template. If sample and reference template are consistent according to a former specified threshold, the authentication was successful. As template and sample data are practically never identical due to ever variable conditions and natural fluctuations, the calculation of biometric authentication systems follows statistical distributions. Therefore, their performance is primarily evaluated by two empirical error rates (Jain and Ross 2007; Mansfield and Wayman 2002): (1) False Acceptance Rate (FAR, percentage of wrongly approved unauthorized persons) and (2) False Rejection Rate (FRR, percentage of wrongly rejected authorized persons). Both rates directly depend on the specified threshold. The higher the intended similarity between reference and sample, the lower the risk of accepting an unauthorized person. Unfortunately, the probability of rejecting an authorized person increases simultaneously. Thus, the threshold is always a trade-off between security and comfort which has to be specified according to application requirements. For effective biometric authentication, features have to meet four basic requirements. First of all, every subject in the present context should be able to provide it. Otherwise, subjects are unable to enroll in particular cases and have to be authenticated by other means. Secondly, the feature should provide sufficient unique information about an individual to enable the clear distinction of all subjects in a context. A further prerequisite is the permanence of a feature meaning that the correlation of sample and reference template is durable over time. The aging of biometric features is considered to be a problem especially for behavioral traits. This problem can be addressed by adoption mechanisms that incrementally adjust the reference template according to changes of sample inputs during authentication (Bakdi 2007; Olden 2008). Lastly, the feature must be quantifiable. For automated authentication, this includes the ability to be digitalized by specific hardware-based input devices (sensors) (Maltoni et al. 2009). In line with these requirements, many biometric characteristics can be methodically applied for authentication. The most common ones include the recognition of eye, fingerprint, face, ear, facial or hand thermogram, hand vein, hand geometry, signature, voice, and typing dynamics (Maltoni et al. 2009; Weber 2008). All biometric features have one major advantage in common: they are naturally bound to a person. As the feature cannot easily be shared or stolen (Jain and Ross 2007), authentication checks the presence of a person and not just the availability of a feature. Due to this fact, the strength of authentication can potentially be increased in relation to non-biometric approaches (Jain and Ross 2007). Though replay attacks are possible, the risk can be minimized by the implementation of live detection mechanisms. Furthermore, the conjunction of feature and person potentially advances the practicability from a user's perspective since there is no need to carry a token or memorize passwords. To summarize, biometrics are potentially more practical, more secure, and legally more binding than traditional methods and thus steadily gain relevance in practice (Albrecht and Probst 2001; Jain and Ross 2007; Pope and Bartmann 2009; van Graevenitz 2006; Weber 2008)

4 BIOMETRIC AUTHENTICATION METHODS

4.1 Application requirements

Biometrics is evaluated as an emerging key technology for authentication, presumably replacing passwords in future. Nevertheless, biometric authentication systems still face several challenges. These are mainly caused by issues of low maturity but also by inherent privacy problems that have to be addressed appropriately at the system level (Pfitzmann 2006; van Graevenitz 2006; Weber 2008).

So far several methods have obtained practical relevance. Each trait or method implies individual advantages and drawbacks. So for practical use a biometric authentication system must satisfy specific demands of the respective application context (Maltoni et al. 2009). Hence, biometric authentication is broadly deployed in the public sector (e.g. passport control, law enforcement) and selectively in the private sector, e.g. for physical AC or the AC to personal devices like personal computers and cell phones. Indeed, in common BP scenarios traditional authentication is still favored over biometric methods (Behrens 2001; Pfitzmann 2006; von Graevenitz 2006).

In common BP scenarios authentication is required for logical AC to protect resources in a network. Workflow participants are usually all kinds of business users interfacing the actual workflow using a standardized personal computer deployed in an office workspace. Furthermore, employees in health care, e.g., might use different work stations for their day-to-day business. In general, a biometric authentication system must satisfy the needs of both the business user and the operating organization (Ried 2004; Weber 2008). From a user's point of view the system must provide appropriate security and comfort (Weber 2008). Low functional performance and perceived risks respecting health and privacy lower the acceptability significantly (Weber 2008). In contrast, organizational requirements are primarily directed by economical considerations. Thus, a biometric authentication system has to be cost-effective, mature, as well as effectively and efficiently deployable within the respective application context (Ried 2004). Analyzing the major challenges mentioned in the literature,² five success factors for biometric authentication systems for BP and hBP environments can be identified:

- **High usability.** Authentication quality as well as low complexity
- **Method security.** Low risk of circumvention or low attack vulnerability
- **Structural flexibility.** Flexible and cost-effective deployment (especially applying for hBP)
- **Scalability.** Ability to maximize the user's comfort according to the required security level
- **Non-Invasiveness.** Use of non-invasive, privacy-friendly and generally accepted methods

In the following, the most common biometric methods of fingerprint, voice, and typing recognition (Pope and Bartmann 2009), are described briefly and evaluated against these success factors.

4.2 Selected methods

Fingerprint recognition. Fingerprints represent the epidermis of a finger which provides unique patterns of ridges and valleys (Maltoni 2008). Those can be digitalized using different kinds of sensors which can be classified by the underlying physical method (Breitenstein 2002). The authentication process is based on the digitalization of the fingerprint and the matching of distinctive patterns (Maltoni 2008). Due to decreasing size and prices as well as to high maturity, fingerprint recognition methods are becoming very popular in various applications (Jain and Ross 2007; van Graevenitz 2006; Weber 2008). Nevertheless, cost-effective sensors dispense with mechanisms for living detection. Since fingerprints are often left behind unknowingly, fake fingers can be fabricated to fool biometric systems (Breitenstein 2002; von Graevenitz 2006). Another major disadvantage is the inherent invasiveness when the template data is stored centrally (Pope and Bartmann 2009). Firstly, fingerprints provide information about possible genetic illnesses (van Graevenitz 2006) and secondly,

² e.g. (Benantar 2006; Olden 2008; Pope and Bartmann 2009; Ried 2004; Smith 2002; van Graevenitz 2006; Weber 2008)

users might fear the misuse of their fingerprints for forensic science. Alternatively, the template can be stored decentralized in a trusted environment of a user's personal device. Indeed, this might restrict the flexibility. The usability of fingerprint recognition systems is theoretically high because the user is mainly required to place a finger at (respectively near) the sensor; in practice though, quality issues, e.g. due to soiled sensor surfaces or wrongly placed fingers, complicate the authentication and reduce the overall usability (Behrens and Heumann 2001). In order to scale security, the resolution of the fingerprint sensor might be enhanced. Indeed, this approach is limited to the available information provided by a specific finger. Alternatively, the number of used fingers can be increased.

Voice recognition. Voice recognition methods can be classified into text-dependent and text-independent ones. For authentication usually text-dependent technologies are used. Therefore, a user is required to speak a specific phrase using a microphone. The system then matches the provided speech pattern to the reference data of the user either applying template-based or statistical models. The distinctiveness of the speaker is established by physiological factors as well as sociolinguistic ones like level of education or dialectal differences. A general advantage of voice-based authentication systems is their ease of use. However, the overall usability correlates with the quality of recognition which is significantly influenced by several factors including sensing conditions (speech channel, speaker's environment), natural fluctuations of the voice characteristics (due to aging, illness etc.), and quality of available training material (González-Rodríguez et al. 2007). As within enterprises a telephone infrastructure is supposed to be available, there are no significant investment costs for input devices. Due to low entry barriers, voice recognition systems (particularly Voice.Trust) are already broadly deployed in password reset applications (Pope and Bartmann 2009). However, according to a survey conducted in a German major bank voice-based methods are not well-accepted by business users. So 80 per cent still prefer to call the helpdesk for password reset instead of using the voice recognition system (Pope and Bartmann 2009). Besides quality issues, perceived risks include the possible determination of illnesses, the discomfort of being recorded or listened to in an open plan office. Hence, voice recordings implicate security problems for text-dependent methods. Recordings can be fabricated for replay attacks or to be shared among users (González-Rodríguez et al. 2007). As the recorded sample is altered using different speech channels, the detection of replay samples is complicated. Voice recognition systems are principally scalable, since the user can be prompted to speak longer phrases (Pope and Bartmann 2009). This directly decreases the FAR.

Typing recognition. Typing recognition is based on the analysis of specific patterns of a user's typing. Analog to voice recognition, it is differentiated between text-dependent and text-independent methods. Whereas methods based on predefined input texts associate the typing behavior to one constant character string, text-independent methods utilize variable text inputs. In that case, authentication is potentially more flexible because any typed input during the user's daily work can continuously be recorded and evaluated in the background. Indeed, since the user is not aware of how his data is processed, that method conflicts with privacy issues. As in addition the performance and usability of text-dependent approaches is potentially higher, such methods are more applicable for common BP authentication scenarios (Bakdi 2007). Many available approaches are limited to the symmetric recognition of pure keystroke dynamics including typing speed and rhythm (Bakdi 2007; Bartmann et al. 2007). Such methods suffer from susceptibility to typing fluctuations e.g. caused by mood or external circumstances (Bartmann et al. 2007). To increase the robustness, advanced methods applying complex statistical models have been developed (Bartmann et al. 2007). One example is a system known as Psylock, based on the work of Bartmann (2000). Using a standard keyboard, Psylock records not only typing speed and rhythms but also statistically more stable characteristics like typing agility, continuity, typical mistakes, incoherent typing, and use of the shift key (Bartmann et al. 2007). Additionally, Psylock provides a mechanism to adapt the reference data to changes of a user's typing over time. This results in significantly increased robustness (Bakdi 2007). The vulnerability of Psylock is evaluated as low. Firstly, the user's typing behavior cannot be recorded or imitated before it is quantified by the sensor. Afterwards, in order to block possible replay attacks e.g. using key loggers, an integrated filter recognizes cloned sample inputs effectively. Another advantage of Psylock is its scalability. As the security directly correlates with the information provided by a specific sample text,

it can be dynamically increased according to the desired security level by scaling length and complexity of a sequence (Pope and Bartmann 2009). To indicate the performance and scalability of Psylock, actual statistics were compared to data collected within the BioP II study conducted by the German Federal Office for Information Security in 2005 (Psylock 2009). At a working point of FAR equals 0.1 %, Psylock with a predefined input text of 42 characters length featured a FRR practically equal to fingerprint recognition. Iris and face recognition perform significantly worse. For voice recognition no accurate data was available to the author. However, the comparison also revealed the significant increase in performance of Psylock doubling the length of the input text; FRR is reduced from 3.3% to 0.8%. Due to high authentication performance and low complexity of the method, Psylock is a highly usable approach. Furthermore, typing recognition does, in contrast to other methods, not conflict with legally implied privacy concerns³ and is thus evaluated as non-invasive (Dotzler 2009). From an organizational point of view the major advantage of typing-based authentication is the fact that no special hardware equipment is needed. As the system is a practically pure software solution it can be deployed and scaled very flexible in common BP application contexts in a very cost-effective way.

4.3 Comparative Evaluation

Table 2. Evaluation of authentication methods (enhancing Pope and Bartmann 2009)

Feature	Method				
	Passwords	Tokens	Fingerprint	Voice	Typing
Non-repudiation	low	low	high	high	high
Method security	low	high	medium	medium	high
Structural flexibility	yes	no	no	depends	yes
Scalability	medium	low	medium	medium	high
Usability	high	medium	medium	medium	high
Non-invasiveness	high	high	low	medium	high

As shown below, text-dependent typing recognition using Psylock is a highly practical way to realize biometric authentication. Compared with other biometric methods, typing ranks best regarding the identified success factors. The results are summarized in Table 2. For a comprehensive comparison password- and token-based authentication is evaluated as well. The security objective non-repudiation is characteristic for biometric authentication and cannot be ensured by isolated password- or token-based methods. Generalized, method and system security is rated highest for tokens and typing. The security of fingerprint and voice recognition systems highly depends on the system design and the specifics of the application context. Since PW- and typing-based authentication is mainly software-based, the deployment is very flexible and cost-effective. Concerning scalability features, typing is rated best. Due to the simplicity and effectiveness of the methods, passwords and typing are most usable. Whereas knowledge-based authentication consumes less time, typing disburdens the user from the restraint of memorizing passwords. Last but not least, typing shows best results concerning the non-invasiveness of biometric features. Concluding, text-dependent typing recognition based on Psylock is considered to be a highly applicable solution for authentication in hBP scenarios. On the one hand, the system is very mature and unsusceptible to sensing quality-related distortions; on the other hand, since typing is generally privacy-friendly, Psylock annuls the most serious point of critique concerning biometric authentication in open systems. Structural flexibility is provided since no special hardware is required. In dynamic business environments the security can be further increased applying multi-factor authentication by combining typing recognition with password-based authentication, or in use cases with an existing infrastructure with token-based authentication.

³ according to German law respectively the national federal data protection act (Bundesdatenschutzgesetz)

5 COMBINING TYPING RECOGNITION AND USAGE CONTROL

For service-oriented hBP authentication based on typing can be enforced centrally in the resource owner's security domain. FIM approaches were evaluated as most qualified in the context of hBP. An implementation for Psylock authentication in federations based on SAML already exists (Psylock 2009). Thus, effective AC of document-centric hBP remains a major problem. As UCON extends the scope of trust of the document owner's security domain, it directly addresses this issue from an AC point of view. In order to enforce strong authentication without constraining structural flexibility a combination of UCON and biometric authentication, based on Psylock, is proposed.

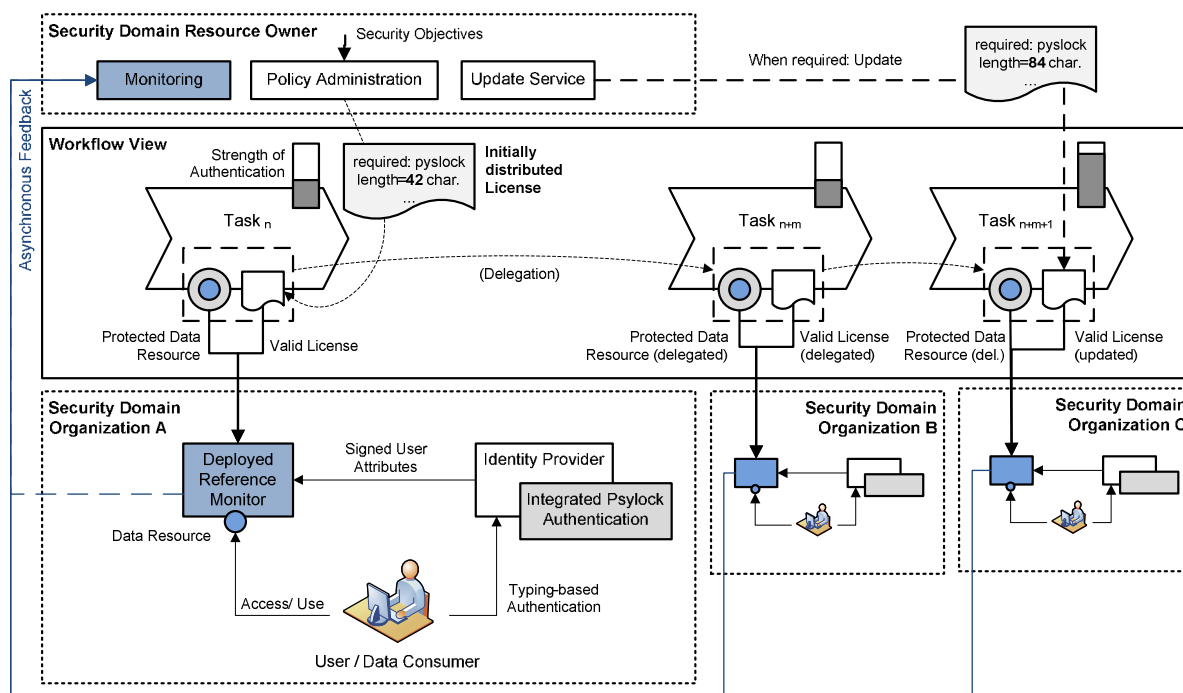


Figure 1. Access control in workflows based on usage control and typing biometrics (simplified)

Document-centric workflows are characterized by data objects passing various security domains where they are accessed by data consumers. As illustrated in Figure 1, each request is intercepted by an RM which is deployed within the user's security domain. If a valid license is available and the authenticated user's action request complies with the license the user will be allowed to access the data object. The enforcement of strong authentication requires the license to specify the authentication method. Respecting data with medium security, the standard Psylock authentication setting (text-dependent, 42 characters) is assumed to be appropriate. The user's IDP must be integrated with Psylock either by running an own authentication component or using a central biometric authentication service (Senk 2009). User attributes like business role and authentication details are provided to the RM. The application of FIM standards enables interoperability. In order to protect the authenticity of the biometric authentication assertion it must be signed by the authenticator. As Psylock is currently being certified by Common Criteria (Psylock 2009), qualified electronic signatures in line with the German Signature Law can be created for users to proof accountability and legal liability of workflow tasks. Within the scope of the available license, users can autonomously redistribute resources (with attached licenses) to other security domains for further (delegated) action. This ensures high flexibility. By enforcing the RM to send feedback information periodically, AC remains transparent. Push or pull mechanisms can be applied for required license updates. For instance, if due to changed content or modified security objectives a resource's security level increases and requires stronger authentication, updated licenses are distributed to relevant RM. These include new authentication rules that enforce e.g. doubled input text length for Psylock authentication for

decreased FAR and increased security. Henceforward, this method is enforced by RM until the license expires or is overwritten.

6 DISCUSSION

The present work examines AC issues of inter-organizational workflows in highly flexible environments (hBP). Applicable approaches are at least partly decentralized. Therefore, the effectiveness of AC inherently depends on trust between the relying parties regarding policy enforcement and authentication. The enforcement of strong authentication with biometrics potentially decreases this dependency and establishes legal security. Typing recognition with Psylock was found to be very practical in this context and can be applied for service-oriented hBP with FIM technologies. Document-centric hBP require additional trust-building measures like implied by UCON. Thus a combined approach was described which explicitly increases control regarding the two identified vulnerabilities by process-wide enforcement of strong authentication and effective AC even for document-centric hBP. As the solution is software-based, flexibility in application and deployment is provided. This approach contrasts with prior work because it explicitly examines the applicability of biometric authentication methods in the context of hBP and introduces a solution that enables the authenticity and legal liability of document-centric actions in inter-organizational hBP.

7 FUTURE WORK

Directions for future research are: (1) the classification of strength of authentication in order to map desired security levels of business resources logically to authentication configurations; (2) the prototypical implementation and practical validation of the proposed model (e.g. in health care); (3) enhancement of the model in order to cover service-oriented workflow scenarios.

References

- Albrecht, A.; Probst, T. (2001). Bedeutung der politischen und rechtlichen Rahmenbedingungen für biometrische Identifikationssysteme. In *Biometrische Identifikation: Grundlagen, Verfahren, Perspektiven.* (Behrens, M. et al. Ed.), 27-54 Vieweg, Wiesbaden.
- Bakdi, I. (2007). Benutzerauthentifizierung anhand des Tippverhaltens bei Verwendung fester Eingabetexte. Dissertation, Regensburg.
- Bartmann, D. (2000). Benutzerauthentisierung durch Analyse des Tippverhaltens mit Hilfe einer Kombination aus statistischen und neuronalen Verfahren. Dissertation, München.
- Bartmann, D.; Bakdi, I.; Achatz, M. (2007). On the Design of an Authentication System Based on Keystroke Dynamics Using a Predefined Input Text, In *International Journal of Information Security and Privacy*, 1(2), 1-12.
- Benatar, M. (2006). *Access Control Systems. Security, Identity Management and Trust Models.* Springer, New York.
- Behrens, M.; Roth, R. (2001). Biometrische Identifikation aus Nutzerperspektive. *Grundlagen, Verfahren, Perspektiven* (Behrens, M. et al. Ed.), 195-220. Vieweg, Wiesbaden.
- Behrens, M.; Heumann, B. (2001). Fingerbilderkennung. In *Biometrische Identifikation: Grundlagen, Verfahren, Perspektiven* (Behrens, M. et al. Ed.), 81-104. Vieweg, Wiesbaden.
- Breitenstein, M. (2002). Überblick über biometrische Verfahren. In *Biometrische Verfahren: Körpermerkmale als Passwort: Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation* (Nolde V. et al. Ed.). 35-82. Deutscher Wirtschaftsdienst, Köln.
- Danwei, C.; Xiuli, H.; Xunyi, R. (2009). Access Control of Cloud Service Based on UCON. In *LCNS 5931*, 559-564. Springer, Berlin.
- Dotzler, F. (2009). *Psylock Password Reset und Datenschutz.* Psylock, Regensburg.
- Ghattas, J.; Soffer, P. (2009). Evaluation of inter-organizational business process solutions: A conceptual model-based approach. In *Information Systems Frontiers*, 11 (3), 273-291.

- González-Rodríguez, J.; Toledano, D.T.; Ortega-García, J. (2009). In Handbook of Biometrics (Jain, A.K. et al. Ed.), 151-170. Springer, New York.
- Haffner, M.; Breu, R. (2009). Security Engineering for Service-Oriented Architectures. Springer, Berlin.
- Hommel, W. (2008). Architektur- und Werkzeugkonzepte für föderiertes Identitäts-Management. Dissertation, München.
- Jain, A.K.; Ross, A. (2007). Introduction to Biometrics. In Handbook of Biometrics (Jain, A.K. et al. Ed.), 1-22. Springer, New York.
- Keromytis, A.D.; Smith, J.M. (2007). Requirements for Scalable Access Control and Security Management Architectures. In ACM Transactions on Internet Technologies 7(4), n.p.
- Lotz, V.; Pigout, E.; Fischer, P.M.; Kossmann, D.; Massacci, F.; Pretschner, A. (2008). Towards Systematic Achievement of Compliance in Service-Oriented Architectures: The MASTER Approach. In Wirtschaftsinformatik 50(5), 383-391.
- Mansfield, A.J.; Wayman, J.L. (2002). Best Practices in Testing and Reporting Performance of Biometric Devices, Version 2.01. http://www.cesg.gov.uk/policy_technologies/biometrics/media/bestpractice.pdf. last access: 2009-09-14.
- Maltoni, D.; Maio, D.; Jain, A.K.; Prabhakar, S. (2009). Handbook of Fingerprint Recognition. 2nd Edition. Springer, London.
- Müller, T. (2008). Trusted Computing Systeme. Konzepte und Anforderungen. Springer, Berlin.
- Nauman et al. (2009). Remote Attestation of Attribute Updates and Information Flows in a UCON System. In 2009, LCNS 55471, 63-80. Springer, Berlin.
- OASIS (2005). XACML Version 2.0. http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-core-spec-os.pdf. last access: 2010-01-12.
- Olden, M. (2008). Biometric Authentication and Authorization Infrastructures. Dissertation, Regensburg.
- Opplinger, R. (2002). Internet and Intranet Security. 2nd Edition. Artech House, Boston.
- Park, J.; Sandhu, R. (2004). The UCONABC Usage Control Model. In ACM Transactions on Information and System Security 7(1). 128-173.
- Pfitzmann, A. (2006). Biometrie: wie einsetzen und wie keinesfalls. In Informatik Spektrum 29(5), 353-356.
- Pütz, C.; Wagner, D.; Ferstl, O.K.; Sinz, E.J. (2009). Geschäftsprozesse in Medizinischen Versorgungszentren und ihre Flexibilitätsanforderungen. Forflex, Bamberg.
- Pope, J.A.; Bartmann, D. (2009). Securing On-Line Transactions with Biometric Methods. In International Journal of Electronic Marketing and Retailing 2(5), n.p.
- Pretschner, A.; Hilty, M.; Basin, D. (2006). Distributed usage control. In Communications of the ACM 49(9), 39-44.
- Psylock (2009). Comparison of Psylock with BioPII, Psylock GmbH (internal), Regensburg.
- Reiser, H. (2008). Ein Framework für föderiertes Sicherheitsmanagement. Habilitation, München.
- Ried, P. (2004). Biometrics for Network Security. Prentice-Hall, Upper Saddle River.
- Schläger, C. (2008). Attribute-based Infrastructures for Authentication and Authorization. EUL, Lohmar.
- Senk C. (2009). Biometrie im Kontext hochflexibler Geschäftsprozesse. Forflex, Bamberg.
- Smith, R.E. (2002). Authentication: From Passwords to Public Keys. Addison-Wesley, Amsterdam.
- St. Clair, L.; Johansen, L.; Enck, W.; Pirretti, M.; Traynor, P.; McDaniel, Patrick-Jaeger, T. (2006) Password Exhaustion: Predicting the End of Password Usefulness. In LNCS 432, (Bagchi, A. and Atluri, V. Ed.), 37-55. Springer, Heidelberg.
- Von Graevenitz, G. (2006). Erfolgskriterien und Absatzchancen biometrischer Identifikationssysteme. LIT, Berlin.
- Weber, M. (2008). Akzeptanz biometrischer Authentifizierungssysteme. Dissertation, Mannheim.
- Workflow Management Coalition (1999). Terminology & Glossary. WFMC, Winchester.
- Zhang, X. and Seifert, J.P. (2008). Security Enforcement Model for Distributed Usage Control. In IEEE International Conference on Sensor Networks, Ubiquitous, Trustworthy Computing, 10-18.