Authentication Systems for Securing Clinical Documentation Workflows
A Systematic Literature Review

J. Schwartze¹; B. Haarbrandt¹; D. Fortmeier²; R. Haux¹; C. Seidel¹

¹Peter L. Reichertz Institute for Medical Informatics, University of Braunschweig – Institute of Technology and Hannover Medical School, Braunschweig, Germany;
²University of Luebeck, Institute of Medical Informatics, Luebeck, Germany;
³Medical Center Braunschweig, Department for Information Technology and Business Development, Braunschweig, Germany

Keywords
Security, digital signature, electronic signature, authentication system

Summary
Context: Integration of electronic signatures embedded in health care processes in Germany challenges health care service and supply facilities. The suitability of the signature level of an eligible authentication procedure is confirmed for a large part of documents in clinical practice. However, the concrete design of such a procedure remains unclear.

Objective: To create a summary of usable user authentication systems suitable for clinical workflows.

Data Source: A Systematic literature review based on nine online bibliographic databases. Search keywords included authentication, access control, information systems, information security and biometrics with terms user authentication, user identification and login in title or abstract. Searches were run between 7 and 12 September 2011. Relevant conference proceedings were searched manually in February 2013. Backward reference search of selected results was done.

Selection: Only publications fully describing authentication systems used or usable were included. Algorithms or purely theoretical concepts were excluded. Three authors did selection independently.

Data Extraction and Assessment: Semi-structured extraction of system characteristics was done by the main author. Identified procedures were assessed for security and fulfillment of relevant laws and guidelines as well as for applicability. Suitability for clinical workflows was derived from the assessments using a weighted sum proposed by Bonneau.

Results: Of 7575 citations retrieved, 55 publications meet our inclusion criteria. They describe 48 different authentication systems; 39 were biometric and nine graphical password systems. Assessment of authentication systems showed high error rates above European CENELEC standards and a lack of applicability of biometric systems. Graphical passwords did not add overall value compared to conventional passwords. Continuous authentication can add an additional layer of safety. Only few systems are suitable partially or entirely for use in clinical processes.

Conclusions: Suitability strongly depends on national or institutional requirements. Four authentication systems seem to fulfill requirements of authentication procedures for clinical workflows. Research is needed in the area of continuous authentication with biometric methods. A proper authentication system should combine all factors of authentication implementing and connecting secure individual measures.

Correspondence to:
Jonas Schwartze, M.Sc.
Peter L. Reichertz Institute for Medical Informatics
Technische Universität Braunschweig
and Hannover Medical School
Mühlenfeldstraße 23
38106 Braunschweig
Germany
E-mail: Jonas.Schwartze@plri.de

Methods Inf Med 2014; 53: 3–13
do: 10.3414/ME12-01-0078
received: August 23, 2012
accepted: September 12, 2013
prepublished: November 19, 2013

1. Integration of Electronic Signatures
1.1 Rationale
Integration of electronic signatures and timestamps to secure clinical archiving and documentation processes challenges German health care providers [1–4]. The signature law (SigG) [5] and the signature decree (SigV) [6] are defining frameworks. Specifications and action-oriented guidelines are in development to close the gap between law and application. An example represents the work of the Competence Center for Electronic Signatures in Healthcare (CCESigG). With its introductory “recommendations for use of electronic signatures and timestamps in health care facilities” [7], CCESigG gives an overview of the legally defined stages of the signa-
tation of the user by creating a biometric template.
2. Determine and verify the identity by comparing the template to the current dataset.

A key point is the reduction of error rates, i.e. rate of false accepted impostors (FAR) and rate of false rejected genuine users (FRR). The combination of these failures is called equal error rate (EER). It is calculated by adjusting the classification threshold such that FAR = FRR and provides a tool to compare authentication system performance in terms of accuracy [14].

Authentication of users can be divided into two groups. While conventional authentication systems verify identity of users only at the beginning of a workflow or session, continuous authentication systems are checking constantly. The source biometric signal has to be available constantly as it is possible by evaluating keyboard typing characteristics first presented by Spillane [61].

The European Committee for Electrotechnical Standardization released a standard for access-control systems demanding an FAR of less than 0.001% and an FRR of 1% [62]. Various studies compare existing biometric methods [63–68] showing that iris recognition and some keystroke verifiers are able to meet these requirements. As a component of the eligible authentication procedure, proposed by the CCE-SigG, the authentication to health care software application components has to meet requirements not covered by these reviews.

1.2 Objectives

The term “eligibility authentication procedure” is either not at all or insufficiently specified by the corresponding laws or regulations. Besides requirement for integrity preserving measures [7], usage of state of the art technologies [16] and a secure signature creating device [5, 6, 17] no technical specifications or guidelines exist. The concrete design of an eligible authentication procedure, especially of the involved authentication method, is unknown. The suitability of potentially usable procedures is not sufficiently investigated regarding the German legal frameworks and the needs of health care environments.

Therefore, we created a summary of usable authentication systems composed of an authentication method to an application component and respective physical data processing components. To identify systems suitable for clinical workflows, we assessed selected methods regarding safety and fulfillment of German regulations as well as general applicability.

2. Methods

2.1 Systematic Review

We specified the methods for identifying usable authentication systems in advance. The selection and extraction process were documented by protocols including time of search, search term used and the results as BibTeX exports.

We defined elgibly criteria. Publications of interest are explicit descriptions of systems used or usable and evaluation studies on these systems. Pure algorithm descriptions or theoretical concepts were excluded.

The search has been done with nine electronic literature databases MEDLINE (Pubmed), IEEEeXplore, ScienceDirect (Elsevier), Thomson Reuters (Web of Knowledge), ACM, Wiley, SciVerse Scopus, CoRR and CiteSeerX. A general search term has been iteratively defined using IEEEeXplore. Therefore, a set of index terms has been conducted by initially searching for the keywords “authentication; user identification; login” and successively adding suitable index terms of the first 100 results. This process has been repeated until no new index terms appeared. The result set built by searching with these index terms has been limited by keywords of unwanted domains identified by iteratively scanning the first 100 results. “Current” has been interpreted as publications after 2005. The resulting general search term can be seen in Figure 1.

For MEDLINE index terms have been translated into adjacent MeSH terms. Time limits in IEEEeXplore, ACM, Reuters and Wiley could not be integrated into the search term and had to be set afterwards. Searches were run between September 7 and 12, 2011. Additionally the IEEE Symposium on Security and Privacy 2005 to 2012, the ACM CCS, SACMAT, AISACCS and CODASPY as well as the USENIX Security Symposium, USENIX HotSec and HealthSec were searched through manually.

The results have been examined by three reviewers (J. S., B. H. and D. F.). Differences were discussed to reach a consensus. The same three reviewers independently examined the abstracts and full text articles, where again disagreements were solved by discussion. On the identified set a two-stage backward literature search was performed.

For summarizing identified systems a one-page data extraction table has been developed. It was structure into sections containing:

1. General information about the authentication method like type, factor(s) used and a short description.
2. The application scenarios with the location, period of time and the environment (like evaluation studies) and
3. Given valuations of the system presented like error rates or advantages and disadvantages.

Data extraction has been done by the main author only.

2.2 Evaluation of Systems

To assess the suitability of the identified systems the following literature has been analyzed.
1. Recommendations for application of electronic signatures and timestamps in health care facilities by the CCESigG [7].
2. Technical guidelines and publications of the Federal Office for Information Security (BSI), in particular the “IT-Grundschutz”-catalogs [16, 18].
3. Technical guidelines and reports of the International Civil Aviation Organization (ICAO), especially publications to security measures at border controls.

Bonneau et al. propose a comprehensive methodology for benchmarking web authentication proposals [69]. Evaluation is categorized into security (S), usability (U) and deployability (D). Criteria relevant for clinical environments have been integrated into our assessment methodology.

2.2.1 Security and Legal Compliance

Conditions prescribed by law can be extracted directly out of the SigG and SigV. 1. The identity is ascertainable and verifiable without a doubt. This follows from §15 Para 2 No. 1b SigV [6].
2. The signature creation device is “safe” in sense of § 2 No. 10 SigG [5].

These are essential prerequisites fulfilled obviously by all authentication systems. More general regulations mainly focus on security. Therefore security and compliance with legal requirements is assessed combined by the following points.
1. Handling of passwords is BSI-compliant according to their rules for password use. [18, M2.11 – p1175] This covers resilience to throttled and unthrottled guessing (S3 and S4 of [69]).
2. Measures for a secure login are applied. [18, M4.15 – p2550] This includes physical access restrictions and covers physical observation prevention (S1 of [69]).
3. Biometric methods used have low error rates. [18, M1.73 – p1137] More specifically an FAR of < 0.001% and an FRR of < 1% according to EN-50133-1 [62].
4. Target Impersonation is not possible (S2 of [69]).
5. Private data, in particular access to biometric templates, is additionally secured. [58, 59] Especially an unwanted evaluation of authentication features is prevented (S10 of [69]).
6. If physical tokens are involved, they can not be stolen or are protected by a PIN (S4 of [69]).

The assessment always regards the complete system. If multi factor authentication is used and one unsecure factor breaks the others, the whole system is regarded as unsecure.

Figure 1 General search term

2.2.2 Applicability

Applicability of an authentication system is derived from requirements to users and general costs of integration (deployability). A properly implemented system using username and password serves as reference value. Regarding usability, U1 and U4 to U7 of the evaluation framework by Bonneau et al. [69] have been assessed. For U7 (Infrequent-Errors) biometric approaches with an FRR less than or equal 1% are rated with two points, assuming that one failed of 100 login attempts is reasonable. FRRs between 1% and 10% received one point and greater than 10% no points accordingly. Deployability has been evaluated by D2, D5 and D6.

U2 is not relevant since we are regarding a single clinical environment with only one authentication solution. U3 is not relevant since tokens are limited to the working environment. U8 is explicitly unwanted due to security reasons. D1 addresses accessibility, which is generally set by the working environment. D3 and D4 are not relevant since all client and server software components are under full control of the clinical administration and have to be adjusted for all systems.
2.2.3 Suitability for Use in Clinical Practice

The eligible authentication procedure is intended to be used as security measure in clinical documentation processes. An evaluation regarding the suitability for this purpose is based on criteria analyzed before. Some requirements are more significant than others. While security in general is crucial, efficiency in use (U6) and negligible cost per user (D2) are important for usability and deployability in clinical environments. As proposed in [69] a weighted sum over all assessment values is calculated taking mentioned requirements into account via selected weights.

3. Results

The database search provided a basic set of 7575 publications. After removing all duplicates and faulty entries a cleared set of 4115 publications remained. A total of 232 abstracts showed relevance and were retrieved in full text (all accessible). After discussion of six disagreements, 39 publications were selected describing 32 different systems. In five cases two or three publications focused on the same system. The manual conference search resulted in seven additional publications. Backwards searching the references of all 46 citations revealed nine additional publications meeting the inclusion criteria. Overall 55 papers describing 48 systems were analyzed. A respective flow diagram shows Figure 1.

3.1 Authentication Systems Overview

3.1.1 Conventional Authentication

Initial identification and verification of the user can be supported by a number of features. Biometric authentication is the predominant factor, but is sometimes supported by possession like an RFID token, which stores biometric templates. Knowledge-based authentication is primarily done with graphical passwords but sometimes also combined with biometric features like typing characteristics of passwords.

Many authentication procedures determine identity by characteristics of facial images. Recent developments in this field focused mainly on reduction of error rates by introducing new ways of image acquisition. Using three-dimensional images [19–21] or special mathematical approaches like the Eigenface algorithm [22] can improve recognition rate. Precision of nearly 100% is possible by combining more images and additional factors as fingerprint [23]. Privacy is especially addressed by a system called SciFi from Osadchy et al. [71] capable of secure computing face recognition.

Focusing on iris recognition, several improvements have been proposed. While Daugman further developed his original scheme by improving several calculation and selection aspects [72], Si et al. [73] primarily improved indexing methods to speed calculation. An overview and combination of iris matching algorithms is given by Ajay et al. [74]. A near perfect recognition rate is reached by a system proposed by Monro et al. [76].

Eliminating special sensor requirements can enhance deployability. Regarding this, Hiew et al. propose a system with an off-the-shelf digital camera [24], while Savic et al. used a document scanner [26]. Analysis of additional features can drastically decrease error rates. Use of whole hand images allows extraction of the knuckle region [25], palmar surface [26] or hand geometry and skin color [27]. Further, Sun et al. showed suitability of finger vein patterns as biometric feature [28]. Most finger and hand based systems reach EER near or below 0.5%.

Other than physiological characteristics, behavioral based systems are in earlier development stage. Keyboard handling approaches extract i.e. keystroke timings, correction behavior and overall typing speed. Increased discernibility of users is achieved by use of the standard username-password combination [77], long texts with about 150 signs [29], predefined typing rhythms [30, 31] or an additional RFID token [32]. Error rates are extremely different, where best results are reached by a special pressure sensor enhanced keyboard [33–35] and the rhythm based approach of Fang et al. [30].

As a second major input device, mice offer features usable for user identification and verification. All identified systems utilize static challenges like clicking points on screen [36], navigating through a maze [37] or clicking special rhythms [38] to collect movement and keystroke information. Combination with additional features is done by Hamdy et al. [39], who tried to measure short-term memory and perceptual capabilities. However, all mouse-based systems show high error rates.

A different approach of authenticating users is shown by El-Bendary et al. [40] who use sounds of the beating heart. Though the signal is very hard to reproduce error rates are too high. The approach is quite invasive and needs to be seen as proof of concept.

Graphical passwords are a kind of knowledge-based authentication. The challenge is to recognize or recall a single or a sequence of images. With the contextual information of images as hints, a better memorability is aspired. Security enhancement is addressed by adding descriptions to special image points [11], using unclear images [41] or unique image sequences [42], as well as biographic information [43]. A unique set of selectable images is created by the system of Van-Oorschot et al. [44, 45] determined by the username. This allows mutual authentication. Special requirements like prevention from shoulder surfing are also addressed both for graphical passwords [46] and conventional PINs [85].

In addition to select predefined images there are systems which demand users to create their own image, scribble or signature and recall it at login time. Two possible implementations are shown by Oka and Weiss et al. [46, 47] which demand the user to scribble a simple image. User determination and verification is done by extraction of edge directions. Despite error rates of 2%, Oka et al. could not show significantly better memorability compared to alphanumeric passwords. Using own signature, no memorability requirements are set, but Maiorana et al. [60] could not show adequate error rates. Moreover, all scribble based procedures have partly three times longer logins compared to alphanumeric passwords (46 p 7).
3.1.2 Continuous Authentication

To make a steadily reliable statement about the users’ authenticity a continuous analysis of data is required. All identified systems of this kind are working with biometric features, since they are continuously available. If a proper initial authentication is achieved continuous systems are able to maintain authentication status as shows by a single-sign-on solution from Mustafiæ et al. [78].

Various systems are using mouse dynamics for user recognition and verification [79–84]. Jagadeesan et al. [15] combined mouse movements and keyboard typing behavior. Error rates are sufficient for continuous authentication. In two publications, Yap and Kumar et al. [49, 50] used a facial image and fingerprints to continuously secure a computer system on operating system level.

Systems authenticating users conventionally based on iris images have been noted earlier. By combining this approach with an eye-tracker Mock et al. [75] created a continuous authentication system. In addition to characteristics not or hardly changeable, soft biometrics can be used to monitor authenticity of a user. Cloth, skin color and basic face proportions do usually not change during a session. Niinuma et al. [12, 51] and Dantcheva et al. [70] published a system that uses these particular features. A system based on sound absorption of the human head are showing Rodwell et al. [52]. The system, called “HAT”, records two sound signals, one at the larynx and one at the ear. Differences between them are used to identify persons.

3.1.3 Hybrid Authentication

The only system intended to provide initial as well as continuous authentication is part of the HUMABIO project and in prototype stage [53–55]. It consists of a seat or chair enhanced by 28 piezoresistive sensor strains [56]. Determination of identity and even gesture recognition is possible in both cars [55] and office environments [57] by analyzing pressure pattern changing in time, position and strength.

3.2 Assessment Results

Most conventional authentication systems try to address the memorability issue of passwords by either helping to recall knowledge or completely remove cognitive requirements by using biometrics as authentication factor. The limitation of continuous systems to biometrics emphasizes criteria like low error rates and privacy robustness.

3.2.1 Security and Legal Compliance

Password handling according to BSI rules and resilience to guessing is mostly not an issue. Systems allowing creation of small entropy passwords, like small scribbles, are downgraded. A BSI compliant secure login includes observation prevention, which most (graphical) password based schemes did not offer. CENELEC compliant error rates are only an issue of pure biometric systems of which only four fulfilled this requirement. Two systems combined password and typing characteristics making error rates only an issue of the usability criteria infrequency of errors. Target impersonation is possible in personal knowledge related systems and those using soft biometrics. Privacy and authentication with consent is only addressed by three biometric systems. All image-based methods have the ability to authenticate a user without consent. Respective reductions have been made. Theft prevention is applicable for systems demanding physical presence of a token but also for biometrics using body characteristics and biometric templates that can be stolen.

3.2.2 Applicability

Biometrics are all memorywise-effortless if not combined with a knowledge based factor. Graphical passwords try to address this weakness but are rarely able to show better memorability. Physical effortlessness kind of inverts the security need or authentication only with consent. Here only systems solely using camera images or special biometric features offer additional value. However, some approaches reduce effort to only scanning a finger or an eye and are rated accordingly. If physical effort is necessary and memorywise effort is reduced, mostly a new authentication technique has to be learned. How easy to learn, can be assessed by the number of successful login attempts. Only five systems have minor drawbacks regarding this criterion. Efficiency to use is no issue for biometric systems including continuous authentication. All knowledge-based procedures require more time or effort than simply typing a password. Infrequency of errors for biometric systems was directly related to error rates of the security assessment and thus mirrored these results. All knowledge-based methods and biometric systems using existing hardware had negligible costs per user. Some approaches only required a simple web-cam or a cheap RFID token and therefore received a small deduction. Almost all assessed systems are in (early) development stage. Only four systems using either well known factors or are evaluated under real environments can be regarded as mature. However, iris and face images are generally well researched but specific implementations are not tested under real-world conditions. Despite two systems, which invented a specific, not further described sensor, all methods were non-proprietary.

3.2.3 Suitability for Use in Clinical Practice

Clinical environments have special requirements, which are addressed by a weighted sum of all assessment criteria. Most important is security, especially low error rates of biometric procedures. The respective security criteria are ranked highest. Password handling and a secure login with observation prevention are addressed by rules of conduct or existing physical access restrictions. For a productive clinical environment efficiency and economy is crucial. Therefore, the respective criteria U6 and D2 are weighted heavier. For maximized user satisfaction, privacy and improvement of the current situation using username and password, the usability criteria U1 and U5 as well as the security criterion privacy and authentication with consent are ranked higher.

Results of the assessment show that no conventional system is able to reach the
### Table 1  Assessment of conventional authentication systems

<table>
<thead>
<tr>
<th>System</th>
<th>Type</th>
<th>Factor</th>
<th>Reference</th>
<th>Security and legal compliance</th>
<th>Applicability</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Password handling, resilience to guessing (S3/S4)</td>
<td>U1 Memory-wise-Effortless</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>BSI “Secure Login” including observation prevention</td>
<td>U2 Physically-Effortless</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>target impersonation-impossible (S2)</td>
<td>U3 Easy-to-Learn</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>privacy of biometric template and authentication (S10)</td>
<td>U4 Inefficient-Errors</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>theft prevention (S4)</td>
<td>U5 Negligible-Cost-per-User</td>
</tr>
<tr>
<td>Username and password</td>
<td>k</td>
<td></td>
<td></td>
<td>+</td>
<td>18  28 61% 70%</td>
</tr>
<tr>
<td>Alphanumeric and graphical password</td>
<td>k</td>
<td>[44]</td>
<td></td>
<td>+</td>
<td>18  28 61% 70%</td>
</tr>
<tr>
<td>Face recognition</td>
<td>b f</td>
<td>[71]</td>
<td></td>
<td>+</td>
<td>18  28 61% 70%</td>
</tr>
<tr>
<td>Iris recognition</td>
<td>b i</td>
<td>[76]</td>
<td></td>
<td>+</td>
<td>18  28 61% 70%</td>
</tr>
<tr>
<td>PIN with cognitive trapdoor</td>
<td>k</td>
<td>[85]</td>
<td></td>
<td>+</td>
<td>18  28 61% 70%</td>
</tr>
<tr>
<td>Graphical passwords</td>
<td>k</td>
<td>[11]</td>
<td></td>
<td>+</td>
<td>18  28 61% 70%</td>
</tr>
<tr>
<td>Graphical password</td>
<td>k</td>
<td>[42]</td>
<td></td>
<td>+</td>
<td>18  28 61% 70%</td>
</tr>
<tr>
<td>Graphical password (blurred images)</td>
<td>k</td>
<td>[41]</td>
<td></td>
<td>+</td>
<td>18  28 61% 70%</td>
</tr>
<tr>
<td>Fingerprint recognition</td>
<td>b h</td>
<td>[24]</td>
<td></td>
<td>+</td>
<td>18  28 61% 70%</td>
</tr>
<tr>
<td>3D face and hand recognition</td>
<td>b k</td>
<td>[19]</td>
<td></td>
<td>+</td>
<td>18  28 61% 70%</td>
</tr>
<tr>
<td>Keystroke dynamics for password</td>
<td>b k</td>
<td>[30]</td>
<td></td>
<td>+</td>
<td>18  28 61% 70%</td>
</tr>
<tr>
<td>Polyline password</td>
<td>k</td>
<td>[48]</td>
<td></td>
<td>+</td>
<td>18  28 61% 70%</td>
</tr>
<tr>
<td>Graphical password (haptic feedback)</td>
<td>k</td>
<td>[46]</td>
<td></td>
<td>+</td>
<td>18  28 61% 70%</td>
</tr>
<tr>
<td>Finger vein scan</td>
<td>b h</td>
<td>[28]</td>
<td></td>
<td>+</td>
<td>18  28 61% 70%</td>
</tr>
<tr>
<td>Face recognition</td>
<td>b f</td>
<td>[22]</td>
<td></td>
<td>+</td>
<td>18  28 61% 70%</td>
</tr>
<tr>
<td>Iris recognition</td>
<td>b i</td>
<td>[73]</td>
<td></td>
<td>+</td>
<td>18  28 61% 70%</td>
</tr>
<tr>
<td>Iris recognition</td>
<td>b i</td>
<td>[72]</td>
<td></td>
<td>+</td>
<td>18  28 61% 70%</td>
</tr>
<tr>
<td>Iris recognition</td>
<td>b i</td>
<td>[74]</td>
<td></td>
<td>+</td>
<td>18  28 61% 70%</td>
</tr>
<tr>
<td>Graphical password (personal inform.)</td>
<td>k</td>
<td>[43]</td>
<td></td>
<td>+</td>
<td>18  28 61% 70%</td>
</tr>
<tr>
<td>Finger back and hand geometry</td>
<td>b h</td>
<td>[25]</td>
<td></td>
<td>+</td>
<td>18  28 61% 70%</td>
</tr>
<tr>
<td>Signature</td>
<td>b o</td>
<td>[60]</td>
<td></td>
<td>+</td>
<td>18  28 61% 70%</td>
</tr>
<tr>
<td>Active mouse dynamics</td>
<td>b m</td>
<td>[36]</td>
<td></td>
<td>+</td>
<td>18  28 61% 70%</td>
</tr>
<tr>
<td>Heart sounds</td>
<td>b o</td>
<td>[40]</td>
<td></td>
<td>+</td>
<td>18  28 61% 70%</td>
</tr>
</tbody>
</table>
The integration of the eligible authentication procedure. Not only as sole signature procedure but also as part of all electronic signature stages – in all areas. Appropriate authentication of users is crucial for border controls, juristic documentation and even personal use. Particularly in clinical documentation processes securing all computer based application components is essential.

Among the considered publications, 39 were descriptions of biometric procedures, which is a share of 70%. One explanation on this is a high relevance of this topic. Knowledge and possession based procedures are largely described and demand only marginal improvements. Optimization in memorability of passwords is one example. Nine other systems, being graphical passwords, emphasize this. Biometrics, on the other hand, are still mostly uncertain which gives more opportunity for research and refinement leading to more publications about this topic.

Almost all systems are in prototype or testing stage. Since current systems were focused explicitly, this has been expected. Direction of research is shown even more clearly.

4.1 User Name and Password

The assessment of all identified authentication systems showed, that passwords are superior to all other authentication mechanisms. However, some biometric systems are able to provide more security but momentarily have drawbacks in privacy and usability. Especially adding biometric authentication on top of existing username and password schemes could provide a more secure initial login, if error rates are reduced satisfactorily and privacy preserving measures are applied. Continuous authentication systems are currently not used in practical but could address issues especially important for clinical environments.

4.2 Focusing Clinical Requirements

Login sessions for application components in clinical environments are currently handled like “one login per working day”. Neither unintentionally forgetting to log out nor intended use of another account is actively prevented. This gains importance especially for electronically signed clinical
documentation processes since a constantly assuring eligibility of the current user is crucial. Regarding the assessment results, only few continuous authentication systems are able to meet these requirements. Since the weighted sum primarily focused on security and economics in comparison to passwords continuous approaches may lose out. Main focus is adding security to a currently unsecured part of the workflows, so even small improvements are desirable. Weighting respective criteria like infrequency of errors or efficiency and redefine physically effortless to “effort to be done additionally to regular user tasks”, would lead to four systems being rated 80% or more [12, 15, 80, 83]. If developed further with regards to privacy and error rates they would be a suitable solution (Table 3).

Although the assessment criteria combined with the weighted sum allowed identification of the best systems for clinical use, different weights do apply for different health care environments. In Germany adding constant camera surveillance to a software system is unacceptable, especially in clinical environments. The assessment on the other hand, showed a camera system to be the best continuous

<table>
<thead>
<tr>
<th>System</th>
<th>Type</th>
<th>Factor</th>
<th>Reference</th>
<th>Security and legal compliance</th>
<th>Applicability</th>
<th>Weighted Sum</th>
<th>Percentage of maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>soft biometrics</td>
<td>b</td>
<td>x</td>
<td>[12, 51]</td>
<td>+</td>
<td>+</td>
<td>21</td>
<td>37</td>
</tr>
<tr>
<td>mouse dynamics</td>
<td>b</td>
<td>m</td>
<td>[83]</td>
<td>+</td>
<td>+</td>
<td>20</td>
<td>32</td>
</tr>
<tr>
<td>keystroke dynamics for SSO</td>
<td>b</td>
<td>k</td>
<td>[78]</td>
<td>+</td>
<td>+</td>
<td>19</td>
<td>30</td>
</tr>
<tr>
<td>mouse dynamics (multiple extractors)</td>
<td>b</td>
<td>m</td>
<td>[80]</td>
<td>+</td>
<td>+</td>
<td>19</td>
<td>29</td>
</tr>
<tr>
<td>keystroke and mouse dynamics</td>
<td>b</td>
<td>x</td>
<td>[15]</td>
<td>+</td>
<td>+</td>
<td>19</td>
<td>29</td>
</tr>
<tr>
<td>keystroke pressure sensor</td>
<td>b</td>
<td>k</td>
<td>[33–35]</td>
<td>+</td>
<td>+</td>
<td>18</td>
<td>30</td>
</tr>
<tr>
<td>mouse dynamics</td>
<td>b</td>
<td>m</td>
<td>[37]</td>
<td>+</td>
<td>+</td>
<td>18</td>
<td>29</td>
</tr>
<tr>
<td>keystroke dynamics and RFID</td>
<td>b</td>
<td>k</td>
<td>[32]</td>
<td>+</td>
<td>+</td>
<td>18</td>
<td>29</td>
</tr>
<tr>
<td>mouse dynamics</td>
<td>b</td>
<td>m</td>
<td>[81]</td>
<td>+</td>
<td>+</td>
<td>18</td>
<td>28</td>
</tr>
<tr>
<td>sensor seat</td>
<td>b</td>
<td>o</td>
<td>[55, 57]</td>
<td>+</td>
<td>+</td>
<td>18</td>
<td>26</td>
</tr>
<tr>
<td>Head Authentication Technique</td>
<td>b</td>
<td>o</td>
<td>[52]</td>
<td>+</td>
<td>+</td>
<td>18</td>
<td>24</td>
</tr>
<tr>
<td>soft biometrics</td>
<td>b</td>
<td>x</td>
<td>[70]</td>
<td>+</td>
<td>+</td>
<td>17</td>
<td>27</td>
</tr>
<tr>
<td>keystroke dynamics</td>
<td>b</td>
<td>k</td>
<td>[29]</td>
<td>+</td>
<td>+</td>
<td>17</td>
<td>27</td>
</tr>
<tr>
<td>mouse dynamics</td>
<td>b</td>
<td>m</td>
<td>[82]</td>
<td>+</td>
<td>+</td>
<td>17</td>
<td>27</td>
</tr>
<tr>
<td>face and fingerprint recognition</td>
<td>b</td>
<td>x</td>
<td>[49, 50]</td>
<td>+</td>
<td>+</td>
<td>17</td>
<td>26</td>
</tr>
<tr>
<td>iris recognition</td>
<td>b</td>
<td>i</td>
<td>[75]</td>
<td>+</td>
<td>+</td>
<td>15</td>
<td>23</td>
</tr>
</tbody>
</table>

Methods Inf Med 1/2014 © Schattauer 2014
authentication system for clinical use because all other criteria are ranked high. Defining not only weights but also exclusion criteria would solve this issue. Regarding the only average score of the other systems none of these are sufficient for the strict requirements of clinical use.

### 4.3 Limitations

Most of the publications focusing on authentication are schemes, algorithms or improvements for specific schemes. Therefore, the given search term had to be very restrictive eventually missing publications of interest. Of 16 additionally identified publications most recent keyword were "biometrics" (10) and "humans" (4), which were covered as index terms but not as keywords in document titles. A query on IEEEExplore (2013-11-02, 1pm) with "biometrics" returned 3238 results, which are 1022 (31.56%) results more than a query without "biometrics": Regarding the overall precision of 0.51% (without manual conference scan) we can estimate a miss of 12 publications of the projected base set of 9966 results (131.56% of 7575).

We strongly focused on implemented, evaluated and usable systems from the security point of view. This could have lead to a selection bias since publications may have no clear description of the invented system. We detected significant variety in the evaluations of systems assessed. Often only a small number of users were included and no information on how results were calculated were given. Beyond this, no formalized analyzes for risk of bias had been calculated.

Clinical requirements are extremely different. Assessment for suitability was mainly based on experiences in German institutions.

### 5. Conclusion and Future Work

We gave an overview of possible authentication systems. Identified systems have been evaluated showing suitability of few. In particular, no conventional authentication system was able to reach a security and applicability level of the username-password-combination. Continuous systems could add value to currently unsecured workflows. Therefore, the need for further research arises. Subject of future research could be design and practical implementation of a system suitable for use in clinical workflows. Besides that, application throughout the clinic and across is imaginable. Even apart from health care, securing documentation is essential. Abstraction to all fields of computer-aided documentation seems possible. An appropriate evaluation could finally scientifically underpin an increase of value of evidence of relevant data and documents.

### Acknowledgments

We would like to thank all people who contributed to this paper. A special thanks goes to all anonymous reviewers for greatly improving the paper.

### References


© Schattauer 2014


70. Dantcheva A, Dugelay JL. Frontal-to-side face re-identification based on hair skin and clothes patches. In: 8th IEEE International Conference on Advanced Video and Signal-Based Surveillance (AVSS); Aug 30 – Sep 2, 2011; Klagenfurt, Austria. pp 309–313.


© Schattauer 2014 Methods Inf Med 1/2014